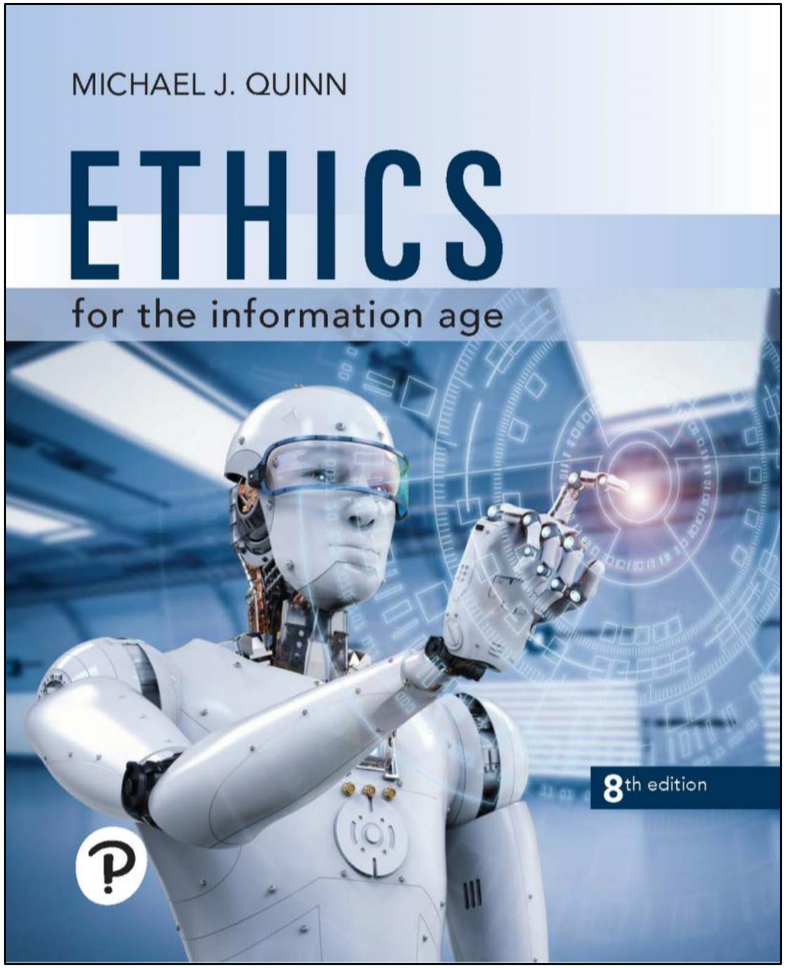
Ethics for the Information Age

Eighth Edition



Chapter 7

Computer and Network Security

Pearson

7.2 Hacking

Hackers, Past and Present

- **Original meaning of hacker**: explorer, risk taker, system innovator, write elegant or clever piece of code.
  - MIT's Tech Model Railroad Club in 1950s
- 1960s-1980s: Focus shifted from electronics to computers and networks
  - 1983 movie **WarGames**
- **Modern meaning of hacker:** someone who gains unauthorized access to computers and computer networks

Obtaining Login Names, Passwords

1. Eavesdropping
2. Dumpster diving
3. Social engineering
4. Brute-force searches
5. Dictionary attacks

Password Dos and Don’ts

- Do not use short passwords.
- Do not rely solely on words from the dictionary.
- Do not rely on substituting numbers for letters.
- Do not reuse passwords.
- Give ridiculous answers to security questions.
- Enable two-factor authentication if available.
- Have password recoveries sent to a secure email address.

Computer Fraud and Abuse Act

- Criminalizes wide variety of hacker-related activities
  1. Transmitting code that damages a computer
  2. Accessing any Internet-connected computer without authorization
  3. Transmitting classified government information
  4. Traffickingالاتجار in computer passwords
  5. Computer fraud
  6. Computer extortionابتزاز
- Maximum penalty: 20 years in prison and $250,000 fine

Electronic Communications Privacy Act

- Illegal to intercept اعتراض…
  - Telephone conversations
  - Email
  - Any other data transmission
- Crime to access stored email messages without authorization

Pearson

FBI and the Locked iPhone (1 of 3)

- December 2015
  - Syed Rizwan Farook and Tashfeen Malik killed 14, wounded 22 others at holiday gathering in San Bernardino, California
  - Malik pledged allegiance to the Islamic Stateيعلن ولاءه لتنظيم الدولة الإسلامي
  - Farook and Malik died in shootout with police
  - FBI recovered Malik’s work-issued iPhone 5C, but it was locked
- Built-in security features of iPhone 5C
  - All personal data encrypted
  - After 10 consecutive incorrect passcode entry attempts, encryption key deleted, rendering all personal data inaccessible
  - When incorrect passcodes are entered, delay introduced between passcode entry attempts

FBI and the Locked iPhone (2 of 3)

- February 2016
  - FBI asked Apple to create a new version of iOS that disabled the passcode security features
  - Apple refused to cooperate
  - FBI convinced a US magistrate to issue an order for Apple to comply
- Apple’s argument
  - If “backdoor” version of iOS that disabled security features fell into wrong hands, criminals would be able to unlock any iPhone
  - All iPhone users would be harmed

FBI and the Locked iPhone (3 of 3)

- Department of Justice’s argument
  - Apple could maintain custody of software
  - Apple could destroy software after being used by FBI
- March 2016
  - Department of Justice withdrew request, declared it had gotten into locked iPhone
  - Inspector General of DoJ later determined FBI had made request of Apple before exploring whether FBI had means to unlock iPhone
  - Skeptics المتشككين claimed FBI more interested in getting legal precedent than gaining access to Farook’s data

Sidejacking

- **Sidejacking**: hijacking of an open Web session by capturing a user's cookie, giving the attacker the same privileges as the user on that Web site.
- Ecommerce Web sites typically use *encryption* to protect the username and password people provide when logging in, but they do not encrypt the cookie that the Web browser sends to the user to continue the session.
- Sidejacking possible on unencrypted wireless networks because many sites send cookies "in the clear"
- Internet security community complained about sidejacking vulnerability for years, but ecommerce sites did not change practices

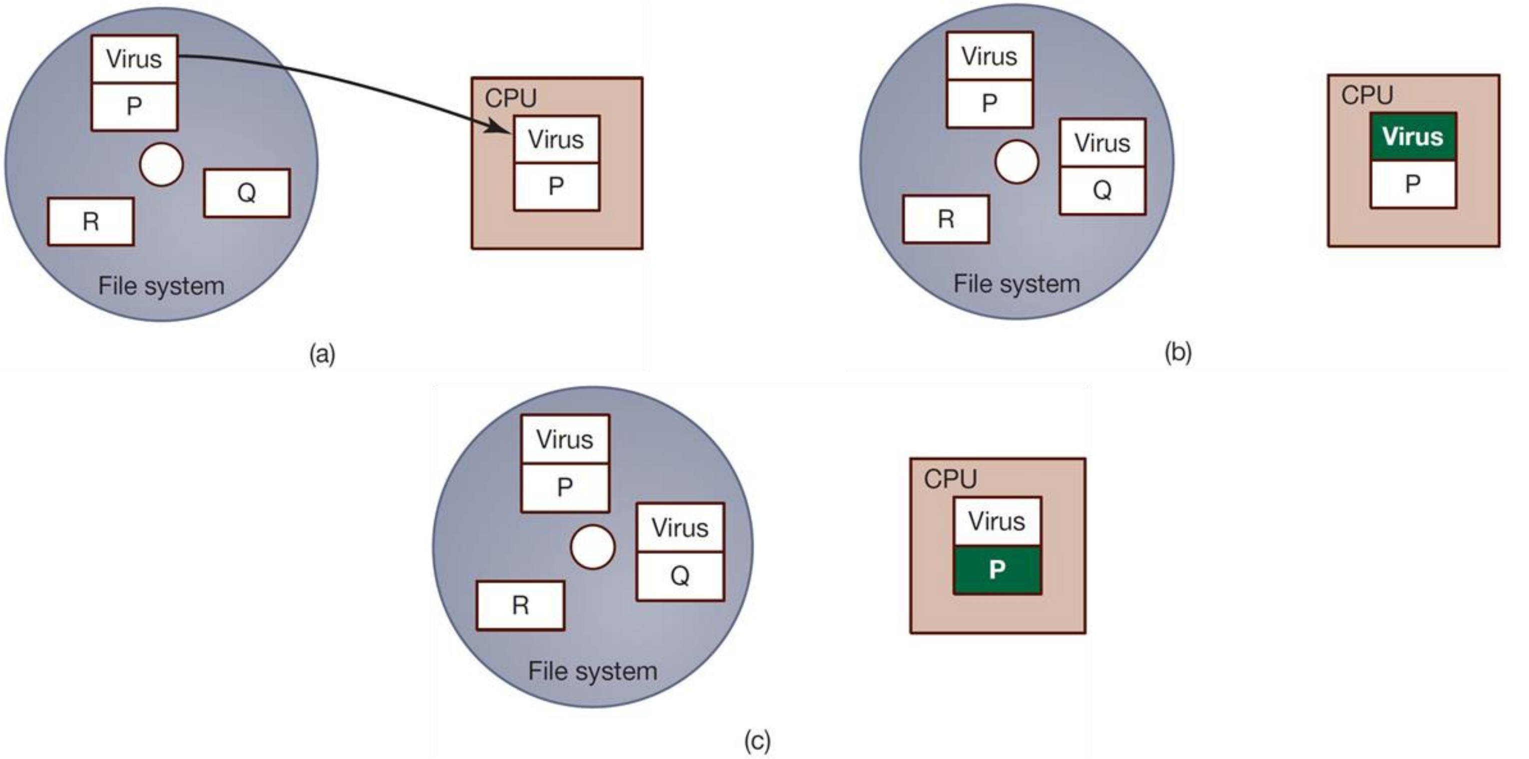
Pearson

7.3 Malware

Viruses

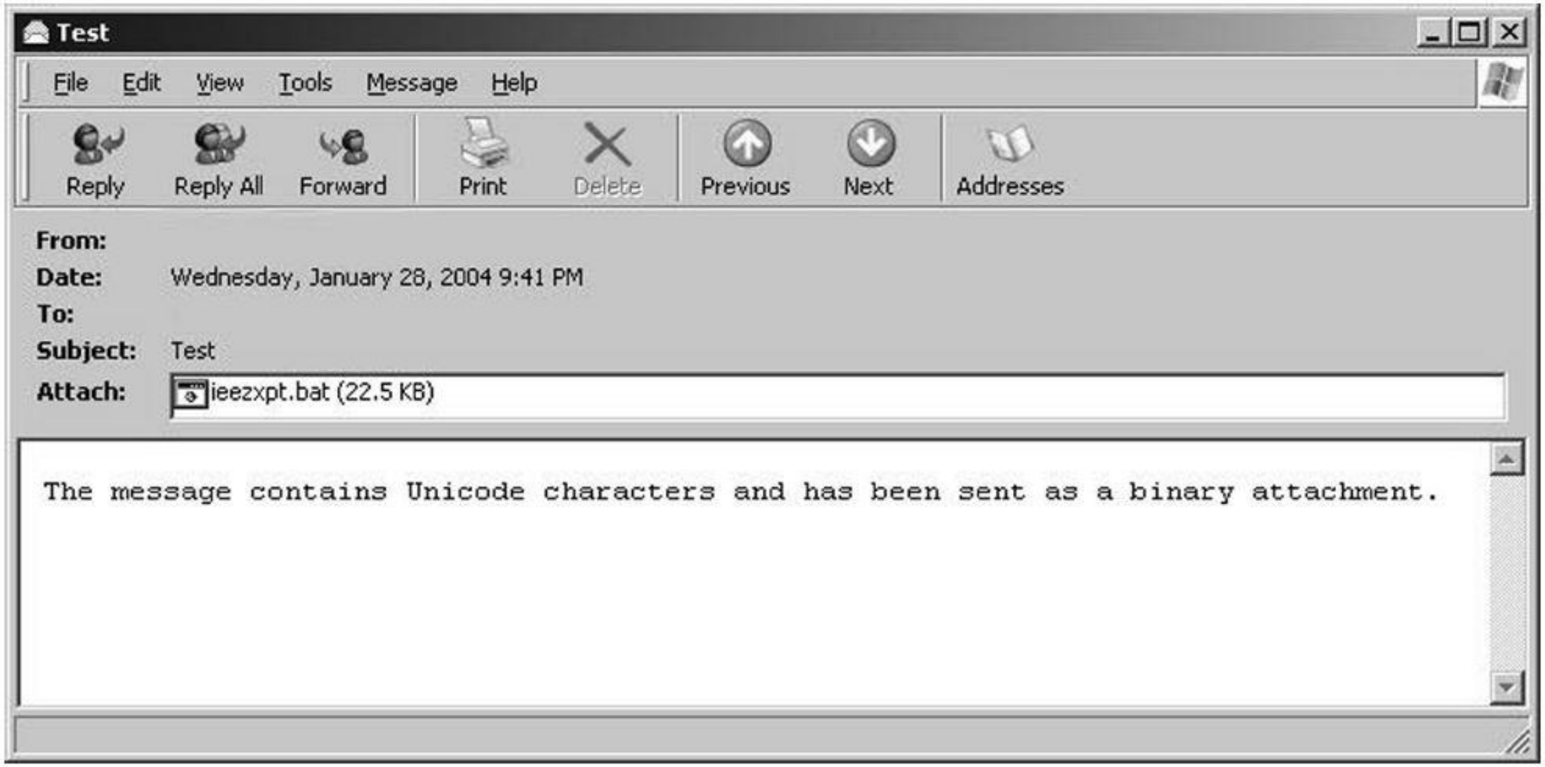
- **Virus: Piece of self-replicating code embedded within another program (host)**
- Viruses associated with program files
  - Hard disks, floppy disks, CD-ROMS
  - Email attachments
- How viruses spread
  - Diskettes or CDs
  - Email
  - Files downloaded from Internet

One Way a Virus Can Replicate



(a) A computer user executes program P, which is infected with a virus. (b) The virus code begins to execute. It finds another executable program Q and creates a new version of Q infected with the virus. (c) The virus passes control to program P. The user, who expected program P to execute, suspects nothing

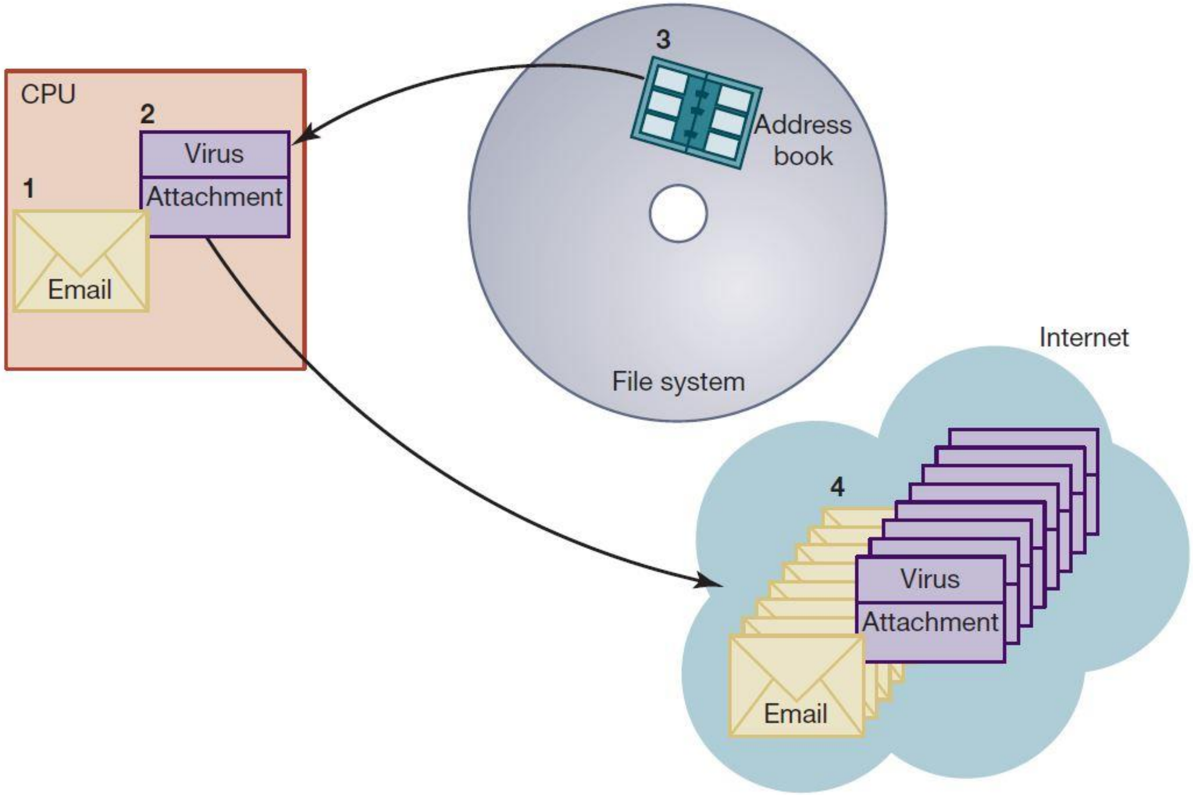
Email Attachment with Possible Virus



From:
Date: Wednesday, January 28, 2004 9:41 PM
To:
Subject: Test
Attach: ieezxpt.bat (22.5 KB)

```
The message contains Unicode characters and has been sent as a binary attachment.
```

How an Email Virus Spreads



A computer user reads an email with an attachment (1). The user opens the attachment, which contains a virus (2). The virus reads the user's email address book (3). The virus sends emails with virus-containing attachments (4).

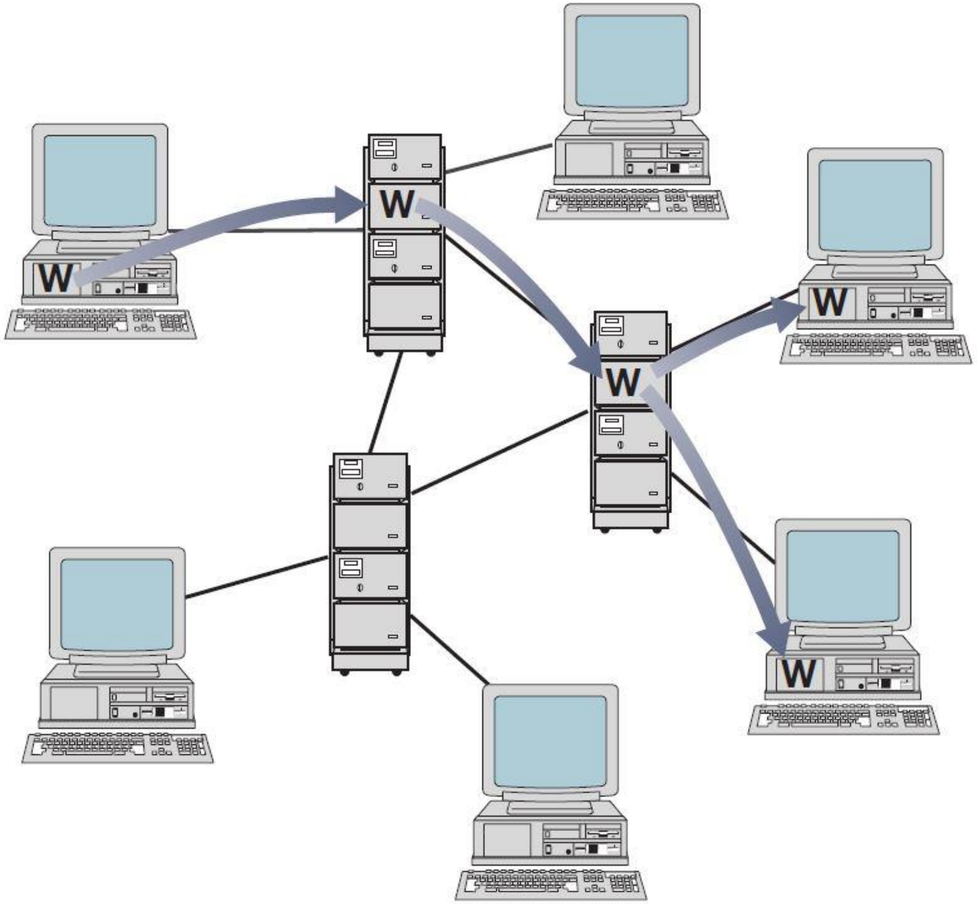
Antivirus Software Packages

- Allow computer users to detect and destroy viruses
- Must be kept up-to-date to be most effective
- Many people do not keep their antivirus software packages up-to-date
- Consumers need to beware of fake antivirus applications

Worm

- **Self-contained program**
- Spreads through a computer network
- Exploits security holes in networked computers

Worm Propagation



A worm spreads to other computers by exploiting security holes in computer networks.

The Internet Worm

- Robert Tappan Morris, Jr.
  - Graduate student at Cornell
  - Released worm onto Internet from MIT computer
- Effect of worm
  - Spread to significant numbers of Unix computers
  - Infected computers kept crashing or became unresponsive
  - Took a day for fixes to be published
- Impact on Morris
  - Suspended from Cornell
  - 3 years’ probation + 400 hours community service
  - $150,000 in legal fees and fines

Cross-Site Scripting

- Another way malware may be downloaded without user’s knowledge
- Problem appears on Web sites that allow people to read what others have posted
- **Attacker injects client-side script into a Web site**
- Victim’s browser executes script, which may steal cookies, track user’s activity, or perform another malicious action

Drive-By Downloads

- **Unintentional downloading of malware caused by visiting a compromised Web site**
- Also happens when Web surfer sees pop-up window asking permission to download software and clicks “Okay”
- Google Anti-Malware Team says 1.3 percent of queries to Google’s search engine return a malicious URL somewhere on results page

Trojan Horses and Backdoor Trojans

- **Trojan horse:** Program with benign capability that masks a sinister purpose
- **Backdoor Trojan:** Trojan horse that gives attack access to victim’s computer

Ransomware

- Definition: **Malware designed to extort money from victim**
- How installed
  - Drive-by download
  - Trojan Horse
  - Email attachment
  - Other means
- Early versions accused victims of illegal activities, demanded “fines”
- Modern versions encrypt all files on victim’s computer and demand payment in return for decryption key

Rootkits

- **Rootkit: A set of programs that provides privileged access to a computer**
- Activated every time computer is booted
- Uses security privileges to mask its presence

Spyware and Adware

- **Spyware: Program that communicates over an Internet connection without user's knowledge or consent**
  - Monitor Web surfing
  - Log keystrokes
  - Take snapshots of computer screen
  - Send reports back to host computer
- **Adware: Type of spyware that displays pop-up advertisements related to user's activity**
- Backdoor Trojans often used to deliver spyware and adware

Bots

- **Bot: A kind of backdoor Trojan that responds to commands sent by a command-and-control program on another computer**
- First bots supported legitimate activities
  - Internet Relay Chat
  - Multiplayer Internet games
- Other bots support illegal activities
  - Distributing spam
  - Collecting person information for ID theft
  - Denial-of-service attacks

Bots and Botnets

- **Botnet: Collection of bot-infected computers controlled by the same command-and-control program**
- Some botnets have over a million computers in them
- Bot herder: Someone who controls a botnet
- Uses of botnets
  - Distribute spam
  - Launch distributed denial-of-service attacks

Protecting Your Internet-Connected Devices

- Make sure you’ve installed latest security patches.
- Install anti-malware tools on your computer.
- Before buying an Internet-connected device, see if manufacturer is taking reasonable security precautions.
- Immediately change the default password of devices you connect to the Internet.
- Choose a different password for each of your devices.
- Consider replacing insecure Internet-of-Things devices.

Pearson

Security Risks of “Bring Your Own Device”

- 87% of US companies rely on employees accessing mobile business aps from their personal smartphones
- Benefits of “Bring Your Own Device”
  - Employers reduce hardware, software expenditures
  - Increased productivity and job satisfaction of employees
- Potential harms of “Bring Your Own Device”
  - Company data may be compromised if device stolen
  - Insecure device can make company vulnerable to data breach

“Bring Your Own Device” Policy Discussion

- What are the security standards for personal devices (password requirements, anti-malware packages, etc.)?
- What applications can employees run from their devices?
- What level of support will company’s I T department provide?
- Does the company have right to erase all data from a personal device that has been stolen?
- When employees leave company, how will company data be removed from their devices?

7.4 Cyber Crime and Cyber Attacks

Phishing and Spear-Phishing

- **Phishing: Large-scale effort to gain sensitive information from gullible computer users**
  - At least 124,000 phishing attacks globally in second half of 2014
  - New development: phishing attacks on Chinese e-commerce sites
- **Spear-phishing: Variant of phishing in which email addresses chosen selectively to target particular group of recipients**

SQL Injection

- Method of attacking a database-driven Web application with improper security
- Attack inserts (injects) SQL query into text string from client to application
- Application returns sensitive information

Denial-of-Service and Distributed Denial-of-Service Attacks

- **Denial-of-service attack: Intentional action designed to prevent legitimate users from making use of a computer service**
- Aim of a DoS attack is not to steal information but to disrupt a server's ability to respond to its clients
- **Distributed denial-of-service attack: DoS attack launched from many computers, such as a botnet**

Internet-of-Things Devices Co-opted for DDoS Attack

- DDoS attack of October 21, 2016 on domain name service provider Dyn
  - Netflix, Twitter, Spotify, Reddit, PayPal, Pinterest, CNN, Fox News, the Guardian, the New York Times, the Wall Street Journal unreachable for several hours
- Attack launched by Mirai botnet, perhaps 100,000 devices
  - Network routers
  - Security cameras
  - Baby monitors
- IoT devices easy to co-opt
  - Many people never change default passwords
  - Some devices have no password protection

Cyber Crime

- Criminal organizations making significant amounts of money from malware
- Jeanson James Ancheta
- Pharmamaster
- Albert Gonzalez
- Avalanche Gang

Attacks on Twitter and Other Social Networking Sites

- Massive DDoS attack made Twitter service unavailable for several hours on August 6, 2009
- Three other sites attacked at same time: Facebook, LiveJournal, and Google
- All sites used by a political blogger from the Republic of Georgia
- Attacks occurred on first anniversary of war between Georgia and Russia over South Ossetia

Fourth of July Attacks

- 4th of July weekend in 2009: DDoS attack on governmental agencies and commercial Web sites in United States and South Korea
- Attack may have been launched by North Korea in retaliation for United Nations sanctions عقوبات

Supervisory Control and Data Acquisition (SCADA) Systems

- Industrial processes require constant monitoring
- Computers allow automation and centralization of monitoring
- Today, SCADA systems are open systems based on Internet Protocol
  - Less expensive than proprietary systems
  - Easier to maintain than proprietary systems
  - Allow remote diagnostics
- Allowing remote diagnostics creates security risk

SCADA Systems Carry Security Risks

Internet-based supervisory control and data acquisition (SCADA) systems can save money and make systems easier to administer, but they also carry security risks. (Dave and Les Jacobs/Kolostock/Blend Images)

Stuxnet Worm (2009)

- Attacked SCADA systems running Siemens software
- Targeted five industrial facilities in Iran that were using centrifuges to enrich uranium
- Caused temporary shutdown of Iran's nuclear program
- United States and Israel cooperated to develop and launch the worm

Cyber Espionage Attributed to People’s Liberation Army

- Hundreds of computer security breaches over a decade in more than a dozen countries investigated by Mandiant
- Hundreds of terabytes of data stolen
- Mandiant blamed Unit 61398 of the People’s Liberation Army
- China’s foreign ministry stated that accusation was groundless and irresponsible
- US government disclosed in 2015 that SSNs and other personal information from 22 million Americans stolen from Office of Personnel Management computers
- Prime suspect: Unit 61398 of People’s Liberation Army

Anonymous

- **Anonymous: loosely organized international movement of hacktivists (hackers with a social or political cause)**
- Various DDoS attacks attributed to Anonymous members

Actions Attributed to Anonymous

Year	Victim	Reason
2008	Church of Scientology	Attempted suppression of Tom Cruise interview
2009	RIAA, MPAA	RIAA, MPAA’s attempt to take down the Pirate Bay
2009	PayPal, VISA, MasterCard	Financial organizations freezing funds flowing to Julian Assange of WikiLeaks
2012	U.S. Dept. of Justice, RIAA, MPAA	U.S. Dept. of Justice action against Megaupload
2013	Israel	Protest Israeli treatment of Palestinians
2014	City of Cleveland	Protest killing of 12-year-old Tamir Rice by a Cleveland police officer
2015	Jihadist groups	Terrorist attack on Paris office of Charlie Hebdo magazine

Convictions of Anonymous Members

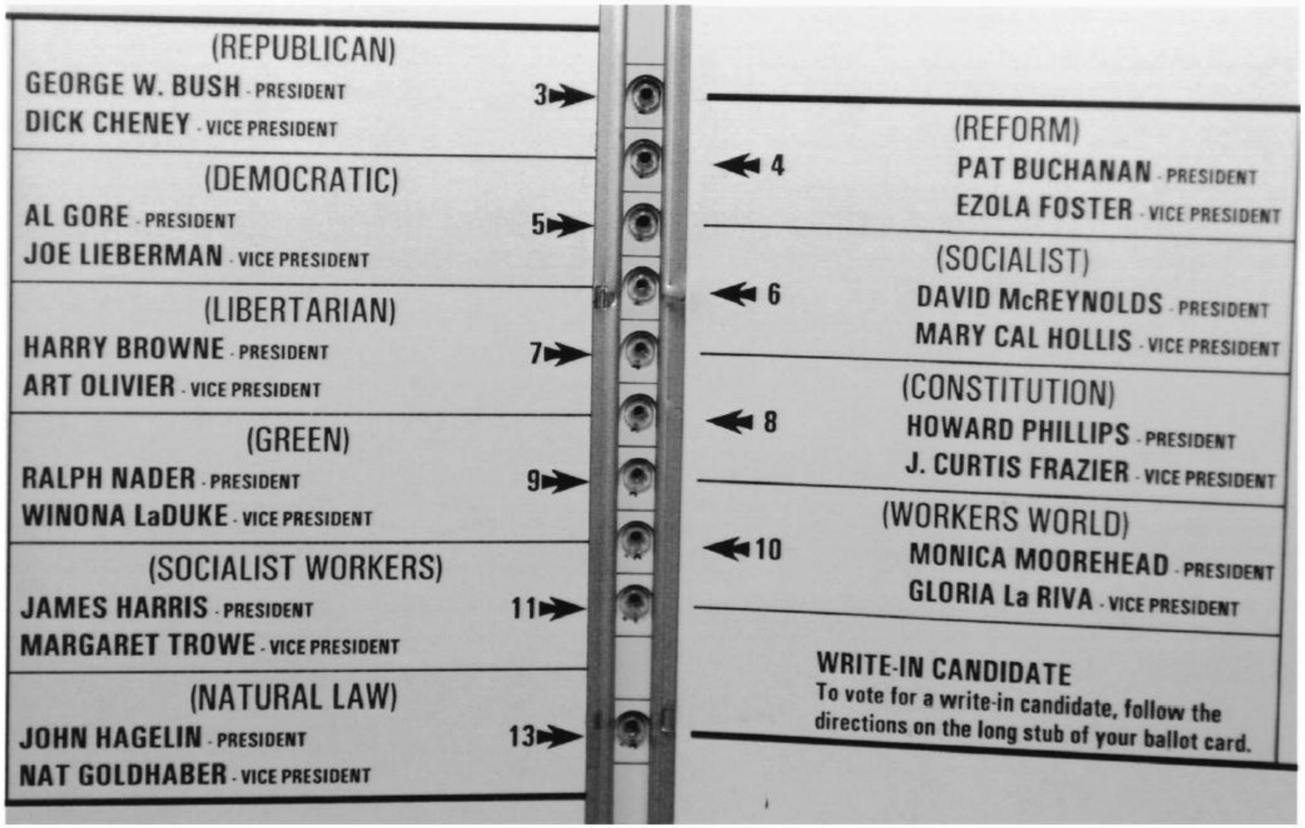
- Dozens of people around the world have been arrested for participation in Anonymous cyber attacks
- Dmitriy Guzner (Church of Scientology attacks): 366 days in prison and $37,500 in restitution
- Brian Mettenbrink (Church of Scientology attacks): 1 year in prison and $20,000 in restitution
- Jake Davis (Sony Pictures attacks): 2 years in prison

7.5 Online Voting

Motivation for Online Voting

- 2000 U.S. Presidential election closely contested
- Florida pivotal state
- Most Florida counties used keypunch voting machines
- Two voting irregularities traced to these machines
  - Hanging chad
  - “Butterfly ballot” in Palm Beach County

The Infamous “Butterfly Ballot”



(REPUBLICAN)
GEORGE W. BUSH - PRESIDENT
DICK CHENEY - VICE PRESIDENT
3 →

(DEMOCRATIC)
AL GORE - PRESIDENT
JOE LIEBERMAN - VICE PRESIDENT
5 →

(LIBERTARIAN)
HARRY BROWNE - PRESIDENT
ART OLIVIER - VICE PRESIDENT
7 →

(GREEN)
RALPH NADER - PRESIDENT
WINONA LaDUKE - VICE PRESIDENT
9 →

(SOCIALIST WORKERS)
JAMES HARRIS - PRESIDENT
MARGARET TROWE - VICE PRESIDENT
11 →

(NATURAL LAW)
JOHN HAGELIN - PRESIDENT
NAT GOLDHABER - VICE PRESIDENT
13 →

← 4
(REFORM)
PAT BUCHANAN - PRESIDENT
EZOLA FOSTER - VICE PRESIDENT

← 6
(SOCIALIST)
DAVID McREYNOLDS - PRESIDENT
MARY CAL HOLLIS - VICE PRESIDENT

← 8
(CONSTITUTION)
HOWARD PHILLIPS - PRESIDENT
J. CURTIS FRAZIER - VICE PRESIDENT

← 10
(WORKERS WORLD)
MONICA MOOREHEAD - PRESIDENT
GLORIA La RIVA - VICE PRESIDENT

WRITE-IN CANDIDATE
To vote for a write-in candidate, follow the directions on the long stub of your ballot card.

The layout of the “butterfly ballot” apparently led thousands of Palm Beach County, Florida, voters supporting candidate Al Gore to punch the hole associated with Pat Buchanan by mistake. (AP Photo/Gary I. Rothstein)

Benefits of Online Voting

- More people would vote
- Votes would be counted more quickly
- No ambiguity with electronic votes
- Cost less money
- Eliminate ballot box tamperingالعبث
- Software can prevent accidental over-voting
- Software can prevent under-voting

Risks of Online Voting

- Gives unfair advantage to those with home computers
- More difficult to preserve voter privacy
- More opportunities for vote selling
- Obvious target for a DDoS attack
- Security of election depends on security of home computers
- Susceptible to vote-changing virus or remote access Trojan
- Susceptible to phonyالزائفة vote servers
- No paper copies of ballots for auditing or recounts

Conclusions

- Existing systems are highly localized
- Widespread tainting more possible with online system
- No paper records with online system
- Evidence of tampering with online elections
- Relying on security of home computers means system vulnerable to fraud
- All in all, strong case for not allowing online voting

Copyright

This work is protected by United States copyright laws and is provided solely for the use of instructors in teaching their courses and assessing student learning. Dissemination or sale of any part of this work (including on the World Wide Web) will destroy the integrity of the work and is not permitted. The work and materials from it should never be made available to students except by instructors using the accompanying text in their classes. All recipients of this work are expected to abide by these restrictions and to honor the intended pedagogical purposes and the needs of other instructors who rely on these materials.