

Principles of Cybersecurity



Principles of Cybersecurity

Principles of Cybersecurity

Editor
Joy Crelin

SALEM PRESS
A Division of EBSCO Information Services, Inc.
Ipswich, Massachusetts

GREY HOUSE PUBLISHING

Cover photo: Just_Super/iStock

Copyright © 2024, by Salem Press, A Division of EBSCO Information Services, Inc., and Grey House Publishing, Inc.

Principles of Cybersecurity, published by Grey House Publishing, Inc., Amenia, NY, under exclusive license from EBSCO Information Services, Inc.

All rights reserved. No part of this work may be used or reproduced in any manner whatsoever or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage and retrieval system, without written permission from the copyright owner. For information, contact Grey House Publishing/Salem Press, 4919 Route 22, PO Box 56, Amenia, NY 12501.

∞ The paper used in these volumes conforms to the American National Standard for Permanence of Paper for Printed Library Materials, Z39.48 1992 (R2009).

Publisher's Cataloging-In-Publication Data
(Prepared by Parlew Associates, LLC)

Names: Crelin, Joy, editor.

Title: Principles of cybersecurity / editor, Joy Crelin.

Description: Ipswich, MA : Salem Press, a division of EBSCO Information Services, Inc. ; Amenia, NY : Grey House Publishing, 2024. | Series: [Principles of science]. | Includes bibliographic references and index. | Includes b&w photos and illustrations.

Identifiers: ISBN 9781637007501 (hardback)

Subjects: LCSH: Computer security – Encyclopedias. | Computer networks - Security measures - Encyclopedias. | Computer crimes – Prevention – Encyclopedias. | BISAC: COMPUTERS / Security / General. | COMPUTERS / Security / Network Security. | COMPUTERS / Reference.

Classification: LCC TK5105.59 C74 2024 | DDC 005.803–dc23

FIRST PRINTING
PRINTED IN THE UNITED STATES OF AMERICA

CONTENTS

| | |
|---|-----|
| Publisher's Note | vii |
| Introduction..... | ix |
| Contributors | xv |
| | |
| Aadhaar Hack..... | 1 |
| Access Control..... | 3 |
| Advanced Encryption Standard | 5 |
| Algorithm | 7 |
| Android OS..... | 9 |
| Anonymity and Anonymizers | 11 |
| Anonymous..... | 13 |
| Artificial Intelligence | 17 |
| Artificial Intelligence and Terrorism | 24 |
| Artificial Intelligence Cold War | 27 |
| Autonomous Cars | 31 |
| Big Data | 37 |
| Biometric Identification Systems | 39 |
| Blockchain | 43 |
| Bots..... | 46 |
| Browsers | 49 |
| Cambridge Analytica Facebook Data Scandal .. | 55 |
| Catfishing | 58 |
| Changing Passwords | 61 |
| China's Cyberinvasion | 66 |
| Cloud Computing..... | 69 |
| Combinatorics..... | 71 |
| Computer and Technical Support Specialist | 73 |
| Computer Crime Investigation..... | 76 |
| Computer Fraud | 81 |
| Computer Fraud and Abuse Act | 83 |
| Computer Hardware Engineer..... | 85 |
| Computer Hardware Security..... | 88 |
| Computer Languages, Compilers, and Tools.... | 90 |
| Computer Memory and Storage..... | 94 |
| Computer Network Architect | 96 |
| Computer Networks | 99 |
| Computer Programmer | 104 |
| Computer Security | 106 |
| Computer Software..... | 108 |
| Computer Viruses and Worms | 109 |
| Cryptography | 112 |
| Cyber Command..... | 114 |
| | |
| Cyberbullying | 117 |
| Cybercrime | 121 |
| Cybercrime, Social Impacts of | 124 |
| Cybersecurity Basics | 128 |
| Cybersecurity Testing | 130 |
| Cyberterrorism | 132 |
| Cyberwarfare..... | 136 |
| Cyberweapon | 141 |
| Dark Web | 145 |
| Data Breach | 148 |
| Data Harvesting | 150 |
| Data Mining | 152 |
| Data Protection | 155 |
| Database | 158 |
| Database Design | 160 |
| Debugging | 161 |
| Deepfake..... | 163 |
| Demon Dialing/War Dialing | 167 |
| Device Drivers..... | 169 |
| Digital Forensics | 170 |
| Digital Watermarking | 172 |
| Doxing | 174 |
| E-banking | 179 |
| Electronic Bugs | 181 |
| Electronic Commerce Technology | 183 |
| Email and Business..... | 188 |
| Encryption | 191 |
| End-User Cybersecurity Education..... | 193 |
| Estonia Cyberattack | 195 |
| Fax Machine, Copier, and Printer Analysis..... | 199 |
| Firewalls | 201 |
| Firmware..... | 204 |
| Fuzzy Logic | 205 |
| Graphical User Interface | 209 |
| Hacking..... | 211 |
| HTML..... | 216 |
| HTTP Cookie | 219 |
| Identity Theft | 223 |
| ILOVEYOU Virus | 228 |
| Industrial Espionage..... | 231 |
| Information Security Analyst | 233 |
| Information Technology | 236 |

| | | | |
|---|-----|---|-----|
| Internet of Things | 238 | Russian Hacking Scandal | 307 |
| Internet Protocol..... | 240 | Servers | 313 |
| Internet Tracking and Tracing..... | 241 | Smart City..... | 315 |
| Intrusion Detection and Prevention | 244 | Social Engineering | 318 |
| iOS | 246 | Software Developer/Quality Assurance Analyst/Tester..... | 320 |
| Mac OS | 249 | Spam | 322 |
| Machine Learning | 252 | Spam Filters | 327 |
| Malware..... | 253 | Spyware..... | 329 |
| Marriott Starwood Hotels Hack | 256 | Stuxnet Virus..... | 331 |
| Metadata..... | 258 | Systems Security Engineering..... | 335 |
| Michelangelo Computer Virus | 260 | Targeted Advertising..... | 337 |
| Microprocessor | 261 | Usability | 341 |
| Mobile Apps | 263 | Virtual Private Network | 343 |
| Mobile Web Technology | 265 | Web Developer | 345 |
| Network and Computer Systems Administrator .. | 267 | Windows Operating System | 348 |
| Online Piracy | 271 | Wireless Networks..... | 351 |
| Operating System..... | 273 | Workplace Monitoring | 353 |
| Personal Computers | 277 | XML | 357 |
| Phishing | 280 | Y2K Crisis | 361 |
| Privacy Breaches | 284 | Zero Trust Security | 367 |
| Privacy Rights | 287 | | |
| Privacy Settings..... | 289 | Bibliography | 371 |
| Public-Key Cryptography | 291 | Glossary..... | 403 |
| Random-Access Memory | 295 | Organizations | 407 |
| Ransomware | 297 | Subject Index | 409 |
| Risk Management..... | 300 | | |

PUBLISHER'S NOTE

Cybersecurity is the next volume in Salem's *Principles of Science* series, which includes *Microbiology*, *Energy*, *Marine Science*, *Geology*, *Information Technology*, and *Mathematics*, to name a few.

This new resource explores important aspects of cybersecurity and introduces readers to the history of cybersecurity as well as how it affects government, business, media, and other fields.

Principles of Cybersecurity begins with a comprehensive Editor's Introduction to this important topic written by Joy Crelin. Following the Introduction, this book includes 120+ entries that follow a convenient alphabetical arrangement, making specific topics easy to find.

Cybersecurity is multifaceted, encompassing the protection of computers, mobile devices, networks, websites, cloud services, and other computer and internet-connected technologies from a wide range of cyberattacks. This volume takes a broad view, covering security-enhancing technologies like encryption and zero trust as well as underlying hardware, software, and internet technologies. Topics discussed range from common cyberattacks and cybercrimes, famous computer viruses and hacking incidents, doxing, cyberbullying, and cyberwarfare and

cyberterrorism. *Principles of Cybersecurity* will provide a strong understanding of the importance of cybersecurity in the twenty-first century and the many directions from which security threats can emerge.

Entries begin with a brief Abstract describing the key elements of the article, followed by a Background section and an Overview. All entries end with a helpful Further Reading section.

This work also includes helpful appendices, including:

- Bibliography;
- Glossary;
- Organizations;
- Subject Index.

Salem Press extends appreciation to all involved in the development and production of this work. Names and affiliations of contributors to this work follow the Editor's Introduction.

Principles of Cybersecurity, as well as all Salem Press reference books, is available in print and as an e-book. Please visit www.salempress.com for more information.

INTRODUCTION

DEFINING CYBERSECURITY

The Merriam-Webster dictionary defines the term *cybersecurity* as “measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.” The Oxford English Dictionary (OED) offers a similar definition, describing cybersecurity as “security relating to computer systems or the internet, esp. that intended to protect against viruses or fraud.” Those definitions, and particularly the latter, call attention to the complex and multifaceted nature of cybersecurity, which by the third decade of the twenty-first century had come to encompass the protection of computers, mobile devices, networks, websites, cloud services, and other computer and internet-connected technologies from a wide range of cyberattacks.

This volume takes a broad view of the field of cybersecurity, presenting entries that cover not only technologies and practices used to enhance computer security, such as encryption and the zero trust security model, but also the underlying hardware, software, and internet technologies. Additional entries deal with common cyberattacks and cybercrimes, notable computer viruses and hacking incidents, social issues such as doxing and cyberbullying, and geopolitical topics such as cyberwarfare and cyberterrorism. Designed to provide a strong understanding of the importance of cybersecurity in the twenty-first century and the many directions from which security threats can emerge, this volume likewise features several entries on cybersecurity-related professions that will benefit students or adult career-changers interested in entering this rapidly evolving and increasingly critical field.

HISTORY

While Merriam-Webster states that the term cybersecurity dates back to 1989, and the OED dates the

term to 1990, the concept of cybersecurity—and the awareness of a need for it—dates back quite a bit farther, having arisen alongside the development of computers. A more commonly used term during the early years of cybersecurity was computer security; beginning in 1972, for instance, the US National Bureau of Standards (later known as the National Institute of Standards and Technology, or NIST) became home to a program dedicated specifically to computer security research.

From the early days of computers, efforts to increase the capabilities of computer technology were often accompanied by corresponding attempts to identify vulnerabilities in computer systems and potentially to exploit them, either for malicious purposes, for comedic purposes, or simply out of curiosity. Over the years, the field of cybersecurity was increasingly complicated by the development of new technologies, including the Advanced Research Projects Agency Network (ARPANET) and, eventually, the publicly accessible internet and World Wide Web. The emergence of the latter technologies enabled everyday people to gain access to the internet and communicate with one another regardless of location. That change resulted in countless positive developments, but it also made cybersecurity a more pressing concern. The internet allowed for the rapid spread of viruses and malware, which could at times be obvious to the user and at other times could infect a computer or system without the user’s knowledge. As a result, researchers and technology companies turned their attention toward developing new means of detecting and combating cybersecurity threats, including programs capable of scanning computers for malicious software, firewalls used to filter or block incoming traffic, advanced user-authentication protocols and security models, and many more innovations. Likewise, organizations

increasingly recognized the need to take preventive measures well before a computer system could be compromised. Such measures included penetration testing, a longstanding means of testing computer systems for vulnerabilities, as well as the development of automated systems capable of identifying vulnerabilities to be addressed.

Efforts to monitor and address cybersecurity concerns in a proactive manner proved to be of vital importance by the third decade of the twenty-first century, by which point the number and variety of computerized and network-connected devices in use had increased dramatically. In addition to traditional computers and networks, such devices had come to include tablet computers, mobile devices such as smartphones, wearable devices such as smartwatches, internet-connected appliances, smart speakers, smart thermostats, and a host of other items that had become part of everyday life for many in the United States and elsewhere. While offering a host of benefits in areas such as entertainment and home automation, each category of device offered its own potential vulnerabilities that could be exploited by bad actors, and cybersecurity initiatives were required to expand their reach in order to ensure the security of such devices. The emergence of technologies such as artificial intelligence (AI) and machine learning likewise had implication for cybersecurity during that period. In some cases, such technology was beneficial to the field; AI technology, for example, was being used to develop automated intrusion detection systems and other valuable cybersecurity tools. At the same time, AI technologies also represented potential security risks, as they could possibly be incorporated into malware or otherwise used to violate the security of computers, networks, and devices.

CYBERSECURITY IN BUSINESS

Though applicable to nearly all spheres of twenty-first-century life in the United States, cybersecurity

is of particular concern in the business world. Businesses in all industries are at risk of experiencing a cyberattack; according to a worldwide report published by the statistics firm Statista, the industries most plagued by cybercrime incidents between 2021 and 2022 included the public administration, information, finance, professional, healthcare, education, entertainment, and retail industries. In addition to targeting businesses within varied fields, cyberattacks can come in numerous forms. According to Statista, the most common cyberattack US companies experienced during the year 2022 was network intrusion, which represented 45 percent of that year's business-focused cyberattacks. Business email compromise made up 30 percent of the attacks, while other, less-common types of attacks included inadvertent disclosure, intentional disclosure, and account takeover, among others.

Cyberattacks against businesses may be carried out for a variety of purposes. One of those is corporate espionage, in which individuals or groups attempt to access computer systems owned by a company in order to steal trade secrets, access financial data, or otherwise obtain internal information that would give another company a competitive advantage. In other attacks, the true target is not the company itself but the customer or user information that is stored within the company's computer system. In some cases, businesses may store valuable information such as credit card numbers or banking details, which bad actors could go on to exploit or sell to other malicious individuals. A prominent example of such an attack, reported to the public in 2018, was the breach of Marriott International's Starwood database. In that incident, customer information—including credit card numbers—for more than 300 million hotel guests was accessed by hackers, and those guests' identities and financial well-being were thus put at risk. In some cases, cyberattacks against businesses are politically motivated. One such incident took place in 2014, when

intruders gained access to employee data and emails, among other information, belonging to the film studio Sony Pictures Entertainment. The hack was attributed to a hacking group based in North Korea, which claimed to have carried out the attack in response to Sony's plan to release a comedy film, *The Interview* (2014), that included a satirical depiction of North Korea's leader, Kim Jong Un. The hacking group subsequently released many of the stolen emails online, which drew further attention to the hack and made Sony the center of intense public scrutiny.

In addition to causing a great deal of embarrassment for employees, as was the case with the Sony hack, cyberattacks against businesses often damage the reputations of the companies involved. If a company experiences a substantial data breach, or a series of multiple breaches, customers may become less willing to patronize that company or give the company access to sensitive information such as payment details. Likewise, business cyberattacks often cause extensive financial damage. According to IBM's 2023 Cost of a Data Breach Report, a data breach—a particularly common result of a business-oriented cyberattack—cost a company an average of \$4.45 million as of 2023. In light of the severe ramifications of cyberattacks, many businesses had chosen to increase their investments in cybersecurity as of 2023, with the goal of improving the security of their systems and protecting their customer relationships, finances, and reputations.

CYBERSECURITY IN GOVERNMENT

Another sector highly concerned with cybersecurity is that of government, particularly on the federal level. Due to the nature of their work, federal agencies often handle a large quantity of sensitive data, which can range from the social security numbers of average citizens to the names of covert agents to the technical specifications of the latest military equipment. To protect the data stored in their computer

systems or accessed via their networks, federal agencies must implement strong security procedures and take a vigilant and proactive approach to addressing potential threats. Another area of serious concern for the US government is that of cyberwarfare—the use of cyberattacks as a deliberate form of warfare—and associated threats such as cyberespionage and cyberterrorism. Publicized in 2010, the computer worm Stuxnet's success in attacking and destroying a portion of Iran's nuclear infrastructure aptly demonstrated the capacity for cyberattacks to cause real-world damage to a country's most important facilities. As such, the US government must safeguard its own infrastructure from such worms, which have proven to be a substantial threat.

In addition to protecting its own data and interests, the US government works to inform businesses, institutions, and the public about the importance of cybersecurity through a variety of initiatives, including the Cybersecurity & Infrastructure Security Agency (CISA) Cybersecurity Awareness Program. The Federal Bureau of Investigation (FBI) operates the Internet Crime Complaint Center (IC3), which accepts complaints about hacking and other forms of cybercrime, while the NIST provides cybersecurity awareness education in addition to performing research in areas such as cryptography and risk management. Other government initiatives include the State and Local Cybersecurity Grant Program and the Tribal Cybersecurity Grant Program, introduced in 2022 for the purpose of funding cybersecurity improvements for state, local, and tribal governments throughout the United States. Government agencies likewise work to protect the public from falling prey to malicious actors while attempting to carry out government-related business. The Internal Revenue Service (IRS), for instance, issues frequent warnings cautioning taxpayers about scams they might encounter while attempting to file their tax returns, pay taxes or obtain tax refunds. A 2023 consumer alert about tax scams specifically warned

of the prevalence of phishing emails disguised as messages from the IRS, which the agency specifically noted “lure the victims into the scam by telling them that they are due a tax refund.” To combat such cyber threats, the IRS urged taxpayers to forward suspicious emails to a dedicated email address for further investigation.

CYBERSECURITY AND THE PUBLIC

For many individuals not employed in cybersecurity or a related field, initial exposure to cybersecurity practices and the concept of security vulnerabilities may come through workplace computer security training. Some organizations require employees to undergo such training as a requirement of their jobs and stage regular tests to assess the effectiveness of a given training initiative. One popular form of test, often carried out by an organization’s information technology (IT) department, involves simulating a phishing attack by sending employees an email message that is designed to appear suspicious and contains a link to an external website. A well-trained employee will refrain from clicking on the link and instead delete the email, report it to the IT department, or both. However, if the employee clicks on the suspicious link, the IT department is alerted of that fact. In failing the test, employees who clicked on the link have demonstrated that they are vulnerable to possible exploitation by bad actors; as such, they must undergo further security training to reduce the risk that they will one day allow a malicious individual or organization access to company systems.

Cybersecurity also enters the public consciousness when a major data breach, hack, or other security incident takes place or when a new virus or form of computer-aided crime makes headlines. In addition to being costly for the companies that experience them, data breaches can cause a great deal of stress among members of the public whose information has been exposed to bad actors. The theft of such of

information—which may include credit card or banking details, social security numbers, or passwords—can cause the average person further distress if that information is not only leaked but also put to use by a malicious individual or organization. Consider, for example, a data breach that results in the exposure of website login details belonging to individuals who patronized a specific website. This exposure places the individual’s account on the breached website at risk, but the site’s ownership may choose to mitigate that risk by automatically resetting all user passwords after the breach is discovered. If, however, the individual made the common cybersecurity mistake of reusing the same login details for an account on another website, a bad actor may be able to use those credentials to log into that other website and take over the individual’s account, make unauthorized purchases, or use that account to perpetrate fraud. Often, data breaches such as the one that led to this hypothetical, yet all too common, situation are viewed as being outside of the average person’s control. After all, a single customer or user can do little to influence the cybersecurity procedures in place within a large company or other organization. However, lapses in personal cybersecurity—such as the reuse of passwords—can increase the severity of such problems for members of the public.

As that scenario demonstrates, a basic knowledge of cybersecurity is essential to people from all walks of life, regardless of their field of employment. In addition to avoiding mistakes such as password reuse, members of the public can better protect the security of their devices and information through measures such as keeping their computer and smartphone operating systems up to date, enabling multifactor authentication whenever possible, avoiding visiting suspect or insecure websites, refraining from clicking on links or downloading files that come from unknown sources, and double-checking the source of emails or other messages to ensure that the sender’s information has not been falsified,

or “spoofed.” It is also essential for the general public to possess a basic understanding of confidence schemes, scams, and fraudulent activities that are perpetrated through electronic means. Similarly, the public must be made aware of the prevalence of deepfake technology, which can be used not only to spread misinformation but also to trick individuals into sending money, cryptocurrency, or personal information to bad actors.

FUTURE PROSPECTS

As both computer technologies and means of exploiting them continue to develop throughout the twenty-first century, cybersecurity appears poised to remain of great importance in a wide range of industries. As high-profile security breaches demonstrate the consequences of poor security on revenues and reputations, businesses will likely make greater investments in technologies and employees capable of ensuring the security of proprietary and customer information. Though already vital in government and military environments, cybersecurity will also likely increase in importance in those areas, particularly if cyberterrorism, cyberespionage, and cyberwarfare incidents become more prevalent and if the latter two gain greater acceptance on the global level. The continuing development of AI-based technologies will likewise demonstrate increased relevance to the field of cybersecurity, potentially finding use in security technologies as well as in malware, social-engineering attacks, and other security threats. Technological changes may also necessitate the development of new encryption methods or security models; as such, there will be ample opportunities for further research and development within the field.

As a career field, cybersecurity is projected to remain a promising one for the foreseeable future. According to the *Occupational Outlook Handbook (OOH)* produced by the US Bureau of Labor Statistics (BLS), employment in cybersecurity and related

fields was projected to grow substantially in the decade between 2022 and 2032. The occupation of information security analyst, specifically, was listed in the *OOH* as one of the fastest growing occupations in the United States, with a projected growth rate of 32 percent for that period. The *OOH* further projected that employment of software developers, quality assurance analysts, and testers would increase by 25 percent and computer and information systems managers by 15 percent, while other occupations relevant to the field, such as the occupations of network administrator or computer systems administrator, would maintain an average rate of growth during the same period.

In addition to representing a field of strong employment, cybersecurity will likewise remain a key field of education, both for those seeking to enter the field as employees and those seeking simply to use computers and the internet in a safe and secure manner. The US public will likely continue to benefit from education in the realms of both cybersecurity and computer literacy, as knowledge of such topics is lacking among many adults.

According to a 2023 survey by the Pew Research Center, while 87 percent of US adults were capable of identifying the most secure password out of a group of four options and 67 percent knew the purpose of HTTP cookies, only 48 percent could identify an example of two-factor authentication, and only 42 percent could define the term deepfake. In addition, less than 25 percent of respondents were able to answer key questions about US data privacy laws. In an era in which individuals must often take responsibility for elements of their own cybersecurity and must possess the knowledge to distinguish between trustworthy and fraudulent emails, websites, and online services, computer literacy and a strong understanding of the basics of cybersecurity have become increasingly essential. As such, those seeking to find work in the field may choose to focus on the

educational side of cybersecurity and provide relevant education and training to the public as well as to businesses, institutions, and agencies.

—Joy Crelin

Further Reading

- “Cost of a Data Breach Report 2023.” *IBM*, 2023, www.ibm.com/reports/data-breach. Accessed 30 Nov. 2023.
- “Cybersecurity.” *Merriam-Webster*, 20 Nov. 2023, www.merriam-webster.com/dictionary/cybersecurity. Accessed 30 Nov. 2023.
- “Cybersecurity.” *OED*, 2010, www.oed.com/dictionary/cybersecurity_n?tab=meaning_and_use#117229282. Accessed 30 Nov. 2023.
- “Information Security Analysts.” *US Bureau of Labor Statistics Occupational Outlook Handbook*, 6 Sept. 2023, www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm. Accessed 30 Nov. 2023.
- Petrosyan, Ani. “Global Number of Cybercrime Incidents from November 2021 to October 2022, by Industry and Organization Size.” *Statista*, 13 Oct. 2023,

www.statista.com/statistics/194246/cybercrime-incidents-victim-industry-size/. Accessed 30 Nov. 2023.

Petrosyan, Ani. “Most Common Types of Cyber Attacks Experienced by Companies in the United States in 2022.” *Statista*, 17 Aug. 2023, www.statista.com/statistics/293256/cyber-crime-attacks-experienced-by-us-companies/. Accessed 30 Nov. 2023.

Sidoti, Olivia, and Emily A. Vogels. “What Americans Know about AI, Cybersecurity and Big Tech.” *Pew Research Center*, 17 Aug. 2023, www.pewresearch.org/internet/2023/08/17/what-americans-know-about-ai-cybersecurity-and-big-tech/. Accessed 30 Nov. 2023.

Sjouwerman, Stu. “Malicious AI Isn’t a Distant Reality Anymore.” *Forbes*, 15 July 2022, www.forbes.com/sites/forbestechcouncil/2022/07/15/malicious-ai-isnt-a-distant-reality-anymore/?sh=27a7db2c1fd6. Accessed 30 Nov. 2023.

“State and Local Cybersecurity Grant Program.” *Cybersecurity & Infrastructure Security Agency*, www.cisa.gov/state-and-local-cybersecurity-grant-program. Accessed 30 Nov. 2023.

“Suspicious Emails and Identity Theft.” *IRS*, 1 May 2023, www.irs.gov/newsroom/suspicious-emails-and-identity-theft. Accessed 30 Nov. 2023.

CONTRIBUTORS

Zenia C. Bahorski
Independent Scholar

Ashley Baker
Pernod Ricard

Robert A. Beeler
Eastern Tennessee State University

Michael S. Bendele
Indiana University-Purdue University, Fort Wayne

Robert A. Bendele
Northeast Editing, Inc.

Tyler Biscontini
Independent Scholar

Cait Caffrey
Northeast Editing, Inc.

Josephine Campbell
Northeast Editing, Inc.

Kelly J. Cooper
Independent Scholar

Patrick G. Cooper
Orlando, FL

Joy Crelin
Independent Scholar

D. Alan Dean
Independent Scholar

Richard De Veaux
Williams College

Joseph Dewey
University of Pittsburgh

Tracey M. DiLascio
Independent Scholar

Myra Din
Proskauer Rose LLP

Donald R. Dixon
California State University, Sacramento

Kristina Domizio
Independent Scholar

Matt Donnelly
Loyola Marymount University

Sally Driscoll
Fairfield University

Maria Droujkova
Natural Math

Mark Dziak
Northeast Editing, Inc.

Andrew Farrell
Independent Scholar

I. Flair
Independent Scholar

Simone I. Flynn
Yale University

Julia Gilstein
New England Journal of Medicine Group

Harold Goldmeier
Independent Scholar

Jim Greene
Jacksonville Public Library

Bethany Groff
Historic New England

Mark Grossman
Independent Scholar

David T. Hardy
Tucson, AZ

Stuart A. Hargreaves
Chinese University of Hong Kong

- James J. Heiney
Lock Haven University of Pennsylvania
- Mary Woodbury Hooper
Dynamed
- Micah L. Issitt
St. Louis, MO
- Gayla Koerting
University of South Dakota
- Aaron Korora
Independent Scholar
- Bill Kte'pi
Independent Scholar
- Jeanne L. Kuhler
Benedictine University
- Jack Lasky
Northeast Editing, Inc.
- L. L. Lundin
Independent Scholar
- J. N. Manuel
Independent Scholar
- Douglas B. McKechnie
United States Air Force Academy
- Trudy Mercadal
EBSCO Information Services
- Eric Metchik
Salem State College
- Elizabeth Mohn
Northeast Editing, Inc.
- Jake D. Nicosia
Stevens Institute of Technology
- Gretchen Nobahar
Washington Area Metropolitan Transit Authority
- Stuart Paterson
Independent Scholar
- A. Petruso
Independent Scholar
- John Pritchard
Richmond, VT
- Elizabeth Rholetter Purdy
Georgia State University
- Christopher Rager
Pasadena, CA
- Richard M. Renneboog
Independent Scholar
- Mari Rich
NYU Tandon School of Engineering
- Lindsay Rock Roland
Penn Foster
- Michael Ruth
Independent Scholar
- Teresa E. Schmidt
Independent Scholar
- Richard Sheposh
Northeast Editing, Inc.
- Martha Sherwood
University of Oregon
- Noëlle Sinclair
University of Iowa
- Roger Smith
Portland, OR
- Robert N. Stacy
Leominster, MA
- Randa Tantawi
EBSCO Information Services
- Janine Ungvarsky
Kings College
- Maura Valentino
Central Washington University
- Linda Volonino
Canisius College
- Kathy Warnes
University of Toledo

Donald A. Watt
Dakota Wesleyan University

Nathan A. B. Watt
Independent Scholar

Bethany White
Mississippi College

George M. Whitson III
University of Texas at Tyler

Max Winter
University of Iowa

Scott Zimmer, JD
Alliant International University

A

AADHAAR HACK

ABSTRACT

The Aadhaar hack of 2018 was a cyberattack targeting India's controversial national biometric identification system, Aadhaar. Several major leaks of personal data were reported, though denied by the Indian government. Cybercriminals also created a software patch, sold online, allowing individuals the ability to generate fake Aadhaar profiles.

BACKGROUND

Aadhaar is a biometric identification system introduced by the Indian government in 2009. It provides registered users—who can be any Indian resident—with a unique twelve-digit number linked to the individual's biometric data, including photographs, iris scans, and fingerprints. The system is managed by the Unique Identification Authority of India (UIDAI), which was established specifically for the program.

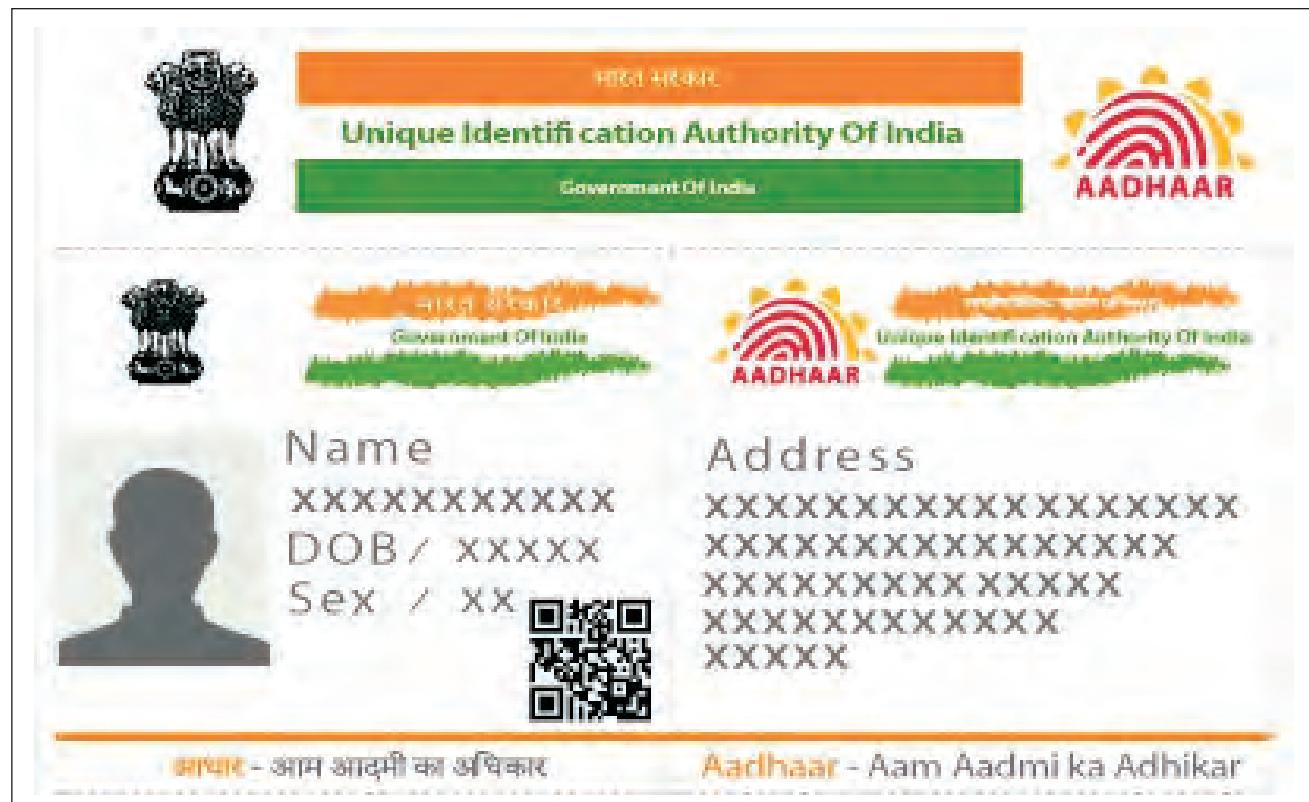
When first developed, the Aadhaar system was presented as a voluntary service that would enhance security and streamline the process of applying for various consumer and citizen services. The system became controversial with the National Identification Authority of India bill, revealed in 2010, which essentially sought to make registration with Aadhaar necessary to obtain government services. An increasing number of private companies also linked receipt of service to Aadhaar accounts, despite a lack of legal backing for such a requirement. In November 2012 a group of activists filed suit in the Indian Supreme Court challenging the constitutionality of Aadhaar, and subsequent rulings suggested that

Aadhaar could not be made mandatory. Despite this, in 2016 a bill providing a legal framework for the system was passed, and government agencies began moving toward requiring Aadhaar registration for things such as scholarships, maternity benefits, and meal programs.

The legal debate over the constitutionality of the Aadhaar project was accompanied by public debate over possible security concerns. Some criticisms took issue with the program as a whole. For example, it was argued that, because biometric data cannot be changed, identity theft through the Aadhaar system could leave victims without any recourse to change the stolen data. Reports also emerged that the program had, in some cases, made it more difficult for those in need to access services due to inflexibility and bureaucratic impediments. Several individuals reportedly died when denied access to food rations, pensions, and hospital treatment because of Aadhaar problems. Meanwhile, complaints of general security flaws and data leaks mounted. Two notable examples came in 2017, when one telecommunications company allegedly leaked Aadhaar data on as many as 120 million customers and another reportedly opened bank accounts for customers without their consent after gathering Aadhaar biometric data to authenticate mobile phone accounts. However, the UIDAI maintained that the system was safe and secure.

OVERVIEW

More security concerns emerged in 2018. That January, an investigative report by journalist Rachna Khaira published in the Indian newspaper the *Tribune* alleged that hackers communicating through



A computer-rendered sample of Aadhaar card. Image by PageImp, via Wikimedia Commons.

the WhatsApp messaging application were selling access to the personal data of all the more than 1 billion registered Aadhaar users for just Rs 500 (less than US\$10). Compromised information included names, photographs, addresses, phone numbers, and emails, although not biometric information. The report also found that software could be purchased allowing anyone to print Aadhaar cards. Representatives of the UIDAI and the ruling Bharatiya Janata political party claimed that the *Tribune* report was false and that there had been no unauthorized data breach.

In March 2018 a separate data leak was reported. Due to a lapse in a system run by the state-owned utility company Indane, it was allegedly possible to download private information for Aadhaar users including names, unique twelve-digit identity numbers, and information about services to which an

individual was connected. The breach was discovered by security researcher Karan Saini, who warned that anyone registered for the system was vulnerable to having their data stolen. UIDAI again denied the validity of the report and claimed that there had been no data breach, though after media reports circulated, the vulnerable system was taken offline.

Another major hack of the Aadhaar system was reported in September 2018 by Khaira, Aman Sethi, and Gopal Sathe for *HuffPost India*. After a three month-long investigation, the report publicized the existence of a software patch, available for sale through WhatsApp for a price of Rs 2,500 (approximately US\$35), that allowed any individual to generate Aadhaar numbers and integrate them into the system. According to the investigation, five security and software analysts confirmed the patch's function and authenticity. The patch allowed individuals to

bypass biometric authentication, making it possible for anyone in the world to register with Aadhaar. Specifically, it enabled users to cheat the iris-recognition program by reducing the sensitivity of the iris-scanning technology, thus allowing an individual to gain access using a photograph, and disabled the global position system (GPS) location security feature.

The vulnerability was said to be deeply rooted in the system's structure, meaning a fix would require a total overhaul. It was noted that the hack was unusual in that the hackers were not trying to retrieve data from the system but instead attempting to introduce new data. Still, it was regarded as a serious problem compounding the potential for fraud, identity theft, and related cybercrime—issues Aadhaar was intended to resolve. The UIDAI and other authorities did not immediately respond and eventually dismissed the reported hack, which came as the Indian Supreme Court was considering the constitutionality of the Aadhaar system. Later that month the court ruled that Aadhaar overall met constitutional guidelines, but struck down provisions requiring citizens to register with Aadhaar in order to open a bank account, obtain a mobile phone, or to be admitted to educational institutions.

In the years following the 2018 Aadhaar hack, the security of the Aadhaar system and the personal information collected within it remained in question. In October of 2023, the US-based cybersecurity firm Resecurity reported that more than 800 million Aadhaar records were being offered for sale on a hacking forum alongside other leaked data, including Indian passport records.

—Micah L. Issitt

Further Reading

“Chronology of Aadhaar Case.” *Economic Times*, 26 Sept. 2018, economictimes.indiatimes.com/news/politics-and-nation/chronology-of-aadhaar-case/articleshow/65965443.cms.

D'Mello, Gwyn. “French Cyber Expert Cracks Official Aadhaar App in 1 Minute, Realizes UIDAI's Worst Nightmare.” *India Times*, 13 Mar. 2018, www.indiatimes.com/technology/news/french-cyber-expert-cracks-official-aadhaar-app-in-1-minute-realizes-uidai-s-worst-nightmare-341416.html.

Khaira, Rachna. “Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details.” *Tribune*, 5 Jan. 2018, www.tribuneindia.com/news/archive/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details-523361.

Khaira, Rachna, Aman Sethi, and Gopal Sathe. “UIDAI's Aadhaar Software Hacked, ID Database Compromised, Experts Confirm.” *HuffPost India*, 26 Sept. 2018, www.huffpost.com/archive/in/entry/uidai-s-aadhaar-software-hacked-id-database-compromised-experts-confirm_in_5c128ddee4b0e15b460af020.

Malhotra, Ashish. “The World's Largest Biometric ID System Keeps Getting Hacked.” *Motherboard*, 8 Jan. 2018, www.vice.com/en/article/43q4jp/aadhaar-hack-insecure-biometric-id-system.

“PII Belonging to Indian Citizens, Including Their Aadhaar IDs, Offered for Sale on the Dark Web.” *Resecurity*, 15 Oct. 2023, www.resecurity.com/blog/article/pii-belonging-to-indian-citizens-including-their-aadhaar-ids-offered-for-sale-on-the-dark-web.

Sethi, Aman. “UIDAI Aadhaar Hack: New Analysis Shows Hackers Changed Enrolment Software Code in 26 Places.” *HuffPost India*, 14 Sept. 2018, www.huffpost.com/archive/in/entry/uidai-aadhaar-hack-new-analysis-shows-hackers-changed-enrolment-software-code-in-26-places_in_5c10764fe4b0a9576b528527.

Whittaker, Zack. “A New Data Leak Hits Aadhaar, India's National Id Database.” *ZDNet*, 23 Mar. 2018, www.zdnet.com/article/another-data-leak-hits-india-aadhaar-biometric-database.

ACCESS CONTROL

ABSTRACT

Access control refers to the procedures and technologies put in place to ensure that only authorized individuals are permitted to access a particular location, item, or digital file. In the twenty-first century, access control technologies include passcodes and biometric identification technologies.

BACKGROUND

When specific means are used to limit access or entry to a place or system, those means are a form of access control. Access control is typically used to ensure privacy and security. It has taken many different forms over the years and has gone from being primarily physical in the early twentieth century to mostly digital in the early twenty-first century (e.g., computer privacy). While a business may be protected by a gate and a safe by a combination lock, an email address is protected by a password, and data stored by a business is protected by software. These examples of access control are different ways to achieve the same privacy and security objective, adapted to different situations.

OVERVIEW

In the twenty-first century, access control has become not only more electronic but also more specific. For example, the passcode of an entry-level employee at a large company might only allow them access to basic information in the company's computer systems. However, the passcode of a chief executive officer (CEO) entered into the same system would result in access to all available information. This is an example of how modern software allows different "keys," in this case passcodes, to be used in the same "locks," or computer systems. In this way, access control is used to share systems while strictly controlling who can view and manipulate specific information.

Passcodes are a simple example. A more advanced one is biometrics, the examination of a person's unique eye, fingerprint, or facial characteristics to allow or deny entry to a building or system. Biometric measures are becoming more prevalent because they are hard to duplicate and provide advanced security, and they are increasingly incorporated into consumer technologies. Many smartphones, for instance, include fingerprint readers or facial-recognition systems as means of

ensuring that only the right person has access to a given phone and its contents.

When access control is used for physical entry to a place, such as a restricted records room at a company, biometric or password information may be required. Alternatively, a card or other security credential, such as an identification with a magnetic strip, may be used. Companies often use a combination of different forms of access control.

In addition to determining who can gain entry to a system or place, these safeguards can also set additional parameters such as when access is permitted and for how long. For example, an employee at a bank may be allowed access to a vault during standard business hours but not before or after those times. They may also have duration-limited access, meaning they are allowed access only for a specific amount of time.

These examples illustrate the advanced nature of access control in the twenty-first century. Greater access control allows those in charge to have greater control than they would with a lock and key or with just a password. Access control will continue to evolve as business owners and private citizens use it to maximize their professional and personal security.

—I. Flair

Further Reading

- "Access Control." *NIST Computer Security Resource Center*, csrc.nist.gov/glossary/term/access_control.
- Gibbons, Robert, and John Roberts. *The Handbook of Organizational Economics*. Princeton UP, 2012.
- Jasper, Scott. *Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security*. Georgetown UP, 2012.
- Mayer-Schönberger, Viktor. *Delete: The Virtue of Forgetting in the Digital Age*. Princeton UP, 2011.
- Padgett, John F., and Walter W. Powell. *The Emergence of Organizations and Markets*. Princeton UP, 2012.
- Rawal, Bharat S., Gunasekaran Manogaran, and Alexender Peter. *Cybersecurity and Identity Access Management*. Springer, 2023.

- Rogers, David L. *The Network Is Your Customer: Five Strategies to Thrive in a Digital Age*. Yale UP, 2011.
- Snickars, Pelle, and Patrick Vonderau. *Moving Data: The iPhone and the Future of Media*. Columbia UP, 2012.
- West, Darrell M. *The Next Wave: Using Digital Technology to Further Social and Political Innovation*. Brookings Institution, 2011.

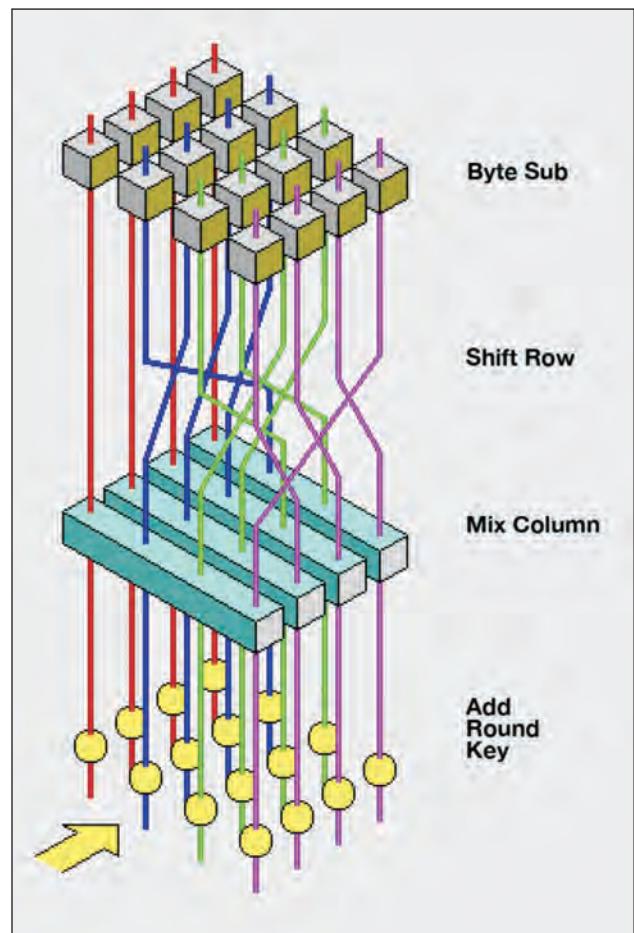
ADVANCED ENCRYPTION STANDARD

ABSTRACT

Advanced Encryption Standard (AES) is a data encryption standard widely used by many parts of the US government and by private organizations. Data encryption standards such as AES are designed to protect data on computers. AES is a symmetric block cipher algorithm, which means that it encrypts and decrypts information using an algorithm. Since AES was first chosen as the US government's preferred encryption software, hackers have tried to develop ways to break the cipher, but some estimates suggest that it could take billions of years for current technology to break AES encryption. In the future, however, new technology could make AES obsolete.

BACKGROUND

The US government has used encryption to protect classified and other sensitive information for many years. During the 1990s, the US government relied mostly on the Data Encryption Standard (DES) to encrypt information. The technology of that encryption code was aging, however, and the government worried that encrypted data could be compromised by hackers. The DES was introduced in 1976 and used a 56-bit key, which was too small for the advances in technology that were happening. Therefore, in 1997, the government began searching for a new, more secure type of encryption software. The new system had to be able to last the government into the twenty-first century, and it had to be simple to implement in software and hardware.



Visualization of the AES round function. Image via Wikimedia Commons. [Public domain.]

The process for choosing a replacement for the DES was transparent, and the public had the opportunity to comment on the process and the possible choices. The government chose fifteen different encryption systems for evaluation. Different groups and organizations, including the National Security Agency (NSA), had the opportunity to review these fifteen choices and provide recommendations about which one the government should adopt.

Two years after the initial announcement about the search for a replacement for DES, the US government chose five algorithms to research even further. These included encryption software developed

by large groups (e.g., a group at International Business Machines Corporation [IBM]) and software developed by a few individuals.

The US government found what it was looking for when it reviewed the work of Belgian cryptographers Joan Daemen and Vincent Rijmen. Daemen and Rijmen had created an encryption process they called Rijndael. This system was unique and met the US government's requirements. Prominent members of the cryptography community tested the software. The government and other organizations found that Rijndael had block encryption implementation; it had 128-, 192-, and 256-bit keys; it could be easily implemented in software, hardware, or firmware; and it could be used around the world. Because of these features, the government and others believed that the use of Rijndael as the AES would be the best choice for government data encryption for at least twenty to thirty years.

OVERVIEW

The process of locating and implementing the new encryption code took five years. The National Institute of Standards (NIST) finally approved the AES as Federal Information Processing Standards Publication (FIPS PUB) 197 in November 2001. (FIPS PUBs are issued by NIST after approval by the secretary of commerce, and they give guidelines about the standards people in the government should be using.) When the NIST first made its announcement about using AES, it allowed only unclassified information to be encrypted with the software. Then, the NSA did more research into the program and any weaknesses it might have. In 2003—after the NSA gave its approval—the NIST announced that AES could be used to encrypt classified information. The NIST announced that all key lengths could be used for information classified up to SECRET, but TOP SECRET information had to be encrypted using 192- or 256-bit key lengths.

Although AES is an approved encryption standard in the US government, other encryption standards are used. Any encryption standard that has been approved by the NIST must meet requirements similar to those met by AES. The NSA has to approve any encryption algorithms used to protect national security systems or national security information.

According to the US federal government, people should use AES when they are sending sensitive (unclassified) information. This encryption system also can be used to encrypt classified information as long as the correct size of key code is used according to the level of classification. Furthermore, people and organizations outside the federal government can use the AES to protect their own sensitive information. When workers in the federal government use AES, they are supposed to follow strict guidelines to ensure that information is encrypted correctly.

THE FUTURE OF AES

The NIST continues to follow developments with AES and within the field of cryptology to ensure that AES remains the government's best option for encryption. The NIST formally reviews AES (and any other official encryption systems) every five years. The NIST will make other reviews as necessary if any new technological breakthroughs or potential security threats are uncovered.

Although AES is one of the most popular encryption systems on the market, encryption itself may become obsolete in the future. With 2020s technologies, it would likely take billions of years to break an AES-encrypted message. However, quantum computing is becoming an important area of research, and developments in this field could make AES and other encryption software outdated. DES, AES's predecessor, can now be broken in a matter of hours, but when it was introduced, it also was considered unbreakable. As technology advances, new ways to encrypt information will have to be developed and

tested. Some experts believe that AES will be effective until the 2030s or 2040s, but the span of its usefulness will depend on other developments in technology.

—Elizabeth Mohn

Further Reading

- “Cryptographic Standards and Guidelines.” *NIST*, 8 May 2023, csrc.nist.gov/projects/cryptographic-standards-and-guidelines/archived-crypto-projects/aes-development.
- Daemen, Joan, and Vincent Rijmen. *The Design of Rijndael: The Advanced Encryption Standard (AES)*. 2nd ed., Springer, 2020.
- National Institute for Standards and Technology. “Announcing the Advanced Encryption Standard (AES): Federal Information Processing Standards Publication 197.” *NIST*, 2001, csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
- Rouse, Margaret. “Advanced Encryption Standard.” *Techopedia*, 26 June 2023, www.techopedia.com/definition/1763/advanced-encryption-standard-aes.
- Simmons, Gustavus J. “AES.” *Encyclopaedia Britannica*, 30 Apr. 2023, www.britannica.com/topic/AES/additional-info#history.
- Wood, Lamont. “The Clock Is Ticking for Encryption.” *Computerworld*, 21 Mar. 2011, www.computerworld.com/article/2550008/security/0/the-clock-is-ticking-for-encryption.html.

ALGORITHM

ABSTRACT

An algorithm is a set of steps to be followed in order to solve a particular type of problem. Having originated within the field of mathematics, algorithms make it easier for mathematicians to think of better ways to solve certain types of problems, because looking at the steps needed to reach a solution sometimes helps them to see where an algorithm can be made more efficient by eliminating redundant steps or using different methods of calculation. Algorithms are key to computer science and enable the automation of various processes, including data encryption

and cybersecurity threat detection. They are likewise essential to the creation and use of artificial intelligence and machine learning technologies.

BACKGROUND

The word “algorithm” originally came from the name of a Persian mathematician, Al-Khwarizmi, who lived in the ninth century CE and wrote a book about the ideas of an earlier mathematician from India, Brahmagupta. At first the word simply referred to the author’s description of how to solve equations using Brahmagupta’s number system, but as time passed it took on a more general meaning. At first it was used to refer to the steps required to solve any mathematical problem, and later it broadened still further to include almost any kind of method for handling a particular situation. The concept has been analogized to a recipe for baking a cake; just as the recipe describes a method for accomplishing a goal (baking the cake) by listing each step that must be taken throughout the process, an algorithm is an explanation of how to solve a problem that describes each step necessary.

OVERVIEW

Algorithms are often used in mathematical instruction because they provide students with concrete steps to follow, even before the underlying operations are fully comprehended. There are algorithms for most mathematical operations, including subtraction, addition, multiplication, and division.

For example, a well-known algorithm for performing subtraction is known as the left to right algorithm. As its name suggests, this algorithm requires one to first line up the two numbers one wishes to find the difference between so that the units digits are in one column, the tens digits in another column, and so forth. Next, one begins in the leftmost column and subtracts the lower number from the upper, writing the result below. This step is then repeated for the next column to the

| Diagram for the computation by the Engine of the Numbers of Bernoulli. See Note G. (page 722 et seq.) | | | | | | | | | | | | | | | | | | |
|---|----------------------|--|--|---|--|----------------|----------------|----------------|--------------------|----------------|------------------|-------------------|---|------------------------------------|--|--|----------------|--|
| Number of Operation. | Nature of Operation. | Variables acted upon. | Variables receiving results. | Indication of change in the value on any Variable. | Statement of Results. | Data. | | | Working Variables. | | | Result Variables. | | | | | | |
| | | | | | | V ₁ | V ₂ | V ₃ | v ₄ | v ₅ | v ₆ | v ₇ | v ₈ | v ₉ | v ₁₀ | v ₁₁ | | |
| 1 | \times | V ₂ \times V ₃ | V ₄ , V ₅ , V ₆ | $\begin{cases} V_5 = V_2 \\ V_6 = V_3 \end{cases}$ | $= 2n$ | 2 | n | 2n | 2n | 2n | | | | | | | | |
| 2 | - | V ₄ - V ₁ | V ₂ | $\begin{cases} V_4 = 0 \\ V_5 = 2V_4 \\ V_6 = V_1 \end{cases}$ | $= 2n - 1$ | 1 | ... | ... | 2n - 1 | | | | | | | | | |
| 3 | + | V ₃ + V ₁ | V ₂ | $\begin{cases} V_3 = V_1 \\ V_4 = V_2 \\ V_5 = 0 \\ V_6 = 2V_5 \end{cases}$ | $= 2n + 1$ | 1 | ... | ... | 2n + 1 | | | | | | | | | |
| 4 | + | 2V ₃ - 2V ₄ | V ₁₁ | $\begin{cases} V_{11} = V_3 \\ V_5 = V_4 \end{cases}$ | $\frac{2n+1}{2n+1}$ | ... | ... | 0 | 0 | ... | ... | ... | ... | ... | $\frac{2n-1}{2n+1}$ | | | |
| 5 | + | V ₁₁ - 2V ₃ | V ₁₁ | $\begin{cases} V_{11} = 2V_3 \\ V_5 = V_{11} \end{cases}$ | $\frac{1}{2} \cdot \frac{2n-1}{2n+1}$ | 2 | ... | ... | ... | ... | ... | ... | ... | ... | $\frac{1}{2} \cdot \frac{2n-1}{2n+1}$ | | | |
| 6 | - | V ₁₁ - 2V ₃ | V ₁₂ | $\begin{cases} V_{12} = V_{11} \\ V_{12} = V_{13} \end{cases}$ | $= \frac{1}{2} \cdot \frac{2n-1}{2n+1} = A_0$ | ... | ... | ... | ... | ... | ... | ... | ... | ... | 0 | $= -\frac{1}{2} \cdot \frac{2n-1}{2n+1} = A_n$ | | |
| 7 | - | V ₃ - V ₁ | V ₁₀ | $\begin{cases} V_{10} = V_3 \\ V_{10} = V_1 \end{cases}$ | $= n - 1 (= 3)$ | 1 | ... | n | ... | ... | ... | ... | ... | ... | n - 1 | | | |
| 8 | + | V ₂ + 2V ₂ | V ₇ | $\begin{cases} V_7 = V_2 \\ V_7 = V_2 \end{cases}$ | $= 2 + 0 = 2$ | 2 | ... | ... | ... | ... | 2 | | | | | | | |
| 9 | + | V ₅ + V ₇ | V ₁₁ | $\begin{cases} V_{11} = V_5 \\ V_{11} = V_7 \end{cases}$ | $= \frac{2n}{2} = A_1$ | ... | ... | ... | ... | 2n | 2 | ... | ... | ... | $\frac{2n}{2} = A_1$ | | | |
| 10 | \times | V ₂₁ \times V ₁₀ | V ₁₂ | $\begin{cases} V_{12} = V_{21} \\ V_{12} = V_{10} \end{cases}$ | $= B_1 \cdot \frac{2n}{2} = B_1 A_1$ | ... | ... | ... | ... | ... | ... | ... | ... | $B_1 \cdot \frac{2n}{2} = B_1 A_1$ | | | | |
| 11 | + | V ₁₀ + V ₁₂ | V ₁₂ | $\begin{cases} V_{12} = V_{10} \\ V_{12} = V_{12} \end{cases}$ | $= \frac{1}{2} \cdot \frac{2n-1}{2n+1} + B_1 \cdot \frac{2n}{2}$ | ... | ... | ... | ... | ... | ... | ... | ... | 0 | $\left\{ -\frac{1}{2} \cdot \frac{2n-1}{2n+1} + B_1 \cdot \frac{2n}{2} \right\}$ | B ₁ | | |
| 12 | - | V ₁₀ - V ₁₂ | V ₁₀ | $\begin{cases} V_{10} = V_{12} \\ V_{10} = V_1 \end{cases}$ | $= n - 2 (= 2)$ | 1 | ... | ... | ... | ... | ... | ... | ... | n - 2 | | | | |
| 13 | - | V ₆ - V ₁ | V ₆ | $\begin{cases} V_6 = 2V_6 \\ V_6 = V_1 \end{cases}$ | $= 2n - 1$ | 1 | ... | ... | ... | 2n - 1 | | | | | | | | |
| 14 | + | V ₁ + V ₇ | V ₂ | $\begin{cases} V_2 = V_1 \\ V_2 = V_7 \end{cases}$ | $= 2 + 1 = 3$ | 1 | ... | ... | ... | 3 | | | | | | | | |
| 15 | + | V ₈ + V ₇ | V ₈ | $\begin{cases} V_8 = V_7 \\ V_8 = V_8 \end{cases}$ | $= \frac{2n-1}{3}$ | ... | ... | ... | 2n - 1 | 3 | $\frac{2n-1}{3}$ | | | | | | | |
| 16 | \times | V ₈ \times V ₁₀ | V ₁₁ | $\begin{cases} V_{11} = V_8 \\ V_{11} = V_{10} \end{cases}$ | $= \frac{2n}{3}$ | ... | ... | ... | ... | ... | 0 | ... | ... | $\frac{2n}{3}$ | $\frac{2n}{3}$ | | | |
| 17 | - | V ₆ - V ₇ | V ₆ | $\begin{cases} V_6 = V_6 \\ V_6 = V_7 \end{cases}$ | $= 2n - 2$ | 1 | ... | ... | ... | 2n - 2 | | | | | | | | |
| 18 | + | V ₁ + 2V ₇ | V ₇ | $\begin{cases} V_7 = 3V_7 \\ V_7 = V_1 \end{cases}$ | $= 2 + 1 = 4$ | 1 | ... | ... | ... | 4 | | | | | | | | |
| 19 | + | V ₆ + 2V ₇ | V ₉ | $\begin{cases} V_9 = 2V_7 \\ V_9 = V_6 \end{cases}$ | $= 2 + 2 = 4$ | ... | ... | ... | 2n - 2 | 4 | $\frac{2n-2}{4}$ | ... | $\left\{ \frac{2n}{3}, \frac{2n-1}{3}, \frac{2n-2}{3} \right\}$ | | | | | |
| 20 | \times | V ₉ \times V ₁₀ | V ₁₁ | $\begin{cases} V_{11} = V_9 \\ V_{11} = V_{10} \end{cases}$ | $= \frac{2n}{3}$ | ... | ... | ... | 2n - 2 | 4 | 0 | ... | | | | | | |
| 21 | \times | V ₂₀ \times V ₁₁ | V ₁₂ | $\begin{cases} V_{12} = 2V_{11} \\ V_{12} = V_{20} \end{cases}$ | $= B_3 \cdot \frac{2n}{3}$ | ... | ... | ... | ... | ... | 0 | ... | ... | 0 | $B_3 A_2$ | | | |
| 22 | + | V ₁₀ + 2V ₁₂ | V ₁₂ | $\begin{cases} V_{12} = 2V_{12} \\ V_{12} = V_{10} \end{cases}$ | $= A_0 + B_1 A_1 + B_3 A_2$ | ... | ... | ... | ... | ... | ... | ... | ... | 0 | $\left\{ A_3 + B_1 A_1 + B_3 A_2 \right\}$ | | | |
| 23 | - | V ₁₀ - V ₁₂ | V ₁₀ | $\begin{cases} V_{10} = V_{12} \\ V_{10} = V_1 \end{cases}$ | $= n - 3 (= 1)$ | 1 | ... | ... | ... | ... | ... | ... | ... | n - 3 | | | | |
| Here follows a repetition of Operations thirteen to twenty-three. | | | | | | | | | | | | | | | | | | |
| 24 | + | V ₁₀ + 2V ₁₂ | V ₂₄ | $\begin{cases} V_{24} = 2V_{12} \\ V_{24} = V_{10} \end{cases}$ | $= B_7$ | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | B ₇ | |
| 25 | + | V ₁ + V ₂ | V ₃ | $\begin{cases} V_3 = V_1 \\ V_3 = V_2 \end{cases}$ | $= n + 1 = 4 + 1 = 5$ | 1 | ... | n + 1 | ... | 0 | 0 | | | | | | | |

Ada Lovelace's diagram from "Note G," the first published computer algorithm. Photo via Wikimedia Commons. [Public domain.]

right, until the values in the units column have been subtracted from one another. At this point the results from the subtraction of each column, when read left to right, constitute the answer to the problem.

By following these steps, it is possible for a subtraction problem to be solved even by someone still in the process of learning the basics of subtraction. This demonstrates the power of algorithms both for performing calculations and for use as a source of instructional support.

Algorithms are also important within the field of computer science. For example, without algorithms, a computer would have to be programmed

with the exact answer to every set of numbers that an equation could accept in order to solve an equation—an impossible task. By programming the computer with the appropriate algorithm, the computer can follow the instructions needed to solve the problem, regardless of which values are used as inputs. Algorithms are crucial to a wide range of computer technologies, facilitating the sorting and analysis of data, the use of automated decision-making processes, data encryption, threat detection, and other key functions. They are especially crucial to the fields of artificial intelligence and machine learning.

—Scott Zimmer

Further Reading

- Cormen, Thomas H. *Algorithms Unlocked*. MIT Press, 2013.
- Ferguson, R. Stuart. *Practical Algorithms for 3D Computer Graphics*. 2nd ed., AK Peters/CRC Press, 2013.
- Fitter, Hetal N., Akash B. Pandey, Divyang D. Patel, and Jitendra M. Mistry. "A Review on Approaches for Handling Bezier Curves in CAD for Manufacturing." *Procedia Engineering*, vol. 97, 2014, pp. 1155–66.
- Kamhoua, Charles A., Christopher D. Kiekintveld, Fei Fang, and Quanyan Zhu, editors. *Game Theory and Machine Learning for Cyber Security*. Wiley, 2021.
- MacCormick, John. *Nine Algorithms That Changed the Future: The Ingenious Ideas That Drive Today's Computers*. Princeton UP, 2012.
- O'Leary, Timothy, Linda O'Leary, and Daniel O'Leary. *Computing Essentials 2023*. McGraw-Hill, 2022.
- Parker, Matt. *Things to Make and Do in the Fourth Dimension: A Mathematician's Journey through Narcissistic Numbers, Optimal Dating Algorithms, at Least Two Kinds of Infinity, and More*. Farrar, 2014.
- Rychagov, Michael N., Ekaterina V. Tolstaya, and Mikhail Y. Sirotenko, editors. *Smart Algorithms for Multimedia and Imaging*. Springer Cham, 2021.
- Sarkar, Jayanta. *Computer Aided Design: A Conceptual Approach*. CRC Press, 2017.
- Schapire, Robert E., and Yoav Freund. *Boosting: Foundations and Algorithms*. MIT Press, 2012.
- Steiner, Christopher. *Automate This: How Algorithms Came to Rule Our World*. Penguin, 2012.
- Valiant, Leslie. *Probably Approximately Correct: Nature's Algorithms for Learning and Prospering in a Complex World*. Basic, 2013.

ANDROID OS

ABSTRACT

Introduced to consumers by the technology company Google, the Android operating system (OS) debuted on the mobile-device market with the release of the T-Mobile G1 (or HTC Dream) smartphone in 2008. The OS quickly became a major competitor in that market and as of 2023 was the dominant mobile OS both in the United States and worldwide.

BACKGROUND

Mobile computing is the fastest-growing segment of the tech market. As pricing has become more affordable, developing nations, particularly in Africa, are the largest growing market for smartphones. With smartphones, users shop, gather information, connect via social media such as X (previously Twitter) and Facebook, and communicate—one of the uses more traditionally associated with phones.

By far the most popular operating system running on mobile phones is Android. Since its launch in 2008, Android has far and away overtaken the competition, which has included popular operating systems such as Apple's iOS. By mid-2023, more than 3 billion Android devices were active worldwide.

OVERVIEW

Android came about amid a transformative moment in mobile technology. Prior to 2007, slide-out keyboards mimicked the typing experience of desktop personal computers (PCs). In June of that year, Apple released its first iPhone, forever altering the landscape of mobile phones. Apple focused on multitouch gestures and touch-screen technology. Nearly concurrent with this, Google's Android released its first application program interface (API).

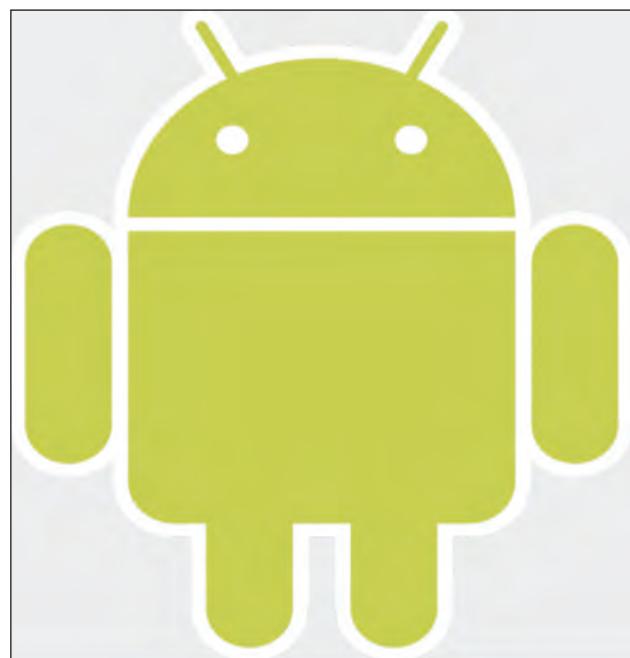
The original API of Google's new OS first appeared in October 2008. The Android OS was first installed on the T-Mobile G1, also known as the HTC Dream. This prototype had a very small set of preinstalled apps, and as it had a slide-out QWERTY keyboard, there were no touch-screen capabilities. It did have native multitasking, which Apple's iOS did not yet have. Still, to compete with Apple, Google was forced to replace physical keyboards and access buttons with virtual onscreen controls. The next iteration of Android shipped with the HTC Magic and was accompanied by a virtual keyboard and a more robust app marketplace. Among the other early features that have stood the

test of time are the pull-down notification list, home-screen widgets, and strong integration with Google's Gmail service.

One later feature, the full-screen immersive mode, became quite popular as it reduces distractions. First released with Android 4.4, "KitKat," in 2013, it hides the navigation and status bars while certain apps are in use. It was retained for the release of Android 5.0, "Lollipop," in 2015, as well as for subsequent releases.

ANDROID CHANGES AND GROWS

Both of Google's operating systems—Android and its cloud-based desktop OS, ChromeOS—are based on the free open-source OS Linux, created by engineer Linus Torvalds and first released in 1991. Open-source software is created using publicly available source code. The open-source development of Android has allowed manufacturers to produce robust, affordable products that contribute to its widespread popularity in emerging and developing markets. This may be one reason why Android has



Android logo. Image by Google Inc., via Wikimedia Commons.

captured many more new users than its closest rival, Apple's iPhone operating system (iOS). This strategy has kept costs down and has also helped build Android's app marketplace, the Google Play Store, which offers millions of apps, many free of charge. As of 2023, Android made up more than 70 percent of the global mobile operating system market.

This open-source development of Android has had one adverse effect: the phenomenon known as "forking," which occurs primarily in China. Forking is when a private company takes the OS and creates their own products apart from native Google services such as email. Google seeks to prevent this loss of control (and revenue) by not supporting these companies or including their apps in its marketplace.

Google's business model has always focused on rapid iteration. By contrast, rivals such as Microsoft and Apple have had a far slower, more deliberate pace due to hardware issues. One benefit of Google's faster approach is the ability to address issues and problems in a timely manner. A drawback is the phenomenon known as "cloud rot." As the cloud-based OS grows older, servers that were once devoted to earlier versions are repurposed. Since changes to the OS initially came every few months, apps that worked a month prior would suddenly lose functionality or become completely unusable. Later Android updates have been released on a timescale of six months or more.

Throughout many of Android's first years of existence, new versions of the OS were known by both version numbers and dessert-themed code names, such as Cupcake (version 1.5), Ice Cream Sandwich (version 4.0), and Oreo (versions 8.0 and 8.1). Following the release of Pie (version 9), however, Google moved away from that naming scheme with Android version 10, released in 2019. Android version 11, released as a public beta in June of 2020, was likewise referred to by its version number rather than by a themed nickname. Google

continued that practice with the subsequent versions of Android, including Android 14, released in late 2023.

ANDROID'S FUTURE

One of the biggest concerns about Android's future is the issue of forking. Making the code available to developers at no cost has made Android a desirable and cost-effective alternative to higher-end makers such as Microsoft and Apple, but it has also made Google a target of competitors. Another consideration for Android's future is its link to ChromeOS, also a Google product. Google plans to keep the two separate. Further, Google executives have made it clear that Chromebooks (laptops that run Chrome) and Android devices have distinct purposes.

Android's focus has been on touch-screen technology, multitouch gesturing, and screen resolution, making it a purely mobile OS for phones, tablets, wearable devices, and televisions. Meanwhile, Chrome has developed tools that are more useful in the PC and laptop environment, such as keyboard shortcuts. However, an effort to unify the appearance and functionality of Google's different platforms and devices called Material Design was introduced in 2014. Further, Google has ensured that Android apps can be executed on Chrome and has made the Google Play Store available on Chromebooks. Such implementations suggest a slow merging of the Android and Chrome user experiences.

—Andrew Farrell

Further Reading

- Amadeo, Ron. "Report: Google Will Graciously Let Android OEMs Build Amazon Fire Devices." *Ars Technica*, 28 Oct. 2022, arstechnica.com/gadgets/2022/10/report-google-will-graciously-let-android-oems-build-amazon-fire-devices.
- _____. "The (Updated) History of Android." *Ars Technica*, 31 Oct. 2016, arstechnica.com/gadgets/2016/10/building-android-a-40000-word-history-of-googles-mobile-os.

Curry, David. "Android Statistics (2023)." *Business of Apps*, 27 Feb. 2023, www.businessofapps.com/data/android-statistics.

Edwards, Jim. "Proof That Android Really Is for the Poor." *Business Insider*, 27 June 2014, www.businessinsider.in/Proof-That-Android-Really-Is-For-The-Poor/articleshow/37328668.cms.

"Mobile Operating System Market Share Worldwide—June 2023." *Statcounter*, June 2023, gs.statcounter.com/os-market-share/mobile/worldwide/#monthly-202206-202306.

Newman, Jared. "With Android Lollipop, Mobile Multitasking Takes a Great Leap Forward." *Fast Company*, 6 Nov. 2014, www.fastcompany.com/3038213/with-android-lollipop-mobile-multitasking-takes-a-great-leap-forward.

"Number of Available Applications in the Google Play Store from December 2009 to June 2023." *Statista*, June 2023, www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store.

Raphael, J. R. "Android Versions: A Living History from 1.0 to 14." *Computerworld*, 7 Apr. 2023, www.computerworld.com/article/3235946/android-versions-a-living-history-from-1-0-to-today.html.

ANONYMITY AND ANONYMIZERS

ABSTRACT

Anonymity and anonymizers are concepts that have taken on a new significance in the digital age. While anonymous communication is protected by the First Amendment of the US Constitution, complete anonymity, particularly when communicating on the internet, is difficult to achieve for the average person. Anonymizers can be used to accomplish nearly complete anonymity in digital communication.

BACKGROUND

In *Talley v. California*, 362 U.S. 60 (1960), the US Supreme Court determined that the First Amendment's free speech clause protects anonymous speech. Long before digital communication existed, a City of Los Angeles ordinance prohibited the distribution of a leaflet or handbill unless it

identified the name and address of its publisher. A leafleteer was arrested for failing to comply with the ordinance and argued that the requirement that he identify himself by name and address violated his constitutional right to freedom of speech. The Court agreed.

The Court reasoned that anonymous communication has historically played an important part in the development of society and social change. For example, the Court pointed to various instances in US history where colonists who supported the revolution and the Founding Fathers themselves engaged in anonymous speech. The Court determined that prohibiting anonymous speech would have a chilling effect on speech and, in particular, would lessen the distribution of literature critical of government. The Court has affirmed this protection of anonymous speech in cases such as *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995).

OVERVIEW

The internet has provided the appearance of facilitating anonymous communication. Users are able to access digital communication platforms and contribute to the discussion of ideas without revealing much, if any, information about themselves. Whether through social networks, email, blogs, or chatrooms, users can create fabricated persona, or no persona at all, and engage in an exchange of ideas without revealing their true identities—thus retaining anonymity. Many scholars argue that this anonymity provided by the internet democratizes communication and thus increases the exchange of ideas that the First Amendment was intended to protect. Others argue that anonymous communication through the internet results in more caustic, hurtful speech and disconnects speakers from the emotional injury they may cause. Anonymous speech may simply provide protection for people who engage in illegal threats and intimidation.

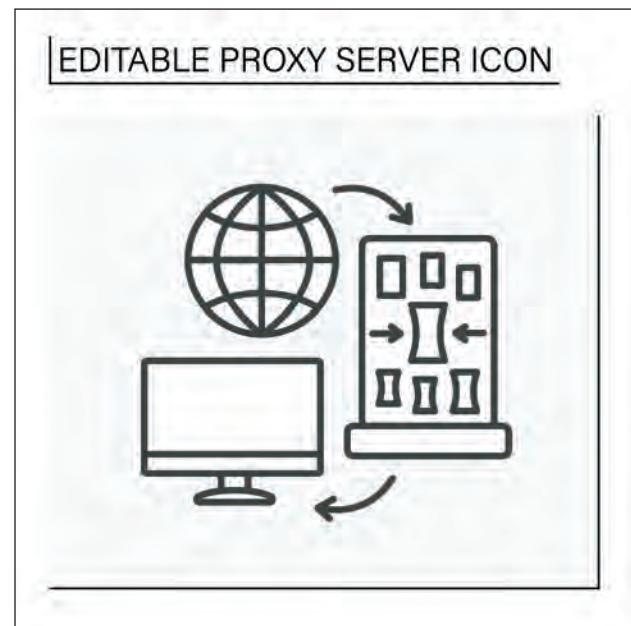


Image via iStock/Anatolii Shcherbatiuk. [Used under license.]

Many people access the internet through an entity, such as a private company, that acts as an internet service provider. The internet service provider connects its users to the internet and thus often has access to its customers' information. While most internet service providers allow their customers to engage others on the internet anonymously, the internet service provider nevertheless retains the customer's name and other personally identifiable information. As a result, when users have anonymously communicated via the internet and the communication is the basis for legal action, courts have been asked to order internet service providers to reveal the identity of the anonymous user. Because of the constitutional commitment to protect anonymous speech, courts have struggled to articulate the proper standard for when to require internet service providers to reveal their users' identities. Moreover, the US government has allegedly accessed users' identity and data through internet service providers' records regardless of users' attempts to remain anonymous.

Because a user may not want his or her internet use to be traceable, he or she may use an anonymizer to try to accomplish complete anonymity. Anonymizers are tools that protect a user's personally identifiable information by masking his or her internet protocol address—the way a computer and its user is identified on an internet service provider's network. Masking the internet protocol address makes it difficult to trace a user's internet usage, thus ensuring his or her privacy.

There are two basic forms of anonymizers: networked anonymizers and single-point anonymizers:

* Networked anonymizers transfer the user's communication or other internet traffic through a network of internet server computers before it arrives at its destination website. The destination website then routes its information back to the user through the same network. The path the information takes between the original sources is thus obscured and difficult to map, and the user's internet protocol address is not associated with having visited a particular website, where he or she may have shared information or communicated. These sorts of anonymizers are generally considered more secure because of the multiple connections through which the information must travel.

* A single-point anonymizer is a website through which a user can surf the web. The anonymizer website communicates on behalf of the user and sends a request to the destination website for the user. The destination website then sends information back to the anonymizer website, which then encrypts the communication and provides it to the user seeking anonymity.

As with any technology, anonymizers are used by people with both good and ill intentions. They can be used to engage in debate and criticism without the threat of being exposed and retaliated against for one's beliefs. At the same time, however, anonymizers can be used by people with nefarious goals, such as internet-related crime.

Anonymity has long been recognized as a valuable tool for communicating fringe, minority, or unpopular views without the threat of retaliation. Online anonymity has extended that benefit to millions of people while at the same time providing protection for those that might abuse it. Although true online anonymity is difficult to achieve, technology such as anonymizers allow those who seek anonymity to protect their identity from those who may want to reveal it.

—Douglas B. McKechnie

Further Reading

- Barrett Lidsky, Lyrissa. "Silencing John Doe: Defamation and Discourse in Cyberspace." *Duke Law Journal*, vol. 49, no. 4, 2000, pp. 855–946.
- Griffith, Eric. "How to Completely Disappear from the Internet." *PCMag*, 24 Oct. 2022, www.pcmag.com/how-to/how-to-stay-anonymous-online.
- Kizza, Joseph Migga. *Ethical and Social Issues in the Information Age*. 7th ed., Springer, 2023.
- Payton, Theresa, and Theodore Claypoole. *Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family*. Rowman & Littlefield, 2014.

ANONYMOUS

ABSTRACT

Anonymous is a loose association of online activists and followers who advocate internet freedom via attacks against websites of government agencies, corporations, and others. *Anonymous* often leaves this motto as a calling card: "We are Anonymous. We are legion. We never forgive. We never forget. Expect us." The group coalesced on an internet site where contributors to discussions were not required to register; all participants were automatically identified as "Anonymous." *Anonymous* gained wide attention in 2008 with a campaign against the Church of Scientology. Later targets included MasterCard, the Motion Picture Association of America, the Federal Bureau of

Investigation (FBI), and computer security firms. The group's trademark method of attack is to overwhelm a website with requests for service. In some cases, individual hackers penetrate site security to vandalize web pages and steal data. Anonymous activities hit a peak in 2011, followed by waves of arrests in 2012. Anonymous claims it cannot be stopped because it is a leaderless organization with inexhaustible ranks of hackers.

BACKGROUND

The organization called Anonymous emerged from discussions at an internet site that required no user registration. The site, named 4chan, was created in 2003 by fifteen-year-old Christopher Poole as a forum for fans of anime, comic books, and movies. The 4chan /b/ discussion board, designated for miscellaneous topics, evolved into a hotspot for boasts, pranks, and occasional political discussion. By 2007, the name Anonymous had been associated in news reports with online attacks—notably, a campaign to swamp the website of a white supremacist talk-show host and, later the same year, with tracking a pedophile who was subsequently arrested by Toronto police. In 2008, Anonymous demonstrated a higher level of tactical organization as Project Chanology called on supporters not only to deluge the Church of Scientology website with traffic but also to participate in demonstrations at church facilities. At the demonstrations, many protesters wore Guy Fawkes masks, a symbol of anonymity from the graphic novel and film *V for Vendetta*.

Anonymous expanded from 4chan to various other online sites and continued to stage attacks, usually in response to perceived attempts to restrict freedom on the internet. The basic method for disabling a target's website is the distributed denial of service (DDoS) attack, in which the website is overwhelmed with repeated contacts from a network of "bots," personal computers controlled by a remote command post. A network of ten thousand bots is sufficient to take down even robust websites that

have ample server capacity. In some cases, Anonymous participants volunteered their personal computers for the bot network by downloading software called the Low Orbit Ion Cannon, a tool originally developed for stress-testing corporate computer systems.

Other forms of attack—defacing a webpage or stealing confidential data—require penetrating the target's security system, which is done by various means. Password-cracking software runs through millions of permutations to arrive at too-easy passwords. Phishing emails trick legitimate users into divulging access codes or clicking a link that installs spyware. In some cases, access is facilitated by a whistleblower or Anonymous sympathizer. These tactics require higher levels of programming knowledge and distinguish operational leaders within Anonymous. Anonymous characterizes itself as a decentralized collective, with no formal leadership structure. As a result, operational leadership may shift from project to project. Decision making at the



An emblem that is commonly associated with Anonymous. The "man without a head" represents anonymity and leaderless organization. Image via Wikimedia Commons. [Public domain.]



Individuals appearing in public as Anonymous, wearing Guy Fawkes masks. Photo by Vincent Diamante, via Wikimedia Commons.

strategic level is done through a democratic process of discussion, often on an internet relay chat (IRC) channel. Announcements are issued via YouTube or through Anonymous accounts on social media. Of the individuals arrested worldwide for Anonymous-related activities, the overwhelmingly majority are males in their teens and twenties.

OVERVIEW

Online attacks by Anonymous were sporadic in 2009 and 2010 but spiked in 2011. The increase was attributable in large part to LulzSec, a subgroup of Anonymous that declared itself less dedicated to political activism than to the thrill of cyber-breaking and entering. The combined operations in 2011 continued to reflect the group's past zeal in favor of internet freedom and against pedophiles and homophobes.

In its April 2009 campaign to support The Pirate Bay, Anonymous launched DDoS attacks on the

International Federation of the Phonographic Industry website and also encouraged followers to send all-black faxes and make threatening calls. In December 2010, Anonymous made the decision to launch Operation Payback against MasterCard, Visa, PayPal, and the Swiss postal system for refusing to process contributions to WikiLeaks. WikiLeaks was the whistleblowing group that posted thousands of classified documents on the internet, attracting the full fury of all branches of the US government. Among all its investigations of internet crime, Operation Payback was the case the Federal Bureau of Investigation (FBI) pursued most assiduously, and it led to a raft of arrests the following year. PayPal resisted Operation Payback's DDoS onslaught successfully. MasterCard and Visa experienced brief interruptions of service to customers. Switzerland's PostFinance site was driven offline.

Anonymous took aim at a variety of targets in 2011, starting with governments that were

overthrown in the Arab Spring. In January, DDoS attacks shut down Tunisian government websites. Later, the group hacked into Egyptian government sites and posted email addresses and passwords of officials in Egypt, Bahrain, Jordan, and Morocco. Then, in February 2011, Anonymous humiliated the internet security firm HBGary Federal by erasing all the data from one of its servers and posting 70,000 company emails. Also in February 2011, Anonymous began a running battle with the Westboro Baptist Church, notorious for picketing funerals of service members killed in Iraq. The church's webpage was replaced during a radio talk show—while a church spokesperson was ranting against Anonymous on the air—with an Anonymous graphic, a figure with a question mark in place of a head. Anonymous struck Westboro again in December 2012, posting names and addresses of church members in retaliation for picketing Newtown Massacre funerals. In March 2013, Anonymous defaced the church's Facebook page after it called for picketing funerals of victims of the Boston Marathon bombing. Anonymous turned its attention to pedophiles with Operation Darknet in October 2011, publishing 1,500 names of visitors to Lolita City, a child pornography site.

The second half of 2011 saw a deluge of hacks and DDoS attacks as LulzSec launched Operation AntiSec. The wider Anonymous community joined in against a range of police, military, and security agencies. On June 15, a LulzSec DDoS attack took down the Central Intelligence Agency's public website. On June 27, Anonymous posted documents stolen from an anti-cyberterrorism program run by the Department of Homeland Security. The group breached the Arizona Department of Public Safety (state police) twice and published compromising information about twelve individual officers.

In January 2012, protesting the shutdown of the file sharing site Megaupload, Anonymous attacked the websites of the Department of Justice, FBI, Motion Picture Association of America, Recording

Industry Association of America, and Broadcast Music Inc.

Law enforcement agencies made arrests worldwide in 2012, cooling the pace of Anonymous campaigns. An Interpol operation in February swept up twenty-five hackers in Europe and South America. In March, police in the United Kingdom and the FBI arrested five top hackers in LulzSec. In July 2012, the FBI apprehended sixteen hackers in connection with Operation Payback, the 2010 campaign against MasterCard, Visa, and PayPal. In December 2012, UK police arrested Christopher (Nerdo) Weatherhead, a university student who pleaded guilty to masterminding Operation Payback. The police successes in 2012 began in August 2011 with the arrest of Hector (Sabu) Monsegur, a New York resident and cofounder of LulzSec, who then assisted the FBI in its investigations. Anonymous maintains in public statements that the arrests are regrettable but do not diminish the power of the collective. There are always more hackers.

In early 2013, with DDoS and hacking campaigns against Israel and North Korea, Anonymous appeared to choose sides in long-running, nation-based conflicts—a departure from the group's earlier emphasis on universalist themes of internet freedom. During OpIsrael, on April 7, 2013, DDoS attacks on the websites of Israeli government offices and banks caused minor disruptions, and a number of small businesses saw their homepages defaced. Also in early April 2013, as tensions mounted between South and North Korea, Anonymous hackers drove North Korea's *Uriminzokkiri* news site offline and vandalized North Korean accounts on Twitter and Flickr. In Canada, a third mid-April project drew attention to the case of a high school girl who committed suicide. She had been gang-raped at a party, and her attackers posted a video online. Police did not have sufficient evidence to file criminal charges. Anonymous announced it would publish the names of the

attackers if the police did not make arrests. For some observers, the fragmentation of Anonymous activities during that period indicated a rising level of chaos in a group that had lost influential leaders or a shift in the importance of subgroups within the Anonymous collective.

Anonymous remained active throughout the second decade of the twenty-first century, carrying out operations against a variety of websites and organizations. In 2017, a group that claimed to be associated with Anonymous took over thousands of websites on the dark web after gaining access to the service used to host them. Anonymous-affiliated hackers took part in politically motivated actions during the early 2020s, targeting the websites of the Minneapolis, Minnesota, police department in 2020 and the Republican Party of Texas in 2021. In 2022, following Russia's invasion of Ukraine, Anonymous targeted multiple websites and organizations based in Russia, including the *RT* news site.

Further Reading

- Arquilla, John. "Cyberwar Is Already Upon Us." *Foreign Policy*, 27 Feb. 2012, foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us.
- Dysart, Joe. "The Hacktivists." *ABA Journal*, vol. 97, no. 12, 2011, pp. 40–46.
- Elias, Marilyn. "Operation Blitzkrieg." *Intelligence Report*, vol. 146, 2012, pp. 44–47.
- Holt, Thomas, et al. "Comparing Civilian Willingness to Attack Critical Infrastructure on and off Line." *Proceedings of the European Conference on e-Government*, 2012, pp. 345–51.
- Molloy, David, and Joe Tidy. "George Floyd: Anonymous Hackers Re-Emerge Amid US Unrest." *BBC*, 1 June 2020, www.bbc.com/news/technology-52879000.
- Novell, Carly. "Anonymous Hacks Texas GOP Website, Floods It with Memes." *Daily Dot*, 13 Sept. 2021, www.dailyydot.com/debug/anonymous-hacks-texas-gop-website-floods-it-with-memes.
- Olson, Parmy. "Is Anonymous the Internet's Most Powerful Mirage?" *Forbes*, 30 May 2012, www.forbes.com/sites/parmyolson/2012/05/30/is-anonymous-the-internets-most-powerful-mirage/?sh=394245e86ba6.
- Pitrelli, Monica. "Anonymous Declared a 'Cyber War' against Russia: Here Are the Results." *CNBC*, 16 Mar. 2022, www.cnbc.com/2022/03/16/what-has-anonymous-done-to-russia-here-are-the-results-.html.

ARTIFICIAL INTELLIGENCE

ABSTRACT

Artificial intelligence (AI) is the design, implementation, and use of programs, machines, and systems that exhibit human intelligence, with its most important activities being knowledge representation, reasoning, and learning. Artificial intelligence encompasses a number of important subareas, including voice recognition, image identification, natural language processing, expert systems, neural networks, planning, robotics, and intelligent agents. Several important programming techniques have been enhanced by AI researchers, including classical search, probabilistic search, and logic programming.

BACKGROUND

Although the concept of "artificial intelligence" probably has existed since antiquity, the term was first used by American scientist John McCarthy at a conference held at Dartmouth College in 1956. In 1955–56, the first AI program, Logic Theorist, had been written in IPL, a programming language, and in 1958, McCarthy invented Lisp, a programming language that improved on IPL. *Syntactic Structures* (1957), a book about the structure of natural language by American linguist Noam Chomsky, made natural language processing into an area of study within AI. In the next few years, numerous researchers began to study AI, laying the foundation for many later applications, such as general problem-solvers, intelligent machines, and expert systems.

In the 1960s, Edward Feigenbaum and other scientists at Stanford University built two early expert systems: DENDRAL, which classified chemicals, and MYCIN, which identified diseases. These early expert systems were cumbersome to modify because they had hard-coded rules. By 1970, the OPS expert system shell, with variable rule sets, had been released by Digital Equipment Corporation as the first commercial expert system shell. In addition to expert systems, neural networks became an important area of AI in the 1970s and 1980s. Frank Rosenblatt introduced the perceptron (an algorithm for supervised learning of binary classifier) in 1957, but it was *Perceptrons: An Introduction to Computational Geometry* (1969), by Marvin Minsky and Seymour Papert, and the two-volume *Parallel Distributed Processing: Explorations in the Microstructure of Cognition* (1986), by David Rumelhart, James McClelland, and the PDP Research Group, that really defined the field of neural networks. Development of AI has continued, with game theory, speech recognition, robotics, and autonomous agents being some of the best-known examples.

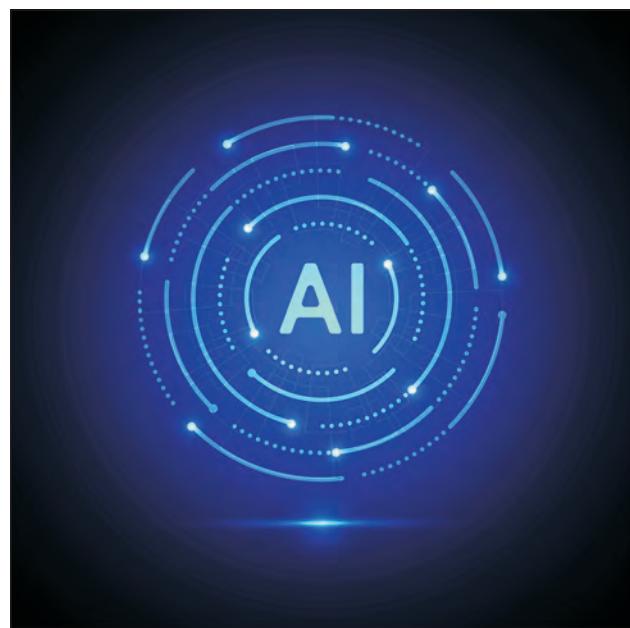


Image via iStock/royyimzy. [Used under license.]

OVERVIEW

Artificial intelligence is a broad field of study, and definitions of the field vary by discipline. For computer scientists, AI refers to the development of programs that exhibit intelligent behavior. The programs can engage in intelligent planning (timing traffic lights), translate natural languages (converting a Chinese website into English), act like an expert (selecting the best wine for dinner), or perform many other tasks. For engineers, AI refers to building machines that perform actions often done by humans. The machines can be simple, like a computer vision system embedded in an automated teller machine (ATM); more complex, like a robotic rover sent to Mars; or very complex, like an automated factory that builds an exercise machine with little human intervention. For cognitive scientists, AI refers to building models of human intelligence to better understand human behavior. In the early days of AI, most models of human intelligence were symbolic and closely related to cognitive psychology and philosophy, the basic idea being that regions of the brain perform complex reasoning by processing symbols. Later, many models of human cognition were developed to mirror the operation of the brain as an electrochemical computer, starting with the simple Perceptron, an artificial neural network described by Minsky in 1969, graduating to the backpropagation algorithm described by Rumelhart and McClelland in 1986, and culminating in a large number of supervised and nonsupervised learning algorithms.

When defining AI, it is important to remember that the programs, machines, and models developed by computer scientists, engineers, and cognitive scientists do not actually have human intelligence; they only exhibit intelligent behavior. This can be difficult to remember because artificially intelligent systems often contain large numbers of facts (e.g., weather information for New York City; complex reasoning patterns (e.g., the reasoning needed to

prove a geometric theorem from axioms); complex knowledge (e.g., an understanding of all the rules required to build an automobile); and the ability to learn (e.g., a neural network learning to recognize cancer cells). Scientists continue to look for better models of the brain and human intelligence.

HOW IT WORKS

The first activity of AI is to understand how multiple facts interconnect to form knowledge and to represent that knowledge in a machine-understandable form. The next task is to understand and document a reasoning process for arriving at a conclusion. The final component of AI is to add, whenever possible, a learning process that enhances the knowledge of a system.

Knowledge representation. Facts are simple pieces of information that can be seen as either true or false, although in fuzzy logic, there are levels of truth. When facts are organized, they become information, and when information is well understood, over time, it becomes knowledge. To use knowledge in AI, especially when writing programs, it has to be represented in some concrete fashion. Initially, most of those developing AI programs saw knowledge as represented symbolically, and their early knowledge representations were symbolic. Semantic nets, directed graphs of facts with added semantic content, were highly successful representations used in many of the early AI programs. Later, the nodes of the semantic nets were expanded to contain more information, and the resulting knowledge representation was referred to as frames. Frame representation of knowledge was very similar to object-oriented data representation, including a theory of inheritance.

Another popular way to represent knowledge in AI is as logical expressions. English mathematician George Boole represented knowledge as a Boolean expression in the 1800s. English mathematicians Bertrand Russell and Alfred Whitehead expanded

this to quantified expressions in 1910, and French computer scientist Alain Colmerauer incorporated it into logic programming, with the programming language Prolog, in the 1970s. The knowledge of a rule-based expert system is embedded in the if-then rules of the system, and because each if-then rule has a Boolean representation, it can be seen as a form of relational knowledge representation.

Neural networks model the human neural system and use this model to represent knowledge. The brain is an electrochemical system that stores its knowledge in synapses. As electrochemical signals pass through a synapse, they modify it, resulting in the acquisition of knowledge. In the neural network model, synapses are represented by the weights of a weight matrix, and knowledge is added to the system by modifying the weights.

Reasoning. Reasoning is the process of determining new information from known information. Artificial intelligence systems add reasoning soon after they have developed a method of knowledge representation. If knowledge is represented in semantic nets, then most reasoning involves some type of tree search. One popular reasoning technique is to traverse a decision tree, in which the reasoning is represented by a path taken through the tree. Tree searches of general semantic nets can be very time-consuming and have led to many advancements in tree-search algorithms, such as placing bounds on the depth of search and backtracking.

Reasoning in logic programming usually follows an inference technique embodied in first-order predicate calculus. Some inference engines, such as that of Prolog, use a back-chaining technique to reason from a result, such as a geometry theorem, to its antecedents, the axioms, and also show how the reasoning process led to the conclusion. Other inference engines, such as that of the expert system shell C language integrated production system (CLIPS), use a forward-chaining inference engine to see what facts can be derived from a set of known facts.

Neural networks, such as backpropagation, have an especially simple reasoning algorithm. The knowledge of the neural network is represented as a matrix of synaptic connections, possibly quite sparse. The information to be evaluated by the neural network is represented as an input vector of the appropriate size, and the reasoning process is to multiply the connection matrix by the input vector to obtain the conclusion as an output vector.

Learning. Learning in an AI system involves modifying or adding to its knowledge. For both semantic net and logic programming systems, learning is accomplished by adding or modifying the semantic nets or logic rules, respectively. Although much effort has gone into developing learning algorithms for these systems, all of them, to date, have used ad hoc methods and experienced limited success. Neural networks, on the other hand, have been very successful at developing learning algorithms.

Backpropagation has a robust supervised learning algorithm in which the system learns from a set of training pairs, using gradient-descent optimization, and numerous unsupervised learning algorithms learn by studying the clustering of the input vectors.

APPLICATIONS AND PRODUCTS

There are many important applications of AI, ranging from computer games to programs designed to prove theorems in mathematics. This section contains a sample of both theoretical and practical applications.

Expert systems. One of the most successful areas of AI is expert systems. Literally thousands of expert systems are being used to help both experts and novices make decisions. There are several categories of expert systems, but by far the most popular are the rule-based expert systems. Most rule-based expert systems are created with an expert system shell. The first successful rule-based expert system shell was the OPS 5 of Digital Equipment Corporation (DEC), and the most popular modern systems

are CLIPS, developed by the National Aeronautics and Space Administration (NASA) in 1985, and its Java clone, Jess, developed at Sandia National Laboratories in 1995. All rule-based expert systems have a similar architecture, and the shells make it fairly easy to create an expert system as soon as a knowledge engineer gathers the knowledge from a domain expert. The most important component of a rule-based expert system is its knowledge base of rules. Each rule consists of an if-then statement with multiple antecedents, multiple consequences, and possibly a rule certainty factor. The antecedents of a rule are statements that can be true or false and depend on facts that are either introduced into the system by a user or derived as the result of a rule being fired. For example, a fact could be red-wine and a simple rule could be if (red-wine) then (it-tastes-good). The expert system also has an inference engine that can apply multiple rules in an orderly fashion so that the expert system can draw conclusions by applying its rules to a set of facts introduced by a user. Although it is not absolutely required, most rule-based expert systems have a user-friendly interface and an explanation facility to justify its reasoning.

Theorem provers. Most theorems in mathematics can be expressed in first-order predicate calculus. For any particular area, such as synthetic geometry or group theory, all provable theorems can be derived from a set of axioms. Mathematicians have written programs to automatically prove theorems since the 1950s. These theorem provers either start with the axioms and apply an inference technique, or start with the theorem and work backward to see how it can be derived from axioms. Resolution, developed in Prolog, is a well-known automated technique that can be used to prove theorems, but there are many others. For Resolution, the user starts with the theorem, converts it to a normal form, and then mechanically builds reverse decision trees to prove the theorem. If a reverse decision tree

whose leaf nodes are all axioms is found, then a proof of the theorem has been discovered.

Gödel's incompleteness theorem (proved by Austrian-born American mathematician Kurt Gödel) shows that it may not be possible to automatically prove an arbitrary theorem in systems as complex as the natural numbers. For simpler systems, such as group theory, automated theorem proving works if the user's computer can generate all reverse trees or a suitable subset of trees that can yield a proof in a reasonable amount of time. Efforts have been made to develop theorem provers for higher order logics than first-order predicate calculus, but these have not been very successful.

Computer scientists have spent considerable time trying to develop an automated technique for proving the correctness of programs, that is showing that any valid input to a program produces a valid output. This is generally done by producing a consistent model and mapping the program to the model. The first example of this was given by English mathematician Alan Turing in 1931, by using a simple model now called a Turing machine. A formal system that is rich enough to serve as a model for a typical programming language, such as C++, must support higher order logic to capture the arguments and parameters of subprograms. Lambda calculus, denotational semantics, von Neuman geometries, finite state machines, and other systems have been proposed to provide a model onto which all programs of a language can be mapped. Some of these do capture many programs, but devising a practical automated method of verifying the correctness of programs has proven difficult.

Intelligent tutor systems. Almost every field of study has many intelligent tutor systems available to assist students in learning. Sometimes the tutor system is integrated into a package. For example, in some versions of Microsoft Office developed during the late 1990s and early 2000s, an embedded intelligent helper provided popup help boxes to a user when it

detected the need for assistance and full-length tutorials if it detected more help was needed. In addition to the intelligent tutors embedded in programs as part of context-sensitive help systems, there are a vast number of stand-alone tutoring systems in use.

The first stand-alone intelligent tutor was SCHOLAR, developed by J. R. Carbonell in 1970. It used semantic nets to represent knowledge about South American geography, provided a user interface to support asking questions, and was successful enough to demonstrate that it was possible for a computer program to tutor students. At about the same time, the University of Illinois developed its PLATO computer-aided instruction system, which provided a general language for developing intelligent tutors with touch-sensitive screens, one of the most famous of which was a biology tutorial on evolution. Of the thousands of later intelligent tutors, SHERLOCK, a training environment for electronic troubleshooting, and PUMP, a system designed to help learn algebra, are typical.

Electronic games. Electronic games have been played since the invention of the cathode-ray tube for television. In the 1980s, games such as *Solitaire*, *Pac-Man*, and *Pong* for personal computers became almost as popular as the stand-alone game platforms. By the 2020s, multiuser internet games were enjoyed by young and old alike, and game playing on mobile devices had become an important application. In all of these electronic games, the user competes with one or more intelligent agents embedded in the game, and the creation of these intelligent agents uses considerable AI. When creating an intelligent agent that will compete with a user or, as in *Solitaire*, just react to the user, a programmer has to embed the game knowledge into the program. For example, in chess, the programmer would need to capture all possible configurations of a chess board. The programmer also would need to add reasoning procedures to the game; for example,

there would have to be procedures to move each individual chess piece on the board. Finally, and most important for game programming, the programmer would need to add one or more strategic decision modules to the program to provide the intelligent agent with a strategy for winning. In many cases, the strategy for winning a game would be driven by probability; for example, the next move might be a pawn, one space forward, because that yields the best probability of winning, but a heuristic strategy is also possible; for example, the next move is a rook because it may trick the opponent into a bad series of moves.

CAREERS AND COURSEWORK

A major in computer science is the most common way to prepare for a career in AI. One needs substantial coursework in mathematics, philosophy, and psychology as a background for this degree. For many of the more interesting jobs in AI, one needs a master's or doctoral degree. Most universities teach courses in AI, neural networks, or expert systems, and many have courses in all three. Although AI is usually taught in computer science, it is also taught in mathematics, philosophy, psychology, and electrical engineering. Taking a strong minor in any field is advisable for someone seeking a career in AI because the discipline is often applied to another field.

Those seeking careers in AI generally take a position as a systems analyst or programmer. They work for a wide range of companies, including those developing business, mathematics, medical, and voice recognition applications. Those obtaining an advanced degree often take jobs in industrial, government, or university laboratories developing new areas of AI.

SOCIAL CONTEXT, ETHICS, AND FUTURE PROSPECTS

After AI was defined by McCarthy in 1956, it has had a number of ups and downs as a discipline, but

the future of AI looks good. Almost every commercial program has a help system, and increasingly these help systems have a major AI component. Health care is another area that has been poised to make major use of AI to improve the quality and reliability of the care provided, as well as to reduce its cost by providing expert advice on best practices in health care. Smartphones and other digital devices employ AI for an array of applications, syncing the activities and requirements of their users.

Ethical questions have been raised about trying to build a machine that exhibits human intelligence. Many of the early researchers in AI were interested in cognitive psychology and built symbolic models of intelligence that were considered unethical by some. Later, many AI researchers developed neural models of intelligence that were not always deemed ethical. The social and ethical issues of AI are nicely represented by HAL, the Heuristically programmed ALgorithmic computer, in Stanley Kubrick's 1968 film *2001: A Space Odyssey*, which first works well with humans, then acts violently toward them, and is in the end deactivated.

Another important ethical question posed by AI is the appropriateness of developing programs to collect information about users of a program. Intelligent agents are often embedded in websites to collect information about those using the site, generally without the permission of those using the website, and many question whether this should be done.

In the mid-to-late 2010s, fully autonomous self-driving cars were developed and tested in the United States. In 2018, an Uber self-driving car hit and killed a pedestrian in Tempe, Arizona. There was a safety driver at the wheel of the car, which was in self-driving mode at the time of the accident. While the accident led Uber to suspend its driverless-car testing program for a time, by the next year testing had resumed, initially at a smaller scale. Even before the accident occurred, ethicists had raised questions regarding collision avoidance

programming, moral and legal responsibility, among others. By mid-2020, companies such as Tesla had continued devoting resources to developing fully autonomous vehicles for eventual widespread use, but despite sustained technological advancements concerning AI, projections about getting driverless cars on the road by that point had not been met. Commentators noted that though some related technology had been incorporated into cars in use, such as automatic braking, object sensitivity, and lane detection, a lack of training data meant that the proper technology had still not been perfected for a car to be able to drive on its own reliably. Still, Waymo, which had begun implementing a commercial self-driving ride-hailing service in the Phoenix area run through a smartphone application, had made efforts to further expand the service by 2020, including adding different vehicles to its fleet and testing the program in other areas. In 2021, companies such as Waymo and Apple continued to improve their self-driving cars. Also in 2021 was the deployment of delivery robots. The company Starship announced that it had made 2 million successful deliveries while Alibaba had made 1 million. During the same year, three companies in China began deploying robotaxis without safety drivers.

As more complex AI is created and imbued with general, humanlike intelligence (instead of concentrated intelligence in a single area, such as Deep Blue and chess), it will run into moral requirements as humans do. According to researchers Nick Bostrom and Eliezer Yudkowsky, if an AI is given “cognitive work” to do that has a social aspect, the AI inherits the social requirements of these interactions. The AI then needs to be imbued with a sense of morality to interact in these situations. If an AI has humanlike intelligence and agency, then Bostrom has also theorized that AI will need to also be considered both persons and moral entities. There is also the potential for the development of

superhuman intelligence in AI, which would breed superhuman morality. The questions of intelligence and morality and who is given personhood are some of the most significant issues to be considered contextually as AI advance. Additionally, as AI technology such as facial recognition and data algorithms continued evolving and played even larger roles in society, some worried about a progressive erosion of privacy.

By 2021, following the declaration of the coronavirus 2019 (COVID-19) pandemic in early 2020, some health-care facilities had been experimenting more with incorporating AI models and algorithms into their treatment and monitoring processes in an effort to cope with the surge of illness, particularly when little was still known about the novel coronavirus and the disease it caused. However, debates still existed around such use of AI in clinical settings, and some argued that there were unsolved ethical issues and that the data used by algorithms would need consistent updating, meaning that they should be used cautiously and not fully relied upon.

In 2022, AI research group OpenAI released ChatGPT, an AI chatbot capable of generating complex responses to user prompts. In the months following its release, ChatGPT went viral for its potential real-world applications, including uses in business, research, and education. However, several flaws were soon identified with the program, including potential factual unreliability in its responses. In January 2023, NBC News reported that the New York City Department of Education had banned the use of ChatGPT in the classroom due to the program’s potential impact on student learning. (Users discovered that ChatGPT can be used to write essays, solve complex problems, and generate computer code, among other uses, which caused fears among many that students could use the program to complete their coursework.) The following month, OpenAI announced ChatGPT Plus, a subscription to

an enhanced version of the chatbot with expanded features. As ChatGPT continued to gain popularity in 2023, critics also raised concerns about the ethics of using ChatGPT and other AI-based tools to create written and visual works.

—George M. Whitson III

Further Reading

- Audry, Sofian. *Art in the Age of Machine Learning*. MIT Press, 2021.
- Basl, John. "The Ethics of Creating Artificial Consciousness." *American Philosophical Association Newsletters: Philosophy and Computers*, vol. 13, no. 1, 2013, pp. 25–30.
- Belani, Gaurav. "The Use of Artificial Intelligence in Cybersecurity: A Review." *IEEE Computer Society*, www.computer.org/publications/tech-news/trends/the-use-of-artificial-intelligence-in-cybersecurity.
- Berlatsky, Noah. *Artificial Intelligence*. Greenhaven Press, 2011.
- Bostrom, Nick. "Ethical Issues in Advanced Artificial Intelligence." *NickBostrom.com*, 2003, nickbostrom.com/ethics/ai.html.
- Bostrom, Nick, and Eliezer Yudkowsky. "The Ethics of Artificial Intelligence." *The Cambridge Handbook of Artificial Intelligence*, edited by Keith Frankish and William M. Ramsay, Cambridge UP, 2014, pp. 316–34.
- Heikkilä, Melissa. "The Algorithm: AI-Generated Art Raises Tricky Questions about Ethics, Copyright, and Security." *MIT Technology Review*, 20 Sept. 2022, www.technologyreview.com/2022/09/20/1059792/the-algorithm-ai-generated-art-raises-tricky-questions-about-ethics-copyright-and-security.
- Laalaoui, Yacine, and Nizar Bouguila, editors. *Artificial Intelligence Applications in Information and Communication Technologies*. Springer International Publishing, 2015.
- Lee, Timothy B. "Why It's Time for Uber to Get Out of the Self-Driving Car Business." *Ars Technica*, 27 Mar. 2018, arstechnica.com/cars/2018/03/ubers-self-driving-car-project-is-struggling-the-company-should-sell-it.
- Metz, Cade. "OpenAI to Offer New Version of ChatGPT for a \$20 Monthly Fee." *New York Times*, 1 Feb. 2023, www.nytimes.com/2023/02/01/technology/openai-chatgpt-plus-subscription.html.
- Miller, Arthur I. *The Artist in the Machine: The World of AI-Powered Creativity*. MIT Press, 2019.
- Minsky, Marvin, and Seymour A. Papert. *Perceptrons: An Introduction to Computational Geometry*. Reissue ed., MIT Press, 2017.
- Morrison, Jim. "How Doctors Are Using Artificial Intelligence to Battle Covid-19." *Smithsonian Magazine*, 5 Mar. 2021, www.smithsonianmag.com/science-nature/how-doctors-are-using-artificial-intelligence-battle-covid-19-180977124.
- Nyholm, Sven, and Jilles Smids. "The Ethics of Accident-Algorithms for Self-Driving Cars: An Applied Trolley Problem?" *Ethical Theory & Moral Practice*, vol. 19, no. 5, 2016, pp. 1275–89.
- Rosenblatt, Kalhan. "ChatGPT Banned from New York City Public Schools' Devices and Networks." *NBC News*, 5 Jan. 2023, www.nbcnews.com/tech/tech-news/new-york-city-public-schools-ban-chatgpt-devices-networks-rcna64446.
- Rumelhart, David E., James L. McClelland, and the PDP Research Group. *Parallel Distributed Processing: Explorations in the Microstructure of Cognition*. 1986. MIT Press, 1989. 2 vols.
- Russell, Stuart, and Peter Norvig. *Artificial Intelligence: A Modern Approach*. 4th ed. Pearson, 2020.
- Templeton, Brad. "Self-Driving Cars 2021: Year in Review." *Forbes*, 3 Jan. 2022, www.forbes.com/sites/bradtempleton/2022/01/03/self-driving-cars-2021-year-in-review/?sh=4aa85563773b.

ARTIFICIAL INTELLIGENCE AND TERRORISM

ABSTRACT

For all of the benefits that are believed will come with the development of artificial intelligence, or AI, there is also a “dark side” to the technology. The worst of the possible uses of AI, and the most worrisome, is the use of AI in committing acts of terrorism.

BACKGROUND

What is terrorism? In its basest and most visceral form, acts of terrorism are carried out against people—men, women, and children—who are unsuspecting and innocently going through their day or

night as best they can. It should be noted here that it does not matter what is the ideology driving an act of terrorism, nor the national or ethnic stripe of the perpetrators; any act that can be described as above, intended to instill a sense of demoralizing fear in a population, qualifies as an act of terrorism. The firebombing of the beautiful, old city of Dresden in Germany during World War II by Allied forces was as much an act of terrorism as was the attack on the World Trade Center in New York in 2001 by Islamic fanatics, or the bombing carried out by Timothy McVeigh that killed a large number of innocents, including dozens of small children in the targeted Federal Bureau of Investigation (FBI) center's daycare facility.

These are the kinds of acts people think of when they speak of terror attacks. But it is doubtful that any kind of advanced artificial intelligence (AI) played any role in such dramas. The role in terrorism of AI, if it is used, will be infinitely more subtle, and more devastating. Terrorism's goal is to cause upheaval in the target's society. For the advanced societies that would actually be able to develop advanced AI systems, and those that would acquire them, terrorism would not involve explosions such as those mentioned nor the unleashing of nuclear weapons on an unsuspecting target. One has only to consider what makes a society—any society—stable and prosperous.

Our present society, as well as those in other parts of the world with its globalized system of trade and commerce, depends on so-called democratically elected governments enforcing the “rule of law” to keep its population safe and its economy functioning as smoothly as possible. This requires a constant and stable supply of energy as electricity to be available in any particular country. In North America, control of the electrical grid system is maintained through the use of computer systems at all levels, and interconnections between them abound as the system spans essentially all of North America. The

electricity that powers this grid comes from a variety of sources, including hydroelectric dams, coal-, gas- or oil-fired generating plants, solar farms, and nuclear power plants. Many of the processes involved in the operation of these facilities are automated under computer control, though overseen by human operators. But human operators are fallible, as has been amply demonstrated by events at Chernobyl, Three Mile Island, Fukushima Daiichi, and various other nuclear facilities that did not get reported in the news media. Imagine the chaos that would result should a terrorist organization acquire and use an advanced AI system—not to take over such facilities—but simply to interfere randomly with their operation and interrupting the power supply (e.g., shutting down hospitals during critical surgeries, traffic during rush hour, banking systems, transit systems, factories, and any number of other things that rely on the constancy of the electrical grid). Worse, imagine the consequences if such AI-empowered terrorists were to not just affect control of the electrical grid in its operation, but at the various sources of the electricity itself. Picture a scenario in which the AI would be able to make all of the status indicators of a nuclear plant indicate that it is operating within safe limits when in actuality it has drained the coolant from the reactor core housing. That is potentially a Chernobyl-like event that would happen in many places across the continent. Or perhaps it could lock out the coal feeding systems of coal-fired plants, causing them to shut down or to overheat. The possibilities for any number of different scenarios are endless, and every one of them can have disastrous consequences for an advanced technological society.

These are ambitious theoretical scenarios. Far more plausible are small scale acts of AI terrorism, such as the use of AI to disseminate false information that affects how societies are governed. This could be false information given to media outlets and intended to steer the population toward division

and destabilization. Or it could be the generation of false documents and records—or the elimination of actual records demonstrating corruption and other criminal activities. It can also be, and indeed it has been, the growing problem of data theft as AI systems are used to break into the data repositories of financial and governmental institutions. Every year, there are reports that an institution's cybersecurity protocol has been breached and large amounts of confidential personal and financial information has been taken. This becomes ever easier as AI systems become more capable. At a minimum, individuals can see their life savings vanish in an instant. At worst, the targeted institution could be forced to collapse. Encryption is a valuable deterrent, but it is not a guarantee. It is a simple tenet in cybersecurity than anything that can be done can be undone. A sufficiently powerful AI system using an equally powerful algorithm would be able to take apart the 256-bit encryption currently being used, rendering it useless. Quantum computers, once fully developed, will be able to carry out the computations that would be necessary to break the encryption thousands of times faster than the most powerful supercomputers in the world today.

This would be the tool of a government bent on destroying the economic power of another nation, or even the nation itself. In the twenty-first century, attempts have been made to compromise the stability of the United States by Russia, China, North Korea, and even by homegrown American terrorists. On the other side of the world, a virus called Stuxnet appeared on the computers that control the operation of the gas centrifuges in Iran's uranium enrichment plants. One has to wonder about the extent of AI involvement in these planned attacks.

OVERVIEW

What about the role AI could play with its own kind of inadvertent terrorism? In August 2023, the AI program called Blenderbot 3, from Meta, falsely

labeled well-respected longtime journalist and political scientist Marietje Schaake a terrorist. The error was quickly corrected, but not quickly enough to prevent that designation from reaching officials in different countries. In a televised interview, Schaake explained that in its workings to answer the simple question "Who is a terrorist?" it had associated her name with the word "terrorist" based on online research she had carried out, ironically enough, about AI and terrorism. This is not the only incident of AI providing very wrong information, but it is perhaps the best example of the kind of inadvertent terrorism that could result from the current state of AI development. What could be more terrifying to an unsuspecting individual and her or his family than to be erroneously labeled as a terrorist, especially if that were to happen while they were visiting a foreign country where suspected terrorists are not treated with any leniency? And, what a disaster it would be if an AI began randomly identifying innocent travelers as terrorists in large numbers!

In its own way, AI has the potential to create both terrorism and terrorists, simply because it exists. In the eighteenth century, when powered looms began to replace master weavers in the factories, the weavers rose up violently behind a mythical weaver named Ned Ludd, hence gaining for them the appellation "Luddites," which has since come to refer to those opposed to "the machine." In his novel *1984*, George Orwell's antisocialist allegory, he introduced the concept of "Big Brother," the entity that watches everyone and everything in society. In the present day we now have AI programs that have that same ability and may in fact already be watching like Orwell's "Big Brother." One has to wonder if this could eventually incite a kind of modern-day Luddism in which, ironically, humanity rises up against the machine? This is speculation, of course, but given the state of AI at present and its verifiable potential for creating a kind of chaos that is the hallmark of terrorism, it would be prudent for

developers to build better safeguards into future AI programs, hopefully preventing their use as tools of terrorism.

—Richard M. Renneboog

Further Reading

- Cronin, Audrey Kurth. *Power to the People: How Open Technological Innovation Is Arming Tomorrow's Terrorists*. Oxford UP, 2019.
- Hoffman, Bruce. *Inside Terrorism*. Columbia UP, 2006.
- Hsu, Tiffany. "What Can You Do When AI Lies About You?" *New York Times*, 7 Aug. 2023, www.nytimes.com/2023/08/03/business/media/ai-defamation-lies-accuracy.html.
- Institute for Economics and Peace. *Global Terrorism Index 2022: Measuring the Impact of Terrorism*. Institute for Economics and Peace, 2022.
- Montasari, Reza. *Countering Cyberterrorism: The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity*. Springer Nature, 2023.
- Montasari, Reza, editor. *Artificial Intelligence and National Security*. Springer Nature, 2022.

ARTIFICIAL INTELLIGENCE COLD WAR

ABSTRACT

The term “artificial intelligence cold war” refers to rivalries between multiple nations in developing artificial intelligence (AI) to attack and cripple one another. Experts suggest an AI arms race, or development of military uses of AI by the United States, China, and Russia (formerly the Soviet Union), could involve disinformation campaigns or create chaos by targeting critical infrastructure, satellite security, or software supply chains.

BACKGROUND

“Artificial intelligence cold war” is the rivalry between multiple nations in developing artificial intelligence (AI) to attack and cripple one another. Use of the term “cold war” is a reference to the Cold

War between the United States and Union of Soviet Socialist Republics (USSR, or Soviet Union) following World War II. This was an era when both countries engaged in an arms race as a means of deterring the other from attacking.

The primary focus of the first Cold War, which began in 1947 and ended in 1991 with the breakup of the Soviet Union, was buildup of defenses and weaponry. This buildup was based on the principle of mutually assured destruction (MAD), or the idea that if one superpower launched a nuclear attack on another, the aggressor would be destroyed by a nuclear counterattack. In short, both would be destroyed. This principle was believed to be a means to deter attacks. The United States built tens of thousands of nuclear weapons. Long after the Cold War ended, in the 2020s the country continued to spend \$70 billion a year to maintain these weapons. A second cold war likely would involve cyberattacks on critical infrastructure, disinformation campaigns, satellite attacks, and threats to software supply chains.

Much discussion about an AI cold war dates to the late 2010s. The US government published several reports about AI, laying out benefits and risks of the technology and making recommendations for the government response to advances in the private sector. Among the recommendations were suggestions about investing in machine learning development efforts and exploring ways to cut job losses that would result from increased automation. In China, science and technology policy advisers had for some time been developing a national plan for AI. They viewed these new US papers developed by the administration of President Barack Obama as an indication that the United States was developing an AI strategy and increased their efforts.

The Chinese people had become interested in AI in early 2016, when an AI system faced off against a world champion Go player in Seoul, South Korea, and won. Go is an Asian board game created more



Image via iStock/blackdovfx. [Used under license.]

than three thousand years ago in China but little known in the West. The AI, AlphaGo, was developed by DeepMind, a division of the American tech company Alphabet, which also owns Google. About 280 million people in China watched the match. They were aghast at the implications of an AI from a country where few people play Go defeating a South Korean champion. The stakes increased in early 2017 when AlphaGo defeated a Chinese master of Go at the Future of Go Summit in China.

Several weeks after the summit, China's central government published its Next Generation Artificial Intelligence Development Plan. This document was the government's plan to become a world leader in AI by 2030. Various branches of government and local governments around the country followed by developing complementary plans based on Beijing's stated goals. The government used Chinese tech companies to make the end goals possible. The

government enlisted Alibaba, an online retailer, to develop an AI for a new Special Economic Zone. Already, Alibaba had been collecting data using street cameras in the city of Hangzhou and was using AI to control signal lights to make the flow of traffic as efficient as possible. The company went to work designing AI into the infrastructure of the new Special Economic Zone city. In October 2017, President Xi Jinping publicly stated his plans for the future of the Communist Party. Artificial intelligence, big data, and the internet were at the heart of his plans to make China an even bigger player in the world's economy.

While this was happening, the US government under President Donald Trump gave scant attention to AI technology and moved the AI reports to an archived website. In March 2017, Treasury Secretary Steven Mnuchin said it would be fifty to one hundred years before humans would lose jobs because of

AI. However, the Pentagon pressured the administration to fund a government commission to study AI, and soon the possibility of an AI cold war arms race emerged in international discussions.

OVERVIEW

Experts suggest that an AI arms race, or development of military uses of AI by the United States, China, and Russia, would amount to a second Cold War. Some potential attacks could involve disinformation campaigns or create chaos by targeting critical infrastructure, satellite security, or software supply chains. While a great deal of discussion and speculation about an AI cold war has occurred, experts disagree on whether an AI military race is already taking place. In 2021, the United Nations (UN) reported that an autonomous drone, or lethal autonomous weapons system (LAWS), was used in combat in Libya; however, the organization was unsure if the drone was used to kill.

In the 2020s, most scrutiny and discussion of an AI cold war focused on the United States and China; many analysts discounted Russia's likelihood of excelling in technological development. This assessment came about in part because of sanctions levied against Russia when it annexed Crimea in 2014. Other factors were demographic analysis that found Russia's population to be declining and an ongoing "brain drain" in which educated individuals pursued careers offering greater opportunities and pay in other countries. Moscow devoted a fraction of the funding toward technology that China and the United States allocated, but Russia excelled in disinformation campaigns, and AI technology had the potential to boost its capacity.

The US Congress created the National Security Commission on Artificial Intelligence (NSCAI) in 2018 to make recommendations about developing AI and related technologies in the interests of national security and defense. The independent commission's report in March 2021 concluded that

the country was unprepared for any attacks by or competition with China and suggested that AI technologies be integrated into all areas of combat. This was in opposition to discussions across the Atlantic. About the same time, European authorities were focused on legal guidelines toward ensuring AI use was ethical and secure. The European Parliament advised nations to ensure that military systems do not substitute human decision-making with AI. Thousands of researchers in AI and robotics strenuously opposed permitting AI to decide when to kill.

Some consequences of the AI cold war have already emerged. As was the case during the twentieth-century Cold War, countries that do not have their own technology have begun to choose sides. Many have made statements with their choices of partners in projects. For example, Pakistan partnered with Chinese companies to install a fiber-optic cable between China and Pakistan and for installation of surveillance cameras in cities in the name of public safety. China wins because it is paid for these systems and gains access to troves of data.

Experts say some incidents that have taken place in modern times highlight the importance of being vigilant and continuing research. For example, adversaries have struck and exposed a few of the weaknesses in US infrastructure and security. Some vulnerable targets include the power grid and water supplies. Analysts say that some types of attacks, such as hacking satellites, could qualify as acts of war. Control of satellites could enable threat actors to scramble geospatial data or sabotage systems such as air traffic, banking, cloud storage, and power grids. Experts warn that these and similar acts could tip the geopolitical sphere and create conditions similar to those that preceded World War I and World War II in the early twentieth century.

Digital disinformation campaigns have become the tool of choice for actors wishing to spread propaganda. Artificial intelligence can alter images and videos to create what are called "deepfakes." When

Russia attacked Ukraine in early 2022, some actors produced deepfake videos that attempted to persuade Ukrainian troops to surrender. Many times, individuals have trouble recognizing these as fake. Experts say that in time, deepfakes may become nearly impossible to differentiate from genuine videos and images.

FURTHER INSIGHTS

Computers learn to make independent decisions using AI. The computer must learn rules and be exposed to data, such as ways to strategize in chess. Artificial intelligence is the machine's ability to learn, plan, reason, and be creative. The two types of AI are software and embodied. Examples of AI software include face recognition systems, search engines, and virtual assistants. For example, AI offers personalized suggestions based on previous searches that an individual conducts. Embodied AI include autonomous vehicles, drones, robots, and internet-connected household appliances. Countries that invest in AI technologies become more efficient and therefore more prosperous. For this and other reasons, the world's superpowers have pursued superiority in the field of AI development.

Military systems and law enforcement have used some applications of AI for some time. For example, AI facial recognition software is used for surveillance in some cities and countries. China uses such software and has sold the technology to other countries. This AI use in surveilling the general population is often viewed as intrusive and a violation of human rights. The US military, and the military systems of other countries, has used AI in a variety of roles for years. The public learned in 2017 about the US military's Project Maven, which is an object recognition program, and robots have been added to security patrols at military facilities. Analysts expect near-future uses of autonomous systems to focus on reconnaissance work to avoid

endangering troops. The US Department of Defense has for some time used AI to analyze footage collected by drones and moved on to doing the same with images from satellites. In early 2022 the US Department of Defense used AI to analyze publicly available imagery to aid Ukraine when Russia attacked the country. It simultaneously analyzed its data about this AI analysis to refine the software and was developing new modeling systems to try to understand what warfare of the future will look like and how it will progress. The poor showing of Russia's military and resulting sanctions suggested its AI development would slow, so officials were primarily examining the potential of China.

Some AI applications to warfare will likely involve rapid analysis of data to discover opponents' military strengths, discern weak points, and track and predict troop movements. Artificial intelligence would aid in determining the best times and means to attack or when to withdraw and could be used to analyze movements. For example, AI could determine if a truck might be attacking or is likely to contain explosives. These applications are expected to lead to fully autonomous fighting systems. Some analysts suggest that AI systems can also be programmed to use only necessary force, which could protect many civilians from violence.

Analysts predict that future conflicts may be unbalanced because of AI capabilities. Asymmetric warfare is conflict between forces with military power that is so greatly unequal that they cannot attack one another in the same way. Many countries have experienced asymmetric warfare, typically involving a conventional army fighting a guerrilla force. Suicide bombings and other forms of terrorism are also examples of asymmetric warfare. AI-driven asymmetric warfare (ADAW) will involve one party having at its disposal vastly superior, rapid intelligence gathering and analysis.

—Josephine Campbell

Further Reading

- Bendett, Samuel. "Russia's Artificial Intelligence Boom May Not Survive the War." *Center for a New American Security*, 15 Apr. 2022, www.cnas.org/publications/commentary/russias-artificial-intelligence-boom-may-not-survive-the-war.
- Heath, Ryan. "Artificial Intelligence Cold War on the Horizon." *Politico*, 16 Oct. 2020, www.politico.com/news/2020/10/16/artificial-intelligence-cold-war-on-the-horizon-429714.
- Hernandez, Joe. "A Military Drone with a Mind of Its Own Was Used in Combat, U.N. Says." *NPR*, 1 June 2021, www.npr.org/2021/06/01/1002196245/a-u-n-report-suggests-libya-saw-the-first-battlefield-killing-by-an-autonomous-d.
- Lague, David. "In U.S.-China AI Contest, the Race Is on to Deploy Killer Robots." *Reuters*, 8 Sept. 2023, www.reuters.com/investigates/special-report/us-china-tech-drones.
- Manson, K. "US Has Already Lost AI Fight to China, Says Ex-Pentagon Software Chief." *Financial Times*, 10 Oct. 2021, www.ft.com/content/f939db9a-40af-4bd1-b67d-10492535f8e0.
- Piper, Steve. "Four Critical Risks to Watch as Experts Predict a Cyber Cold War." *Forbes*, 23 May 2022, www.forbes.com/sites/forbestechcouncil/2022/05/23/four-critical-risks-to-watch-as-experts-predict-a-cyber-cold-war.
- Polyakova, Alina. "Weapons of the Weak: Russia and AI-Driven Asymmetric Warfare." *Brookings Institution*, 15 Nov. 2018, www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare.
- Raska, Michael, Katarzyna Zysk, and Ian Bowers, editors. *The Fourth Industrial Revolution: Security Challenges, Emerging Technologies, and Military Implications*. Routledge, 2022.
- Thompson, Nicholas, and Ian Bremmer. "The AI Cold War That Threatens Us All." *Wired*, 23 Oct. 2018, www.wired.com/story/ai-cold-war-china-could-doom-us-all.
- Tucker, Patrick. "AI Is Already Learning from Russia's War in Ukraine, DOD Says." *Defense One*, 21 Apr. 2022, www.defenseone.com/technology/2022/04/ai-already-learning-russias-war-ukraine-dod-says/365978.

AUTONOMOUS CARS

ABSTRACT

An autonomous car, also known as a “robotic car” or “driverless car,” is a vehicle designed to operate without the guidance or control of a human driver. Engineers began designing prototypes and control systems for autonomous vehicles as early as the 1920s, but the development of the modern autonomous vehicle began in the late 1980s. Proponents of autonomous car technology believe that driverless vehicles will reduce the incidence of traffic accidents, reduce fuel consumption, alleviate parking issues, and reduce car theft, among other benefits. One of the most significant potential benefits of “fully autonomous” vehicles is to provide independent transportation to disabled individuals who are not able to operate a traditional motor vehicle. Potential complications or problems with autonomous vehicles include the difficulty in assessing liability in the case of accidents, a reduction in the number of driving-related occupations available to workers, and the risk that such vehicles could be hacked or otherwise compromised by malicious parties.

BACKGROUND

Autonomous car technology has its origins in the early twentieth century, when a few automobile manufacturers, inspired by science fiction, envisioned futuristic road systems embedded with guidance systems that could be used to power and navigate vehicles through the streets. For instance, the Futurama exhibit at the 1939 New York World’s Fair, planned by designer Norman Bel Geddes, envisioned a future where driverless cars would be guided along electrically charged roads.

Until the 1980s, proposals for autonomous vehicles involved modifying roads with the addition of radio, magnetic, or electrical control systems. During the 1980s, automobile manufacturers working with university engineering and computer science programs began designing autonomous vehicles that

were self-navigating, rather than relying on modification of road infrastructure. Bundeswehr University in Munich, Germany produced an autonomous vehicle that navigated using cameras and computer vision. Similar designs were developed through collaboration between the US Defense Advanced Research Projects Agency (DARPA) and researchers from Carnegie Mellon University. Early prototypes developed by DARPA used LIDAR, a system that uses lasers to calculate distance and direction. In July 1995, the NavLab program at Carnegie Mellon University produced one of the first successful tests of an autonomous vehicle, known as “No Hands Across America.”

The development of American autonomous vehicle technology accelerated quickly between 2004 and 2007 due to a series of research competitions, known as “Grand Challenges,” sponsored by DARPA. The 2007 event, called the “Urban Challenge,” drew eleven participating teams designing

vehicles that could navigate through urban environments while avoiding obstacles and obeying traffic laws; six designs successfully navigated the course. Partnerships formed through the DARPA challenges resulted in the development of autonomous car technology for public use. Carnegie Mellon University and General Motors partnered to create the Autonomous Driving Collaborative Research Lab, while rival automaker Volkswagen partnered with Stanford University on a similar project.

Stanford University artificial intelligence expert Sebastien Thrun, a member of the winning team at the 2005 DARPA Grand Challenge, was a founder of technology company Google’s “Self-Driving Car Project” in 2009, which is considered the beginning of the commercial phase of autonomous vehicle development. Thrun and researcher Anthony Levandowski helped to develop “Google Chauffeur,” a specialized software program designed to navigate using laser, satellite, and computer vision



Photo via iStock/metamorworks. [Used under license.]

systems. Other car manufacturers, including Audi, Toyota, Nissan, and Mercedes, also began developing autonomous cars for the consumer market in the early 2010s. In 2011, Nevada became the first state to legalize testing autonomous cars on public roads, followed by Florida, California, the District of Columbia, and Michigan by 2013.

OVERVIEW

In May of 2013, the United States Department of Transportation's National Highway Traffic Safety Administration (NHTSA) released an updated set of guidelines to help guide legal policy regarding autonomous vehicles. The NHTSA guidelines classify autonomous vehicles based on a five-level scale of automation, from zero, indicating complete driver control, to four, indicating complete automation with no driver control.

Between 2011 and 2016, several major manufacturers released partially automated vehicles for the consumer market, including Tesla, Mercedes-Benz, BMW, and Infiniti. The Mercedes S-Class featured automated options including parking assistance, lane correction, and a system to detect when the driver may be at risk of fatigue. Such features became increasingly common in consumer vehicles in the years that followed.

According to a November 2014 article in the *New York Times*, most manufacturers exploring autonomous vehicles at that time were developing vehicles that would require "able drivers" to sit behind the wheel, even though the vehicle's automatic systems would operate and navigate the car. Google's "second generation" autonomous vehicles were an exception, as the vehicles lacked steering wheels or other controls, therefore making human intervention impossible. According to Google, complete automation would reduce the possibility that human intervention will lead to driving errors and accidents. Google argued further that fully autonomous vehicles could open the possibility of independent

travel to the blind and individuals suffering from a variety of other disabilities that impair the ability to operate a car. In September 2016 Uber launched a test group of automated cars in Pittsburgh, Pennsylvania. They started with four cars that had two engineers in the front seats to correct errors. The company rushed to be the first to market and planned to add additional fully automated cars to the fleet.

Modern autonomous vehicles utilize laser guidance systems, a modified form of LIDAR, as well as global positioning system (GPS) satellite tracking, visual computational technology, and software that allows for adaptive response to changing traffic conditions. Companies at the forefront of automated car technology are also experimenting with computer software designed to learn from experience, thereby making the vehicle's onboard computer more responsive to driving situations following encounters.

While Google was optimistic about debuting autonomous cars for public use by 2020, other industry analysts were skeptical about this, given the significant regulatory difficulties that would need to be overcome before driverless cars could become a viable consumer product. A 2014 poll from Pew Research indicated that approximately 50 percent of Americans were not currently interested in driverless cars. Other surveys also indicated that a slight majority of consumers were uninterested in owning self-driving vehicles, though a majority of consumers approved of the programs to develop the technology. A survey conducted two years later by New Morning Consult showed a similar wariness of self-driving cars, with 43 percent of registered voters considering autonomous cars unsafe.

Proponents of autonomous vehicles have cited driver safety as one of the chief benefits of automation. The RAND Corporation's 2014 report on autonomous car technology cites research indicating that computer-guided vehicles will reduce the incidence and severity of traffic accidents, congestion,

and delays, because computer-guided systems will be more responsive than human drivers and are immune to driving distractions that contribute to a majority of traffic accidents. Research also indicates that autonomous cars will help to conserve fuel, reduce parking congestion, and will allow consumers to be more productive while commuting by freeing them from the job of operating the vehicle.

The first fatal accident in an autonomous car happened in July 2016, when a Tesla in automatic mode crashed into a truck. The driver was killed. A second fatal accident involving a Tesla in autonomous mode occurred in early 2018. The first fatal accident involving an autonomous car and a pedestrian occurred in March 2018, when one of Uber's autonomous cars struck and killed a pedestrian in Tempe, Arizona. Uber suspended its road tests after the incident but resumed testing its vehicles on public streets by mid-2020.

Throughout the next several years, both technology start-ups and major automobile manufacturers such as General Motors and Nissan continued their efforts to develop fully autonomous vehicles, including passenger cars and tractor trailers. The parent company of Google, Alphabet, remained active in that space through its subsidiary Waymo, which formed in 2016 out of the Google Self-Driving Car Project and began testing autonomous vehicles on public roads in 2017. In May of 2023, Waymo and Uber formed a partnership that would result in the use of Waymo-produced fully autonomous taxis as rideshare vehicles. The vehicles began operating in Phoenix, Arizona, in October of that year.

IMPACT

The development of autonomous cars will likely take longer than researchers initially anticipated, when companies began testing this technology in recent years. The potential benefits are numerous: fewer traffic accidents, decreased traffic congestion, and economic gains caused by increased transportation

efficiency. However, as with any new technology, there are also potential risks: unemployment in the transportation sector, hackers taking over vehicles, and liability issues.

The most significant issue faced by companies looking to create and sell autonomous vehicles is the issue of liability. Before autonomous cars can become a reality for consumers, state and national lawmakers and the automotive industry must debate and determine the rules and regulations governing responsibility and recourse in the case of automated system failure.

—Micah L. Issitt

Further Reading

- Anderson, James M., et al. "Autonomous Vehicle Technology: A Guide for Policymakers." *RAND*, 2014, www.rand.org/pubs/research_reports/RR443-2.html.
- Bogost, Ian. "The Secret History of the Robot Car." *The Atlantic*, 14 Oct. 2014, www.theatlantic.com/magazine/archive/2014/11/the-secret-history-of-the-robot-car/380791.
- Capoot, Ashley, and Jake Piazza. "Uber Begins Offering Rides in Self-Driving Waymo Cars." *CNBC*, 26 Oct. 2023, www.cnbc.com/2023/10/26/uber-begins-offering-rides-in-self-driving-waymo-cars.html.
- Davies, Alex. "In 20 Years, Most New Cars Won't Have Steering Wheels or Pedals." *Wired*, 21 July 2014, www.wired.com/2014/07/in-20-years-most-new-cars-wont-have-steering-wheels-or-pedals.
- Hayes, Adam. "The Unintended Consequences of Self-Driving Cars." *Investopedia*, 31 Aug. 2021, www.investopedia.com/articles/investing/090215/unintended-consequences-selfdriving-cars.asp.
- Kagubare, Ines. "Increasingly Autonomous Cars Raise Cybersecurity Fears." *Hill*, 8 June 2022, thehill.com/driving-into-the-future/3514634-increasingly-autonomous-cars-raise-cybersecurity-fears.
- Moon, Mariella. "Now California's DMV Can Allow Fully Driverless Car Testing." *Engadget*, 3 Apr. 2018, www.engadget.com/2018/04/03/california-fully-driverless-car-testing.
- Ramsey, Mike. "Tesla CEO Musk Sees Fully Autonomous Car Ready in Five or Six Years." *Wall Street Journal*, 17 Sept. 2014, www.wsj.com/articles/tesla-ceo-sees-fully-autonomous-car-ready-in-five-or-six-years-1410990887.

Smith, Aaron. "U.S. Views of Technology and the Future." *Pew Research*, 17 Apr. 2014, www.pewresearch.org/internet/2014/04/17/us-views-of-technology-and-the-future.

Stenquist, Paul. "In Self-Driving Cars, a Potential Lifeline for the Disabled." *New York Times*, 7 Nov. 2014, www.nytimes.com/2014/11/09/automobiles/in-self-driving-cars-a-potential-lifeline-for-the-disabled.html.

Vanderbilt, Tom. "Autonomous Cars through the Ages." *Wired*, 6 Feb. 2012, www.wired.com/2012/02/autonomous-vehicle-history.

Wakabayashi, Daisuke. "Uber's Self-Driving Cars Were Struggling before Arizona Crash." *New York Times*, 23 Mar. 2018, www.nytimes.com/2018/03/23/technology/uber-self-driving-cars-arizona.html.

B

BIG DATA

ABSTRACT

In the cutting-edge world of data retrieval systems, big data refers to the sheer mass of data produced daily by and within global computer networks at a pace that far exceeds the capacity of current databases and software programs to organize and process. Virtually any organization that gathers information—government, businesses, retail stores, services, hospitals, social media outlets—faces an enormous challenge in gathering information that is generated at massive rates every minute, reading that data into meaningful and coherent information, and then storing it efficiently and effectively. Given that the number of qualified computer software engineers savvy in this burgeoning field is far below industry needs, the strategies for directing and controlling big data represent a primary challenge to those who rely on computers for operating information.

BACKGROUND

The amount of information processed by computer networks globally every day is measured in terabytes (1 trillion bytes) and petabytes (1 quadrillion bytes). Such information includes general information, statistics, medical records, science and research data, phone records, business records, government records, and many other types of data. Data generation on that scale is measured four ways: (1) the variety of the information available (from cell phone records to air travel information, from social network inputs to stock trading); (2) the volume of information produced, measured per second; (3) the velocity at which the information is produced; and (4) its veracity (i.e., its meaningfulness). The ability to harness and direct that information represents an

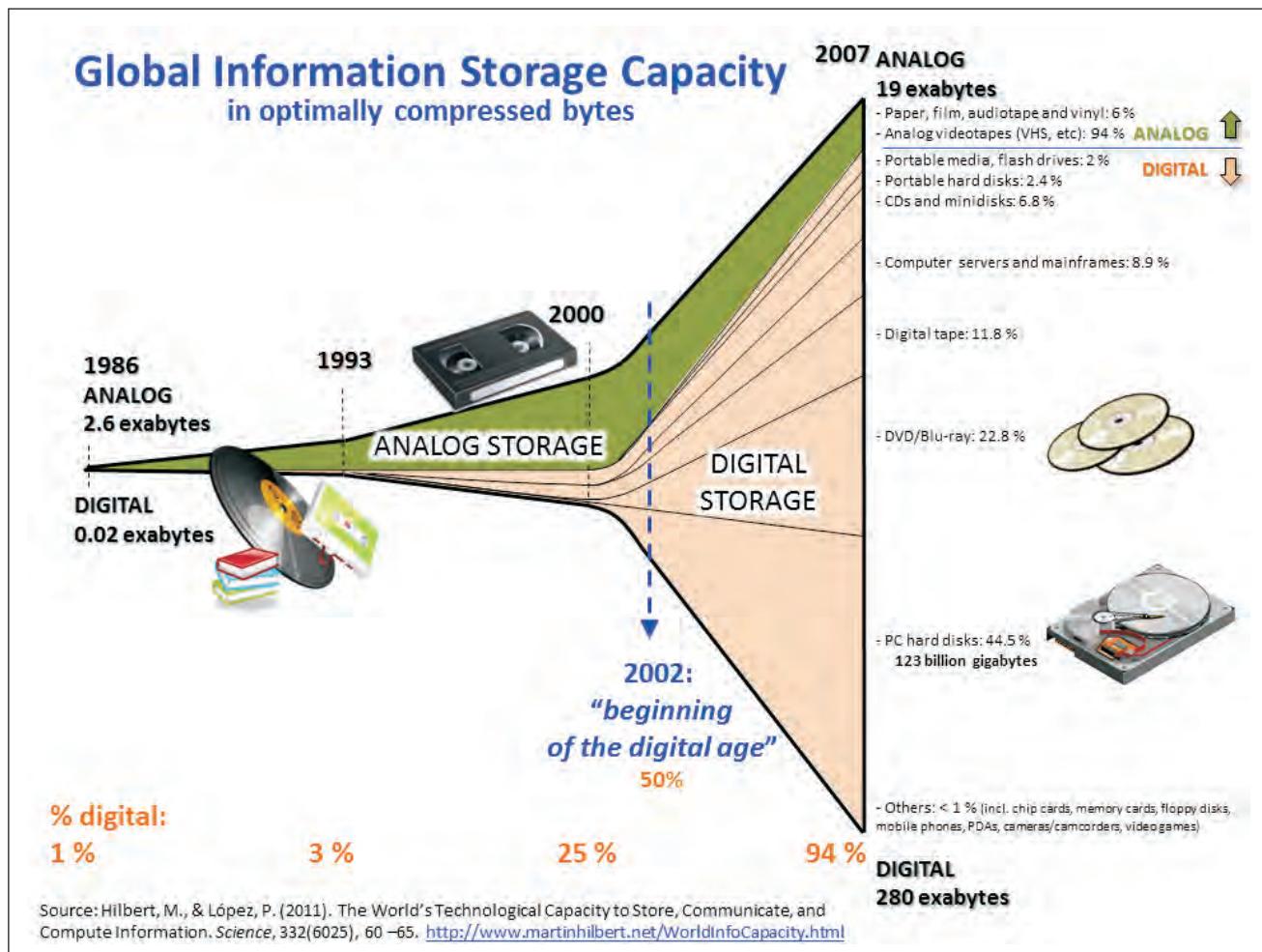
entirely new paradigm for virtually any organization from governments to businesses, from hospitals to school systems. The potential rewards are significant. Any interaction with computers—smartphones, e-readers, digital music players, tablets, laptops, internet searches—generates data about individuals.

OVERVIEW

Data about individuals is useful to businesses seeking to direct their resources most favorably, from accumulating customer profiles to directing product development and marketing. In the media and entertainment industries, for instance, companies analyze user data to glean insight into the media consumed by different demographics as well as user behavior. Data analytics is likewise a critical component of business operations within social media companies as well as in the field of advertising.

Beyond media and entertainment, big data could have numerous far-reaching research applications. Big data research could be directed toward the global monitoring of potential terrorist activities, given that chatter from such sources is nearly constant. Medical records could be synthesized and coordinated globally with and against available research data about treatments. Government records could be streamlined, and government services could be made far more efficient. Organization performance could be boosted, records could be made more accessible, and networks could communicate effectively across traditional boundaries. Information itself could become fluid and transparent.

Critics of big data research, however, point to a Big Brother scenario, in which intrusion into privacy



Non-linear growth of digital global information-storage capacity and the waning of analog storage. Image by Myworkforwiki, via Wikimedia Commons.

could proceed unchecked. All computer activity could be monitored and theoretically stored by the government, by employers, by businesses—really by anyone with access to what would become unprecedentedly massive data reservoirs. In addition, such widespread harvesting of information creates new threats to intellectual property rights and copyright infringements. Gathering data, these critics point out, is not effectively analyzing it, thus stripping the data from the sociocultural context that provides its true meaning. People, they argue, are more than data points.

In recognition of the privacy and security ramifications of data collection and research, some governments introduced regulations governing the collection and use of individuals' data. One such regulation was the General Data Protection Regulation (GDPR), which was introduced in the European Union in 2016 and came into force two years later.

—Joseph Dewey

Further Reading

Cukier, Kenneth. *Big Data: A Revolution that Will Transform How We Live, Work, and Think*. Dolan, 2013.

- Erl, Thomas, editor. *Big Data Fundamentals: Concepts, Drivers & Techniques*. Pearson, 2016.
- Horner, Veronica. "How Big Data Analytics Is Changing the Media Industry." *SEI*, 5 Oct. 2020, www.sei.com/insights/article/how-big-data-analytics-is-changing-the-media-industry.
- Kolb, Jason, and Jeremy Kolb. *The Big Data Revolution*. Applied Data Labs, 2013.
- Pentland, Alex. "Saving Big Data from Itself." *Scientific American*, vol. 311, no. 2, 2014, pp. 65–67.
- Savas, Onur, and Julia Deng, editors. *Big Data Analytics in Cybersecurity*. Routledge, 2017.
- Schmidt, Eric, and Jared Cohen. *The New Digital Age: Reshaping the Future of People, Nations, and Business*. Knopf, 2013.
- Smith, Michael D., and Rahul Telang. *Streaming, Sharing, Stealing: Big Data and the Future of Entertainment*. Reprint ed., MIT Press, 2017.
- "What Is Big Data?" Oracle, www.oracle.com/big-data/what-is-big-data.

BIOMETRIC IDENTIFICATION SYSTEMS

ABSTRACT

Biometric identification systems are becoming increasingly important given heightened concerns with security in many contexts. Compared with many other means of authorization and authentication, including password recognition, biometric technologies represent a significant advance in terms of ease of use, reliability, and validity.

BACKGROUND

The constantly evolving science of biometrics has produced a wide variety of systems capable of comparing hand, facial, eye, signature, vocal, and deoxyribonucleic acid (DNA) and brain measures of given individuals against profiles of such measures stored in large databases. The applications of this technology for law enforcement purposes are extensive. Biometric systems have been used to identify offenders who are using aliases, fight illegal immigration,

and identify inmates as they are moved through various phases of the correctional system. Biometric data can be used to verify identity claims or screen for persons who have been identified as potential security risks.

Biometric identification systems represent a huge improvement over the traditional "token" (credit card or document) and password systems. Credit cards can be lost or stolen and then used as false identification. Similarly, passwords can be "cracked," forgotten, or stolen. Biometric characteristics, on the other hand, are much more stable and permanent. Their inherent complexity renders them difficult or impossible to replicate, and the person being identified usually needs to be physically present at the time of the verification attempt. In addition, biometric systems can couple identifying information with other important background data, such as health or employment records (a fact that has led some to criticize the use of these systems as infringing on civil liberties).

The components of the typical biometric system are relatively straightforward; they consist of a sensor and a computer. The sensor is the device that gathers the biometric data from the individual being evaluated. The computer then processes the data collected; in some cases, the computer may refine the data by removing irrelevant information and background "noise" that can interfere with the interpretation of the results. The computer captures the biometric features being measured and creates a template, which it then compares to a database of biometric information on known individuals, looking for an identification match, or "hit." The consequences of a successful identification are as varied as the systems themselves. At the point of identification, an individual might be allowed into a restricted area, picked up for further questioning in a specific investigation, or observed further for any suspicious behavior.

The accuracy of a biometric system is typically assessed using one or more of the following measures: the failure-to-acquire rate (a measure of the percentage of unsuccessful attempts by the system to obtain specific biometric information from subjects), the false accept rate (also known as the false positive rate, a measure of the percentage of incorrect matches of subjects' biometric profiles to profiles already included in the database), and the false reject rate (also known as the false negative rate, the percentage of failures to match subjects' biometric profiles with identical profiles already included in the database). Minimization of all these kinds of error rates reduces the numbers of suspects who are needlessly detained, restricted from air travel, or otherwise affected by law enforcement "false alarms" while maximizing the appropriate identification of true security threats.

OVERVIEW

Law enforcement agencies employ biometric technologies in many ways, including fingerprint and DNA identification and facial, iris and voice

recognition. Facial recognition systems use specific aspects of facial features from scanned photographs to make identifications. The features analyzed may include the physical distance between specific parts of the face, skin color, thermal patterns of blood flow, and facial lines. One application of facial recognition technology is the establishment by police departments of archives containing many thousands of offender photographs. These are matched with suspects' pictures or used to produce photo lineups that can be shown to crime victims or witnesses.

Numerous evaluations of facial recognition technology have produced mixed results. One Australian system, for example, tested in the Sydney airport, was found to have a false reject rate of 2 percent. This rate was confirmed by tests sponsored by the US government. Although this error rate seems low, major world airports typically service several million passengers annually, which means that the systems could potentially falsely reject many thousands of people. On the other hand, with the advent of the newest technologies such as three-dimensional (3D) scanners, current recognition rates frequently

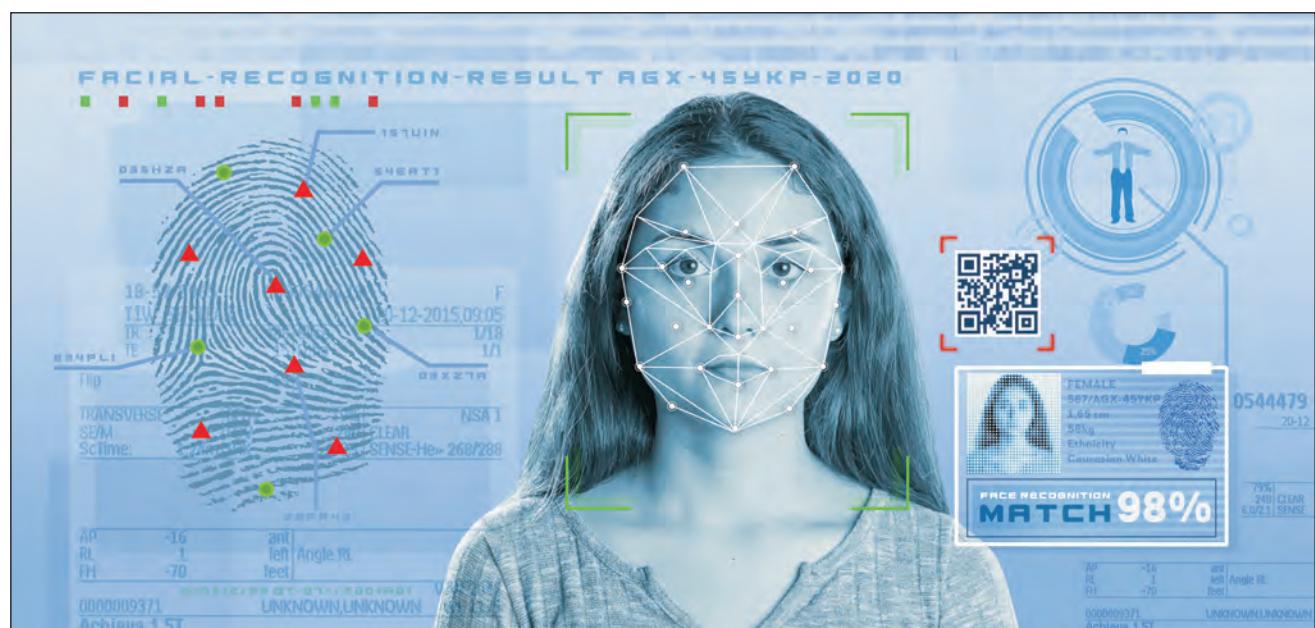


Photo via iStock/Grafissimo. [Used under license.]

exceed 90 percent. Factors affecting accuracy include lighting, the quality of the photographs taken, movements of the subjects, the angles of the poses in the photographs, and the presence of eyeglasses on subjects. In general, male subjects and older persons were more easily recognized than female and younger subjects. An inverse relationship was also found between accuracy and the size of the database against which the subjects' facial features were compared. With the ubiquity of closed-circuit television (CCTV) monitoring, difficult ethical issues arise in terms of possibly capturing faces for databases when those photographed have no knowledge of their inclusion. In addition, the use of artificial intelligence (AI) and machine learning technologies in facial recognition systems have raised ethical questions regarding the potential impact that implicit biases may have on the algorithms that power them.

Fingerprint identification is the oldest form of biometrics, having been in use for more than one hundred years. The Federal Bureau of Investigation (FBI) established a central database of fingerprints in 1924 against which law enforcement agencies can seek to match the prints of crime suspects and victims.

With modern electronic and laser technology, fingerprint images are often taken and transmitted "live" to a database. Efforts to automate the analysis and identification of fingerprints began in the 1960s. Using today's sophisticated computer systems, hundreds of thousands of fingerprints in a database can be analyzed in one second.

Fingerprint identification systems use electronic fingerprint readers to locate where the ridges of fingerprints start, end, or split up. These areas, known as minutiae points, form the basis for the identification. Each fingerprint typically contains thirty to forty minutiae points, and no two people's prints will match on more than eight such points. The accuracy of the analysis of fingerprints taken from

crime scenes, however, is often reduced because of the poor quality of the prints themselves. In addition, although it is often assumed that fingerprints are stable over a lifetime, research has shown that they in fact can change in response to physiological growth, activity, or intentional alteration. It has also been shown that many fingerprint matching systems can be "spoofed." Despite some limitations, fingerprinting is less controversial and more highly developed than many other types of biometric identification systems. This is reflected in court acceptance of fingerprinting evidence.

In iris recognition systems, an image of the iris of the eye of the person to be identified (the colored ring surrounding the pupil) is recorded by a digital camera and then converted into a template, which is checked for matches against an existing database. An advantage of using this biometric is that, unlike fingerprints, the structure of the iris is permanent by the age of one and is unique for each person (this includes comparisons between identical twins and even between the left and right eyes of the same person). A review of six iris databases ranging greatly in size (from 384 to 16,000 images) showed that each of them had one or more "noise factors." The latter most commonly included eyelid or eyelash obstructions. It should be noted that iris evidence is not left at crime scenes. In addition, failure rates as high as 15 percent have been found when iris-scanning technology is used in brightly lit settings. This technology has many potential applications, including security screening at airports and borders, passport and immigration control, and identification for banking and issuance of drivers' licenses. Iris recognition biometrics has also been scored jointly with face recognition to achieve greater accuracy than through either biometric alone.

Voice recognition systems use physical and behavioral aspects of the voice to identify individuals. The features measured are based on the physiology of the windpipe, nasal cavity, and vocal cords. A digital

“voice signature” is recorded, and a computer measures the features and compares them against known samples for identification and verification. One drawback to the use of voice biometrics is that patterns can vary with age. They can also be affected by medical problems (including even a cold) and the emotional state of the examinee. Background noise can also be a problem with the use of this identification technology.

Another biometric identification technology that has been investigated is hand geometry scanning, which involves more than ninety measurements of different parts of the hand. To detect forgery, dynamic signature identification has been developed. In this system, the specific dimensions of the pen strokes a person makes while writing his or her signature (including pressure, speed, and direction) are recorded and stored for later matching. This technology is prone to high false negative rates, however, because even though signatures are ubiquitous in daily transactions, only specific parts of a person’s signature remain constant across every signing. Gait analysis, which focuses on people’s unique walking patterns, is another type of biometric technique. Limitations to gait analysis include the fact that making gait measurements may be invasive. Gait can also be affected by injury or a change in shoes. CCTV footage has been systematically analyzed for suitability in terms of gait analysis. This is obviously less invasive but it would be subject to the same ethical dilemma mentioned in connection with facial recognition analysis through CCTV as the data source.

The future of biometric identification systems will likely be characterized by diverse measures collected simultaneously and interactively. The data will be shared across law enforcement agencies and their social welfare counterparts, both nationally and internationally. Social scientists have documented the use of relatively sophisticated biometric programs in developing countries, with half the

applications donor-supported. This largely represents an effort to develop efficient, broad-based national identity systems in countries whose poorer population segments have lacked the rights and services afforded citizens with more “officially recorded” identities. For many, privacy concerns related to the invasive nature of many of these measures are frequently of secondary importance in a global society increasingly preoccupied with defending itself against the threat of sophisticated terrorist attacks.

Beyond their use in law enforcement and national security contexts, biometric identification systems will likely also become increasingly prevalent components of the cybersecurity landscape. By the early 2020s, technologies such as fingerprint and facial recognition were commonly used in lieu of passcodes on smartphones, and similar systems were being built into consumer devices such as laptop computers. Voice recognition was likewise a common component of devices such as smartphones, enabling users to control certain functions of their devices through vocalized commands. While many consumers made use of such features, some security experts cautioned that the biometric systems in place could still be defeated by motivated hackers: in 2023, for instance, researchers affiliated with China’s Tencent Labs and Zhejiang University succeeded in developing a means of bypassing fingerprint authentication on some Android smartphones through what they termed a “BrutePrint” attack.

—Eric Metchik

Further Reading

- Eskadari, M., and T. Onsen. “A New Approach for Face-Iris Multimodal Biometric Recognition Using Score Fusion.” *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 27, no. 3, 2013, pp. 1–15.
- “FTC Warns About Misuses of Biometric Information and Harm to Consumers.” *Federal Trade Commission*, 18 May 2023, www.ftc.gov/news-events/news/press-releases/

- 2023/05/ftc-warns-about-misuses-biometric-information-harm-consumers.
- Gelb, A., and J. Clark. "Identification for Development: The Biometrics Revolution." *Center for Global Development Working Paper 315*, 2013, papers.ssrn.com/sol3/papers.cfm?abstract_id=2226594.
- Jain, Anil K., Arun Russ, and Sharath Pankanti. "Biometrics: A Tool for Information Security." *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, 2006, pp. 125–43.
- Krishnan, K. N., with D. R. Berwick. *Developing a Police Perspective and Exploring the Use of Biometrics and Other Emerging Technologies as an Investigative Tool in Identity Crimes*. Australasian Centre for Policing Research, 2004.
- Kumar, M. J. "Facial Recognition by Machines: Is it an Effective Surveillance Tactic?" *IETE Technical Review*, vol. 30, no. 2, 2013, pp. 93–94.
- Obaidat, Mohammad S., Issa Traore, and Isaac Woungang, editors. *Biometric-Based Physical and Cybersecurity Systems*. Springer, 2019.
- Parashar, R., and J. Sandeep. "Comparative Study of Iris Databases and UBIRIS Database for Iris Recognition Methods for Noncooperative Environment." *International Journal of Engineering, Research and Technology*, vol. 1, no. 5, 2012, pp. 1–6.
- Peralta, D., I. TrigueroI, R. Sanchez-Reillo, F. Herrera, and J. Benitez. "Fast Fingerprint Identification for Large Databases." *Pattern Recognition*, vol. 47, no. 2, 2014, pp. 588–602.
- Toulas, Bill. "Android Phones Are Vulnerable to Fingerprint Brute-Force Attacks." *BleepingComputer*, 21 May 2023, www.bleepingcomputer.com/news/security/android-phones-are-vulnerable-to-fingerprint-brute-force-attacks.
- Vacca, John R. *Biometric Technologies and Verification Systems*. Elsevier, 2007.

BLOCKCHAIN

ABSTRACT

Blockchains are a form of decentralized recordkeeping popularized by cryptocurrency. The first blockchain was created alongside the cryptocurrency Bitcoin in 2009. Shortly after that, blockchain technology began to be utilized for additional cryptocurrencies and other applications.

BACKGROUND

Blockchains function on a peer-to-peer network. Computers connecting to the network serve as nodes. Nodes are responsible for validating modifications to data. These modifications are called transactions. Once validated, transactions are converted to blocks and permanently attached to the end of the chain. The collective record of all transactions is called the blockchain. Because prior blocks on the blockchain cannot usually be modified, the blockchain itself serves as a permanent record of all information altered on a blockchain network.

The peer-to-peer nature of a blockchain provides several advantages. It makes the network difficult to disable or modify in an unintended manner and improves its stability. However, it is also extremely inefficient in terms of computing power and electricity usage.

The white paper detailing the first blockchain was posted by an anonymous individual or group under the alias of Satoshi Nakamoto. It was released in 2009 alongside Bitcoin, the first cryptocurrency. Nakamoto stepped away from the project in 2010.

Bitcoin used the blockchain to function. Marketed as an anonymous form of online currency, Bitcoin quickly became popular. Consumers, businesses, and computer experts found the idea of a functioning currency independent of any organization, bank, or government attractive. As Bitcoin grew in popularity, so did the idea of blockchains. Soon, other cryptocurrencies based on blockchains were developed and marketed as competitors to Bitcoin.

One of these competitors, Ethereum, pioneered the next advancement to blockchains. It developed the smart contract, which allowed blockchains to be generated with computer programs working within and alongside them. This allowed financial institutions to create tools within the blockchain that represented loans and bonds. Prior to the smart contract, only transactions were represented in cryptocurrency software.



Image via iStock/elenabs. [Used under license.]

The next major innovation in blockchain technology was called “proof of stake.” Early blockchains used “proof of work” systems. In such systems, the contributor who commits the most computing power is rewarded with influence, control, and currency. In a proof of stake system, individuals are granted more power and rewards based on the amount of cryptocurrency they already hold. The more cryptocurrency an individual holds, the greater his or her rewards. This approach levels the playing field by reducing the influence of those who own the most powerful computers.

OVERVIEW

In a traditional database, only one individual can modify a set of data at a time. This slows data editing procedures that need to be updated from multiple sources in rapid succession. Blockchains are a form of decentralized record keeping. Although it could only be utilized for cryptocurrency at first, blockchain technology can now be used for contracts and other forms of data.

Blockchain work begins with a transaction. In this case, a transaction refers to any requested change in the data values of the blockchain. With cryptocurrency, this could refer to a transfer of funds from one individual to another. In contracts, database editing, or other forms of record keeping, it may mean modifying the text or numbers in a document.

The requested transaction is then broadcast on a peer-to-peer network. On a peer-to-peer network, each computer that can transmit and receive data is called a node. Information can be uploaded to one node, which will then send the data to all other connected nodes. Each of these nodes will also subsequently transmit the information, thus allowing it to spread throughout the entire network. In a blockchain, nodes are used to verify the validity of transactions through the use of specialized algorithms.

Once the transaction is verified, a new block of data is created. This data is added to the blockchain, which is then updated on every computer in the

network through peer-to-peer nodes. In most cases, nodes are not capable of removing blocks from the block chain. This means that once a block is attached, the change in data is permanent. It also means that a permanent record of all data modifications is inherent in the blockchain system.

Blockchain systems have several advantages over traditional database systems. They do not require a central server with which users must connect to access data. Instead, they run on a peer-to-peer network. Because blockchains are not controlled by a single entity, they are incredibly resistant to attacks or attempts to unethically manipulate data. Decentralized networks also lack a singular fail point. If part of the network goes down, validations will be completed by other nodes. As a result, the blockchain itself should remain undamaged.

Blockchains also allow individuals to complete independent transactions without the involvement of any mitigating third party. For example, money can be transferred without the use of a bank. Blockchains are also entirely transparent. The software to create a blockchain is usually open source, meaning that the code itself is available for anyone to inspect.

Blockchains also have several disadvantages. In order to maintain total consensus across an incredibly large peer-to-peer network, most of the nodes on the network must remain running at all times. Often, many more nodes are involved in a calculation than would be required by a traditional system. This is wasteful in terms of processing power and electricity. It also makes processing slower and more expensive than traditional computing.

As blockchains become longer and more complex, it becomes more difficult for them to store information. Every node in the blockchain has to maintain the full chain, which continuously grows as more transactions are conducted. This increases the processing power required to maintain the chain and makes it more difficult for each node to run efficiently.

By the late 2010s, companies had increasingly begun to experiment with using blockchain technology to improve business practices. In 2018 it was announced that International Business Machines Corporation (IBM) had partnered with blockchain consulting firm Chainyard as well as other top businesses, such as Cisco and Nokia, to create a blockchain network to manage suppliers more efficiently.

Innovations in blockchain technology continued into the early 2020s. For example, 2022 saw what many experts considered a watershed moment in the technology's developmental history. That year, Ethereum, one of the world's leading cryptocurrency platforms, successfully completed a highly complex upgrade of its blockchain from a proof of work system to a proof of stake system, which is considered more egalitarian and energy efficient. Amid increasing awareness of the high levels of energy consumed by cryptocurrency mining and other related activities, many observers viewed this as a highly positive development.

Around that time, nonfungible tokens (NFTs), unique digital assets recorded on blockchain, also attracted increased attention. NFTs, often used to buy and sell digital artwork, became more popular with investors in the early 2020s and reached a market value of \$41 billion by 2021. Some investors and financial experts considered NFTs to be a bubble and argued that many individual NFTs were extremely overvalued, while others considered NFTs a major development in the world of investing.

While the early 2020s were marked by a number of problems with cryptocurrency, including crashes in value, illegal hacks of cryptocurrency exchanges, and scams, many businesses and individuals remained optimistic about the potential benefits of blockchain technology. According to professional services firm Deloitte, 76 percent of respondents surveyed in 2021 indicated that blockchain

technology had become a critical priority for their company.

—*Tyler Biscontini*

Further Reading

- Conti, Robyn, and Benjamin Curry. “What Is an NFT? Non-Fungible Tokens Explained.” *Forbes Advisor*, 17 Mar. 2023, www.forbes.com/advisor/investing/cryptocurrency/nft-non-fungible-token.
- D’Aliessi, Michele. “How Does the Blockchain Work?” *Medium*, 1 June 2016, medium.com/@micheledaliessi/how-does-the-blockchain-work-98c8cd01d2ae.
- “Deloitte’s 2021 Global Blockchain Survey.” *Deloitte Insights*, 2021, www2.deloitte.com/us/en/insights/topics/understanding-blockchain-potential/global-blockchain-survey.html.
- Fauvel, Warren. “Blockchain Advantages and Disadvantages.” *Medium*, 11 Aug. 2017, medium.com/nudged/blockchain-advantage-and-disadvantages-e76dfde3bbc0.
- Frankenfield, Jake. “What Does Proof-of-Stake (PoS) Mean in Crypto?” *Investopedia*, 31 May 2023, www.investopedia.com/terms/p/proof-stake-pos.asp.
- Gupta, Vinay. “A Brief History of Blockchain.” *Harvard Business Review*, 28 Feb. 2017, hbr.org/2017/02/a-brief-history-of-blockchain.
- Laurence, Tiana. “A Brief History of the Bitcoin Blockchain.” *Dummies*, 31 July 2017, www.dummies.com/personal-finance/brief-history-bitcoin-blockchain.
- Marr, Bernard. “A Short History of Bitcoin and Crypto Currency Everyone Should Read.” *Forbes*, 6 Dec. 2017, www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/#4ad41aa13f27.
- Mearian, Lucas. “IBM, Chainyard Unveil Blockchain-Based ‘Trust Your Supplier’ Network.” *Computerworld*, 5 Aug. 2019, www.computerworld.com/article/3429642/ibm-chainyard-unveil-blockchain-based-trust-your-supplier-network.html.
- Roose, Kevin. “Can ‘the Merge’ Save Crypto?” *New York Times*, 15 Sept. 2022, www.nytimes.com/2022/09/15/technology/merge-ethereum-crypto.html.
- Williams, Sean. “5 Big Advantages of Blockchain and 1 Reason to Be Very Worried.” *Motley Fool*, 11 Dec. 2017, www.fool.com/investing/2017/12/11/5-big-advantages-of-blockchain-and-1-reason-to-be.aspx.

BOTS

ABSTRACT

The term “bot” refers to any autonomous software application that runs automated tasks over a network, often the internet. Typically performed at a much faster rate than that which would be possible for a human, the tasks are simple and repetitive. By some estimates, bots make up more than half the traffic on the internet. Bots fit broadly into four categories: social, commercial, malicious, and helpful—which can at times overlap. Most scholars also include automated personal assistants such as Amazon’s Alexa, Apple’s Siri, and Google Assistant in discussions of bots.

BACKGROUND

Some scholars trace the origin of bots to Alan Turing and the Turing Test. In 1964 Joseph Weizenbaum at the Massachusetts Institute of Technology (MIT) Artificial Intelligence Laboratory created the ELIZA, a social or chatbot programmed to respond to a number of keywords. Though incapable of “learning” through interaction alone, ELIZA caused several participants in the experiment to become emotionally attached to it during their “conversations.” As Weizenbaum noted at the time, “extremely short exposures to a relatively simple computer program could induce powerful delusional thinking in quite normal people.”

OVERVIEW

Modern chatbots are far more adaptive than ELIZA and employ natural language processing systems to relate keywords and patterns from a database and formulate their responses. Companies will often employ chatbots as a first layer of customer service on a website. Chatbots can also be routed through third-party platforms, such as WeChat or Facebook Messenger.

Another form of social bot is a fraudulent account on social media. This type of bot came to prominence during the 2016 American presidential election cycle. Often, these accounts feature profile images and details that make them appear as if they are real people. However, they interact on social media at a rate that no human possibly could. In a 2018 article for *Wired* magazine, Paris Martineau gave the example of a Twitter (later known as X) bot account that had tweeted more than 2,000 times in three days, averaging 660 retweets and seven original tweets per day.

This type of social bot is often referred to as a troll due to its programmed behavior, usually political. A well-programmed bot of this variety can be very difficult to discern from an actual person, even for social media companies themselves. Two prominent platforms for bots of this variety, Facebook and Twitter, both launched campaigns to rid themselves of bots following bad press in the aftermath of the

2016 presidential race. In 2022, Twitter leadership reported that bots represented less than 5 percent of the service's daily active users; however, other analyses, including a study conducted by the technology intelligence company Cyabira, suggested that that proportion could exceed 13 percent.

While politically motivated social bots are widely regarded as malicious, other social bots function as news aggregators and might retweet articles that feature certain keywords. Others are used to archive threads on social media or for parody, and some can be helpful or even commercial. Helpful or commercial bots, however, usually disclose that they are bots. Malicious social bots attempting to impersonate genuine accounts typically will not disclose their true nature.

Another variety of malicious bot is represented by “botnets,” a portmanteau of “robot” and “internet.” Botnets are composed of a number of internet-connected devices, each of which is running a particular

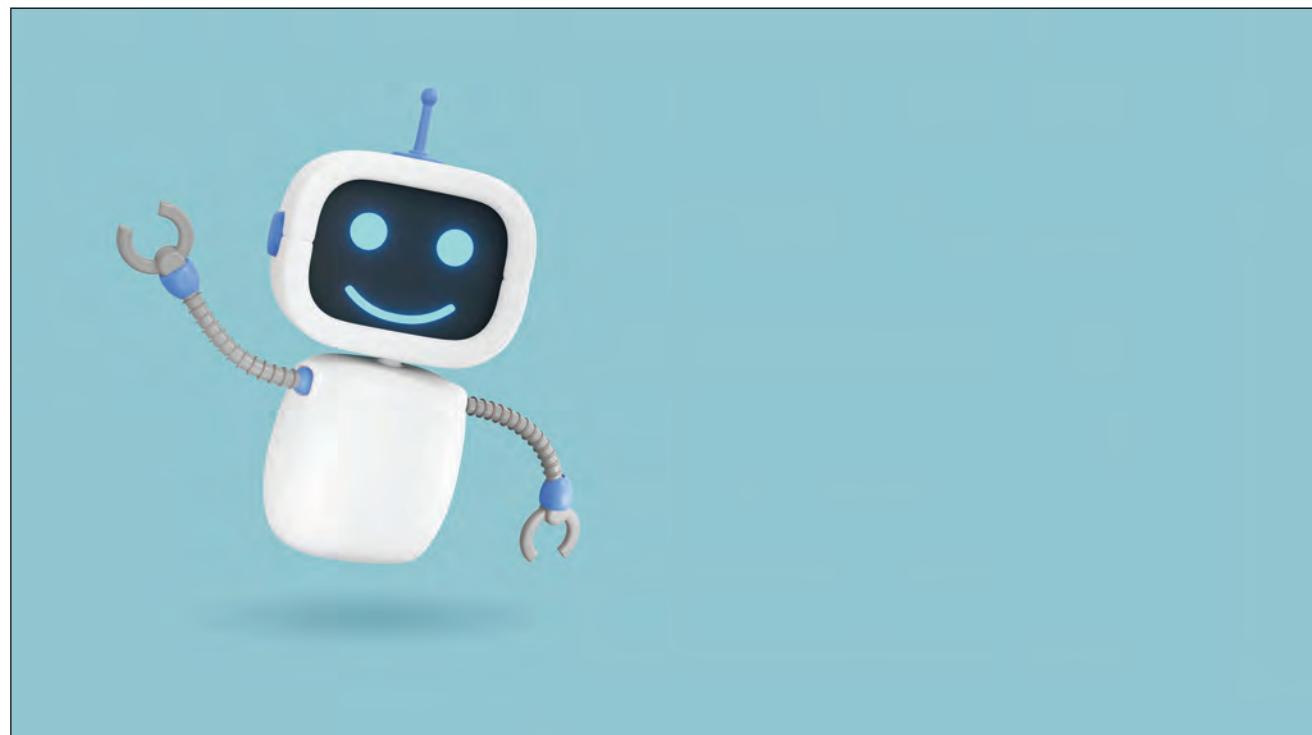


Image via iStock/volodyar. [Used under license.]

bot application. Devices can be part of a botnet without their users knowing. The botnets can then be used to perform a variety of tasks, including distributed denial of service (DDoS) attacks, cryptocurrency mining, and data mining.

Computers compromised by a botnet are often referred to as zombie computers. Their users may have no idea that they are being employed for malicious purposes. Often, computers are infected via spam email or fraudulent downloads. They can also be infected by visiting an infected website, or by exploited vulnerabilities in a web browser. The decentralized nature of botnets makes them difficult to quarantine after a number of machines have been infected. Moreover, after zombie computers have reconnected to the botnet's "home," malicious software download packets often delete themselves, leaving little visible evidence of the botnet's presence on the zombie machine.

Legally, there is not much precedent for bots or botnets. Until 2016, many gaps existed in the Federal Rules of Criminal Procedure, creating substantial obstacles both for prosecuting the creators of botnets and also when attempting to de-infect zombie computers. Following the passage of the new regulation, which went into effect on December 1, 2016, investigators were allowed to bring a single warrant to search infected computers to one federal court rather than being required to craft identical warrants in up to ninety-four jurisdictions. Previously, individual warrants had to be issued for each computer, regardless of whether they were in the same jurisdiction, making the process slow and ineffectual.

The State of California passed a law that went into effect in July 2019 requiring chatbots to identify themselves as not being human. While most commercial chatbots already did so, the law's author, State Senator Robert Herzberg, said that the measure was particularly targeted at "deceptive commercial and political bots." Some legal scholars

questioned whether this might constitute "compelled speech," either from the bot, its programmer, or the company that owns it. Moreover, as the law was at the state level, its overall efficacy remained uncertain. Companies that did not already have their bots disclose that they were not human would likely simply reprogram their bots to do so in order to do business within California, but malicious bots were unlikely to comply regardless of the legislation.

More legislation is likely to focus on bots, particularly as home assistants such as Amazon's Alexa, Google Assistant, and Apple's Siri become more prevalent. Questions have already been raised about the potential for Alexa to monitor its users in order to gain marketing information on them. In the early 2020s, however, users widely privileged the convenience of such bots over their potential negative side effects.

—J. N. Manuel

Further Reading

- Dang, Sheila, Katie Paul, and Dawn Chmielewski. "Focus: Do Spam Bots Really Comprise Under 5% of Twitter Users? Elon Musk Wants to Know." *Reuters*, 13 May 2022, www.reuters.com/technology/do-spam-bots-really-comprise-under-5-twitter-users-elon-musk-wants-know-2022-05-13.
- "Election Security Spotlight—Bots." *Center for Internet Security*, www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-bots.
- "Ensuring BotNets Are Not 'Too Big to Investigate.'" *US Department of Justice*, 22 Nov. 2016, www.justice.gov/archives/opa/blog/ensuring-botnets-are-not-too-big-investigate.
- Gershgorn, Dave. "A California Law Now Means Chatbots Have to Disclose They're Not Human." *BoLaw. Quartz*, 3 Oct. 2018, qz.com/1409350/a-new-law-means-californias-bots-have-to-disclose-theyre-not-human.
- Matineau, Paris. "What Is a Bot?" *Wired*, 16 Nov. 2018, www.wired.com/story/the-know-it-alls-what-is-a-bot.
- Shah, H., K. Warwick, J. Vallverdú, and D. Wu. "Can Machines Talk? Comparison of Eliza with Modern Dialogue Systems." *Computers in Human Behavior*, vol. 58, 2016, pp. 278–95.

- Stricklin, Kasey. "Social Media Bots: Laws, Regulations, and Platform Policies." *CNA*, Sept. 2020, www.cna.org/reports/2020/10/DIM-2020-U-028193-Final.pdf.
- Swaine, Jon. "Twitter Admits Far More Russian Bots Posted on Election Than It Had Disclosed." *The Guardian*, 19 Jan. 2018, www.theguardian.com/technology/2018/jan/19/twitter-admits-far-more-russian-bots-posted-on-election-than-it-had-disclosed.
- Weizenbaum, J. *Computer Power and Human Reason: From Judgement to Calculation*. W. H. Freeman, 1976.

BROWSERS

ABSTRACT

A web browser is an application utilized to access data and information on the World Wide Web. Browsers may be used on personal computers as well as on mobile devices such as smartphones. In the third decade of the twenty-first century, popular browsers included Microsoft Edge, Google Chrome, Firefox, and Safari.

BACKGROUND

Following the advent of the publicly accessible World Wide Web in the early 1990s, a variety of browsers were developed to grant users access to the content available on the web. One of the most versatile browser applications of that era was Netscape Navigator, produced by Netscape Communications Corporation in 1994. As befit the graphics capabilities of the time, the on-screen appearance of Navigator was simple in design. Navigator was essentially limited to a hypertext markup language (HTML)-based display of text and still images. Within that limitation though, Navigator was a very capable and reliable browser with excellent operating speed. It also had one unique feature that no other browser application offered; its users could design and compose their own HTML-based web pages using native HTML code or with Navigator's

built-in HTML coding functions and then view those pages before uploading them to a website.

Navigator also introduced a number of user-friendly features that made accessing the internet during the times of slow dial-up modem transfers almost tolerable for users. One such feature was the ability to view web pages as they were downloading rather than having to wait for the entire page to download before any of it could be viewed. Netscape also introduced the use of cookies, frames, proxy-auto configuration, and JavaScript, a kind of intermediate language that augmented mark-up languages by providing computational functionality that markup languages do not possess on their own.

Navigator, and its successor Netscape Communicator, were widely available at no cost through 2007 and subsequently continued to be found as legacy applications. They were written to run on a variety of operating platforms, including Windows, Linux, OS/2, Macintosh, and many of the UNIX variants. They looked and operated almost exactly the same on each operating system. Netscape's great success with Navigator and Communicator, however, ultimately lead to its downfall. Browsers developed to compete with them, chiefly Microsoft's Internet Explorer (IE), eventually displaced Netscape's browsers from their position as the leading browser applications of the time.

Given the power of Microsoft's marketing strategies, it should come as no surprise that the IE browser that came with every single personal computer (PC) operating on Microsoft Windows would displace Netscape's browsers at some point. Explorer was introduced in 1995 to compete with Netscape Navigator, and by 2003, IE held a 95 percent usage share of browser applications. In turn, IE decreased in popularity throughout the following years, as other competing browser applications had taken over. In 2015, Microsoft replaced IE with the browser Microsoft Edge.

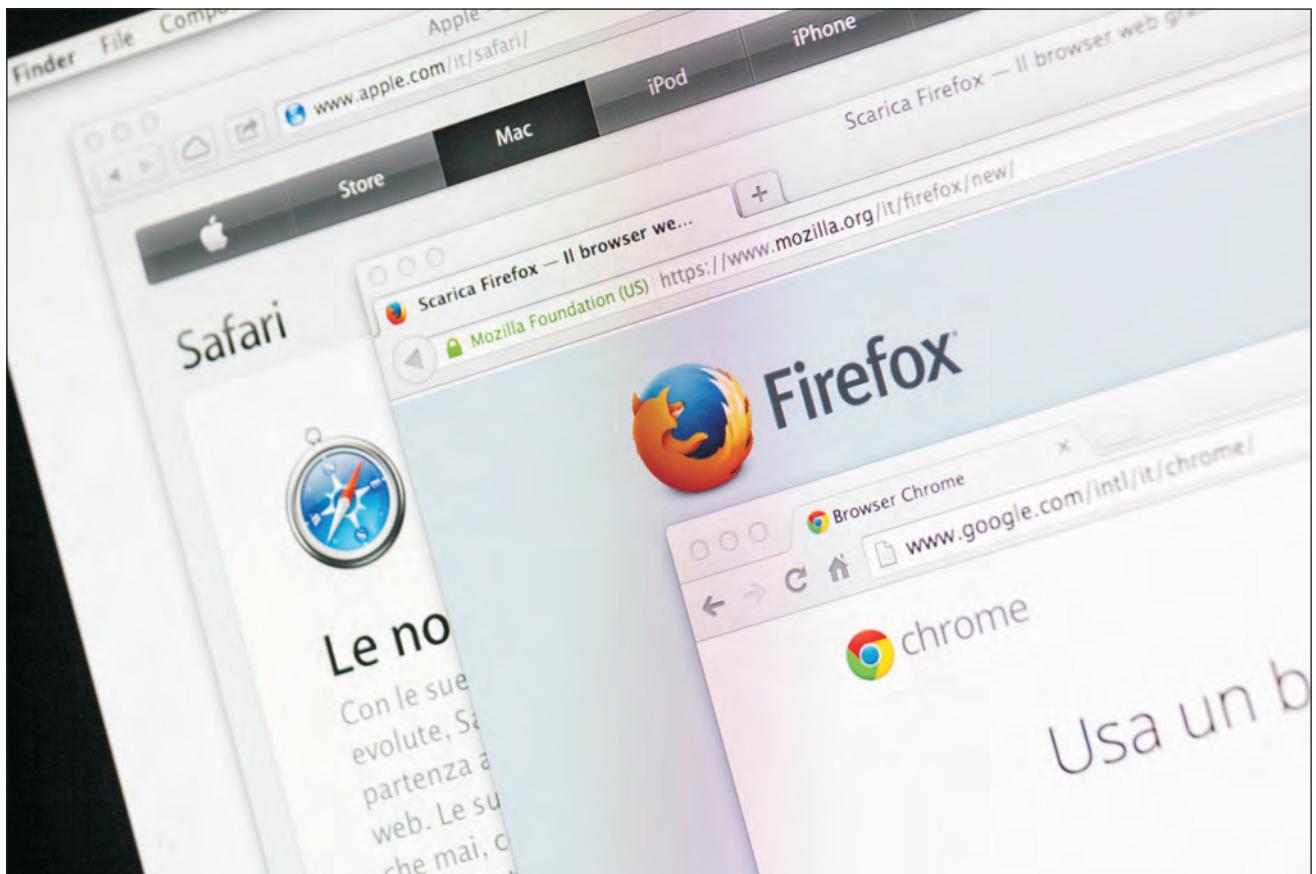


Photo via iStock/lelepad. [Used under license.]

OVERVIEW

In the third decade of the twenty-first century, numerous browser applications are available. While they all function in the same way, each one has its own unique appearance and built-in capabilities. Each browser has its own strengths, weaknesses, and configurability, and therefore its own usefulness. One common characteristic is the ability to open multiple web pages at one time and display those pages in separate tabs. This makes it easy for users to multitask, perform research, compare products, or otherwise maintain concurrent access to information.

Firefox. According to Mozilla.org, the producer of the browser application, Firefox is not just a browser, but a collection of products designed for

users to promote safer and smarter browsing while online. The main feature of the Firefox family of products however, is the Firefox browser application itself. The browser is produced for desktop and laptop computers, mobile systems such as cell phones and tablets, and for enterprise computing systems and mainframes. In all iterations, the browser automatically blocks more than 2000 known data trackers, small third-party programs that monitor a user's online activity and returns a record of that activity to the data trackers' sources for different purposes.

Firefox was created in 2002, when Microsoft's IE 6 was the dominant browser in general use. The beta version of Firefox proved to be faster, more secure, and with better add-on features than IE 6. By 2009, Firefox had exceeded IE's share of browser usage,

before both fell behind Google's Chrome browser in popularity. Originally part of a collection of utility programs called Mozilla Suite, Firefox (originally called Phoenix) was developed to be a stand-alone application in order to reduce what was thought of as Mozilla Suite's "bloated" code. The term refers to program code that requires so many coded instructions to run all of the program's features that it causes program functioning to bog down or become too slow to be useful. Firefox quickly proved itself to be a fast, efficient browser that is easy to use, with user-friendly usability and security features. While Firefox declined in popularity in the decades following its initial release, it remained the preferred browser for some users and in May of 2023 had a global market share of about 2.8 percent, according to the statistics platform Statista.

Google Chrome. Google's Chrome browser was first released in 2008 to compete with Firefox and quickly displaced both Firefox and IE as the browser of choice. By May of 2023, the browser had a global market share of 63 percent. Chrome is a fast, robust browser that is exceedingly simple to use due to its minimalist presentation. Initially, new tabs in Chrome displayed only a wallpaper screen image and the search bar/address bar called the "omnibox." Users type in a web address, search term, or keyword. If a search term or keyword is entered, Chrome uses the Google search engine to call up every instance of the word that it can locate. The minimalism of the new tab display was subsequently augmented to add a selection of topical links that appear each time a new tab is opened.

Chrome is readily configured and maintained by its users, with numerous preference settings and "housekeeping" utilities. Chrome also has a large library of extensions available as add-ons, allowing users to add features such as other languages, translation, mathematics, and others that are not part of the basic structure of Chrome's provided release. Many such extensions are written and produced by

third-party developers and may not be entirely compatible with a particular version of Chrome.

Safari. Because Safari was developed to run on Mac computers rather than Windows PCs, it is a graphics-based browser and unique to the MacOS, iOS, and iPadOS operating systems. A Windows version was offered in 2007, but it was discontinued after several years. Safari was initially offered in 2003 and as of 2023 is in its sixteenth iteration. Its performance in the 2020 version was 50 percent faster than Google Chrome and consumed significantly less power than its competitors. In May 2023, Safari usage was second only to Google Chrome, with a global market share of about 20.9 percent. New versions of Safari were released every two years from 2003 to 2007 and were later released yearly.

Safari functions like all web browsers, the essential difference being that internet connections and data are displayed through graphics processing rather than the text-based processing of other computers. In graphics processing the hyperlinks to other web pages may be embedded within the digital code of graphics images, whereas in text-based processing the hyperlinks are merely associated with a string of text that typically identifies the URL of the target of the hyperlink, or is perhaps just an underlined word or an instruction such as "click here." The hyperlinks in both text-based and graphics processing can also be associated with an image.

Chromium. As the name would suggest, Chromium, like Chrome, is a product of Google. Though not a browser per se, it is a free and open-source browser project representing the very large codebase used by Chrome. As such, Google does not provide an official stable version of Chromium. While the program codes within the Chromium codebase are the property of Google, it is available freely for use by other developers and has been utilized to produce other web browsers, including Opera, Microsoft Edge and Samsung Internet. Users of Chromium code are able to develop and enhance

the code they use and add those new features to the Chromium codebase. In addition, they can use their features with the Chrome brand attached.

Microsoft Edge. The successor to IE, Microsoft Edge was first released in 2015. Much like IE, it was automatically provided alongside the Windows operating system. Versions of Edge were also released for other operating systems, including macOS. The browser underwent substantial updates in the years following its initial release, and in 2020, Microsoft released a new version of Edge that was based on Chromium. Edge ranked third among browsers globally as of May 2023, with a market share of about 5.3 percent.

Brave. Brave, launched in 2016, is one of the several web browsers that have been constructed using the Chromium codebase. Brave recaptures the minimalistic appearance of new tabs, displaying only a beautifully composed high-resolution photographic wallpaper background, an omnibox search bar, and a small number of quick access icons linked to as many web locations as the user has accessed frequently. The icons are unobtrusive and can be removed either manually or when the browser cache is cleared.

Brave's main attractions are its built-in automatic blocking of ads and data trackers and its high user security capabilities. In normal use Brave runs the Chrome browser, but with enhanced user security features. Chrome itself gives the option of using a private window for browsing, as do other browsers, that does not log the browsing history of the user's current session. When the option to open a new private window is selected in Brave, however, the user is presented with a choice to use either Chrome's basic private window service or Brave's private window with Tor connectivity. (Tor is short for The Onion Router, a free and open-source software for enabling anonymous communication). With Tor connectivity, the user's internet protocol (IP) address is completely masked as the browsing

requests are passed through any number of other Tor server nodes. Accordingly, this may slow down browser response, and Brave warns that some websites may not function through Tor and so will not be accessible. The Tor connectivity option also requires that the Tor browser be resident on the user's device.

Opera. Opera is one of the oldest web browsers, having been developed in 1995 by its namesake company. Until 2005, Opera was available only as commercial software based on Opera's Presto engine. Opera was switched from Presto to Chromium in 2013 and continues to develop from the Chromium codebase. In 2016, the Opera brand was sold to a consortium of Chinese investors.

The Opera browser has many of the features common to Chromium-based browsers, such as ad blocking, tabbed browsing, private browsing, and others. A particular feature of interest in Opera is that an unlimited number of recently viewed web pages are shown as thumbnail views when a new tab is opened. Opera also has embedded links to social media messaging applications. Opera is contracted to use the Google search engine as its default. Opera runs on Windows, Mac, Linux, iOS, and Android operating systems.

—Richard M. Renneboog, Jake D. Nicosia

Further Reading

"Global Market Share Held by Leading Internet Browsers from January 2012 to May 2023." *Statista*, May 2023, www.statista.com/statistics/268254/market-share-of-internet-browsers-worldwide-since-2009.

Gralla, Preston. *How the Internet Works*. 4th ed., Que Publishing, 1998.

"The History of Web Browsers." *Mozilla*, www.mozilla.org/en-US/firefox/browsers/browser-history.

Hofmann, Chris, Marcia Knous, and John V. Hedke. *Fox and Thunderbird Garage*. Prentice Hall Professional Technical Reference, 2005.

Huddleston, Rob. *HTML, XHTML, and CSS: Your Visual Blueprint for Designing Effective Web Pages*. John Wiley & Sons, 2009.

- La Counte, Scott. *The Ridiculously Simple Guide to Surfing the Internet with Google Chrome*. SL Editions, 2020.
- LeJeune, Urban A., and Jeff Duntemann. *Netscape and HTML Explorer*. Coriolis Group Books, 1995.
- Markelo, Steve. *Microsoft Edge: A Beginner's Guide to the Windows 10 Browser*. Conceptual Kings, 2015.
- McDaniel, Adam. *HTML 5: Your Visual Blueprint for Designing Rich Web Pages and Applications*. John Wiley & Sons, 2011.
- Mehta, Prateek. *Creating Google Chrome Extensions*. Springer Science + Business Media, 2016.
- O'Leary, Timothy, Linda O'Leary, and Daniel O'Leary. *Computing Essentials 2023*. McGraw-Hill, 2022.
- Ramos, Emmanuel. "Web Browsers: Examining the Latest Threats, Solutions and Trends." *Forbes*, 14 Aug. 2023, www.forbes.com/sites/forbestechcouncil/2023/08/14/web-browsers-examining-the-latest-threats-solutions-and-trends/?sh=c9be852187b8.
- Stockson, Eric. *Brave Browser: Blockchain Internet Browsing Made Easy*. First Rank, 2019.
- Wilton, Paul, and Jeremy McPeak. *Beginning JavaScript*. 5th ed., Wrox, 2015.

C

CAMBRIDGE ANALYTICA FACEBOOK DATA SCANDAL

ABSTRACT

The Cambridge Analytica Facebook data scandal was a political scandal that erupted in 2018 when press reports revealed that British political consulting firm Cambridge Analytica had taken data, without user authorization, from millions of Facebook social media profiles and used it to aid conservative political candidates and movements in the United States and the United Kingdom. The incident inspired a more robust debate about digital data and privacy in both countries.

BACKGROUND

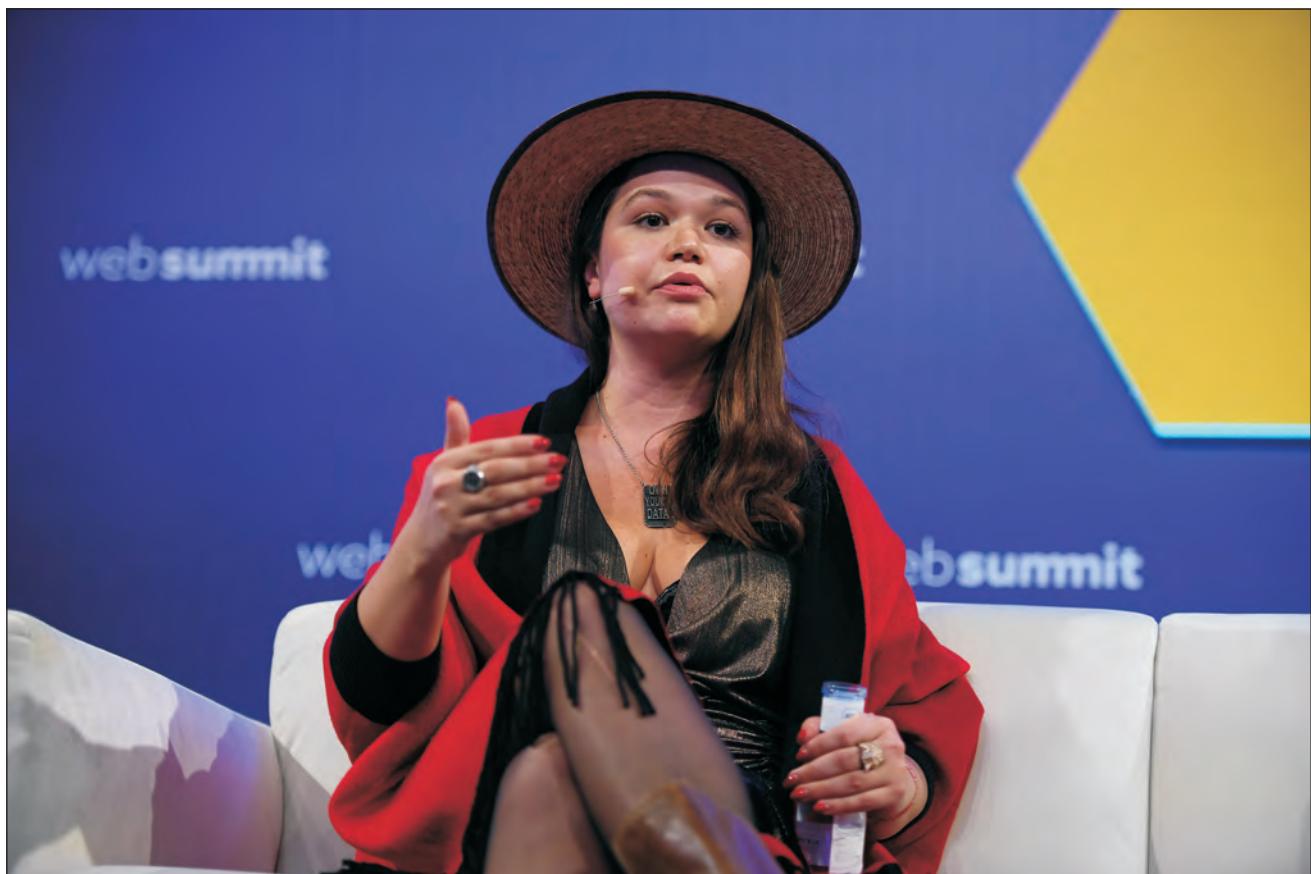
Facebook is a social media company that began operation in 2004 and offers users the ability to share messages, images, and other data. (The social media site's parent company was renamed Meta in 2021.) In December 2009, Facebook altered the programming of its website such that information that users had previously designated as "private" was made public. Facebook made no prior attempt to notify users of the company's policy changes. In addition, a Federal Trade Commission (FTC) investigation found that Facebook had allowed third-party developers and advertisers to access data that users had designated as private. In a November 2011 settlement with the FTC, Facebook signed a consent decree, agreeing to make certain changes to its policies so as to avoid violating privacy settings designated by users. Specifically, Facebook agreed to cease misrepresenting user privacy or security, agreed to obtain consumers' express consent before enacting changes that altered or superseded user

privacy settings, agreed to prevent any access to user data more than thirty days after the data in question had been deleted by the user, and agreed to establish a privacy program certified by periodic independent third-party audits.

The political research and consulting firm Cambridge Analytica was established in 2013 as an offshoot of the British data analysis firm Strategic Communication Laboratories (SCL), with help from a large infusion of cash by United States investor and conservative activist Robert Mercer. Led by



Facebook CEO Mark Zuckerberg. Photo by Anthony Quintano from Honolulu, HI, United States, via Wikimedia Commons.



Brittany Kaiser testified about her involvement in the work of Cambridge Analytica before a select committee of the UK Parliament and to the Mueller investigation. Photo by Web Summit, via Wikimedia Commons.

chief executive officer (CEO) Alexander Nix, Cambridge Analytica was in the business of harvesting huge amounts of voter data, including online behavior used to determine personality traits—a methodology known as psychographics—and using that information to precisely target political advertising and influence voter behavior. The company was active in the United States 2014 midterm elections and was then hired in 2015 by the presidential campaign of Republican Ted Cruz. The next year, it was hired by the campaign of Donald Trump at the urging of Trump adviser and eventual campaign manager Steve Bannon, who had also advised Robert Mercer and sat on Cambridge Analytica's board of directors. The company also provided services to a

group active in the “leave” side of the Brexit campaign, the 2016 British referendum in which voters called for the United Kingdom to leave the European Union.

OVERVIEW

Cambridge Analytica's role in fine-tuning and deploying a powerful new voter-profiling methodology was reported sporadically in the news media from at least 2015. However, their activities became a scandal when news broke in March 2018 (reported simultaneously by the *New York Times* in the United States and *The Guardian* in the UK) that a huge amount of the data the company relied on was harvested from Facebook profiles in violation of Facebook's privacy

rules. Furthermore, records showed that during the United States presidential campaign, Nix had reached out to WikiLeaks founder Julian Assange seeking help obtaining private emails from Democratic presidential nominee Hillary Clinton (a proposal Assange said he rejected).

A major source for these reports was Christopher Wylie, a Cambridge Analytica whistleblower who said the company's goal was to "fight a culture war in America" using "big data" as a weapon. In order to get the amount of data the company needed quickly and cheaply, Wylie had retained the services of a Russian American psychology professor at Cambridge University named Aleksandr Kogan. Kogan built a Facebook app—a personality quiz—from which he harvested user data for Cambridge Analytica. Only about 270,000 users took the quiz, but Cambridge Analytica also obtained the user data of all their friends—a violation of Facebook's privacy

policy that ultimately amounted to a data leak affecting about 87 million users.

IMPACT

The fallout from the Cambridge Analytica/Facebook scandal was multilayered. Facebook claimed it had been deceived and banned Cambridge Analytica and Aleksandr Kogan from its platform. Still, the social media giant faced investigation for violating its 2011 consent decree requiring that it protect users' privacy. United States special counsel Robert Mueller, head of the investigation into Russian meddling in the 2016 presidential election, requested documents from Cambridge Analytica pertaining to the Trump campaign, and the company ultimately shuttered in May 2018. However, a number of its officials started a new company, Data Propria, which was later reported to have worked with Trump's unsuccessful 2020 reelection campaign.



Whistleblower Christopher Wylie during Cambridge Analytica protest. Photo by Jwslubbock, via Wikimedia Commons.

In January 2019, the *Washington Post* reported that the FTC was considering levying a record-setting fine against Facebook if the organization determines that Facebook violated the consent decree that Facebook entered into with the FTC in 2012. According to the *Post*, the fine could exceed the \$22.5 million fine that the FTC imposed on Google in 2012 after finding that Google had engaged in unauthorized tracking of consumers using Apple's Safari browser. In July 2019, it was announced that the FTC had levied a fine of \$5 billion against Facebook for privacy violations and found its CEO Mark Zuckerberg liable to a limited degree.

On January 10, 2019, British courts ruled on another case brought by an American who sued the UK-based parent company of Cambridge Analytica, SCL Group (both of which went out of business in May 2018), because the company would not turn over his personal data upon request as required by UK law. The company pleaded guilty and was forced to hand over its server passwords to British authorities. This development meant that substantive investigation of how much data Cambridge Analytica obtained from Facebook, and how, could begin. In 2020, leaked documents revealed that Cambridge Analytica's efforts to influence elections had extended far beyond the United States and United Kingdom, although the company did not always rely on data gleaned from Facebook for its operations.

—Micah L. Issitt

Further Reading

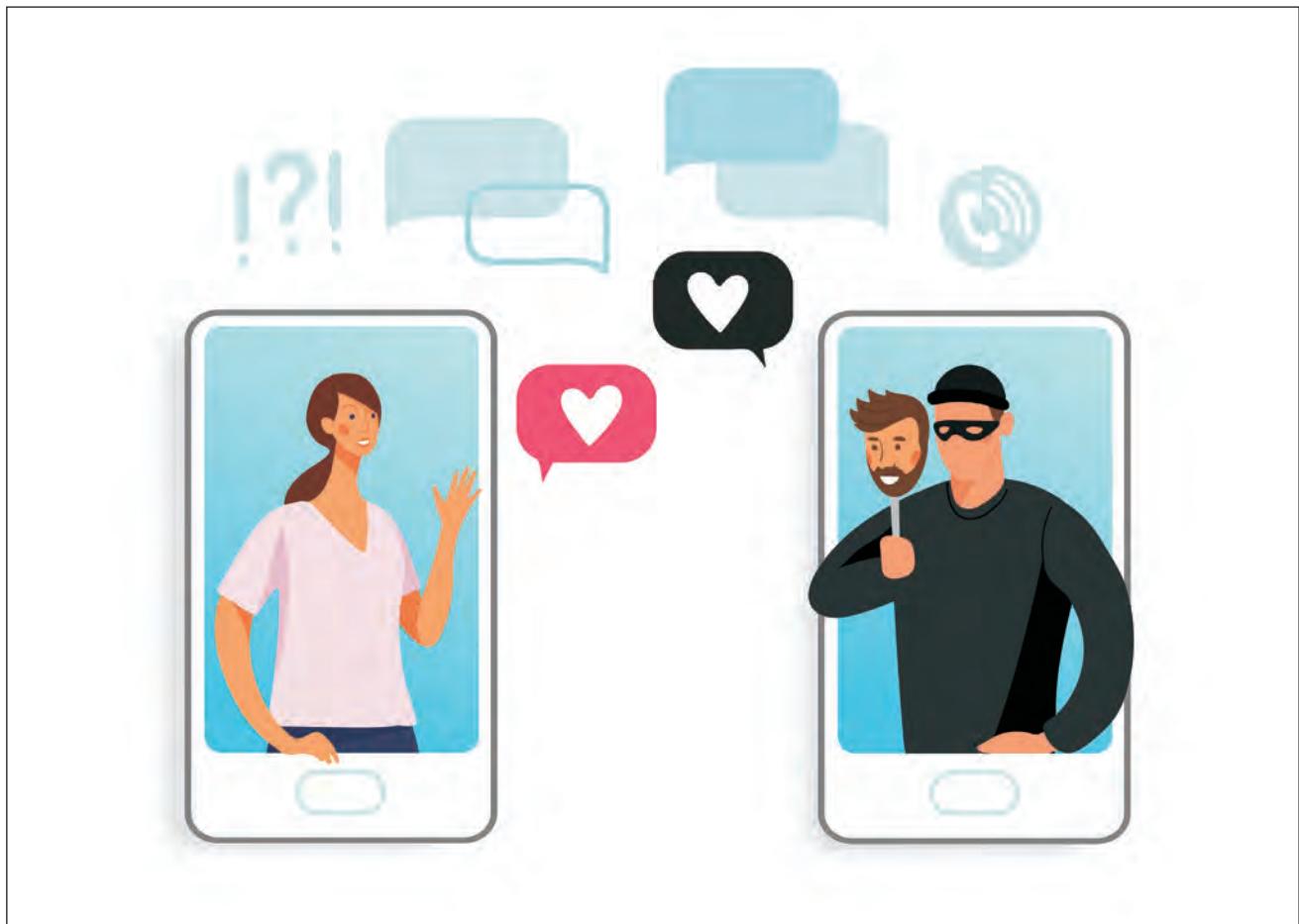
- Cadwalladr, Carole. "Fresh Cambridge Analytica Leak 'Shows Global Manipulation Is Out of Control.'" *The Guardian*, 4 Jan. 2020, www.theguardian.com/uk-news/2020/jan/04/cambridge-analytica-data-leak-global-election-manipulation.
- Confessore, Nicholas. "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far." *New York Times*, 4 Apr. 2018, www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

- "Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises." *Federal Trade Commission*, 29 Nov. 2011, www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.
- "FTC Fines Facebook \$5B for Privacy Violations." *CBC*, 24 July 2019, www.cbc.ca/news/business/facebook-privacy-ftc-fine-1.5222943.
- Purdy, Chase. "Did Facebook Violate Its FTC Agreement? Here's What Investigators Will Ask." *Quartz*, 21 Mar. 2018, qz.com/1233597/did-facebook-violate-its-ftc-agreement-heres-what-investigators-will-ask.
- Romm, Tony, and Elizabeth E. Dwoskin. "U.S. Regulators Have Met to Discuss Imposing a Record-Setting Fine against Facebook for Privacy Violations." *Washington Post*, 18 Jan. 2019, www.washingtonpost.com/technology/2019/01/18/us-regulators-have-met-discuss-imposing-record-setting-fine-against-facebook-some-its-privacy-violations.
- Rosenberg, Matthew, Nicolas Confessore, and Carole Cadwalladr. "How Trump Consultants Exploited the Facebook Data of Millions." *New York Times*, 17 Mar. 2018, www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.
- Weissman, Cale Guthrie. "The Cambridge Analytica Revelations Are Only Beginning." *Fast Company*, 10 Jan. 2019, www.fastcompany.com/90290604/cambridge-analytica-pleads-guilty-hands-over-passwords.

CATFISHING

ABSTRACT

Catfishing refers to intentionally using a false online identity in order to trick someone into engaging in an emotional and/or romantic relationship. In documented cases of catfishing, the motivation for deception varies and can include boredom, loneliness, revenge, and simple curiosity. The term was first coined in the documentary Catfish (2010), in which the filmmaker learns that the woman with whom he believes he is having an online relationship is in reality someone completely different. The term's position in the cultural lexicon was further cemented in 2014, when Merriam-Webster amended the definition of the



[Used under license.]

word “catfish” to include a person who uses a deceptive social networking profile.

BACKGROUND

The use of false or anonymous online identities has been commonplace since use of the internet became widespread in the early 1990s. People have used fake identities when writing book or film reviews, commenting on blogs, and when intending to aggravate or escalate online arguments. What distinguishes catfishing is its end goal of cultivating an online romantic relationship.

With the rise in popularity of social media networks in the 2000s, catfishing became more

advanced and elaborate. Through websites such as Myspace and Facebook, users could create deceptive accounts using fabricated biographical information and photographs that were downloaded from the internet. Additional social media accounts were often created to give the illusion of a network of family members and friends.

The rise in popularity of online dating also led the way for an increase in catfishing. According to a study performed by the Pew Research Center in 2016, nearly six percent of internet users in a committed relationship first met their partner online. This figure was twice that of those polled in 2005. A 2013 Pew study also found that 54 percent of those

polled believed that they had also been given false biographical information by others online at some point.

OVERVIEW

The motivation for people to catfish others varies. Sometimes catfishers are lonely or feel ostracized by their peers or community, so they turn to online companionship. Other times there are malicious reasons, such as a drive for aggression or for revenge, and in some cases catfishing occurs as part of a financial crime. Some catfishers create a false online profile in order to explore aspects of their sexuality they are afraid to reveal or confront in real life. Catfishing is also considered by experts as a form of cyberstalking.

A 2012 study in the *Journal of Adolescence* found that young people were increasingly using social networking websites as a means for identity exploration. By creating fake profiles, users could explore different facets of their personality. The study states that while this exploration helps adolescents measure and understand themselves and form an identity, it can grow harmful if the user isolates from reality in order to nurture intimate relationships online, which then leads to negative psychological patterns. There have been various studies done on the psychology of both the catfisher and the victim as well as numerous articles on the warning signs of being catfished.

CATFISH THE DOCUMENTARY AND THE SERIES

The term “catfish” was first coined in the documentary *Catfish* (2010), which followed photographer Yaniv “Nev” Schulman as he developed a romantic relationship online. He believed he was in a relationship with a young single woman named Megan, but when Schulman and the filmmakers tracked her down, they unveiled a series of untruths culminating in the realization that Megan was actually Angela Wesselman, an older married woman with two sons.

In the film, an anecdote is told about how fishermen place catfish in shipping tanks with live cod when sending the fish overseas. The catfish harass the cod, thereby keeping them active and their meat firmer and better tasting. People who act as catfish, the documentary explains, keep others alert and never bored.

The success of the *Catfish* documentary led to the cable network MTV producing *Catfish: The Series* in 2012. In each episode, Schulman and *Catfish* filmmaker Max Joseph connect people who have an online relationship in order to determine whether someone in the relationship is catfishing the other. *Catfish: The Series* remained on the air through late 2023.

In the wake of the popularity of the *Catfish* documentary and television series, several catfishing incidents involving sports and entertainment personalities received substantial publicity. One case involved University of Notre Dame linebacker Manti Te'o, who in September 2013 led his team in an exciting upset against Michigan State University. Fans were especially inspired by his performance because three days before, Te'o had learned that his grandmother and his girlfriend, Lennay Kekua, had both died. Te'o and Kekua had met online and had developed a romantic relationship without ever having met in person, and Te'o's ability to overcome adversity garnered a tremendous amount of national attention. Following Kekua's reported death, journalists discovered that, unbeknownst to Te'o, Lennay Kekua did not exist. In fact, the religious musician Ronaiah Tuiasosopo had been pretending to be Kekua because, as he later admitted, he was secretly in love with Te'o. Also in 2013, it was revealed that actor Thomas Gibson, a star of the popular television series *Criminal Minds*, was the victim of an elaborate catfish scam. The news broke when an entertainment news agency released an embarrassing video that Gibson took of himself in a hot tub. Reports indicated that Gibson and his catfisher had been

exchanging photos and videos of themselves for at least two years, with Gibson's catfisher sending him images she downloaded from pornographic websites.

—Patrick G. Cooper

Further Reading

- Caspi, Avner, and Paul Gorsky. "Online Deception: Prevalence, Motivation, and Emotion." *CyberPsychology & Behavior*, vol. 9, no 1, 2006, pp. 54–59.
- D'Costa, Krystal. "Catfishing: The Truth about Deception Online." *Scientific American*, 25 Apr. 2014, blogs.scientificamerican.com/anthropology-in-practice/catfishing-the-truth-about-deception-online.
- Fernando, Jason. "Catfishing: What It Is, Examples of Financial Fraud." *Investopedia*, 23 Apr. 2023, www.investopedia.com/terms/c/cat-fishing.asp.
- Israelashvili, Moshe, et al. "Adolescents' Over-Use of the Cyber World: Internet Addiction or Identity Exploration?" *Journal of Adolescence*, vol. 35, no. 2, 2012, pp. 417–24.
- McCarthy, Ellen. "What Is Catfishing? A Brief (and Sordid) History." *Washington Post*, 9 Jan. 2016, www.washingtonpost.com/news/arts-and-entertainment/wp/2016/01/09/what-is-catfishing-a-brief-and-sordid-history.
- Moss, Caroline. "Strangers Have Been Using This Woman's Photos to Catfish People Online for Ten Years." *Business Insider*, 21 Jan. 2015, www.businessinsider.com/strangers-have-been-using-this-womans-photos-to-catfish-people-for-10-years-2015-1.
- Scott, A. O. "The World Where You Aren't What You Post." *New York Times*, 16 Sept. 2010, www.nytimes.com/2010/09/17/movies/17catfish.html.
- Smith, Aaron, and Maeve Duggan. "Online Dating & Relationships." *Pew Research*, 21 Oct. 2013, www.pewresearch.org/internet/2013/10/21/online-dating-relationships.

CHANGING PASSWORDS

ABSTRACT

There are a number of factors that come into play when thinking about creating or changing a password. First, is

the ease in which you can remember the password (and not confuse it with other passwords). Second, are the characteristics involved in generating a strong/secure password (i.e., size of the character set and the length of the password). Both of these can influence the overall strength of the password but not necessarily in the same manner. Related issues to consider when changing a password include characteristics that create a weak password and methods that are used to break passwords.

BACKGROUND

In the electronic age, we can access our bank account at night, pay our bills during nonbusiness hours, purchase merchandise in a different state, and check our work email all from the convenience of our homes. We are no longer limited to conducting business transactions at a particular time and at a specific location. Our ability to securely do many of these activities hinges on limiting who has access to the various accounts or information. The use of a password is one way of limiting access to this information. While many would agree with limiting access, many users create weak passwords that leave their accounts or information vulnerable. Many users choose to create easy-to-remember passwords over secure passwords. Surprisingly though, these same users not only know how to make strong passwords but also know the risks involved in having a password compromised. Some of the common practices people use will be explored. The technology side of passwords is presented to illustrate the variability in time for breaking passwords of different strengths. A variety of topics related to the construction of a password and how passwords are broken are explored. These topics will be used in discussing how to create a strong password.

OVERVIEW

The purpose of a password is to allow access to information, services, or resources only to those individuals who should have access. Conversely, the

purpose is to deny access to individuals who should not have access. The password then serves as a means for verifying or authenticating who the user is. Authenticating a person (user) for access can take many forms (see Renaud and Ramsay), but in general comes down to three categories: (1) what a person knows (e.g., information such as a password), (2) what a person has (e.g., an object such as a bank card), and (3) what a person is (e.g., biometrics such as a fingerprint). Of these three, what a person knows (passwords) is the easiest to implement. Systems requiring additional security may require multifactor authentication, that is, using two or all three of the categories for authenticating who you are (e.g., using a fingerprint and a password).

The personal repercussions from a compromised password could include identity theft, damage to

reputation, lost privacy, and lost data. Depending on your company policy, you may be held accountable at work for not adhering to password policies. The consequences for businesses for a breach in the computer system can be extreme, resulting in down time, lost productivity, lost data, recovery, and lost revenue.

The next two sections will deal with: (1) decisions people make when creating their password, which often lead to weak passwords, and (2) the use of technology and various techniques to break a password.

UNDERSTANDING VULNERABLE PASSWORDS

In 2014, the top five worst passwords in use, as provided by SplashData, were: 123456, password, 12345678, qwerty (the first 5 letters on the

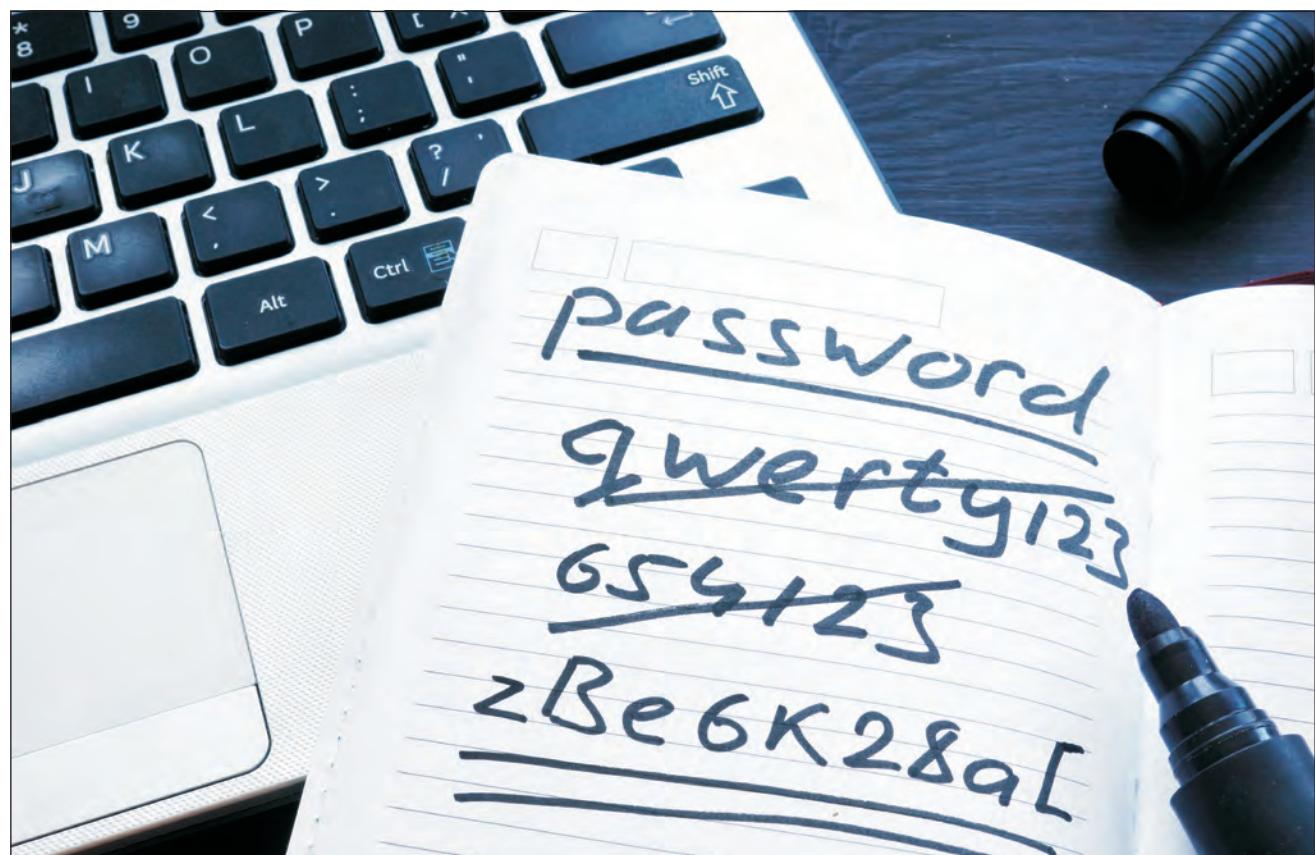


Photo via iStock/designer491. [Used under license.]

keyboard top row), and abc123. Such passwords remained common throughout the subsequent years despite warnings from security experts, in large part because they were easy for users to recall. Researchers Brown, Bracken, Zoccoli, and Douglas point out the irony of passwords in that someone else should have a difficult time figuring it out, and yet it should be something easy to remember. When constructing a password, users often desire a convenient and memorable password. Unfortunately, these two often lead to what is considered a weak password (as can be seen in the top five worst passwords).

Below are choices people often make in managing their passwords that are related to convenience and memorability, which can lead to a weak or insecure password. These are presented for two reasons: to show that a good number of people tend to make the same choices that lead to a weak password, and as examples of what to avoid when constructing or changing your own password.

Researchers such as Tam, Glassman, and Vandewauver have explored the ways in which people manage their passwords. The actual creating or changing of a password is seen as a neutral behavior. It is the other behaviors involved in password management that commonly lead to the creation of weak passwords. One of the leading categories for poor password management is the use of personal information to construct a password. Examples include using information such as one's phone number, birthday, first name, last name, or the name of family members, loved ones, or pets. If someone knows you, or knows things about you, all of these make it easy for them to guess your password. Another common poor password management behavior is displaying the password near the computer (e.g., taped to the monitor, "hidden" below the keyboard, etc.). A third area of concern is sharing one's password with someone. This defeats the notion of limited access if you are "giving" it away. If you are in a

relationship that ends and you have shared your passwords then you should change them immediately.

UNDERSTANDING THE VULNERABILITY OF PASSWORDS

Computers can be used to figure out a password, and the weaker the password, the easier it is for a computer to break it. Even a secure password can be compromised given enough time and unlimited attempts. This is the philosophy behind a method called "brute force" in which every possible combination of characters is tried. The shorter and less complex the password is, the faster it is for a computer using this approach to break the password. The more complex the password is, the longer it would take to "crack" it.

A more sophisticated approach to breaking passwords involves the use of a dictionary table. This approach tests all the words in a dictionary including spelling, common misspellings, and pseudowords. This method is effective because many people like to use something memorable, such as a word. Passwords consisting of a single word are one of the easiest passwords to break.

Recommended standards for constructing passwords. The Federal Information Processing Standards (FIPS), provided by the Department of Commerce in 1985, are guidelines that identify specific features that contribute to making a complex password. The intent was to have users construct "strong" passwords that would take more time to break. These guidelines state that the length of the password should be a minimum of 8 characters, consist of both numbers and letters, and should include special characters (e.g., any of the characters at the top of the number keys such as "!" or "@").

These recommended standards can be summed up as two key components that influence the strength of a password. The two components are: (1) the overall length of the password (i.e., a password

of length 12 would be stronger than a password of length eight), and (2) the variety of characters used (e.g., letters, numbers, and special characters). Researchers Keith, Shao, and Steinbart review a mathematical way of representing the contribution of these two components as c^d . “C” is the number of potential characters and “d” is equal to the length of the password used. The more original characters in your character set, the more potential options there are for the password. When you increase both the “size of the character set” and “the length of the password” you increase the total possible number of combinations that a computer would potentially have to examine.

Breaking passwords. The importance of following the FIPS guidelines when creating a password can be seen in the examples below. Researchers such as Keith, Shao, and Steinbart have provided estimates of the amount of time it would take a password to be broken by a password cracking program. The estimates provided were based on using a typical home computer making about 3,000,000 attempts per second; this estimate is a few years old, and as computers have become faster, this is already an underestimate of the length of time it would take to crack a password. A weak password constructed of only lowercase letters (26 possible letters) with a length of 5 characters would take, on average, a few seconds to compromise. Again working with just lowercase letters, a password with a length of 8 characters would take, on average, about 9.6 hours to compromise. Changing the length of a password from 5 to 8 characters resulted in a dramatic increase in the amount of time needed to crack the password (a few seconds versus 9.6 hours).

The other FIPS guideline was to include additional characters in the character set. The character set can be increased by including features such as upper and lowercase letters, numbers, and special characters. The standard keyboard has a possibility of 62 unique alphanumeric characters (letters and

numbers) and 32 special characters. By including all of the alphanumeric characters and the special characters, we now have a complex set of 94 potential items. A password constructed with the more complex character set of 94 items with a length of 5 characters would take, on average, about 21 minutes to crack (better than a length of 5 lowercase but not as impressive as a length of 8 with lowercase). A password with a length of 8 items and the complex character set of 94 items would, on average, take about thirty-five years to crack.

The FIPS recommendations impact the number of possible combinations a password could have. Using the above examples: a password of length of 5 with 26 items would result in 26^5 or over 11 million combinations; a password of length 5 with 94 items would result in 94^5 or over 7 billion combinations; a password of length 8 with 26 lowercase characters would results in 26^8 or over 208 billion combinations; a password with a length of 8 items with character set of 94 items would result in 94^8 or over 6 quadrillion combinations. The number of special characters can be increased beyond the 94 by using the extended character set (in Windows the extended characters can be entered with ALT + the ASCII code, in MAC it is the Option key + the ASCII code, and in Linux (verified in Ubuntu) Ctrl+shift+U then the Unicode). As these examples show, both length of the password and the number of potential characters used are important for creating a strong password. Use of the extended character set can further add to the complexity of the password.

PASSWORDS PROTECT YOU—PROTECT IT

When changing a password, it is important to keep in mind several of the following points. The importance of length and the number of characters used (FIPS recommendations). Both of these contribute to a larger number of potential combinations and thus add to the complexity of the password and the

security of your system. As you increase the complexity of your passwords, it may be helpful to learn techniques that will help you to remember those complex passwords.

Researchers such as Charoen, Rauman, and Olfman show that when given time to think about a password versus immediately entering one in, users typically construct a stronger password. Another possibility is for the user to make use of mnemonic techniques. One technique is taking a phrase known to you and then using the first letter of each word for your password (plus adding special characters, see Schneier below). Another technique includes using passphrases and/or mnemonic devices to make the password more memorable to you (see Nelson and Vu, or for a more general introduction to potential mnemonic techniques see McCabe).

Other recommendations include using a different password for different sites. Sometimes people will use the same password for multiple sites. If one site is compromised, all of them may be compromised. For those who have difficulties with remembering several passwords a password keeper (or password vault) may be an option. Use a reputable one. The advantage to this type of service is that you need only one password (often these password keepers can generate a random password for each of your accounts). When using a public computer or open Wi-Fi, be cautious, there is the potential for passwords to be captured.

In summary, remember to do the following: follow FIPS guidelines about length and type of characters used, keep your password to yourself (do not share with others), take time to plan your password (they tend to be better), consider a password vault if you have difficulties with remembering your passwords, and if you think a loved one may need access should something happen to you, consider using a safety deposit box or a safe for your password.

Remember to avoid the following: avoid the mistake of using personal information to construct a

password, avoid reusing passwords, avoid using similar passwords, avoid patterns in creating your passwords (e.g., increasing a number at the end of the password), and avoid substitutions like “\$” for “s” and other such substitutions which create pseudo words (e.g., “P@\$\$w0rD”) because standard password cracking programs are capable of exploiting this. Finally, never continue to use a default password or a password that has been assigned to you (e.g., many home routers [in simple terms your connection to the internet] have been compromised because people did not change the default password; always create your own password).

These tips, what to do and what to avoid, are aimed at making it harder for people to guess, find, or break your password and therefore limit their access to your account or data. Following these steps will make it harder for others to compromise your password. Keep in mind that this is an introduction to a complex topic and that password security starts with creating a strong password.

—Michael S. Bendele, Robert A. Bendele

Further Reading

- “123456’ Maintains the Top Spot on SplashData’s Annual ‘Worst Passwords’ List.” *SplashData News*, 20 Jan. 2015, web.archive.org/web/20150207065500/http://splashdata.com/press/worst-passwords-of-2014.htm.
- Black, Damien. “Weakest Passwords of 2023.” *Cybernews*, 15 Nov. 2022, cybernews.com/security/weakest-passwords-2022.
- McCabe, J. A. “Integrating Mnemonics into Psychology Instruction.” *OTRP Online*, 2011, teachpsych.org/resources/Documents/otrp/resources/mccabe11.pdf.
- Nelson, D., and K. L. Vu. “Effectiveness of Image-Based Mnemonic Techniques for Enhancing the Memorability and Security of User-Generated Passwords.” *Computer in Human Behavior*, 2010, 26, pp. 705–15.
- Schneier, B. “Choosing Secure Passwords.” *Schneier on Security*, 3 Mar. 2014, www.schneier.com/blog/archives/2014/03/choosing_secure_1.html.
- Spice, B. “Press Release: Carnegie Mellon Scheme Uses Shared Visual Cues to Help People Remember Multiple

Passwords.” *Carnegie Mellon University*, 4 Dec. 2013, www.cmu.edu/news/stories/archives/2013/december/dec4_passwordscheme.html.

CHINA'S CYBERINVASION

ABSTRACT

For years it was an open secret that the dramatic rise in infiltration of government and corporate computer systems had been traced repeatedly, but not conclusively, to China. Then, in February 2013, the security firm Mandiant released a report with evidence linking massive hacking operations to a unit of the Chinese army in Shanghai.

BACKGROUND

Until about 2004, China used its hacker population in the same way Russia did, encouraging them to attack websites of adversaries on an ad hoc basis. As a more strategic view took hold, China's computer network operations became more organized toward long-term national goals. To counter threats to domestic stability, the government secretly searched the computers of journalists and vandalized dissident websites. Faced with superior US military capabilities, the People's Liberation Army looked for infrastructure vulnerabilities that could deter the United States from acting in the Pacific. Seeing a need to “leapfrog” its technology development, China planted surveillance tools in computer systems of high-tech companies in the United States and other English-speaking countries.

A November 2011 study by the National Intelligence Council, “Foreign Spies Stealing US Economic Secrets in Cyberspace,” said China's hackers focused on companies with advanced maritime technologies, anticipating China's naval buildup, and companies in the aerospace industry, where China has rapidly developed a full line of unmanned aerial vehicles (UAVs). An August 2012 report by McAfee Security, “Revealed: Operation Shady RAT,”

identified US defense contractors and others as targets of hackers in China and detailed their use of remote access tools, or RATs.

To install a RAT in a targeted system, the hacker first sends a spear-phishing email to a legitimate system user. The email comes with an attached file, which appears to be a routine business document. Clicking the file activates hidden malware, which then installs a backdoor or several backdoors into the network. Having gained access, hackers may install additional tools to transmit screen images or keystrokes or even activate microphones and webcams. Hackers can then explore the target system carefully before capturing large amounts of data.

The intrusion of hackers into the *New York Times'* computer network in 2012 offers a useful example of a company that was expecting a break-in. AT&T notified the *Times* of unusual telephone traffic in October, shortly before publication of a story about the billion-dollar fortune accumulated by relatives of Premier Wen Jiabao. The *Times* hired Virginia-based security consulting firm Mandiant to track the intruders, who began by setting up backdoors in three employee computers. After exploring the network for two weeks, the hackers found the usernames and passwords of all system users. The passwords were “hashed,” but even scrambled passwords can be decrypted with “rainbow tables,” databases compiled for use by hackers and available on various websites. The hackers wanted emails related to the story about Wen Jiabao and soon retrieved them from reporters' archives. By the end of the year, the hackers had installed forty-five customized tools. Even with knowledge of the break-in as it was happening, it was a painstaking process to close the backdoors and remove the malware. After a similar cleanup at the US Chamber of Commerce in 2011, investigators found months later that a computer-controlled thermostat and an office printer were still in contact with computers in China.

The *New York Times* anticipated that there might be an attempt on its network once officials became aware of the Wen Jiabao story. Western journalists in China have been subject to surveillance of emails since 2008, the year of the Beijing Olympics, when Chinese anxiety about unfavorable publicity reached a high point. Political dissidents, regional separatists, and religious organizations such as Falun Gong have also been targets of spying and vandalism.

In 2009, the Canada-based research group Information Warfare Monitor (IWM) uncovered extensive cyberspying on the Tibetan independence movement, with malware installed in Tibetans' computers in China and India and spreading out to embassies and nonprofit organizations worldwide. The spying operation, dubbed GhostNet by IWM, used the spear-phishing technique to infect systems in Delhi, New York, and London and retrieved information via command-and-control servers in China.

GhostNet also targeted organizations connected to other issues of concern to China, such as Taiwan independence.

Cybervandalism against dissidents and their supporters has been sporadic and may be the work of patriotic hackers who are tolerated by the Chinese government. In 2010, hackers attacked the Nobel Prize committee website after human rights advocate Liu Xiaobo was awarded the Peace Prize. In 2011, a website offering a petition in support of dissident artist Ai Weiwei was hit by a distributed denial of service (DDoS) attack, a technique that overwhelms a server with requests for access.

Bringing the topic of cyberattacks into the open became a component of US counterstrategy in March 2013. Director of National Intelligence James R. Clapper Jr., told the Senate Intelligence Committee that potential cyberattacks on vital infrastructure, including power grids and communications systems, had become the number-one threat to US security, moving ahead of terrorist attacks. On the same day, General Keith Alexander, head of the US

Cyber Command, revealed to the House Armed Services Committee that the United States had cyberweapons ready to respond in the event of attacks on US systems.

OVERVIEW

In 2006, the computer security firm Mandiant began following a group they identified as APT1. Hackers in this group route their attacks through internet protocol (IP) addresses set up by known APT1 agents and use certain tools unique to the group. Two of these tools—GETMAIL and MAPIGET—retrieve emails from a target's inbox and archives. Mandiant identified three APT1 agents to illustrate the group's operations. A hacker using the online name UglyGorilla, who expressed support for China's "cybertroops" in January 2004, registered several of the internet domains used by APT1 and wrote some of its malware, or malicious software. A second hacker, code-named DOTA by Mandiant, using the same domains and IP ranges as UglyGorilla, created dozens of email accounts that were used to carry out social engineering attacks, in which the victim is tricked into volunteering information, and spear-phishing attacks, in which the victim opens an attached file believing the email is from a colleague. In registering the email accounts, DOTA gave a telephone number in Shanghai. The third hacker, known as SuperHard, who wrote code for APT1 tools in the AURIGA and BANGAT families, revealed he was working from the Pudong New Area of Shanghai.

The scale and duration of AT1 operations imply support from a large organization with access to a variety of resources. In 2011 and 2012, APT1 set up more than nine hundred servers hosted at more than eight hundred IP addresses in thirteen countries. These servers functioned as command-and-control centers for the theft of hundreds of terabytes of information from more than 140 organizations across twenty industries. APT1

hijacked data from dozens of corporations simultaneously. For operations at this level, APT1 had to have an extensive frontline staff, possibly hundreds of hackers. To search for targets inside a high-technology corporation, the hackers must have had support from specialists in a range of disciplines, including linguists, industry experts, and programmers to write customized malware. To manage the huge volume of stolen data, APT1 had to have a substantial inventory of equipment and technicians to maintain it, in addition to administrative support for finances, logistics, and so on.

The epicenter of APT1 activity is Shanghai, and specifically the Pudong New Area, where two of the four large networks used by the group physically reside. A survey of facilities capable of supporting APT1 leads to the twelve-story headquarters of Unit 61398 of the People's Liberation Army (PLA). While the mission of Unit 61398 is officially secret, it has recruited publicly for computer science graduates who have both a master's degree and proficiency in English. Records show China Telecom installed fiber-optic cable near the unit's Datong Road building as a "national defense construction." While the evidence linking the PLA to APT1 is circumstantial, any alternative explanation requires the existence of a second institution near the same location with the same combination of staff capabilities in computers and English and an enduring interest in documents from a broad spectrum of high-technology companies in the West.

In February of 2013, Mandiant published a report, *APT1: Exposing One of China's Cyber Espionage Units*, in which the firm identified the PLA's Unit 61398 as the point of origin for massive hacking operations. The Mandiant report set the stage for a US initiative on several fronts to restrain cyberattacks from overseas. In a policy document titled "Administration Strategy on Mitigating the Theft of US Trade Secrets," the White House called for tighter coordination of intelligence about system

intrusions and urged businesses to work with law enforcement. The strategy includes gaining support from allies and trade organizations for international standards and accountability. By mid-2013, computer hacking had become a top issue for discussion in diplomacy with China, notably during visits by Secretary of the Treasury Jack Lew and Secretary of State John Kerry. The Chinese government initially denied any involvement with APT1's efforts or other hacking initiatives; however, China's leadership later admitted to engaging in cyberattacks.

CYBERWEAPONS AS DETERRENTS

China's military planners acknowledge the US advantage in weapons with superior firepower and control. To counter the advantage, China's defense strategy emphasizes asymmetrical measures to slow down or neutralize an enemy's ability to deploy such weapons. Cyberattacks against command-and-control centers are a rapidly attainable, low-cost, and effective means to hobble superior forces, and cyberwarfare has been a component of PLA doctrine since 2004. The US military is developing its response to asymmetrical interference strategies, such as might be seen in the South China Sea or Strait of Hormuz, under a concept called Air-Sea Battle, promulgated by the Pentagon in 2009.

Intrusions by China-based hackers into systems that control US power grids, nuclear generation plants, and other critical infrastructure may also play a role in China's defense strategy. By demonstrating its ability to enter systems considered vital to national security, China introduces a powerful consideration to US strategic thinking—the possibility of a disabling attack far from the scene of a confrontation that might occur, for example, in the South China Sea. Strategists have recommended that the US advertise its cyberweapons as a deterrent, and in March 2013 General Keith Alexander, commander of the US Cyber Command, told a Senate committee the United States is prepared to use

offensive cyberweapons against an enemy who uses them first.

Chinese officials point out that the United States was the first to militarize cyberspace with the establishment of Cyber Command in 2009. Moreover, China is itself under constant attack by hackers. Two defense ministry websites were bombarded by more than 140,000 attacks per month in 2012, and 62 percent originated from servers in the United States.

Further Reading

- Crosston, Matthew. "Virtual Patriots and a New American Cyber Strategy: Changing the Zero-Sum Game." *Strategic Studies Quarterly*, vol. 6, no. 4, 2012, pp. 100–118.
- Holland, Steve, and Doina Chiacu. "U.S. and Allies Accuse China of Global Hacking Spree." *Reuters*, 20 July 2021, www.reuters.com/technology/us-allies-accuse-china-global-cyber-hacking-campaign-2021-07-19.
- Magnuson, Stew. "U.S. Government Attempts to Thwart Chinese Network Intrusions." *National Defense*, vol. 97, no. 704, 2012, pp. 58–60.
- Nagy, Viktor. "The Geostrategic Struggle in Cyberspace between the United States, China, and Russia." *AARMS: Academic & Applied Research in Military Science*, vol. 11, no. 1, 2012, pp. 13–26.
- Roberts, Mary Rose. "An Invisible Enemy." *Urgent Communications*, vol. 30, no. 3, 2012, pp. 18–21.
- Segal, Adam. "Chinese Computer Games." *Foreign Affairs*, vol. 91, no. 2, 2012, pp. 14–20.

CLOUD COMPUTING

ABSTRACT

Cloud computing is a networking model that allows users to remotely store or process data. Several major internet service and content providers offer cloud-based storage for user data. Others provide virtual access to software programs or enhanced processing capabilities. Cloud computing is among the fastest-growing areas of the internet services industry. It has also been adopted by government and research organizations.

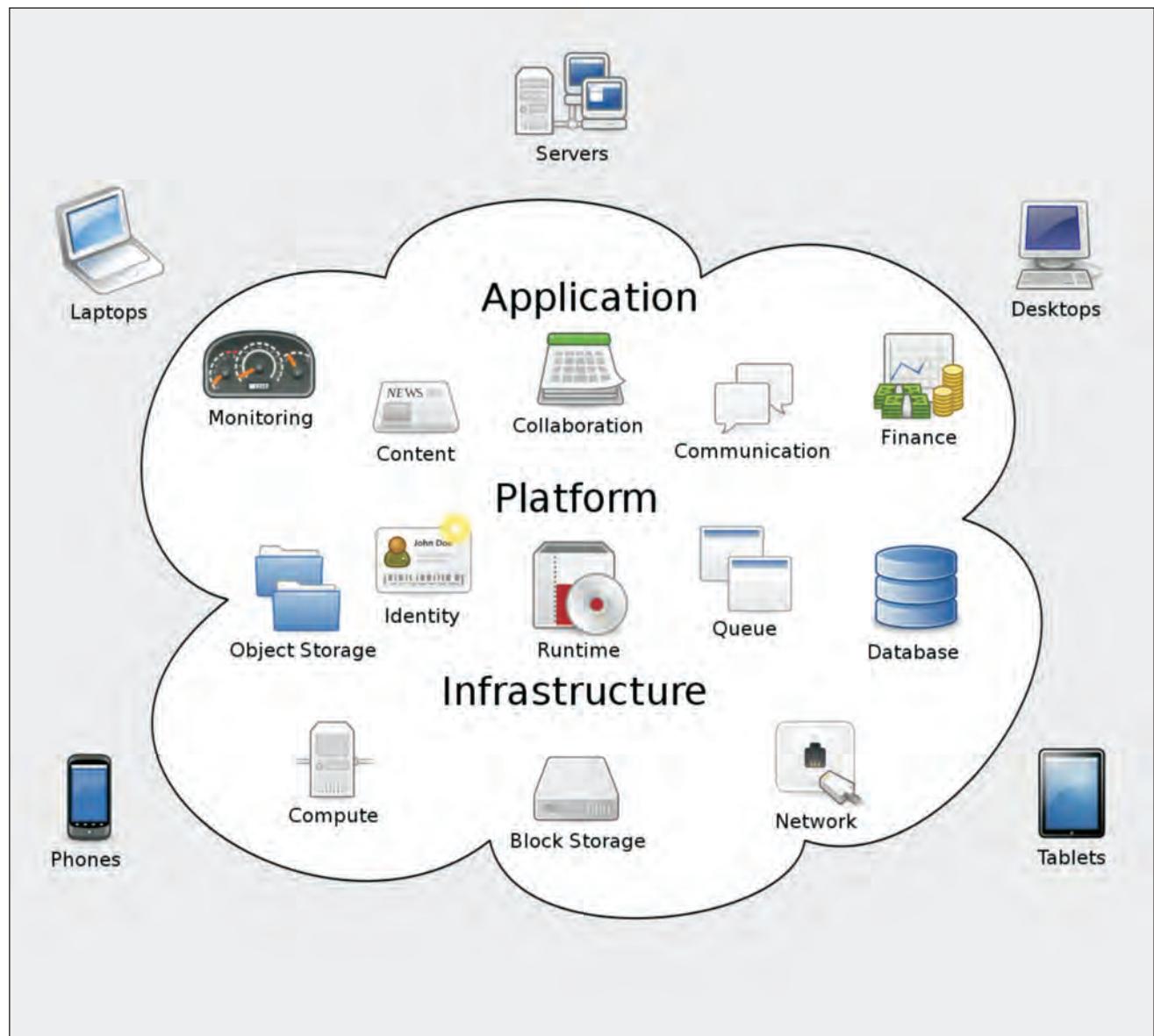
BACKGROUND

Private clouds are virtual networks provided to a limited number of known users. These are often used in corporations and research organizations. Operating a private cloud requires infrastructure (software, servers, etc.), either on-site or through a third party. Public clouds are available to the public or to paying subscribers. The public-cloud service provider owns and manages the infrastructure. Unlike private clouds, public clouds provide access to an unknown pool of users, making them less secure. Public clouds are sometimes based on open-source code, which is free and can be modified by any user.

The hybrid cloud lies somewhere between the two. It offers access to private cloud storage or software services, such as database servers, while keeping some services or components in a public cloud. Setup costs may be lower with hybrid cloud services. A group using a hybrid cloud outsources some aspects of infrastructure investment and maintenance but still enjoys greater security than with a public cloud. Hybrid clouds have become widespread in the health care, law, and investment fields, where sensitive data must be protected on-site.

OVERVIEW

The infrastructure as a service (IaaS) model offers access to virtual storage and processing capability through a linked network of servers. Cloud-based storage has become popular, with services such as Apple iCloud and Dropbox offering storage alternatives beyond the memory on users' physical computers. IaaS can also give users greater computing power by allowing certain processes to run on virtual networks, rather than on the hardware of a single system. Using IaaS enables companies to create a corporate data center through third-party data centers. These third-party centers provide expert IT assistance and server resources, generally for subscription fees.



Cloud computing metaphor: the group of networked elements providing services does not need to be addressed or managed individually by users; instead, the entire provider-managed suite of hardware and software can be thought of as an amorphous cloud. Image by Sam Johnston, via Wikimedia Commons.

Cloud computing refers to the use of processors, memory, and other peripheral devices offsite, connected by a network to one's workstation. Use of the cloud protects data by storing it and duplicating it offsite and reduces infrastructure and personnel needs.

The platform as a service (PaaS) model mainly offers access to a specific platform that multiple users can use to develop software applications, or apps. Many apps require access to specific development programs. The Google App Engine, for example, provides an environment that stores, supports,

and runs web apps. PaaS allows software developers to create apps without investing in infrastructure and data center support. Providers may also offer virtual storage, access to virtual networks, and other services.

The software as a service (SaaS) model offers users subscription-based or shared access to software programs through a virtual network. Adobe Creative Cloud provides access to Adobe, Inc., programs such as Photoshop, Illustrator, and Lightroom for a monthly or yearly fee. Users pay a smaller amount over time rather than paying a higher cost up front to purchase the programs. SaaS supports multitenancy, in which a single copy of a program is available to multiple clients. This allows software providers to earn revenue from multiple clients through a single instance of a software program.

ADVANTAGES AND DISADVANTAGES OF THE CLOUD

Cloud networking allows small companies and individuals access to development tools, digital storage, and software that once were prohibitively expensive or required significant management and administration. By paying subscription fees, users can gain monthly, yearly, or as-used access to software or other computing tools with outsourced administration. For service providers, cloud computing is cost effective because it eliminates the cost of packaging and selling individual programs and other products.

Data security is the chief concern among those considering cloud computing. The private and hybrid cloud models provide a secure way for companies to reap the benefits of cloud computing. Firewalls and encryption are common means of securing data in these systems. Providers are working to increase the security of public clouds, thus reducing the need for private or hybrid systems.

—Micah L. Issitt

Further Reading

- Beattie, Andrew. "Cloud Computing: Why the Buzz?" *Techopedia*, 9 Feb. 2012, www.techopedia.com/2/27830/trends/cloud-computing/cloud-computing-why-the-buzz.
- Dotson, Chris. *Practical Cloud Security: A Guide for Secure Design and Deployment*. O'Reilly, 2019.
- Huth, Alexa, and James Cebula. *The Basics of Cloud Computing*. Carnegie Mellon U and US Computer Emergency Readiness Team, 2011, www.cisa.gov/sites/default/files/publications/USCERT-CloudComputing_HuthCebula.pdf.
- Kale, Vivek. *Guide to Cloud Computing for Business and Technology Managers*. CRC, 2015.
- Kruk, Robert. "Public, Private and Hybrid Clouds: What's the Difference?" *Techopedia*, 5 July 2022, www.techopedia.com/2/28575/trends/cloud-computing/public-private-and-hybrid-clouds-whats-the-difference.
- Rountree, Derrick, and Ileana Castrillo. *The Basics of Cloud Computing*. Elsevier, 2014.
- Ryan, Janel. "Five Basic Things You Should Know about Cloud Computing." *Forbes*, 30 Oct. 2013, www.forbes.com/sites/sungardas/2013/10/30/five-basic-things-you-should-know-about-cloud-computing/?sh=78e67d3560fa.
- Sanders, James, and Conner Forrest. "Hybrid Cloud: What It Is, Why It Matters." *ZDNet*, 1 July 2014, www.zdnet.com/article/hybrid-cloud-what-it-is-why-it-matters.
- "What Is Cloud Security?" *IBM*, www.ibm.com/topics/cloud-security.

COMBINATORICS

ABSTRACT

Combinatorics is a branch of mathematics that determines the number of ways that something can be done.

Combinatorics has numerous applications to probability, computer science, and experimental design.

BACKGROUND

Combinatorics is the mathematics of counting. It has numerous applications to probability, computer science, and experimental design. For example, the probability of a favorable outcome can be

determined by dividing the number of favorable outcomes by the total number of outcomes. The number of ways that a set of outcomes A can occur may be represented by the symbol $|A|$.

OVERVIEW

One of the most basic methods in combinatorics is the Addition Principle. The Addition Principle states that if A and B cannot both occur, then the number of ways A or B can occur is computed by

$$|A \cup B| = |A| + |B|.$$

A generalization of the Addition Principle is the Principle of Inclusion and Exclusion. This principle states that the number of ways that A or B can occur is given by

$$|A \cup B| = |A| + |B| - |A \cap B|,$$

where $|A \cap B|$ is the number of ways both A and B can occur.

Another basic method is the Multiplication Principle. The Multiplication Principle states that if outcome of A does not affect the outcome of B, then the combination of A and B is computed by $|A| |B|$. As an example, consider ordering a meal at a restaurant. This boils down to a series of choices (drink, appetizer, entrée, side, and dessert), none of which affects any other choice. So if there are five choices for drink, three for appetizer, ten for entrée, seven for side, and three for dessert, then the number of unique meals that can be ordered is $5(3)(10)(7)(3) = 3150$.

The Multiplication Principle allows us to count a number of things. For example, suppose that we want to give out k different trophies to n different people in such a way that each person can receive multiple trophies or go home with nothing. There are n choices for the first trophy, n choices for the second, and so on. Hence, the Multiplication Principle gives the number of distributions as $n^k = n(n)...(n)$.

Consider the problem of lining up n people. There are n ways to place the first person in line. Regardless of who is selected, there are $n-1$ ways to place the second $n-2$ for the third, and so on. Thus, the Multiplication Principle shows that the number of ways to line up the people is $n! = n(n-1)(n-2)...(2)(1)$. The symbol $n!$ is read “ n factorial.”

Using a similar technique, we can count the number of ways to select n officers of different rank from a group of n people. Again, there are n choices for the first individual, $n-1$ choices for the second, and so on, with $n-k+1$ choices for the last individual. So, the number of ways to select and rank the individuals is given by

$$P(n, k) = n(n-1)...(n-k+1) = \frac{n!}{(n-k)!}$$

Suppose that instead we want to determine the number of ways to select a committee of k (where every member has the same rank) from a group of n people. To do this, we can simply divide $P(n, k)$ by $k!$, the number of ways to rank the n individuals. This results in

$$C(n, k) = \frac{n!}{k!(n-k)!}$$

As an example, consider the problem of drawing a “three of a kind” in five-card poker. There are $C(13, 3)$ ways to select ranks for the hand. There are 3 ways to select which of these ranks to triple. There are $C(4, 3)$ ways to select suits for the triple. There are 4^2 ways to select suits for the other two cards. Thus, the Multiplication Principle yields the number of acceptable hands as $C(13, 3)*C(4, 3)*4^2 = 18304$.

COMBINATORICS IN COMPUTER SCIENCE

Combinatorics has multiple applications within the field of computer science, including applications related to the development of machine-learning and artificial intelligence technologies.

Combinatorial testing methods are also valuable within the field of cybersecurity, as they enable security professionals to identify errors and vulnerabilities in security software more efficiently, among other uses. In the United States, organizations engaged in researching combinatorics' security applications include the Computer Security Resource Center (CSRC) at the National Institute of Standards and Technology (NIST).

—Robert A. Beeler

Further Reading

- Benjamin, Arthur T., and Jennifer J. Quinn. *Proofs That Really Count—The Art of Combinatorial Proof*. Mathematical Association of America, 2003.
- “Combinatorial Testing.” NIST Computer Security Resource Center, 19 Oct. 2023, csrc.nist.gov/Projects/automated-combinatorial-testing-for-software/cybersecurity-testing-1/cybersecurity-testing.
- DeGroot, Morris H., and Mark J. Schervish. *Probability and Statistics*. 4th ed., Pearson, 2011.
- Hollos, Stefan, and J. Richard Hollos. *Combinatorics Problems and Solutions*. Abrazol, 2013.
- Martin, George E. *Counting: The Art of Enumerative Combinatorics*. Springer, 2001.
- Simos, Dimitris E., et al. “Combinatorial Methods in Security Testing.” *Computer*, vol. 49, 2016, pp. 80–83.
- Tucker, Alan. *Applied Combinatorics*. Wiley, 2012.

COMPUTER AND TECHNICAL SUPPORT SPECIALIST

ABSTRACT

Computer and technical support specialists provide support to internal or external users of a particular technology or group of technologies. They work in a wide range of businesses, institutions, and government agencies. Students aspiring to enter the profession should pursue studies in subjects such as computer programming and computer science.

BACKGROUND

Computer and technical support specialists provide technical support for computers, online services, video games, and a variety of related devices and programs. They may work in an internal support capacity, helping their fellow employees, or they may provide support to many organizations or individuals as contractors or employees of dedicated technical support companies. Computer and technical support specialists may specialize in one type of system or software or offer general support. They must be able to offer solutions to complex issues in a high-pressure environment.

OVERVIEW

Computer and technical support specialists generally work in office facilities, although they may at times be required to provide on-site support in other locations. A specialist may work independently to meet the needs of a small organization or alongside other specialists performing similar tasks in a large help-desk facility. Computer and technical support specialists may work more than forty hours per week and may be required to work nights, weekends, and on-call hours as needed.

Individuals drawn to the profession of computer and technical support specialist are skilled in computer technology and customer service. They are capable problem solvers interested in understanding complex software and the interactions between various forms of technology. Specialists must be excellent communicators and able to work with customers who are often frustrated or under time constraints. Those who work in the gaming industry must be familiar with a range of video games.

Duties and Responsibilities

The daily duties of a computer and technical support specialist vary according to the organization for which he or she works and the type of support the specialist provides. In general, computer support specialists respond to inquiries or requests for help

from clients, customers, or fellow employees. They may be responsible for the oversight of all computer systems, or they may specialize in troubleshooting and problem-solving for one type of software or computer function.

If they are responsible for organizational systems, computer support specialists may spend their time setting up and programming new computers, repairing and replacing malfunctioning units, installing software, training employees to use the systems in place, and maintaining internal networks and servers. They may also provide help-desk services, answering user queries and ensuring that systems function smoothly.

Help-desk specialists may receive requests for assistance in person or via phone or email. They

often access users' computers remotely. They must be familiar with a variety of operating systems and computer types and be able to identify and understand physical, electronic, and software problems. If the cause of a problem is difficult to identify, a computer support specialist must be able to run diagnostic tests to pinpoint the issue. Specialists reinstall operating systems, remotely clean infected or malfunctioning systems, and work with customers to ensure that problems do not reoccur. They often provide support related to printers, scanners, email, networking and internet access, and word-processing and spreadsheet software.

Computer and technical support specialists must remain up to date regarding advances in computer or video game technology and must be able to



Photo via iStock/PeopleImages. [Used under license.]

explain complex systems in a clear and understandable manner. Because of this, specialists typically undergo a significant amount of ongoing training and may occasionally attend workshops or industry conferences.

WORK ENVIRONMENT

Physical environment. Computer and technical support specialists typically work in office environments, but the nature of these facilities varies based on industry. A specialist may work in a small office in an individual company or be one of many support specialists housed in a large facility. Though most large support facilities are operated as call centers, some companies have begun to allow employees to work in flexible or shared office spaces or even from their own homes.

Human environment. Computer and technical support specialists spend their workdays in constant interaction with clients or customers. They may also interact with managers, coworkers, and other support specialists throughout the day. In office support environments, specialists interact regularly with fellow employees.

Technological environment. A computer and technical support specialist must be familiar with all computer or video game technology used by his or her employing organization and should also be able to recommend advances and upgrades to existing systems. A specialist generally must have a thorough knowledge of both hardware and software as well as network systems and other peripheral equipment and accessories.

EDUCATION AND TRAINING

High school/secondary. Students interested in the field of computer and technical support should take courses in computer programming and computer science, as well as algebra and calculus. Business or applied mathematics classes may be useful as well. Those interested in joining the gaming industry

must become familiar with a wide range of video games.

College/postsecondary. While an associate's degree from a technical or two-year college is generally the minimum educational requirement for computer and technical support specialists in some companies, a four-year degree in computer science is preferred by many employers. A specialist seeking to advance to a specialized, higher-level position may benefit from pursuing a master's degree or doctorate, but this level of expertise is generally not needed for a support position.

Adult job seekers. Adult job seekers in this field may benefit from the wide variety of computer courses available at vocational, technical, and community colleges. Valuable experience can also be gained in the military, which relies heavily on computer systems.

Professional certification and licensure. There is no required certification or licensure for computer and technical support specialists. However, specialists may choose to gain voluntary certification in a number of computer systems, programs, and skills. Such certifications are offered by professional organizations and training centers and may demonstrate to prospective employers that an applicant is well versed in a particular area. Computer support specialists should consult credible professional associations within the field and follow professional debates as to the relevance and value of any certification program.

Additional requirements. Computer and technical support specialists must have excellent problem-solving and communication skills. A degree of creativity is also helpful, as specialists may at times be required to devise unusual solutions to problems.

—Bethany Groff

Further Reading

Campbell-Kelly, Martin, William F. Aspray, Jeffrey R. Yost, Honghong Tinn, and Gerardo Con Díaz.

- Computer: A History of the Information Machine.* 4th ed., Routledge, 2023.
- O'Leary, Timothy, Linda O'Leary, and Daniel O'Leary. *Computing Essentials 2023*. McGraw-Hill, 2022.
- Watters, Paul A. *Cybercrime and Cybersecurity*. CRC Press, 2023.

COMPUTER CRIME INVESTIGATION

ABSTRACT

Computer crimes are crimes in which computers, computer networks or databases, digital devices, or the internet have been attacked or infiltrated as well as crimes that are facilitated by computers, wireless web devices, or the internet.

BACKGROUND

In its earliest forms, cybercrime was carried out with hacker tools that required computer expertise to use. During the 1970s, most computer criminals were hackers who were highly motivated people with technical knowledge; some worked at universities or computer centers. In 1988, Robert Morris, Jr., a graduate student at Cornell University and son of a chief scientist at the US National Security Agency (NSA), developed an internet worm that infected thousands of computers and cost an estimated \$100 million in cleanup.

In 1992, the Federal Bureau of Investigation (FBI) proposed expanding federal wiretapping laws to require all public and private networks in the United States to be capable of intercepting an intruder's or suspect's activities. The FBI wanted real-time remote access to all data, fax, voice, and video traffic in the United States. Civil liberties groups contested this proposal, however, and were able to defeat it.

The first federal computer crime statute was the Computer Fraud and Abuse Act of 1984 (CFAA). Only one indictment was made under the CFAA before it was amended in 1986. By the mid-1990s,

almost every US state had enacted a computer crime statute. These statutes criminalize any wrongful access into a computer, regardless of whether any damage occurs as a result. Other statutes under which the FBI investigates computer-related crimes include the Economic Espionage Act and the Trade Secrets Act.

Many countries have adopted similar statutes designed to protect electronic commerce, the financial industry, and information stored on computers. An ongoing challenge for those investigating computer crime is keeping up with hardware and software advances that can affect forensic analysis.

OVERVIEW

The investigation and prosecution of computer crimes are concerns for the private, public, and government sectors responsible for information security. Computer crime, also called cybercrime, is one of the highest priority crimes investigated by the FBI, alongside terrorism and espionage.

Computer-based crimes caused an estimated \$14.2 billion in damages to businesses throughout the world in 2005, including the cost of repairing systems and lost business. Costs to individuals who were victims of identity theft were also tremendous. The financial impacts of computer crimes continued to increase throughout the next decades, and by the year 2023, the cost of cybercrime had reached an estimated annual, global cost of \$8 trillion, according to the statistics platform Statista.

Because computer crime can be committed anonymously from anywhere in the world, and because it is difficult to prove who was at the keyboard in any given case, capturing and prosecuting computer criminals has historically been difficult. The people who carry out such crimes are difficult to identify or locate in part because they work hard to hide the electronic tracks left by their activities. They can disguise or hide their identities by hacking into and taking control of internet-connected computers

anywhere in the world and routing their activities through them.

With few effective deterrents in place, traditional criminals such as con artists, extortionists, child pornographers, money launderers, industrial spies, and drug dealers have been able to increase the scope and frequency of their crimes by using computer and communication technologies. In addition, with increasing numbers of users connected to the internet, particularly in developing countries, geographic barriers to entry into criminal activity have been eliminated. One of the greatest financial threats in computer crime comes from spyware programs sent from developing countries that secretly record passwords, banking information, or other keystrokes. These confidential data are then sent to data thieves who sell them to money launderers or other criminals.

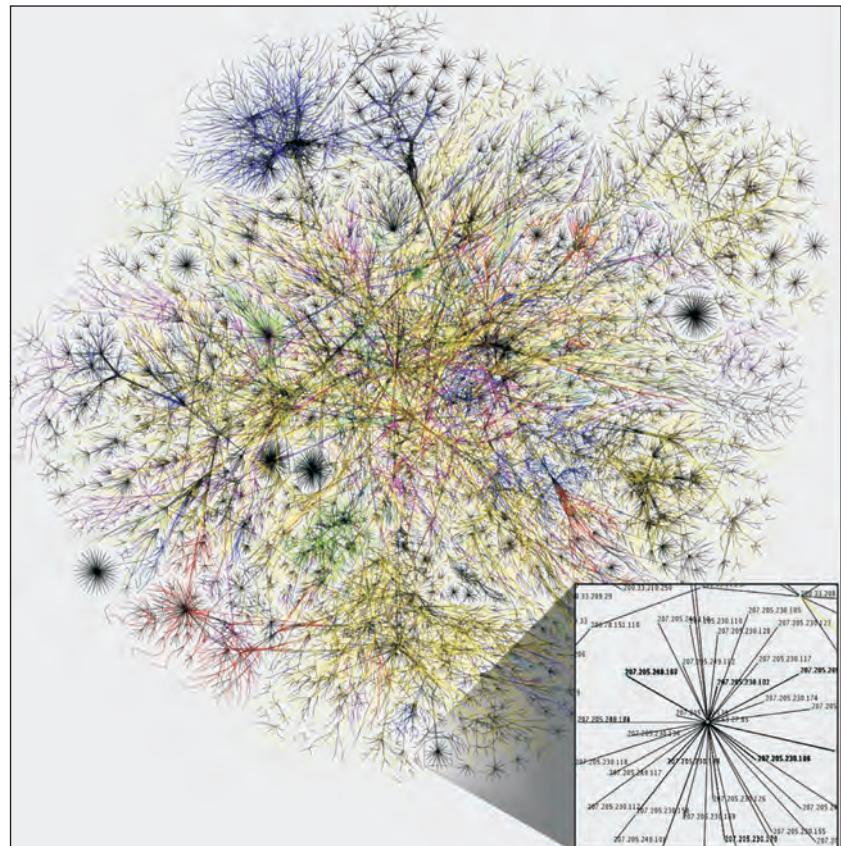
Serious crimes involving the exploitation of children have moved online. Pedophiles cultivate relationships with children using social network websites and then arrange to meet them in public places. Child pornographers use file servers, chat rooms, and email to distribute images.

Computer crimes do leave electronic evidence on individual computers, on computer networks, and in log files. The downloading, storage, and distribution of images or files leave electronic evidence. Because spyware programs get installed on victims' computers, evidence of their existence can be found in the receiving computers' registries. Although different types of computer crimes are investigated differently, a number of generally accepted policies and procedures, if strictly followed, can help

investigators to locate, acquire, and recover electronic evidence that is admissible in court.

Computer Crime and Physical Investigations

Because considerable overlap exists between computer crimes and traditional physical and financial crimes, traditional criminal personality profiling is valuable in computer forensic investigations, where computers and the internet are the electronic crime scenes. For example, fraud and extortion are age-old crimes that are more easily committed using computer technology. Cyberterrorists have extorted millions of British pounds by threatening to knock out computer-dependent financial systems, and extortionists have hacked into corporate databases and demanded huge payoffs in exchange for not destroying or publishing the data stored there.



An Opte Project visualization of routing paths through a portion of the Internet. Image by The Opte Project, via Wikimedia Commons.

Investigators should assess how they would investigate particular crimes or criminals in the physical world and then apply that knowledge to the digital world. By examining the similarities between crimes committed through physical methods and those committed using electronic methods, investigators can better understand the perpetrators and where to search for evidence.

Given the dramatic increase in the incidence of computer crimes throughout the first decades of the twenty-first century, prosecutors and law-enforcement agents must be knowledgeable concerning how to go about obtaining the electronic evidence stored in computers. Electronic records such as computer network logs, emails, and electronic documents and picture files increasingly provide authorities with essential evidence in criminal cases. Computer hard drives and other storage media are the digital equivalents of filing cabinets holding information that investigators can turn into proof of a variety of crimes, including the distribution of child pornography, embezzlement, drug trafficking, money laundering, identity theft, sexual harassment, theft of trade secrets, cyberterrorism, and cyberstalking.

Computer investigations, like other forensic investigations, require specialized knowledge to acquire, preserve, analyze, and interpret the evidence. Incriminating evidence may be found in email and logs of internet activity on a single computer or may reside on many computers that cannot be physically located. Complicating computer investigations are criminals' attempts to avoid detection by deleting electronic files or formatting hard drives to hide the evidence, but even in such cases, trained computer forensic examiners can almost always find electronic evidence of crimes as well as evidence of the efforts made to hide or delete incriminating material.

In some ways, computer forensic examiners must take even greater care than investigators of traditional crime scenes because of the extremely fragile and easily altered nature of electronic evidence.

Because electronic evidence has become increasingly crucial to many civil and criminal cases, the field of computer forensics has gained national recognition. In the United States, the FBI established multiple state-of-the-art Regional Computer Forensics Laboratories (RCFLs). In these labs, computer forensics techniques are increasingly applied to the investigation of a variety of crimes, not just those involving computers, as internet and mobile phone technologies become a pervasive part of everyday life and criminal activity.

In 2008, the US Secret Service has established a national computer forensics lab—the National Computer Forensics Institute (NCFI)—in Alabama with partial funding by the Department of Homeland Security's National Cyber Security Division. The facility serves as a national cybercrimes training center for prosecutors and judges as well as law-enforcement investigators. The NCFI expanded significantly in the years following its creation, encompassing about 40,000 square feet of space within the Hoover Public Safety Center by late 2022.

PRESERVING ELECTRONIC EVIDENCE

Computers can be the instruments used to commit crimes as well as the targets of crimes. These crimes leave electronic evidence, but that evidence is rarely readily apparent. To obtain and protect potential legal evidence for use in criminal prosecutions, investigators must search computers, computer networks, and data storage devices using generally accepted computer forensics methods and tools. Experts use established investigative and analysis techniques to uncover information and system data, including damaged, deleted, hidden, or encrypted files. They seize and collect digital evidence at crime scenes, conduct impartial examination of the computer evidence, and then testify as required.

In matters of evidence, it is mandatory that law enforcement personnel observe strict procedures regarding chain of custody, and all items must be

preserved for independent analysis. The successful prosecution of computer criminals depends on the presentation of evidence that shows the connections between the suspects and the crimes. All records concerning the illegal intrusions or incidents of interest must be preserved; nothing should be deleted, tampered with, or altered.

To ensure the preservation of electronic evidence, an investigator needs to be prepared with a forensic kit that includes the following: tools such as screwdrivers, pliers, and scissors; watertight and static-resistant plastic bags to store collected evidence; labels to use in marking items such as cables, connections, and evidence bags; power, universal serial bus (USB), and printer cables; logbook to record the investigator's actions; and external USB hard drive to transfer large amounts of data or images.

STEPS IN THE FORENSIC EXAMINATION

When the evidence arrives at the computer forensic lab, the investigator must document the time and date and complete the appropriate chain-of-custody forms. The evidence must be stored in a secure area, where access to it is limited and controlled.

The acquisition phase of a computer investigation can take place either on-site or in the forensic lab. In either case, steps must be taken to ensure the integrity of the evidence. The preferred method is to conduct this phase in the trusted environment of the laboratory whenever circumstances permit. The acquisition of electronic evidence is a crucial step in the investigation because this is where the potential for alteration of the original evidence is greatest. It is vitally important that the investigator follow standard procedures and document all actions in order to ensure the integrity of the evidence beyond a reasonable doubt.

At the start of the acquisition process, the investigator must document the computer hardware and software that will be used to conduct the acquisition

and analysis. After this documentation is complete, the next step is to disassemble the suspect computer. The main purpose of this is to allow the investigator access to the storage device on the suspect computer. The investigator must have access to the storage device to get data off the label of the device and to identify all storage devices, both internal and external, that are part of the computer.

The acquisition of evidence then proceeds with the copying of the suspect computer's hard drive; this process is called imaging or mirroring. The acquired forensic image must be verified to be an exact copy of the original. Specialized computer forensics software, such as EnCase or Forensic Toolkit (FTK), is typically used to create and verify the image. After a forensic image has been created, the investigator makes a duplicate to have a working copy of the image to analyze, so that if one image is destroyed or damaged or becomes corrupted, another copy is available without having to involve the original evidence.

The next phase is examination of the forensic image. Although computer forensic examiners should always follow certain basic procedures and start the examination phase in particular areas, an experienced examiner will also try to understand how the suspect thinks and works and then use that information to steer the examination method. For example, if the suspect is a novice computer user, the examination will usually cover only the basics. In contrast, examining the machine of an expert user who can hide or manipulate data forces the examiner to look for stealth activities when searching for evidence. Usually, this work is done with an image of the suspect's drive, and a separate hard drive is used to save evidence and tools for the case.

In the extraction phase, the examiner extracts data files for further analysis. It is during this step of the investigation that the data are searched for proof of crimes. The files are searched using key words, names, dates, and other file properties. One

challenge faced by computer forensic examiners is data hiding—that is, the files to be examined may be password protected, encrypted, disguised, compressed, deleted, or corrupted. To crack a password, an examiner needs password-cracking software for the specific data file type. The difficulty of cracking a password is usually in direct correlation to the sophistication of the computer user.

One form of data hiding is the disguising of files by changing their file extensions. This is easily detected by most forensic software packages that do an analysis of file headers and compare them to established file extensions. Passwords on files usually yield clues in and of themselves, in that some passwords are very personal in nature and connect users to particular files. Another reason passwords are evidentiary in nature is that they help to prove that suspects intended to hide the contents of their files.

For file compression, forensic examiners use utilities that simply let the software reverse the compression process and specify where the uncompressed versions are to be saved. Dealing with encrypted files is much more difficult, as the encryption of a file itself may be so strong it can literally take years to decrypt.

Another method of data hiding is steganography, in which data are hidden within another file, such as a picture or music file. The technologies used in steganography vary, but the basic premise is that a small portion of an existing file is replaced by an embedded or hidden file. If a suspect has used “stego,” it is very hard for an investigator to find the hidden file unless “before-and-after” versions of the file in which it is hidden are available. If the user has kept the original file on the computer’s storage device and embedded data in a copy, the investigator can literally compare the two files bit by bit to determine whether they are different. The investigator must then find out which stego program was used to embed the file, because only the software used can realistically reverse the process.

In the final step of a computer forensic examination, the examiner completes the necessary documentation and writes a report of the processing, analysis, and interpretation of the evidence. Most organizations have standard sets of forms that forensic examiners must use in documenting their cases; these forms also provide examiners with guidelines to follow.

TRACKING CRIMINALS IN INTERNET RELAY CHAT

Investigators sometimes track criminals through their use of internet chat rooms.

Pedophiles and other criminals often meet in such chat rooms to find victims, advertise, learn new skills, or teach others. They may also discuss their personal lives, allowing law-enforcement personnel to learn more about the social cultures of these criminals. System logs can enable investigators to track down criminals because such logs hold evidence that crimes have been committed and where the intrusions occurred. These logs cannot identify intruders, however—that is, they cannot indicate who was physically using given keyboards at any particular times. In internet relay chat (IRC), however, individuals can be identified.

Hackers often do not connect to IRC directly. By using a variety of servers or hosts, hackers can subvert bans or trick others into thinking they are other people. Usually, hackers seek to hide their real internet protocol (IP) addresses so that no one can find them and monitor their activities. They do so by using bounce programs, which read from one port and write to another.

These programs allow users to make a connection, connect to a destination, and then relay anything from the original connection to the destination. Hackers who have access to such programs can “bounce” through proxy servers to hide their tracks. Even if a complete audit trail shows that an intruder came from a specific account on a specific internet

service provider (ISP), the only evidence will be billing information for the account, which does not prove identity.

—Linda Volonino

Further Reading

- Anderson, Jon. “National Computer Forensics Institute Opens 7th Classroom in Hoover.” *Hoover Sun*, 18 Oct. 2022, hooversun.com/news/national-computer-forensics-institute-opens-7th-classroom.
- Casey, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. 3rd ed., Academic Press, 2011.
- Holt, Thomas J., Adam M. Bossler, and Kathryn C. Seigfried-Spellar. *Cybercrime and Digital Forensics: An Introduction*. 3rd ed., Routledge, 2022.
- Kipper, Gregory. *Wireless Crime and Forensic Investigation*. Auerbach, 2007.
- Petrosyan, Ani. “Annual Cost of Cybercrime Worldwide 2017–2028.” *Statista*, 15 Sept. 2023, www.statista.com/forecasts/1280009/cost-cybercrime-worldwide.
- US Department of Justice. Criminal Division. *Federal Guidelines for Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*. US Government Printing Office, 2002.
- Volonino, Linda, Reynaldo Anzaldua, and Jana Godwin. *Computer Forensics: Principles and Practice*. Prentice Hall, 2007.
- Watters, Paul A. *Cybercrime and Cybersecurity*. CRC Press, 2023.

COMPUTER FRAUD

ABSTRACT

Computer fraud is a type of crime that involves using computers to defraud businesses, governments, or individuals. This could include stealing money, identity theft, illegally accessing private information, or intentionally preventing revenue. It is primarily carried out through viruses, phishing, distributed denial-of-service (DDoS) attacks, and social engineering.

BACKGROUND

The term “computer fraud” refers to any attempt to use computers or computer software to defraud governments, corporations, or individuals. It may involve the theft of private or important information, such as internet histories, bank account numbers, and contacts. It may also involve the theft of money or other valuable resources. In the United States, computer fraud is illegal under the Comprehensive Crime Control Act. The act was passed on October 12, 1984, and was updated in 2008.

Computer fraud comes in many forms. These include phishing, malware, distributed denial-of-service (DDoS) attacks, and social engineering. Computer users should be wary against attacks and take a number of precautions to keep their digital information safe from criminals. Operating systems and antimalware software should be kept up to date, passwords should be crafted in a manner that makes both guessing and cracking them difficult, and anyone who asks for log-in information should be carefully scrutinized. Most legitimate businesses will never ask for a customer’s username and password.

OVERVIEW

Phishing is a type of email scam perpetrated by a criminal intending to steal personal information, such as bank account numbers, usernames, passwords, or Social Security numbers. It involves creating a falsified email, usually claiming to belong to a reputable online store or banking institution. This email asks for the log-in or purchasing information of the user. Because users erroneously believe the email is from a reputable source, they are likely to enter their information into the email. In some cases, the email links to a false page designed to look like the impersonated website. Users then attempt to log into the fake website and transmit their credentials to the criminal. This information can be used to steal money or perpetrate identity theft, or it can be sold to other criminals.



Image via iStock/Mykyta Dolmatov. [Used under license.]

Malware is malicious programming installed on individuals' computers without their knowledge or consent. It includes viruses, spyware, adware, and any other variety of malicious software.

Viruses are computer programs or scripts that modify the files on computers in disadvantageous or unethical ways. The malware may steal information, delete files, display messages, send false emails, or cause a computer to run slowly. Viruses spread by copying themselves to other computers through emails or other forms of file sharing.

Spyware is software designed to illegally spy on a computer user. It keeps a record of the user's activities, including keystrokes and browser history. This information is sent to a remote computer, where it can be used or sold. Adware is malware designed to

show advertisements to a computer user. It is often coupled with spyware, allowing the malware to use an individual's search history to show targeted advertisements.

All varieties of malware can be extremely damaging to a computer. Users should run reputable antivirus or antimalware software to stop infections before they occur. If computer users suspect their devices may be infected by malware, they should take the equipment to a professional for proper removal of the virus. Failure to remove malicious software could result in identity theft, loss of personal files, or monetary theft.

DDoS attacks are used to disrupt a website or digital service. They utilize a botnet, or a network of computers remotely controlled through software. In

many cases, botnets are created by viruses. They infect computers without the knowledge of the users, allowing criminals to control the users' computers without their knowledge or consent. To orchestrate a DDoS attack, botnet controllers order their botnets to attack a small number of servers or computers. The large botnet is able to overwhelm its target, disabling it. This is most commonly used to temporarily disable the web presence of certain news outlets, stores, businesses, and government agencies.

Social engineering involves tricking a person into providing important information used for cybercrime. For example, a criminal could trick an employee of a company into believing he is from the company's information technology division. The criminal could use this deception to convince the employee to allow the criminal to use his computer account, granting the criminal access to a company's computer network. Other common social engineering techniques include pretending to be a parent, spouse, or student to gain access to accounts or computer networks.

PREVENTION

Computer fraud can be prevented in a number of ways. Proper cybersecurity measures will stop most attempts at computer fraud. These include keeping antimalware software updated, creating difficult-to-crack passwords, and utilizing two-factor authentication for important accounts. Two-factor authentication involves linking a cell phone with a specific computer account. If the computer fails to recognize a user's password, or suspects that someone may have hacked into the account, the computer can send a code to the cell phone linked with the account. Without this code, the account cannot be accessed. While it is possible for criminals to acquire a password, it is extremely unlikely that they also have access to the cell phone linked to it.

In addition to these steps, users should verify that important information being transmitted, such as

passwords and credit card numbers, are only sent through encrypted channels. Encryption means that even if the information is intercepted by a third party, it will be extremely difficult for that party to unlock any important data.

—Tyler Biscontini

Further Reading

- “Computer Fraud.” *Computer Hope*, 18 Oct. 2022, www.computerhope.com/jargon/c/computer-fraud.htm.
 - “Computer Internet Fraud.” *Cornell Law School*, www.law.cornell.edu/wex/computer_and_internet_fraud.
 - “Distributed Denial of Service Attacks.” *Imperva*, www.imperva.com/learn/ddos/denial-of-service.
 - “How to Protect Yourself While on the Internet.” *Computer Hope*, 1 May 2023, www.computerhope.com/issues/ch000507.htm.
 - “Phishing.” *Computer Hope*, 1 Oct. 2023, www.computerhope.com/jargon/p/phishing.htm.
 - “Tech Support Scams.” *Federal Trade Commission*, Sept. 2022, www.consumer.ftc.gov/articles/0346-tech-support-scams.
- Watters, Paul A. *Cybercrime and Cybersecurity*. CRC Press, 2023.

COMPUTER FRAUD AND ABUSE ACT

ABSTRACT

As amended in 1994, the Computer Fraud and Abuse Act (CFAA) allows a private party who suffers damages or loss as a result of hacking, or unauthorized computer access, to bring a civil action and obtain compensatory damage, injunctive relief, or other equitable relief.

BACKGROUND

The US Congress enacted the first version of the Computer Fraud and Abuse Act (CFAA) in 1984. It was originally entitled the Counterfeit Access Device and Computer Fraud and Abuse Act. This act imposed criminal sanctions on hackers and other criminals who accessed computers without authorization. Ratified during the dawn of the internet era,

the statute prohibited hacking of certain types of information, such as matters concerning national security, foreign relations, and financial credit.

In 1986, the act was renamed the Computer Fraud and Abuse Act. In 1994, the CFAA underwent a notable expansion and established a private right of action for individuals harmed by certain violations of the CFAA. But for an individual to be exposed to civil liability, the individual's actions must meet one of at least six additional factors listed in the statute.

The six bases for civil liability include: loss aggregating to at least \$5,000 in value; the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals; physical injury to any person; a threat to public health or safety; damage affecting a computer used by or for the US government to further the administration of justice, national defense, or national security; or damage affecting ten or more protected computers during any one-year period.

OVERVIEW

CFAA claims are most often brought under 18 U.S.C. §1030(a)(2), §1030(a)(4), and §1030(a) (5). Each of these sections includes either the phrase “without authorization” or the phrase “exceeds authorized access.” While the phrase “exceeds authorized access” is defined in the statute as “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled to so obtain or alter,” the term “authorized” is never defined. Consequently, courts in different federal circuits have used varying definitions of “authorized.”

The different interpretations of the term “authorization” are relevant because, under a broad interpretation, more conduct constitutes a federal crime. Under a narrow interpretation, only a small subset of conduct that meets that definition is prohibited.

In federal circuits that adopt a broad definition of authorization, employers have been able to bring lawsuits under the CFAA for conduct such as unfair competition and trade secret misappropriation. However, in circuits that had adopted a narrow definition, less conduct has qualified as lacking or exceeding authorization, and fewer types of lawsuits have been successful.

The Fourth and Ninth Circuit courts have adopted a narrow definition of authorization. Under this definition, only a *technical* breach of access is deemed to lack or exceed authorization. The reason behind this narrow view is discussed at length in the seminal Ninth Circuit case *United States v. Nosal* (9th Cir. 2012). In that case, current employees of an executive search firm used their employer-granted access to the company database to obtain and pass along confidential information to a former employee who was setting up a competing business. The Ninth Circuit held that, because the current employees had logged into the firm database with their valid log-in credentials, they had proper authorization and did not violate the CFAA, despite the fact that their ultimate use of the information breached the company’s policies. The court stated that any other meaning would turn a serious federal criminal hacking statute into “sweeping internet-policing mandate” and “make criminals of large groups of people who would have little reason to suspect they are committing a federal crime.”

In contrast to this, other legal courts have adopted broad definitions of authorization. To do so, they have creatively adapted agency theories, contract theories, and use-based theories to find CFAA liability in situations in which computer users had been given technical access but were violating an employment contract or company policy. Thus, in the case *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.* (W.D. Wash. 2000), the District Court held that the plaintiff lost authorization and breached the CFAA when he became an agent of a

direct competitor and used his former employer's proprietary information in a way that damaged his former employer.

Several courts have both employed an "intended use" analysis. These courts looked at the underlying purpose of certain company policies to determine whether an employee breached or exceeded technically authorized access. This theory resembles contract theory but is broader because it considers how employees used the information they attained, even if there was no direct contradiction of a written policy or contract. Thus, in *United States v. John* (2010), the Fifth Circuit held that an employee violated the statute when she used data from Citigroup's internal computer system to attain customer account information, which she then shared with others in order to engage in fraudulent activities. The court reasoned that such use was *unlikely* to be what the company intended when it granted her access.

Ultimately, as society's dependency on computers continues to grow, there is a growing need for the judiciary to offer clearer guidance for applying this statute.

—Myra Din

Further Reading

- Bernescu, Laura. "When Is a Hack Not a Hack: Addressing the CFAA's Applicability to the Internet Service Context." *University of Chicago Legal Forum*, 2013, p. 633.
- Kerr, Orin S. "Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes." *New York University Law Review*, vol. 78, 2003, p. 1596.
- _____. "Vagueness Challenges to the Computer Fraud and Abuse Act." *Minnesota Law Review*, vol. 94, 2010, p. 1561.
- Murray, Ryan Patrick. "Myspace-ing Is Not a Crime: Why Breaching Terms of Service Agreements Should Not Implicate the Computer Fraud and Abuse Act Written February 2, 2009." *Loyola of Los Angeles Entertainment Law Review*, vol. 29, no. 3, June 2009, p. 475.
- Olivenbaum, Joseph M. "Ctrl-Alt-Delete: Rethinking Federal Computer Crime Legislation." *Seton Hall Law Review*, vol. 27, 1997, p. 574.

Patterson, Kelsey T. "Narrowing It Down to One Narrow View: Clarifying and Limiting the Computer Fraud and Abuse Act." *Charleston Law Review*, vol. 7, no. 3, Mar. 2013, p. 489.

Rosen, David J. "Limiting Employee Liability under the CFAA: A Code-Based Approach to 'Exceeds Authorized Access.'" *Berkeley Technology Law Journal*, vol. 27, 2012, p. 737.

Schieck, Glenn R. "Undercutting Employee Mobility: The Computer Fraud and Abuse Act in the Trade Secret Context." *Brooklyn Law Review*, vol. 79, no. 2, 2014, p. 831.

Watters, Paul A. *Cybercrime and Cybersecurity*. CRC Press, 2023.

COMPUTER HARDWARE ENGINEER

ABSTRACT

Computer hardware engineers design and develop computer hardware components. They work in a variety of industries and contribute to the creation of numerous computerized devices, including personal computers, smartphones, automobiles, and appliances. Students aspiring to enter the profession should pursue studies in subjects such as computer science, engineering, and mathematics.

BACKGROUND

Computer hardware engineers research, design, develop, and test computer systems and components such as processors, circuit boards, memory devices, networks, and routers. Many hardware engineers design devices used in manufactured products that incorporate processors and other computer components and that connect to the internet. For example, many new cars, home appliances, and medical devices have internet-ready computer systems built into them. Computer hardware engineers ensure that computer hardware components work together with the latest software. Therefore, hardware engineers often work with software developers. For example, the hardware and software for mobile

phones and other devices frequently are developed at the same time.

OVERVIEW

Most computer hardware engineers typically work inside research laboratories, offices, or manufacturing firms where they test different types of computer models. The location of these research labs is most commonly found in or nearby large metropolitan cities. The majority of a computer hardware engineer's time would be spent working at their computer workstation. Engineers may also spend their time overseeing the installation and testing of what they created. In these instances, proper safety precautions must be taken—including a sterile

environment—to ensure the safety of each engineer. Most computer hardware engineers work a standard full-time week of forty hours, and depending on the time sensitivity of the workload, overtime may be required to complete projects.

A career as a computer hardware engineer will appeal to individuals who not only have a strong interest in computer science and engineering but also are strong critical thinkers when faced with complex problems. Computer hardware engineers must troubleshoot and find solutions for hardware and computer problems when it comes to their work. They should also be interested in the latest technology and open to constantly learning as technology continues to advance.



Photo via iStock/golubovy. [Used under license.]

DUTIES AND RESPONSIBILITIES

Computer hardware engineers use their education and skills to design, develop, and test new computer hardware and components. These include computer systems, computer chips, and the physical parts of computers. Engineers are also involved in the design and development of new routers, printers, and keyboards. Their daily responsibilities vary depending on the project they are working on. Meetings may be held throughout the day with other engineers, technology vendors, and various other employees.

Computer hardware engineers are normally involved in the entire process of product development and implementation. This includes the manufacturing process. Throughout the day, an engineer will provide technical support to other employees, including designers, the marketing department, and technology vendors. As computer technology is developed and created, engineers will perform tests and ensure that everything meets specifications and requirements. This testing process usually involves analyzing test data, product prototypes, or theoretical models. As new hardware is implemented, an engineer will monitor how it is functioning and make any modifications necessary so that it performs according to specifications. Engineers also make recommendations for additional hardware, such as keyboards, routers, and printers.

When new components are designed and manufactured, engineers have to make sure that the hardware is compatible with software developments. Because of this, hardware engineers collaborate closely with software developers throughout the process.

WORK ENVIRONMENT

Physical environment. The physical work environment for computer hardware engineers is predominantly in a research lab. These spaces are where they would design, build, and test what they have built. Overall, the laboratories where engineers

work are typically bright and open spaces that are clean and well-ventilated.

Human environment. Throughout the day, computer hardware engineers can go between solitarily working on projects and communicating with their colleagues when needed. Engineers may also find themselves collaborating with other professionals in similar fields, ranging from software engineers, manufacturers, other engineers, or technology vendors.

Technological environment. Computer hardware engineers work with a wide array of computer-based technologies that range from circuit boards and processors, to chips, electronic equipment, and computer hardware and software, including applications and programming. During the design process, computer-aided design (CAD) software is used, as well as servers that store large amounts of data. Computer hardware engineers must be aware of the latest advances in cutting-edge technology such as artificial intelligence (AI) in order to adequately meet the needs of burgeoning technologies in their designs.

EDUCATION AND TRAINING

High school/secondary. A requirement of employers is that an applicant must have a high school diploma or a GED certificate equivalent. High school courses such as science, mathematics, engineering, or computer science will greatly benefit anyone interested in pursuing a career as a computer hardware engineer. Schools that offer extracurricular clubs involving computer science, robotics, or science are also beneficial to those wishing to get into engineering.

College/postsecondary. Entry-level computer hardware engineers typically need a bachelor's degree in computer engineering or a related field, such as computer and information technology. Employers may prefer to hire candidates who have graduated from an engineering program accredited by a professional association, such as the Accreditation Board for Engineering and Technology, Inc.

(ABET). To prepare for a major in computer or electrical engineering, students should have a solid background in math and science.

Because hardware engineers commonly work with computer software systems, a familiarity with computer programming is usually expected. This background may be obtained through computer science courses.

Some large firms or specialized jobs may require a master's degree in computer engineering. Some experienced engineers obtain a master's degree in business administration (MBA). All engineers must continue their learning over the course of their careers in order to keep up with rapid advances in technology.

Adult job seekers. If an adult job seeker with no prior experience in computer engineering or similar fields wishes to pursue such a career, they should enroll in a college that offers a program to expand their skills. As technology continues to advance, a computer hardware engineer must be open to continuously learning during the span of their career.

Professional certification and licensure. Although certification is not typically required by employers, there are organizations that offer certifications should an individual decide to pursue one.

Additional requirements. Computer hardware engineers must exhibit exceptional analytical skills when it comes to examining and developing complex computer equipment. Critical thinking is an important skill for engineers in order for them to troubleshoot problems and determine proper solutions. Additionally, engineers must be willing to continue learning throughout their careers as technology advances and their knowledge must expand with it.

—Kristina Domizio, Patrick G. Cooper

Further Reading

Bhunia, Swarup, and Mark Tehranipoor. *Hardware Security: A Hands-On Learning Approach*. Morgan Kaufmann, 2019.

O'Leary, Timothy, Linda O'Leary, and Daniel O'Leary. *Computing Essentials 2023*. McGraw-Hill, 2022.
Smith, Monica. "Computer Engineers Crucial to Network Security." *FIU News*, 9 Aug. 2022, news.fiu.edu/2022/computer-engineers-crucial-to-network-security.

COMPUTER HARDWARE SECURITY

ABSTRACT

Computer hardware security can refer to a physical device used to scan a system or monitor network traffic such as a proxy server or hardware security module (HSM), which employs cryptographic keys for important functions like authentication (verifying the identity of a user or command). It also refers to the methods used to protect physical components, such as computer chips, from being hacked.

BACKGROUND

Almost all savvy computer users realize the importance of keeping their computer software safe from hackers. They purchase virus protection, install security updates when prompted, and avoid responding to obvious online scams. Many, however, do not pay attention to hardware security, exhibiting blind trust that the computer chips and other components that go into their devices pose no dangers. That attitude might have made sense in past decades. Then, chips were designed and manufactured at trusted foundries, under guarded conditions. By the 2010s, however, chips could be designed in the United States and digital blueprints then sent to Asia and elsewhere to be manufactured cheaply, keeping costs low for consumers. Those cost savings came with a price, however. With an insecure supply chain and an estimated 90 percent of US computer chips being manufactured in East Asia, individual hackers and even nation-states could easily find opportunities to install malicious "Trojan horse" circuits for their own nefarious purposes.

OVERVIEW

Computer chips that have been tampered with threaten the smartphones and computers that hold our personal information, and as more devices connect to each other due to Internet of Things (IoT) technology, the threat intensifies. Smart, connected cars, appliances, medical implants, and security cameras have become more accessible to consumers, and thus, more attractive to hackers. Reports have emerged, for example, that one brand of voice-controlled remote controls had been hacked so that they could be used as listening devices in corporate or government conference rooms, and in another instance, instructions were circulated for a device that looked and functioned like a universal serial bus (USB) wall charger while also decrypting and revealing all keystrokes from wireless keyboards in the vicinity. (The parts to build the device could be purchased for around \$80.) In 2015 a hacker, who claimed he was merely trying to help the airline by pointing out vulnerabilities, reportedly took control of a commercial flight by plugging his laptop into the electronic box mounted under his seat: he gained access not only to the in-flight entertainment system as intended, but also to the thrust-management system responsible for providing power to the plane's engines. Experts warn that there may come a day when malefactors tamper with smart automotive systems, causing mass accidents on American roads, or when terrorists target high-profile figures known to have implantable pacemakers.

While it is frightening to consider the impacts hardware Trojans can have on our automotive, healthcare, flight, and banking systems, it is perhaps even more disturbing to consider the implications for our national defense, power grids, and nuclear facilities.

THE PENTAGON PROBLEM

In 2012 the Senate Armed Services Committee completed a probe of counterfeit electronic parts being

used by the US military. The committee discovered 1 million bogus parts, including vital components for certain models of combat aircraft. Most of the parts had originated in China, which, on the whole, had little respect for intellectual property rights. Fears arose that the parts might be not only counterfeit, but actively malicious, and successive presidential administrations have all wrestled with ensuring that hardware components are secure. They tried boosting their "Trusted Foundries" initiative, which had been set up to source especially vital chips—those meant to survive nuclear war or used in highly secret programs, for example—from a handful of facilities in the United States. The initiative was expanded to include not just manufacturers but packaging and testing companies as well. Still, those chips were only a small percentage of the total purchased each year by the military, and from 2010 to 2019, China's share of the Defense Department's chip budget almost doubled. By the end of the decade, China was the undisputed leader in semiconductor manufacturing, supplying not just the United States. But the rest of the world. Some Pentagon analysts estimate that the Chinese government has access to about 80 percent of the world's communications and data because of that situation.

WHAT TECHNOLOGISTS ARE DOING

Cybersecurity experts point out that a very basic level of protection can be achieved simply by providing on-site, physical barriers to access, such as keeping mission critical computers and servers in a locked room with restricted entry. Strong passwords can also function as a form of internal lock, although a determined hacker can sometimes circumvent even the most robust password. Experts also suggest that institutional purchasers verify that their chip manufacturers have adequate documentation of their processes and security measures and that plans are in place for downloading and updating security patches.

There are several more sophisticated techniques being used to protect hardware, including designing attack-resilient chip architecture; microchip camouflaging, a tactic that prevents reverse engineering; and split manufacturing, which thwarts counterfeiting by an untrusted foundry by dividing a chip's blueprint into several components and distributing each to a different fabricator. Tools have also been developed that employ artificial intelligence to determine the normal, baseline behavior of a device and trigger an alert when that deviates, indicating that the device has been hacked. (Even rigorous postfabrication testing cannot always determine immediately if a malicious Trojan has been installed; problems may not arise until years later.)

IMPACT

Although software-based malware had long been an acknowledged problem, hardware security issues came to the fore during the 2010s and remained of great concern throughout the 2020s. With a \$400 billion global supply chain vulnerable to Trojan horses and intellectual piracy, the security of every connected device in the world is at stake. In response to concerns regarding hardware security, the US government in 2023 introduced its CHIPS for America funding project, which would provide financial assistance and incentives to companies seeking to manufacture computer chip components in the United States.

—Mari Rich

Further Reading

- “Biden-Harris Administration Announces CHIPS for America Funding Opportunity to Strengthen Semiconductor Supply Chains.” *US Department of Commerce*, 29 Sept. 2023, www.commerce.gov/news/press-releases/2023/09/biden-harris-administration-announces-chips-america-funding-opportunity.
- Donnelly, John M. “Pentagon Races to Shore Up Supply Chain Security.” *Government Technology*, 9 Apr. 2021, www.govtech.com/security/pentagon-races-to-shore-up-supply-chain-security.html.

- Kassner, Michael. “Self-Checking Chips Could Eliminate Hardware Security Issues.” *Tech Republic*, 31 Aug. 2016, engineering.nyu.edu/news/self-checking-chips-could-eliminate-hardware-security-issues.
- Marena, Ted, and Jenny Yao. “Hardware Security in the IoT.” *Embedded Computing Design*, 24 July 2015, www.embeddedcomputing.com/technology/security/hardware-security-in-the-iot.
- Markoff, John. “Smaller, Faster, Cheaper, Over: The Future of Computer Chips.” *New York Times*, 25 Sept. 2015, www.nytimes.com/2015/09/27/technology/smaller-faster-cheaper-over-the-future-of-computer-chips.html.
- Segal, Edward. “Worsening Computer Chip Crisis Shows Supply Chains Are Still at Risk.” *Forbes*, 12 July 2021, www.forbes.com/sites/edwardsegal/2021/07/12/worsening-computer-chip-crisis-shows-supply-chains-are-still-at-risk.

COMPUTER LANGUAGES, COMPILERS, AND TOOLS

ABSTRACT

Computer languages are used to provide the instructions for computers and other digital devices based on formal protocols. Low-level languages, or machine code, were initially written using the binary digits needed by the computer hardware, but since the 1960s, languages have evolved from early procedural languages to object-oriented high-level languages, which are more similar to English. There are many of these high-level languages, with their own unique capabilities and limitations, and most require some type of compiler or other intermediate translator to communicate with the computer hardware. Computer languages underlie the multitude of programs in use in the twenty-first century, from word-processing and design programs to data-analysis and simulation software. The popularity of the internet has created the need to develop numerous applications and tools designed to share data across the internet.

BACKGROUND

Early computers such as Electronic Numerical Integrator and Computer (ENIAC), the first general-purpose computer, were based on the use of switches that could be turned on or off. Thus, the binary digits of 0 and 1 were used to write machine code. In addition to being tedious for a programmer, the code had to be rewritten if used on a different type of machine, and it certainly could not be used to transmit data across the internet, where different computers all over the world require access to the same code.

Assembly language evolved by using mnemonics (alphabetic abbreviations) for code instead of the binary digits. Because these alphabetic abbreviations of assembly language no longer used the binary digits, additional programs were developed to act as intermediaries between the human programmers writing the code and the computer itself. These additional programs were called “compilers,” and this process was initially known as compiling the code. This compilation process was still machine and vendor dependent, however, meaning, for example, that there were several types of compilers that were used to compile code written in one language. This was expensive and made communication of computer applications difficult.

The evolution of computer languages from the 1950s has accompanied technological advances that have allowed languages to become increasingly powerful, yet easier for programmers to use. FORTRAN and COBOL languages led the way for programmers to develop scientific and business application programs, respectively, and were dependent on a command-line user interface, which required a user to type in a command to complete a specific task. Several other languages were developed, including Basic, Pascal, PL/I, Ada, Lisp, Prolog, and Smalltalk, but each of these had limited versatility and various problems. The C and C++ languages of the 1970s and 1980s, respectively, emerged as the most useful

and powerful languages and are still in use. These were followed by development tools written in the Java and Visual Basic languages, including integrated development environments with editors, designers, debuggers, and compilers all built into a single software package.

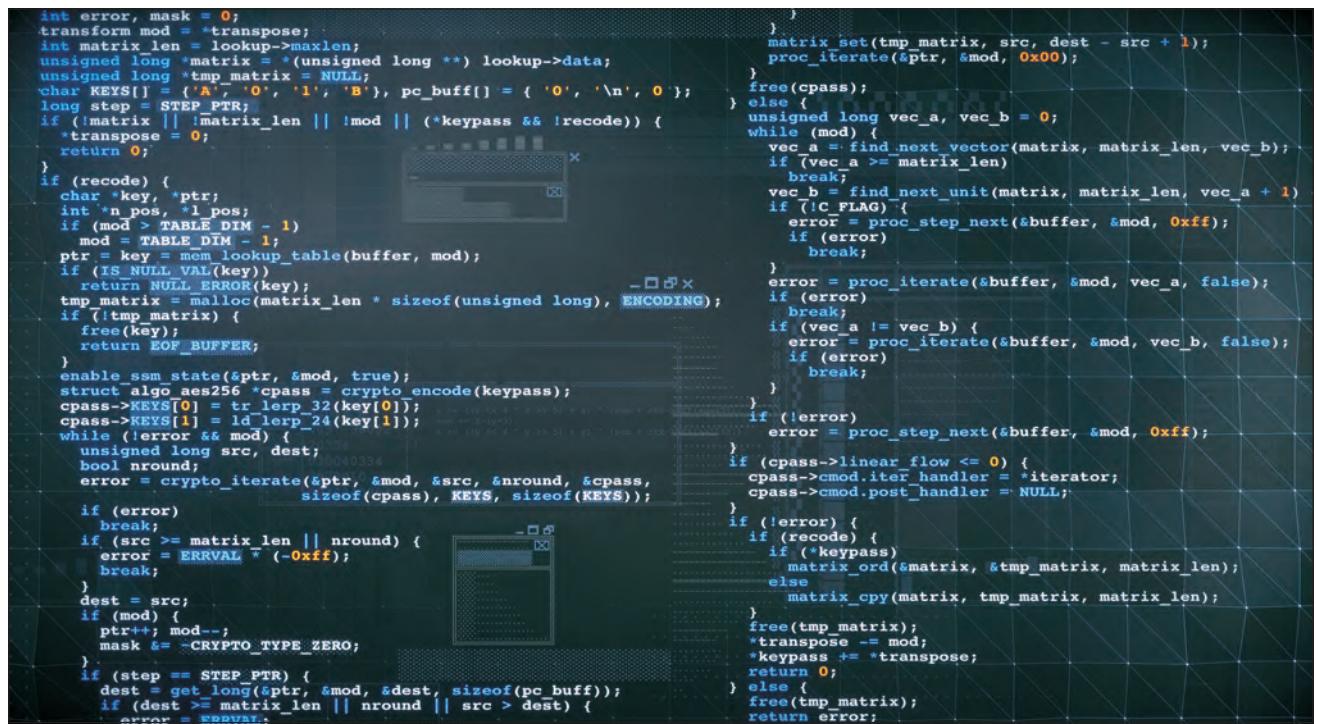
OVERVIEW

The traditional process of using a computer language to write a program has generally involved the initial design of the program using a flowchart based on the purpose and desired output of the program, followed by typing the actual instructions for the computer (the code) into a file using a text editor, and then saving this code in a file (the source code file). A text editor is used because it does not have the formatting features of a word processor. An intermediate tool, the compiler, then has been used to convert this source code into a format that can be run (executed) by a computer.

However, in the 2010s, a tool much faster and more efficient than compilers, called “interpreters,” gained prominence and replaced most compilers. Larger, more complex programs have evolved that have required an additional step to link external files. This process is called “linking,” and it joins the main, executable program created by the compiler to other necessary programs. Finally, the executable program is run and its output is displayed on the computer monitor, printed, or saved to another digital file. If errors are found, the process of debugging is followed to go back through the code to make corrections.

HOW IT WORKS

BIOS and operating system. The programs within the BIOS are the first and last programs to execute whenever a computer device is turned on or off. These programs interact directly with the operating system (OS). The early mainframe computers that were used in the 1960s and 1970s depended on



```

int error, mask = 0;
transform mod = *transpose;
int matrix_len = lookup->maxlen;
unsigned long *matrix = *(unsigned long **) lookup->data;
unsigned long *tmp_matrix = NULL;
char KEYS[] = {'A', '0', '1', 'B'}, pc_buff[] = { '0', '\n', 0 };
long step = STEP_PTR;
if (!matrix || !matrix_len || !mod || (*keypass && !recode)) {
    *transpose = 0;
    return 0;
}
if (recode) {
    char *key, *ptr;
    int n_pos, l_pos;
    if (mod > TABLE_DIM - 1)
        mod = TABLE_DIM - 1;
    ptr = key = mem_lookup_table(buffer, mod);
    if (IS_NULL_VAL(key))
        return NULL_ERROR(key);
    tmp_matrix = malloc(matrix_len * sizeof(unsigned long), ENCODING);
    if (!tmp_matrix) {
        free(key);
        return EOF_BUFFER;
    }
    enable_ssm_state(&ptr, &mod, true);
    struct algo_aes256 *cpass = crypto_encode(keypass);
    cpass->KEYS[0] = tr_lerp_32(key[0]);
    cpass->KEYS[1] = ld_lerp_24(key[1]);
    while (!error && mod) {
        unsigned long src, dest;
        bool nround;
        error = crypto_iterate(&ptr, &mod, &src, &nround, &cpass,
                               sizeof(cpass), KEYS, sizeof(KEYS));
        if (error)
            break;
        if (src >= matrix_len || nround) {
            error = ERRVAL ^ (-0xff);
            break;
        }
        dest = src;
        if (mod) {
            ptr++; mod--;
            mask &= ~CRYPTO_TYPE_ZERO;
        }
        if (step == STEP_PTR) {
            dest = get_long(&ptr, &mod, &dest, sizeof(pc_buff));
            if (dest >= matrix_len || nround || src > dest) {
                error = error;
            }
        }
    }
}
matrix_set(tmp_matrix, src, dest - src + 1);
proc_iterate(&ptr, &mod, 0x00);
}
free(cpass);
} else {
    unsigned long vec_a, vec_b = 0;
    while (mod) {
        vec_a = find_next_vector(matrix, matrix_len, vec_b);
        if (vec_a >= matrix_len)
            break;
        vec_b = find_next_unit(matrix, matrix_len, vec_a + 1);
        if (!C_FLAG) {
            error = proc_step_next(&buffer, &mod, 0xff);
            if (error)
                break;
        }
        error = proc_iterate(&buffer, &mod, vec_a, false);
        if (error)
            break;
        if (vec_a != vec_b) {
            error = proc_iterate(&buffer, &mod, vec_b, false);
            if (error)
                break;
        }
    }
}
if (!error)
    error = proc_step_next(&buffer, &mod, 0xff);
}
if (cpass->linear_flow <= 0) {
    cpass->cmod.iterator_handler = *iterator;
    cpass->cmod.post_handler = NULL;
}
if (error) {
    if (recode) {
        if (*keypass)
            matrix_ord(&matrix, &tmp_matrix, matrix_len);
        else
            matrix_cpy(matrix, tmp_matrix, matrix_len);
    }
    free(tmp_matrix);
    *transpose -= mod;
    *keypass += *transpose;
    return 0;
}
else {
    free(tmp_matrix);
    return error;
}

```

Photo via iStock/matejmo. [Used under license.]

several different OSs, most of which are no longer in use, except for UNIX and DOS (disk operating system). DOS was used on the initial microcomputers of the 1980s and early 1990s, and it is still used for certain command-line specific instructions.

Graphical user interfaces (GUIs). Microsoft dominates the personal computer (PC) market with its many updated OSs, which feature user-friendly GUIs. These OSs consist of computer programs and software that act as the management system for all of the computer's resources, including the various applications most taken for granted, such as Word (for documents), Excel (for mathematical and spreadsheet operations), and Access (for database functions). Each of these applications is a program itself, and there are many more that are also available.

Since the 1980s, many programming innovations increasingly have been built to involve the client-server model, with less emphasis on large

mainframes and more emphasis on the GUIs for smaller microcomputers and handheld devices that allow consumers to have deep color displays with high resolution and voice and sound capabilities. However, these initial GUIs on client computers required additional upgrades and maintenance to be able to interact effectively with servers.

World Wide Web (WWW). The creation of the WWW provided new means of accessing information, and the widespread use of the internet led to the creation of new programming languages and tools. The browser was developed to allow an end user (client) to be able to access web information, and hypertext markup language (HTML) was developed to display web pages. Because the client computer was manufactured by many different companies, the Java language was developed to include applets, which are mini-programs embedded into web pages that could be displayed on any type of client computer. This was made possible by a special

type of compiler-like tool called the “Java Virtual Machine,” which translated byte code.

APPLICATIONS AND PRODUCTS

FORTRAN and COBOL. FORTRAN (sometimes written as Fortran) was developed by a team of programmers at International Business Machines Corporation (IBM) and was first released in 1957 to be used primarily for highly numerical and scientific applications. It derived its name from formula translation. Initially, it used punched cards for input, because the text editors were not available in the 1950s. It has evolved but still continues to be used primarily in many engineering and scientific programs. Several updated versions have been released, including the 2023 revision Fortran 2023.

FORTRAN77, released in 1980, had the most significant language improvements. Common Business-Oriented Language (COBOL) was released in 1959 with the goal of being used primarily for tracking retail sales, payroll, inventory control, and many other accounting-related activities.

C and C++. The C computer language was the predecessor to the C++ language. Programs written in C were procedural and based on the usage of functions, which are small programming units. As programs grew in complexity, more functions were added to a C program. The problem was that eventually it became necessary to redesign the entire program, because trying to connect all of the functions was too difficult. C++ was created in the 1980s based on the idea of objects grouped into classes as the building blocks of the programs. Object-oriented programming made developing complex programs much more efficient.

Microsoft.NET. In June 2000, Microsoft introduced a suite of languages and tools named Microsoft.NET along with its new language called “Visual C#.”

Later known simply as .NET or the .NET framework, Microsoft.NET is a software infrastructure that consists of many programs that allow a user to write

programs for a range of new applications such as server components and web applications by using new tools. Although programs written in Java can be run on any machine, as long as the entire program is written in Java, .NET allows various programs to be run on the Windows OS. Additional advantages of .NET involve its use of Visual C#. Visual C# provides services to help web pages already in existence, and C# can be integrated with the Visual Basic and Visual C++ languages, which facilitate the work of web programmers by allowing them to update existing web applications, rather than having to rewrite them.

The .NET framework uses a common type system (CTS) tool to compile programs written in a variety of languages into an intermediate language. This common intermediate language (CIL) can then be compiled to a common language runtime (CLR). The result is that the .NET programming environment promotes interoperability to allow programs originally written in different languages to be executed on a variety of OSs and computer devices. This interoperability is crucial for sharing data and communication across the internet.

SOCIAL CONTEXT AND FUTURE PROSPECTS

The internet continues to bring the world together at a rapid pace, which has both positive and negative ramifications. Consumers have much easier access to many services, such as online education and telemedicine, and can use free search tools to locate doctors, learn more about any topic, comparison shop and purchase, and immediately access software, movies, pictures, and music. However, along with this increase in electronic commerce involving credit card purchases, bank accounts, and additional financial transactions has been the increase of cybercrime. Thousands of dollars are lost each year to various internet scams and the accessing of private financial information by hackers. Some programmers even use computer

languages to produce viruses and other destructive programs for purely malicious purposes, which have a negative impact on computer security. Such phenomena have given rise to the development of improved security features within computer languages and tools.

—Jeanne L. Kuhler

Further Reading

- Carpenter, Adam. "What Programming Languages Are Used in Cybersecurity?" *Codecademy*, 15 June 2021, www.codecademy.com/resources/blog/what-programming-languages-are-used-in-cybersecurity.
- Das, Sumitabha. *Your UNIX/Linux: The Ultimate Guide*. 3rd ed., McGraw-Hill, 2012.
- Dhillon, Gupreet. "Dimensions of Power and IS Implementation." *Information and Management*, vol. 41, no. 5, 2004, pp. 635–44.
- Horstmann, Cay. *Big Java: Early Objects*. 7th ed., John Wiley & Sons, 2018.
- Lee, Kent D. *Foundations of Programming Languages*. 2nd ed., Springer, 2017.
- O'Leary, Timothy, Linda O'Leary, and Daniel O'Leary. *Computing Essentials 2023*. McGraw-Hill, 2022.
- Petzold, Charles. *Code: The Hidden Language of Computer Hardware and Software*. 2nd ed., Microsoft Press, 2022.
- Scott, Michael L. *Programming Language Pragmatics*. 4th ed., Morgan Kaufmann, 2016.
- Sellers, Audrey. "Top Programming Languages of 2023." *Coding Dojo*, 3 Feb. 2023, www.codingdojo.com/blog/top-programming-languages.

COMPUTER MEMORY AND STORAGE

ABSTRACT

There are different types of memory inside a computer, including temporary memory, read-only memory (ROM), random-access memory (RAM), and programmable read-only memory (PROM). Computer storage technologies include hard drives and cloud storage. Memory and storage are used for different purposes. Fast, temporary memory such as RAM is used to make quick calculations, while hard drives are used for long-term storage of

programs and files. Without memory and storage, computers would not be able to function in any meaningful capacity.

BACKGROUND

In their earliest days, computers were strictly mechanical devices. They used punch cards for memory and output. These machines were developed for utility rather than for the multitude of tasks for which modern computers are designed. They were primarily used for complex calculations.

Alan Turing, a famous computer scientist, is credited with the idea for the first multipurpose computer. In the 1930s, J. V. Atanasoff created the first computer that contained no gears, cams, belts, or shafts. Atanasoff and his team then designed the first computer with functioning, nonmechanical memory devices. Primitive when compared to today's devices, Atanasoff's creation allowed the computer to solve up to twenty-nine equations simultaneously.

The next major leap in computing power was the usage of vacuum tubes. In 1944, professors John Mauchly and J. Presper Eckert built the first tube-powered electronic calculator. This is commonly considered the first digital computer. It was a massive machine, taking up the entirety of a large room. They soon began to market this computer to governments and businesses. However, tube computers became obsolete in 1947 with the invention of the transistor.

Ten years later, the transistor was used by Robert Noyce and Jack Kilby to create the first computer chip. This spurred the development of the first devices recognizable as modern computers. Computers took another leap forward with the graphical user interface (GUI), which projects options as images on a screen instead of requiring users to learn to code. Computers advanced further with the inventions of random-access memory (RAM) in 1970 and floppy disks in 1971. Floppy disks were a form

of permanent storage used in the early days of computers. They could easily be transferred from one computer to another, making them ideal for transporting information. Floppy disks were made obsolete by CD-ROMs, which are small plastic discs that store large amounts of information.

OVERVIEW

Computer memory and storage are measured in binary digits, called bits. One bit is an extremely small amount of information. Eight bits is the equivalent of one byte. 1,024 bytes is called a kilobyte (KB); 1,024 KB makes a megabyte (MB); 1,024 MB makes a gigabyte (GB); and 1,024 GB makes a terabyte (TB). Over time, the cost of large amounts of computer memory and storage has drastically fallen. However, the amount of memory and storage required by computers has also drastically increased.

Computers contain and utilize several types of memory and storage.

Temporary memory. The most common type contained in a computer is temporary memory, which is designed to hold information for only a short period. Most of a computer's temporary memory is RAM. RAM is designed to quickly write and erase information. It performs calculations, runs scripts, and enacts most of the computer's functions. A computer with more RAM can perform more functions at once, making it more powerful and more capable of running resource-intensive programs.

Permanent storage. Permanent storage may refer to several devices. In most cases, information is stored on the computer's hard disk drive (HDD). Some HDDs use a spinning disk and an actuator arm. The actuator arm writes to the spinning disk by rearranging electrons. In this scenario, the entire inside of the HDD is located inside an airtight seal. These hard drives can be found in many sizes. However, HDDs of the twenty-first century are often found in capacities of hundreds of gigabytes to terabytes.



Image via iStock/Andrew_Rybalko. [Used under license.]

Many high-quality computer manufacturers have begun replacing HDDs with solid-state drives (SSDs). Solid-state drives contain no moving parts. In most instances, these drives can read and write data much faster than HDDs. Because they have no moving parts, SSDs are also much quieter than HDDs. However, SSDs are also more expensive than HDDs. For this reason, if a device needs large quantities of storage, it may be more cost-effective to use HDDs. However, if the device needs to be able to access data quickly, be durable, or be compact in size, manufacturers may use an SSD.

External storage. Some computers utilize external forms of storage. These are drives located outside the device. If it is connected to the device by a universal serial bus (USB) cable or other interface, it is called an “external hard drive.” External hard drives are easily transferable from one device to another, making them useful for quickly moving large media files. They may also be used to back up large amounts of important files, protecting them from computer malfunction or viruses.

If the external storage is accessed through the internet, it is referred to as cloud storage. Many services offer large amounts of external storage for purchase. This may be used for server backups, media storage, or any number of other applications. Cloud storage allows users to expand the storage capacity of their machines without making any physical alterations to the computers. The cloud also features many of the same benefits as an external hard drive. Files can easily be relocated to a new machine in the event of a hardware or software failure and can likewise be shared among those collaborating on a group project, such as an engineering design. Additionally, renting space from a cloud storage service may be cheaper than purchasing and installing additional physical storage devices.

—Tyler Biscontini

Further Reading

- Brant, Tom. “SSD vs. HDD: What’s the Difference?” *PCMag*, 26 Aug. 2022, www.pc当地/news/ssd-vs-hdd-whats-the-difference.
- “Data Measurement Chart.” *University of Florida*, www.wu.ece.ufl.edu/links/dataRate/DataMeasurementChart.html.
- “Hard Drive.” *Computer Hope*, 18 Oct. 2022, www.computerhope.com/jargon/h/harddriv.htm.
- “How Computers Work: The CPU and Memory.” *University of Rhode Island*, homepage.cs.uri.edu/faculty/wolfe/book/Readings/Reading04.htm.
- O’Leary, Timothy, Linda O’Leary, and Daniel O’Leary. *Computing Essentials* 2023. McGraw-Hill, 2022.
- “Storage vs. Memory.” *PCMag*, www.pc当地/encyclopedia/term/storage-vs-memory.
- “Timeline of Computer History.” *Computer History Museum*, www.computerhistory.org/timeline/computers.

COMPUTER NETWORK ARCHITECT

ABSTRACT

Computer network architects build and maintain computer networks. They are sometimes referred to as data communications analysts or network analysts. Students aspiring to enter the profession should pursue studies in subjects such as computer science, mathematics, and network architecture.

BACKGROUND

Computer network architects—also known as data communications analysts or network analysts—conceptualize, build, and maintain computer information networks for businesses and organizations. Network architects may be employed as part of an organization’s computing staff or by companies who specialize in assisting businesses with setting up, monitoring, and maintaining their computer networks. They work closely with other senior members of a company’s computing staff, including network security personnel and systems administrators.



Photo via iStock/gremlin. [Used under license.]

OVERVIEW

Network architects work almost exclusively in administrative and office settings. Some projects, however, may require off-site work. The majority of network architects are employed by computer companies, educational organizations, governments, and finance companies. They are also employed in manufacturing and telecommunications.

Network architects have a passion and commitment to computing. The field attracts technically skilled individuals who enjoy analyzing, dissecting, and developing solutions for complex problems. In addition to significant experience with computers and electronics, most network architects are also well versed in fields such as engineering technology, mathematics, and telecommunications.

DUTIES AND RESPONSIBILITIES

Network systems and data communication analysts traditionally work regular business hours, with some exceptions and lengthier hours required during emergencies or for the completion of large-scale projects.

Network architects are responsible for a diverse workload that can require involvement in different tasks and projects simultaneously. Those who are employed by a singular entity are able to focus on modifications and maintenance of one system; conversely, network architects who are employed by computer firms that work with several business clients often work on multiple systems simultaneously.

Computer network architects who are employed by a singular organization, government agency, or

business spend their days adjusting network technologies to ensure they meet the organization's necessary capacity or traffic volumes. They also address any errors that arise within network systems and repair them quickly to avoid lapses in productivity or communication.

Network architects employed by telecommunications and computer companies specialize in designing, installing, and maintaining networks that are custom-made for the needs of a specific business or organization. The planning process involves extensive collaboration with administrators and staff members. Insight into a particular company's or organization's production process helps network architects determine the type of system and related technical apparatus that can best suit any data communications needs. Network architects also custom-design systems to cater to the needs of business customers, a task that is particular common in industries such as e-commerce, education, media, and publishing.

WORK ENVIRONMENT

Physical environment. Computer network architects work primarily in administrative and office settings.

Human environment. Many tasks inherent in the work of a network architect require strong collaboration skills. Network architects are also required to solicit information from coworkers and explain complex processes to colleagues and fellow professionals on a daily basis.

Technological environment. Data architects traditionally have expert-level knowledge of numerous technological tools and software applications ranging from network management, administration, and transaction security software. They are also experts in computer server systems, network switches, programming languages, and connectivity technologies.

EDUCATION AND TRAINING

High school/secondary. High school students can best prepare for a career in network architecture and data communication analysis by completing courses in algebra, calculus, geometry, trigonometry, desktop publishing, programming, and computer science. Advanced placement classes in mathematics and computer-related subjects are also recommended.

Many high school students take advantage of summer internships and volunteer programs offered by local companies to gain a better understanding of computers and computer networks in everyday applications in the professional world.

College/postsecondary. Possession of a bachelor's degree in a computer technology-related field is a commonplace requirement for nearly all employment vacancies in network architecture, particularly those at the entry level. While professionals reach the career path of networks system and data communications architect from numerous academic and professional experiences, network architecture is a distinct field of study at many colleges and universities throughout the United States.

Students enrolled in degree paths related to network design and administration complete coursework in programming, network security, systems analysis and design, technical writing, advanced mathematics, and project management.

Adult job seekers. Individuals with no background in a related field should enroll in a college or a technical or vocational school that offers a program in network systems data. Technical schools are also a great place for job seekers to network. Communication technologies and standards are always changing, so those making a career transition into the network systems field should be willing to continue learning throughout their career.

Given the amount of technical aptitude required of the position, data communications is not traditionally a field that people seek out when changing

careers. Individuals with previous professional experience or academic training in a technological field might find the transition possible.

Professional certification and licensure. Dozens of networking certifications are available for professionals in the data communications industry. Network certifications are tailored to specific industries and network communications needs and are available from myriad vendors, associations, and professional organizations that are recognized by professionals in the network communications industry. Additionally, the accumulation of certificates is a common way of illustrating expertise throughout the industry.

Additional requirements. In addition to excellent technological and computer skills, network architects must possess the patience and resolve to work on complex problems for long periods until the most effective and efficient solution is uncovered. Network professionals must also be willing team players who can work in concert with other computing professionals in a productive manner.

—John Pritchard

Further Reading

- Kizza, Joseph Migga. *Guide to Computer Network Security*. 6th ed., Springer, 2024.
- Peterson, Larry L., and Bruce S. Davie. *Computer Networks: A Systems Approach*. 6th ed., Morgan Kaufmann, 2021.
- Stewart, Andrew J. *A Vulnerable System: The History of Information Security in the Computer Age*. Cornell UP, 2021.

COMPUTER NETWORKS

ABSTRACT

Computer networks consist of the hardware and software needed to support communications and the exchange of data between computing devices. The computing devices connected by computer networks include large servers, business workstations, home computers, and a wide array

of smart mobile devices. The most popular computer network application is email, followed by exchanging audio and video files. Computer networks provide an infrastructure for the internet, which in turn provides support for the World Wide Web (WWW).

BACKGROUND

A computer network is a collection of computer devices that are connected in order to facilitate the sharing of resources and information. Underlying the computer network is a communications network that establishes the basic connectivity of the computing devices. This communications network is often a wired system but can include radio and satellite paths as well. Devices used on the network include large computers, used to store files and execute applications; workstations, used to execute small applications and interact with the servers; home computers, connected to the network through an internet service provider (ISP); and mobile devices, connected to the network by radio wave transmissions. Middleware is the software that operates on top of the communications network to provide a software layer for developers to add high-level applications, such as a search engine, to the basic network.

The scientists who developed the first computers in the 1950s recognized the advantage of connecting computing devices. Teletype machines were in common use at that time, and many of the early computers were “networked” with these teletype machines over wired networks. By 1960, American Telephone and Telegraph (AT&T) had developed the first modem to allow terminal access to mainframes, and in 1964, International Business Machines Corporation (IBM) and American Airlines introduced the Semi-Automated Business Research Environment (SABRE) networked airline reservation system.

The Defense Department created (Advanced Research Projects Agency Network (ARPANET) in 1966 to connect its research laboratories with

college researchers. The early experience of ARPANET led the government to recognize the importance of being able to connect different networks so they could interoperate. One of the first efforts to promote interoperability was the addition of packet switching to ARPANET in 1969. In 1974, Robert Kahn and Vinton Cerf published a paper on packet-switching networks that defined the transmission control protocol/internet protocol (TCP/IP), and in 1980, the US government required all computers it purchased to support TCP/IP. When Microsoft added a TCP/IP stack to its Windows 95 operating system, TCP/IP became the standard wide area network in the world.

The development of the microcomputer led to the need to connect these devices to themselves and the wide area networks. In 1980, the Institute of Electrical and Electronics Engineers (IEEE) 802 standard was announced. It has provided most of

the connectivity to networks since that time, although many wireless computing devices can connect with Bluetooth.

The high-level applications are what most people using the network see as the network. Some of the most important computer network applications provide communications for users. Earlier examples of this are email, instant messaging, chat rooms, and videoconferencing. Later examples of communications software are the multitude of social networks, such as Facebook and X (formerly known as Twitter). Other high-level applications allow users to share files. One of the oldest and still quite popular file-sharing programs is the file transfer protocol (FTP) program. Another way to use computer networks is to share computing power. The Telnet program (terminal emulation program for TCP/IP networks) allowed one to use an application on a remote mainframe in the early days of networking,

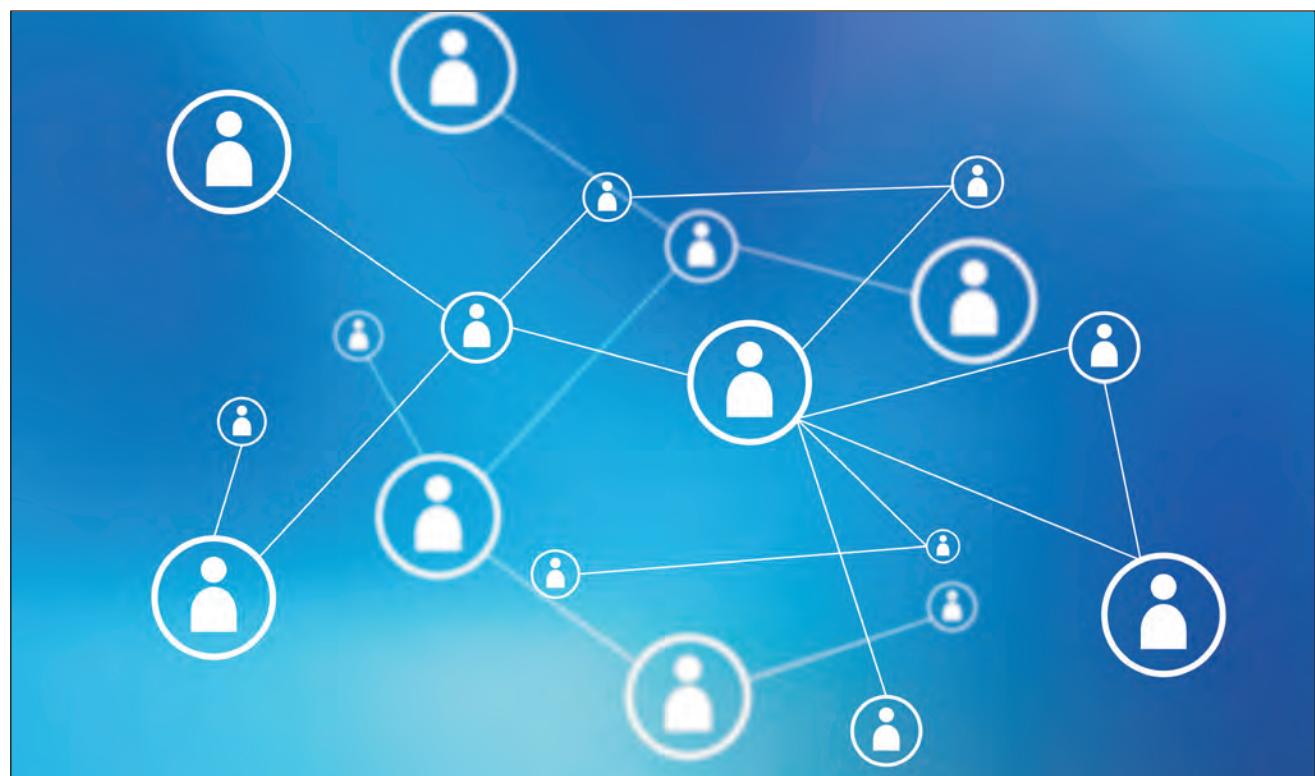


Image via iStock/Mara Yagmur Rozendaal. [Used under license.]

and twenty-first-century web services allow one to run an application on a mobile device while getting most of the functionality from a remote server.

OVERVIEW

Computer networks consist of the hardware needed for networking, such as computers and routers; the software that provides the basic connectivity, such as the operating system; and middleware and applications, the programs that allow users to use the network. In understanding how these components work together, it is useful to look at the basic connectivity of the wide area network and contrast that to the way computers access the wide area network.

Wide area networks. A wide area network is one that generally covers a large geographic area and in which each pair of computers connect via a single line. The first wide area networks consisted of a number of connected mainframes with attached terminals. By connecting the mainframes, a user on one system could access applications on every networked computer. IBM developed the Systems Network Architecture (SNA), which was a popular early wide area network in the United States. The X.25 packet switching protocol standard provided a common architecture for the early wide area networks in Europe. Later, as all computers provided support for the TCP/IP protocol, it became possible for different computer networks to work together as a single network. In the twenty-first century, any device on a single network, whether attached as a terminal by X.25 or as a part of a local area network (LAN), can access applications and files on any other network on the internet. This complete connectivity allows browsers on any type of mobile device to access content over the World Wide Web (WWW), because it runs transparently over the internet.

Routing. A key to making the internet operate efficiently is the large number of intermediate devices that route IP packets from the computer making a

connection to the computer receiving the data. These devices are called routers, and they are the heart of the internet. When a message is sent from a computer, it is decomposed into IP packets, each having the IP address of the receiver. Then each packet is forwarded to a border router of the sender. From the border router, the packet is routed through a set of intermediate routers, using an algorithm-like best path, and delivered to the border router of the receiver, and then the receiver. Once all the packets have arrived, the message is reassembled and used by the receiver.

Local area networks. A local area network (LAN) is a collection of computers, servers, printers, and the like that are logically connected over a shared media. A media access control protocol operates over the LAN to allow any two devices to communicate at the link level as if they were directly connected. There are a number of LAN architectures, but Ethernet is the most popular LAN protocol for connecting workplace computers on a LAN to other networks. Ethernet is also usually the final step in connecting home computers to other networks using regular, cable, and asymmetric digital subscriber line (ADSL) modems. The original coaxial cable Ethernet, developed by Robert Metcalfe in 1973, has been largely supplanted by the less expensive and easier to use twisted-pair networks. The IEEE 802.11 wireless LAN is a wireless protocol that is almost as popular as Ethernet.

Wireless networks. A laptop computer's initial connection to a network is often through a wireless device. The most popular wireless network standard is the IEEE 802.11, which provides a reliable and secure connection to other networks by using an access point, a radio transmitter/receiver that usually includes border-routing capabilities. The Bluetooth network is another wireless network that is often used for peer-to-peer connection of cameras and cell phones to a computer and then through the computer to other networks. Cell

phones also provide network connectivity of computing devices to other networks.

APPLICATIONS AND PRODUCTS

Computer networks have many applications. Some improve the operation of networks, while others provide services to people who use the network. The WWW supplies many exciting new applications, and technologies such as teleconferencing and cloud computing have revolutionized computing. The adoption of such technologies was spurred on by the COVID-19 pandemic, during which many workers and schoolchildren relied on these technologies from their homes.

Network infrastructure. Computer networks are complex, and many applications have been developed to improve their operation and management. A typical example of the software developed to manage networks is Cisco's Internetwork Operating System (IOS) software, an operating system for routers that also provides full support for the routing functions.

Communications and social networking. Communications programs are among the most popular computer applications in use. Early file-sharing applications, such as FTP, retain their popularity, and later protocols such as BitTorrent, which enables peer-to-peer sharing of very large files, and file hosting services such as Dropbox, which provides cloud storage and online backup services, are widely used. Teleconferencing through platforms such as Zoom is used to create virtual workplaces, and voice over internet protocol (VoIP) allows businesses and home users to use the internet for digital telephone service.

The earliest computer network communications application, email, is still the largest and most successful network application. One accesses email services through an email client. The client can be a stand-alone program, such as Microsoft Outlook, or it can be web-based (webmail), accessed using a

browser such as Safari, Microsoft Edge, or Google Chrome. The email server can be a proprietary system such as HCL Notes or one of the many webmail programs, such as Gmail, Outlook.com, or Yahoo! Mail.

One of the most important types of applications for computer networks is social networking sites. Facebook was by far the most widely used online social network of the early 2020s, claiming more than 2.9 billion monthly active users as of April 2023, although services such as X (previously Twitter), TikTok, and YouTube were also very popular. Facebook was conceived by Mark Zuckerberg in 2004 while he was still a student at Harvard University. Facebook members can set up a profile that they can share with other members. The site supports a message service, event scheduling service, and news feed. By setting up a “friend” relationship with other members, one can quickly rekindle old friendships and gain new acquaintances. Although Zuckerberg’s initial goal was to create an interactive environment for individuals, Facebook has fast become a way to promote businesses, organizations, and even politicians. Facebook does not charge a subscription fee and has a business model based on selling customer information and advertising as well as working with partners. Facebook’s parent company, Meta, also owns several other social media services, including Instagram and WhatsApp, which each boasted about 2 billion monthly active users as of April 2023.

Cloud computing. Cloud computing refers to the hosting of data and applications on remote servers and networks (“the cloud”) instead of on local computers. Among other things, this makes the data and software services accessible from multiple locations, such as both home and office computers, as well as from mobile devices. This has benefits for data accessibility as well as businesses’ approach to their technology needs, as cloud computing essentially allows them to outsource some of their information

technology (both hardware and software) for an ongoing service fee rather than up-front capital costs. For individuals, it allows ready access to one's files and programs anywhere one has access to the internet. Platforms include Microsoft Azure, Amazon Web Services, and Google Cloud, among others. Communication services such as Slack and Microsoft Teams are further examples of cloud computing that gained popularity among businesses during the COVID-19 pandemic.

Next to email, the most common application is word processing, and Microsoft Word is the dominant word processor. Microsoft offers online versions of Word and its other Microsoft Office software through a service called Microsoft 365. Google offers similar cloud-based services, such as Google Workspace. As more and more applications are produced to run in the cloud, it is predicted that this will become the dominant form of computing, replacing the desktop computers of the early twenty-first century.

CAREERS AND COURSEWORK

A major in computer science is the traditional way to prepare for a computer networking job. Students first need courses in ethics, mathematics, and physics to form the basis for a computer science degree. Then they take courses in computer hardware and software. Those getting a computer science degree often take jobs developing network software or managing a network.

A major in information systems is another way to prepare for a computer networking job. Students must take courses in mathematics and business as a background for this degree in addition to courses on information systems development. Those getting degrees in computer information systems often take jobs as network managers, especially in small businesses.

In addition to the traditional academic programs that prepare someone for a computer networking job,

a large number of professional training programs result in certification. Novell was the first company to develop a certification program for its NetWare network operating system. The Cisco Certified Network Professional (CCNP) program is a large certification program that covers a variety of topics related to networking, including network design.

SOCIAL CONTEXT AND FUTURE PROSPECTS

The development of computer networks and network applications has often resulted in some challenging legal issues. File exchange programs are very popular but can have real copyright issues. Napster developed a successful peer-to-peer file exchange program but was forced to close after only two years of operation by a court decision in 2001. Legislation has played an important role in the development of computer networks in the United States. The initial deregulation of the communications system and the breakup of AT&T in 1982 reduced the cost of the base communications system for computer networks and thus greatly increased the number of networks in operation. Opening up the National Science Foundation Network (NSFNET) for commercial use in 1991 made the internet possible.

Networking and access to the web have been increasingly important to business development and improved social networking. The emergence of cloud computing as an easy way to do computing has been just as transformative, especially as evidenced during the COVID-19 pandemic that began in 2020. Although there are still security and privacy issues to be solved, people are increasingly using mobile devices to access a wide variety of web services through the cloud. Using just a smartphone, people are able to communicate with friends and associates, transact business, compose letters, pay bills, read books, and watch films.

—George M. Whitson III

Further Reading

- Comer, Douglas. *Computer Networks and Internets*. Pearson, 2015.
- _____. *The Internet Book: Everything You Need to Know about Computer Networking and How the Internet Works*. 5th ed., Chapman and Hall/CRC, 2018.
- Dordal, Peter L. "An Introduction to Computer Networks." *Loyola University Chicago*, 2015, intronetworks.cs.luc.edu/current/html.
- Easttom, Chuck. *Computer Security Fundamentals*. 5th ed., Pearson, 2023.
- FitzGerald, Jerry, Alan Dennis, and Alexandra Durcikova. *Business Data Communications and Networking*. 14th ed., Wiley, 2020.
- Forouzan, Behrouz. *Data Communications and Networking*. 5th ed., McGraw-Hill, 2013.
- "Global Social Media Statistics." *Datareportal*, Apr. 2023, datareportal.com/social-media-users.
- Griffith, Eric. "What Is Cloud Computing?" *PCMag*, 15 Feb. 2022, www.pcmag.com/news/what-is-cloud-computing.
- O'Leary, Mike. *Cyber Operations: Building, Defending, and Attacking Modern Computer Networks*. 2nd ed., Apress, 2019.
- O'Leary, Timothy, Linda O'Leary, and Daniel O'Leary. *Computing Essentials 2023*. McGraw-Hill, 2022.
- Stallings, William. *Data and Computer Communications*. 10th ed., Prentice Hall, 2014.

COMPUTER PROGRAMMER

ABSTRACT

Computer programmers write code and scripts that enable computer programs to function. They work in collaboration with software developers and engineers. Students aspiring to enter the profession should pursue studies in subjects such as computer science, coding, and mathematics.

BACKGROUND

Computer programmers write, modify, and test code and scripts that allow computer software and applications to function properly. They turn the designs created by software developers and engineers into instructions that a computer can follow.

In addition, programmers run tests to ensure that newly created applications and software produce the expected results. If the products do not work correctly, programmers check the code or scripts for mistakes and modify them. This work can be exceedingly complex, depending on the nature of the program being written, and programmers must work to ensure that their code does not contain vulnerabilities that could be exploited by malicious individuals or groups.

OVERVIEW

Computer programmers work in office settings, which may include working from home.

Computer programmers are analytical and methodical by nature and do not mind spending many hours in front of their computers, working on writing or tweaking lines of code. Moreover, they take great satisfaction in applying their knowledge of computer languages to writing programs that serve real-world functions, in many cases vital functions that factor into numerous sectors of society.

DUTIES AND RESPONSIBILITIES

Programmers work closely with software developers, and in some businesses their duties overlap. When such overlap occurs, programmers may be required to take on some of the tasks that are typically assigned to developers, such as designing programs.

Programmers use code libraries, which are collections of independent lines of code, to simplify their writing and improve their efficiency. They may create their own code libraries or make use of existing ones.

In addition, programmers may write or use software-as-a-service (SaaS) applications that are centrally hosted online. Although programmers typically need to rewrite their programs to work on different system platforms, such as Windows or macOS, applications created with SaaS work on all platforms. Accordingly, programmers writing SaaS

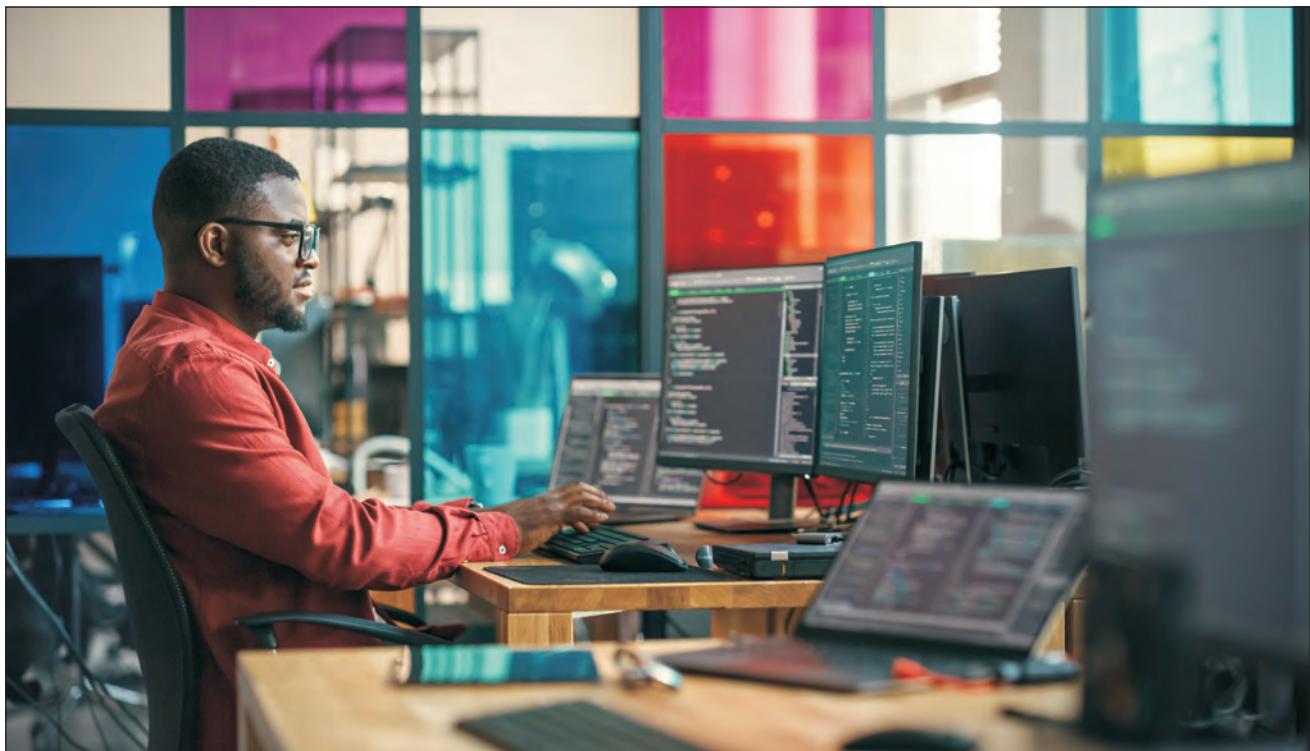


Photo via iStock/gorodenkoff. [Used under license.]

applications may not have to rewrite as much code as other programmers do and can instead spend more time writing new programs.

Some programmers may specialize in highly advanced and complex programming, such as that associated with artificial intelligence (AI) systems. In fact, and in detriment to the programming profession, some AI can now write its own computer code.

WORK ENVIRONMENT

Physical environment. Computer programmers typically work in an office setting, whether in a traditional office or at home. Regardless of the setting, they must be conscious of the health risks associated with prolonged sitting and computer use: namely, lack of exercise and strain to eyes and hands. Most computer programmers work full-time.

Human environment. Computer programmers may lead solitary work-lives, depending on their setting

and the nature of the projects on which they work. More likely, however, they will need to liaise with other programmers, software developers, and engineers in the creation of a program or product. They must be able to take direction from senior programmers and project leads and implement those ideas in practical terms.

Technological environment. Computer programmers must be especially tech-savvy in order to perform their duties and stay on top of evolving trends. Intimate knowledge of one or more computer languages is essential, as is the ability to work with databases, development environment software, object or component-oriented development software, web development software, and other applications such as common word processors and presentation software. Depending on the nature of the project, programmers may be required to utilize advanced and highly complex programming methods.

EDUCATION AND TRAINING

High school/secondary. High school students interested in programming as a career should take computer science-related courses and expand their knowledge in their spare time at home. The internet offers a wealth of resources about all aspects of coding and computer languages, so students should have no trouble finding this information at their fingertips and can develop coding skills early. Interest in this subject may lead to programming as a hobby, which will serve the student well in their future career.

College/postsecondary. Computer programmers typically need a bachelor's degree in computer and information technology or a related field, such as mathematics. However, some employers hire workers who have other degrees or experience in specific programming languages. Programmers who work in specific fields, such as healthcare or accounting, may take classes in that field to supplement their computer-related degree. In addition, employers may prefer to hire candidates who have experience gained through internships.

Most programmers learn computer languages while in school. However, a computer science degree gives students the skills they need to learn new computer languages easily. Students get experience writing code, testing programs, fixing errors, and doing many other tasks that they will perform on the job.

Adult job seekers. If an adult job seeker with no prior experience in computer programming or similar fields wishes to pursue such a career, they should enroll in a college that offers a program to expand their skills. Adults with some programming experience, even on a hobby basis, should still find out what skills are necessary for the type of programming they wish to do on a career basis, and obtain the relevant education.

To keep up with changing technology, computer programmers may take continuing education classes and attend professional development seminars to

learn new programming languages or about upgrades to programming languages they already know.

Professional certification and licensure. Programmers may become certified in specific programming languages or for vendor-specific programming products. Some companies require their computer programmers to be certified in the products they use.

—Stuart Paterson

FURTHER READING

- Easttom, Chuck. *Computer Security Fundamentals*. 5th ed., Pearson, 2023.
Petzold, Charles. *Code: The Hidden Language of Computer Hardware and Software*. 2nd ed., Microsoft Press, 2022.
Wassberg, Joakim. *Computer Programming for Absolute Beginners*. Packt, 2020.

COMPUTER SECURITY

ABSTRACT

The field of computer security encompasses hardware security, network security, and software security, each of which is essential to ensuring the security of computer systems and the data contained within. Computer security professionals work to identify and address vulnerabilities in the systems for which they are responsible.

BACKGROUND

Computer security professionals have an unenviable task. They must interfere with the way users wish to use their computers, to make sure that hardware and software vulnerabilities are avoided as much as possible. Often, the same users whom they are trying to protect attempt to circumvent those protective measures, finding them inconvenient or downright burdensome. Computer security in these cases can become a balancing act between safety and functionality.

OVERVIEW

Hardware security. The first line of defense in the field of computer security concerns the computer hardware itself. At a basic level, computer hardware must be stored in secure locations where it can only be accessed by authorized personnel. Thus, in many organizations, access to areas containing employee workstations is restricted. It may require a badge or other identification to gain access. Sensitive equipment such as an enterprise server is even less accessible, locked away in a climate-controlled vault. It is also possible to add hardware security measures to existing computer systems to make them more secure. One example of this is using biometric devices, such as fingerprint scanners, as part of the user login. The computer will only allow logins from people whose fingerprints are authorized. Similar restrictions can be linked to voice authentication, retina scans, and other types of biometrics.

Inside a computer, a special type of processor based on a trusted platform module (TPM) can manage encrypted connections between devices. This ensures that even if one device is compromised, the whole system may still be protected. Another type of security, device fingerprinting, can make it possible to identify which device or application was used to access a system. For example, if a coffee shop's wireless access point was attacked, the access point's logs could be examined to find the machine address of the device used to launch the attack. One highly sophisticated piece of security hardware is an intrusion detection system. These systems can take different forms but generally consist of a device through which all traffic into and out of a network or host is filtered and analyzed. The intrusion detection system examines the flow of data to pinpoint any attempt at hacking into the network. The system can then block the attack before it can cause any damage.

Network security. Network security is another important aspect of computer security. In theory,

any computer connected to the internet is vulnerable to attack. Attackers can try to break into systems by exploiting weak points in the software's design or by tricking users into giving away their usernames and passwords. The latter method is called phishing, because it involves "fishing" for information. Both methods can be time consuming, however. So once a hacker gains access, they may install a backdoor. Backdoors allow easy, undetected access to a system in future.

Computer security can come in many forms to ensure data and programs are protected. Passwords limit who can access a computer, key encryption limits who can read transmitted data, and firewalls can limit intrusion from the internet.

One way of preventing attackers from tricking authorized users into granting access is to follow the principle of least privilege. According to this principle, user accounts are given the minimum amount of access rights required for each user to perform their duties. For instance, a receptionist's account would be limited to email, scheduling, and switchboard functions. This way, a hacker who acquired the receptionist's username and password could not do things such as set their own salary or transfer company assets to their own bank account. Keeping privileges contained thus allows an organization to minimize the damage an intruder may try to inflict.

Software security. Software represents another vulnerable point of computer systems. This is because software running on a computer must be granted certain access privileges to function. If the software is not written in a secure fashion, then hackers may be able to enhance the software's privileges. Hackers can then use these enhanced privileges to perform unintended functions or even take over the computer running the software. In the vernacular of hackers, this is known as "owning" a system.

—Scott Zimmer

Further Reading

- Boyle, Randall, and Raymond R. Panko. *Corporate Computer Security*. 5th ed., Pearson, 2020.
- Brooks, R. R. *Introduction to Computer and Network Security: Navigating Shades of Gray*. CRC, 2014.
- Easttom, Chuck. *Computer Security Fundamentals*. 5th ed., Pearson, 2023.
- Jacobson, Douglas, and Joseph Idziorek. *Computer Security Literacy: Staying Safe in a Digital World*. CRC, 2013.
- Kizza, Joseph Miggia. *Guide to Computer Network Security*. 6th ed., Springer, 2024.
- Schou, Corey, and Steven Hernandez. *Information Assurance Handbook: Effective Computer Security and Risk Management Strategies*. McGraw, 2015.
- Vacca, John R. *Computer and Information Security Handbook*. Kaufmann, 2013.
- Williams, Richard N. *Internet Security Made Easy: Take Control of Your Computer*. Flame Tree, 2015.

COMPUTER SOFTWARE

ABSTRACT

Computer software refers to one or more programs that determine how a computer operates. Software works along with a computer's hardware, or physical parts, to make the computer function efficiently for various tasks. There are two main kinds of computer software: system software and application software. System software is mainly used by the computer to help its parts communicate and cooperate.

Application software is generally added to allow humans to perform specific tasks with the computer. Together, these kinds of software make computers valuable machines for work and entertainment alike.

BACKGROUND

Computers are electronic machines that can accept and interpret different forms of data and perform various operations using the data. People use computers for a great variety of purposes ranging from complex scientific research to entertainment. After several generations of development, computers have taken on a wide range of forms in the modern

world. People today may use large computers on desktops or smaller laptop computers. Notebook computers and relatively tiny mobile versions become more popular each year, and embedded computers are critical parts of most automobiles and many appliances.

Despite the great variety in modern computers, they share some important similarities. One of the main similar features of all computers is that they use hardware and software. Hardware refers to the physical parts of a computer. These parts include easily identifiable external features such as the central processing unit (CPU), keyboard, and mouse or touchpad. They also include smaller, internal features such as hard disks, or devices that allow the computer to store and access information. Hardware is important because it creates a basis upon which people may add software that will make the computer perform specific tasks.

OVERVIEW

Computer software is a much broader category than computer hardware. Software refers to all the programs that manufacturers or users may install on a computer. Software may be used by the computer, by the user, or by both to organize and use files and other data for specific tasks.

The most important software on a computer, and the first program that should be installed, is called the operating system (OS). The OS serves as a wide-reaching interface, or a digital workstation through which users can install, organize, and operate other, smaller programs. It also helps the computer share its memory and other resources among its various tasks, handle input and output functions, and store new data.

For most computer users, the OS is the first thing visible once the computer loads after it is turned on. Microsoft Windows is one of the most common OS in use, but some types of computers and computer hardware may work better with other OSs. Some of

the main competitors to Windows include macOS, ChromeOS, iOS, Linux, and Android.

Although the OS is the most important software, there are dozens of other kinds of software available to modern computer users for both personal and professional tasks. This software can generally be divided into two main categories based on their types: the work they do, and the fields in which they are most commonly used. These main categories are system software and application software.

SYSTEM SOFTWARE

System software includes any kind of program that controls other programs or the computer's systems. These programs are meant to function closely with the hardware and are useful for making the computer and all of its other programs run more efficiently. The OS is one prime example of system software. Another important example is a compiler, a program that translates the codes, or computer "language," used by the programs and hardware.

Other types of system software include programming tools such as loaders, linkers, and assemblers, which also gather and translate data. There are also drivers, or programs that assist hardware in performing its necessary tasks. All of these kinds of system software help the various features of a computer communicate and cooperate. Some also allow users to diagnose and solve problems with, or maximize the efficiency of, the computer or its programs.

APPLICATION SOFTWARE

The other main category of software is application software. Whereas system software is mostly used to help the computer function properly, application software is generally more focused on the needs of the user. This category includes all programs that are added to a computer to perform tasks for people using the computer. These tasks can be for

productivity, for fun, or both, and may be general in nature or meant for specific goals.

Hundreds of examples of application software are available to computer users, each designed to meet specific user needs. Most of this software falls into broad categories. For instance, multimedia software lets computer users view, listen to, or even create visual and audio files. Spreadsheet and database software helps users store, sort, and analyze large amounts of information. Word processing software lets users create various kinds of documents, and presentation software helps users display their creations for others. Internet browsers, gaming programs, and communication tools are also popular types of application software.

—Mark Dziak

Further Reading

- Campbell-Kelly, Martin, William F. Aspray, Jeffrey R. Yost, Honghong Tinn, and Gerardo Con Díaz. *Computer: A History of the Information Machine*. 4th ed., Routledge, 2023.
- "Different Types of Software." *Introduction to IT English*, web2.uvcs.uvic.ca/elc/sample/ite/u01/u1_1_03.html.
- Easttom, Chuck. *Computer Security Fundamentals*. 5th ed., Pearson, 2023.
- O'Leary, Timothy, Linda O'Leary, and Daniel O'Leary. *Computing Essentials 2023*. McGraw-Hill, 2022.
- Patterson, David A., and John L. Hennessy. *Computer Organization and Design: The Hardware/Software Interface*. 6th ed., Morgan Kaufmann, 2020.
- Rosencrance, Linda. "Software." *Tech Target*, Mar. 2021, www.techtarget.com/searchapparchitecture/definition/software.

COMPUTER VIRUSES AND WORMS

ABSTRACT

Computer viruses and worms are malicious computer programs, also known as malware, that use embedded instructions to carry out destructive behavior on computers, computer networks, and digital devices.

BACKGROUND

Computer viruses and worms have the potential to disrupt computer networks and thus to cause great damage to a nation's economy. The US Department of Justice has devoted significant resources to investigating and prosecuting persons who release viruses or worms on the internet. In addition, government agencies investigate connections between malware and organized crime, identity theft, and terrorism.

Given the capacity of computer viruses and worms to spread to millions of computers within minutes and cause billions of dollars in damage, the distribution of malware is a criminal act. In the United States, causing damage to a computer connected to the internet is a federal crime that carries substantial penalties for those convicted. The principal US law enforcement weapon against malware is the Computer Fraud and Abuse Act of 1984.

Many dangerous computer viruses have been spread through email attachments and files downloaded from websites, and a rise has been seen in the numbers of professional virus writers—that is, people who are paid to infect computers with malware.

OVERVIEW

Tracking down and catching virus authors is extremely difficult. The investigative methods used in this work include analyzing virus code for clues about the authors; searching online forums or social media platforms where virus authors may boast of their accomplishments; and reviewing network log files for originating internet protocol (IP) addresses of viruses. Even when law enforcement agencies make concerted efforts in applying these techniques, it is still extremely difficult to track down virus and worm authors.



Photo via iStock/Arkadiusz Wargu?a. [Used under license.]

Some malware authors have been apprehended, however. When the Melissa virus overwhelmed commercial, government, and military computer systems in 1999, the Federal Bureau of Investigation (FBI) launched a large-scale internet manhunt. Investigators succeeded in tracking down the virus creator by following several evidence trails. They identified David L. Smith of Aberdeen, New Jersey, as the suspect by analyzing the virus and the email account used to send it, by searching America Online (AOL) log files that showed whose phone line had been used to send the virus, and by searching online bulletin boards intended for people interested in learning how to write viruses. Smith tried to hide the electronic evidence related to Melissa by deleting files from his computer and then disposing of it. The FBI found the computer, however, and used computer forensics techniques to recover incriminating evidence. Smith was caught within two weeks. He was the first person prosecuted for spreading a computer virus.

In August 2005, Turkish and Moroccan hackers released an internet worm named Zotob to steal credit card numbers and other financial information from infected computers. Zotob crashed innumerable computer systems worldwide. Investigators gathered data, including IP addresses, email addresses, names linked to those addresses, hacker nicknames, and other clues uncovered in the computer code. Less than eight days after the malicious code hit the internet, two suspects were arrested. Computer forensic experts on the FBI's Cyber Action Team (CAT) verified that the code found on seized computers matched what was released into cyberspace.

Government responses to hacking became more intense following several high-profile computer security breaches targeting government servers in the 2010s. In 2014, the US government charged five Chinese military hackers working for the Chinese military's Unit 61398 for cyberespionage against American corporations, which was undertaken to

gain a competitive advantage. The indictment marked the first time criminal charges were filed against known state actors for hacking. In 2015, the Chinese military's Unit 61398 was again implicated in cyberattacks against the Australian Bureau of Meteorology, in which hundreds of terabytes of data were stolen. In 2016, the US Central Intelligence Agency (CIA) reported that the Russian government was behind a hack of the Democratic National Convention in which nearly 20,000 emails were stolen and leaked. The CIA told US legislators that the agency had concluded Russia carried out the hack with the aim of influencing the 2016 US presidential election. The following year, the WannaCry virus took computer files hostage in 150 countries, and in 2020, the US medical field experienced its largest ransomware attack, stalling surgeries and procedures. As such incidents become more common, the targets more prominent, and the stakes higher, computer forensics techniques will need to become ever more advanced to prevent attacks and prosecute the creators of computer viruses and other malicious programs.

—Linda Volonino

Further Reading

- Dwight, Ken. *Bug-Free Computing: Stop Viruses, Squash Worms, and Smash Trojan Horses*. TeleProcessors, 2006.
- Entous, Adam, Ellen Nakashima, and Greg Miller. "Secret CIA Assessment Says Russia Was Trying to Help Trump Win White House." *Washington Post*, 9 Dec. 2016, www.washingtonpost.com/world/national-security/obama-orders-review-of-russian-hacking-during-presidential-campaign/2016/12/09/31d6b300-be2a-11e6-94ac-3d324840106c_story.html.
- Erbschloe, Michael. *Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code*. Butterworth-Heinemann, 2005.
- Maras, Marie-Helen. *Computer Forensics: Cybercriminals, Laws and Evidence*. Jones & Bartlett Learning, 2015.
- Stewart, Andrew J. *A Vulnerable System: The History of Information Security in the Computer Age*. Cornell UP, 2021.

“U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage.” US Department of Justice, 19 May 2014, www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

Watters, Paul A. *Cybercrime and Cybersecurity*. CRC Press, 2023.

CRYPTOGRAPHY

ABSTRACT

Early cryptography focused on ensuring that written messages could be sent to their intended recipients without being intercepted and read by other parties. This was achieved through various encryption techniques. Encryption is based on a simple principle: the message is transformed in such a way that it becomes unreadable. The encrypted message is then transmitted to the recipient, who reads it by transforming (decrypting) it back into its original form. The development of modern computer systems in the 1950s changed the world of cryptography in major ways, and further technological advancements rendered cryptography increasingly essential to business, government, and society throughout the late twentieth and early twenty-first centuries.

BACKGROUND

The word “cryptography” comes from the Greek words *kryptos* (“hidden,” “secret”) and *graphein* (“writing”). Early forms of encryption were based on ciphers. A cipher encrypts a message by altering the characters that comprise the message. The original message is called the “plaintext,” while the encrypted message is the “ciphertext.” Anyone who knows the rules of the cipher can decrypt the ciphertext, but it remains unreadable to anyone else.

Among the earliest ciphers used were the transposition cipher and the substitution cipher. A transposition cipher encrypts messages by changing the order of the letters in the message using a

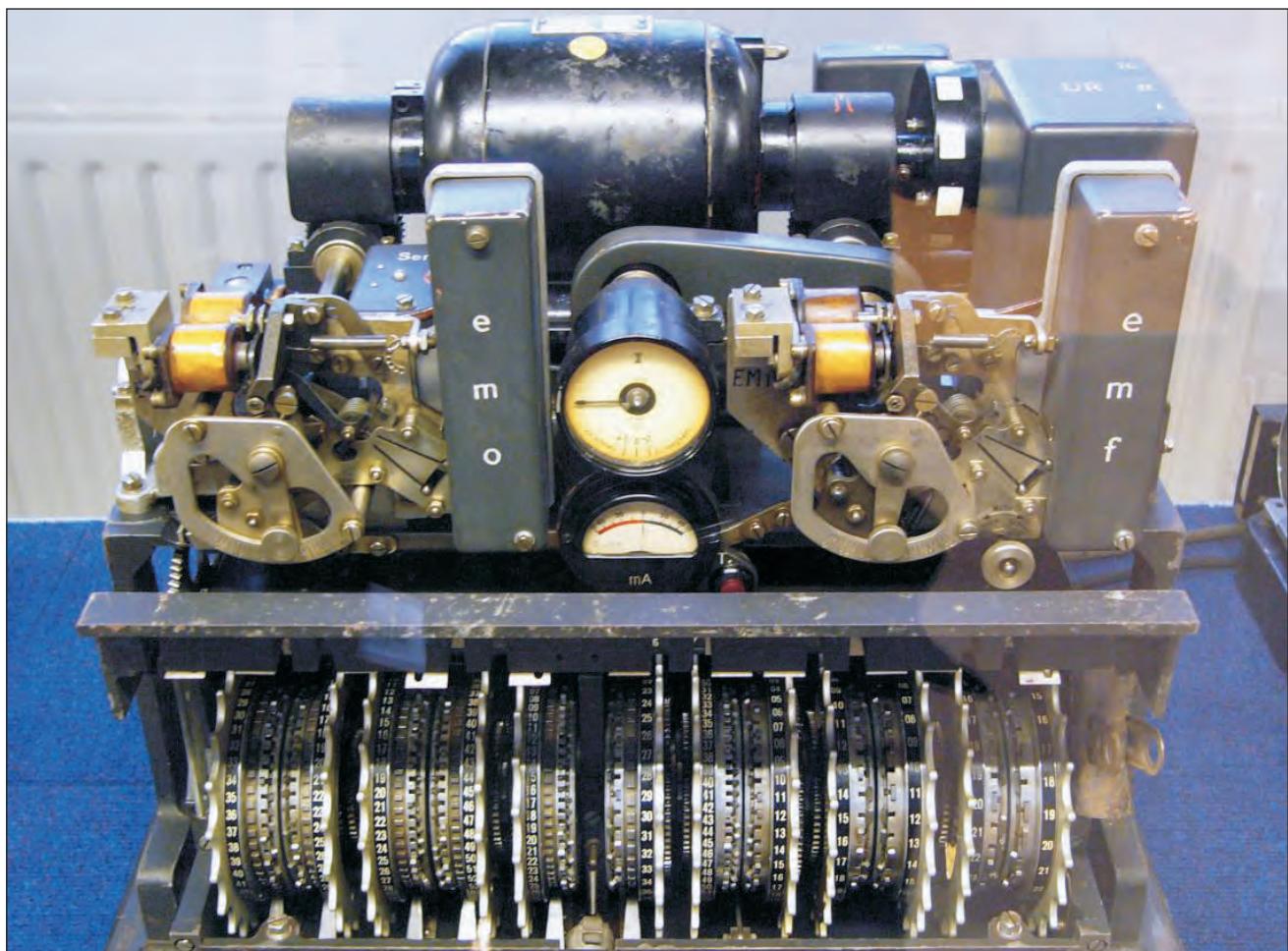
well-defined scheme. One of the simplest transposition ciphers involves reversing the order of letters in each word. When encrypted in this fashion, the message “MEET ME IN THE PARK” becomes “TEEM EM NI EHT KRAP.” More complicated transposition ciphers might involve writing out the message in a particular orientation (such as in stacked rows) and then reading the individual letters in a different orientation (such as successive columns).

A substitution cipher encodes messages by substituting certain letters in the message for other letters. One well-known early substitution cipher is the Caesar cipher, named after Julius Caesar. This cipher encodes messages by replacing each letter with a letter that is a specified number of positions to its right or left in the alphabet. For example, Caesar is reported to have used a left shift of three places when encrypting his messages.

Early ciphers were relatively easy to break, given enough time and a working knowledge of statistics. By the 1920s, electromechanical cipher machines called “rotor machines” were creating complex ciphers that posed a greater challenge. The best-known example of a rotor machine was the Enigma machine, used by the German military in World War II. Soon after, the development of modern computer systems in the 1950s would change the world of cryptography in major ways.

OVERVIEW

With the introduction of digital computers, the focus of cryptography shifted from just written language to any data that could be expressed in binary format. The encryption of binary data is accomplished through the use of keys. A key is a string of data that determines the output of a cryptographic algorithm. While there are many different types of cryptographic algorithms, they are usually divided into two categories. Symmetric-key cryptography uses a single key to both encrypt and decrypt the data. Public-key cryptography, also called “asymmetric-key



Lorenz cipher machine, used in World War II to encrypt communications of the German High Command.

cryptography,” uses two keys, one public and one private. Usually, the public key is used to encrypt the data, and the private key is used to decrypt it.

When using symmetric-key cryptography, both the sender and the recipient of the encrypted message must have access to the same key. This key must be exchanged between parties using a secure channel, or else it may be compromised. Public-key cryptography does not require such an exchange. This is one reason that public-key cryptography is considered more secure.

Another cryptographic technique developed for use with computers is the digital signature. A

digital signature is used to confirm the identity of the sender of a digital message and to ensure that no one has tampered with its contents. Digital signatures use public-key encryption. First, a hash function is used to compute a unique value based on the data contained in the message. This unique value is called a “message digest,” or just “digest.” The signer’s private key is then used to encrypt the digest. The combination of the digest and the private key creates the signature. To verify the digital signature, the recipient uses the signer’s public key to decrypt the digest. The same hash function is then applied to the data in the

message. If the new digest matches the decrypted digest, the message is intact.

WHY IS CRYPTOGRAPHY IMPORTANT?

The ability to secure communications against interception and decryption has long been an important part of military and international affairs. In the modern age, the development of new computer-based methods of encryption has had a major impact on many areas of society, including law enforcement, international affairs, military strategy, business, and media. It has also led to widespread debate over how to balance the privacy rights of organizations and individuals with the needs of law enforcement and government agencies. Businesses, governments, and consumers must deal with the challenges of securing digital communications for commerce and banking on a daily basis. The impact of cryptography on society is likely to increase as computers grow more powerful, cryptographic techniques improve, and digital technologies become ever more important.

—Maura Valentino

Further Reading

- Hoffstein, Jeffrey, Jill Pipher, and Joseph H. Silverman. *An Introduction to Mathematical Cryptography*. 2nd ed., Springer, 2014.
- “How Cryptography and Web3 Can Help Restore Trust in Digital Media.” *Stanford Engineering*, 17 June 2022, engineering.stanford.edu/magazine/how-cryptography-and-web3-can-help-restore-trust-digital-media.
- Katz, Jonathan, and Yehuda Lindell. *Introduction to Modern Cryptography*. 3rd ed., Chapman and Hall, 2020.
- Menezes, Alfred J., Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.
- Niederreiter, Harald, and Chaoping Xing. *Algebraic Geometry in Coding Theory and Cryptography*. Princeton UP, 2009.
- Paar, Christof, Jan Pelzl, and Tim Güneysu. *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer Cham, 2023.

CYBER COMMAND

ABSTRACT

In 2009, Defense Secretary Robert Gates announced plans to organize a new “subcommand” in the US Department of Defense to deal with the emerging threat of cyberwarfare. The formation of the US Cyber Command (USCYBERCOM) reflected growing concern within the Pentagon about “probes” of military computer networks, which were of increasing importance in conducting high-tech warfare. Cyber Command became a unified combatant command in 2018.

BACKGROUND

The Cyber Command was first proposed by US Defense Secretary Robert Gates in June 2009 with two purposes: to consolidate and coordinate cyberwar plans and to build more effective American responses—both defensive and offensive—in the developing area of cyberwarfare. The US Cyber Command was put under the Strategic Command. The missions of the Strategic Command are:

to deter attacks on U.S. vital interests, to ensure U.S. freedom of action in space and cyberspace, to deliver integrated kinetic and non-kinetic effects to include nuclear and information operations in support of U.S. Joint Force Commander operations, to synchronize global missile defense plans and operations, to synchronize regional combating of weapons of mass destruction plans, to provide integrated surveillance and reconnaissance allocation recommendations to the [Secretary of Defense], and to advocate for capabilities as assigned.

After prolonged discussion, Gates ordered that the Cyber Command would be headquartered at Ft. Meade, Maryland, home of the National Security Agency (NSA), with which it would share a

commander. However, Cyber Command's top general would report to the Strategic Command, part of the Air Force, based in Omaha, Nebraska. The newly organized Cyber Command was to be a subcommand within the Strategic Command. Commands and subcommands are part of the "unified command" structure first established after World War II. These commands cut across the traditional military divisions to coordinate the nation's response to threats or attacks. Commands may be organized geographically, as in the case of the Northern Command (homeland defense) and Pacific Command (Asia and the Pacific), or they may be functional, as in the case of Transportation Command and Strategic Command (nuclear deterrence and offense and, more recently, cyberwarfare).

Gates nominated Army Lt. General Keith B. Alexander to be in charge of the Cyber Command. Alexander was already in charge of the NSA, and if confirmed would play a dual role in both the NSA and the Cyber Command. The activities of the Cyber Command and of the NSA in some respects overlap. The NSA is in charge of acquiring intelligence by monitoring communications, both by telephone and computer networks, and is believed to have developed sophisticated computer systems for scanning huge numbers of messages in search of communications that might relate to possible terrorist attacks, as well as military communications. Hearings on Alexander's nomination were held in mid-April 2010, and he was confirmed as commander of the Cyber Command and promoted to the rank of general the following month. The Cyber Command began operations shortly thereafter.

OVERVIEW

At the time of its establishment, the primary realm of the Cyber Command, also known as USCYBERCOM, was intended to be military electronic networks in an era when the military increasingly depends on high-speed computer systems for

command and control of both battlefield and strategic systems. At his confirmation hearing in April 2010, Alexander told senators: "This [command] is not about efforts to militarize cyberspace. Rather it's about safeguarding the integrity of our military system. My goal if confirmed will be to significantly improve the way we defend ourselves in this domain." He also said that the Cyber Command would develop offensive capabilities in case of a "cyberwar."

Cyberwarfare refers not only to attacks on military computer networks but also civilian systems, including financial networks, energy grids, and transportation systems. Establishment of the Cyber Command came at a time of frequent reports of hacking into civilian and government computer networks. The Cyber Command was not the only agency charged with defending the nation against computer networks from attack at that time. The two main tasks of the Department of Homeland Security's National Cyber Security Division (NCSD) were "to build and maintain an effective national cyberspace response



Seal of the United States Cyber Command. Image via Wikimedia Commons. [Public domain.]

system” and “to implement a cyber-risk management program for protection of critical infrastructure.”

LATER DEVELOPMENTS

Establishment of the Cyber Command represented formal recognition by the Pentagon of the importance of networked computers in running military operations, both by the United States and by its prospective enemies, as well as evidence that the threat of such attacks is increasing.

In April 2010 General Alexander told senators that there were hundreds of thousands of probes of defense networks every day, evidently aimed at discovering vulnerabilities in the network. “We have been alarmed by the increase, especially this year. It’s growing rapidly.”

Unlike traditional military warfare, which typically involves large-scale, expensive munitions systems designed to go up against similar systems mounted by other governments, cyberwarfare blurs the distinction between military and civilian targets. For example, attacks on financial or communications networks could immobilize or seriously damage a national economy without a shot ever being fired.

Tracking the origins of such attacks is often difficult. Published reports have said China and Russia in particular are frequent sources of hacker intrusions. The nature of these probes or attacks underscores another distinction between traditional warfare and cyberwarfare—the blurring of the distinction between official versus nonofficial and military versus civilian attackers. Hacker intrusions are sometimes routed through innocent third-party computers or servers, making it difficult or impossible to trace them back to the country of origin. Individuals launching such attacks may be acting at the behest of a government agency, or simply individuals equipped with nothing more than a personal computer and access to the internet. The fact that such hacker probes and attacks can be routed

through third-party servers, including computers inside the United States, blurs another distinction between the purview of the Department of Homeland Security and entities such as the NSA or the Cyber Command.

Alexander remained commander of the Cyber Command and director of the NSA until 2014, when he retired and was succeeded in those roles by Admiral Michael S. Rogers. Rogers retired in 2018 and was succeeded by Paul M. Nakasone. Throughout its first decade of existence, the Cyber Command evolved to encompass a Cyber Mission Force made up of several specialized categories of teams, including National Mission Force and Cyber Protection teams. In 2018, the Cyber Command was named a unified combatant command, and in 2020, the command celebrated its tenth year of operation. In addition to carrying out its own work, the Cyber Command partnered with bodies such as the NSA’s Election Security Group, the Department of Defense, and the Army Cyber Command to protect the United States’ cyberinterests.

Further Reading

- “Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities.” *US Government Accountability Office*, 2005, www.gao.gov/new.items/d05434.pdf.
- Mills, James H. “Make Way for the Cyber Fleet!” *US Naval Institute Proceedings*, vol. 136, no. 1, 2010, www.usni.org/magazines/proceedings/2010/january/make-way-cyber-fleet.
- “Our History.” *US Cyber Command*, www.cybercom.mil/About/History.
- “Securing the Cyber Advantage: U.S. Cyber Command Celebrates Its 11th Year.” *US Cyber Command*, 21 May 2021, www.cybercom.mil/Media/News/Article/2626906/securing-the-cyber-advantage-us-cyber-command-celebrates-its-11th-year.
- Wright, Austin. “The Unseen Cyber-War: National Security Infrastructure Faces Relentless Cyberespionage Campaign.” *National Defense*, vol. 94, no. 673, 2009, pp. 28–32, www.jstor.org/stable/45370556.

CYBERBULLYING

ABSTRACT

The advent of any new communication technology has historically brought with it new forms of bullying. Newspapers presented bullying on a widespread basis via the printed word; telephones created prank calls; and the internet has presented an even quicker, broader form of harassment. Intimidation transpiring via the latest computer technologies is dubbed cyberbullying. Cyberbullying is especially prevalent on social networking websites and is most commonly experienced by young people.

BACKGROUND

The term “cyberbullying” was first used by educator Bill Belsey in 2004 in an essay detailing the emerging threat of harassment through the use of information and communication technologies. He described cyberbullying as a pervasive form of intentional harassment by a group or individual acting with hostility toward another person, aided by the internet’s invasive capabilities. The act of cyberbullying, however, was present long before it was given a name. When the internet became a significant source of connectivity near the close of the twentieth century, a new kind of rapport developed between people. Individuals communicating through a computer screen were able to behave and interact differently than they could or normally would face to face. Technology allowed for an anonymity that made bullying easier. Paired with the distancing effect many experienced through the use of such devices, bullying had the potential to be even more vicious than it would be in face-to-face situations.

As awareness of cyberbullying increased, researchers began surveying students about their personal experiences to learn more about the incidence of such harassment among American youth. Teenagers seemed to be the main demographic affected by cyberharassment. In 2000, the Crimes Against

Children Research Center interviewed 1,501 young people ages ten to seventeen. At that time, the survey found that one in seventeen children—about 6 percent—had experienced threats or harassment online. This number increased to 9 percent five years later and to 11 percent in 2011. Other studies supported these findings. In 2004, the internet safety education website i-Safe surveyed the same number of students between grades four and eight and found that 42 percent of students had been bullied online; 35 percent of those surveyed had been threatened and many said it had happened more than once.

OVERVIEW

Many researchers showed rising rates of cyberbullying through the 2010s, as internet access and portable electronic devices became increasingly common with young people. As part of its biannual nationwide Youth Risk Behavior Surveillance survey, the Centers for Disease Control and Prevention (CDC) reported that in 2017, 14.9 percent of high school students surveyed stated that they had been bullied electronically in the previous twelve months. Similarly, the National Center for Education Statistics reported in 2019 that during the 2016–17 school year, 15 percent of the 20 percent of students between the ages of twelve and eighteen who had reported being bullied had experienced this bullying online or by text; this marked an increase over the 2015–16 school year, during which time 11.5 percent of bullied students were bullied online or by text.

A Pew Research Center survey published in September 2018 found that 59 percent of US teens had experienced cyberbullying. The same survey revealed that the most common type of online harassment reported by American teens was name calling, with 42 percent of those surveyed saying they had experienced this type of bullying online or on their cell phone; another 32 percent reported



Photo via iStock/SolStock. [Used under license.]

that someone had spread false rumors about them online. Because of the anonymity provided by online platforms, there was a rise in hate speech used to cyberbully during the late 2010s.

In 2013, elevated concern over the possibly devastating effects of unchecked cyberbullying occurred following the suicides of at least seven teenagers in both the United States and the United Kingdom that were linked to incidents of bullying taking place on a largely unfamiliar social application, Ask.fm. The application, which did not have the privacy settings associated with popular social media sites such as Facebook, offered an open forum for questions and answers that allowed for anonymous bullying. However, even more prominent social media

platforms such as Instagram, Facebook, and Snapchat struggled to limit cyberbullying.

LEGAL AND INSTITUTIONAL RESPONSES

In late 2006, thirteen-year-old Megan Meier of Missouri committed suicide after a campaign of harassment over the internet. After an investigation, Meier's death was attributed to repeated cyberbullying via the then-popular social networking website Myspace. There were no laws against cyberbullying at the time, so the offenders—including an adult neighbor—were indicted on charges of "unauthorized access of a computer system with intent to harm another person." The case incited intense public outrage and prompted many states to take

legislative action against cyberbullying; soon, many had passed laws criminalizing it.

Inspired by the case, Congresswoman Linda Sanchez proposed a bill referred to as the Megan Meier Cyberbullying Prevention Act in an attempt to decrease such tragic incidents at the federal level. However, the bill largely stalled as several congressional members argued that the legislation would conflict with the constitutional right to free speech. According to the Cyberbullying Research Center, by early 2021, forty-eight US states had legislation and/or policies that specifically addressed cyberbullying. All fifty states and the District of Columbia had more general antibullying legislation in place.

Schools, too, began taking steps to prevent cyberbullying, and many instituted programs of awareness and established punishments for those found guilty. However, although most schools in the United States block social networking sites from school computers, not all have programs teaching students responsible internet use. Additionally, states that do have laws addressing cyberbullying and even school codes often do not include any insight into whether and how schools should intervene in such cases, or even clearly define cyberbullying. Principals are also often conflicted as to whether they have any power to discipline students if the cyberbullying is conducted outside of the school. Some states have statutes reflecting the fact that “federal case law allows schools to discipline students for off-campus behavior that results in a substantial disruption of the learning environment at school,” as per the Cyberbullying Research Center. Yet the application of such legislation can be unclear and sometimes controversial.

CAMPAIGNS AGAINST CYBERBULLYING

To increase understanding of the issue, many international organizations have dedicated themselves to bringing awareness to the problem of cyberbullying as well as preventing it. Founded in 2005, the

STOMP Out Bullying campaign helped over 100,000 students through their HelpChat Line and partnered with over 15,000 schools to raise awareness of cyberbullying by 2020. In 2007, the US-based National Crime Prevention Council created a public advertising campaign and initiated a contest that challenged entrants to create their own public service announcements. Stopbullying.gov, a US government website, provides information on cyberbullying and how to prevent and report it. The Cybersmile Foundation is an international nonprofit organization committed to reducing incidents of cyberbullying and helping victims of cyberbullying regain control of their lives. Several countries, such as Canada and Spain, have a national antibullying day in order to bring awareness to the problem.

People worldwide also use social networking websites to combat cyberbullying. For example, Sarah Ball, who was once cyberbullied, created a Facebook page called “Hernando Unbreakable” in order to help other victims. She earned attention by posting uplifting messages, updates on antibullying legislation, and examples of hate-based websites on the internet. The video-sharing website YouTube created an antibullying channel designed to encourage teens to speak out against internet harassment. As part of the “Be Best” campaign she officially launched in May 2018, First Lady Melania Trump held a summit on cyberbullying in August of that year; the importance of educating the American youth, particularly, about proper online etiquette was one of the foundations of her initiative. However, some commentators expressed concern regarding the effectiveness of her campaign, as her husband, then President Donald Trump, was often seen using his social media posts to bully and to disparage his opponents and others.

IMPACT

The rise of cyberbullying in America has led to increased awareness among the public and in the

government and has inspired legislation intended to prevent such offenses.

Though cyberbullying is predominantly seen among teenagers, all age groups are affected by this type of harassment. Cyberbullying has had distressing effects on victims and is damaging to their mental and emotional health. Many experience anxiety, depression, and other related stress disorders. Victims have also been known to become isolated and undergo severe changes in behavior and mood. Some have committed suicide as a result of being relentlessly cyberbullied. Anticyberbullying campaigns have raised public awareness of different forms of harassment that occur both online and offline. Despite such efforts, cyberbullying remained an issue of concern during the early 2020s. According to a 2022 Pew Research Center poll, 46 percent of US teens reported having experienced a form of cyberbullying at some point in their lives.

—Cait Caffrey

Further Reading

- Alejandro Arzate, Hector. "Cyberbullying Is on the Rise among Teenagers, National Survey Finds." *Education Week*, 15 July 2019, blogs.edweek.org/edweek/District_Dossier/2019/07/cyberbullying_is_on_the_rise_a.html.
- Anderson, Monica. "A Majority of Teens Have Experienced Some Form of Cyberbullying." *Pew Research Center*, 27 Sept. 2018, www.pewresearch.org/internet/2018/09/27/a-majority-of-teens-have-experienced-some-form-of-cyberbullying/.
- Bagwell, Karen. "Teaching, Not Technology, Needed to Enforce Internet Rules." *Education Daily*, vol. 40, no. 212, 2007, p. 2.
- Belsey, Bill. "Cyberbullying: An Emerging Threat to the 'Always On' Generation." *Bullying.org*, 2004, cyberbullying.ca/pdf/Cyberbullying_Article_by_Bill_Belsey.pdf.
- "Bullying Laws across America." *Cyberbullying Research Center*, cyberbullying.org/bullying-laws.
- Centers for Disease Control and Prevention. *Youth Risk Behavior Surveillance—United States, 2017*. CDC, 15 June 2018, www.cdc.gov/healthyyouth/data/yrbs/pdf/2017/ss6708.pdf.

- Cloud, John. "Bullied to Death?" *Time*, 18 Oct. 2010, pp. 60–63.
- "Cyberbullying: Definition." *Pacer's National Bullying Prevention Center*, 2020, www.pacer.org/bullying/resources/cyberbullying.
- Donegan, Richard. "Bullying and Cyberbullying: History, Statistics, Law, Prevention and Analysis." *Elon Journal of Undergraduate Research in Communications*, vol. 3, no. 1, 2012, pp. 34–36.
- Hern, Alex. "Ask.fm's New Owners Vow to Crack Down on Bullying or Shut the Site." *The Guardian*, 19 Aug. 2014, www.theguardian.com/technology/2014/aug/19/askfm-askcom-bullying.
- Hinduja, Sameer, and Justin W. Patchin. *Cyberbullying Prevention and Response: Expert Perspectives*. Routledge, 2012.
- Hoffman, Jan. "Online Bullies Pull Schools into the Fray." *New York Times*, 27 June 2010, www.nytimes.com/2010/06/28/style/28bully.html.
- Mahdawi, Arwa. "Melania Trump Rails against Cyberbullying—But She Is Using Social Media to Gaslight the World." *The Guardian*, 21 Aug. 2018, www.theguardian.com/commentisfree/2018/aug/21/melania-trump-rails-against-cyberbullying-social-media-gaslight-world.
- "Parents: Cyber Bullying Led to Teen's Suicide." *ABC News*, 19 Nov. 2007, abcnews.go.com/GMA/story?id=3882520.
- Polanin, Joshua R., et al. "A Meta-Analysis of School-Based Bullying Prevention Programs' Effects on Bystander Intervention Behavior." *School Psychology Review*, vol. 41, no. 1, 2012, pp. 47–65.
- Schneider, Shari Kessel, et al. "Cyberbullying, School Bullying, and Psychological Distress: A Regional Census of High School Students." *American Journal of Public Health*, vol. 102, no. 1, 2012, p. 171.
- Siegel, Lee. "The Kids Aren't Alright." *Newsweek*, 15 Oct. 2012, pp. 18–20.
- STOMP Out Bullying*, 2023, www.stompoutbullying.org.
- Vogels, Emily A. "Teens and Cyberbullying 2022." *Pew Research Center*, 15 Dec. 2022, www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022.
- "What Is Cyberbullying." *StopBullying.gov*, 21 July 2020, www.stopbullying.gov/cyberbullying/what-is-it.
- Ybarra, Michele L., and Kimberly J. Mitchell. "How Risky Are Social Networking Sites? A Comparison of Places Online Where Youth Sexual Solicitation and Harassment Occurs." *Pediatrics*, vol. 121, no. 2, 2008, pp. e350–e357.

CYBERCRIME

ABSTRACT

Cybercrime refers to any crime that uses a computer, often attached to the internet, as a target, weapon, or accessory for attacking individuals, groups, or their property. There are many examples of cybercrime, including identity theft, denial-of-service (DoS) attacks, internet fraud, predatory online behavior, and theft of intellectual property.

BACKGROUND

With the advent of computers in the 1950s, criminals immediately began exploiting the technology in creative ways. The introduction of the internet in the 1980s led to a marked increase in cybercrime, but the development of the ubiquitous World Wide Web in the 2000s—with access from home, work, and mobile devices—led to exponential growth of all types of cybercrime.

One of the most popular digital identity attacks of the early twenty-first century was phishing with email. In a phishing attack, the thief sends an email to an unsuspecting victim, requesting their digital information under false pretenses, such as pretending to be the victim's bank and asking for their social security and bank account numbers. Once the thief has the banking information, they then empty the victim's bank account. Thieves also steal identities by placing spyware in a victim's computer to secretly log their private information. Protection from an identity theft attack is tailored to the attack. For example, training has helped reduce phishing attacks, while internet security programs that specialize in antispyware are the best protection against a spyware attack.

Accessing and storing child pornography on a computer is another common type of cybercrime that increased as the web became more popular and accessible. Sites exhibiting a wide range of images and videos of child pornography are easily accessible from a web browser unless some type of blocking

software has been installed. Many public libraries and home computers installed blocking software over the course of the early twenty-first century. Social media sites generally tried to control improper content by carefully monitoring their sites. Law enforcement personnel involved in computer forensics spent much of their time searching computers for child pornography and then testifying in court.

One of the most popular uses of the internet is to download and listen to music. The first decades of the twenty-first century saw the creation of hundreds of sites where one can download all types of music in several formats, and many artists began marketing their music from their own websites. In spite of the large number of legal websites to download and play music, there were even more illegal sites created. These illegal sites have greatly reduced the profitability of the recording industry. The Recording Industry Association of America (RIAA), initially founded in 1952 to administer standards of frequency during recording, focused in the 2000s on helping to fight the illegal downloading of music. The RIAA became a leader in developing ways to secure the music downloading process, using special formats to protect music files and taking legal action at the discovery of illegal downloading sites.

Illegal downloading of motion pictures is another common form of cybercrime. Some popular films of the early twenty-first century were recorded with cell phones and placed on illegal websites within days of their release. The Motion Picture Association of America (MPAA) is a trade group that has increasingly worked to combat this type of theft, using technology and lawsuits. The theft of music and motion pictures on the internet is just one example of the theft of intellectual property that became prevalent throughout the early twenty-first century. Theft of software, images, and even company secrets also became a major problem for industry. To protect against such attacks, companies have implemented



Image via iStock/Nanzeeba Ibnat. [Used under license.]

expensive network and computer software, conducted massive training programs, and employed many computer security specialists.

OVERVIEW

The most common form of attack on a computer in the early twenty-first century is an intrusion attack. These have many forms: viruses, codes that can replicate themselves and damage computers; worms, programs that can replicate themselves and damage computers; bots, programs that help attack other computers; and spyware, programs that collect and forward private information. Trojan horses are one of the most dangerous forms of intrusion attack, as they are often launched from a hacker website, masquerading as a useful site. For example, starting in 2007, the Trojan horse ZeuS was

used to steal online banking information after infecting a user through a download from a website—whether a malicious site or an infected legitimate site—or by a link in an email to such a site. Almost all intrusion attacks constitute a crime, although some are simply attempts to irritate the attacked user. Training about how to avoid attacks and protecting software—antivirus, antispyware, and intrusion protection systems—provided reasonable protection from intrusion attacks, but hackers still found vulnerabilities to attack.

Another well-known type of attack on computers is a denial of service (DoS) attack, during which a hacker sends a massive volume of messages to a server, usually on the internet, that interfere with the server's ability to function properly. A 2007 attack that interrupted electric service in Estonia is

probably the best-known DoS attack of the 2000s, but there were many others. DoS attacks are generally cybercrimes, but they can be hard to prosecute. DoS attacks were also sometimes mounted by nations as a part of cyberwarfare, and in these cases were not technically a crime. A variety of defenses are used to combat DoS attacks. One of the most effective is to employ a honeypot, a computer that appears to be the server under attack, and let it draw the attacking traffic to it; intelligent firewalls and routers have also proven to be effective.

INTERNET FRAUD

Fraud has always been a major problem for law enforcement, and in the early twenty-first century it largely migrated to the internet. Digital identities can be hard to recognize and validate on the internet. For example, customers can log in to what they think is the rewards site for their credit card and give all their credit card information to a thief who proceeds to buy the maximum amount with their card.

In another famous example of internet fraud during the decade, a criminal or criminals posed as a Nigerian lawyer who solicited victims via email by promising to transfer an inheritance into their bank accounts upon receipt of their account numbers, and instead took all their money. Consumer education is one of the best defenses against internet fraud, but it has needed to be combined with improved authentication techniques. One example is to give each internet user or site a digital certificate, thus creating a digital identity for all on the internet, so that cybercriminals intent on committing internet fraud can be detected and stopped.

CYBERBULLYING AND PHARMING

Cyberbullying is the use of communications devices or the internet to verbally abuse or threaten another individual. During the early twenty-first century, many laws were passed to limit cyberbullying, but it

has continued to be a difficult type of cybercrime to control, especially on social media sites.

The first two decades of the twenty-first century saw an increase in an additional form of cyberattack known as pharming, which, like phishing, is a type of digital scam that allows an individual to steal a user's personal information via the internet. Rather than using email to lure in victims, pharming targets a person's web browser by using a malicious code installed on the computer and browser to redirect the unsuspecting user away from a legitimate website (such as PayPal or eBay) to another, similar but fraudulent site. When the user visits the site and makes financial transactions or exchanges personal information under the impression that they are using a legitimate service, the hacker then actually receives the information instead of the intended company. This form of cyberattack has largely been considered even more dangerous, as users are not required to click on a link or respond to an email but instead are automatically redirected without their knowledge. While software has been created to help detect fraudulent websites, hackers have continued to come up with alternative methods of illegally acquiring digital information.

IMPACT

The twenty-first century has seen rapid growth in using the internet to communicate, transact business, access entertainment, and obtain information. Along with this growth came a proportionate increase in cybercrimes. Initially, most internet users paid little attention to these cybercrimes. However, publicity about the financial losses incurred by identity theft victims, the physical harm suffered by cyberbullying victims, and damage done to companies and nations by DoS attacks made people aware of the dangers of cybercrime. As a result, internet users have developed a healthy fear of cybercrime. Industry, educational institutions, and individuals have also purchased security software and hardware

to protect their systems, greatly increasing the cost of using the internet.

—George M. Whitson III

Further Reading

- Bradbury, David. "When Borders Collide: Legislating Against Cybercrime." *Computer Fraud and Security*, vol. 2, 2012, pp. 11–15.
- Cilli, Claudio. "Identity Theft: A New Frontier for Hackers and Cybercrime." *Information Systems Control Journal*, vol. 6, 2005, pp. 1–4.
- Doyle, Charles. *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*. Congressional Research Service, 2010.
- Holt, Thomas J., Adam M. Bossler, and Kathryn C. Seigfried-Spellar. *Cybercrime and Digital Forensics: An Introduction*. 3rd ed., Routledge, 2022.
- McLaurin, Joshua. "Making Cyberspace Safe for Democracy: The Challenge Posed by Denial-of-Service Attacks." *Yale Law and Policy Review*, vol. 30, no. 1, 2011, p. 11.
- Schell, Bernadette H., and Clemens Martin. *Cybercrime: A Reference Handbook*. ABC-CLIO, 2004.
- Singer, P. W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford UP, 2014.
- Wall, David. *Cybercrimes: The Transformation of Crime in the Information Age*. Polity, 2007.
- Watters, Paul A. *Cybercrime and Cybersecurity*. CRC Press, 2023.
- "What Is Pharming and How to Protect Yourself." [Kaspersky Lab, usa.kaspersky.com/internet-security-center/definitions/pharming#.WDXNKLrJQI](https://www.kaspersky.com/internet-security-center/definitions/pharming#.WDXNKLrJQI).

CYBERCRIME, SOCIAL IMPACTS OF

ABSTRACT

Cybercriminals take full advantage of the anonymity, secrecy, and interconnectedness provided by the internet, therefore attacking the very foundations of the modern information society. Cybercrime can involve botnets, computer viruses, cyberbullying, cyberstalking, cyberterrorism, cyberpornography, denial of service (DoS) attacks,

hacktivism, identity theft, malware, and spam. Law enforcement officials have struggled to keep pace with cybercriminals, who cost the global economy billions annually. Police are attempting to use the same tools cybercriminals use to perpetrate crimes in an effort to prevent those crimes and bring the guilty parties to justice. This essay begins by defining cybercrime and then moves to a discussion of its economic and social impacts. It continues with detailed excursions into cyberbullying and cyberpornography, two especially representative examples of cybercrime, and concludes with a discussion of ways to curtail the spread of cybercrime.

BACKGROUND

Computer-related crime dates to the origins of computing, though the greater connectivity between computers through the internet has brought the concept of cybercrime into the public consciousness of the information society.

Cybercrime, as distinguished from computer crime, is an umbrella term for the various crimes committed using the World Wide Web (WWW), such as:

- The theft of one's personal identity (identity theft) or financial resources;
- The spread of malicious software code such as computer viruses;
- The use of others' computers to send spam email messages (botnets);
- Denial of service (DoS) attacks on computer networks or websites by the hacker;
- Hacktivism, or attacking the computer servers of those organizations felt by the hacker to be unsavory or ethically dubious;
- Cyberstalking, by which predators use internet chat rooms, social networking sites, and other online venues to find and harass their victims;
- Cyberbullying, where individuals are harassed by others, causing severe mental anguish;
- Cyberpornography, the use of the internet to spread child and adult pornography;

- Internet gambling and software piracy;
- Cyberterrorism, the use of the internet to stage intentional, widespread attacks that disrupt computer networks; using the internet to spread violent messages, recruit terrorists, and plan attacks;
- Cybertrespass (hacktivism, viruses, denial of service attacks);
- Cyberdeceptions (identity theft, fraud, piracy); and
- Cyberviolence (cyberbullying, cyberstalking).

Several of these activities have a long history that predates the internet, and they also have technological antecedents.

Media reports since the 1990s have documented the many methods by which criminals have used the internet to commit crimes. Cyberthieves have become skilled at using the anonymity and secrecy of the internet to defraud their victims of their money, their peace of mind, and indeed even their lives. When victims let their guard down by muting a healthy skepticism and caution, cybercrime takes place.

OVERVIEW

As more and more people have used the internet to do their shopping, communicating, banking, and bill paying, they have become targets for cybercriminals. There are commonsense steps that can prevent or reduce having one's financial information stolen online, as well as to avoid other scams and threats, but cybercrime in these areas persists largely due to a lack of consumer education.

Some varieties of cybercrime, such as hacktivism, are ostensibly motivated by noble intentions, such as protest against perceived abuses by governments and corporations. Often these attacks involve posting comments on official government websites and are not motivated by a desire for monetary gain. However, other forms of cybercrime have a much

more violent intent. These include cyberstalking, cyberbullying, and cyberterrorism.

Law enforcement officials have struggled to identify, arrest, and prosecute tech-savvy offenders, even as sociologists have sought to get to the root of cybercrime. The Federal Bureau of Investigation (FBI) created a special cyber division in 2002 to address cybercrime in a coordinated and cohesive manner with cybersquads in each of its field offices, "cyberaction teams" that travel worldwide to address cyberattacks, and nationwide computer task forces. The field of cybercrime has spawned the field of cybercriminology.

By the second decade of the twenty-first century, the scope and financial costs of cybercrime had become staggering. In 2012, for instance, the US economy lost \$525.5 million to cybercrime, an increase of over \$40 million from 2011, with the most common complaints in 2012 being impersonation email scams, intimidation crimes, and scams that attempted to extort money from computer users. In 2012, cybercrime cost British businesses £21 billion, and over 1 million computer users in the European Union (EU) were affected every day by cybercrime. According to the Federal Bureau of Investigation's (FBI's) Internet Crime Complaint Center's 2016 report, victims of cybercrime lost a total of \$1.33 billion that year; by that point, the organization was receiving an average of 280,000 complaints of cybercrime victimization per year.

The financial impacts of cybercrime continued to worsen during the 2020s, and by the year 2023, the statistics platform Statista estimated that the worldwide cost of cybercrime was in excess of \$8 trillion. In the same report, Statista estimated that cybercrime's annual worldwide cost would rise to more than \$13 trillion by 2028.

CYBERCRIME AND SOCIETY

While the economic impact of cybercrime is beyond dispute, rather less attention has been given to the

social implications of cybercrime. Psychologists and psychiatrists can help victims cope with the fallout from identity theft, sexual abuse, or financial ruin, whereas sociologists are well-positioned to look at the broader social impacts and explanations of cybercrime.

Cybercrime attacks the very foundations of modern, technological societies, bound up as they are with the rapid flow of computer data facilitated by the internet. At the most basic level, cybercriminals often take advantage of technologically unsophisticated individuals who nonetheless find themselves in a world where the internet plays an increasingly central role in both community and private life. Cybercrime depends, at this level, on the ability of those who are more technologically sophisticated to use that knowledge to trick others into surrendering vital information, such as their bank account information or Social Security number. While it is possible in some situations for the victim of cybercrime to restore stolen money or even their personal online identity, the event often leaves the victim traumatized and deeply suspicious of the internet and other trappings of modern life. In this way the cybercriminal deprives his or her victim of many of the conveniences of today's information economy.

Experts in cybercrime have noted that its impact occurs on multiple levels. First, on a purely economic level, cybercrime involves the theft of millions, and in some instances billions, of dollars every year. In addition, cybercrime requires individuals and institutions to take on the added cost of security software and other means by which to frustrate the cybercriminals.

Second, on a broader cultural level, cybercrime helps to sour general perceptions about the internet in particular and new technology in general. Paradoxically, it can also make those who have been victims of one type of cybercrime more vulnerable to other types of cybercrime because of their lack of awareness of new and evolving cybercrime methods.

Third, and perhaps most alarming of all, cybercrime creates traumatized individuals who are less able to cope with the demands of life. Whether one is the victim of identity theft, a credit card scam, or cyberbullying, and regardless of whether restitution is made, the effects of cybercrime can impact the psyche as much as any crime.

STOPPING CYBERCRIME

In his 1995 essay, Gene Stephens offered what one might call a traditionally libertarian way to combat cybercrime that fits well with the open ethos of cyberspace. Given the massive proliferation of cybercrime since 1995, Stephens began in 2008 to see things differently and argued that stopping cybercrime will depend largely on two factors: a more secure internet infrastructure, redesigned with security foremost in mind; and coordinated, global policing of cyberspace to back up other security methods such as biometrics. Stephens also argued that fighting cybercrime involves tackling a larger and more fundamental issue: How can one police an area, such as cyberspace, that very obviously no one person owns and has jurisdiction over? The answer, he argues, is voluntary, multinational policing, with the price of failure being too great to ignore.

The exponentially improving capabilities of emerging web technologies spotlights the long-ignored issues of who owns the WWW, who manages it, and who has jurisdiction over it. The answer now is: Nobody! Can the world's most powerful socio-politico-economic network continue to operate almost at random, open to all, and thus be excessively vulnerable to cybercriminals and terrorists alike? Yet any attempt to restrict or police the web can be expected to be met by extreme resistance from a plethora of users for a variety of reasons, many of which seem contradictory. Biometrics and more-advanced systems of ID will need to be perfected to protect users and the network. In addition, multinational cybercrime units will be required to

catch those preying on users worldwide, as web surfers in Arlington, Virginia, and Victoria, British Columbia, may be victims of cyberscams perpetrated in Cairo or Budapest.

Although the task is daunting, governments worldwide are taking steps. In 2012, the EU announced the establishment of a cybercrime center aimed at stopping identity thieves and other online criminals. The policymaking arm of the EU, the European Commission, proposed mandatory jail time for online crimes. In the United States, multiple federal agencies conducted investigations into cybercrime; however, a 2023 investigation by the US Government Accountability Office (GAO) found that ongoing efforts to combat cybercrime were insufficient, in large part because of variations in reporting methods between agencies.

Can one be optimistic about the containment of cybercrime? If history is any judge, the same internet technology that empowers criminals to evade the law can enable law enforcement to defend the law.

—Matt Donnelly

Further Reading

- “2012 Internet Crime Report Released: More Than 280,000 Complaints of Online Criminal Activity Reported in 2012.” *Federal Bureau of Investigation*, 14 May 2013, www.fbi.gov/sandiego/press-releases/2013/2012-internet-crime-report-released.
- “Annual Reports.” *Internet Crime Complaint Center (IC3)*, 2022, www.ic3.gov/Home/AnnualReports?redirect=true.
- “Cyber Crime.” *Federal Bureau of Investigation*, www.fbi.gov/investigate/cyber.
- “Cybercrime: Reporting Mechanisms Vary, and Agencies Face Challenges in Developing Metrics.” *GAO*, 20 June 2023, www.gao.gov/products/gao-23-106080.
- Duggan, M. “Online Harassment 2017.” *Pew Research Center*, 11 July 2017, www.pewinternet.org/2017/07/11/online-harassment-2017.
- Dupont, B. “Bots, Cops, and Corporations: On the Limits of Enforcement and the Promise of Polycentric Regulation as a Way to Control Large-Scale

Cybercrime.” *Crime, Law and Social Change*, vol. 67, no. 1, 2017, pp. 97–116.

Guarascio, Francesco. “EU Prepares to Launch First Cybercrime Centre.” *Euractive*, 29 Mar. 2012, www.euractiv.com/infosociety/eu-prepares-launch-cybercrime-ce-news-511823.

“Internet Porn ‘Increasing Child Abuse.’” *The Guardian*, 12 Jan. 2004, www.guardian.co.uk/technology/2004/jan/12/childprotection.childrensservices.

Jaishankar, K. “Cyber Criminology: Evolving a Novel Discipline with a New Journal.” *International Journal of Cyber Criminology*, vol. 1, no. 1, 2007, www.cybercrimejournal.com/pdf/editorialijcc.pdf.

Kizza, Joseph Migga. *Ethical and Social Issues in the Information Age*. 7th ed., Springer, 2023.

Lenhart, A. “Cyberbullying and Online Teens.” *Pew Research Center*, 27 June 2007, www.pewresearch.org/internet/2007/06/27/cyberbullying.

Levi, M. “Assessing the Trends, Scale and Nature of Economic Cybercrimes: Overview and Issues.” *Crime, Law and Social Change*, vol. 67, no. 1, 2017, pp. 3–20.

Liebowitz, M. “Online Bullying Rampant Among Teens, Survey Finds.” *NBC News*, 9 Nov. 2011, www.nbcnews.com/id/wbna45227264.

Marcum, C., G. Higgins, T. Freiburger, et al. “Exploration of the Cyberbullying Victim/Offender Overlap by Sex.” *American Journal of Criminal Justice*, vol. 39, 2014, pp. 538–48.

Morris, H. “Europe Cracks Down on Cybercrime.” *International New York Times*, 12 Mar. 2012, archive.nytimes.com/rendezvous.blogs.nytimes.com/2012/03/29/europe-cracks-down-on-cybercrime.

Petrosyan, Ani. “Annual Cost of Cybercrime Worldwide 2017–2028.” *Statista*, 15 Sept. 2023, www.statista.com/forecasts/1280009/cost-cybercrime-worldwide.

Stanglin, D., and W. M. Welch. “Two Girls Arrested on Bullying Charges after Suicide.” *USA Today*, 16 Oct. 2013, www.usatoday.com/story/news/nation/2013/10/15/florida-bullying-arrest-lakeland-suicide/2986079.

Stephens, G. “Crime in Cyberspace.” *Futurist*, vol. 29, 1995, pp. 24–31.

_____. “Cybercrime in the Year 2025.” *Futurist*, vol. 42, 2008, pp. 32–36.

Wall, D. *Cybercrime: The Transformation of Crime in the Information Age*. Polity, 2007.

- Wall, D. S., and M. L. Williams. "Policing Cybercrime: Networked and Social Media Technologies and the Challenges for Policing." *Policing and Society*, vol. 23, 2013, pp. 409–12.
- Wayne L., A., and L. A. Johnson. "Current United States Presidential Views on Cyber Security and Computer Crime with Corresponding Department of Justice Enforcement Guidelines." *Journal of International Diversity*, 2011, pp. 116–19.
- Yar, M. *Cybercrime and Society*. SAGE, 2006.

CYBERSECURITY BASICS

ABSTRACT

Any computer with access to the internet can suffer a cyberattack that can cause damage to the computer itself or to the users of that computer. Damages may include physical damage to the electronic structure of the computer, theft of personal and confidential information, financial loss, or any combination of these and other damages. Cybersecurity is the implementation of practices and systems to prevent or at least mitigate such events.

BACKGROUND

Any computer connected to the internet is vulnerable to a cyberattack. A cyberattack is harm done to a computer or network. There are many different kinds of cyberattacks. When a computer is hacked, someone in another location is viewing or taking the computer's information without permission. A person who hacks into computers is a hacker. Some hackers try to find bank account or credit card information. They use this information to steal money or make purchases. Other hackers steal passwords. Passwords are special words or phrases that people use to protect their information. Hackers use passwords to access a person's email or other accounts. Some hackers install viruses on computers just to cause damage.

Viruses are programs meant to harm computers. A program is a set of directions that tell a computer

what to do. Viruses enter computers in several ways. Some viruses enter when people visit certain websites. Some look like advertisements or even security updates. When people click them, they allow the virus in. Other viruses spread through email.

Spam is unwanted email. Another name for "spam" is "junk mail." Many businesses send spam advertisements. They want people to buy the product in the ad. Most spam is harmless, but some spam has links to websites that contain viruses that can damage computers.

Cyberattacks became increasingly common throughout the early twenty-first century, and in June of 2012, US president Barack Obama stated that cyberattacks were a serious threat. Hackers launched cyberattacks against multiple large companies during that period; stores such as T. J. Maxx, Marshall's, Target, and Barnes & Noble were all victims of cyberattacks between 2007 and 2013. Hackers stole credit card information and other data from millions of customers in those attacks, calling attention to the need for companies to implement enhanced cybersecurity measures. Cyberattacks remained troubling occurrences into the 2020s, which saw further thefts of customer information from businesses as well as incidents of politically motivated hacking.

OVERVIEW

Computers serve many purposes in the twenty-first-century world. Computers help people stay connected to friends and family. People talk or send messages to one another with the click of a button. They use the internet to shop for anything from shirts to cars. Computers make it possible to send, receive, sort, and save all kinds of information quickly and easily. As a result, people are entering and saving more private information on computers.

Doctors and hospitals use computers to save patients' medical records. Banks and credit card



Image via iStock/Funtap. [Used under license.]

companies use computers to store information about people's money. Businesses use computers to keep records of customers' purchases. Governments use computers to store tax records, driver's license information, and other documents. People use computers to store pictures and videos. They use computers to send and receive email messages. They may use computers to connect to social networks.

The more that people save and share on computer networks, the more they are at risk of experiencing cyberattacks. Some ways to avoid becoming a victim of cyberattacks are the following:

- Install security software, dedicated programs that check computers for viruses and other threats. Security software should be added to anything that connects to the internet, such as printers and game consoles. This software is also essential to the security of devices such as

smartphones and tablets, and it should be updated often to protect against new viruses.

- Choose good passwords. A password should be long and use uppercase and lowercase letters as well as numbers and symbols. Do not use the same password for everything. Keep a list of passwords in a safe place.
- Avoid sharing private information on the internet. Never list phone numbers or addresses on social network websites.
- Only shop and bank on trusted websites. Web addresses that begin with "https://" or "shttp://" are secure and safe. Addresses that begin "http://" are not secure, and financial and other private information should not be shared on these websites.

People connect to the internet now more than ever. As a result, personal information stored on comput-

ers has never been more at risk. Following recommended cybersecurity practices is the only way to keep this information safe from cyberattacks.

—Lindsay Rock Rohland

Further Reading

- Easttom, Chuck. *Computer Security Fundamentals*. 5th ed., Pearson, 2023.
- Finkle, Jim, Soham Chatterjee, and Lehar Maan. “eBay Asks 145 Million Users to Change Passwords after Cyber Attack.” *Reuters*, 21 May 2014, www.reuters.com/article/us-ebay-password/ebay-asks-145-million-users-to-change-passwords-after-cyber-attack-idUSBREA4K0B420140521.
- Jamieson, Alastair, and Eric McClam. “Millions of Target Customers’ Credit, Debit Card Accounts May Be Hit by Data Breach.” *NBC News*, 19 Dec. 2013, www.nbcnews.com/business/consumer/millions-target-customers-credit-debit-card-accounts-may-be-hit-f2D11775203.
- Obama, Barack. “Taking the Cyberattack Threat Seriously.” *Wall Street Journal*, 19 July 2012, online.wsj.com/news/articles/SB10000872396390444330904577535492693044650.
- “Online Safety Basics.” *National Cybersecurity Alliance*, 26 May 2022, staysafeonline.org/resources/online-safety-basics.

BACKGROUND

Cybersecurity was of relatively little concern during the first decades of digital computing, as only a small group of people had access to computers during that period, but became more relevant in the late 1960s and early 1970s. In this period, access to large computers was still limited, but multiple users on one system had become standard. The Advanced Research Projects Agency Network (APANET), a predecessor to the internet, also emerged. Basic computer security, such as the use of passwords to protect sensitive data, was practiced. However, computers had vulnerable points of access that created security risks.

An early example of cybersecurity testing took place at International Business Machines Corporation (IBM). In 1967, IBM asked students to test a new computer. During the test, the students went beyond the test to investigate the parts of the computer system that were accessible to them. IBM subsequently patched the vulnerabilities the students had discovered and devised new means of protecting its computers going forward. More widely, leading computer experts developed deliberate tests to find security vulnerabilities in this period.

One of the earliest types of cybersecurity testing was penetration testing, also known as “ethical hacking.” Penetration testing exposes and exploits security vulnerabilities on computers, their systems, and their programs. The first “tiger teams,” which performed penetration testing on computer systems, emerged in the early 1970s.

Penetration testing continued to expand in the 1980s and 1990s, as the internet was introduced and access to the internet became mainstream. At the same time, the first computer viruses were introduced. Over the next few decades, viruses and other attacks became increasingly common. As the cyberthreats increased in number and the nature of computing evolved, cybersecurity testing expanded to include other types of security testing as well as

CYBERSECURITY TESTING

ABSTRACT

Cyberattacks on organizations and personal users can be costly, resulting in such issues as financial loss, reputational and trust damage, intellectual property theft, and legal and regulatory consequences. Cybersecurity testing works to prevent cyberattacks from occurring and lessening their negative effects. Testing involves the identification of security vulnerabilities and weaknesses—in hardware, software, systems, and networks—before they can be exploited by an attacker. Identifying actions to fix these vulnerabilities and weaknesses is also part of cybersecurity testing.

audits, scans, and assessments to address a broad variety of cybersecurity issues.

OVERVIEW

Cybersecurity testing has several general facets. They include checking on the vulnerability of software to cyberattacks. Another aspect is determining the operational impact of malicious or unexpected inputs. Finally, cybersecurity testing ensures the reliability and safety of systems and that these systems do not accept unauthorized inputs. Cybersecurity testing can be conducted manually by an internal or third-party security specialist or by automated testing solutions, depending on the type of cybersecurity testing and the organization or user.

TYPES OF CYBERSECURITY TESTING

The oldest type of cybersecurity testing is penetration testing. This type of testing simulates a realistic cyberattack under safe conditions. Penetration testing can reveal how well existing security measures will fare when a system, network, application, or software is under attack. Though penetration testing, unknown security vulnerabilities are identified.

Several types of cybersecurity testing focus specifically on applications. Web application security testing and mobile application testing focus on identifying vulnerabilities in web software and mobile applications, respectively. Those types of application testing gather information about programs and look for security problems. The testing also determines if vulnerabilities can be exploited easily and estimates related risks.

Application security testing (AST) outlines steps to take to eliminate software application vulnerabilities as soon as possible in the software development lifecycle (SDLC). Ideally, vulnerabilities are found before the software is produced or shortly after. In AST, the security posture of a software application is tested, monitored, and reported.

Another type of security testing is application programming interface (API) security testing. APIs provide a way to access sensitive information that attackers can use to gain access to internal systems. Through regular API security testing, security vulnerabilities in applications and web services are identified and shared with programmers and developers.

An additional type of security testing, cloud security testing, focuses on identifying configuration vulnerabilities, access control, and data encryption. Similarly, data security testing evaluates the security of data storage, transmission, and access controls. Information security testing evaluates how effective security policies, controls, and procedures are in protecting sensitive information from any unauthorized breaches or leaks.

Other types of cybersecurity testing include vulnerability management, configuration scanning, security auditing, and cybersecurity auditing. To protect endpoints, workloads, and networks, companies use vulnerability management to locate, evaluate, report, manage, and address related vulnerabilities using vulnerability-scanning tools. Configuration scanning, also known as security scanning, compares a set of standards created by a regulatory body or research group to the security gaps found in software, networks, or computer systems.

A security audit is a review of software and applications under a specific standard, such as a security requirement. Specifically, an audit may involve reviewing code or architecture and hardware configuration security postures. It may also include an analysis of security gaps or operating systems. A cybersecurity audit focuses on an assessment of related policies, procedures, and effectiveness. This audit may identify any internal controls or regulatory weaknesses that could create risk for the organization.

Additional cybersecurity testing types include cybersecurity risk assessment and red team

assessment. Cybersecurity risk assessment focuses on identifying, evaluating, and prioritizing risk to an organization and offering appropriate risk responses. Red team assessment evaluates the level of risk and vulnerability associated with an organization's assets, including technology.

BEST PRACTICES

Cybersecurity threats are dynamic and ever-changing. To protect organizations and users against cyberattacks, cybersecurity testing is most effective when it takes place regularly. When cybersecurity testing begins, a clear definition of what is included and what is not included in the testing should be in place, and all parties involved should agree on the scope. Testing objectives should also be defined.

Other best practices include selecting the appropriate testing methods to address the cybersecurity issues, automating testing when possible, and testing all secure interfaces. It is also important to keep complete records of testing procedures for future reference.

—A. Petruso

Further Reading

- “6 Types of Cyber Security Testing and Assessments.” *Sapphire*, www.sapphire.net/cybersecurity/cyber-security-testing.
- Brennan, Tom. “Penetration Testing: A Needed Defense against Cyber Threats.” *Security*, 28 Apr. 2022, www.securitymagazine.com/articles/97509-penetration-testing-a-needed-defense-against-cyber-threats.
- Crandall, Carolyn. “What Can We Learn by Analyzing 197 Years of Cumulative Cybersecurity Testing?” *Cyber Defense Magazine*, 26 July 2023, www.cyberdefensemagazine.com/what-can-we-learn-by-analyzing-197-years-of-cumulative-cybersecurity-testing.
- Mack, George. “The Fascinating History of Cyber Security You Never Knew.” *CyberTalk.org*, 14 June 2023, www.cybertalk.org/2023/06/14/the-fascinating-history-of-cyber-security-you-never-knew.
- Messier, Ric. *Build Your Own Cybersecurity Testing Lab: Low-Cost Solutions for Testing in Virtual and Cloud-Based Environments*. McGraw Hill, 2020.

Mowbray, Thomas J. *Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions*. John Wiley & Sons, 2014.

CYBERTERRORISM

ABSTRACT

The word “cyberterrorism” was coined in the late twentieth century to denote security threats arising from acts of sabotage perpetrated via networked computers. Determining whether or not a cyberterrorist attack has ever taken place is controversial, because scholars, politicians, and members of the media do not always agree on what constitutes cyberterrorism. However, fears about cyberterrorism reached new heights after al-Qaeda’s terrorist attacks on the United States on September 11, 2001, and presidential administrations following President George W. Bush’s continued to claim protecting national cybersecurity as a major priority.

Strategies concerning cybersecurity were consistently reassessed, especially after further high-profile cyberattacks such as those that occurred against the Democratic National Committee prior to the 2016 presidential election and against a crucial, large pipeline in 2021. Criminals choose to engage in cyberterrorism over traditional forms of terrorism due to its inherent anonymity, its ability to do major damage from any distance to large areas or groups simultaneously, and the fact that it is relatively easy and inexpensive to carry out.

BACKGROUND

Barry Collin, a researcher at California’s Institute for Security and Intelligence, originated the term “cyberterrorism” in the 1980s. Since then, two schools of thought on cyberterrorism have arisen. The first is represented by Dorothy Denning, a professor of computer science and an internationally renowned expert on information security. Denning has identified cyberterrorism as illegal and highly damaging attacks that target computers, networks,

and digitally stored information for the purposes of causing harm to people or property or generating fear.

The second school of thought includes the military, government officials, and others who define cyberterrorism as virtually any cyberattack that threatens computers and networks. Myriam Dunn-Cavelty, a security information expert and the head of Switzerland's New Risks Research Unit at the Center for Security Studies, divides those who analyze cyberterrorism into "hypers"—those who believe that cyberattacks have occurred—and "de-hypers"—those who believe that no such attack has ever occurred.

The growth of personal computing in the 1990s made the World Wide Web available to individuals all over the world. Simultaneously, computer hackers began exploiting website and software security holes to gain access to information, chiefly targeting governments, banks, large corporations, academic

institutions, and research centers. A 1991 report by the National Research Council and other agencies maintained in *Computers at Risk: Safe Computing in the Information Age* that cyberterrorists could wreak more havoc with a computer keyboard than with a bomb. In 2007 the US Department of Homeland Security (DHS) announced that more than 840 attempts had been made to hack into DHS computers over the past two years. Most of the DHS attacks involved failed attempts to access classified information.

Those like Denning who define cyberterrorism narrowly believe that cyberterrorism should not be confused with hacktivism, the term associated with computer hackers who insist they are motivated by politics rather than maliciousness or desire for financial gain. Activities carried out by hacktivists include denial of service (DoS) attacks, email attacks, hacking into computer networks to steal information and make it public, and destroying data through

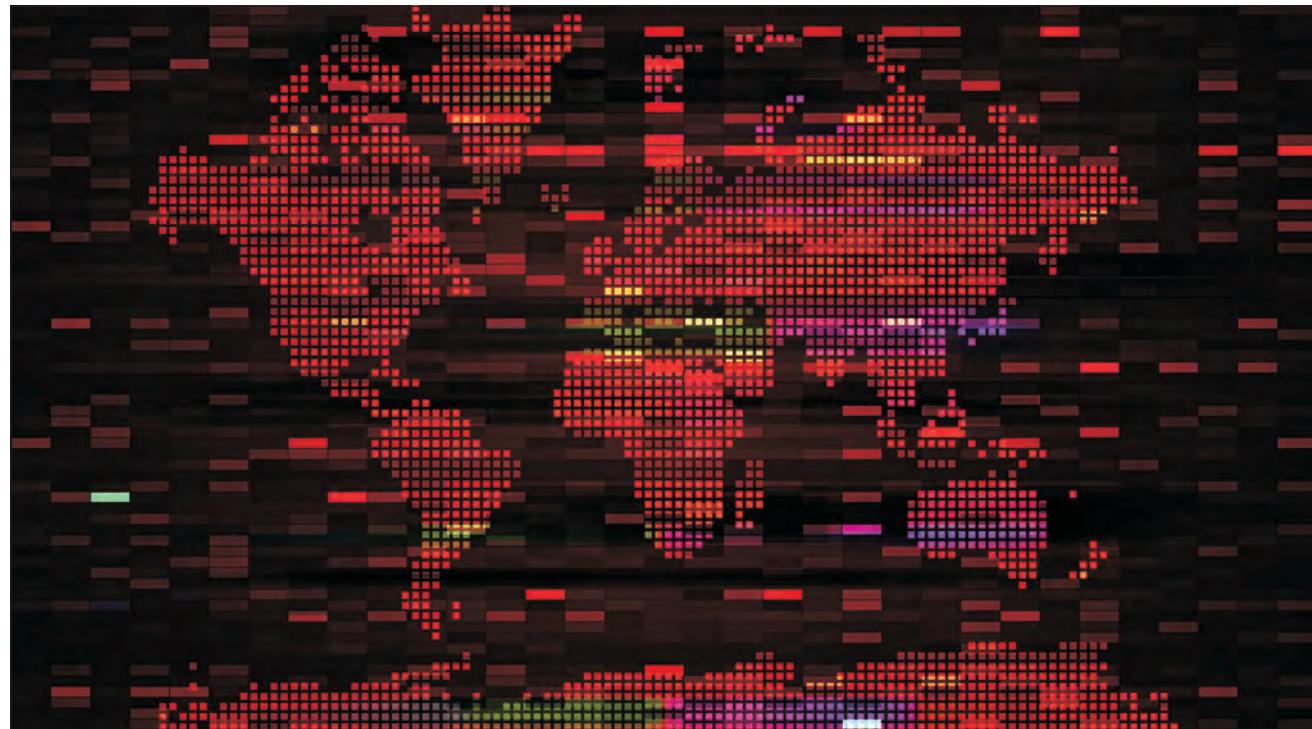


Image via iStock/Lidia Moor. [Used under license.]

viruses and worms. Many would consider the activities of WikiLeaks, the online organization founded by Australian Julian Assange that publishes secret information from anonymous sources, and Anonymous, a loose association of hackers who came to light after engaging in high-profile distributed DoS attacks, as hacktivism, not cyberterrorism.

OVERVIEW

By the early twenty-first century, most nations acknowledged that the threat of cyberterrorism had become a major national security issue. Many were particularly alarmed about national power grids, which are especially vulnerable to cyberattacks and have the potential to cripple large areas if they go offline.

In a 2008 article for *Information Security Journal: A Global Perspective*, Jonathan Matusitz identifies seven types of cyberterrorist activity: destroying the machinery of an infrastructure; commandeering controls of nuclear power plants or hazardous waste facilities; using computers to control dams; hacking into power grids; using technology to commit sabotage; initiating protests that involve hacking into government computers; and compromising information illegally accessed through computers.

Incidents that are often cited as examples of cyberterrorist attacks include an incident in 1999 when the North Atlantic Treaty Organization (NATO) forces allegedly bombed the Chinese Embassy in Bombay by accident. In 2000, a Filipino man launched the so-called Love Bug virus that attacked the Pentagon, a number of government agencies, banks, and international corporations, causing millions of dollars in damages. Because the Philippines had no cyberlaws, the perpetrator walked free. That same year, a disgruntled employee hacked into a local government system in Queensland, Australia, causing 264,000 gallons of raw sewage to contaminate rivers and parks.

The cyberterrorist attack usually identified as the event that focused international attention on cyberterrorism is the Stuxnet computer worm incident of July 2010. Iranian computers were hacked in order to destroy plutonium enrichment plants, thus hampering the country's efforts to develop a nuclear bomb. It was rumored that the attacks were engineered through a joint effort between the United States and Israel. Allegedly, Iran responded by launching a cyberattack on US financial institutions. In 2007, the Eastern European nation of Estonia was hit with a massive DoS attack that affected government and corporate websites. Estonia blamed the Russian government, which denied responsibility.

Fears of cyberterrorism have been heightened through depictions in popular novels and movies. As early as 1983, the spotlight was turned on cyberterrorism with *WarGames*, a film in which a young hacker breaks into a US military supercomputer and sets in motion a chain of events that will start World War III. *Goldeneye*, the seventeenth James Bond film, also dealt with cyberterrorism. Novels that feature cyberterrorism include Tom Clancy's Net Force series and several works by Winn Schwartau, particularly *Pearl Harbor.com* (2002).

Efforts to pass federal legislation on cyberterrorism have typically led to partisan wrangling over increased government regulation, and Congress has repeatedly failed to pass them. On February 18, 2013, President Barack Obama responded to those failures by issuing an executive order titled "Improving Critical Infrastructure Cybersecurity," which encouraged voluntary implementation of improved computer security measures among those involved in critical infrastructures.

In November 2014 US-based Sony Pictures Entertainment suffered a cyberattack in which its computer networks were hacked. A group calling itself Guardians of Peace leaked data from Sony's computers, including embarrassing emails and personal information about its actors. The group also

threatened movie theater chains that were planning to screen *The Interview*, a comedic satire about North Korea, with a September 11-style terror attack. In response, President Obama and the Federal Bureau of Investigation (FBI) blamed the attack on North Korea, which praised the cyberattack but refused to take responsibility for it. On January 2, 2015, Obama signed an executive order to impose largely symbolic sanctions on North Korean organizations and ten individuals.

National and international debate around cybersecurity next became more prominent in the lead-up to the 2016 presidential election, as it was discovered that an orchestrated cyberattack campaign had been employed by Russian hackers that had involved a breach of the Democratic National Committee's computer system as well as email accounts within Democratic candidate Hillary Clinton's campaign; other targeted attempts against some Republican politicians and organizations had also been made. The level of this cyberattack, in addition to questions regarding whether there had been any link between Republican candidate and eventual president-elect Donald Trump and the Russian interference in this democratic institution, resulted in lengthy federal investigations.

In 2018, Trump, as president, signed a bill that established a new agency, the Cybersecurity and Infrastructure Security Agency (which rebranded the former National Protection and Programs Directorate launched in 2007), to put more emphasis on and resources toward cybersecurity. Between 2020 and mid-2021, a series of major cyberattacks hit different sectors. These included the technology sector with Microsoft's announcement that its software for its Exchange Server email, used worldwide by a number of businesses, had been hacked, and the energy sector with the report that Coastal Pipeline had been compelled to shut down its pipeline responsible for transporting a significant percentage of jet fuel and gasoline across the country due to a ransomware

attack on its central networks. In May 2021, President Joe Biden signed an executive order that outlined specific actions to be taken to make the country's defenses against such attacks stronger.

There is no widespread consensus on how to fight cyberterrorism, and information experts tend to agree that the United States lacks the capability of preventing all such attacks. However, most accept that basic security measures, such as implementing defense mechanisms, identifying potential cyberterrorists, eliminating known threats, and instituting international cooperation designed to mitigate damage and bring perpetrators to justice, are necessary steps in battling cyberterrorism.

—Elizabeth Rholetter Purdy

Further Reading

- Abrams, Abigail. "Here's What We Know So Far about Russia's 2016 Meddling." *Time*, 18 Apr. 2019, time.com/5565991/russia-influence-2016-election.
- Assante, Mike. *CyberSkills Task Force Report Fall 2012*. US Department of Homeland Security, 2012.
- Colarik, Andrew Michael. *Cyber Terrorism: Political and Economic Implications*. IGI Global, 2006.
- Collin, Barry. "The Future of Cyberterrorism." *Crime and Justice International*, vol. 13, no. 2, 1997, pp. 15–18.
- Conway, Maura. "Against Cyberterrorism." *Communications of the ACM*, vol. 54, no. 2, 2011, pp. 26–28.
- Denning, Dorothy. "A View of Cyberterrorism Five Years Later." *Internet Security: Hacking, Counterhacking, and Society*, edited by Kenneth Elinor Himma, Jones, 2007.
- Dunn-Cavelty, Myriam. *Cyber-Security and Threat Politics: U.S. Efforts to Secure the Information Age*. Routledge, 2008.
- Herbert, Lin. "A Virtual Necessity: Some Modest Steps toward Greater Cybersecurity." *Bulletin of the Atomic Scientists*, vol. 68, no. 5, 2012, pp. 75–87.
- Matusitz, Jonathan. "Cyberterrorism: Postmodern State of Chaos." *Information Security Journal: A Global Perspective*, vol. 17, no. 4, 2008, pp. 179–87.
- National Research Council, et al. *Computers at Risk: Safe Computing in the Information Age*. National Academy, 1991.
- Ordoñez, Franco. "In Wake of Pipeline Hack, Biden Signs Executive Order on Cybersecurity." *NPR*, 12 May 2021,

- www.npr.org/2021/05/12/996355601/in-wake-of-pipeline-hack-biden-signs-executive-order-on-cybersecurity.
- Sanger, David E., et al. “Cyberattack Forces a Shutdown of a Top U.S. Pipeline.” *New York Times*, 13 May 2021, www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html.
- “Sony Cyber-Attack: North Korea Faces New US Sanctions.” *BBC News*, 3 Jan. 2015, www.bbc.com/news/world-us-canada-30661973.
- Tafoya, William L. “Cyber Terror.” *FBI Law Enforcement Bulletin*, 1 Nov. 2011, leb.fbi.gov/articles/featured-articles/cyber-terror.

CYBERWARFARE

ABSTRACT

The increasing reliance of both public and private infrastructure in the United States on computer systems, the threat of cyberwarfare, or one country (or an organized nonstate actor) attacking the computer systems of another nation, has received significant attention in the US government and press. This attention generally increases whenever a particularly bad breach of security is made public. Many people believe cyberwarfare poses a serious threat to both public and private interests and that more resources should be devoted to improving system security and tracking down those responsible for any attacks. While institutions have suffered billions of dollars in economic loss due to various forms of computer crime, an increasing concern for government is the threat to life and limb posed by vulnerabilities in the computer systems controlling basic national assets, from military information to transportation networks, telecommunications, and the power grid. As awareness of the problem has grown, so have calls to consider when and how to respond to such attacks and in what circumstances offensive cyberattacks could or should be deployed.

BACKGROUND

Ever since computers have been able to communicate with one another, people have been finding

ways to subvert this connectivity. Computer viruses, self-reproducing programs that spread from computer to computer and disrupt their operations to varying degrees, predate the existence of the internet and are perhaps the most common computer security threat. Other forms of computer crime (or cybercrime) can include hacking, or circumventing computer security measures, either for fun or to steal information, such as financial data or government secrets. Computer networks can also simply be prevented from operating effectively, as in a denial-of-service (DoS) attack, in which a network is flooded with so many bits of information that it either slows down or crashes completely. Antivirus and other security software designed to protect users from these threats is now a multibillion-dollar industry: the estimated revenue from worldwide sales of security software reached \$43.2 billion in 2019, according to the research firm Statista.

Cybercrime becomes cyberwarfare when the activity is sponsored by a state government and directed against the assets of another state. Cyberwarfare can involve espionage, as when government computer systems are infiltrated to steal military or other secrets, or it can involve an attempt to disrupt the flow of information or the operation of computer systems.

An international incident widely considered an example of cyberwarfare took place in 2007, when the internet infrastructure of Estonia was brought to a near standstill—including the temporary shutdown of government, banking, and media websites—by a DoS attack believed to have been orchestrated by the Russian government. The attack took place during a heated disagreement between Russia and Estonia over the relocation of a World War II-era Soviet war memorial in Estonia. The following year, during the armed conflict between Russia and Georgia over South Ossetia, similar DoS attacks of allegedly Russian origin were reported.



Cyberwarfare specialists of the United States Army's 782nd Military Intelligence Battalion (Cyber) supporting the 3rd Brigade Combat Team, 1st Cavalry Division during a training exercise in 2019. Photo via Wikimedia Commons. [Public domain.]

The US government is a frequent target of less high-profile cyberattacks, and the threat appears to be growing. In 2006, the Pentagon reported around 6 million attempts to break into its computer systems. By 2008, that number had increased to 360 million. While it is not clear how serious these efforts were, or how many were successful, there have been several confirmed instances of security breaches of classified US military data as a result of cyberattacks.

A notable example of this took place in 2009, when intruders gained access to information about the military's newest aircraft development program, the \$300 billion Joint Strike Fighter project. The perpetrators—believed to be Chinese—gained access to documents describing the aircraft's design

and performance statistics, as well as its in-flight self-diagnostic routines. It was later learned that the information was accessed by hacking into the computers of the contractors who were working on the aircraft designs. While the companies insist that no classified information was obtained through the attacks because it was stored on computers not connected to the internet, the incident left many people feeling unsettled at the possibility of such high-level military security vulnerabilities.

Also in 2009, there were reports that hackers had broken into the US Air Force's air traffic control system to gain secret information about the location of US fighter jets. While it is not clear that anything was done with this information, the report again left

government officials and the general public feeling uneasy with the current level of cybersecurity in place for these sensitive systems. It was believed that these attacks originated in China, although it is difficult to determine exactly where a cyberattack originates because of the “borderless” nature of cyberspace, and the relative ease of disguising one’s true location.

Despite these highly publicized incidents, many people remained skeptical about the true level of threat the United States faced from cyberattacks. Computer security is a multibillion-dollar industry, and many contractors in the information technology

field stand to make huge amounts of money from government and corporate spending on defense of their data and file infrastructure. While such attacks do happen, critics expressed concerns that companies who stand to profit from fear mongering could be exaggerating the threat of an all-out cyberwar, in the interest of making money. Some even drew parallels to the Cold War, when the United States and the Soviet Union were involved in an expensive arms race, as each country tried to prepare itself for the attack it believed the other could launch. Skeptics then saw a shady connection between public fears and company profits.

TOP SECRET//SI//ORCON//NOFORN

SPECIAL SOURCE OPERATIONS

(TS//SI//NF)

PRISM Collection Details

Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

A large green arrow points from the 'Current Providers' list to the 'What Will You Receive in Collection' section.

What Will You Receive in Collection (Surveillance and Stored Comms)?

It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN

PRISM: a clandestine surveillance program under which the NSA collects user data from companies like Facebook and Google. Image via Wikimedia Commons. [Public domain.]

In addition, because it is so new and so rapidly evolving, US cyberwarfare doctrine has raised issues surrounding government transparency, interagency cooperation, and international law—especially regarding the offensive component of cyberwarfare. In 2008, for example, US military officials determined that a website set up by the Central Intelligence Agency (CIA) and the government of Saudi Arabia to entrap terrorists was, in fact, posing a threat to US troops in the region. Despite the objections of the CIA and the Saudis, the Department of Defense launched a cyberattack that disabled the website, which it said was helping rather than hindering terrorist activity. The attack disrupted servers in Saudi Arabia, Germany, and Texas, raising yet another issue in cyberwarfare: the difficulty of restricting the damage of an attack to the intended target.

President Barack Obama was a strong supporter of efforts to secure computer infrastructure against cyberattacks. For him, the issue was personal: his campaign website was hacked in 2008, and intruders gained access to emails, travel records, and other important documents.

In 2009, a new military command was established, the United States Cyber Command (USCYBERCOM), with the mission of protecting US military computer networks and disrupting enemy actions in cyberspace. Cyber Command, which became fully operational in May 2010, was expected to refine US cyberwarfare doctrine and policy guiding operations such as the one in Saudi Arabia in 2008.

Cyber Command was exclusively tasked with military operations, while the defense of US civilian information infrastructure remained the job of the Department of Homeland Security (DHS). In 2008 the DHS established the National Cybersecurity Center, charged with protecting US government communication and information networks. Also under the DHS was the slightly broader National

Cyber Security Division. In 2013, leaks from whistleblower Edward Snowden began to reveal the cyberwarfare operations of US government organizations, including the CIA and National Security Agency (NSA).

OVERVIEW

Throughout the 2000s and 2010s, numerous US companies faced cyberattacks. Some large-scale actions were linked to foreign intelligence services and therefore represented cyberwarfare. In November 2014 the Sony Pictures film studio was hacked and large amounts of private data was released, and the group responsible called for Sony to cancel the release of the film *The Interview*, which featured a plot revolving around an attempt to assassinate dictator Kim Jong-un of North Korea. Security experts suggested the attack indeed was supported by North Korea, although the country denied any involvement. Other companies that faced massive hacking attacks included PayPal and Twitter (later known as X). The US government was also directly targeted, with one notable instance coming in 2015, when the US Office of Personnel Management (OPM) was compromised and over 21 million personal records were obtained by hackers. The stolen information included social security numbers, names, and addresses.

National cybersecurity once again made headlines in 2016, when the US intelligence community found that the Russian government used various methods to interfere in the 2016 US presidential election campaign, with the intention of favoring Republican candidate Donald Trump. Allegations focused on the fact that the computer systems of the Democratic National Committee (DNC) were hacked and many private emails and other information was released that damaged the reputation of top Democratic Party officials, while no Republican records were leaked. The story dominated election coverage late in the campaign and, according to many reports,

undermined public trust in Democratic candidate Hillary Clinton and other Democratic leaders. Other factors that damaged the Clinton campaign, such as the proliferation of fake news stories and conspiracy theories, would also later be linked to foreign cyberespionage activity.

After Clinton narrowly lost the election to Trump in the Electoral College, many US intelligence experts expressed concern that Russia deliberately used hacks, leaked information, and disinformation to influence American politics. In an example of credible deterrence, before leaving office, President Obama initiated new sanctions against Russia in response to reports from the DHS and the US director of national intelligence that directly accused Russia of election tampering. Because of the 2017–19 investigation by Special Counsel Robert Mueller, several of Trump's associates were indicted and found guilty of a range of charges. In February 2018 a federal grand jury indicted the Russian government's propaganda organization, the Internet Research Agency, two other firms, and more than a dozen Russians on charges of election tampering. That same month, the United States and the United Kingdom blamed Russia for what became known as the NotPetya malware attack, which the US Treasury Department characterized as "the most destructive and costly cyber-attack in history," as quoted by Caroline Cournoyer for *Governing* magazine in 2018. In March 2018 the Trump administration sanctioned nineteen Russian organizations and individuals for 2016 election interference and other cyberattacks targeting the US electrical grid and water supply. On July 13 of that year, twelve Russian military intelligence officers were indicted by a federal grand jury for hacking Democratic Party networks and releasing documents—charges that Russia denied.

In mid-2019 the US Cyber Command reportedly infiltrated Russian electrical utilities and implanted

potentially disruptive malware as a way to deter Russian hackers from waging further cyberattacks on the United States. The US Cyber Command had also conducted cyberattacks against an Iranian intelligence organization that US officials suspected was responsible for planning attacks against US oil tankers.

In December 2020 hackers supported by a foreign government breached the US Treasury Department and the Commerce Department's National Telecommunications and Information Administration. Trump's secretary of state, Michael Pompeo, announced that the cyberattackers were Russians who had embedded SolarWinds' network-management software with a code that allowed access to the networks and technology systems of at least one hundred private companies as well as state agencies, and at least nine federal government agencies in the United States, including the US nuclear weapons agency and the Pentagon. Trump, however, declined to impose further sanctions on Russia in the waning days of his presidency. In February 2021, the administration of President Joe Biden pledged to investigate the SolarWinds breach and respond accordingly. The Biden administration subsequently blamed Russia for the hack and in April of that year issued an executive order imposing sanctions on the country. In October of 2023, the US Security and Exchange Commission (SEC) filed a lawsuit against SolarWinds, which the SEC accused of failing to disclose its cybersecurity vulnerabilities in key documents prior to the breach.

Given that the number of cyberattacks grew throughout the 2000s and 2010s, the debate around cyberwarfare has shifted accordingly from whether or not such attacks constitute a real and present danger to how the United States could and should engage in cyberwarfare. Some contend that an offensive strategy could be an effective deterrent to would-be attackers and a useful tool for pursuing

foreign-policy objectives, while others argue for a defensive strategy that seeks to protect the nation's infrastructure first and foremost.

—Tracy M. DiLascio

Further Reading

- Barnes, Julian E., and Thomas Gibbons-Neff. "U.S. Carried Out Cyberattacks on Iran." *New York Times*, 22 June 2019, www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html.
- Bennett, Brian, and Chris Megerian. "U.S. Sanctions Russians for Cyberattacks on Power Grid and Election Meddling." *Governing*, 16 Mar. 2018, www.governing.com/archive/tns-russia-water-electric-energy-grid-cyber.html.
- Bing, Christopher. "REFILE-EXCLUSIVE-U.S. Treasury Breached by Hackers Backed by Foreign Government—Sources." *Reuters*, 13 Dec. 2020, www.reuters.com/article/usa-cyber-treasury-idUSKBN2IT0I8.
- Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. HarperCollins, 2010.
- Danks, David, and Joseph H. Danks. "The Moral Permissibility of Automated Responses during Cyberwarfare." *Journal of Military Ethics*, vol. 12, no. 1, 2013, pp. 18–33.
- Fung, Brian. "Biden Administration Says Investigation into SolarWinds Hack Is Likely to Take 'Several Months.'" *CNN Politics*, 17 Feb. 2021, www.cnn.com/2021/02/17/politics/solarwinds-hack-investigation/index.html.
- Gorman, Siobhan, August Cole, and Yochi Dreazen. "Computer Spies Breach Fighter-Jet Project." *Wall Street Journal*, 21 Apr. 2009, online.wsj.com/article/SB124027491029837401.html.
- Liff, Adam P. "Cyberwar: A New 'Absolute Weapons'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *Journal of Strategic Studies*, vol. 35, no. 3, 2012, pp. 401–28.
- Morozov, Evgeny. "Battling the Cyber Warmongers." *Wall Street Journal Dow Jones*, 8 May 2010, online.wsj.com/article/SB10001424052748704370704575228653351323986.html.
- Morrison, Sara. "Biden Makes Good on His Promise to Punish Russia for the Massive SolarWinds Hack." *Vox*,

15 Apr. 2021, www.vox.com/recode/22385555/biden-solarwinds-hack-russia-sanctions.

Nakashima, Ellen. "Dismantling of Saudi-CIA Web Site Illustrates Need for Clearer Cyberwar Policies." *Washington Post*, 19 Mar. 2010, www.washingtonpost.com/wp-dyn/content/article/2010/03/18/AR2010031805464%5Fpf.html.

Nance, Malcolm. *The Plot to Hack America: How Putin's Cyberspies and WikiLeaks Tried to Steal the 2016 Election*. Skyhorse Publishing, 2016.

Prentice, Chris, Jonathan Stempel, and Raphael Satter. "US SEC Sues SolarWinds for Concealing Cyber Risks before Massive Hacking." *Reuters*, 30 Oct. 2023, www.reuters.com/legal/us-sues-solarwinds-court-records-2023-10-30.

"Security Software—Statistics & Facts." *Statista*, 7 July 2023, www.statista.com/topics/2208/security-software.

"Wanted: Global Rules on Cyberwarfare." *Christian Science Monitor*, 19 Feb. 2013, www.csmonitor.com/Commentary/the-monitors-view/2013/0219/Wanted-global-rules-on-cyberwarfare.

Weinberger, Sharon. "Computer Security: Is This the Start of Cyberwarfare?" *Nature*, 9 June 2011, www.nature.com/articles/474142a.

CYBERWEAPON

ABSTRACT

In cybersecurity and national defense, a cyberweapon is broadly defined as any type of malware or malicious computer code capable of stealing highly valuable or sensitive data or causing harm or disruption on a mass scale. Narrower definitions describe cyberweapons as computer code specifically designed to cause or threaten physical, mental, economic, or functional harm to structures, institutions, systems, or living beings, especially by targeting critical infrastructure or the data it contains to impede, alter, or interrupt its normal operating capacity. Cyberweapons are an area of increasing military focus, as they can be used in coordination with more conventional tactics to achieve a broader range of potential objectives regarding attacking, neutralizing, or disadvantaging an adversary.

BACKGROUND

The early years of the commercial internet were marked by multiple examples of viruses and other forms of malware that circulated on a mass scale and inflicted major economic damage. One such incident, which is often described as the worst computer virus attack in internet history, occurred in 2004 and involved malware known as Mydoom. The Mydoom worm infected email systems, using email as a platform for spreading itself and linking infected computers to a centralized network used to carry out distributed denial of service (DDoS) cyberattacks. At its peak, the Mydoom worm was responsible for an estimated 25 percent of all email sent worldwide, and analysts have placed its financial toll at \$38 billion, or about \$54 billion when adjusted for inflation into 2020 dollars.

While this style of attack was common during the initial stages of internet history, the people responsible for such attacks often lacked tangible goals or objectives beyond causing chaos. As the 2000s continued, both state and nonstate actors began to recognize the growing potential and possible strategic utility of cyberweapons as repositories of sensitive, classified, and valuable information became increasingly digitized, and as critical infrastructure systems such as electrical grids and energy pipelines migrated online at accelerating rates.

Observers often cite the 2010 Stuxnet incident as the first example of a cyberweapon being deployed with the specific intent of causing physical damage. Stuxnet, which is believed to have been developed through the cooperative efforts of the United States and Israel, targeted an Iranian nuclear facility with the objective of exploiting previously undetected loopholes in the Windows operating system to disable multiple nuclear systems. The worm is reported to have rendered up to one-fifth of Iran's nuclear centrifuges inoperable, thus seriously disrupting the country's suspected ongoing effort to develop nuclear weapons.

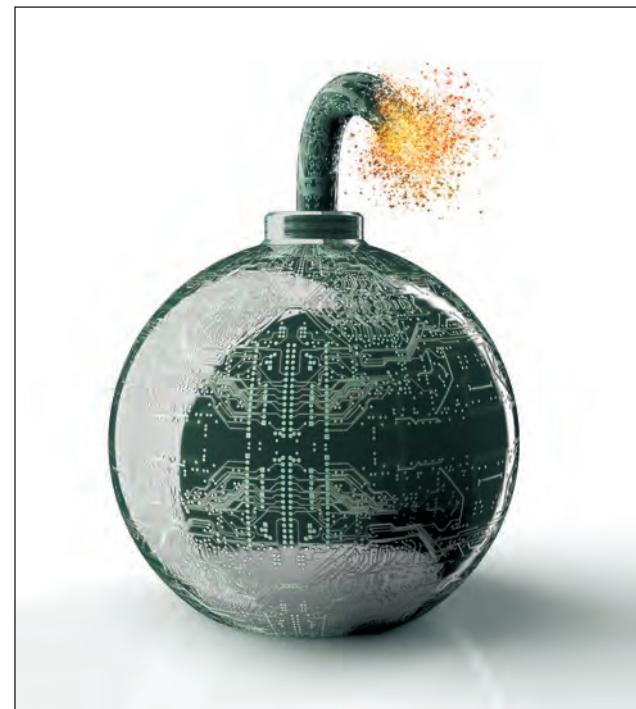


Image via iStock/posteriori. [Used under license.]

In March 2014, Russia launched a massive DDoS attack in Ukraine, which had the effect of disabling internet access across Ukraine as Russian-backed rebels were engaged in an active military effort to take control of the Crimean Peninsula, which was Ukrainian territory at the time. Analysts state that the attack was at least thirty-two times more powerful than the largest-known DDoS attack in internet history to that point. Two months later, suspected Russian cyber operatives launched another targeted cyberattack on online Ukrainian election infrastructure as the country's voters prepared to cast their ballots in a presidential election.

The NotPetya incident, which began in June 2017, has been described as the first large-scale example of ransomware being used as a cyberweapon. Originating from within Ukraine, the NotPetya ransomware quickly established a global footprint. It was disguised as ransomware, which is a type of malware in which cyberattackers seize a

network, a computer, or digital files before attempting to extort the owner into paying a ransom to secure the safe release of their property. However, NotPetya's actual goal was to destroy infected files. It caused damages estimated at approximately ten-billion dollars, with a 2018 assessment by the United Kingdom's National Cyber Security Center concluding that the incident was almost certainly the work of the Russian military.

In May 2021, a coordinated ransomware attack infected some of the online systems used by Colonial Pipeline to distribute oil from refineries to consumer markets. The attack shut down multiple oil pipelines for several days, resulting in localized energy and gasoline shortages. At the time, the Colonial Pipeline incident was the largest cyberattack on US critical infrastructure ever disclosed to the public, with the event highlighting the growing capabilities of nonstate actors to engage in the development and use of cyberweapons. A hacking collective known as DarkSide claimed responsibility for the attack and succeeded in extorting payments from Colonial Pipeline to secure the release of affected digital assets.

OVERVIEW

Experts use varying systems to classify cyberweapons and their capabilities. One model categorizes cyberweapons according to their purpose, grouping them as offensive, defensive, and dual-use cyberweapons. Offensive cyberweapons are used to initiate attacks intended to cause harm or damage on a mass scale, while defensive cyberweapons are exclusively reserved for preventing or responding to such attacks. Dual-use weapons have both offensive and defensive capabilities.

An alternative model describes cyberweapons in terms of their capabilities across four key areas including precision, intrusion, visibility, and ease of implementation. The precision factor relates to a cyberweapon's ability to target a specific system or

asset or carry out a single objective. Cyberweapons with higher levels of precision reduce or eliminate collateral damage to unrelated systems or assets, with those with lower levels of precision have a greater likelihood of spreading beyond their intended target(s).

Intrusion describes the level to which the weapon can penetrate its intended target. More intrusive cyberweapons have greater potential to cause damage but are also more readily detectable. Less intrusive cyberweapons tend to have lower ceilings with respect to damage potential but are also more likely to remain undetected for longer periods of time. The concept of intrusion is closely related to visibility, which exclusively considers the cyberweapon's ability to evade cybersecurity defenses. Cyberweapons with high levels of intrusion but low levels of visibility are considered particularly difficult to develop but have a highly desirable utility profile.

Ease of implementation considers cyberweapons in the context of the resources required to develop them. Resource-intensive cyberweapons are more likely to offer appealing capabilities but carry significant risks. They could potentially be neutralized by adversaries, resulting in the loss of the financial, human, and digital resources that were committed to the weapon's development. Less resource-intensive weapons have considerable appeal but often carry limited utility or functionality compared to their more elaborate counterparts.

Cyberweapons take many forms, but most harness principles similar to those used by hackers and other malicious actors when creating computer worms, viruses, trojans, spyware, and other forms of malware. Cyberweapons attack targets using three main modes of action: destroying targeted files or systems; conducting espionage and collecting information; and carrying out acts of physical sabotage. The Pegasus spyware platform, described in a 2022 *New York Times* article as the most powerful cyberweapon in the world, is an

information-collecting system reportedly capable of decoding encrypted communications sent or received by virtually any iOS- or Android-powered smartphone.

Experts note that cyberweapons are particularly appealing to state actors because they offer “plausible deniability,” a term used in political science and diplomacy to describe a situation in which a government or its senior members can credibly deny knowledge of or involvement in a hostile act. For example, a country’s political leadership might claim that a particular cyberattack was perpetrated by a rogue actor or underground hacking group when it was really carried out by military or intelligence assets. Plausible deniability allows countries to carry out overtly hostile acts on rivals or adversaries while also shielding themselves from accountability or direct retaliation. Cybersecurity and cyberwarfare experts also note that cyberweapons are increasingly being used as a supplementary or an adjunct tool alongside conventional military capabilities. In these contexts, cyberweapons can be used to disable or disrupt an adversary’s defenses or critical infrastructure, facilitate stealth and quick-strike attacks, and to gain intelligence about an opponent’s capabilities prior to launching wider attacks.

Common cyberweapon targets include electronic and online national defense and military systems, hospitals, and the digital infrastructure controlling water supplies, electricity management systems, industrial systems, and transportation systems. Despite their destructive capabilities, cyberweapons also display significant limitations. They inherently have limited life spans, as they are always designed to exploit specific weaknesses or vulnerabilities that can be remedied once they have been identified. Upon using cyberweapons, perpetrators may provide their targets with the information needed to reverse-engineer similar weapons for potential retaliatory use. State actors may also be reluctant to use

certain particularly unpredictable cyberweapons, as these weapons may carry a risk of inflicting unintended damage on the host country’s systems and online assets.

Experts estimate that at least one-hundred forty countries are actively developing cyberweapons. According to the National Cyber Power Index 2022, published by the Belfer Center for Science and International Affairs at Harvard University, the ten countries with the most advanced cyber capabilities include the United States, China, Russia, the United Kingdom, Australia, the Netherlands, South Korea, Vietnam, France, and Iran.

—Jim Greene

Further Reading

- Bergman, Ronen, and Mark Mazzetti. “The Battle for the World’s Most Powerful Cyberweapon.” *New York Times*, 31 Jan. 2022, www.nytimes.com/2022/01/28/magazine/nsa-group-israel-spyware.html.
- “Cyber Weapon.” *Australian Cyber Security Institute*, www.cyber.gov.au/acsc/view-all-content/glossary/cyber-weapon.
- Gerencer, Tom. “The Top 10 Worst Computer Viruses in History.” *Hewlett-Packard*, 4 Nov. 2020, www.hp.com/us-en/shop/tech-takes/top-ten-worst-computer-viruses-in-history.
- Halpern, Sue. “How Cyber Weapons Are Changing the Landscape of Modern Warfare.” *New Yorker*, 18 July 2019, www.newyorker.com/tech/annals-of-technology/how-cyber-weapons-are-changing-the-landscape-of-modern-warfare.
- Orr, Trystan. “A Brief History of Cyberwarfare.” *GRA Quantum*, 1 Nov. 2018, graquantum.com/a-brief-history-of-cyberwarfare.
- Van Wie Davis, Elizabeth. *Cyberwar Policy in the United States, Russia, and China*. Rowman & Littlefield, 2021.
- Voo, Julia, Irfan Hemani, and Daniel Cassidy. “National Cyber Power Index 2022.” *Belfer Center for Science and International Affairs*, Sept. 2022, www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf.

D

DARK WEB

ABSTRACT

As the name suggests, the term “dark web” refers to a section of the internet that is not easily seen. People using the most common software tools and browsers to search or conduct business on the internet do not normally encounter the dark web. Although news accounts focus on the dark web’s sinister aspects and controversial sites, of which there are many, some uses of and sites on this area of the internet do not fit that description. Since communications undertaken on the dark web are not easily intercepted by any person, company, or government (hence, its use as a venue for illegal activities), any individual, government, or group not wanting others to have easy access to their communications can make use of the dark web. In addition to the dark web’s common use for illegal commerce, it is also used for political ends by terrorist, revolutionary, and opposition groups desiring to evade governmental restrictions. Ironically, the initial development of many dark web tools was for all diplomatic, military, and other governmental security forces to have a secure form of electronic communication.

BACKGROUND

In the mid-1960s the first long-distance, two-computer network allowed digital communications between the machines via normal telephone wires. As what eventually became known as the internet grew, advances in both the hardware and software used in the system began to allow a virtually unlimited number of computers to communicate via the web. Early in this process it was recognized that not all information should be available to every computer and user, resulting in systems of encryption

being developed and put into use in the 1970s. Originally established to secure military and civilian governmental data and computer systems, private companies expanded their computer networks and needed to secure their data as well. The spread of encryption was the foundation for what is called the deep web: sites and information not available to the general user. (It is estimated that significantly less than ten percent of the World Wide Web is visible to internet users via popular browsers or search engines.) Encryption of the deep web is the foundation for internet commerce, as the encryption keeps data, such as credit card numbers, safe from those seeking to steal this type of information. However, given the type of encryption and security necessary for commerce and deep web communication, it was only a small step to strengthen the encryption and bury sites deeper, to create the dark web.

The dark web is generally seen as beginning in the 1990s with not only the explosion of internet availability and usage but also the development of new, relatively easy-to-use, free programs for the encryption and decryption of data. The two major systems/programs developed during the 1990s were Freenet and The Onion Router (TOR). Freenet was established as an alternative to the mainstream internet, as an attempt to allow uncensored, private communication among its users. The amount of security and anonymity one has depends on whether one uses the open or the darknet mode, with the latter being the most secure. For many ordinary purposes, the separation from other, larger sections of the internet makes this mode less useful, yet many users find that it meets certain needs. Nevertheless, bridges to the mainstream internet have been

developed, and these tend to negate much of the security available using Freenet.

TOR was developed by the US Navy as a means for secure communication, with it becoming available to the general public in the early twenty-first century, although still partially funded by the American and Swedish governments. TOR can work within the general internet, but it strengthens its encryption by sending information through several routers/relays that encrypt/decrypt the information several times before it reaches the desired destination. Having multiple layers of encryption (hence, the onion analogy in its name) makes breaking the security of any given transmission through the system, as well as finding the physical location of the sender, extremely difficult. In addition to the network aspects of TOR, it can be used to create generally inaccessible websites that have a .onion suffix, which can only be reached using the TOR browser.

In subsequent years, I2P gained popularity among those attempting to avoid government

surveillance, especially in light of some governmental success against selected TOR dark websites and malware released into the system. As with TOR, I2P uses multiple intermediary points where the information is encrypted and decrypted, making it difficult to intercept or locate the origin of the information. While the general internet can be reached using I2P, some functions such as email are secure only when sent between two computers that are both running I2P. As with TOR, I2P has its own section of the internet that uses the .i2p suffix.

OVERVIEW

Although most people do not think too much about it, general use of the internet results in records to which government agencies, as well as internet providers, browser owners, and operators of search engines, have access. Thus, there is a small segment of people obsessed with privacy who go to the extreme of using the dark web for what most people would see as mundane purposes. They are not



Image via iStock/thomaguerry. [Used under license.]

intentionally using the web for any illegitimate or illegal purposes; they only want complete privacy, if possible, when accessing the internet. Such users make up a relatively small portion of dark web users, yet they often complain loudly when any government or international action is contemplated regarding possible dark web restrictions.

While the deep web is an area in which many secretive yet legitimate/legal communication/data files are located, the dark web appeals to those seeking even greater security along with those seeking to conduct illicit activities. The main purpose for which the US Navy developed TOR, namely, secure communications between government entities, still exists; secure electronic communications between people in Washington, D.C., and various agents of the government, whether military or civilian, is still needed and conducted on part of the dark web. Additionally, some private commercial interests have similar needs and make use of the dark web for these purposes.

Reliable statistics regarding dark web usage do not exist, and yet many experts agree that illegal, or at least illicit, activities seem to be its greatest use. This would principally be divided between politics and commerce, although there is an overlap on sites dealing with weapons or weapon technology. Terrorist groups and other extremist organizations make extensive use of the dark web for internal communications as well as recruitment. While obviously a recruitment ad on a general internet site would reach more people, it would quickly be shut down and the site owner located with relative ease. Thus, in addition to coded ads on the general internet, these organizations make more explicit information available to individuals drawn to their message on the dark web.

Dark web commerce incorporates all manner of illegal product and service offerings. Illegal drugs, almost any type of gun or tactical weapon, illegal

forms of pornography, stolen goods (including numbers for credit cards, banks, or the totality of a person's identification), and other things that require the transaction being outside government surveillance are found on the dark web. Services that must be discreetly arranged, whether sexual or a wide range of illegal or violent acts, are found on dark web sites. The first iteration of Silk Road, one of the earliest large-scale dark web marketplaces, ran for about two years. It has been estimated that over \$1 billion passed through the site during this period. Numerous other sites, large and small, also operated during this time, with an unknown amount of money changing hands.

In addition to encryption techniques and basic legal protections such as the right to privacy, the development that has done the most to boost dark web commerce is the reliance on cryptocurrencies such as Bitcoin. As with many other things associated with the dark web, cryptocurrencies are not illegal, but they do make illegal transactions easier. Bitcoins, and other cryptocurrencies, can be transferred in such a manner as to conceal the identity of the sender, thus making it ideal for dark web transactions. Using markets like Silk Road has proved beneficial to both buyers and sellers, in that the market acts as a kind of intermediary entity that holds the cryptocurrency and guarantees to the seller that adequate funds are available, and then sends it to the seller once the buyer has acknowledged that the goods or service has been delivered.

Although efforts by a variety of law enforcement agencies around the world have diminished the illegal activities occurring on the dark web in recent years, human ingenuity has allowed many criminal entrepreneurs to transform their operations and continue exploiting the less well-known recesses of the internet.

—Donald A. Watt, Nathan A. B. Watt

Further Reading

- Choudhury, Saheli Roy, and Arjun Kharpal. "The 'Deep Web' May Be 500 Times Bigger than the Normal Web. Its Uses Go Well beyond Buying Drugs." *CNBC*, 6 Sept. 2018, www.cnbc.com/2018/09/06/beyond-the-valley-understanding-the-mysteries-of-the-dark-web.html.
- Gehl, Robert W. *Weaving the Dark Web: Legitimacy on Freenet, Tor, and I2P*. MIT Press, 2018.
- Guccione, Darren. "What Is the Dark Web? How to Access It and What You'll Find." *CSO*, 1 July 2021, www.csionline.com/article/564313/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html.
- Patterson, Dan. "Dark Web: A Cheat Sheet for Business Professionals." *TechRepublic*, 26 Oct. 2018, www.techrepublic.com/article/dark-web-the-smart-persons-guide.
- Porolli, Matías. "Cybercrime Black Markets: Dark Web Services and Their Prices." *Welivesecurity by eset*, 31 Jan. 2019, welivesecurity.com/2019/01/31/cybercrime-black-markets-dark-web-services-and-prices.
- Retzkin, Sion. *Hands-On Dark Web Analysis: Learn What Goes on in the Dark Web, and How to Work with It*. Packt, 2018.

DATA BREACH

ABSTRACT

A data breach occurs when sensitive or confidential information is stolen or accessed by an unauthorized individual, group, or software program. In most cases, the information involved in a data breach is personal information, such as home addresses, Social Security numbers, or credit card numbers. Data breaches may also involve personal health information or business trade secrets. Most modern data breaches are executed through computer technology; however, a breach may also occur if the information is physically lost or simply viewed by an unauthorized individual. During the first three decades of the twenty-first century, multiple notable companies fell victim to data breaches. Among the largest were incidents involving the retailer Target, the credit reporting agency Equifax, and the online service provider Yahoo!.

BACKGROUND

Because most modern information is stored on computer systems, many data breaches occur through hacking intrusions or malware. Hacking refers to the unauthorized access of a computer system. Malware—short for malicious software—is a program designed to infiltrate and spread through a computer or network. Another potential cause of a data breach is the loss or theft of a portable device that contains sensitive information. Other causes include the unintended disclosure of data, information leaks from an inside source, or information stolen through payment card fraud, such as through the use of a credit card skimming device.

Hackers intending to break into a specific computer network generally follow a pattern to gain access. They first analyze their target, looking for weaknesses in its computer network, employees, and security practices. This phase often lasts weeks or months until the attacker is familiar with the target. The next step is to gain access to the network, usually by injecting harmful code into a system, infecting emails, or by tricking a person into revealing usernames and passwords.

Once inside the system, an attacker tries to establish a presence, gaining additional access and searching for vulnerabilities. Attackers rarely enter a system with full access. They must move around within the network until they find what they are looking for. When they gain access to the sensitive data they are searching for, the attackers remove it and quickly leave. If steps are not taken to close down the pathway to the data, an attacker can exploit the entry point to gain future access to the data.

The majority of data stolen in a breach is personally identifiable information (PII). PII is data that can be used to personally identify an individual. It can range from nonsensitive information, such as names and addresses found in a phone book, to highly sensitive information, such as Social Security

numbers. Another prime target of a data breach is financial information, such as bank account numbers and credit card numbers. Hackers also go after a person's protected health information (PHI), the privacy of which is guaranteed by federal law. PHI may include personal health data, medical test results, and insurance information. Businesses are at risk of having their trade secrets and intellectual property stolen in a data breach. For example, the cable and satellite television network HBO had several episodes of its popular series *Game of Thrones* stolen in a 2017 breach.

OVERVIEW

Data breaches have occurred for many years but began to increase in the 1980s and 1990s amid rapid advancements in computer technology. Modern companies budget a significant amount of money to protect themselves, but hackers often find ways to exploit security weaknesses and gain access to data. Statistics on data breaches have only been compiled since the early twenty-first century, but in that time, several high-profile companies have been the victim of hackers.

In 2013, the retail giant Target announced that the personal information of millions of customers had been stolen in a breach. Hackers gained entry to the system through a third-party heating and air-conditioning contractor used by Target. The attack occurred before Thanksgiving and was not discovered until weeks later. Months after the attack, Target said the hackers had accessed the credit and debit card numbers of 110 million people.

In 2017, hackers gained access to the personal information of about 143 million customers of the credit reporting bureau Equifax. Among the data stolen were Social Security numbers, birth dates, addresses, and driver's license numbers; about 209,000 people had their credit card information stolen.

The online auction company eBay reported a data breach in 2014 that accessed the names, addresses, birthdays, and passwords of all of its 145 million users. The company said the hackers gained access using the credentials of three eBay employees.

In 2016, the FriendFinder Network, an online site that specializes in adult entertainment, was the victim of a data breach that affected more than 412 million people. Hackers gained access to twenty years' worth of customer email addresses, personal addresses, and passwords.

A particularly large data breach took place via two attacks on the online service provider Yahoo! in 2013 and 2014. The company first announced in 2016 that the names, email addresses, dates of birth, and telephone numbers of 500 million users had been stolen in a 2014 attack. The passwords for most of those users were compromised as well. The company called the attack a "state sponsored" incident, meaning officials believed a foreign nation was behind the intrusion. Later in 2016, Yahoo! announced that an earlier attack in 2013 had accessed the personal information of more than one billion accounts. This attack was initiated by a different group than the 2014 incident. In 2017, Yahoo! revised its estimates, saying that the accounts of all three billion of its users had been compromised. Names, email addresses, and passwords were also stolen in the 2013 attack, as were personal security questions and their answers.

While businesses and institutions became increasingly aware of the risks and ramifications of data breaches during the second decade of the twenty-first century, prominent organizations continued to experience them. In 2018, for instance, the Marriott hotel chain experienced a data breach in which more than 380 million guest records were accessed by hackers. The company went on to face further data breaches in 2020 and 2022. A number of other prominent companies also experienced

significant data breaches during the early 2020s, the cellular service provider T-Mobile among them.

—Richard Sheposeh

Further Reading

- “Data Breach.” *Trend Micro*, www.trendmicro.com/vinfo/us/security/definition/data-breach.
- “Data Breach Chronology.” *Privacy Rights Clearinghouse*, www.privacyrights.org/data-breaches.
- “Data Breaches 101: How They Happen, What Gets Stolen, and Where It All Goes.” *Trend Micro*, 10 Aug. 2018, www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101.
- Faife, Corin. “The Marriott Hotel Chain Has Been Hit by Another Data Breach.” *The Verge*, 6 July 2022, www.theverge.com/2022/7/6/23196805/marriott-hotels-maryland-data-breach-credit-cards.
- Fowler, Kevvie. *Data Breach Preparation and Response: Breaches Are Certain, Impact Is Not*. Syngress, 2016.
- Hill, Michael, and Dan Swinhoe. “The 15 Biggest Data Breaches of the 21st Century.” *CSO*, 8 Nov. 2022, www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html.
- “Rules and Policies—Protecting PII—Privacy Act.” *General Services Administration*, 11 Aug. 2023, www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act.
- Singletary, Michelle. “Yahoo. Target. Equifax. Sonic: All Category 5 Data Breaches. Is Your Information Safe Anymore?” *Washington Post*, 5 Oct. 2017, www.washingtonpost.com/news/get-there/wp/2017/10/05/yahoo-target-equifax-sonic-all-category-5-data-breaches-is-your-information-safe-anymore/?utm_term=.1ef401a8f845.
- Weatherbed, Jess. “T-Mobile Discloses Its Second Data Breach So Far This Year.” *The Verge*, 2 May 2023, www.theverge.com/2023/5/2/23707894/tmobile-data-breach-april-personal-data-pin-hack-security.

DATA HARVESTING

ABSTRACT

Data harvesting (also known as web harvesting, data scraping, data aggregation, or data mining) is the process

of digitally compiling large amounts of information such as search results, purchasing preferences, commercial offerings, product prices, and demographic data from the internet. Data harvesting is usually done through the use of robots known as web harvesters or screen scrapers that collect data, filter inappropriate content, and present it to consumers in easy-to-use formats, such as graphs, tables, and indexes.

BACKGROUND

Businesses, banks, credit card bureaus, and even certain public-sector agencies often hire experts to design sophisticated web harvesters to collect data that is hard to retrieve manually. Indeed, most web harvesters can translate various computer languages, such as hypertext markup language (HTML), JavaScript, and PHP: Hypertext Preprocessor (PHP), among others.

Experts at web harvesting are highly sought after by businesses because they can engage in data collection and data translation at warp speeds. Most web harvesters can retrieve several pages on a server simultaneously and can automatically access target websites repeatedly throughout the day. As such, web harvesting allows businesses to create reports, presentations, and profiles about individuals and groups of consumers quickly.

Because many web harvesters are quite inexpensive and can be accessed easily through a basic internet search, many individuals engage in web harvesting as well. The use of web harvesters has recently grown so much that internet users frequently interact with harvesters without even knowing that they are doing so. Common examples of web harvesters that consumers frequently come into contact with include search engines, business advertisers, auction compilers, price aggregators, real estate listing services, financial data aggregators, financial money management applications, and social media websites. The websites that are targeted

by web harvesting are usually referred to as data hosts.

OVERVIEW

Whether web harvesting is a socially beneficial or harmful activity often depends on the collateral damage that the web harvester causes to a data host. For example, certain web harvesters, such as price amalgamators and targeted advertisers, cause minimal or no damage to data hosts and allow businesses to match consumer needs with commercial offerings efficiently. In fact, web harvesters such as price amalgamators and targeted advertisers often benefit both consumers and data hosts because, in addition to causing the data hosts at most minimal harm, they increase the visibility of the data hosts' products and services.

Another example of a web harvester that internet users frequently interact with is a search engine. These web harvesters are almost universally lauded for the benefits they provide to end users through constant accessing of thousands of websites, pulling bits of information from these websites, and presenting the data in the form of easily readable search engine results. Search engines are also particularly useful web harvesters because they can collect archived data that is stored on a system but that can no longer be accessed due to the incompatibility of an old system or internet website with newer computer hardware or software.

On the other hand, web harvesting can also cause extensive damage to data hosts. If a web harvester is designed to overcome a technical barrier such as a password or other code barrier, the web harvester may end up undercutting a competing business's revenue, gaining access to confidential company information, or damaging the physical infrastructure of the data host. Indeed, some web harvesting has caused data hosts to suffer extensive damage, such as increased bandwidth usage, system crashes, the need to purchase antispam devices, the need to

erect technical barriers, the need to clear up consumer confusion, and damage to reputation.

Because of some of the negative effects caused by web harvesting, it is not surprising that there have been many lawsuits involving web harvesting and data scraping. In addition to the prevalent use of web harvesters, a primary reason for these lawsuits is that many websites are poorly equipped to fend off web harvesting and want to deter web harvesters from gaining unfettered access to their data.

For example, in *eBay v. Bidder's Edge*, 100 F. Supp. 2d 1058 (N.D. Cal. 2000), a federal lawsuit that was litigated in Northern California in 2000, eBay complained that Bidder's Edge (BE) was unlawfully compiling eBay's auction listings and copying eBay's auction format on its own website without incurring any of the investment and operating costs that eBay incurs. eBay showed the court that it had unsuccessfully tried to block BE's data scrapers through telephonic and written communications and by trying to block BE's internet protocol (IP) addresses. The court sided with eBay and held that BE was liable for aggregating data from eBay's servers without attaining prior authorization and that BE was free-riding on the time, effort, and money that eBay had invested in its system.

A similar situation was litigated the following year in *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001). In this case, EF Cultural Travel BV (EF), a company that offered tour guides for groups of teenagers, complained that Explorica was unlawfully scraping information about EF's tour prices in order to undercut EF from the teenage tour market. The First Circuit sided with EF and approved an injunction against Explorica to prohibit further scraping that would be to EF's detriment.

During the 2016 US election, a major scandal involving data harvesting became headline news when a company named Cambridge Analytica harvested personal data from millions of people's

Facebook profiles without their knowledge or consent. The campaigns of US Senator Ted Cruz (R-TX) and presidential candidate Donald Trump both used Cambridge Analytica's data to target their campaign efforts. Eventually, Facebook chief executive officer (CEO) Mark Zuckerberg was called to testify before Congress about the compromising of the privacy rights of over 80 million users.

Facebook was once again in the news for data harvesting in 2019, when a virtual private network (VPN) app they owned, named Onavo, was revealed to actually be collecting user data rather than protecting it, which is the entire purpose of a VPN. VPNs are gateways through which users' internet traffic goes in order to protect the identity of the user. Rather than protecting the user, Onavo was used by Facebook as a source of information concerning users' web and app use habits.

Because of the ubiquity of web harvesters, and in light of the numerous benefits that they provide, it is critical for users of web harvesters to become familiar with the laws governing web harvesting. Again, many uses of web harvesting are considered harmless to data hosts and beneficial to consumers. Such uses are unlikely to lead to legal disputes. But given that some data hosts are opposed to unknown web harvesting, it is critical for users of web harvesters to know what types of web harvesting may expose them to liability. Similarly, it is important for data hosts that are opposed to web harvesting to stay abreast of the capabilities of web harvesters so that they can erect technical barriers and other sophisticated blockades to protect their data.

—Myra Din

Further Reading

Chadwick, Paul. "How Many People Had Their Data Harvested by Cambridge Analytica?" *The Guardian*, 16 Apr. 2018, www.theguardian.com/commentisfree/2018/apr/16/how-many-people-data-cambridge-analytica-facebook.

- Feldman, Brian. "Even If Facebook Stops Aggressively Collecting Data, Developers Will Still Supply It." *New York*, 22 Feb. 2019, nymag.com/intelligencer/2019/02/why-facebooks-data-collection-practice-is-so-messy.html.
- Fibbe, George H. "Screen-Scraping and Harmful Cyber-trespass after Intel." *Mercer Law Review*, vol. 55, no. 1011, 2004, pp. 1011–27.
- Gladstone, Julia Alpert. "Data Mines and Battlefields: Looking at Financial Aggregators to Understand the Legal Boundaries and Ownership Rights in the Use of Personal Data." *John Marshall Journal of Computer and Information Law*, vol. 19, no. 1, 2001, pp. 313–29.
- Hirshey, Jeffrey Kenneth. "Symbiotic Relationships: Pragmatic Acceptance of Data Scraping." *Berkeley Technical Law Journal*, vol. 29, 2014, pp. 897–927.
- Rubin, Aaron. "How Website Operators Use CFAA to Combat Data-Scraping." *Law360*, 25 Aug. 2014, www.law360.com/articles/569325.
- Wierzel, Kimberly L. "If You Can't Beat Them, Join Them: Data Aggregators and Financial Institutions." *North Carolina Banking Institute*, vol. 5, no. 1, 2001, pp. 457–83.

DATA MINING

ABSTRACT

Advances in technology in the latter half of the twentieth century led to the accumulation of massive data sets in government, business, industry, and various sciences. Extracting useful information from these large-scale data sets required new mathematical and statistical methods to model data, account for error, and handle issues like missing data values and different variable scales or measures. Data mining uses tools from statistics, machine learning, computer science, and mathematics to extract information from data, especially from large databases.

BACKGROUND

Data mining has roots in three areas: classical statistics, artificial intelligence (AI), and machine learning. In the late 1980s and early 1990s, companies that owned large databases of customer information, in particular credit card banks, wanted to explore

the potential for learning more about their customers through their transactions. The term “data mining” had been used by statisticians since the 1960s as a pejorative term to describe the undisciplined exploration of data. It was also called “data dredging” and “fishing.” However, in the 1990s, researchers and practitioners from the field of machine learning began successfully applying their algorithms to these large databases in order to discover patterns that enable businesses to make better decisions and to develop hypotheses for future investigations.

Partly to avoid the negative connotations of the data mining, researchers coined the term knowledge discovery in databases (KDD) to describe the entire process of finding useful patterns in databases, from the collection and preparation of the data to the end product of communicating the results of the analyses to others. This term gained popularity in the machine learning and AI fields, but the term “data mining” is still used by statisticians. Those who use the term KDD refer to data mining as only the specific part of the KDD process where algorithms are applied to the data. The broader interpretation will be used in this discussion.

Software programs to implement data mining emerged in the 1990s and continue to evolve today. There are open-source programs and many commercial programs that offer easy-to-use graphical user interfaces (GUIs), which can facilitate the spread of data mining practice throughout an organization.

OVERVIEW

The concepts involved in data mining are drawn from many mathematical fields, such as fuzzy sets, developed by mathematician and computer scientist Lotfi Zadeh, and genetic algorithms, based on the work of mathematicians such as Nils Barricelli. Because of the massive amounts of data processed, data mining relies heavily on computers, and

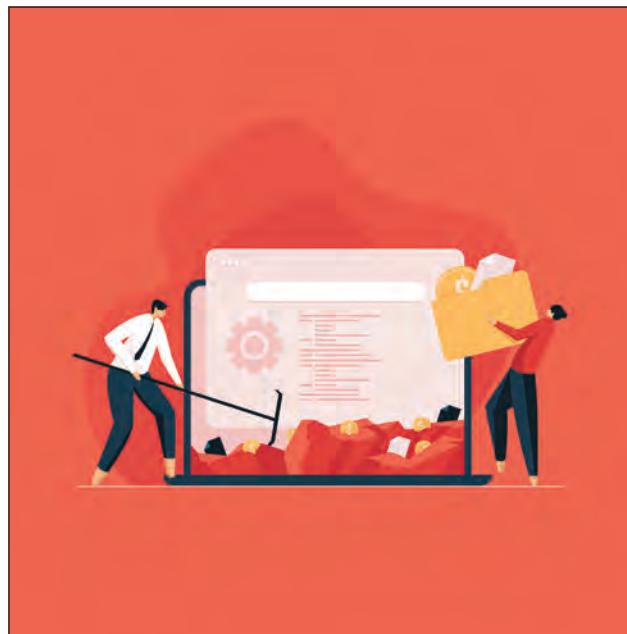


Image via iStock/uniquepixel. [Used under license.]

mathematicians contribute to the development of new algorithms and hardware systems. For example, the Gfarm Grid File System was developed in the early twenty-first century to facilitate high-performance petascale-level computing and data mining.

The specific types of tasks that data mining addresses are typically broken into four types: predictive modeling (classification, regression), segmentation (data clustering), summarization, and visualization.

Predictive modeling is the building of models for a response variable for the main purpose of predicting the value of that response under new—or future—values of the predictor variables. Predictive modeling problems, in turn, are further broken into classification problems or regression problems, depending on the nature of the response variable being predicted. If the response variable is categorical (e.g., whether a customer will switch telephone providers at the end of a subscription period or will stay with his or her current company), the problem is called a classification. If the response is

quantitative (e.g., the amount a customer will spend with the company in the next year), the problem is a “regression problem.” The term “regression” is used for these problems even when techniques other than regression are used to produce the predictions. Because there is a clear response variable, predictive modeling problems are also called supervised problems in machine learning. Sometimes there is no response variable to predict, but an analyst may want to divide customers into segments based on a variety of variables. These segments may be meaningful to the analyst, but there is no response variable to predict in order to evaluate the accuracy of the segmentation. Such problems with no specified response variable are known as unsupervised learning problems.

Summarization describes any numerical summaries of variables that are not necessarily used to model a response. For example, an analyst may want to examine the average age, income, and credit scores of a large batch of potential new customers without wanting to predict other behaviors. Any use of graphical displays for this purpose, especially those involving many variables at the same time, is called visualization.

ALGORITHMS

Data mining uses a variety of algorithms (computer code) based on mathematical equations to build models that describe the relationship between the response variable and a set of predictor variables. The algorithms are taken from statistics and machine learning literature, including such classical statistical techniques as linear regression and logistic regression and time series analysis, as well as more recently developed techniques like classification and regression trees (ID3 or C4.5 in machine learning), neural networks, naïve Bayes, K-nearest neighbor techniques, and support vector machines.

One of the challenges of data mining is to choose which algorithm to use in a particular application.

Unlike the practice in classical statistics, the data miner often builds multiple models on the same data set, using a new set of data (called the “test set”) to evaluate which model performs best.

Recent advances in data mining combine models into ensembles in an effort to collect the benefits of the constituent models. The two main ensemble methods are known as bootstrap aggregation (bagging) and boosting. Both methods build many (possibly hundreds or even thousands of) models on resampled versions of the same data set and take a (usually weighted) average (in the case of regression) or a majority vote (in the case of classification) to combine the models. The claim is that ensemble methods produce models with both less variance and less bias than individual models in a wide variety of applications. This is an area of extensive research in data mining.

APPLICATIONS

Data mining techniques are being applied everywhere there are large data sets. A number of important application areas include the following.

Customer relationship management (CRM). Credit card banks formed one of the first groups of companies to use large transactional databases in an attempt to predict and understand patterns of customer behavior. Models help banks understand acquisition, retention, and cross-selling opportunities.

Risk and collection analytics. Predicting both who is most likely to default on loans and which type of collection strategy is likely to be successful is crucial to banks.

Direct marketing. Knowing which customers are most likely to respond to direct marketing could save companies billions of dollars a year in junk mail and other related costs.

Fraud detection. Models to identify fraudulent transactions are used by banks and a variety of government agencies, including state

comptroller's offices and the Internal Revenue Service (IRS).

Terrorist detection. Data mining has been used by various government agencies in an attempt to help identify terrorist activity—although concerns of confidentiality have accompanied these uses.

Genomics and proteomics. Researchers use data mining techniques in an attempt to associate specific genes and proteins with diseases and other biological activity. This field is also known as bioinformatics.

Healthcare. Data mining is increasingly used to study efficiencies in physician decisions, pharmaceutical prescriptions, diagnostic results, and other healthcare outcomes.

CONCERNS AND CONTROVERSIES

Privacy issues are some of the main concerns of the public with respect to data mining. In fact, some kinds of data mining and discovery are illegal. There are federal and state privacy laws that protect the information of individuals. Nearly every website, credit card company, and other information collecting organization has a publicly available privacy policy. Social networking sites, such as Facebook, have been criticized for sharing and selling information about subscribers for data mining purposes. In healthcare, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted to help protect individuals' health information from being shared without their knowledge. Other regulations dealing with data privacy include the General Data Protection Regulation (GDPR), which was introduced in the European Union in 2016 and came into effect two years later.

—Richard De Veaux

Further Reading

Berry, M. A. J., and G. Linoff. *Data Mining Techniques for Marketing, Sales and Customer Support*. Wiley, 1997.

Plotkin, David. *Data Stewardship: An Actionable Guide to Effective Data Management and Data Governance*. 2nd ed., Academic Press, 2020.

Wiggins, Chris, and Matthew L. Jones. *How Data Happened: A History from the Age of Reason to the Age of Algorithms*. Norton, 2023.

Witten, Ian H., Eibe Frank, Mark A. Hall, and Christopher J. Pal. *Data Mining: Practical Machine Learning Tools and Techniques*. 4th ed., Morgan Kaufmann, 2016.

DATA PROTECTION

ABSTRACT

Originating in the 1980 Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines, data protection regimes typically include a usually wide definition of “personal information” and place a heavy emphasis on the knowledge of and/or consent to collection of personal information by the data subject. Globally, there are two broad approaches taken to protect personal information: a sectoral approach in which various legislative regimes create standards and rules in discrete areas of the economy and an alternative approach in which the collection, use, and disclosure of personal information are regulated under a single data protection regime.

BACKGROUND

The origin of comprehensive data protection regimes may be found in the 1980 Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines, the core of which was the adoption of eight fair information practice principles (FIPPS) intended to give direction to the collection, use, and disclosure of personal information. Though having jointly developed the OECD Guidelines, the United States and Europe went in two different directions regarding their applicability in the years that followed.

The United States saw them as a framework of useful guidelines that could be freely adopted by

industry if they so choose, while in Europe they were gradually strengthened and made directly enforceable. This strengthening culminated in the passage of the European Union (EU) Data Protection Directive. In one form or another, an enforceable version of the FIPPS can be found in all other modern data protection regimes, such as Canada's Personal Information & Protection of Electronic Documents Act, Hong Kong's Personal Data (Privacy) Ordinance, South Africa's Protection of Personal Information Act, and so on.

Because of this common ideological heritage, data protection regimes typically share some general features. These include a usually wide definition of "personal information" (such as any information that can lead to an identifiable individual) and of activities that count as "data processing" (both manual and automatic). Data protection regimes place a heavy emphasis on the knowledge of and/or consent to collection of personal information by the data subject and a strict limitation on the purposes to which collected information can be put. In other words, an individual must generally be informed at the time of collection of her or his information as to the purpose of the collection, and any new purpose must receive new consent.

OVERVIEW

Globally, there are two broad approaches taken to protect personal information. One may be generally described as sectoral (referring to a distinct part or area) in nature: There are various legislative regimes that create standards and rules in discrete areas of the economy. Beyond those areas, privacy protection is left purely to the free market: If people desire privacy, then they can (in theory) pay for it. Different jurisdictions regulate different areas, and at different levels of protection.

The United States, for instance, has legislated privacy protections in various areas—including, but not limited to, telecommunications, health information,

credit reporting, and websites aimed at children—but there is little consistency as to the kind of privacy protection offered in each area. Proponents of a sectoral or free-market approach argue that excessive privacy laws impose costs on business and are therefore a threat to technological innovation and economic growth.

But the sectoral model is a global outlier. Critics argue that it leaves gaps in the law and creates confusing inconsistencies. Leaving privacy protections to the free market in those gaps is ineffective since there are great disparities in bargaining power between individuals and large organizations that seek to profit off their personal information. As a result, the approach adopted by much of the rest of the world is to legislate a single data protection regime applicable to all organizations that seek to collect, use, or disclose personal information. Broad state involvement through data protection regimes is justified because privacy is understood as a human right connected to individuality, dignity, and autonomy; while there may be economic costs to robust privacy rights, they are justified because of the values at play.

THEORY AND PRACTICE

Generally speaking, under a data protection regime, *all* organizations that collect, use, or disclose personal information will be subject to the same rules; this is in clear contrast to the sectoral approach. Some jurisdictions, however, may choose to have two separate regimes for public and private organizations. Likewise, while all data protection regimes grant exemptions for data processing or collection in specified areas such as journalism, statistical research, or public security, only some may grant exemptions to all noncommercial or personal use of information. Finally, while the definition of "personal information" tends to be broad, some regimes treat certain classes of information as particularly sensitive (e.g., medical information, financial

records, and political opinions) and thus deserving of additional protections, while others do not.

Data protection regimes are also typically supervised by an independent commissioner, though the exact power of that commissioner may vary. Canada's Privacy Commissioner, for instance, lacks the power to issue fines directly to violators of the relevant law, while under the EU General Data Protection Regulation (GDPR)—adopted in 2016 and implemented in 2018—national data protection authorities are granted the power to issue sanctions to organizations found to be in noncompliance. Beyond sanctioning, other powers that may vary across regimes include the possibility of an independent lawsuit absent public complaint, compelling reporting of data breaches, strength of independence from government, and so on.

Further, shared features most data protection regimes include a right of individual access to information held about them, and the right to seek erasure or correction of information where it is incorrect. However, differing interpretations of this basic principle (drawn from the FIPPS) can be found in the recent discussion over the right to be forgotten—whether individuals can request online sources to remove information about them. Interpretation of the Data Protection Directive by the European Court of Justice has found such a right to exist.

In *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (2014), the Court found that existing provisions that granted the data subject the right to erasure of irrelevant data could support the right to be forgotten and required the well-known search engine to delete links to a news story regarding the complainant's financial difficulties from some fifteen years prior. The GDPR explicitly recognizes and expands the application of this right. In other jurisdictions, however, the prevailing argument is that as long as the information is true, forcing its deletion is incompatible with the right to free expression.

Indeed, the debate over the right to be forgotten is indicative of a new set of challenges that data protection regimes face. The FIPPS were developed in the 1970s in response to a particular set of privacy issues relevant at the time. The twenty-first century, however, is, an age of "always-on" internet-connected devices that are carried voluntarily and an economy the lifeblood of which is information. There are thus disputes about whether data protection regimes can be adapted (or need to be adapted) to respond to these changes.

—Stuart A. Hargreaves

Further Reading

- Bygrave, Lee A. *Data Privacy Law, an International Perspective*. Oxford UP, 2014.
- _____. "The Place of Privacy in Data Protection Laws." *University of New South Wales Law Journal*, vol. 24, no. 1, 2001, pp. 277–83.
- Cate, Fred. "The Changing Face of Privacy Protections in the European Union and the United States." *Indiana Law Review*, vol. 33, 1999, pp. 173–232.
- Jarmul, Katharine. *Practical Data Privacy: Enhancing Privacy and Security in Data*. O'Reilly Media, 2023.
- Koops, Bert-Jaap. "The Trouble with European Data Protection Law." *International Data Privacy Law*, vol. 4, no. 4, 2014, pp. 250–61.
- Levin, Avner, and Mary Jo Nicholson. "Privacy Law in the United States, the EU, and Canada: The Allure of the Middle Ground." *University of Ottawa Law & Technology Journal*, vol. 2, no. 2, 2005, pp. 357–95.
- Mantlero, Alessandro. "The EU Proposal for a General Data Protection Regulation and the Roots of the 'Right to Be Forgotten'." *Computer Law & Security Review*, vol. 29, no. 3, June 2013, pp. 229–35.
- Quinn, Brendan. *Data Protection Implementation Guide: A Legal, Risk and Technology Framework for the GDPR*. Wolters Kluwer, 2021.
- Raul, Alan Charles, et al. "The Privacy, Data Protection and Cybersecurity Law Review." *Sidley*, Nov. 2022, www.sidley.com/en/insights/publications/2022/11/the-privacy-data-protection-and-cybersecurity-law-review.
- Shoenberger, Allen. "Privacy Wars." *Indiana International & Comparative Law Review*, vol. 17, 2007, pp. 355–93.

Whitman, James Q. "Two Western Cultures of Privacy: Dignity versus Liberty." *Yale Law Journal*, vol. 113, no. 6, Apr. 2004, pp. 1151–221.

DATABASE

ABSTRACT

An electronic database is a collection of data used for specific purposes, stored and organized in ways that enhance rapid search and retrieval by computer. If it is a database-management system, information is retrievable in response to questions and keywords. A database will respond to metadata that is either structural or descriptive describing other data or information about data that makes searching a database quicker. Data are grouped and selected from fields to produce statistics, manage data, and create reports. Governments, businesses, banks and financial investment firms, hospitals, and charities are among the plethora of organizations collecting data and building databases to better manage their security, sales, customer service, outreach, and money collection from target markets.

BACKGROUND

A database is organized to provide information about people, places, uses, and actions. A database is generally organized into one of five types: flat, hierarchical, network, relational, and object-oriented. A flat database is the simplest format for easy and rapid access to information. A hierarchical database has data in larger categories with subcategories for detailed data retrieval with links among records at various levels. Network databases have multiple links and indicators to various records. In cases where links do not yield the data, relations are probed among records; thus, the relational database. Their development was concomitant to technological advancements in processors, computer memory, storage, and networking. Size, type, report capabilities, and overall performance were only limited by the

technology because database architecture had little trouble keeping up.

Big data collection and user companies such as Facebook, Groupon, Google, and others spirited the rapid growth of the database. Facebook (the parent company of which would later be renamed Meta) used a relational organization but moved on to build its own graph database in order to store, expand, and deliver on the relationships among people, places, and things, i.e., social networking more effectively and efficiently. Changing database architectures made it possible for Facebook to serve billions of users around the world. Universities maintain among the largest databases archiving journals, books, texts, and related materials valuable and available to researchers worldwide. Crime fighting and homeland security are among the fastest growing database uses by government and subcontractors.

A fascinating case study reported in 1993 reveals the early use of database information built by a business for targeted marketing under a US government patent. It is a method and system for target marketing infrequent shoppers from a database built from

| title | release_year | length | replacement_cost |
|-------------------------|--------------|--------|------------------|
| West Lion | 2006 | 159 | 29.99 |
| Virgin Daisy | 2006 | 179 | 29.99 |
| Uncut Suicides | 2006 | 172 | 29.99 |
| Tracy Cider | 2006 | 142 | 29.99 |
| Song Hedwig | 2006 | 165 | 29.99 |
| Slacker Liaisons | 2006 | 179 | 29.99 |
| Sassy Packer | 2006 | 154 | 29.99 |
| River Outlaw | 2006 | 149 | 29.99 |
| Right Cranes | 2006 | 153 | 29.99 |
| Quest Mussolini | 2006 | 177 | 29.99 |
| Poseidon Forever | 2006 | 159 | 29.99 |
| Loathing Legally | 2006 | 140 | 29.99 |
| Lawless Vision | 2006 | 181 | 29.99 |
| Jingle Sagebrush | 2006 | 124 | 29.99 |
| Jericho Muñan | 2006 | 171 | 29.99 |
| Japanese Run | 2006 | 135 | 29.99 |
| Gilmore Bottled | 2006 | 163 | 29.99 |
| FLOATS Garden | 2006 | 145 | 29.99 |
| Fantasia Park | 2006 | 131 | 29.99 |
| Extraordinary Conqueror | 2006 | 122 | 29.99 |
| Everyone Craft | 2006 | 163 | 29.99 |
| Dirty Ace | 2006 | 147 | 29.99 |
| Clyde Theory | 2006 | 139 | 29.99 |
| Clockwork Paradise | 2006 | 143 | 29.99 |
| Ballroom Mockingbird | 2006 | 173 | 29.99 |

(25 rows)

An SQL select statement and its result. Photo by Bernardo Sulzbach, via Wikimedia Commons.

bank check codes collected from a store's customer accounts relating to customer shopping habits. A check reader builds a database from the circuitry and terminal data collection on all transactions. It developed prior credit verification systems for check verifications. The database not only became a marketing networking system based on prior shopping history data collection system, but also enabled stores to better handle risk management to check verification.

OVERVIEW

Individual government agencies build databases. Institutions build them according to their needs. Hospitals and insurance companies build databases from electronic medical records for billing, epidemiological studies, management efficiency, savings on labor and supplies, target marketing, and other needs. Scientists use database information to tell them about all kinds of environmental changes and alterations to plant life, the universe, and the earth. Many databases are freely accessible on the internet and allow users access to legal documents, medical information, and a vast array of other data.

Security of the database is a major concern of twenty-first-century information technology (IT) specialists. Hacking has cost millions of people their privacy; companies millions of dollars in upgrading their technology fast and furiously; and banks, governments, and insurance companies billions of dollars in illegal database break-ins and stolen cash. In 2016, for instance, the Bank of Bangladesh experienced a cyber break-in that resulted in the loss of \$81 million. That year also saw media reports of an unprecedented database leak—over 11 million files—from the world's fourth biggest law firm specializing in offshore (tax evasion) accounts. The leaked files became known in the media as the Panama Papers, and their revelation

forced the prime minister of Iceland to resign and sent political shockwaves through governments elsewhere—all from a hack or leak in the firm's database.

In the years that followed, databases remained crucial to the operations of countless companies, institutions, and government agencies around the world, and their security continued to be of paramount importance. Despite efforts to improve database security measures, high-profile data breaches continued to occur. In 2023, for instance, data breaches at several different major companies exposed customer details, employee information, and other data to unauthorized users; companies that experienced data breaches during that period included the cellular service provider T-Mobile, the restaurant management company Yum! Brands, and the genetic testing company 23andMe.

—Harold Goldmeier

Further Reading

- "Database." *Encyclopaedia Britannica*, 30 June 2023, www.britannica.com/technology/database.
- Harding, Luke. "What Are the Panama Papers? A Guide to History's Biggest Data Leak." *The Guardian*, 5 Apr. 2016, www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers.
- Kabir, Arafat. "After Hackers Steal \$81 Million, What Now for Bangladesh Central Bank?" *Forbes*, 16 Mar. 2016, www.forbes.com/sites/arafatkabir/2016/03/16/after-hackers-steal-81-million-what-now-for-bangladesh-central-bank/?sh=1bbda9762156.
- Liu, Ling, and M. Tamer Özsu, editors. *Encyclopedia of Database Systems*. Springer, 2009.
- Stonebraker, Michael. "The Elephant's Dilemma: What Does the Future of Databases Really Look Like?" Interview with Colin Barker. *ZDNet.com*, 17 Apr. 2015, www.zdnet.com/article/the-elephants-dilemma-what-does-the-future-of-databases-really-look-like.
- Weatherbed, Jess. "T-Mobile Discloses Its Second Data Breach So Far This Year." *The Verge*, 2 May 2023, www.theverge.com/2023/5/2/23707894/tmobile-data-breach-april-personal-data-pin-hack-security.

DATABASE DESIGN

ABSTRACT

Database design comprises the plan, models, specifications, and instructions for creating a structure (database) where data can be stored in a permanent (persistent) manner. Users can extract that data in combinations that answer questions in a particular area (domain). Successful database design requires complete and current understanding of database technologies and methods. Further, designers must understand how people work and the types of questions a database will answer. Because of the wide variety of technical and intellectual skills that come into play, there is an ongoing debate as to whether database design is an art or a science.

OVERVIEW

Databases store data so users can access it to provide information and insights into how an organization is functioning. Electronic databases date back to the late 1950s, when they were developed for the US Department of Defense. By the 1960s databases were being designed and created for business and academic use.

In the intervening years database design has changed in response to increased computing capabilities and, just as importantly, to the changing needs of organizations and the increasingly sophisticated information expertise of potential users.

Several database design methods have come into favor over the years, resulting from an evolution in how users and designers have looked at data and how it can serve their needs. Organizations' information requirements have become larger and more complex; how people look at information and its use has also grown more sophisticated.

OVERVIEW

Variations in database design exist but methodologies generally follow a sequence of steps starting with gathering information and user requirements

through choosing the appropriate software and hardware technologies and then iterative development and testing. A six-step process defined by the University of Liverpool's Computer Science Department is typical.

The first step in the Liverpool methodology is the requirements analysis where an organization's information needs are documented. What does the organization need to know? What pieces of data are required to form the picture that the organization requires? How are these data to be organized and relationships defined? The second step, conceptual database design, identifies all of the pieces of data and puts them into a model in which their place and relationships are also defined. At the same time, the business processes that create the data are also modeled. This second step is extremely critical because it requires that the database designers thoroughly understand the customers' needs and way of working. Often a problem arises at this stage because while database designers are experts at databases they do not always have similar expertise in the organization's business area.

The third step is the choice of hardware and software, including the choice of security programs to protect the database. In some instances, the available options are wide, allowing potential users to get the capabilities they need on an affordable scale.

The fourth step is logical design. Business processes (transactions) are documented and diagrammed followed by a mapping of these workflows to the capabilities of the selected (or newly developed) database. The fifth step (physical design) determines where data will be stored and how it is moved in the database.

The final step is planning how the database is actually developed with continual (iterative) testing at every stage until installation and use when it is then usually managed by a company's database administrator.

—Robert N. Stacy

Further Reading

- Badia, Antonio, and Daniel Lemire. "A Call to Arms: Revisiting Database Design." *ACM SIGMOD Record*, vol. 40, no. 3, 2009, pp. 61–69.
- Buxton, Stephen. *Database Design: Know it All*. Morgan Kaufmann, 2009.
- Churcher, Clare. *Beginning Database Design: From Novice to Professional*. 2nd ed., Apress, 2012.
- Creswell, John W. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Sage, 2013.
- Currim, Sabah, et al. "Using a Knowledge Learning Framework to Predict Errors in Database Design." *Information Systems*, vol. 40, 2014, pp. 11–31.
- Grad, Burton, and Thomas J. Bergin. "History of Database Management Systems." *IEEE Annals of the History of Computing*, vol. 31, no. 4, 2009, pp. 3–5.
- Hernandez, Michael J. *Database Design for Mere Mortals: A Hands-On Guide to Relational Database Design*. 4th ed., Addison-Wesley, 2020.
- Sciore, Edward. *Database Design and Implementation*. 2nd ed., Springer, 2020.
- "What Is Database Security?" IBM, www.ibm.com/topics/database-security.

DEBUGGING

ABSTRACT

Debugging is the process of identifying and addressing errors, known as "bugs," in computer systems. It is an essential step in the development of all kinds of programs, from consumer programs such as web browsers and video games to the complex systems used in transportation and infrastructure. Debugging can be carried out through a number of methods depending on the nature of the computer system in question.

BACKGROUND

Debugging tests software or other computer systems, noting any errors that occur, and finding the cause of those errors. Errors, or "bugs," in a computer program can seriously affect the program's operations or even prevent it from functioning altogether. The goal of debugging is to get rid of the bugs that

have been identified. This should ensure the smooth and error-free operation of the computer program or system.

Computer programs consist of long strings of specialized code that tell the computer what to do and how to do it. Computer code must use specific vocabulary and structures to function properly. As such code is written by human programmers, there is always the possibility of human error, which is the cause of many common bugs. Perhaps the most common bugs are syntax errors. These are the result of small mistakes, such as typos, in a program's code. In some cases, a bug may occur because the programmer neglected to include a key element in the code or structured it incorrectly. For example, the code could include a command instructing the computer to begin a specific process but lack the corresponding command to end it.

Bugs fall into one of several categories, based on when and how they affect the program. Compilation errors prevent the program from running. Run-time errors, meanwhile, occur as the program is running. Logic errors, in which flaws in the program's logic produce unintended results, are a particularly common form of bug. Such errors come about when a program's code is syntactically correct but does not make logical sense. For instance, a string of code with flawed logic may cause the program to become caught in an unintended loop. This can cause it to become completely unresponsive, or freeze. In other cases, a logic error might result when a program's code instructs the computer to divide a numerical value by zero, a mathematically impossible task.

OVERVIEW

Bugs may interfere with a program's ability to perform its core functions or even to run. Not all bugs are related to a program's core functions, and some programs may be usable despite the errors they contain. However, ease of use is an important factor that many people consider when deciding which

| | |
|------------|--|
| 92 | |
| 9/9 | |
| 0800 | Actan started |
| 1000 | " stopped - actan ✓ |
| 1300 (033) | MP-MC PRO 2 cosine |
| | $\begin{array}{l} 1.2700 \quad 9.037847025 \\ \{ \quad \quad \quad 9.037846995 \text{ correct} \\ 1.982147000 \quad 4.615925059(-2) \\ 1.50476715(-3) \end{array}$ |
| 1700 | Started Cosine Tape (Sine check) Relays changed |
| 1525 | Started Multi+ Adder Test. |
| 1545 |  |
| | Relay #70 Panel F (moth) in relay. |
| 1630 | First actual case of bug being found. Actangent started. |
| 1700 | closed down. |

Admiral Grace Hopper is credited with coining the terms 'bug' and 'debugging' in the 1940s. While working on a Mark II computer at Harvard University, her colleagues found a moth stuck in a relay, which hindered the system's operation. Hopper referred to this process as 'debugging'. Here pictured, a computer log entry from the Mark II, with a moth taped to the page. Photo via Wikimedia Commons. [Public domain.]

program to use. It is therefore in the best interest of software creators to ensure that their programs are as free of errors as possible. In addition to testing a program or other computer system in house prior to releasing them to the public, many software companies collect reports of bugs from users following its release. This is often done through transfers of collected data commonly referred to as memory dumps. They can then address such errors through updates known as software patches.

While bugs are an inconvenience in consumer computer programs, in more specialized computer

systems, they can have far more serious consequences. In areas such as transportation, infrastructure, and finance, errors in syntax and logic can place lives and livelihoods at risk. Perhaps the most prominent example of such a bug was the so-called Y2K bug. This bug was projected to affect numerous computer systems beginning on January 1, 2000. The problem would have resulted from existing practices related to the way dates were written in computer programs. However, it was largely averted through the work of programmers who updated the affected programs to prevent that issue.

As the example of the far-reaching Y2K bug shows, the world's growing reliance on computers in all areas of society has made thorough debugging even more important.

Identifying and Addressing Bugs

The means of debugging vary based on the nature of the computer program or system in question. However, in most cases bugs may be identified and addressed through the same general process. When a bug first appears, the programmer or tester must first attempt to reproduce the bug in order to identify the results of the error and the conditions under which they occur. Next, the programmer must attempt to determine which part of the program's code is causing the error to occur. As programs can be quite complex, the programmer must simplify this process by eliminating as much irrelevant data as possible. Once the faulty segment of code has been found, the programmer must identify and correct the specific problem that is causing the bug. If the cause is a typo or a syntax error, the programmer may simply need to make a small correction. If there is a logic error, the programmer may need to rewrite a portion of the code so that the program operates logically.

DEBUGGING IN PRACTICE

Programmers use a wide range of tools to debug programs. As programs are frequently complex and lengthy, automating portions of the debugging process is often essential. Automated debugging programs, or “debuggers,” search through code line by line for syntax errors or faulty logic that could cause bugs. A technique known as delta debugging provides an automated means of filtering out irrelevant information when the programmer is looking for the root cause of a bug.

Different types of programs or systems often require different debugging tools. An in-circuit emulator is used when the computer system being tested is an embedded system (i.e., one located within a

larger system) and cannot otherwise be accessed. A form of debugging known as integration testing is often used when a program consists of numerous components. After each component is tested and debugged on its own, they are linked together and tested as a unit. This ensures that the different components function correctly when working together.

—Joy Crelin

Further Reading

- Burger, Arnold S. *Debugging Embedded and Real-Time Systems*. Newnes, 2020.
- Foote, Steven. *Learning to Program*. Pearson, 2015.
- Lettnin, Djones, and Markus Winterholer, editors. *Embedded Software Verification and Debugging*. Springer-Verlag New York, 2017.
- McCauley, Renée, et al. “Debugging: A Review of the Literature from an Educational Perspective.” *Computer Science Education*, vol. 18, no. 2, 2008, pp. 67–92.
- Myers, Glenford J., Tom Badgett, and Corey Sandler. *The Art of Software Testing*. 3rd ed., Wiley, 2012. Print.
- O’Leary, Timothy, Linda O’Leary, and Daniel O’Leary. *Computing Essentials 2023*. McGraw-Hill, 2022.
- Patt, Yale, and Sanjay Patel. *Introduction to Computing Systems: From Bits & Gates to C/C++ & Beyond*. 3rd ed., McGraw-Hill, 2019.
- “What Is Debugging?” AWS, 2023, aws.amazon.com/what-is/debugging.
- Zeller, Andreas. *Why Programs Fail: A Guide to Systematic Debugging*. Kaufmann, 2009.

DEEPMODE

ABSTRACT

The term “deepfake” refers to emerging technology that allows computer users to create fabricated but highly convincing sounds, static images, and moving pictures. Deepfake technologies are assisted by advanced artificial intelligence (AI), mostly from a class of AI known as “generative adversarial networks” (GANs). Using sophisticated algorithms, GANs manipulate user-supplied input to generate sounds, images, and videos, resulting in strikingly

realistic simulated content. The word “deepfake” was derived from the words “deep learning” and “fake.”

BACKGROUND

The invention of deepfake technology is generally credited to Ian Goodfellow, a machine-learning expert who created his first GAN-powered deepfakes in 2014 while he was a PhD student at the University of Montreal. Goodfellow went on to work for several major companies carrying out research within the AI space, including Google, OpenAI, Apple, and the Google subsidiary DeepMind.

Deepfake technology allows computer users to create fabricated but highly convincing sounds, static images, and moving pictures. It relies on algorithms, which are systematized sequences of programming

instructions that tell a computer how to handle a complex task. In particular, it uses advanced AI-powered GAN processes that push the limits of conventional algorithms. Most algorithms are focused on simply sorting or classifying data, while GANs use multiple algorithms that try to trick each other into categorizing a manufactured sound, image, or video as real. Specifically, they function by simultaneously adopting the roles of generator and discriminator, where the generator is responsible for drawing on user input to manufacture a fake sound clip, image, or video clip and the “discriminator” is responsible for comparing the simulated content against the authentic input. GANs are capable of testing simulated content against millions of evaluative parameters very quickly, ultimately



Image via iStock/dem10. [Used under license.]

allowing users to generate fake sounds, images, and videos realistic enough to convince viewers of their authenticity.

One definitive aspect of deepfake technology is that it does not require much initial input to create a believable result. A *Popular Mechanics* article from August 2019 noted that GANs only need a few images to generate output that appears genuine to the untrained eye.

OVERVIEW

Deepfake software is openly available for download on the internet, enabling any user with the requisite computer skills to use it to produce fake audio, image, and video content. According to a *BBC News* report published in October 2019, which drew on data supplied by the cybersecurity firm Deeptrace, approximately 15,000 deepfake videos were online by that point, marking a sharp rise from the nearly 8,000 the firm counted in December 2018. Observers and analysts believe that amateur computing hobbyists are responsible for a large majority of existing deepfake content and emphasize that deepfake production is a worldwide phenomenon. The BBC report also noted that Deeptrace's analysis found 96 percent of deepfakes to be pornographic in nature, with most simulated videos superimposing the likenesses of famous actresses onto the bodies of adult performers.

Deeptrace's report also addressed claims that deepfake videos were used in recent political campaigns in Malaysia and Gabon. According to the firm, allegations that deepfake videos were used to influence voters in both countries did not withstand scrutiny and can be dismissed as false. Deeptrace did note that deepfake videos had the potential to be weaponized for political purposes. However, as of the report's October 2019 publication date, the firm's expert analysts believed the most pressing threat came from the technology's potential misuse as a cybercriminal and cyberbullying tactic.



A fake Midjourney-created image of Donald Trump being arrested.
Image via Wikimedia Commons. [Public domain.]

A different analysis, conducted in February 2019 by a collaborative group known as Witness Media Lab, reported that existing deepfake technologies required a significant level of specialized knowledge to use effectively. However, Witness Media Lab researchers also stated that the end-user landscape was changing quickly, with increasingly advanced deepfake technologies requiring less and less user skill. Witness Media Lab's conclusions matched the Deeptrace analysis, with both organizations agreeing that the production of simulated, personalized, and highly sophisticated fake content represented a pressing threat to individual users, and particularly to girls and women who faced the risk of having their likenesses imposed on explicit adult videos for the purposes of phishing, extortion, harassment, and cyberbullying.

Deepfakes continued to proliferate throughout the next several years, with the number of deepfake videos online exceeding 85,000 by the end of 2020, according to a 2021 report by the firm Sensity. While some security experts predicted that

deepfakes would be widely used to create political propaganda and false news stories in an effort to influence the results of the 2020 US presidential election, deepfake technology did not make a significant impact on the 2020 presidential campaigns or on the election's outcome. However, deepfake technology remained concerning in the early 2020s due to its frequent use in the creation of explicit videos as well as in online scams. One prominent group of scammers became known for its livestreamed deepfake videos featuring technology executive Elon Musk, which the group used to entice victims into sending cryptocurrency to the perpetrators. Though present on other websites as well, the scam became particularly common on YouTube, with scammers gaining unauthorized access to popular YouTube accounts in order to reach large audiences and make their fake livestreams appear more legitimate.

IMPACT

During their early years of existence, persuasive deepfakes were largely confined to sounds, static images, and a genre of content commonly known as "talking head videos," which depicted immobile individuals speaking. However, as the underlying technologies continued to advance and improve, experts voiced concerns that deepfake technology heralded the impending arrival of a dangerous virtual landscape. Its potential criminal and political applications were particularly worrisome to many observers. The consensus among experts was that deepfake technology was likely to introduce unprecedented complications to the problem of "fake news" through artificially manufactured but believable video clips featuring politicians and other high-profile public figures.

With authorities on the topic agreeing that the technology poses new dangers in the virtual environment, many experts believed that deepfakes would soon become a central part of political disinformation campaigns and cyberwarfare. In response to

such concerns, US government agencies and other cybersecurity stakeholders worked to develop technology capable of recognizing deepfakes in what some observers described as a kind of virtual arms race meant to limit or prevent deepfakes from exerting a disruptive or damaging influence on society.

—Jim Greene

Further Reading

- Cellan-Jones, Rory. "Deepfake Videos 'Double in Nine Months.'" *BBC News*, 7 Oct. 2019, www.bbc.com/news/technology-49961089.
- Chen, Angela. "Three Threats Posed by Deepfakes That Technology Won't Solve." *MIT Technology Review*, 2 Oct. 2019, www.technologyreview.com/s/614446/deepfake-technology-detection-disinformation-harassment-revenge-porn-law.
- Gregory, Sam, and Eric French. "How Do We Work Together to Detect AI-Manipulated Media?" *Witness Media Lab*, 2019, lab.witness.org/projects/osint-digital-forensics.
- Libby, Kristina. "This Bill Hader Deepfake Video Is Amazing: It's Also Terrifying for Our Future." *Popular Mechanics*, 13 Aug. 2019, www.popularmechanics.com/technology/security/a28691128/deepfake-technology.
- Petkauskas, Vilius. "Report: Number of Expert-Crafted Video Deepfakes Double Every Six Months." *Cybernews*, 28 Sept. 2021, cybernews.com/privacy/report-number-of-expert-crafted-video-deepfakes-double-every-six-months.
- Porup, J. M. "How and Why Deepfake Videos Work—And What Is at Risk." *CSO*, 10 Apr. 2019, www.csoonline.com/article/3293002/deepfake-videos-how-and-why-they-work.html.
- Shao, Grace. "What 'Deepfakes' Are and How They May Be Dangerous." *CNBC*, 13 Oct. 2019, www.cnbc.com/2019/10/14/what-is-deepfake-and-how-it-might-be-dangerous.html.
- Simonite, Tom. "Prepare for the Deepfake Era of Web Video." *Wired*, 6 Oct. 2019, www.wired.com/story/prepare-deepfake-era-web-video.
- Tidy, Joe. "YouTube Accused of Not Tackling Musk Bitcoin Scam Streams." *BBC News*, 10 June 2022, www.bbc.com/news/technology-61749120.
- "What Is a Deepfake?" *The Economist*, 7 Aug. 2019, www.economist.com/the-economist-explains/2019/08/07/what-is-a-deepfake.

DEMON DIALING/WAR DIALING

ABSTRACT

War dialing is the practice of autodialing a large range of phone numbers to find computer modems. It involves using a software program to call all of the phone numbers within an area code to see which ones are set up to accept incoming connections. Demon dialing is a synonym for war dialing, though it has also been used to describe making repeated calls to a single modem in a brute-force attempt to guess its password.

BACKGROUND

Prior to the mid-1990s, the vast majority of people wishing to go online did so using dial-up modems. A dial-up modem connected a computer to the telephone network via a telephone wall jack. It accessed

the internet by making a phone call to another computer or a server and transmitting data over the telephone line. Most early internet connections were made to limited, self-contained services, such as local area networks (LANs) and bulletin-board systems (BBSs) hosted on computer systems running terminal programs. In order for a connection to be established, the computer user would have to have the phone number of the host computer, and the host computer would have to be available. If the host computer was not online or had too many connections already, it could not accept another connection. Eventually the first internet service providers (ISPs) were established, allowing many computers to access the public internet simultaneously.

As the number of computers with modems increased, computer hackers began to try to discover



Blue boxes were electronic devices used in early phreaking practices to exploit telephone systems and make free long-distance calls. Pictured is a blue box designed and built by Steve Wozniak and sold by Steve Jobs before they founded Apple. Displayed at the Powerhouse Museum, from the collection of the Computer History Museum. Photo by Maksym Kozlenko, via Wikimedia Commons.

and connect to them. For some, hacking became a hobby of sorts. It presented a challenge that was exciting and intellectually stimulating. For crackers, or criminal hackers, it was a way to steal data or commit other malicious acts. Regardless of the hackers' motives, they all needed some way to find the phone numbers of computers with modems.

One such way was war dialing. Hackers wrote software that would use a computer's modem to dial every phone number in a given area code. The software ran through each number, dialing and then hanging up after two rings. Most modems were set up to pick up after one ring, so if a number rang twice it most likely did not have a modem. The war-dialing software recorded which numbers had modems so that hackers could try to connect to them later.

"Demon dialing" originally meant making repeated calls to a single modem in a brute-force attempt to guess its password. The practice was named for the Demon Dialer, a telephone dialer once sold by Zoom Telephonics. This device could automatically redial a busy phone number until the call went through. Over time, demon dialing became a synonym for war dialing.

OVERVIEW

There have been many changes in technology that make the old methods of war dialing obsolete. The number of computers still connecting to the internet via dial-up modems decreased sharply after broadband internet access and wireless networking became mainstream in the mid-2000s. However, war dialing itself continued to be practiced in the twenty-first century; it simply required different techniques. For example, the open-source software WarVOX was a war-dialing tool that connected via voice over internet protocol (VoIP) systems instead of landline telephones. It used signal-processing techniques to probe and analyze telephone systems. Some information technology (IT) security personnel use

VoIP-based war dialers to find unauthorized modems and faxes on their organization's computer networks.

Another modern technique similar to war dialing is called port scanning. Computers connect to the internet using different ports, which are like virtual connection points. Some ports are traditionally used for certain connections, such as printers or web browsing. Other ports are left open for whichever application needs to create a connection. When a computer has been secured, ports not in use are kept closed to prevent unauthorized connections. Port scanners bombard computers with connection attempts on many different ports at once, then report vulnerable port numbers back to the hacker. To protect against port scanning, many companies now use intrusion-detection systems that can identify when a port scan is underway. This security measure has in turn motivated hackers to develop port-scanning methods that can gather information without openly trying to connect to each port.

WI-FI WAR DIALING

Some hackers target wireless networks instead of wired ones. One technique for doing so is wardriving, in which hackers drive around a neighborhood with a laptop running Wi-Fi scanning software. The software identifies wireless networks as it passes through them and collects information about the type of security each wireless access point is using. Hackers can then sort through this information to find vulnerable networks. A hacker may exploit the network to gain free wireless internet access or to disguise their online identity.

—Scott Zimmer

Further Reading

- Coleman, E Gabriella. *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton UP, 2013.
Haerens, Margaret, and Lynn M. Zott, editors. *Hacking and Hackers*. Greenhaven, 2014.

- Kizza, Joseph Migga. *Guide to Computer Network Security*. 6th ed., Springer, 2024.
- Morselli, Carlo, editor. *Crime and Networks*. Routledge, 2014.
- Naraine, Ryan. "Metasploit's H. D. Moore Releases 'War Dialing' Tools." ZDNet, 6 Mar. 2009, www.zdnet.com/article/metasploits-hd-moore-releases-war-dialing-tools.
- Netzley, Patricia D. *How Serious a Problem Is Computer Hacking?* ReferencePoint, 2014.
- Shakarian, Paulo, Jana Shakarian, and Andrew Ruef. *Introduction to Cyber-Warfare: A Multidisciplinary Approach*. Syngress, 2013.
- Watters, Paul A. *Cybercrime and Cybersecurity*. CRC Press, 2023.

DEVICE DRIVERS

ABSTRACT

Device drivers enable programmers to write software that will run on a computer regardless of the type of devices that are connected to that computer. Using device drivers allows the program to simply command the computer to save data to a file on the hard drive. It needs no specific information about what type of hard drive is installed in the computer or connections the hard drive has to other hardware in the computer. The device driver acts as an interface between computer components.

BACKGROUND

When a program needs to send commands to a peripheral connected to the computer, the program communicates with the device driver. The device driver receives the information about the action that the device is being asked to perform. It translates this information into a format that can be input into the device. The device then performs the task or tasks requested. When it finishes, it may generate output that is communicated to the driver, either as a message or as a simple indication that the task has been completed. The driver then translates this information into a form that the original program can understand. The device driver acts as a kind of

translator between the computer and its peripherals, conveying input/output instructions between the two. Thus, the computer program does not need to include all the low-level commands needed to make the device function. The program only needs to be able to tell the device driver what it wants the device to do. The device driver takes care of translating this into concrete steps.

Each device connected to a central processing unit (CPU) is controlled by a device driver, software that controls, manages, and monitors a specific device (e.g., keyboard, mouse, monitor, digital versatile disc [DVD] reader). Device drivers may also drive other software that drives a device (e.g., system management bus, universal serial bus [USB] controller).

OVERVIEW

Writing device drivers is a highly technical undertaking. It is made more challenging by the fact that device drivers can be unforgiving when a mistake is made in their creation. This is because higher-level applications do not often have unlimited access to all of the computer's functionality. Issuing the wrong command with unrestricted privileges can cause serious damage to the computer's operating system (OS) and, in some cases, to the hardware. This is a real possibility with device drivers, which usually need to have unrestricted access to the computer.

Because writing a device driver requires a lot of specialized information, most device drivers are made by software engineers who specialize in driver development and work for hardware manufacturers. Usually the device manufacturer has the most information about the device and what it needs to function properly. The exception to this trend is the impressive amount of driver development accomplished by the open-source movement. Programmers all over the world have volunteered their own time and talent to write drivers for the Linux OS.

Often development is separated into logical and physical device driver development. Logical device

driver development tends to be done by the creator of the OS that the computer will use. Physical device driver development, meanwhile, is handled by the device manufacturer. This division of labor makes sense, but it does require coordination and a willingness to share standards and practices among the various parties.

VIRTUAL DEVICE DRIVERS

Virtual device drivers are a variation on traditional device drivers. They are used when a computer needs to emulate a piece of hardware. This often occurs when an OS runs a program that was created for a different OS by emulating that operating environment. One example would be a Windows OS running a disk operating system (DOS) program. If the DOS program needed to interface with an attached printer, the computer would use a virtual device driver.

DEVICE MANAGERS

Most OSs now include device managers that make it easier for the user to manage device drivers. They allow the user to diagnose problems with devices, troubleshoot issues, and update or install drivers. Using the graphical interface of a device manager is less intimidating than typing in text commands to perform driver-related tasks.

—Scott Zimmer

Further Reading

- Corbet, Jonathan, Alessandro Rubini, and Greg Kroah-Hartman. *Linux Device Drivers*. 3rd ed., O'Reilly, 2005.
- “Driver Security Checklist.” Microsoft, 4 May 2023, learn.microsoft.com/en-us/windows-hardware/drivers/driversecurity/driver-security-checklist.
- McFedries, Paul. *Fixing Your Computer: Absolute Beginner’s Guide*. Que, 2014.
- Mueller, Scott. *Upgrading and Repairing PCs*. 22nd ed., Que, 2015.
- O’Leary, Timothy, Linda O’Leary, and Daniel O’Leary. *Computing Essentials 2023*. McGraw-Hill, 2022.

“What Is a Driver?” Microsoft, 4 Nov. 2022, learn.microsoft.com/en-us/windows-hardware/drivers/gettingstarted/what-is-a-driver-.

DIGITAL FORENSICS

ABSTRACT

Digital forensics is the science of recovering and studying digital data, typically in criminal investigations. Digital forensic science is used to investigate cybercrimes. These crimes target or involve the use of computer systems. Examples include identity theft, digital piracy, hacking, data theft, and cyberattacks. The Scientific Working Group on Digital Evidence (SWGDE), formed in 1998, develops industry guidelines, techniques, and standards. Digital forensics encompasses computer forensics, mobile forensics, computer network forensics, social networking forensics, database forensics, and forensic data analysis or the forensic analysis of large-scale data.

BACKGROUND

Digital forensics emerged in the mid-1980s in response to the growing importance of digital data in criminal investigations. The first cybercrimes occurred in the early 1970s. This era saw the emergence of “hacking,” or gaining unauthorized access to computer systems. Some of the first documented uses of digital forensics data were in hacking investigations.

Prior to the Electronic Communications Privacy Act (ECPA) of 1986, digital data or communications were not protected by law and could be collected or intercepted by law enforcement. The ECPA was amended several times in the 1990s and 2000s to address the growing importance of digital data for private communication. In 2014, the Supreme Court ruled that police must obtain a warrant before searching the cell phone of a suspect arrested for a crime.

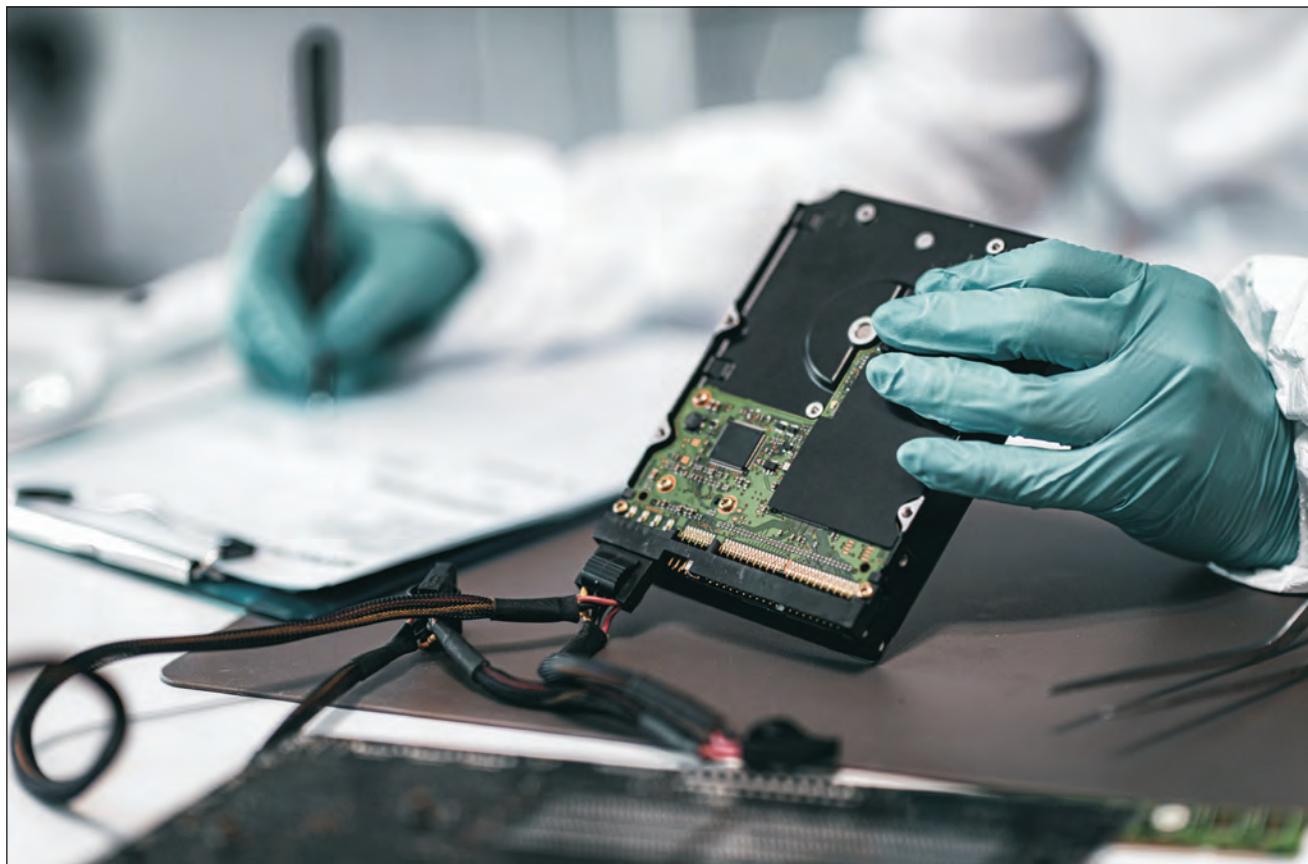


Photo via iStock/microgen. [Used under license.]

OVERVIEW

Once forensic investigators have access to equipment that has been seized or otherwise legally obtained, they can begin forensic imaging. This process involves making an unaltered copy, or forensic image, of the device's hard drive. A forensic image records the drive's structures, all of its contents, and metadata about the original files.

A forensic image is also known as a "physical copy." There are two main methods of copying computer data, physical copying and logical copying. A physical copy duplicates all of the data on a specific drive, including empty, deleted, or fragmented data, and stores it in its original configuration. A logical copy, by contrast, copies active data but ignores deleted files, fragments, and empty space. This

makes the data easier to read and analyze. However, it may not provide a complete picture of the relevant data.

After imaging, forensics examiners analyze the imaged data. They may use specialized tools to recover deleted files using fragments or backup data, which is stored on many digital devices to prevent accidental data loss. Automated programs can be used to search and sort through imaged data to find useful information. (Because searching and sorting are crucial to the forensic process, digital forensics organizations invest in research into better search and sort algorithms). Information of interest to examiners may include emails, text messages, chat records, financial files, and various types of computer code. The tools and techniques used for

analysis depend largely on the crime. These specialists may also be tasked with interpreting any data collected during an investigation. For instance, they may be called on to explain their findings to police or during a trial.

CHALLENGES FOR THE FUTURE

Digital forensics is an emerging field that lags behind fast-changing digital technology. For instance, cloud computing is a fairly new technology in which data storage and processing is distributed across multiple computers or servers. In 2014, the National Institute of Standards and Technology identified sixty-five challenges that must be addressed regarding cloud computing. These challenges include both technical problems and legal issues.

The SWGDE works to create tools and standards that will allow investigators to effectively retrieve and analyze data while keeping pace with changing technology. It must also work with legal rights organizations to ensure that investigations remain within boundaries set to protect personal rights and privacy. Each forensic investigation may involve accessing personal communications and data that might be protected under laws that guarantee free speech and expression or prohibit unlawful search and seizure. The SWGDE and law enforcement agencies are debating changes to existing privacy and surveillance laws to address these issues while enabling digital forensic science to continue developing.

—Micah L. Issitt

Further Reading

- “Digital Evidence and Forensics.” *National Institute of Justice*, nij.ojp.gov/digital-evidence-and-forensics.
- Gogolin, Greg. *Digital Forensics Explained*. CRC, 2013.
- Holt, Thomas J., Adam M. Bossler, and Kathryn C. Seigfried-SPELLAR. *Cybercrime and Digital Forensics: An Introduction*. 3rd ed., Routledge, 2022.
- Oettinger, William. *Learn Computer Forensics*. 2nd ed., Packt, 2022.

Pollitt, Mark. “A History of Digital Forensics.” *Advances in Digital Forensics VI*, edited by Kam-Pui Chow and Sujeet Shenoi, Springer, 2010, pp. 3–15.

Sammons, John. *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics*. 2nd ed., Syngress, 2014.

DIGITAL WATERMARKING

ABSTRACT

Digital watermarking protects shared or distributed intellectual property by placing an additional signal within the file. This signal can be used to inform users of the copyright owner’s identity and to authenticate the source of digital data. Digital watermarks may be visible or hidden.

BACKGROUND

A paper watermark is an image embedded within another image or a piece of paper. It can be seen by shining light on the image. Watermarks are used on banknotes, passports, and other types of paper documents to verify their authenticity. Similarly, digital watermarking involves embedding data within a digital signal in order to verify the authenticity of the signal or identify its owners. Digital watermarking was invented in the late 1980s or early 1990s. It uses techniques that are also used in steganography (the concealment of messages, files, or other types of data within images, audio, video, or even text).

OVERVIEW

Digital watermarking is a technique that embeds digital media files with a hidden digital code. These hidden codes can be used to record copyright data, track copying or alteration of a file, or prevent alteration or unauthorized efforts to copy a copyrighted file. Digital watermarking is therefore commonly used for copyright-protected music, video, and software downloads. Governments and banks also rely on it to ensure that sensitive documents and currency are protected from counterfeiting and fraud.

Most digital watermarks are not detectable without an algorithm that can search for the signal embedded in the carrier signal. In order for a carrier signal to be watermarked, it must be tolerant of noise. Noise-tolerant signals are generally strong signals that resist degradation or unwanted modulation. Typically, digital watermarks are embedded in data by using an algorithm to encode the original signal with a hidden signal. The embedding may be performed using either public- or private-key encryption, depending on the level of security required.

QUALITIES OF DIGITAL WATERMARKS

One way to classify digital watermarks is by capacity, which measures how long and complex a watermarking signal is. The simplest type is 1-bit watermarking. This is used to encode a simple message that is meant only to be detected or not (a binary result of 1 or 0). In contrast, multibit watermarking embeds multiple bits of data in the original signal. Multibit systems may be more resistant to attack, as an attacker will not know how or where the watermark has been inserted.

Watermarks may also be classified as either robust or fragile. Robust watermarks resist most types of modification and therefore remain within the signal after any alterations, such as compression or

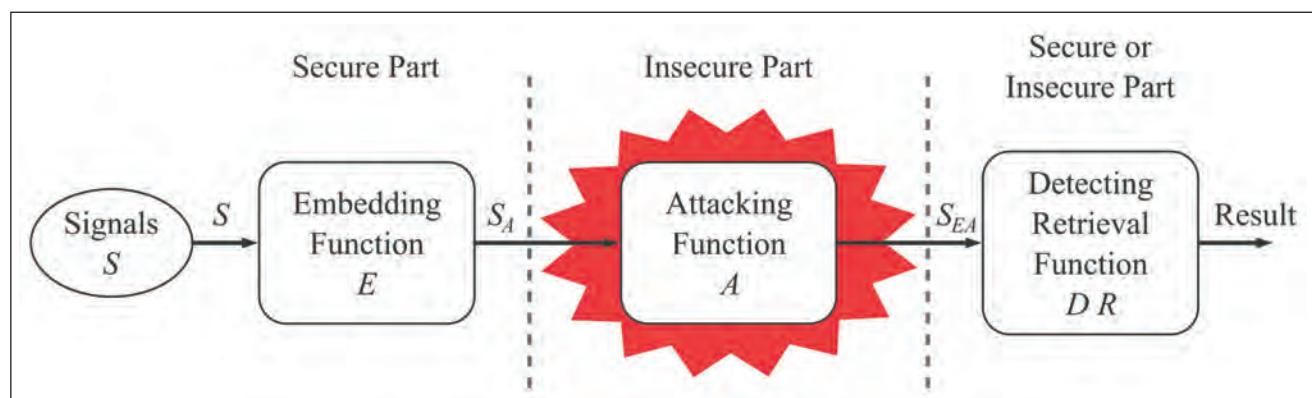
cropping. These watermarks are often used to embed copyright information, as any copies of the file will also carry the watermark. Fragile watermarks cannot be detected if the signal is modified and are therefore used to determine if data has been altered.

In some cases, a digital watermark is designed so that users can easily detect it in the file. For instance, a video watermark may be a visible logo or text hovering onscreen during playback. In most cases, however, digital watermarks are hidden signals that can only be detected using an algorithm to retrieve the watermarking code. Reversible data hiding refers to cases in which the embedding of a watermark can be reversed by an algorithm to recover the original file.

APPLICATIONS OF DIGITAL WATERMARKING

A primary function of digital watermarking is to protect copyrighted digital content. Audio and video players may search for a digital watermark contained in a copyrighted file and only play or copy the file if it contains the watermark. This essentially verifies that the content is owned legally.

Certain types of programs, known colloquially as “crippleware,” use visible digital watermarks to ensure that they are legally purchased after an initial free evaluation period. Programs used to produce



General digital watermark life-cycle phases with embedding-, attacking-, and detection and retrieval functions. Image by Amit6 at English Wikipedia, via Wikimedia Commons.

digital media files, such as image- or video-editing software, can often be downloaded for free so users can try them out first. To encourage users to purchase the full program, these trial versions will output images or videos containing a visible watermark. Only when the program has been registered or a product key has been entered will this watermark be removed.

Some creators of digital content use digital watermarking to embed their content with their identity and copyright information. They use robust watermarks so that even altered copies of the file will retain them. This allows a content owner to claim their work even if it has been altered by another user. In some cases, watermarked data can be configured so that any copies can be traced back to individual users or distributors. This function can be useful for tracing illegal distribution of copyrighted material. It can also help investigations into the unauthorized leaking of sensitive or proprietary files.

Digital watermarking has also been used to create hidden watermarks on product packaging. This is intended to make it easier for point-of-sale equipment to find and scan tracking codes on a product. Digital watermarking is also increasingly being used alongside or instead of regular watermarking to help prevent the counterfeiting of important identification papers, such as driver's licenses and passports.

—Micah L. Issitt

Further Reading

- Bas, Patrick, et al. *Watermarking Security*. Springer Singapore, 2016.
- Chao, Loretta. "Tech Partnership Looks beyond the Bar Code with Digital Watermarks." *Wall Street Journal*, 12 Jan. 2016, www.wsj.com/articles/tech-partnership-looks-beyond-the-bar-code-with-digital-watermarks-1452623450.
- Giri, Kaiser J., Shabir Ahmad Parah, Rumaan Bashir, and Khan Muhammad, editors. *Multimedia Security: Algorithm Development, Analysis and Applications*. Springer Nature Singapore, 2021.

- Gupta, Siddarth, and Vagesh Porwal. "Recent Digital Watermarking Approaches, Protecting Multimedia Data Ownership." *Advances in Computer Science* vol. 4, no. 2, 2015, pp. 21–30.
- Nematollahi, Mohammad Ali, Chalee Vorakulpipat, and Hamurabi Gamboa Rosales. *Digital Watermarking: Techniques and Trends*. Springer Singapore, 2017.
- Patel, Ruchika, and Parth Bhatt. "A Review Paper on Digital Watermarking and Its Techniques." *International Journal of Computer Applications*, vol. 110, no. 1, 2015, pp. 10–13.
- "Quick Facts about the Digital Watermarking Alliance." *Digital Watermarking Alliance*, digitalwatermarkingalliance.org/about/quick-facts.
- Su, Qingtang. *Color Image Watermarking*. Tsinghua UP/Walter de Gruyter, 2017.

DOXING

ABSTRACT

Doxing (sometimes spelled doxxing) is the sharing of someone's personal information on the internet without their consent. Information shared in doxing is personal, such as cell phone numbers and work or home addresses. Sometimes it includes more sensitive material, such as Social Security numbers, personal messages, and photos.

BACKGROUND

The word "dox" derives from having someone's documents, or information, which was shortened to "docs" and then to "dox." It is an abbreviation of "dropping dox," a revenge tactic used on hacker bulletin boards in the 1990s. As much of hacker culture depended on anonymity, disclosing someone's personal information (or PI) was a way to retaliate against them in an argument, show them to be vulnerable, and open them up to harassment or prosecution if they were breaking any laws. While initially doxing mostly revealed user profile information, the tactic expanded as the internet grew.



Hacker Lorem

@Hacker_Lorem

@Ipsum434's real name is Happy Traveler. He lives at 123 Sit Amet Avenue.



A fictional example of a doxing post on social media. In this case, the victim's personal name and address are shown. Photo via Wikimedia Commons. [Public domain.]

Doxing began to receive increased public recognition during the first decade of the twenty-first century, a period in which several major doxing incidents took place. In 2006, a YouTube channel called Vigilantes was created. Its mission was to locate and publish the personal information of other YouTube channels that posted what Vigilantes deemed to be hateful or racist content. In January 2007, the head of the Vigilantes group was doxed by members of *Encyclopedia Dramatica*. The information included her name, address, and personal posts she made to a newsgroup.

At this point in time, the hacker collective Anonymous and associated groups, such as Chan Enterprises LLC and Lulzsec, began to use doxing in targeted campaigns. One of the first documented doxing campaigns focused on white nationalist and radio host Hal Turner. Turner shared the telephone numbers of prank callers that phoned in to his radio show in December 2006. In response, Anonymous

members calling themselves Chan Enterprises LLC began a doxing investigation that discovered Turner's criminal record, home address, and phone number, which they posted. Turner filed several lawsuits against the online forums and websites that posted his dox, such as 4chan, eBaums World, and 7chan, in January 2007. However, all the cases were dismissed by December of that year.

Forums like 4chan and 7chan are similar to discussion sites such as Reddit, except that they have no usernames and few rules. They are considered to be the antithesis of social media, where people anonymously say and post whatever they wish with few or no consequences. These forums are often hosts to doxing campaigns or other anonymous postings. For instance, 4chan was blamed for the leaks of many female celebrity nudes.

In January 2008, anonymous hackers started Project Chanology, a doxing campaign that targeted members of Scientology. The hackers published the

personal information of high-ranking members and internal memos from the church. This doxing campaign received international coverage.

OVERVIEW

By 2008, “doxing” had become more widely known and was added to the *Urban Dictionary*, which defined it as personal information leaked by a third party. *Wiktionary* added a doxing definition in 2011. The term would later appear in mainstream dictionaries such as the *Oxford English Dictionary (OED)*, which added the term in 2015.

The definition of doxing is generally perceived to be negative, as it violates privacy and was historically used for retaliation. However, there is some debate about whether doxing is, at times, warranted, when the goals achieved outweigh a person’s privacy and anonymity. There are a wide variety of motives for doxing someone.

Internet vigilantism often uses doxing, where those who disagree with an individual’s actions publish the person’s personal information so that they are subject to harassment and criticism. Groups on both the left and the right of the political spectrum have employed this technique. It is not just political or hacker groups that use doxing. In July 2015, newspapers reported that Cecil the Lion was illegally killed by a hunter from Minnesota. The *Telegraph*, a British newspaper, identified the hunter as a dentist from Minnesota. His address, website, work, and vacation homes were vandalized, and he received death threats and protests.

Doxing can serve as a tool for protest or exposing corruption. Government corruption in China was the target of the Human Flesh Search Engine, a group of internet citizens who search for and publish information about government wrongdoing. One of their doxes exposed government officials using public funds for recreational trips.

Sometimes doxing is used to expose perceived wrongdoing. In 2015, a group of hackers called the

Impact Team breached the Ashley Madison database. The online dating site catered to married people wishing to have affairs. The hackers demanded that the site shut down permanently or they would dox the information they obtained. When the site remained up, the hackers released 30 million user email addresses and profiles. The doxing led to several suicides, extortion attempts, and general embarrassment.

Certain types of investigative journalism can have the effect of doxing, such as the disclosure of the identity of the presumed Bitcoin inventor, Satoshi Nakamoto. This has spurred debate about where the line between investigative journalism and doxing lies, and whether and when it might be acceptable to disclose the names of individuals that are making efforts to remain anonymous.

Doxing is most commonly understood to be a means of harassment or a form of cyberbullying. It is intended to threaten someone and make them feel vulnerable. In the worst cases, it is used in cyberstalking and makes someone fearful for their safety or life to the point where they need to go into hiding.

A Pew Research Center survey in 2014 stated that 40 percent of adult internet users have experienced some form of harassment and 7 percent have experienced “sustained” periods of harassment. Since information on the internet is difficult to erase, a dox may haunt the targeted person both personally and professionally for years. All one has to do is enter the person’s name into a search engine for the material to come back up.

Due to the difficult task of fighting this sort of harassment, numerous groups have formed to offer support to victims of doxing. For instance, Crash Override Network was established as “a crisis helpline, advocacy group and resource center for people who are experiencing online abuse.” The group was formed by two victims of doxing during Gamergate, a 2014–15 campaign of online

harassment against women gamers, developers, and videogame critics.

Following the launch of the service, Crash Override Network offered the assistance of social workers, lawyers, and computer security professionals. Doxing is the most frequent sort of harassment they encountered, as it is relatively easy to find information about someone on the internet and it has a strong impact. The harasser is also able to rationalize doxing actions as benign and deny responsibility for other's actions, even though the intention is to violate another's personal space and sense of security.

As the internet has evolved, opportunities to share personal data have increased in myriad ways, such as through social media, online shopping, and other means. Doxing, through its use and misuse, highlights the challenge of balancing online interconnection with anonymity and privacy, both personally and in relation to others.

—Noëlle Sinclair

Further Reading

- Citron, Danielle Keats. *Hate Crimes in Cyberspace*. Harvard UP, 2014.
- Douglas, David M. "Doxing: A Conceptual Analysis." *Ethics and Information Technology*, vol. 18, no. 3, 2016, pp. 199–210.
- Harcourt, Bernard E. *Exposed: Desire and Disobedience in the Digital Age*. Harvard UP, 2015.
- Kizza, Joseph Migga. *Ethical and Social Issues in the Information Age*. 7th ed., Springer, 2023.
- Li, Lisa Bei. "Data Privacy in the Cyber Age: Recommendations for Regulating Doxing and Swatting." *Federal Communications Law Journal*, vol. 70, no. 3, 2018, pp. 317–28.
- Rainie, Lee, Janna Anderson, and Jonathan Albright. "The Future of Free Speech, Trolls, Anonymity and Fake News Online." *Pew Research Center*, 29 Mar. 2017, www.pewresearch.org/internet/2017/03/29/the-future-of-free-speech-trolls-anonymity-and-fake-news-online.
- "So You've Been Doxed: A Guide to Best Practices." *Crash Override Network*, [crashoverridenetwork.com/soyouvebeendoxed.html](http://crashoverridenetwork.com/crashoverridenetwork.com/soyouvebeendoxed.html).

E

E-BANKING

ABSTRACT

E-banking, also referred to as internet banking or online banking, enables individuals to conduct banking transactions online. While many customers appreciate the convenience of online banking, the practice has also prompted concerns regarding the security of users' data and money.

BACKGROUND

E-banking allows customers of a financial institution the opportunity to conduct their financial transactions—from day-to-day account statements to loan applications—in an online, virtual environment.

Most traditional banks, such as Bank of America or Chase, offer extensive online services that allow customers to avoid brick-and-mortar locations altogether. These services include deposits, transfers, payments, account management, budgeting tools, and loan applications. In fact, there are a number of banks, such as Ally and Synchrony Bank, that operate completely online.

E-banking is built on a foundation of multiple electronic and mobile technologies, such as online data transfers and automated data collection systems. In the world's global market, e-banking has played a significant role in the rise of e-commerce, especially in how people and businesses interact in

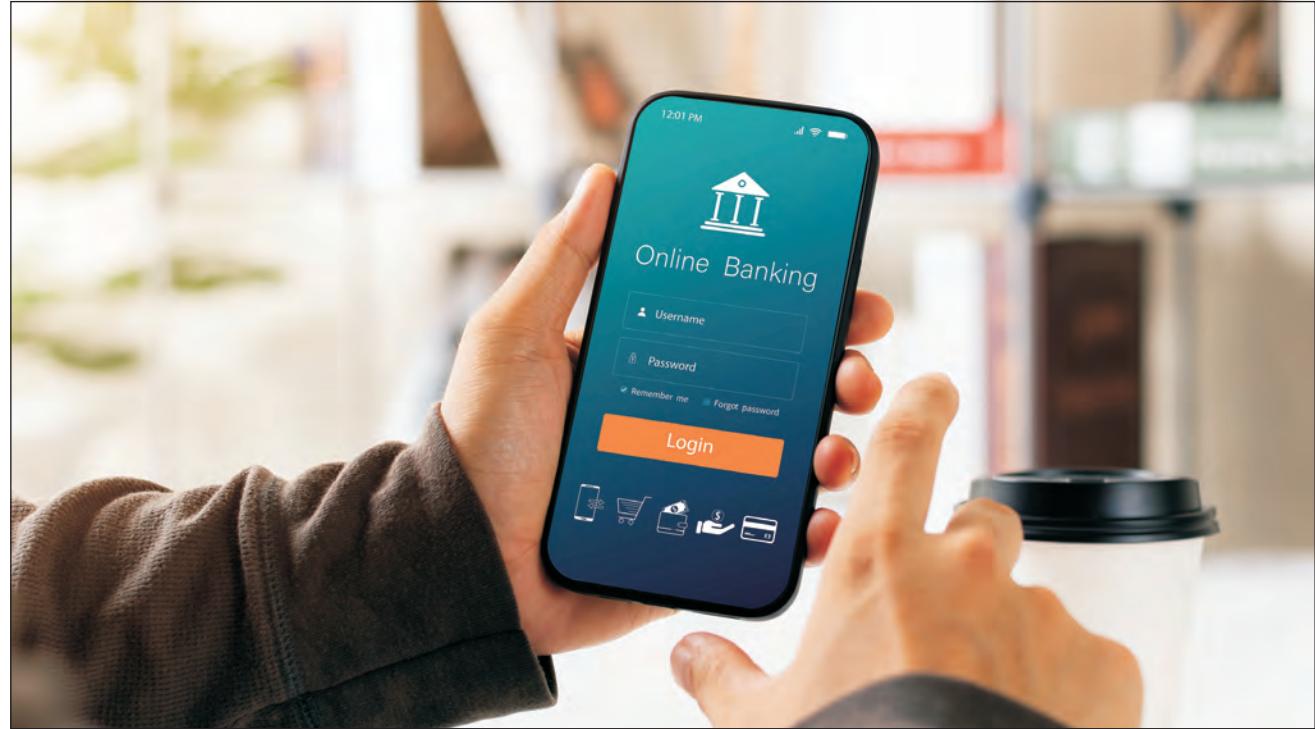


Photo via iStock/ Thapana Onphalai. [Used under license.]

the buying and selling of goods and services. Due in part to a rise in online banking, e-commerce has gained a significant foothold in the consumer environment and has increased the consumer base of many businesses exponentially because e-banking and e-commerce are not limited to specific geographic locations.

OVERVIEW

Modern banking no longer relies on geographic locations; instead, the industry has come to embrace consumers who prefer an online, virtual environment that may be accessed through an internet browser, a dedicated application, or both. One benefit of e-banking is a reduction in overhead costs usually associated with a brick-and-mortar location that are passed on to the customer. Other benefits include convenience and instant access for the customer to manage financial accounts and holdings. E-banking also plays a large role in the success of the electronic commerce environment in a global market, allowing financial transactions to happen almost instantaneously, regardless of geographic location.

However, online security of account information is a concern for both the online banking industry and its customers. This has spawned the rise of the information security industry, or infosec, which is the practice of protecting information from unauthorized use, disclosure, access, modification, or destruction. Infosec applies to all information regardless of the form it may take and is composed of two major categories: information assurance, which is ability to ensure data is not lost to a breakdown in system security, due to theft, natural disasters, or technological malfunction; and information technology (IT) security, which is the security applied to computer networks where information resides. Improvements in IT and related security elements are integral to the e-banking industry and foster reliable and effective security practices to

protect proprietary and confidential information. Overall, consumers are operating more and more in an online environment and are demanding e-banking capabilities for their smartphones and other devices. Businesses and banks will continue to adapt toward this trend by providing secure applications and environments.

—L. L. Lundin

Further Reading

- Cavusgil, S., Tamer, et al. *International Business: The New Realities*. Frenchs Forest, 2015.
- Chau, S. C., and M. T. Lu. "Understanding Internet Banking Adoption and Use Behavior: A Hong Kong Perspective." *Journal of Global Information Management*, vol. 12, no. 3, 2009, pp. 21–43.
- Dahlberg, T., et al. "Past, Present, and Future of Mobile Payments Research: A Literature Review." *Electronic Commerce Research and Applications*, vol. 7, no. 2, 2008, pp. 165–81.
- Demirkan, H., and R. J. Kauffman. "Service-Oriented Technology and Management: Perspectives on Research and Practice for the Coming Decade." *Electronic Commerce Research and Applications*, vol. 7, no. 4, 2008, 356–76.
- Fox, Susannah. "51% of U.S. Adults Bank Online." *Pew Research Center*, 7 Aug. 2013, www.pewresearch.org/internet/2013/08/07/51-of-u-s-adults-bank-online.
- Gkoutzinis, Apostolos. *Internet Banking and the Law in Europe: Regulation, Financial Integration and Electronic Commerce*. Cambridge UP, 2010.
- Hoehle, Hartmut, Eusebio Scornavacca, and Sid Huff. "Three Decades of Research on Consumer Adoption and Utilization of Electronic Banking Channels: A Literature Analysis." *Decision Support Systems*, vol. 54, no. 1, 2012, pp. 122–32.
- Lee, M. C. "Factors Influencing the Adoption of Internet Banking: An Integration of TAM and TPB with Perceived Risk and Perceived Benefit." *Electronic Commerce Research and Applications*, vol. 8, no. 3, 2009, pp. 130–41.
- Pomerleau, Pierre-Luc, and David L. Lowery. *Countering Cyber Threats to Financial Institutions*. Palgrave Macmillan, 2020.
- Sayegh, Emil. "Potential for Devastation: The Impact of a Cyberattack on the Banking System." *Forbes*, 6 June

2023, www.forbes.com/sites/emilsayegh/2023/06/06/potential-for-devastation-the-impact-of-a-cyberattack-on-the-banking-system/?sh=52bb1a1f1b45.

ELECTRONIC BUGS

ABSTRACT

Bugs are hidden microphones used to listen in on conversations surreptitiously. Bug detectors are devices designed to find any bugs in a given area.

BACKGROUND

The invention and subsequent deployment of bugs in covert surveillance was quickly followed by the invention of bug detectors. Over time, the makers of bugs have created increasingly sophisticated devices in their attempts to evade the ever-widening scope of detection achieved by competing detectors.

The designs of the listening devices known as bugs are limited only by the imaginations of the designers. Bugs can be broadly divided into four types: radio-transmitting, nonradio, telephone-based, and reflection-based.

OVERVIEW

Radio-transmitting bugs. The simplest type of bug to place, and the simplest to detect, is the type that functions by transmitting a radio signal to the listener or, more often, to a remotely located tape recorder.

Such a bug can be placed quickly because it requires no installation of wires; in addition, the user can change recording tapes without having to gain access to the bug itself. Bugs of this type can be extremely small. They can operate off battery power or, if located in an electrical or telephone outlet, can draw power from the outlet and operate indefinitely. The simplest detectors for radio-transmitting bugs are broad-spectrum radio receivers. These report, by indicator lights or audio hum, whether radio signals,

at any frequency, are being emitted near them. In practice, the sensitivity of a radio receiver being used for bug detection must be lowered so that it does not report ordinary radio and television signals. Once the sensitivity is lowered, the broad-spectrum receiver has a very short detection range for bugs, so the user must conduct a careful sweep with the detector to ensure that no bugs are missed. Better than the broad-spectrum receiver is the frequency counter, which displays the frequency of a radio signal upon detecting it. A great (and quite costly) improvement over both the broad-spectrum receiver and the frequency counter is the spectrum analyzer, which not only detects all radio signals but also displays their frequencies and strengths on a bar graph. The user can thus ignore powerful but innocent transmissions—radio and television stations—and focus on others. A more sophisticated search for radio bugs requires two tools.

The first, an audio emitter, is placed in the room being swept and emits a loud audio signal on a single frequency. The other tool is a radio scanner that automatically sweeps all frequencies within its range, briefly listening to each frequency. It stops and sounds an alert if it hears a radio transmission containing the audio signal given off by the emitter. Bug manufacturers attempt to evade these detectors with technology such as burst transmission, in which the bug itself records signals, compresses them, and then sends them in brief bursts, five or ten minutes apart. Another device that can evade such detectors is the remotely controlled bug, which is turned on only when a conversation is to be overheard and thus is likely to be missed in general sweeps.

Nonradio bugs. Detecting bugs that do not transmit radio signals is much more difficult, but makers of bug detectors have evolved tools aimed at these as well. The simplest is an ultrasound generator, which, under the right conditions, can cause a microphone's diaphragm to vibrate and give off an audible sound. This kind of detector can find hidden

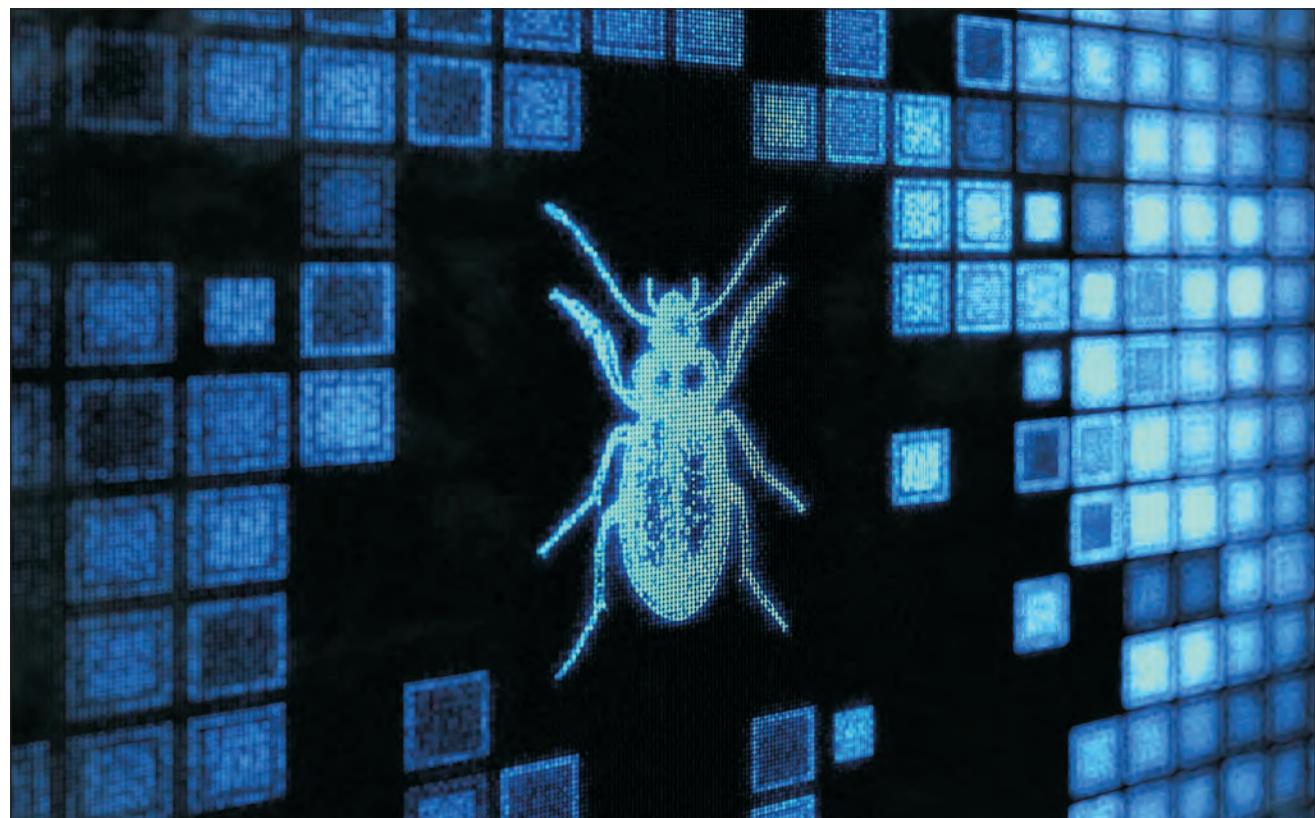


Photo via iStock/alengo. [Used under license.]

tape recorders because most of them, when running, give off faint ultrasonic signals that can be picked up by specialized listening devices. The most sophisticated tool for seeking nonradio bugs is the nonlinear junction detector. This device transmits a microwave signal that is reflected back (at a slightly different frequency, known as a harmonic) by transistors and similar electronic components used in bugs. This type of detector will spot even bugs that are not transmitting. Bug makers seek to evade these detectors by encasing their bugs in metal shielding that blocks the microwaves.

Telephone- and reflection-based bugs. Telephone-based bugs, also known as infinity transmitters, rely on devices, usually installed in telephones, that allow them to transmit over telephone lines and allow the listeners to call in without the telephones ringing.

Such devices can be detected by electronic tests of the telephone lines.

A reflection-based bug functions by reflecting radiation off an object that serves as a diaphragm. Sound causes the object to move, and the movement is shown in the reflected radiation. At a simple level, an infrared laser can be reflected off a windowpane to reveal conversations inside the room where the window is located. During the Cold War, the Soviets used a more complex reflection-based system to bug the US embassy in Moscow. Soviet schoolchildren presented the embassy with a gift: a wooden carving of the Seal of the United States in which was hidden a metal diaphragm with a tiny antenna. When a microwave beam was directed at the seal, the antenna absorbed the energy and radiated it back, varying with the audio in the room. The bug was

operational for seven years before it was accidentally detected. Searches for reflection-based bugs center on searches for the beams used to radiate them, which are usually infrared or microwave beams. Such searches are complicated by the fact that the beams are radiated only when the bugs' users are attempting to listen in on conversations.

CIA REVELATIONS

In 2009, the Central Intelligence Agency (CIA) authorized the retired director of its Office of Technical Service to publish *Spycraft*, which detailed some of its bugging and other techniques. Among the book's revelations were the use of extremely thin and almost invisible wires, the concealment of bugs in items of furniture, and the development of special drills to penetrate concrete while leaving only a tiny hole showing inside the room. Some of the agency's greater accomplishments were described, including tapping of supposedly secure underground telephone lines in Moscow and elsewhere. *Spycraft* also disclosed how the CIA's need for tiny but powerful batteries had led to breakthroughs in hearing aid battery technology.

—David T. Hardy

Further Reading

- Allsopp, Wil. *Unauthorized Access: Physical Penetration Testing for IT Security Teams*. Wiley, 2009.
- Clark, Laura, and William E. Algaier. *Surveillance Detection: The Art of Prevention*. Cradle Press, 2007.
- Hauser, Greg. *Techniques in Countersurveillance: The Fine Art of Bug Extermination in the Real World of Intelligence Gathering*. Paladin Press, 1999.
- Shannon, M. L. *Don't Bug Me: The Latest High-Tech Spy Methods*. Paladin Press, 1992.
- Stewart, Andrew J. *A Vulnerable System: The History of Information Security in the Computer Age*. Cornell UP, 2021.
- Wallace, Robert, and M. Keith Melton. *Spycraft: The Secret History of the CIA's Spytchcs, from Communism to Al-Qaeda*. Plume, 2009.

ELECTRONIC COMMERCE TECHNOLOGY

ABSTRACT

Electronic commerce (e-commerce) is the buying, selling, and transfer of products and services using the internet. It offers enormous advantages for supply-chain management and the coordination of distribution channels, in addition to being convenient for consumers. Convenience is a big selling point; in 2021, global retail e-commerce sales reached about \$5.2 trillion, according to the statistics platform Statista. A great amount of technology goes into supporting the online platforms used for e-commerce, facilitating financial transactions, and coordinating the logistics of inventory and shipping.

BACKGROUND

The communications between customers, vendors, and business partners over the internet is referred to as electronic commerce (or e-commerce). The term “e-business” incorporates the additional activities carried out within a business using intranets, such as communications related to production management and product development. Many also view e-business as referring to collaborations with partners and e-learning organizations.

In addition to online purchases of goods and services, e-commerce involves bill payments, online banking, e-wallets, smart cards, and digital cash. E-commerce depends on secure connections to the Internet. Many precautions to ensure security are necessary to maintain successful e-commerce, including public-key cryptography, secure sockets layer (SSL) and transport layer security (TLS) protocols, digital signatures, digital certificates, firewalls, and antivirus programs. New technology is constantly being developed to protect against computer worms and viruses and other cyberattacks.

In 1969, the Advanced Research Projects Agency (now the Defense Advanced Research Projects

Agency, or DARPA) of the US Department of Defense proposed a method to link together the computers at several universities to share computational data via networks. This network became known as ARPANET, the precursor of the internet. As a result, electronic mail (email) was developed, along with protocols for sending information over phone lines in packets. The protocols for the transmission of these packets of data came to be known as transmission control protocol (TCP) and internet protocol (IP). Together, these two protocols, known as TCP/IP, are still in use and are responsible for the efficient communication conducted through the network of networks referred to as the internet.

Oxford University graduate Tim Berners-Lee initially created the World Wide Web in 1989 while working at CERN, the European Organization for Nuclear Research, and made it available to the public in 1991. During this time, Cisco Systems was growing to become the first company to produce the

broad range of hardware products that allowed ordinary individuals to access the internet. In 1993, Marc Andreessen and Eric Bina, employees at the National Center for Supercomputing Applications (NCSA), created Mosaic, the first web browser that supported clickable buttons and links and allowed users to view text and images on the same page. New software and programming-language developments rapidly followed, allowing ordinary consumers easy access to the internet. As a result, companies saw the opportunity to gain customers, resulting in the creation of online businesses, including Amazon.com in 1994, eBay in 1995, and PayPal and Priceline in 1998.

OVERVIEW

The engineers who developed ARPANET created digital packets to use for transmitting data via packet switching. The theory was that it would be faster and cheaper to transmit digital data using



Photo via iStock/nndanko. [Used under license.]

small packets that could be sent, or routed, to their destination in the most efficient way possible, even if the original message had to be split up into smaller packets that were then joined back together at their destination. In order to accomplish the packaging of data and transmission via the best routes, the engineers who developed ARPANET also developed TCP. The first and most common access method to the internet was through the wiring that transmitted telephone calls. However, wireless internet connections can now be made much faster from many locations, even through cellular phones. The economy has become dependent on digital communication, and the companies that sell the most goods and services have a strong online presence. A great deal of planning goes into the maintenance of an effective website.

E-commerce business establishment. After first developing a practical business plan, the process for establishing an online business that will be able to successfully compete for sales can be overwhelming. One way to start an e-business is by using a turnkey solution, which is essentially a prepackaged type of software specifically for a new business. An alternative is to use the services of an internet incubator, which is a company that specializes in e-business development. An internet incubator typically obtains ownership of at least 50 percent of the business and may also enlist funding help from venture capitalists to get started. Web-hosting companies sell space on a web server to customers, maintain enough storage space for the website, and provide support services. A domain name for the website must be chosen and registered. This domain name is to be used in the uniform resource locator (URL) for the website. The URL, or website's internet address, consists of three parts: the host name, which is shown by the "www" for World Wide Web; the domain name, which is usually the name of the company; and lastly, the top-level domain (TLD), which describes the type of organization that owns the domain name, such as

".com" for a commercial organization or ".gov" for a government organization. An initial public offering (IPO) of stock to assist with funding usually follows for enterprises that achieve a certain level of success.

Design of markets and mechanisms of transactions. Initially the primary e-commerce activities were business-to-business (B2B) transactions. These activities quickly expanded to include sales to consumers via electronic retailing (e-tailing), often called business-to-consumer (B2C). Since the late 1990s, e-commerce has expanded to include consumer-to-consumer (C2C) websites, including eBay, and consumer-to-business (C2B) services such as Priceline, where several hotels will compete for the purchase dollars of consumers. Each of these types of transactions can be completed within the general structure of one of the many different types of e-commerce models to generate revenue.

Automated negotiation and peer-to-peer distribution systems. Auction models allow an internet user to assume the role of a buyer using either the reverse-auction model, where the buyer sets a price and sellers have to compete to beat that price, or the reverse-price model, where the seller sets the minimum price that will be accepted. Auction sites such as eBay update listings, feature items, facilitate payments, and earn submission and commission fees, but they leave the process of delivery up to the actual buyers.

Dynamic-pricing models include the name-your-price companies, such as Priceline, that use a shopping bot to collect bids from customers and deliver these bids to the providers of services to see if they are accepted. A shopping bot is a computer program that searches through vast amounts of information, then collects, summarizes, and reports the information. This is one example of the use of intelligent agents, or software programs that have been designed to gather information, by e-businesses. Priceline's immense success is due in part to its use of this technology; however, the

company phased out its name-your-price tool for flights in 2016 and for car rentals in 2018.

Network resource allocation: electronic data interchange (EDI). Portal models present a variety of news, weather, sports, and shopping all on one web page, allowing a visitor to see an overview and then choose to obtain more in-depth information. Vertical portals are specific for a single item, while horizontal portals function as search engines with access to a large range of items. Storefront models require a product line to be accessible online via the merchant server so that customers can select items from the database of products and collect them in the order-processing technology called a shopping cart. Businesses use EDI as a standardized protocol for communication to monitor daily inventory, shipments, and payments. Standardized forms for invoices and purchase orders are routinely accessible via the use of extensible markup language, or XML. Companies such as TIBCO Software and Commerce One (which was later acquired by Perfect Commerce and in turn by Proactis) were created to help companies move their businesses to the web via B2B techniques. The transition of traditional brick-and-mortar stores to click-and-mortar stores has helped decrease lead time and has caused an increase of just-in-time (JIT) inventory management. JIT inventory management allows e-businesses to save money because the companies do not overbuy goods and create an inventory surplus that they then have to worry about storing and selling, which decreases overhead costs.

APPLICATIONS AND PRODUCTS

E-commerce has spawned a variety of applications and products that both facilitate e-businesses and enhance people's lives.

Consumer products. Smartphones and tablet computers have been among the most popular consumer digital purchases. The proliferation of mobile devices, including laptop computers and smartphones, boosts the e-commerce industry by giving

consumers the means to remain almost constantly connected to the internet and therefore more likely to make online purchases. The rapid expansion of the market for application software, or apps, in the 2010s presented a major development in internet retailing, including the controversial practice of in-app purchases. In the 2020s, developments such as augmented reality (AR) technology benefit e-commerce, especially fashion and décor industries, as it provides a virtual interaction with products before purchases. Other tools include artificial intelligence (AI) and progressive web applications (PWAs). AI helps e-commerce companies personalize customer experiences and enables them to offer benefits such as visual search, which allows customers to submit pictures of products they are interested in.

Both contact and contactless "smart cards," which resemble credit cards, have been developed to store much more information (banking, retail, identification, health care) on a microprocessor embedded in the card. Examples of smart cards include cards used to make contactless fare payments in public-transportation systems throughout the United States, such as the Massachusetts Bay Transportation Authority's CharlieCard. Smart cards are more secure than credit cards because they are encrypted and password protected.

Security applications and products. Companies have been created to help merchants accept credit-card payments online, which are called card-not-present (CNP) transactions. These companies, such as Stripe and Square, offer services to facilitate the authentication and authorization processes through SSL or TLS protocols to minimize fraud. Additional security features include firewalls, encryption, and antivirus software. A number of companies, including many major credit-card companies, have introduced digital wallets that allow customers to save their shipment address and payment information securely in an online database so that purchases can be made with one click of the mouse, instead of

having to reenter the same information each time. In 1999, the Electronic Commerce Modeling Language (ECML) emerged as the protocol for digital-wallet usage by merchants. PayPal can be used to transfer payments between consumers securely by simply creating an account using an email address and a credit card or checking account, which is then used to pay for goods and services. PayPal is especially secure because credit-card information is checked before the transaction actually begins. This allows for payment to take place in real time, minimizing the opportunity for fraud. Other applications, such as Venmo, have made person-to-person payments by phone extremely easy, and services such as Apple Pay and Google Pay can be used to make secure online payments in addition to offline contactless payments.

Applications using wireless transactions. Mobile e-commerce, or m-commerce, has become increasingly important due to significant advances in wireless technology. The fourth generation of mobile technology, called 4G, offers a maximum speed of 150 megabits per second (Mbps), while successor 4G Long Term Evolution Advanced (LTE-A) offers a maximum speed of between 300 Mbps and 1,000 Mbps, or one gigabit per second (Gbps). The fifth generation of mobile technology, 5G, is significantly faster, with a maximum speed of between one and ten Gbps. With the increased popularity of apps, such as those offered by Apple's iOS App Store and Android's Google Play, m-commerce has become an important segment of the e-commerce market.

CAREERS AND COURSEWORK

Universities such as the University of California in Los Angeles and Arizona State University offer undergraduate courses in digital and integrated marketing communication. Job titles, career paths, and salaries within the field of e-commerce vary a great deal. Some of the typical job titles include website developer, web designer, database

administrator, web analyst, website manager, and programmer. Jobs related to web content require skills in web-development tools and software languages, including hypertext markup language (HTML), XML, Java, and JavaScript. Database administrators focus less on these web tools and languages and more on database-related tools, such as structured query language (SQL), Microsoft Access, and Oracle Database. Knowledge of computer networks and operating systems is also very helpful. Aspirants can work as e-commerce specialists, online sales consultants, customer service specialists, and operations logistics.

SOCIAL CONTEXT AND FUTURE PROSPECTS

Due in part to the easy accessibility of goods and services via the internet, online businesses have become increasingly competitive, with more made-to-order goods being produced by companies of all sizes and corresponding decreases in the costs associated with the maintenance of a large inventory. Since so much more data is exchanged digitally via stock trades, mortgages, purchases of consumer goods, payment of bills, and banking transactions, it is conceivable that eventually digital cash and smart cards could replace traditional cash completely. Because consumers enjoy the comparison shopping among goods offered by companies all over the world, as well as the twenty-four-hour-a-day, seven-days-a-week convenience of online shopping, sales at traditional brick-and-mortar stores will no doubt continue to decline, or at least migrate toward those goods that consumers prefer not to purchase online.

Online retailers such as Amazon continue to experiment with methods for more efficient supply chain and logistics systems; one notable project has involved the use of drones to deliver packages to consumers after an online purchase. Other shipping innovations have included Amazon's partnership with the US Postal Service (USPS) to provide package delivery on Sundays and the creation of local

centers where consumers can pick up purchased items rather than wait for local delivery.

Despite continuing growth, e-commerce does face important challenges. Security threats such as hacking, identity theft, and other types of cybertheft have become problems, which has only increased the need for better security tools, such as digital certificates and digital signatures. Increased security needs will continue to fuel the ever-expanding internet security industry.

Beginning in 2020, the coronavirus (COVID-19) pandemic negatively affected global economic activities and industries alike due to lockdowns imposed by governments. The only sector that saw growth during this period was e-commerce, as consumers and businesses used this channel to buy and sell products and services online. Experts believed that the impact of the pandemic on the growth of the e-commerce sector would be long-term due to increased digitalization.

—Jeanne L. Kuhler

Further Reading

- Castro, Elizabeth, and Bruce Hyslop. *HTML and CSS*. 8th ed., Peachpit Press, 2014.
- Chaffey, Dave, Tanya Hemphill, and David Edmundson-Bird. *Digital Business and E-Commerce Management*. 7th ed., Pearson Education, 2019.
- Chevalier, Stephanie. “Global Retail E-Commerce Sales 2014–2026.” *Statista*, 21 Sept. 2022, www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales.
- Cramer-Flood, Ethan. “Global Ecommerce Update 2021: Worldwide Ecommerce Will Approach \$5 Trillion This Year.” *eMarketer, Business Insider Intelligence*, Jan. 2021, www.emarketer.com/content/global-ecommerce-update-2021.
- “E-Commerce Cyber Security: An Introduction for Online Merchants.” *Get Cyber Safe*, 15 June 2020, www.getcybersafe.gc.ca/en/blogs/e-commerce-cyber-security-introduction-online-merchants.
- Jansen, Mark, and Paula Beaton. “5G vs. 4G: How Does the Newest Network Improve on the Last?” *DigitalTrends*, 22 Apr. 2022, www.digitaltrends.com/mobile/5g-vs-4g.

Laudon, Kenneth C., and Carol Guercio Traver.

E-Commerce 2019. 15th ed., Pearson Education, 2020.

Sherif, Mostafa Hashem. *Protocols for Secure Electronic Commerce*. 3rd ed., CRC Press, 2018.

Turban, Efraim, Carol Pollard, and Gregory Wood. *Information Technology for Management: On-Demand Strategies for Performance, Growth and Sustainability*. 11th ed., John Wiley & Sons, 2018.

Umar, Amjad. “IT Infrastructure to Enable Next Generation Enterprises.” *Information Systems Frontiers*, vol. 7, no. 3, 2005, pp. 217–56.

Wei, June. *Mobile Electronic Commerce: Foundations, Development, and Applications*. CRC Press, 2015.

EMAIL AND BUSINESS

ABSTRACT

Electronic mail, or email, started in 1965 as a way for users who were time-sharing a single mainframe computer to communicate with one another. The ability to communicate with others who were on different time schedules was of immense value, and the technology was soon expanded to allow users to pass messages between different servers. Although initially email was used in government and research institutions, businesses soon adopted it when the benefits became evident. Email has replaced voice and physical mail as the primary means of communication in many businesses. It has spawned support industries that earn billions of dollars per year.

BACKGROUND

Much of the business world relies on communication between parties in separate physical locations. Email provides a fast and efficient method of information exchange at little cost per message. It also eliminates the need for communicating parties to interface with one another at the same time, as is required in telephone calls or teleconferences.

Email technology’s savings in time alone was enough to motivate most businesses to adopt the technology as a standard medium of

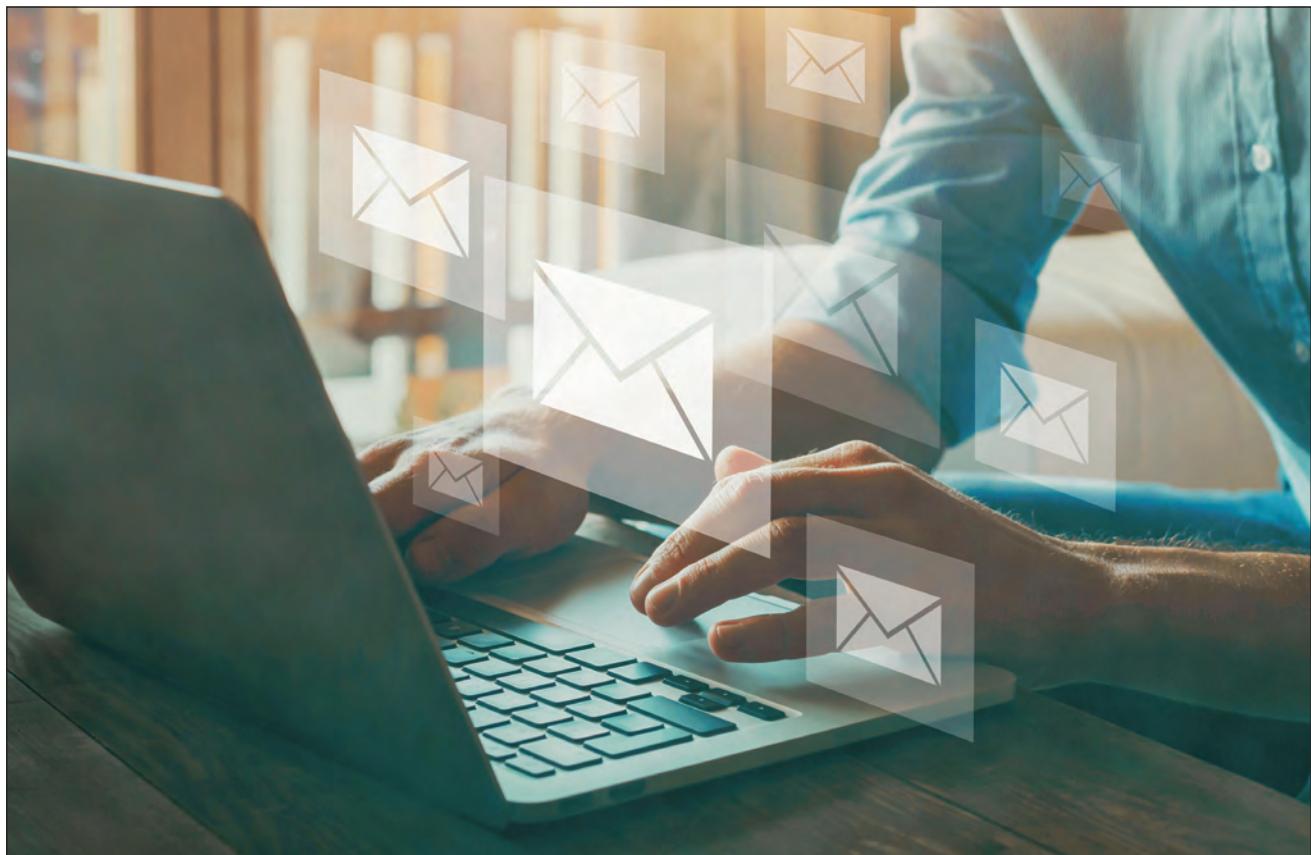


Photo via iStock/ anyaberkut. [Used under license.]

communication. As the medium developed, the ability to store and quickly access email messages as well as attached documents, files, and other information provided new valuable functions and created more cost savings for companies. Email quickly became such a vital resource that many business professionals are estimated to spend up to 50 percent of their working time using email. In fact, many analysts see modern businesses as almost dangerously reliant on email for communication; many studies have found that internet-based businesses stand to lose tens of thousands of dollars per hour if there is an outage of their email servers. The drop in communications can also reduce the ability of workers to complete their tasks, resulting in a loss of person-hours and damaging customer relations.

Psychological and sociological studies have also questioned the impact of many employees' near-constant connection to work through email, as the technology brings the expectation of rapid response to any communication and therefore potentially increased stress. Nevertheless, companies' use of email continues to grow, with an increasing focus on effective use of mobile platforms such as smartphones and tablet computers.

OVERVIEW

While email has proven vital to the operations of most businesses, the email industry itself has grown into a major branch of internet-based business. Companies providing email services, such as Apple, Google, and Microsoft, compete for users by

designing email features to be easily compatible with their other products. Each email interface, whether its own program or accessed through a web browser, provides different details that may appeal to the specific needs of the user; some elements may also be customizable on the individual level. The design, construction, sales, and maintenance of the servers needed to sustain email operations have also developed into a significant industry.

Businesses have also capitalized on the ability to mass market to consumers via email as part of their wider internet marketing strategies. More customers can be reached at little or no cost by email than by previous outreach methods such as telephone calls and traditional media advertising. The business of selling lists of email addresses has become a staple of the mass-mailing industry generating millions of dollars. Another method is the use of opt-in lists, in which consumers voluntarily choose to receive emails from companies they are interested in. This helps companies ensure their emails and marketing materials are reaching customers rather than going undelivered or ignored. Such emails (often composed and sent automatically) may include promotional offers or exclusive information as an incentive for consumers to sign up, expanding the company's advertising audience and providing other valuable statistics about its customers that can be used to further develop effective marketing strategies.

Increasingly, businesses focus on making their email efforts compatible and effective with mobile devices such as smartphones and tablets used by more and more consumers. As data collection and advanced metric analysis becomes more sophisticated, email marketing has also moved towards providing a higher level of personalization, with content tailored towards the interest of each recipient.

Despite the success of mass emailing as a marketing tool, it has created problems as well as business opportunities. Unsolicited commercial email, commonly called "spam," comes from a business or

individual misusing the system. Spam has the potential to clog users' email inboxes, wasting valuable work hours that must be spent separating important messages from unwanted advertisements. An industry quickly arose aimed at blocking spam, based around spam filter programs using statistical methods to weed out undesirable emails. Several countries have even passed laws in attempts to combat rampant spam emailing, including the CAN-SPAM Act of 2003 (United States) and the Canada Anti-Spam Law that became effective in 2014, which often require that commercial emails include the ability for recipients to unsubscribe from the mailing list.

The ability to attach files to email messages has also led to the propagation of computer viruses, another potential danger to businesses that rely on computers. Phishing and social engineering attempts carried out via email likewise represent substantial threats to businesses in a wide range of industries. The need to guard against these problems has itself spawned another industry that makes billions of dollars per year on computer security efforts.

—James J. Heiney

Further Reading

- Cortada, James W. *The Digital Hand: How Computers Changed the Work of American Manufacturing, Transportation, and Retail Industries*. Oxford UP, 2004.
- Gibbs, Samuel. "How Did Email Grow from Messages between Academics to a Global Epidemic?" *The Guardian*, 7 Mar. 2016, www.theguardian.com/technology/2016/mar/07/email-ray-tomlinson-history.
- Hughes, Arthur Middleton. "Why Email Marketing Is King." *Harvard Business Review*, 21 Aug. 2012, hbr.org/2012/08/why-email-marketing-is-king.
- Okin, J. R. *The Internet Revolution: The Not-for-Dummies Guide to the History, Technology, and Use of the Internet*. Ironbound, 2005.
- Segal, Edward. "How and Why Businesses Are Vulnerable to Email-Based Cyberattacks: New Study." *Forbes*, 10 Nov. 2022, www.forbes.com/sites/edwardsegal/2022/11/10/how-and-why-businesses-are-vulnerable-to-email-based-cyberattacks-new-study/?sh=2f370f692ae0.

ENCRYPTION

ABSTRACT

Encryption is a process in which data is translated into code that can only be read by a person with the correct encryption key. It focuses on protecting data content rather than preventing unauthorized interception. Encryption is essential in intelligence and national security and is also common in commercial applications. Various software programs are available that allow users to encrypt personal data and digital messages.

BACKGROUND

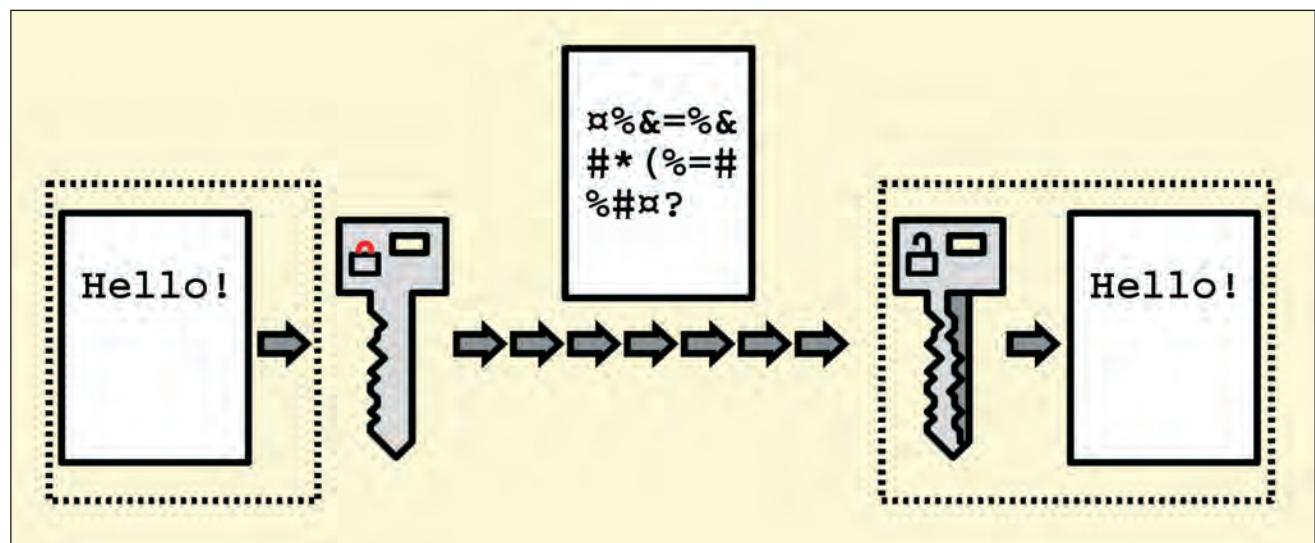
The study of different encryption techniques is called “cryptography.” The original, unencrypted data is called the “plaintext.” Encryption uses an algorithm called a “cipher” to convert plaintext into ciphertext. The ciphertext can then be deciphered by using another algorithm known as the “decryption key” or “cipher key.”

A key is a string of characters applied to the plaintext to convert it to ciphertext, or vice versa. Depending on the keys used, encryption may be either symmetric or asymmetric. Symmetric-key encryption uses the same key for both encoding and

decoding. The key used to encode and decode the data must be kept secret, as anyone with access to the key can translate the ciphertext into plaintext. The oldest known cryptography systems used alphanumeric substitution algorithms, which are a type of symmetric encryption. Symmetric-key algorithms are simple to create but vulnerable to interception.

In asymmetric-key encryption, the sender and receiver use different but related keys. First, the receiver uses an algorithm to generate two keys, one to encrypt the data and another to decrypt it. The encryption key, also called the “public key,” is made available to anyone who wishes to send the receiver a message. (For this reason, asymmetric-key encryption is also known as “public-key encryption.”) The decryption key, or private key, remains known only to the receiver. It is also possible to encrypt data using the private key and decrypt it using the public key. However, the same key cannot be used to both encrypt and decrypt.

Asymmetric-key encryption works because the mathematical algorithms used to create the public and private keys are so complex that it is computationally impractical to determine the private key based on the public key. This complexity



A simple illustration of public-key cryptography, one of the most widely used forms of encryption. Image by Johannes Landin, via Wikimedia Commons.

also means that asymmetric encryption is slower and requires more processing power. First developed in the 1970s, asymmetric encryption is the standard form of encryption used to protect internet data transmission.

OVERVIEW

Authentication is the process of verifying the identity of a sender or the authenticity of the data sent. A common method of authentication is a hashing algorithm, which translates a string of data into a fixed-length number sequence known as a “hash value.” This value can be reverted to the original data using the same algorithm. The mathematical complexity of hashing algorithms makes it extremely difficult to decrypt hashed data without knowing the exact algorithm used. For example, a 128-bit hashing algorithm can generate 2^{128} different possible hash values.

In order to authenticate sent data, such as a message, the sender may first convert the data into a hash value. This value, also called a “message digest,” may then be encrypted using a private key unique to the sender. This creates a digital signature that verifies the authenticity of the message and the identity of the sender. The original unhashed message is then encrypted using the public key that corresponds to the receiver’s private key. Both the privately encrypted digest and the publicly encrypted message are sent to the receiver, who decrypts the original message using their private key and decrypts the message digest using the sender’s public key. The receiver then hashes the original message using the same algorithm as the sender. If the message is authentic, the decrypted digest and the new digest should match.

ENCRYPTION SYSTEMS IN PRACTICE

One of the most commonly used encryption programs is Pretty Good Privacy (PGP). It was developed in 1991 and combines symmetric- and

asymmetric-key encryption. The original message is encrypted using a unique one-time-only private key called a “session key.” The session key is then encrypted using the receiver’s public key, so that it can only be decrypted using the receiver’s private key. This encrypted key is sent to the receiver along with the encrypted message. The receiver uses their private key to decrypt the session key, which can then be used to decrypt the message. For added security and authentication, PGP also uses a digital signature system that compares the decrypted message against a message digest. The PGP system is one of the standards in personal and corporate security and is highly resistant to attack. The data security company Symantec acquired PGP in 2010 and subsequently incorporated the software into many of its encryption programs. The relevant division of Symantec was in turn acquired by the company Broadcom in 2019.

Encryption can be based on either hardware or software. Most modern encryption systems are based on software programs that can be installed on a system to protect data contained in or produced by a variety of other programs. Encryption based on hardware is less vulnerable to outside attack. Some hardware devices, such as self-encrypting drives (SEDs), come with built-in hardware encryption and are useful for high-security data. However, hardware encryption is less flexible and can be prohibitively costly to implement on a wide scale. Essentially, software encryption tends to be more flexible and widely usable, while hardware encryption is more secure and may be more efficient for high-security systems.

—Micah L. Issitt

Further Reading

Delfs, Hans, and Helmut Knebl. *Introduction to Cryptography: Principles and Applications*. 3rd ed., Springer, 2015.

History of Cryptography: An Easy to Understand History of Cryptography. Thawte, 2013.

- Holden, Joshua. *The Mathematics of Secrets: Cryptography from Caesar Ciphers to Digital Encryption*. Princeton UP, 2018.
- “How to: Use PGP for Windows.” *Surveillance Self-Defense*, 17 June 2018, ssd.eff.org/module/how-use-pgp-windows.
- Levy, Stephen. “Almost 50 Years into the Crypto Wars, Encryption’s Opponents Are Still Wrong.” *Wired*, 21 July 2023, www.wired.com/story/plaintext-50-years-into-the-crypto-wars-encryptions-opponents-are-still-wrong.
- Watters, Paul A. *Cybercrime and Cybersecurity*. CRC Press, 2023.

END-USER CYBERSECURITY EDUCATION

ABSTRACT

The end user is the primary person who uses a product or service. In information technology (IT), that person accesses the product or service via a smartphone, a tablet, a computer, a gaming console, or some other terminal. Because the end user is not involved in the creation or ongoing maintenance of the product or service, they have less technical expertise. For this reason, their cybersecurity knowledge and education requirements are different from those of the individuals who created or maintain the product or service. Unfortunately, because technology evolves and new versions of products and new services are often released, security threats evolve along with them. Security education is not static. End-user security education is an ongoing concern.

BACKGROUND

The *Merriam-Webster* dictionary defines the end user as “the ultimate consumer of a finished product.” While the term has been around since 1945, its usage shifted to a more computer- and internet-related focus by the twenty-first century, while the end user in other contexts is more commonly referred to as the consumer. The term end user became more common in the IT context and is used in contrast to those who design, create, support, and

maintain the product. It should be noted that while an organization such as a hospital may buy a product, the doctors and nurses are the end users, not the hospital.

The term “cyber,” according to *Merriam-Webster*, generally refers to anything “of, relating to, or involving computers or computer networks,” so cybersecurity involves security matters with regard to computers or the internet. The prefix “cyber-” came from the word “cybernetic,” which in turn originated from the ancient Greek word *kubernetes*, meaning “steersman,” as in one who steers a ship.

OVERVIEW

While cybersecurity is widely understood to be important, it is not always clear what cybersecurity entails. Society has become progressively more reliant on computers and networks for everything from making a phone call to driving a car or paying for groceries. There are computers and networks involved in nearly every aspect of twenty-first-century life, and there are people who seek to exploit those computers and networks to enrich themselves. Although there are many ways to discuss information technology (IT), three key areas of cybersecurity are vulnerability, exploitation, and social engineering.

Per the Common Vulnerabilities and Exposures (CVE) Program, whose mission it is to “identify, define, and catalog publicly disclosed cybersecurity vulnerabilities” and thus create a standard way of communicating across many organizations, a vulnerability is a “flaw in a software, firmware, hardware, or service component resulting from a weakness that can be exploited, causing a negative impact to the confidentiality, integrity, or availability of an impacted component or components.”

For example, an author places a form on their website for fans of their writing to contact them. The fan must fill in their name and email address before they can write a note. If the program that allows

them to fill in the form is not properly configured, this is a vulnerability. When a bad actor tries putting a variety of different things into the form to abuse it and successfully gains access to the website or even the computer behind the form, this is an exploitation of a vulnerability. If the bad actor gains access to the computer behind the form and sends out emails to the author's fans asking for money, this is social engineering.

As defined by the Carnegie Mellon University Information Security Office, "social engineering is the tactic of manipulating, influencing, or deceiving a victim in order to gain control over a computer system, or to steal personal and financial information. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information."

Banks and credit card companies reach end users via email, but bad actors also send out emails that look exactly the same. This is one of the most common types of social engineering, known as "phishing," a play on the word "fishing." Through these lookalike emails (or "phish"), bad actors try to manipulate end users into divulging personal identifiable information (PII) or financial information that can be used to defraud the end user.

The challenge of cybersecurity education is that the level of complexity required to create, manage, and use these systems makes it very difficult to educate the end user in how to remain secure. For instance, cybersecurity experts require end users to use complicated passwords and simultaneously tell the end users that they should not write those passwords down. This leaves end users confused about what is secure and what is not secure.

To assist the end user in avoiding cybersecurity problems, many organizations offer cybersecurity education. Some of it is aimed at the general public, as when the IRS takes out advertisements to remind people that the agency will never contact taxpayers about their bills or refunds through electronic

means. Other companies have their own information, explanations, and disclaimers on their websites. Many organizations put their employees through professional training sessions in cybersecurity, because mistakes by those employees can impact their whole organization.

Because cybersecurity threats evolve as technology evolves, end users should consider approaching the subject with the mindset of continuing education, especially with regard to the brands of software, hardware, and applications that they use. Most systems and software are capable of automatically updating to apply patches or switch to the latest version, and end users should configure their systems to allow those updates. End users should talk to their employers about whether they offer cybersecurity education; likewise, they should consider taking a class, reading a book, or searching for articles on the subject. Overall, it is crucial for end users to stop and think before reacting to an email, a text message, a pop-up window, or anything else that seems a little unusual. Cybersecurity takes many forms, and there is no single path to knowledge.

—Kelly J. Cooper

Further Reading

- Coe, Taylor. "Where Does the Word *Cyber* Come From?" *OUPblog*, 28 Mar. 2015, blog.oup.com/2015/03/cyber-word-origins/.
- "Cyber." *Merriam-Webster*, 2023, www.merriam-webster.com/dictionary/cyber.
- Cybersecurity & Infrastructure Security Agency*, 2023, www.cisa.gov.
- "End User." *Merriam-Webster*, 2023, www.merriam-webster.com/dictionary/end%20user.
- "Free Cyber Security Training." *SANS*, 1 June 2023, www.sans.org/cyberaces.
- Hafner, Katie. *Where Wizards Stay Up Late: The Origins of The Internet*. Simon & Schuster, 1998.
- Levy, Steven. *Hackers: Heroes of the Computer Revolution*. O'Reilly Media, 2010.

Recommendations for Database Management System Standards:
NBS Special Publication 500-51. US Department of Commerce National Bureau of Standards, 1979, www.govinfo.gov/content/pkg/GOVPUB-C13-d091da4af6988e05e8ebba2ee5df278d/pdf/GOVPUB-C13-d091da4af6988e05e8ebba2ee5df278d.pdf.

“Social Engineering.” *Carnegie Mellon University Information Security Office*, www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html.

STOP. THINK. CONNECT, 2023, www.stopthinkconnect.org.

“Taxpayers See Wave of Summer Email, Text Scams; IRS Urges Extra Caution with Flood of Schemes Involving Economic Impact Payments, Employee Retention Credits, Tax Refunds.” *IRS*, 21 July 2023, www.irs.gov/newsroom/taxpayers-see-wave-of-summer-email-text-scams-irs-urges-extra-caution-with-flood-of-schemes-involving-economic-impact-payments-employee-retention-credits-tax-refunds.

“Vulnerability.” *CVE*, 2023, www.cve.org/Resources/Support/Glossary?activeTerm=glossaryVulnerability.

ESTONIA CYBERATTACK

ABSTRACT

Starting at the end of April and continuing into May of 2007, several institutions in Estonia, including the nation’s parliament, largest bank, and newspapers, were the target of cyberattacks. Computers linked to the internet were bombarded with “requests for service”—in the form of messages, efforts to log in, or simply logging on (as to a newspaper site)—many times greater than normal. The sudden burst in volume of requests caused computers to crash. Because the bursts of requests, known as distributed denial-of-service (DDoS) attacks, coincided with a political controversy over the government’s decision to relocate a statue commemorating the Russian army’s expulsion of German troops at the end of World War II, the computer attacks were widely viewed by North Atlantic Treaty Organization (NATO) officials as an example of “cyberwar,” an organized attempt to bring an entire country’s computer network to its knees.

BACKGROUND

For about a month, from late April through May 2007, computers in Estonia linked to the internet were the targets of an intense attack evidently designed to bring the computers down and, in the process, wreak havoc on the Estonian economy. Experts in the topic of cyberwar and cyberterrorism from several countries, including the United States, point to the events in Estonia as a prototype of a new form of economic warfare in the twenty-first century.

The basic weapon in the cyberwar waged against Estonia was the distributed denial-of-service (DDoS) attack. Such an attack involves bombarding target computers, such as those operated by banks and available to consumers via internet connections, with tens of millions of simultaneous requests for service, such as a query about an account balance or other information available on the computer. When the level of requests exceeds normal expectations by many times over, the target computers cannot cope and crash, thus denying service to legitimate users.

DDoS attacks often involve “botnets” (as in robotic networks) and “zombies.” Those orchestrating the attack implant, usually surreptitiously but sometimes in the open, microprograms that instruct unsuspecting computers on the internet to begin asking the target computer(s) for service at a given time. This malicious software (malware) can be spread to large numbers of computers—numbering in the hundreds of thousands, including individual person computers connected to the internet on a more or less continuous basis—thereby creating a large network of zombie computers located around the world.

Computer experts who analyzed the cyberattack in Estonia in 2007 believe such a botnet was responsible for attacks that brought down large numbers of computers in Estonia, which is among the countries with the largest networks used for such commonplace activities as paying for parking on the street,

retail sales, and communications ranging from email between members of parliament to internet chat sessions. While DDoS attacks are not uncommon, the instance in Estonia in 2007 was different in its scale, insofar as the attacks lasted for many hours at a time and were repeated day after day. Several of the country's banks, for example, were unable to transfer funds (both between accounts and to automated teller machines [ATMs]) or service retail terminals.

The attack on Estonia was not a single, sustained burst, but rather a series of attacks that occurred over several weeks. Two of the most intense days were May 9, 2007—which coincided with Victory Day, a Russian holiday marking the Soviet defeat of Nazi Germany—and May 10, 2007, when Estonia's largest bank had to shut down its online services for an hour in the face of a DDoS assault. According to an analysis of the May 10 attack, organizers had rented time on servers in order to launch the onslaught; when their time expired, so did the intensity of the DDoS. Computers in Estonia targeted with DDoS attacks included the websites of the Estonian president, prime minister, parliament, and several government agencies, as well as several daily newspapers and Estonia's largest bank.

The last major wave of DDoS assaults occurred on May 18, 2007, although attacks at a lower level continued through the end of the month.

OVERVIEW

One reason the Estonian experience became the subject of intense interest by government officials from the United States, among other countries, was its presumed political background. Estonian authorities had decided to move a memorial statue commemorating the role of the Red Army in expelling German troops from Estonia during World War II from a prominent park in the capital, Tallinn. The move of the statue sparked two nights of rioting in Tallinn in late April as well as a protest at the Estonian embassy in Moscow. The protests underscored

underlying tensions between Estonia's community of ethnic Russians, comprising about one-fourth of the population, and ethnic Estonians. The tensions reflected a long history of conflict over the status of Estonia, which was for centuries traded between shifting empires in Europe, including the Russian empire. Estonia fell under Soviet occupation in 1940, part of the Hitler-Stalin pact, and was later occupied by Nazi Germany from 1941 until 1944, when the Red Army drove out the German army. Several thousand Estonian guerrillas subsequently resisted the reincorporation of Estonia into the Union of Soviet Socialist Republics (USSR). It was in light of this history that removal of the memorial to Soviet troops was viewed by ethnic Russians—and possibly by the government of Russia—as a hostile act.

In advance of the attacks, detailed instructions were posted anonymously, but in the Russian language, on several websites telling how to participate in a DDoS siege and which computers inside Estonia to target. During the course of the attacks, Estonia's defense minister said that "at the present time, we are not able to prove direct state links. All we can say is that a server in our president's office got a query from an internet protocol (IP) address in the Russian administration." The foreign ministry also circulated a list of internet addresses that participated in the attacks, including some inside the Russian government. The Russian government formally denied having any role in the DDoS attacks. (Requests that seemed to comprise the DDoS were also traced to many other countries.) Part of the nature of cyberattacks is that their origins are difficult if not impossible to trace, especially since botnets can be constructed to include computers from around the globe. In the case of the Estonia attacks, for example, computers in Vietnam and the United States were among those found to be participating in the DDoS attacks, presumably unconsciously.

No quid pro quo, such as payment of funds, was ever demanded as a condition of halting the cyberattacks.

DEFENSE AND PREVENTION

The first layer of defense in a DDoS attack is to block traffic from suspected computers—technically, from suspected internet addresses. In the case of the attack on Estonia, this meant addresses based outside the country, from countries ranging from Peru to China to the United States. This isolation began on the first day of DDoS attacks that had shut down servers for Estonia’s parliament—among other things, depriving legislators of email—and a hacker’s penetration of the Reform Party’s website.

The DDoS attacks in Estonia were quickly the subject of investigation by cyberwarfare experts from several countries, including the United States and Israel, partly because of the presumed background suggested that the Estonian experience could be a precursor of future cyberwars. The headquarters of the North Atlantic Treaty Organization (NATO) dispatched experts to Tallinn to advise the Estonian government.

In general, a defense against a DDoS attack relies on blocking messages from designated internet addresses or, as in the case of Estonia, shutting down large parts of the national network to access from outside the country. One side effect of doing so

was to deprive Estonians traveling outside the country from access to email stored on domestic servers, or to their bank accounts.

In August of 2022, additional DDoS attacks—allegedly perpetrated by a Russian hacker organization called Killnet—were carried out against Estonian government agencies and other institutions. However, the attacks received relatively little notice in Estonia, and the country’s government attributed the minimal impacts to cybersecurity improvements made within Estonia in the years following the 2007 attacks.

Further Reading

- “Estonian Denial of Service Incident.” *Council on Foreign Relations*, May 2007, www.cfr.org/cyber-operations/estonian-denial-service-incident.
- Granville, Johanna. “Tracking Computer Hacking: The Dangers of Cyber Terrorism.” *Global Society: Journal of Interdisciplinary International Relations*, vol. 17, no. 1, 2003, pp. 89–97.
- Stytz, Martin R. “Cyber-warfare Distributed Training.” *Military Technology*, vol. 30, no. 11, 2006, pp. 95–99.
- Sytas, Andrius. “Estonia Says It Repelled Major Cyber Attack after Removing Soviet Monuments.” *Reuters*, 18 Aug. 2022, www.reuters.com/world/europe/estonia-says-it-repelled-major-cyber-attack-after-removing-soviet-monuments-2022-08-18.
- Wilson, Clay. *CRS Report for Congress: Information Warfare and Cyberwar; Capabilities and Related Policy Issues*. Congressional Research Service, 2004, apps.dtic.mil/sti/tr/pdf/ADA477185.pdf.

F

FAX MACHINE, COPIER, AND PRINTER ANALYSIS

ABSTRACT

Fax machine, copier, and printer analysis is the examination of output from inkjet and laser computer printers, electrostatic copiers, and fax machines to determine the origin and/or authenticity of printed documents.

BACKGROUND

Since the mid-1980s, a high proportion of documents relevant to civil and criminal cases have been produced by fax machines, photocopiers, and printers connected to computers. Although appearing uniform to casual inspection, such documents have physical and chemical characteristics enabling a forensic examiner to identify the equipment used to produce the output and the time frame in which it was generated. Techniques rely on the extremely rapid rate of change in the printer industry and require sophisticated equipment linked to computer programs capable of discerning subtle differences in the patterns of complex digital signals.

Printer analysis based on output is useful in two broad classes of cases: document authentication (generally in cases of suspected forgery) where the main aim is to demonstrate that the document, or portions of it, could *not* have come from a specific source, and document tracing, where the aim is to connect the item with a specific printer and time frame. The latter is considerably more difficult. Document tracing is most likely to arise in criminal cases involving ransom notes, extortion, and blackmail. It may also provide key evidence in terrorism and espionage investigations.

OVERVIEW

Magnification. Examination under low magnification is usually sufficient to distinguish different classes of printers. Inkjet printers produce a more blurred outline than laser printers and toner-based photocopiers. Older single-element printers leave an indentation on the paper similar to an electric typewriter. Printer output of any description can be distinguished from a typewritten original by the complete absence of erasures and strikeovers.

In an authentication case, the key question is usually whether two documents were produced on the same equipment. Visual inspection under low magnification can detect differences between typewritten text, and inkjet, laser and thermal printer output. Should this fail to detect any difference, the wide array of sophisticated techniques outlined below is available, but unless large sums of money are involved or the case is politically charged, these are seldom employed.

In their efforts to keep documents more secure from forgery, agencies are increasingly pairing the incorporation of features that cannot be faithfully reproduced by any current duplicating process into documents, with tools that the offices and individuals can use to rapidly scan for forgeries as a routine part of business practice. Microprinting, for example, uses minute hexagons to make up images on currency, licenses, and legal forms; no scanner or photocopier can currently reproduce the pattern precisely, and while the difference is not necessarily apparent to the naked eye, digital image scanners coupled with appropriate software can readily spot fakes, and this technology is becoming available to stores and offices. Unique biological taggants,

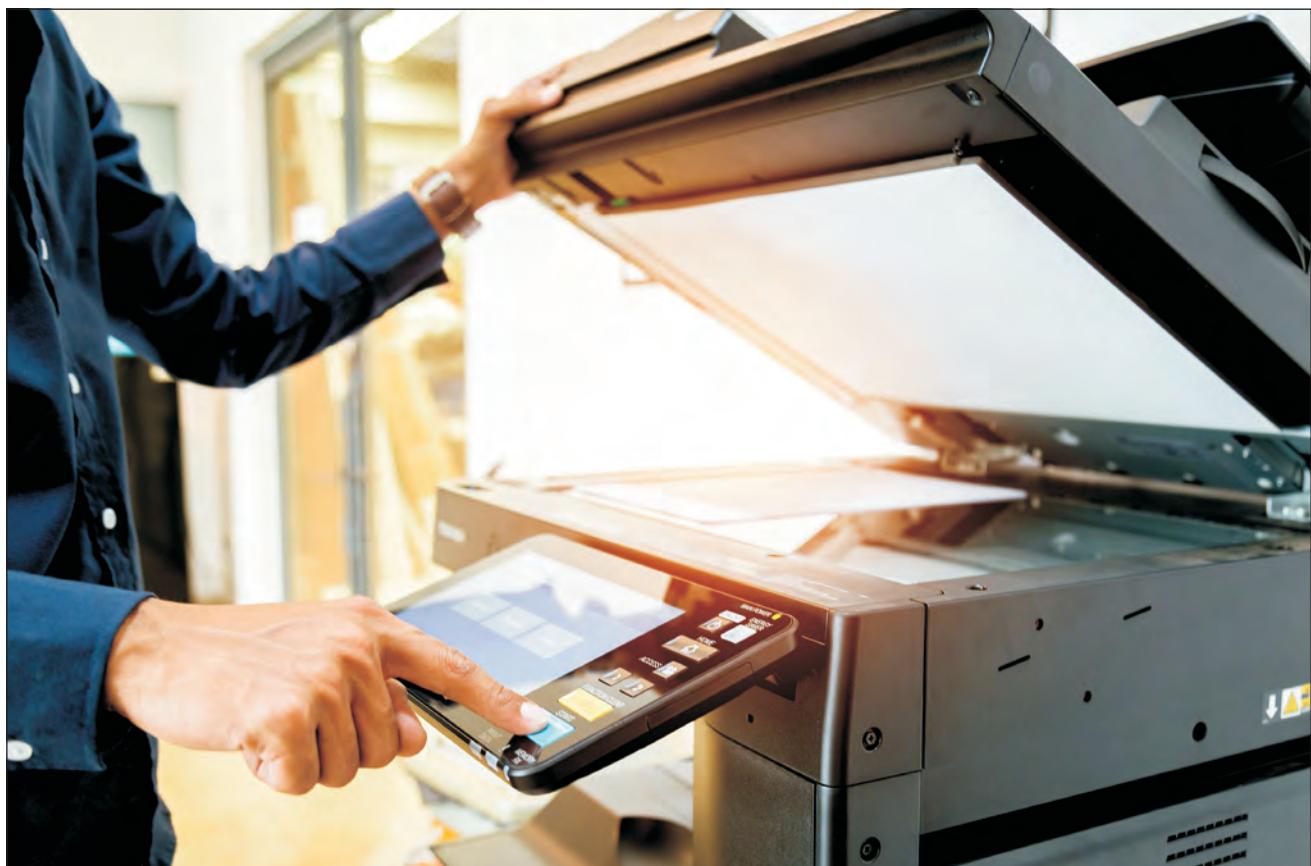


Photo via iStock/A stockphoto. [Used under license.]

thermochromics ink and ultraviolet (UV) visible features are other means of making documents difficult to forge.

An area of particular concern in the global market involves packaging on counterfeit goods, notably pharmaceuticals. Manufacturers are increasingly using the sophisticated technology developed for currency to render wholesale and retail packages difficult to forge, while detection techniques are used at destination to verify the authenticity of the packaging.

Electronic and chemical analysis methods. When low-volume laser and inkjet printers and copiers first hit the mass market, forensic specialists assumed that this would make tracing documents to individual printers virtually impossible. In fact, every brand

and model of printer (including the newer photocopiers that scan input prior to printing) has a distinctive electronic signature that can be “read” from the output using a scanner and appropriate software. One brand of higher-end color copier invisibly attaches the serial number of its machine to copies, a practice that may well expand. Computer analysis will also reveal banding and other flaws resulting from machine malfunction. Paper may be marked by damaged or improperly aligned feeding machinery. Incidental marks associated with dirty glass can originate either at input (scanner/fax) or at the time of printing.

The most powerful tools for tracing printer and copier output, however, rely on the chemical composition of dyes and toner, both the pigments

themselves and the compounds used to bind them to the paper. The exact formulation is specific not only to the manufacturer but also to a narrow time frame, measured in months.

Different tools provide complementary information. Scanning electron microscopy (SEM) produces a high-resolution image of surface features, including drying patterns of inks. As an adjunct to SEM, energy dispersive X-rays (EDX) analysis measures the X-ray emission spectra of compounds bombarded by electrons. An EDX reading indicates which atomic elements are present in which proportions. X-ray fluorescence spectroscopy detects the presence of certain compounds by the visible or UV light they emit when bombarded by X-rays.

Infrared absorption spectrometry detects specific types of chemical bonds in organic molecules. It is useful for distinguishing between chemically similar bonding agents. Thin layer chromatography and pyrolysis gas chromatography depend on the rate of diffusion of compounds and are useful for distinguishing mixtures of complex organic chemicals, such as those in dye-based inks.

In some cases the sequence and timing of an imprint may be at issue. Some inks and toners change in chemical composition over time. If portions of one part of a document overlap other portions, the sequence can be determined by partially stripping the upper layer and using digital imaging to determine which layer was stripped.

All of these spectrographic and chromatographic methods require extensive costly equipment, most of it, however, not specific to forensics. Most techniques involve sample destruction but can be used on very small amounts of material. Once a reading is obtained, the examiner uses a computer program to compare that reading either to a sample of known origin, or to a library of chemical signatures. Such libraries are maintained both by leading national forensic laboratories and by toner and ink manufacturers.

Analyses involving spectrography and digital image analysis have not replaced observers trained in visual examination, but increasingly courts are favoring hard scientific evidence over the more subjective testimony of human experts, especially in high-stakes cases.

Fraud and forgery detection is a growing field, particularly in Asia. The most persistent and organized criminals will undoubtedly become more adept at circumventing techniques now in place for detecting fraudulent and extortionist use of printers and photocopiers, rendering it necessary for forensic investigators to stay abreast of the rapidly evolving technology.

—Martha Sherwood

Further Reading

- Cicconi, Falvio, et al. "Forensic Analysis of Commercial Inks by Laser-Induced Breakdown Spectroscopy (LIBS)." *Sensors*, vol. 20, no. 13, 2020, www.mdpi.com/1424-8220/20/13/3744.
- Eckert, William G. *Introduction to Forensic Sciences*. CRC Press, 1997.
- Gianelli, Paul C., Edward J. Imwinkelried, Andrea Roth, and Jane Moriarty. *Scientific Evidence*. Lexis Nexis, 2012.
- Houck, Max M. *Forensic Science: Modern Methods of Solving Crime*. Praeger, 2007.
- Li, Ling. "Technology Designed to Combat Fakes in the Global Supply Chain." *Business Horizons*, vol. 56, no. 2, 2013, pp. 167–77.
- Nickell, Joe. *Detecting Forgery: Forensic Investigation of Documents*. UP of Kentucky, 1996.

FIREWALLS

ABSTRACT

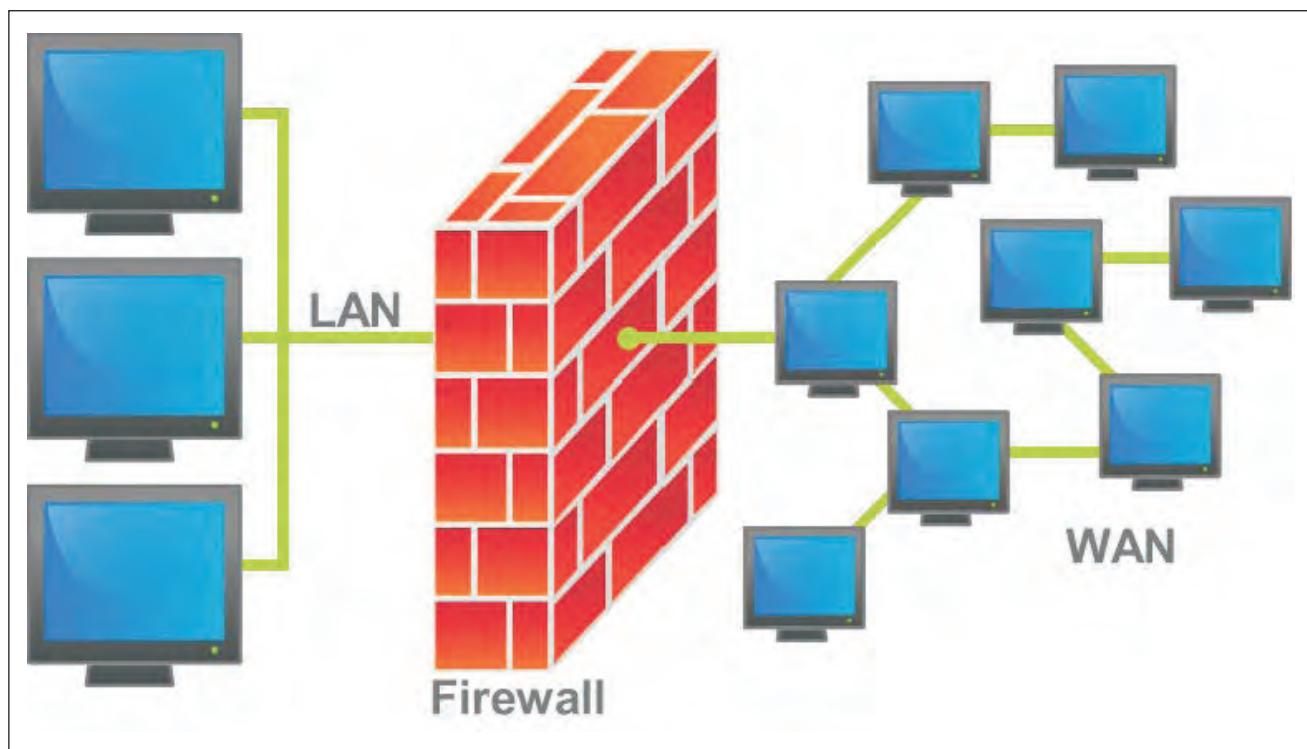
A firewall is a program designed to monitor the traffic entering and leaving a computer network or single device and prevent malicious programs or users from entering the protected system. Firewalls may protect a single device, such as a server or personal computer (PC), or even an entire computer network. They also differ in how they filter

data. Firewalls are used alongside other computer security measures to protect sensitive data.

BACKGROUND

In the early twenty-first century, increasing cybercrime and cyberterrorism made computer security a serious concern for governments, businesses and organizations, and the public. Nearly any computer system connected to the internet can be accessed by malicious users or infected by harmful programs such as viruses. Both large networks and single personal computers (PCs) face this risk. To prevent such security breaches, organizations and individuals use various security technologies, particularly firewalls. Firewalls are programs or sometimes dedicated devices that monitor the data entering a system and prevent unwanted data from doing so. This protects the computer from both malicious programs and unauthorized access.

The term “firewall” is borrowed from the field of building safety. In that field it refers to a wall specially built to stop the spread of fire within a structure. Computer firewalls fill a similar role, preventing harmful elements from entering the protected area. The idea of computer firewalls originated in the 1980s. At that time, network administrators used routers, devices that transfer data between networks, to separate one network from another. This stopped problems in one network from spreading into others. By the early 1990s, the proliferation of computer viruses and increased risk of hacking made the widespread need for firewalls clear. Some of the advances in that era, such as increased access to the internet and developments in operating systems, also introduced new vulnerabilities. Early firewalls relied heavily on the use of proxy servers. Proxy servers are servers through which all traffic flows before entering a user’s computer or network. In the



An illustration of a network-based firewall within a network. Image by Bruno Pedrozo, via Wikimedia Commons.

twenty-first century, firewalls can filter data according to varied criteria and protect a network at multiple points.

OVERVIEW

All firewalls work to prevent unwanted data from entering a computer or network. However, they do so in different ways. Commonly used firewalls can be in various positions relative to the rest of the system. An individual computer may have its own personal firewall, as may other networked devices such as servers. These are known as host-based firewalls because they protect a single host rather than the whole network. They protect computers and other devices not only from malicious programs or users on the internet but also from viruses and other threats that have already infiltrated the internal network, such as a corporate intranet, to which they belong. Network firewalls, on the other hand, are positioned at the entrance to the internal network. All traffic into or out of that network must filter through them. A network firewall may be a single device, such as a router or dedicated computer, which serves as the entrance point for all data. It then blocks any data that is malicious or otherwise unwanted. Application-level firewalls, which monitor and allow or disallow data transfers from and to applications, may be host based or network based.

Firewalls also vary based on how they filter data. Packet filters examine incoming data packets individually and determine whether to block or allow each one to proceed. They decide this based on factors such as the origin and destination of the packets. Stateful filters determine whether to admit or block incoming data based on the state of the connection. Firewalls that use stateful filtering can identify whether data packets trying to enter the computer system are part of an ongoing, active connection and determine whether to let them in based on that context. This allows them to examine

and filter incoming data more quickly than their stateless counterparts.

FIREWALLS AND COMPUTER SECURITY

By preventing malicious programs or users from accessing systems, firewalls protect sensitive data stored in or transmitted via computers. They are used to protect personally identifying information, such as Social Security numbers, as well as proprietary trade or government information. Both the technology industry and the public have put increased emphasis on such protections in the early twenty-first century, as identity theft, fraud, and other cybercrimes have become major issues. In light of such threats, firewalls play an essential role in the field of computer security. However, experts caution that a firewall should not be the sole security measure used. Rather, firewalls should be used along with other computer security practices. These practices include using secure passwords, regularly updating software to install patches and eliminate vulnerabilities, and avoiding accessing compromised websites or downloading files from suspicious sources.

—Joy Crelin

Further Reading

- “About Firewalls.” *University Information Technology Services Knowledge Base*, 1 June 2021, kb.iu.edu/d/aoru.
- Easttom, Chuck. *Computer Security Fundamentals*. 5th ed., Pearson, 2023.
- “How Firewalls Work.” *Boston University TechWeb*, www.bu.edu/tech/about/security-resources/host-based/intro.
- Kizza, Joseph Migga. *Guide to Computer Network Security*. 6th ed., Springer, 2024.
- Musa, Sarhan M. *Network Security and Cryptography*. Mercury Learning and Information, 2018.
- Stallings, William, and Lawrie Brown. *Computer Security: Principles and Practice*. 4th ed. Pearson, 2018.
- Vacca, John, editor. *Network and System Security*. 2nd ed., Elsevier, 2014.

FIRMWARE

ABSTRACT

The term “firmware” refers to a variety of embedded systems found within a wide range of devices, including computers, gaming consoles, and smartphones. Firmware is a topic of concern for computer security professionals due to its potential to include security vulnerabilities such as “backdoors,” through which unauthorized individuals could gain access to users’ personal information.

BACKGROUND

Many consumer devices have become so complex that they need a basic computer to operate them. However, they do not need a fully featured computer with an operating system (OS) and specially designed software. The answer to this need is to use embedded systems. These systems are installed on microchips inside devices as simple as children’s toys and as complex as medical devices such as digital thermometers. The term “embedded” is used because the chips containing firmware are ordinarily not directly accessible to consumers. They are installed within the device or system and expected to work throughout its life span.

Computers also use firmware, which is called the “basic input/output system,” or BIOS. Even though the computer has its own OS installed and numerous programs to accomplish more specific tasks, there is still a need for firmware. This is because, when the computer is powered on, some part of it must be immediately able to tell the system what to do in order to set itself up. The computer must be told to check the part of the hard drive that contains the start-up sequence, then to load the OS, and so on. The firmware serves this purpose because, as soon as electric current flows into the system, the information stored in the computer’s nonvolatile memory is loaded and its instructions are executed. Firmware is usually unaffected even when a different OS is installed. However, the user can also configure



Firmware is commonly stored in an EEPROM, which makes use of an I/O protocol such as SPI. Photo by Raimond Spekking, via Wikimedia Commons.

the BIOS to some extent and can boot the computer into the BIOS to make changes when necessary. For example, a computer that is configured to boot from the CD-ROM drive first could have this changed in the BIOS so that it would first attempt to read information from an attached universal serial bus (USB) drive.

OVERVIEW

Sophisticated users of technology sometimes find that the firmware installed by a manufacturer does not meet all of their needs. When this occurs, it is possible to update the BIOS through a process known as flashing. When the firmware is flashed, it is replaced by a new version, usually with new capabilities. In some cases, the firmware is flashed because the device manufacturer has updated it with a new version. This is rarely done, as firmware functionality is so basic to the operation of the device that it is thoroughly tested prior to release. From time to time, however, security vulnerabilities or

other software bugs are found in firmware. Manufacturers helping customers with troubleshooting often recommend using the latest firmware to rule out such defects.

Some devices, especially gaming consoles, have user communities that can create their own versions of firmware. These user-developed firmware versions are referred to as homebrew software, as they are produced by users rather than manufacturers. Homebrew firmware is usually distributed on the internet as free software, or freeware, so that anyone can download it and flash their device. In the case of gaming consoles, this can open up new capabilities. Manufacturers tend to produce devices only for specialized functions. They exclude other functions because the functions would increase the cost or make it too easy to use the device for illegal or undesirable purposes. Flashing such devices with homebrew software can make these functions available.

AUTOMOBILE SOFTWARE

One of the market segments that has become increasingly reliant on firmware is automobile manufacturing. More and more functions in cars are now controlled by firmware. Firmware is relevant to the operation not only of speedometer and fuel gauge computer displays but also of music players, real-time navigation and map displays, and applications that interface with passengers' cell phones.

FIRMWARE AS VULNERABILITY

Although firmware is not very visible to users, it has still been a topic of concern for computer security professionals. With homebrew firmware distributed over the internet, the concern is that the firmware may contain "backdoors." A backdoor is a secret means of conveying the user's personal information to unauthorized parties. Even with firmware from official sources, some worry that it would be possible for the government or the device manufacturer to

include security vulnerabilities, whether deliberate or inadvertent.

—Scott Zimmer

Further Reading

- Banik, Subrata, and Vincent Zimmer. *System Firmware: An Essential Guide to Open Source and Embedded Solutions*. Apress, 2022.
- "Device Security Guidance." *National Cyber Security Centre*, 5 Oct. 2021, www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/managing-device-firmware.
- Dice, Pete. *Quick Boot: A Guide for Embedded Firmware Developers*. Intel, 2012.
- Iniewski, Krzysztof. *Embedded Systems: Hardware, Design, and Implementation*. Wiley, 2012.
- Khan, Gul N., and Krzysztof Iniewski, editors. *Embedded and Networking Systems: Design, Software, and Implementation*. CRC, 2014.
- Noergaard, Tammy. *Embedded Systems Architecture: A Comprehensive Guide for Engineers and Programmers*. 2nd ed., Elsevier, 2013.
- Sun, Jiming, Vincent Zimmer, Marc Jones, and Stefan Reinauer. *Embedded Firmware Solutions: Development Best Practices for the Internet of Things*. ApressOpen, 2015.

FUZZY LOGIC

ABSTRACT

Fuzzy logic is a system of logic in which statements can vary in degrees of truthfulness rather than be confined to true or false answers. The human brain operates on fuzzy logic as it breaks down information into areas of probability. The idea was first developed in the 1960s by a computer scientist trying to discover a way to make computers mimic the human decision-making process. Fuzzy logic is widely used in the field of artificial intelligence (AI) as well as in fields such as cybersecurity.

BACKGROUND

The standard form of computer logic is often referred to as Boolean logic, named after

nineteenth-century English mathematician George Boole. It is a system based on absolute opposite values such as yes or no, true or false. In computing, this form of logic is applied to the binary values used in machine language. Binary values consist of 1s and 0s, which correspond to high and low voltages applied to the transistors within a computer's circuitry.

The task of processing information within the human brain does not operate on an absolute system. It uses a method that closely resembles fuzzy logic to arrive at a result within a degree of uncertainty between a range of possibilities. For example, five people of varying heights can be standing in a line. Standard logic would answer the question of "Is a person tall?" with a yes or no response. Six feet may be considered tall, while five feet, eleven inches would not be. Fuzzy logic allows for a number of responses between yes and no. A person may be considered tall, or somewhat tall, short or somewhat short. It also allows for personal interpretation, as six feet may be considered tall if a person is standing alone but not if he or she is standing next to an individual who is seven feet tall.

OVERVIEW

In 1965, professor Lotfi Zadeh at the University of California, Berkeley, developed the concept of fuzzy logic while attempting to find a way for computers to understand human language. Because humans do not think or communicate in 0s and 1s, Zadeh created a data set that assigned objects within the set values between 0 and 1. The values of 0 and 1 were included in the set but marked its boundary values. For example, instead of a computer categorizing a person as old or young, it was assigned values that allowed it to classify a person as a percentage of young. Age five may be considered 100 percent young, while age twenty may be 50 percent young. Instead of determining data in absolutes, computers that used fuzzy logic measured the degree of probability that a statement was correct.

A concept important in fuzzy logic is the idea of a fuzzy set. A "fuzzy set" is a data set without a crisp, easily defined boundary. It is in contrast to a classical set in which the elements can clearly be placed within defined parameters. For example, it is easy to find a classical data set for months of the year from a list that includes June, Monday, July, Tuesday, August, Wednesday, and September. The answer is obviously June, July, August, and September. However, change the data set to summer months and it becomes a fuzzy set. While June, July, and August are often associated with summer, only about ten June days occur after the summer solstice. Conversely, the majority of September, which is often considered a fall month, actually corresponds with the end of summer. As a result, fuzzy logic holds that July and August are 100 percent summer months, while June is roughly 33 percent summer and September is 66 percent summer.

Fuzzy logic also involves an input of information that is run through a series of "if-then" statements called rules to produce an output of information. In order to achieve a valid result, all the variables must be defined prior to the input of information. A program designed to detect temperature changes in a room and adjust the air-conditioning accordingly must first be told what values constitute hot, warm, and cold and the proper air-conditioning output corresponding to those values. Then the program will run through a series of rules such as "if the temperature value is a certain percentage of hot and rising, then increase air conditioner output," or "if temperature value is a percentage of cold and falling, then decrease output."

While Zadeh developed fuzzy logic in the 1960s, it took almost a decade of advances in computer technology to allow it to be used in practical applications. Fuzzy logic applications became more common in Japan than in the United States, where the computing concept was slow to catch on. Because it tries to replicate the human thought process, fuzzy

logic is often used in the field of artificial intelligence (AI) and robotics. In the field of cybersecurity, fuzzy logic has been used to perform risk assessments and assess cyberthreats. It has found a more practical application, however, on lower-level AI systems such as those found in smart consumer and industrial products. Fuzzy logic is the process that allows vacuum cleaners to detect the amount of dirt on a surface and adjust its suction power to compensate. It allows cameras to adjust to the proper amounts of light or darkness in an environment, microwaves to coordinate cooking time with the amount of food or washing machines to compensate for added volume of laundry. Fuzzy logic programs are also very flexible and continue to function if they encounter an unexpected value. They are also easily fine-tuned, often needing only an input of a new set of values to change the system's production.

—Richard Sheposh

Further Reading

Alali, Mansour, et al. "Improving Risk Assessment Model of Cyber Security Using Fuzzy Logic Inference System." *Computers & Security*, vol. 74, 2018, pp. 323–39.

- Cintula, Petr, et al. "Fuzzy Logic." *Stanford Encyclopedia of Philosophy*, 11 Nov. 2021, plato.stanford.edu/entries/logic-fuzzy.
- Dingle, Norm. "Artificial Intelligence: Fuzzy Logic Explained." *Control Engineering*, 4 Nov. 2011, www.controleng.com/single-article/artificial-intelligence-fuzzy-logic-explained/8f3478c13384a2771ddb7e93a2b6243d.html.
- Elizondo, David A., Agusti Solanas, and Antoni Martinez-Balleste. *Computational Intelligence for Privacy and Security*. Springer, 2012.
- "Foundations of Fuzzy Logic." *MathWorks*, www.mathworks.com/help/fuzzy-foundations-of-fuzzy-logic.html.
- McNeill, Daniel, and Paul Freiberger. *Fuzzy Logic: The Revolutionary Computer Technology That Is Changing Our World*. Touchstone, 1993.
- Ross, Timothy J. *Fuzzy Logic with Engineering Applications*. 4th ed., Wiley, 2016.
- Scott, Gordon. "Fuzzy Logic: Definition, Meaning, Examples, and History." *Investopedia*, 4 Apr. 2023, www.investopedia.com/terms/f/fuzzy-logic.asp.
- "What Is 'Fuzzy Logic'? Are There Computers That Are Inherently Fuzzy and Do Not Apply the Usual Binary Logic?" *Scientific American*, 21 Oct. 1999, www.scientificamerican.com/article/what-is-fuzzy-logic-are-t.

G

GRAPHICAL USER INTERFACE

ABSTRACT

Graphical user interfaces (GUIs) are human-computer interaction systems. In these systems, users interact with the computer by manipulating visual representations of objects or commands. GUIs are part of common operating systems such as Windows and macOS. They are also used in other applications.

BACKGROUND

A user interface is a system for human-computer interaction. The interface determines the way that a user can access and work with data stored on a computer or within a computer network. Interfaces can be either text-based or graphics-based. Text-based systems allow users to input commands. These commands may be text strings or specific words that activate functions. By contrast, graphical user interfaces (GUIs) are designed so that computer functions are tied to graphic icons such as folders, files, and drives. Manipulating an icon causes the computer to perform certain functions.

The earliest computers used a text-based interface. Users entered text instructions into a command line. For instance, typing “run” in the command line would tell the computer to activate a program or process. One of the earliest text-based interfaces for consumer computer technology was known as a disk operating system (DOS). Using DOS-based systems required users to learn specific text commands, such as “del” for deleting or erasing files or “dir” for listing the contents of a directory. One of the earliest known GUIs was the interactive interface provided in Sketchpad, an early

computer-aided design program created in the 1960s. Further early GUIs were created in the 1970s as visual “shells” built over DOS systems.

GUIs transform the computer screen into a physical map on which graphics represent functions, programs, files, and directories. In GUIs, users control an onscreen pointer, usually an arrow or hand symbol, to navigate the computer screen. Users activate computing functions by directing the pointer over an icon and “clicking” on it. For instance, GUI users can cause the computer to display the contents of a directory (the “dir” command in DOS) by clicking on a folder or directory icon on the screen. Twenty-first-century GUIs combine text-based icons, such as those found in menu bars and movable windows, with linked text icons that can be used to access programs and directories.

OVERVIEW

Computer programs are built using coded instructions that tell the computer how to behave when given inputs from a user. Many different programming languages can be used to create GUIs. These include C++, C#, JavaFX, XAML, and XUL, among others. Each language offers different advantages and disadvantages when used to create and modify GUIs.

User-centered design focuses on understanding and addressing user preferences, needs, capabilities, and tendencies. According to these design principles, interface metaphors help make GUIs user friendly. Interface metaphors are models that represent real-world objects or concepts to enhance user understanding of computer functions. For example, the desktop structure of a GUI is designed using the metaphor of a desk. Computer desktops, like actual

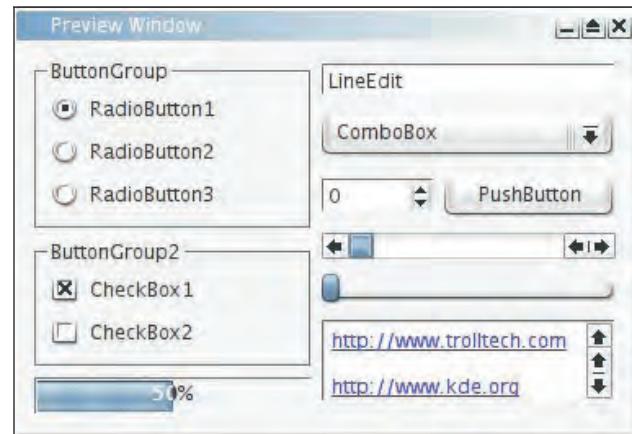
desktops, might have stacks of documents (windows) and objects or tools for performing various functions. Computer folders, trash cans, and recycle bins are icons whose functions mirror those of their real-world counterparts.

Object-oriented user interfaces (OOUIs) allow a user to manipulate objects onscreen in intuitive ways based on the function that the user hopes to achieve. Most modern GUIs have some object-oriented functionality. Icons that can be dragged, dropped, slid, toggled, pushed, and clicked are “objects.” Objects include folders, program shortcuts, drive icons, and trash or recycle bins. Interfaces that use icons can also be direct manipulation interfaces (DMI). These interfaces allow the user to adjust onscreen objects as though they were physical objects to get certain results. Resizing a window by dragging its corner is one example of direct manipulation used in many GUIs.

FUTURE OF INTERFACE DESIGN

GUIs have long been based on a model known as WIMP. WIMP stands for “windows, icons, menus, and pointer objects,” which describes the ways that users can interact with the interface. Modern GUIs are a blend of graphics-based and text-based functions, but this system is more difficult to implement on modern handheld computers, which have less space to hold icons and menus. Touch-screen interfaces represent the post-WIMP age of interface design. With touch screens, users more often interact directly with objects on the screen, rather than using menus and text-based instructions. Touch screen design is important in many application-specific GUIs. These interfaces are designed to handle a single process or application, such as self-checkout kiosks in grocery stores and point-of-sale retail software.

Computer interfaces of the early twenty-first century typically require users to navigate through files, folders, and menus to locate functions, data, or programs. However, voice activation of programs or functions is also available on many computing



A graphical user interface (GUI) showing various elements: radio buttons, checkboxes, and other elements. Image by Sikon at English Wikipedia, via Wikimedia Commons.

devices. As this technology becomes more common and effective, verbal commands may replace many functions that have been accessed by point-and-click or menu navigation.

—Micah L. Issitt

Further Reading

- “Graphical User Interface.” *Techopedia*, 28 May 2021, www.techopedia.com/definition/5435/graphical-user-interface-gui.
- Jackson, Daniel. *The Essence of Software Design: Why Concepts Matter for Great Design*. Princeton UP, 2023.
- Johnson, Jeff. *Designing with the Mind in Mind*. 2nd ed., Morgan Kaufmann, 2014.
- Long, Simon. *An Introduction to C & GUI Programming*. Raspberry Pi Press, 2019.
- Norman, Jeremy M. “Ivan Sutherland Creates the First Graphical User Interface.” *Historyofinformation.com*, historyofinformation.com/detail.php?id=805.
- Reimer, Jeremy. “A History of the GUI.” *Ars Technica*, 5 May 2005, arstechnica.com/features/2005/05/gui.
- Tidwell, Jenifer, Charles Brewer, and Aynne Valencia. *Designing Interfaces: Patterns for Effective Interaction Design*. 3rd ed., O'Reilly Media, 2020.
- “User Interface Design Basics.” *Usability.gov*, www.usability.gov/what-and-why/user-interface-design.html.
- Wood, David. *Interface Design: An Introduction to Visual Communication in UI Design*. Fairchild Books, 2014.

H

HACKING

ABSTRACT

Hacking is using programming knowledge to illegally access a computer or network. The term “hack” originated at the Massachusetts Institute of Technology (MIT) in the mid-twentieth century. By the third decade of the twenty-first century, numerous forms of hacking existed, but the practice was perhaps most closely linked with the security breaches that placed many individuals’ personal data at risk of misuse during that period.

BACKGROUND

The word “hack,” by most accounts, originated at the Massachusetts Institute of Technology (MIT), where the Tech Model Railroad Club (TMRC) was founded in 1946. The members of the club created automated model trains that operated using telephone relays; they used the word *hack* to mean a creative way of solving a problem. A second meaning of *hack*, also in use at MIT, was “an ingenious, benign, and anonymous prank or practical joke, often requiring engineering or scientific expertise and often pulled off under cover of darkness.” This sense of hacking as a creative solution with an element of humor or mischief has remained steady through time. Like the multiple meanings within the etymology of the term, the various meanings of computer hacking have evolved as our technological world has evolved.

In 1961, MIT purchased the first programmed data processor (PDP)-1. While it was a large computer that filled much of a room and cost (at the time) a whopping \$120,000, it was compact and inexpensive compared to the hulking mainframe

computers previously available. The members of the TMRC were fascinated with the new computer, and many of the club members formed MIT’s computer science department. These students spent a great deal of time exploring and expanding the PDP-1’s capabilities. They developed programming tools for it, composed and played music on it, and even played chess on it. In 1962, they created the very first video game, called *Spacewar!*

The precursor to today’s internet, Advanced Research Projects Agency Network (ARPANET), appeared in 1969. Built by the US Department of Defense (DoD) as an experiment in digital communications, ARPANET was the first transcontinental high-speed computer network. It linked universities, contractors, and labs, providing students and researchers a place to communicate with each other without regard to geographical boundaries. A hacker community formed through these networks, sharing hardware and software hacks and developing a shared vocabulary.

The earliest hackers were known as phreakers and explored the telephone system. The term *phreakers* comes from the combination of “phone” and “freak.” In 1971, John Draper discovered that a prize whistle from Cap’n Crunch cereal (the origin of his nickname) could reproduce the 2,600-hertz tone needed to access American Telephone and Telegraph’s (AT&T’s) long-distance system in “operator mode.” This allowed phreakers to explore proprietary aspects of the system, as well as make free calls. Draper was arrested many times over the following few years for phone tampering.

In 1975, two members of the Homebrew Computer Club in California started selling blue boxes, tone

producers based on Draper's discovery, to allow people to make free long-distance phone calls. Those two individuals were Steve Wozniak and Steve Jobs, who would go on to start Apple Computers in 1977.

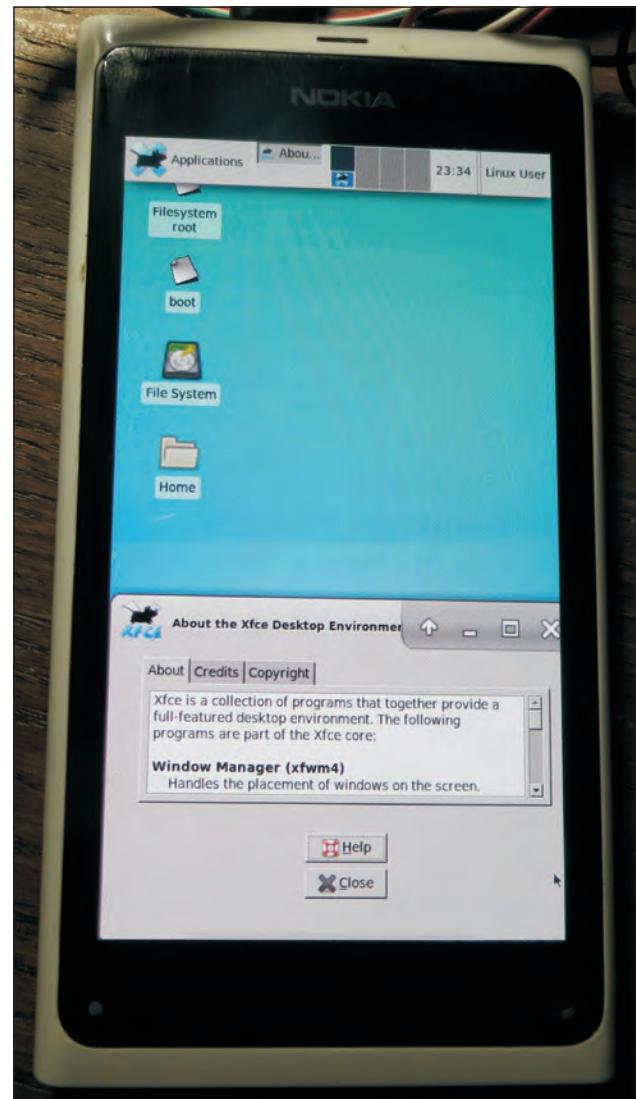
While exploring the phone system was not illegal, stealing long-distance telephone service was. In spite of the involvement of the Federal Bureau of Investigation (FBI) at this point, hackers continued exploring new technologies without much legal or law enforcement interference.

When hackers were prosecuted, they were often given probation and a small fine. Hackers often sought to share what they discovered, either through publication or online bulletin boards, much to the chagrin of companies whose security flaws or functions were discovered. As technology advanced at a rapid pace, hacker knowledge and ability to locate weaknesses in systems outpaced the law. This somewhat antiauthoritarian spirit of exploration and sharing of knowledge would remain in the nuances of hacking's definition, although the technological universe was about to change.

OVERVIEW

The early 1980s saw the first personal computers (PCs): The IBM PC, running Microsoft-Disk Operating System (MS-DOS), appeared in 1981, and Apple's Macintosh appeared in 1984. These computers sold for as low as \$1,500, a fraction of the cost of the mainframe or PDP computers of the past. Computers were no longer confined to universities and laboratories—they were affordable enough for people to have them in their homes. ARPANET was still in service, so these desktop computers—instead of whole-room computers—could be hooked up to the telephone network and talk with each other.

The potential universe for hackers to explore grew exponentially. The demand for new software applications and faster computers continued to grow as computer software companies sprung up. People could now explore the new technology easily on



Hardware hacking has allowed this smartphone to run with a desktop interface on an alternative operating system. Photo by Filip Matijevi?, via Wikimedia Commons.

their desktop computers. Consequently, the hacker community grew, and online bulletin-board systems thrived where groups could meet to share tips. With the growth of the computer and software industry, many security flaws could be found, and hackers were interested to see what they might unlock.

In 1983, the movie *WarGames*, starring Matthew Broderick, was released. He played a teenage hacker

who accesses a Pentagon supercomputer and narrowly avoids starting a nuclear war. The computer is named War Operation Plan Response (WOPR), supposedly a pun on an early North American Aerospace Defense Command (NORAD) computer that was called BRGR. While the idea of teenager starting a nuclear war was perhaps far-fetched, it illustrated a growing concern about what these new technologies and the information they controlled might do should they be compromised.

In a case of life imitating art, that same year the FBI arrested six teenagers in Milwaukee who referred to themselves as the 414s, after the city's area code. They were accused of breaking into over sixty computer networks, including the Los Alamos National Laboratory. One hacker received immunity for testifying against the others; the rest received probation.

Hackers already had a tradition of publishing and sharing their discoveries, and in 1984 a hacker magazine, *2600: The Hacker Quarterly*, began publication. The magazine's name comes from the 2,600-hertz tone that John Draper used to hack into AT&T's operator mode. The editor, Eric Corley, went by the pen name Emmanuel Goldstein, a reference to the narrator in George Orwell's *1984*. The magazine published articles on a variety of topics, including privacy issues, computer security, and the digital underground.

By the mid-1980s, repeated break-ins into government and corporate databases and networks forced Congress to respond. The Counterfeit Access Device and Abuse Act (18 U.S.C. § 1030) was passed in 1984. It was the first federal law designed specifically to prosecute computer crimes. It focused on prosecuting computer activity that accessed government information protected for national defense or foreign relations, financial information from financial institutions, and government computers. In 1986, the Computer Fraud and Abuse Act (CFAA) amended the Counterfeit Access Device and Abuse

Act and expanded the law's coverage from a "federal interest computer" to *any* "protected computer."

The first known computer virus, called Brain, appeared in 1987. It infected MS-DOS systems and was released through the internet. It was benign compared to the viruses we see today: The virus simply put a small file on the computer's hard drive with business card information for Brain Computer Services in Pakistan.

Hackers were not just limited to computers; changes in hardware and software on media players and game consoles could allow these devices to use media that was homemade, pirated, or free. In 1988, the Digital Millennium Copyright Act (DMCA) was passed; it criminalized the creation and distribution of hardware and software that disabled copyright protections on digital media.

In 1988, twenty-three-year-old Cornell University graduate student Robert Morris created the internet's first worm. The son of a National Security Agency (NSA) computer security expert, he wrote ninety-nine lines of code and released them to the internet as an experiment. The self-replicating software multiplied more quickly than anticipated and infected more than 6,000 systems. Almost one-tenth of the entire internet at the time was affected, and the network was out of service for days. The first person tried under the CFAA, Morris was arrested and sentenced to three years of probation, 400 hours of community service, and a \$10,000 fine. He later formed an internet start-up, Viaweb, which he sold in 1998 for almost \$49 million. A hacker going under the moniker "The Mentor" published what is now a classic treatise on hacking, *The Conscience of a Hacker*, in 1989. The last line reads: "You may stop this individual, but you can't stop us all."

THE RISE OF THE INTERNET

In the late 1980s and early 1990s, commercial internet service providers (ISPs) began to emerge. They replaced ARPANET, the first internet, which

was decommissioned in 1990. Online retailers began to appear, such as Amazon.com in 1995. Personal information began flowing through the internet—hackers noticed. Enthusiasm for the growing internet led to more serious hacks, some just for exploration, and some for criminal gain.

Four hackers calling themselves the Legion of Doom were arrested in 1990 for stealing technical information on BellSouth's 911 emergency telephone network. While they did not do anything with it, the information could have disabled 911 service for the entire country. Three of the hackers were found guilty and received prison sentences ranging from fourteen to twenty-one months, along with almost \$250,000 in damages.

In 1990, the Secret Service and Arizona's organized crime unit joined forces to create Operation Sundevil, a crackdown on illegal computer hacking activities. It resulted in three arrests and the confiscation of computers, the contents of electronic bulletin board systems (BBSs), and floppy disks. The arrests and following court cases resulted in the creation of the Electronic Frontier Foundation (EFF), which focuses on defending civil liberties issues affected by technology.

The 1990s also saw the first hacker breach of big banking. In 1994, Russian hacker Vladimir Levin had Citibank's computers transfer an estimated \$10 million to his accounts; Citibank recovered all but \$400,000 of what was stolen. In January 1998, Levin pled guilty in federal court to charges of conspiracy to commit bank, wire, and computer fraud. He admitted using passwords and codes stolen from Citibank customers to make the transfers. Levin was sentenced to three years in prison and was ordered to pay Citibank \$240,000.

The first “Defcon” hacker conference was held in Las Vegas, Nevada, in 1993 and continues as an annual event. The term comes from the movie *WarGames* and references the US Armed Forces Defense Readiness Condition (DEFCON). In the

movie, Las Vegas was selected as a nuclear target. It also references DEF, the letters on the number 3 on a standard phone, with “con” meaning conference.

Defcon and the other big hacker conferences (such as Black Hat or RSA) focus on so-called ethical hacking. There are demonstrations of security flaws, such as an eleven-year-old child hacking into a replica of Florida's election website and changing votes in under 10 minutes in 2018, or the takeover of a Jeep's computer system while it was driving (which led to a recall of over 1 million cars). Bug bounties are offered by companies large and small (such as Facebook, Microsoft, and the Justice Department) for hackers that turn in security flaws.

Shame boards list those who attend and find themselves hacked, as well as an award for the most epic fail. In 2018, some of the contenders were Under Armour's MyFitnessPal for compromising personal information for over 150 million people, and the Facebook website hack, that exposed “access tokens” affecting the accounts of 29 million people.

Despite the CFAA, hackers continued to break into government computers. In 1996, the General Accounting Office reported that hackers tried to break into DoD files more than 250,000 times in 1995; about 65 percent of the attempts succeeded. In August, hackers added swastikas and a picture of Adolf Hitler to the US Department of Justice (DOJ) website and renamed it the Department of Injustice. The next month, hackers broke into the Central Intelligence Agency's (CIA's) website and changed the department's name to Central Stupidity Agency.

By 1998, the Symantec AntiVirus Research Center estimated that 30,000 computer viruses were circulating on the internet. That same year, federal prosecutors charged a juvenile for the first time with computer hacking after a boy shut down an airport communications system in Massachusetts. No accidents occurred and his name was not released; however, he pled guilty and was sentenced to two years

of probation, 250 hours of community service, and restitution to Bell Atlantic for \$5,000.

A hacker think tank called “L0pht” (pronounced “loft”) testified before Congress in 1998 that it could shut down the internet in half an hour. (The congressional hearings were about software and internet security flaws.) With the government, retailers, and financial institutions utilizing the internet, more personal and financial data than ever before had become accessible to hackers who had an interest in finding it.

HACKING TODAY

Verizon’s *2018 Data Breach Investigations Report*, the best-known annual study of data breaches, indicated that the majority of the breaches, about three out of every four attacks, were due to criminals looking to steal money in some fashion. Thieves use more than payment systems to steal money. In 2017, the use of ransomware increased, accounting for 40 percent of malware incidents. Ransomware locks a victim’s data and then threatens to erase or publish it if money, or a “ransom” is not paid. Ransom demands in 2017 averaged about \$500.

Information is also a valuable commodity to thieves. For instance, in August 2015, nine people were charged in the largest known computer hacking and securities fraud scheme to date. They stole over 150,000 press releases from three major newswire companies about publicly traded companies and made insider stock trades, which generated over \$30 million, based on the information. The defendants were in Ukraine and various locations in the United States. In addition to stealing information and money, sometimes hacks cost money simply because of their disruption. As of 2000, a new computer virus was created every hour, according to the Symantec AntiVirus Research Center. In 2017, distributed denial-of-service (DDoS) attacks were the leading cause of security breaches. DDoS attacks overwhelm a server with requests so that it cannot accept more traffic and sometimes crashes.

While large attacks tend to make the news, such as the February 2000 DDoS attack on Yahoo!, eBay, CNN, Amazon.com, and E*Trade, even short-lived smaller attacks can cause security issues. The FBI estimated that such attacks cost about \$1.7 billion in lost business and other damages. To counteract this trend, in 2003, Microsoft started a \$5 million bounty on hackers attacking Windows. It continues a bug bounty program to this day. These bounties provide balance to the black market for unpatched bugs because members of organized crime and others are willing to pay well for these access points.

Viruses and malware have also shown that they can wreak havoc on systems ranging from phones to appliances, to nuclear power plants. These systems are managed and maintained by computers and internet connections. For example, between 2009 and 2010, Iran’s nuclear program was infected by a virus named Stuxnet. This virus was unlike any other because it caused physical destruction of the equipment controlled by the computers. Stuxnet targeted the rotation speeds of centrifuges and caused one-fifth of them to destroy themselves, which delayed the progress of Iran’s nuclear program. The attackers also took over the facilities’ workstations and blasted “Thunderstruck” by AC/DC at highest volume. It is suspected that the virus was developed by the US and Israeli governments, but in the digital realm, reliable attribution of any hack is very difficult.

Hacking has also taken on social and political purposes; this kind of hacking is called “hacktivism.” Hacktivists sometimes work alone, like The Jester, who takes down Islamic jihadist websites. Some work in loose groups, such as Anonymous and Lulz Security (abbreviated to LulzSec). Their targets have been varied, ranging from the Church of Scientology to PayPal. There is no defined leadership for such groups, and sometimes their actions are condemned by others within the group.

During the 2020s, security breaches resulting in the exposure of employee or customer information

remained issues of substantial concern in many industries, including retail, hospitality, and manufacturing. In some breaches, malicious individuals or groups took advantage of vulnerabilities in computer systems to access information without authorization; in others, less technologically oriented strategies such as social engineering were used to gain access to computer systems or individual user accounts. It would appear that as technology evolves, hacking will do likewise. Both are works in progress, and they are inextricably interwoven.

—Noëlle Sinclair

Further Reading

- Carlin, John P. *Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat*. Hachette, 2018.
- Coleman, E. Gabriella. *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton UP, 2013.
- Goldstein, Emmanuel. *Best of 2600: A Hacker Odyssey*. Wiley, 2008.
- Greenberg, Andy. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday, 2019.
- Lapsley, Phil. *Exploding the Phone: The Untold Story of the Teenagers and Outlaws Who Hacked Ma Bell*. Grove Press, 2013.
- Levy, Steven. *Hackers: Heroes of the Computer Revolution—25th Anniversary Edition*. O'Reilly Media, 2010.
- Mitnick, Kevin. *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*. Little, Brown and Company, 2011.
- Olson, Parmy. *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*. Little, Brown and Company, 2012.
- Peterson, T. F., and Institute Historian. *Nightwork: A History of Hacks and Pranks at MIT*. Updated ed., MIT Press, 2011.
- Smith, Jeremy N. *Breaking and Entering: The Extraordinary Story of a Hacker Called "Alien."* Eamon Dolan/Houghton Mifflin Harcourt, 2019.
- Stewart, Andrew J. *A Vulnerable System: The History of Information Security in the Computer Age*. Cornell UP, 2021.

Watters, Paul A. *Cybercrime and Cybersecurity*. CRC Press, 2023.

Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Broadway, 2014.

HTML

ABSTRACT

HTML, which stands for hypertext markup language, is a code used to control the functionality of web pages. It was invented in the late twentieth century and has become an indispensable part of online technology. Hypertext consists of a set of instructions for the creation of display pages on browsers, which made the World Wide Web (WWW) possible. By the mid-1990s, HTML embedded codes that defined fonts, layouts, graphics, and hypertext links provided a standard protocol that allowed web page designers to distribute content to any computer.

BACKGROUND

Timothy Berners-Lee developed hypertext markup language (HTML) over several years during the 1980s while working as a software engineering consultant at the Conseil Européen pour la Recherche Nucléaire (CERN; later known as the Organisation Européen pour la Recherche Nucléaire, or the European Organization for Nuclear Research) in Geneva, Switzerland. He attempted to organize laboratory research documents and statistics from incompatible computer systems submitted by physicists from around the world. In order to pool all of these files for sharing information, Berners-Lee developed a set of formatting codes to work with hypertext protocol by linking text within the files. His invention was called hypertext.

Later in the decade, Berners-Lee invented systems that enabled computers within the same network to communicate with each other. In 1989, he proposed developing a network that would allow computers all over the world to connect. Rather

than communicating by email, files could be located on a page on the web, where they could be accessed by anyone with the right technology and credentials—the code that would make this possible was HTML. Although the specific name for this language has changed significantly since its invention, its purpose has remained the same: to facilitate the smooth operation of web pages of all types.

Hypertext enables the computer user to cross-reference information and link formats together through multiple gateways on the World Wide Web (WWW). Each page is provided with a unique location address known as a universal document locator (URL). Robert Cailliau, who worked in the Office Computing Systems, Data Handling Division, at CERN, collaborated with Berners-Lee to get the web under way. Cailliau's contributions were essential to the development of the web. He rewrote the original proposal, lobbied administrators for funding, presented papers at conferences, and got programmers to work on the project.

Berners-Lee derived HTML from standard generalized markup language (SGML), an international

standard that emphasized document structure and textual relationships. However, SGML proved too complex for the average web page creator, so HTML was developed as a nonproprietary format in order to embed code for text, images, and other files to make them easily accessible through the web. Berners-Lee's prototype for hypertext was the NeXT computer station, but he encouraged others to program, design, and improve software for displaying HTML documents. In 1993, Marc Andreessen, an undergraduate student at the National Center of Supercomputing Applications (NCSA) at the University of Illinois, designed a web browser to display HTML documents, called Mosaic, which was widely adopted and accelerated internet traffic over the following three years.

OVERVIEW

Although the language of HTML is not necessarily second nature to all users, it is extremely systematic, with a few basic, important components. The file in which HTML code is written is called a document, which usually has an .html extension. The

```
<!/DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <title>HTML</title>
  </head>
  <body>
    <h1>Hello World!</h1>
    <p>This is my first web page.</p>
    <img alt="A small red square" data-bbox="400 300 450 350" style="display: block; margin: auto;"/>
  </body>
</html>
```

Image via iStock/Mak Art. [Used under license.]

term HTML is in brackets that look like this-<>-at the beginning and end of a document. The words inside the brackets are called “tags.” Tags are a crucial component of an HTML document.

Tags are generally in pairs. The first tag, called the start tag, looks like this: <tag>, and the second tag, called the end tag, looks like this: </tag>. Keywords, the text between tags, depend on the content of a page. Keywords may be of many different types, with many different degrees of significance. Many tags will simply designate the exact words and phrases that will appear on a page. For example, the words <title>My Favorite Job Ever</title> would probably appear at the top of the screen on the web version of an HTML document. This code might appear in the first paragraph under the title: <p> I have had many jobs. But one stood out as a favorite. </p>

It is important to remember that HTML is a unique language. The text within tags is read and interpreted by a computer's software, so the rules of the language must be followed. For example, the tag <!DOCTYPE html> must be used at the beginning of an HTML document to indicate the document type. When an HTML document is opened within a web browser, the language of the document guides the appearance and function of the page. The tags <title>text</title> indicate the title of a document, <body> and </body> indicate the start and end of the main text of a document, and <p>text</p> indicate the starting and ending points of a paragraph within a document. To place headers within a document, these tags must be used: <h1> and </h1>. To create headers of different sizes, these tags are used: <h2> and </h2>, <h3> and </h3>. Images to be inserted in a document are preceded and followed with the tags and .

The characteristics of an HTML document, such as the size of an image, are called “attributes.” They are usually placed between the brackets of a start tag

and are followed by an equals (=) sign; the exact attribute itself is in quotes. For example, to display an image that is 600 pixels wide, this text would be used: width=“600.” Every element of a web page has its own designation in HTML. HTML has codes for tables, animations, different tabs within a page, and the size and shape of a page. Once an HTML document is complete, it is opened in a browser, which is when the person writing the HTML code can see whether or not the code has been properly written.

As time has passed, HTML has been modified and used in different ways, such as in mobile devices. A notable development is XHTML. The X stands for extensible, indicating that the language can be used in a wider variety of situations than web development. As programmers continue to write code and as the internet continues to become more pervasive in daily life, the true significance of Berner-Lee's invention becomes more and more evident.

SIGNIFICANCE

The WWW became a global, economic, and social phenomenon by the end of the 1990s. However, American businesses shied away from the internet in the early part of the decade, believing that it would be used only for research in the academic environment. In 1994, Berners-Lee, who was now working at the Massachusetts Institute of Technology (MIT), founded the World Wide Web Consortium (W3C) to promote guidelines regarding the growth of network infrastructure and strict language syntax with HTML, especially with the emerging browser battles between Netscape and Microsoft Explorer. HTML promoted interoperability, causing internet traffic to explode.

Search engines had difficulty trying to track all of the pages found on the web. Companies soon embraced the WWW for commercial ventures, and in response, HTML continued to improve support.

Browsers adopted cascading style sheets (CSS) to improve document appearance. Dynamic HTML added capabilities to respond interactively with JavaScript. Extensible markup language (XML), a relative of HTML, created additional tags to identify structures and relationships within a document. XML had two important features. First, web-page creators had more flexibility to create their own tags. Second, XML separated content from formatting through the use of sophisticated style sheets, ensuring that all data structures and relationships were identified within the XML tags in which they were enclosed. XML made search engines more powerful for cataloging contents, enabling computers to become even more interactive and responsive to user actions.

—Max Winter, Gayla Koerting

Further Reading

- Bell, Mary Ann, Mary Ann Berry, and James L. Van Roekel. *Internet and Personal Computing Fads*. Haworth Press, 2004.
- Berners-Lee, Tim. *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor*. Harper, 1999.
- Cailliau, Robert, and Helen Ashman. “Hypertext in the Web: A History.” *ACM Computing Surveys*, vol. 31, Dec. 1999, pp. 1–6.
- Campbell-Kelly, Martin, William F. Aspray, Jeffrey R. Yost, Honghong Tinn, and Gerardo Con Díaz. *Computer: A History of the Information Machine*. 4th ed., Routledge, 2023.
- Costello, Vic. *Multimedia Foundations: Core Concepts for Digital Design*. 3rd ed., Focal Press, 2023.
- “Deprecated HTML5 Tags and Attributes.” DESE, 14 Mar. 2018, www.doe.mass.edu/nmg/html5-deprecated.html.
- Frain, Ben. *Responsive Web Design with HTML5 and CSS*. 4th ed., Packt, 2022.
- “HTML Tutorial.” W3Schools, www.w3schools.com/html.
- Mowery, David C., and Timothy Simcoe. “Is the Internet a US Invention? An Economic and Technological History of Computer Networking.” *Research Policy*, vol. 31, Dec. 2002, pp. 1369–87.

Musciano, Chuck, and Bill Kennedy. *HTML and XHTML: The Definitive Guide*. 6th ed., O’Reilly, 2006.

Nielsen, Jakob. *Multimedia and Hypertext: The Internet and Beyond*. SunSoft Press, 1995.

HTTP COOKIE

ABSTRACT

A hypertext transfer protocol (HTTP) cookie is a piece of data that is stored on a user’s computer when it accesses a website and is then later retrieved by that site. Also known as an “internet cookie,” “web cookie,” or “browser cookie,” this data may record and track a user’s browsing history, account details, or form entries, among other information. While some types of cookies are necessary for web browsers to function, their use has raised concerns about violation of privacy.

BACKGROUND

Hypertext transfer protocol (HTTP) cookies were introduced by Netscape Communications in the first edition of its Netscape Navigator browser, released in 1994. The name comes from “magic cookie,” a computing term used since the 1970s to describe a piece of data exchanged between programs, often for identification purposes.

In basic HTTP functioning, every time a browser interacts with the server hosting a particular website, the server treats the connection as a brand-new request, not recognizing it from previous

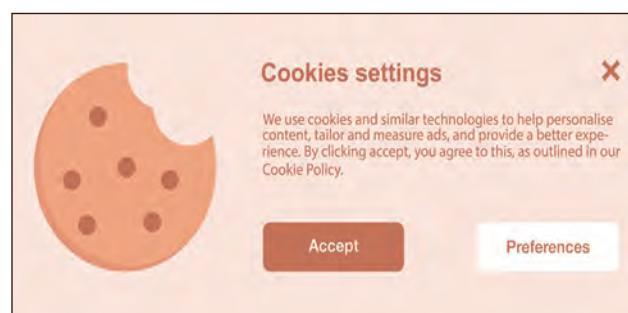
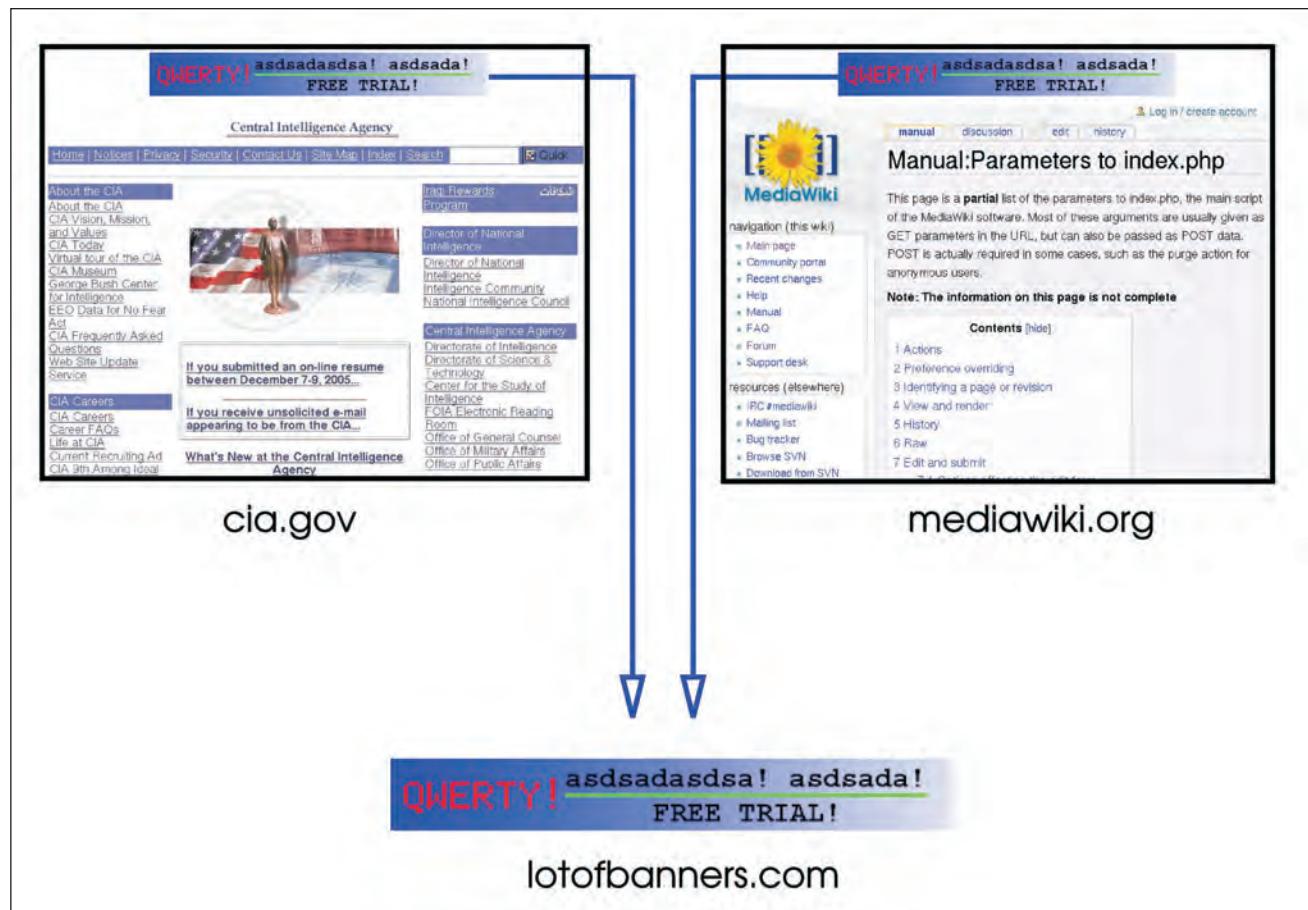


Image via iStock/Kojaif. [Used under license.]



In this fictional example, an advertising company has placed banners in two websites. By hosting the banner images on its servers and using third-party cookies, the advertising company is able to track the browsing of users across these two sites. Image by Tizio, via Wikimedia Commons.

interactions. As such, HTTP is considered a “stateless” protocol, meaning it stores no information on its own. In order for a website or other application to remember such things as the identity of a logged-in user or the items placed in a virtual shopping cart, when a browser connects with a host server for the first time, the server stores a cookie on the browser’s computer. The next time the browser connects to the server, the cookie reminds the application of the stored information—that is, its state. If the user does something to change the application’s state, such as adding an additional item to his or her virtual shopping cart, the server updates the information in the cookie.

OVERVIEW

Different types of cookies are used for different purposes. All cookies fall into one of two categories: session cookies, which are stored only for the length of a user’s browsing session and are deleted when the browser is closed, and persistent cookies, which remain stored on the user’s computer until they either reach a predetermined expiration date or are manually deleted. First-party cookies are those created and stored by a site the user chooses to visit, while third-party cookies are installed by some entity other than the site the user is visiting, often by companies advertising on that site.

First-party cookies include authentication cookies,

which are created when a user logs into an account on a particular website and identify that user until he or she logs out, and may be either session cookies or persistent cookies. Third-party cookies are usually persistent. One common type is the third-party tracking cookie; these cookies maintain a record of a user's browsing history, which companies may then use to gather consumer data or to target advertisements more precisely. Other types of cookies include HTTP-only cookies, which are only used when HTTP requests are being transmitted and thus are more secure, and opt-out cookies, which prevent advertising companies from showing users targeted ads.

The use of third-party tracking cookies has raised concerns among users who do not want companies to be able to monitor their online habits. Responses to these concerns include the European Union's (EU's) Directive on Privacy and Electronic Communications, introduced in 2002 and updated in 2009, which requires companies to obtain consent before installing unnecessary cookies on a user's computer. The General Data Protection Regulation (GDPR), implemented within the EU in 2018, further touched on the privacy ramifications of cookies, identifying them as a form of personal data due to their ability to identify individual users. In addition,

many browsers have the ability to block third-party cookies, though some companies have developed methods of circumventing that block. In 2012, for example, Google was discovered to have been deliberately defying the Safari browser's default privacy setting, which banned the installation of third-party cookies.

—Randa Tantawi

Further Reading

- Gourley, David, et al. "Client Identification and Cookies." *HTTP: The Definitive Guide*. O'Reilly Media, 2002, pp. 257–76.
- Hofmann, Markus, and Leland R. Beaumont. "Content Transfer." *Content Networking: Architecture, Protocols, and Practice*. Elsevier, 2005, pp. 25–52.
- "How Websites and Apps Collect and Use Your Information." *Federal Trade Commission Consumer Advice*, Sept. 2023, consumer.ftc.gov/articles/how-websites-and-apps-collect-and-use-your-information.
- Koch, Richie. "Cookies, the GDPR, and the ePrivacy Directive." *GDPR.EU*, gdpr.eu/cookies.
- Kristol, David M. "HTTP Cookies: Standards, Privacy, and Politics." *ArXiv*, 9 May 2001, arxiv.org/abs/cs/0105018.
- Singel, Ryan. "Google Busted with Hand in Safari-Browser Cookie Jar." *Wired*, 17 Feb. 2012, www.wired.com/2012/02/google-safari-browser-cookie.
- "Using HTTP Cookies." *MDN Web Docs*, 10 Apr. 2023, developer.mozilla.org/en-US/docs/Web/HTTP/Cookies.

I

IDENTITY THEFT

ABSTRACT

Identity theft is among the most frequent consumer complaints reported to the Federal Trade Commission (FTC). Though a relatively new crime, it is often perpetrated through various familiar crimes, such as forgery; counterfeiting; and check, credit, and computer fraud. The National Crime Victimization Survey (NCVS) defines identity theft as (1) unauthorized use or attempted use of an existing account; (2) unauthorized use or attempted use of personal information to open a new account; and (3) misuse of personal information for a fraudulent purpose.

BACKGROUND

The term “identity theft” did not appear in federal laws until 1998. Prior to 1998, crimes related to identity theft were charged under late nineteenth-century false personation statutes. False personation refers to impersonating another individual, such as a police officer or other official, and does not have the financial connotations that the term “identity theft” now carries. The late 1990s saw a staggering increase in reporting on identity theft. TransUnion, one of the three major national credit bureaus, reported that the total number of identity theft inquiries to its fraud department rose from about 35,000 in 1992 to almost 523,000 in 1997. While these numbers did not indicate what percentage of the inquiries were actual identity thefts, they did indicate a growing concern on the part of consumers. In 1998, Congress responded to these growing numbers and passed the Identity Theft and Assumption Deterrence Act, 112 Stat. 3007, making identity theft a federal crime. It expanded 18 U.S.C.

§ 1028, “Fraud and related activity in connection with identification documents,” to make it a federal crime to “knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.”

According to the Office for Victims of Crime, the Identity Theft and Assumption Deterrence Act accomplished four things:

1. Identity theft became a separate crime against the person whose identity was stolen. Previously, victims were defined as those who had financial losses, so the emphasis was on banks and other financial institutions rather than on individuals.



Image via iStock/pressureUA. [Used under license.]

2. It made the FTC the federal government's point of contact for reporting instances of identity theft by creating the Identity Theft Data Clearinghouse.

3. Criminal penalties for identity theft and fraud were increased, providing for up to fifteen years' incarceration as well as substantial fines.

4. The act closed loopholes so it became a crime to steal another person's identifying information. Previously, it was a crime only to produce or possess false identity documents. The act has been updated several times. The Identity Theft Penalty Enhancement Act of 2004, Pub. L. 108-275 § 1028A, established penalties for aggravated identity theft, which is when a stolen identity is used to commit felony crimes, including immigration violations, theft of another's Social Security benefits, and acts of domestic terrorism.

The Identity Theft Enforcement and Restitution Act of 2008 amended 18 U.S.C. § 3663(b) to clarify that restitution for identity theft cases may include the value of the victim's time spent repairing harm from the identity theft. It also allows federal courts to prosecute even if the criminal and the victim live in the same state. Under the previous law, federal courts had jurisdiction only if the thief used interstate communication to access the victim's information. In addition to the federal laws, state laws help victims of identity theft. Because most crimes are prosecuted at the state level, the Identity Theft Resource Center has a list of state-specific laws that deal with identity theft.

OVERVIEW

Identity thieves continue to target individuals but also use security flaws to break into retailer and other databases to steal personal and financial information. For instance, in 2017 Equifax, one of the three major credit reporting agencies, was breached. The breach went undetected for seventy-six days, and Equifax waited another six weeks to disclose it.

By March of 2018, the credit card and driver's license details, Social Security numbers, and other personal information of more than 148 million people had been compromised.

In May 2018, President Donald Trump signed a bill that made freezing one's credit easier and requires the three credit agencies to share fraud reports among themselves. However, a September 2018 report issued by the US General Accounting Office (GAO), which investigated the Equifax breach indicated that there were still many unresolved issues and sensitive data remained at risk.

Selling large collections of account information on the black market to thieves who then use the information has become lucrative. It is extremely difficult to identify the perpetrators in these data breaches; when they then sell the stolen data to third parties, the waters become even more muddied.

For instance, in December 2013, in the final shopping days before Christmas, the department store Target had the credit and debit card information of 40 million customers stolen. While Target's security software set off alarms when the offending malware was uploaded, it was not fully investigated. Because the breach was not identified quickly, additional personal information, including email and mailing addresses, for about 70 million people was compromised. The same Eastern European group that attacked Target was also suspected in breaches at Neiman Marcus and Michaels. Millions of people had to cancel and replace their credit and debit cards; many also became victims of identity theft due to the breach.

In August 2014, the *New York Times* reported that a Russian crime ring had assembled the largest known collection of stolen internet information, including 1.2 billion username and password combinations and more than 500 million email addresses. The information was used to send spam, for which the group collected a fee.

Another method of identity theft used by thieves to steal money is tax fraud. The Internal Revenue Service (IRS) publishes an annual list of its so-called dirty dozen tax scams. In 2011, only one involved identity theft. By 2015, about one-quarter of all IRS criminal investigations focused on identity theft.

In 2015, the IRS itself became a victim of an online attack that stole personal information, including Social Security numbers, and diverted tax refunds from over 610,000 taxpayers. The breach occurred through a new online service that provided access to past tax returns. The stolen data was subsequently used to file fraudulent tax returns totaling about \$39 million. The IRS believed the identity thieves to be part of a criminal group from Russia.

The IRS's attempts to modernize and increase taxpayer convenience with online resources highlight the challenge any business faces—how to outpace criminals, provide online convenience, and still keep data secure. The IRS is an interesting combination of old and new in this respect, and some of its seemingly outdated practices actually serve a protective function. For instance, the IRS communicates with taxpayers only by mail; it never initiates any contacts by phone or email. Commissioner John Koskinen acknowledged, at a Tax Policy Center conference, that the agency's database software was so old that hackers did not have the programming knowledge to break in.

METHODS OF STEALING DATA

Both low- and high-tech methods are used to steal personal information, although recent years have seen growth in scams resulting from our increasing use of computers, including email and the internet. Low-tech methods include purse snatching or digging through trash, known as “dumpster diving.” High-tech methods use technology to acquire information, such as phishing emails, spyware, and malware. According to Verizon's annual *Data Breach Investigations Report*, the majority of computer hacks

occur because people click on links in emails, companies do not apply patches to software flaws in a timely fashion, and computer systems are improperly configured (which includes failure to install updated security software).

Scams that occur through email are called “phishing.” Phishing scams target people by sending an email that seems to be from a trustworthy source, such as a well-known store or a bank. It asks the recipient to enter personal information, often indicating that there is a problem with an account or enticing the recipient with coupons or other gains. Once the phishing target has entered his or her personal information, the scammer can use it to open new accounts or access existing accounts. Emails and pop-up messages that request personal and financial information should be viewed with suspicion; calling a business or contacting it through its official website to verify the request can help keep personal information safe. Many institutions, such as the IRS, have policies where they do not ask for personal information through email.

Malware is short for “malicious software.” There are many types of malware, including viruses and spyware, that can steal personal information; use a computer for unauthorized activities, such as sending spam; or cause damage to a computer. Computers without security software are especially vulnerable to malware attacks. Spyware is a type of malware that records one's computer use. It is often used to display targeted advertisements, redirect internet surfing to certain websites, monitor internet surfing, or record keystrokes to obtain passwords and other personal information. Malware can infect a computer in a variety of ways, and antivirus software is constantly struggling to identify and protect against the most recent malware.

BUYING AND SELLING DATA

An entire industry exists to acquire and sell stolen personal data. The *Christian Science Monitor* reported

in 2015 that the prevalence of black-market forums and stores that trade in stolen personal information was increasing. With names like Rescator, Republic of Lampeduza, McDumpals, and Blackstuff, such stores sell stolen Social Security numbers, bank account information, credit card data, and other personal and financial information. They also offer hardware and malware meant to steal this type of information.

In July 2015, a hacking forum called Darkode, which allowed users to buy and sell cybercrime tools and services such as malware, spam services and other items, was infiltrated by the Federal Bureau of Investigation (FBI) and dismantled. Twenty-eight people were arrested, and twelve were charged as a result of international law enforcement efforts involving twenty countries. Indictments included charges such as authoring and selling malware to steal bank account credentials, selling access to botnets (a group of compromised computers used to send spam and other malware), and money laundering.

The only way to become a member of Darkode was to convince existing members of the value of the abilities or products that an individual could bring to the forum. Membership had to be approved by the other members. Just weeks after the indictments, however, Darkode was ready to reopen with a different domain suffix (Darkode.cc instead of the original Darkode.me). Most of the staff members appeared to be untouched by the arrests, and the forum implemented even more stringent membership requirements to keep out informants.

A report published by the RAND Corporation and titled *Markets for Cybercrime Tools and Stolen Data* predicts that the future will see an expansion of darknets, in terms of both numbers and activity. It also anticipates that, while greater attention will be paid to encrypting and protecting communications and transactions, the ability to generate successful cyberattacks will likely outpace the ability to defend

against them. “Crime,” the report’s authors write, “will increasingly have a networked or cyber component, creating a wider range of opportunities for black markets; and . . . there will be more hacking for hire, as-a-service offerings, and brokers.”

The report says that there is disagreement on who will be the target of the black market (e.g., small or large businesses, or individuals), what products will be on the rise in the black markets (e.g., fungible goods, such as data records and credit card information; nonfungible goods, such as intellectual property), and which types of attacks will be most prevalent (e.g., persistent, targeted attacks; opportunistic, mass smash-and-grab attacks).

IDENTITY PROTECTION SERVICES

As the black market that facilitates identity theft grows, so does another market—companies that offer protection against identity theft. The increasing number and size of data breaches causes concern and is fueling a growth in identity protection services from companies such as LifeLock, ezShield, and IdentityForce. In 2015, consumers spent \$3.8 billion on identity protection services, an 18 percent increase from the previous year, according to Javelin Strategy & Research. These services may check to see if customer data is being bought and sold on darknets or other places that are difficult for an average person to access. Another possible benefit of such a service may be the remediation services some offer in case of theft. It is a great deal of work to repair the damage once an identity has been stolen. While an individual can do it, having assistance may make a difficult situation easier. Some insurance companies, banks, and employers offer these services for little or no cost.

It appears that the companies that are looking to help prevent identity theft, however, are not without their own problems. In a suit against LifeLock, the FTC asserted that, from 2012 to 2014, the company failed to alert customers as soon as their identities

were used by thieves and also failed to protect data with the same high-level safeguards used by financial institutions, both claims the company has made to its customers. The company has since settled the lawsuit with the FTC.

Another concern about identity theft and the need for protection services is that it may not be as dire a problem as it appears in recent news. The *New York Times* reported that it is the type of data stolen that actually determines the seriousness of a data breach. The theft of Social Security numbers can allow thieves the opportunity to open new accounts in the victim's name, a particularly damaging type of identity theft. These types of theft are also difficult to discover and fix before significant damage occurs.

Many times, however, large breaches expose data that is available through other, legal means, such as email and home addresses, or information that is shared willingly, such as through social media. The size and surreptitious nature of the breach are alarming and leads to concern, even though breaches of this type of data do not often lead to crimes of identity theft. The *Times* reported that, according to the American Bankers Association, the largest expense that occurred from the 2013 Target breach was the cost of reissuing compromised debit and credit cards and assisting affected customers. Also, merchants and banks, rather than individual consumers, generally bear the financial cost of stolen credit card numbers. Because of their interest in keeping these losses to a minimum, banks and merchants are investing in better ways to find and prevent fraudulent purchases.

The government is taking the increased reporting of identity theft seriously. An entire FTC website, www.identitytheft.gov, has been created to assist those dealing with identity theft. It offers step-by-step advice on detecting identity theft, as well as how to repair the various types of damage that may be the result. The FTC also provides

resources on their website for law enforcement, attorneys assisting victims of identity theft, and businesses trying to prevent future data breaches. Despite efforts to prevent identity theft and prosecute those who perpetrate it, however, identity theft remained common throughout the early 2020s. In 2023, the FTC reported that the www.identitytheft.gov website had received more than 1.1 million reports about identity theft over the course of the previous year.

—Noëlle Sinclair

Further Reading

- Abagnale, Frank W. *Stealing Your Life: The Ultimate Identity Theft Prevention Plan*. Broadway Books, 2008.
- Ablon, Lillian, Martin C. Libicki, and Andrea A. Golay. Markets for Cybercrime Tools and Stolen Data. RAND Corporation, 2014, www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.
- Copes, Heith, and Lynne M. Vieraitis. *Identity Thieves: Motives and Methods*. Northeastern UP, 2012.
- Harrell, Erika. "Victims of Identity Theft, 2016." *Bureau of Justice Statistics*, Jan. 2019, www.bjs.gov/index.cfm?ty=pb&detail&iid=6467.
- Hastings, Glen, and Richard Marcus. *Identity Theft, Inc.: A Wild Ride with the World's #1 Identity Thief*. The Disinformation Company, 2006.
- Hoofnagle, Chris Jay. "Identity Theft: Making the Known Unknowns Known." *Harvard Journal of Law and Technology*, vol. 21, no. 1, 2007, pp. 97–122.
- "Federal Identity Theft Laws." *Office for Victims of Crime*, Oct. 2010, ocv.ojp.gov/sites/g/files/xyckuh226/files/pubs>ID_theft/idtheftlaws.html.
- McNally, Megan. *Identity Theft in Today's World*. Praeger, 2012.
- "New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021." *Federal Trade Commission*, 22 Feb. 2022, www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0.
- "New FTC Data Show Consumers Reported Losing Nearly \$8.8 Billion to Scams in 2022." *Federal Trade Commission*, 23 Feb. 2023, www.ftc.gov/news-events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022.

- Poulsen, Kevin. *Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground*. Broadway Paperbacks, 2011.
- “Verizon 2018 Data Breach Investigations Report.” *Verizon*, 2018, www22.verizon.com/wholesale/contenthub/data_breach_investigation_report.html.
- Vijayan, Jaikumar. “The Identity Underworld: How Criminals Sell Your Data on the Dark Web.” *Christian Science Monitor*, 6 May 2015, www.csmonitor.com/World/Passcode/2015/0506/The-identity-underworld-How-criminals-sell-your-data-on-the-Dark-Web.
- Watters, Paul A. *Cybercrime and Cybersecurity*. CRC Press, 2023.

ILOVEYOU VIRUS

ABSTRACT

At the time of its outbreak, the ILOVEYOU virus was the fastest spreading, most damaging computer virus ever seen, and the damage it did prompted changes in government response to such viruses. It also raised awareness about the need to educate casual computer users about malware and pushed organizations to retool their strategies for dealing with such outbreaks in the future.

BACKGROUND

The concept of a self-replicating computer program first arose in 1949. The first actual computer virus did not appear until 1981, on the Apple platform. Since then, many computer viruses have been created. Some have been relatively harmless, whereas others have carried destructive payloads that destroyed data and made computers unusable until the viruses were removed. One of the first incidents of widespread so-called malware (a fusion of the words “malicious” and “software”) was the Morris worm, which appeared in 1988 and infected more than six thousand UNIX computers—roughly 15 percent of the computers connected to the internet at the time. Later years brought increased bandwidth and more advanced virus techniques that allowed for more pervasive viruses.

On May 4, 2000, the I LOVEYOU virus started spreading in the Far East during business hours. It spread through Asia and Europe with remarkable speed. By mid-morning in Western Europe, the impact of the virus was becoming drastically evident. Morning in the United States saw major carriers closing their email gateways in an attempt to combat the spread of the virus. The Computer Emergency Response Team (CERT), created in response to the Morris worm, sent an alert to media sources, but by that time the virus had done a great deal of its damage. Asian Wall Street, the Central Intelligence Agency, the Federal Bureau of Investigation, the Federal Reserve, AT&T, the US Department of Defense, and England’s House of Commons were some, but by no means all, of the entities affected by the ILOVEYOU virus. Many of the agencies were inundated with millions of email messages, and their mail servers crashed because of the load.

OVERVIEW

ILOVEYOU was initially transmitted via email and originated in the Philippines. It required Microsoft Outlook and a Microsoft Windows operating system for infection to occur. ILOVEYOU spread rapidly for many reasons, one of which is that it was both a virus and a worm. A virus requires a host such as a file, program, or boot sector to spread. A worm can spread over a network by searching for open connections and copying itself to another machine. It took only a single user on a network opening the email to which ILOVEYOU was attached to infect the entire network. Once a machine was infected, the virus sent itself to all the addresses in the user’s address book. Each infected message appeared to be from a valid sender and contained the attachment LOVE-LETTER-FOR-YOU.TXT.vbs; spread of the virus relied on the probability that most recipients would want to read a “love letter.” The “vbs” extension signified that the attachment was a Microsoft Visual Basic Script file, but the default installation of

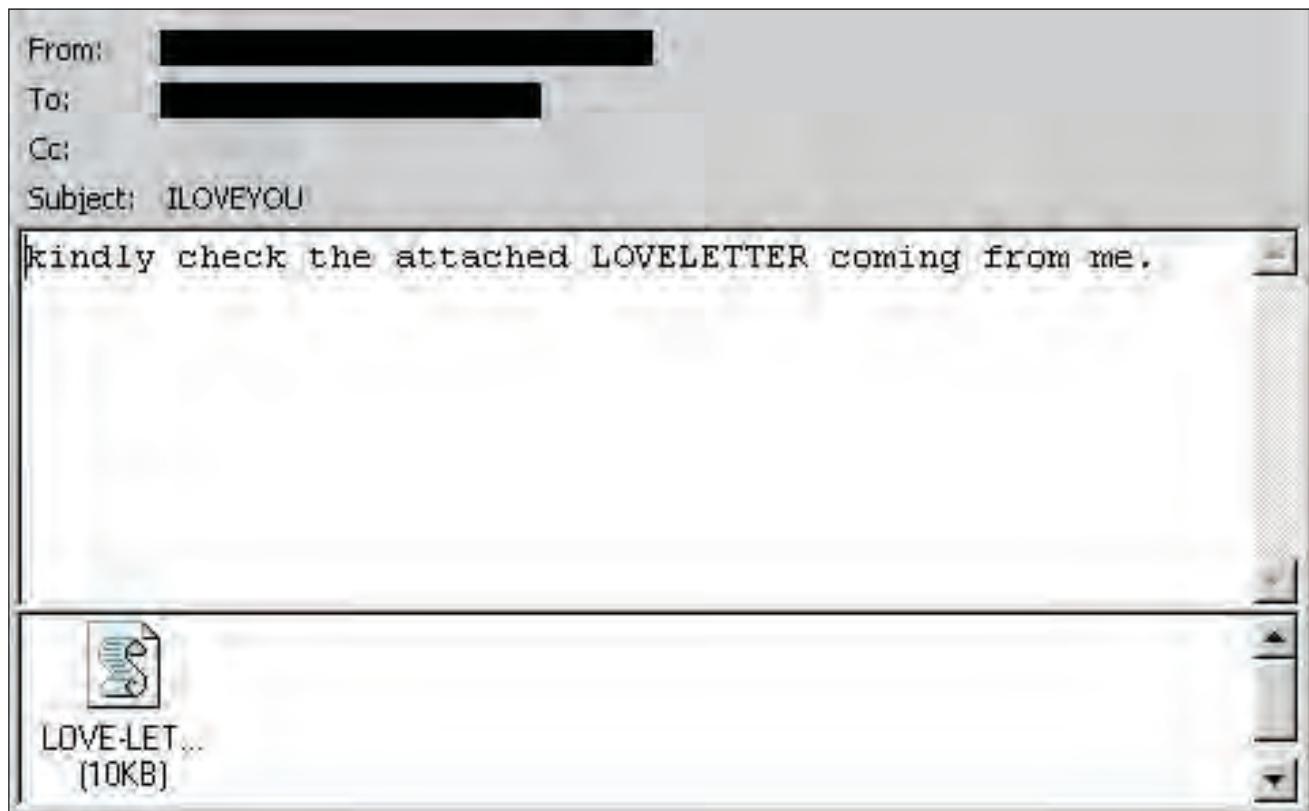


Image via Wikimedia Commons. [Public domain.]

Windows was configured so that most users did not see the extension. Many users who did see the extension opened the attachment anyway, as few knew what a Visual Basic Script was at the time.

Microsoft Outlook relied heavily on Visual Basic. The company had opted to choose functionality over security. Once the attachment was run, it easily accessed the user's address book and sent copies of itself without any interaction from the victim. The virus then made three copies of itself on the host machine and made the appropriate entries on the computer to ensure that the virus ran every time the machine was restarted or reset. It then tried to connect to the internet to download a separate Trojan horse, or Trojan (a program that is not self-replicating and has a function other than what the user thinks it will perform), that attempted to steal

passwords from a person's computer and email them to the virus creator. The sites that unknowingly hosted the Trojan removed the file from their servers soon after ILOVEYOU was released.

The virus also found other scripts on a computer and overwrote them with copies of itself. This tactic was highly effective on web servers, which would then push the virus to visitors to the infected website. Picture files with "jpg" and "jpeg" extensions were overwritten and replaced with the virus. Music files with the extension "mp2" or "mp3" were marked hidden, and a copy of the virus was put in the original file's place. The final action of the virus was that it searched for internet relay chat (IRC) files on the computer and, if found, altered them so that when someone joined a chat channel with an infected user, that person was sent a

LOVE-LETTERFOR-YOU.HTM message that would further spread the virus if opened.

Methods of containment in the early stages of the outbreak consisted of shutting down mail gateways to try to contain the virus and having mail administrators filter email based on the subject line. The latter method inhibited warnings about the viruses and did not address the issue of later versions that had differing subject lines. Virus patterns were created quickly by the major antivirus companies, but the internet was so congested from the volume of email and the demand was so high for the updated patterns that it was often days before a person could obtain the needed patch that would fix the problem. Microsoft released a patch for Outlook eighteen days after the outbreak.

The estimates for the damage that the virus caused range from \$3 to \$15 billion. Most of the damage estimate was for labor cost for virus removal—which is one of the reasons it is so difficult to assess the precise amount. It took days for infected organizations to recover from the virus. Some of the files damaged by the virus were recovered but many were lost.

The hunt for the originator of the virus led to the Philippines, where the Trojan was hosted. After looking into the virus's code, an email account was discovered. Reomel Lamores, believed to have been the owner of the account, was taken in for questioning when a disk containing a virus similar to ILOVEYOU was found in his apartment. His girlfriend, Irene de Guzman, was also questioned. Both were released, and eventually Irene's brother, Onel de Guzman, was questioned. He admitted that he may have accidentally released the virus, but no charges were ever pressed since at the time there was no law in the Philippines against hacking.

SIGNIFICANCE

Although the ILOVEYOU attachment file was relatively small in size, its effects were far-ranging and

hit hard around the world. It became the first virus to receive widespread media coverage, from drive-time radio announcements to the lead story on major news networks. It was the fastest-spreading virus to date and also the most expensive, with the average estimate of damage somewhere around \$7 billion. Most of the loss was due to intangible labor costs, but some of the data that were lost were irreplaceable.

In response to the failure to prosecute anyone for the case, the Philippine government passed a law against hacking so that future cases could be successfully brought to trial. A movement was made by employers to educate all users about malicious code threats from email and the internet so that at the very least, an organization's own employees would not contribute to the spread of viruses. Antivirus vendors made changes to their virus pattern distribution. Centralizing the patches on their own servers created too much congestion, so they moved to allow organizations to download the updates to one of their own servers and distribute it internally. Also, the virus prompted congressional investigations into why the virus caused so much damage and spread so quickly through government agencies. The investigation created a more streamlined, coordinated response for future malware attacks.

—James J. Heiney

Further Reading

- Caldwell, Wilma R., editor. *Computer Security Sourcebook*. Omnigraphics, 2003.
- Erbschloe, Michael. *Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code*. Butterworth-Heinemann, 2005.
- Furnell, Steven. *Cybercrime: Vandalizing the Information Society*. Addison-Wesley, 2002.
- Stewart, Andrew J. *A Vulnerable System: The History of Information Security in the Computer Age*. Cornell UP, 2021.

INDUSTRIAL ESPIONAGE

ABSTRACT

Industrial espionage is the theft of trade secrets from a corporation for use by a rival. Trade secrets are designs, plans, or techniques that a company has trademarked as its original creations, which help the company to succeed commercially. Competitors who steal these secrets can be other corporations or foreign governments. Despite companies' increasingly high-tech efforts to protect themselves from this kind of theft, industrial espionage continues to threaten modern businesses and economies.

BACKGROUND

The goal of industrial espionage is to gain an economic advantage. This differs from traditional espionage, which is usually conducted for purposes of national security. Industrial espionage refers to the stealing of information a corporation intends to

keep secret. The term “competitive intelligence” describes the legal observation of a company’s strengths and weaknesses by a rival to enhance the performance of its own business. Though the theft of trade secrets sometimes involves human agents operating in restricted settings, other methods, such as blackmail, bribery, and clandestine surveillance, can also be used.

The Federal Bureau of Investigation (FBI) outlines several methods by which trade secrets can be stolen and classified as industrial espionage. One involves the acquisition of protected information by deception or fraud. Another consists of any type of transmission or replication—including sketching, photographing, or downloading—of the information. A person or an entity that buys or receives the information after it has been stolen is considered an accomplice to the theft.

Industrial espionage is not unique to modern times. One of the first recorded instances of the

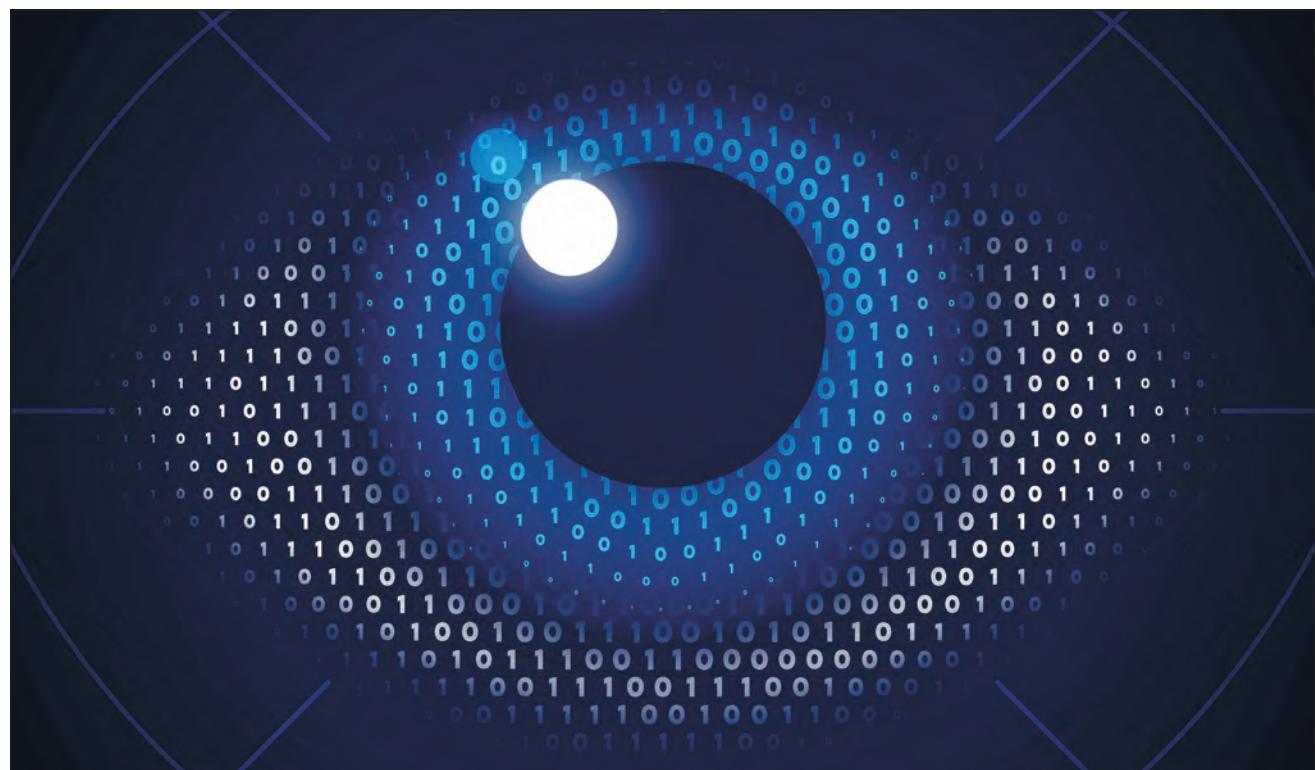


Image via iStock/filo. [Used under license.]

practice occurred in the 1680s, when a French Jesuit priest named Pere François Xavier d'Entrecolles traveled to Jingdezhen, China. He meticulously recorded the Chinese method of making hard-paste porcelain, at that time a highly valued product in Europe. Within decades after d'Entrecolles returned home, French porcelain factories began making exact copies of the Chinese porcelain. Great Britain later stole the process from France and started manufacturing the porcelain as well.

Britain and France continued to steal trade secrets from each other throughout the 1700s. French agents routinely stole British blueprints and other plans to aid French industries. French recruiters even attempted to lure skilled British laborers into defecting to work in France. Britain later decreed that any British citizens who took up these offers would be fined. Another British law of the era prohibited the exporting of machinery from certain industries for fear its designs would be stolen.

The United States engaged in industrial espionage throughout the 1800s, gleaning numerous business secrets from other countries. The information was one of many factors that led the United States to become the world's largest economy by the 1870s. Since that time, the country's industrial and technological advancements have become a target for much of the still-developing world. During the Cold War period of the twentieth century, the communist Soviet Union attempted to steal American trade secrets to improve its own economy. The end of the Cold War in the 1990s, however, brought free-market economies to much of the modern world, leaving the communist giant China as the main perpetrator of industrial espionage.

OVERVIEW

Exact details of modern industrial espionage are difficult to identify. This type of theft frequently takes place through computer technology and can go

unnoticed. In the twenty-first century, China has often been accused of stealing trade secrets by more technologically advanced Western governments. Computers and automobiles are two of the most targeted markets for Chinese industrial espionage. The amount of funding devoted to research and development of these technologies makes their secrets especially valuable.

In 2009, for example, Germany estimated that it lost about €50 billion annually to industrial espionage by foreign nations. China, it claimed, was the primary culprit, using spies, phone taps, and computer hacking to steal sensitive business secrets. Germany also accused Russia of stealing its industrial information, claiming the thefts saved the Russian economy billions of dollars on performing its own technological research and development.

Chinese industrial espionage has also plagued the American economy for many years. Much of it is carried out by individuals or organizations supported by the Chinese government. A 2015 FBI survey found that half of 165 private companies claimed to have been victims of industrial espionage, with most cases being orchestrated from China. In May 2015, the US Justice Department indicted six Chinese citizens on charges of stealing confidential wireless technology from American companies Avago Technologies and Skyworks Solutions Inc., which manufacture components for the Apple iPhone. The individuals had established a market through the Chinese government-controlled Tianjin University to manufacture and sell the technology to Chinese businesses and military contractors. Incidents of industrial espionage continued to occur throughout the subsequent years, and in 2021, a chemist who had worked for the Coca-Cola Company was convicted of stealing and attempting to profit from trade secrets regarding the chemical coatings used on the interiors of soda cans.

—Michael Ruth

Further Reading

- Bruer, Wesley. "FBI Sees Chinese Involvement amid Sharp Rise in Economic Espionage Cases." *CNN*, 24 July 2015, www.cnn.com/2015/07/24/politics/fbi-economic-espionage.
- Connolly, Kate. "Germany Accuses China of Industrial Espionage." *The Guardian*, 22 July 2009, www.theguardian.com/world/2009/jul/22/germany-china-industrial-espionage.
- Grossman, Andrew. "U.S. Charges Six Chinese Citizens with Economic Espionage." *Wall Street Journal*, 19 May 2015, www.wsj.com/articles/u-s-charges-six-chinese-citizens-with-economic-espionage-1432046527.
- Kenton, Will. "Industrial Espionage: Definition, Examples, Types, Legality." *Investopedia*, 12 July 2022, www.investopedia.com/terms/i/industrial-espionage.asp.
- Mihm, Stephen. "China Didn't Invent Industrial Espionage." *Bloomberg*, 26 May 2015, www.bloomberg.com/view/articles/2015-05-26/china-didnt-invent-industrial-espionage.
- "PH.D. Chemist Sentenced to 168 Months for Conspiracy to Steal Traded Secrets, Economic Espionage, Theft of Trade Secrets, and Wire Fraud." *US Attorney's Office Eastern District of Tennessee*, 9 May 2022, www.justice.gov/usao-edtn/pr/phd-chemist-sentenced-168-months-conspiracy-steal-traded-secrets-economic-espionage.
- "What Is 'Economic Espionage'?" *FBI*, www.fbi.gov/about/faqs/what-is-economic-espionage.

INFORMATION SECURITY ANALYST

ABSTRACT

Information security analysts use encryption techniques, firewalls, and other tools and strategies to ensure the security of an organization's computer networks and systems. They work in a variety of fields, including both industry and government. Students aspiring to enter the profession should pursue studies in subjects such as computer science, programming, and cryptography.

BACKGROUND

Information security analysts design and monitor technological systems that shield computer networks

from outside threats. They encrypt system data, erect firewalls, and utilize a wide variety of hardware and software tools to ensure that homes, businesses, and government agencies remain protected from criminals, viruses, hackers, and other security threats. Information security analysts who work in the video game industry, known as game security analysts, strive to ensure that the games they work on are secure from cheating and fraud. They also investigate cheaters and monitor cheat communities.

OVERVIEW

Information security analysts work primarily in administrative and office settings. Analysts work at a variety of locations in and around offices and organizational complexes, most often at their own private workstations. They may also spend time working at the workstations of other employees, servicing their computers or installing equipment. Information security analysts also work in temperature-controlled server housing rooms and may be required to work remotely.

The field of information security attracts critical thinkers with a passion for electronics and computing who enjoy tackling complex problems. Information security analysts often get a tremendous amount of satisfaction from staying ahead of and repeatedly outsmarting security threats. Analysts also possess the patience to scrutinize extremely complicated data.

DUTIES AND RESPONSIBILITIES

Information security analysts handle a wide variety of duties and responsibilities on an everyday basis. Their main responsibility is to protect computer systems from constant outside threats. They are also tasked with identifying new potential security threats and encrypting archival data.

Data encryption is one of the central tasks of information security analysts. They are also responsible for constructing firewalls to protect

organizational information. Some information security analysts are responsible for building, monitoring, and maintaining custom firewall and encryption systems for specific organizations and businesses, while others operate standard network-based firewall applications for a collection of clients.

Information security analysts are constantly on the lookout for security breaches, evidenced by the presence of outside influences on a computer network or traces of past network violations. In the event of a security breach, analysts will alert senior staff members and recommend enhancements to prevent future violations. This constant need for adaptation requires analysts to stay abreast of new developments in computer security technology through ancillary academic coursework, industry publications, annual meetings, and training seminars.

In addition to constantly monitoring the potential security risks that may target their business or organization, information security analysts must also stay informed of legislation and political developments related to digital security, particularly those that affect the rights of business clients and the civil liberties of individuals.

Game security analysts are responsible for protecting the intellectual property of the video game companies for which they work. They are charged with supporting the day-to-day operations of their company's anticheat and antifraud programs. They monitor various metrics to determine the levels and incidence of cheating on the games within their purview and tune and support security measures to ensure that problems are fixed. They develop new anticheat measures and, in some companies, are charged with investigating reported cheaters or other bad actors.



Photo via iStock/gorodenkoff. [Used under license.]

They may also monitor cheating communities to document the latest trends in cheating. Finally, they prepare detailed reports and intelligence analysis to present to the company's executives.

WORK ENVIRONMENT

Physical environment. Information security analysts predominantly work in office settings with occasional off-site work. They work in almost every industry, from business and finance to education, government, transportation, communications, and the military.

Human environment. Many of the tasks of information security analysts are conducted individually. However, the explanation of different security systems to coworkers and clients requires group and one-on-one interactions.

Technological environment. Information security analysts are highly trained in technology. They utilize a variety of computer science technologies, including software, hardware, and network technology. They must also be well adept at computer programming languages and web communication.

EDUCATION AND TRAINING

High school/secondary. High school students can best prepare for a career as an information security analyst by completing courses in algebra, calculus, geometry, trigonometry, and computer courses such as introductory programming. Exposure to computer systems via internships or volunteer work can also build an important foundation for students interested in being employed in computer science.

College/postsecondary. A bachelor's degree is a standard requirement for nearly all employment vacancies in the information security profession. Most candidates arrive to the field after academic training in general computer science, programming or software development while others prepare for the role by completing degree programs dedicated specifically to computer and network security.

Postsecondary students who study information security complete coursework in such topics as network design, intrusion detection, wireless security, system administration, and cryptography. Additional related coursework also includes system administration and architecture and firewall construction.

Adult job seekers. The field of information security requires extensive academic and professional training. Individuals with no background in a related field should enroll in a college or a technical or vocational school that offers a program in computer security. Technical schools are also a great place for job seekers to network. Communication technologies and standards are always changing, so information security analysts should be willing to continue learning throughout their career.

Professional certification and licensure. There are numerous professional certifications available for information security professionals, each of which expands their frame of reference while making them attractive candidates for professional vacancies. Certifications include Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), Certified Information Security Manager (CISM), and Global Information Assurance Certification (GIAC).

Additional requirements. Information security is a constantly evolving field. Those interested in a career as an information security analyst must possess the patience and professionalism to stay up to date on rapidly emerging developments in a variety of technical disciplines, notably mobile communications, network diagnostics, software development, and hardware design. A knowledge of a number of basic programming languages, such as C++, is generally required. Game security analyst positions may require knowledge of C, C++, Cheat Engine, and interactive disassembler (IDA). Python and structured query language (SQL) are also recommended.

—John Pritchard

Further Reading

- Easttom, Chuck. *Computer Security Fundamentals*. 5th ed., Pearson, 2023.
- Rocchi, Walter. *Cybersecurity and Privacy Law Handbook*. Packt, 2022.
- Stewart, Andrew J. *A Vulnerable System: The History of Information Security in the Computer Age*. Cornell UP, 2021.

INFORMATION TECHNOLOGY

ABSTRACT

Information technology (IT) encompasses a wide range of activities, from pure theory to hands-on jobs. At one end of the spectrum are IT professionals who design software and create system-level network designs. These help organizations to maximize their efficiency in handling data and processing information. At the other end are positions in which physical hardware, from telecom equipment to devices such as routers and switches, are connected to one another to form networks. They are then tested to make sure that they are working correctly. This range includes many different types of employees. For example, there are computer technicians, system administrators, programmers at the system and application levels, chief technology officers, and chief information officers.

BACKGROUND

One way of studying the history of information technology (IT) is to focus on the ways that information has been stored. Information technology's history can be divided into different eras based on what type of information storage was available. These eras include prehistoric, before information was written down, and early historical, when information started to be recorded on stone tablets. In the middle historical period, information was recorded on paper and stored in libraries and other archives. In the modern era, information has moved from physical storage to electronic storage. Over time, information storage has become less

physical and more abstract. Information technology now usually refers to the configuration of computer hardware in business networks. These allow for the manipulation and transfer of electronically stored information.

Information technology gained prominence in the 1990s, as the internet began to grow rapidly and become more user-friendly than it had been in the past. Many companies arose to try to take advantage of the new business models that it made possible. Computer programmers and network technology experts found themselves in high demand. Startup companies tried to build online services quickly and effectively. Investment in technology companies put hundreds of millions of dollars into IT research. Even established companies realized that they needed to invest in their IT infrastructure and personnel if they wanted to stay competitive. As the IT sector of the economy grew rapidly, financial experts began to worry that it was forming an economic bubble. An economic bubble occurs when a market grows rapidly and then that growth declines abruptly. The bubble eventually "pops," and investors pull their money out. This did happen, and many internet startups shut down.



Zuse Z3 replica on display at Deutsches Museum in Munich. The Zuse Z3 is the first programmable computer. Photo by Venusianer, via Wikimedia Commons.

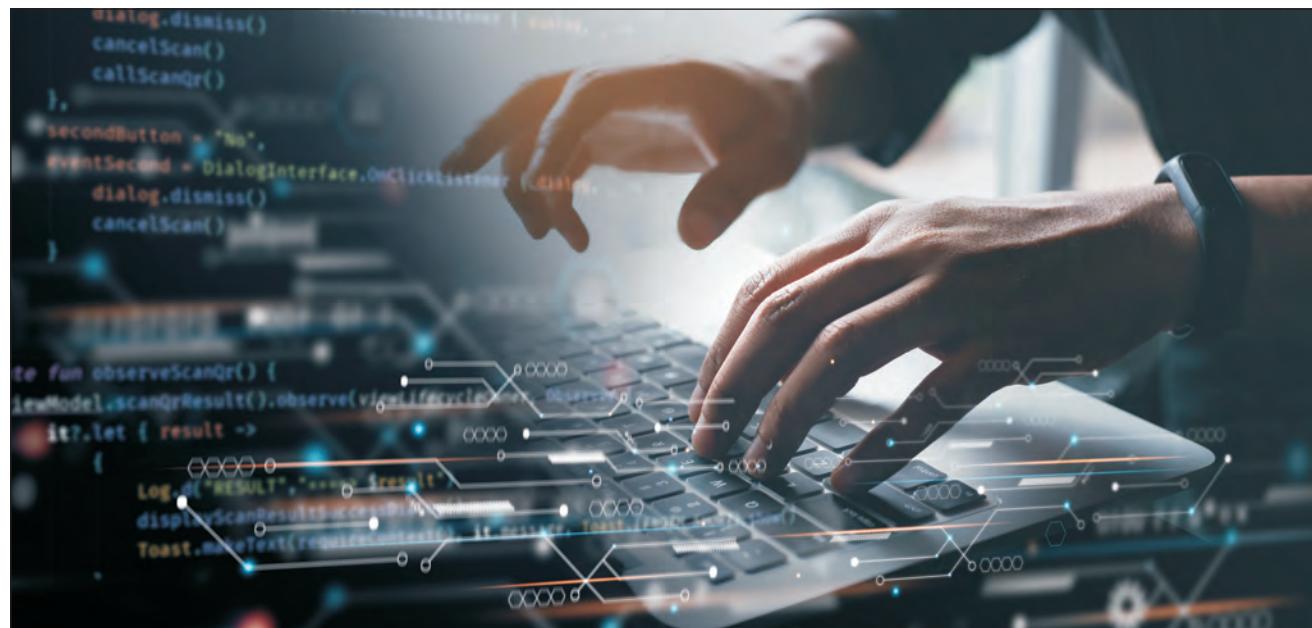


Photo via iStock/Tippapatt. [Used under license.]

OVERVIEW

While the dot-com bubble, as it came to be known, passed quickly, IT remained a central part of life. Simple tasks that used to be done without sophisticated technology, such as banking, shopping, and even reading a book, now involve computers, mobile phones, tablets, or e-readers. This means that the average person must be more familiar with IT in the twenty-first century than in any previous era. Because of this, IT has become a topic of general interest. For example, an average person needs to know a bit about network configuration in order to set up a home system.

With IT, new information is constantly being created. Once it was possible for a single person to master all of society's knowledge. In the modern world, more data is produced every year than a person could assimilate in a lifetime. The availability of IT is the factor most responsible for the explosion in data production. Most cell phone plans measure customer data in how many gigabytes (GBs) per month may be used, for example. This is because of

the many photos, videos, and social media status updates people create and share on the internet every day. The pace of this data explosion increases as time goes on.

—Scott Zimmer

Further Reading

- Black, Jeremy. *The Power of Knowledge: How Information and Technology Made the Modern World*. Yale UP, 2014.
- Bwalya, Kelvin J., Nathan M. Mnjama, and Peter M. I. I. M. Sebina. *Concepts and Advances in Information Knowledge Management: Studies from Developing and Emerging Economies*. Elsevier, 2014.
- Campbell-Kelly, Martin, William F. Aspray, Jeffrey R. Yost, Honghong Tinn, and Gerardo Con Díaz. *Computer: A History of the Information Machine*. 4th ed., Routledge, 2023.
- Fox, Richard. *Information Technology: An Introduction for Today's Digital World*. CRC, 2013.
- Lee, Roger Y., editor. *Applied Computing and Information Technology*. Springer, 2014.
- Marchewka, Jack T. *Information Technology Project Management*. 5th ed., Wiley, 2015.
- O'Leary, Timothy, Linda O'Leary, and Daniel O'Leary. *Computing Essentials 2023*. McGraw-Hill, 2022.

INTERNET OF THINGS

ABSTRACT

The Internet of Things (IoT) describes the trend of more and more devices being connected to the internet and to each other. As smartphones, wearable data collection devices, and other “connected” products become more common, the IoT is becoming more useful and more popular. The IoT became a real factor beginning in the early 2010s, as high-speed internet became more readily available and hardware and software became less expensive to produce. It has been said that IoT could potentially affect all devices with an on/off switch. The impact of the IoT will most likely be far-reaching, as it will affect people’s personal lives as well as businesses.

BACKGROUND

The Internet of Things (IoT) is a term used to describe a trend in which numerous devices are

designed to be connected to the internet and to each other. The IoT has become possible for a number of reasons, perhaps most notably the increasing availability of broadband internet throughout the first decades of the twenty-first century. As more people become connected to the web, the demand for data and connectivity has increased. At the same time, the cost of hardware and software production has decreased. Another reason the IoT has become more prevalent is that more people are using smartphones, wearable data collection devices, and “smart” devices such as smart televisions and smart speakers. Computing technology gives people access to the internet and data at all times and in all places.

People are also becoming more aware of the IoT’s importance. The IoT will have far-reaching effects, and many people believe that it will also have great economic value. Connected devices that send information can help reduce the amount of time that



Image via iStock/NicoElNino. [Used under license.]

humans spend collecting and analyzing data. In other words, the IoT can help businesses and people be more efficient and save them money.

OVERVIEW

Objects that can be connected using the IoT include almost anything that can be turned on and off. These devices include home security systems, vehicles, medical devices, appliances, smartphones, and much more. Some examples of the IoT at work are a thermostat that a homeowner can change using a smartphone or a wearable device that tells a person how far she ran during a workout.

The IoT depends a great deal on data. Many modern devices collect and track data. When devices are connected through the IoT, they can transmit the data they collect. The IoT will help devices connect with people and other devices. In addition, it will help people connect with other people.

EFFECTS OF THE IOT

The IoT could possibly affect every business sector in the world. The fields that will most likely see important effects include manufacturing and production, health and medicine, and transportation.

Manufacturing and production. The IoT will affect many business sectors, but it has the potential to change manufacturing and production greatly. A manufacturing facility could use the IoT to reorder supplies when they are running low without a human having to check inventory. Company machines connected to the IoT could inform an employee when they need to be repaired, a capability known as “predictive maintenance.” Such practices can increase efficiency, production uptime, and product quality while lowering costs and energy use. IoT manufacturing equipment may also enhance workers’ safety and productivity.

Health and maintenance. Wearable devices that track exercise and fitness are already a significant part of the IoT; others serve as medical emergency

bracelets. Still other medical devices connected to the IoT have the potential to be even more important for health and medicine. It is possible that someday scanning devices could analyze results and help doctors prescribe treatments for patients. Medical devices connected to the IoT could also connect doctors located in different parts of the world. These types of collaborations could help patients receive improved care.

Transportation. The IoT could help automobiles locate empty parking spaces and drivers locate available vehicles via car-sharing apps. In addition, cars could be fitted with technology that would automatically send a message to friends, family members, or colleagues when drivers are stuck in heavy traffic. They could also use diagnostic sensors to alert drivers and manufacturers to maintenance and repair needs. IoT technology might also help airplanes avoid deadly collisions or enable the planes to report when they require maintenance. Onboard devices have expanded travelers’ wireless internet connectivity for cell phones and computers, and popular smartphone navigation and music apps have increasingly been integrated into automotive electronics systems.

Everyday effects. Most people can see the effects that the IoT will have on business. However, the IoT also has the potential to impact everyday life. Homeowners are already using security systems, smoke detectors, and lighting that can be accessed from smartphones, as well as virtual personal assistants via smart speakers. Both smart speakers and smart televisions facilitate the consumption of digital media, including music, podcasts, web videos, and films. Indoor air quality, energy management, and water use are other areas in which IoT assists property owners. People could also see their lives change in other small ways thanks to the IoT. For example, an IoT refrigerator could tell people when they are running low on milk or eggs. A person could locate a wallet, purse, phone, remote

control, or lost pet using an app on a computer or smartphone.

The IoT could also affect towns and cities. Smart cities could use the IoT to control traffic lights to make roads less congested. Devices connected with the IoT could also track water and air pollution in an attempt to identify the causes. Cities could easily provide visitors with information about local attractions, including real-time data. For instance, an amusement park could provide guests with data about the current wait times at particular attractions.

Security Concerns and the IoT

The IoT relies a great deal on the sharing of data. Because of that, some experts are concerned about data security on the IoT. According to the statistics platform *Statista*, 11.28 billion IoT connected devices were in use worldwide as of 2021, and that number was projected to increase to more than 29 billion by 2030. The widespread adoption of such devices gives hackers access to a large quantity of potentially sensitive personal information, including medical records, city utility details, and more.

Experts have pointed out that many devices are unencrypted, which means the data is easy for hackers to read and understand. In addition, many devices and software platforms require, or even provide, only weak passwords. A number of factors leave IoT devices and their users vulnerable to hackers, surveillance, and malware, including the difficulty or infeasibility of upgrading many IoT devices and the inclusion of “backdoors” by manufacturers. To ensure data, software, and hardware are secure in the future, IoT users, businesses, and governments will have to make internet security a priority and develop new ways to protect data on the IoT.

—Elizabeth Mohn

Further Reading

Burgess, Matt. “What Is the Internet of Things? WIRED Explains.” *Wired*, 16 Feb. 2018, www.wired.co.uk/article/internet-of-things-what-is-explained-iot.

Greengard, Samuel. *The Internet of Things*. Rev. ed., MIT Press, 2021.

Kumar, Raghvendra, Rohit Sharma, and Prasant Kumar Pattnaik, editors. *Multimedia Technologies in the Internet of Things Environment*. Springer, 2021.

Meola, Andrew. “Smart Buses, Trains, Cars & Planes: How IoT Will Create Private and Public Smart Transportation.” *Business Insider*, 30 Jan. 2020, www.businessinsider.com/smart-transportation-iot.

Morgan, Jacob. “A Simple Explanation of ‘The Internet of Things.’” *Forbes*, 13 May 2014, www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand.

“Number of Internet of Things (IoT) Connected Devices Worldwide from 2019 to 2021, with Forecasts from 2022 to 2030.” *Statista*, July 2022, www.statista.com/statistics/1183457/iot-connected-devices-worldwide.

O’Marah, Kevin, and Pierfrancesco Manenti. “The Internet of Things Will Make Manufacturing Smarter.” *Industry Week*, 14 Aug. 2015, www.industryweek.com/manufacturing-smarter.

INTERNET PROTOCOL

ABSTRACT

The internet protocol (IP) is the main communications protocol of the internet protocol suite (commonly called the TCP/IP), the networking model that establishes the internet. A network enables the exchange of information, while a protocol is a set of conventions for formatting communications data. The IP is the method by which data is transferred between computers via the internet. Thus, its routing system, or system for directing, is what makes the internet a place for exchanging information.

BACKGROUND

Two versions of the internet protocol (IP) are in use: four (IPv4) and six (IPv6). IPv4 is the most common, as nations have been slow to adopt IPv6. Each computer connected to the internet has an IP address, a set of numbers that uniquely identify the computer. IPv4 addresses consist of 32 bits of digital space,

while IPv6 uses 128-bit addresses. There are two parts to the address identification: the specific computer network and the specific device within that network. On the internet itself, between routers that move packets of information, only the network address needs to be accessed. Both pieces of information are necessary for sending the message from a network point directly to a computer.

OVERVIEW

When data such as a website page or an email is sent via the internet, the message is divided into packets called “datagrams.” Each datagram is composed of a header and a payload. The header contains the source (sender) and destination (receiver) IP addresses, each of which includes the computer’s unique network and device addresses, and other metadata needed for routing and delivering the packet. The payload is the message data itself.

The datagram is first sent to a gateway computer—a network point that functions as the entranceway to another network—which reads the destination address and forwards the message to the next gateway. This gateway reads and forwards the address to yet another gateway, and so on, until the message reaches the closest gateway to its destination. The last gateway recognizes the datagram’s address as belonging to its domain, or the set of network addresses under its control, and forwards the message directly to the final device destination.

IP routing service is considered unreliable because of the dynamic nature of the internet and the possibility that any network element may also be unreliable. Therefore, the IP has no continuing connection between end points. Each packet of data is treated independently from all other packets of data. Individual datagrams may not necessarily travel the same route across the internet, as they are trying to get past any errors along the way, and they may arrive in a different order than they were sent. The IP is just a delivery service, so another internet

protocol, the transmission control protocol (TCP), reorganizes the datagrams into their original order.

—Julia Gilstein

Further Reading

- Abraham, Prabhakaran, Mustafa Almahdi Algaet, and Ali Ahmad Milad. “Performance and Efficient Allocation of Virtual Internet Protocol Addressing in Next Generation Network Environment.” *Australian Journal of Basic & Applied Sciences*, vol. 7, no. 7, 2013, pp. 827–32.
- Blank, Andrew G. *TCP/IP Jumpstart: Internet Protocol Basics*. 2nd ed., Sybex, 2002.
- Cirani, Simone, Gianluigi Ferrari, and Luca Veltri. “Enforcing Security Mechanism in the IP-Based Internet of Things: An Algorithmic Overview.” *Algorithms*, vol. 6, no. 2, 2013, pp. 197–226.
- Clark, Martin P. *Data Networks, IP, and the Internet*. Wiley, 2003.
- Coleman, Liv. “‘We Reject: Kings, Presidents, and Voting’: Internet Community Autonomy in Managing the Growth of the Internet.” *Journal of Information Technology & Politics*, vol. 10, no. 2, 2013, pp. 171–89.
- Gaffin, Julie C. *Internet Protocol 6*. Novinka, 2007.
- Loshin, Peter. *IPv6: Theory, Protocol, and Practice*. 2nd ed., Morgan Kaufmann, 2004.
- Oki, Eiji, et al. *Advanced Internet Protocols, Services, and Applications*. Wiley, 2012.
- O’Leary, Timothy, Linda O’Leary, and Daniel O’Leary. *Computing Essentials 2023*. McGraw-Hill, 2022.
- “What Is the Internet Protocol?” *Cloudflare*, www.cloudflare.com/learning/network-layer/internet-protocol.
- Yoo, Christopher S. “Protocol Layering and Internet Policy.” *University of Pennsylvania Law Review*, vol. 161, no. 6, 2013, pp. 1707–71.

INTERNET TRACKING AND TRACING

ABSTRACT

Internet tracking is the collection of information about the websites and online services visited by internet users, as well as emails and instant messages sent and received. Internet tracing consists of following selected internet activity between senders and receivers.

BACKGROUND

To determine whether particular persons have used the internet to commit crimes, and later to prove in legal settings that such crimes were committed, law-enforcement authorities have to track suspects' internet activities. This forensic work often requires tracing how suspects use the internet.

Law-enforcement authorities can use internet tracking and tracing to identify and prosecute persons who are responsible for irresponsible or malicious Internet activity. Internet tracking and tracing are used, for example, in the identification, capture, and conviction of those who mount denial-of-service (DoS) attacks against online companies. In such attacks, the perpetrators attempt to stop particular internet sites from functioning.

Internet tracking and tracing techniques were successfully used to identify perpetrators of DoS attacks as early as the dawn of the twenty-first century. In a DoS case that took place in February 2000, for instance, a number of websites—including those of Yahoo!, CNN, and eBay—were overrun, and essentially disabled, by requests that were orchestrated by a young boy in Montreal, Canada, who used the alias “Mafiaboy.” Agents for the Federal Bureau of Investigation (FBI) and the Royal Canadian Mounted Police (RCMP) began to suspect that Mafiaboy was behind the DoS attacks after they tracked activity in

an internet chat room. After they established that Mafiaboy was a suspect, they used standard software to trace his uniform resource locator (URL)—that is, his online address—and obtain his internet protocol (IP) address. With this information, they obtained permission to tap the suspect's telephone and recorded his descriptions of the DoS attacks in subsequent phone conversations. Mafiaboy ultimately pleaded guilty to fifty-six charges related to his DoS attacks. Although estimates differ, it is generally agreed that his attacks caused more than \$1 million worth of damage to the companies he victimized.

OVERVIEW

The activities of internet tracking and tracing are often done by humans. For example, undercover agents might pose as children in online chat rooms to catch child predators. Humans also inspect internet log files heuristically to detect the misuse of browsers to search the internet for illegal items such as drugs and weapons.

Many of the forensic tools used for internet tracking and tracing are computer programs that are designed to search chat rooms, websites, and email automatically. For example, during the first decade of the twenty-first century, the social-networking site MySpace partnered with Sentinel Tech Holding Corporation to build a sexual predator database and search program that could automatically discover sexual predators using MySpace. The effort was so successful that several state attorneys general demanded and received predator information from MySpace to assist in the prosecutions of sexual predators in their states.

“Honey pots” are network resources that law-enforcement authorities use to fool potential online attackers into thinking they can easily perpetrate attacks; the authorities then let the attacks occur and collect important information about the attackers from these activities. Most honey pots are websites, but a number of wireless access-point



Image via iStock/mustafahacalaki. [Used under license.]

honey pots have been developed to defend against those attacking wireless networks. Honey pots have been very successful tools for the early identification of computer hackers and crackers.

TRACKING INDIVIDUAL USERS

Employers and concerned parents of internet-using children sometimes use internet tracking to detect and then prevent or control undesirable internet behavior. This type of tracking is generally done at individual computers with software programs that record every keystroke made by users. Individual internet tracking software packages record such information as messages and emails sent and received; peer-to-peer file searching and swapping; internet search strings typed; internet sites visited; and web-oriented programs used. By installing an individual tracking package on each computer, a company can encourage all employees to make proper use of the internet, catch those employees who abuse the internet, and document the company's efforts to secure its computer systems. Home and corporate products aimed at defending against malware (malicious software, including viruses and worms) often have databases of dangerous sites that function to stop users from visiting those sites. These software packages also keep records of users' attempts to access forbidden sites, such as pornography sites; this could be valuable information for parents, employers, or law-enforcement agencies if they need to prove that particular users have been misusing their internet access.

TRACKING AT ROUTERS AND FIREWALLS

Some of the most important internet tracking done by organizations takes place at border routers and firewalls, where it is routine to inspect all incoming internet traffic. If a firewall serves as a bastion host, for example, it will check all requests of the corporate web server for known attackers. Also, all emails arriving at an organization's email post office are

usually checked for viruses, with attachments opened and scanned as well. In addition to tracking incoming traffic, it is common for computer systems to track outgoing traffic as well.

Internet tracing to determine all routers used in the sending of web requests or emails is an important activity carried out by both individuals and organizations, including law-enforcement agencies. Numerous computer programs have been designed to carry out automatic traces to find the home addresses of online attackers or email senders. For example, some internet security packages intended for home use can provide the home IP addresses of suspected web server attacks with a simple mouse click on the URL.

The US government tracks web activity and email use as part of ongoing efforts to defend against potential terrorist threats. For example, for a period the FBI used a system known as Carnivore to monitor emails sent and received as a tool for identifying, deterring, and prosecuting terrorists. Public uproar over the use of such a system caused the government to drop the project, but the FBI is reported to have replaced Carnivore with commercial products that collect much of the same desired information.

—George M. Whitson III

Further Reading

- Almulhem, Ahmad, and Issa Traore. *Experience with Engineering a Network Forensics System*. Springer, 2005.
- Berghel, Hal. "The Discipline of Internet Forensics." *Communications of the ACM*, vol. 46, 2003, pp. 15–20.
- Easttom, Chuck. *Computer Security Fundamentals*. 5th ed., Pearson, 2023.
- Lutgens, Jason T., Matthew Pepe, and Kevin Mandia. *Incident Response and Computer Forensics*. 3rd ed., McGraw-Hill, 2014.
- Marcella, Albert J., and Robert S. Greenfield, editors. *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*. CRC Press, 2002.
- Shinder, Debra Littlejohn. *Scene of the Cybercrime: Computer Forensics Handbook*. Syngress, 2002.

- Stouffer, Clare. "Internet Tracking: How and Why We're Followed Online." *Norton*, 28 June 2021, us.norton.com/blog/privacy/internet-tracking.
- Vacca, John R. *Computer Forensics: Computer Crime Scene Investigation*. 2nd ed., Charles River Media, 2005.

INTRUSION DETECTION AND PREVENTION

ABSTRACT

In the information technology (IT) context, administrators of computer systems and networks watch for attempts (both successful and not) to break into their systems and networks. Over the course of more than four decades, the technology used to detect these intrusion attempts and prevent them from succeeding has gone from a haphazard set of homegrown tools with limited automation, heavily reliant on the human administrator, to near instantaneous automated responses.

BACKGROUND

An "intrusion" within an IT context, as defined by the National Institute of Standards and Technology's (NIST's) Computer Security Resource Center, is "a security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without having authorization to do so."

Detecting and preventing intrusions into computer systems is a practice as old as access control. Whether the urge to control access to certain systems happened first or the abuse of certain systems—necessitating the requirement to control access—happened first might be lost to time.

The shift from manual reviews to conceptualizing a more automated process can be traced to 1980, when computer security expert James Anderson wrote the paper "Computer Security Threat Monitoring and Surveillance." In that paper, Anderson

suggested creating tools to help security personnel audit logs; he also thought it was possible to use statistical analysis to detect anomalies in log data.

In 1987, the Institute of Electrical and Electronics Engineers (IEEE) published a paper by Dorothy E. Denning of SRI International in the journal *IEEE Transactions on Software Engineering*. Titled "An Intrusion-Detection Model," her paper "describes a model for a real-time intrusion-detection expert system that aims to detect a wide range of security violations ranging from attempted break-ins by outsiders to system penetrations and abuses by insiders." The framework was used by SRI International to develop its Intrusion Detection Expert System (IDES), one of the earliest intrusion detection systems.

Intrusion detection systems only look at activity to check it against patterns of behavior. They are looking for patterns that match signatures, which are set patterns found in malicious software (also known as malware). The idea of the signature originated with antivirus software, which was designed to recognize common behaviors that each virus was known to perform on a computer.

OVERVIEW

There are many ways to classify different types of intrusion detection systems, but the two most common types are a network intrusion detection system (NIDS) and a host-based intrusion detection system (HIDS), where a host is another name for a computer.

Computers (hosts) generate and store system logs—historical records of things that happened within the computer—using a protocol called "syslog," which has led to the colloquial use of the term to reference any logs on a system. Reviewing those log files can allow a systems administrator to figure out why a given computer had a problem. Over time, they also became useful for tracking who logged into the system, when they logged in, and what actions they took at a system level that might impact the

system for good or for bad. The evolution of troubleshooting from figuring out problems to figuring out abusive behavior was a natural one.

In contrast, a NIDS scans network traffic, looking for common patterns. For instance, someone repeatedly connecting to a host over and over is usually an indication that someone is trying to guess a password. Another example is traffic looking for web pages that do not exist, trying to exploit old versions of known software at commonly designated locations.

Over time, intrusion detection and prevention technologies evolved into sophisticated systems that review the logs and, when combined with an intrusion prevention system (IPS), can automatically act based on rules that were put in place in advance or after detecting statistically anomalous behavior. Due to the high ratio of false positives (detecting something that is actually fine) and false negatives (failing to detect problems), many systems administrators prefer their intruder detection system (IDS) to generate notifications so that a human can intervene and take action.

However, there are events that can cause significant problems before a human gets a chance to review an alert. System and network administrators must perform a risk analysis to determine how strictly rules are applied. If the rules are too strict, end users can become frustrated and even try to find workarounds to bypass security. If the rules are too lax, successful attacks can cause problems across systems and networks.

As networks and connections to the internet get bigger and faster, it is becoming increasingly difficult for a NIDS to keep track of the flood of traffic. This prioritizes the need for an HIDS. But the current state of an HIDS as of the early 2020s is signature-based, and one problem is that signatures for new attacks are only published every few days to once a week. That is a long time during which bad actors can play havoc with hosts. This is why it is

important to use an HIDS in combination with other countermeasures, such as an IPS looking for unusual behaviors. Again, system administrators must perform a risk analysis to determine how strictly the IPS responds.

A network-based IPS monitors traffic in both directions and maintains awareness of the complete connection. Most network protocols go through multiple steps of synchronization and acknowledgement, with traffic going back and forth between two hosts before data begins to flow. This allows the IPS to determine whether a connection might be malicious and respond accordingly. However, an IPS capable of tracking all aspects of a connection requires significant processing power and speed. There are some who theorize that moving the IPS into the cloud might be a solution, but this introduces other issues such as response lag, which can be particularly problematic when there is already a network issue in play.

As attacks get more complex and harder to detect, tuning an IPS with a small false positive rate will be a challenge. As the techniques being used by bad actors evolve, intrusion detection and prevention must constantly evolve as well, to play catch-up.

—Kelly J. Cooper

Further Reading

- Anderson, James. “Computer Security Threat Monitoring and Surveillance.” James P. Anderson Co., 1980, [csric.nist.gov/files/pubs/conference/1998/10/08-proceedings-of-the-21st-nissc-1998/final/docs/early-cs-papers/ande80.pdf](https://www.csric.nist.gov/files/pubs/conference/1998/10/08-proceedings-of-the-21st-nissc-1998/final/docs/early-cs-papers/ande80.pdf).
- “Catching the Hackers—Introduction to Intrusion Detection Certification Training Class.” NICCS, 16 Aug. 2022, [niccs.cisa.gov/education-training/catalog/security-university/catching-hackers-introduction-intrusion-detection](https://www.niccs.cisa.gov/education-training/catalog/security-university/catching-hackers-introduction-intrusion-detection).
- “Computer System Engineering.” MIT Open Courseware, 2018, ocw.mit.edu/courses/6-033-computer-system-engineering-spring-2018/pages/week-13.
- Denning, Dorothy. “An Intrusion-Detection Model.” IEEE Transactions on Software Engineering, vol. SE-13, no. 2,

1987, pp. 222–32, ieeexplore.ieee.org/document/1702202.

Easttom, Chuck. *Network Defense and Countermeasures: Principles and Practices*. 4th ed., Pearson, 2023.

“Intrusion.” NIST Computer Security Resource Center, csrc.nist.gov/glossary/term/intrusion.

“Intrusion Detection System (IDS).” Geeks for Geeks, 14 Mar. 2023, www.geeksforgeeks.org/intrusion-detection-system-ids.

IOS

ABSTRACT

Apple’s iPhone operating system (iOS) is an operating system designed for mobile computing. It is used on the company’s iPhone and iPod Touch products and was previously used on the iPad. The system, which debuted in 2007, was based on the company’s OS X. iOS was the first mobile OS to incorporate advanced touch-screen controls.

BACKGROUND

Apple’s iOS is an OS designed for use on Apple’s mobile devices, including the iPhone and iPod Touch. In 2020, iOS was the world’s second most popular mobile OS after the Android OS. Between 2010 and 2019, Apple’s iPad tablet devices also used iOS. However, Apple renamed the variant of iOS used for the iPad the iPadOS in mid-2019.

Introduced in 2007, iOS (then known as iPhone OS) was one of the first mobile OSs to incorporate a capacitive touch-screen system. The touch screen allows users to activate functions by touching the screen with their fingers. The Apple iOS was also among the first mobile OSs to give users the ability to download applications (apps) to their mobile devices. The iOS is therefore a platform for numerous apps, including the approximately 1.8 million apps available in the App Store by mid-2023. The first iOS system and iPhone were unveiled at the 2007 Macworld Conference.

OVERVIEW

The original iOS had a number of limitations. For example, it was unable to run third-party apps, had no copy and paste functions, and could not send email attachments. It was also not designed for multitasking, forcing users to wait for each process to finish before beginning another. However, iOS introduced a sophisticated capacitive touch screen. The iOS touch features allowed users to activate most functions with their fingers rather than needing a stylus or buttons on the device. The original iPhone had only five physical buttons. All other functions, including the keyboard, were integrated into the device’s touch screen. In addition, the iOS system supports multitouch gestures. This allows a user to use two or more fingers (pressure points) to activate additional functions. Examples include “pinching” and “stretching” to shrink or expand an image.

JAILBREAKING

Computer hobbyists soon learned to modify the underlying software restrictions built into iOS, a process called “jailbreaking.” Modified devices allow users greater freedom to download and install apps. It also allows users to install iOS on devices other than Apple devices. Apple has not typically pursued legal action against those who jailbreak iPhones or other devices. In 2010, the US Copyright Office authorized an exception permitting users to jailbreak their legally owned copies of iOS for select legal purposes. However, jailbreaking iOS voids Apple warranties.

VERSION UPDATES

The second version of iOS was launched in July 2008. With iOS 2, Apple introduced the App Store, where users could download third-party apps and games. In 2009, iOS 3 provided support for copy and paste functions and multimedia messaging. A major advancement came with the release of iOS 4



Photo via iStock/borchee. [Used under license.]

in 2010. This update introduced the ability to multitask, allowing iOS to begin multiple tasks concurrently without waiting for one task to finish before initiating the next task in the queue. The iOS 4 release was also the first to feature a folder system in which similar apps could be grouped together on the device's home screen (called the "springboard"). FaceTime video calls also became available with iOS 4.

The release of iOS 5 in 2011 integrated the voice-activated virtual assistant Siri as a default app. Other iOS 5 updates include the introduction of iMessage, Reminders, and Newsstand. In 2012, iOS 6 replaced Google Maps with Apple Maps and redesigned the App Store, among other updates. Released in 2013, iOS 7 featured a new aesthetic and introduced the Control Center, AirDrop, and iTunes Radio.

FURTHER INNOVATIONS

With the release of iOS 8, Apple included third-party widget support for the first time in the company's history. Widgets are small programs that do not need to be opened and continuously run on a device. Examples include stock tickers and weather widgets that display current conditions based on data from the web. Widgets had been a feature of Android and Windows mobile OSs for years. However, iOS 8 was the first iOS version to support widgets for Apple. Since their release, Apple has expanded the availability of widgets for users.

The release of iOS 9 in 2015 marked a visual departure for Apple. This update debuted a new typeface for iOS called San Francisco. This specially tailored font replaced the former Helvetica Neue. The release of iOS 9 also improved the battery life of Apple devices. This update introduced a

low-power mode that deactivates high-energy programs until the phone is fully charged. Low-power mode can extend battery life by as much as an hour on average.

Coinciding with the release of iOS 9, Apple also debuted the iPhone 6S and iPhone 6S Plus, which introduced 3D Touch. This new feature is built into the hardware of newer Apple devices and can sense how deeply a user is pressing on the touch screen. 3D Touch is incorporated into iOS 9 and enables previews of various functions within apps without needing to fully activate or switch to a new app. For instance, within the camera app, lightly holding a finger over a photo icon will bring up an enlarged preview without needing to open the iPhoto app.

Apple added additional features to iOS over the subsequent years, including implementing the use of apps within iMessage in iOS 10. The OS continued to evolve through the releases of iOS 11 and iOS 12, the latter of which introduced a function known as Screen Time, used to track and limit an individual's time using a device or a specific app. Released in September of 2019, iOS 13 introduced Dark Mode as well as a variety of tweaks to existing apps and features. In September of 2020, iOS 14 introduced features such as home-screen widgets, pinned conversations in Messages, and an App Library.

The iOS 15 update, released in September 2021, added features such as Live Text and new focus modes, while iOS 16, introduced the following year, made changes to the lock screen and notifications,

among other elements of the OS. Apple released iOS 17 in September of 2023. Among other new elements, the updated OS included a Personal Voice feature that enabled users to train their phones to mimic their voices as well as enhanced security features.

—Micah L. Issitt

Further Reading

- “App Store.” *Apple*, 2023, www.apple.com/app-store.
- Chakkattu, Julian. “The Top New Features in Apple’s iOS 17 and iPadOS 17.” *Wired*, 8 June 2023, www.wired.com/story/apple-iphone-ios-17-ipados-17-new-features.
- Costello, Sam. “The History of iOS, from Version 1.0 to 17.0.” *Lifewire*, 5 June 2023, www.lifewire.com/ios-versions-4147730.
- Heisler, Yoni. “The History and Evolution of iOS, from the Original iPhone to iOS 9.” *BGR*, 19 Dec. 2018, bgr.com/2016/02/12/ios-history-iphone-features-evolution.
- “iOS: A Visual History.” *The Verge*, 16 Sept. 2013, www.theverge.com/2011/12/13/2612736/ios-history-iphone-ipad.
- Whittaker, Zack. “iOS 17 Includes These New Security and Privacy Features.” *TechCrunch*, 18 Sept. 2023, techcrunch.com/2023/09/18/ios-17-includes-these-new-security-and-privacy-features.
- Williams, Rhiannon. “Apple iOS: A Brief History.” *The Telegraph*, 17 Sept. 2015, www.telegraph.co.uk/technology/apple/11068420/Apple-iOS-a-brief-history.html.
- Wuerthele, Mike. “Apple Unveils iPadOS, Adding Features Specifically to iPad.” *AppleInsider*, 2 June 2019, appleinsider.com/articles/19/06/03/apple-supplements-ios-13-with-new-tablet-specific-ipad-os-branch.

M

MAC OS

ABSTRACT

Mac OS is a family of operating systems—programs used to run computers—pioneered by the Apple computer company and utilized on a wide variety of Apple systems. Noted for being the first successful graphical interface operating system and for making its debut on the original 1984 Macintosh, Mac OS played a key role in the emergence of the personal computer as a popular consumer product. Though later overshadowed by Microsoft Windows, Mac OS continued to be one of the most recognized and widely used operating systems on the market. Over the years, it evolved through a variety of iterations, each of which has offered new features and an improved user experience. From 2016 on, Mac OS was referred to as macOS.

BACKGROUND

Although Mac OS often receives credit for being the first graphical interface operating system, it actually had two predecessors. The first of these was the operating system featured on the Xerox Alto. The Alto was a computer manufactured in the 1970s with a graphical operating system that was the first of its kind. This software replaced the traditional command-line operating system that required users to issue text commands. However, its staggering cost of \$32,000 ensured that it would never be a commercial success. Regardless, after visiting Xerox's facilities in the early 1980s, Apple engineers recognized the potential of the graphical interface to the future of computing. Eventually, the Apple team members incorporated lessons from Xerox when they produced the Lisa, the first

Apple computer to feature a graphical interface operating system. Like the Xerox Alto, however, the Lisa was a commercial failure.

Still determined to make an affordable personal computer that would appeal to the average consumer, Apple introduced the Macintosh in 1984. Powering the Macintosh was a graphical interface operating system that, although unnamed at the time, would eventually become known as System 1, the first version of Mac OS. With a virtual desktop, windows, icons, menus, scrollbars, a file manager called Finder, and mouse control, System 1 represented a revolutionary shift in the user experience that would soon become the industry standard.

OVERVIEW

When the Macintosh proved to be a success, Apple engineers began working to improve its operating system. The result of their efforts was System 2, released in 1985. Though very similar to System 1, System 2 featured several key upgrades, such as the inclusion of key-commands for creating new folders and shutting down the computer, as well as an enhanced version of Finder. Thanks to these and other tweaks, System 2 ran 20 percent faster than System 1.

After Microsoft released the inaugural version of Windows in late 1985, Apple once again revisited the design of its own operating system. When System 3 debuted the following year, it included a new version of Finder that came equipped with file-nesting capabilities that allowed users to create folders within folders for the first time. It also included Disk Cache, a program that improved performance by



Photo via iStock/Ake Ngiamsanguan. [Used under license.]

storing commonly used commands in memory. While these improvements were helpful for users, System 3 was plagued by bugs and, as a result, did not work as well as hoped.

Apple released System 4 in 1987. Among other updates, System 4 offered support for disk drives and multiple monitors. It also included MultiFinder, a new version of Finder that allowed systems with enough memory to run more than one program at a time. The following year, Apple skipped System 5 and jumped ahead to System 6. The most notable improvement in System 6 was the inclusion of color support. Although the desktop and Finder were still rendered in black and white as they had been since System 1, System 6 made it possible for third-party applications to run in full color.

With the release of System 7 in 1991, Mac OS took its first major step forward. In addition to including a new version of Finder that combined the previously separate Finder and MultiFinder into a single file manager, System 7 introduced virtual memory, which turned unused disc drive space into random-access memory (RAM), a type of memory designed to improve system performance. Until the release of Mac OS X in 2001, System 7 was Apple's longest running operating system.

In 1997, Apple made the decision to officially rename its operating system series Mac OS. Thus, Mac OS 8 was the first title in the series not to bear the "System" name. Along with a number of other upgrades, Mac OS 8 featured the debut of Sherlock, an integrated web search function that worked in tandem with Finder.

Although not substantially different from Mac OS 8, 1999's Mac OS 9 offered several key improvements. Most notably, it allowed multiple users to create individual accounts on a single machine. Mac OS 9 also gave users the ability to download system updates from the internet.

The launch of Mac OS X in 2001 marked the debut of the modern Mac OS. Touting a completely redesigned user interface and a brand-new code base, Mac OS X radically changed the Apple experience. Along with several new features, Mac OS X also introduced the concept of protected memory, which prevented applications from corrupting one another's data. The debut of Mac OS X also enabled the creation of an array of new programs, including the Safari web browser. OS X, the tenth version of the Macintosh OS, was released on March 24, and it combined a stable Unix-based platform with a visually appealing user interface called Aqua. For software developers, OS X introduced the Carbon application programming interface (API) and the X-code integrated development environment (IDE) for writing code. OS X was a key step in making Macs a central focus of consumer computing culture. Cat-themed names for OS X releases were popular with enthusiasts and eventually became marketing devices. OS X versions progressed from Cheetah (version 10.0) and Puma (10.1) in 2001 to Jaguar (10.2) in 2002, Panther (10.3) in 2003, Tiger (10.4) in 2005, Leopard (10.5) in 2007, Snow Leopard (10.6) in 2009, Lion (10.7) in 2011, and Mountain Lion (10.8) in 2012.

Beginning with Mavericks (10.9) in 2013, the company moved away from the cat-themed names to names associated with California, subsequently introducing Yosemite (10.10) in 2014 and El Capitan (10.11) in 2015. In 2016, macOS Sierra (10.12) was released. Using the name "macOS" rather than "Mac OS," the release represented Apple's attempt to bring some consistency to the

naming of operating systems for all of its products, which also included iOS and watchOS. macOS High Sierra (10.13) followed in 2017, and macOS Mojave (10.14) followed in 2018.

In 2019, iTunes was dismantled, and macOS Catalina (10.15) allowed users to connect an iPad screen to their Mac. In 2020, macOS Big Sur (11) allowed users to run iOS apps natively on their Mac computers. These were called universal apps. Shortly afterward, in fall 2021, macOS Monterey (12) enabled Shortcuts and a wide range of FaceTime augmentations. The next version of macOS, macOS Ventura (13), was released in late 2022 and featured several new or renamed applications. In June of 2023, Apple announced that version 14 of macOS, known as macOS Sonoma, would be released later that year. The OS was made available to the public in September of 2023.

—Jack Lasky

Further Reading

- Edwards, Benj. "The Little-Known Apple Lisa: Five Quirks and Oddities." *Macworld*, 30 Jan. 2013, www.macworld.com/article/2026544/the-little-known-apple-lisa-five-quirks-and-oddities.html.
- Haslam, Karen. "macOS Versions: Every Version Including the Latest." *Macworld*, 13 June 2023, www.macworld.com/article/672681/list-of-all-macos-versions-including-the-latest-macos.html.
- "An Illustrated History of Mac OS X." *Tower*, 12 Jan. 2016, www.git-tower.com/blog/history-of-osx.
- Moretti, Marcus. "Before Mac OS X, There Was OS 1 Through 9: A History of Apple's Operating System." *Business Insider*, 10 July 2012, www.businessinsider.com/mac-os-i-through-x-2012-7?op=1.
- Porter, Jon. "Apple Announces macOS Sonoma with Game Mode and Support for Desktop Widgets." *The Verge*, 5 June 2023, www.theverge.com/2023/6/5/23745460/apple-macos-14-sonoma-features-updates-wwdc-2023.
- Warren, Christina. "The Evolution of Mac OS, From 1984 to Mountain Lion." *Mashable*, 17 Feb. 2012, mashable.com/2012/02/17/mac-os-timeline/#KKsyA8f26qqR.

MACHINE LEARNING

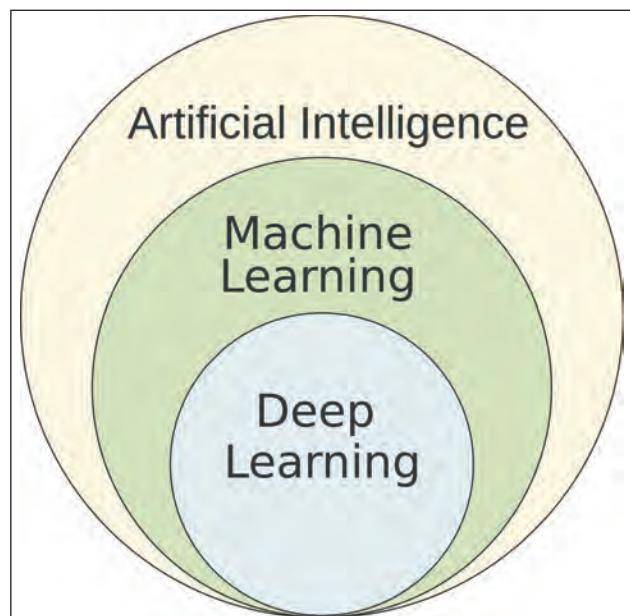
ABSTRACT

Machine learning is a branch of computer-science algorithms that allow the computer to display behavior learned from past experience, rather than human instruction.

Machine learning is essential to the development of artificial intelligence, but it is also applicable to many everyday computing tasks. Common examples of programs that employ machine learning include email spam filters, optical character recognition, and news feeds on social networking sites that alter their displays based on previous user activity and preferences.

BACKGROUND

One of the earliest attempts to enable machine learning was the perceptron algorithm, developed by Frank Rosenblatt in 1957. The algorithm was intended to teach pattern recognition and was based on the structure of a neural network, which is a computing model designed to imitate an animal's central nervous system. While the perceptron model



Machine learning as subfield of AI. Image by Lollizxc, via Wikimedia Commons.

showed early promise, Marvin Minsky and Seymour Papert demonstrated in their 1969 book *Perceptrons: An Introduction to Computational Geometry* that it had significant limitations, as there were certain classes of problems the model was unable to learn. Consequently, researchers did not pursue this area of study for some time.

In the 1980s, after other avenues for developing artificial intelligence had resulted in only limited success, scientists began to revisit the perceptron model. Multilayer perceptrons, or neural networks composed of multiple layered computational units, proved to have the processing power to express problems that Rosenblatt's single-layer, or linear, perceptrons could not. Around the same time, John Ross Quinlan introduced decision-tree algorithms, which use predictive models to determine a variable's value based on available data.

OVERVIEW

Since then, numerous machine-learning algorithms have been developed. Among those most commonly used are support vector machines (SVMs) and naive Bayes classifiers. SVMs, introduced by Vladimir N. Vapnik and Corinna Cortes in 1995 and based on an algorithm previously created by Vapnik, are used to recognize patterns in data and classify the various data points. Naive Bayes classifiers are applications of Bayes's theorem, named for the eighteenth-century mathematician and reverend Thomas Bayes, which deals with conditional probabilities. This algorithm was used in one of the earliest email spam filters, iFile, released by Jason Rennie in 1996. Many email clients still employ Bayesian spam filtering, which works by determining the probability that an email containing certain keywords is spam.

Machine-learning algorithms can be divided into categories based on how they train the machine. These categories include supervised learning, in which the machine learns from inputs that are mapped to desired outputs; unsupervised learning,

in which the machine analyzes input without knowledge of the desired output; semisupervised learning, in which some of the input is paired with a desired output and some is not; transduction, in which the machine tries to predict new outputs based on training with previous inputs and outputs; reinforcement learning, in which the machine must form a policy on how to act based on observing how certain actions affect its environment; and learning to learn, which teaches inductive bias based on previous experience. SVMs, multilayer perceptrons, decision trees, and naive Bayes classifiers all fall into the category of supervised learning.

It is important to distinguish between machine learning and data mining. Although the two concepts are related and use similar, often overlapping, methods, data mining is focused on discovering information about given data, while machine learning focuses more on learning from the given data in order to make predictions about other data in the future. Many consider data mining to be a subset of machine learning.

—Randa Tantawi

Further Reading

- Abu-Mostafa, Yaser S. “Machines That Think for Themselves.” *Scientific American*, July 2012, pp. 78–81.
- Alpaydin, Ethem. *Machine Learning*. Rev. ed., MIT Press, 2021.
- Audry, Sofian. *Art in the Age of Machine Learning*. MIT Press, 2021.
- Brodley, Carla E. “Challenges and Opportunities in Applied Machine Learning.” *AI Magazine*, vol. 33, no. 1, 2012, pp. 11–24.
- Domingos, Pedro. “A Few Useful Things to Know about Machine Learning.” *Communications of the ACM*, vol. 55, no. 10, 2012, pp. 78–87.
- Heaven, Douglas. “Not Like Us: Artificial Minds We Can’t Understand.” *New Scientist*, 7 Aug. 2013, www.newscientist.com/article/mg21929290-700-not-like-us-artificial-minds-we-can-t-understand.
- James, Mike. “The Triumph of Deep Learning.” *I Programmer*, 14 Dec. 2012, www.i-programmer.info/programming/article/intelligence/5206-the-triumph-of-deep-learning.html.

[programming/article/intelligence/5206-the-triumph-of-deep-learning.html](http://www.i-programmer.info/programming/article/intelligence/5206-the-triumph-of-deep-learning.html).

Marsland, Stephen. *Machine Learning: An Algorithmic Perspective*. Taylor, 2009.

Miller, Arthur I. *The Artist in the Machine: The World of AI-Powered Creativity*. MIT Press, 2019.

Mitchell, Tom M. *Machine Learning*. McGraw, 1997.

Piore, Adam. “The Quest to Build a Silicon Brain.” *Discover*, 24 May 2013, www.discovermagazine.com/mind/the-quest-to-build-a-silicon-brain.

MALWARE

ABSTRACT

Malware, or malicious software, is a form of software designed to disrupt a computer or to take advantage of computer users. Creating and distributing malware is a form of cybercrime. Criminals have frequently used malware to conduct digital extortion.

BACKGROUND

Malware is a name given to any software program or computer code that is used for malicious, criminal, or unauthorized purposes. While there are many different types of malware, all malware acts against the interests of the computer user, either by damaging the user’s computer or extorting payment from the user. Most malware is made and spread for the purposes of extortion. Other malware programs destroy or compromise a user’s data. In some cases, government defense agencies have developed and used malware. One example is the 2010 Stuxnet virus, which attacked digital systems and damaged physical equipment operated by enemy states or organizations.

The earliest forms of malware were viruses and worms. A virus is a self-replicating computer program that attaches itself to another program or file. It is transferred between computers when the infected file is sent to another computer. A worm is similar to a virus, but it can replicate itself and send



Image via iStock/Olemedia. [Used under license.]

itself to another networked computer without being attached to another file. The first viruses and worms were experimental programs created by computer hobbyists in the 1980s. As soon as they were created, computer engineers began working on the first antivirus programs to remove viruses and worms from infected computers.

Public knowledge about malware expanded rapidly in the late 1990s and early 2000s due to several well-publicized computer viruses. These included the Happy99 worm in 1999 and the ILOVEYOU worm in May 2000, the latter of which infected nearly 50 million computers within ten days. According to research from the antivirus company Symantec in 2015, more than 317 million new malware programs were created in 2014. Yet despite public awareness of malware, many large organizations are less careful than they should be. In a 2015 study of seventy major companies worldwide, Verizon reported that almost 90 percent of data breaches in 2014 exploited known vulnerabilities that were reported in 2002 but had not yet been patched.

OVERVIEW

One of the most familiar types of malware is adware. This refers to programs that create and display unwanted advertisements to users, often in pop-ups or unclosable windows. Adware may be legal or illegal, depending on how the programs are used. Some internet browsers use adware programs that analyze a user's shopping or web-browsing history in order to present targeted advertisements. A 2014 survey by Google and the University of California, Berkeley, showed that more than 5 million computers in the United States were infected by adware.

Another type of malware is known as spyware. This is a program that is installed on a user's computer to track the user's activity or provide a third party with access to the computer system. Spyware programs can also be legal. Many can be unwittingly downloaded by users who visit certain sites or attempt to download other files.

One of the more common types of malware is scareware. Scareware tries to convince users that their computer has been infected by a virus or has experienced another technical issue. Users are then

prompted to purchase “antivirus” or “computer cleaning” software to fix the problem.

Although ransomware dates back as far as 1989, it gained new popularity in the 2010s and remained of widespread concern into the 2020s. Ransomware is a type of malware that encrypts or blocks access to certain features of a computer or programs. Users with infected computers are then asked to pay a ransom to have the encryption removed.

ADDRESSING THE THREAT

Combating malware is difficult for various reasons. Launching malware attacks internationally makes it difficult for police or national security agencies to target those responsible. Cybercriminals may also use zombie computers to distribute malware. Zombie computers are computers that have been infected with a virus without the owner’s knowledge. Cybercriminals may use hundreds of zombie computers simultaneously. Investigators may therefore trace malware to a computer only to find that it is a zombie distributor and that there are no links to the program’s originator. While malware is most common on personal computers, there are a number of malware programs that can be distributed through tablets and smartphones.

Often creators of malware try to trick users into downloading their programs. Adware may appear in the form of a message from a user’s computer saying that a “driver” or other downloadable “update” is needed. In other cases, malware can be hidden in social media functions, such as the Facebook “like” buttons found on many websites. The ransomware program Locky, which appeared in February 2016, used Microsoft Word to attack users’ computers. Users would receive an email containing a document that prompted them to enable “macros” to read the document. If the user followed the instructions, the Locky program would be installed on their computer. Essentially, users infected by Locky made two mistakes. First, they downloaded a Word document

attachment from an unknown user. Then they followed a prompt to enable macros within the document—a feature that is automatically turned off in all versions of Microsoft Word. Many malware programs depend on users downloading or installing programs. Therefore, computer security experts warn that the best way to avoid contamination is to avoid opening emails, messages, and attachments from unknown or untrusted sources.

Despite efforts to educate the public about malware and implement stronger cybersecurity measures within businesses and institutions, malware remained a significant problem in the third decade of the twenty-first century. According to the statistics platform Statista, more than 5 billion malware attacks took place globally in 2022, targeting individuals as well as organizations operating within fields such as manufacturing, education, and healthcare.

—Micah L. Issitt

Further Reading

- Brandom, Russell. “Google Survey Finds More than Five Million Users Infected with Adware.” *The Verge*, 6 May 2015, www.theverge.com/2015/5/6/8557843/google-adware-survey-ad-injectors-security-malware.
- Franceschi-Bicchieri, Lorenzo. “Love Bug: The Virus That Hit 50 Million People Turns 15.” *Motherboard*, 4 May 2015, www.vice.com/en/article/d73jn/love-bug-the-virus-that-hit-50-million-people-turns-15.
- Gallagher, Sean. “‘Locky’ Crypto-Ransomware Rides in on Malicious Word Document Macro.” *Ars Technica*, 17 Feb. 2016, arstechnica.com/information-technology/2016/02/locky-crypto-ransomware-rides-in-on-malicious-word-document-macro.
- Harrison, Virginia, and Jose Pagliery. “Nearly 1 Million New Malware Threats Released Every Day.” *CNN Business*, 14 Apr. 2015, money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security.
- Petrosyan, Ani. “Malware—Statistics.” *Statista*, 31 Aug. 2023, www.statista.com/topics/8338/malware/#topic_Overview.
- Spence, Ewan. “New Android Malware Strikes at Millions of Smartphones.” *Forbes*, 4 Feb. 2015, www.forbes.com/

<sites/ewanspence/2015/02/04/android-malware-apps-deleted/?sh=f8676a1d88b4.>
“Spyware.” *Secure Purdue*, www.purdue.edu/securepurdue/forms-and-resources/spyware.php.

MARRIOTT STARWOOD HOTELS HACK

ABSTRACT

In November of 2018, Marriott International, one of the world’s largest hotel companies, announced that hackers had infiltrated its Starwood reservation database, compromising the information of guests staying at Starwood hotel properties from as far back as 2014. While initially the company estimated that 500 million guest records had been affected, after further investigation they revised this number to around 383 million in January 2019. Following an investigation, government officials pointed to Chinese hackers as the likely culprits.

BACKGROUND

Hacking, whether conducted at an individual, group, or even state-sponsored level, has been an increasing threat in the United States and around the world as societies have become more dependent upon the internet for record retention, commerce, communication, and other business and personal transactions. While the motive behind such cyberattacks have varied from efforts to steal intellectual property or personal information to simply causing damage, most companies have ramped up their cybersecurity policies and systems to protect themselves and their customers. However, incidents of hacking have persisted, with targets in the United States between 2014 and 2015 alone including JPMorgan Chase, Home Depot, Sony Pictures Entertainment, and the US Office of Personnel Management. Additionally, concerns have grown, particularly in the United States, that there have been links between the hacks and efforts by foreign governments to

acquire large amounts of American citizens’ data. In October 2018, the US Justice Department announced that charges had been brought against Chinese intelligence officers and hackers who had infiltrated the computer systems of a number of companies in the United States and abroad in an attempt to obtain sensitive aerospace information between 2010 and 2015.

In November 2018, Marriott International revealed that their Starwood database, which holds the reservation information for those who have stayed at any of the Starwood hotel properties, including St. Regis, Sheraton, and Westin, had been breached. Marriott International, one of the largest hotel companies in the world, had acquired Starwood in 2016 and had not yet merged the databases. According to analysts, upon initial investigation, the hack began in 2014 and continued until 2018, during which time as many as 500 million guest records may have been compromised. Marriott International’s November statement indicated that an internal security tool alerted company personnel about suspicious database activity in September 2018, though the breach was not disclosed until November. Among the data reportedly accessed by hackers was credit card information, mailing addresses, phone numbers, email addresses, and passport numbers. The president and chief executive officer (CEO) of Marriott International, Arne Sorenson, publicly apologized to customers of the hotel company and promised that the company would learn from the incident.

OVERVIEW

Almost immediately, the legal and financial consequences of the hack were discussed in the media. Some news reports noted that the breach may have placed Marriott in violation of the European Union data privacy law enacted in 2018 that holds companies responsible for ensuring the security of

customers' data. Within days, customers began filing lawsuits against the company. Meanwhile, several commentators and security experts criticized the length of time the infiltration went unnoticed, as well as the perceived failure of Marriott International to institute a background check comprehensive enough to detect the breach before finalizing the purchase of Starwood. According to media reports in early December, clues uncovered in the investigation pointed to Chinese hackers, suspected of being sponsored by the Chinese Ministry of State Security, being behind the breach.

Near the end of December, the US Department of Justice announced the indictment of two Chinese nationals on charges of "conspiracy to commit computer intrusions, conspiracy to commit wire fraud, and aggravated identity theft" in collaboration with

the Ministry of State Security. They were said to have attacked the computer systems of companies in at least twelve countries from around 2006 to 2018 (though the Marriott hack was not specifically mentioned in the indictment). The indictment accused Zhu Hua and Zhang Shilong, said to be members of a hacking group known as "Advanced Persistent Threat 10," of stealing hundreds of gigabytes of confidential business data.

By January 4, 2019, a new statement from Marriott provided updates regarding the ongoing investigation and analysis of the data thought to have been involved in the breach. According to the statement, expanded analysis led to the company's belief that around 383 million guest records had actually been compromised. Furthermore, about 5 million unencrypted passport numbers and



Photo via iStock/PixelsEffect. [Used under license.]

approximately 8 million encrypted payment cards had been part of the hack.

Despite the reveal in 2018 of the database hack and the lessons learned in its aftermath, Marriott remained vulnerable to data breaches in the years that followed. In 2020, the hotel chain experienced a data breach in which hackers accessed guest information for more than 5 million individuals. An additional data breach took place in 2022, when a malicious individual used social engineering techniques to access and steal information, including customer credit card details, from a computer system at a Marriott hotel in Maryland.

—Micah L. Issitt

Further Reading

- Falfe, Corin. “The Marriott Hotel Chain Has Been Hit by Another Data Breach.” *The Verge*, 6 July 2022, www.theverge.com/2022/7/6/23196805/marriott-hotels-maryland-data-breach-credit-cards.
- Lyles, Taylor. “Marriott Discloses Another Security Breach That May Impact Over 5 Million Guests.” *The Verge*, 1 Apr. 2020, www.theverge.com/2020/4/1/21203313/marriott-database-security-breach-5-million-guests.
- Mak, Aaron. “Marriott Hit by One of the Biggest Hacks in History.” *Slate*, 30 Nov. 2018, slate.com/technology/2018/11/marriott-hack-guest-personal-information.html.
- “Marriott Provides Update on Starwood Database Security Incident.” *Marriott International*, 4 Jan. 2019, news.marriott.com/2019/01/marriott-provides-update-on-starwood-database-security-incident.
- Nakashima, Ellen, and David J. Lynch. “U.S. Charges Chinese Hackers in Alleged Theft of Vast Trove of Confidential Data in 12 Countries.” *Washington Post*, 21 Dec. 2018, www.washingtonpost.com/world/national-security/us-and-more-than-a-dozen-allies-to-condemn-china-for-economic-espionage/2018/12/20/cdfd0338-0455-11e9-b5df-5d3874f1ac36_story.html.
- Nakashima, Ellen, and Craig Timberg. “U.S. Investigators Point to China in Marriott Hack Affecting 500 Million Guests.” *Washington Post*, 11 Dec. 2018, www.washingtonpost.com/technology/2018/12/12/us-investigators-point-china-marriott-hack-affecting-million-travelers.

METADATA

ABSTRACT

Metadata is descriptive, structural, or administrative information included as part of a digital file, electronic record, or other resource. It often includes information such as the file or resource’s title, creator, and structure. Metadata is used to catalog and preserve information. By including keywords and descriptions within the metadata, creators or archivists enable users to search for specific records as well as discover similar ones. Metadata is related to the fields of both computer science and library science, as it combines traditional cataloging methods with new electronic file types and distribution methods.

BACKGROUND

Often described as “data about data,” metadata consists of information either embedded in a digital file or stored as a separate record in a database or similar directory. The concept is closely related to the cataloging systems used for centuries in libraries and archives, which typically consist of collections of listings—either physical or, following the advent of computers, digital—that include the title, the creator, and a description of each work or artifact, among other key facts. Metadata is intended to assist people in searching for and retrieving the files or information they seek. Similarly, this data enables archivists and catalogers to ensure that information will be well organized and preserved for future reference.

OVERVIEW

Metadata is an evolving concept, and the term has consequently been used in various ways by different organizations and in different fields. Considered broadly, metadata can be divided into three areas based on the type of information being preserved. Information such as the title and author of an e-book falls under the classification of descriptive

metadata, while data regarding the structure of the e-book—the order of the pages and chapters—is considered structural metadata. Administrative metadata is somewhat more loosely defined but generally includes information regarding when the file was created. This category may also include the sub-categories of technical metadata, which concerns file formats and sizes; preservation metadata, which can include information about the file’s relationships to other files; and intellectual property rights metadata, which is used to capture copyright information. In other cases, technical, preservation, and intellectual property rights metadata are considered distinct categories.

When an item exists in only physical form, as in the case of physical artifacts and texts that have not been digitized, the metadata for that item is typically stored in a searchable database. When dealing with electronic files and other resources, however, creators and catalogers often embed metadata within the files. In hypertext markup language (HTML) files such websites, metadata is typically embedded in the files through the use of specialized HTML tags. Image, audio, and video files can likewise include embedded metadata, usually added by the creator or, in the case of commercially distributed films or music, the studio or distributor. Some cameras, including many smartphone cameras, automatically embed metadata such as the date, time, and place a photograph was taken in each file they produce. This capability has led to concerns that sensitive personal information could be distributed in the form of metadata without an individual’s knowledge or permission, and the use of metadata thus remains a topic of debate among individuals and institutions concerned about privacy.

In 2013, National Security Agency (NSA) contractor Edward Snowden revealed that the agency was collecting, analyzing, and storing bulk telephone and online metadata from US citizens and others under the auspices of the USA PATRIOT Act

(2001). Though the agency argued that the practice was necessary to detect and fight terrorism, the US Court of Appeals ruled that such bulk data collection and retention was illegal in May 2015. In June 2015 President Barack Obama signed the USA Freedom Act, which put new restrictions on the NSA surveillance of phone metadata. The issue of the US government’s access to metadata remained a contentious one in the years that followed, particularly in light of the fact that government agencies did not need to obtain a warrant in order to access some metadata stored in remote cloud storage.

—Joy Crelin

Further Reading

- Baca, Murtha, editor. *Introduction to Metadata*. 3rd ed., Getty Research Institute, 2016.
- Cox, Mike, Ellen Mulder, and Linda Tadic. *Descriptive Metadata for Television*. Focal, 2006.
- García-Barriocanal, Elena, et al., editors. *Metadata and Semantic Research*. Springer, 2011.
- Hider, Philip. *Information Resource Description: Creating and Managing Metadata*. American Library Association, 2012.
- Horodyski, John. *Metadata Matters*. CRC Press, 2022.
- Lima, Cristiano. “Want Our Metadata? Get a Warrant, Rep. Ted Lieu Says.” *Washington Post*, 20 Apr. 2022, www.washingtonpost.com/politics/2022/04/20/want-our-metadata-get-warrant-rep-ted-lieu-says.
- Miller, Steven Jack. *Metadata for Digital Collections*. 2nd ed., ALA Neal-Schuman, 2022.
- National Information Standards Organization. *Understanding Metadata*. NISO Press, 2004.
- Park, Jung-ran. *Metadata Best Practices and Guidelines*. Routledge, 2011.
- Roberts, Dan, and Spencer Ackerman. “NSA Mass Phone Surveillance Revealed by Edward Snowden Ruled Illegal.” *The Guardian*, 7 May 2015, www.theguardian.com/us-news/2015/may/07/nsa-phone-records-program-illegal-court.
- Smiraglia, Richard P., editor. *Metadata: A Cataloger’s Primer*. Routledge, 2012.
- Steinhauer, Jennifer, and Jonathan Weisman. “U.S. Surveillance in Place since 9/11 Is Sharply Limited.” *New York Times*, 2 June 2015, www.nytimes.com/2015/06/03/us/politics/senate-surveillance-bill-passes-hurdle-but-showdown-looms.html.

MICHELANGELO COMPUTER VIRUS

ABSTRACT

The Michelangelo computer virus was a destructive piece of computer code designed to make a person's computer unusable and trigger on March 6 of a given year. The virus was hyped by the media to proportions that far exceeded its actual distribution and caused panic among computer users. The incident also damaged the credibility of many of the industry experts.

BACKGROUND

The Michelangelo computer virus was first discovered in 1991. It overwrote the boot sector of a computer's hard drive running an operating system based on disk operating system (DOS) as well as floppy disks inserted into an infected machine. The boot sector contains the information that a computer needs to start. This virus would have made the computer unusable and the data irretrievable for the average user. The name is derived from the virus's activation date of March 6, the birthday of Italian Renaissance artist Michelangelo.

Leading Edge, a major computer manufacturer at the time, inadvertently shipped five hundred computers infected with the virus in January of 1992. This prompted the manufacturer to start shipping all new computers with antivirus software preinstalled. A computer virus expert wrongly called the Michelangelo virus the third most commonly distributed virus after the announcement. Soon after, about nine hundred infected floppy disks were shipped by another vendor in the computer industry. The two incidents brought the virus to the forefront of media attention. The infection numbers were further inflated to 5 million possible computers worldwide by the antivirus industry, and the media also reported, incorrectly, that the virus could be spread through computer bulletin boards.

OVERVIEW

A few reporters and industry experts remained skeptical about the claims of millions of infected computers, but by the end of February 1992, the media had fueled the public's fears and the experts were largely ignored. The antivirus industry added to the furor by offering free detectors that could be downloaded. Symantec, another industry leader, placed a full-page ad in *Computerworld* in order to take advantage of the media attention. The days leading up to the virus activation date saw the virus receiving constant media reports, including speculation that damages could be in the millions. March 6, 1992, brought a mere ten to twenty thousand cases of reported data loss. The low rates of infection were touted as a success by the antivirus industry and media coverage. Analysts, however, saw nowhere near the initial reported rates of infection. The virus dropped from the headlines by the following day. The first report about the virus surfaced a full two weeks after the virus release date and criticized the industry and the media for the whole incident.

The media hype and poor reporting about the Michelangelo virus caused a panic among computer users. Antivirus experts inflated claims of infection and companies that produced antivirus programs took advantage of the hysteria to sell their products. The poor handling of the reporting damaged the reputation of computer-virus experts for some time to come, and the media lost a measure of credibility.

—James J. Heiney

Further Reading

- Caldwell, Wilma R., editor. *Computer Security Sourcebook*. Omnigraphics, 2003.
- Erbschloe, Michael. *Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code*. Elsevier Butterworth Heinemann, 2005.
- Furnell, Steven. *Cybercrime: Vandalizing the Information Society*. Addison-Wesley, 2002.
- Stewart, Andrew J. *A Vulnerable System: The History of Information Security in the Computer Age*. Cornell UP, 2021.

MICROPROCESSOR

ABSTRACT

Microprocessors are one of the critical components of the personal computer. They process all of the information entered into the computer through input devices, including mice, keyboards, cameras, and microphones. A more powerful microprocessor allows a computer to process more information at once. Microprocessors have become increasingly powerful over the years. Smaller, more powerful microprocessors allow devices such as smartphones to exist.

BACKGROUND

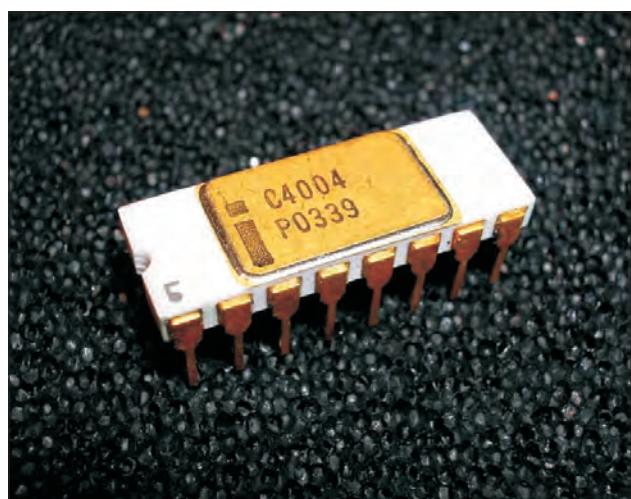
Computers were not always a big business. In the era before personal computers, building and maintaining computers was done by rare hobbyists. At this time, computers required specialized knowledge to build. They were usually ordered in kits, which had to be assembled by a skilled technician. Computer owners would have to solder their own computer components into place and write their own code. Because of these limitations, computers appealed to a very limited market. For this reason, they were not mass produced.

Employees at major technology firms such as Intel and Hewlett-Packard urged their employers to enter the personal computer market. Both companies began manufacturing various computer chips, including different types of memory and processors. At the time, computer processors were large, inefficient, and composed of several separate devices.

In 1969, a small technology firm approached Intel with a simplified computer design. Their computer would have only four chips: a chip for input and output devices, a read-only memory (ROM) chip, a random-access memory (RAM) chip, and a general processor chip. The general processor chip would handle sorting information between the other parts. Intel bought the rights to one of these chips, the 4004, in 1970 and began commercial production the following year. While the 4004 was designed to

serve as a tiny central processing unit for digital calculators, engineers at Intel believed it could be applied to many of their devices. Under Intel, the 4004 became the first commercially marketed microprocessor.

Intel continued to improve their chips, dominating the fledgling microprocessor market. Their 8008 processor chip helped grow the computer-building hobbyist movement and was used in the famous Altair 8800 computer build. The Altair 8800 was the first machine to use the BASIC programming language. BASIC was the first programming language written specifically for use on personal computers. This led to the development of the Intel 8080 chip, which was used on some of the first popular personal computers. Eventually, chip manufacturers developed even more powerful chips. This began in 1978 with Intel's 16-bit microprocessors. These were followed by 32-bit microprocessors in the 1980s, which slowly gained market share until the 1990s. That decade, 32-bit microprocessors were replaced by 64-bit microprocessors, which first became available in 1992. Over the following decades, increasingly powerful 64-bit microprocessors became the industry standard.



Intel 4004, released by Intel Corporation in 1971. It was the first commercially produced microprocessor, and the first in a long line of Intel CPUs. Photo via Wikimedia Commons. [Public domain.]

OVERVIEW

Modern microprocessors are used in a variety of devices. They are found in personal computers, smartphones, microwaves, dishwashers, refrigerators, digital video disk (DVD) and Blu-ray players, televisions, alarm systems, electric toothbrushes, and washing machines. They also may be found in any other electronic device that uses a small computer for basic operations.

The most recent generations of microprocessors have a variety of advantages over older models. Despite being exponentially more powerful, modern microprocessors are small, low-profile, and easy for computer engineers to utilize in a variety of hardware setups. They are cheap to manufacture, even though the process of doing so is extremely complex and delicate. Finished, tested products are very reliable and should not fail for many years. Lastly, microprocessors require very little electrical power to operate, making them energy efficient.

The microprocessor manages all data that enters a device. It then sorts the data through the appropriate parts. For example, any information typed on a keyboard first would enter the microprocessor. The microprocessor then would know to send that information to the video card, showing it on the computer's screen, and to one of the computer's memory units. The microprocessor usually has to communicate with every chip in the device, and it is one of the core parts of the modern personal computer. Other central parts include RAM, hard drives or flash drives, the motherboard, and the power supply.

PARTS OF A MICROPROCESSOR

All microprocessors can be divided into six parts: the arithmetic and logic unit (ALU), the registers, the control unit, the instruction register, the program counter, and the bus. The ALU is the part of the microprocessor that performs all of the

mathematical calculations necessary for the device to function. Higher-bit processors can perform more calculations at once. Most computer functions are broken down into mathematical functions and are processed here. The registers are the internal storage device of the microprocessor. Any data that the microprocessor needs to temporarily store is stored in this part. The control unit sorts all data entering and leaving the microprocessor, directing it to the appropriate parts. The instruction register is a separate temporary memory storage device used only for storing task instructions. It makes sure the microprocessor remembers how to perform all of its necessary operations. The program counter temporarily stores the address of the next instruction to be executed. Lastly, the bus is a set of connective cables that allows all of the microprocessor parts to communicate with one another.

—Tyler Biscontini

Further Reading

- Campbell-Kelly, Martin, William F. Aspray, Jeffrey R. Yost, Honghong Tinn, and Gerardo Con Díaz. *Computer: A History of the Information Machine*. 4th ed., Routledge, 2023.
- “A Computer in Your Pocket: The Rise of Smartphones.” *Science Museum*, 13 Nov. 2018, www.sciencemuseum.org.uk/objects-and-stories/computer-your-pocket-rise-smartphones.
- Gordon, Whitson. “How to Build a Computer, Lesson 1: Hardware Basics.” *Lifehacker*, 1 Aug. 2011, lifehacker.com/5826509/how-to-build-a-computer-from-scratch-lesson-1-hardware-basics.
- “Intel’s First Microprocessor: Its Invention, Introduction, and Lasting Influence.” *Intel*, www.intel.com/content/www/us/en/history/museum-story-of-intel-4004.html.
- O’Leary, Timothy, Linda O’Leary, and Daniel O’Leary. *Computing Essentials 2023*. McGraw-Hill, 2022.
- Singer, Graham. “The History of the Microprocessor and the Personal Computer.” *TechSpot*, 1 Oct. 2020, www.techspot.com/article/874-history-of-the-personal-computer.

MOBILE APPS

ABSTRACT

Mobile applications usually perform a specific task, such as reporting the weather forecast, or displaying maps for navigation. These applications, or apps, are programs designed to run on smartphones, tablets, and other mobile devices. Mobile devices have special requirements because of their small screens and limited input options. Furthermore, a touch screen is the primary means of entering information into a mobile device. Programmers need special knowledge to understand the mobile platform for which they wish to create apps.

BACKGROUND

Mobile applications, or apps, are computer programs designed specifically to run on smartphones, tablets, and other mobile devices. Apps must be designed for a specific platform. A mobile platform is the hardware and system software on which a mobile device operates. Some of the most widely used mobile platforms include Google's Android and Apple's iOS. Mobile devices support a variety of software. At the most basic level, a platform's system software includes its operating system (OS). The OS supports all other programs that run on that device, including apps. In addition to the OS, smartphones and tablets come with a variety of preinstalled utility programs, or utilities, that manage basic functions. Examples of utilities include a clock and a calendar, photo storage, security programs, and clipboard managers. While utilities are not essential to the functionality of the OS, they perform key tasks that support other programs.

However, the real power of mobile devices has come from the huge assortment of mobile apps they can run. The app stores for various mobile devices contain hundreds of thousands of different apps to download. Each app has been designed with different user needs in mind. Many are games of one sort or another. There are also vast numbers of apps for

every pursuit imaginable, including video chat, navigation, social networking, file sharing and storage, and banking.

Developers of mobile apps use various approaches to design their software. In some cases, an app is little more than a mobile website that has been optimized for use with small touch screens. Other mobile apps are developed specifically for the mobile devices they run on. Programmers must program their apps for a specific mobile platform. App developers usually use a special software development kit and an emulator for testing the app on a virtual version of a mobile device. Emulators provide a way of easily testing mobile apps. Emulators generate detailed output as the app runs, so the developer can use this data to diagnose problems with the app.

OVERVIEW

Mobile apps have evolved into a multibillion-dollar business. Before the advent of mobile devices, software was developed for use on personal computers, and a software package often sold for hundreds of dollars. The mobile app marketplace has adopted a very different model. Instead of creating apps that cost a large amount of money and try to provide a wide range of functions, the goal is to create an app that does one thing well and to charge a small amount of money. Many apps are free to download, and paid apps are typically priced anywhere from ninety-nine cents to a few dollars. Despite such low price points, developers of successful apps can still earn large sums of money. This is in part due to the large numbers of smartphone and tablet users.

Mobile apps also have a low cost of distribution. In the past, software was sold on physical media such as floppy disks or CD-ROMs. These had to be packaged and shipped to retailers at the software developer's expense. With mobile apps, there are no such overhead costs because apps are stored online by the platform's app store and then downloaded by users.



Photo via iStock/hapabapa. [Used under license.]

Aside from the time and effort of developing an app, the only other financial cost to the developer is an annual registration fee to the platform's app store and a percentage of revenue claimed by the platform. App stores typically vet apps to make sure they do not contain malware, violate intellectual property, or make false advertising claims. App developers can earn revenue from the download fee, in-app advertisements, and in-app purchases, the latter of which are particularly common in mobile games.

MOBILE APPS AND SOCIAL CHANGE

Mobile apps can do much more than entertain and distract. For example, X (previously known as Twitter) is a microblogging app that allows users to post short messages and read updates from others. Twitter played a significant role in social movements such as the Arab Spring of 2011 and the Black Lives

Matter protests of 2020 and likewise served as a means of disseminating information—and misinformation—during the COVID-19 pandemic. Because it relies on telecommunications technology that continues to function even when there are disruptions in other media, the X/Twitter app has allowed people to communicate even during major disasters and political upheavals. Other apps allow users to report and pinpoint environmental damage or potholes for government agencies to fix.

PLATFORM LOCK

Mobile apps must be designed for a particular mobile platform. Sometimes, a developer will make a version of an app for each major platform. In other cases, however, developers only create an app to run on a single platform. This leaves users of other mobile platforms unable to use the app. In the

case of popular apps, this can cause frustration among those who want to be able to use whatever apps they want on their platform of choice.

—Scott Zimmer

Further Reading

- Banga, Cameron, and Josh Weinhold. *Essential Mobile Interaction Design: Perfecting Interface Design in Mobile Apps*. Addison-Wesley, 2014.
- Glaser, J. D. *Secure Development for Mobile Apps: How to Design and Code Secure Mobile Applications with PHP and JavaScript*. CRC Press, 2015.
- Goggin, Gerard. *Apps: From Mobile Phones to Digital Lives*. Wiley, 2021.
- Heckman, Rocky. *Designing Platform Independent Mobile Apps and Services*. Wiley-IEEE Computer Society Press, 2016.
- Knott, Daniel. *Hands-On Mobile App Testing*. Pearson Education, 2015.
- Miller, Charles, and Aaron Doering. *The New Landscape of Mobile Learning: Redesigning Education in an App-Based World*. Routledge, 2014.
- “Mobile Application Security.” US Department of Homeland Security Science and Technology, 12 Jan. 2023, www.dhs.gov/science-and-technology/cybersecurity-mobile-app-security.
- Platz, Cheryl. *Design Beyond Devices: Creating Multimodal, Cross-Device Experiences*. Rosenfeld Media, 2020.
- Whitaker, Rob. *Developing Inclusive Mobile Apps*. Apress, 2020.

MOBILE WEB TECHNOLOGY

ABSTRACT

The mobile web refers to the use of the internet through handheld mobile devices such as smartphones and tablets. Thanks to increasingly sophisticated technology, these small devices now boast more computing power than National Aeronautics and Space Administration’s (NASA’s) original mainframes. Although challenges remain for both users and developers of mobile web technology, it allows for much the same online access as desktop or laptop computers, and its use is expected only to grow.

BACKGROUND

Mobile technology has come a long way since 1973, when Motorola engineer Martin Cooper became the first person to make a call on a portable device—one that weighed more than two pounds, cost \$4,000, and took ten hours to charge for just thirty-five minutes of power. Mobile communications devices are, by definition, small enough to be mobile. Screen size can be an issue, particularly for older people with declining vision. Their small size also has ramifications for those with less dexterity, who may find it difficult to manipulate keyboards and pointing devices. Technologists must therefore take those factors into consideration when designing mobile interfaces, keeping in mind that mobile users expect the same quality experience as that available on desktop or laptop devices but operate in a much different context.

As mobile devices became increasingly ubiquitous, the World Wide Web Consortium (W3C) created a set of universal standards for mobile web access and developed web technologies that consider the challenges associated with mobile devices, thus allowing designers to create pages that look good on both handheld and larger devices. These tools include CSS Mobile and XHTML Mobile, versions of the cascading style sheets (CSS) language and extensible hypertext markup language (XHTML) optimized for mobile use.

Besides screen size, speed poses a major issue for mobile users, many of whom have experienced the frustratingly slow download of a movie, game, or other such content. Following the commercial introduction of fifth-generation (5G) mobile service in 2019, however, latency (the time it takes for information to travel from the browser to the server) was vastly reduced.

OVERVIEW

Developers must decide whether a mobile app or mobile-optimized website best meets their needs.

Although any website can be viewed with a mobile browser, unoptimized sites can be uncomfortable or unreadable for the user. Websites optimized for mobile devices, on the other hand, have readable fonts, images that scale well on a small screen, and a vertical layout.

Just like traditional websites, mobile sites consist of browser-based hypertext markup language (HTML) pages linked together and display text, data, images, and video. They can also access mobile-specific features, including one-button click-to-call and location-based mapping. So-called responsive sites, which are designed to be compatible with different platforms and adjust to different screen sizes and layouts, are also common.

Mobile apps, by contrast, are installed on a user's mobile device and can download content so that it can be accessed without an internet connection. A mobile app is often an attractive choice for a company seeking to build brand loyalty, as it serves as an ever-present extension of a company's website and allows a consumer to set up preferences and customize their experience. Mobile apps can also seamlessly interface with devices' cameras, global positioning system (GPS) functions, and other features.

While they have limited access to a device's features and require an internet connection to run, optimized mobile websites have their own benefits, including broader reach (since unlike an app, a website does not have to be located in and downloaded from an app store) and cost efficiency. Mobile websites may also offer greater visibility in search engine results.

USABILITY IS KEY

Whether a designer chooses to build a mobile app or mobile website, overall usability is central, along with availability and accessibility. Mobile sites must be hosted on reliable servers with good uptime to



Image via iStock/exdez. [Used under license.]

ensure that users do not receive an error message while trying to load them, and designers should regularly check for and eliminate dead links. Both mobile sites and apps should contain clear, easy-to-explore, relevant content, formatted within a sensible information architecture. Intuitive interfaces that do not require instructions or repeated trial and error to figure out are also imperative.

—Mari Rich

Further Reading

- Abraham, Nikhil. "Building Mobile Web Apps." *Dummies*, 26 Mar. 2016, www.dummies.com/programming/building-mobile-web-apps.
- Goggin, Gerard. *Apps: From Mobile Phones to Digital Lives*. Wiley, 2021.
- "Mobile Application Security." *US Department of Homeland Security Science and Technology*, 12 Jan. 2023, www.dhs.gov/science-and-technology/cybersecurity-mobile-app-security.
- Moscaritolo, Angela. "5G Will Save You Almost 24 Hours of Download Time Per Month." *PCMag*, 16 Oct. 2018, www.pc当地.com/news/5g-will-save-you-almost-24-hours-of-download-time-per-month.
- O'Leary, Timothy, Linda O'Leary, and Daniel O'Leary. *Computing Essentials 2023*. McGraw-Hill, 2022.
- "Principles for Useable Design." *Usability Body of Knowledge*, www.usabilitybok.org/principles-for-useable-design.
- Rouse, Margaret. "Mobile Web." *Techopedia*, 4 Apr. 2017, www.techopedia.com/definition/23588/mobile-web.
- "Web Standards." *W3C*, 2023, www.w3.org/standards.

N

NETWORK AND COMPUTER SYSTEMS ADMINISTRATOR

ABSTRACT

Network and computer systems administrators design, build, and maintain computer systems. They work closely with computer security professionals to ensure the security of the computer networks and systems under their purview. Students aspiring to enter the profession should pursue studies in subjects such as computer science and networking.

BACKGROUND

Network and computer systems administrators build, design, and maintain computer systems for businesses and organizations. In addition to constructing local area networks (LANs) and wide area networks (WANs), systems administrators also support and maintain organizational internet systems and related infrastructure. Any computer problems or computer-related questions posed by employees of a company are traditionally handled by system administrators or their staff.

Network and computer systems administrators work closely with computer security professionals and other senior administrative staff to ensure that the computing needs of a business or organization are in place and are functioning properly. They also assist fellow employees with computer-related projects and routine maintenance.

OVERVIEW

Network and computer systems administrators work predominantly in business, administrative, and office settings. They are employed by large

companies and often have their own workspaces adjacent to facilities that house computer servers and other hardware relevant to network systems. Network and computer systems administrators are often required to strike a balance between work conducted on their own and collaborative work with other staff members, which can include system maintenance, demonstrations of hardware and software capabilities, or developing and implementing new technologies with fellow staff.

The field of computer administration traditionally attracts professionals with technological skills who have a lengthy history of involvement with and demonstrated passion for computing, be it through academic study, personal interest, or professional development. Most network and computer systems administrators develop an interest in working with and around computers at a young age and are intricately familiar with modern developments in personal and business computing. They may also enter the discipline through previous exposure to programming, software development, or any one of numerous disciplines related to computer science.

DUTIES AND RESPONSIBILITIES

Network and computer systems administrators divide their time between monitoring and maintaining existing computer systems, devising new computer and network technologies with other staff, and assisting different departments and fellow employees with their computing and networking needs through maintenance, troubleshooting, and conducting training seminars.

Network and computer system administrators are traditionally the primary individuals

responsible for the configuration and maintenance of network email systems. In addition to monitoring archival systems and implementing virus prevention programs, they are also called upon to set up network and mobile email accounts for new employees or vendors.

In addition to email systems, network and computer system administrators also maintain computer systems related to inventories, financial records, meeting logs, and other relevant data. They build, maintain, and monitor backup systems for archival data. They often work in concert with organizational computer security specialists to ensure that data can be recovered in the event of an unforeseen system failure.

Network and computer system administrators also spend a great deal of time troubleshooting and installing new programs on network computers, making updates to employee machines so productivity is not interrupted, or routing out any viruses or system malfunctions that are preventing them from accessing projects. They are traditionally in charge of the master computer and network systems from which all company computers are connected. They may be called upon to supervise access to particular network locations.

Computer security specialists plan, coordinate, and implement their organization's information security program.

WORK ENVIRONMENT

Physical environment. Network and computer systems administrators work primarily in computer labs and office settings. They balance a workload that is performed at their own individual workstation and the workstations of other employees.

Network and computer systems administrators work in nearly every type of industry and organization, including local, state, and federal governments; construction; medical research; publishing; education; and media.

Human environment. Systems administration requires patience, collaboration, and explanatory skills. Network and computer systems administrators normally interact with colleagues across various departments on a daily basis, including engineers, technicians, managers, directors, and executive staff.

Technological environment. Network and computer systems administrators must be well versed in the entire gamut of contemporary computer systems technologies, ranging from circuitry, processors, and programming languages, and all computer hardware and software relevant to their industry of expertise, including applications and database platforms.

EDUCATION AND TRAINING

High school/secondary. High school students can best prepare for a career in network and computer systems administration by completing coursework in algebra, calculus, geometry, trigonometry, introductory computer science, and programming. Specialized seminars or advanced placement coursework related to computer topics are also recommended.

Many high school students supplement their course load by participating in volunteer programs and summer internships in which they can work directly with system administration fundamentals and its importance in the professional world.

College/postsecondary. Systems administration has evolved from a niche field to an academic and professional specialty widely studied across postsecondary institutions in the United States. Requirements for specific academic training in the field often vary from position to position and industry to industry, though a bachelor's degree in a related field is commonplace for most entry-level positions. Several certificate-level and undergraduate programs are available nationwide.

While graduate programs specifically related to systems administration are rare, applicants with master's-level accreditation in fields such as programming, computer science, and networking are

often prime candidates for senior management positions related to network and systems administration in major companies, research institutes, and universities. Basic bachelor's degree coursework in systems administration programs includes topics such as system administration, network infrastructures, UNIX, business telecommunications, and information security.

Adult job seekers. Network and computer systems administrators are often employed by businesses and organizations of all sizes and scopes. Senior-level positions at large organizations and companies are usually the domain of professionals with extensive academic and professional experience in computing. However, adult job seekers interested in a career change to the field can, with requisite training, acquire the skills necessary to become eligible for systems administrator positions at smaller organizations. Network and computer systems administrators traditionally work regular business hours.

Professional certification and licensure. The number of available and required certifications for network

and computer systems administrators is complex and varied. Examples include Microsoft Certified Professional certification and Linux certification.

Additional requirements. Network and computer systems administrators must possess a constant desire to stay up to date with emerging developments in digital technology, networking, and database systems. Organizations rely on network and computer systems administrators to help their firms stay in tune with the technologies that can expand their production and profitability.

—John Pritchard

Further Reading

Campbell-Kelly, Martin, William F. Aspray, Jeffrey R. Yost, Honghong Tinn, and Gerardo Con Díaz.

Computer: A History of the Information Machine. 4th ed., Routledge, 2023.

Kizza, Joseph Migga. *Guide to Computer Network Security.* 6th ed., Springer, 2024.

Stewart, Andrew J. *A Vulnerable System: The History of Information Security in the Computer Age.* Cornell UP, 2021.

O

ONLINE PIRACY

ABSTRACT

Online piracy refers to the unauthorized downloading, viewing, copying, or distribution of copyrighted digital content. Targeted content includes films, television, music, games, and books. Piracy of this content has become so commonplace that some people consider it a right instead of a crime. The significant financial impact of online piracy on copyright holders has become the concern of individuals, businesses, and the US Congress, while advocates for internet freedom of speech are just as concerned about remedies that might unduly restrict online expression and legitimate use of content.

BACKGROUND

While the use of the term “piracy” in reference to intellectual property has a long history, it only entered widespread use with the advent of the internet, especially when compact disc (CD) burners made copying and distributing music, software, and other material from the internet as easy as a few clicks. The most commonly pirated content includes music, films, television shows, e-books, and software. Digital music files, typically in MP3 format, were one of the first types of files to be extensively copied, due to the development of several file-sharing programs in the 1990s that made it easy to transfer such files both legally and illegally.

Internet pirates have turned illegal copying and sharing of intellectual property into thriving businesses, with numerous websites specializing in hosting pirated files for download. One popular site was megaupload.com, hosted by the Hong Kong-based company Megaupload Limited. In 2012, the US

Department of Justice shut down the company’s sites and indicted its owners for allegedly operating an organization based on copyright infringement, and Hong Kong’s Customs and Excise Department froze the company’s \$42 million worth of assets.

As quickly as authorities shut down pirating services, others just as quickly spring up to take their place. According to a report by Digimarc, a company that provides antipiracy technology for publishers and authors, in the first month after Megaupload shut down, two other sites, Putlocker and Rapidshare, raised the total of pirated books to 13 percent. In another piracy report, brand-protection firm NetNames reported that in Europe and North America, the peer-to-peer file-sharing protocol BitTorrent is the most popular method of downloading pirated material, while in the Asia-Pacific region, pirates prefer direct-download websites.

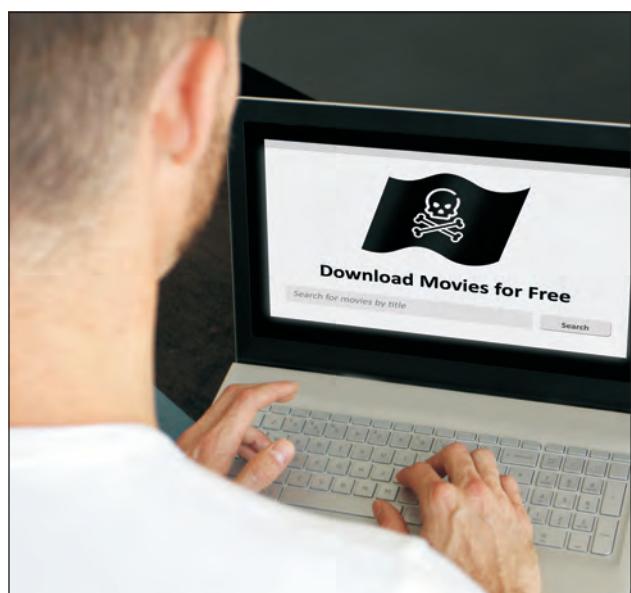


Photo via iStock/glegorly. [Used under license.]

Software piracy has also continued to advance as technology has improved. The main types of software piracy include “softlifting,” in which users share their software with other, unauthorized users; uploading and downloading; software counterfeiting; original equipment manufacturer (OEM) unbundling, in which OEM software is separated from the hardware it was originally sold with and distributed independently; and hard disk loading, in which unauthorized software is preinstalled on hardware before it is sold.

OVERVIEW

According to a 2011 study by Envisional, a subsidiary of NetNames, digital piracy of music, movies, and other copyrighted material accounted for 23.76 percent of internet bandwidth worldwide and 17.53 percent of bandwidth in the United States. Commenting on the study, Republican senator Orrin Hatch of Utah, cochair of the International Anti- Piracy Caucus, argued that online piracy hijacks the earnings of artists and creators of movies, television, and music, which discourages reinvestment in new job-creating projects and thus weakens the American economy.

Internet book piracy affects millions of writers and publishers whose books have been scanned or their digital files copied and uploaded to websites that feature pirated works, sometimes alongside legitimate uploads. A study published in January 2010 by Attributor, which was later acquired by Digimarc, found that writers and publishers had lost an estimated \$2.8 billion to date because of internet piracy, assuming that each illegal download represented a lost sale.

Internet theft of music is a constant challenge. The volume of pirated music and the drop in music industry revenues is significant, with rising digital sales not closing the gap. The Recording Industry Association of America (RIAA) reported that a decade after Napster introduced its file-sharing site in 1999, music sales in the United States dropped

from \$14.6 billion to \$7.7 billion. In 2003, with the launch of the Apple iTunes Store, steady options for legal digital music downloads became available.

The Motion Picture Association of America (MPAA) reported that in 2005, the major US motion-picture studios lost \$6.1 billion worldwide to internet piracy, and the worldwide motion-picture industry, including foreign and domestic producers, distributors, theaters, video stores, and pay-per-view operations, lost \$18.2 billion. With these statistics in mind, the entertainment industry has countered internet piracy of music, television, and movies with more legal options. As broadband speeds have increased, so too have the opportunities to legally watch television shows and movies or listen to music online. Popular legal streaming services include Netflix, Hulu, Amazon Prime Video, Disney+, AppleTV+, Apple Music, Amazon Music, Spotify, and Pandora, among others.

In 2013, major internet service providers and the entertainment industry announced a partnership to attempt to curb piracy of copyrighted material online. Under the Copyright Alert System (CAS) or “six strikes” system, internet subscribers accused of online piracy received a series of alerts each time they were found pirating material. The sixth copyright violation potentially resulted in the user being punished by the internet provider. Subscribers who illegally shared movies or songs could be punished by losing their internet access or having the speed of their broadband downloads reduced to a crawl. After several years of operation, however, the system was deemed unsuccessful, and the CAS initiative came to an end in early 2017.

Responding to an outcry from internet users and technology companies including Google, Congress defeated the Stop Online Piracy Act (SOPA) and the PROTECT IP Act (PIPA) in 2012. SOPA and PIPA would have imposed strict penalties on websites carrying copyright-violating material, which Google and other critics claimed would curtail free speech.

Reputable companies who advertise on the internet have also been pulled into the online piracy problem. Because most internet ad placement is generated automatically through algorithms, companies cannot always control where their ads are placed. Often these ads appear on sites that offer illegal downloads of music and films. A 2015 report issued by Digital Citizens alliance and MediaLink, a consulting firm, found that “theft” websites earned more than \$200 million from advertising placed on their pages in 2014. This phenomenon has been termed “ad fraud” and is an effect of online piracy, illustrating the ubiquity of the problem.

As the internet has continued to grow more technologically sophisticated, online piracy has kept pace. A study funded by the UK government and released by the Intellectual Property Office found that during January 2021, the overall level of infringement for all content categories (excluding digital visual images) was at 23 percent. While the unauthorized downloading of files remained popular, the use of illegal streaming sites made up a substantial portion of all online piracy during the early 2020s.

—Kathy Warnes

Further Reading

- Fisk, Nathan W. *Understanding Online Piracy: The Truth about Illegal File Sharing*. ABC-CLIO, 2009.
- Gordon, Sherri Mabry. *Downloading Copyrighted Stuff from the Internet: Stealing or Fair Use?* Enslow, 2005.
- Hamedy, Saba. “Report: Online Piracy Remains Multi-Hundred-Million-Dollar Business.” *Los Angeles Times*, 19 May 2015, www.latimes.com/entertainment/envelope/cotown/la-et-ct-report-online-piracy-digital-citizens-alliance-medialink-20150518-story.html.
- Hinduja, Sameer. *Music Piracy and Crime Theory*. LFB, 2005.
- Husak, Douglas. *Overcriminalization: The Limits of the Criminal Law*. Oxford UP, 2008.
- Johns, Adrian. *Piracy: The Intellectual Property Wars from Gutenberg to Gates*. U of Chicago P, 2009.

- Kastrenakes, Jacob. “Six Strikes’ Anti-Piracy Initiative Ends after Failing to Scare Off ‘Hardcore’ Pirates.” *The Verge*, 30 Jan. 2017, www.theverge.com/2017/1/30/14445596/six-strikes-piracy-system-failed-ending.
- Murray, Brian H. *Defending the Brand: Aggressive Strategies for Protecting Your Brand in the Online Arena*. AMACOM, 2004.
- Nhan, Johnny. *Policing Cyberspace: A Structural and Cultural Analysis*. LFB, 2010.
- “Research and Analysis: Online Copyright Infringement Tracker Survey (10th Wave) Executive Summary.” *Intellectual Property Office*, gov.uk/government/publications/online-copyright-infringement-tracker-survey-10th-wave/online-copyright-infringement-tracker-survey-10th-wave-executive-summary.
- Riley, Gail Blasser. *Internet Piracy*. Cavendish, 2010.
- Torr, James D. *Internet Piracy*. Greenhaven, 2004.

OPERATING SYSTEM

ABSTRACT

The operating system (OS) is the broker between software applications and a computer’s hardware. After being loaded into a computer, usually by the manufacturer via a boot program, the OS manages the myriad programs running on the device. The most common computer OS is Microsoft Windows, while Apple’s macOS also holds a noteworthy share of the OS market. Many devices, from personal computers to electronic readers and smartphones, require an OS to process data and commands.

BACKGROUND

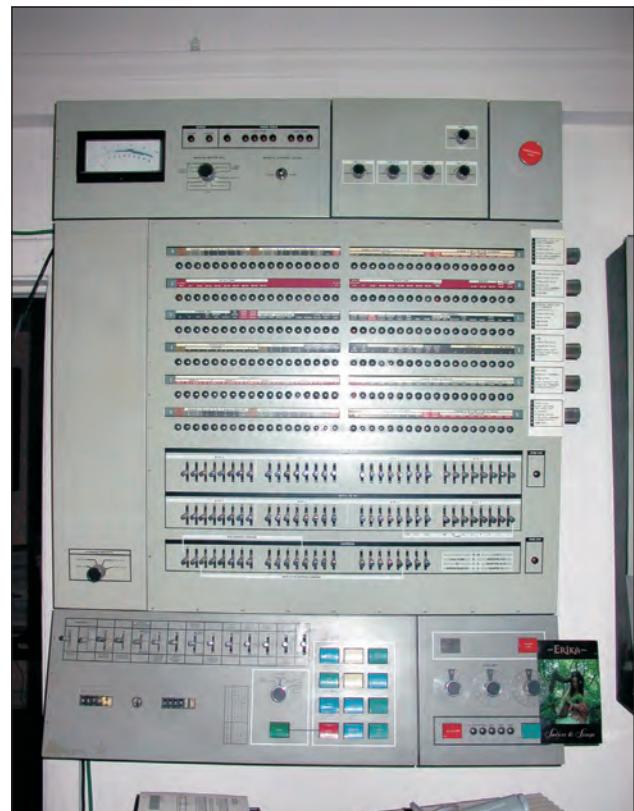
At a basic level, operating systems allow computers to complete simple tasks such as connecting to a keyboard or mouse, maintaining files on a hard drive, or managing connected devices such as a printer. At a higher level, an operating system (OS) controls access to a specific computer, ensuring the proper security is in place. For most devices, an OS regulates the flow of competing programs and information, allowing a computer to engage simultaneously in multiple tasks—such as word processing

and file downloading—without causing a data traffic jam or crash.

Four general types of OS exist, each with specific tasks and types of users. A real-time OS must perform tasks immediately, processing data in tenths of a second in order to transmit “real-time” information, such as a high-definition live broadcast. A single-user, single-task OS, such as Microsoft Disk Operating System (MS-DOS)—a system that is now essentially obsolete—can run only one program at a particular time. A multitasking OS for a single user is the most common one found on a personal computer, allowing someone to engage multiple applications at once. In a multiuser OS, more than one person can access hardware and software simultaneously. A company’s content management system is a type of multiuser OS, allowing employees to obtain information remotely and without interruption from other users.

OVERVIEW

Windows OS and Apple’s macOS are the most widely used systems, but others exist that can perform either similar or unique tasks. First developed by American Telephone & Telegraph (AT&T) in 1969, Unix became the de facto OS for academic institutions during the 1970s, and it spawned both a grouping of related operating systems—often termed “Unix-like” systems—and a debate about the proprietary nature of operating systems. Perhaps most notably, Steve Jobs used the Unix-like Berkeley Software Distribution (BSD) for NeXTSTEP, an OS used by Tim Berners-Lee to develop the internet. GNU/Linux is an example of a Unix-like OS developed from open-source software. Google also entered the OS market with the Chrome OS, which garnered attention for its unusual, heavily cloud-based approach to computing, though its market share as of 2023 was less than 4 percent. Both Chrome OS and Android, Google’s mobile OS, are based on Linux, though they operate very differently from it.



An IBM System 360/65 Operator’s Panel. OS/360 was used on most IBM mainframe computers beginning in 1966, including computers used by the Apollo program. Photo by Arnold Reinhold, via

As personal computing has evolved away from desktop systems to handheld machines such as smartphones, the Android and iOS operating systems have become integral aspects of information technology and data sharing. Bankrolled by Google, the Android OS is used across a wide spectrum of mobile devices. Apple’s iOS is specifically used with the iPhone, while iPadOS is used with iPads and watchOS with Apple Watch devices. The Symbian OS, the most popular OS for mobile technology until the Android, found success through affiliation with Nokia’s S60 platform. Though declining in popularity, BlackBerry devices, which use a specific, closed-source OS, were some of the first to integrate tasks in a way that became an industry standard.

—Christopher Rager

Further Reading

- Garrido, Josei M. *Principles of Modern Operating Systems*. Jones, 2013.
- Hansen, Per Brinch. *Classic Operating Systems: From Batch Processing to Distributed Systems*. Springer, 2001.
- “Market Share Held by the Leading Computer (Desktop/Tablet/Console) Operating Systems Worldwide from January 2012 to June 2023.” *Statista*, 5 Sept. 2023,

www.statista.com/statistics/268237/global-market-share-held-by-operating-systems-since-2009.

Peek, Jerry D., Grace Todino, and John Strang. *Learning the UNIX Operating System*. 5th ed., ProQuest, 2002.

Silberschatz, Abraham, Peter Baer Galvin, and Greg Gagne. *Operating System Concepts*. 10th ed., Wiley, 2021.

Tanenbaum, Andrew S., and Herbert Bos. *Modern Operating Systems*. 4th ed., Prentice, 2014.

P

PERSONAL COMPUTERS

ABSTRACT

The typical personal computer (PC) has devices for the input and output of information and a means of retaining programs and data in memory. It also has the means of interacting with programs, data, and memory. PCs enable users to perform a vast array of tasks and to connect with other users around the world through the internet.

BACKGROUND

A computer is a device that manipulates raw data into potentially useful information. Computers may be analog or electronic. Analog computers use mechanical elements to perform functions. For example, Stonehenge in England is believed by some to be an analog computer. It allegedly uses the stones along with the positions of the sun and moon to predict celestial events like the solstices and eclipses. Electronic computers use electrical components like transistors for computations.

Modern computing can be traced to nineteenth-century mathematician Charles Babbage's analytical engine. Boolean algebra, devised by mathematician George Boole later in the same century, provided a logical basis for digital electronics. Lambda calculus, developed by mathematician Alonso Church in the early twentieth century, also laid the foundations for computer science, while the Turing machine, a theoretical representation of computing developed by mathematician Alan Turing, essentially modeled computers before they could be built. In the 1940s, mathematicians Norbert Wiener and Claude Shannon researched

information control theory, further advancing the design of digital circuits.

The Electrical Numerical Integrator and Calculator (ENIAC) was the first general purpose electronic computer. It was created shortly after World War II by physicist-engineer John Mauchly and engineer J. Presper Eckert. They also developed the Binary Automatic Computer (BINAC), the first dual-processor computer, which stored information on magnetic tape rather than punch cards, and the first commercial computer, Universal Automatic Computer (UNIVAC). Mathematician John von Neumann made important modifications to ENIAC, including serial operations to facilitate mathematical calculations. Scientists William Bradford Shockley, John Bardeen, and Walter Brattain won the 1956 Nobel Prize in Physics for transistor and semiconductor research, which influenced the development of most subsequent electronic devices, including personal computers (PCs).

During the latter half of the twentieth century, countless mathematicians, computer scientists, engineers, and others advanced the science and technology of PCs, and research has continued into the twenty-first century. For example, Microsoft cofounder Bill Gates published a paper on sorting pancakes, which has extensions in the area of computer algorithms. PCs have facilitated mathematics teaching and research in many areas such as simulation, visualization, and random number generation, though the use of calculators and software for teaching mathematics generated controversy.

Many consider the first PC to be Sphere 1, created by Michael Wise in the mid-1970s. The Apple

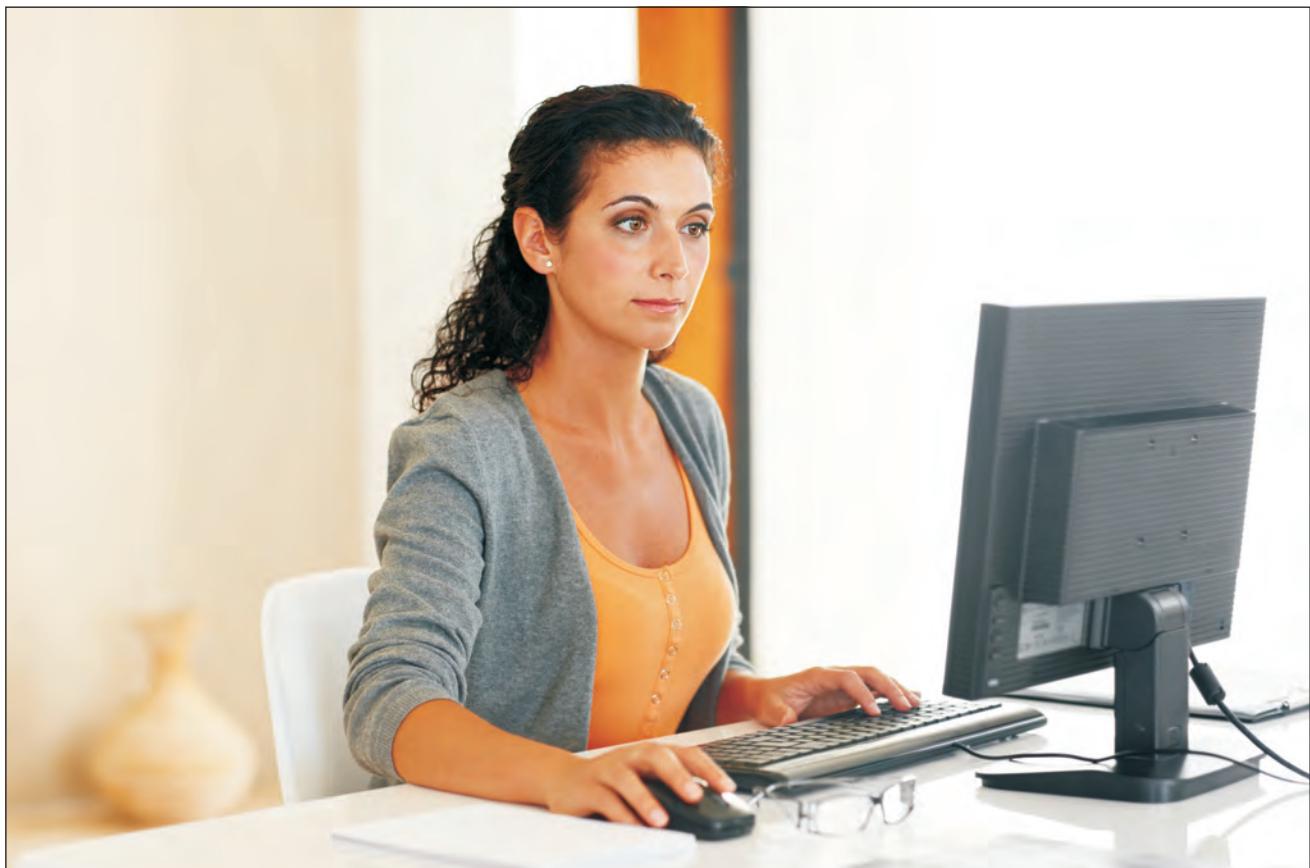


Photo via iStock/GlobalStock. [Used under license.]

II was introduced in 1977, and Apple Inc. offered the Macintosh, which had the first mass-marketed graphical user interface (GUI), by 1984. IBM debuted its PC in 1981. “Macs” and Windows PCs quickly became common in businesses and schools for a variety of purposes. Processing speed, size, memory capacity, and other functional components became faster, smaller, lighter, and cheaper over time, and PCs evolved into a multitude of forms designed to be customizable to each user’s needs. During the first decades of the twenty-first century, desktops, laptops, netbooks, tablets, smartphones, handheld programmable calculators, digital book readers, smartwatches, and other devices began to offer enhanced access to computing, the internet, and other functions.

OVERVIEW

The typical PC has devices for the input and output of information and a means of retaining programs and data in memory. It also has the means of interacting with programs, data, memory, and devices attached to the computer’s central processing unit (CPU). Input devices have historically included a keyboard and a mouse, while newer systems frequently use touch technology, either in the form of a special pad or directly on the screen. Other devices include scanners, digital cameras, and digital recorders. Memory storage devices are classified as “primary memory” or “secondary” devices. The primary memory is composed of the chips on the board inside the case of the computer. Primary memory comes in two types:

read-only memory (ROM) and random-access memory (RAM). ROM contains the rudimentary part of the operating system, which controls the interaction of the computer components. RAM holds the programs and data while the computer is in use. Popular types of secondary memory used for desktop computers include magnetic disk drives, optical compact discs (CD) and digital video disc (DVD) drives, and universal serial bus (USB) flash memory.

The speed of the computer operation is an important factor. Computers use a set clock cycle to send the voltage pulses throughout the computer from one component to another. Faster processing enables computers to run larger, more complex programs. The disadvantage is that heat builds up around the processor, caused by electrical resistance. ENIAC was one thousand times faster than the electromechanical computers that preceded it because it relied on vacuum tubes rather than physical switches. Turing made predictions regarding computer speeds in the 1950s, while Moore's law, named for Intel cofounder Gordon Moore, quantified the doubling rate for transistors per square inch on integrated circuits. The number doubled every year from 1958 into the 1960s, according to Moore's data. The rate slowed through the end of the twentieth century to roughly a doubling every eighteen months. Some scientists predict more slowdowns because of the heat problem. Others, such as mathematician Vernor Vinge, have asserted that exponential technology growth will produce a singularity, or essentially instantaneous progress. Processing speed, memory capacity, pixels in digital images, and other computer capabilities have been limited by this effect. There has also been a disparity in the growth rates of processor speed and memory capacity, known as memory latency, which has been addressed in part by mathematical programming techniques, like caching and dynamic optimization.

Carbon nanotubes and magnetic tunnels might be used to produce memory chips that retain data even when a computer is powered down. At the start of the twenty-first century, this approach was being developed with extensive mathematical modeling and physical testing. Other proposed solutions involved biological, optical, or quantum technology. Much of the physics needed for quantum computers exists only in theory, but mathematicians such as Peter Shor had already begun working on the mathematics of quantum programming, which involves ideas such as Fourier transforms, periodic sequences, prime numbers, and factorization. Fourier transforms are named for mathematician Joseph Fourier.

PERSONAL COMPUTERS AND THE DIGITAL DIVIDE

The digital divide is the technology gap between groups that have differential access to PCs and related technology. The gap is measured both in social metrics, such as soft skills required to participate in online communities, and infrastructure metrics, such as ownership of digital devices. Mathematical methods are used to quantify the digital divide. Comparisons may be made using probability distributions and Lorenz curves, developed by economist Max Lorenz, and measures of dispersion such as the Gini coefficient, developed by statistician Corrado Gini. Researchers have found digital divides among different countries, and within countries, among people of different ages, between genders, and among socioeconomic strata.

The global digital divide quantifies the digital divides among countries and is typically given as the differences among the average numbers of computers per hundred citizens. In the early twenty-first century, this metric varied widely. Several concerted private and government efforts, such as One Laptop Per Child, were directed at reducing the global digital divide by providing

computers to poor countries. The breakthroughs connected to these efforts, such as mesh internet access architecture, benefited all users.

—Zenia C. Bahorski, Maria Droujkova

Further Reading

- Campbell-Kelly, Martin, William F. Aspray, Jeffrey R. Yost, Honghong Tinn, and Gerardo Con Díaz. *Computer: A History of the Information Machine*. 4th ed., Routledge, 2023.
- Lauckner, Kurt, and Zenia Bahorski. *The Computer Continuum*. 5th ed., Pearson, 2009.
- Lemke, Donald, and Tod Smith. *Steve Jobs, Steve Wozniak, and the Personal Computer*. Capstone Press, 2010.
- O'Leary, Timothy, Linda O'Leary, and Daniel O'Leary. *Computing Essentials 2023*. McGraw-Hill, 2022.
- Wozniak, Steve, and Gina Smith. *iWoz: Computer Geek to Cult Icon: How I Invented the Personal Computer, Co-Founded Apple, and Had Fun Doing It*. W. W. Norton, 2007.

PHISHING

ABSTRACT

Phishing is the act of using communication devices such as email and telephones in an attempt to trick individuals into either revealing their personal information, including passwords and Social Security numbers, or installing malicious software (malware). Phishing is used by identity thieves to acquire the confidential personal and financial information of victims.

BACKGROUND

The term “phishing” is derived from the word “fishing” and refers to identity thieves fishing for victims. Identity thieves, also referred to as “phishers,” pose as representatives from banks, credit card companies, or other institutions and email or call victims requesting their personal information. Phishers offer fraudulent reasons for why the victim must enter their personal information.

Phishing first became popular during the early days of America Online (AOL), one of the first widely used internet service providers (ISPs). Phishers would pretend to be AOL employees and send users instant messages requesting their passwords for confirmation purposes. Once they procured users’ passwords, phishers could use them to access their accounts for spamming or other nefarious purposes. AOL eventually put policies into place to delete the accounts of anyone involved with phishing and to quickly detect any instant messages that contained phishing-related words.

After AOL’s security increased, phishers started to pretend to be financial institutions such as banks and credit card companies. The first known phishing attempt in which the perpetrator pretended to be a financial institution occurred in June 2001. A phisher posed as e-gold, a website that allowed users to instantly transfer gold currency. Although this attempt was unsuccessful, it was used by phishers as a test to develop more successful methods.

Following the terrorist attacks of September 11, 2001, phishers began sending out fraudulent identification check emails. Recipients were asked to enter their personal information to confirm their identities for reasons of national security. These attempts were also seen as failures but were used to test new methods of phishing.

OVERVIEW

After unsuccessful attempts in the early part of the 2000s, phishers started implementing more sophisticated methods to acquire victims’ personal information. By 2004, phishing was seen as a serious and lucrative criminal activity. It led to heightened online security, increased awareness, lawsuits, and government actions.

Many phishers pose as social media websites such as Facebook. In some cases, they send users emails claiming that they noticed a security issue on the

account and that, as a result, users must fill out legal forms, such as terms of use or copyright law forms. These phishers typically state that if users do not comply and fill out the form, their account will be suspended or terminated. A link is usually included in the email that is disguised with a legitimate address, such as Facebook's web address; in reality, the link will download an executable file if clicked. This kind of trickery is how phishers get victims to download malicious software that exposes personal information and passwords. In some cases, the link may lead not to a malicious download but to a fake log-in page into which victims may enter their credentials, thus unknowingly giving the phishers access to their accounts. Oftentimes phishers include company logos in their emails to make them look legitimate. There are several ways to tell whether an email is a phishing scam or not. Common indicators of scam emails include misspelled words and threats of account deletion.

In 2006, phishers began using emails to pose as the US Internal Revenue Service (IRS). In response, the IRS issued numerous consumer warnings about the use of the IRS logo for phishing and

identity-theft purposes. Several of these IRS-related email phishing scams claimed that the individual was owed a tax refund. The individual was then asked to enter personal information in order to receive the money owed them. The IRS established several ways for consumers to report suspicious emails that might be phishing scams.

Some phishers set up fraudulent or replica websites to pose as financial institutions. Once one of these fake websites is visited, users can unknowingly receive malicious software. Even on legitimate websites, phishers can alter the sites' scripts and security aspects to fool users. This is a particularly successful phishing method because the fraudulent websites are nearly undetectable to average online users.

In 2006, this type of phishing was done on the website PayPal, which allows users to easily transfer money to merchants or other individuals online. Phishers used the PayPal website to trick users into going to a uniform resource locator (URL) hosted on the legitimate PayPal website. Phishers created a warning message that appeared when users visited the website that said the user's account was disabled

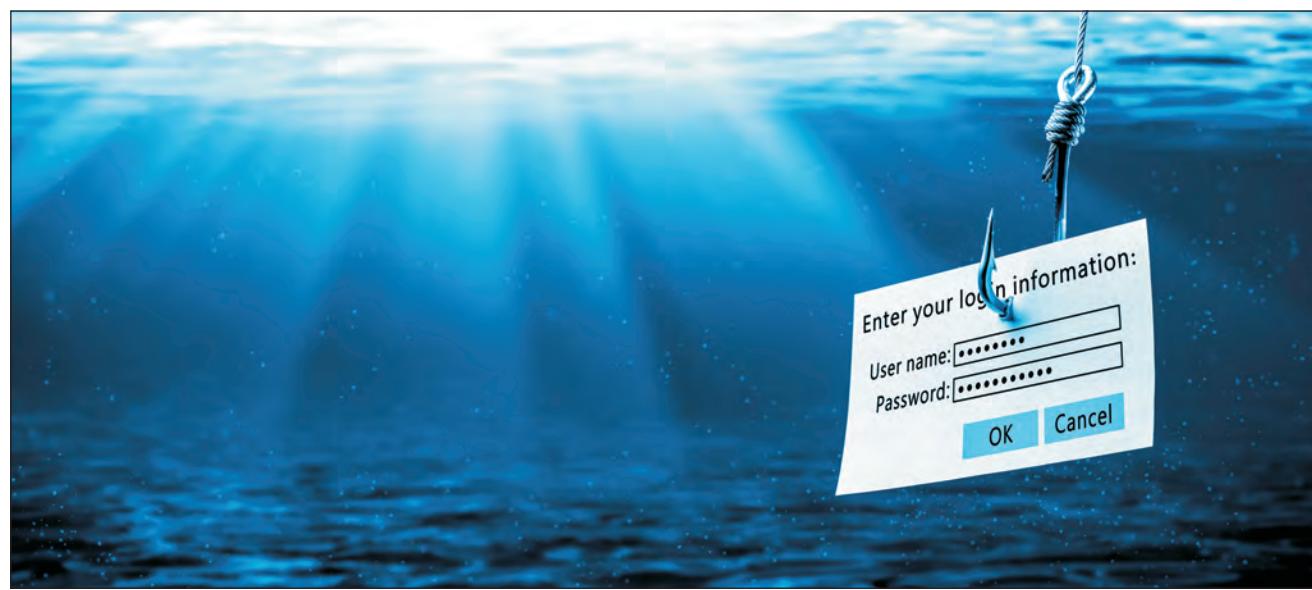


Photo via iStock/Philip Steury. [Used under license.]

because it may have been accessed unlawfully by a third party. Users were then redirected to a fraudulent PayPal log-in page that looked extremely similar to the actual log-in page.

This technique has also frequently been used on the websites of banks. When users visit the sites, a pop-up window appears, requesting their personal log-in information for security purposes. Financial institutions responded by increasing online security measures through the use of security questions and images. For example, in 2008, Bank of America implemented a SiteKey system on its website, in which users chose an image that appeared every time they logged in. If the image did not appear during the log-in process, the user had been led to a fraudulent site. Other companies hit with phishing attacks during the 2000s included Best Buy, the United Parcel Service (UPS), and First Union Bank.

File-sharing websites and services such as RapidShare have also been used by phishers to harvest information or leave computers vulnerable to later attack. Phishers would use fake websites or alter legitimate ones to sell users RapidShare upgrades that did not exist. Sometimes phishers would send out email newsletters posing as file-sharing websites or would post in forums, encouraging users to pay for fake upgrades. Both of these phishing methods were used to steal victims' credit card information.

A majority of online phishing in the 2000s was traced to the Russian Business Network (RBN). RBN is a cybercrime organization based in Russia that performs identity theft on a large scale. It undertook some of the largest and most successful phishing scams of the decade, oftentimes selling personal information to criminals for use in identity theft. RBN developed malicious software such as the MPack, which is a kit that was sold to hackers to infect hundreds of thousands of personal computers.

Phishing remained a significant problem following the first decade of the twenty-first century, despite increased public awareness of phishing

methods and means of avoiding them. Among the most notable phishing attacks in the 2010s were a 2013 attack on the big-box retailer Target, in which over 100 million customer credit card numbers were stolen, and a similar-sized 2014 attack on the home-improvement chain Home Depot. During the early 2020s, malicious individuals and organizations continued to conduct phishing attacks on individuals and businesses. In addition to social media services and the IRS, which remained perennial targets of impersonation, phishers often posed as popular businesses, such as the streaming content provider Netflix, as well as financial and government institutions when contacting their would-be victims. During the COVID-19 pandemic, phishers sometimes posed as public-health agencies, contact tracers, or other authorities while carrying out attacks.

PHONE PHISHING

Phishers also use phones to acquire personal financial information. This method became known as "vishing" (voice phishing). Sometimes they email messages posing as financial institutions or internet providers. At other times, phishers may steal a list of phone numbers from financial institutions and call the victims themselves. Once victims are on the phone, they may be asked to enter their debit card information, Social Security number, or other personal information. The phishers typically use voice over internet protocol (VoIP) to disguise the location of their numbers, making the phishers difficult to locate. A VoIP number allows phishers to make and receive phone calls using their computer and internet connection and to disguise the caller identification on the victims' end. They can call a victim and have the caller identification information correspond to that of a trusted bank or other entity. This makes vishing hard to monitor.

Other phishers use phones to pose as technical support departments from internet providers or software companies such as Microsoft. Phishers use

this method to install malware to gain access to sensitive information. Frequently, once the malicious software has been installed, phishers charge victims to remove it from their computer.

Phishers also use this method to adjust the settings on victims' computers to leave them vulnerable to further unlawful access. In response, financial institutions, internet providers, and software companies have released warnings stating that they will never call and request information or make charges via the phone. They have stated that if anyone calls claiming to be from their institution, that individuals should hang up and report the number.

COMBATING PHISHING

The rise of phishing and the massive financial losses it has caused has led to antiphishing responses on public and private levels. The most basic method of combating phishing has been to educate the public on how to recognize these scams. The IRS has released numerous consumer warnings throughout the years, and software companies, including Microsoft, have published materials online to inform the public about phishing. Along with online consumer warnings, the IRS has released informational videos and podcasts and provided consumers with emails and telephone numbers they can contact if they suspected they have been the target of phishing attempts.

Because of phishing, several websites, financial institutions, and other entities have changed the way they handle emails and information online. For example, PayPal began to include users' log-in names in emails to let them know they were not being phished. Typically, PayPal phishing emails would address users with generic greetings, such as "Dear PayPal user." In a similar fashion, banks have started to include partial account numbers in emails.

Many popular internet browsers have implemented measures for what is known as secure browsing. Several internet browsers now also include

antiphishing technology as part of their browsers and services. If a user attempts to visit a website that is not recognized as secure by Firefox, for example, a warning box will appear, or Firefox will simply block the website.

Email providers such as Gmail have increased their email spam filters to help combat phishing. Many of these filters utilize language processing to recognize and block emails that include common phishing words and sentences.

The US Federal Trade Commission (FTC) has set up services to help reduce telephone phishing scams. Their services encourage users to report suspicious phone calls and phone numbers. The FTC then passes this information on to appropriate law enforcement officials. Individuals can also register their phone number on the National Do Not Call Registry, which limits the number of telemarketers and potential phishers that can call the number.

FEDERAL RESPONSES

In 2004, the FTC filed a lawsuit against a seventeen-year-old in California who was suspected of perpetrating phishing scams to acquire credit card information. This was the first law-enforcement action brought against a phisher. In 2006, the Federal Bureau of Investigation (FBI) enacted an operation code-named Cardkeeper that led to the arrest of seventeen people involved with international phishing scams in the United States, Poland, and Romania. This group allegedly stole identities, credit card information, and bank information. Four suspects from the group were arrested in the United States and were in possession of machines used to encode cards with victims' bank information.

On December 16, 2003, President George W. Bush signed the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act). This act established national standards for the distribution of commercial email. The FTC was given authority to enforce the provisions

put forth by the act. It was created to reduce the amount of unwarranted and unwanted emails, including phishing-related messages. Although many critics saw it as a failure, the first individual convicted under its provisions was sentenced in 2007. This individual, Jeffrey Brett Goodin, sent thousands of emails posing as the AOL billing department and requesting users' personal information. He was sentenced to serve seventy months in prison.

IMPACT

Phishing has raised many concerns about the security of valuable personal information that is frequently used online by banks and other entities. During the first several decades of the twenty-first century, various phishing methods managed to successfully rob victims of millions of dollars. Businesses affected by phishing also suffered severe financial losses. Phishing was the most successful cybercrime method of the early twenty-first century and changed the way information is distributed online. Its rise has also led to an increase in awareness and heightened security on several fronts.

—Patrick G. Cooper

Further Reading

- “Coronavirus Scams—Consumer Resources.” *Federal Communications Commission*, 7 Mar. 2022, www.fcc.gov/covid-scams.
- Hong, Jason. “The State of Phishing Attacks.” *Communications of the ACM*, vol. 55, no. 1, 2012, pp. 74–81.
- “How to Recognize and Avoid Phishing Scams.” *Federal Trade Commission Consumer Advice*, Sept. 2022, consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams.
- Jakobsson, Markus, and Steven Myers, editors. *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*. John Wiley & Sons, 2007.
- James, Lance. *Phishing Exposed*. Syngress Publishing, 2005.
- Krebs, Brian. “Shadowy Russian Firm Seen as Conduit for Cybercrime.” *Washington Post*, 13 Oct. 2007,

www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461.html.

Lininger, Rachael, and Russell Dean Vines. *Phishing: Cutting the Identity Theft Line*. Wiley, 2005.

Watters, Paul A. *Cybercrime and Cybersecurity*. CRC Press, 2023.

PRIVACY BREACHES

ABSTRACT

Online privacy breaches can lead to the destruction, loss, unauthorized disclosure, and exposure of personal data. Malicious individuals and groups seeking to obtain private information target a wide range of organizations, including businesses, educational institutions, and government agencies.

BACKGROUND

With so many systems instrumental to daily life being carried out online—from banking to healthcare—a vast amount of personal data is vulnerable to cyberattacks. The 2010s saw a number of high-profile breaches that cost people their privacy and companies hundreds of millions of dollars. Ten of the fifteen largest data breaches to that date took place between 2010 and 2019. At times, individuals or hacking collectives out for financial gain were to blame; other instances involved cyberespionage attacks carried out by foreign governments. Collectively, billions of records—for example, login credentials, credit-card numbers, and social security numbers—fell into the wrong hands over the course of the decade.

The United States itself has been involved in cyberespionage, as the public learned in 2010, when Stuxnet was revealed. A computer “worm” (a type of malware that spreads copies of itself from one computer to the next), Stuxnet was likely codeveloped by American and Israeli intelligence agencies, with the goal of sabotaging Iran’s nuclear weapons program.



Image via iStock/Black_Kira. [Used under license.]

The worm destroyed supervisory control and data acquisition (SCADA) equipment being used by Iran to enrich nuclear fuel, and it gained national attention for its ability to not merely steal data but to cause actual physical destruction—a new frontier in cyberwar.

In early 2010 Operation Aurora also came to light. A coordinated series of attacks on major American tech companies, including Google, Microsoft, and Adobe, Aurora was orchestrated by the Chinese government's military hackers whose motives were said to include trying to infiltrate the accounts of Chinese human rights advocates and probing to discover if the US government had uncovered the identity of clandestine Chinese operatives. (Soon after Aurora was discovered, Google shut down operations in China.)

In 2014, a group calling themselves the Guardians of Peace, later linked to North Korean intelligence agencies, carried out an audacious breach of Sony Pictures' online systems in an effort to force the studio to abandon plans to release a comedy film called *The Interview*, which revolved around a plot to kill North Korean leader Kim Jong-un. The hack

mainly caused embarrassment—many sensitive private emails were made public—but it conformed the scope of North Korea's previously unknown cybercapabilities.

A hotel chain may seem like an unlikely target for nation-state hackers, but in 2018, the personal data of 500 million customers who had stayed at a Marriott Starwood hotel was compromised. Hackers had uncovered guest names, room numbers, birthdates, and credit card information, among other details, and the chain was fined \$24 million for failing to keep customers' personal data secure. The attack was later found to be the work of a Chinese intelligence group seeking to gather data on American citizens. Marriott would go on to experience further data breaches in 2020 and 2022.

OVERVIEW

In 2011, in what was then one of the biggest hacks that had ever occurred, Sony announced that financial data and personal information from 77 million users of the PlayStation Network had been accessed illegally, and cyberexperts pointed to the incident as concrete proof that businesses needed to proactively

invest in security. (Despite that advice, Sony's first step was to add clauses to their Terms of Service requiring users to give up on their right to sue after security breaches, and other companies subsequently did the same.)

Two years later, another high-profile case made even more evident how lax some companies were in their treatment of sensitive data: in 2013 a cohort of Eastern European hackers was charged by federal prosecutors for stealing more than 160 million credit card numbers and additional records from 7-Eleven, J.C. Penney, and other companies. The group's nefarious activities had begun back in 2005, and by the time they were caught, they had netted hundreds of millions of dollars.

Dwarfing all previous breaches, in 2013 every existing Yahoo! account—an estimated 3 billion—were also compromised. Although no financial information was stolen, the hackers got access to names, emails, passwords, and the answers to security questions, and Yahoo! was forced to pay \$117 million towards a class action settlement. (At the time, Yahoo! was being acquired by Verizon, and while the deal was not totally derailed, the sales price was greatly reduced in the wake of the incident.) That year retail giant Target was also hacked, with attackers accessing the company's servers via credentials stolen from a third-party vendor. Some 70 million customers were affected, and the incident cost Target more than \$150 million. The following year 145 eBay users suffered a similar situation.

While those attacks attracted some media attention, the press came out in full force in 2015, when Ashley Madison, a dating site for people who were married and interested in cheating on their partners, was breached. A hacking collective called the Impact Team had managed to access more than 300 gigabytes (GBs) of company and customer data, and after the owners of Ashley Madison refused to comply with the group's request to shut down the site, the names of 30 million users were

released publicly, leading to a spate of work resignations, divorces, and suicides—making this one of the rare instances in which a breach led directly to someone's death.

The highest-profile incident of the decade, however, came in 2017, when Equifax, one of the largest consumer credit reporting agencies in the world, allowed the names, social security numbers, addresses, and driver's licenses numbers of 150 million Americans (more than 40 percent of the country's adult population) to fall into the hands of hackers. The company subsequently reached a settlement with the Federal Trade Commission (FTC) that required them to pay out \$425 million to those affected; total cost to the company, including legal fees and new security technology, was an estimated \$1.4 billion.

As cybercriminals found increasingly sophisticated ways to circumvent security measures, experts continued to try to devise stronger protections and more robust systems. In 2019 alone, however, more than 5,000 breaches of various sizes were recorded, and about 8 billion records were compromised. Privacy breaches remained incidents of major concern during the early 2020s, a period in which malicious individuals or groups gained access to data from multiple companies, including Marriott, 23andme, T-Mobile, and many others.

—Mari Rich

Further Reading

- Bray, Chad, and Danny Yadron. "Nasdaq, Others, Targeted by Hackers." *Wall Street Journal*, 26 July 2013, www.wsj.com/articles/SB10001424127887324564704578627640005242794.
- Cimpanu, Catalin. "A Decade of Hacking." *ZDNet*, 12 Dec. 2019, www.zdnet.com/article/a-decade-of-hacking-the-most-notable-cyber-security-events-of-the-2010s.
- Faife, Corin. "The Marriott Hotel Chain Has Been Hit by Another Data Breach." *The Verge*, 6 July 2022, www.theverge.com/2022/7/6/23196805/marriott-hotels-maryland-data-breach-credit-cards.

- Holmes, Aaron. "Hackers Have Become So Sophisticated That Nearly 4 Billion Records Have Been Stolen from People in the Last Decade Alone: Here Are the 10 Biggest Data Breaches of the 2010s." *Business Insider*, 13 Nov. 2019, www.businessinsider.com/biggest-hacks-2010s-facebook-equifax-adobe-marriott-2019-10.
- Koshiw, Isobel. "How an International Hacker Network Turned Stolen Press Releases into \$100 Million." *The Verge*, 22 Aug. 2018, www.theverge.com/2018/8/22/17716622/sec-business-wire-hack-stolen-press-release-fraud-ukraine.
- Scropton, Alex. "Data Breaches Are a Ticking Timebomb for Consumers." *Computer Weekly*, 9 Feb. 2021, www.computerweekly.com/news/252496079/Data-breaches-are-a-ticking-timebomb-for-consumers.
- Weatherbed, Jess. "T-Mobile Discloses Its Second Data Breach So Far This Year." *The Verge*, 2 May 2023, www.theverge.com/2023/5/2/23707894/tmobile-data-breach-april-personal-data-pin-hack-security.

PRIVACY RIGHTS

ABSTRACT

The privacy right of individuals versus the need of law enforcement to build tight cases against suspected offenders creates an ongoing dilemma. New technologies have made it easier to gather information, but privacy advocates contend that they have also made it easier to infringe on the rights of innocent individuals. The debate surrounding privacy rights and technology has numerous implications for the field of cybersecurity.

BACKGROUND

Before the 1960s, the right to privacy was not articulated in US law. It was generally understood that US citizens had a right to privacy that protected their persons and property, but it was unclear what was involved in that right. In 1965, in part as the result of widespread cultural changes, the Supreme Court acknowledged the right to privacy for the first time in *Griswold v. Connecticut*, which gave married couples the right to make their own decisions about

obtaining birth control. Eight years later in *Roe v. Wade*, the Supreme Court based its support for the right to obtain an abortion on the right to privacy. (That decision would later be overruled in the 2022 *Dobbs v. Jackson Women's Health Organization* decision.)

Since that time, the concept of the right of privacy has been expanded to encompass everything from protection from illegal searches to the sexual rights of homosexuals. Following the 9/11 terrorist attacks on the United States by members of Al-Qaeda, the war on terror stood the right to privacy on its head and initiated a lengthy battle between civil libertarians and those who believed privacy should take a back seat to national security.

Following acceptance of the right to privacy by state and federal courts, privacy debates erupted over such diverse issues as the right of gay men to engage in consensual sex within the privacy of their own homes, which was in violation of many state sodomy laws (*Bowers v. Hardwick*) and the right of high school students to be free from drug testing without cause for suspicion (*Board of Education v. Earls*). The Supreme Court did not uphold the privacy right in either case. However, in the 2003 decision *Lawrence v. Texas* the Supreme Court overturned *Bowers v. Hardwick*, holding that state sodomy laws were unconstitutional.

OVERVIEW

The privacy right of individuals versus the need of law enforcement to build tight cases against suspected offenders creates an ongoing dilemma. New technologies have made it easier to gather information, but privacy advocates contend that they have also made it easier to infringe on the rights of innocent individuals. In the early twenty-first century, one ongoing battle concerns the use of automatic license plate readers (ALPRs), which randomly read and analyze data on all vehicles, not just those of suspected criminals. Another battle involves routine

collection of deoxyribonucleic acid (DNA) of individuals arrested but not convicted of any crime.

Privacy rights of celebrities versus the freedom of the press guaranteed in the First Amendment has also created heated debate in the United States and abroad. When paparazzi were suspected of causing the death of Diana, Princess of Wales, in France in August 1997, there was a global backlash against intrusive press tactics. In 2009, California passed the Paparazzi Reform Initiative, establishing fines for paparazzi that crossed the line into offensiveness. Similar laws were already in effect in Europe.

Two years later, another international scandal over privacy rights erupted when it was reported that media mogul Rupert Murdoch, who owned Fox News, the *New York Post* and the *Wall Street Journal*, was encouraging his reporters for the *Sun* and *News of the World* to tap the telephones of celebrities such as Prince William, actor Hugh Grant, *Harry Potter* author J. K. Rowling, and noncelebrity individuals and families involved in news stories. The resulting scandal brought down *News of the World* and toppled careers of top executives in the Murdoch empire while strengthening support for privacy rights in the United Kingdom and elsewhere.

In the United States, passage of the Privacy Act of 1974 restricted the right of government agencies to collect and disseminate information. However, the terrorist attacks of 9/11 ripped away privacy rights as well as the sense of security that many Americans took for granted. The post-9/11 era was defined by George W. Bush's war on terror, in which Congress complied with the president's request for unprecedented authority by passing the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, better known as the USA PATRIOT Act. Amid accusations of bypassing established rules of due process, the act contained more than a thousand provisions that gave the government the right to tap telephones, carry out surveillance of electronic

media, track library activity, and collect DNA samples indiscriminately.

The ongoing battle over privacy took on added heat in the summer of 2013 when Edward Snowden, a former contractor with the National Security Agency (NSA) fled the country after leaking classified information about the government's gathering information on private telephone calls and emails. Snowden's actions led to national outrage concerning the secret Foreign Intelligence Surveillance Court, which was established in 1978 and was being used to allow the NSA to collect information on a variety of activities. Privacy groups ranging from church groups to human rights activists responded by filing suits designed to halt government spying without just cause.

PRIVACY RIGHTS AND CYBERSECURITY

The Federal Bureau of Investigation (FBI) and the technology company Apple got into a dispute in 2016 over privacy rights on Apple products. On December 2, 2015, Syed Rizwan Farook and Tashfeen Malik killed fourteen people and injured twenty-two at an office holiday party in San Bernardino, California. Both shooters were later killed by police. The FBI was unable to access the data on Farook's iPhone because of the security features on the phone. The federal agency requested that Apple help them hack into the phone, which the company refused on the grounds of maintaining customer privacy and concerns over setting precedents. The FBI eventually dropped the request to Apple and bypassed the company completely by hiring outside coders to write a program to hack the phone.

In the years that followed, the 2016 dispute and others called attention to the gray area of citizens' rights to privacy with new technology in the face of potential threats to national security. The incident also raised awareness of the intersections between privacy and cybersecurity. In addition to placing

user data at risk of misuse by hacking groups, security vulnerabilities and so-called backdoors in smartphone operating systems, computer software, and websites could facilitate surveillance by government agencies.

—Elizabeth Rholetter Purdy

Further Reading

- Alderman, Ellen, and Caroline Kennedy. *The Right to Privacy*. Knopf, 1995.
- Allen, Anita L. *Unpopular Privacy: What Must We Do?* Oxford UP, 2011.
- Bernal, Paul. *Internet Privacy Rights: Right to Protect Autonomy*. Cambridge UP, 2014.
- Brill, Steven. *After: How America Confronted the September 12 Era*. Simon & Schuster, 2003.
- Clark, Mitchell. “Here’s How the FBI Managed to Get into the San Bernardino Shooter’s iPhone.” *The Verge*, 14 Apr. 2021, www.theverge.com/2021/4/14/22383957/fbi-san-bernardino-iphone-hack-shooting-investigation.
- Epstein, Lee, Kevin T. McGuire, and Thomas G. Walker. *Constitutional Law for a Changing America: A Short Course*. 8th ed., Sage, 2015.
- Keizer, Garret. *Privacy*. Picador, 2012.
- Kemper, Bitsy. *The Right to Privacy: Interpreting the Constitution*. Rosen, 2015.
- Kizza, Joseph Migga. *Ethical and Social Issues in the Information Age*. 7th ed., Springer, 2023.
- Krimsky, Sheldon, and Tania Simoncelli. *Genetic Justice: DNA Data Banks, Criminal Investigations, and Civil Liberties*. Columbia UP, 2011.
- Lichtblau, Eric. “In Secret, Court Vastly Broadens Powers of N.S.A.” *New York Times*, 7 July 2013, www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html.
- Rocchi, Walter. *Cybersecurity and Privacy Law Handbook*. Packt, 2022.
- Strahilevitz, Lior Jacob. “Toward a Positive Theory of Privacy Law.” *Harvard Law Review*, vol. 126, no. 7, 2013, pp. 2010–42.
- Wheeler, Leigh Ann. *How Sex Became a Civil Liberty*. Oxford UP, 2013.
- Wright, Oliver, et al. “Hacking Scandal: Is This Britain’s Watergate?” *Independent*, 9 July 2011, www.independent.co.uk/news/uk/crime/hacking-scandal-is-this-britain-s-watergate-2309487.html.

Zetter, Kim, and Brian Barrett. “Apple to FBI: You Can’t Force us to Hack the San Bernardino iPhone.” *Wired*, 25 Feb. 2016, www.wired.com/2016/02/apple-brief-fbi-response-iphone.

PRIVACY SETTINGS

ABSTRACT

Privacy settings are the means by which users of a website or application manipulate and control the amount and type of personal information about them that is collected and disseminated. Forms of privacy settings range from the ability to control what other users see to what information might be passed on to third parties for targeted advertising or other purposes by the company providing the service.

BACKGROUND

Privacy settings have become essential in the digital world. An option to enable standard privacy settings or the ability to manipulate and personalize privacy settings is available on almost every form of digital platform—from operating systems to applications and websites. Google, Facebook, and even web browsers include options to determine what data users reveal to third parties—to an extent—during their time online.

Privacy settings became important as a way to implement the fair information practice principles (FIPPs) drafted by the Federal Trade Commission (FTC) in May 2000. No company is legally required to have privacy settings that consumers can manipulate or to have privacy settings at all, but companies are required to comply with the principles. Nearly ten years after FIPPs were created, websites began to experiment with more substantial and customizable privacy settings.

Currently, in the digital world, most websites and software provide privacy policies that detail whether a user has the ability to manipulate his or her

privacy settings. The most significant and often cited example of privacy policies online is Facebook's policy. Many Facebook users know that the website allows users to manipulate privacy settings to a certain degree. Users may decide with whom to share their posts and information—from a small group of friends to the general public. Because it is so simple to disseminate information online, privacy settings are essential to the preservation of an individual's personal information and online image, which may affect his or her personal and professional life, especially on a site as widely used as Facebook. Privacy settings have been controversial, however, since their inception because the existence of privacy settings does not mean that the settings are actually followed or enforced.

OVERVIEW

The issue of privacy settings is a largely unregulated area. No government agency is authorized to govern all the areas of cyberspace. In online services such as Google and Facebook, the FTC has the ability only to enforce the privacy settings, which companies disclose to consumers, to alleviate consumer fraud. In some controversial cases, the FTC may enter into legal agreements with companies to preserve consumer privacy and security. Google, for instance, made an agreement with the FTC in 2011 stating that the company will honor user privacy settings and will not circumvent them.

Specifically, the FTC ordered Google "not [to] misrepresent in any manner, expressly or by implication...the extent to which consumers may exercise control over the collection, use or disclosure of covered information." Although the FTC seems to exert control over one of the world's most significant online companies through this 2011 order, this contract demonstrates the current limit of the FTC's power. The FTC can only ensure that Google and other corporations do not engage in consumer fraud. Beyond this, the FTC is powerless to control

how these massive online corporations handle private consumer data.

Privacy settings are also controversial because consumers face many challenges even when privacy settings are in place. First, consumers often ignore privacy settings or do not have the technical skills that may be necessary to take advantage of the available protections. Privacy settings tend to be opt-in rather than opt-out provisions, which means that, unless requested, users' privacy settings will be off or set to the least restrictive settings. To protect privacy rights, consumers must be proactive and search for additional protection. Each update to a company's privacy policy may result in an individual's personal privacy settings are no longer as active or as restrictive as the user requested prior to the policy change.

Despite the controversy over privacy settings in the United States, few relevant laws had been put in place by the third decade of the twenty-first century, although several legislative efforts had been made. These included the Do Not Track Me Online Act of 2011 (H.R. 654, 2011), which would have required the FTC to "establish standards for the required use of an online opt-out mechanism," placed within an application or website's privacy settings. This bill did not gain sufficient support in 2011 but was reintroduced in 2015 as the Do Not Track Kids Act of 2015 (H.R. 2734, 2015), with a focus on children. The bill would have required companies to gain verifiable consent from parents before the companies are able to track any of the information within the application regarding children. The parents, via privacy settings, would be able to control exactly what information about their children is collected and how companies may then use the information. However, the Do Not Track Kids Act of 2015 was not enacted, and privacy settings continued to be a largely unregulated area with the potential danger to privacy rights that this entails. A subsequent (re)introduction of the Do Not Track Act (2019) would have applied to more than merely web browsers and

extended to all online activities, including mobile and phone applications. The bill would have allowed individuals to prevent organizations and companies from collecting any data beyond that which is necessary to supporting its goods and services, in addition to enforcing rigorous consequences for any violations. Much like its predecessors, however, the 2019 effort proved unsuccessful.

Many of the most ubiquitous web presences in modern society, including Facebook, Apple, and Google, continue to have a contentious relationship with users who want their data, browsing habits, and purchasing habits kept private. Turning off location services may prevent some parts of the companies' services from working but can keep people's private information more secure. Apps that use augmented reality or virtual reality rely on location services as well. Many apps track users' movements whether or not the app itself is open unless users change their privacy settings to prevent it.

Privacy settings remain a legally murky area. The FTC has little power to regulate the way in which privacy settings are presented or enforced. Consumers must trust that online companies provide users with options to safeguard their privacy while still being able to apprise themselves of the benefits of the various services. As the digital landscape has evolved, privacy settings began and continue to be a point of contention among consumers, government administrations, and online corporations.

—Ashley Baker

Further Reading

- Datta, Anwitaman, et al. *Social Informatics: Third International Conference, SocInfo, 2011, Singapore, October 2011*. Springer-Verlag, 2011.
- Rocchi, Walter. *Cybersecurity and Privacy Law Handbook*. Packt, 2022.
- Trepte, Sabine, and Leonard Reinecke. *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*. Springer-Verlag, 2011.

"Windows 10 Privacy Settings: How to Stop Microsoft from Spying on You." *The Star*, 16 Feb. 2019, www.thestar.com.my/tech/tech-news/2019/02/16/windows-10-privacy-settings-how-to-stop-microsoft-from-spying-on-you.

Zetlin, Minda. "Want to Make Facebook Stop Tracking Your Location When Not in Use? Here's How." *Inc.*, 22 Feb. 2019, www.inc.com/minda-zetlin/facebook-location-tracking-mobile-privacy-paul-mcdonald.html.

PUBLIC-KEY CRYPTOGRAPHY

ABSTRACT

Public-key cryptography is a form of data encryption technology used to protect confidential information. Data encryption refers to using a code as a key to protect important information and limit access to a certain user or group of users. Public-key cryptography, also called "public-key encryption," uses an asymmetric algorithm, or mathematical formula, that applies one key to encrypt the information and another one to decode it. Data is more secure when the encryption key does not have to be shared.

BACKGROUND

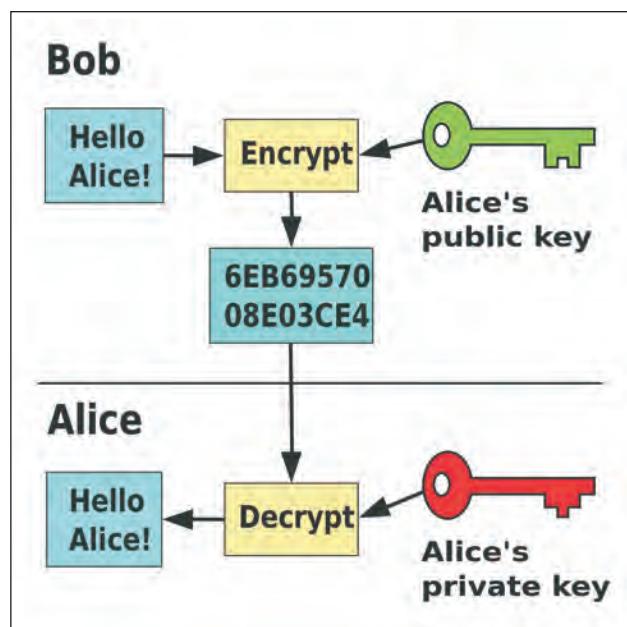
Ciphers and codes are two ways of protecting data so that it can remain secret. A code is a list of prearranged substitutes in which one thing replaces another. One simple form involves simply substituting a number for a letter; for instance, if A=1, B=2, etc., cat becomes "3-1-20." To decode a message, one uses the key to replace the substitutes with the original letters, words, or phrases. Every party who will be sharing the message needs the key to code or decode messages.

Ciphers are more complicated and use a mathematical algorithm to both substitute for the original information and multiply that result by another number that is the key to the algorithm. Using the example above, for instance, and encrypting it with a cipher with a key of 3, means multiplying "3-1-20" by 3 to get "9-3-60." To decipher the message, the

recipient needs the specific key, or algorithm, that works for the cipher. The recipient applies the key in reverse to decode the message. Real ciphers use complicated mathematical keys that may be complex algebraic functions.

The earliest known cipher is the Caesar cipher, which originated in the sixth century BCE. It is a symmetric cipher, meaning both parties use the same code to send and receive messages that either can read. For many centuries, this was the only type of cipher that existed. As technology increased to allow information to be shared faster and more easily between places, it became necessary to change codes more frequently. A code that fell into the wrong hands could be used to decode secret messages and also allowed an enemy to encrypt and send fake messages. To keep information safe, users were forced to develop more complicated codes and to change them often. This created administrative problems to manage and track multiple keys.

Cryptologists—those who work with codes and ciphers—realized that the way to solve the problem



Public-key cryptography, where different keys are used for encryption and decryption. Image via Wikimedia Commons. [Public domain.]

was to have a separate way to encrypt and decrypt the messages. This asymmetrical method means that data coded with the public key can only be decrypted with the private key, and vice versa. The public key could even be widely available and still protect the information because it can only be accessed by someone with the private key. Meanwhile, those with the private key do not have to worry about replacing the key to protect sensitive information. Public-key cryptography protects that data and can be used to determine if the information is coming from an authentic source, since only a holder of the private key can send a message. This is the basis of a digital signature in electronic data transmissions.

This asymmetric encryption form was first explored secretly by British intelligence services in the early 1970s. Around the same time, Stanford mathematicians Whitfield Diffie (1944–) and Martin Hellman (1945–) proved it was theoretically possible to develop an asymmetric ciphering method that uses two keys. In 1977, Massachusetts Institute of Technology (MIT) mathematicians Ronald L. Rivest (1947–), Adi Shamir (1952–), and Leonard M. Adleman (1945–) devised an algorithm based on factoring that allows for the first public-key encryption coding. Their method, known as the Rivest-Shamir-Adleman encryption, or RSA, created a special algorithm that can be used with multiple keys to encrypt information.

OVERVIEW

Factoring is the secret behind public-key cryptography. Factoring a number means identifying the two prime numbers that can be multiplied together to produce the original number. The process of factoring very large numbers is difficult and slow, even when computers are used. This makes the encryption secure. The person, company, or other entity that wants to encrypt a message chooses—or has a computer choose—two prime numbers that

are each more than 100 digits long and multiplies them together. This becomes the key and can be made public without endangering the code because it is so difficult to factor it back to the two prime numbers with which the person or entity started. It can be and often is published freely—the key is made public—and can be used by parties to send coded messages that only the originator of the code can read.

For example, Company A wants to be able to receive coded messages from its customers. Company A uses a computer to choose two large prime numbers— x and y —and multiplies them to get z . Company A then shares z on its website. Customer B can now take his message and the key z and enter them into the RSA algorithm. The algorithm will encode the message, which can now be sent to Company A. The key to unlocking it is x and y , which only Company A knows, so the company can decipher the message. The message remains secure because factoring z to x and y is difficult and time-consuming.

This process is used in countless computer transactions every day, often without the person encrypting the message even realizing it is taking place.

The method was so transformative for computer cryptography that the Association for Computing Machinery awarded the ACM Turing Award and \$1 million in prize money to Diffie and Hellman in March 2016.

—Janine Ungvarsky

Further Reading

- Bright, Peter. “Locking the Bad Guys Out with Asymmetric Encryption.” *Ars Technica*, 12 Feb. 2013, arstechnica.com/security/2013/02/lock-robster-keeping-the-bad-guys-out-with-asymmetric-encryption.
- Mann, Charles C. “A Primer in Public-Key Encryption.” *The Atlantic*, Sept. 2002, www.theatlantic.com/magazine/archive/2002/09/a-primer-on-public-key-encryption/302574.
- Niccolai, James. “As Encryption Debate Rages, Inventors of Public Key Encryption Win Prestigious Turing Award.” *PCWorld*, 2 Mar. 2016, www.pcworld.com/article/3039911/encryption/as-encryption-debate-rages-inventors-of-public-key-encryption-win-prestigious-turing-award.html.
- “Public Key Cryptography.” *IBM*, 8 Mar. 2021, www.ibm.com/docs/en/ztpf/1.1.0.15?topic=concepts-public-key-cryptography.
- “Public Key Cryptography.” *PCMag*, www.pcmag.com/encyclopedia/term/40522/cryptography.

R

RANDOM-ACCESS MEMORY

ABSTRACT

Random-access memory (RAM) is a form of memory that allows the computer to retain and quickly access program and operating system data. RAM hardware consists of an integrated circuit chip containing numerous transistors. Most RAM is dynamic, meaning it needs to be refreshed regularly, and volatile, meaning that data is not retained if the RAM loses power. However, some RAM is static or nonvolatile.

BACKGROUND

The speed and efficiency of computer processes are among the areas of greatest concern for computer users. Computers that run slowly (lag) or stop working altogether (hang or freeze) when one or more programs are initiated are frustrating to use. Lagging or freezing is often due to insufficient computer memory, typically random-access memory (RAM). RAM is an essential computer component that takes the form of small chips. It enables computers to work faster by providing a temporary space in which to store and process data. Without RAM, this data would need to be retrieved from direct-access storage or read-only memory (ROM), which would take much longer.

Computer memory has taken different forms over the decades. Early memory technology was based on vacuum tubes and magnetic drums. Between the 1950s and the mid-1970s, a form of memory called “magnetic-core memory” was most common. Although RAM chips were first developed during the same period, they were initially unable to replace core memory because they did not yet have enough memory capacity.

A major step forward in RAM technology came in 1968, when International Business Machines Corporation (IBM) engineer Robert Dennard patented the first dynamic random-access memory (DRAM) chip. Dennard’s original chip featured a memory cell consisting of a paired transistor and capacitor. The capacitor stored a single bit of binary data as an electrical charge, and the transistor read and refreshed the charge thousands of times per second. Over the following years, semiconductor companies such as Fairchild and Intel produced DRAM chips of varying capacities, with increasing numbers of memory cells per chip. Intel also introduced DRAM with three transistors per cell, but over time the need for smaller and smaller computer components made this design less practical. By the 2010s, commonly used RAM chips incorporated billions of memory cells. There are two major categories of random-access memory: static RAM (SRAM) and dynamic RAM (DRAM).

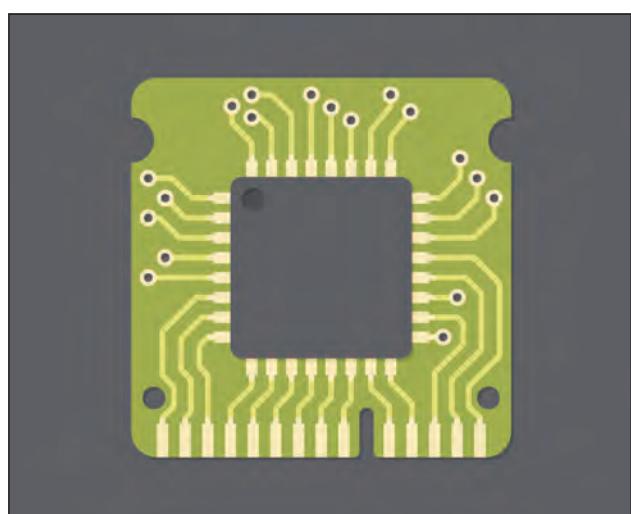


Image via iStock/Nik01ay. [Used under license.]

OVERVIEW

Although all RAM serves the same basic purpose, there are a number of different varieties. Each type has its own unique characteristics. The RAM most often used in personal computers (PCs) is a direct descendant of the DRAM invented by Dennard and popularized by companies such as Intel. DRAM is dynamic, meaning that the electrical charge in the memory cells, and thus the stored data, will fade if it is not refreshed often. A common variant of DRAM is speed-focused double data rate synchronous DRAM (DDR SDRAM), the fifth generation of which entered the market in 2020.

RAM that is not dynamic is known as static random-access memory (SRAM). SRAM chips contain many more transistors than their DRAM counterparts. They typically use six transistors per cell: two to control access to the cell and four to store a single bit of data. As such, they are much more costly to produce. A small amount of SRAM is often used in a computer's central processing unit (CPU), while DRAM performs the typical RAM functions.

Just as the majority of RAM is dynamic, most RAM is also volatile. Thus, the data stored in the RAM will disappear if it is no longer being supplied with electricity—for instance, if the computer in which it is installed has been turned off. Some RAM, however, can retain data even after losing power. Such RAM is known as nonvolatile random-access memory (NVRAM).

USING RAM

RAM works with a computer's other memory and storage components to enable the computer to run more quickly and efficiently, without lagging or freezing. Computer memory should not be confused with storage. Memory is where application data is processed and stored. Storage houses files and programs. It takes a computer longer to

access program data stored in ROM or in long-term storage than to access data stored in RAM. Thus, using RAM enables a computer to retrieve data and perform requested functions faster. To improve a computer's performance, particularly when running resource-intensive programs, a user may replace its RAM with a higher-capacity chip so the computer can store more data in its temporary memory.

SHADOW RAM

While RAM typically is used to manage data related to the applications in use, at times it can be used to assist in performing functions that do not usually involve RAM. Certain code, such as a computer's basic input/output system (BIOS), is typically stored within the computer's ROM. However, accessing data saved in ROM can be time consuming. Some computers can address this issue by copying data from the ROM and storing the copy in the RAM for ease of access. RAM that contains code copied from the ROM is known as shadow RAM.

—Joy Crelin

Further Reading

- Dieny, Bernard, Ronald B. Goldfarb, and Kyung-Jin Lee. *Introduction to Magnetic Random-Access Memory*. IEEE Press/John Wiley & Sons, 2017.
- Hey, Tony, and Gyuri Pápay. *The Computing Universe: A Journey through a Revolution*. Cambridge UP, 2015.
- McLoughlin, Ian. *Computer Systems: An Embedded Approach*. McGraw-Hill, 2018.
- “Media Arts, Design and Technology Computer Requirements.” *NC State College of Design*, May 2023, academics.design.ncsu.edu/it/docs/artdesign-computer-requirements.
- O’Leary, Timothy, Linda O’Leary, and Daniel O’Leary. *Computing Essentials 2023*. McGraw-Hill, 2022.
- Siddiqi, Muzaffer A. *Dynamic RAM: Technology Advancements*. CRC Press, 2013.
- “SK Hynix Launches World’s First DDR5 DRAM.” *HPC Wire*, 7 Oct. 2020, www.hpcwire.com/off-the-wire/sk-hynix-launches-worlds-first-ddr5-dram.

RANSOMWARE

ABSTRACT

Ransomware is a form of malicious software used by cybercriminals to hijack a user's computer or mobile device and keep it under their control until the user pays for its release. Cybercriminals use various strategies to try to extort money from unsuspecting users with ransomware, such as encrypting files saved on the user's device; threatening to erase important files; denying access to key programs and applications; and entrapping the user by linking him or her to extreme or illegal pornographic material. The user will then be instructed to submit some form of untraceable payment to the cybercriminals behind the ransomware attack, though antifraud authorities stress that making such a payment does not guarantee the release of the user's device.

BACKGROUND

The first known example of ransomware was launched by Dr. Joseph Popp, a Harvard-educated evolutionary biologist who distributed an estimated 20,000 virus-infected floppy disks to attendees of the World Health Organization's (WHO's) international acquired immunodeficiency syndrome (AIDS) conference in December 1989. Popp's program, known as the AIDS Trojan, used a technique known as "symmetric cryptography" to encrypt files after users loaded the infected disks into their computers. No reason was ever given for Popp's actions, though media reports stated that Popp had been rejected for a job with the WHO just prior to the attack.

A ransomware platform known as Archievus was one of the earliest such programs to be widely distributed over the internet. Archievus first appeared in 2006 and targeted Microsoft's Windows operating system by encrypting all the files saved in the infected computer's "My Documents" directory. To secure the release of their files, victims were instructed to purchase specific products in exchange for the decryption password.

Ransomware became more prevalent with the advent of anonymous internet-based payment-processing platforms, which made it easier for cyber-criminals to extract ransoms directly from their victims. Since 2011, there has been a sharp rise in the frequency and scale of ransomware attacks, as well as in the number of malicious programs used to infect victims' computers. One particularly noteworthy campaign began in 2014 with the launch of the CryptoDefense and CryptoWall ransomware platforms. These programs infected computers and encrypted victims' saved files, using anonymity network internet browsing and the untraceable Bitcoin cryptocurrency to secure payments. According to a 2015 report published by the Cyber Threat Alliance, the CryptoDefense and CryptoWall campaigns generated \$325 million in revenues for the criminal network behind the software.

Ransomware has since extended beyond personal computing to affect smartphones and other mobile devices. Smartphone-specific forms of ransomware initially locked users out of their phones but have evolved to encrypt files and folders saved on affected devices. Advancements in cloud computing technology have also led to the rise of a malware distribution strategy known as Ransomware as a Service, or RaaS. RaaS first appeared in 2015, enabling individuals to purchase ransomware platforms on digital black markets. Buyers could then distribute the malicious programs on their own, sharing a percentage of their revenues with the malware's anonymous vendors.

OVERVIEW

Ransomware programs use a range of techniques to extort payments from users, but most fall into two broad categories known as "lockscreen ransomware" and "encryption ransomware."

Lockscreen ransomware hijacks a user's device, displaying a full-screen message that cannot be closed, minimized, or otherwise removed. The



[Image via iStock/tupungato. [Used under license.]

full-screen message prevents a user from accessing files and programs on his or her device and may also use scare tactics, such as allegations that the device has been associated with illegal or extreme pornographic material, with an accompanying threat to report the activity to authorities. In other cases, ransomware appropriates the names and logos of local law enforcement agencies, claiming to represent the agency and demanding that the user submit payment to avoid fines or criminal prosecution for illegal online activity. A variant strategy sees the ransomware use sexually explicit images in the lockscreen message, claiming that the images cannot be removed unless the user complies with the criminal's demands.

Encryption ransomware targets specific files saved on the device, which the ransomware distributors often identify beforehand by employing phishing techniques to research the end user. Once the files are encrypted, the user will be instructed to submit payment in exchange for the decryption key. This

technique typically targets confidential, sensitive, or important information saved on the user's device and is a favored form of ransomware for attacking businesses.

According to a comprehensive report by Symantec Corporation, criminal networks using ransomware were becoming increasingly sophisticated and were displaying very high levels of expertise by the year 2016. The report stated that the average ransomware demand that year was \$679, representing a sharp year-over-year increase from 2015 demands, which averaged \$294. Symantec also reported that more than one hundred new ransomware families were identified in 2015.

Users usually unwittingly install ransomware on their own devices. Cybercriminals use various strategies to spread ransomware; it may be embedded in unsafe websites or installed on a user's computer after the user is redirected to a fake website designed to mirror a legitimate one. Email, social media, and personal communication platforms are

also used to distribute links that will install ransomware on a user's device if they are clicked.

While individual users continued to fall afoul of ransomware distributors throughout the second decade of the twenty-first century, that period also saw a growing trend toward the victimization of businesses. Attacks on businesses were usually targeted, and Symantec reported that 38 percent of ransomware infections in 2016 affected enterprises in the services sector. Manufacturing, finance, real estate, and public administration organizations were also leading targets of enterprise-oriented attacks during that period.

A major worldwide ransomware attack occurred in May 2017, using software known as WannaCry. This encryption program locked users out of many documents on their computers and demanded US\$300 in Bitcoin to restore access. Within days, more than 300,000 computers in over 150 countries were infected, with Europe and Asia seeing higher rates than the United States. Individuals and businesses were both targeted, and the impact on major companies led to travel delays and other serious consequences. Perhaps most notable was the targeting of the National Health Service (NHS) in Great Britain, with tens of thousands of NHS computers affected and many services disrupted.

The WannaCry software used a vulnerability in the Microsoft Windows operating system to infect computers. Not long after the spread of WannaCry died down, another ransomware program, NotPetya (derived from an older program known as Petya), spread by exploiting the same vulnerability. It was later revealed that the US National Security Agency (NSA) had previously discovered the vulnerability but exploited it for its own work rather than alerting Microsoft, creating a "backdoor" known as DoublePulsar to allow them to access computers running Windows. This backdoor was stolen by hackers in 2016 and is thought to have been used in the WannaCry attack. Microsoft eventually released

security updates to address this vulnerability. In addition, a computer security researcher discovered a section of the ransomware's code that was able to be used as a kill switch, effectively slowing down the rate at which WannaCry could spread.

In June 2018, McAfee, a company that produces antivirus software, reported that ransomware attacks were down 32 percent from the previous quarter, while cryptojacking—infected computers with malware that makes the target machine mine cryptocurrency (such as Bitcoin) that is then deposited into the attacker's cryptocurrency wallet—had increased by 300 percent. Some technology commentators theorized that this shift was the result of low-level criminals turning from ransomware to cryptojacking as a safer way of obtaining money; ransomware by definition involves the victim knowing they have been attacked, while cryptojacking often goes undetected. However, high-profile ransomware attacks continue to occur; for example, in 2018, the computer systems of the City of Atlanta were infected with the ransomware program SamSam, and in 2020, the University of California at San Francisco paid a ransom of more than \$1.1 million to the hacker group Netwalker after the group gained access to some of the university's computer systems. According to a 2023 report published by the company Malwarebytes, ransomware remained a major concern in the third decade of the twenty-first century, with nearly two thousand ransomware attacks having taken place between July of 2022 and June of the following year.

—Jim Greene

Further Reading

- Cabaj, Krzysztof, and Wojciech Mazurczyk. "Using Software-Defined Networking for Ransomware Mitigation: The Case of CryptoWall." *IEEE Network*, vol. 30, no. 6, 2016, pp. 14–20.
- Dossett, Julian. "A Timeline of the Biggest Ransomware Attacks." *CNET*, 15 Nov. 2021, www.cnet.com/personal-computing/security/a-timeline-of-the-biggest-ransomware-attacks/.

- finance/crypto/a-timeline-of-the-biggest-ransomware-attacks.
- Fiscutean, Andrada. "A History of Ransomware: The Motives and Methods behind Those Evolving Attacks." *CSO*, 27 July 2020, www.csoonline.com/article/569617/a-history-of-ransomware-the-motives-and-methods-behind-these-evolving-attacks.html.
- "Global Ransomware Attacks at an All-Time High, Shows Latest 2023 State of Ransomware Report." *Malwarebytes Labs*, 3 Aug. 2023, www.malwarebytes.com/blog/threat-intelligence/2023/08/global-ransomware-attacks-at-an-all-time-high-shows-latest-2023-state-of-ransomware-report.
- HHS Cybersecurity Program. "Ransomware Trends 2021." *US Department of Health and Human Services*, 3 June 2021, hhs.gov/sites/default/files/ransomware-trends-2021.pdf.
- Kharaz, Amin, et. al. "UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware." *USENIX: The Advanced Computing Systems Association*, 2016, www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_kharraz.pdf.
- Liska, Allan, and Timothy Gallo. *Ransomware: Defending Against Digital Extortion*. O'Reilly Media, 2016.
- "Ransomware and Businesses 2016." *Symantec Corporation*, 2016, conferences.law.stanford.edu/cyberday/wp-content/uploads/sites/10/2016/10/5cISTR2016_Ransomware_and_Businesses.pdf.
- Sobers, Rob. "Ransomware Statistics, Data, Trends, and Facts." *Varonis*, 6 Sept. 2023, www.varonis.com/blog/ransomware-statistics.
- Stobing, Chris. "Ransomware Is the New Hot Threat Everyone Is Talking About; What Do You Need to Know?" *Digital Trends*, 6 June 2015, www.digitaltrends.com/computing/what-is-ransomware-and-should-you-be-worried-about-it.
- "What Is Ransomware?" *Microsoft*, 24 Apr. 2023, www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx.
- Whittaker, Zack. "Atlanta, Hit by Ransomware Attack, Also Fell Victim to Leaked NSA Exploits." *ZDNet*, 27 Mar. 2018, www.zdnet.com/article/atlanta-hit-by-ransomware-attack-also-fell-victim-to-leaked-nsa-exploits.
- Woollaston, Victoria. "WannaCry Ransomware: What Is It and How to Protect Yourself." *Wired*, 22 May 2017, www.wired.co.uk/article/wannacry-ransomware-virus-patch.

RISK MANAGEMENT

ABSTRACT

The term "risk management" refers to the process of evaluating, classifying, and reducing risks to a level acceptable by stakeholders. In the field of cybersecurity, the risk-management process typically includes multiple forms of risk assessment and mitigation.

BACKGROUND

Organizations face risks from strategic, market, credit, operational, and financial exposure as well as man-made and natural disasters. These organization identify and mitigate these risks through active risk management. Risk management, which refers to the process of evaluating, classifying, and reducing risks to a level acceptable by stakeholders, is common practice in both the public and private sectors. Risk evaluation, classification, and management are undertaken for large and small projects and organizational decisions. Identifying and mitigating risk is the primary role of risk managers. The potential benefits of risk-management practices include the reduction of anticipated dead-weight bankruptcy costs, minimization of tax payments, and protection of optimal investment programs. The potential costs of risk-management practices include transaction costs and exacerbating corporate conflicts.

Corporations adopt risk-management strategies for the potential performance benefits as well as to satisfy increasingly stringent government regulations. In particular, the Sarbanes-Oxley Act, passed in 2002 in response to corporate auditing scandals, requires that corporations engage in risk assessment and risk auditing to monitor financial reporting and auditing processes. Section 404 of the Sarbanes-Oxley Act, which focuses on management's assessment of internal control over financial reporting, instructs corporations to conduct a top-down risk assessment to evaluate the corporation's

internal controls systems. Risk management has become a ubiquitous corporate practice.

Risk management is an outgrowth of insurance management. While corporate insurance dates back to 1878 when railroad interests began the practice of offering insurance to offset the inherent risk of railroad work, the practice of risk management did not emerge until the 1960s. The first corporation to explicitly implement risk-management practices was the Canadian firm Massey-Ferguson. In 1966, Massey-Ferguson hired a risk manager and developed an explicit policy statement on risk-management practices. The adoption of risk-management practices was slowed by the lack of professionals trained in risk-management strategies.

While risk management was practiced in the 1960s and 1970s by public and private organizations, corporate risk management was not widely adopted until the 1980s. The 1980s were characterized by increasing government regulations, a growing economy, and insurance crisis. The federal

government passed laws, such as the Occupational Safety and Health Act, the Environmental Protection Act, and Superfund legislation, which required corporate compliance. Corporations created new positions, such as risk manager, to address liability, safety, and environmental compliance issues. In addition, the business boom of the mid 1980s, characterized by an increase in production plants, business locations, operations and workers, required new types and larger amounts of insurance. Companies demanded more insurance options and coverage from their insurers and insurance companies balked at the demands. Companies struggled both with financing their increasing insurance needs and finding insurance policies that met the needs of their expanding businesses. Corporations increasingly hired risk managers to assess their risks and select the best insurance options for their expanding businesses.

Thus, as a result of increased government regulation and expanding businesses, the position of risk



Image via iStock/Muharrem huner. [Used under license.]

manager became common in large corporations in the 1980s and largely replaced the positions of insurance clerk, insurance buyer, and insurance manager. Risk manager, as a distinct occupation, functioned as in-house insurance expertise. Prior to in-house risk management, corporations relied on their insurance company's broker to inform the corporation of potential corporate risk and potential insurance options. The creation of risk-management divisions reduced potential conflicts of interest in the insurance industry by separating insurance purchasing decisions from insurance commissions. Risk managers tend to have strong relationships with insurance brokers and are responsible for negotiating broker commissions and fees. Corporations that do not wish to hire their own in-house risk managers have the option of hiring risk-management consultants. These outside advisers can be hired for discreet projects or periods of time and are generally less expensive than a full-time employee with benefits.

In the twenty-first century, risk management is an established profession supported by professional organizations and numerous higher education programs. For example, the American Risk and Insurance Association (ARIA), founded in 1932, supports the career development of risk management and insurance professionals. The association's goals also include "the expansion and improvement of academic instruction to students of risk management and insurance" (Hoyt, 2006). The association supports the Risk Theory Society, founded in 1963, to foster research of topics in risk theory and risk management. Risk-management career opportunities are being expanded and strengthened by the large number of colleges and universities offering risk-management majors and programs of study.

The following section describes the main risk-management strategies and approaches, including enterprise risk management (ERM), alternative risk transfer (ART), and differentiating corporate risks,

used in corporations. This section will serve as a foundation for later discussion of the issues surrounding the management of geopolitical risk.

A corporate risk-management strategy is generally a corporate-wide approach to business practice. The main methods and elements of risk-management strategy operate to integrate the risk-management approach into all levels of operation and the corporate culture itself. There are six main strategies or principles that characterize corporate risk management:

- Develop intimate company knowledge: Risk managers require intimate knowledge of corporate operations, goals, and missions to successfully evaluate risk exposures relating to all areas of the company.
- Align risk-management vision with that of the company: Risk managers are responsible for creating an integrated risk-management strategy that reflects and furthers the goals and values of the company.
- Identify and analyze the company's areas of risk: Risk managers develop successful risk-management strategies by analyzing and planning for potential losses vertically and horizontally across an organization.
- Balance financials and objectives: Risk managers are responsible for determining how much time, effort, and money is required to achieve a given objective. Risk managers use a balanced scorecard (BSC) methodology, a management tool that translates the strategy into operational terms, to connect internal and external processes with corporate cultural and financial objectives.
- Close the gaps with strategic initiatives: Risk managers should identify the gaps between where the company is in relation to their goals and objectives and their final goals and objectives. Risk managers, along with corporate management, are responsible for finding strategies

to close any existing gaps in corporate performance and achievement.

- Continual measurement and improvement after implementation: Risk managers are responsible for creating a risk-management system as well as evaluating and improving its performance. Risk managers use data capture and reporting to measure the effectiveness of risk-management initiatives.

Risk analysis is one of the first and most important steps in the risk-management process. Risk analysis involves risk evaluation and classification. Risk classification is performed in an effort to create or select effective, efficient, and feasible strategies for risk reduction and mitigation. Risk management works to transform unacceptable risks into acceptable risks within a normal range.

Different types of risks require different types of risk-management tools such as risk-based, precaution-based, and discourse-based approaches. Once the risk evaluation and risk classification are conducted, the proper risk-management tool can be chosen and applied to the problem or situation. The most common risk-management tools include ERM, ART, and risk differentiation.

ENTERPRISE RISK MANAGEMENT

During the first decade of the twenty-first century, economic and political events such as the September 11, 2001, terrorist attacks and the collapse of the Enron Corporation brought a new awareness of business risk and exposure to corporations around the world. In the years that followed, more businesses employed EMR to address this new awareness of corporate risk and vulnerability. This risk management refers to the holistic reconceptualization of corporate risk and loss management. It employs tools such as alternative risk financing tools, risk control, business process reengineering, and new corporate governance.

Enterprise risk management differs from traditional risk management in its wholistic, integrated, and centralized approach to managing risk. Traditional risk management, often referred to as the silo or stovepipe approach, focuses on a single category of risk or exposure. Enterprise risk management centralizes risk management under the control and oversight of a chief risk officer or risk committee. The chief risk officer or risk committee is responsible for identifying the amount of risk the corporation can tolerate and assessing mitigation tactics. Enterprise risk management prepares corporations for a wide range of problems caused by strategic, market, credit, operational, and financial exposure as well as man-made and natural disasters. These risks will be identified, quantified, and monitored through a holistic, portfolio-based management system.

The chief risk officer or the risk committee will ask the following questions as part of the enterprise risk-management process: Are our risk-management policies and structures clearly identified, communicated and endorsed by the board? Is the process for identifying and analyzing risk part of the organizational process? What is our risk culture? What is our risk appetite? With the answers to these questions in mind, enterprise risk managers proactively manage the strategic, operational, reputation, regulatory, and information risks across organizations. In the final analysis, factors and variables that influence the success of enterprise risk-management strategies include the following: visible board commitment; organizational infrastructure and managing processes; integrating existing practices into the risk-management framework; adopting the right kind and amount of risk; risk assessment of the activities of the board and strategic leadership; consensus swiftly on exposure, accountability, and action to control the risk; acknowledgement of risk/functional interdependencies; implementation of a common language and framework; and a

risk-based approach to organizational planning and strategy stages.

ALTERNATIVE RISK TRANSFERS

Corporations use ARTs to manage their own risk without involving outside insurers. Examples of ARTs include captives, risk-retention groups and pools, self-insurance, credit wraps, integrated risk programs, large deductible plans, catastrophe bonds, and weather derivatives. Alternative risk transfers were developed in the 1980s, when corporations were growing at a pace that insurance providers could not or would not sufficiently insure, and grew further post-September 11, 2001, when some insurers began to raise rates or refuse to insure the risks associated with terrorism and other high risks. Businesses have combined risk transfer and risk retention strategies to form the ART market. The most common alternative transfer mechanisms used today are self-insurance and captives.

Self-insurance, also referred to as self-funding, refers to a method of funding the claims of a benefit plan directly from the employer on an ongoing basis. Organizations choosing self-funding may be partially or fully self-funded. Organizations with a small number of employees, or those wanting greater control over the costs and services of benefit plans, may choose to self-finance their employee benefit plan. Small employers find that self-funded insurance offers both cost-savings and benefits flexibility. Variables that affect the effectiveness of self-funding include the average age of the employees, level of benefits, cash flow, multiple plan options, and multistate locations. The potential disadvantages of self-funded insurance are many. In particular, catastrophic situations, such as multiple employee sicknesses or deaths, may result in a significant financial burden for the company as it pays for medical bills and life insurance. Small companies may protect against a catastrophic scenario,

and share some of the insurance risk with an outside party, through the purchase of stop-loss insurance. Stop-loss insurance is a type of security coverage that small and mid-sized employers use to limit the actual claims liability to the employer. Ultimately, stop-loss insurance is the key for many companies to making self-financed benefit plans a feasible option. Stop-loss coverage transforms self-funding from a high-risk option to a moderate risk option that many small companies choose.

Captive insurance refers to a type of insurance company owned by the parent company that acts as a safety net by insuring or reinsuring the risks of that company. Captive insurers protect employees, and their dependents, against loss of earnings, or savings, due to illness or accidental injury, disability or death. Benefits covered by captive insurance include death benefits in lump sums; death benefits in dependents' pensions; personal accident benefits; short-term sickness benefits; long-term disability income benefits; medical and hospital expenses benefits; and retirement benefits. Organizations use captive insurance to lower the costs for many types of business insurance plans and to keep control of financial assets that would, in other financing situations, be funding the insurance costs. Captives offer numerous advantages including gaining control over both reserves and investment return; evening out rates for individual country operations; providing coverage not easily available in the commercial market; and improving health care costs by analyzing health related trends and offering managed care in place of increased rates. Captive insurers were first used in the mid-nineteenth century and have been used as a benefit risk-management tool ever since. Ultimately, risk transfer mechanisms are an expanding risk-financing option for corporations interested in maintaining complete control over their risk-management operations.

RISK DIFFERENTIATION

Risk management requires long-term strategic planning and analysis to achieve favorable insurance coverage terms and conditions. Risk managers must differentiate corporate risks to identify, evaluate, and mitigate each risk through a customized insurance package. Risk managers can differentiate their business' risks by providing as much information as possible to the insurer who then can outline the risk characteristics and risk-management tools. Risks can be differentiated through the following strategies: reducing loss; changing the company's risk profile; increasing risk transparency; and improving insurance policy terms and conditions. The potential benefits of risk differentiation include reliable access to capacity; an increase in stability, flexibility, and predictability; and access to better services from the firm's insurance provider.

GEOPOLITICAL RISK

Geopolitical risk—which refers to any peril that arises from geographic, historic, and societal variables related to international politics—is a concern for the majority of corporate risk managers. Examples of geopolitical risk include terrorism and cyberterrorism, regional nationalism, frequency of government changes, amount of violence in the country, number of armed insurrections, conflicts with other countries, inflation, balance of payments, deficits, surpluses, and the growth rate of the gross national product (GNP). The losses associated with geopolitical risks may be catastrophic for businesses. Risk managers assess and manage political risk through global strategies and organizational planning. These two approaches, global strategy and organizational planning, differ in scale. Global strategy is a macrolevel activity that actively tries to connect the proposed project to a firm's overall goals and objectives. Organizational planning is a microlevel activity that actively works to connect the proposed project with project-level goals, objectives, and tools.

Global strategy refers to the methods, approaches, and objectives developed by a business to increase competitive advantage in the market by increasing competitive scope worldwide. A global strategy allows a company to determine the real cost of capital for a foreign investment. The majority of global strategies involve a combination of trade and direct investment in foreign countries. Global strategy requires capital investment decisions. The investment decision-making process involves seven steps:

- Determine that the project meets the firm's strategic objectives.
- Compute the costs, revenue, and benefits of the project.
- Assess the risk associated with the project.
- Determine the cost of capital to be used in the evaluation.
- Conduct the evaluation analysis.
- Select or reject the project.
- Perform a follow-up evaluation and tracking on selected project.

Determining the true cost of capital required for a foreign project is crucial to the profit margin of the project. The appropriate cost of capital for an investment project is a function of the perceived risk of the investment. Country specific factors that influence perceived investment risk include political risk, interest rate differential, and tax rate differential. Country risk surveys and country ratings, produced by independent services, provide the information businesses use to measure geopolitical risk.

Political risk to a specific foreign investment is managed, in large part, through organizational planning. Organizational planning is conducted prior to final investment decisions. The preentry planning or preinvestment stage involves the following eight steps:

- Describe investment objectives.
- Assess company's knowledge and expertise related to proposed foreign investment.

- Integrate political risk assessment into global strategy.
- Identify opportunities that benefit company and avoid risk.
- Establish structure of operations.
- Development of strategy and contingency plans.
- Develop security plans for the protection or evacuation of employees.
- Choose insurance coverage.

Organizational planning occurs both within and outside of organizations. In-house centers gather, process, and disseminate information. Consulting firms also assess country, regional, and global political risk and monitor foreign political environments. When geopolitical risk assessment is completed, the information and knowledge gained through global strategizing and organizational planning allows managers to make informed decisions about the type, degree, and probability of political risk in a business scenario. With this information in mind, geopolitical risk managers may choose to mediate political risk through use of a geopolitical risk strategy such as adapting, politick, negotiating, withdrawing, or political risk insurance (PRI). Worldwide political upheaval has resulted in the demand for political risk insurance to protect businesses engaged in international business. Businesses obtain political risk insurance coverage during the initial stages of the project. Businesses pay a small commitment fee to the insurance underwriters and are guaranteed coverage often for the life of the project.

RISK MANAGEMENT AND CYBERSECURITY

In the twenty-first century, many of the risks an organization may face are related in some way to the security of that organization's computer systems. Cyberterrorism, cyberwarfare, hacktivism, and financially motivated hacking incidents can result in the loss of millions of dollars, and high-profile data

breaches can cost a business its reputation among consumers. Insufficient cybersecurity measures can likewise facilitate the theft of trade secrets and diminish a business's competitive advantage within its industry. In light of the severity of such security breaches, organizations seeking to reduce their cybersecurity risk may choose to follow a risk-management process such as that set forth in the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which provides guidance on the detection and mitigation of cybersecurity threats as well as best practices for responding to them.

CONCLUSION

Risk management provides numerous potential financial and organizational benefits to corporations and is, in some forms, required by the federal government. While once an extension of the insurance industry, risk management has grown into its own industry with its own tools and strategies. ERM promises to establish risk management as an even more central and necessary component of effective business strategy and practice.

—Simone I. Flynn

Further Reading

- Banham, R. "Enterprising Views of Risk Management." *Journal of Accountancy*, 1 June 2004, www.journalofaccountancy.com/issues/2004/jun/enterprisingviewsofriskmanagement.html.
- Brazeau, P. "Managing Your Costs by Differentiating Your Risks." *Canadian Underwriter*, vol. 74, 2007, pp. 36–38.
- Carbone, T., and D. Tippett. "Project Risk Management Using the Project Risk FMEA." *Engineering Management Journal*, vol. 16, no. 4, 2004, pp. 28–35.
- Coffin, B. "The I Word." *Risk Management*, vol. 54, 2007, pp. 4–5.
- "Cybersecurity Framework." NIST, 2023, www.nist.gov/cyberframework.
- Dugan, W. "Global Dangers." *Risk Management*, vol. 46, 1999, pp. 13–16.

- Ellul, A., and V. Yerramilli. "Stronger Risk Controls, Lower Risk: Evidence from U.S. Bank Holding Companies." *Journal of Finance*, vol. 68, no. 5, 2013, pp. 1757–803.
- Englehart, J. "A Historical Look at Risk Management." *Risk Management*, vol. 41, no. 3, 1994, pp. 65–72.
- Galvao, D. "Handling Global Political Risk." *Canadian Underwriter*, vol. 74, no. 3, 2007, pp. 46–47.
- Hoyt, Robert. "American Risk and Insurance Association (ARIA)." *Encyclopedia of Actuarial Science*. Wiley, 2006.
- Jorgensen, H. "Methods & Elements of a Solid Risk Management Strategy." *Risk Management*, vol. 52, 2005, pp. 53–54.
- Klinke, A., and O. Renn. "A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies." *Risk Analysis: An International Journal*, vol. 22, no. 6, 2002, pp. 1071–94.
- Krivkovich, A., and C. Levy. "Managing the People Side of Risk." *McKinsey & Company*, 1 May 2015, www.mckinsey.com/capabilities/risk-and-resilience/our-insights/managing-the-people-side-of-risk.
- Martinson, O. "Global Investments: Discover Your Real Cost of Capital—and Your Real Risk." *Journal of Corporate Accounting & Finance*, vol. 11, no. 6, 2000, pp. 23–28.
- Morales, R., and B. Kleiner. "New Development in Techniques for Analyzing Diversified Companies in Today's Global Environment." *Management Research News*, vol. 19, 1996, pp. 41–49.
- Pérez-González, F., and H. Yun. "Risk Management and Firm Value: Evidence from Weather Derivatives." *Journal of Finance*, vol. 68, no. 5, 2013, pp. 2143–76.
- Rose, J. "Promising Career Opportunities in Risk Management and Insurance." *Baylor Business Review*, vol. 18, pp. 10–11.
- Sharman, R. "Enterprise Risk Management—The KPMG Approach." *British Journal of Behavioral Management*, vol. 31, 2002, pp. 26–29.
- Strazewski, L. "Awareness of Risk Sparks Renewed Interest in ERM." *Rough Notes*, vol. 145, 2002, pp. 111–14.
- Tufano, P. "Agency Costs of Corporate Risk Management." *FM: The Journal of the Financial Management Association*, vol. 27, 1998, pp. 67–77.

RUSSIAN HACKING SCANDAL

ABSTRACT

A major issue that emerged during the presidential election campaign of 2016 and the early months of the administration of President Donald Trump in 2017 was the concern of hacking by Russian intelligence services of the computer systems at the Democratic National Committee (DNC) headquarters. During this period, Americans were often left bewildered by a Hydra-headed scandal replete with charges and countercharges, leaks of information, "unmasking," turmoil in the Trump administration, resignations and firings, and claims that Trump and his campaign staff colluded with the Russians to discredit his opponent, Hillary Clinton, and tip the election scales in his favor. Numerous investigations were conducted; witnesses were called to testify before congressional committees; social media was often alight with highly partisan rhetoric, including retorts from Trump himself; and consumers of political news were greeted seemingly every day with a new revelation or controversy. The issue of Russian hacking in American elections raised cybersecurity concerns, calling into question the integrity of election systems.

BACKGROUND

US officials had known for years that US political campaigns had been targeted by hackers. In 2008, Chinese hackers penetrated the computer systems of both Barack Obama and his opponent, John McCain. In 2012, foreign hackers attempted to gain access to the campaign networks of both Obama and his opponent that year, Mitt Romney. Suspicions that foreign intelligence services were rummaging around in the computer systems of both the Democrats and the Republicans and trying to interfere with the 2016 election process were raised in 2015, but it was not until March 2016 that these suspicions were confirmed by James Clapper, the Director of National Intelligence, at a cyberevent at the Bipartisan Policy Center in Washington, DC. At that point,

however, he declined to elaborate. On June 14, 2016, it was reported for the first time that in 2015 and again in 2016, Russian hackers had gained access to the Democratic National Committee's (DNC's) computer network and stolen opposition research on Trump.

Complicating matters were ongoing questions raised about Clinton's use of a private email server and what some observers regarded as her cavalier handling of classified and other sensitive materials on her electronic devices during her years as secretary of state in the Obama administration. The issue focused further attention on the United States' cybersecurity and the possible ease with which foreign governments and those bent on doing the nation harm could penetrate computer networks for ideological reasons or simply to cause

mischief. On July 5, 2016, however, Federal Bureau of Investigation (FBI) director James Comey held what many observers regarded as an extraordinary news conference in which he announced that no criminal charges would be filed against Clinton—while during the same news conference outlining actions on her part that contravened federal law as it pertained to classified information. He famously stated that “no reasonable prosecutor” would charge Clinton over her handling of emails, although on October 28, less than two weeks before the election, Comey made a bombshell announcement that the FBI was reopening its probe of Clinton's emails.

During this time, the Trump campaign often did not help itself, for just prior to the Republican National Convention in July 2016, the campaign

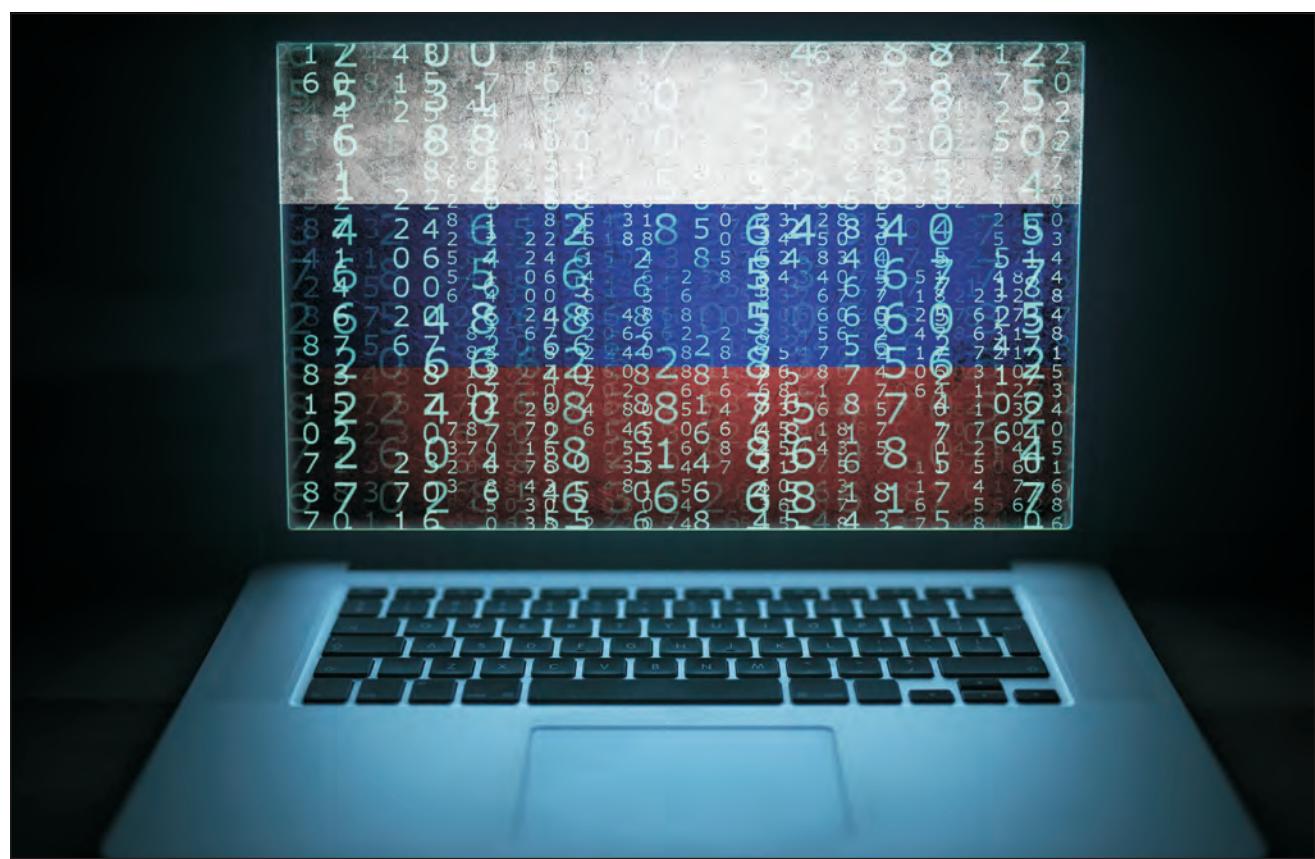


Photo via iStock/Smederevac. [Used under license.]

softened its stance against Russian intervention in Ukraine. This course correction contributed to a perception that Trump was going soft on Russia, and for some it was evidence that he was colluding with Russian president Vladimir Putin to damage the Clinton campaign. Later that summer, Trump stated that he believed it would be a good thing to get along with Russia, and what seemed to be his near admiration for Putin's authoritarian approach to governance confirmed the perception for some observers that he and Putin were in cahoots. Further complicating matters for the Trump campaign was that during the convention, Jeff Sessions, the former Alabama senator who would become Trump's attorney general, met with Russian ambassador Sergey Kislyak. Later, on September 8, Sessions again met with Kislyak in his Senate office. During his confirmation hearings for attorney general, however, Sessions would claim that he did not remember meeting with Kislyak. When it became undeniable that he had, he recused himself from any involvement in the investigation of Russian hacking.

Further revelations followed. Trump's campaign chairman, Paul Manafort, a political consultant and lobbyist, had had extensive business dealings with Viktor Yanukovych, the former leader of Ukraine who was backed by Russia, and Manafort later admitted that Yanukovych's political party paid him \$17 million in off-the-books funds as consulting fees. Manafort resigned as campaign chairman on August 19. Trump was also receiving campaign advice from Carter Page, an oil industry consultant who had extensive business dealings with Putin's allies and who was later questioned extensively by the FBI in its Russia probe. Similarly, lobbyist and political consultant Roger Stone, a longtime Trump friend and an informal campaign adviser, was also alleged to have ties to Russia. All of these associations led to suspicions that Trump may have been complicit in the hacking, or at least knew more than he was willing to say.

OVERVIEW

On July 21, 2016, the White House convened an interagency meeting on Russian hacking. Participants included the FBI, the Defense Department, and members of the intelligence community. The next day, on July 22, just days before the DNC, WikiLeaks—an organization that publishes secret and classified information, news leaks, and similar confidential materials—dumped online nearly 20,000 emails that were stolen from DNC computers. United States officials believed that the materials came to WikiLeaks through the agency of Russian hackers, although a Romanian hacker claimed responsibility, but the head of WikiLeaks, Julian Assange, claimed that there was no proof that the materials he received came from the Russians. The emails appeared to show coordinated efforts by the DNC to help Clinton at the expense of her rival for the Democratic nomination, Vermont senator Bernie Sanders, undermining Democratic Party claims that the nomination process was fair and open and thus potentially weakening Clinton's candidacy. Fallout from the WikiLeaks revelations led to the resignation of Debbie Wasserman Schultz, the chair of the DNC, on July 24, 2016, on the eve of the Democratic National Convention. The Clinton campaign, meanwhile, asserted that the leaks were part of a Russian effort to boost the Trump campaign. In late July, however, Clapper continued to state that US intelligence was uncertain who was behind the DNC hack.

In August 2016, President Obama received a highly confidential report from Central Intelligence Agency (CIA) director John Brennan. According to the report, a source inside the Russian government outlined the direct involvement of Vladimir Putin in efforts to discredit the American election process. The source also alleged that Putin issued specific instructions regarding the objectives of the hacking: to undermine the Democratic nominee, Clinton, and help get Trump elected. Russia, as might be

expected, denied the claims. Trump characterized the story as a distraction and suggested that the Democrats had concocted it to gain attention and to use it as a cudgel against him. In August, the Obama administration urged the intelligence community to assess United States' vulnerabilities and Russia's role and intentions, but the National Security Agency (NSA) was unwilling to confirm that Russia was the chief agent behind the hacking. In early September, however, it was reported that Clapper was heading an investigation by US intelligence into the scope of Russian interference in the election.

During the fall of 2016, as the election campaign heated up, frustration mounted on all sides. Democrats and Republicans seemed unable to cooperate in getting to the bottom of the matter. Trump continued to assert that the hacking scandal was fomented by the Democrats. Congressional representatives, particularly Republicans, were skeptical about the intelligence gathered on Russia. The White House seemed reluctant to forcefully call out Russia for its actions for fear of seeming to be interfering in the election. People were wondering whether Russia had information on Trump that they could use as blackmail. Finally, on October 7, 2016, Clapper and Homeland Security Secretary Jeh Johnson issued a joint statement formally blaming Russia for interfering in the United States election.

On November 8, Trump confounded expectations, pollsters, the news media, the Democratic Party, the White House, and even many Republicans by winning the presidential election. In the days following the election, he offered the position of attorney general to Jeff Sessions and that of national security advisor to retired Lieutenant General Michael Flynn. Sometime in early December, Flynn had a meeting with Ambassador Kislyak and Jared Kushner, a New York real estate developer with extensive Russian ties. The involvement of Kushner, Trump's son-in-law, added another layer of complication, for he functioned as a senior adviser to

Trump and was alleged to have failed to disclose his meetings with Russians on security clearance forms. Also in early December, the CIA arrived at the conclusion that Russia had interfered in the election specifically to help Trump, a conclusion seconded by the FBI on December 16. While Trump continued to dismiss the story, the Obama administration leveled new sanctions against Russia and expelled a number of Russian diplomats, including some with technical skills who were suspected of aiding the Russian operation from within the United States.

Finally, on January 6, 2017, the Office of the Director of National Intelligence (i.e., Clapper) released a declassified report that conclusively confirmed the positions of the CIA and the FBI: that Russia was behind the hacking and that the purpose of the operation was to discredit Clinton and help Trump. The report begins:

Russian efforts to influence the 2016 U.S. presidential election represent the most recent expression of Moscow's longstanding desire to undermine the US-led liberal democratic order, but these activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations. We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the U.S. presidential election. Russia's goals were to undermine public faith in the U.S. democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump. We have high confidence in these judgments.

That same day, FBI director James Comey met with President-elect Trump and informed him that he was not under investigation as part of the FBI's probe. But on May 9, 2017, Trump suddenly fired

Comey, purportedly for botching the investigation of Clinton's handling of classified information. Comey, though, would later testify that Trump repeatedly pressured him into denying that he, Trump, was under investigation in the hacking probe, and adding to the turmoil was the question of whether Trump had tape recordings of their conversations. In the wake of Comey's abrupt firing, on May 17, 2017, former FBI director Robert Mueller was appointed as special counsel to investigate whether Trump obstructed justice by trying to detour the FBI investigation but also to identify "any links and/or coordination between the Russian government and individuals associated with the campaign of President Donald Trump." Trump characterized the ongoing probe as a "witch hunt," suggesting that he knew that he himself was under investigation. Meanwhile, on February 13, Trump fired Flynn as his director of national intelligence for having lied to Vice President Mike Pence about his contacts with Russian officials.

Matters became even murkier on July 11, 2017, when the president's son Donald Trump Jr. released a chain of emails having to do with a meeting he had with a Russian official. The emails show that he knew that the Russian government intended to provide damning information about Hillary Clinton. The emails were from Rob Goldstone, a publicist who was friends with a Russian pop star, Emin Agalarov. Agalarov is the son of Aras Agalarov, a wealthy Russian oligarch who wanted to give the information to the Trump campaign. To that end, Goldstone arranged a meeting between Trump Jr. and an attorney representing the Russian government, Natalia Veselnitskaya. Shortly after the Republican convention in 2016, she met with Trump Jr., Jared Kushner, and Paul Manafort, who at the time of the meeting was the senior Trump's campaign manager. For some observers, this revelation provided further evidence of collusion between Trump and the Russians.

It should be noted that Russian intelligence was doing more than hacking computers. They were allegedly using "trolls" and "bots" to affect the US news cycle by artificially creating online surges in commentary. Further, Russia used propaganda outlets such as RT ("Russia Today"), a Russian English-language news channel, to influence debate in the United States by introducing themes into the minds of the American electorate, such as the view that the election was "rigged" against Trump. At home, the early months of the Trump administration were roiled by numerous anonymous leaks of confidential information that were ascribed to career government employees who were hostile to the Trump administration and wanted to undermine it. A term that was bandied about was "soft coup," a figure of speech referring to the notion that a cabal of career members of the intelligence and national-security establishments and holdovers from the Obama administration wanted to see Trump impeached, perhaps for collusion with the Russians, perhaps for obstruction of justice—or for both.

By the early summer of 2017, Americans were left with a number of unresolved questions. It was clear that Russia attempted to meddle in the election with a view to undermining its legitimacy and thereby weaken the United States, but it was less clear what the US government should do in response. It was also clear that the Russians did not hack the election itself. They were able to penetrate computers at party headquarters, but no evidence suggests that they tampered with any voting machines or procedures to manipulate vote totals. Further, no firm evidence had come to light that Trump colluded with the Russians.

Special counsel Robert S. Mueller III was appointed by Deputy Attorney General Rod J. Rosenstein in May 2017 to investigate Russian influence in the 2016 election. Two years later, Mueller submitted a confidential report on his findings to Attorney General William P. Barr, who then released

the findings to Congress: the investigation did not find sufficient evidence of Russian collaboration with Trump's campaign. Thus, the report was not enough for Barr to conclude that Trump had obstructed justice by trying to block the investigation in the first place. Nonetheless, the Senate Intelligence Committee continued to conduct investigations into election interference. In a report released in April of 2020, the committee expressed its agreement with intelligence officials regarding the events that had taken place, confirming that Russia had interfered in the 2016 election and had specifically sought to ensure Trump's election as president.

—Mark Grossman

Further Reading

- “2016 Presidential Campaign Hacking Fast Facts.” *CNN*, 23 Oct. 2023, www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html.
- “Assessing Russian Activities and Intentions in Recent US Elections.” *Office of the Director of National Intelligence*, 6 Jan. 2017, www.dni.gov/files/documents/ICA_2017_01.pdf.
- Dinan, Stephen. “FBI Reopens Clinton Email Investigation.” *Washington Times*, 28 October 2016, www.washingtontimes.com/news/2016/oct/28/james-comey-fbi-director-reopens-clinton-email-inv.
- Entous, Adam, Ellen Nakashima, and Greg Miller. “Secret CIA Assessment Says Russia Was Trying to Help Trump Win White House.” *Washington Post*, 9 December 2016, www.washingtonpost.com/world/national-security/obama-orders-review-of-russian-hacking-during-presidential-campaign/2016/12/09/31d6b300-be2a-11e6-94ac-3d324840106c_story.html?utm_term=.4fe64b5e2a5e.
- Federal Election Commission. “Official 2016 Presidential General Election Results.” *FEC*, 30 Jan. 2017, transition.fec.gov/pubrec/fe2016/2016presgeresults.pdf.
- Foer, Franklin, “Putin Is Well on His Way to Stealing the Next Election.” *The Atlantic*, June 2020, www.theatlantic.com/magazine/archive/2020/06/putin-american-democracy/610570.
- Gearan, Anne, Philip Rucker, and Abby Phillip. “DNC Chairwoman Will Resign in Aftermath of Committee Email Controversy.” *Washington Post*, 24 July 2016, www.washingtonpost.com/politics/hacked-emails-cast-doubt-on-hopes-for-party-unity-at-democratic-convention/2016/07/24/a446c260-51a9-11e6-b7de-dfe509430c39_story.html?utm_term=.ce78e21f0d9f.
- Gumbel, Andrew, “Why US Elections Remain ‘Dangerously Vulnerable’ to Cyber-Attacks.” *The Guardian*, 13 Aug. 2018, www.theguardian.com/us-news/2018/aug/13/us-election-cybersecurity-hacking-voting.
- Jalonick, Mary Clare, and Eric Tucker. “Senate Panel Backs Assessment That Russia Interfered in 2016.” *AP News*, 21 Apr. 2020, apnews.com/article/d094918c0421b872eac7dc4b16e613c7.
- Korte, Gregory. “The Many Tentacles of the Trump-Russia Probe.” *USA Today*, 18 June 2017, www.msn.com/en-us/news/politics/the-many-tentacles-of-the-trump-russia-probe/ar-BBCOtnL?li=BBnbcA1.
- Mazzetti, Mark, and Eric Lichtblau. “C.I.A. Judgment on Russia Built on Swell of Evidence.” *New York Times*, 12 Dec. 2016, www.nytimes.com/2016/12/11/us/politics/cia-judgment-intelligence-russia-hacking-evidence.html.
- Miller, Greg. “Trump’s Pick for National Security Adviser Brings Experience and Controversy.” *Washington Post*, 17 Nov. 2016, www.washingtonpost.com/world/national-security/trumps-pick-for-national-security-adviser-brings-experience-and-controversy/2016/11/17/0962eb88-ad08-11e6-8b45-f8e493f06fc_story.html?utm_term=.dea1837ab124.
- Miller, Greg, Ellen Nakashima, and Adam Entous. “Obama’s Secret Struggle to Punish Russia for Putin’s Election Assault.” *Washington Post*, 23 June 2017, www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking.
- Nakashima, Ellen. “National Intelligence Director: Hackers Have Targeted 2016 Presidential Campaigns.” *Washington Post*, 18 May 2016, www.washingtonpost.com/world/national-security/national-intelligence-director-hackers-have-tried-to-spy-on-2016-presidential-campaigns/2016/05/18/2b1745c0-1d0d-11e6-b6e0-c53b7ef63b45_story.html?tid=a_inl&utm_term=.135518fa2e97.
- Shear, Michael D. “How the White House Explains Waiting 18 Days to Fire Michael Flynn.” *New York Times*, 9 May 2017, www.nytimes.com/2017/05/09/us/politics/michael-flynn-russia.html?_r=0.
- Zapototsky, Matt, and Rosalind S. Helderman. “FBI Recommends No Criminal Charges in Clinton Email Probe.” *Washington Post*, 5 July 2016, www.washingtonpost.com/world/national-security/fbi-chief-plans-remarks-to-media-amid-heightened-focus-on-clinton-email-probe/2016/07/05/a53513c4-42b9-11e6-bc99-7d269f8719b1_story.html?utm_term=.c63e789a7af3.

S

SERVERS

ABSTRACT

Servers help users connect to networks, including the internet. The term “server” refers to any computer running a server program.

BACKGROUND

The Advanced Research Projects Agency Network (ARPANET), the first network of time-sharing computers, was connected in 1969. In subsequent decades, technology developments and the increasing benefits of distributed, shared access spurred network growth, ultimately resulting in the internet and World Wide Web (WWW). Most local, national, and global networks rely on servers, which manage network resources for client computers that are connected to it. A server may be a physical computer, a program, or a combination of hardware and software. In some cases, a system is a dedicated server. In other cases, software servers operate on multipurpose systems. A distributed server is a scalable grouping in which several computers act as one entity and share the work. In general, a network server manages overall network traffic, while specialty servers handle other tasks. European Organization for Nuclear Research (CERN) httpd (or W3C httpd), which debuted in 1990, is considered to be the first web server. It was developed by scientists Tim Berners-Lee, Ari Luotonen, and Henrik Frystyk Nielsen at CERN.

Servers and clients use communication protocols to exchange information to carry out tasks. There are server-to-server and client-server variations. Mathematicians, computer scientists, and others

work to create technology and algorithms that make servers possible and increase their efficiency. They also study the properties of networks and servers, which facilitates advances in both mathematics and computers. For example, in a system with multiple parallel servers, jobs may be assigned to any server. Often, jobs are modeled with an exponentially distributed processing time or some other probabilistic distribution with some resource cost per unit of time. Mathematical methods may be used to find the optimal strategy for allocating jobs to servers to minimize costs.

OVERVIEW

The term “server” does not describe a specific type of computer in the same sense that “desktop” or “Windows machine” does. When used in reference to hardware, a server is any computer running a server program, which can—and in practice does—include all configurations and operating systems. Since the 1990s and the increased demand for internet services, there have been more and more computers that have been designed specifically to be used as internet servers. Because they need to run for long periods of time without interruption, they must be durable, reliable, and have uninterruptible power supplies. Typically, hardware redundancy is incorporated, so that if a hard drive fails, another one is automatically put online—a feature rarely found in personal computers. There is also a great deal of server-specific hardware, such as water-cooling systems, which help reduce heat, and Error-Correcting Code (ECC) memory, which corrects memory errors as they happen, preventing data corruption. Many components are designed to be



The server room of a data processing and storage center. Photo via iStock/Andrey Semenov. [Used under license.]

hot-swappable, meaning that they can be replaced while the server runs—without needing to power it down. Furthermore, ordinary server operations including turning the power on or off can often be conducted remotely; for example, from a home computer. Some system operators maintain watch over multiple servers in multiple locations and physically visit the site only when necessary because of a crisis.

Sockets are the primary means by which network computers in a network communicate. They are the endpoints of the flow of interprocess communication (IPC) and provide application services. They are also the place where many security breaches take place. Mathematicians and computer scientists study the different socket types and their states to understand how they work and to improve function and security. Servers create sockets on start-up that are in listening state, waiting for contact to be made by client programs. For instance, a web browser, such as Firefox, is a client program used to access content from web servers. Most servers

connected to the internet use a protocol known as transmission control protocol (TCP), developed by computer scientists Vinton Cerf and Robert Kahn for ARPANET. An internet socket is referred to by its socket number, a unique integer that includes internet protocol (IP) address and socket number. Listening sockets using TCP are usually assigned the remote address 0.0.0.0 and the remote port number 0. TCP servers can serve multiple concurrent clients by creating what is called a “child process” associated with each client and establishing TCP connections between child processes and clients. Each connection uses a unique dedicated socket. Two communicating sockets—the local socket created by the server and the remote socket of the client—are called a “socket pair,” and their activity is referred to as a “TCP session.”

A common feature of web servers is server-side scripting, which allows web pages to be created in response to client activity. For instance, a search for a book on Amazon.com results in a unique search results page. Without this capacity, every possible

search would need to be conducted in anticipation of client needs.

—Bill Kte'pi

Further Reading

- Chevance, Rene. *Server Architectures: Multiprocessors, Clusters, Parallel Systems, Web Servers, and Storage Solutions*. Elsevier, 2005.
- Dshalalow, Jewgeni H. *Frontiers in Queueing Models and Applications in Science and Engineering*. CRC Press, 1997.
- Gray, Neil A. B. *Web Server Programming*. Wiley, 2003.
- O'Leary, Timothy, Linda O'Leary, and Daniel O'Leary. *Computing Essentials 2023*. McGraw-Hill, 2022.

SMART CITY

ABSTRACT

The term “smart city” is used in various ways and does not have a universally accepted definition. According to the European Smart Cities initiative, a smart city has six key “smart” features: smart economy, smart mobility, smart environment, smart people, smart living, and smart governance. In this context, “smart” refers to progressive, inclusive, sustainable, and forward-thinking policies that leverage technology, human capital, and social responsibility. In some cases, however, smart cities are also considered to be cities that make substantial use of information and communication technologies (ICTs)—potentially including Internet of Things (IoT) technologies—in their operations.

BACKGROUND

Trends in urban planning and development have contributed to the rise of the concept of the “smart city.” The term is used in various ways and does not have a universally accepted definition, but one widely cited conceptualization was developed by European Smart Cities, an initiative of the Vienna University of Technology in Austria. According to the European Smart Cities model, a smart city has six key smart features: smart economy, smart mobility, smart environment, smart people, smart living,

and smart governance. In this context, “smart” refers to progressive, inclusive, sustainable, and forward-thinking policies that leverage technology, human capital, and social responsibility.

Connectivity technologies play a major role in the ongoing move toward building smart cities. With the internet of things (IoT) continuing to develop at a rapid pace, technology is playing an increasingly prominent and essential role in the development of smart urban spaces. However, as the issue of data privacy became a matter of greater public concern at the end of the 2010s, some began asking how smart cities would handle their residents’ data, and who would own it.

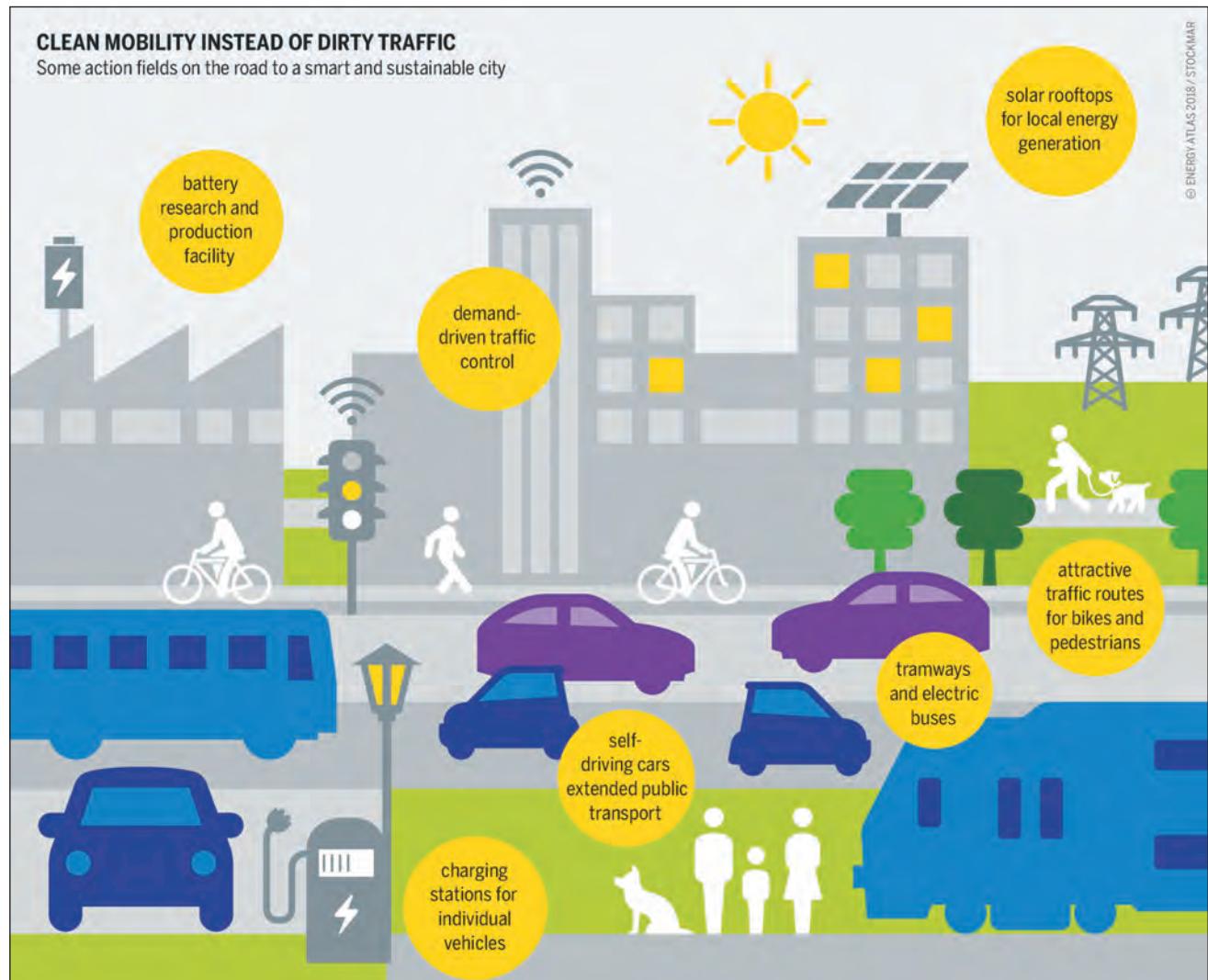
According to the World Bank, in 2022, 56 percent of the world’s population, 4.4 billion people, lived in cities, and this population was expected to double by 2050. In a related trend, European Smart Cities notes that globalization is driving economic changes with widespread impacts. Among other effects, globalization and increasing levels of urbanization are forcing cities in both developed and developing countries to explore new ways to remain competitive. Meanwhile, as technology continues to develop at an unprecedented rate, new applications that could positively affect urban life are emerging. Thus, while the smart city concept has been defined in many ways, the vast majority of theoretical models circle back to these two core principles: competitiveness and the transformative power of technology.

Cities that remain competitive tend to have stronger economies, lower unemployment rates, and offer a better overall quality of life than cities that lag behind. The ability to innovate also gives cities a competitive edge, which is why human and social capital investments are so important to the development of smart cities. Most smart city conceptualizations also focus on sustainability, with technology viewed as a core means of achieving this goal. Finally, some models emphasize the importance of civic participation in governance and the need for

city residents and businesses to make equitable use of available resources.

Sustainability has become a particularly pertinent issue. Governments around the world have become increasingly focused on minimizing the environmental toll of human activity, especially in urban areas. According to the United Nations (UN), cities consume about 78 percent of the world's energy, with higher levels of energy consumption and transportation-related pollution being associated with lower-density urban areas. Thus, increasing urban

population density and decreasing reliance on less efficient forms of transportation are salient topics in the smart city sphere. To boost urban population density, cities are looking to build "up" rather than "out" by building more mid-rise and high-rise residential buildings rather than continually expanding the reaches of suburbs and city limits. On the transportation front, smart cities look to decrease the use of single-occupancy vehicles by encouraging residents and commuters to explore the growing number of available alternatives.



Possible scenario of smart and sustainable mobility. Image by Bartz/Stockmar, via Wikimedia Commons.

OVERVIEW

It is possible to explore current and developing trends in modern urban planning using the six key “smart” features cited in the European Smart Cities model. From an economic standpoint, one of the features that differentiates smart cities is the implementation of mixed-use land development policies. Mixed-use land development designates specific urban spaces for various uses, including a blend of commercial, cultural, industrial, institutional, residential, and retail applications. One of the key advantages of mixed-use development is that it makes cities and neighborhoods far more walkable, which helps fight traffic congestion, improves community safety, and reduces pollution. Researchers and experts have also noted that information and communication technologies (ICTs) are influencing practically every aspect of contemporary urban economies, including changes in land use trends.

However, the mobility aspect of smart cities is the area in which ICTs are widely considered to have the greatest potential for positive change. Examples of smart mobility technologies include traffic light and traffic flow sensors that ease gridlock and congestion, especially during peak periods, and public transportation and parking apps that help users plan journeys using mass transit and spend less time searching for parking spots. These applications, along with the rising trends toward car-sharing and ride-sharing programs, as well as the development of self-driving vehicles, are expected to continue to improve and advance as IoT technologies proliferate in urban areas.

From an environmental standpoint, energy efficiency is one of the smart city’s primary goals. IoT technologies are poised to bring about major shifts in urban power generation and distribution strategies. According to one proposal, public and industrial buildings would supplement their use of grid-supplied electricity by generating their own using wind and solar power technologies to capture

energy and IoT applications to store excess electricity for later use. Internet-connected sensor networks would monitor individual and municipal power generation and distribution systems in real time, with some projections indicating that such initiatives could cut energy costs by 25 percent or more.

Beyond driving innovation, the inhabitants of a smart city have a major role to play in the ongoing effort to improve the quality of life for urban residents. The European Smart Cities model cites four key characteristics of smart city residents: educated, engaged in lifelong learning, multicultural, and open-minded. While these notions have drawn some criticism for being too abstract, they nevertheless reveal a possible path forward for cultivating a population base that is more civic oriented.

Living in a smart city has implications that extend beyond using ICTs to increase efficiency and accessibility. In designating cities as “smart,” European Smart Cities evaluates criteria including the presence of cultural facilities, leisure facilities, quality housing, and educational infrastructure. High levels of safety, security, and social cohesion are also considered favorable, and cities that make concerted efforts to improve these characteristics generate higher scores due to their strong associations with improved quality of life.

Finally, on the topic of governance, smart cities display high levels of cooperation between citizens and municipal officials and between residents and the local business community. Smart cities aim to share key resources to the greatest possible degree, and the European Smart Cities model cites social service availability, government transparency, and high levels of political awareness and public engagement as desirable elements.

A notable example of a smart-city initiative was a project launched in 2017 in Toronto by Sidewalk Labs, a subsidiary of Alphabet focused on urban innovation. Sidewalk Labs won a bid to develop a twelve-acre lot in Toronto’s East Bayfront

neighborhood into a project called Quayside, which would implement all the emerging smart-city technologies, including hyperefficient energy systems, sensor-embedded sidewalks and roads that respond to weather conditions and traffic flows, and autonomous transportation systems. A similar but larger project was launched by Microsoft founder Bill Gates in Arizona, where he and a group of investors planned to build a smart city called Belmont.

By the end of the 2010s, however, critiques of the smart city concept arose, in tandem with news stories about how big tech companies such as Facebook and Google—the same sorts of companies developing smart-city technology—had business models that were based on selling user data for profit. Critics such as science-fiction writer Bruce Sterling questioned whether smart cities would really result in greater sustainability, affordability, or equity, or whether they would merely reproduce or even exacerbate the traditional social inequities of large cities under a veneer of technological sophistication. Such concerns remained relevant throughout the early 2020s, during which cybersecurity experts also cautioned that the implementation of smart city technologies could leave cities vulnerable to cyberattacks. In 2023, the US Cybersecurity and Infrastructure Security Agency (CISA), along with several domestic and international partners, published *Cybersecurity Best Practices for Smart Cities*, a document in which the agencies offered guidance on the protection of cities' ICT infrastructure.

—Jim Greene

Further Reading

- Batty, M., et. al. "Smart Cities of the Future." *European Physical Journal: Special Topics*, vol. 214, no. 1, Nov. 2012, pp. 481–518.
- "Cybersecurity Best Practices for Smart Cities." CISA, 19 Apr. 2023, www.cisa.gov/sites/default/files/2023-04/cybersecurity-best-practices-for-smart-cities_508.pdf.
- "European Smart Cities." Vienna University of Technology, www.smart-cities.eu/?cid=-1&ver=4.

- Hornyak, Tim. "Why Japan Is Building Smart Cities from Scratch." *Nature*, 17 Aug. 2022, www.nature.com/articles/d41586-022-02218-5.
- IEEE Smart Cities*, 2023, smartcities.ieee.org.
- Macomber, John. "The Smart Way to Build Smart Cities." *Forbes*, 4 Apr. 2018, www.forbes.com/sites/hbsworkingknowledge/2018/04/04/the-smart-way-to-build-smart-cities.
- Sterling, Bruce. "Stop Saying 'Smart Cities.'" *The Atlantic*, 12 Feb. 2018, www.theatlantic.com/technology/archive/2018/02/stupid-cities/553052.
- Sukhdev, Ashima, and James Pennington. "4 Ways Smart Cities Will Make Our Lives Better." *World Economic Forum*, 10 Feb. 2016, www.weforum.org/agenda/2016/02/4-ways-smart-cities-will-make-our-lives-better.
- "Urban Development." *World Bank*, 3 Apr. 2023, www.worldbank.org/en/topic/urbandevelopment/overview.
- Vinod Kumar, T. M., editor. *Smart Economy in Smart Cities*. Springer Singapore, 2017.
- Zanella, A., et. al. "Internet of Things for Smart Cities." *IEEE Internet of Things Journal*, vol. 1, no. 1, 2014, pp. 22–32.

SOCIAL ENGINEERING

ABSTRACT

Social engineering, also known as "human hacking," refers to the art and technique of convincing people to release confidential information or engage in a course of action they may not necessarily choose for themselves. Often associated with security testing services, social engineering makes up a critical part of "red cell missions" in which security penetration testers attempt to gain access to confidential or proprietary information to better understand the limitations of established security techniques.

BACKGROUND

Criminals and con artists engage in social engineering, but this not to say that the practice concerns only those operating outside the law. While the term initially got its name from the activities of computer hackers attempting to influence people into



PROTECT YOUR INFO!
PSEC ALERT

What is social engineering?

Social engineering is the art of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud or computer system access; in most cases the attacker never comes face-to-face with the victim. Social engineering using impersonation (e.g. to gain information over the phone, or to gate-crash) is known informally as blagging. In addition to criminal purposes, social engineering has also been employed by debt collectors, skip tracers, private investigators, bounty hunters and tabloid journalists. A study by Google researchers found that up to 90 percent of all domains involved in distributing fake antivirus software used social engineering techniques.

| TROOPER TO TROOPER | THE WIRE | PAGE 3

OPSEC alert. Photo via Wikimedia Commons. [Public domain.]

divulging personal or confidential information about themselves or their company, it has evolved into much more than an illegal pursuit for profit. Social engineering is employed by a variety of people within the corporate and national security industries in order to make sure that personal and commercial data is kept safe.

OVERVIEW

The cornerstone of a successful social-engineering approach is the collection of intelligence. Intelligence consists of all the actionable information one can compile about the target of an attack in order to gain the highest likelihood of success. During the process of intelligence gathering, it may be impossible to tell what information may be actionable, so anything one can gather at this stage may later be useful. Intelligence can be gathered from a variety of sources, ranging from personal postings on the internet to rummaging through the target's trash. Once sufficient intelligence has been gathered, the target is approached either in person, by phone, or by email or another electronic method.

The best approach consists of developing a believable pretext in order to successfully use the

information gathered to ask questions and direct action. The type of pretext that is most successful is one that puts the target at ease in divulging information. Are you a fellow employee from another department? A new acquaintance at the bar who holds similar interests and views as the target? Someone from an institution with which they are familiar or highly respect? The answers to these questions depend greatly on the information gathered and how this allows the social engineer to craft questions and approaches that lead to the desired outcome.

While the concept of social engineering may seem to be far removed from the lives of most people, it is important to remember that everyone has engaged in, or been influenced by, the process of social engineering. While most people have not approached someone with the intended goal of obtaining confidential corporate information, everyone has at some point in his or her life used what they know about someone to gain information or shape the other's person's behavior. Equally important is to remember that anyone could potentially be the target of a social engineering attack regardless of how important they view their role within a particular business.

—Aaron Korora

Further Reading

- Bravo, Cesar, and Desilda Toska. *The Art of Social Engineering: Uncover the Secrets behind the Human Dynamics in Cybersecurity*. Packt, 2023.
- Conheady, Sharon. *Social Engineering in IT Security: Tools, Tactics, and Techniques*. McGraw, 2014.
- Contos, Brian T. *Enemy at the Water Cooler: True Stories of Insider Threats and Enterprise Security Management Countermeasures*. Syngress, 2007.
- Hadnagy, Christopher. *Social Engineering: The Science of Human Hacking*. 2nd ed., Wiley, 2018.
- Long, Johnny. *No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing*. Syngress, 2008.
- Mann, Ian. *Hacking the Human: Social Engineering Techniques and Security Countermeasures*. Gower, 2008.
- Mitnick, Kevin D., and William L. Simon. *The Art of Deception: Controlling the Human Element of Security*. Wiley, 2002.
- _____. *The Art of Intrusion: The Real Stories behind the Exploits of Hackers, Intruders, and Deceivers*. Wiley, 2006.
- Wiles, Jack, et al. *Low Tech Hacking: Street Smarts for Security Professionals*. Syngress, 2012.

SOFTWARE DEVELOPER/QUALITY ASSURANCE ANALYST/TESTER

ABSTRACT

Software developers design all types of computer software. Quality assurance analysts and testers test software to identify problems and assess its usability and security. Students aspiring to enter those professions should pursue studies in subjects such as computer science, programming, and engineering.

BACKGROUND

Software developers create the computer applications that allow users to do specific tasks and the underlying systems that run the devices or control networks. Software quality assurance analysts and testers design and execute software tests to identify problems and learn how the software works. Both of these functions are crucial in the development and

maintenance of complex technologies such as artificial intelligence (AI) systems, which require a high degree of knowledge and skill to program and evaluate.

OVERVIEW

Software development takes place in office settings and is a collaborative process, with teams of people performing various duties to create the finished whole. Software developers and quality assurance analysts and testers all have strong foundations in computer programming and coding, and they apply that knowledge and interest in creating new software programs in different aspects of the process.

Duties and responsibilities. Software developers, quality assurance analysts, and testers are involved in the entire process of creating a software program. Developers may begin by asking how the customer plans to use the software so that they can identify the core functionality the user needs. Software developers also determine other requirements, such as security. They design the program and then work closely with programmers, who write computer code. However, some developers write code themselves instead of giving instructions to programmers.

Software quality assurance analysts and testers design and execute systems to check the software for problems. As part of their testing, these workers document and track the software's potential defects or risks. They also assess its usability and functionality to identify difficulties a user might have. After completing testing, they report the results to software or web developers and review ways to solve any problems they found.

After the program is released to the customer, a developer may perform upgrades and maintenance. Quality assurance analysts and testers run manual and automated checks to look for errors and usability problems once the software is released and after any upgrades or maintenance.

Developers who supervise a software project from the planning stages through implementation sometimes are called information technology (IT) project managers. These workers monitor the project's progress to ensure that it meets deadlines, standards, and cost targets.

OCCUPATION SPECIALTIES

Applications software developers. Applications software developers design computer applications, such as games, for consumers. They may create custom software for a specific customer or commercial software to be sold to the general public. Some applications software developers create databases or programs for use internally or online.

Software engineers. Software engineers take a broad view of a project's system and software requirements,

planning its scope and order of work. These workers may direct software developers, quality assurance analysts, and testers.

Systems software developers. Systems software developers create operating systems for the public or specifically for an organization. These operating systems keep computers functioning and control most of the consumer electronics in use today, including those in cell phones and cars. Often, systems software developers also build the interface that allows users to interact with the computer.

WORK ENVIRONMENT

Physical environment. Developing software is usually a collaborative process. As a result, developers, quality assurance analysts, and testers work on teams with others who also contribute to

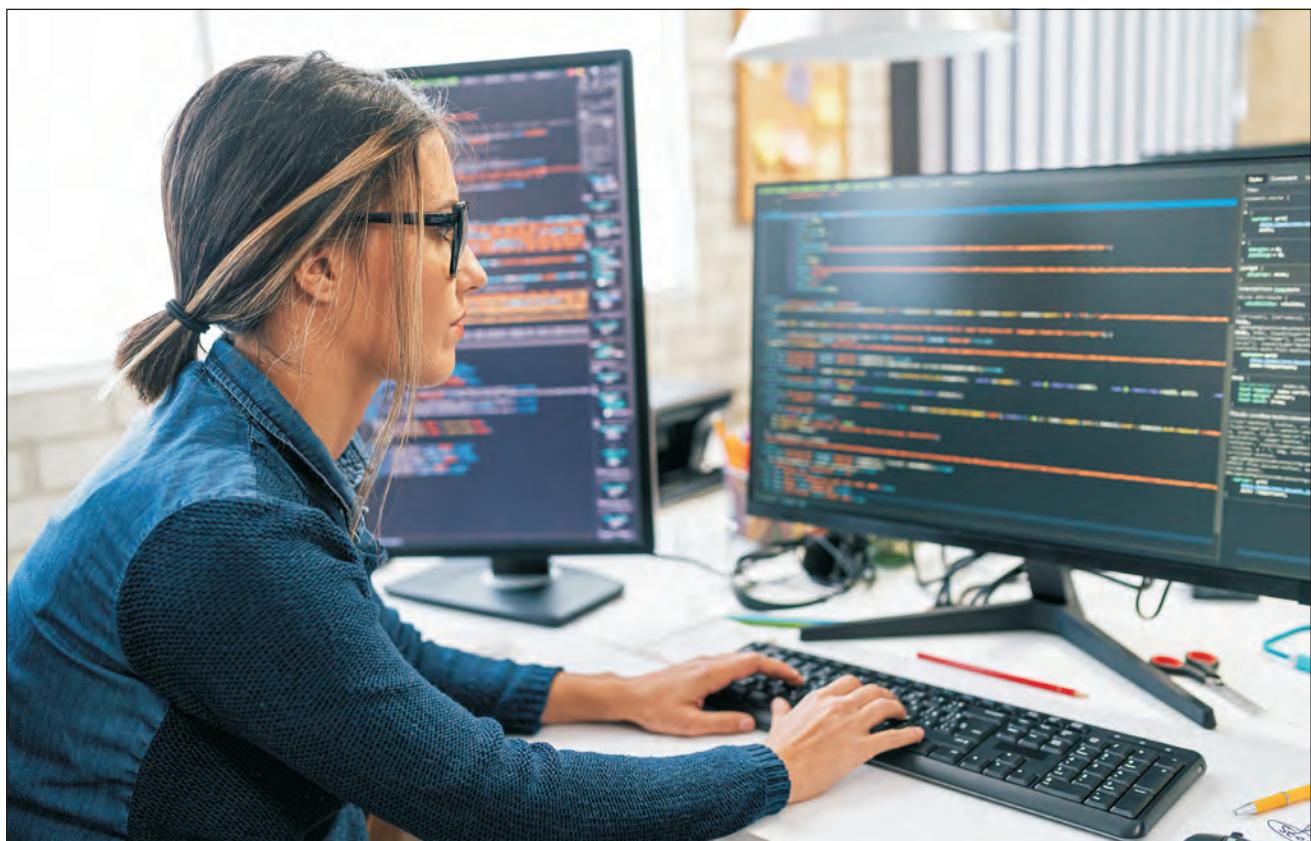


Photo via iStock/valentinrussanov. [Used under license.]

designing, developing, and programming successful software.

Most software developers, quality assurance analysts, and testers work full time.

Human environment. Software developers and quality assurance analysts and testers must be able to maintain their focus and work with others for long periods during the development phase and be meticulous about their testing during the end-phase and routine maintenance. Software is becoming ever more complex, and as these systems become more commonplace in everyday life, their safe operation is paramount. Developers and analysts must take direction from their clients and may report to more senior developers.

Technological environment. Software developers and quality assurance analysts and testers must be apprised of the latest developments in computer programming and software engineering in order to keep pace with trends, and the desires of their clients.

EDUCATION AND TRAINING

High school/secondary. High school students interested in becoming software developers or quality assurance analysts or testers should concentrate on computer science, math, and other science-related courses, as well as participating in after-school computer activities to hone their skills. They should plan on attending college or university to further their knowledge of programming and software development.

College/postsecondary. Software developers, quality assurance analysts, and testers typically need a bachelor's degree in computer and IT or a related field, such as engineering or mathematics. Computer and IT degree programs cover a broad range of topics. Students may gain experience in software development by completing an internship, such as at a software company, while in college. For some software developer positions, employers may prefer that applicants have a master's degree.

Although writing code is not their primary responsibility, developers must have a strong background in computer programming. They usually gain this experience in school. Throughout their career, developers must keep up to date on new tools and computer languages.

Adult job seekers. Adults from related fields such as software engineering may be able to transition into development or analysis, however extensive coursework and practical experience may be required in order to gain familiarity with the coding and programming needed to perform the duties in this area.

—Stuart Paterson

Further Reading

Helfrich, James N. *Security for Software Engineers*. CRC Press, 2019.

"QA and Cybersecurity." *QANTUM*, 21 Jan. 2020, quantum.medium.com/qa-and-cybersecurity-fa1968cd728c.

Stewart, Andrew J. *A Vulnerable System: The History of Information Security in the Computer Age*. Cornell UP, 2021.

SPAM

ABSTRACT

Spam is a general term for an abuse of email technology to transmit a large amount of unsolicited junk email in bulk, often for commercial reasons. Spam is often sent by "botnets," networks of virus-infected computers, and this hinders the prosecution of spammers. The prevalence of spam led to the development of legislation such as the United States' Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM) of 2003.

BACKGROUND

For computer users, spam can be annoying. Spam is often used to send fraudulent offers or to disseminate malicious software such as viruses. Spammers



The screenshot shows an email inbox with a search bar at the top left and a status filter at the top right set to "Any Status". The inbox lists numerous messages, mostly from spammers, with columns for Subject, Sender, and Date. The subjects include various spam offers like "check this out man...", "Help me!", "Have Arthritis pains? There is help for you.", and "We need to render the delight of having the finest". The senders are mostly generic names or random email addresses. The dates range from 2001 to 2005.

| Subject | Sender | Date |
|--|-------------------------|--------------------|
| check this out man... | Nelda Romano | Thursday 14:59:37 |
| Help me! | Osvaldo MANNING | Thursday 12:47:59 |
| Have Arthritis pains? There is help for you. | Orsa | Thursday 03:45:36 |
| down on her, and | Reginald Stubbs | Wednesday 06:02:05 |
| natural enlargement | diane george | Tuesday 16:37:15 |
| No Subject | fabian dickhaut | Monday 10:38:59 |
| only Youngest have Shocking sexuality other | Kristie Sapp | Monday 01:07:32 |
| Reduces stress | frankie kim | 06.02.2005 16:27 |
| PERSONAL | esnol2005 | 06.02.2005 04:56 |
| We need to render the delight of having the finest | Clotilda Gadnumqt | 06.02.2005 02:10 |
| Find more savings online | kennith draper | 05.02.2005 22:30 |
| faster cheaper meds | Lidia White | 05.02.2005 16:37 |
| Breaking News | Dee H. Edwardsd | 05.02.2005 14:40 |
| We have your wanted meds at low prices only. | lucien hyatt | 04.02.2005 06:59 |
| 100% zum einladen_1679438 | Isel Rios | 03.02.2005 03:34 |
| Enjoy your wanted meds. | tracey uliano | 03.02.2005 02:28 |
| Confirm Your Washington Mutual Online Banking | Washington Mutual On... | 02.02.2005 22:03 |
| out PINNACLE SYSTEM, MACROMEDIA, SYMANTEC, PC GAMES, ... | Valerie Ileen | 02.02.2005 19:11 |
| Finished | Cecilia Fuller | 02.02.2005 05:57 |
| You can save more thru ordering meds on our site. | mel sevick | 02.02.2005 01:21 |
| The most insane action | Katrina Souza | 31.01.2005 08:19 |
| You don't have to be fat Noel | Kristin | 28.01.2005 03:22 |

An email inbox containing a large amount of spam messages. Image by Ascánder, via Wikimedia Commons.

harvest and compile bulk listings of email addresses through automated scanning of popularly used websites or by intercepting the transmission of electronic mailing lists.

What is now known as spam (sometimes referred to as SPAM) has existed since the mid-1970s. It originated as postings to newsgroups, evolved into advertisements and solicitations, and soon got out of hand, with individual members receiving numerous unwanted emails. With the rapid expansion of the internet during the 1990s, the problem of unsolicited email began to grow exponentially. By 2005, most internet email users were receiving dozens—sometimes even hundreds—of pieces of spam every day. The origin of the term “spam” is said to come from a 1970 Monty Python’s Flying Circus comedy troupe skit about an American diner that included SPAM, the canned meat, in each of its breakfast offerings, often in multiple helpings, each mentioned separately. Then the group broke into song

with the repetitive lyrics: “SPAM, SPAM, SPAM, SPAM, SPAM, SPAM, SPAM, SPAM, lovely SPAM! Wonderful SPAM!”

Spam messages include legal and illegal solicitations of all kinds, running from advertisements—including a large proportion of pornographic advertisements—to chain letters and jokes. Volume is not the only problem that spam presents to computer users. Many spam messages contain computer viruses and worms that can inflict serious damage on the computers receiving the unwanted messages. The annoyance that spam causes computer users is difficult to exaggerate. In addition to offending users with unwanted solicitations, spam forces users to spend time and resources filtering and removing spam, while increasing their anxieties about the safety and security of their computers.

During the 1990s, increasing numbers of lawsuits were being filed against the purveyors of spam, known as spammers, in state and federal

courts—primarily under fraud statutes. The Coalition Against Unsolicited Commercial E-mail (CAUCE) was one of a number of groups that lobbied for criminalizing spam in the United States and Europe. During the 2003–4 session of the US Congress, at least six pieces of legislation designed to regulate spam were introduced. By the year 2005, no blanket national law made spam illegal, but by then as many as twenty-one states had passed, or were then considering, laws to criminalize spam.

OVERVIEW

One problem with criminalizing spam is the fact that much of it falls under laws protecting legitimate commerce and trade. The state of California found a way around this problem by enacting a law requiring that spam messages be labeled as advertising and that they offer ways for recipients to have their names removed from mailing lists. The California law was upheld by an appeals court as constitutional.

Existing federal and state laws protect citizens from fraud and illegal pornography. The Federal Trade Commission (FTC), the Federal Bureau of Investigation (FBI), the Internet Crime Complaint Center (IC3), and the National White Collar Crime Center (NW3C) may all investigate complaints concerning spam. However, spam messages are difficult to trace back to their senders. Moreover, even when the senders are identified, they are rarely prosecuted or sued unless criminal activity and criminal intent can clearly be demonstrated.

In 1979, the US Supreme Court recognized an individual's "right to be let alone" and held that a mailer's right to communicate ends at the mailbox of an uninterested addressee. The law was challenged but was held to be constitutional similar to the laws that prohibited sexually explicit mailings on free speech grounds. The Court pointed to the necessity that the "right to be let alone" must balance with the right of others to communicate: "Individual autonomy must survive to permit every

householder to exercise control over unwanted mail." Accordingly, the statute served to protect individuals' privacy and passed constitutional muster. The Court stated: "In effect, Congress allows each citizen to erect a wall that no advertiser may penetrate without his acquiescence.... Nor should the householder have to risk that offensive material come into the hands of children before it can be stopped."

Similarly, the right of spammers to solicit others must end at the outer edge of each individual's private home. The sanctuary of the home in this case includes the mailbox *and* an email inbox, both are meant to send and receive communications. Individuals maintain a higher expectation of privacy in email addresses. Email addresses maintain anonymity and are not a matter of public record. Each recipient must have a password to access an inbox, just as one must have a key to enter a residence. Thus, an inbox must be considered part of the home and enjoy at least the same protected status as the mailbox. It follows that no one has the right to impose ideas on unwilling recipients in the sanctuary of his or her email inbox. Spammers do not have a fundamental right to send unsolicited commercial emails to individuals' inboxes. Consequently, spam encroaches upon the personal space of individuals and violates their "right to be let alone," their right to be free from objectionable intrusion, and their right to privacy.

Spam invades the privacy of email recipients by sending objectionable content to them, whether or not they want this type of material. Spam imposes significant costs on email users. By the first decade of the twenty-first century, spam cost both individuals and businesses a considerable amount of time and money. Both the privacy and cost issues contributed to demands that spam be curtailed, including by federal legislation.

Congress recognized the importance of email and the harms caused by spammers. To shift the costs of

advertising to the spammer and to enhance the privacy of email users, Congress enacted the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003. The statute became effective January 1, 2004. Finding that many spammers purposely mislead recipients and often conceal their identity, Congress justified the statute, asserting that there is a substantial government interest in regulating commercial email on a national level, spammers should not mislead recipients about the source or content of electronic messages, and recipients of commercial email have the right to decline additional spam messages. To enforce this statute, the FTC promulgated and enforced protocols for the commercial use of bulk email.

The statute prohibits predatory and abusive commercial email. The law penalizes those who knowingly engage in one or more of the following behaviors: (1) accessing a protected computer without authorization and intentionally initiating the transmission of multiple commercial email messages through that computer; (2) sending several multiple commercial email messages with the intent to deceive or mislead recipients, or any internet access service, as to the origin of such messages; (3) materially falsifying header information in several commercial emails and intentionally initiating the transmission of such messages; (4) registering for five or more email accounts or online user accounts or two or more domain names using false identification and intentionally sending spam from such accounts or domain names; and (5) falsely representing oneself to be the registrant of five or more internet protocol addresses and intentionally initiating the transmission of spam. Individuals participating in these activities could be imprisoned for up to five years and be liable for a maximum of \$6 million in fines.

The statute's opt-out provision requires commercial email messages to include a functioning return email address that a recipient may use to opt out of

future spam from the sender. The email address provided must remain active for at least thirty days after the original message was transmitted. Once a consumer effectively chooses to opt out of future email messages, the sender must respect the decision. After this point, it would be unlawful for the initial sender or anyone acting on such person's behalf to transmit, or to assist in the transmission of, a commercial email message upon the expiration of ten business days after the receipt of the opt-out notice. The initial sender and any person with knowledge of the opt-out request must refrain from selling, leasing, exchanging, or transferring the recipient's email address. Also, commercial email messages must provide clear and conspicuous identification that the message is an advertisement or solicitation, notice of the opportunity to decline to receive further messages, and a valid physical postal address for the sender.

The CAN-SPAM statute also prohibits harvesting and dictionary attacks and requires individuals to place warning labels on commercial emails with sexually oriented material. Email messages containing sexually explicit content must include in the subject line the marks or notices prescribed by the FTC. Such messages must further ensure that the message, when initially opened, contains only the content required by the opt-out provision and instructions on how to access the sexually explicit material, unless the sender receives the prior affirmative consent of the recipient. An individual in violation of this provision can face up to five years in jail and/or fines.

This legislative action enjoyed rare overwhelming bipartisan support. This support indicated a substantial legislative commitment to the spam issue and understanding of the severity of this problem. The act was a significant step forward in supporting the individual's "right to be let alone" in balancing privacy with free speech rights. The CAN-SPAM Act served to deter spammers from

sending fraudulent or misleading email messages, from concealing their identity, and from using intrusive methods to collect email addresses. Email users would be able to identify spam messages as advertisements generally and as pornographic messages specifically due to the provisions of the act. The CAN-SPAM Act has had a valuable role in initiating legislative action, which would restrict spam, increase the privacy of the email inboxes of Americans, and relieve Americans from the financial burdens of unwanted advertising.

Despite the promise of the law, some observers argue that the statute was not effective enough in fighting spam. These critics believe that spam needs to be subject to further restriction through a combination of market-based initiatives and additional restrictive statutes and regulations. Some critics also warned that the CAN-SPAM Act would actually increase the volume of spam in the United States. The fear was that by signaling to the world that spam is legal in the United States, it might prompt foreign spammers to send more messages than ever. Also, requiring recipients to read unwanted emails to opt out was considered unfair.

OPTING IN/OPTING OUT

The spam law debate shifted into a controversy over two conflicting approaches: the opt-in and the opt-out mechanisms. The opt-in approach requires that all spammers obtain express permission before transmitting any email addresses. The more lenient opt-out approach allows spammers to send messages as long as each message offers a legitimate link from which one can request that the spammer refrain from sending future emails. Congress favored the opt-out approach because it allowed marketers and businesses the most leeway to conduct their work.

The opt-out method of regulation has failed, however, to protect individual privacy fully. It continues to allow uninvited and unwelcome messages to individual inboxes in homes and businesses. Under

current law, to halt unwanted email, individual users must take an affirmative step against each piece of unwanted mail; such a move wastes more time and money than the underlying problem. By implementing the opt-out approach, Congress developed a method that imposed additional costs on individuals because it is a competitive, repetitive, and labor-intensive method to oppose spam.

In terms of privacy, the opt-in approach protects consumers to a significantly greater degree and in a more effective manner. The opt-in approach prohibits unsolicited intrusions and requires that spammers send invited messages only. Like a vaccine prevents a disease, the opt-in approach stops the widespread dissemination of spam. Rather than imposing the costs of the remedy on all email users for each uninvited message like the opt-out approach, the opt-in approach imposes costs on spammers and those interested in receiving spam. In other words, it shifts the burden of sending spam onto spammers. Spammers must ask permission to enter an inbox instead of entering and then being asked to leave. The opt-in approach would ultimately serve to reduce the enormous volume of spam clogging networks and flooding the email system, and it would halt the widespread waste of time and money directed at eliminating spam.

IMPACT

Most spam sent following the passage of the CAN-SPAM Act remains illegal. Nothing in the law will stop illegal spammers from sending spam. The general consensus toward fighting spam seems to be on the side of private sector response. Individual computer users should use devices such as firewalls and antivirus programs to protect their computers from invasive email threats; users can also set up filters within their email to detect and divert spam to a specific folder so that it does not clutter their inbox. Internet service providers are developing “black hole” technologies to help prevent spam from

reaching subscribers. These are seen as more effective than additional layers of legislation.

According to the National Conference of State Legislatures, as of 2015, thirty-seven states had instituted laws designed to regulate spam. However, according to research, as of 2016, there were still billions of spam emails sent daily. Additionally, while traditional methods of bulk spamming are typically detected by antispam software and filters, some spammers have come up with more creative ways of fooling these common levels of protection. Referred to in the technology world as “snowshoe spamming,” this technique, which has been used increasingly in the 2010s and is harder to detect, involves distributing the unsolicited advertising over several different IP addresses in lower volumes over a longer period of time.

Spam remained a common annoyance into the 2020s, although the percentage of email traffic made up of spam had decreased substantially over the preceding decade. According to a 2023 report published by the statistics platform Statista, spam made up 80.26 percent of all emails in 2011. By 2022, however, that number had decreased to 48.63 percent.

—Donald R. Dixon, Gretchen Nobahar

Further Reading

- Beales, J. Howard. *Legislative Efforts to Combat Spam: Joint Hearing before...108th Congress, 1st Session, July 9, 2003*. US Government Printing Office, 2003.
- “CAN-SPAM.” FCC, 13 Aug. 2021, www.fcc.gov/general/can-spam.
- Clifford, Ralph D., editor. *Cybercrime: The Investigation, Prosecution, and Defense of a Computer-Related Crime*. Carolina Academic Press, 2001.
- The Criminal Spam Act of 2003: Report (to Accompany S. 1293)*. US Government Printing Office, 2003.
- Feinstein, Ken. *Fight Spam, Viruses, Pop-Ups and Spyware (How to Do Everything)*. McGraw-Hill, 2004.
- Garfinkel, Simson, and Gene Spafford. *Web Security, Privacy & Commerce*. 2nd ed., O'Reilly Media, 2011.
- Gelman, Robert B., and Stanton McCandlish. *Protecting Yourself Online: The Definitive Resource on Safety, Freedom, and Privacy in Cyberspace*. HarperEdge, 1998.

- Himma, Kenneth Einar. *The Handbook of Information and Computer Ethics*. Wiley, 2008.
- Jasper, Margaret C. *The Law of Obscenity and Pornography*. 2nd ed., Oceana, 2009.
- Jenkins, Simms. *The Truth about Email Marketing*. FT Press, 2009.
- Manishin, Glenn B. *Complying with the CAN-SPAM Act and Other Critical Business Issues: Staying Out of Trouble*. Practicing Law Institute, 2004.
- Petrosyan, Ani. “Spam: Share of Global Email Traffic 2011–2022.” *Statista*, Feb. 2023, www.statista.com/statistics/420400/spam-email-traffic-share-annual.
- Reduction in Distribution of Spam Act of 2003: Hearing before the Subcommittee on Crime, Terrorism, and Homeland Security of the Committee on the Judiciary, House of Representatives, One Hundred Eighth Congress, First Session, on H.R. 2214, July 8, 2003*. US Government Printing Office, 2003.
- Schwabach, Aaron. *Internet and the Law: Technology, Society, and Compromises*. ABC-CLIO, 2006.
- Smith, Marcia S. “*Junk E-mail*: An Overview of Issues and Legislation concerning Unsolicited Commercial Electronic Mail (“Spam””). Congressional Research Service, Library of Congress, 2001.

SPAM FILTERS

ABSTRACT

Spam filters are computer programs that screen email messages as they are received. Any email suspected to be spam will be redirected to a junk mail folder so that it does not clutter up a user's inbox. How does the filter decide which messages are suspect? Spam filters are implementations of statistical models that predict the probability that a message is spam given its characteristics. The filter classifies messages with large predicted probabilities of being spam as spam.

BACKGROUND

Spam is an electronic version of junk mail and has been around since the introduction of the internet. The senders of spam (called “spammers”) are usually attempting to sell products or services.

Sometimes, their intent is more sinister—they may be trying to defraud their message recipients. Since the cost of sending spam is negligible to spammers, it has been bombarding email servers at a tremendous rate. Some estimate that as much as 40 to 50 percent of all emails are spam. The cost to the message recipients and businesses can be considerable in terms of decreased productivity and unwelcome exposure to inappropriate content and scams. As frustrating and potentially damaging as spam email is, fortunately, much of it does not reach recipients thanks to spam filters.

Primitive filters designed to catch up to spammers who had perfected an early version of their craft simply classified a message as spam if it contained a word or phrase that frequently appeared in spam messages. However, spammers only need to adjust their messages slightly to outsmart the filter, and all legitimate messages containing these words would automatically be classified as spam.

OVERVIEW

Modern spam filters are designed using a branch of statistics known as classification. Bayesian filtering is a particularly effective probability modeling approach in the war on spam. Bayesian methods are named for eighteenth-century mathematician and minister Thomas Bayes. He formulated Bayes's theorem, which relates the conditional probability of two events, A and B, such that one can find both the probability of A given that one already knows B (e.g., the probability that a specific word occurs in the text of an email given that the email is known to be spam); the reverse, the probability of B given that one knows A (e.g., the probability that an email is spam given that a specific word is known to appear in the text of the email).

The underlying logic for this type of filter is that if a combination of message features occurs more or less often in spam than in legitimate messages, then it would be reasonable to suspect a message



Image via iStock/THANIT SEEPRASET. [Used under license.]

with these features as being or not being spam. An extensive collection of email messages is used to build a prediction model via data analysis. The data consist of a comprehensive collection of message characteristics, some of which may include the number of capital letters in the subject line, the number of special characters (e.g., \$, *, !) in the message, the number of occurrences of the word “free,” the length of the message, the presence of html in the body of the message, and the specific words in the subject line and body of the message. Each of these messages will also have the true spam classification recorded. These email messages are split into a large training set and a test set. The filter will first be developed using the training set, and then its performance will be assessed using the test set. A list of characteristics is refined based on the messages in the training set so that each of the characteristics provides information about the chance the message is spam.

However, no spam filter is perfect. Even the best filter will likely misclassify spam from time to time. False positives are legitimate emails that are mistakenly classified as spam, and false negatives are spam that appear to be legitimate emails so they slip through the filter unnoticed. An effective spam filter will correctly classify spam and legitimate email messages most of the time. In other words, the misclassification rates will be small. The spam filter developer will set tolerance levels on these rates based on the relative seriousness of missing legitimate messages and allowing spam in user inboxes.

Spam filters need to be customized for different organizations because some spam features may vary from organization to organization. For instance, the word “mortgage” in an email subject line would be quite typical for emails circulating within a banking institution but may be somewhat unusual for other businesses or personal emails. Filters should also be updated frequently.

Spammers are becoming more sophisticated and are figuring out creative ways to design messages that will filter though unnoticed. Spam filters must constantly adapt to meet this challenge.

—Bethany White

Further Reading

- “How to Get Less Spam in Your Email.” *Federal Trade Commission Consumer Advice*, May 2021, consumer.ftc.gov/articles/how-get-less-spam-your-email.
- Madigan, D. “Statistics and the War on Spam.” *Statistics: A Guide to the Unknown*. 4th ed., Thompson Higher Education, 2006.
- Zdziarski, J. *Ending Spam: Bayesian Content Filtering and the Art of Statistical Language Classification*. No Starch Press, 2005.

SPYWARE

ABSTRACT

Spyware is software that accesses a user’s private information without that user’s consent, often for malicious purposes. It can be difficult to detect and remove.

BACKGROUND

Software that performs certain behaviors, such as being downloaded to a user’s computer without being given permission, is generally considered spyware, although the definition may be expanding to include any software, or website, that acts in any way without the user’s consent. These programs are aimed to obtain the owner’s private information, such as lists of websites visited, passwords, and credit card numbers.

Some spyware gets installed onto a user’s computer through electronic games, legitimate programs that have been tampered with, infected attachments, infected email links, even advertisements that seem innocent but are created to get users to click on buttons or links. Spyware can spread quickly if left unchecked.



Image via iStock/Moor Studio. [Used under license.]

OVERVIEW

With many types of malicious software on the internet, users must be aware of what spyware is and what spyware does. Spyware generally performs certain behaviors, including (1) advertising, (2) collecting personal information, and (3) changing the configuration of the user's computer. Spyware is often associated with software that displays advertisements (known as adware) or software that tracks personal or sensitive information.

Not all software that has advertisements or tracks user online activities is harmful. For example, a user may sign up for a free service, and in return for the service, she or he must agree to receive targeted ads. If the user understands these terms and agrees to them, the user may decide that this trade-off is worthwhile. The user may also agree to let the company track his or her online activities to determine which ads to show the individual. For any software program, the user must understand what the software will do and have agreed to install the software on his or her computer.

Detecting spyware can often be difficult process because most spyware is intended to be difficult to remove. Spyware that changes the computer's configuration can be annoying and can cause the computer to slow down or crash.

Spyware can alter the web browser's home page or search page or add additional components to the browser that users may not want. Spyware also makes it difficult for the user to change the settings. One common tactic is that spyware is covertly installed along with the software a user may want, such as a music or video file-sharing program.

Whenever a user installs software on a computer, he or she must carefully read all disclosures, including the license agreement and privacy statement. Sometimes the inclusion of unwanted software in a given software installation is documented, but it might appear at the end of a license agreement or privacy statement.

—Gretchen Nobahar

Further Reading

- Aycock, John Daniel. *Spyware and Adware*. Springer, 2011.
- Bennett, Colin J. *The Privacy Advocates: Resisting the Spread of Surveillance*. MIT Press, 2008.
- Easttom, Chuck. *Computer Security Fundamentals*. 5th ed., Pearson, 2023.
- Erbschloe, Michael. *Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code*. Elsevier Butterworth Heinemann, 2005.
- Marzolf, Julie Schwab. *Online Privacy*. Gareth Stevens, 2013.

STUXNET VIRUS

ABSTRACT

Stuxnet was a computer virus, known as a “worm,” that was created by US and Israeli intelligence agencies in a successful effort to disable key components of the Iranian nuclear program. Stuxnet exploited vulnerabilities in the Windows operating system and deactivated Iran’s centrifuges for the enrichment of uranium, to be used in the construction of nuclear weapons. The worm was used for the first time in 2010 after being developed over a five-year period with assistance from private cyberthreat analysts and designers. Stuxnet is sometimes called the first true cyberweapon in history.

BACKGROUND

While it is widely believed that US and Israeli intelligence agencies worked together to create the Stuxnet virus, the names of the engineers most directly involved in creating this weapon have remained classified. The effort to develop the virus, code named “Operation Olympic Games,” is believed to have begun in 2005, under the George W. Bush Administration, and continued under President Barack Obama when he took office in 2009. Neither the United States nor Israel have confirmed their role in the virus, and what is known about the development of Stuxnet is based largely on journalistic investigations and probes into the issue by

cybersecurity experts. The connection to Israel was first highlighted in a *New York Times* article claiming that a file within Stuxnet contained a reference to the biblical figure of Esther, who fought against the Persians to defend the Jewish people. Some experts have doubted the legitimacy of this connection, but a further piece of evidence came in the form of promotional materials honoring Israeli Lieutenant General Gaby Ashkenazi’s career, in which the Stuxnet virus was listed among Ashkenazi’s accomplishments.

Russian cybersecurity firm Kaspersky Labs investigated the Stuxnet virus after it was launched and concluded that the coding time likely consisted of at least ten people working over the course of about three years. There have been at least two other viruses, one called “Duqu” and the other called “Flame” that are similar in functionality to Stuxnet and are suspected to have been created by the same development team, which many cybersecurity experts believe remained active into the 2020s. Kaspersky researchers later concluded that the Stuxnet system was created through a modular development effort, with various labs of hackers and coders working on various pieces of the final virus, before it was assembled and released. Kaspersky Labs suggested that a cyberattack team known as the Equation Group was responsible for developing the virus. Kaspersky connected the Equation Group to at least 500 different infections in forty-two different countries, primarily developing countries. The top sites for Equation Group attacks were Iran, Russia, Pakistan, Afghanistan, India, Syria, and Mali. Since then, Kaspersky researchers have forwarded the theory that the Stuxnet virus was created by an independent group that is linked to Equation Group, known as “GOSSIP GIRL,” and includes the groups responsible for the Flame and Duqu malware programs, also linked to the Equation Group. In 2020, Kaspersky Labs identified a suspected fourth group working under the Equation Group banner that

created a program named Flowershop that infected numerous targets in the Middle East between 2002 and 2013. The same malware used in Flowershop was discovered in “Stuxshop,” a component of the Stuxnet virus system.

To infect computers, Stuxnet used four “zero-day” exploits. A “zero-day” is a term used to describe a security vulnerability that attackers can then use to launch a cyberattack. The term “zero-day” refers to the fact that the vendor, developer, or user of the system has not learned of the vulnerability until the day that the attack occurs, meaning that the individuals responsible have zero (0) days to fix the problem. Cybersecurity researchers believe that the Stuxnet program utilized four zero-day vulnerabilities that may have been provided by independent cybersecurity hackers and researchers and then sold to intelligence agencies or to members of the Equation Group through the black market for cyberdata and security exploits. The use of at least four zero-day faults was an unusual strategy, because the attack revealed all four faults and therefore gave Windows and Siemens engineers the opportunity to address these vulnerabilities in future builds. The virus is known to have exploited a Windows Shortcut flaw, and then also a bug in the print spooler system, and then two vulnerabilities linked to the privileges system.

While the core data set for Stuxnet was not revealed, reverse engineering and studies indicate that the program was written in several languages, including C and C++. This level of sophistication differs from previously detected malware attacks and made the virus more difficult to both counter and to replicate.

OVERVIEW

Stuxnet’s primary purpose was to delay or destroy Iran’s nuclear enrichment program. To produce nuclear weaponry, Iran first needed to isolate the isotope U-235 from the heavier U-238, which is the

form that most uranium has in nature. To accomplish this, nuclear enrichment technicians utilize centrifuges, devices that spin chemical samples at high speeds, separating components by weights thanks to centrifugal forces. The centrifuges used in uranium enrichment are highly sensitive, complex devices that are prone to damage. To maintain this system, the Iranian nuclear system operators used programmable logic controllers (PLCs) manufactured by Siemens. These PLCs allow computers to control other mechanical devices, translating digital signals into electrical and mechanical signals. In the case of the Iranian nuclear program, the Siemens PLCs were used to control the operation of uranium centrifuges.

The Stuxnet virus contains three basic parts. First there is a “worm,” which is a standalone computer program capable of replicating itself onto other computers. Then there is a file that automatically executes upon encountering the Windows system and sends copies of the worm out. The third component is a rootkit program, which is a type of malware that enables access to a computer system but conceals itself by returning false signals to diagnostic systems. While the Stuxnet virus can easily travel through an internet system, the Iranian nuclear facility was “air gapped,” which means that the facility utilized a closed, internal network not connected to the internet. The program therefore had to be manually inserted into the Iranian internal network. Stuxnet is designed to be stored and delivered through the use of a universal serial bus (USB) stick or other device that can then insert the program on a computer.

When the Stuxnet program infiltrates a computer, one part of the program’s code conducts a search looking for programs from the Siemens company, specifically Siemens Step 7, a PLC system created by Siemens Systems. If no PLCs are found, then virus remains inactive. This enables the virus to avoid detection, by remaining inactive within systems not

connected to target equipment. If the virus detects links to PLCs, a different set of programming is activated, deploying the rootkit program. This delivers a false signal from the Windows system indicating that Windows is performing regularly, despite altered blocks of code. The program then alters the code used by the Siemens PLC devices and impacts only those PLCs that are connected to variable-frequency drives. Further, it only targets variable-frequency drives from two different vendors. This specificity was purposefully built into the program by engineers who understood not only how the Iranian nuclear enrichment program worked but also what vendors and specific software programs were being installed.

Once the virus has identified a system with a linked Siemens Step 7-controlled PLC, which is further linked to a variable drive from one of the two vendors, the program installs a malware program into the PLC that modifies the frequency at which the centrifuges spin, changing the speed of the attached rotors and forcing the entire machine out of sync. The rootkit program meanwhile delivers false signals to operators indicating that the machine is functioning normally within designed parameters. The imbalanced operation of the machine eventually damages and deactivates the centrifuges, potentially leading to catastrophic failure of the entire system.

Because damage to centrifuges used in enrichment is common, Iranian engineers did not initially notice the attack, even as centrifuge units continued to fail, derailing their enrichment program. By some estimates, the total damage that occurred likely set the Iranian enrichment program back by as much as two years.

DISCOVERY AND SPREAD

The cause of the failure at Iran's Natanz facility was not understood until inspectors from the International Atomic Energy Agency (IAEA) were allowed

access to the Natanz enrichment plant to conduct a review of damaged centrifuge parts. The IAEA investigates damaged centrifuge parts to ensure that radioactive material is not transmitted or smuggled from one plant to another. While centrifuge damage is not uncommon, in 2010 IAEA researchers noticed a higher-than-average number of damaged centrifuges, with one inspector estimating that at least two thousand centrifuges had been fatally damaged, while they expected to find about eight hundred damaged parts at Natanz. It was the IAEA that initially issued a report indicating that the facility had suffered some kind of unusually aggressive failure.

The virus responsible for the attack might not have been detected until it spread outside of the Natanz facility where the attack occurred. It is uncertain how the virus managed to spread, given that the Natanz facility was air-gapped and not connected to the world internet. An employee of the facility might have used a computer from the internal network to connect to the internet after the program had infiltrated the internal network, thus accidentally releasing the program. Alternatively, some suggested that the program was purposefully leaked onto the internet, where it quickly spread.

The program caused computer crashes and difficulties across Iran, and one security expert at an Iranian company not connected to the military called in Belarusian company VirusBlokAda to get advice on the problem. Security expert Sergey Ulasen and a team managed to isolate the program and quickly realized the sophistication of the program, with the capability to exploit multiple vulnerabilities and the rootkit concealing the activity of the virus. Ulasen shared information about the virus with the broader international security community and Liam O'Murchu, director of the Security Technology and Response group for the company Symantec, was the first to examine the code. Over time, one small part of the code, controlling one driver, was reverse engineered; however, the initial Stuxnet code was not

fully discovered or revealed. O'Murchu and his team analyzed the code and realized that it had been specifically tailored to attack not just nuclear uranium enrichment facilities but the Natanz facility specifically, as the Natanz facility had eight arrays of 168 centrifuges, matching with the number of centrifuges that could be attacked with the virus. In September of 2010, Symantec issued a statement on what they had discovered and it was quickly understood by security experts that this strange computer problem was linked to a purposeful and specific attack targeting the Natanz facility.

The Stuxnet virus has since spread around the world, infecting hundreds of millions of computers. As long as none of these computers are connected to a Siemens system logic controller, the virus remains inactive and does nothing on the computer, thus providing no real risk. However, Siemens and Microsoft have issued fixes that remove the Stuxnet virus from infected systems, and the companies involved have fixed the vulnerabilities that Stuxnet originally exploited, such that even if a virus was connected to a PLC system, it would no longer disable the system. While the Stuxnet virus is no longer considered a serious security threat, some have argued that the widespread nature of the virus leaves open the possibility that engineers will learn to use the virus to conduct different kinds of attacks, thus potentially creating new cybersecurity threats.

SIGNIFICANCE

In the years following the detection of the Stuxnet virus, many other technologically advanced nations developed and deployed cyberweapons, but none of those attacks were as direct and impactful as the Stuxnet attack. Most subsequent uses of cyberweapons targeted industrial or economic data, rather than striking at military or industrial facilities. Some historians therefore consider the Stuxnet virus to be potentially the first cyberweapon and the attack on the Natanz facility the world's first cyberattack. In

the years since, cyberweapons have become more numerous and complex, and many national and international security experts consider cyberwarfare the chief threat of the future. Many cybersecurity experts further note that the United States has taken steps to protect US intelligence and infrastructure from similar kinds of attacks in the future.

—Micah L. Issitt

Further Reading

- Barth, Bradley. "GOSSIPGIRL Stuxnet Group Had '4th Man'; Unknown Version of Flame & Duqu Found." *SC Media*, 10 Apr. 2019, web.archive.org/web/20200806024942/www.scmagazineuk.com/gossipgirl-stuxnet-group-4th-man-unknown-version-flame-duqu-found/article/1581579.
- Franceschi-Bicchieri, Lorenzo. "The History of Stuxnet: The World's First True Cyberweapon." *Vice*, 9 Aug. 2016, www.vice.com/en/article/ezp58m/the-history-of-stuxnet-the-worlds-first-true-cyberweapon-5886b74d80d84e45e7bd22ee.
- Fruhlinger, Josh. "Stuxnet Explained: The First Known Cyberweapon." *CSO*, 31 Aug. 2022, www.csionline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html.
- Goodin, Dan. "How 'Omnipotent' Hackers Tied to NSA Hid for 14 Years—and Were Found at Last." *Ars Technica*, 16 Feb. 2015, arstechnica.com/information-technology/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last.
- Jenkinson, A. J. *Stuxnet to Sunburst: 20 Years of Digital Exploitation and Cyber Warfare*. CRC Press, 2022.
- Kushner, David. "The Real Story of Stuxnet." *IEEE Spectrum*, 26 Feb. 2013, spectrum.ieee.org/the-real-story-of-stuxnet.
- Naraine, Ryan. "Stuxnet Attackers Used 4 Windows Zero-Day Exploits." *ZDNet*, 14 Sept. 2010, www.zdnet.com/article/stuxnet-attackers-used-4-windows-zero-day-exploits.
- Rosenbaum, Ron. "Richard Clarke on Who Was Behind the Stuxnet Attack." *Smithsonian Magazine*, Apr. 2012, www.smithsonianmag.com/history/richard-clarke-on-who-was-behind-the-stuxnet-attack-160630516.
- Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Broadway Books, 2014.

SYSTEMS SECURITY ENGINEERING

ABSTRACT

Systems security engineering (SSE) is a type of systems engineering. It applies principles of science, engineering, and assurance to identify and mitigate cybersecurity vulnerabilities. Systems security engineering also minimizes or contains risks related to these vulnerabilities. Additionally, SSE identifies related security requirements and verification methods. One goal of SSE is to ensure systems are trusted and meet stakeholder risk tolerance requirements.

BACKGROUND

Systems engineering is the primary integrating mechanism for technical, management, and support activities related to engineering a system. It enables engineered systems to be effectively realized, used, and retired. To be successful, systems engineering must meet the needs and priorities of stakeholders and achieve their desired outcome. Systems engineering is guided by data and analytics to limit uncertainty and manage risk.

Risk drives all types of systems security. Systems security risk considers both the severity of impact of an event, such as an attack, and the probability that the event will occur. The level of acceptable security risk depends on risk appetite for that system, as defined by stakeholders.

Systems security engineering (SSE) builds on systems security and includes cybersecurity, hardware assurance, software assurance, supply chain risk management, technology sharing, security testing and evaluation, and security specialties. To develop trustworthy systems and ensure their operational security, SSE addresses threats from insider attacks, social engineering attacks, physical attacks, and cyberattacks. Attacks on global supply chains and development processes and tools are also addressed by SSE.

Effective SSE mitigates an attacker's attempt to exploit any weakness in a system. When SSE is poor, attackers can employ a wider range of attacks to take advantage of system vulnerabilities.

OVERVIEW

Systems security engineering ensures that systems and platforms of organizations are secure and meet trust requirements in all operational environments. System security engineers consider all system life cycle processes. They identify threats, vulnerabilities, risks, and appropriate protection measures across the life cycle of a system.

Protection measures are of two types. One is a description of what the system capabilities and attributes must be. This information is incorporated into the design and requirements of the system. The second is a description of how the system will be built, maintained, and/or procured.

Systems security engineering that focuses specifically on cybersecurity identifies and incorporates related security design and process requirements, often tied to risk identification and management, into systems. It also balances security with system performance, costs, and schedules, all of which have been defined by stakeholders.

Ideally, SSE is implemented and integrated early in the development of hardware, software, networks, and other systems to better understand security risks and to identify protection requirements. This process continues during the life cycle of the system, with different SSE processes and activities occurring throughout this cycle. As a result, systems can be better managed and delivered.

Effective SSE includes protective security measures in architectural design. A system architecture identifies and defines the way a system interacts with people, processes, and information and communication technology systems. Systems security engineering can be used during the architectural design process to identify and eliminate vulnerabilities before they become problematic. The architecture design should be refined to identify, minimize, and contain the impact of any vulnerabilities.

Systems security engineering also plays a significant role during the configuration management and

control processes. It ensures that security requirements are considered and configuration control is maintained as threats evolve and updates to systems are implemented. With SSE, security requirements are captured, refined, and integrated into products and systems through purposeful security design or configuration.

Additionally, effective SSE verifies that a system was built correctly and makes sure that operations processes are effective. Secure operations and engineering support are two kinds of operations processes. Another type of operations process is incident handling. The lessons learned from incidents should be applied to improve systems.

RISK MANAGEMENT

Security risks can be introduced into systems through multiple means. SSE protects systems by removing risks, reducing risks, and responding to realized risks. In an SSE context, risk may be managed in part through the performance of vulnerability and threat assessments. Systems security engineering can also involve maintaining a security risk register, which includes records of how security issues have been addressed and the risks that may remain. A strong SSE culture in an organization results in increased protections for the organization, its employees, customers, and the organization's reputation.

DEFINING SUCCESS

When SSE is successful, effective risk management practices, design reviews, and configuration management are implemented as part of the system

development effort. Additionally, hiring qualified workers, practicing quality control and quality assurance, and fostering a mindful security culture that emphasizes security responsibilities for everyone is part of successful SSE. When SSE is effective, a system is protected from misuse and malicious behavior. The system also delivers value, even when cyberspace conditions are adverse.

—A. Petruso

Further Reading

- Anderson, Ross. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 3rd ed., Wiley, 2020.
- Doohan, Bradley, et al. *The Black Book: A Starter Guide to Systems Security Engineering for Acquisition. Defence Research and Development Canada*, 2016, cradpdf.drdc-rddc.gc.ca/PDFS/unc265/p805130_A1b.pdf.
- INCOSE Systems Security Engineering Working Group. “Introduction to Systems Security Engineering Vocabulary.” *Insight*, vol. 23, no. 3, 2020, doi.org/10.1002/inst.12301.
- Mead, Nancy R., and Carol C. Woody. *Cyber Security Engineering: A Practical Approach for Systems and Software Assurance*. Addison-Wesley Professional, 2016.
- Nejib, Perri, and Dawn Beyer. “Systems Security Engineering: Whose Job Is It Anyway?” *Insight*, vol. 19, no. 2, 2016, pp. 47–53, doi.org/10.1002/inst.12089.
- Ross, Ron, Mark Winstead, and Michael McEvilley. *Engineering Trustworthy Secure Systems*, Nov. 2022, nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1r1.pdf.
- Ross, Ron, Michael McEvilley, and Janet Carrier Oren. *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*. National Institute of Standards and Technology, 2017.

T

TARGETED ADVERTISING

ABSTRACT

Targeted advertising is directed to narrow groups of consumers on the basis of preferences or other personal traits which are deemed to make the targets more receptive to the ads. In order for this type of advertising to work, online and other behaviors have to be tracked and various kinds of personal information collected. Advertisers today can assemble complex data profiles of internet users by gathering information from myriad sources.

BACKGROUND

The first banner ad on the internet appeared in 1994 on the site HotWired. It was an ad for American Telephone & Telegraph (AT&T), and because the concept was so novel, the click-through rate (the percentage of people who clicked on the link) was an astounding 44 percent. The first pop-up ad appeared in 1997. But it was not only advertising techniques that were being developed in the 1990s; an entirely new advertising model was also emerging. The internet—an “information superhighway”—made it extremely easy for information to flow back to the owners and advertisers of websites as much as it flowed from them to users in the form of content. Two early forms of targeted advertising emerged in 1995. In that year, Yahoo began placing ads on its site on the basis of users’ previous search terms. In the same year, an advertising company called WebConnect developed a tracking tool that collected anonymized information about the various sites visited by internet users. WebConnect used that information to sell advertisers on the possibility of targeting their ads to consumers who had specific

interests, which were known from their browsing habits. Thus began a revolution in advertising that was also to have broad social consequences in the years ahead.

Reliance on targeted advertising, something made possible by the collection of user data, was innovative in two ways. First, it was a novel business model. While plenty of media companies in the past had relied on advertising sales to earn money (like television and newspapers), only internet-based businesses were able to harvest the kind and scale of user data necessary for effective targeted ads. Second, targeted advertising became the reigning model for the entire internet: since the 1990s, websites offer users apparently “free” content thanks to advertising.

OVERVIEW

For ten or fifteen years, most people either did not notice or were not bothered by targeted advertising. As social media sites like Facebook became prominent, however, and as users began spending more and more time on the internet, the presence of targeted ads became more visible and a topic for debate. Millions of users by then had experienced situations in which keyword searches resulted in potentially embarrassing advertisements appearing in their news feeds or elsewhere. Earlier, internet privacy concerns had focused on such things as identity theft, the permanence of one’s “digital footprint,” or the hazards of sharing too much personal information. Around the same time, the leaks of Edward Snowden, made public in 2012, revealed a network of secret government spy programs that swept up information on nearly every American



Image via iStock/Enis Aksoy. [Used under license.]

citizen and gave (often fairly indiscriminate) access to citizens' internet activities. Although the set of problems that Snowden uncovered were quite distinct and had very little to do with how businesses were operating on the internet, concerns over internet privacy and so-called corporate surveillance swelled following news reports of his revelations. In 2014, for example, the Pew Research Center issued a report stating that 91 percent of adults at that time felt that "consumers have lost control over how personal information is collected and used by companies." In 2019, a further Pew study showed that 81 percent "think the potential risks of data collection by companies about them outweigh the benefits."

In 2016, charges of election interference and misinformation campaigns during the United States presidential election focused attention on targeted political advertising on the internet. As a result of the controversy, some companies, such as Google and Twitter (later renamed X), instituted relatively robust policies to limit so-called microtargeting, making it difficult for political ads to reach too-narrow audiences.

Facebook, the company that was most implicated in the 2016 controversy, implemented more controls

and some transparency regarding its political advertisement policy following a series of Congressional hearings in which Mark Zuckerberg faced harsh criticism. For example, Facebook—the parent company of which was renamed Meta in 2021—began requiring groups posting political ads to undergo an "authorization process" before posting their ads.

IMPACT

Targeted ads began as a refinement of traditional advertising techniques, a development that relied upon the ability to easily gather user information over the internet, and it quickly became the dominant business model for websites operating on the internet. In the 2010s, targeted ads became a topic of controversy with regards to privacy rights and their unanticipated social consequences, such as increased political polarization.

Some critics of targeted advertising, such as the technologist Jaron Lanier, point to the social and other ill effects of targeted advertising and have gone so far as to call the advertising model of the internet a "fake" business model, because it only "appears" to offer users content for free. Lanier and others have suggested that the success (and the

high-quality content) of subscriber-based companies like Netflix suggest an alternative model for funding the internet. In 2019, Harvard Business School professor Shoshana Zuboff published *The Age of Surveillance Capitalism*, a well-received scholarly treatment of the data collection and its psychological, sociological, and political implications that will likely be a touchstone for discussion going forward. Targeted advertising remained a controversial topic into the third decade of the twenty-first century, and in 2021, a survey conducted by the firm Morning Consult revealed that 64 percent of US adults considered the targeted advertisements served to them on streaming services to be invasive.

—D. Alan Dean

Further Reading

- Auxier, Brooke, et. al. *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*. Pew Research Center, 2019.
- Lanier, Jaron. *Ten Arguments for Deleting Your Social Media Accounts Right Now*. Henry Holt, 2018.
- Smith, Mike. *Targeted: How Technology Is Revolutionizing Advertising and the Way Companies Reach Consumers*. Amacom Publishing, 2014.
- “Survey: 64% Find Targeted Ads Invasive.” *Advanced Television*, 20 Oct. 2021, advanced-television.com/2021/10/20/survey-64-find-targeted-ads-invasive.
- Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs, 2019.

U

USABILITY

ABSTRACT

Usability refers to how well a product, service, or system meets the needs of a user in terms of ease, efficiency, and effectiveness. Meeting these qualities makes something more valuable to the user. It also makes it more likely to be successful and to be viewed in a favorable way by consumers. Usability is related to how well something functions; however, usability and functionality are different qualities.

BACKGROUND

The word “usable” comes from an old French word meaning “available.” Although the word came into use in the fourteenth century, it did not gain widespread usage until the middle of the nineteenth century. The idea of studying usability has its origins about 150 years later.

In the early twentieth century, some researchers began looking into ways to improve the efficiency of various products and services. These researchers included industrial engineers Frank Gilbreth and his wife, Lillian Moller Gilbreth. The couple, who specialized in time and motion efficiency, had twelve children whom they raised according to their theories on time management and organization; they were the inspiration for the *Cheaper by the Dozen* book and films.

By 1936, companies could see the advantages of promoting the usability of their products. Over the next several decades, there was an increased focus on improving usability. By the 1970s, scientists were making usability a formal topic of their research. During the last few years of the 1980s, experts began making usability their career specialty. In

1998, the concept had reached such universal acceptance that the International Organization for Standardization (ISO), a nongovernmental organization dedicated to creating standards to facilitate global interactions, adopted ISO 9241-11, a standard addressing the definition and basic requirements for usability.

OVERVIEW

The usability of a product, service, or system is an important consideration for anyone or any company designing something that will be used by others. While it is often thought of in terms of “ease of use,” usability goes beyond how easily something can be used. Something can be easy to use but not necessarily fulfill the needs of the user. For instance, a television might be very easy to operate, but if it cannot be turned off and on without a remote, it will not meet the user’s needs if the remote batteries are drained or the remote is missing. In other words, it is functional but not usable.

Experts list five characteristics something must provide to its users for it to be considered usable. It should be effective, meeting the purpose for which the user needs it. It should be efficient, meeting that purpose with the least effort and time. It should be engaging, having appeal to the user while it is being used; for instance, a website should have interesting graphics appropriate to the site’s topic. It should be error tolerant; this means both taking steps to help prevent user error—clearly labeled buttons, for instance—and making recovery from mistakes easy, such as giving the user a way to back out if an incorrect choice is made. It should be easy to learn; for example, if the settings menu on a television

requires the use of the channel up and down buttons on one screen to set sound options, it should not require the use of the volume up and down buttons to set color options. These five attributes—effective, efficient, engaging, error tolerant, and easy to learn—are called the five E's of usability.

Understanding the potential user is the first step in ensuring usability. Designers will determine who the target audience for their product or service will be and what they will be expecting from the item. It is also important to anticipate mistakes, unusual expectations, or unorthodox attempts the user might make. For instance, what happens if someone using an automated phone answering program to pay a utility bill wants to pay an amount larger than the amount due on the bill? A usable system should include an option that allows the input of the dollar amount, or if the company requires the customer to make these arrangements directly with a representative, the system should provide a means for the customer to speak to a representative. A system demonstrating usability would not permit the customer to make a payment that is not allowed, or would simply cut the customer off because of the unusual action.

As development is underway on a product, service, or system, it is necessary to assess usability at various stages in the process. This can be done using prototypes, simulations, or other means of having users interact with the item to determine how well it is meeting the users' needs and expectations. It can also be accomplished through feedback, such as a "How did we do?" survey that pops up after someone uses a website. Designers should conduct regular evaluations as well, using a method appropriate for the item. For example, a mailed survey might be the best way to determine what people think of a new car design, while statistics about merchandise returns might be a good way to judge the usability of a new electronic device.

Usability has been deemed such a universally important concept that the ISO, an independent agency made up of dozens of organizations that establish standards and guidelines within a number of countries, has established guidelines and an official definition for usability. The ISO guidelines help with international trade by standardizing definitions and parameters for products, systems, and services that are recognized by all participating organizations. The ISO guidelines for usability are included in ISO 9241-11. First discussed in 1990, the guidelines were formally adopted in 1998. More than 160 member-countries of the ISO recommend these guidelines to the companies that look to them for standards, certification, and other services when engaging in global trade.

—Janine Ungvarsky

Further Reading

- "About Us." *ISO*, www.iso.org/about-us.html.
- Grobler, Marthie, Raj Gaire, and Surya Nepal. "User, Usage and Usability: Redefining Human Centric Cyber Security." *Frontiers in Big Data*, vol. 4, 2021, doi.org/10.3389/fdata.2021.583723.
- "Introduction to User-Centered Design." *Usability First*, www.usabilityfirst.com/about-usability/introduction-to-user-centered-design.
- Komninos, Andreas. "An Introduction to Usability." *Interaction Design Foundation*, 22 July 2020, www.interaction-design.org/literature/article/an-introduction-to-usability.
- Quesenberry, Whitney. "What Does Usability Mean: Looking Beyond Ease of Use." *WQusability*, www.wqusability.com/articles/more-than-ease-of-use.html.
- Sauro, Jeff. "A Brief History of Usability." *Measuring U*, 11 Feb. 2013, measuringu.com/usability-history.
- "Usability." *Technopedia*, 8 Sept. 2011, www.techopedia.com/definition/4919/usability.
- "Usability Evaluation Basics." *Usability.gov*, www.usability.gov/what-and-why/usability-evaluation.html.

V

VIRTUAL PRIVATE NETWORK

ABSTRACT

A virtual private network (VPN) forms a secure, virtual connection to a private network through a public network, most typically the internet. A VPN connection enables authorized users to send and receive data and to access networked resources as if they were directly plugged into private network servers. Virtual private network connections are most often used to connect a company's disparate office locations or to enable employees to access a company's private network from home or other remote locations, but VPNs can also be used to securely connect multiple home networks for personal use.

BACKGROUND

Microsoft software engineer Gurdeep Singh Pall coauthored the first virtual private network (VPN) protocol, point-to-point tunneling protocol (PPTP), in 1996. PPTP enables a computer to establish a secure connection, called a "tunnel," to a remote server. Pall created PPTP to enable his coworkers to work effectively and securely from home or other remote locations without the need to connect to the company's servers through slow dialup connections. Instead, with PPTP, users could log on to Microsoft's servers using high-speed internet.

Prior to the development of VPNs, networked computers were connected through leased lines, which were often slow, expensive, and difficult to expand. Before VPN technology was widely adopted, businesses typically rented leased lines from telecommunications companies to create wide-area networks (WANs) that connected various office locations. However, leased lines were

extremely expensive, with costs rising as the distance between two connected locations increased.

A VPN enables a private network to be extended across a public network, such as the internet. Virtual private networks offer the benefits of security, reliability, and scalability, meaning that they are easily extended and modified. VPNs encrypt and encapsulate outgoing data to protect it from public view. However, security concerns remain when connecting two private networks through a public resource. A disadvantage of VPN is that all computers connected to the VPN become part of the internal network. If one machine connected to the VPN is hacked, the hacker will then be able to access the VPN to attack the intranet.

OVERVIEW

There are two primary types of VPN connections: remote-access and site-to-site VPNs. A remote-access VPN enables individual users to connect to a private network from a remote location using any computer with internet access. To form a remote-access VPN,

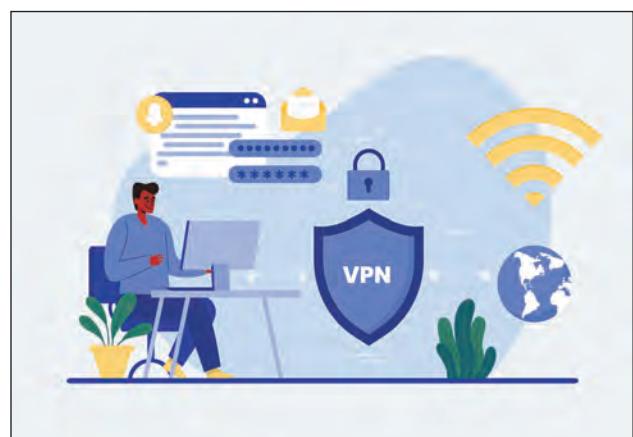


Image via iStock/Nadezhda Ivanova. [Used under license.]

a network-access service (NAS), which may be a server or a software application, prompts the user to enter valid credentials before accessing the VPN, and client software establishes and maintains the connection to the VPN. Site-to-site VPNs, which connect entire private networks together, do not require client software. Site-to-site connections are either intranet-based VPNs, which form a single private internal network, or extranet-based VPNs, which form a secure, shared network while preventing shared access to separate intranets. Intranet-based VPNs are useful for connecting a branch office network to a company headquarters network, while extranet-based VPNs are used to connect companies with their partners, vendors, and customers without granting full access to the company's internal network.

In 2023 *Forbes* reported that the personal use of VPNs had become more widespread than VPNs used for business and that 33 percent of all internet users have utilized a VPN. By this time, numerous VPN providers were available to consumers, and *Forbes* estimated that the VPN market will reach a value of \$107.5 billion by 2027.

—*Mary Woodbury Hooper*

Further Reading

- Bidgoli, Hossein, editor. "Infrastructure for the Internet, Computer Networks, and Secure Information Transfer." *Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management*. Vol. 3, Wiley, 2006, pp. 337–808.
- Crail, Chauncey. "VPN Statistics and Trends in 2023." Reviewed by Kelly Main. *Forbes Advisor*, 9 Feb. 2023, www.forbes.com/advisor/business/vpn-statistics.
- Geier, Eric. "How (and Why) to Set Up a VPN Today." *PCWorld*, 19 Mar. 2013, www.pcworld.com/article/457163/how-and-why-to-set-up-a-vpn-today.html.
- "How Virtual Private Networks Work." *Cisco*, 13 Oct. 2008, www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html.
- Mairs, John. *VPNs: A Beginner's Guide*. McGraw-Hill, 2002.
- Raghunath, Satish. "Resource Management for Virtual Private Networks." *IEEE Communications Magazine*, vol. 45, no. 4, 2007, pp. 38–44.
- Rosenberg, Eric, and James Uttaro. "Scaling Virtual Private Networks." *Recent Patents on Engineering*, vol. 1, no. 3, 2007, pp. 206–13.
- Stewart, Andrew J. *A Vulnerable System: The History of Information Security in the Computer Age*. Cornell UP, 2021.
- Zwicky, Elizabeth D., Simon Cooper, and D. Brent Chapman. *Building Internet Firewalls*. 2nd ed., O'Reilly, 2000.

W

WEB DEVELOPER

ABSTRACT

Web developers generate the look and feel of a website. They are also responsible for a website's performance and capacity. Students aspiring to enter the profession should pursue studies in subjects such as web design, computer science, graphic design, and communication.

BACKGROUND

Website developers create the public appearance, functionality, and general design, or interface, of websites according to the client's needs and the principles of a chosen design them. They brainstorm both the creative and technical design of websites. Website developers design a basic webpage structure, or architecture, and select fonts, colors, graphics, and other visual elements, to apply creatively to that architecture. They are also responsible for a website's performance and capacity, meaning how fast it runs and how much data and user traffic it can handle.

OVERVIEW

Having a company or organizational website has become nearly universal. Web developers work in many settings, including software or graphic design firms, advertising agencies, and large and small corporations. They may also be employed in government, hospitals, schools, and colleges, and a multitude of different types of organizations. Some are self-employed. In larger firms or departments, the website developer is part of a team of creative and technical professionals who share responsibility for websites. Their "clients" are divisions or departments

inside the company. Web developers spend their days working on computers. The forty-hour work week is most prevalent, although sometimes developers must work long hours to meet deadlines.

Designing websites requires creativity, color and design skills, technical knowledge about computer code languages and software, and strong organizational skills. Developers must also communicate effectively with team members and clients. They must keep up with technology and trends and be willing to update websites as necessary. They are fast, creative problem-solvers who understand the needs of business and their clients. Many also enjoy the competition inherent in their industry.

DUTIES AND RESPONSIBILITIES

Sometimes web developers begin work with the acquisition of a domain name (web address) and a suitable website host provider (server). Other projects might consist of updating an existing website. These and other details are usually worked out during meetings with clients and may also be discussed with colleagues.

One of the most important steps in designing a new site is planning its structure, or architecture. Before beginning work on the actual page, the developer compiles a list of all the necessary components, including databases, shopping carts, calendars, and directories. He or she then decides how each element will best fit into the overall structure of the website.

The website developer next creates an attractive layout for individual pages. This might involve coding a cascading style sheet (CSS), which allows colors, fonts, and other aesthetic elements to be



Image via iStock/Aleksei Naumov. [Used under license.]

automatically applied to all pages. The developer imports files, such as the company logo, graphics, and navigational buttons, to the website and arranges them in the layout. Sometimes the website developer creates these graphics files.

The website developer might then add coding language to make the page dynamic, mapping out illustrations, adding hyperlinks to text, and so on. Alternatively, he or she might create the site in a WYSIWYG (“what you see is what you get”) editor that requires less technical knowledge. The website developer ensures that links work properly and that the site displays correctly on various monitors, with different browsers, and on varied mobile devices. When the developer is satisfied with the work and the client has approved it, the developer publishes the website on the internet. Additional responsibilities of a website developer sometimes include website maintenance, depending on the client’s expectations.

OCCUPATION SPECIALTIES

Web architects or programmers. Web architects or programmers are responsible for the overall technical construction of the website. They create the basic framework of the site and ensure that it works as expected. Web architects also establish procedures for allowing others to add new pages to the website and meet with management to discuss major changes to the site.

Web designers. Web designers are responsible for how a website looks. They create the site’s layout and integrate graphics, applications (such as a retail checkout tool), and other content into the site. They also write web-design programs in a variety of computer languages, such as hypertext markup language (HTML) or JavaScript.

Webmasters. Webmasters maintain websites and keep them updated. They ensure that websites operate correctly and test for errors such as broken links. Many webmasters respond to user comments as well.

WORK ENVIRONMENT

Physical environment. Web developers typically work in offices or studios, either alone or with other developers and programmers. They spend long hours working at a computer. Self-employed web developers frequently work out of home offices.

Human environment. Most web developers either report to art directors or technical managers. They may supervise part-time staff or interns. In many cases, they work on teams that include illustrators, photographers, videographers, copywriters, and programmers. Web developers who work for a large company or organization may interact with marketing and advertising specialists and the many different people who are responsible for web content. Self-employed web developers necessarily are the sole point of contact for clients.

Technological environment. Web developers should be familiar with HTML, CSS, WYSIWYG editors, and other basic website design programming languages and tools. They should be comfortable using art-creation and graphic-design programs, basic office software, and various operating systems, browsers, and displays. Developers must use scanners, printers, digital cameras, smartphones, and other electronic equipment. Those who do more substantive programming should learn more specialized skills in other programs. Some developers need to be familiar with web analytics, while others may need to know computer animation and modeling programs.

EDUCATION AND TRAINING

High school/secondary. Aspiring web developers may benefit from taking a college preparatory program with an emphasis in English, mathematics, speech communication, and computer science, and additional electives in graphic design, fine art, photography, video, and other subjects that develop the imagination. Learning new techniques and computer programs outside of school hours is essential.

Prospective web developers should consider volunteer or part-time work designing websites for local individuals and businesses.

College/postsecondary. There is no specific postsecondary degree or certificate required by all employers; however, most employers prefer some type of certification. Building a professional portfolio is vital. There are many different learning opportunities that will meet individual employment needs and provide the education needed to prepare an attractive portfolio. Programs in web design are offered through college continuing education programs and in business, technical, and commercial art schools.

Students may opt to enter an associate's or bachelor's degree program in graphic design with an emphasis in web design. They can also pursue an undergraduate degree in computer science or information technology, with additional courses in art and design. Disciplines such as business or marketing can also be advantageous areas of study for aspiring web developers. Independent study in website design, internships, workshops offered by software developers, and distance education courses are other options.

Adult job seekers. Web design can be an attractive occupation for adults, especially those with some design or computer aptitude and an interest in working from home. Those who need to update their skills or learn new techniques can choose from many courses offered in the evenings, weekends, or online.

Advancement is dependent upon experience, education, and talent. Developers who acquire more specialized software skills may be given more sophisticated, prestigious jobs or additional responsibilities, such as programming or creating multimedia content. Some developers may move into supervisory positions or start their own design firms.

Professional certification and licensure. There are no mandatory licenses or standardized certificates;

however, individual schools, vendors, and professional associations offer various certificates. Some of these meet the standards set for the Certified Web Professional (CWP) program established by the World Organization of Webmasters (WOW).

Additional requirements. Web developers must be internet savvy and enjoy keeping up with the latest trends in web design and technology. They should be creative, detail-oriented individuals capable of learning various software languages, programs, and computer operating systems relatively quickly, often without formal training. Web developers need strong communication and business skills, and they must work well independently or in teams on deadline-oriented projects. Those who wish to establish their own design firms should also have business acumen and strong marketing skills.

—Sally Driscoll

Further Reading

- Costello, Vic. *Multimedia Foundations: Core Concepts for Digital Design*. 3rd ed., Focal Press, 2023.
- Felke-Morris, Terry. *Web Development and Design Foundations with HTML5*. 10th ed., Pearson, 2020.
- Hardy, David Leicester. *Introduction to Digital Media Design: Transferable Hacks, Skills, and Tricks*. Bloomsbury Visual Arts, 2022.
- “Website Security.” MDN, 3 July 2023, developer.mozilla.org/en-US/docs/Learn/Server-side/First_steps/Website_security.

WINDOWS OPERATING SYSTEM

ABSTRACT

Microsoft Windows is the most dominant group of operating systems available for personal computers. Operating systems are software programs that support and manage the basic functioning of the computer. Operating systems provide a graphical interface through which users can easily execute tasks by clicking on icons or typing into a command prompt. Since its initial release in 1985, Windows

has evolved with consistently improved functionality that has kept the brand at the forefront of the market for decades. Despite occasionally being the target of vocal criticism, Windows remained the most popular operating system for personal computers by 2023.

BACKGROUND

Prior to the mid-1980s, most early computers ran on simplistic operating systems that required users to input complex text-based commands into command prompts. Starting in 1981, the most common of these rudimentary operating systems was the Microsoft Disk Operating System (MS-DOS). Although MS-DOS was reasonably functional and reliable for its time, it was quickly overshadowed when Apple Computer’s Macintosh debuted in 1984. Rather than using a text-based operating system like MS-DOS, the Macintosh featured one of the earliest examples of a graphical interface-based operating system that allowed users to interact with the machine by clicking on icons.

The arrival of the graphical interface represented a major step forward in personal computing and presented a significant challenge for Microsoft. Undaunted, the company responded by developing



Retail box of Microsoft Windows Operating System Version 3.1 (for MS-DOS 5.0/V), released in Japan on May 18, 1993. Photo via Wikimedia Commons. [Public domain.]

its own graphical interface-based operating system. Referred to internally as Interface Manager, the new operating system featured a sort of virtual desktop on which programs ran in boxes called windows. These windows eventually became the inspiration for the operating system's official name when it was released in 1985. Even though the early Windows system offered mouse support; included features such as drop-down menus and scroll bars; and came loaded with a range of basic programs such as Paint, Notepad, and Calculator, Windows 1.0 was generally considered inferior to the Macintosh operating system and was a commercial failure.

OVERVIEW

Undeterred by the initial negative response to Windows 1.0, Microsoft worked to create a better product. In an effort to emulate its competitor's success, Microsoft entered a licensing agreement that allowed it to incorporate some of Apple's graphical interface features in Windows 2.0. With these added features, improved graphics, and the inclusion of additional software, Windows 2.0 clearly improved upon its predecessor and enjoyed a more positive reception upon its release in 1987.

While Windows 2.0 proved to be a step in the right direction, Microsoft's first real operating system breakthrough came with the 1990 debut of Windows 3.0 and the enhanced Windows 3.1 two years later. Touting an entirely new file management system, visual customization, alternative operating modes, and more bundled software, the new Windows was an immediate hit, selling 10 million copies in just two years. Crucially, Microsoft also released a software development kit with Windows 3.0 that made it easier for third-party software developers to write programs to run on the operating system. This effort helped to solidify the place of Windows in the personal computing market.

With the internet emerging as the driving force in the computer industry, Microsoft unveiled

Windows 95 in 1995. This product featured a totally redesigned operating system with a unique look and feel. Unlike earlier releases that ran on top of MS-DOS and required a manual launch from the user, Windows 95 loaded automatically when the computer was started. Most notably, Windows 95 included the first taskbar and Start menus, which offered users easy access to programs, documents, and settings. Windows 95 also provided a gateway to the internet through the inclusion of the internet browser, Internet Explorer. With these new features, Windows 95 was a success, selling 7 million copies in only five weeks. Three years later, Microsoft returned with Windows 98, a release that was essentially an improved version of Windows 95.

Through the early 2000s, Microsoft released several new versions of Windows, including Windows 2000, which was an updated iteration of the professional Windows NT line, and Windows Millennium Edition. The latter was notoriously unstable, largely because it was rushed to the marketplace in anticipation of the debut of Windows XP in 2001. Windows XP was designed to address many of the issues that plagued Microsoft's previous releases and, as a result, offered significantly improved speed, stability, and file management. Thanks to these key tweaks, Windows XP became one of Microsoft's most widely used products.

Windows Vista (2007) was the next version of the product. Though this product boasted the strongest security system and most impressive graphics that had yet been seen in a Windows operating system, it was critically panned. Much of the criticism was focused on Vista's extensive compatibility issues, which convinced many XP users to delay upgrading. Microsoft released Windows 7 in 2009. With better compatibility and even more new features, Windows 7 resolved the Vista issues and satisfied critics and customers alike.

MOVE TOWARD TOUCH SCREENS

Acknowledging the growing consumer interest in tablets and smartphones, Microsoft radically changed its approach when it released Windows 8 in 2012. Specifically tailored for compatibility with touch-screen devices, Windows 8 rejected the traditional Start menu in favor of a tile-based layout. While tablet and smartphone users welcomed this design, traditional desktop and laptop users did not.

Hoping to reconcile its new aesthetic design with the user desire for traditional functionality, Microsoft introduced Windows 10 in 2015. This was the first version of their OS to be offered as a free upgrade. Windows 10 also introduced a new service model in which the OS would continually receive updates to various features and functions. This model is similar to that employed by Microsoft's competitor Apple. Windows 10 was also the first version of Windows that had a universal application architecture. This meant that apps on Windows 10 could be used on smartphones, tablets, and the Xbox One gaming system as well. This package included options for both the Start menu and the new tile scheme. Windows 10 also featured the debut of Cortana, Microsoft's first digital personal assistant. In 2021, Microsoft released Windows 11. Much like its predecessor, the new operating system was made available to users of the prior version as a free update.

DOMINANCE AND REINVENTION

Just under 75 percent of desktop PCs worldwide ran some version of Windows by January of 2023, according to the website *Statcounter*. The majority (about 69 percent) ran Windows 10, while about 18 percent ran Windows 11. Some PCs also continued to run older Windows OSs, including Windows 7 and Windows 8.1. Windows is sold around the world and comes formatted for a variety of languages. In addition, language interface packs are available for free download and offer support for languages not found

in full versions. Each pack requires a base language that can be activated within the OS after installation.

Given the rising popularity of handheld computing devices, such as tablets and smartphones, the global computer market is no longer based solely on the PC market. While Microsoft continued to dominate the PC market into 2023, the company controlled only about 0.02 percent of the global mobile and tablet OS markets by the start of that year, falling far behind Android and Apple iPhone operating system (iOS). As a result, beginning with the release of Windows 10, Microsoft made changes to its basic strategy. The company reduced its focus on proprietary software. Instead, the company increasingly embraced the potential of open-source software. Future versions of Windows will likely show an increased focus on cloud-based computing, intuitive touch-screen technology, and alternative interface controls such as voice activation and multitouch gestures.

—Jack Lasky, *Micah L. Issitt*

Further Reading

- Brown, Michael. "Microsoft Windows Is 30: A Short History of One of the Most Iconic Tech Products Ever." *International Business Times*, 20 Nov. 2015, www.ibtimes.com/microsoft-windows-30-short-history-one-most-iconic-tech-products-ever-2194091.
- Calore, Michael. "A History of Microsoft Windows." *Wired*, 10 Dec. 2008, www.wired.com/2008/12/wiredphotos31.
- Gibbs, Samuel. "From Windows 1 to Windows 10: 29 Years of Windows Evolution." *The Guardian*, 2 Oct. 2014, www.theguardian.com/technology/2014/oct/02/from-windows-1-to-windows-10-29-years-of-windows-evolution.
- Holcombe, Jane, and Charles Holcombe. *Survey of Operating Systems*. 6th ed., McGraw-Hill Education, 2020.
- McLellan, Charles. "The History of Windows: A Timeline." *ZDNet*, 14 Apr. 2014, www.zdnet.com/article/the-history-of-windows-a-timeline.
- "Operating System Market Share Worldwide—June 2023." *Statcounter*, June 2023, gs.statcounter.com/os-market-share/desktop/worldwide/#monthly-202206-202306.

- Panay, Panos. "Introducing Windows 11." *Microsoft*, 24 June 2021, blogs.windows.com/windowsexperience/2021/06/24/introducing-windows-11.
- Warren, Tom. "Windows Turns 35: A Visual History." *The Verge*, 20 Nov. 2020, www.theverge.com/2015/11/19/9759874/microsoft-windows-35-years-old-visual-history.
- "What Is the History of Microsoft Windows?" *Indiana University Knowledge Base*, 18 Jan. 2018, kb.iu.edu/d/abwa.

WIRELESS NETWORKS

ABSTRACT

Wireless networks allow computers and other internet-enabled devices to connect to the internet without being wired directly to a modem or router. They transmit signals across radio waves instead. Wireless networks make communication services available almost anywhere, without the need for wired connections.

BACKGROUND

Computer networks allow multiple computers to access information stored in other locations and to use common devices, such as printers and file servers. Setting up a traditional computer network requires cables, distributors, routers, and internal and external network cards.

As computers became smaller and therefore more mobile, cables and wires presented challenges. The development of wireless connectivity made it more convenient to use laptops, tablets, and other mobile devices in more places. Wireless networks provide the same connectivity and access as traditional networks without the need for physical cables.

Most wireless networks transmit signals using radio waves, the lowest-frequency waves in the electromagnetic spectrum. A computer sends data across a wireless network through nodes, which are all the hubs, switches, and devices connected to the network. The data are translated into a radio signal and transmitted to the wireless router. The router then

sends the information to the internet through an Ethernet cable. Multiple devices can access the same wireless router to connect to the internet.

OVERVIEW

Broadly speaking, the different types of wireless networks can be divided into four main categories, based on range and how they transmit information.

A personal area network (PAN) covers the shortest range. PANs are typically used by one person to transmit information between two or more devices. The network is generated by one device, such as a cell phone. Any device within range of that device can then communicate with it, or with any other device within its range. The range of a wireless PAN (WPAN) is generally no more than a few meters.

The next-largest type of network is a local area network (LAN). The term was initially used to refer to devices within a limited area, such as a single building, that are connected via cables to a central access point, such as a modem. A wireless LAN (WLAN) works much the same way. Instead of being connected to the individual devices by cables, however, the access point connects to a router that generates a wireless network. This network is omnidirectional, meaning that it is equally strong in all directions. As a result, the signal is weaker, and thus has a shorter range, than if it were focused in one direction.

A wireless wide-area network (WWAN) can cover a range of several miles. To accomplish this, WWANs use directional antennas and typically transmit signals via microwaves. Microwaves have a higher frequency than radio waves, although there is some overlap. While microwaves can travel farther, they cannot penetrate obstacles as well as radio waves. Thus, to use the network, a device must have a direct line of sight to the antenna or be connected to another node that does. A WWAN may be either point-to-point (P2P) or point-to-multipoint (P2MP). P2P, the simplest type, connects one node to



Image via iStock/drogatnev. [Used under license.]

another. P2MP connects multiple nodes to one central access point.

Finally, a mesh network is a wireless network in which all devices connect to each other and relay signals from device to device, without a wired infrastructure. In a mesh network, all nodes—that is, all devices connected to the network—transmit signals.

PROS AND CONS OF WIRELESS

WLANs gained popularity over regular LANs because of their convenience and cost savings. In fact, wireless networks became so prolific that some computer manufacturers phased out Ethernet connection ports on the laptops they produced. By investing in wireless networking hardware, businesses can avoid the trouble and expense of installing cables throughout a building. They can quickly

expand the network when needed. Consumers can easily set up home networks for use with laptops, tablets, and smartphones. Users can be more productive by accessing the internet wherever they are.

However, wireless networks have drawbacks as well. Their smaller range makes additional equipment, such as repeaters, necessary for larger buildings. In addition, radio waves are prone to interference, making reliability an issue. Security is also a concern. Since data are transmitted through the air, wireless networks involve greater risk.

A BIG IMPACT FROM INVISIBLE RADIO WAVES

Wireless networks have allowed more people around the world to access the internet from more locations than ever. In business, wireless networks enable

companies to operate with more speed, flexibility, and connection. In health care, they allow physicians to consult with faraway specialists or to check in with patients in rural areas. For individuals, wireless networks bring friends and families closer, enabling them to keep in more frequent contact and allow users to stream entertainment or download books while on the go. News is delivered as it happens. People immediately share their reactions, while families and friends can check on those affected.

Without wireless technology, there would be no smartphones and no texting, and there would be less access to social media. Social media enables people all over the world to express themselves, whether for personal or political reasons, and has become an important force for political awareness and connection over shared interests.

EVOLUTION OF WIRELESS NETWORKS

Businesses are increasingly moving to cloud-based networks, which eliminate on-site hardware and move all infrastructure, administration, and processes to remote servers. Communities are creating mesh networks with their own infrastructure to share resources and connect through their mobile devices. Such mesh networks provide more reliable communication and connection during emergencies or natural disasters. At home, consumers are taking advantage of new technology to make wireless connection to the internet easier and more convenient. It is clear that the proliferation of wireless networks has changed the way the world learns, communicates, and conducts business. As the cost of wireless technology decreases, the benefits will spread even further.

Further Reading

- “Computer—Networking.” *Tutorials Point*, www.tutorialspoint.com/computer_fundamentals/computer_networking.htm.
- “Data Communication & Computer Network.” *Tutorials Point*, www.tutorialspoint.com/data_communication_computer_network/index.htm.

De Filippi, Primavera. “It’s Time to Take Mesh Networks Seriously (and Not Just for the Reasons You Think).” *Wired*, 2 Jan. 2014, www.wired.com/2014/01/its-time-to-take-mesh-networks-seriously-and-not-just-for-the-reasons-you-think.

Kizza, Joseph Migga. *Guide to Computer Network Security*. 6th ed., Springer, 2024.

Lander, Steve. “Disadvantages or Problems for Implementing Wi-Fi Technology.” *Chron*, smallbusiness.chron.com/disadvantages-problems-implementing-wifi-technology-61914.html.

O’Leary, Timothy, Linda O’Leary, and Daniel O’Leary. *Computing Essentials* 2023. McGraw-Hill, 2022.

Smith, Matthew S. “Wi-Fi vs. Ethernet: Has Wireless Killed Wired?” *Digital Trends*, 18 Jan. 2013, www.digitaltrends.com/computing/wi-fi-vs-ethernet-has-wireless-killed-wired.

“Types of Wireless Networks.” *Commotion Wireless*, commotionwireless.net/docs/cck/networking/types-of-wireless-networks.

“Wireless History Timeline.” *Wireless History Foundation*, wirelesshistoryfoundation.org/wireless-history-project/wireless-history-timeline.

WORKPLACE MONITORING

ABSTRACT

Modern technology makes it possible for firms to monitor many aspects of the workplace, particularly employee activities and performance. Most monitoring systems used are electronic, including computer terminals, email, internet, telephone and smartphone systems, a global position system (GPS), drones, and others. Challenges to workplace monitoring appear in the arena of employee rights and privacy legislation.

BACKGROUND

The practice of monitoring employees at work is known as “workplace monitoring.” According to the US Office of Technology Assessment, workplace monitoring is the collection, storage, analysis, and reporting of information about workers’ activities.

The introduction of computers and other telecommunication technologies in the workplace brought great changes to monitoring practices. Workplace monitoring includes a wide variety of technologies, such as hidden or overt video cameras, a global positioning system (GPS), landline telephones, cell phones and smartphones, computer software and systems, the internet, and drones. Many techniques have been developed to improve workplace monitoring. For example, packet sniffers are computer programs that can analyze communication flow across networks and intercept malicious files. Many businesses monitor all network traffic passing through their servers. Automatic programs can alert managers if a networked computer connects to a malicious domain, block particular websites, and scan emails for spam.

Many organizations monitor their workers in order to protect their property and information, protect employees, and measure the quality of their work and productivity. However, employers must

also be mindful of legal and ethical considerations of workplace monitoring. Employers must work to maintain a sense of trust in their employees when engaging in monitoring. Monitoring practices can generate negative feeling among employees and create legal problems for the employer if they are not implemented carefully.

Further complicating the issue is the increasingly fluid nature of workplace boundaries. For instance, work is often spread across geographical spaces. Many employers have a large number of employees who work away from headquarters, either because they travel or work remotely. This has led to remote monitoring by way of varied technologies and devices, including GPS and drones.

Moreover, a growing amount of work is computerized, through intranet and internet networks. As a result, employers face real risks of employee misuse of these systems. However, these same systems have led to improvements in workplace monitoring technology.

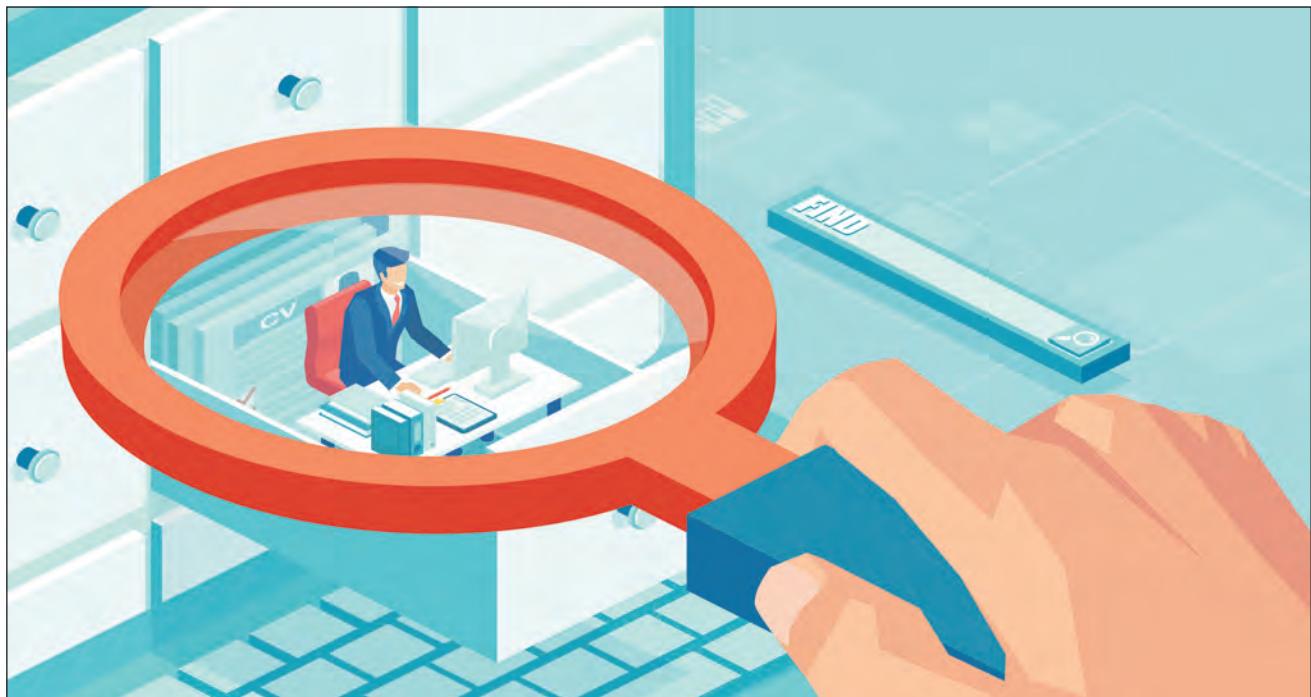


Image via iStock/Feodora Chiosea. [Used under license.]

OVERVIEW

Because of the growing instances of hacking and information theft, employers have legitimate concerns about the security of workplace information. They may also want to conduct quality controls and monitor employee productivity. For example, it is a common practice for call centers to record customer service calls, in a system commonly known as silent monitoring. Another type of system, real-time monitoring, allows managers to analyze usage on computer systems as it occurs. Real-time monitoring helps track not only employee activity but also other firm processes, such as sales data and other trends. It is often used in conjunction with remote monitoring. Remote monitoring involves tracking the activity of employees who work off-site.

Hundreds of software programs and other technologies are available to monitor the workplace. Some of these programs are free. Companies can establish their own monitoring systems. Others prefer to hire firms that provide the technology and analyze the data. The data retrieved by monitoring technologies may be used to identify information leaks or theft, evaluate employee performance, detect malware, or analyze business trends. Among the latest monitoring technologies are drones. Drones are mainly used in real estate, construction, and agriculture.

There are many ways in which electronic workplace monitoring is used. According to the company ExpressVPN, nearly 80 percent of US employers used electronic monitoring software to monitor their employees as of 2023. In addition to monitoring workers' email communication and internet usage, some employers use monitoring technology in order to assess employee performance by measuring time spent at the computer or keystroke speed.

LEGAL AND ETHICAL CONSIDERATIONS

The increasing breadth of workplace monitoring has raised ethical and legal concerns. On the balance are

the privacy rights of workers. Electronic workplace monitoring has become so common that labor rights advocates have raised concerns about the abuse or inappropriate use of monitoring practices. On the other hand, employers are concerned about liability costs and legal consequences.

In the opinion of some experts, electronic workplace monitoring is subject to insufficient government regulation. This may be due to its constant innovations and its relatively new status. Technically, employers are legally allowed to listen to, watch over, record, and read all work-related forms of communication. However, federal law stipulates that personal calls cannot be monitored.

Experts recommend companies ensure their monitoring practices are fair and consistent. It is crucial to implement measures to prevent managers from engaging in abuse of power and other illegal activities using monitoring technologies. Staff in charge of workplace monitoring must be adequately trained. Some organizations implement transparent monitoring in order to make employees feel more at ease with the process. Transparent monitoring welcomes the participation of employees in the process. Finally, when employers suspect employees of engaging in criminal action, experts recommend they alert the authorities rather than try to set up a sting operation on their own.

Debate continues about what employers should be allowed to monitor and to what extent employees have the right to know they are being monitored. Nevertheless, employees should always assume that they are being monitored and keep all private or personal communication in separate accounts and devices.

—Trudy Mercadal

Further Reading

Marks, Gene. "Yes, You Should Monitor Your Remote Workers—But Not Because You Don't Trust Them."

- The Guardian*, 25 Sept. 2022, www.theguardian.com/business/2022/sep/25/monitor-workers-at-home-security-cybercrime.
- Plumb, Charles. “Drones in the Workplace.” *McAfee and Taft*, 14 Dec. 2015, www.mcafeetaft.com/drones-in-the-workplace.
- Rocchi, Walter. *Cybersecurity and Privacy Law Handbook*. Packt, 2022.
- Smith, Eric N. *Workplace Security Essentials: A Guide for Helping Organizations Create Safe Work Environments*. Butterworth-Heinemann, 2014.
- Tabak, Filiz, and William Smith. “Privacy and Electronic Monitoring in the Workplace: A Model of Managerial Cognition and Relational Trust Development.” *Employee Responsibilities and Rights Journal*, vol. 17, no. 3, 2005, pp. 173–89.
- Tong, Goh Chiew. “Employee Surveillance Is on the Rise—and That Could Backfire on Employers.” *CNBC Make It*, 25 Apr. 2023, www.cnbc.com/2023/04/24/employee-surveillance-is-on-the-rise-that-could-backfire-on-employers.html.
- Yakowitz, Will. “When Monitoring Your Employees Goes Horribly Wrong.” *Inc.*, www.inc.com/will-yakowicz/drones-catch-employees-having-sex-and-other-employee-monitoring-gone-wrong.html.
- Yerby, Jonathan. “Legal and Ethical Issues of Employee Monitoring.” *Online Journal of Applied Knowledge Management*, vol. 1, no. 2, 2013, pp. 4–54.

X

XML

ABSTRACT

Extensible markup language (XML) is a programming language used to categorize and describe data. As a type of markup language, XML uses tags or rules for tags to add information about data. Tags used in XML coding help describe the data inside the tags. XML does not rely on any particular software or hardware. It also is written in plain text, so it can be shared easily among different programs and devices.

BACKGROUND

The World Wide Web Consortium (W3C)—a group of volunteers and paid employees who create standards for the web—wanted to create a new type of markup language that was useful on the internet. The group decided to base the new language on another type of markup language called standard generalized markup language (SGML). Standard generalized markup language is made up of elements, and these elements usually consist of a start tag, content, and an end tag (e.g., <firstname>Jose</firstname>). The group from W3C structured XML in much the same way.

Members of W3C developed the first draft of XML in 1996. They distributed coding instructions in a twenty-five-page manual and released it to the public. The W3C recommended the use of XML in 1998. Soon, XML became an important markup language that many people used for different purposes. Some people used XML on the web, and others used it in electronic publishing, in databases, and in other types of documents. The W3C working group intended to create a markup

language for the internet, but they created a markup language capable of being used in many different situations.

Throughout the history of XML, groups at W3C and other individuals and groups around the world have worked to further develop the language. The W3C publishes its work so others can use XML and make changes and enhancements to the language. Multiple conferences about XML, its standards, and its uses are held around the world each year, proving the language's continued popularity.

OVERVIEW

Even though XML is a markup language, it is different from some other markup languages because it



Image via iStock/Eugene B-sov. [Used under license.]

was created to label and categorize data rather than display data. One of the most popular markup languages is hypertext markup language (HTML).

HTML adds information about the format and the appearance of text. XML, however, adds information about the data included inside the tags. The goal of HTML is to display text in a certain way, while the goal of XML is to describe data.

XML and HTML have another important difference: XML tags are not predefined, but HTML tags are. A person using HTML has to memorize or look up specific tags to use to have data display in a particular way. XML users, however, can develop unique tags to describe data. One other difference between XML and HTML is that XML is more rigid. HTML is a fairly flexible language and can tolerate some coding errors. XML, however, has to be formatted very specifically because errors can be introduced easily.

USES OF XML

One of the main uses of XML is to categorize data. XML can be used on the web to classify information. The idea of data categorization is especially important on the Semantic Web, which is the web of data. XML also can be used to separate data from other elements on a web page. For example, a programmer can use XML to keep the data of a web page separate from the HTML coding on that page. This separation allows the programmer to update the data without updating the HTML.

Another important use of XML is data transport. At times, data has to be shared between two different programs that are incompatible with one another. Because XML does not rely on a specific type of software, it is compatible with many different programs. Sometimes XML can help two incompatible programs share data with each other. In a similar way, data sometimes has to be shared when a platform (either software or hardware) is being upgraded. These upgrades can be time consuming

because of the large amount of data that needs to be shared. However, XML is useful because it can make transferring the data much simpler.

ADDING XML TO DOCUMENTS

One way people use XML is to add markup to documents. Often in documents using XML, the first line of code is called the declaration line. The declaration line states that XML is being used and identifies the version of XML being used (e.g., <?xml version='1.0' encoding='UTF-8'?>). The line after the declaration is a line that describes the root element. This information tells what type of document is being coded (e.g., <note>). The lines after the root element contain the content of the document and can be coded to show the function of each piece of data (e.g., <heading>, <body>, <conclusion>). The document then ends with a tag that shows the text is complete (e.g., </note>).

People using XML have to remember some important rules about the language. If any opening tag is used, a corresponding closing tag must also be used (e.g., <firstname> and </firstname> or <note> and </note>). Other markup languages, such as HTML, do not always require closing tags, but XML does. Along the same lines, XML tags have to be nested properly. That means the elements opened first must be closed last. For example, <i>word</i> is nested incorrectly, but <i>word</i> is nested correctly. Another factor people using XML have to remember is that the language is case sensitive, so the tag <Note> and the tag <note> are not the same.

—Elizabeth Mohn

Further Reading

“A Brief SGML Tutorial.” *W3C*, www.w3.org/TR/WD-html40-970708/intro/sgmltut.html. Campbell-Kelly, Martin, William F. Aspray, Jeffrey R. Yost, Honghong Tinn, and Gerardo Con Díaz.

- Computer: A History of the Information Machine.* 4th ed., Routledge, 2023.
- “Development History.” *W3C*, 6 Jan. 2003, www.w3.org/XML/hist2002.
- “Extensible Markup Language (XML).” *W3C*, 11 Oct. 2016, www.w3.org/XML.
- Frain, Ben. *Design with HTML5 and CSS*. 4th ed., Packt, 2022.
- “XML.” *PC Mag*, www.pc当地/encyclopedia/term/55048/xml.
- “XML Tutorial.” *W3Schools*, www.w3schools.com/xml.

Y

Y2K CRISIS

ABSTRACT

In the years leading up to the year 2000, some computer experts warned that the longtime practice of rendering years in a two-digit format could cause problems within computer systems, prompting global efforts to mitigate the effects of the so-called Y2K bug as well as widespread public concern. Despite predictions of disaster to businesses, governments, and public services, the worldwide transition to the year 2000 caused few problems for computers, thanks to extensive preparations.

BACKGROUND

Across North America and around the world, people waited nervously as midnight approached on December 31, 1999. Many wondered whether predictions of doom about the year 2000 computer transition, popularly called the Y2K (for “year 2000,” with *k* representing the Greek *kilo* for “thousand”) problem or the millennium bug, would prove correct: would power and water supplies fail, food distribution be disrupted, the economy begin to disintegrate, nuclear missiles launch accidentally, and widespread civil disturbances begin as computers and computer networks failed everywhere? No one was completely sure how to answer these questions, even though massive efforts to avert any possible problems occupied governments and businesses throughout the late 1990s.

A definitive answer was apparent within days after January 1, 2000, came and went: There were no disasters. Some computer problems did occur on New Year’s Day and afterward, but they were so few, so inconsequential, and so easily corrected

that even the most optimistic experts were surprised.

The story of the Y2K transition problem began with the development of commercial computing. In 1957, Rear Admiral Grace Murray Hopper invented a programming language called FLOW-MATIC, the first to be based on English in order to make computers easier for businesses to use. FLOW-MATIC formed the basis for COBOL, the name of which derived from “common business-oriented language.” The principal data storage device of the times was the eighty-column punch card. To conserve space, COBOL used only six digits to represent any given calendar date—two each for the month, the day, and the year, as in “04/15/53” for April 15, 1953. This shortcut dating method saved as much as twenty dollars in the production of a date-sensitive record, so it was an important way of economizing as businesses grew dependent on computers.

Computer scientists, led by Robert Bemer, one of COBOL’s developers, warned that using only two digits for each year designation would later cause problems and argued for a four-digit style. However, the desire of businesses to minimize their immediate expenses overwhelmed such objections. When International Business Machines Corporation (IBM) designed its System/360 mainframe computer (marketed in 1964), it incorporated the COBOL two-digit year format. That computer, and its dating style, became the industry standard. Bemer again published warnings about the dating problem in 1971 and 1979, but his protests stirred little interest and no change. To most businesses and government agencies the heart of the danger—the arrival of the



A Best Buy sticker from 1999 recommending that their customers turn off their computers ahead of midnight. Image via Wikimedia Commons. [Public domain.]

year 2000—seemed too far away to worry about at the time.

In 1993, Peter de Jager, a Canadian computer engineer, published an article with the alarming title "Doomsday 2000" in *Computerworld*, a magazine aimed at technology managers. In that article and subsequent lectures, de Jager argued that the Y2K bug could initiate massive disruptions and plunge the economy into a recession. Computers, he pointed out, would read a date such as "01/01/00" as "January 1, 1900," because there was no provision for numbers 2000 and higher in their software, and computer-processed date-sensitive information was fundamental to national infrastructures. There were already signs that he was right: That same year, a US missile warning system malfunctioned when its computer clocks were experimentally turned forward to 01/01/00.

During the next seven years, other glitches turned up sporadically during testing. At the same time,

with gathering momentum, attempts were under way to remedy the date problem. In 1996, Senator Daniel Patrick Moynihan of New York held committee hearings on the Y2K bug and directed the Congressional Research Service to study the potential problem. The report produced as a result helped to convince President Bill Clinton to establish the President's Council on Year 2000 Conversion, directed by John A. Koskinen, in 1998. Koskinen oversaw programs to adjust the software used by government agencies. The US government also ordered many organizations essential to the economy, such as stock brokerages, to fix the problem—that is, to "become Y2K compliant"—by August 31, 1999.

Despite initial skepticism about the true seriousness of the Y2K problem, big companies soon undertook remediation efforts of their own. Most employed one or more of three basic methods, termed "windowing," "time shifting," and "encapsulation." Windowing, the most common, entailed

teaching computers to read 00 as 2000 and to place other two-digit year dates in their appropriate century. Time shifting involved programming computers to recalculate dates automatically following a formula. Encapsulation, a refinement of time shifting, added 28 to two-digit years to synchronize computers with the cycles of days of the week and of leap years. January 1, 2000, for instance, would not fall on the same day of the week as January 1, 2005, and so adjustments were necessary to accommodate such discrepancies. All three techniques required exhaustive searches and reprogramming of mainframes and personal computers that processed time-sensitive information, such as pay schedules and product expiration dates.

Computer chips embedded in various kinds of equipment posed further difficulties. Since their introduction in the early 1970s, microprocessors had been built into appliances, tools, automobiles, and machinery of all kinds: By the late 1990s, they controlled the operations of nuclear power plants, utilities, hospital technology, weaponry, and climate control systems in buildings, in addition to such mundane devices as home microwave ovens. With between 32 billion and 40 billion chips in use by 2000, their potential for causing trouble was enormous even if only a fraction of them controlled time-sensitive operations, and often the chips were difficult to extract and replace.

OVERVIEW

As the year 2000 approached, the frenzy of preparation increased, and predictions of disaster grew more ominous. Some consumers stockpiled generators, money, food, and fuel in case utility and supply systems became disrupted on January 1, 2000. Some government agencies failed to meet their August 31 deadline for Y2K compliance. Large corporations worried that their preparations were insufficient, and about a third of small American businesses made no preparations whatsoever.

When the moment of truth came and passed on New Year's Day of 2000, no system failures occurred, and essential services were uninterrupted even in countries, such as Russia, that were both sophisticated in terms of the computer technology in use and largely unprepared for the date turnover. There were problems, however. Some were comical, as when a 105-year-old man was directed to attend kindergarten, some newborn children were registered as born in 1900, and the website of the US Naval Observatory, the government's official time-keeper, proclaimed the date as "January 1, 19100."

Most problems were simply annoyances. Some records were accidentally deleted, software used to service credit cards double-charged some users, renters returning videos that were one day overdue were billed for thousands of dollars in late charges, and cell phone messages were lost. Most such problems were easily corrected. Other problems were potentially more serious. For example, one Wall Street computer inflated a few stock values, and a small number of company security systems failed. Some satellites, including one US spy satellite, lost contact with their controllers. Software modifications and simple common sense were sufficient to rectify the errors.

The Y2K problem did not end with the New Year's date turnover, however. One expert calculated that only about 10 percent of the problems would turn up immediately. For instance, the leap year day February 29, 2000, caused at least 250 glitches in seventy-five countries, although none was major.

SIGNIFICANCE

Even though the year 2000 turnover passed without disaster, the event itself and the preparations for it revealed how thoroughly modern society had come to rely on a sophisticated technological infrastructure. Controlling and coordinating that infrastructure are computers and, increasingly since about

1990, computer networks, especially the internet. The Y2K threat to information technology (IT) elicited one of the largest and most effective joint responses among businesses and government agencies in US history as well as extensive international cooperation. Programmers successfully corrected well over 95 percent of Y2K-related problems. People around the world, particularly Americans, became more keenly aware of their dependence on computers, but they also learned that managing computers is not beyond their control.

Because of its very success, the remediation effort had its critics, some of them bitterly vocal. In part, critics wondered how so little could go wrong if the Y2K bug had really been as big a threat as IT experts had insisted. Editorials and letters to the editors of business periodicals accused the large coterie of Y2K experts of exaggerating the danger in order to scare businesses into spending money unnecessarily on remediation. They denounced the media hoopla and claimed that the predictions of doom had been psychologically harmful.

Critics were also outraged by the price of remediation. In 1993, de Jager estimated that addressing the problem would cost between \$50 billion and \$75 billion worldwide. He was far too conservative. The United States alone spent \$100 billion, including \$8.5 billion by the federal government, according to the US Department of Commerce. The worldwide bill was estimated at between \$500 billion and \$600 billion. De Jager and his colleagues admitted that costs may have been unnecessarily high, but they insisted that the money was well spent, because without remediation largescale systems malfunctions would have occurred, costing much more money to repair and causing civil disorder. The controversy created a measure of ill will between businesses and IT specialists.

In addition to avoiding disaster, Y2K remediation had immediate tangible benefits for some segments of society. The rush to stockpile food and equipment

before the New Year brought record profits to some manufacturers and retailers. Computer programmers were in high demand, and consultants earned money with books, articles, lectures, and websites offering advice. Companies were launched specifically to solve Y2K problems for businesses; many of them afterward diversified to serve the general needs of electronic commerce. The close scrutiny of programmers benefited companies' overhead expenses as well. Programmers removed the clutter of computer code that had accumulated during decades of reprogramming and computer upgrades and uncovered applications that could be eliminated, streamlining business computer systems. Many companies learned how to conduct contingency planning for IT malfunctions. Others, especially small businesses, learned how to use computers effectively for the first time.

Less tangible, but at least as important, were two general lessons for businesses and governments. First, they were forced to reevaluate their dependence on technology, to understand the complexity of that technology, and to be aware of the danger to the technology from unforeseen conditions, such as the Y2K date problem. Second, they learned dramatically that forty years of development and use had built a computer infrastructure with serious inconsistencies and imperfections. Accordingly, commentators suggested that IT specialists, especially those developing large projects, should undergo certification to ensure coherent planning.

The President's Council on Year 2000 Conversion was demobilized after February 29, 2000, but the Y2K bug continued to have direct and indirect effects on business. Many organizations had deferred computer data entry and innovations in order to devote employee time to Y2K remediation, so following the New Year, they had to clear up the work backlog. Moreover, according to de Jager and other analysts, the programming techniques used to remedy Y2K dating problems were stopgaps, often

not coordinated between computer systems and potentially only temporarily effective. Windowing and time shifting could insinuate subtle changes into computer codes, changes that might not cause problems for decades.

—Roger Smith

Further Reading

De Jager, Peter. “Y2K: So Many Bugs...So Little Time.” *Scientific American*, Jan. 1999, pp. 88–93.

Halton, Clay. “The Truth about Y2K: What Did and Didn’t Happen in the Year 2000.” *Investopedia*, 30 May 2023, www.investopedia.com/terms/y/y2k.asp.

JD Consulting. *Y2K Procrastinator’s Guide*. Charles River Media, 2000.

Kuo, L. Jay, and Edward M. Dua. *Crisis Investing for the Year 2000: How to Profit from the Coming Y2K Computer Crash*. Birch Lane Press, 1999.

McGuigan, Dermot, and Beverly Jacobson. *Y2K and Y-O-U: A Sane Person’s Home-Preparation Guide*. Chelsea Green, 1999.

Uenuma, Francine. “20 Years Later, the Y2K Bug Seems Like a Joke—Because Those Behind the Scenes Took It Seriously.” *Time*, 30 Dec. 2019, time.com/5752129/y2k-bug-history/.

Yourdon, Edward, and Jennifer Yourdon. *Time Bomb 2000*. 2nd ed., Prentice Hall, 1999.

Z

ZERO TRUST SECURITY

ABSTRACT

Zero trust security is an information technology (IT) model that assumes that all of a private network's traffic, no matter what the source, should be seen as untrusted. Trust is established by identity verification for everyone and everything trying to gain access to a network and the resources stored there. A primary goal of zero trust security is to achieve the highest level of security possible while maintaining the highest level of usability. As a result, network access abuse is limited, and resources stored on a network are protected.

BACKGROUND

Traditional information technology (IT) security was built on the concept of implicit acceptance of trust inside a private network. That is, if a credential checked out, network access was automatically granted by default. Resources on a private network were considered secure if accessed with credentials. Resources were difficult to access outside of the network perimeter. For example, an organization could store company data in a data center or network it controlled, have dedicated centralized security, and reject any attempt to access data from outside the network.

This IT security protocol did not provide enough security as computing evolved in the early twenty-first century. The late 2000s saw the rise of cloud services and vendors as well as the increasing popularity of remote working. Cloud services involve storing resources outside of a private network perimeter. A third-party vendor generally provides cloud services.

Cloud services are convenient because resources can be easily accessed outside of an office environment. However, cloud services are also less secure because resources are stored outside of an organization's private network and centralized network security. The ability to access an organization's resources from anywhere created new security challenges for organizations seeking to ensure the safety of their resources. A new network security model was needed because the nature of the network had fundamentally changed.

In 2009, analyst John Kindervag of the research and consulting firm Forrester devised a model that addressed this security issue, which he called *zero trust*. Instead of assuming trust for network and data access, Kindervag's zero trust model assumes that all network traffic is untrusted. To access a network, trust has to be explicitly proven by users and machines. Kindervag's model also calls for all resources to be accessed securely, no matter what the location, and for all network traffic to be inspected and logged so security issues can be more easily identified.

OVERVIEW

In 2014, a zero trust security model was implemented by Google in the form of BeyondCorp, which offered a practical application of zero trust security within that company. With BeyondCorp, all access to a network and its resources had to be authenticated, authorized, and encrypted. Securing user access with strong authentication greatly enhanced security at Google.

Adoption of zero trust security soon spread throughout the tech community and the business

world. At the same time, workforces became increasingly mobile and cloud services more widely used.

Analysts at Gartner, a global research and advisory company, had begun working on a concept for the same purpose as zero trust by 2017. The Gartner concept was originally called continuous adaptive risk and trust assessment (CARTA). In 2019, Gartner analyst Steve Riley renamed that security concept Zero Trust Network Access, or ZTNA, and published an influential market report on the subject. ZTNA became a primary technology for implementing zero trust security within organizations. Zero trust security also became a key part of what Gartner dubbed secure access service edge (SASE) solutions. SASE is an IT model that brings together networking and security services, including ZTNA, on a single cloud platform.

PRINCIPLES

The implementation of zero trust security on a network involves several key principles and practices. First, because there is no automatic trust on a network, the identities and privileges of users as well as devices must be continuously verified. Once a login and connection have been established, they time out regularly, and users and devices must be verified over and over again. This practice enhances resource security.

The principle of multifactor authentication, or MFA, is particularly important to zero trust security. To authenticate a user under MFA, at least two pieces of evidence are needed. Users cannot gain access merely by entering a password. Some platforms require two-factor authorization (2FA), a type of MFA. After entering a password, a user also must enter a code sent to another device to complete the authentication process.

Another key principle is that of least privilege. Under this principle, users are given only as much access as they need to resources on a network. User permissions, which determine what can be accessed

by each user and device, are carefully managed. As a result, sensitive resources are better protected.

Microsegmentation is another important principle of zero trust security. In microsegmentation, security parameters are broken up into small segments called microsegments. Authenticated users are granted access only to the microsegments of the network they need. Such users cannot access any other part of the network without a separate authorization for each.

Lastly, lateral movement prevention is a core concept of zero trust security. Before zero trust security, when an attacker gained access to a network, the attacker could move around the network and compromise other parts even if the attacker's entry point was discovered. Zero trust contains attackers because networks are segmented. If an attacker gains access to one part of a network, they cannot move to other microsegments. Network security also limits the damage an attacker can cause. After an attacker is detected, a compromised user account or device can immediately have its network access revoked.

BENEFITS

By implementing zero trust security measures, IT security professionals can ensure that there are fewer ways to attack and compromise a network and its resources. Constant verification and the use of MFA reduces the risk of attack and the outfall from the theft of user credentials. When a successful attack on a network does occur, damage is limited because any breach is restricted to a network microsegment. As a result, the impact of the breach is reduced.

—A. Petruso

Further Reading

Apirion, Almog. "Zero-Trust Access Is the Future of Secure Remote Access." *Forbes*, 27 July 2023, www.forbes.com/sites/forbestechcouncil/2023/07/27/zero-trust-access-is-the-future-of-secure-remote-access/?sh=708bcae67454.

Garbis, Jason, and Jerry W. Chapman. *Zero Trust Security: An Enterprise Guide*. Apress, 2021.

Gilman, Evan, and Doug Barth. *Zero Trust Networks: Building Secure Systems in Untrusted Networks*. O'Reilly Media, 2017.

“How to Implement Zero Trust: A Comprehensive Guide.” *Security Boulevard*, 31 July 2023, securityboulevard.com/2023/07/how-to-implement-zero-trust-a-comprehensive-guide.

Kudrati, Abbas, and Binil Pillai. *Zero Trust Journey across the Digital Estate*. CRC Press, 2022.

Townsend, Kevin. “The History and Evolution of Zero Trust.” *SecurityWeek*, 11 July 2022, www.securityweek.com/history-and-evolution-zero-trust.

“What Is Zero Trust Security? Zero Trust Architecture Model Explained.” *ASEE*, 13 Mar. 2023, cybersecurity.asee.co/blog/zero-trust-security-architecture-explained.

BIBLIOGRAPHY

- “‘123456’ Maintains the Top Spot on SplashData’s Annual ‘Worst Passwords’ List.” *SplashData News*, 20 Jan. 2015, web.archive.org/web/20150207065500/http://splashdata.com/press/worst-passwords-of-2014.htm.
- “6 Types of Cyber Security Testing and Assessments.” *Sapphire*, www.sapphire.net/cybersecurity/cyber-security-testing.
- “2012 Internet Crime Report Released: More Than 280,000 Complaints of Online Criminal Activity Reported in 2012.” *Federal Bureau of Investigation*, 14 May 2013, www.fbi.gov/sandiego/press-releases/2013/2012-internet-crime-report-released.
- “2016 Presidential Campaign Hacking Fast Facts.” *CNN*, 23 Oct. 2023, www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html.
- Abagnale, Frank W. *Stealing Your Life: The Ultimate Identity Theft Prevention Plan*. Broadway Books, 2008.
- Ablon, Lillian, Martin C. Libicki, and Andrea A. Golay. Markets for Cybercrime Tools and Stolen Data. RAND Corporation, 2014, www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.
- “About Firewalls.” *University Information Technology Services Knowledge Base*, 1 June 2021, kb.iu.edu/d/aoru.
- “About Us.” *ISO*, www.iso.org/about-us.html.
- Abraham, Nikhil. “Building Mobile Web Apps.” *Dummies*, 26 Mar. 2016, www.dummies.com/programming/building-mobile-web-apps.
- Abraham, Prabhakaran, Mustafa Almahdi Algaet, and Ali Ahmad Milad. “Performance and Efficient Allocation of Virtual Internet Protocol Addressing in Next Generation Network Environment.” *Australian Journal of Basic & Applied Sciences*, vol. 7, no. 7, 2013, pp. 827-32.
- Abrams, Abigail. “Here’s What We Know So Far about Russia’s 2016 Meddling.” *Time*, 18 Apr. 2019, time.com/5565991/russia-influence-2016-election.
- Abu-Mostafa, Yaser S. “Machines That Think for Themselves.” *Scientific American*, July 2012, pp. 78-81.
- “Access Control.” *NIST Computer Security Resource Center*, csrc.nist.gov/glossary/term/access_control.
- Alali, Mansour, et al. “Improving Risk Assessment Model of Cyber Security Using Fuzzy Logic Inference System.” *Computers & Security*, vol. 74, 2018, pp. 323-39.
- Alderman, Ellen, and Caroline Kennedy. *The Right to Privacy*. Knopf, 1995.
- Alejandro Arzate, Hector. “Cyberbullying Is on the Rise among Teenagers, National Survey Finds.” *Education Week*, 15 July 2019, blogs.edweek.org/edweek/District_Dossier/2019/07/cyberbullying_is_on_the_rise_a.html.
- Allen, Anita L. *Unpopular Privacy: What Must We Do?* Oxford UP, 2011.
- Allsopp, Wil. *Unauthorized Access: Physical Penetration Testing for IT Security Teams*. Wiley, 2009.
- Almulhem, Ahmad, and Issa Traore. *Experience with Engineering a Network Forensics System*. Springer, 2005.
- Alpaydin, Ethem. *Machine Learning*. Rev. ed., MIT Press, 2021.
- Amadeo, Ron. “Report: Google Will Graciously Let Android OEMs Build Amazon Fire Devices.” *Ars Technica*, 28 Oct. 2022, arstechnica.com/gadgets/2022/10/report-google-will-graciously-let-android-oems-build-amazon-fire-devices.
- _____. “The (Updated) History of Android.” *Ars Technica*, 31 Oct. 2016, arstechnica.com/gadgets/2016/10/building-android-a-4000-word-history-of-googles-mobile-os.
- Anderson, James. “Computer Security Threat Monitoring and Surveillance.” James P. Anderson Co., 1980, csrc.nist.gov/files/pubs/conference/1998/10/08/proceedings-of-the-21st-nissc-1998/final/docs/early-cs-papers/ande80.pdf.
- Anderson, James M., et al. “Autonomous Vehicle Technology: A Guide for Policymakers.” *RAND*, 2014, www.rand.org/pubs/research_reports/RR443-2.html.
- Anderson, Jon. “National Computer Forensics Institute Opens 7th Classroom in Hoover.” *Hoover Sun*, 18 Oct. 2022, hooversun.com/news/national-computer-forensics-institute-opens-7th-classroom.
- Anderson, Monica. “A Majority of Teens Have Experienced Some Form of Cyberbullying.” *Pew Research Center*, 27 Sept. 2018, www.pewresearch.org/internet/2018/09/27/a-majority-of-teens-have-experienced-some-form-of-cyberbullying.
- Anderson, Ross. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 3rd ed., Wiley, 2020.
- “Annual Reports.” *Internet Crime Complaint Center (IC3)*, 2022, www.ic3.gov/Home/AnnualReports?redirect=true.
- Apirion, Almog. “Zero-Trust Access Is the Future of Secure Remote Access.” *Forbes*, 27 July 2023, www.forbes.com/sites/forbestechcouncil/2023/07/27/zero-

- trust-access-is-the-future-of-secure-remote-access/?sh=7
08bcae67454.
- “App Store.” *Apple*, 2023, www.apple.com/app-store.
- Arquilla, John. “Cyberwar Is Already Upon Us.” *Foreign Policy*, 27 Feb. 2012, foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us.
- Assante, Mike. *CyberSkills Task Force Report Fall 2012*. US Department of Homeland Security, 2012.
- “Assessing Russian Activities and Intentions in Recent US Elections.” *Office of the Director of National Intelligence*, 6 Jan. 2017, www.dni.gov/files/documents/ICA_2017_01.pdf.
- Audry, Sofian. *Art in the Age of Machine Learning*. MIT Press, 2021.
- Auxier, Brooke, et. al. *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*. Pew Research Center, 2019.
- Aycock, John Daniel. *Spyware and Adware*. Springer, 2011.
- Baca, Murtha, editor. *Introduction to Metadata*. 3rd ed., Getty Research Institute, 2016.
- Badia, Antonio, and Daniel Lemire. “A Call to Arms: Revisiting Database Design.” *ACM SIGMOD Record*, vol. 40, no. 3, 2009, pp. 61-69.
- Bagwell, Karen. “Teaching, Not Technology, Needed to Enforce Internet Rules.” *Education Daily*, vol. 40, no. 212, 2007, p. 2.
- Banga, Cameron, and Josh Weinhold. *Essential Mobile Interaction Design: Perfecting Interface Design in Mobile Apps*. Addison-Wesley, 2014.
- Banham, R. “Enterprising Views of Risk Management.” *Journal of Accountancy*, 1 June 2004, www.journalofaccountancy.com/issues/2004/jun/enterprisingviewsofriskmanagement.html.
- Banik, Subrata, and Vincent Zimmer. *System Firmware: An Essential Guide to Open Source and Embedded Solutions*. Apress, 2022.
- Barnes, Julian E., and Thomas Gibbons-Neff. “U.S. Carried Out Cyberattacks on Iran.” *New York Times*, 22 June 2019, www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html.
- Barrett Lidsky, Lyrissa. “Silencing John Doe: Defamation and Discourse in Cyberspace.” *Duke Law Journal*, vol. 49, no. 4, 2000, pp. 855-946.
- Barth, Bradley. “GOSSIPGIRL Stuxnet Group Had ‘4th Man’; Unknown Version of Flame & Duqu Found.” *SC Media*, 10 Apr. 2019, web.archive.org/web/20200806024942/www.scmagazineuk.com/gossipgirl-stuxnet-group-4th-man-unknown-version-flame-duqu-found/article/1581579.
- Bas, Patrick, et al. *Watermarking Security*. Springer Singapore, 2016.
- Basl, John. “The Ethics of Creating Artificial Consciousness.” *American Philosophical Association Newsletters: Philosophy and Computers*, vol. 13, no. 1, 2013, pp. 25-30.
- Batty, M., et. al. “Smart Cities of the Future.” *European Physical Journal: Special Topics*, vol. 214, no. 1, Nov. 2012, pp. 481-518.
- Beales, J. Howard. *Legislative Efforts to Combat Spam: Joint Hearing before...108th Congress, 1st Session, July 9, 2003*. US Government Printing Office, 2003.
- Beattie, Andrew. “Cloud Computing: Why the Buzz?” *Techopedia*, 9 Feb. 2012, www.techopedia.com/2/27830/trends/cloud-computing/cloud-computing-why-the-buzz.
- Belani, Gaurav. “The Use of Artificial Intelligence in Cybersecurity: A Review.” *IEEE Computer Society*, www.computer.org/publications/tech-news/trends/the-use-of-artificial-intelligence-in-cybersecurity.
- Bell, Mary Ann, Mary Ann Berry, and James L. Van Roekel. *Internet and Personal Computing Fads*. Haworth Press, 2004.
- Belsey, Bill. “Cyberbullying: An Emerging Threat to the ‘Always On’ Generation.” *Bullying.org*, 2004, cyberbullying.ca/pdf/Cyberbullying_Article_by_Bill_Belsey.pdf.
- Bennett, Samuel. “Russia’s Artificial Intelligence Boom May Not Survive the War.” *Center for a New American Security*, 15 Apr. 2022, www.cnas.org/publications/commentary/russias-artificial-intelligence-boom-may-not-survive-the-war.
- Benjamin, Arthur T., and Jennifer J. Quinn. *Proofs That Really Count-The Art of Combinatorial Proof*. Mathematical Association of America, 2003.
- Bennett, Brian, and Chris Megerian. “U.S. Sanctions Russians for Cyberattacks on Power Grid and Election Meddling.” *Governing*, 16 Mar. 2018, www.governing.com/archive/tns-russia-water-electric-energy-grid-cyber.html.
- Bennett, Colin J. *The Privacy Advocates: Resisting the Spread of Surveillance*. MIT Press, 2008.
- Berghel, Hal. “The Discipline of Internet Forensics.” *Communications of the ACM*, vol. 46, 2003, pp. 15-20.
- Bergman, Ronen, and Mark Mazzetti. “The Battle for the World’s Most Powerful Cyberweapon.” *New York Times*, 31 Jan. 2022, www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html.
- Berlatsky, Noah. *Artificial Intelligence*. Greenhaven Press, 2011.

- Bernal, Paul. *Internet Privacy Rights: Right to Protect Autonomy*. Cambridge UP, 2014.
- Berners-Lee, Tim. *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor*. Harper, 1999.
- Bernescu, Laura. "When Is a Hack Not a Hack: Addressing the CFAA's Applicability to the Internet Service Context." *University of Chicago Legal Forum*, 2013, p. 633.
- Berry, M. A. J., and G. Linoff. *Data Mining Techniques for Marketing, Sales and Customer Support*. Wiley, 1997.
- Bhunia, Swarup, and Mark Tehranipoor. *Hardware Security: A Hands-On Learning Approach*. Morgan Kaufmann, 2019.
- "Biden-Harris Administration Announces CHIPS for America Funding Opportunity to Strengthen Semiconductor Supply Chains." *US Department of Commerce*, 29 Sept. 2023, www.commerce.gov/news/press-releases/2023/09/biden-harris-administration-announces-chips-america-funding-opportunity.
- Bidgoli, Hossein, editor. "Infrastructure for the Internet, Computer Networks, and Secure Information Transfer." *Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management*. Vol. 3, Wiley, 2006, pp. 337-808.
- Bing, Christopher. "REFILE-EXCLUSIVE-U.S. Treasury Breached by Hackers Backed by Foreign Government-Sources." *Reuters*, 13 Dec. 2020, www.reuters.com/article/usa-cyber-treasury-idUSL1N2IT0I8.
- Black, Damien. "Weakest Passwords of 2023." *Cybernews*, 15 Nov. 2022, cybernews.com/security/weakest-passwords-2022.
- Black, Jeremy. *The Power of Knowledge: How Information and Technology Made the Modern World*. Yale UP, 2014.
- Blank, Andrew G. *TCP/IP Jumpstart: Internet Protocol Basics*. 2nd ed., Sybex, 2002.
- Bogost, Ian. "The Secret History of the Robot Car." *The Atlantic*, 14 Oct. 2014, www.theatlantic.com/magazine/archive/2014/11/the-secret-history-of-the-robot-car/380791.
- Bostrom, Nick, and Eliezer Yudkowsky. "The Ethics of Artificial Intelligence." *The Cambridge Handbook of Artificial Intelligence*, edited by Keith Frankish and William M. Ramsay, Cambridge UP, 2014, pp. 316-34.
- Bostrom, Nick. "Ethical Issues in Advanced Artificial Intelligence." *NickBostrom.com*, 2003, nickbostrom.com/ethics/ai.html.
- Boyle, Randall, and Raymond R. Panko. *Corporate Computer Security*. 5th ed., Pearson, 2020.
- Bradbury, David. "When Borders Collide: Legislating Against Cybercrime." *Computer Fraud and Security*, vol. 2, 2012, pp. 11-15.
- Brandom, Russell. "Google Survey Finds More than Five Million Users Infected with Adware." *The Verge*, 6 May 2015, www.theverge.com/2015/5/6/8557843/google-adware-survey-ad-injectors-security-malware.
- Brant, Tom. "SSD vs. HDD: What's the Difference?" *PCMag*, 26 Aug. 2022, www.pc当地新闻/news/ssd-vs-hdd-whats-the-difference.
- Bravo, Cesar, and Desilda Toska. *The Art of Social Engineering: Uncover the Secrets behind the Human Dynamics in Cybersecurity*. Packt, 2023.
- Bray, Chad, and Danny Yadron. "Nasdaq, Others, Targeted by Hackers." *Wall Street Journal*, 26 July 2013, www.wsj.com/articles/SB10001424127887324564704578627640005242794.
- Brazeau, P. "Managing Your Costs by Differentiating Your Risks." *Canadian Underwriter*, vol. 74, 2007, pp. 36-38.
- Brennan, Tom. "Penetration Testing: A Needed Defense against Cyber Threats." *Security*, 28 Apr. 2022, www.securitymagazine.com/articles/97509-penetration-testing-a-needed-defense-against-cyber-threats.
- "A Brief SGML Tutorial." *W3C*, www.w3.org/TR/WD-html40-970708/intro/sgmltut.html.
- Bright, Peter. "Locking the Bad Guys Out with Asymmetric Encryption." *Ars Technica*, 12 Feb. 2013, arstechnica.com/security/2013/02/lock-robster-keeping-the-bad-guys-out-with-asymmetric-encryption.
- Brill, Steven. *After: How America Confronted the September 12 Era*. Simon & Schuster, 2003.
- Brodley, Carla E. "Challenges and Opportunities in Applied Machine Learning." *AI Magazine*, vol. 33, no. 1, 2012, pp. 11-24.
- Brooks, R. R. *Introduction to Computer and Network Security: Navigating Shades of Gray*. CRC, 2014.
- Brown, Michael. "Microsoft Windows Is 30: A Short History of One of the Most Iconic Tech Products Ever." *International Business Times*, 20 Nov. 2015, www.ibtimes.com/microsoft-windows-30-short-history-one-most-iconic-tech-products-ever-2194091.
- Bruer, Wesley. "FBI Sees Chinese Involvement amid Sharp Rise in Economic Espionage Cases." *CNN*, 24 July 2015, www.cnn.com/2015/07/24/politics/fbi-economic-espionage.
- "Bullying Laws across America." *Cyberbullying Research Center*, cyberbullying.org/bullying-laws.
- Burger, Arnold S. *Debugging Embedded and Real-Time Systems*. Newnes, 2020.

- Burgess, Matt. "What Is the Internet of Things? WIRED Explains." *Wired*, 16 Feb. 2018, www.wired.co.uk/article/internet-of-things-what-is-explained-iot.
- Buxton, Stephen. *Database Design: Know it All*. Morgan Kaufmann, 2009.
- Bwalya, Kelvin J., Nathan M. Mnjama, and Peter M. I. I. M. Sebina. *Concepts and Advances in Information Knowledge Management: Studies from Developing and Emerging Economies*. Elsevier, 2014.
- Bygrave, Lee A. *Data Privacy Law, an International Perspective*. Oxford UP, 2014.
- _____. "The Place of Privacy in Data Protection Laws." *University of New South Wales Law Journal*, vol. 24, no. 1, 2001, pp. 277-83.
- Cabaj, Krzysztof, and Wojciech Mazurczyk. "Using Software-Defined Networking for Ransomware Mitigation: The Case of CryptoWall." *IEEE Network*, vol. 30, no. 6, 2016, pp. 14-20.
- Cadwalladr, Carole. "Fresh Cambridge Analytica Leak 'Shows Global Manipulation Is Out of Control.'" *The Guardian*, 4 Jan. 2020, www.theguardian.com/uk-news/2020/jan/04/cambridge-analytica-data-leak-global-election-manipulation.
- Cailliau, Robert, and Helen Ashman. "Hypertext in the Web: A History." *ACM Computing Surveys*, vol. 31, Dec. 1999, pp. 1-6.
- Caldwell, Wilma R., editor. *Computer Security Sourcebook*. Omnipress, 2003.
- Calore, Michael. "A History of Microsoft Windows." *Wired*, 10 Dec. 2008, www.wired.com/2008/12/wiredphotos31.
- Campbell-Kelly, Martin, William F. Aspray, Jeffrey R. Yost, Honghong Tinn, and Gerardo Con Díaz. *Computer: A History of the Information Machine*. 4th ed., Routledge, 2023.
- "CAN-SPAM." FCC, 13 Aug. 2021, www.fcc.gov/general/can-spam.
- Capoot, Ashley, and Jake Piazza. "Uber Begins Offering Rides in Self-Driving Waymo Cars." *CNBC*, 26 Oct. 2023, www.cnbc.com/2023/10/26/uber-begins-offering-rides-in-self-driving-waymo-cars.html.
- Carbone, T., and D. Tippett. "Project Risk Management Using the Project Risk FMEA." *Engineering Management Journal*, vol. 16, no. 4, 2004, pp. 28-35.
- Carlin, John P. *Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat*. Hachette, 2018.
- Carpenter, Adam. "What Programming Languages Are Used in Cybersecurity?" *Codecademy*, 15 June 2021, www.codecademy.com/resources/blog/what-programming-languages-are-used-in-cybersecurity.
- Casey, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. 3rd ed., Academic Press, 2011.
- Caspi, Avner, and Paul Gorsky. "Online Deception: Prevalence, Motivation, and Emotion." *CyberPsychology & Behavior*, vol. 9, no 1, 2006, pp. 54-59.
- Castro, Elizabeth, and Bruce Hyslop. *HTML and CSS*. 8th ed., Peachpit Press, 2014.
- "Catching the Hackers-Introduction to Intrusion Detection Certification Training Class." NICCS, 16 Aug. 2022, niccs.cisa.gov/education-training/catalog/security-university/catching-hackers-introduction-intrusion-detection.
- Cate, Fred. "The Changing Face of Privacy Protections in the European Union and the United States." *Indiana Law Review*, vol. 33, 1999, pp. 173-232.
- Cavusgil, S. Tamer, et al. *International Business: The New Realities*. Frenchs Forest, 2015.
- Cellan-Jones, Rory. "Deepfake Videos 'Double in Nine Months.'" *BBC News*, 7 Oct. 2019, www.bbc.com/news/technology-49961089.
- Centers for Disease Control and Prevention. *Youth Risk Behavior Surveillance-United States, 2017*. CDC, 15 June 2018, www.cdc.gov/healthyyouth/data/yrbs/pdf/2017/ss6708.pdf.
- Chadwick, Paul. "How Many People Had Their Data Harvested by Cambridge Analytica?" *The Guardian*, 16 Apr. 2018, www.theguardian.com/commentisfree/2018/apr/16/how-many-people-data-cambridge-analytica-facebook.
- Chaffey, Dave, Tanya Hemphill, and David Edmundson-Bird. *Digital Business and E-Commerce Management*. 7th ed., Pearson Education, 2019.
- Chao, Loretta. "Tech Partnership Looks beyond the Bar Code with Digital Watermarks." *Wall Street Journal*, 12 Jan. 2016, www.wsj.com/articles/tech-partnership-looks-beyond-the-bar-code-with-digital-watermarks-1452623450.
- Chau, S. C., and M. T. Lu. "Understanding Internet Banking Adoption and Use Behavior: A Hong Kong Perspective." *Journal of Global Information Management*, vol. 12, no. 3, 2009, pp. 21-43.
- Chen, Angela. "Three Threats Posed by Deepfakes That Technology Won't Solve." *MIT Technology Review*, 2 Oct. 2019, www.technologyreview.com/s/614446/deepfake-technology-detection-disinformation-harassment-revenge-porn-law/.
- Chevalier, Stephanie. "Global Retail E-Commerce Sales 2014-2026." *Statista*, 21 Sept. 2022,

- www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales.
- Chevance, Rene. *Server Architectures: Multiprocessors, Clusters, Parallel Systems, Web Servers, and Storage Solutions*. Elsevier, 2005.
- Chokkattu, Julian. "The Top New Features in Apple's iOS 17 and iPadOS 17." *Wired*, 8 June 2023, www.wired.com/story/apple-iphone-ios-17-ipados-17-new-features.
- Choudhury, Saheli Roy, and Arjun Kharpal. "The 'Deep Web' May Be 500 Times Bigger than the Normal Web. Its Uses Go Well beyond Buying Drugs." *CNBC*, 6 Sept. 2018, www.cnbc.com/2018/09/06/beyond-the-valley-understanding-the-mysteries-of-the-dark-web.html.
- "Chronology of Aadhaar Case." *Economic Times*, 26 Sept. 2018, economictimes.indiatimes.com/news/politics-and-nation/chronology-of-aadhaar-case/articleshow/65965443.cms.
- Churcher, Clare. *Beginning Database Design: From Novice to Professional*. 2nd ed., Apress, 2012.
- Cicconi, Falvio, et al. "Forensic Analysis of Commercial Inks by Laser-Induced Breakdown Spectroscopy (LIBS)." *Sensors*, vol. 20, no. 13, 2020, www.mdpi.com/1424-8220/20/13/3744.
- Cilli, Claudio. "Identity Theft: A New Frontier for Hackers and Cybercrime." *Information Systems Control Journal*, vol. 6, 2005, pp. 1-4.
- Cimpanu, Catalin. "A Decade of Hacking." *ZDNet*, 12 Dec. 2019, www.zdnet.com/article/a-decade-of-hacking-the-most-notable-cyber-security-events-of-the-2010s.
- Cintula, Petr, et al. "Fuzzy Logic." *Stanford Encyclopedia of Philosophy*, 11 Nov. 2021, plato.stanford.edu/entries/logic-fuzzy.
- Cirani, Simone, Gianluigi Ferrari, and Luca Veltri. "Enforcing Security Mechanism in the IP-Based Internet of Things: An Algorithmic Overview." *Algorithms*, vol. 6, no. 2, 2013, pp. 197-226.
- Citron, Danielle Keats. *Hate Crimes in Cyberspace*. Harvard UP, 2014.
- Clark, Laura, and William E. Algaier. *Surveillance Detection: The Art of Prevention*. Cradle Press, 2007.
- Clark, Martin P. *Data Networks, IP, and the Internet*. Wiley, 2003.
- Clark, Mitchell. "Here's How the FBI Managed to Get into the San Bernardino Shooter's iPhone." *The Verge*, 14 Apr. 2021, www.theverge.com/2021/4/14/22383957/fbi-san-bernardino-iphone-hack-shooting-investigation.
- Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. HarperCollins, 2010.
- Clifford, Ralph D., editor. *Cybercrime: The Investigation, Prosecution, and Defense of a Computer-Related Crime*. Carolina Academic Press, 2001.
- Cloud, John. "Bullied to Death?" *Time*, 18 Oct. 2010, pp. 60-63.
- Coe, Taylor. "Where Does the Word *Cyber* Come From?" *OUPblog*, 28 Mar. 2015, blog.oup.com/2015/03/cyber-word-origins.
- Coffin, B. "The I Word." *Risk Management*, vol. 54, 2007, pp. 4-5.
- Colarik, Andrew Michael. *Cyber Terrorism: Political and Economic Implications*. IGI Global, 2006.
- Coleman, E Gabriella. *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton UP, 2013.
- Coleman, Liv. "'We Reject: Kings, Presidents, and Voting': Internet Community Autonomy in Managing the Growth of the Internet." *Journal of Information Technology & Politics*, vol. 10, no. 2, 2013, pp. 171-89.
- Collin, Barry. "The Future of Cyberterrorism." *Crime and Justice International*, vol. 13, no. 2, 1997, pp. 15-18.
- "Combinatorial Testing." *NIST Computer Security Resource Center*, 19 Oct. 2023, csrc.nist.gov/Projects/automated-combinatorial-testing-for-software/cybersecurity-testing-1/cybersecurity-testing.
- Comer, Douglas. *Computer Networks and Internets*. Pearson, 2015.
- _____. *The Internet Book: Everything You Need to Know about Computer Networking and How the Internet Works*. 5th ed., Chapman and Hall/CRC, 2018.
- "Computer Fraud." *Computer Hope*, 18 Oct. 2022, www.computerhope.com/jargon/c/computer-fraud.htm.
- "A Computer in Your Pocket: The Rise of Smartphones." *Science Museum*, 13 Nov. 2018, www.sciencemuseum.org.uk/objects-and-stories/computer-your-pocket-rise-smartphones.
- "Computer Internet Fraud." *Cornell Law School*, www.law.cornell.edu/wex/computer_and_internet_fraud.
- Computer-Networking." *Tutorials Point*, www.tutorialspoint.com/computer_fundamentals/computer_networking.htm.
- "Computer System Engineering." *MIT Open Courseware*, 2018, ocw.mit.edu/courses/6-033-computer-system-engineering-spring-2018/pages/week-13.
- Confessore, Nicholas. "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far." *New York Times*, 4 Apr. 2018, www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.
- Conheady, Sharon. *Social Engineering in IT Security: Tools, Tactics, and Techniques*. McGraw, 2014.

- Connolly, Kate. "Germany Accuses China of Industrial Espionage." *The Guardian*, 22 July 2009, www.theguardian.com/world/2009/jul/22/germany-china-industrial-espionage.
- Conti, Robyn, and Benjamin Curry. "What Is an NFT? Non-Fungible Tokens Explained." *Forbes Advisor*, 17 Mar. 2023, www.forbes.com/advisor/investing/cryptocurrency/nft-non-fungible-token.
- Contos, Brian T. *Enemy at the Water Cooler: True Stories of Insider Threats and Enterprise Security Management Countermeasures*. Syngress, 2007.
- Conway, Maura. "Against Cyberterrorism." *Communications of the ACM*, vol. 54, no. 2, 2011, pp. 26-28.
- Copes, Heith, and Lynne M. Vieraitis. *Identity Thieves: Motives and Methods*. Northeastern UP, 2012.
- Corbet, Jonathan, Alessandro Rubini, and Greg Kroah-Hartman. *Linux Device Drivers*. 3rd ed., O'Reilly, 2005.
- Cormen, Thomas H. *Algorithms Unlocked*. MIT Press, 2013.
- "Coronavirus Scams-Consumer Resources." *Federal Communications Commission*, 7 Mar. 2022, www.fcc.gov/covid-scams.
- Cortada, James W. *The Digital Hand: How Computers Changed the Work of American Manufacturing, Transportation, and Retail Industries*. Oxford UP, 2004.
- Costello, Sam. "The History of iOS, from Version 1.0 to 17.0." *Lifewire*, 5 June 2023, www.lifewire.com/ios-versions-4147730.
- Costello, Vic. *Multimedia Foundations: Core Concepts for Digital Design*. 3rd ed., Focal Press, 2023.
- Cox, Mike, Ellen Mulder, and Linda Tadic. *Descriptive Metadata for Television*. Focal, 2006.
- Crail, Chauncey. "VPN Statistics and Trends in 2023." Reviewed by Kelly Main. *Forbes Advisor*, 9 Feb. 2023, www.forbes.com/advisor/business/vpn-statistics.
- Cramer-Flood, Ethan. "Global Ecommerce Update 2021: Worldwide Ecommerce Will Approach \$5 Trillion This Year." *eMarketer, Business Insider Intelligence*, Jan. 2021, www.emarketer.com/content/global-ecommerce-update-2021.
- Crandall, Carolyn. "What Can We Learn by Analyzing 197 Years of Cumulative Cybersecurity Testing?" *Cyber Defense Magazine*, 26 July 2023, www.cyberdefensemagazine.com/what-can-we-learn-by-analyzing-197-years-of-cumulative-cybersecurity-testing.
- Creswell, John W. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Sage, 2013.
- The Criminal Spam Act of 2003: Report (to Accompany S. 1293)*. US Government Printing Office, 2003.
- "Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities." *US Government Accountability Office*, 2005, www.gao.gov/new.items/d05434.pdf.
- Cronin, Audrey Kurth. *Power to the People: How Open Technological Innovation Is Arming Tomorrow's Terrorists*. Oxford UP, 2019.
- Crosston, Matthew. "Virtual Patriots and a New American Cyber Strategy: Changing the Zero-Sum Game." *Strategic Studies Quarterly*, vol. 6, no. 4, 2012, pp. 100-118.
- "Cryptographic Standards and Guidelines." *NIST*, 8 May 2023, csrc.nist.gov/projects/cryptographic-standards-and-guidelines/archived-crypto-projects/aes-development.
- Cukier, Kenneth. *Big Data: A Revolution that Will Transform How We Live, Work, and Think*. Dolan, 2013.
- Currim, Sabah, et al. "Using a Knowledge Learning Framework to Predict Errors in Database Design." *Information Systems*, vol. 40, 2014, pp. 11-31.
- Curry, David. "Android Statistics (2023)." *Business of Apps*, 27 Feb. 2023, www.businessofapps.com/data/android-statistics.
- "Cyber." *Merriam-Webster*, 2023, www.merriam-webster.com/dictionary/cyber.
- "Cyberbullying: Definition." *Pacer's National Bullying Prevention Center*, 2020, www.pacer.org/bullying/resources/cyberbullying.
- "Cyber Crime." *Federal Bureau of Investigation*, www.fbi.gov/investigate/cyber.
- "Cybercrime: Reporting Mechanisms Vary, and Agencies Face Challenges in Developing Metrics." *GAO*, 20 June 2023, www.gao.gov/products/gao-23-106080.
- "Cybersecurity Best Practices for Smart Cities." *CISA*, 19 Apr. 2023, www.cisa.gov/sites/default/files/2023-04/cybersecurity-best-practices-for-smart-cities_508.pdf.
- "Cybersecurity Framework." *NIST*, 2023, www.nist.gov/cyberframework.
- Cybersecurity & Infrastructure Security Agency*, 2023, www.cisa.gov.
- "Cyber Weapon." *Australian Cyber Security Institute*, www.cyber.gov.au/acsc/view-all-content/glossary/cyber-weapon.
- D'Aliessi, Michele. "How Does the Blockchain Work?" *Medium*, 1 June 2016, medium.com/@micheledaliessi/how-does-the-blockchain-work-98c8cd01d2ae.
- D'Costa, Krystal. "Catfishing: The Truth about Deception Online." *Scientific American*, 25 Apr. 2014,

- <blogs.scientificamerican.com/anthropology-in-practice/catfishing-the-truth-about-deception-online>.
- D'Mello, Gwyn. "French Cyber Expert Cracks Official Aadhaar App in 1 Minute, Realizes UIDAI's Worst Nightmare." *India Times*, 13 Mar. 2018, <www.indiatimes.com/technology/news/french-cyber-expert-cracks-official-aadhaar-app-in-1-minute-realizes-uidai-s-worst-nightmare-341416.html>.
- Daemen, Joan, and Vincent Rijmen. *The Design of Rijndael: The Advanced Encryption Standard (AES)*. 2nd ed., Springer, 2020.
- Dahlberg, T., et al. "Past, Present, and Future of Mobile Payments Research: A Literature Review." *Electronic Commerce Research and Applications*, vol. 7, no. 2, 2008, pp. 165-81.
- Dang, Sheila, Katie Paul, and Dawn Chmielewski. "Focus: Do Spam Bots Really Comprise Under 5% of Twitter Users? Elon Musk Wants to Know." *Reuters*, 13 May 2022, <www.reuters.com/technology/do-spam-bots-really-comprise-under-5-twitter-users-elon-musk-wants-know-2022-05-13>.
- Danks, David, and Joseph H. Danks. "The Moral Permissibility of Automated Responses during Cyberwarfare." *Journal of Military Ethics*, vol. 12, no. 1, 2013, pp. 18-33.
- Das, Sumitabha. *Your UNIX/Linux: The Ultimate Guide*. 3rd ed., McGraw-Hill, 2012.
- "Data Breach." *Trend Micro*, <www.trendmicro.com/vinfo/us/security/definition/data-breach>.
- "Data Breach Chronology." *Privacy Rights Clearinghouse*, <www.privacyrights.org/data-breaches>.
- "Data Breaches 101: How They Happen, What Gets Stolen, and Where It All Goes." *Trend Micro*, 10 Aug. 2018, <www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101>.
- Data Communication & Computer Network." *Tutorials Point*, www.tutorialspoint.com/data_communication_computer_network/index.htm.
- "Database." *Encyclopaedia Britannica*, 30 June 2023, <www.britannica.com/technology/database>.
- "Data Measurement Chart." *University of Florida*, www.wu.ece.ufl.edu/links/dataRate/DataMeasurementChart.html.
- Datta, Anwitaman, et al. *Social Informatics: Third International Conference, SocInfo, 2011, Singapore, October 2011*. Springer-Verlag, 2011.
- Davies, Alex. "In 20 Years, Most New Cars Won't Have Steering Wheels or Pedals." *Wired*, 21 July 2014, <www.wired.com/2014/07/in-20-years-most-new-cars-wont-have-steering-wheels-or-pedals>.
- De Filippi, Primavera. "It's Time to Take Mesh Networks Seriously (and Not Just for the Reasons You Think)." *Wired*, 2 Jan. 2014, <www.wired.com/2014/01/its-time-to-take-mesh-networks-seriously-and-not-just-for-the-reasons-you-think>.
- De Jager, Peter. "Y2K: So Many Bugs...So Little Time." *Scientific American*, Jan. 1999, pp. 88-93.
- DeGroot, Morris H., and Mark J. Schervish. *Probability and Statistics*. 4th ed., Pearson, 2011.
- Delfs, Hans, and Helmut Knebl. *Introduction to Cryptography: Principles and Applications*. 3rd ed., Springer, 2015.
- "Deloitte's 2021 Global Blockchain Survey." *Deloitte Insights*, 2021, <www2.deloitte.com/us/en/insights/topics/understanding-blockchain-potential/global-blockchain-survey.html>.
- Demirkan, H., and R. J. Kauffman. "Service-Oriented Technology and Management: Perspectives on Research and Practice for the Coming Decade." *Electronic Commerce Research and Applications*, vol. 7, no. 4, 2008, 356-76.
- Denning, Dorothy. "An Intrusion-Detection Model." *IEEE Transactions on Software Engineering*, vol. SE-13, no. 2, 1987, pp. 222-32, <ieeexplore.ieee.org/document/1702202>.
- _____. "A View of Cyberterrorism Five Years Later." *Internet Security: Hacking, Counterhacking, and Society*, edited by Kenneth Elinor Himma, Jones, 2007.
- "Deprecated HTML5 Tags and Attributes." *DESE*, 14 Mar. 2018, <www.doe.mass.edu/nmg/html5-deprecated.html>.
- "Development History." *W3C*, 6 Jan. 2003, <www.w3.org/XML/hist2002>.
- "Device Security Guidance." *National Cyber Security Centre*, 5 Oct. 2021, <www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/managing-device-firmware>.
- Dhillon, Gupreet. "Dimensions of Power and IS Implementation." *Information and Management*, vol. 41, no. 5, 2004, pp. 635-44.
- Dice, Pete. *Quick Boot: A Guide for Embedded Firmware Developers*. Intel, 2012.
- Dieny, Bernard, Ronald B. Goldfarb, and Kyung-Jin Lee. *Introduction to Magnetic Random-Access Memory*. IEEE Press/John Wiley & Sons, 2017.
- "Different Types of Software." *Introduction to IT English*, web2.uvcs.uvic.ca/elc/sample/ite/u01/u1_1_03.html.
- "Digital Evidence and Forensics." *National Institute of Justice*, <nij.ojp.gov/digital-evidence-and-forensics>.

- Dinan, Stephen. "FBI Reopens Clinton Email Investigation." *Washington Times*, 28 October 2016, www.washingtontimes.com/news/2016/oct/28/james-comey-fbi-director-reopens-clinton-email-inv.
- Dingle, Norm. "Artificial Intelligence: Fuzzy Logic Explained." *Control Engineering*, 4 Nov. 2011, www.controleng.com/single-article/artificial-intelligence-fuzzy-logic-explained/8f3478c13384a2771ddb7e93a2b6243d.html.
- "Distributed Denial of Service Attacks." *Imperva*, www.imperva.com/learn/ddos/denial-of-service.
- Domingos, Pedro. "A Few Useful Things to Know about Machine Learning." *Communications of the ACM*, vol. 55, no. 10, 2012, pp. 78-87.
- Donegan, Richard. "Bullying and Cyberbullying: History, Statistics, Law, Prevention and Analysis." *Elon Journal of Undergraduate Research in Communications*, vol. 3, no. 1, 2012, pp. 34-36.
- Donnelly, John M. "Pentagon Races to Shore Up Supply Chain Security." *Government Technology*, 9 Apr. 2021, www.govtech.com/security/pentagon-races-to-shore-up-supply-chain-security.html.
- Doohan, Bradley, et al. The Black Book: A Starter Guide to Systems Security Engineering for Acquisition. *Defence Research and Development Canada*, 2016, cradpdf.drdc-rddc.gc.ca/PDFS/unc265/p805130_A1b.pdf.
- Dordal, Peter L. "An Introduction to Computer Networks." *Loyola University Chicago*, 2015, intronetworks.cs.luc.edu/current/html.
- Dossett, Julian. "A Timeline of the Biggest Ransomware Attacks." *CNET*, 15 Nov. 2021, www.cnet.com/personal-finance/crypto/a-timeline-of-the-biggest-ransomware-attacks.
- Dotson, Chris. *Practical Cloud Security: A Guide for Secure Design and Deployment*. O'Reilly, 2019.
- Douglas, David M. "Doxing: A Conceptual Analysis." *Ethics and Information Technology*, vol. 18, no. 3, 2016, pp. 199-210.
- Doyle, Charles. *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*. Congressional Research Service, 2010.
- "Driver Security Checklist." *Microsoft*, 4 May 2023, learn.microsoft.com/en-us/windows-hardware/drivers/driver-security/driver-security-checklist.
- Dshalalow, Jewgeni H. *Frontiers in Queueing Models and Applications in Science and Engineering*. CRC Press, 1997.
- Dugan, W. "Global Dangers." *Risk Management*, vol. 46, 1999, pp. 13-16.
- Duggan, M. "Online Harassment 2017." *Pew Research Center*, 11 July 2017, www.pewinternet.org/2017/07/11/online-harassment-2017.
- Dunn-Cavelty, Myriam. *Cyber-Security and Threat Politics: U.S. Efforts to Secure the Information Age*. Routledge, 2008.
- Dupont, B. "Bots, Cops, and Corporations: On the Limits of Enforcement and the Promise of Polycentric Regulation as a Way to Control Large-Scale Cybercrime." *Crime, Law and Social Change*, vol. 67, no. 1, 2017, pp. 97-116.
- Dwight, Ken. *Bug-Free Computing: Stop Viruses, Squash Worms, and Smash Trojan Horses*. TeleProcessors, 2006.
- Dysart, Joe. "The Hacktivists." *ABA Journal*, vol. 97, no. 12, 2011, pp. 40-46.
- Easttom, Chuck. *Computer Security Fundamentals*. 5th ed., Pearson, 2023.
- _____. *Network Defense and Countermeasures: Principles and Practices*. 4th ed., Pearson, 2023.
- Eckert, William G. *Introduction to Forensic Sciences*. CRC Press, 1997.
- "E-Commerce Cyber Security: An Introduction for Online Merchants." *Get Cyber Safe*, 15 June 2020, www.getcybersafe.gc.ca/en/blogs/e-commerce-cyber-security-introduction-online-merchants.
- Edwards, Benj. "The Little-Known Apple Lisa: Five Quirks and Oddities." *Macworld*, 30 Jan. 2013, www.macworld.com/article/2026544/the-little-known-apple-lisa-five-quirks-and-oddities.html.
- Edwards, Jim. "Proof That Android Really Is for the Poor." *Business Insider*, 27 June 2014, www.businessinsider.in/Proof-That-Android-Really-Is-For-The-Poor/articleshow/37328668.cms.
- "Election Security Spotlight-Bots." *Center for Internet Security*, www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-bots.
- Elias, Marilyn. "Operation Blitzkrieg." *Intelligence Report*, vol. 146, 2012, pp. 44-47.
- Elizondo, David A., Agusti Solanas, and Antoni Martinez-Balleste. *Computational Intelligence for Privacy and Security*. Springer, 2012.
- Ellul, A., and V. Yerramilli. "Stronger Risk Controls, Lower Risk: Evidence from U.S. Bank Holding Companies." *Journal of Finance*, vol. 68, no. 5, 2013, pp. 1757-803.
- "End User." *Merriam-Webster*, 2023, www.merriam-webster.com/dictionary/end%20user.
- Englehart, J. "A Historical Look at Risk Management." *Risk Management*, vol. 41, no. 3, 1994, pp. 65-72.
- "Ensuring BotNets Are Not 'Too Big to Investigate.'" *US Department of Justice*, 22 Nov. 2016,

- www.justice.gov/archives/opa/blog/ensuring-botnets-are-not-too-big-investigate.
- Entous, Adam, Ellen Nakashima, and Greg Miller. "Secret CIA Assessment Says Russia Was Trying to Help Trump Win White House." *Washington Post*, 9 Dec. 2016, www.washingtonpost.com/world/national-security/obama-orders-review-of-russian-hacking-during-presidential-campaign/2016/12/09/31d6b300-be2a-11e6-94ac-3d324840106c_story.html.
- Epstein, Lee, Kevin T. McGuire, and Thomas G. Walker. *Constitutional Law for a Changing America: A Short Course*. 8th ed., Sage, 2015.
- Erbschloe, Michael. *Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code*. Butterworth-Heinemann, 2005.
- Erl, Thomas, editor. *Big Data Fundamentals: Concepts, Drivers & Techniques*. Pearson, 2016.
- Eskadari, M., and T. Onsen. "A New Approach for Face-Iris Multimodal Biometric Recognition Using Score Fusion." *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 27, no. 3, 2013, pp. 1-15.
- "Estonian Denial of Service Incident." *Council on Foreign Relations*, May 2007, www.cfr.org/cyber-operations/estonian-denial-service-incident.
- "European Smart Cities." *Vienna University of Technology*, www.smart-cities.eu/?cid=-1&ver=4.
- "Extensible Markup Language (XML)." *W3C*, 11 Oct. 2016, www.w3.org/XML.
- "Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises." *Federal Trade Commission*, 29 Nov. 2011, www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.
- Faife, Corin. "The Marriott Hotel Chain Has Been Hit by Another Data Breach." *The Verge*, 6 July 2022, www.theverge.com/2022/7/6/23196805/marriott-hotels-maryland-data-breach-credit-cards.
- Fauvel, Warren. "Blockchain Advantages and Disadvantages." *Medium*, 11 Aug. 2017, medium.com/nudged/blockchain-advantage-and-disadvantages-e76dfde3bbc0.
- Federal Election Commission. "Official 2016 Presidential General Election Results." *FEC*, 30 Jan. 2017, transition.fec.gov/pubrec/fe2016/2016presgeresults.pdf.
- "Federal Identity Theft Laws." *Office for Victims of Crime*, Oct. 2010, ovc.ojp.gov/sites/g/files/xyckuh226/files/pubs/ID_theft/idtheftlaws.html.
- Feinstein, Ken. *Fight Spam, Viruses, Pop-Ups and Spyware (How to Do Everything)*. McGraw-Hill, 2004.
- Feldman, Brian. "Even If Facebook Stops Aggressively Collecting Data, Developers Will Still Supply It." *New York*, 22 Feb. 2019, nymag.com/intelligencer/2019/02/why-facebooks-data-collection-practice-is-so-messy.html.
- Felke-Morris, Terry. *Web Development and Design Foundations with HTML5*. 10th ed., Pearson, 2020.
- Ferguson, R. Stuart. *Practical Algorithms for 3D Computer Graphics*. 2nd ed., AK Peters/CRC Press, 2013.
- Fernando, Jason. "Catfishing: What It Is, Examples of Financial Fraud." *Investopedia*, 23 Apr. 2023, www.investopedia.com/terms/c/cat-fishing.asp.
- Fibbe, George H. "Screen-Scraping and Harmful Cyber-trespass after Intel." *Mercer Law Review*, vol. 55, no. 1011, 2004, pp. 1011-27.
- Finkle, Jim, Soham Chatterjee, and Lehar Maan. "eBay Asks 145 Million Users to Change Passwords after Cyber Attack." *Reuters*, 21 May 2014, www.reuters.com/article/us-ebay-password/ebay-asks-145-million-users-to-change-passwords-after-cyber-attack-idUSBREA4K0B420140521.
- Fiscutean, Andraida. "A History of Ransomware: The Motives and Methods behind Those Evolving Attacks." *CSO*, 27 July 2020, www.csoonline.com/article/569617/a-history-of-ransomware-the-motives-and-methods-behind-these-evolving-attacks.html.
- Fisk, Nathan W. *Understanding Online Piracy: The Truth about Illegal File Sharing*. ABC-CLIO, 2009.
- Fitter, Hetal N., Akash B. Pandey, Divyang D. Patel, and Jitendra M. Mistry. "A Review on Approaches for Handling Bezier Curves in CAD for Manufacturing." *Procedia Engineering*, vol. 97, 2014, pp. 1155-66.
- FitzGerald, Jerry, Alan Dennis, and Alexandra Durcikova. *Business Data Communications and Networking*. 14th ed., Wiley, 2020.
- Foer, Franklin. "Putin Is Well on His Way to Stealing the Next Election." *The Atlantic*, June 2020, www.theatlantic.com/magazine/archive/2020/06/putin-american-democracy/610570.
- Foote, Steven. *Learning to Program*. Pearson, 2015.
- Forouzan, Behrouz. *Data Communications and Networking*. 5th ed., McGraw-Hill, 2013.
- "Foundations of Fuzzy Logic." *MathWorks*, www.mathworks.com/help/fuzzy-foundations-of-fuzzy-logic.html.
- Fowler, Kevvie. *Data Breach Preparation and Response: Breaches Are Certain, Impact Is Not*. Syngress, 2016.
- Fox, Richard. *Information Technology: An Introduction for Today's Digital World*. CRC, 2013.

- Fox, Susannah. "51% of U.S. Adults Bank Online." *Pew Research Center*, 7 Aug. 2013, www.pewresearch.org/internet/2013/08/07/51-of-u-s-adults-bank-online.
- Frain, Ben. *Design with HTML5 and CSS*. 4th ed., Packt, 2022.
- _____. *Responsive Web Design with HTML5 and CSS*. 4th ed., Packt, 2022.
- Franceschi-Bicchieri, Lorenzo. "The History of Stuxnet: The World's First True Cyberweapon." *Vice*, 9 Aug. 2016, www.vice.com/en/article/ezp58m/the-history-of-stuxnet-the-worlds-first-true-cyberweapon-5886b74d80d84e45e7bd22ee.
- _____. "Love Bug: The Virus That Hit 50 Million People Turns 15." *Motherboard*, 4 May 2015, www.vice.com/en/article/d73jnk/love-bug-the-virus-that-hit-50-million-people-turns-15.
- Frankenfield, Jake. "What Does Proof-of-Stake (PoS) Mean in Crypto?" *Investopedia*, 31 May 2023, www.investopedia.com/terms/p/proof-stake-pos.asp.
- "Free Cyber Security Training." SANS, 1 June 2023, www.sans.org/cyberaces.
- Fruhlinger, Josh. "Stuxnet Explained: The First Known Cyberweapon." *CIO*, 31 Aug. 2022, www.csionline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html.
- "FTC Fines Facebook \$5B for Privacy Violations." *CBC*, 24 July 2019, www.cbc.ca/news/business/facebook-privacy-ftc-fine-1.5222943.
- "FTC Warns About Misuses of Biometric Information and Harm to Consumers." *Federal Trade Commission*, 18 May 2023, www.ftc.gov/news-events/news/press-releases/2023/05/ftc-warns-about-misuses-biometric-information-harm-consumers.
- Fung, Brian. "Biden Administration Says Investigation into SolarWinds Hack Is Likely to Take 'Several Months.'" *CNN Politics*, 17 Feb. 2021, www.cnn.com/2021/02/17/politics/solarwinds-hack-investigation/index.html.
- Furnell, Steven. *Cybercrime: Vandalizing the Information Society*. Addison-Wesley, 2002.
- Gaffin, Julie C. *Internet Protocol 6*. Novinka, 2007.
- Gallagher, Sean. "'Locky' Crypto-Ransomware Rides in on Malicious Word Document Macro." *Ars Technica*, 17 Feb. 2016, arstechnica.com/information-technology/2016/02/locky-crypto-ransomware-rides-in-on-malicious-word-document-macro.
- Galvao, D. "Handling Global Political Risk." *Canadian Underwriter*, vol. 74, no. 3, 2007, pp. 46-47.
- Garbis, Jason, and Jerry W. Chapman. *Zero Trust Security: An Enterprise Guide*. Apress, 2021.
- Garcia-Barriocanal, Elena, et al., editors. *Metadata and Semantic Research*. Springer, 2011.
- Garfinkel, Simson, and Gene Spafford. *Web Security, Privacy & Commerce*. 2nd ed., O'Reilly Media, 2011.
- Garrido, Josei M. *Principles of Modern Operating Systems*. Jones, 2013.
- Gearan, Anne, Philip Rucker, and Abby Phillip. "DNC Chairwoman Will Resign in Aftermath of Committee Email Controversy." *Washington Post*, 24 July 2016, www.washingtonpost.com/politics/hacked-emails-cast-doubt-on-hopes-for-party-unity-at-democratic-convention/2016/07/24/a446c260-51a9-11e6-b7de-dfe509430c39_story.html?utm_term=.ce78e21f0d9f.
- Gehl, Robert W. *Weaving the Dark Web: Legitimacy on Freenet, Tor, and I2P*. MIT Press, 2018.
- Geier, Eric. "How (and Why) to Set Up a VPN Today." *PCWorld*, 19 Mar. 2013, www.pcworld.com/article/457163/how-and-why-to-set-up-a-vpn-today.html.
- Gelb, A., and J. Clark. "Identification for Development: The Biometrics Revolution." *Center for Global Development Working Paper 315*, 2013, papers.ssrn.com/sol3/papers.cfm?abstract_id=2226594.
- Gelman, Robert B., and Stanton McCandlish. *Protecting Yourself Online: The Definitive Resource on Safety, Freedom, and Privacy in Cyberspace*. HarperEdge, 1998.
- Gerencer, Tom. "The Top 10 Worst Computer Viruses in History." *Hewlett-Packard*, 4 Nov. 2020, www.hp.com/us-en/shop/tech-takes/top-ten-worst-computer-viruses-in-history.
- Gershgorn, Dave. "A California Law Now Means Chatbots Have to Disclose They're Not Human." *BotLaw*. Quartz, 3 Oct. 2018, qz.com/1409350/a-new-law-means-californias-bots-have-to-disclose-theyre-not-human.
- Gianelli, Paul C., Edward J. Imwinkelried, Andrea Roth, and Jane Moriarty. *Scientific Evidence*. Lexis Nexis, 2012.
- Gibbons, Robert, and John Roberts. *The Handbook of Organizational Economics*. Princeton UP, 2012.
- Gibbs, Samuel. "From Windows 1 to Windows 10: 29 Years of Windows Evolution." *The Guardian*, 2 Oct. 2014, www.theguardian.com/technology/2014/oct/02/from-windows-1-to-windows-10-29-years-of-windows-evolution.
- _____. "How Did Email Grow from Messages between Academics to a Global Epidemic?" *The Guardian*, 7 Mar. 2016, www.theguardian.com/technology/2016/mar/07/email-ray-tomlinson-history.
- Gilman, Evan, and Doug Barth. *Zero Trust Networks: Building Secure Systems in Untrusted Networks*. O'Reilly Media, 2017.

- Giri, Kaiser J., Shabir Ahmad Parah, Rumaan Bashir, and Khan Muhammad, editors. *Multimedia Security: Algorithm Development, Analysis and Applications*. Springer Nature Singapore, 2021.
- Gkoutzinis, Apostolos. *Internet Banking and the Law in Europe: Regulation, Financial Integration and Electronic Commerce*. Cambridge UP, 2010.
- Gladstone, Julia Alpert. "Data Mines and Battlefields: Looking at Financial Aggregators to Understand the Legal Boundaries and Ownership Rights in the Use of Personal Data." *John Marshall Journal of Computer and Information Law*, vol. 19, no. 1, 2001, pp. 313-29.
- Glaser, J. D. *Secure Development for Mobile Apps: How to Design and Code Secure Mobile Applications with PHP and JavaScript*. CRC Press, 2015.
- "Global Market Share Held by Leading Internet Browsers from January 2012 to May 2023." *Statista*, May 2023, www.statista.com/statistics/268254/market-share-of-internet-browsers-worldwide-since-2009.
- "Global Ransomware Attacks at an All-Time High, Shows Latest 2023 State of Ransomware Report." *Malwarebytes Labs*, 3 Aug. 2023, www.malwarebytes.com/blog/threat-intelligence/2023/08/global-ransomware-attacks-at-an-all-time-high-shows-latest-2023-state-of-ransomware-report.
- "Global Social Media Statistics." *Datareportal*, Apr. 2023, datareportal.com/social-media-users.
- Goggin, Gerard. *Apps: From Mobile Phones to Digital Lives*. Wiley, 2021.
- Gogolin, Greg. *Digital Forensics Explained*. CRC, 2013.
- Goldstein, Emmanuel. *Best of 2600: A Hacker Odyssey*. Wiley, 2008.
- Goodin, Dan. "How 'Omnipotent' Hackers Tied to NSA Hid for 14 Years-and Were Found at Last." *Ars Technica*, 16 Feb. 2015, arstechnica.com/information-technology/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last.
- Gordon, Sherri Mabry. *Downloading Copyrighted Stuff from the Internet: Stealing or Fair Use?* Enslow, 2005.
- Gordon, Whitson. "How to Build a Computer, Lesson 1: Hardware Basics." *Lifehacker*, 1 Aug. 2011, lifehacker.com/5826509/how-to-build-a-computer-from-scratch-lesson-1-hardware-basics.
- Gorman, Siobhan, August Cole, and Yochi Dreazen. "Computer Spies Breach Fighter-Jet Project." *Wall Street Journal*, 21 Apr. 2009, online.wsj.com/article/SB124027491029837401.html.
- Gourley, David, et al. "Client Identification and Cookies." *HTTP: The Definitive Guide*. O'Reilly Media, 2002, pp. 257-76.
- Grad, Burton, and Thomas J. Bergin. "History of Database Management Systems." *IEEE Annals of the History of Computing*, vol. 31, no. 4, 2009, pp. 3-5.
- Gralla, Preston. *How the Internet Works*. 4th ed., Que Publishing, 1998.
- Granville, Johanna. "Tracking Computer Hacking: The Dangers of Cyber Terrorism." *Global Society: Journal of Interdisciplinary International Relations*, vol. 17, no. 1, 2003, pp. 89-97.
- "Graphical User Interface." *Techopedia*, 28 May 2021, www.techopedia.com/definition/5435/graphical-user-interface-gui.
- Gray, Neil A. B. *Web Server Programming*. Wiley, 2003.
- Greenberg, Andy. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday, 2019.
- Greengard, Samuel. *The Internet of Things*. Rev. ed., MIT Press, 2021.
- Gregory, Sam, and Eric French. "How Do We Work Together to Detect AI-Manipulated Media?" *Witness Media Lab*, 2019, lab.witness.org/projects/osint-digital-forensics.
- Griffith, Eric. "How to Completely Disappear from the Internet." *PCMag*, 24 Oct. 2022, www.pc当地.com/how-to/how-to-stay-anonymous-online.
- _____. "What Is Cloud Computing?" *PCMag*, 15 Feb. 2022, www.pc当地.com/news/what-is-cloud-computing.
- Grobler, Marthie, Raj Gaire, and Surya Nepal. "User, Usage and Usability: Redefining Human Centric Cyber Security." *Frontiers in Big Data*, vol. 4, 2021, doi.org/10.3389/fdata.2021.583723.
- Grossman, Andrew. "U.S. Charges Six Chinese Citizens with Economic Espionage." *Wall Street Journal*, 19 May 2015, www.wsj.com/articles/u-s-charges-six-chinese-citizens-with-economic-espionage-1432046527.
- Guarascio, Francesco. "EU Prepares to Launch First Cybercrime Centre." *Euractiv*, 29 Mar. 2012, www.euractiv.com/infosociety/eu-prepares-launch-cybercrime-ce-news-511823.
- Guccione, Darren. "What Is the Dark Web? How to Access It and What You'll Find." *CSO*, 1 July 2021, www.csoonline.com/article/564313/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html.
- Gumbel, Andrew, "Why US Elections Remain 'Dangerously Vulnerable' to Cyber-Attacks." *The Guardian*, 13 Aug. 2018, www.theguardian.com/us-news/2018/aug/13/us-election-cybersecurity-hacking-voting.
- Gupta, Siddarth, and Vagesh Porwal. "Recent Digital Watermarking Approaches, Protecting Multimedia Data

- Ownership.” *Advances in Computer Science* vol. 4, no. 2, 2015, pp. 21-30.
- Gupta, Vinay. “A Brief History of Blockchain.” *Harvard Business Review*, 28 Feb. 2017, hbr.org/2017/02/a-brief-history-of-blockchain.
- Hadnagy, Christopher. *Social Engineering: The Science of Human Hacking*. 2nd ed., Wiley, 2018.
- Haerens, Margaret, and Lynn M. Zott, editors. *Hacking and Hackers*. Greenhaven, 2014.
- Hafner, Katie. *Where Wizards Stay Up Late: The Origins of The Internet*. Simon & Schuster, 1998.
- Halpern, Sue. “How Cyber Weapons Are Changing the Landscape of Modern Warfare.” *New Yorker*, 18 July 2019, www.newyorker.com/tech/annals-of-technology/how-cyber-weapons-are-changing-the-landscape-of-modern-warfare.
- Halton, Clay. “The Truth about Y2K: What Did and Didn’t Happen in the Year 2000.” *Investopedia*, 30 May 2023, www.investopedia.com/terms/y/y2k.asp.
- Hamedy, Saba. “Report: Online Piracy Remains Multi-Hundred-Million-Dollar Business.” *Los Angeles Times*, 19 May 2015, www.latimes.com/entertainment/envelope/cotown/la-et-ct-report-online-piracy-digital-citizens-alliance-medialink-20150518-story.html.
- Hansen, Per Brinch. *Classic Operating Systems: From Batch Processing to Distributed Systems*. Springer, 2001.
- Harcourt, Bernard E. *Exposed: Desire and Disobedience in the Digital Age*. Harvard UP, 2015.
- “Hard Drive.” *Computer Hope*, 18 Oct. 2022, www.computerhope.com/jargon/h/harddriv.htm.
- Harding, Luke. “What Are the Panama Papers? A Guide to History’s Biggest Data Leak.” *The Guardian*, 5 Apr. 2016, www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers.
- Hardy, David Leicester. *Introduction to Digital Media Design: Transferable Hacks, Skills, and Tricks*. Bloomsbury Visual Arts, 2022.
- Harrell, Erika. “Victims of Identity Theft, 2016.” *Bureau of Justice Statistics*, Jan. 2019, www.bjs.gov/index.cfm?ty=pb&detail&iid=6467.
- Harrison, Virginia, and Jose Pagliery. “Nearly 1 Million New Malware Threats Released Every Day.” *CNN Business*, 14 Apr. 2015, money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security.
- Haslam, Karen. “macOS Versions: Every Version Including the Latest.” *Macworld*, 13 June 2023, www.macworld.com/article/672681/list-of-all-macos-versions-including-the-latest-macos.html.
- Hastings, Glen, and Richard Marcus. *Identity Theft, Inc.: A Wild Ride with the World’s #1 Identity Thief*. The Disinformation Company, 2006.
- Hauser, Greg. *Techniques in Countersurveillance: The Fine Art of Bug Extermination in the Real World of Intelligence Gathering*. Paladin Press, 1999.
- Hayes, Adam. “The Unintended Consequences of Self-Driving Cars.” *Investopedia*, 31 Aug. 2021, www.investopedia.com/articles/investing/090215/unintended-consequences-selfdriving-cars.asp.
- Heath, Ryan. “Artificial Intelligence Cold War on the Horizon.” *Politico*, 16 Oct. 2020, www.politico.com/news/2020/10/16/artificial-intelligence-cold-war-on-the-horizon-429714.
- Heaven, Douglas. “Not Like Us: Artificial Minds We Can’t Understand.” *New Scientist*, 7 Aug. 2013, www.newscientist.com/article/mg21929290-700-not-like-us-artificial-minds-we-can’t-understand.
- Heckman, Rocky. *Designing Platform Independent Mobile Apps and Services*. Wiley-IEEE Computer Society Press, 2016.
- Heikkilä, Melissa. “The Algorithm: AI-Generated Art Raises Tricky Questions about Ethics, Copyright, and Security.” *MIT Technology Review*, 20 Sept. 2022, www.technologyreview.com/2022/09/20/1059792/the-algorithm-ai-generated-art-raises-tricky-questions-about-ethics-copyright-and-security.
- Heisler, Yoni. “The History and Evolution of iOS, from the Original iPhone to iOS 9.” *BGR*, 19 Dec. 2018, bgr.com/2016/02/12/ios-history-iphone-features-evolution.
- Helfrich, James N. *Security for Software Engineers*. CRC Press, 2019.
- Herbert, Lin. “A Virtual Necessity: Some Modest Steps toward Greater Cybersecurity.” *Bulletin of the Atomic Scientists*, vol. 68, no. 5, 2012, pp. 75-87.
- Hern, Alex. “Ask.fm’s New Owners Vow to Crack Down on Bullying or Shut the Site.” *The Guardian*, 19 Aug. 2014, www.theguardian.com/technology/2014/aug/19/askfm-askcom-bullying.
- Hernandez, Joe. “A Military Drone with a Mind of Its Own Was Used in Combat, U.N. Says.” *NPR*, 1 June 2021, www.npr.org/2021/06/01/1002196245/a-u-n-report-suggests-libya-saw-the-first-battlefield-killing-by-an-autonomous-d.
- Hernandez, Michael J. *Database Design for Mere Mortals: A Hands-On Guide to Relational Database Design*. 4th ed., Addison-Wesley, 2020.
- Hey, Tony, and Gyuri Pápay. *The Computing Universe: A Journey through a Revolution*. Cambridge UP, 2015.

- HHS Cybersecurity Program. "Ransomware Trends 2021." *US Department of Health and Human Services*, 3 June 2021, hhs.gov/sites/default/files/ransomware-trends-2021.pdf.
- Hider, Philip. *Information Resource Description: Creating and Managing Metadata*. American Library Association, 2012.
- Hill, Michael, and Dan Swinhoe. "The 15 Biggest Data Breaches of the 21st Century." *CSO*, 8 Nov. 2022, www.csponline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html.
- Himma, Kenneth Einar. *The Handbook of Information and Computer Ethics*. Wiley, 2008.
- Hinduja, Sameer. *Music Piracy and Crime Theory*. LFB, 2005.
- Hinduja, Sameer, and Justin W. Patchin. *Cyberbullying Prevention and Response: Expert Perspectives*. Routledge, 2012.
- Hirshey, Jeffrey Kenneth. "Symbiotic Relationships: Pragmatic Acceptance of Data Scraping." *Berkeley Technical Law Journal*, vol. 29, 2014, pp. 897-927.
- History of Cryptography: An Easy to Understand History of Cryptography*. Thawte, 2013.
- "The History of Web Browsers." Mozilla, www.mozilla.org/en-US/firefox/browser/browser-history.
- Hoehle, Hartmut, Eusebio Scornavacca, and Sid Huff. "Three Decades of Research on Consumer Adoption and Utilization of Electronic Banking Channels: A Literature Analysis." *Decision Support Systems*, vol. 54, no. 1, 2012, pp. 122-32.
- Hoffman, Bruce. *Inside Terrorism*. Columbia UP, 2006.
- Hoffman, Jan. "Online Bullies Pull Schools into the Fray." *New York Times*, 27 June 2010, www.nytimes.com/2010/06/28/style/28bully.html.
- Hoffstein, Jeffrey, Jill Pipher, and Joseph H. Silverman. *An Introduction to Mathematical Cryptography*. 2nd ed., Springer, 2014.
- Hofmann, Chris, Marcia Knous, and John V. Hedke. *Firefox and Thunderbird Garage*. Prentice Hall Professional Technical Reference, 2005.
- Hofmann, Markus, and Leland R. Beaumont. "Content Transfer." *Content Networking: Architecture, Protocols, and Practice*. Elsevier, 2005, pp. 25-52.
- Holcombe, Jane, and Charles Holcombe. *Survey of Operating Systems*. 6th ed., McGraw-Hill Education, 2020.
- Holden, Joshua. *The Mathematics of Secrets: Cryptography from Caesar Ciphers to Digital Encryption*. Princeton UP, 2018.
- Holland, Steve, and Doina Chiacu. "U.S. and Allies Accuse China of Global Hacking Spree." *Reuters*, 20 July 2021, www.reuters.com/technology/us-allies-accuse-china-global-cyber-hacking-campaign-2021-07-19.
- Hollo, Stefan, and J. Richard Hollo. *Combinatorics Problems and Solutions*. Abrazol, 2013.
- Holmes, Aaron. "Hackers Have Become So Sophisticated That Nearly 4 Billion Records Have Been Stolen from People in the Last Decade Alone: Here Are the 10 Biggest Data Breaches of the 2010s." *Business Insider*, 13 Nov. 2019, www.businessinsider.com/biggest-hacks-2010s-facebook-equifax-adobe-marriott-2019-10.
- Holt, Thomas, et al. "Comparing Civilian Willingness to Attack Critical Infrastructure on and off Line." *Proceedings of the European Conference on e-Government*, 2012, pp. 345-51.
- Holt, Thomas J., Adam M. Bossler, and Kathryn C. Seigfried-Spellar. *Cybercrime and Digital Forensics: An Introduction*. 3rd ed., Routledge, 2022.
- Hong, Jason. "The State of Phishing Attacks." *Communications of the ACM*, vol. 55, no. 1, 2012, pp. 74-81.
- Hoofnagle, Chris Jay. "Identity Theft: Making the Known Unknowns Known." *Harvard Journal of Law and Technology*, vol. 21, no. 1, 2007, pp. 97-122.
- Horner, Veronica. "How Big Data Analytics Is Changing the Media Industry." *SEI*, 5 Oct. 2020, www.sei.com/insights/article/how-big-data-analytics-is-changing-the-media-industry.
- Hornyak, Tim. "Why Japan Is Building Smart Cities from Scratch." *Nature*, 17 Aug. 2022, www.nature.com/articles/d41586-022-02218-5.
- Horodyski, John. *Metadata Matters*. CRC Press, 2022.
- Horstmann, Cay. *Big Java: Early Objects*. 7th ed., John Wiley & Sons, 2018.
- Houck, Max M. *Forensic Science: Modern Methods of Solving Crime*. Praeger, 2007.
- "How Computers Work: The CPU and Memory." *University of Rhode Island*, homepage.cs.uri.edu/faculty/wolfe/book/Readings/Reading04.htm.
- "How Cryptography and Web3 Can Help Restore Trust in Digital Media." *Stanford Engineering*, 17 June 2022, engineering.stanford.edu/magazine/how-cryptography-and-web3-can-help-restore-trust-digital-media.
- "How Firewalls Work." *Boston University TechWeb*, www.bu.edu/tech/about/security-resources/host-based/intro.
- "How to Get Less Spam in Your Email." *Federal Trade Commission Consumer Advice*, May 2021, consumer.ftc.gov/articles/how-get-less-spam-your-email.
- "How to Implement Zero Trust: A Comprehensive Guide." *Security Boulevard*, 31 July 2023,

- securityboulevard.com/2023/07/how-to-implement-zero-trust-a-comprehensive-guide.
- “How to Protect Yourself While on the Internet.” *Computer Hope*, 1 May 2023, www.computerhope.com/issues/ch000507.htm.
- “How to Recognize and Avoid Phishing Scams.” *Federal Trade Commission Consumer Advice*, Sept. 2022, consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams.
- “How to: Use PGP for Windows.” *Surveillance Self-Defense*, 17 June 2018, ssd.eff.org/module/how-use-pgp-windows.
- “How Virtual Private Networks Work.” *Cisco*, 13 Oct. 2008, www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html.
- “How Websites and Apps Collect and Use Your Information.” *Federal Trade Commission Consumer Advice*, Sept. 2023, consumer.ftc.gov/articles/how-websites-and-apps-collect-and-use-your-information.
- Hoyt, Robert. “American Risk and Insurance Association (ARIA).” *Encyclopedia of Actuarial Science*. Wiley, 2006.
- Hsu, Tiffany. “What Can You Do When AI Lies About You?” *New York Times*, 7 Aug. 2023, www.nytimes.com/2023/08/03/business/media/ai-defamation-lies-accuracy.html.
- “HTML Tutorial.” *W3Schools*, www.w3schools.com/html.
- Huddleston, Rob. *HTML, XHTML, and CSS: Your Visual Blueprint for Designing Effective Web Pages*. John Wiley & Sons, 2009.
- Hughes, Arthur Middleton. “Why Email Marketing Is King.” *Harvard Business Review*, 21 Aug. 2012, hbr.org/2012/08/why-email-marketing-is-king.
- Husak, Douglas. *Overcriminalization: The Limits of the Criminal Law*. Oxford UP, 2008.
- Huth, Alexa, and James Cebula. *The Basics of Cloud Computing*. Carnegie Mellon U and US Computer Emergency Readiness Team, 2011, www.cisa.gov/sites/default/files/publications/USCERT-Cloud ComputingHuthCebula.pdf.
- IEEE Smart Cities, 2023, smartcities.ieee.org.
- “An Illustrated History of Mac OS X.” *Tower*, 12 Jan. 2016, www.git-tower.com/blog/history-of-osx.
- INCOSE Systems Security Engineering Working Group. “Introduction to Systems Security Engineering Vocabulary.” *Insight*, vol. 23, no. 3, 2020, doi.org/10.1002/inst.12301.
- Iniewski, Krzysztof. *Embedded Systems: Hardware, Design, and Implementation*. Wiley, 2012.
- Institute for Economics and Peace. *Global Terrorism Index 2022: Measuring the Impact of Terrorism*. Institute for Economics and Peace, 2022.
- “Intel’s First Microprocessor: Its Invention, Introduction, and Lasting Influence.” *Intel*, www.intel.com/content/www/us/en/history/museum-story-of-intel-4004.html.
- “Internet Porn ‘Increasing Child Abuse.’” *The Guardian*, 12 Jan. 2004, www.guardian.co.uk/technology/2004/jan/12/childprotection.childrensservices.
- “Introduction to User-Centered Design.” *Usability First*, www.usabilityfirst.com/about-usability/introduction-to-user-centered-design.
- “Intrusion.” *NIST Computer Security Resource Center*, csrc.nist.gov/glossary/term/intrusion.
- “Intrusion Detection System (IDS).” *Geeks for Geeks*, 14 Mar. 2023, www.geeksforgeeks.org/intrusion-detection-system-ids.
- “iOS: A Visual History.” *The Verge*, 16 Sept. 2013, www.theverge.com/2011/12/13/2612736/ios-history-iphone-ipad.
- Israelashvili, Moshe, et al. “Adolescents’ Over-Use of the Cyber World: Internet Addiction or Identity Exploration?” *Journal of Adolescence*, vol. 35, no. 2, 2012, pp. 417-24.
- Jackson, Daniel. *The Essence of Software Design: Why Concepts Matter for Great Design*. Princeton UP, 2023.
- Jacobson, Douglas, and Joseph Idziorek. *Computer Security Literacy: Staying Safe in a Digital World*. CRC, 2013.
- Jain, Anil K., Arun Russ, and Sharath Pankanti. “Biometrics: A Tool for Information Security.” *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, 2006, pp. 125-43.
- Jaishankar, K. “Cyber Criminology: Evolving a Novel Discipline with a New Journal.” *International Journal of Cyber Criminology*, vol. 1, no. 1, 2007, www.cybercrimejournal.com/pdf/editorialijcc.pdf.
- Jakobsson, Markus, and Steven Myers, editors. *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*. John Wiley & Sons, 2007.
- Jalonick, Mary Clare, and Eric Tucker. “Senate Panel Backs Assessment That Russia Interfered in 2016.” *AP News*, 21 Apr. 2020, apnews.com/article/d094918c0421b872eac7dc4b16e613c7.
- James, Lance. *Phishing Exposed*. Syngress Publishing, 2005.
- James, Mike. “The Triumph of Deep Learning.” *I Programmer*, 14 Dec. 2012, www.i-programmer.info/programming/article-intelligence/5206-the-triumph-of-deep-learning.html.
- Jamieson, Alastair, and Eric McClam. “Millions of Target Customers’ Credit, Debit Card Accounts May Be Hit by Data Breach.” *NBC News*, 19 Dec. 2013, www.nbcnews.com/business/consumer/millions-target-cards-breached.

- customers-credit-debit-card-accounts-may-be-hit-f2D117
75203.
- Jansen, Mark, and Paula Beaton. "5G vs. 4G: How Does the Newest Network Improve on the Last?" *DigitalTrends*, 22 Apr. 2022, www.digitaltrends.com/mobile/5g-vs-4g.
- Jarmul, Katharine. *Practical Data Privacy: Enhancing Privacy and Security in Data*. O'Reilly Media, 2023.
- Jasper, Margaret C. *The Law of Obscenity and Pornography*. 2nd ed., Oceana, 2009.
- Jasper, Scott. *Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security*. Georgetown UP, 2012.
- JD Consulting. *Y2K Procrastinator's Guide*. Charles River Media, 2000.
- Jenkins, Simms. *The Truth about Email Marketing*. FT Press, 2009.
- Jenkinson, A. J. *Stuxnet to Sunburst: 20 Years of Digital Exploitation and Cyber Warfare*. CRC Press, 2022.
- Johns, Adrian. Piracy: The Intellectual Property Wars from Gutenberg to Gates. U of Chicago P, 2009.
- Johnson, Jeff. *Designing with the Mind in Mind*. 2nd ed., Morgan Kaufmann, 2014.
- Jorgensen, H. "Methods & Elements of a Solid Risk Management Strategy." *Risk Management*, vol. 52, 2005, pp. 53-54.
- Kabir, Arafat. "After Hackers Steal \$81 Million, What Now for Bangladesh Central Bank?" *Forbes*, 16 Mar. 2016, www.forbes.com/sites/arafatkabir/2016/03/16/after-hackers-steal-81-million-what-now-for-bangladesh-central-bank/?sh=1bbda9762156.
- Kagubare, Ines. "Increasingly Autonomous Cars Raise Cybersecurity Fears." *Hill*, 8 June 2022, thehill.com/driving-into-the-future/3514634-increasingly-autonomous-cars-raise-cybersecurity-fears.
- Kale, Vivek. *Guide to Cloud Computing for Business and Technology Managers*. CRC, 2015.
- Kamhoua, Charles A., Christopher D. Kiekintveld, Fei Fang, and Quanyan Zhu, editors. *Game Theory and Machine Learning for Cyber Security*. Wiley, 2021.
- Kassner, Michael. "Self-Checking Chips Could Eliminate Hardware Security Issues." *Tech Republic*, 31 Aug. 2016, engineering.nyu.edu/news/self-checking-chips-could-eliminate-hardware-security-issues.
- Kastrenakes, Jacob. "'Six Strikes' Anti-Piracy Initiative Ends after Failing to Scare Off 'Hardcore' Pirates." *The Verge*, 30 Jan. 2017, www.theverge.com/2017/1/30/14445596/six-strikes-piracy-system-failed-ending.
- Katz, Jonathan, and Yehuda Lindell. *Introduction to Modern Cryptography*. 3rd ed., Chapman and Hall, 2020.
- Keizer, Garret. *Privacy*. Picador, 2012.
- Kemper, Bitsy. *The Right to Privacy: Interpreting the Constitution*. Rosen, 2015.
- Kenton, Will. "Industrial Espionage: Definition, Examples, Types, Legality." *Investopedia*, 12 July 2022, www.investopedia.com/terms/i/industrial-espionage.asp.
- Kerr, Orin S. "Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes." *New York University Law Review*, vol. 78, 2003, p. 1596.
- _____. "Vagueness Challenges to the Computer Fraud and Abuse Act." *Minnesota Law Review*, vol. 94, 2010, p. 1561.
- Khaira, Rachna. "Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details." *Tribune*, 5 Jan. 2018, www.tribuneindia.com/news/archive/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details-523361.
- Khaira, Rachna, Aman Sethi, and Gopal Sathe. "UIDAI's Aadhaar Software Hacked, ID Database Compromised, Experts Confirm." *HuffPost India*, 26 Sept. 2018, www.huffpost.com/archive/in/entry/uidai-s-aadhaar-software-hacked-id-database-compromised-experts-confirm_in_5c128ddee4b0e15b460af020.
- Khan, Gul N., and Krzysztof Iniewski, editors. *Embedded and Networking Systems: Design, Software, and Implementation*. CRC, 2014.
- Kharaz, Amin, et. al. "UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware." *USENIX: The Advanced Computing Systems Association*, 2016, www.usenix.org/system/files/conference/usenix-security16/sec16_paper_kharaz.pdf.
- Kipper, Gregory. *Wireless Crime and Forensic Investigation*. Auerbach, 2007.
- Kizza, Joseph Migga. *Ethical and Social Issues in the Information Age*. 7th ed., Springer, 2023.
- _____. *Guide to Computer Network Security*. 6th ed., Springer, 2024.
- Klinke, A., and O. Renn. "A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies." *Risk Analysis: An International Journal*, vol. 22, no. 6, 2002, pp. 1071-94.
- Knott, Daniel. *Hands-On Mobile App Testing*. Pearson Education, 2015.
- Koch, Richie. "Cookies, the GDPR, and the ePrivacy Directive." *GDPR.EU*, gdpr.eu/cookies.
- Kolb, Jason, and Jeremy Kolb. *The Big Data Revolution*. Applied Data Labs, 2013.
- Komninos, Andreas. "An Introduction to Usability." *Interaction Design Foundation*, 22 July 2020,

- www.interaction-design.org/literature/article/an-introduction-to-usability.
- Koops, Bert-Jaap. "The Trouble with European Data Protection Law." *International Data Privacy Law*, vol. 4, no. 4, 2014, pp. 250-61.
- Korte, Gregory. "The Many Tentacles of the Trump-Russia Probe." *USA Today*, 18 June 2017, www.msn.com/en-us/news/politics/the-many-tentacles-of-the-trump-russia-probe/ar-BBCOtnL?li=BBnbcA1.
- Koshiw, Isobel. "How an International Hacker Network Turned Stolen Press Releases into \$100 Million." *The Verge*, 22 Aug. 2018, www.theverge.com/2018/8/22/17716622/sec-business-wire-hack-stolen-press-release-fraud-ukraine.
- Krebs, Brian. "Shadowy Russian Firm Seen as Conduit for Cybercrime." *Washington Post*, 13 Oct. 2007, www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461.html.
- Krimsky, Sheldon, and Tania Simoncelli. *Genetic Justice: DNA Data Banks, Criminal Investigations, and Civil Liberties*. Columbia UP, 2011.
- Krishnan, K. N., with D. R. Berwick. *Developing a Police Perspective and Exploring the Use of Biometrics and Other Emerging Technologies as an Investigative Tool in Identity Crimes*. Australasian Centre for Policing Research, 2004.
- Kristol, David M. "HTTP Cookies: Standards, Privacy, and Politics." *ArXiv*, 9 May 2001, arxiv.org/abs/cs/0105018.
- Krivkovich, A., and C. Levy. "Managing the People Side of Risk." *McKinsey & Company*, 1 May 2015, www.mckinsey.com/capabilities/risk-and-resilience/our-insights/managing-the-people-side-of-risk.
- Kruk, Robert. "Public, Private and Hybrid Clouds: What's the Difference?" *Techopedia*, 5 July 2022, www.techopedia.com/2/28575/trends/cloud-computing/public-private-and-hybrid-clouds-whats-the-difference.
- Kudrati, Abbas, and Binil Pillai. *Zero Trust Journey across the Digital Estate*. CRC Press, 2022.
- Kumar, M. J. "Facial Recognition by Machines: Is it an Effective Surveillance Tactic?" *IETE Technical Review*, vol. 30, no. 2, 2013, pp. 93-94.
- Kumar, Raghvendra, Rohit Sharma, and Prasant Kumar Pattnaik, editors. *Multimedia Technologies in the Internet of Things Environment*. Springer, 2021.
- Kuo, L. Jay, and Edward M. Dua. *Crisis Investing for the Year 2000: How to Profit from the Coming Y2K Computer Crash*. Birch Lane Press, 1999.
- Kushner, David. "The Real Story of Stuxnet." *IEEE Spectrum*, 26 Feb. 2013, spectrum.ieee.org/the-real-story-of-stuxnet.
- La Counte, Scott. *The Ridiculously Simple Guide to Surfing the Internet with Google Chrome*. SL Editions, 2020.
- Laalaoui, Yacine, and Nizar Bouguila, editors. *Artificial Intelligence Applications in Information and Communication Technologies*. Springer International Publishing, 2015.
- Lague, David. "In U.S.-China AI Contest, the Race Is on to Deploy Killer Robots." *Reuters*, 8 Sept. 2023, www.reuters.com/investigates/special-report/us-china-tech-drones.
- Lander, Steve. "Disadvantages or Problems for Implementing Wi-Fi Technology." *Chron*, smallbusiness.chron.com/disadvantages-problems-implementing-wifi-technology-61914.html.
- Lanier, Jaron. *Ten Arguments for Deleting Your Social Media Accounts Right Now*. Henry Holt, 2018.
- Lapsley, Phil. *Exploding the Phone: The Untold Story of the Teenagers and Outlaws Who Hacked Ma Bell*. Grove Press, 2013.
- Lauckner, Kurt, and Zenia Bahorski. *The Computer Continuum*. 5th ed., Pearson, 2009.
- Laudon, Kenneth C., and Carol Guercio Traver. *E-Commerce 2019*. 15th ed., Pearson Education, 2020.
- Laurence, Tiana. "A Brief History of the Bitcoin Blockchain." *Dummies*, 31 July 2017, www.dummies.com/personal-finance/brief-history-bitcoin-blockchain.
- Lee, Kent D. *Foundations of Programming Languages*. 2nd ed., Springer, 2017.
- Lee, M. C. "Factors Influencing the Adoption of Internet Banking: An Integration of TAM and TPB with Perceived Risk and Perceived Benefit." *Electronic Commerce Research and Applications*, vol. 8, no. 3, 2009, pp. 130-41.
- Lee, Roger Y., editor. *Applied Computing and Information Technology*. Springer, 2014.
- Lee, Timothy B. "Why It's Time for Uber to Get Out of the Self-Driving Car Business." *Ars Technica*, 27 Mar. 2018, arstechnica.com/cars/2018/03/ubers-self-driving-car-project-is-struggling-the-company-should-sell-it.
- LeJeune, Urban A., and Jeff Duntemann. *Netscape and HTML Explorer*. Coriolis Group Books, 1995.
- Lemke, Donald, and Tod Smith. *Steve Jobs, Steve Wozniak, and the Personal Computer*. Capstone Press, 2010.
- Lenhart, A. "Cyberbullying and Online Teens." *Pew Research Center*, 27 June 2007, www.pewresearch.org/internet/2007/06/27/cyberbullying.
- Lettnin, Djones, and Markus Winterholer, editors. *Embedded Software Verification and Debugging*. Springer-Verlag New York, 2017.

- Levi, M. "Assessing the Trends, Scale and Nature of Economic Cybercrimes: Overview and Issues." *Crime, Law and Social Change*, vol. 67, no. 1, 2017, pp. 3-20.
- Levin, Avner, and Mary Jo Nicholson. "Privacy Law in the United States, the EU, and Canada: The Allure of the Middle Ground." *University of Ottawa Law & Technology Journal*, vol. 2, no. 2, 2005, pp. 357-95.
- Levy, Stephen. "Almost 50 Years into the Crypto Wars, Encryption's Opponents Are Still Wrong." *Wired*, 21 July 2023, www.wired.com/story/plaintext-50-years-into-the-crypto-wars-encryptions-opponents-are-still-wrong.
- Levy, Steven. *Hackers: Heroes of the Computer Revolution*. O'Reilly Media, 2010.
- Li, Ling. "Technology Designed to Combat Fakes in the Global Supply Chain." *Business Horizons*, vol. 56, no. 2, 2013, pp. 167-77.
- Li, Lisa Bei. "Data Privacy in the Cyber Age: Recommendations for Regulating Doxing and Swatting." *Federal Communications Law Journal*, vol. 70, no. 3, 2018, pp. 317-28.
- Libby, Kristina. "This Bill Hader Deepfake Video Is Amazing: It's Also Terrifying for Our Future." *Popular Mechanics*, 13 Aug. 2019, www.popularmechanics.com/technology/security/a28691128/deepfake-technology.
- Lichtblau, Eric. "In Secret, Court Vastly Broadens Powers of N.S.A." *New York Times*, 7 July 2013, www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html.
- Liebowitz, M. "Online Bullying Rampant Among Teens, Survey Finds." *NBC News*, 9 Nov. 2011, www.nbcnews.com/id/wbna45227264.
- Liff, Adam P. "Cyberwar: A New 'Absolute Weapons'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *Journal of Strategic Studies*, vol. 35, no. 3, 2012, pp. 401-28.
- Lima, Cristiano. "Want Our Metadata? Get a Warrant, Rep. Ted Lieu Says." *Washington Post*, 20 Apr. 2022, www.washingtonpost.com/politics/2022/04/20/want-our-metadata-get-warrant-rep-ted-lieu-says.
- Lininger, Rachael, and Russell Dean Vines. *Phishing: Cutting the Identity Theft Line*. Wiley, 2005.
- Liska, Allan, and Timothy Gallo. *Ransomware: Defending Against Digital Extortion*. O'Reilly Media, 2016.
- Liu, Ling, and M. Tamer Özsü, editors. *Encyclopedia of Database Systems*. Springer, 2009.
- Long, Johnny. *No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing*. Syngress, 2008.
- Long, Simon. *An Introduction to C & GUI Programming*. Raspberry Pi Press, 2019.
- Loshin, Peter. *IPv6: Theory, Protocol, and Practice*. 2nd ed., Morgan Kaufmann, 2004.
- Luttgens, Jason T., Matthew Pepe, and Kevin Mandia. *Incident Response and Computer Forensics*. 3rd ed., McGraw-Hill, 2014.
- Lyles, Taylor. "Marriott Discloses Another Security Breach That May Impact Over 5 Million Guests." *The Verge*, 1 Apr. 2020, www.theverge.com/2020/4/1/21203313/marriott-database-security-breach-5-million-guests.
- MacCormick, John. *Nine Algorithms That Changed the Future: The Ingenious Ideas That Drive Today's Computers*. Princeton UP, 2012.
- Mack, George. "The Fascinating History of Cyber Security You Never Knew." *CyberTalk.org*, 14 June 2023, www.cybertalk.org/2023/06/14/the-fascinating-history-of-cyber-security-you-never-knew.
- Macomber, John. "The Smart Way to Build Smart Cities." *Forbes*, 4 Apr. 2018, www.forbes.com/sites/hbsworkingknowledge/2018/04/04/the-smart-way-to-build-smart-cities.
- Madigan, D. "Statistics and the War on Spam." *Statistics: A Guide to the Unknown*. 4th ed., Thompson Higher Education, 2006.
- Magnuson, Stew. "U.S. Government Attempts to Thwart Chinese Network Intrusions." *National Defense*, vol. 97, no. 704, 2012, pp. 58-60.
- Mahdawi, Arwa. "Melania Trump Rails against Cyberbullying-But She Is Using Social Media to Gaslight the World." *The Guardian*, 21 Aug. 2018, www.theguardian.com/commentisfree/2018/aug/21/melania-trump-rails-against-cyberbullying-social-media-gaslight-world.
- Mairs, John. *VPNs: A Beginner's Guide*. McGraw-Hill, 2002.
- Mak, Aaron. "Marriott Hit by One of the Biggest Hacks in History." *Slate*, 30 Nov. 2018, slate.com/technology/2018/11/marriott-hack-guest-personal-information.html.
- Malhotra, Ashish. "The World's Largest Biometric ID System Keeps Getting Hacked." *Motherboard*, 8 Jan. 2018, www.vice.com/en/article/43q4jp/aadhaar-hack-insecure-biometric-id-system.
- Manishin, Glenn B. *Complying with the CAN-SPAM Act and Other Critical Business Issues: Staying Out of Trouble*. Practicing Law Institute, 2004.
- Mann, Charles C. "A Primer in Public-Key Encryption." *The Atlantic*, Sept. 2002, www.theatlantic.com/magazine/archive/2002/09/a-primer-on-public-key-encryption/302574.
- Mann, Ian. *Hacking the Human: Social Engineering Techniques and Security Countermeasures*. Gower, 2008.

- Manson, K. "US Has Already Lost AI Fight to China, Says Ex-Pentagon Software Chief." *Financial Times*, 10 Oct. 2021, www.ft.com/content/f939db9a-40af-4bd1-b67d-10492535f8e0.
- Mantlero, Alessandro. "The EU Proposal for a General Data Protection Regulation and the Roots of the 'Right to Be Forgotten.'" *Computer Law & Security Review*, vol. 29, no. 3, June 2013, pp. 229-35.
- Maras, Marie-Helen. *Computer Forensics: Cybercriminals, Laws and Evidence*. Jones & Bartlett Learning, 2015.
- Marcella, Albert J., and Robert S. Greenfield, editors. *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*. CRC Press, 2002.
- Marchewka, Jack T. *Information Technology Project Management*. 5th ed., Wiley, 2015.
- Marcum, C., G. Higgins, T. Freiburger, et al. "Exploration of the Cyberbullying Victim/Offender Overlap by Sex." *American Journal of Criminal Justice*, vol. 39, 2014, pp. 538-48.
- Marena, Ted, and Jenny Yao. "Hardware Security in the IoT." *Embedded Computing Design*, 24 July 2015, www.embeddedcomputing.com/technology/security/hardware-security-in-the-iot.
- Markelo, Steve. *Microsoft Edge: A Beginner's Guide to the Windows 10 Browser*. Conceptual Kings, 2015.
- "Market Share Held by the Leading Computer (Desktop/Tablet/Console) Operating Systems Worldwide from January 2012 to June 2023." *Statista*, 5 Sept. 2023, www.statista.com/statistics/268237/global-market-share-held-by-operating-systems-since-2009.
- Markoff, John. "Smaller, Faster, Cheaper, Over: The Future of Computer Chips." *New York Times*, 25 Sept. 2015, www.nytimes.com/2015/09/27/technology/smaller-faster-cheaper-over-the-future-of-computer-chips.html.
- Marks, Gene. "Yes, You Should Monitor Your Remote Workers-But Not Because You Don't Trust Them." *The Guardian*, 25 Sept. 2022, www.theguardian.com/business/2022/sep/25/monitor-workers-at-home-security-cybercrime.
- Marr, Bernard. "A Short History of Bitcoin and Crypto Currency Everyone Should Read." *Forbes*, 6 Dec. 2017, www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/#4ad41aa13f27.
- "Marriott Provides Update on Starwood Database Security Incident." *Marriott International*, 4 Jan. 2019, news.marriott.com/2019/01/marriott-provides-update-on-starwood-database-security-incident.
- Marsland, Stephen. *Machine Learning: An Algorithmic Perspective*. Taylor, 2009.
- Martin, George E. *Counting: The Art of Enumerative Combinatorics*. Springer, 2001.
- Martinson, O. "Global Investments: Discover Your Real Cost of Capital-and Your Real Risk." *Journal of Corporate Accounting & Finance*, vol. 11, no. 6, 2000, pp. 23-28.
- Marzolf, Julie Schwab. *Online Privacy*. Gareth Stevens, 2013.
- Matineau, Paris. "What Is a Bot?" *Wired*, 16 Nov. 2018, www.wired.com/story/the-know-it-alls-what-is-a-bot.
- Matusitz, Jonathan. "Cyberterrorism: Postmodern State of Chaos." *Information Security Journal: A Global Perspective*, vol. 17, no. 4, 2008, pp. 179-87.
- Mayer-Schönberger, Viktor. *Delete: The Virtue of Forgetting in the Digital Age*. Princeton UP, 2011.
- Mazzetti, Mark, and Eric Lichtblau. "C.I.A. Judgment on Russia Built on Swell of Evidence." *New York Times*, 12 Dec. 2016, www.nytimes.com/2016/12/11/us/politics/cia-judgment-intelligence-russia-hacking-evidence.html.
- McCabe, J. A. "Integrating Mnemonics into Psychology Instruction." *OTRP Online*, 2011, teachpsych.org/resources/Documents/otrp/resources/mccabe11.pdf.
- McCarthy, Ellen. "What Is Catfishing? A Brief (and Sordid) History." *Washington Post*, 9 Jan. 2016, www.washingtonpost.com/news/arts-and-entertainment/wp/2016/01/09/what-is-catfishing-a-brief-and-sordid-history.
- McCauley, Renée, et al. "Debugging: A Review of the Literature from an Educational Perspective." *Computer Science Education*, vol. 18, no. 2, 2008, pp. 67-92.
- McDaniel, Adam. *HTML 5: Your Visual Blueprint for Designing Rich Web Pages and Applications*. John Wiley & Sons, 2011.
- McFedries, Paul. *Fixing Your Computer: Absolute Beginner's Guide*. Que, 2014.
- McGuigan, Dermot, and Beverly Jacobson. *Y2K and Y-O-U: A Sane Person's Home-Preparation Guide*. Chelsea Green, 1999.
- McLaurin, Joshua. "Making Cyberspace Safe for Democracy: The Challenge Posed by Denial-of-Service Attacks." *Yale Law and Policy Review*, vol. 30, no. 1, 2011, p. 11.
- McLellan, Charles. "The History of Windows: A Timeline." *ZDNet*, 14 Apr. 2014, www.zdnet.com/article/the-history-of-windows-a-timeline.
- McLoughlin, Ian. *Computer Systems: An Embedded Approach*. McGraw-Hill, 2018.
- McNally, Megan. *Identity Theft in Today's World*. Praeger, 2012.

- McNeill, Daniel, and Paul Freiberger. *Fuzzy Logic: The Revolutionary Computer Technology That Is Changing Our World*. Touchstone, 1993.
- Mead, Nancy R., and Carol C. Woody. *Cyber Security Engineering: A Practical Approach for Systems and Software Assurance*. Addison-Wesley Professional, 2016.
- Mearian, Lucas. "IBM, Chainyard Unveil Blockchain-Based 'Trust Your Supplier' Network." *Computerworld*, 5 Aug. 2019, www.computerworld.com/article/3429642/ibm-chainyard-unveil-blockchain-based-trust-your-supplier-network.html.
- "Media Arts, Design and Technology Computer Requirements." *NC State College of Design*, May 2023, academics.design.ncsu.edu/it/docs/artdesign-computer-requirements.
- Mehta, Prateek. *Creating Google Chrome Extensions*. Springer Science + Business Media, 2016.
- Menezes, Alfred J., Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.
- Meola, Andrew. "Smart Buses, Trains, Cars & Planes: How IoT Will Create Private and Public Smart Transportation." *Business Insider*, 30 Jan. 2020, www.businessinsider.com/smart-transportation-iot.
- Messier, Ric. *Build Your Own Cybersecurity Testing Lab: Low-Cost Solutions for Testing in Virtual and Cloud-Based Environments*. McGraw Hill, 2020.
- Metz, Cade. "OpenAI to Offer New Version of ChatGPT for a \$20 Monthly Fee." *New York Times*, 1 Feb. 2023, www.nytimes.com/2023/02/01/technology/openai-chatgpt-plus-subscription.html.
- Mihm, Stephen. "China Didn't Invent Industrial Espionage." *Bloomberg*, 26 May 2015, www.bloomberg.com/view/articles/2015-05-26/china-didnt-invent-industrial-espionage.
- Miller, Arthur I. *The Artist in the Machine: The World of AI-Powered Creativity*. MIT Press, 2019.
- Miller, Charles, and Aaron Doering. *The New Landscape of Mobile Learning: Redesigning Education in an App-Based World*. Routledge, 2014.
- Miller, Greg. "Trump's Pick for National Security Adviser Brings Experience and Controversy." *Washington Post*, 17 Nov. 2016, www.washingtonpost.com/world/national-security/trumps-pick-for-national-security-adviser-brings-experience-and-controversy/2016/11/17/0962eb88-ad08-11e6-8b45-f8e493f06fcd_story.html?utm_term=.dea1837ab124.
- Miller, Greg, Ellen Nakashima, and Adam Entous. "Obama's Secret Struggle to Punish Russia for Putin's Election Assault." *Washington Post*, 23 June 2017, www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking.
- Miller, Steven Jack. *Metadata for Digital Collections*. 2nd ed., ALA Neal-Schuman, 2022.
- Mills, James H. "Make Way for the Cyber Fleet!" *US Naval Institute Proceedings*, vol. 136, no. 1, 2010, www.usni.org/magazines/proceedings/2010/january/make-way-cyber-fleet.
- Minsky, Marvin, and Seymour A. Papert. *Perceptrons: An Introduction to Computational Geometry*. Reissue ed., MIT Press, 2017.
- Mitchell, Tom M. *Machine Learning*. McGraw, 1997.
- Mitnick, Kevin. *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*. Little, Brown and Company, 2011.
- Mitnick, Kevin D., and William L. Simon. *The Art of Deception: Controlling the Human Element of Security*. Wiley, 2002.
- _____. *The Art of Intrusion: The Real Stories behind the Exploits of Hackers, Intruders, and Deceivers*. Wiley, 2006.
- "Mobile Application Security." *US Department of Homeland Security Science and Technology*, 12 Jan. 2023, www.dhs.gov/science-and-technology/cybersecurity-mobile-app-security.
- "Mobile Operating System Market Share Worldwide-June 2023." *Statcounter*, June 2023, gs.statcounter.com/os-market-share/mobile/worldwide/#monthly-202206-202306.
- Mollo, David, and Joe Tidy. "George Floyd: Anonymous Hackers Re-Emerge Amid US Unrest." *BBC*, 1 June 2020, www.bbc.com/news/technology-52879000.
- Montasari, Reza. *Countering Cyberterrorism: The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity*. Springer Nature, 2023.
- Montasari, Reza, editor. *Artificial Intelligence and National Security*. Springer Nature, 2022.
- Moon, Mariella. "Now California's DMV Can Allow Fully Driverless Car Testing." *Engadget*, 3 Apr. 2018, www.engadget.com/2018/04/03/california-fully-driverless-car-testing.
- Morales, R., and B. Kleiner. "New Development in Techniques for Analyzing Diversified Companies in Today's Global Environment." *Management Research News*, vol. 19, 1996, pp. 41-49.
- Moretti, Marcus. "Before Mac OS X, There Was OS 1 Through 9: A History of Apple's Operating System." *Business Insider*, 10 July 2012, www.businessinsider.com/mac-os-1-through-x-2012-7?op=1.

- Morgan, Jacob. "A Simple Explanation of 'The Internet of Things.'" *Forbes*, 13 May 2014, www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand.
- Morozov, Evgeny. "Battling the Cyber Warmongers." *Wall Street Journal Dow Jones*, 8 May 2010, online.wsj.com/article/SB10001424052748704370704575228653351323986.html.
- Morris, H. "Europe Cracks Down on Cybercrime." *International New York Times*, 12 Mar. 2012, archive.nytimes.com/rendezvous.blogs.nytimes.com/2012/03/29/europe-cracks-down-on-cybercrime.
- Morrison, Jim. "How Doctors Are Using Artificial Intelligence to Battle Covid-19." *Smithsonian Magazine*, 5 Mar. 2021, www.smithsonianmag.com/science-nature/how-doctors-are-using-artificial-intelligence-battle-covid-19-180977124.
- Morrison, Sara. "Biden Makes Good on His Promise to Punish Russia for the Massive SolarWinds Hack." *Vox*, 15 Apr. 2021, www.vox.com/recode/22385555/biden-solarwinds-hack-russia-sanctions.
- Morselli, Carlo, editor. *Crime and Networks*. Routledge, 2014.
- Moscaritolo, Angela. "5G Will Save You Almost 24 Hours of Download Time Per Month." *PCMag*, 16 Oct. 2018, www.pc当地新闻.com/news/5g-will-save-you-almost-24-hours-of-download-time-per-month.
- Moss, Caroline. "Strangers Have Been Using This Woman's Photos to Catfish People Online for Ten Years." *Business Insider*, 21 Jan. 2015, www.businessinsider.com/strangers-have-been-using-this-womans-photos-to-catfish-people-for-10-years-2015-1.
- Mowbray, Thomas J. *Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions*. John Wiley & Sons, 2014.
- Mowery, David C., and Timothy Simcoe. "Is the Internet a US Invention? An Economic and Technological History of Computer Networking." *Research Policy*, vol. 31, Dec. 2002, pp. 1369-87.
- Mueller, Scott. *Upgrading and Repairing PCs*. 22nd ed., Que, 2015.
- Murray, Brian H. *Defending the Brand: Aggressive Strategies for Protecting Your Brand in the Online Arena*. AMACOM, 2004.
- Murray, Ryan Patrick. "Myspace-ing Is Not a Crime: Why Breaching Terms of Service Agreements Should Not Implicate the Computer Fraud and Abuse Act Written February 2, 2009." *Loyola of Los Angeles Entertainment Law Review*, vol. 29, no. 3, June 2009, p. 475.
- Musa, Sarhan M. *Network Security and Cryptography*. Mercury Learning and Information, 2018.
- Musciano, Chuck, and Bill Kennedy. *HTML and XHTML: The Definitive Guide*. 6th ed., O'Reilly, 2006.
- Myers, Glenford J., Tom Badgett, and Corey Sandler. *The Art of Software Testing*. 3rd ed., Wiley, 2012. Print.
- Nagy, Viktor. "The Geostrategic Struggle in Cyberspace between the United States, China, and Russia." *AARMS: Academic & Applied Research in Military Science*, vol. 11, no. 1, 2012, pp. 13-26.
- Nakashima, Ellen. "Dismantling of Saudi-CIA Web Site Illustrates Need for Clearer Cyberwar Policies." *Washington Post*, 19 Mar. 2010, www.washingtonpost.com/wp-dyn/content/article/2010/03/18/AR2010031805464%5Fpf.html.
- _____. "National Intelligence Director: Hackers Have Targeted 2016 Presidential Campaigns." *Washington Post*, 18 May 2016, www.washingtonpost.com/world/national-security/national-intelligence-director-hackers-have-tried-to-spy-on-2016-presidential-campaigns/2016/05/18/2b1745c0-1d0d-11e6-b6e0-c53b7ef63b45_story.html?tid=a_inl&utm_term=.135518fa2e97.
- Nakashima, Ellen, and David J. Lynch. "U.S. Charges Chinese Hackers in Alleged Theft of Vast Trove of Confidential Data in 12 Countries." *Washington Post*, 21 Dec. 2018, www.washingtonpost.com/world/national-security/us-and-more-than-a-dozen-allies-to-condemn-china-for-economic-espionage/2018/12/20/cdf0338-0455-11e9-b5df-5d3874f1ac36_story.html.
- Nakashima, Ellen, and Craig Timberg. "U.S. Investigators Point to China in Marriott Hack Affecting 500 Million Guests." *Washington Post*, 11 Dec. 2018, www.washingtonpost.com/technology/2018/12/12/us-investigators-point-china-marriott-hack-affecting-million-travelers.
- Nance, Malcolm. *The Plot to Hack America: How Putin's Cyberspies and WikiLeaks Tried to Steal the 2016 Election*. Skyhorse Publishing, 2016.
- Naraine, Ryan. "Metasploit's H. D. Moore Releases 'War Dialing' Tools." *ZDNet*, 6 Mar. 2009, www.zdnet.com/article/metasploits-hd-moore-releases-war-dialing-tools.
- _____. "Stuxnet Attackers Used 4 Windows Zero-Day Exploits." *ZDNet*, 14 Sept. 2010, www.zdnet.com/article/stuxnet-attackers-used-4-windows-zero-day-exploits.
- National Information Standards Organization. *Understanding Metadata*. NISO Press, 2004.
- National Institute for Standards and Technology. "Announcing the Advanced Encryption Standard (AES): Federal Information Processing Standards Publication

- 197." *NIST*, 2001, csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
- National Research Council, et al. *Computers at Risk: Safe Computing in the Information Age*. National Academy, 1991.
- Nejib, Perri, and Dawn Beyer. "Systems Security Engineering: Whose Job Is It Anyway?" *Insight*, vol. 19, no. 2, 2016, pp. 47-53, doi.org/10.1002/inst.12089.
- Nelson, D., and K. L. Vu. "Effectiveness of Image-Based Mnemonic Techniques for Enhancing the Memorability and Security of User-Generated Passwords." *Computer in Human Behavior*, 2010, 26, pp. 705-15.
- Nematollahi, Mohammad Ali, Chalee Vorakulpipat, and Hamurabi Gamboa Rosales. *Digital Watermarking: Techniques and Trends*. Springer Singapore, 2017.
- Netzley, Patricia D. *How Serious a Problem Is Computer Hacking?* ReferencePoint, 2014.
- "New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021." *Federal Trade Commission*, 22 Feb. 2022, www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0.
- "New FTC Data Show Consumers Reported Losing Nearly \$8.8 Billion to Scams in 2022." *Federal Trade Commission*, 23 Feb. 2023, www.ftc.gov/news-events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022.
- Newman, Jared. "With Android Lollipop, Mobile Multitasking Takes a Great Leap Forward." *Fast Company*, 6 Nov. 2014, www.fastcompany.com/3038213/with-android-lollipop-mobile-multitasking-takes-a-great-leap-forward.
- Nhan, Johnny. *Policing Cyberspace: A Structural and Cultural Analysis*. LFB, 2010.
- Niccolai, James. "As Encryption Debate Rages, Inventors of Public Key Encryption Win Prestigious Turing Award." *PCWorld*, 2 Mar. 2016, www.pcworld.com/article/3039911/encryption/as-encryption-debate-rages-inventors-of-public-key-encryption-win-prestigious-turing-award.html.
- Nickell, Joe. *Detecting Forgery: Forensic Investigation of Documents*. UP of Kentucky, 1996.
- Niederreiter, Harald, and Chaoping Xing. *Algebraic Geometry in Coding Theory and Cryptography*. Princeton UP, 2009.
- Nielsen, Jakob. *Multimedia and Hypertext: The Internet and Beyond*. SunSoft Press, 1995.
- Noergaard, Tammy. *Embedded Systems Architecture: A Comprehensive Guide for Engineers and Programmers*. 2nd ed., Elsevier, 2013.
- Norman, Jeremy M. "Ivan Sutherland Creates the First Graphical User Interface." *Historyofinformation.com*, historyofinformation.com/detail.php?id=805.
- Novell, Carly. "Anonymous Hacks Texas GOP Website, Floods It with Memes." *Daily Dot*, 13 Sept. 2021, www.dailydot.com/debug/anonymous-hacks-texas-gop-website-floods-it-with-memes.
- "Number of Available Applications in the Google Play Store from December 2009 to June 2023." *Statista*, June 2023, www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store.
- "Number of Internet of Things (IoT) Connected Devices Worldwide from 2019 to 2021, with Forecasts from 2022 to 2030." *Statista*, July 2022, www.statista.com/statistics/1183457/iot-connected-devices-worldwide.
- Nyholm, Sven, and Jilles Smids. "The Ethics of Accident-Algorithms for Self-Driving Cars: An Applied Trolley Problem?" *Ethical Theory & Moral Practice*, vol. 19, no. 5, 2016, pp. 1275-89.
- O'Leary, Mike. *Cyber Operations: Building, Defending, and Attacking Modern Computer Networks*. 2nd ed., Apress, 2019.
- O'Leary, Timothy, Linda O'Leary, and Daniel O'Leary. *Computing Essentials* 2023. McGraw-Hill, 2022.
- O'Marah, Kevin, and Pierfrancesco Manenti. "The Internet of Things Will Make Manufacturing Smarter." *Industry Week*, 14 Aug. 2015, www.industryweek.com/manufacturing-smarter.
- Obaidat, Mohammad S., Issa Traore, and Isaac Woungang, editors. *Biometric-Based Physical and Cybersecurity Systems*. Springer, 2019.
- Obama, Barack. "Taking the Cyberattack Threat Seriously." *Wall Street Journal*, 19 July 2012, online.wsj.com/news/articles/SB10000872396390444330904577535492693044650.
- Oettinger, William. *Learn Computer Forensics*. 2nd ed., Packt, 2022.
- Oki, Eiji, et al. *Advanced Internet Protocols, Services, and Applications*. Wiley, 2012.
- Okin, J. R. *The Internet Revolution: The Not-for-Dummies Guide to the History, Technology, and Use of the Internet*. Ironbound, 2005.
- Olivenbaum, Joseph M. "Ctrl-Alt-Delete: Rethinking Federal Computer Crime Legislation." *Seton Hall Law Review*, vol. 27, 1997, p. 574.
- Olson, Parmy. "Is Anonymous the Internet's Most Powerful Mirage?" *Forbes*, 30 May 2012, www.forbes.com/sites/parmyolson/2012/05/30/is-anonymous-the-internets-most-powerful-mirage/?sh=394245e86ba6.

- _____. *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*. Little, Brown and Company, 2012.
- “Online Safety Basics.” *National Cybersecurity Alliance*, 26 May 2022, staysafeonline.org/resources/online-safety-basics.
- “Operating System Market Share Worldwide-June 2023.” *Statcounter*, June 2023, gs.statcounter.com/os-market-share/desktop/worldwide/#monthly-202206-202306.
- Ordoñez, Franco. “In Wake of Pipeline Hack, Biden Signs Executive Order on Cybersecurity.” *NPR*, 12 May 2021, www.npr.org/2021/05/12/996355601/in-wake-of-pipeline-hack-biden-signs-executive-order-on-cybersecurity.
- Orr, Trystan. “A Brief History of Cyberwarfare.” *GRA Quantum*, 1 Nov. 2018, graquantum.com/a-brief-history-of-cyberwarfare.
- “Our History.” *US Cyber Command*, www.cybercom.mil/About/History.
- Paar, Christof, Jan Pelzl, and Tim Güneysu. *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer Cham, 2023.
- Padgett, John F., and Walter W. Powell. *The Emergence of Organizations and Markets*. Princeton UP, 2012.
- Panay, Panos. “Introducing Windows 11.” *Microsoft*, 24 June 2021, blogs.windows.com/windowsexperience/2021/06/24/introducing-windows-11.
- Parashar, R., and J. Sandeep. “Comparative Study of Iris Databases and UBRIS Database for Iris Recognition Methods for Noncooperative Environment.” *International Journal of Engineering, Research and Technology*, vol. 1, no. 5, 2012, pp. 1-6.
- “Parents: Cyber Bullying Led to Teen’s Suicide.” *ABC News*, 19 Nov. 2007, abcnews.go.com/GMA/story?id=3882520.
- Park, Jung-ran. *Metadata Best Practices and Guidelines*. Routledge, 2011.
- Parker, Matt. *Things to Make and Do in the Fourth Dimension: A Mathematician’s Journey through Narcissistic Numbers, Optimal Dating Algorithms, at Least Two Kinds of Infinity, and More*. Farrar, 2014.
- Patel, Ruchika, and Parth Bhatt. “A Review Paper on Digital Watermarking and Its Techniques.” *International Journal of Computer Applications*, vol. 110, no. 1, 2015, pp. 10-13.
- Patt, Yale, and Sanjay Patel. *Introduction to Computing Systems: From Bits & Gates to C/C++ & Beyond*. 3rd ed., McGraw-Hill, 2019.
- Patterson, Dan. “Dark Web: A Cheat Sheet for Business Professionals.” *TechRepublic*, 26 Oct. 2018, www.techrepublic.com/article/dark-web-the-smart-persons-guide.
- Patterson, David A., and John L. Hennessy. *Computer Organization and Design: The Hardware/Software Interface*. 6th ed., Morgan Kaufmann, 2020.
- Patterson, Kelsey T. “Narrowing It Down to One Narrow View: Clarifying and Limiting the Computer Fraud and Abuse Act.” *Charleston Law Review*, vol. 7, no. 3, Mar. 2013, p. 489.
- Payton, Theresa, and Theodore Claypoole. *Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family*. Rowman & Littlefield, 2014.
- Peek, Jerry D., Grace Todino, and John Strang. *Learning the UNIX Operating System*. 5th ed., ProQuest, 2002.
- Pentland, Alex. “Saving Big Data from Itself.” *Scientific American*, vol. 311, no. 2, 2014, pp. 65-67.
- Peralta, D., I. TrigueroI, R. Sanchez-Reillo, F. Herrera, and J. Benitez. “Fast Fingerprint Identification for Large Databases.” *Pattern Recognition*, vol. 47, no. 2, 2014, pp. 588-602.
- Pérez-González, F., and H. Yun. “Risk Management and Firm Value: Evidence from Weather Derivatives.” *Journal of Finance*, vol. 68, no. 5, 2013, pp. 2143-76.
- Peterson, Larry L., and Bruce S. Davie. *Computer Networks: A Systems Approach*. 6th ed., Morgan Kaufmann, 2021.
- Peterson, T. F., and Institute Historian. *Nightwork: A History of Hacks and Pranks at MIT*. Updated ed., MIT Press, 2011.
- Petkauskas, Vilius. “Report: Number of Expert-Crafted Video Deepfakes Double Every Six Months.” *Cybernews*, 28 Sept. 2021, cybernews.com/privacy/report-number-of-expert-crafted-video-deepfakes-double-every-six-months.
- Petrosyan, Ani. “Annual Cost of Cybercrime Worldwide 2017-2028.” *Statista*, 15 Sept. 2023, www.statista.com/forecasts/1280009/cost-cybercrime-worldwide.
- _____. “Malware-Statistics.” *Statista*, 31 Aug. 2023, www.statista.com/topics/8338/malware/#topicOverview.
- _____. “Spam: Share of Global Email Traffic 2011-2022.” *Statista*, Feb. 2023, www.statista.com/statistics/420400/spam-email-traffic-share-annual.
- Petzold, Charles. *Code: The Hidden Language of Computer Hardware and Software*. 2nd ed., Microsoft Press, 2022.
- “PH.D. Chemist Sentenced to 168 Months for Conspiracy to Steal Traded Secrets, Economic Espionage, Theft of Trade Secrets, and Wire Fraud.” *US Attorney’s Office Eastern District of Tennessee*, 9 May 2022, www.justice.gov/usao-edtn/pr/phd-chemist-sentenced-168-months-conspiracy-steal-traded-secrets-economic-espionage.

- "Phishing." *Computer Hope*, 1 Oct. 2023, www.computerhope.com/jargon/p/phishing.htm.
- "PII Belonging to Indian Citizens, Including Their Aadhaar IDs, Offered for Sale on the Dark Web." *Resecurity*, 15 Oct. 2023, www.resecurity.com/blog/article/pii-belonging-to-indian-citizens-including-their-aadhaar-ids-offered-for-sale-on-the-dark-web.
- Piore, Adam. "The Quest to Build a Silicon Brain." *Discover*, 24 May 2013, www.discovermagazine.com/mind/the-quest-to-build-a-silicon-brain.
- Piper, Steve. "Four Critical Risks to Watch as Experts Predict a Cyber Cold War." *Forbes*, 23 May 2022, www.forbes.com/sites/forbestechcouncil/2022/05/23/four-critical-risks-to-watch-as-experts-predict-a-cyber-cold-war.
- Pitrelli, Monica. "Anonymous Declared a 'Cyber War' against Russia: Here Are the Results." *CNBC*, 16 Mar. 2022, www.cnbc.com/2022/03/16/what-has-anonymous-done-to-russia-here-are-the-results-.html.
- Platz, Cheryl. *Design Beyond Devices: Creating Multimodal, Cross-Device Experiences*. Rosenfeld Media, 2020.
- Plotkin, David. *Data Stewardship: An Actionable Guide to Effective Data Management and Data Governance*. 2nd ed., Academic Press, 2020.
- Plumb, Charles. "Drones in the Workplace." *McAfee and Taft*, 14 Dec. 2015, www.mcafeetaft.com/drones-in-the-workplace.
- Polanin, Joshua R., et al. "A Meta-Analysis of School-Based Bullying Prevention Programs' Effects on Bystander Intervention Behavior." *School Psychology Review*, vol. 41, no. 1, 2012, pp. 47-65.
- Pollitt, Mark. "A History of Digital Forensics." *Advances in Digital Forensics VI*, edited by Kam-Pui Chow and Sujeet Shenoi, Springer, 2010, pp. 3-15.
- Polyakova, Alina. "Weapons of the Weak: Russia and AI-Driven Asymmetric Warfare." *Brookings Institution*, 15 Nov. 2018, www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare.
- Pomerleau, Pierre-Luc, and David L. Lowery. *Countering Cyber Threats to Financial Institutions*. Palgrave Macmillan, 2020.
- Porolli, Matías. "Cybercrime Black Markets: Dark Web Services and Their Prices." *Welivesecurity by eset*, 31 Jan. 2019, welivesecurity.com/2019/01/31/cybercrime-black-markets-dark-web-services-and-prices.
- Porter, Jon. "Apple Announces macOS Sonoma with Game Mode and Support for Desktop Widgets." *The Verge*, 5 June 2023, www.theverge.com/2023/6/5/23745460/apple-macos-14-sonoma-features-updates-wwdc-2023.
- Porup, J. M. "How and Why Deepfake Videos Work-And What Is at Risk." *CSO*, 10 Apr. 2019, www.csoonline.com/article/3293002/deepfake-videos-how-and-why-they-work.html.
- Poulsen, Kevin. *Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground*. Broadway Paperbacks, 2011.
- Prentice, Chris, Jonathan Stempel, and Raphael Satter. "US SEC Sues SolarWinds for Concealing Cyber Risks before Massive Hacking." *Reuters*, 30 Oct. 2023, www.reuters.com/legal/us-sues-solarwinds-court-records-2023-10-30.
- "Principles for Useable Design." *Usability Body of Knowledge*, www.usabilitybok.org/principles-for-useable-design.
- "Public Key Cryptography." *IBM*, 8 Mar. 2021, www.ibm.com/docs/en/ztpf/1.1.0.15?topic=concepts-public-key-cryptography.
- "Public Key Cryptography." *PCMag*, www.pc当地/encyclopedia/term/40522/cryptography.
- Purdy, Chase. "Did Facebook Violate Its FTC Agreement? Here's What Investigators Will Ask." *Quartz*, 21 Mar. 2018, qz.com/1233597/did-facebook-violate-its-ftc-agreement-heres-what-investigators-will-ask.
- "QA and Cybersecurity." *QANTUM*, 21 Jan. 2020, quantum.medium.com/qa-and-cybersecurity-fa1968cd728c.
- Quesenberry, Whitney. "What Does Usability Mean: Looking Beyond Ease of Use." *WQusability*, www.wqusability.com/articles/more-than-ease-of-use.html.
- "Quick Facts about the Digital Watermarking Alliance." *Digital Watermarking Alliance*, digitalwatermarkingalliance.org/about/quick-facts.
- Quinn, Brendan. *Data Protection Implementation Guide: A Legal, Risk and Technology Framework for the GDPR*. Wolters Kluwer, 2021.
- Raghunath, Satish. "Resource Management for Virtual Private Networks." *IEEE Communications Magazine*, vol. 45, no. 4, 2007, pp. 38-44.
- Rainie, Lee, Janna Anderson, and Jonathan Albright. "The Future of Free Speech, Trolls, Anonymity and Fake News Online." *Pew Research Center*, 29 Mar. 2017, www.pewresearch.org/internet/2017/03/29/the-future-of-free-speech-trolls-anonymity-and-fake-news-online.
- Ramos, Emmanuel. "Web Browsers: Examining the Latest Threats, Solutions and Trends." *Forbes*, 14 Aug. 2023, www.forbes.com/sites/forbestechcouncil/2023/08/14/web-browsers-examining-the-latest-threats-solutions-and-trends/?sh=c9be852187b8.

- Ramsey, Mike. "Tesla CEO Musk Sees Fully Autonomous Car Ready in Five or Six Years." *Wall Street Journal*, 17 Sept. 2014, www.wsj.com/articles/tesla-ceo-sees-fully-autonomous-car-ready-in-five-or-six-years-1410990887.
- "Ransomware and Businesses 2016." *Symantec Corporation*, 2016, conferences.law.stanford.edu/cyberday/wp-content/uploads/sites/10/2016/10/5c_ISTR2016_Ransomware_and_Businesses.pdf.
- Raphael, J. R. "Android Versions: A Living History from 1.0 to 14." *Computerworld*, 7 Apr. 2023, www.computerworld.com/article/3235946/android-versions-a-living-history-from-1-0-to-today.html.
- Raska, Michael, Katarzyna Zysk, and Ian Bowers, editors. *The Fourth Industrial Revolution: Security Challenges, Emerging Technologies, and Military Implications*. Routledge, 2022.
- Raul, Alan Charles, et al. "The Privacy, Data Protection and Cybersecurity Law Review." *Sidley*, Nov. 2022, www.sidley.com/en/insights/publications/2022/11/the-privacy-data-protection-and-cybersecurity-law-review.
- Rawal, Bharat S., Gunasekaran Manogaran, and Alexander Peter. *Cybersecurity and Identity Access Management*. Springer, 2023.
- Recommendations for Database Management System Standards: NBS Special Publication 500-51*. US Department of Commerce National Bureau of Standards, 1979, www.govinfo.gov/content/pkg/GOV PUB-C13-d091da4af6988e05e8ebba2ee5df278d/pdf/GOV PUB-C13-d091da4af6988e05e8ebba2ee5df278d.pdf.
- Reduction in Distribution of Spam Act of 2003: Hearing before the Subcommittee on Crime, Terrorism, and Homeland Security of the Committee on the Judiciary, House of Representatives, One Hundred Eighth Congress, First Session, on H.R. 2214, July 8, 2003*. US Government Printing Office, 2003.
- Reimer, Jeremy. "A History of the GUI." *Ars Technica*, 5 May 2005, arstechnica.com/features/2005/05/gui.
- "Research and Analysis: Online Copyright Infringement Tracker Survey (10th Wave) Executive Summary." *Intellectual Property Office*, gov.uk/government/publications/online-copyright-infringement-tracker-survey-10th-wave/online-copyright-infringement-tracker-survey-10th-wave-executive-summary.
- Retzkin, Sion. *Hands-On Dark Web Analysis: Learn What Goes on in the Dark Web, and How to Work with It*. Packt, 2018.
- Riley, Gail Blasser. *Internet Piracy*. Cavendish, 2010.
- Roberts, Dan, and Spencer Ackerman. "NSA Mass Phone Surveillance Revealed by Edward Snowden Ruled Illegal." *The Guardian*, 7 May 2015, www.theguardian.com/us-news/2015/may/07/nsa-phone-records-program-illegal-court.
- Roberts, Mary Rose. "An Invisible Enemy." *Urgent Communications*, vol. 30, no. 3, 2012, pp. 18-21.
- Rocchi, Walter. *Cybersecurity and Privacy Law Handbook*. Packt, 2022.
- Rogers, David L. *The Network Is Your Customer: Five Strategies to Thrive in a Digital Age*. Yale UP, 2011.
- Romm, Tony, and Elizabeth E. Dwoskin. "U.S. Regulators Have Met to Discuss Imposing a Record-Setting Fine against Facebook for Privacy Violations." *Washington Post*, 18 Jan. 2019, www.washingtonpost.com/technology/2019/01/18/us-regulators-have-met-discuss-imposing-record-setting-fine-against-facebook-some-its-privacy-violations.
- Roose, Kevin. "Can 'the Merge' Save Crypto?" *New York Times*, 15 Sept. 2022, www.nytimes.com/2022/09/15/technology/merge-ethereum-crypto.html.
- Rose, J. "Promising Career Opportunities in Risk Management and Insurance." *Baylor Business Review*, vol. 18, pp. 10-11.
- Rosen, David J. "Limiting Employee Liability under the CFAA: A Code-Based Approach to 'Exceeds Authorized Access.'" *Berkeley Technology Law Journal*, vol. 27, 2012, p. 737.
- Rosenbaum, Ron. "Richard Clarke on Who Was Behind the Stuxnet Attack." *Smithsonian Magazine*, Apr. 2012, www.smithsonianmag.com/history/richard-clarke-on-who-was-behind-the-stuxnet-attack-160630516.
- Rosenberg, Eric, and James Uttaro. "Scaling Virtual Private Networks." *Recent Patents on Engineering*, vol. 1, no. 3, 2007, pp. 206-13.
- Rosenberg, Matthew, Nicolas Confessore, and Carole Cadwalladr. "How Trump Consultants Exploited the Facebook Data of Millions." *New York Times*, 17 Mar. 2018, www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.
- Rosenblatt, Kalhan. "ChatGPT Banned from New York City Public Schools' Devices and Networks." *NBC News*, 5 Jan. 2023, www.nbcnews.com/tech/tech-news/new-york-city-public-schools-ban-chatgpt-devices-networks-rcna64446.
- Rosencrance, Linda. "Software." *Tech Target*, Mar. 2021, www.techtarget.com/searchapparchitecture/definition/software.
- Ross, Ron, Michael McEvilley, and Janet Carrier Oren. *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*. National Institute of Standards and Technology, 2017.

- Ross, Ron, Mark Winstead, and Michael McEvilley. *Engineering Trustworthy Secure Systems*, Nov. 2022, nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.8-00-160v1r1.pdf.
- Ross, Timothy J. *Fuzzy Logic with Engineering Applications*. 4th ed., Wiley, 2016.
- Rountree, Derrick, and Ileana Castrillo. *The Basics of Cloud Computing*. Elsevier, 2014.
- Rouse, Margaret. "Advanced Encryption Standard." *Techopedia*, 26 June 2023, www.techopedia.com/definition/1763/advanced-encryption-standard-aes. ______. "Mobile Web." *Techopedia*, 4 Apr. 2017, www.techopedia.com/definition/23588/mobile-web.
- Rubin, Aaron. "How Website Operators Use CFAA to Combat Data-Scraping." *Law360*, 25 Aug. 2014, www.law360.com/articles/569325.
- "Rules and Policies-Protecting PII-Privacy Act." *General Services Administration*, 11 Aug. 2023, www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act.
- Rumelhart, David E., James L. McClelland, and the PDP Research Group. *Parallel Distributed Processing: Explorations in the Microstructure of Cognition*. 1986. MIT Press, 1989. 2 vols.
- Russell, Stuart, and Peter Norvig. *Artificial Intelligence: A Modern Approach*. 4th ed. Pearson, 2020.
- Ryan, Janel. "Five Basic Things You Should Know about Cloud Computing." *Forbes*, 30 Oct. 2013, www.forbes.com/sites/sungardas/2013/10/30/five-basic-things-you-should-know-about-cloud-computing/?sh=78e67d3560fa.
- Rychagov, Michael N., Ekaterina V. Tolstaya, and Mikhail Y. Sirotenko, editors. *Smart Algorithms for Multimedia and Imaging*. Springer Cham, 2021.
- Sammons, John. *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics*. 2nd ed., Syngress, 2014.
- Sanders, James, and Conner Forrest. "Hybrid Cloud: What It Is, Why It Matters." *ZDNet*, 1 July 2014, www.zdnet.com/article/hybrid-cloud-what-it-is-why-it-matters.
- Sanger, David E., et al. "Cyberattack Forces a Shutdown of a Top U.S. Pipeline." *New York Times*, 13 May 2021, www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html.
- Sarkar, Jayanta. *Computer Aided Design: A Conceptual Approach*. CRC Press, 2017.
- Sauro, Jeff. "A Brief History of Usability." *Measuring U*, 11 Feb. 2013, measuringu.com/usability-history.
- Savas, Onur, and Julia Deng, editors. *Big Data Analytics in Cybersecurity*. Routledge, 2017.
- Sayegh, Emil. "Potential for Devastation: The Impact of a Cyberattack on the Banking System." *Forbes*, 6 June 2023, www.forbes.com/sites/emilsayegh/2023/06/06/potential-for-devastation-the-impact-of-a-cyberattack-on-the-banking-system/?sh=52bb1a1f1b45.
- Schapire, Robert E., and Yoav Freund. *Boosting: Foundations and Algorithms*. MIT Press, 2012.
- Schell, Bernadette H., and Clemens Martin. *Cybercrime: A Reference Handbook*. ABC-CLIO, 2004.
- Schieck, Glenn R. "Undercutting Employee Mobility: The Computer Fraud and Abuse Act in the Trade Secret Context." *Brooklyn Law Review*, vol. 79, no. 2, 2014, p. 831.
- Schmidt, Eric, and Jared Cohen. *The New Digital Age: Reshaping the Future of People, Nations, and Business*. Knopf, 2013.
- Schneider, Shari Kessel, et al. "Cyberbullying, School Bullying, and Psychological Distress: A Regional Census of High School Students." *American Journal of Public Health*, vol. 102, no. 1, 2012, p. 171.
- Schneier, B. "Choosing Secure Passwords." *Schneier on Security*, 3 Mar. 2014, www.schneier.com/blog/archives/2014/03/choosing_secure_1.html.
- Schou, Corey, and Steven Hernandez. *Information Assurance Handbook: Effective Computer Security and Risk Management Strategies*. McGraw, 2015.
- Schwabach, Aaron. *Internet and the Law: Technology, Society, and Compromises*. ABC-CLIO, 2006.
- Sciore, Edward. *Database Design and Implementation*. 2nd ed., Springer, 2020.
- Scott, A. O. "The World Where You Aren't What You Post." *New York Times*, 16 Sept. 2010, www.nytimes.com/2010/09/17/movies/17catfish.html.
- Scott, Gordon. "Fuzzy Logic: Definition, Meaning, Examples, and History." *Investopedia*, 4 Apr. 2023, www.investopedia.com/terms/f/fuzzy-logic.asp.
- Scott, Michael L. *Programming Language Pragmatics*. 4th ed., Morgan Kaufmann, 2016.
- Scroxton, Alex. "Data Breaches Are a Ticking Timebomb for Consumers." *Computer Weekly*, 9 Feb. 2021, www.computerweekly.com/news/252496079/Data-breaches-are-a-ticking-timebomb-for-consumers.
- "Securing the Cyber Advantage: U.S. Cyber Command Celebrates Its 11th Year." *US Cyber Command*, 21 May 2021, www.cybercom.mil/Media/News/Article/2626906/securing-the-cyber-advantage-us-cyber-command-celebrates-its-11th-year.

- “Security Software-Statistics & Facts.” *Statista*, 7 July 2023, www.statista.com/topics/2208/security-software.
- Segal, Adam. “Chinese Computer Games.” *Foreign Affairs*, vol. 91, no. 2, 2012, pp. 14-20.
- Segal, Edward. “How and Why Businesses Are Vulnerable to Email-Based Cyberattacks: New Study.” *Forbes*, 10 Nov. 2022, www.forbes.com/sites/edwardsegal/2022/11/10/how-and-why-businesses-are-vulnerable-to-email-based-cyberattacks-new-study/?sh=2f370f692ae0.
- _____. “Worsening Computer Chip Crisis Shows Supply Chains Are Still at Risk.” *Forbes*, 12 July 2021, www.forbes.com/sites/edwardsegal/2021/07/12/worsening-computer-chip-crisis-shows-supply-chains-are-still-at-risk.
- Sellers, Audrey. “Top Programming Languages of 2023.” *Coding Dojo*, 3 Feb. 2023, www.codingdojo.com/blog/top-programming-languages.
- Sethi, Aman. “UIDAI Aadhaar Hack: New Analysis Shows Hackers Changed Enrolment Software Code in 26 Places.” *HuffPost India*, 14 Sept. 2018, www.huffpost.com/archive/in/entry/uidai-aadhaar-hack-new-analysis-shows-hackers-changed-enrolment-software-code-in-26-places_in_5c10764fe4b0a9576b528527.
- Shah, H., K. Warwick, J. Vallverdú, and D. Wu. “Can Machines Talk? Comparison of Eliza with Modern Dialogue Systems.” *Computers in Human Behavior*, vol. 58, 2016, pp. 278-95.
- Shakarian, Paulo, Jana Shakarian, and Andrew Ruef. *Introduction to Cyber-Warfare: A Multidisciplinary Approach*. Syngress, 2013.
- Shannon, M. L. *Don’t Bug Me: The Latest High-Tech Spy Methods*. Paladin Press, 1992.
- Shao, Grace. “What ‘Deepfakes’ Are and How They May Be Dangerous.” *CNBC*, 13 Oct. 2019, www.cnbc.com/2019/10/14/what-is-deepfake-and-how-it-might-be-dangerous.html.
- Sharman, R. “Enterprise Risk Management-The KPMG Approach.” *British Journal of Behavioral Management*, vol. 31, 2002, pp. 26-29.
- Shear, Michael D. “How the White House Explains Waiting 18 Days to Fire Michael Flynn.” *New York Times*, 9 May 2017, www.nytimes.com/2017/05/09/us/politics/michael-flynn-russia.html?_r=0.
- Sherif, Mostafa Hashem. *Protocols for Secure Electronic Commerce*. 3rd ed., CRC Press, 2018.
- Shinder, Debra Littlejohn. *Scene of the Cybercrime: Computer Forensics Handbook*. Syngress, 2002.
- Shoenerger, Allen. “Privacy Wars.” *Indiana International & Comparative Law Review*, vol. 17, 2007, pp. 355-93.
- Siddiqi, Muzaffer A. *Dynamic RAM: Technology Advancements*. CRC Press, 2013.
- Siegel, Lee. “The Kids Aren’t Alright.” *Newsweek*, 15 Oct. 2012, pp. 18-20.
- Silberschatz, Abraham, Peter Baer Galvin, and Greg Gagne. *Operating System Concepts*. 10th ed., Wiley, 2021.
- Simmons, Gustavus J. “AES.” *Encyclopaedia Britannica*, 30 Apr. 2023, www.britannica.com/topic/AES/additional-info#history.
- Simonite, Tom. “Prepare for the Deepfake Era of Web Video.” *Wired*, 6 Oct. 2019, www.wired.com/story/prepare-deepfake-era-web-video.
- Simos, Dimitris E., et al. “Combinatorial Methods in Security Testing.” *Computer*, vol. 49, 2016, pp. 80-83.
- Singel, Ryan. “Google Busted with Hand in Safari-Browser Cookie Jar.” *Wired*, 17 Feb. 2012, www.wired.com/2012/02/google-safari-browser-cookie.
- Singer, Graham. “The History of the Microprocessor and the Personal Computer.” *TechSpot*, 1 Oct. 2020, www.techspot.com/article/874-history-of-the-personal-computer.
- Singer, P. W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford UP, 2014.
- Singletary, Michelle. “Yahoo. Target. Equifax. Sonic: All Category 5 Data Breaches. Is Your Information Safe Anymore?” *Washington Post*, 5 Oct. 2017, www.washingtonpost.com/news/get-there/wp/2017/10/05/yahoo-target-equifax-sonic-all-category-5-data-breaches-is-your-information-safe-anymore/?utm_term=.1ef401a8f845.
- “SK Hynix Launches World’s First DDR5 DRAM.” *HPC Wire*, 7 Oct. 2020, www.hpcwire.com/off-the-wire/sk-hynix-launches-worlds-first-ddr5-dram.
- Smiraglia, Richard P., editor. *Metadata: A Cataloger’s Primer*. Routledge, 2012.
- Smith, Aaron. “U.S. Views of Technology and the Future.” *Pew Research*, 17 Apr. 2014, www.pewresearch.org/internet/2014/04/17/us-views-of-technology-and-the-future.
- Smith, Aaron, and Maeve Duggan. “Online Dating & Relationships.” *Pew Research*, 21 Oct. 2013, www.pewresearch.org/internet/2013/10/21/online-dating-relationships.
- Smith, Eric N. *Workplace Security Essentials: A Guide for Helping Organizations Create Safe Work Environments*. Butterworth-Heinemann, 2014.
- Smith, Jeremy N. *Breaking and Entering: The Extraordinary Story of a Hacker Called “Alien.”* Eamon Dolan/Houghton Mifflin Harcourt, 2019.

- Smith, Marcia S. "Junk E-mail": An Overview of Issues and Legislation concerning Unsolicited Commercial Electronic Mail ("Spam"). Congressional Research Service, Library of Congress, 2001.
- Smith, Matthew S. "Wi-Fi vs. Ethernet: Has Wireless Killed Wired?" *Digital Trends*, 18 Jan. 2013, www.digitaltrends.com/computing/wi-fi-vs-ethernet-has-wireless-killed-wired/.
- Smith, Michael D., and Rahul Telang. *Streaming, Sharing, Stealing: Big Data and the Future of Entertainment*. Reprint ed., MIT Press, 2017.
- Smith, Mike. *Targeted: How Technology Is Revolutionizing Advertising and the Way Companies Reach Consumers*. Amacom Publishing, 2014.
- Smith, Monica. "Computer Engineers Crucial to Network Security." *FIU News*, 9 Aug. 2022, news.fiu.edu/2022/computer-engineers-crucial-to-network-security.
- Snickars, Pelle, and Patrick Vonderau. *Moving Data: The iPhone and the Future of Media*. Columbia UP, 2012.
- "So You've Been Doxed: A Guide to Best Practices." *Crash Override Network*, crashoverriddenetwork.com, crashoverriddenetwork.com/soyouvebeendoxed.html.
- Sobers, Rob. "Ransomware Statistics, Data, Trends, and Facts." *Varonis*, 6 Sept. 2023, www.varonis.com/blog/ransomware-statistics.
- "Social Engineering." *Carnegie Mellon University Information Security Office*, www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html.
- "Sony Cyber-Attack: North Korea Faces New US Sanctions." *BBC News*, 3 Jan. 2015, www.bbc.com/news/world-us-canada-30661973.
- Spence, Ewan. "New Android Malware Strikes at Millions of Smartphones." *Forbes*, 4 Feb. 2015, www.forbes.com/sites/ewanspence/2015/02/04/android-malware-apps-deleted/?sh=f8676a1d88b4.
- Spice, B. "Press Release: Carnegie Mellon Scheme Uses Shared Visual Cues to Help People Remember Multiple Passwords." *Carnegie Mellon University*, 4 Dec. 2013, www.cmu.edu/news/stories/archives/2013/december/dec4_passwordscheme.html.
- "Spyware." *Secure Purdue*, www.purdue.edu/securepurdue/forms-and-resources/spyware.php.
- Stallings, William. *Data and Computer Communications*. 10th ed., Prentice Hall, 2014.
- Stallings, William, and Lawrie Brown. *Computer Security: Principles and Practice*. 4th ed. Pearson, 2018.
- Stanglin, D., and W. M. Welch. "Two Girls Arrested on Bullying Charges after Suicide." *USA Today*, 16 Oct. 2013, www.usatoday.com/story/news/nation/2013/10/15/florida-bullying-arrest-lakeland-suicide/2986079.
- Steiner, Christopher. *Automate This: How Algorithms Came to Rule Our World*. Penguin, 2012.
- Steinhauer, Jennifer, and Jonathan Weisman. "U.S. Surveillance in Place since 9/11 Is Sharply Limited." *New York Times*, 2 June 2015, www.nytimes.com/2015/06/03/us/politics/senate-surveillance-bill-passes-hurdle-but-showdown-looms.html.
- Stenquist, Paul. "In Self-Driving Cars, a Potential Lifeline for the Disabled." *New York Times*, 7 Nov. 2014, www.nytimes.com/2014/11/09/automobiles/in-self-driving-cars-a-potential-lifeline-for-the-disabled.html.
- Stephens, G. "Crime in Cyberspace." *Futurist*, vol. 29, 1995, pp. 24-31.
- _____. "Cybercrime in the Year 2025." *Futurist*, vol. 42, 2008, pp. 32-36.
- Sterling, Bruce. "Stop Saying 'Smart Cities.'" *The Atlantic*, 12 Feb. 2018, www.theatlantic.com/technology/archive/2018/02/stupid-cities/553052.
- Stewart, Andrew J. *A Vulnerable System: The History of Information Security in the Computer Age*. Cornell UP, 2021.
- Stobing, Chris. "Ransomware Is the New Hot Threat Everyone Is Talking About; What Do You Need to Know?" *Digital Trends*, 6 June 2015, www.digitaltrends.com/computing/what-is-ransomware-and-should-you-be-worried-about-it.
- Stockson, Eric. *Brave Browser: Blockchain Internet Browsing Made Easy*. First Rank, 2019.
- STOMP Out Bullying*, 2023, www.stompoutbullying.org.
- Stonebraker, Michael. "The Elephant's Dilemma: What Does the Future of Databases Really Look Like?" Interview with Colin Barker. *ZDNet.com*, 17 Apr. 2015, www.zdnet.com/article/the-elephants-dilemma-what-does-the-future-of-databases-really-look-like.
- STOP. THINK. CONNECT*, 2023, www.stopthinkconnect.org.
- "Storage vs. Memory." *PCMag*, www.pcmag.com/encyclopedia/term/storage-vs-memory.
- Stouffer, Clare. "Internet Tracking: How and Why We're Followed Online." *Norton*, 28 June 2021, us.norton.com/blog/privacy/internet-tracking.
- Strahilevitz, Lior Jacob. "Toward a Positive Theory of Privacy Law." *Harvard Law Review*, vol. 126, no. 7, 2013, pp. 2010-42.
- Strazewski, L. "Awareness of Risk Sparks Renewed Interest in ERM." *Rough Notes*, vol. 145, 2002, pp. 111-14.
- Stricklin, Kasey. "Social Media Bots: Laws, Regulations, and Platform Policies." *CNA*, Sept. 2020, www.cna.org/reports/2020/10/DIM-2020-U-028193-Final.pdf.

- Stytz, Martin R. "Cyber-warfare Distributed Training." *Military Technology*, vol. 30, no. 11, 2006, pp. 95-99.
- Su, Qingtang. *Color Image Watermarking*. Tsinghua UP/Walter de Gruyter, 2017.
- Sukhdev, Ashima, and James Pennington. "4 Ways Smart Cities Will Make Our Lives Better." *World Economic Forum*, 10 Feb. 2016, www.weforum.org/agenda/2016/02/4-ways-smart-cities-will-make-our-lives-better.
- Sun, Jiming, Vincent Zimmer, Marc Jones, and Stefan Reinauer. *Embedded Firmware Solutions: Development Best Practices for the Internet of Things*. ApressOpen, 2015.
- "Survey: 64% Find Targeted Ads Invasive." *Advanced Television*, 20 Oct. 2021, advanced-television.com/2021/10/20/survey-64-find-targeted-ads-invasive.
- Swaine, Jon. "Twitter Admits Far More Russian Bots Posted on Election Than It Had Disclosed." *The Guardian*, 19 Jan. 2018, www.theguardian.com/technology/2018/jan/19/twitter-admits-far-more-russian-bots-posted-on-election-than-it-had-disclosed.
- Sytas, Andrius. "Estonia Says It Repelled Major Cyber Attack after Removing Soviet Monuments." *Reuters*, 18 Aug. 2022, www.reuters.com/world/europe/estonia-says-it-repelled-major-cyber-attack-after-removing-soviet-monuments-2022-08-18.
- Tabak, Filiz, and William Smith. "Privacy and Electronic Monitoring in the Workplace: A Model of Managerial Cognition and Relational Trust Development." *Employee Responsibilities and Rights Journal*, vol. 17, no. 3, 2005, pp. 173-89.
- Tafoya, William L. "Cyber Terror." *FBI Law Enforcement Bulletin*, 1 Nov. 2011, leb.fbi.gov/articles/featured-articles/cyber-terror.
- Tanenbaum, Andrew S., and Herbert Bos. *Modern Operating Systems*. 4th ed., Prentice, 2014.
- "Taxpayers See Wave of Summer Email, Text Scams; IRS Urges Extra Caution with Flood of Schemes Involving Economic Impact Payments, Employee Retention Credits, Tax Refunds." *IRS*, 21 July 2023, www.irs.gov/newsroom/taxpayers-see-wave-of-summer-email-text-scams-irs-urges-extra-caution-with-flood-of-schemes-involving-economic-impact-payments-employee-retention-credits-tax-refunds.
- "Tech Support Scams." *Federal Trade Commission*, Sept. 2022, www.consumer.ftc.gov/articles/0346-tech-support-scams.
- Templeton, Brad. "Self-Driving Cars 2021: Year in Review." *Forbes*, 3 Jan. 2022, www.forbes.com/sites/bradtempleton/2022/01/03/self-driving-cars-2021-year-in-review/?sh=4aa85563773b.
- Thompson, Nicholas, and Ian Bremmer. "The AI Cold War That Threatens Us All." *Wired*, 23 Oct. 2018, www.wired.com/story/ai-cold-war-china-could-doom-us-all.
- Tidwell, Jenifer, Charles Brewer, and Aynne Valencia. *Designing Interfaces: Patterns for Effective Interaction Design*. 3rd ed., O'Reilly Media, 2020.
- Tidy, Joe. "YouTube Accused of Not Tackling Musk Bitcoin Scam Streams." *BBC News*, 10 June 2022, www.bbc.com/news/technology-61749120.
- "Timeline of Computer History." *Computer History Museum*, www.computerhistory.org/timeline/computers.
- Tong, Goh Chiew. "Employee Surveillance Is on the Rise-and That Could Backfire on Employers." *CNBC Make It*, 25 Apr. 2023, www.cnbc.com/2023/04/24/employee-surveillance-is-on-the-rise-that-could-backfire-on-employers.html.
- Torr, James D. *Internet Piracy*. Greenhaven, 2004.
- Toulas, Bill. "Android Phones Are Vulnerable to Fingerprint Brute-Force Attacks." *BleepingComputer*, 21 May 2023, www.bleepingcomputer.com/news/security/android-phones-are-vulnerable-to-fingerprint-brute-force-attacks.
- Townsend, Kevin. "The History and Evolution of Zero Trust." *SecurityWeek*, 11 July 2022, www.securityweek.com/history-and-evolution-zero-trust.
- Trepte, Sabine, and Leonard Reinecke. *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*. Springer-Verlag, 2011.
- Tucker, Alan. *Applied Combinatorics*. Wiley, 2012.
- Tucker, Patrick. "AI Is Already Learning from Russia's War in Ukraine, DOD Says." *Defense One*, 21 Apr. 2022, www.defenseone.com/technology/2022/04/ai-already-learning-russias-war-ukraine-dod-says/365978.
- Tufano, P. "Agency Costs of Corporate Risk Management." *FM: The Journal of the Financial Management Association*, vol. 27, 1998, pp. 67-77.
- Turban, Efraim, Carol Pollard, and Gregory Wood. *Information Technology for Management: On-Demand Strategies for Performance, Growth and Sustainability*. 11th ed., John Wiley & Sons, 2018.
- Types of Wireless Networks." *Commotion Wireless*, commotionwireless.net/docs/cck/networking/types-of-wireless-networks.
- Uenuma, Francine. "20 Years Later, the Y2K Bug Seems Like a Joke-Because Those Behind the Scenes Took It Seriously." *Time*, 30 Dec. 2019, time.com/5752129/y2k-bug-history.

- Umar, Amjad. "IT Infrastructure to Enable Next Generation Enterprises." *Information Systems Frontiers*, vol. 7, no. 3, 2005, pp. 217-56.
- "Urban Development." *World Bank*, 3 Apr. 2023, www.worldbank.org/en/topic/urbandevelopment/overview.
- "U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage." *US Department of Justice*, 19 May 2014, www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.
- US Department of Justice. Criminal Division. *Federal Guidelines for Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*. US Government Printing Office, 2002.
- "Usability." *Technopedia*, 8 Sept. 2011, www.techopedia.com/definition/4919/usability.
- "Usability Evaluation Basics." *Usability.gov*, www.usability.gov/what-and-why/usability-evaluation.html.
- "User Interface Design Basics." *Usability.gov*, www.usability.gov/what-and-why/user-interface-design.html.
- "Using HTTP Cookies." *MDN Web Docs*, 10 Apr. 2023, developer.mozilla.org/en-US/docs/Web/HTTP/Cookies.
- Vacca, John, editor. *Network and System Security*. 2nd ed., Elsevier, 2014.
- Vacca, John R. *Biometric Technologies and Verification Systems*. Elsevier, 2007.
- _____. *Computer Forensics: Computer Crime Scene Investigation*. 2nd ed., Charles River Media, 2005.
- _____. *Computer and Information Security Handbook*. Kaufmann, 2013.
- Valiant, Leslie. *Probably Approximately Correct: Nature's Algorithms for Learning and Prospering in a Complex World*. Basic, 2013.
- Van Wie Davis, Elizabeth. *Cyberwar Policy in the United States, Russia, and China*. Rowman & Littlefield, 2021.
- Vanderbilt, Tom. "Autonomous Cars through the Ages." *Wired*, 6 Feb. 2012, www.wired.com/2012/02/autonomous-vehicle-history.
- "Verizon 2018 Data Breach Investigations Report." *Verizon*, 2018, www22.verizon.com/wholesale/contenthub/data_breach_investigation_report.html.
- Vijayan, Jaikumar. "The Identity Underworld: How Criminals Sell Your Data on the Dark Web." *Christian Science Monitor*, 6 May 2015, www.csmonitor.com/World/Passcode/2015/0506/The-identity-underworld-How-criminals-sell-your-data-on-the-Dark-Web.
- Vinod Kumar, T. M., editor. *Smart Economy in Smart Cities*. Springer Singapore, 2017.
- Vogels, Emily A. "Teens and Cyberbullying 2022." *Pew Research Center*, 15 Dec. 2022, www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022.
- Volonino, Linda, Reynaldo Anzaldua, and Jana Godwin. *Computer Forensics: Principles and Practice*. Prentice Hall, 2007.
- Voo, Julia, Irfan Hemani, and Daniel Cassidy. "National Cyber Power Index 2022." *Belfer Center for Science and International Affairs*, Sept. 2022, www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf.
- "Vulnerability." *CVE*, 2023, www.cve.org/Resources/Support/Glossary?activeTerm=glossaryVulnerability.
- Wakabayashi, Daisuke. "Uber's Self-Driving Cars Were Struggling before Arizona Crash." *New York Times*, 23 Mar. 2018, www.nytimes.com/2018/03/23/technology/uber-self-driving-cars-arizona.html.
- Wall, D. *Cybercrime: The Transformation of Crime in the Information Age*. Polity, 2007.
- Wall, D. S., and M. L. Williams. "Policing Cybercrime: Networked and Social Media Technologies and the Challenges for Policing." *Policing and Society*, vol. 23, 2013, pp. 409-12.
- Wall, David. *Cybercrimes: The Transformation of Crime in the Information Age*. Polity, 2007.
- Wallace, Robert, and M. Keith Melton. *Spycraft: The Secret History of the CIA's Spycrafts, from Communism to Al-Qaeda*. Plume, 2009.
- "Wanted: Global Rules on Cyberwarfare." *Christian Science Monitor*, 19 Feb. 2013, www.csmonitor.com/Commentary/the-monitors-view/2013/0219/Wanted-global-rules-on-cyberwarfare.
- Warren, Christina. "The Evolution of Mac OS, From 1984 to Mountain Lion." *Mashable*, 17 Feb. 2012, mashable.com/2012/02/17/mac-os-timeline/#KKsyA8f26qqR.
- Warren, Tom. "Windows Turns 35: A Visual History." *The Verge*, 20 Nov. 2020, www.theverge.com/2015/11/19/9759874/microsoft-windows-35-years-old-visual-history.
- Wassberg, Joakim. *Computer Programming for Absolute Beginners*. Packt, 2020.
- Watters, Paul A. *Cybercrime and Cybersecurity*. CRC Press, 2023.
- Wayne L., A., and L. A. Johnson. "Current United States Presidential Views on Cyber Security and Computer Crime with Corresponding Department of Justice

- Enforcement Guidelines.” *Journal of International Diversity*, 2011, pp. 116-19.
- Weatherbed, Jess. “T-Mobile Discloses Its Second Data Breach So Far This Year.” *The Verge*, 2 May 2023, www.theverge.com/2023/5/2/23707894/tmobile-data-breach-april-personal-data-pin-hack-security.
- “Web Standards.” *W3C*, 2023, www.w3.org/standards.
- “Website Security.” MDN, 3 July 2023, developer.mozilla.org/en-US/docs/Learn/Server-side/First_steps/Website_security.
- Wei, June. *Mobile Electronic Commerce: Foundations, Development, and Applications*. CRC Press, 2015.
- Weinberger, Sharon. “Computer Security: Is This the Start of Cyberwarfare?” *Nature*, 9 June 2011, www.nature.com/articles/474142a.
- Weissman, Cale Guthrie. “The Cambridge Analytica Revelations Are Only Beginning.” *Fast Company*, 10 Jan. 2019, www.fastcompany.com/90290604/cambridge-analytica-pleads-guilty-hands-over-passwords.
- Weizenbaum, J. *Computer Power and Human Reason: From Judgement to Calculation*. W. H. Freeman, 1976.
- West, Darrell M. *The Next Wave: Using Digital Technology to Further Social and Political Innovation*. Brookings Institution, 2011.
- “What Is Big Data?” *Oracle*, www.oracle.com/big-data/what-is-big-data.
- “What Is Cloud Security?” *IBM*, www.ibm.com/topics/cloud-security.
- “What Is Cyberbullying.” *StopBullying.gov*, 21 July 2020, www.stopbullying.gov/cyberbullying/what-is-it.
- “What Is Database Security?” *IBM*, www.ibm.com/topics/database-security.
- “What Is Debugging?” *AWS*, 2023, aws.amazon.com/what-is/debugging.
- “What Is a Deepfake?” *The Economist*, 7 Aug. 2019, www.economist.com/the-economist-explains/2019/08/07/what-is-a-deepfake.
- “What Is a Driver?” *Microsoft*, 4 Nov. 2022, learn.microsoft.com/en-us/windows-hardware/drivers/gettingstarted/what-is-a-driver-.
- “What Is ‘Economic Espionage’?” *FBI*, www.fbi.gov/about/faqs/what-is-economic-espionage.
- “What Is ‘Fuzzy Logic’? Are There Computers That Are Inherently Fuzzy and Do Not Apply the Usual Binary Logic?” *Scientific American*, 21 Oct. 1999, www.scientificamerican.com/article/what-is-fuzzy-logic-are-t.
- “What Is the History of Microsoft Windows?” *Indiana University Knowledge Base*, 18 Jan. 2018, kb.iu.edu/d/abwa.
- “What Is the Internet Protocol?” *Cloudflare*, www.cloudflare.com/learning/network-layer/internet-protocol.
- “What Is Pharming and How to Protect Yourself.” *Kaspersky Lab*, usa.kaspersky.com/internet-security-center/definitions/pharming#.WDXNKLIrJQI.
- “What Is Ransomware?” *Microsoft*, 24 Apr. 2023, www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx.
- “What Is Zero Trust Security? Zero Trust Architecture Model Explained.” *ASEE*, 13 Mar. 2023, cybersecurity.asee.co/blog/zero-trust-security-architecture-explained.
- Wheeler, Leigh Ann. *How Sex Became a Civil Liberty*. Oxford UP, 2013.
- Whitaker, Rob. *Developing Inclusive Mobile Apps*. Apress, 2020.
- Whitman, James Q. “Two Western Cultures of Privacy: Dignity versus Liberty.” *Yale Law Journal*, vol. 113, no. 6, Apr. 2004, pp. 1151-221.
- Whittaker, Zack. “Atlanta, Hit by Ransomware Attack, Also Fell Victim to Leaked NSA Exploits.” *ZDNet*, 27 Mar. 2018, www.zdnet.com/article/atlanta-hit-by-ransomware-attack-also-fell-victim-to-leaked-nsa-exploits.
- _____. “iOS 17 Includes These New Security and Privacy Features.” *TechCrunch*, 18 Sept. 2023, techcrunch.com/2023/09/18/ios-17-includes-these-new-security-and-privacy-features.
- _____. “A New Data Leak Hits Aadhaar, India’s National Id Database.” *ZDNet*, 23 Mar. 2018, www.zdnet.com/article/another-data-leak-hits-india-aadhaar-biometric-database.
- Wierzel, Kimberly L. “If You Can’t Beat Them, Join Them: Data Aggregators and Financial Institutions.” *North Carolina Banking Institute*, vol. 5, no. 1, 2001, pp. 457-83.
- Wiggins, Chris, and Matthew L. Jones. *How Data Happened: A History from the Age of Reason to the Age of Algorithms*. Norton, 2023.
- Wiles, Jack, et al. *Low Tech Hacking: Street Smarts for Security Professionals*. Syngress, 2012.
- Williams, Rhiannon. “Apple iOS: A Brief History.” *The Telegraph*, 17 Sept. 2015, www.telegraph.co.uk/technology/apple/11068420/Apple-iOS-a-brief-history.html.
- Williams, Richard N. *Internet Security Made Easy: Take Control of Your Computer*. Flame Tree, 2015.
- Williams, Sean. “5 Big Advantages of Blockchain and 1 Reason to Be Very Worried.” *Motley Fool*, 11 Dec. 2017,

- [www.fool.com/investing/2017/12/11/5-big-advantages-of-blockchain-and-1-reason-to-be.aspx.](http://www.fool.com/investing/2017/12/11/5-big-advantages-of-blockchain-and-1-reason-to-be.aspx)
- Wilson, Clay. *CRS Report for Congress: Information Warfare and Cyberwar; Capabilities and Related Policy Issues*. Congressional Research Service, 2004, apps.dtic.mil/sti/tr/pdf/ADA477185.pdf.
- Wilton, Paul, and Jeremy McPeak. *Beginning JavaScript*. 5th ed., Wrox, 2015.
- "Windows 10 Privacy Settings: How to Stop Microsoft from Spying on You." *The Star*, 16 Feb. 2019, www.thestar.com.my/tech/tech-news/2019/02/16/windows-10-privacy-settings-how-to-stop-microsoft-from-spying-on-you.
- "Wireless History Timeline." *Wireless History Foundation*, wirelesshistoryfoundation.org/wireless-history-project/wireless-history-timeline.
- Witten, Ian H., Eibe Frank, Mark A. Hall, and Christopher J. Pal. *Data Mining: Practical Machine Learning Tools and Techniques*. 4th ed., Morgan Kaufmann, 2016.
- Wood, David. *Interface Design: An Introduction to Visual Communication in UI Design*. Fairchild Books, 2014.
- Wood, Lamont. "The Clock Is Ticking for Encryption." *Computerworld*, 21 Mar. 2011, www.computerworld.com/article/2550008/security0/the-clock-is-ticking-for-encryption.html.
- Woollaston, Victoria. "WannaCry Ransomware: What Is It and How to Protect Yourself." *Wired*, 22 May 2017, www.wired.co.uk/article/wannacry-ransomware-virus-patch.
- Wozniak, Steve, and Gina Smith. *iWoz: Computer Geek to Cult Icon: How I Invented the Personal Computer, Co-Founded Apple, and Had Fun Doing It*. W. W. Norton, 2007.
- Wright, Austin. "The Unseen Cyber-War: National Security Infrastructure Faces Relentless Cyberespionage Campaign." *National Defense*, vol. 94, no. 673, 2009, pp. 28-32, www.jstor.org/stable/45370556.
- Wright, Oliver, et al. "Hacking Scandal: Is This Britain's Watergate?" *Independent*, 9 July 2011, www.independent.co.uk/news/uk/crime/hacking-scandal-is-this-britain-s-watergate-2309487.html.
- Wuerthele, Mike. "Apple Unveils iPadOS, Adding Features Specifically to iPad." *AppleInsider*, 2 June 2019, appleinsider.com/articles/19/06/03/apple-supplements-ios-13-with-new-tablet-specific-ipad-os-branch.
- "XML." *PC Mag*, www.pc当地/encyclopedia/term/55048/xml.
- "XML Tutorial." *W3Schools*, www.w3schools.com/xml.
- Yakowitz, Will. "When Monitoring Your Employees Goes Horribly Wrong." *Inc.*, www.inc.com/will-yakowitz/when-monitoring-your-employees-goes-horribly-wrong.
- yakowicz/drones-catch-employees-having-sex-and-other-employee-monitoring-gone-wrong.html.
- Yar, M. *Cybercrime and Society*. SAGE, 2006.
- Ybarra, Michele L., and Kimberly J. Mitchell. "How Risky Are Social Networking Sites? A Comparison of Places Online Where Youth Sexual Solicitation and Harassment Occurs." *Pediatrics*, vol. 121, no. 2, 2008, pp. e350-e357.
- Yerby, Jonathan. "Legal and Ethical Issues of Employee Monitoring." *Online Journal of Applied Knowledge Management*, vol. 1, no. 2, 2013, pp. 4-54.
- Yoo, Christopher S. "Protocol Layering and Internet Policy." *University of Pennsylvania Law Review*, vol. 161, no. 6, 2013, pp. 1707-71.
- Yourdon, Edward, and Jennifer Yourdon. *Time Bomb 2000*. 2nd ed., Prentice Hall, 1999.
- Zanella, A., et. al. "Internet of Things for Smart Cities." *IEEE Internet of Things Journal*, vol. 1, no. 1, 2014, pp. 22-32.
- Zapotosky, Matt, and Rosalind S. Helderman. "FBI Recommends No Criminal Charges in Clinton Email Probe." *Washington Post*, 5 July 2016, www.washingtonpost.com/world/national-security/fbi-chief-plans-remarks-to-media-amid-heightened-focus-on-clinton-email-probe/2016/07/05/a53513c4-42b9-11e6-bc99-7d269f8719b1_story.html?utm_term=.c63e789a7af3.
- Zdziarski, J. *Ending Spam: Bayesian Content Filtering and the Art of Statistical Language Classification*. No Starch Press, 2005.
- Zeller, Andreas. *Why Programs Fail: A Guide to Systematic Debugging*. Kaufmann, 2009.
- Zetlin, Minda. "Want to Make Facebook Stop Tracking Your Location When Not in Use? Here's How." *Inc.*, 22 Feb. 2019, www.inc.com/minda-zetlin/facebook-location-tracking-mobile-privacy-paul-mcdonald.html.
- Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Broadway, 2014.
- Zetter, Kim, and Brian Barrett. "Apple to FBI: You Can't Force us to Hack the San Bernardino iPhone." *Wired*, 25 Feb. 2016, www.wired.com/2016/02/apple-brief-fbi-response-iphone.
- Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs, 2019.
- Zwick, Elizabeth D., Simon Cooper, and D. Brent Chapman. *Building Internet Firewalls*. 2nd ed., O'Reilly, 2000.

GLOSSARY

Aadhaar: India's national biometric identification system

access level: in a computer security system, a designation assigned to a user or group of users that allows access to a predetermined set of files or functions

adware: software that generates advertisements to present to a computer user

algorithm: a set of step-by-step instructions for performing computations

Alphabet: the parent company of Google

Android: a mobile operating system introduced by Google in 2008

Anonymous: a loose association of online activists and followers who advocate internet freedom via attacks against websites of government agencies, corporations, and others

antivirus software: software designed to scan a computer system, identify potential computer virus programs, and remove those programs from the computer

application: a program or integrated suite of programs that has a defined function

application program interface (API): the code that defines how two pieces of software interact, particularly a software application and the operating system on which it runs

application suite: a set of programs designed to work closely together, such as an office suite that includes a word processor, spreadsheet, presentation creator, and database application

application-level firewalls: firewalls that serve as proxy servers through which all traffic to and from applications must flow

artificial intelligence (AI): the intelligence exhibited by machines or computers, in contrast to human, organic, or animal intelligence

authentication: the process by which the receiver of encrypted data can verify the identity of the sender or the authenticity of the data

autonomous agent: a system that acts on behalf of another entity without being directly controlled by that entity

backdoor: a hidden method of accessing a computer system that is placed there without the knowledge of the system's regular user in order to make it easier to access the system secretly

behavioral marketing: advertising to users based on their habits and previous purchases

blockchain: a form of decentralized recordkeeping popularized by cryptocurrency

botnet: a collection of computers that have been infected with software by computer hackers to force those computers to commit crimes, such as sending out computer viruses or unsolicited email (spam)

Cambridge Analytica: a British political consulting firm

catfishing: the intentional use of a false online identity in order to trick someone into engaging in an emotional and/or romantic relationship

central processing unit (CPU): electronic circuitry that provides instructions for how a computer handles, processes, and manages data from applications and programs

chatbot: a computer program that mimics human conversation responses in order to interact with people through text; also called "talkbot," "chatterbot," or simply "bot"

ChatGPT: a chatbot created by technology company OpenAI and powered by artificial intelligence technology

cloud computing: a form of technology service where the user's data and applications are stored in and run on a server to which the user connects over the internet

cloud services: computing services that are hosted on external servers and made available to users via the internet

combinatorial design: the study of the creation and properties of finite sets in certain types of designs

computer: any device that can be programmed to perform mechanical or electrical computation, processing numbers; since the middle of the twentieth century, the term has commonly been used for equipment that can be programmed using a binary number system to perform a variety of work; for a computer to process letters, words, graphic images, or maps, human programmers have to encode nonnumerical data in a numeric form

Computer Fraud and Abuse Act (CFAA): a 1986 legislative amendment that made accessing a protected computer without authorization, or exceeding one's authorized level of access, a federal offense

computer virus: a generic term for a malicious and self-replicating program placed on a computer without the user's knowledge or consent

cookies: small data files that allow websites to track users; also referred to as hypertext transfer protocol (HTTP) cookies

cracker: a criminal hacker; one who finds and exploits weak points in a computer's security system to gain unauthorized access for malicious purposes

crippleware: software programs in which key features have been disabled and can only be activated after registration or with the use of a product key

cryptology: the science of encrypting or decrypting information, including creating codes for privacy or security and finding means to break a code by working from a message in an unknown code to learn the pattern

Cyber Command (USCYBERCOM): a US military command dedicated to cyberwarfare

cybercrime: crime that involves targeting a computer or using a computer or computer network to commit a crime, such as computer hacking, digital piracy, and the use of malware or spyware

cyberterrorism: the practice of using cyberattacks to interfere with normal life in such a way as to cause upheaval and chaos in a targeted group or society

cyberwarfare: organized attempts by one country or militant nonstate actor to compromise the computer networks of another, with the goal of disrupting basic systems such as the military, telecommunications, transportation, or finance

cyberweapon: any type of malware or malicious computer code capable of stealing highly valuable or sensitive data or causing harm or disruption on a mass scale

dark web: a section of the internet that is not easily seen and is often associated with illegal activities

data breach: an incident in which sensitive or confidential information is stolen or accessed by an unauthorized individual, group, or software program

data mining: the process of using algorithms to search for meaningful patterns in large collections of data, often without stating any kind of a hypothesis in advance

data source: the origin of the information used in a computer model or simulation, such as a database or spreadsheet

database: a collection of data items used for multiple purposes that is stored on a computer

decryption: the process of converting coded or encrypted data back to its original form

deepfake: an emerging technology that allows computer users to create fabricated but highly convincing sounds, static images, and moving pictures

deep learning: an emerging field of artificial intelligence research that uses neural network algorithms to improve machine learning

denial-of-service (DoS) attack: an attack on a computer system, usually a website, intended to render it unusable

device: equipment designed to perform a specific function when attached to a computer, such as a scanner, printer, or projector

device fingerprinting: information that uniquely identifies a particular computer, component, or piece of software installed on the computer; this can be used to find out precisely which device accessed a particular online resource

digital literacy: familiarity with the skills, behaviors, and language specific to using digital devices to access, create, and share content through the internet

distributed denial-of-service (DDoS) attack: a DoS attack carried out by multiple computers or other devices

Electronic Communications Privacy Act: a 1986 law that extended restrictions on wiretapping to cover the retrieval or interception of information transmitted electronically between computers or through computer networks

embedded systems: computer systems that are incorporated into larger devices or systems to monitor performance or to regulate system functions

encryption: the process of converting data from its original form into a form that must be decoded or decrypted

Federal Communications Commission (FCC): the government agency that regulates radio, television, wire, satellite, and cable broadcasts

firewall: a virtual barrier that filters traffic as it enters and leaves the internal network, protecting internal resources from attack by external sources

graphical user interface (GUI): a computer interface in which the user controls the computer by interacting with menus, icons, and other graphical elements

hacking: the use of technical skill to gain unauthorized access to a computer system; also, any kind of advanced tinkering with computers to increase their utility

hardware: the physical parts that make up a computer; these include the motherboard and processor, as well as input and output devices such as monitors, keyboards, and mice

host-based firewalls: firewalls that protect a specific device, such as a server or personal computer, rather than the network as a whole

hybrid cloud: a cloud-computing model that combines public cloud services with a private cloud platform linked through an encrypted connection

hypertext markup language (HTML): used to define pages on the World Wide Web (WWW)

ILOVEYOU virus: a computer virus that emerged in 2000 and was the fastest spreading, most damaging computer virus ever seen at that time

information technology (IT): the use of computers and related equipment for the purpose of processing and storing data

infrastructure as a service: a cloud computing platform that provides additional computing resources by linking hardware systems through the internet; also called “hardware as a service”

internet: a real, though loosely defined, communication structure by which enabled computers in one part of the world can communicate with enabled computers in any other part of the world by various modes of interconnection

Internet of Things (IoT): a wireless network connecting devices, buildings, vehicles, and other items with network connectivity

intrusion detection system: a system that uses hardware, software, or both to monitor a computer or network in order to determine when someone attempts to access the system without authorization

iOS: Apple’s proprietary mobile operating system, installed on Apple devices such as the iPhone and iPod Touch

machine learning algorithm: an algorithm that is capable of being trained and of learning based on the datasets to which it is exposed and the tasks it completes

malware: a general term for all unauthorized software installed on a computer clandestinely for nefarious purposes, generally to the detriment of the computer and its user

metadata: data that contains information about other data, such as author information, organizational information, or how and when the data was created

Michelangelo computer virus: a destructive piece of computer code discovered in 1991

network: two or more computers being linked in a way that allows them to transmit information back and forth

network firewalls: firewalls that protect an entire network rather than a specific device

networking: the use of physical or wireless connections to link together different computers and computer networks so that they can communicate with one

another and collaborate on computationally intensive tasks

operating system (OS): a specialized program that manages a computer’s functions

packet filters: filters that allow data packets to enter a network or block them on an individual basis

penetration testing: a means of locating and identifying vulnerabilities in a computer, network, or computer system

personally identifiable information (PII): information that can be used to identify a specific individual

phishing: the use of online communications to trick a person into sharing sensitive personal information, such as credit card numbers or Social Security numbers

piracy: in the digital context, unauthorized reproduction or use of copyrighted media in digital form

platform as a service: a category of cloud computing that provides a virtual machine for users to develop, run, and manage web applications

port scanning: the use of software to probe a computer server to see if any of its communication ports have been left open or vulnerable to an unauthorized connection that could be used to gain control of the computer

Pretty Good Privacy: a data encryption program created in 1991 that provides both encryption and authentication

principle of least privilege: a philosophy of computer security that mandates users of a computer or network be given, by default, the lowest level of privileges that will allow them to perform their jobs; this way, if a user’s account is compromised, only a limited amount of data will be vulnerable

programming languages: sets of terms and rules of syntax used by computer programmers to create instructions for computers to follow; this code is then compiled into binary instructions for a computer to execute

proxy server: a computer through which all traffic flows before reaching the user’s computer

random-access memory (RAM): memory that the computer can access very quickly, without regard to where in the storage media the relevant information is located

ransomware: malware that encrypts or blocks access to certain files or programs and then asks users to pay to have the encryption or other restrictions removed

real-time monitoring: a process that grants administrators access to metrics and usage data about a software program or database in real time

remote monitoring: a platform that reviews the activities on software or systems that are located off-site

scareware: malware that attempts to trick users into downloading or purchasing software or applications to address a computer problem

silent monitoring: listening to the exchanges between an incoming caller and an employee, such as a customer service agent

smartphone: a mobile telephone that has the capability of running software applications and accessing the internet

social networking services: online platforms in which one of the primary functions is to create and maintain social networks that users opt into by adding one another as friends or following accounts

software as a service (SaaS): a software service system in which software is stored at a provider's data center and accessed by subscribers

software patches: updates to software that correct bugs or make other improvements

software: the sets of instructions that a computer follows in order to carry out tasks; software may be stored on physical media, but the media is not the software

spam: unsolicited emails or other messages, typically sent for commercial or fraudulent purposes

spyware: software installed on a computer that allows a third party to gain information about the computer user's activity or the contents of the user's hard drive

stateful filters: filters that assess the state of a connection and allow or disallow data transfers accordingly

Stuxnet: a computer worm that infected computers and caused severe damage to centrifuges at the Natanz nuclear facility in Iran

system: either a single computer or, more generally, a collection of interconnected elements of technology that operate in conjunction with one another

system software: the operating system that allows programs on a mobile device to function

tablet: a mobile computer that is small enough to be held in the hand and that provides access to a wide range of software applications and the internet

transparent monitoring: a system that enables employees to see everything that the managers monitoring them can see

trojan horse: computer code embedded in another, seemingly legitimate program, and designed so that the author/distributor is able to control the infected computer remotely without the knowledge or consent of the owner; also known simply as a trojan

trusted platform module (TPM): a standard used for designing cryptoprocessors, which are special chips that enable devices to translate plain text into cipher text and vice versa

utility programs: apps that perform basic functions on a computer or mobile device such as displaying the time or checking for available network connections

wardriving: driving around with a device such as a laptop that can scan for wireless networks that may be vulnerable to hacking

web application: an application that is downloaded either wholly or in part from the internet each time it is used

World Wide Web (WWW): a communication layer that runs atop the infrastructure of the internet and enables communication between computers all over the world using hypertext links

worm: a type of malware that can replicate itself and spread to other computers independently; unlike a computer virus, it does not have to be attached to a specific program

XML: extensible markup language, a programming language used to categorize and describe data.

zero trust security: a cybersecurity model in which all network traffic is initially presumed to be untrusted

zombie computer: a computer that is connected to the internet or a local network and has been compromised such that it can be used to launch malware or virus attacks against other computers on the same network

ORGANIZATIONS

Center for Internet Security

31 Tech Valley Drive
East Greenbush, NY 12061
518.266.3460
www.cisecurity.org

Cloud Security Alliance

709 Dupont Street
Bellingham, WA 98225
www.cloudsecurityalliance.org

Cyberpeace Institute

Campus Biotech Innovation Park
Av. de Sécheron 15
1202 Genève
Switzerland
41.22.518.98.72
cyberpeaceinstitute.org

Cybersecurity and Infrastructure Security Agency (CISA)

US Department of Homeland Security
245 Murray Lane
Stop 0380
Washington, DC 20528-0380
888.282.0870
www.cisa.gov

Forum of Incident Response and Security Teams (FIRST)

2500 Regency Parkway
Cary, NC 27518
www.first.org

Information Security Forum (ISF)

10 Eastcheap
London EC3M 1AJ
United Kingdom
www.securityforum.org

Information Systems Security Association (ISSA)

100 TradeCenter Drive
Suite G-700
Woburn, MA 01801

866.349.5818

www.issa.org

National Cybersecurity Alliance

1333 New Hampshire Avenue NW
Floor 2
Washington, DC 20036
staysafeonline.org

National Cybersecurity Society (NCSS)

1215 31st Street NW
Washington, DC 20007
703.340.7757
nationalcybersecuritysociety.org

The Nonprofit Technology Network (NTEN)

PO Box 86308
Portland, OR 97286-0308
503.272.8800
www.nten.org

Open Worldwide Application Security Project (OWASP)

300 Delaware Avenue
Suite 210, #384
Wilmington, DE 19801
951.692.7703
www.owasp.org

SANS Institute

(SysAdmin, Audit, Network and Security)
11200 Rockville Pike
Suite 200
North Bethesda, MD 20852
www.sans.org

Shadowserver Foundation

www.shadowserver.org

Women in Cybersecurity (WICYS)

370 S Lowe Avenue
Suite A-244
Cookeville, TN 38501
www.wicys.org

SUBJECT INDEX

- 2001: A Space Odyssey*, 22
9/11 terrorist attacks, 287
- Aadhaar hack of 2018, 1-3
access control, 3-5
- Accreditation Board for Engineering and Technology, Inc. (ABET), 87
- acquired immunodeficiency syndrome (AIDS), 297
- Advanced Encryption Standard (AES), 5-7
- Advanced Research Projects Agency Network (ARPANET), 99, 130, 211, 313
- AIDS Trojan, 297
- algorithm, 7-9
- Amazon's Alexa, 46, 48
- America Online (AOL), 111, 280
- American Airlines introduced the Semi-Automated Business Research Environment (SABRE), 99
- American Telephone & Telegraph (AT&T), 274, 337
- Android operating system (OS), 9-11
- anonymity, 11-13
- anonymizers, 11-13
- Anonymous, 13-17
- Apple computer, 212, 249, 348
- Apple iCloud, 69
- Apple's Siri, 46, 48
- application security testing (AST), 131
- application software, 108, 109, 186
- APT1: Exposing One of China's Cyber Espionage Units*, 68
- arithmetic and logic unit (ALU), 262
- artificial intelligence (AI), 17-27
- artificial intelligence cold war, 27-31
- ASCII code, 64
- asymmetric digital subscriber line (ADSL), 101
- asymmetric-key encryption, 191, 192
- autonomous car (also robotic car or driverless car), 31-35
- backdoors, 66, 107, 204, 205, 240, 289
- BBC News*, 165
- Bel Geddes, Norman, 31
- Berners-Lee, Timothy, 216
- big data, 37-39
- Binary Automatic Computer (BINAC), 277
- biometric identification systems, 39-43
- birth control, 287
- bitcoin, 43, 147, 176, 297, 299
- blockchains, 43-46
- Board of Education v. Earls*, 287
- Boole, George, 19, 206, 277
- Boolean logic, 205
- botnets, 47, 48, 83, 124, 195, 196, 226, 322
- bots, 46-49
- Bowers v. Hardwick*, 287
- Broderick, Matthew, 212
- browsers, 49-53
- "BrutePrint" attack, 42
- Bush, George W., 132, 283, 288, 331
- Cambridge Analytica Facebook data scandal, 55-58
- Canada Anti-Spam Law, 190
- Catfish* (documentary), 58, 60
- catfishing, 58-61
- Central Intelligence Agency (CIA), 16, 111, 139, 183, 214, 228, 309
- central processing unit (CPU), 108, 169, 261, 278, 296
- Certified Ethical Hacker (CEH), 235
- Certified Information Security Manager (CISM), 235
- Certified Information Systems Security Professional (CISSP), 235
- changing passwords, 61-66
- ChatGPT, 23, 24
- China's cyberinvasion, 66-69
- Chinese hackers, 256, 257, 307
- Chromebooks, 11
- Church of Scientology, 13, 14, 215
- Clinton, Hillary, 57, 135, 140, 307, 311
- Cloud computing, 69-71
- cloud rot, 10
- COBOL, 91, 93, 361
- combinatorics, 71-73
- common language runtime (CLR), 93
- competitive intelligence, 231
- computer and technical support specialists, 73-76
- computer chips, 87, 88, 89, 261, 363
- computer crime investigation, 76-81
- computer fraud, 81-83
- Computer Fraud and Abuse Act of 1984 (CFAA), 83-85
- computer hardware engineers, 85-88
- computer hardware security, 88-90
- computer languages, 90-94
- computer memory, 94-96
- computer network architects, 96-99
- computer networks, 99-104
- computer programmers, 104-106
- computer security, 106-108

- computer security firms, 14
computer security professionals, 106, 177, 204, 205, 267
Computer Security Resource Center (CSRC), 73, 244
computer software, 108-109
computer viruses, 109-112
computer worms, 109-112
Computers at Risk: Safe Computing in the Information Age, 133
Conscience of a Hacker; The, 213
continuous adaptive risk and trust assessment (CARTA), 368
Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM) of 2003, 190, 283, 322, 325, 326
copier, 199-201
Counterfeit Access Device, 83, 213
COVID-19 pandemic, 23, 102, 103, 188, 264, 282
credit cards, 39, 147, 186, 227, 363
Crimes Against Children Research Center, 117
cryptocurrency, 43, 44, 45, 48, 147, 166, 297, 299
cryptographic keys, 88
cryptography, 112-114
Customer relationship management (CRM), 154
Cyber Action Team (CAT), 111
cyberattacks, 27, 67, 68, 111, 125, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 142, 170, 183, 195, 196, 197, 226, 256, 284, 318, 335
cyberbullying, 117-120
cybercrime, 121-128
cybercriminals, 1, 123, 124, 125, 126, 255, 286, 297, 298
cyberpornography, 124
cybersecurity testing, 130-132
cyberstalking, 60, 78, 124, 125, 176
cyberterrorism, 132-136
cyberthreat, 130, 207, 331
cyberwarfare, 136-141
cyberweapon, 141-144
- dark web, 145-148
data breach, 148-150
data communications analysts (or network analysts), 96
Data Encryption Standard (DES), 5
data harvesting (also web harvesting, data scraping, data aggregation, data mining), 150-152
data mining, 152-155
data protection, 155-158
data theft, 26, 170
database, 158-159
database design, 160-161
debugging, 161-163
deepfake, 163-166
- Defense Advanced Research Projects Agency (DARPA), 32, 183-184
Defense Readiness Condition (DEFCON), 214
Democratic National Committee (DNC), 132, 135, 139, 307, 308
demon dialing, 167-169
denial-of-service (DoS) attacks, 121, 242
Dennard, Robert, 295
deoxyribonucleic acid (DNA), 39, 288
device drivers, 169-170
digital age, 11
digital disinformation, 29
Digital Equipment Corporation (DEC), 18, 20
digital forensics, 170-172
Digital Millennium Copyright Act (DMCA), 213
digital versatile disc (DVD), 169
digital video disk (DVD), 262
digital watermarking, 172-174
direct manipulation interfaces (DMI), 210
disk operating system (DOS), 92, 170, 209, 212, 260, 274, 348
distributed denial-of-service (DDoS) attacks, 81, 195, 215
Do Not Track Act (2019), 290
Dobbs v. Jackson Women's Health Organization, 287
double data rate synchronous DRAM (DDR SDRAM), 296
doxing (or doxxing), 174-177
Dropbox, 69, 102
dynamic random-access memory (DRAM), 295
- e-banking (also internet banking or online banking), 179-181
Eckert, J. Presper, 94, 277
Economic Espionage Act, 76
Electrical Numerical Integrator and Calculator (ENIAC), 277
- electronic bugs, 181-183
electronic commerce (e-commerce) technology, 183-188
Electronic Communications Privacy Act (ECPA) of 1986, 170
- electronic database, 158, 160
electronic mail (or email), 188-190
Electronic Numerical Integrator and Computer (ENIAC), 91
ELIZA, 46
encrypted message, 6, 112, 113, 192
encryption, 191-193
end-user cybersecurity education, 193-195
Environmental Protection Act, 301
Equifax, 148, 149, 224, 286
Error-Correcting Code (ECC), 313
Estonia cyberattack, 195-197

- European Organization for Nuclear Research (CERN), 184, 216, 313
 European Smart Cities initiative, 315
 European Union, 38, 56, 125, 155, 156, 221, 256
 extensible hypertext markup language (XHTML), 265
 extensible markup language (XML), 357-359
- fair information practice principles (FIPPs), 155, 289
 fax machine, 199-201
 Federal Bureau of Investigation (FBI), 15, 25, 41, 76, 111, 125, 135, 212, 226, 228, 231, 242, 283, 288, 308, 324
 Federal Information Processing Standards (FIPS), 63
 Federal Information Processing Standards Publication (FIPS PUB), 6
 Federal Trade Commission (FTC), 55, 223, 283, 286, 289, 324
 file transfer protocol (FTP) program, 100
 Firefox, 49, 50, 51, 283, 314
 firewall, 201-203
 firmware, 204-205
 First Amendment, 11, 12, 288
 Forensic Toolkit (FTK), 79
 FORTRAN, 91, 93
 free speech, 11, 119, 172, 272, 324, 325
 Freenet, 145, 146
 fuzzy logic, 205-207
- Gates, Robert, 114
 General Data Protection Regulation (GDPR), 38, 155, 157, 221
 General Motors, 32, 34
 generative adversarial networks (GANs), 163
GETMAIL, 67
 Global Information Assurance Certification (GIAC), 235
 global positioning system (GPS), 33, 266, 354
 Google Assistant, 46, 48
 Google Chrome, 49, 51, 102
 Google Self-Driving Car Project, 34
 graphical user interface (GUI), 209-210
Griswold v. Connecticut, 287
Guardian, The, 56
- hacking, 211-216
 hacktivism, 124, 125, 133, 134, 215, 306
 hardware security module (HSM), 88
 Hoover Public Safety Center, 78
HuffPost India, 2
 human intelligence, 17, 18, 19, 22, 23
 hybrid cloud, 69, 71
 hypertext markup language (HTML), 216-219
 hypertext transfer protocol (HTTP) cookie, 219-221
- identity theft, 223-228
 Identity Theft and Assumption Deterrence Act, 223
 illegal immigration, 39
 ILOVEYOU virus, 228-230
 industrial espionage, 231-233
 information and communication technologies (ICTs), 117, 315, 317
 information security analysts, 233-236
 information technology (IT), 236-237
 infrastructure as a service (IaaS) model, 69
 Institute of Electrical and Electronics Engineers (IEEE), 100, 244
 Internal Revenue Service (IRS), 155, 225, 281
 International Atomic Energy Agency (IAEA), 333
 International Business Machines Corporation (IBM), 6, 45, 93, 99, 130, 295, 361
 internet cookie (also web cookie or browser cookie), 219
 internet freedom, 13, 15, 16, 271
 Internet of Things (IoT), 238-240
 internet protocol (IP), 240-241
 internet service provider (ISP), 12, 13, 99, 167, 213, 272, 280, 326
 internet tracing, 241-244
 internet tracking, 241-244
 Internetwork Operating System (IOS), 102
 intrusion detection, 244-246
 Intrusion Detection Expert System (IDES), 244
 iPhone operating system (iOS), 246-248
- jailbreaking, 246
 Joint Strike Fighter project, 137
Journal of Adolescence, 60
- Kubrick, Stanley, 22
- law enforcement agencies, 16, 40, 41, 42, 110, 147, 172, 243, 298
Lawrence v. Texas, 287
 lethal autonomous weapons system (LAWS), 29
 local area network (LAN), 101, 167, 267, 351
 logic programming, 17, 19, 20
 low-level languages (or machine code), 90
- Mac OS, 249-251
 machine learning, 252-253
 machine-learning algorithms, 252
 Macintosh, 49, 212, 249, 251, 278, 348, 349
 malware (or malicious software), 253-256
 Mandiant, 66, 67, 68
 MAPIGET, 67

- Marriott International, 256, 257
Massachusetts Institute of Technology (MIT), 46, 211, 218, 292
MasterCard, 13, 15, 16
Mauchly, John, 94, 277
McAfee Security, 66
McIntyre v. Ohio Elections Commission, 12
Megan Meier Cyberbullying Prevention Act, 119
Merriam-Webster dictionary, 193
Metadata, 258-259
Michelangelo computer virus, 260
microprocessors, 261-262
Microsoft Disk Operating System (MS-DOS), 212, 213, 274, 348, 349
Microsoft Edge, 49, 51, 52, 102
Microsoft Windows, 49, 108, 228, 249, 273, 299, 348
mobile applications, 263-265
mobile web, 265-266
Motion Picture Association of America (MPAA), 13, 16, 121, 272
Musk, Elon, 166
- National Aeronautics and Space Administration (NASA), 20, 265
National Computer Forensics Institute (NCFI), 78
National Crime Prevention Council, 119
National Crime Victimization Survey (NCVS), 223
National Cyber Security Center, 143
National Cyber Security Division (NCSD), 78, 115, 139
National Health Service (NHS), 299
National Highway Traffic Safety Administration (NHTSA), 33
National Institute of Standards and Technology (NIST), 6, 73, 172, 244, 306
National Research Council, 133
National Security Agency (NSA), 5, 76, 114, 139, 213, 259, 288, 299, 310
network and computer systems administrators, 267-269
network-access service (NAS), 344
New York Post, 288
New York Times, 33, 56, 66, 67, 143, 224, 227, 331
New York World's Fair, 31
nonradio bugs, 181, 182
nonvolatile random-access memory (NVRAM), 296
North American Aerospace Defense Command (NORAD), 213
North Atlantic Treaty Organization (NATO), 134, 195, 197
Obama, Barack, 27, 128, 134, 139, 259, 307, 331
object-oriented user interfaces (OOUIs), 210
Occupational Safety and Health Act, 301
- Onion Router, The (TOR), 52, 145
online piracy, 271-273
operating system (OS), 273-275
“Operation Olympic Games,” 331
Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines, 155
- Panama Papers*, 159
personal area network (PAN), 351
personal computer (PC), 277-280
Personal Data (Privacy) Ordinance, 156
Personal Information & Protection of Electronic Documents Act, 156
Pew Research Center, 59, 117, 120, 176, 338
phishing, 280-284
platform as a service (PaaS) model, 70
point-to-point tunneling protocol (PPTP), 343
Popular Mechanics, 165
printer, 199-201
privacy breaches, 284-287
privacy rights, 287-289
privacy settings, 289-291
programmable read-only memory (PROM), 94
PROTECT IP Act (PIPA), 272
Protection of Personal Information Act, 156
proxy server, 80, 88, 202
public-key cryptography, 291-293
Putin, Vladimir, 309, 310
- quality assurance analysts, 320-322
QWERTY keyboard, 9
- radio-transmitting bugs, 181
RAND Corporation, 33, 226
random-access memory (RAM), 295-296
ransomware, 297-300
read-only memory (ROM), 94, 261, 279, 295
Recording Industry Association of America (RIAA), 16, 121, 272
red cell missions, 318
“Revealed: Operation Shady RAT,” 66
risk management, 300-307
Rivest-Shamir-Adleman encryption (or RSA), 292
Roe v. Wade, 287
Russian hacking scandal, 307-312
- Safari, 49, 51, 58, 102, 221, 251
Saini, Karan, 2
Sanchez, Linda, 119
Sarbanes-Oxley Act, 300
Scientific Working Group on Digital Evidence (SWGDE), 170

- secure sockets layer (SSL), 183
 "Self-Driving Car Project," 32, 34
 servers, 313-315
 smart city, 315-318
 social engineering (also human hacking), 318-320
 Social Security numbers, 81, 139, 148, 149, 174, 203, 224, 225, 226, 227, 280, 284, 286
 software as a service (SaaS) model, 71
 software developers, 320-322
 spam, 322-327
 spam filters, 327-329
 spyware, 329-331
 standard generalized markup language (SGML), 217, 357
 Starwood reservation database, 256
 static random-access memory (SRAM), 296
 Statista, 51, 76, 125, 136, 183, 240, 255, 327
 STOMP Out Bullying campaign, 119
 Stop Online Piracy Act (SOPA), 272
 Strategic Communication Laboratories (SCL), 55
 Stuxnet virus, 331-334
 Superfund legislation, 301
 support vector machines (SVMs), 154, 252
 Symantec AntiVirus Research Center, 214, 215
 symmetric-key encryption, 191, 192
Syntactic Structures, 17
 system software, 108, 109, 263
 systems security engineering (SSE), 335-336
- Talley v. California*, 11
 targeted advertising, 337-339
 Tech Model Railroad Club (TMRC), 211
 terrorism, 24-27
 testers, 320-322
 T-Mobile G1 (or HTC Dream) smartphone, 9
 Trade Secrets Act, 76
 transmission control protocol (TCP), 100, 184, 241, 314
 transport layer security (TLS), 183
 Trump, Donald, 28, 56, 119, 135, 139, 152, 224, 307, 311
 Turing Test, 46
 Turing, Alan, 21, 46, 94, 277
- uniform resource locator (URL), 185, 242, 281
 Union of Soviet Socialist Republics (USSR, or Soviet Union), 27, 138, 196, 232
 Unique Identification Authority of India (UIDAI), 1
 United Nations (UN), 29, 316
 Universal Automatic Computer (UNIVAC), 277
 universal serial bus (USB), 79, 89, 96, 169, 204, 279, 332
 UNIX computers, 228
 unmanned aerial vehicles (UAVs), 66
 unmasking, 307
- US Congress, 29, 83, 271, 324
 US Constitution, 11
 US Copyright Office, 246
 US Court of Appeals, 259
 US Cyber Command (USCYBERCOM), 114-116
 US Department of Defense (DoD), 30, 114, 116, 139, 160, 184, 211, 228
 US Department of Homeland Security, 16, 78, 115, 116, 133, 139
 US Department of Justice (DOJ), 16, 110, 214, 257, 271
 US Secret Service, 78
 US Security and Exchange Commission (SEC), 140
 US Supreme Court, 11, 324
 USA Freedom Act, 259
 USA PATRIOT Act, 259
 usability, 341-342
- virtual private network (VPN), 343-344
- Wall Street Journal*, 288
 war dialing, 167-169
 War Operation Plan Response (WOPR), 213
WarGames, 134, 212, 214
Washington Post, 58
 web browser, 49-53
 web developers, 345-348
 WebConnect, 337
 Weizenbaum, Joseph, 46
 wide area networks (WANs), 100, 101, 267, 343
 WikiLeaks, 15, 57, 134, 309
 Windows operating system, 348-351
 windows, icons, menus, and pointer objects (WIMP), 210
Wired magazine, 47
 wireless LAN (WLAN), 101, 351, 352
 wireless networks, 351-353
 wireless PAN (WPAN), 351
 wireless wide-area network (WWAN), 351
 workplace monitoring, 353-356
 World Health Organization (WHO), 297
 World War II, 25, 27, 29, 112, 115, 136, 195, 196, 277
 World Wide Web (WWW), 49, 92, 99, 101, 121, 124, 133, 145, 184, 185, 216, 217, 218, 265, 313, 357
 World Wide Web Consortium (W3C), 218, 265, 357
- Y2K bug, 162, 163, 361, 362, 364
 Y2K crisis, 361-365
- Zero Trust Network Access (ZTNA), 368
 zero trust security, 367-369
 Zuckerberg, Mark, 58, 102, 152, 338

The Principles of... Series

Principles of Science

Principles of Aeronautics
Principles of Anatomy
Principles of Astronomy
Principles of Behavioral Science
Principles of Biology
Principles of Biotechnology
Principles of Botany
Principles of Chemistry
Principles of Climatology
Principles of Computer Science
Principles of Computer-Aided Design
Principles of Digital Arts & Multimedia
Principles of Ecology
Principles of Energy
Principles of Fire Science
Principles of Forestry & Conservation
Principles of Geology
Principles of Information Technology
Principles of Marine Science
Principles of Mathematics
Principles of Mechanics
Principles of Microbiology
Principles of Modern Agriculture
Principles of Pharmacology
Principles of Physical Science
Principles of Physics
Principles of Probability & Statistics
Principles of Programming & Coding
Principles of Robotics & Artificial Intelligence
Principles of Scientific Research
Principles of Sports Medicine & Kinesiology
Principles of Sustainability
Principles of Zoology

The Principles of... Series

Principles of Health

Principles of Health: Allergies & Immune Disorders

Principles of Health: Anxiety & Stress

Principles of Health: Depression

Principles of Health: Diabetes

Principles of Health: Nursing

Principles of Health: Obesity

Principles of Health: Occupational Therapy

Principles of Health: Pain Management

Principles of Health: Prescription Drug Abuse

Principles of Business

Principles of Business: Accounting

Principles of Business: Economics

Principles of Business: Entrepreneurship

Principles of Business: Finance

Principles of Business: Globalization

Principles of Business: Leadership

Principles of Business: Management

Principles of Business: Marketing

Principles of Sociology

Principles of Sociology: Group Relationships & Behavior

Principles of Sociology: Personal Relationships & Behavior

Principles of Sociology: Societal Issues & Behavior