

Information security - Wikipedia (Series)

Contents

1	Information security	1
1.1	Overview	1
1.1.1	Threats	1
1.2	History	2
1.3	Definitions	3
1.4	Employment	4
1.5	Basic principles	4
1.5.1	Key concepts	4
1.6	Risk management	5
1.6.1	Controls	7
1.6.2	Defense in depth	8
1.6.3	Security classification for information	9
1.6.4	Access control	9
1.6.5	Cryptography	10
1.7	Process	11
1.7.1	Security governance	11
1.7.2	Incident response plans	12
1.7.3	Change management	12
1.8	Business continuity	14
1.9	Laws and regulations	14
1.10	Information security culture	16
1.11	Sources of standards	16
1.12	Scholars working in the field	17
1.13	See also	18
1.14	Further reading	19
1.14.1	Bibliography	19
1.15	References	19
1.16	External links	21
2	Internet security	22
2.1	Threats	22
2.1.1	Malicious software	22
2.1.2	Denial-of-service attacks	23

2.1.3 Phishing	23
2.1.4 Application vulnerabilities	23
2.2 Remedies	23
2.2.1 Network layer security	23
2.2.2 Internet Protocol Security (IPsec)	23
2.2.3 Security token	24
2.2.4 Electronic mail security	24
2.2.5 Firewalls	25
2.2.6 Browser choice	25
2.3 Internet security products	25
2.3.1 Antivirus	26
2.3.2 Password managers	26
2.3.3 Security suites	26
2.4 See also	26
2.5 References	26
2.6 External links	27
3 Cyberwarfare	28
3.1 Definition	28
3.2 Types of threat	28
3.2.1 Espionage	29
3.2.2 Sabotage	29
3.3 Motivations	30
3.3.1 Military	30
3.3.2 Civil	30
3.3.3 Hacktivism	31
3.3.4 Private sector	31
3.3.5 Non-profit research	31
3.4 By region	31
3.4.1 Asia	31
3.4.2 Europe	34
3.4.3 Middle East	35
3.4.4 North America	36
3.5 Cyberpeace	38
3.6 Cyber counterintelligence	38
3.7 Controversy over terms	39
3.8 Legality, rules	40
3.9 In films	40
3.10 See also	40
3.11 References	41
3.12 External links	48

4 Computer security	49
4.1 Vulnerabilities and attacks	49
4.1.1 Backdoor	49
4.1.2 Denial-of-service attack	49
4.1.3 Direct-access attacks	50
4.1.4 Eavesdropping	50
4.1.5 Spoofing	50
4.1.6 Tampering	50
4.1.7 Privilege escalation	50
4.1.8 Phishing	50
4.1.9 Clickjacking	50
4.1.10 Social engineering	51
4.2 Information security culture	51
4.3 Systems at risk	51
4.3.1 Financial systems	51
4.3.2 Utilities and industrial equipment	52
4.3.3 Aviation	52
4.3.4 Consumer devices	52
4.3.5 Large corporations	52
4.3.6 Automobiles	52
4.3.7 Government	53
4.3.8 Internet of things and physical vulnerabilities	53
4.4 Impact of security breaches	53
4.5 Attacker motivation	54
4.6 Computer protection (countermeasures)	54
4.6.1 Security by design	54
4.6.2 Security architecture	55
4.6.3 Security measures	55
4.6.4 Vulnerability management	55
4.6.5 Reducing vulnerabilities	56
4.6.6 Hardware protection mechanisms	56
4.6.7 Secure operating systems	57
4.6.8 Secure coding	57
4.6.9 Capabilities and access control lists	57
4.6.10 Response to breaches	58
4.7 Notable attacks and breaches	58
4.7.1 Robert Morris and the first computer worm	58
4.7.2 Rome Laboratory	58
4.7.3 TJX customer credit card details	58
4.7.4 Stuxnet attack	59
4.7.5 Global surveillance disclosures	59

4.7.6	Target and Home Depot breaches	59
4.7.7	Office of Personnel Management data breach	59
4.7.8	Ashley Madison breach	59
4.8	Legal issues and global regulation	60
4.9	Role of government	60
4.10	International actions	60
4.10.1	Europe	60
4.11	National actions	61
4.11.1	Computer emergency response teams	61
4.11.2	Canada	61
4.11.3	China	61
4.11.4	Germany	61
4.11.5	India	62
4.11.6	Portugal	62
4.11.7	Pakistan	62
4.11.8	South Korea	62
4.11.9	United States	62
4.12	Modern warfare	63
4.13	Job market	64
4.14	Terminology	65
4.15	Scholars	66
4.16	See also	67
4.17	References	69
4.18	Further reading	75
4.19	External links	76
5	Mobile security	77
5.1	Challenges of mobile security	77
5.1.1	Threats	77
5.1.2	Consequences	78
5.2	Attacks based on communication	78
5.2.1	Attack based on SMS and MMS	79
5.2.2	Attacks based on communication networks	79
5.3	Attacks based on vulnerabilities in software applications	81
5.3.1	Web browser	81
5.3.2	Operating system	81
5.4	Attacks based on hardware vulnerabilities	81
5.4.1	Electromagnetic Waveforms	82
5.4.2	Juice Jacking	82
5.5	Password cracking	82
5.6	Malicious software (malware)	82
5.6.1	The three phases of malware attacks	82

5.6.2 Examples of malware	83
5.6.3 Portability of malware across platforms	85
5.7 Countermeasures	85
5.7.1 Security in operating systems	86
5.7.2 Security software	86
5.7.3 Resource monitoring in the smartphone	87
5.7.4 Network surveillance	87
5.7.5 Manufacturer surveillance	88
5.7.6 User awareness	89
5.7.7 Centralized storage of text messages	89
5.7.8 Limitations of certain security measures	89
5.7.9 Next Generation of mobile security	90
5.8 See also	90
5.9 Notes	91
5.10 References	93
5.10.1 Books	93
5.10.2 Articles	93
5.10.3 Websites	94
5.11 Further reading	94
6 Network security	96
6.1 Network Security concept	96
6.2 Security managements	97
6.2.1 Types of Attacks	97
6.3 See also	97
6.4 References	98
6.5 Further reading	98
7 Cybercrime	100
7.1 Classification	100
7.1.1 Fraud and financial crimes	100
7.1.2 Cyberterrorism	101
7.1.3 Cyberextortion	101
7.1.4 Cyberwarfare	101
7.1.5 Computer as a target	101
7.1.6 Computer as a tool	102
7.2 Documented cases	104
7.3 Combating computer crime	105
7.3.1 Diffusion of cybercrime	105
7.3.2 Investigation	105
7.3.3 Legislation	105
7.3.4 Penalties	106

7.3.5 Awareness	106
7.4 Agencies	106
7.5 See also	106
7.6 References	107
7.7 Further reading	109
7.8 External links	110
7.8.1 Government resources	110
8 Vulnerability (computing)	111
8.1 Definitions	111
8.2 Vulnerability and risk factor models	113
8.3 Information security management system	113
8.4 Classification	113
8.5 Causes	114
8.6 Vulnerability consequences	115
8.7 Vulnerability disclosure	115
8.7.1 Vulnerability inventory	116
8.8 Vulnerability disclosure date	116
8.9 Identifying and removing vulnerabilities	116
8.10 Examples of vulnerabilities	116
8.10.1 Software vulnerabilities	117
8.11 See also	118
8.12 References	118
8.13 External links	119
9 Eavesdropping	120
9.1 Etymology	120
9.2 Techniques	121
9.3 Network attacks	121
9.4 See also	121
9.5 References	122
9.6 External links	122
10 Exploit (computer security)	123
10.1 Classification	123
10.1.1 Types	123
10.1.2 Pivoting	123
10.2 See also	124
10.3 Notes	124
10.4 References	124
11 Trojan horse (computing)	125
11.1 Destructive	125

11.2 Use of resources or identity	125
11.3 Money theft, ransom	126
11.4 Data theft	126
11.5 Spying, surveillance or stalking	126
11.6 Operation of a Trojan horse	126
11.7 Notable examples	127
11.7.1 Private and governmental	127
11.7.2 Publicly available	127
11.7.3 Detected by security researchers	127
11.8 See also	128
11.9 References	128
11.10 External links	129
12 Computer virus	130
12.1 Historical development	131
12.1.1 Early academic work on self-replicating programs	131
12.1.2 First examples	131
12.2 Operations and functions	133
12.2.1 Parts	133
12.2.2 Phases	133
12.3 Infection targets and replication techniques	134
12.3.1 Resident vs. non-resident viruses	134
12.3.2 Macro viruses	134
12.3.3 Boot sector viruses	134
12.3.4 Email virus	134
12.4 Stealth strategies	134
12.4.1 Read request intercepts	135
12.4.2 Self-modification	135
12.5 Vulnerabilities and infection vectors	136
12.5.1 Software bugs	136
12.5.2 Social engineering and poor security practices	136
12.5.3 Vulnerability of different operating systems	137
12.6 Countermeasures	137
12.6.1 Antivirus software	137
12.6.2 Recovery strategies and methods	138
12.6.3 Viruses and the Internet	139
12.7 See also	140
12.8 References	140
12.9 Further reading	144
12.10 External links	144
13 Computer worm	145

13.1 History	145
13.2 Harm	146
13.3 Countermeasures	146
13.4 Worms with good intent	148
13.5 See also	148
13.6 References	149
13.7 External links	149
14 Denial-of-service attack	150
14.1 History	150
14.2 Types	150
14.2.1 Distributed DoS	150
14.2.2 Application layer attacks	152
14.2.3 Advanced persistent DoS	152
14.2.4 Denial-of-service as a service	153
14.3 Symptoms	153
14.4 Attack techniques	153
14.4.1 Attack tools	154
14.4.2 Application-layer floods	154
14.4.3 Degradation-of-service attacks	154
14.4.4 Denial-of-service Level II	154
14.4.5 Distributed DoS attack	155
14.4.6 DDoS extortion	155
14.4.7 HTTP POST DoS attack	156
14.4.8 Internet Control Message Protocol (ICMP) flood	156
14.4.9 Nuke	156
14.4.10 Peer-to-peer attacks	156
14.4.11 Permanent denial-of-service attacks	157
14.4.12 Reflected / spoofed attack	157
14.4.13 R-U-Dead-Yet? (RUDY)	157
14.4.14 Shrew attack	158
14.4.15 Slow Read attack	158
14.4.16 Sophisticated low-bandwidth Distributed Denial-of-Service Attack	158
14.4.17 (S)SYN flood	158
14.4.18 Teardrop attacks	158
14.4.19 Telephony denial-of-service (TDoS)	158
14.5 Defense techniques	159
14.5.1 Application front end hardware	159
14.5.2 Application level Key Completion Indicators	159
14.5.3 Blackholing and sinkholing	160
14.5.4 IPS based prevention	160
14.5.5 DDS based defense	160

14.5.6 Firewalls	160
14.5.7 Routers	160
14.5.8 Switches	160
14.5.9 Upstream filtering	161
14.6 Unintentional denial-of-service	161
14.7 Side effects of attacks	162
14.7.1 Backscatter	162
14.8 Legality	162
14.9 See also	163
14.10 References	164
14.11 Further reading	167
14.12 External links	167
15 Malware	168
15.1 Purposes	168
15.2 Infectious malware	169
15.3 Concealment	170
15.3.1 Viruses	170
15.3.2 Trojan horses	170
15.3.3 Rootkits	170
15.3.4 Backdoors	170
15.3.5 Evasion	171
15.4 Vulnerability	171
15.4.1 Security defects in software	171
15.4.2 Insecure design or user error	172
15.4.3 Over-privileged users and over-privileged code	172
15.4.4 Use of the same operating system	172
15.5 Anti-malware strategies	173
15.5.1 Anti-virus and anti-malware software	173
15.5.2 Website security scans	173
15.5.3 “Air gap” isolation or “Parallel Network”	174
15.6 Grayware	174
15.7 History of viruses and worms	174
15.8 Academic research	175
15.9 See also	175
15.10 References	175
15.11 External links	178
16 Payload (computing)	179
16.1 Security	179
16.2 Programming	179
16.3 Networks	179

16.4 See also	179
16.5 References	179
17 Rootkit	181
17.1 History	181
17.1.1 Sony BMG copy protection rootkit scandal	182
17.1.2 Greek wiretapping case 2004–05	182
17.2 Uses	183
17.3 Types	183
17.3.1 User mode	184
17.3.2 Kernel mode	185
17.3.3 Hypervisor level	185
17.3.4 Firmware and hardware	186
17.4 Installation and cloaking	186
17.5 Detection	187
17.5.1 Alternative trusted medium	187
17.5.2 Behavioral-based	187
17.5.3 Signature-based	187
17.5.4 Difference-based	188
17.5.5 Integrity checking	188
17.5.6 Memory dumps	188
17.6 Removal	188
17.7 Public availability	190
17.8 Defenses	190
17.9 See also	190
17.10 Notes	190
17.11 References	190
17.12 Further reading	194
17.13 External links	194
18 Keystroke logging	195
18.1 Application	195
18.1.1 Software-based keyloggers	196
18.1.2 Hardware-based keyloggers	198
18.2 History	200
18.3 Cracking	200
18.3.1 Trojans	200
18.3.2 Use by police	201
18.4 Countermeasures	201
18.4.1 Anti keyloggers	201
18.4.2 Live CD/USB	201
18.4.3 Anti-spyware / Anti-virus programs	201

18.4.4 Network monitors	202
18.4.5 Automatic form filler programs	202
18.4.6 One-time passwords (OTP)	202
18.4.7 Security tokens	202
18.4.8 On-screen keyboards	202
18.4.9 Keystroke interference software	202
18.4.10 Speech recognition	203
18.4.11 Handwriting recognition and mouse gestures	203
18.4.12 Macro expanders/recorders	203
18.4.13 Deceptive typing	203
18.5 See also	203
18.6 References	204
18.7 External links	205
19 Computer access control	206
19.1 Services	206
19.2 Authorization	206
19.3 Identification and Authentication (I&A)	207
19.4 Access approval	207
19.5 Accountability	208
19.6 Access control models	208
19.6.1 Discretionary access control	208
19.6.2 Mandatory access control	208
19.6.3 Role-based access control	209
19.6.4 Intent-based Access Control (IBAC)	209
19.6.5 Emotion-based Access Control (EBAC)	210
19.6.6 Attribute-based access control	210
19.6.7 Break-Glass Access Control Models	210
19.6.8 Access control based on the responsibility	210
19.6.9 Host-based access control (HBAC)	211
19.7 References	211
20 Application security	212
20.1 Terms	212
20.2 Techniques	212
20.3 Application threats / attacks	213
20.4 Mobile application security	213
20.5 Security testing for applications	213
20.6 Security standards and regulations	214
20.7 See also	214
20.8 References	215
20.9 External links	215

21 Antivirus software	216
21.1 History	217
21.1.1 1949–1980 period (pre-antivirus days)	217
21.1.2 1980–1990 period (early days)	217
21.1.3 1990–2000 period (emergence of the antivirus industry)	218
21.1.4 2000–2005 period	219
21.1.5 2005 to 2014 period	219
21.1.6 2014 to present (rise of next-gen)	219
21.2 Identification methods	220
21.2.1 Signature-based detection	220
21.2.2 Heuristics	220
21.2.3 Rootkit detection	220
21.2.4 Real-time protection	221
21.3 Issues of concern	221
21.3.1 Unexpected renewal costs	221
21.3.2 Rogue security applications	221
21.3.3 Problems caused by false positives	221
21.3.4 System and interoperability related issues	222
21.3.5 Effectiveness	222
21.3.6 New viruses	222
21.3.7 Rootkits	223
21.3.8 Damaged files	223
21.3.9 Firmware issues	223
21.4 Performance and other drawbacks	223
21.5 Alternative solutions	223
21.5.1 Hardware and network firewall	223
21.5.2 Cloud antivirus	224
21.5.3 Online scanning	224
21.5.4 Specialist tools	225
21.6 Usage and risks	225
21.7 See also	225
21.8 References	226
21.9 Bibliography	232
21.10 External links	232
22 Secure coding	233
22.1 Buffer Overflow Prevention	233
22.2 Format String Attack Prevention	233
22.3 Integer Overflow Prevention	234
22.4 See also	234
22.5 References	234
22.6 External links	234

23 Secure by design	235
23.1 Security by design in practice	235
23.2 Server/client architectures	236
23.3 See also	236
23.4 External links	236
24 Security-focused operating system	237
24.1 Linux	237
24.1.1 openSUSE	237
24.1.2 Debian	237
24.1.3 Fedora	238
24.1.4 Arch and Gentoo related	238
24.1.5 Mobile	239
24.1.6 Independent	239
24.2 BSD	240
24.2.1 Anonym.OS	240
24.2.2 OpenBSD	240
24.2.3 TrustedBSD	240
24.2.4 HardenedBSD	240
24.3 Solaris	241
24.3.1 Trusted Solaris	241
24.3.2 Solaris 10 and trusted functionality	241
24.4 Microsoft Windows Server	241
24.5 Object-capability systems	241
24.6 See also	241
24.7 References	242
24.8 External links	243
25 Authentication	244
25.1 Methods	244
25.2 Factors and identity	246
25.2.1 Types	246
25.3 Digital authentication	248
25.4 Product authentication	249
25.4.1 Packaging	250
25.5 Information content	250
25.5.1 Factual verification	251
25.5.2 Video authentication	251
25.5.3 Literacy and literature authentication	251
25.6 History and state-of-the-art	251
25.7 Authorization	252
25.8 Access control	253

25.9 See also	254
25.10 References	255
25.11 External links	256
26 Multi-factor authentication	257
26.1 Authentication factors	257
26.1.1 Knowledge factors	257
26.1.2 Possession factors	258
26.1.3 Inherence factors	258
26.2 Mobile phone two-factor authentication	259
26.2.1 Advances in mobile two-factor authentication	260
26.3 Legislation	260
26.3.1 United States	260
26.4 Security	260
26.5 Industry regulation	261
26.5.1 Payment Card Industry Data Security Standard (PCI-DSS)	261
26.6 Implementation considerations	261
26.7 Examples	261
26.8 See also	261
26.9 References	262
26.10 Further reading	263
26.11 External links	263
27 Authorization	264
27.1 Overview	264
27.2 Related interpretations	265
27.2.1 Public policy	265
27.2.2 Banking	265
27.2.3 Publishing	265
27.3 See also	265
28 Data-centric security	266
28.1 Key concepts	266
28.2 Technology	266
28.2.1 Data access controls and policies	267
28.2.2 Encryption	267
28.2.3 Data masking	267
28.2.4 Auditing	267
28.3 Cloud computing	267
28.3.1 Data-centric security in the public cloud environments	267
28.4 See also	268
28.5 References	268

29 Firewall (computing)	269
29.1 History	269
29.1.1 First generation: packet filters	269
29.1.2 Second generation: “stateful” filters	270
29.1.3 Third generation: application layer	271
29.2 Types	271
29.2.1 Network layer or packet filters	272
29.2.2 Application-layer	272
29.2.3 Proxies	273
29.2.4 Network address translation	273
29.3 See also	273
29.4 References	274
29.5 External links	275
30 Intrusion detection system	276
30.1 Comparison with firewalls	276
30.2 Classifications	276
30.2.1 Analyzed activity	276
30.2.2 Detection method	277
30.3 Intrusion prevention	277
30.3.1 Classification	278
30.3.2 Detection methods	278
30.4 Limitations	278
30.5 Evasion techniques	279
30.6 Development	279
30.7 Free and open source systems	280
30.8 See also	281
30.9 References	281
30.10 Further reading	283
30.11 External links	283
31 Mobile secure gateway	284
31.1 Client library	284
31.2 Gateway	284
31.3 Host	284
31.4 References	284
31.5 External links	285
31.6 Text and image sources, contributors, and licenses	286
31.6.1 Text	286
31.6.2 Images	301
31.6.3 Content license	304

Chapter 1

Information security

Information security, sometimes shortened to **InfoSec**, is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of **information**. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical).^{*[1]}

1.1 Overview

IT security Sometimes referred to as **computer security**, information technology security (IT security) is information security applied to technology (most often some form of computer system). It is worthwhile to note that a **computer** does not necessarily mean a home desktop. A computer is any device with a **processor** and some **memory**. Such devices can range from non-networked standalone devices as simple as calculators, to networked mobile computing devices such as smartphones and tablet computers. IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the **technology** within the company secure from malicious cyber attacks that often attempt to breach into critical private information or gain control of the internal systems.

Information assurance The act of providing trust of the information, that the Confidentiality, Integrity and Availability (CIA) of the information are not violated, e.g. ensuring that **data** is not lost when critical issues arise. These issues include, but are not limited to: natural disasters, computer/server malfunction or physical theft. Since most information is stored on computers in our modern era, information assurance is typically dealt with by IT security specialists. A common method of providing information assurance is to have an off-site backup of the data in case one of the mentioned issues arise.

1.1.1 Threats

Information security threats come in many different forms. Some of the most common threats today are software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion. Most people have experienced software attacks of some sort. Viruses,^{*[2]} worms, phishing attacks, and Trojan horses are a few common examples of software attacks. The theft of intellectual property has also been an extensive issue for many businesses in the IT field. **Identity theft** is the attempt to act as someone else usually to obtain that person's personal information or to take advantage of their access to vital information. Theft of equipment or information is becoming more prevalent today due to the fact that most devices today are mobile. **Cell phones** are prone to theft and have also become far more desirable as the amount of data capacity increases. **Sabotage** usually consists of the destruction of an organization's website in an attempt to cause loss of confidence on the part of its customers. Information extortion consists of theft of a company's property or information as an attempt to receive a payment in exchange for returning the information or property back to its owner, as with **ransomware**. There are many ways to help protect yourself from some of these attacks but one of the most functional precautions is user carefulness.

Governments, military, corporations, financial institutions, hospitals and private businesses amass a great deal of confidential information about their employees, customers, products, research and financial status. Most of this

information is now collected, processed and stored on electronic computers and transmitted across networks to other computers.

Should confidential information about a business' customers or finances or new product line fall into the hands of a competitor or a black hat hacker, a business and its customers could suffer widespread, irreparable financial loss, as well as damage to the company's reputation. From a business perspective, information security must be balanced against cost; the **Gordon-Loeb Model** provides a mathematical economic approach for addressing this concern.*[3]

For the individual, information security has a significant effect on **privacy**, which is viewed very differently in various cultures.

The field of information security has grown and evolved significantly in recent years. It offers many areas for specialization, including securing networks and allied **infrastructure**, securing applications and databases, security testing, information systems auditing, business continuity planning and **digital forensics**.

Responses to threats

Possible responses to a security threat or **risk** are:*[4]

- reduce/mitigate – implement safeguards and countermeasures to eliminate vulnerabilities or block threats
- assign/transfer – place the cost of the threat onto another entity or organization such as purchasing insurance or outsourcing
- accept – evaluate if cost of countermeasure outweighs the possible cost of loss due to threat
- ignore/reject – not a valid or prudent due-care response

1.2 History

Since the early days of communication, diplomats and military commanders understood that it was necessary to provide some mechanism to protect the confidentiality of correspondence and to have some means of detecting tampering. Julius Caesar is credited with the invention of the **Caesar cipher** c. 50 B.C., which was created in order to prevent his secret messages from being read should a message fall into the wrong hands, but for the most part protection was achieved through the application of procedural handling controls.*[5]*[6] Sensitive information was marked up to indicate that it should be protected and transported by trusted persons, guarded and stored in a secure environment or strong box. As postal services expanded, governments created official organizations to intercept, decipher, read and reseal letters (e.g. the UK Secret Office and Deciphering Branch in 1653).

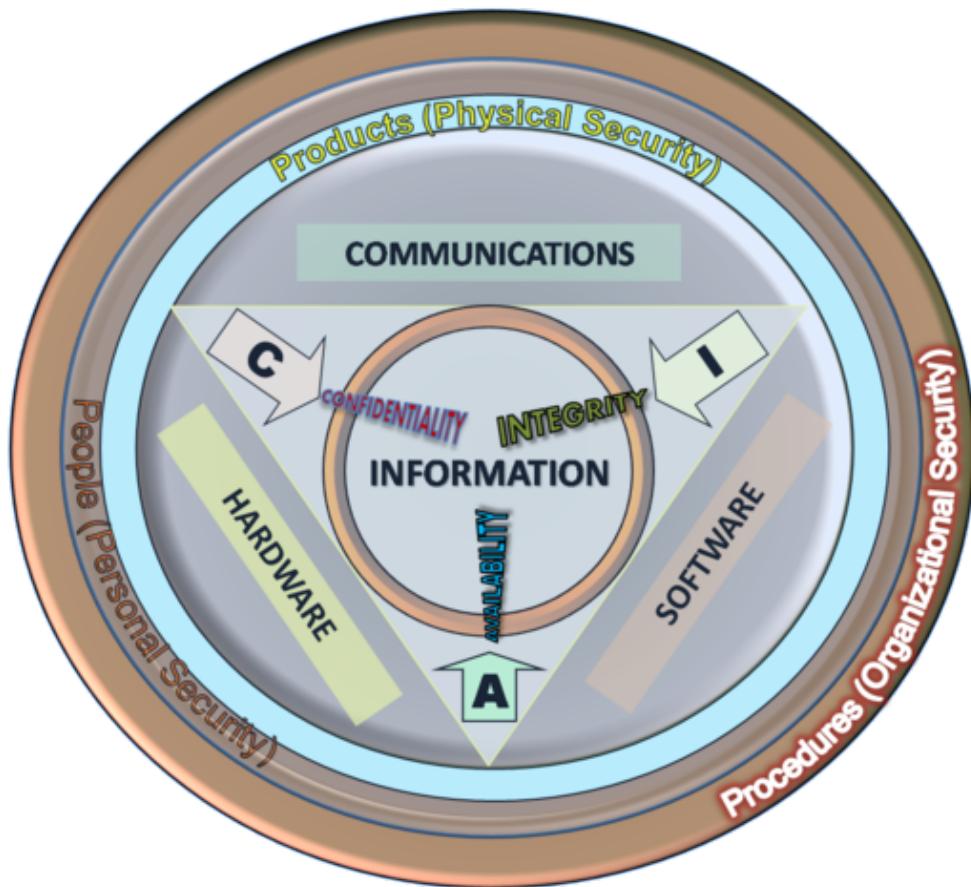
In the mid-19th century more complex **classification systems** were developed to allow governments to manage their information according to the degree of sensitivity. The British Government codified this, to some extent, with the publication of the **Official Secrets Act** in 1889. By the time of the **First World War**, multi-tier classification systems were used to communicate information to and from various fronts, which encouraged greater use of code making and breaking sections in diplomatic and military headquarters. In the United Kingdom this led to the creation of the **Government Code and Cypher School** in 1919. Encoding became more sophisticated between the wars as machines were employed to scramble and unscramble information. The volume of information shared by the Allied countries during the **Second World War** necessitated formal alignment of classification systems and procedural controls. An arcane range of markings evolved to indicate who could handle documents (usually officers rather than men) and where they should be stored as increasingly complex safes and storage facilities were developed. The **Enigma Machine** which was employed by the Germans to encrypt the data of warfare and successfully decrypted by **Alan Turing** can be regarded as a striking example of creating and using secured information. Procedures evolved to ensure documents were destroyed properly and it was the failure to follow these procedures which led to some of the greatest intelligence coups of the war (e.g. U-570).

The end of the 20th century and early years of the 21st century saw rapid advancements in **telecommunications**, computing **hardware** and software, and data **encryption**. The availability of smaller, more powerful and less expensive computing equipment made **electronic data processing** within the reach of **small business** and the home user. These computers quickly became interconnected through the **Internet**.

The rapid growth and widespread use of electronic data processing and **electronic business** conducted through the Internet, along with numerous occurrences of international **terrorism**, fueled the need for better methods of protecting

the computers and the information they store, process and transmit. The academic disciplines of computer security and information assurance emerged along with numerous professional organizations – all sharing the common goals of ensuring the security and reliability of information systems.

1.3 Definitions



Information Security Attributes: or qualities, i.e., Confidentiality, Integrity and Availability (CIA). Information Systems are composed in three main portions, hardware, software and communications with the purpose to help identify and apply information security industry standards, as mechanisms of protection and prevention, at three levels or layers: physical, personal and organizational. Essentially, procedures or policies are implemented to tell people (administrators, users and operators) how to use products to ensure information security within the organizations.

The definitions of InfoSec suggested in different sources are summarized below (adopted from).^{*} [7]

1. “Preservation of confidentiality, integrity and availability of information. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.” (ISO/IEC 27000:2009)^{*} [8]
2. “The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.” (CNSS, 2010)^{*} [9]

3. “Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability).” (ISACA, 2008)*[10]
4. “Information Security is the process of protecting the intellectual property of an organisation.” (Pipkin, 2000)*[11]
5. "...information security is a risk management discipline, whose job is to manage the cost of information risk to the business." (McDermott and Geer, 2001)*[12]
6. “A well-informed sense of assurance that information risks and controls are in balance.” (Anderson, J., 2003)*[13]
7. “Information security is the protection of information and minimizes the risk of exposing information to unauthorized parties.” (Venter and Eloff, 2003)*[14]
8. “Information Security is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security mechanisms of all available types (technical, organizational, human-oriented and legal) in order to keep information in all its locations (within and outside the organization's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destroyed, free from threats. Threats to information and information systems may be categorized and a corresponding security goal may be defined for each category of threats. A set of security goals, identified as a result of a threat analysis, should be revised periodically to ensure its adequacy and conformance with the evolving environment. The currently relevant set of security goals may include: *confidentiality, integrity, availability, privacy, authenticity & trustworthiness, non-repudiation, accountability and auditability.*” (Cherdantseva and Hilton, 2013)*[7]

1.4 Employment

Information security is a stable and growing profession. Information security professionals are very stable in their employment; more than 80 percent had no change in employer or employment in the past year, and the number of professionals is projected to continuously grow more than 11 percent annually from 2014 to 2019.*[15]

1.5 Basic principles

1.5.1 Key concepts

The CIA triad of confidentiality, integrity, and availability is at the heart of information security.*[16] (The members of the classic InfoSec triad —confidentiality, integrity and availability— are interchangeably referred to in the literature as security attributes, properties, security goals, fundamental aspects, information criteria, critical information characteristics and basic building blocks.) There is continuous debate about extending this classic trio.*[7] Other principles such as Accountability*[17] have sometimes been proposed for addition – it has been pointed out that issues such as non-repudiation do not fit well within the three core concepts.

In 1992 and revised in 2002, the OECD's *Guidelines for the Security of Information Systems and Networks**[18] proposed the nine generally accepted principles: awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management, and reassessment. Building upon those, in 2004 the NIST's *Engineering Principles for Information Technology Security**[19] proposed 33 principles. From each of these derived guidelines and practices.

In 2002, Donn Parker proposed an alternative model for the classic CIA triad that he called the six atomic elements of information. The elements are confidentiality, possession, integrity, authenticity, availability, and utility. The merits of the Parkerian Hexad are a subject of debate amongst security professionals.

In 2011, The Open Group published the information security management standard O-ISM3.*[20] This standard proposed an operational definition of the key concepts of security, with elements called “security objectives”, related to access control (9), availability (3), data quality (1), compliance and technical (4). This model is not currently widely adopted.

Confidentiality

In information security, confidentiality “is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes” (Excerpt ISO27000).

Integrity

In information security, data integrity means maintaining and assuring the accuracy and completeness of data over its entire life-cycle.*[21] This means that data cannot be modified in an unauthorized or undetected manner. This is not the same thing as referential integrity in databases, although it can be viewed as a special case of consistency as understood in the classic ACID model of transaction processing. Information security systems typically provide message integrity in addition to data confidentiality.

Availability

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system essentially forcing it to shut down.*[22]

Non-repudiation

In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.

It is important to note that while technology such as cryptographic systems can assist in non-repudiation efforts, the concept is at its core a legal concept transcending the realm of technology. It is not, for instance, sufficient to show that the message matches a digital signature signed with the sender's private key, and thus only the sender could have sent the message and nobody else could have altered it in transit (data integrity). The alleged sender could in return demonstrate that the digital signature algorithm is vulnerable or flawed, or allege or prove that his signing key has been compromised. The fault for these violations may or may not lie with the sender himself, and such assertions may or may not relieve the sender of liability, but the assertion would invalidate the claim that the signature necessarily proves authenticity and integrity; and, therefore, the sender may repudiate the message (because authenticity and integrity are pre-requisites for non-repudiation).

1.6 Risk management

Main article: Risk management

The *Certified Information Systems Auditor (CISA) Review Manual 2006* provides the following definition of risk management: “Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization.”*[23]

There are two things in this definition that may need some clarification. First, the process of risk management is an ongoing, iterative process. It must be repeated indefinitely. The business environment is constantly changing and new threats and vulnerabilities emerge every day. Second, the choice of countermeasures (controls) used to manage risks must strike a balance between productivity, cost, effectiveness of the countermeasure, and the value of the informational asset being protected.

Risk analysis and risk evaluation processes have their limitations since, when security incidents occur, they emerge in a context, and their rarity and even their uniqueness give rise to unpredictable threats. The analysis of these phenomena which are characterized by breakdowns, surprises and side-effects, requires a theoretical approach which is able to examine and interpret subjectively the detail of each incident.*[24]

Risk is the likelihood that something bad will happen that causes harm to an informational asset (or the loss of the asset). A **vulnerability** is a weakness that could be used to endanger or cause harm to an informational asset. A **threat** is anything (man-made or act of nature) that has the potential to cause harm.

The likelihood that a threat will use a vulnerability to cause harm creates a risk. When a threat does use a vulnerability to inflict harm, it has an impact. In the context of information security, the impact is a loss of availability, integrity, and confidentiality, and possibly other losses (lost income, loss of life, loss of real property). It should be pointed out that it is not possible to identify all risks, nor is it possible to eliminate all risk. The remaining risk is called “residual risk”.

A **risk assessment** is carried out by a team of people who have knowledge of specific areas of the business. Membership of the team may vary over time as different parts of the business are assessed. The assessment may use a subjective qualitative analysis based on informed opinion, or where reliable dollar figures and historical information is available, the analysis may use quantitative analysis.

The research has shown that the most vulnerable point in most information systems is the human user, operator, designer, or other human.*[25] The ISO/IEC 27002:2005 Code of practice for information security management recommends the following be examined during a risk assessment:

- security policy,
- organization of information security,
- asset management,
- human resources security,
- physical and environmental security,
- communications and operations management,
- access control,
- information systems acquisition, development and maintenance,
- information security incident management,
- business continuity management, and
- regulatory compliance.

In broad terms, the risk management process consists of:

1. Identification of assets and estimating their value. Include: people, buildings, hardware, software, data (electronic, print, other), supplies.
2. Conduct a **threat assessment**. Include: Acts of nature, acts of war, accidents, malicious acts originating from inside or outside the organization.
3. Conduct a **vulnerability assessment**, and for each vulnerability, calculate the probability that it will be exploited. Evaluate policies, procedures, standards, training, physical security, quality control, technical security.
4. Calculate the impact that each threat would have on each asset. Use qualitative analysis or quantitative analysis.
5. Identify, select and implement appropriate controls. Provide a proportional response. Consider productivity, cost effectiveness, and value of the asset.
6. Evaluate the effectiveness of the control measures. Ensure the controls provide the required cost effective protection without discernible loss of productivity.

For any given risk, management can choose to **accept the risk** based upon the relative low value of the asset, the relative low frequency of occurrence, and the relative low impact on the business. Or, leadership may choose to **mitigate the risk** by selecting and implementing appropriate control measures to reduce the risk. In some cases, the risk can be **transferred** to another business by buying insurance or outsourcing to another business.*[26] The reality of some risks may be disputed. In such cases leadership may choose to **deny the risk**.

1.6.1 Controls

Main article: security controls

Selecting proper controls and implementing those will initially help an organization to bring down risk to acceptable levels. Control selection should follow and should be based on the risk assessment. Controls can vary in nature but fundamentally they are ways of protecting the confidentiality, integrity or availability of information. ISO/IEC 27001:2005 has defined 133 controls in different areas, but this is not exhaustive. Organizations can implement additional controls according to requirement of the organization. ISO 27001:2013 has cut down the number of controls to 113. From 08.11.2013 the technical standard of information security in place is: ABNT NBR ISO/IEC 27002:2013.*[27]

Administrative

Administrative controls (also called procedural controls) consist of approved written policies, procedures, standards and guidelines. Administrative controls form the framework for running the business and managing people. They inform people on how the business is to be run and how day-to-day operations are to be conducted. Laws and regulations created by government bodies are also a type of administrative control because they inform the business. Some industry sectors have policies, procedures, standards and guidelines that must be followed – the Payment Card Industry Data Security Standard (PCI DSS) required by Visa and MasterCard is such an example. Other examples of administrative controls include the corporate security policy, password policy, hiring policies, and disciplinary policies.

Administrative controls form the basis for the selection and implementation of logical and physical controls. Logical and physical controls are manifestations of administrative controls. Administrative controls are of paramount importance.

Logical

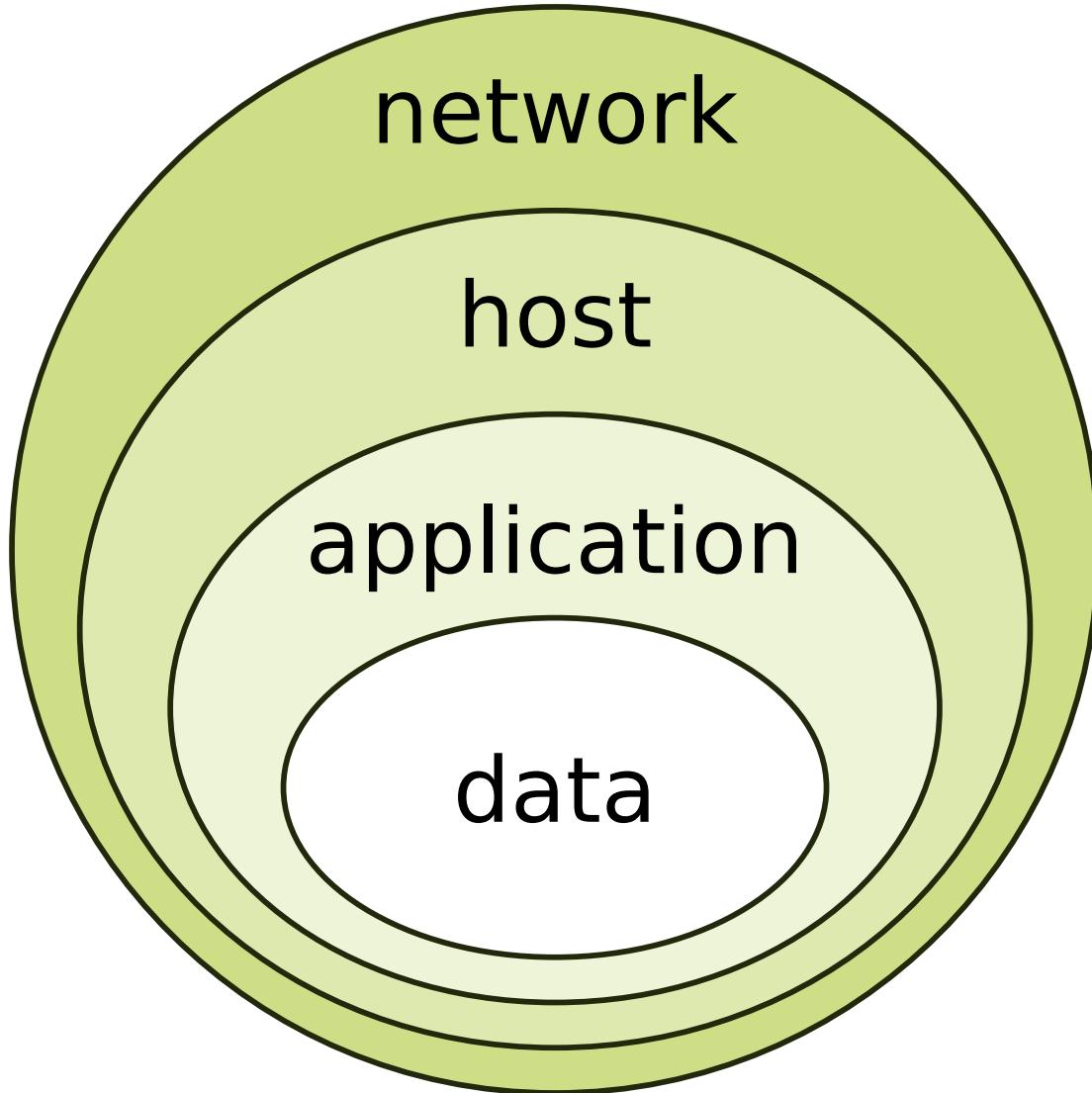
Logical controls (also called technical controls) use software and data to monitor and control access to information and computing systems. For example: passwords, network and host-based firewalls, network intrusion detection systems, access control lists, and data encryption are logical controls.

An important logical control that is frequently overlooked is the **principle of least privilege**. The principle of least privilege requires that an individual, program or system process is not granted any more access privileges than are necessary to perform the task. A blatant example of the failure to adhere to the principle of least privilege is logging into Windows as user Administrator to read email and surf the web. Violations of this principle can also occur when an individual collects additional access privileges over time. This happens when employees' job duties change, or they are promoted to a new position, or they transfer to another department. The access privileges required by their new duties are frequently added onto their already existing access privileges which may no longer be necessary or appropriate.

Physical

Physical controls monitor and control the environment of the work place and computing facilities. They also monitor and control access to and from such facilities. For example: doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks, etc. Separating the network and workplace into functional areas are also physical controls.

An important physical control that is frequently overlooked is the **separation of duties**, which ensures that an individual can not complete a critical task by himself. For example: an employee who submits a request for reimbursement should not also be able to authorize payment or print the check. An applications programmer should not also be the server administrator or the database administrator – these roles and responsibilities must be separated from one another.*[28]



The onion model of defense in depth

1.6.2 Defense in depth

Main article: Defense in depth (computing)

Information security must protect information throughout the life span of the information, from the initial creation of the information on through to the final disposal of the information. The information must be protected while in motion and while at rest. During its lifetime, information may pass through many different information processing systems and through many different parts of information processing systems. There are many different ways the information and information systems can be threatened. To fully protect the information during its lifetime, each component of the information processing system must have its own protection mechanisms. The building up, layering on and overlapping of security measures is called defense in depth. In contrast to a metal chain, which is famously only as strong as its weakest link, the defense-in-depth aims at a structure where, should one defensive measure fail, other measures will continue to provide protection.

Recall the earlier discussion about administrative controls, logical controls, and physical controls. The three types of controls can be used to form the basis upon which to build a defense-in-depth strategy. With this approach, defense-in-depth can be conceptualized as three distinct layers or planes laid one on top of the other. Additional insight into defense-in-depth can be gained by thinking of it as forming the layers of an onion, with data at the core of the onion, people the next outer layer of the onion, and network security, host-based security and application security forming

the outermost layers of the onion. Both perspectives are equally valid and each provides valuable insight into the implementation of a good defense-in-depth strategy.

1.6.3 Security classification for information

An important aspect of information security and risk management is recognizing the value of information and defining appropriate procedures and protection requirements for the information. Not all information is equal and so not all information requires the same degree of protection. This requires information to be assigned a **security classification**.

The first step in information classification is to identify a member of senior management as the owner of the particular information to be classified. Next, develop a classification policy. The policy should describe the different classification labels, define the criteria for information to be assigned a particular label, and list the required **security controls** for each classification.

Some factors that influence which classification information should be assigned include how much value that information has to the organization, how old the information is and whether or not the information has become obsolete. Laws and other regulatory requirements are also important considerations when classifying information.

The Business Model for Information Security enables security professionals to examine security from systems perspective, creating an environment where security can be managed holistically, allowing actual risks to be addressed.

The type of information security classification labels selected and used will depend on the nature of the organization, with examples being:

- In the business sector, labels such as: **Public, Sensitive, Private, Confidential**.
- In the government sector, labels such as: **Unclassified, Unofficial, Protected, Confidential, Secret, Top Secret** and their non-English equivalents.
- In cross-sectoral formations, the **Traffic Light Protocol**, which consists of: **White, Green, Amber, and Red**.

All employees in the organization, as well as business partners, must be trained on the classification schema and understand the required security controls and handling procedures for each classification. The classification of a particular information asset that has been assigned should be reviewed periodically to ensure the classification is still appropriate for the information and to ensure the security controls required by the classification are in place and are followed in their right procedures.

1.6.4 Access control

Access to protected information must be restricted to people who are authorized to access the information. The computer programs, and in many cases the computers that process the information, must also be authorized. This requires that mechanisms be in place to control the access to protected information. The sophistication of the access control mechanisms should be in parity with the value of the information being protected – the more sensitive or valuable the information the stronger the control mechanisms need to be. The foundation on which access control mechanisms are built start with **identification** and **authentication**.

Access control is generally considered in three steps: **Identification, Authentication, and Authorization**.

Identification

Identification is an assertion of who someone is or what something is. If a person makes the statement “Hello, my name is **John Doe**” they are making a claim of who they are. However, their claim may or may not be true. Before John Doe can be granted access to protected information it will be necessary to verify that the person claiming to be John Doe really is John Doe. Typically the claim is in the form of a username. By entering that username you are claiming “I am the person the username belongs to” .

Authentication

Authentication is the act of verifying a claim of identity. When John Doe goes into a bank to make a withdrawal, he tells the **bank teller** he is John Doe—a claim of identity. The bank teller asks to see a photo ID, so he hands the

teller his **driver's license**. The bank teller checks the license to make sure it has John Doe printed on it and compares the photograph on the license against the person claiming to be John Doe. If the photo and name match the person, then the teller has authenticated that John Doe is who he claimed to be. Similarly by entering the correct password, the user is providing evidence that he/she is the person the username belongs to.

There are three different types of information that can be used for authentication:

- Something you know: things such as a PIN, a **password**, or your mother's **maiden name**.
- Something you have: a driver's license or a magnetic **swipe card**.
- Something you are: **biometrics**, including **palm prints**, **fingerprints**, **voice prints** and **retina (eye) scans**.

Strong authentication requires providing more than one type of authentication information (two-factor authentication). The **username** is the most common form of identification on computer systems today and the password is the most common form of authentication. Usernames and passwords have served their purpose but in our modern world they are no longer adequate. Usernames and passwords are slowly being replaced with more sophisticated authentication mechanisms.

Authorization

After a person, program or computer has successfully been identified and authenticated then it must be determined what informational resources they are permitted to access and what actions they will be allowed to perform (run, view, create, delete, or change). This is called **authorization**. Authorization to access information and other computing services begins with administrative policies and procedures. The policies prescribe what information and computing services can be accessed, by whom, and under what conditions. The access control mechanisms are then configured to enforce these policies. Different computing systems are equipped with different kinds of access control mechanisms —some may even offer a choice of different access control mechanisms. The access control mechanism a system offers will be based upon one of three approaches to access control or it may be derived from a combination of the three approaches.

The **non-discretionary** approach consolidates all access control under a centralized administration. The access to information and other resources is usually based on the individuals function (role) in the organization or the tasks the individual must perform. The **discretionary approach** gives the creator or owner of the information resource the ability to control access to those resources. In the **Mandatory access control approach**, access is granted or denied basing upon the security classification assigned to the information resource.

Examples of common access control mechanisms in use today include **role-based access control** available in many advanced database management systems—simple **file permissions** provided in the UNIX and Windows operating systems, **Group Policy Objects** provided in Windows network systems, **Kerberos**, **RADIUS**, **TACACS**, and the simple access lists used in many firewalls and routers.

To be effective, policies and other security controls must be enforceable and upheld. Effective policies ensure that people are held **accountable** for their actions. All failed and successful authentication attempts must be logged, and all access to information must leave some type of **audit trail**.

Also, **need-to-know principle** needs to be in effect when talking about access control. Need-to-know principle gives access rights to a person to perform their job functions. This principle is used in the government, when dealing with difference clearances. Even though two employees in different departments have a **top-secret clearance**, they must have a need-to-know in order for information to be exchanged. Within the need-to-know principle, network administrators grant the employee least amount privileges to prevent employees access and doing more than what they are supposed to. Need-to-know helps to enforce the confidentiality-integrity-availability (C-I-A) triad. Need-to-know directly impacts the confidential area of the triad.

1.6.5 Cryptography

Main article: [Cryptography](#)

Information security uses **cryptography** to transform usable information into a form that renders it unusable by anyone other than an authorized user; this process is called **encryption**. Information that has been encrypted (rendered

unusable) can be transformed back into its original usable form by an authorized user, who possesses the cryptographic key, through the process of decryption. Cryptography is used in information security to protect information from unauthorized or accidental disclosure while the **information** is in transit (either electronically or physically) and while information is in storage.

Cryptography provides information security with other useful applications as well including improved authentication methods, message digests, digital signatures, **non-repudiation**, and encrypted network communications. Older less secure applications such as telnet and ftp are slowly being replaced with more secure applications such as ssh that use encrypted network communications. Wireless communications can be encrypted using protocols such as **WPA/WPA2** or the older (and less secure) **WEP**. Wired communications (such as **ITU-T G.hn**) are secured using **AES** for encryption and **X.1035** for authentication and key exchange. Software applications such as **GnuPG** or **PGP** can be used to encrypt data files and Email.

Cryptography can introduce security problems when it is not implemented correctly. Cryptographic solutions need to be implemented using industry accepted solutions that have undergone rigorous peer review by independent experts in cryptography. The length and strength of the encryption key is also an important consideration. A key that is weak or too short will produce weak encryption. The keys used for encryption and decryption must be protected with the same degree of rigor as any other confidential information. They must be protected from unauthorized disclosure and destruction and they must be available when needed. **Public key infrastructure (PKI)** solutions address many of the problems that surround **key management**.

1.7 Process

The terms **reasonable and prudent person**, **due care** and **due diligence** have been used in the fields of Finance, Securities, and Law for many years. In recent years these terms have found their way into the fields of computing and information security. U.S.A. **Federal Sentencing Guidelines** now make it possible to hold corporate officers liable for failing to exercise due care and due diligence in the management of their information systems.

In the business world, stockholders, customers, business partners and governments have the expectation that corporate officers will run the business in accordance with accepted business practices and in compliance with laws and other regulatory requirements. This is often described as the “**reasonable and prudent person**” rule. A prudent person takes due care to ensure that everything necessary is done to operate the business by sound business principles and in a legal ethical manner. A prudent person is also diligent (mindful, attentive, and ongoing) in their due care of the business.

In the field of Information Security, Harris* [29] offers the following definitions of **due care** and **due diligence**:

“*Due care are steps that are taken to show that a company has taken responsibility for the activities that take place within the corporation and has taken the necessary steps to help protect the company, its resources, and employees.*” And, [Due diligence are the] “*continual activities that make sure the protection mechanisms are continually maintained and operational.*”

Attention should be made to two important points in these definitions. First, in due care, steps are taken to **show** - this means that the steps can be verified, measured, or even produce tangible artifacts. Second, in due diligence, there are **continual activities** - this means that people are actually doing things to monitor and maintain the protection mechanisms, and these activities are ongoing.

1.7.1 Security governance

See also: **Information Security Governance**

The Software Engineering Institute at Carnegie Mellon University, in a publication titled “**Governing for Enterprise Security (GES)**”, defines characteristics of effective security governance. These include:

- An enterprise-wide issue
- Leaders are accountable

- Viewed as a business requirement
- Risk-based
- Roles, responsibilities, and segregation of duties defined
- Addressed and enforced in policy
- Adequate resources committed
- Staff aware and trained
- A development life cycle requirement
- Planned, managed, measurable, and measured
- Reviewed and audited

1.7.2 Incident response plans

Main article: Computer security incident management

1 to 3 paragraphs (non technical) that discuss:

- Selecting team members
- Define roles, responsibilities and lines of authority
- Define a security incident
- Define a reportable incident
- Training
- Detection
- Classification
- Escalation
- Containment
- Eradication
- Documentation

1.7.3 Change management

Main article: Change Management (ITSM)

Change management is a formal process for directing and controlling alterations to the information processing environment. This includes alterations to desktop computers, the network, servers and software. The objectives of change management are to reduce the risks posed by changes to the information processing environment and improve the stability and reliability of the processing environment as changes are made. It is not the objective of change management to prevent or hinder necessary changes from being implemented.

Any change to the information processing environment introduces an element of risk. Even apparently simple changes can have unexpected effects. One of Management's many responsibilities is the management of risk. Change management is a tool for managing the risks introduced by changes to the information processing environment. Part of the change management process ensures that changes are not implemented at inopportune times when they may disrupt critical business processes or interfere with other changes being implemented.

Not every change needs to be managed. Some kinds of changes are a part of the everyday routine of information processing and adhere to a predefined procedure, which reduces the overall level of risk to the processing environment. Creating a new user account or deploying a new desktop computer are examples of changes that do not generally require change management. However, relocating user file shares, or upgrading the Email server pose a much higher level of risk to the processing environment and are not a normal everyday activity. The critical first steps in change management are (a) defining change (and communicating that definition) and (b) defining the scope of the change system.

Change management is usually overseen by a Change Review Board composed of representatives from key business areas, security, networking, systems administrators, Database administration, applications development, desktop support and the help desk. The tasks of the Change Review Board can be facilitated with the use of automated work flow application. The responsibility of the Change Review Board is to ensure the organizations documented change management procedures are followed. The change management process is as follows:

- **Requested:** Anyone can request a change. The person making the change request may or may not be the same person that performs the analysis or implements the change. When a request for change is received, it may undergo a preliminary review to determine if the requested change is compatible with the organizations **business model** and practices, and to determine the amount of resources needed to implement the change.
- **Approved:** Management runs the business and controls the allocation of resources therefore, Management must approve requests for changes and assign a priority for every change. Management might choose to reject a change request if the change is not compatible with the business model, industry standards or best practices. Management might also choose to reject a change request if the change requires more resources than can be allocated for the change.
- **Planned:** Planning a change involves discovering the scope and impact of the proposed change; analyzing the complexity of the change; allocation of resources and, developing, testing and documenting both implementation and backout plans. Need to define the criteria on which a decision to back out will be made.
- **Tested:** Every change must be tested in a safe test environment, which closely reflects the actual production environment, before the change is applied to the production environment. The backout plan must also be tested.
- **Scheduled:** Part of the change review board's responsibility is to assist in the scheduling of changes by reviewing the proposed implementation date for potential conflicts with other scheduled changes or critical business activities.
- **Communicated:** Once a change has been scheduled it must be communicated. The communication is to give others the opportunity to remind the change review board about other changes or critical business activities that might have been overlooked when scheduling the change. The communication also serves to make the Help Desk and users aware that a change is about to occur. Another responsibility of the change review board is to ensure that scheduled changes have been properly communicated to those who will be affected by the change or otherwise have an interest in the change.
- **Implemented:** At the appointed date and time, the changes must be implemented. Part of the planning process was to develop an implementation plan, testing plan and, a back out plan. If the implementation of the change should fail or, the post implementation testing fails or, other “drop dead” criteria have been met, the back out plan should be implemented.
- **Documented:** All changes must be documented. The documentation includes the initial request for change, its approval, the priority assigned to it, the implementation, testing and back out plans, the results of the change review board critique, the date/time the change was implemented, who implemented it, and whether the change was implemented successfully, failed or postponed.
- **Post change review:** The change review board should hold a post implementation review of changes. It is particularly important to review failed and backed out changes. The review board should try to understand the problems that were encountered, and look for areas for improvement.

Change management procedures that are simple to follow and easy to use can greatly reduce the overall risks created when changes are made to the information processing environment. Good change management procedures improve the overall quality and success of changes as they are implemented. This is accomplished through planning, peer review, documentation and communication.

ISO/IEC 20000, The Visible OPS Handbook: Implementing ITIL in 4 Practical and Auditable Steps^{*} [30] (Full book summary),^{*} [31] and Information Technology Infrastructure Library all provide valuable guidance on implementing an efficient and effective change management program information security.

1.8 Business continuity

Business continuity management (BCM) concerns arrangements aiming to protect an organization's critical business functions from interruption due to incidents, or at least minimize the effects. It encompasses:

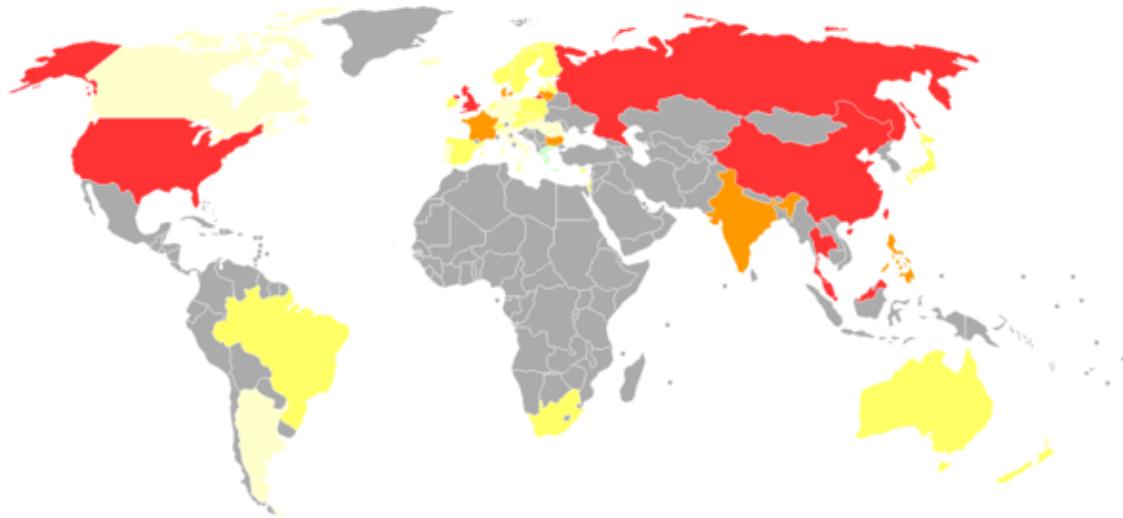
- Analysis of requirements e.g. identifying critical business functions, dependencies and potential failure points, potential threats and hence incidents or risks of concern to the organization;
- Specification e.g. maximum tolerable outage periods; recovery point objectives (maximum acceptable periods of data loss);
- Architecture and design e.g. an appropriate combination of approaches including resilience (e.g. engineering IT systems and processes for high availability, avoiding or preventing situations that might interrupt the business), incident and emergency management (e.g. evacuating premises, calling the emergency services, triage/situation assessment and invoking recovery plans), recovery (e.g. rebuilding) and contingency management (generic capabilities to deal positively with whatever occurs using whatever resources are available);
- Implementation e.g. configuring and scheduling backups, data transfers etc., duplicating and strengthening critical elements; contracting with service and equipment suppliers;
- Testing e.g. business continuity exercises of various types, costs and assurance levels;
- Management e.g. defining strategies, setting objectives and goals; planning and directing the work; allocating funds, people and other resources; prioritization relative to other activities; team building, leadership, control, motivation and coordination with other business functions and activities (e.g. IT, Facilities, HR, Risk Management, Information Risk and Security, Operations); monitoring the situation, checking and updating the arrangements when things change; maturing the approach through continuous improvement, learning and appropriate investment;
- Assurance e.g. testing against specified requirements; measuring, analysing and reporting key parameters; conducting additional tests, reviews and audits for greater confidence that the arrangements will go to plan if invoked.

Whereas BCM takes a broad approach to minimizing disaster-related risks by reducing both the probability and the severity of incidents, a **disaster recovery plan** (DRP) focuses specifically on resuming business operations as quickly as possible *after* a disaster. A disaster recovery plan, invoked soon after a disaster occurs, lays out the steps necessary to recover critical ICT infrastructure. Disaster recovery planning includes establishing a planning group, performing risk assessment, establishing priorities, developing recovery strategies, preparing inventories and documentation of the plan, developing verification criteria and procedure, and lastly implementing the plan.^{*} [32]

1.9 Laws and regulations

Below is a partial listing of European, United Kingdom, Canadian and US governmental laws and regulations that have, or will have, a significant effect on data processing and information security. Important industry sector regulations have also been included when they have a significant impact on information security.

- UK Data Protection Act 1998 makes new provisions for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. The European Union Data Protection Directive (EUDPD) requires that all EU member must adopt national regulations to standardize the protection of data privacy for citizens throughout the EU.
- The Computer Misuse Act 1990 is an Act of the UK Parliament making computer crime (e.g. hacking) a criminal offence. The Act has become a model upon which several other countries including Canada and the Republic of Ireland have drawn inspiration when subsequently drafting their own information security laws.



Privacy International 2007 privacy ranking

green: Protections and safeguards
red: Endemic surveillance societies

- EU Data Retention laws requires Internet service providers and phone companies to keep data on every electronic message sent and phone call made for between six months and two years.
- The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232 g; 34 CFR Part 99) is a US Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record.
- Federal Financial Institutions Examination Council's (FFIEC) security guidelines for auditors specifies requirements for online banking security.
- Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires the adoption of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. And, it requires health care providers, insurance providers and employers to safeguard the security and privacy of health data.
- Gramm–Leach–Bliley Act of 1999 (GLBA), also known as the Financial Services Modernization Act of 1999, protects the privacy and security of private financial information that financial institutions collect, hold, and process.
- Sarbanes–Oxley Act of 2002 (SOX). Section 404 of the act requires publicly traded companies to assess the effectiveness of their internal controls for financial reporting in annual reports they submit at the end of each fiscal year. Chief information officers are responsible for the security, accuracy and the reliability of the systems that manage and report the financial data. The act also requires publicly traded companies to engage independent auditors who must attest to, and report on, the validity of their assessments.
- Payment Card Industry Data Security Standard (PCI DSS) establishes comprehensive requirements for enhancing payment account data security. It was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.
- State security breach notification laws (California and many others) require businesses, nonprofits, and state institutions to notify consumers when unencrypted "personal information" may have been compromised, lost, or stolen.

- Personal Information Protection and Electronics Document Act (**PIPEDA**) – An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the **Canada Evidence Act**, the **Statutory Instruments Act** and the **Statute Revision Act**.
- Hellenic Authority for Communication Security and Privacy (ADAE) (Law 165/2011) - The Greek Law establishes and describes the minimum Information Security controls that should be deployed by every company which provides electronic communication networks and/or services in Greece in order to protect customers' Confidentiality. These include both managerial and technical controls (i.e. log records should be stored for two years).
- Hellenic Authority for Communication Security and Privacy (ADAE) (Law 205/2013)- The latest Greek Law published by ADAE concentrates around the protection of the Integrity and Availability of the services and data offered by the Greek Telecommunication Companies. The new Law forces Telcos and associated companies to build, deploy and test appropriate Business Continuity Plans and redundant infrastructures.

1.10 Information security culture

Employee behavior can have a big impact on information security in organizations. Cultural concepts can help different segments of the organization work effectively or work against effectiveness towards information security within an organization."Exploring the Relationship between Organizational Culture and Information Security Culture" provides the following definition of information security culture: "ISC is the totality of patterns of behavior in an organization that contribute to the protection of information of all kinds."^{*}[33]

Andersson and Reimers (2014) found that employees often do not see themselves as part of the organization Information Security "effort" and often take actions that ignore organizational Information Security best interests.^{*}[34] Research shows Information security culture needs to be improved continuously. In "Information Security Culture from Analysis to Change", authors commented, "It's a never ending process, a cycle of evaluation and change or maintenance." To manage the information security culture, five steps should be taken: Pre-evaluation, strategic planning, operative planning, implementation, and post-evaluation.^{*}[35]

- Pre-Evaluation: to identify the awareness of information security within employees and to analysis current security policy.
- Strategic Planning: to come up a better awareness-program, we need to set clear targets. Clustering people is helpful to achieve it.
- Operative Planning: we can set a good security culture based on internal communication, management-buy-in, and security awareness and training program.^{*}[35]
- Implementation: four stages should be used to implement the information security culture. They are commitment of the management, communication with organizational members, courses for all organizational members, and commitment of the employees.^{*}[35]

1.11 Sources of standards

Main article: Cyber Security Standards

International Organization for Standardization (ISO) is a consortium of national standards institutes from 157 countries, coordinated through a secretariat in Geneva, Switzerland. ISO is the world's largest developer of standards. ISO 15443: "Information technology - Security techniques - A framework for IT security assurance" , ISO/IEC 27002: "Information technology - Security techniques - Code of practice for information security management" , ISO-20000: "Information technology - Service management" , and ISO/IEC 27001: "Information technology - Security techniques - Information security management systems - Requirements" are of particular interest to information security professionals.

The US National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Department of Commerce. The NIST Computer Security Division develops standards, metrics, tests and validation

programs as well as publishes standards and guidelines to increase secure IT planning, implementation, management and operation. NIST is also the custodian of the US **Federal Information Processing Standard** publications (FIPS).

The **Internet Society** is a professional membership society with more than 100 organizations and over 20,000 individual members in over 180 countries. It provides leadership in addressing issues that confront the future of the Internet, and is the organization home for the groups responsible for Internet infrastructure standards, including the **Internet Engineering Task Force** (IETF) and the **Internet Architecture Board** (IAB). The ISOC hosts the Requests for Comments (RFCs) which includes the Official Internet Protocol Standards and the RFC-2196 Site Security Handbook.

The **Information Security Forum** is a global nonprofit organization of several hundred leading organizations in financial services, manufacturing, telecommunications, consumer goods, government, and other areas. It undertakes research into information security practices and offers advice in its biannual **Standard of Good Practice** and more detailed advisories for members.

The **Institute of Information Security Professionals** (IISP) is an independent, non-profit body governed by its members, with the principal objective of advancing the professionalism of information security practitioners and thereby the professionalism of the industry as a whole. The Institute developed the **IISP Skills Framework**©. This framework describes the range of competencies expected of Information Security and Information Assurance Professionals in the effective performance of their roles. It was developed through collaboration between both private and public sector organisations and world-renowned academics and security leaders.

The German Federal Office for Information Security (in German *Bundesamt für Sicherheit in der Informationstechnik (BSI)*) BSI-Standards 100-1 to 100-4 are a set of recommendations including “methods, processes, procedures, approaches and measures relating to information security” . *[36] The BSI-Standard 100-2 *IT-Grundsatz Methodology* describes how an information security management can be implemented and operated. The Standard includes a very specific guide, the **IT Baseline Protection Catalogs** (also known as **IT-Grundsatz Catalogs**). Before 2005 the catalogs were formerly known as “**IT Baseline Protection Manual**” . The Catalogs are a collection of documents useful for detecting and combating security-relevant weak points in the IT environment (IT cluster). The collection encompasses as of September 2013 over 4.400 pages with the introduction and catalogs. The **IT-Grundsatz** approach is aligned with to the ISO/IEC 2700x family.

At the European Telecommunications Standards Institute a catalog of Information security indicators have been standardized by the Industrial Specification Group (ISG) ISI.

1.12 Scholars working in the field

- Adam Back
- Annie Anton
- Brian LaMacchia
- Bruce Schneier
- Cynthia Dwork
- Dawn Song
- Deborah Estrin
- Gene Spafford
- Ian Goldberg
- Lawrence A. Gordon
- Martin P. Loeb
- Monica S. Lam
- Joan Feigenbaum
- L Jean Camp
- Lance Cottrell

- Lorrie Cranor
- Khalil Sehnaoui
- Paul C. van Oorschot
- Peter Gutmann
- Peter Landrock
- Ross J. Anderson
- Stefan Brands

1.13 See also

- Backup
- Data breach
- Data-centric security
- Enterprise information security architecture
- Identity-based security
- Information security audit
- Information security indicators
- Information security standards
- Information technology security audit
- IT risk
- ITIL security management
- Kill chain
- List of Computer Security Certifications
- Mobile security
- Network Security Services
- Privacy engineering
- Privacy software
- Privacy-enhancing technologies
- Security bug
- Security information management
- Security level management
- Security of Information Act
- Security service (telecommunication)
- Single sign-on
- Verification and validation

1.14 Further reading

- Anderson, K., "IT Security Professionals Must Evolve for Changing Market", *SC Magazine*, October 12, 2006.
- Aceituno, V., "On Information Security Paradigms", *ISSA Journal*, September 2005.
- Dhillon, G., *Principles of Information Systems Security: text and cases*, John Wiley & Sons, 2007.
- Easttom, C., *Computer Security Fundamentals (2nd Edition)* Pearson Education, 2011.
- Lambo, T., "ISO/IEC 27001: The future of infosec certification", *ISSA Journal*, November 2006.
- Dustin, D., "Awareness of How Your Data is Being Used and What to Do About It", "CDR Blog", May 2017.

1.14.1 Bibliography

- Allen, Julia H. (2001). *The CERT Guide to System and Network Security Practices*. Boston, MA: Addison-Wesley. ISBN 0-201-73723-X.
- Krutz, Ronald L.; Russell Dean Vines (2003). *The CISSP Prep Guide* (Gold ed.). Indianapolis, IN: Wiley. ISBN 0-471-26802-X.
- Layton, Timothy P. (2007). *Information Security: Design, Implementation, Measurement, and Compliance*. Boca Raton, FL: Auerbach publications. ISBN 978-0-8493-7087-8.
- McNab, Chris (2004). *Network Security Assessment*. Sebastopol, CA: O'Reilly. ISBN 0-596-00611-X.
- Peltier, Thomas R. (2001). *Information Security Risk Analysis*. Boca Raton, FL: Auerbach publications. ISBN 0-8493-0880-1.
- Peltier, Thomas R. (2002). *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. Boca Raton, FL: Auerbach publications. ISBN 0-8493-1137-3.
- White, Gregory (2003). *All-in-one Security+ Certification Exam Guide*. Emeryville, CA: McGraw-Hill/Osborne. ISBN 0-07-222633-1.
- Dhillon, Gurpreet (2007). *Principles of Information Systems Security: text and cases*. NY: John Wiley & Sons. ISBN 978-0-471-45056-6.

1.15 References

- [1] 44 U.S.C. § 3542(b)(1)
- [2] Stewart, James (2012). *CISSP Study Guide*. Canada: John Wiley & Sons, Inc. pp. 255–257. ISBN 978-1-118-31417-3 – via Online PSU course resource, EBL Reader.
- [3] Gordon, Lawrence; Loeb, Martin (November 2002). "The Economics of Information Security Investment". *ACM Transactions on Information and System Security*. 5 (4): 438–457. doi:10.1145/581271.581274.
- [4] Stewart, James (2012). *CISSP Certified Information Systems Security Professional Study Guide Sixth Edition*. Canada: John Wiley & Sons, Inc. pp. 255–257. ISBN 978-1-118-31417-3.
- [5] Suetonius Tranquillus, Gaius (2008). *Lives of the Caesars (Oxford World's Classics)*. New York: Oxford University Press. p. 28. ISBN 978-0199537563.
- [6] Singh, Simon (2000). *The Code Book*. Anchor. pp. 289–290. ISBN 0-385-49532-3.
- [7] Cherdantseva Y. and Hilton J.: "Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals". In: *Organizational, Legal, and Technological Dimensions of Information System Administrator*. Almeida F., Portela, I. (eds.). IGI Global Publishing. (2013)
- [8] ISO/IEC 27000:2009 (E). (2009). Information technology - Security techniques - Information security management systems - Overview and vocabulary. ISO/IEC.

- [9] Committee on National Security Systems: National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, 26 April 2010.
- [10] ISACA. (2008). Glossary of terms, 2008. Retrieved from <http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf>
- [11] Pipkin, D. (2000). *Information security: Protecting the global enterprise*. New York: Hewlett-Packard Company.
- [12] B., McDermott, E., & Geer, D. (2001). Information security is information risk management. In Proceedings of the 2001 Workshop on New Security Paradigms NSPW '01, (pp. 97 – 104). ACM. doi:10.1145/508171.508187
- [13] Anderson, J. M. (2003). “Why we need a new definition of information security”. *Computers & Security*. **22** (4): 308–313. doi:10.1016/S0167-4048(03)00407-3.
- [14] Venter, H. S.; Elof, J. H. P. (2003). “A taxonomy for information security technologies”. *Computers & Security*. **22** (4): 299–307. doi:10.1016/S0167-4048(03)00406-1.
- [15] [https://www.isc2.org/uploadedFiles/\(ISC\)2_Public_Content/2013%20Global%20Information%20Security%20Workforce%20Study%20Feb%202013.pdf](https://www.isc2.org/uploadedFiles/(ISC)2_Public_Content/2013%20Global%20Information%20Security%20Workforce%20Study%20Feb%202013.pdf)
- [16] Perrin, Chad. “The CIA Triad” . Retrieved 31 May 2012.
- [17] “Engineering Principles for Information Technology Security” (PDF). csrc.nist.gov.
- [18] “oecd.org” (PDF). Archived from the original (PDF) on May 16, 2011. Retrieved 2014-01-17.
- [19] “NIST Special Publication 800-27 Rev A” (PDF). csrc.nist.gov.
- [20] Aceituno, Vicente. “Open Information Security Maturity Model” . Retrieved 12 February 2017.
- [21] Boritz, J. Efrim. “IS Practitioners' Views on Core Concepts of Information Integrity” . *International Journal of Accounting Information Systems*. Elsevier. **6** (4): 260–279. doi:10.1016/j.accinf.2005.07.001. Retrieved 12 August 2011.
- [22] Loukas, G.; Oke, G. (September 2010) [August 2009]. “Protection Against Denial of Service Attacks: A Survey” (PDF). *Comput. J.* **53** (7): 1020–1037. doi:10.1093/comjnl/bxp078.
- [23] ISACA (2006). *CISA Review Manual 2006*. Information Systems Audit and Control Association. p. 85. ISBN 1-933284-15-3.
- [24] Spagnoletti, Paolo; Resca A. (2008). “The duality of Information Security Management: fighting against predictable and unpredictable threats” . *Journal of Information System Security*. **4** (3): 46–62.
- [25] Kiountouzis, E.A.; Kokolakis, S.A. *Information systems security: facing the information society of the 21st century*. London: Chapman & Hall, Ltd. ISBN 0-412-78120-4.
- [26] “NIST SP 800-30 Risk Management Guide for Information Technology Systems” (PDF). Retrieved 2014-01-17.
- [27]
- [28] “Segregation of Duties Control matrix” . ISACA. 2008. Archived from the original on 3 July 2011. Retrieved 2008-09-30.
- [29] Shon Harris (2003). *All-in-one CISSP Certification Exam Guide* (2nd ed.). Emeryville, California: McGraw-Hill/Osborne. ISBN 0-07-222966-7.
- [30] itpi.org Archived December 10, 2013, at the Wayback Machine.
- [31] “book summary of The Visible Ops Handbook: Implementing ITIL in 4 Practical and Auditable Steps” . wikisummaries.org. Retrieved 2016-06-22.
- [32] “The Disaster Recovery Plan” . Sans Institute. Retrieved 7 February 2012.
- [33] Lim, Joo S., et al. “Exploring the Relationship between Organizational Culture and Information Security Culture.” Australian Information Security Management Conference.
- [34]
- [35] Schlienger, Thomas; Teufel, Stephanie (2003). “Information security culture-from analysis to change” . *South African Computer Journal*. **31**: 46–52.
- [36] “BSI-Standards” . BSI. Retrieved 29 November 2013.
- Anderson, D., Reimers, K. and Barreto, C. (March 2014). Post-Secondary Education Network Security: Results of Addressing the End-User Challenge.publication date Mar 11, 2014 publication description INTED2014 (International Technology, Education, and Development Conference)

1.16 External links

- DoD IA Policy Chart on the DoD Information Assurance Technology Analysis Center web site.
- patterns & practices Security Engineering Explained
- Open Security Architecture- Controls and patterns to secure IT systems
- IWS - Information Security Chapter
- Ross Anderson's book "Security Engineering"

Chapter 2

Internet security

Internet security is a branch of **computer security** specifically related to the **Internet**, often involving browser security but also **network security** on a more general level as it applies to other applications or **operating systems** on a whole. Its objective is to establish rules and measures to use against attacks over the Internet.^{*[1]} The Internet represents an insecure channel for exchanging information leading to a high risk of **intrusion** or fraud, such as **phishing**.^{*[2]} Different methods have been used to protect the transfer of data, including **encryption** and from-the-ground-up engineering.^{*[3]}

2.1 Threats

2.1.1 Malicious software

A computer user can be tricked or forced into downloading software onto a computer that is of malicious intent. Such software comes in many forms, such as viruses, Trojan horses, spyware, and worms.

- **Malware**, short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to some deficiency. The term **badware** is sometimes used, and applied to both true (malicious) malware and unintentionally harmful software.
- A **botnet** is a network of **zombie computers** that have been taken over by a robot or bot that performs large-scale malicious acts for the creator of the botnet.
- **Computer Viruses** are programs that can replicate their structures or effects by infecting other files or structures on a computer. The common use of a virus is to take over a computer to steal data.
- **Computer worms** are programs that can replicate themselves throughout a computer network, performing malicious tasks throughout.
- **Ransomware** is a type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed.
- **Scareware** is scam software with malicious payloads, usually of limited or no benefit, that are sold to consumers via certain unethical marketing practices. The selling approach uses social engineering to cause shock, anxiety, or the perception of a threat, generally directed at an unsuspecting user.
- **Spyware** refers to programs that surreptitiously monitor activity on a computer system and report that information to others without the user's consent.
- A **Trojan horse**, commonly known as a *Trojan*, is a general term for malicious software that pretends to be harmless, so that a user willingly allows it to be downloaded onto the computer.
- **KeyLogger**, **Keystroke logging**, often referred to as **keylogging** or **keyboard capturing**, is the action of recording (logging) the keys struck on a keyboard

2.1.2 Denial-of-service attacks

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. According to businesses who participated in an international business security survey, 25% of respondents experienced a DoS attack in 2007 and 16.8% experienced one in 2010.*[4]

2.1.3 Phishing

Main article: Phishing

Phishing occurs when the attacker pretends to be a trustworthy entity, either via email or web page. Victims are directed to fake web pages, which are dressed to look legitimate, via spoof emails, instant messenger/social media or other avenues. Often tactics such as email spoofing are used to make emails appear to be from legitimate senders, or long complex subdomains hide the real website host.*[5]*[6] Insurance group RSA said that phishing accounted for worldwide losses of \$1.5 billion in 2012.*[7]

2.1.4 Application vulnerabilities

Main article: Application security

Applications used to access Internet resources may contain security vulnerabilities such as memory safety bugs or flawed authentication checks. The most severe of these bugs can give network attackers full control over the computer. Most security applications and suites are incapable of adequate defense against these kinds of attacks.*[8]*[9]

2.2 Remedies

2.2.1 Network layer security

TCP/IP protocols may be secured with cryptographic methods and security protocols. These protocols include Secure Sockets Layer (SSL), succeeded by Transport Layer Security (TLS) for web traffic, Pretty Good Privacy (PGP) for email, and IPsec for the network layer security.

2.2.2 Internet Protocol Security (IPsec)

IPsec is designed to protect TCP/IP communication in a secure manner. It is a set of security extensions developed by the Internet Task Force (IETF). It provides security and authentication at the IP layer by transforming data using encryption. Two main types of transformation that form the basis of IPsec: the Authentication Header (AH) and ESP. These two protocols provide data integrity, data origin authentication, and anti-replay service. These protocols can be used alone or in combination to provide the desired set of security services for the Internet Protocol (IP) layer.

The basic components of the IPsec security architecture are described in terms of the following functionalities:

- Security protocols for AH and ESP
- Security association for policy management and traffic processing
- Manual and automatic key management for the Internet key exchange (IKE)
- Algorithms for authentication and encryption

The set of security services provided at the IP layer includes access control, data origin integrity, protection against replays, and confidentiality. The algorithm allows these sets to work independently without affecting other parts of the implementation. The IPsec implementation is operated in a host or security gateway environment giving protection to IP traffic.

2.2.3 Security token

Some online sites offer customers the ability to use a six-digit code which randomly changes every 30–60 seconds on a **security token**. The keys on the security token have built in mathematical computations and manipulate numbers based on the current time built into the device. This means that every thirty seconds there is only a certain array of numbers possible which would be correct to validate access to the online account. The website that the user is logging into would be made aware of that device's serial number and would know the computation and correct time built into the device to verify that the number given is indeed one of the handful of six-digit numbers that works in that given 30-60 second cycle. After 30–60 seconds the device will present a new random six-digit number which can log into the website.*[10]

2.2.4 Electronic mail security

Background

Email messages are composed, delivered, and stored in a multiple step process, which starts with the message's composition. When the user finishes composing the message and sends it, the message is transformed into a standard format: an **RFC 2822** formatted message. Afterwards, the message can be transmitted. Using a network connection, the mail client, referred to as a **mail user agent** (MUA), connects to a **mail transfer agent** (MTA) operating on the mail server. The mail client then provides the sender's identity to the server. Next, using the mail server commands, the client sends the recipient list to the mail server. The client then supplies the message. Once the mail server receives and processes the message, several events occur: recipient server identification, connection establishment, and message transmission. Using **Domain Name System** (DNS) services, the sender's mail server determines the mail server(s) for the recipient(s). Then, the server opens up a connection(s) to the recipient mail server(s) and sends the message employing a process similar to that used by the originating client, delivering the message to the recipient(s).

Pretty Good Privacy (PGP)

Pretty Good Privacy provides confidentiality by encrypting messages to be transmitted or data files to be stored using an encryption algorithm such as **Triple DES** or **CAST-128**. Email messages can be protected by using cryptography in various ways, such as the following:

- Signing an email message to ensure its integrity and confirm the identity of its sender.
- Encrypting the body of an email message to ensure its confidentiality.
- Encrypting the communications between mail servers to protect the confidentiality of both message body and message header.

The first two methods, message signing and message body encryption, are often used together; however, encrypting the transmissions between mail servers is typically used only when two organizations want to protect emails regularly sent between each other. For example, the organizations could establish a **virtual private network** (VPN) to encrypt the communications between their mail servers over the Internet.*[11] Unlike methods that can only encrypt a message body, a VPN can encrypt entire messages, including email header information such as senders, recipients, and subjects. In some cases, organizations may need to protect header information. However, a VPN solution alone cannot provide a message signing mechanism, nor can it provide protection for email messages along the entire route from sender to recipient.

Multipurpose Internet Mail Extensions (MIME)

MIME transforms non-ASCII data at the sender's site to Network Virtual Terminal (NVT) ASCII data and delivers it to client's **Simple Mail Transfer Protocol** (SMTP) to be sent through the Internet.*[12] The server **SMTP** at the receiver's side receives the NVT ASCII data and delivers it to MIME to be transformed back to the original non-ASCII data.

Message Authentication Code

A Message authentication code (MAC) is a cryptography method that uses a secret key to encrypt a message. This method outputs a MAC value that can be decrypted by the receiver, using the same secret key used by the sender. The Message Authentication Code protects both a message's data integrity as well as its authenticity.*[13]

2.2.5 Firewalls

A computer firewall controls access between networks. It generally consists of gateways and filters which vary from one firewall to another. Firewalls also screen network traffic and are able to block traffic that is dangerous. Firewalls act as the intermediate server between SMTP and Hypertext Transfer Protocol (HTTP) connections.*[14]

Role of firewalls in web security

Firewalls impose restrictions on incoming and outgoing Network packets to and from private networks. Incoming or outgoing traffic must pass through the firewall; only authorized traffic is allowed to pass through it. Firewalls create checkpoints between an internal private network and the public Internet, also known as *choke points* (borrowed from the identical military term of a combat limiting geographical feature). Firewalls can create choke points based on IP source and TCP port number. They can also serve as the platform for IPsec. Using tunnel mode capability, firewall can be used to implement VPNs. Firewalls can also limit network exposure by hiding the internal network system and information from the public Internet.

Types of firewall

Packet filter A packet filter is a first generation firewall that processes network traffic on a packet-by-packet basis. Its main job is to filter traffic from a remote IP host, so a router is needed to connect the internal network to the Internet. The router is known as a screening router, which screens packets leaving and entering the network.

Stateful packet inspection In a stateful firewall the circuit-level gateway is a proxy server that operates at the network level of an Open Systems Interconnection (OSI) model and statically defines what traffic will be allowed. Circuit proxies will forward Network packets (formatted unit of data) containing a given port number, if the port is permitted by the algorithm. The main advantage of a proxy server is its ability to provide Network Address Translation (NAT), which can hide the user's IP address from the Internet, effectively protecting all internal information from the Internet.

Application-level gateway An application-level firewall is a third generation firewall where a proxy server operates at the very top of the OSI model, the IP suite application level. A network packet is forwarded only if a connection is established using a known protocol. Application-level gateways are notable for analyzing entire messages rather than individual packets of data when the data are being sent or received.

2.2.6 Browser choice

Main article: Browser security

Web browser statistics tend to affect the amount a Web browser is exploited. For example, Internet Explorer 6, which used to own a majority of the Web browser market share,*[15] is considered extremely insecure*[16] because vulnerabilities were exploited due to its former popularity. Since browser choice is now more evenly distributed (Internet Explorer at 28.5%, Firefox at 18.4%, Google Chrome at 40.8%, and so on),*[15] vulnerabilities are exploited in many different browsers.*[17]*[18]*[19]

2.3 Internet security products

2.3.1 Antivirus

Antivirus software and Internet security programs can protect a programmable device from attack by detecting and eliminating viruses; Antivirus software was mainly shareware in the early years of the Internet, but there are now several free security applications on the Internet to choose from for all platforms.* [20]

2.3.2 Password managers

A **password manager** is a software application that helps a user store and organize passwords. Password managers usually store passwords encrypted, requiring the user to create a master password; a single, ideally very strong password which grants the user access to their entire password database.* [21]

2.3.3 Security suites

So called *security suites* were first offered for sale in 2003 (McAfee) and contain a suite of firewalls, anti-virus, anti-spyware and more.* [22] They also offer theft protection, portable storage device safety check, private Internet browsing, cloud anti-spam, a file shredder or make security-related decisions (answering popup windows) and several were free of charge.* [23]

2.4 See also

- Comparison of antivirus software
- Comparison of firewalls
- Cyberspace Electronic Security Act (in the US)
- *Firewalls and Internet Security* (book)
- Goatse Security
- Internet Crime Complaint Center
- Identity Driven Networking
- Internet safety
- Network security policy
- Outpost Security Suite
- Usability of web authentication systems
- Web literacy (Security)

2.5 References

- [1] Gralla, Preston (2007). *How the Internet Works*. Indianapolis: Que Pub. ISBN 0-7897-2132-5.
- [2] Rhee, M. Y. (2003). *Internet Security: Cryptographic Principles, Algorithms and Protocols*. Chichester: Wiley. ISBN 0-470-85285-2.
- [3] An example of a completely re-engineered computer is the **Librem** laptop which uses components certified by web-security experts. It was launched after a crowd funding campaign in 2015.
- [4] “Information Security: A Growing Need of Businesses and Industries Worldwide”. *University of Alabama at Birmingham Business Program*. Retrieved 20 November 2014.
- [5] Ramzan, Zulfikar (2010). “Phishing attacks and countermeasures” . In Stamp, Mark & Stavroulakis, Peter. *Handbook of Information and Communication Security*. Springer. ISBN 9783642041174.

- [6] Van der Merwe, A J, Loock, M, Dabrowski, M. (2005), Characteristics and Responsibilities involved in a Phishing Attack, Winter International Symposium on Information and Communication Technologies, Cape Town, January 2005.
- [7] “2012 Global Losses From Phishing Estimated At \$1.5 Bn” . FirstPost. February 20, 2013. Retrieved December 21, 2014.
- [8] “Improving Web Application Security: Threats and Countermeasures” . *msdn.microsoft.com*. Retrieved 2016-04-05.
- [9] “Justice Department charges Russian spies and criminal hackers in Yahoo intrusion” . *Washington Post*. Retrieved 15 March 2017.
- [10] Margaret Rouse (September 2005). “What is a security token?”. SearchSecurity.com. Retrieved 2014-02-14.
- [11] “Virtual Private Network” . NASA. Retrieved 2014-02-14.
- [12] Asgaut Eng (1996-04-10). “Network Virtual Terminal” . The Norwegian Institute of Technology ppv.org. Retrieved 2014-02-14.
- [13] “What Is a Message Authentication Code?”. Wisegeek.com. Retrieved 2013-04-20.
- [14] “Firewalls - Internet Security” . sites.google.com. Retrieved 2016-06-30.
- [15] “Browser Statistics” . W3Schools.com. Retrieved 2011-08-10.
- [16] Bradly, Tony. “It's Time to Finally Drop Internet Explorer 6” . PCWorld.com. Retrieved 2010-11-09.
- [17] Messmer, Ellen and NetworkWorld (2010-11-16). “Google Chrome Tops 'Dirty Dozen' Vulnerable Apps List” . PC-World.com. Retrieved 2010-11-09.
- [18] Keizer, Greg (2009-07-15). “Firefox 3.5 Vulnerability Confirmed” . PCWorld.com. Retrieved 2010-11-09.
- [19] Skinner, Carrie-Ann. “Opera Plugs “Severe” Browser Hole” . PC World.com. Archived from the original on May 20, 2009. Retrieved 2010-11-09.
- [20] Larkin, Eric (2008-08-26). “Build Your Own Free Security Suite” . Retrieved 2010-11-09.
- [21] “USE A FREE PASSWORD MANAGER” (PDF). scsccbkk.org.
- [22] Rebbapragada, Narasu. “All-in-one Security” . PC World.com. Archived from the original on October 27, 2010. Retrieved 2010-11-09.
- [23] “Free products for PC security” . 2015-10-08.

2.6 External links

- National Institute of Standards and Technology (NIST.gov) - Information Technology portal with links to computer- and cyber security
- National Institute of Standards and Technology (NIST.gov) -Computer Security Resource Center -Guidelines on Electronic Mail Security, version 2
- The Internet Engineering Task Force.org - UK organization -IP Authentication Header 1998
- The Internet Engineering Task Force.org - UK organization -Encapsulating Security Payload
- Wireless Safety.org - Up to date info on security threats, news stories, and step by step tutorials
- PwdHash Stanford University - Firefox & IE browser extensions that transparently convert a user's password into a domain-specific password.
- Internet security.net - by JC Montejo & Goio Miranda (free security programs), est 2007.
- Internet and Data Security Guide UK anonymous membership site
- Cybertelecom.org Security - surveying federal Internet security work
- DSL Reports.com- Broadband Reports, FAQs and forums on Internet security, est 1999
- FBI Safe Online Surfing Internet Challenge - Cyber Safety for Young Americans (FBI)

Chapter 3

Cyberwarfare

“Cyberwar” redirects here. For the video game, see [Cyberwar \(video game\)](#). For the 2004 movie also known as Cyber Wars, see [Avatar \(2004 film\)](#).

Not to be confused with Electronic warfare or software wars.

Cyberwarfare involves the **battlespace** use and targeting of computers and networks in **warfare**. It involves both offensive and defensive operations pertaining to the threat of **cyberattacks**, espionage and sabotage. There has been controversy over whether such operations can duly be called “**war**”. Nevertheless, nations have been developing their capabilities and engaged in cyberwarfare either as an aggressor, defendant, or both.

3.1 Definition

Cyberwarfare has been defined as “actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption”, ^{*[1]}:6 but other definitions also include non-state actors, such as terrorist groups, companies, political or ideological extremist groups, **hacktivists**, and transnational criminal organizations.^{*[2] * [3] * [4] * [5] * [6]}

Some governments have made it an integral part of their overall military strategy, with some having invested heavily in cyberwarfare capability.^{*[7] * [8] * [9] * [10]} Cyberwarfare is essentially a formalized version of penetration testing in which a government entity has established it as a warfighting capability.^{*[11]}

This capability uses the same set of penetration testing methodologies but applies them, in the case of United States doctrine, in a strategical way to

- Prevent cyber attacks against critical infrastructure
- Reduce national vulnerability to cyber attacks
- Minimize damage and recovery time from cyber attacks^{*[11]}

Offensive operations are also part of these national level strategies for officially declared wars as well as undeclared secretive operations.^{*[12]}

3.2 Types of threat

- **Cyberattacks**, where immediate damage or disruption is caused are the main concern.^{*[13]}
- **Cyber espionage**, which can provide the information needed to make a successful **cyberattack** or scandal to launch an **information warfare**.

3.2.1 Espionage

Traditional espionage is not an act of war, nor is cyber-espionage,*[14] and both are generally assumed to be ongoing between major powers. Despite this assumption, some incidents can cause serious tensions between nations, and are often described as “attacks”. For example:

- Massive spying by the US on many countries, revealed by Edward Snowden.
- After the NSA's spying on Germany's Chancellor Angela Merkel was revealed, the Chancellor compared the NSA with the Stasi.*[15]
- The NSA recording nearly every cell phone conversation in the Bahamas, without the Bahamian government's permission,*[16] and similar programmes in Kenya, the Philippines, Mexico and Afghanistan.*[17]
- The "Titan Rain" probes of American defence contractors computer systems since 2003.*[18]
- The Office of Personnel Management data breach, in the US, widely attributed to China.*[19]*[20]

3.2.2 Sabotage

Computers and satellites that coordinate other activities are vulnerable components of a system and could lead to the disruption of equipment. Compromise of military systems, such as C4ISTAR components that are responsible for orders and communications could lead to their interception or malicious replacement. Power, water, fuel, communications, and transportation infrastructure all may be vulnerable to disruption. According to Clarke, the civilian realm is also at risk, noting that the security breaches have already gone beyond stolen credit card numbers, and that potential targets can also include the electric power grid, trains, or the stock market.*[21]

In mid July 2010, security experts discovered a malicious software program called Stuxnet that had infiltrated factory computers and had spread to plants around the world. It is considered “the first attack on critical industrial infrastructure that sits at the foundation of modern economies,” notes *The New York Times*.*[22]

Stuxnet, while extremely effective in delaying Iran's nuclear program for the development of nuclear weaponry, came at a high cost. For the first time, it became clear that not only could cyber weapons be defensive but they could be offensive. The large decentralization and scale of cyberspace makes it extremely difficult to direct from a policy perspective. Non-state actors can play as large a part in the cyberwar space as state actors, which leads to dangerous, sometimes disastrous, consequences. Small groups of highly skilled malware developers are able to as effectively impact global politics and cyber warfare as large governmental agencies. A major aspect of this ability lies in the willingness of these groups to share their exploits and developments on the web as a form of arms proliferation. This allows lesser hackers to become more proficient in creating the large scale attacks that once only a small handful were skillful enough to manage. In addition, thriving black markets for these kinds of cyber weapons are buying and selling these cyber capabilities to the highest bidder without regard for consequences.*[23]

Denial-of-service attack

Main article: Denial-of-service attack

In computing, a denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers. DoS attacks may not be limited to computer-based methods, as strategic physical attacks against infrastructure can be just as devastating. For example, cutting undersea communication cables may severely cripple some regions and countries with regards to their information warfare ability.

Electrical power grid

The federal government of the United States admits that the electric power grid is susceptible to cyberwarfare.*[24]*[25] The United States Department of Homeland Security works with industries to identify vulnerabilities and to help industries enhance the security of control system networks. The federal government is also working to ensure that

security is built in as the next generation of “smart grid” networks are developed.*[26] In April 2009, reports surfaced that China and Russia had infiltrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national security officials.*[27] The North American Electric Reliability Corporation (NERC) has issued a public notice that warns that the electrical grid is not adequately protected from cyber attack.*[28] China denies intruding into the U.S. electrical grid.*[29]*[30] One countermeasure would be to disconnect the power grid from the Internet and run the net with droop speed control only.*[31]*[32] Massive power outages caused by a cyber attack could disrupt the economy, distract from a simultaneous military attack, or create a national trauma.

Howard Schmidt, former Cyber-Security Coordinator of the US, commented on those possibilities:*

It's possible that hackers have gotten into administrative computer systems of utility companies, but says those aren't linked to the equipment controlling the grid, at least not in developed countries. [Schmidt] has never heard that the grid itself has been hacked.

On 23 December 2015, what is believed to be a first known successful cyber attack on a power grid took place in Ukraine leading to temporary blackouts.*[34] The cyber attack is attributed to the Russian advanced persistent threat group called “Sandworm”*[35] and it was performed during an ongoing military confrontation.

3.3 Motivations

3.3.1 Military

In the U.S., General Keith B. Alexander, first head of the recently formed USCYBERCOM, told the Senate Armed Services Committee that computer network warfare is evolving so rapidly that there is a “mismatch between our technical capabilities to conduct operations and the governing laws and policies. Cyber Command is the newest global combatant and its sole mission is cyberspace, outside the traditional battlefields of land, sea, air and space.” It will attempt to find and, when necessary, neutralize cyberattacks and to defend military computer networks.*[36]

Alexander sketched out the broad battlefield envisioned for the computer warfare command, listing the kind of targets that his new headquarters could be ordered to attack, including “traditional battlefield prizes – command-and-control systems at military headquarters, air defense networks and weapons systems that require computers to operate.”*[36]

One cyber warfare scenario, Cyber ShockWave, which was wargamed on the cabinet level by former administration officials, raised issues ranging from the National Guard to the power grid to the limits of statutory authority.*[37]*[38]*[39]*[40]

The distributed nature of internet based attacks means that it is difficult to determine motivation and attacking party, meaning that it is unclear when a specific act should be considered an act of war.*[41]

Examples of cyberwarfare driven by political motivations can be found worldwide. In 2008, Russia began a cyber attack on the Georgian government website, which was carried out along with Georgian military operations in South Ossetia. In 2008, Chinese 'nationalist hackers' attacked CNN as it reported on Chinese repression on Tibet.*[42]

Jobs in cyberwarfare have become increasingly popular in the military. The United States Navy actively recruits for cyber warfare engineers.*[43] The US Army has their Cyber Command where they actively recruit for cryptologic network warfare specialists.

3.3.2 Civil

Potential targets in internet sabotage include all aspects of the Internet from the backbones of the web, to the internet service providers, to the varying types of data communication mediums and network equipment. This would include: web servers, enterprise information systems, client server systems, communication links, network equipment, and the desktops and laptops in businesses and homes. Electrical grids and telecommunication systems are also deemed vulnerable, especially due to current trends in automation.

3.3.3 Hacktivism

Politically motivated hacktivism involves the subversive use of computers and computer networks to promote an agenda, and can potentially extend to attacks, theft and virtual sabotage that could be seen as cyberwarfare – or mistaken for it.*[44]

3.3.4 Private sector

Further information: Cyber-arms industry and Market for zero-day exploits

Computer hacking represents a modern threat in ongoing global conflicts and industrial espionage and as such is presumed to widely occur.*[45] It is typical that this type of crime is underreported to the extent they are known. According to McAfee's George Kurtz, corporations around the world face millions of cyberattacks a day. “Most of these attacks don't gain any media attention or lead to strong political statements by victims.” * [46] This type of crime is usually financially motivated.

3.3.5 Non-profit research

But not all examinations with the issue of cyberwarfare are achieving profit or personal gain. There are still institutes and companies like the University of Cincinnati or the Kaspersky Security Lab which are trying to increase the sensibility of this topic by researching and publishing of new security threats.

3.4 By region

Approximately 120 countries have been developing ways to use the Internet as a weapon and target financial markets, government computer systems and utilities.*[47]

3.4.1 Asia

China

Main article: Cyberwarfare in the People's Republic of China

See also: Chinese intelligence activity abroad, Chinese intelligence operations in the United States, and Chinese Information Operations and Information Warfare

Foreign Policy magazine puts the size of China's “hacker army” at anywhere from 50,000 to 100,000 individuals.*[48]

Diplomatic cables highlight US concerns that China is using access to Microsoft source code and 'harvesting the talents of its private sector' to boost its offensive and defensive capabilities.*[49]

A 2008 article in the *Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies* by Jason Fritz alleges that the Chinese government from 1995 to 2008 was involved in a number of high-profile cases of espionage, primarily through the use of a “decentralized network of students, business people, scientists, diplomats, and engineers from within the Chinese Diaspora”. * [50] A defector in Belgium, purportedly an agent, claimed that there were hundreds of spies in industries throughout Europe, and on his defection to Australia Chinese diplomat Chen Yonglin said there were over 1,000 such in that country. In 2007, a Russian executive was sentenced to 11 years for passing information about the rocket and space technology organization to China. Targets in the United States have included 'aerospace engineering programs, space shuttle design, C4ISR data, high-performance computers, Nuclear weapon design, cruise missile data, semiconductors, integrated circuit design, and details of US arms sales to Taiwan'. * [50]

While China continues to be held responsible for a string of cyber-attacks on a number of public and private institutions in the United States, India, Russia, Canada, and France, the Chinese government denies any involvement in cyber-spying campaigns. The administration maintains the position that China is not the threat but rather the victim of an

increasing number of cyber-attacks. Most reports about China's cyber warfare capabilities have yet to be confirmed by the Chinese government.*[51]

According to Fritz, China has expanded its cyber capabilities and military technology by acquiring foreign military technology.*[52] Fritz states that the Chinese government uses "new space-based surveillance and intelligence gathering systems, Anti-satellite weapon, anti-radar, infrared decoys, and false target generators" to assist in this quest, and that they support their "informationization" of their military through "increased education of soldiers in cyber warfare; improving the information network for military training, and has built more virtual laboratories, digital libraries and digital campuses."* [52] Through this informationization, they hope to prepare their forces to engage in a different kind of warfare, against technically capable adversaries.*[53] Many recent news reports link China's technological capabilities to the beginning of a new 'cyber cold war.'*[54]

In response to reports of cyberattacks by China against the United States, Amitai Etzioni of the Institute for Communitarian Policy Studies has suggested that China and the United States agree to a policy of mutually assured restraint with respect to cyberspace. This would involve allowing both states to take the measures they deem necessary for their self-defense while simultaneously agreeing to refrain from taking offensive steps; it would also entail vetting these commitments.*[55]

Operation Shady RAT is an ongoing series of cyber attacks starting mid-2006, reported by Internet security company McAfee in August 2011. China is widely believed to be the state actor behind these attacks which hit at least 72 organizations including governments and defense contractors.*[56]

India

See also: National Cyber Security Policy 2013

The Department of Information Technology created the Indian Computer Emergency Response Team (CERT-In) in 2004 to thwart cyber attacks in India.*[57] That year, there were 23 reported cyber security breaches. In 2011, there were 13,301. That year, the government created a new subdivision, the National Critical Information Infrastructure Protection Centre (NCIIPC) to thwart attacks against energy, transport, banking, telecom, defence, space and other sensitive areas.

The Executive Director of the Nuclear Power Corporation of India (NPCIL) stated in February 2013 that his company alone was forced to block up to ten targeted attacks a day. CERT-In was left to protect less critical sectors.

A high-profile cyber attack on 12 July 2012 breached the email accounts of about 12,000 people, including those of officials from the Ministry of External Affairs, Ministry of Home Affairs, Defence Research and Development Organisation (DRDO), and the Indo-Tibetan Border Police (ITBP).* [57] A government-private sector plan being overseen by National Security Advisor (NSA) Shivshankar Menon began in October 2012, and intends to beef up India's cyber security capabilities in the light of a group of experts findings that India faces a 470,000 shortfall of such experts despite the country's reputation of being an IT and software powerhouse.*[58]

In February 2013, Information Technology Secretary J. Satyanarayana stated that the NCIIPC was finalizing policies related to national cyber security that would focus on domestic security solutions, reducing exposure through foreign technology.*[57] Other steps include the isolation of various security agencies to ensure that a synchronised attack could not succeed on all fronts and the planned appointment of a National Cyber Security Coordinator. As of that month, there had been no significant economic or physical damage to India related to cyber attacks.

On 26 November 2010, a group calling itself the Indian Cyber Army hacked the websites belonging to the Pakistan Army and the others belong to different ministries, including the Ministry of Foreign Affairs, Ministry of Education, Ministry of Finance, Pakistan Computer Bureau, Council of Islamic Ideology, etc. The attack was done as a revenge for the Mumbai terrorist attacks.*[59]

On 4 December 2010, a group calling itself the Pakistan Cyber Army hacked the website of India's top investigating agency, the Central Bureau of Investigation (CBI). The National Informatics Center (NIC) has begun an inquiry.*[60]

In July 2016, Cymmetria researchers discovered and revealed the cyber attack dubbed 'Patchwork', which compromised an estimated 2500 corporate and government agencies using code stolen from GitHub and the dark web. Examples of weapons used are an exploit for the Sandworm vulnerability (CVE-2014-4114), a compiled AutoIt script, and UAC bypass code dubbed UACME. Targets are believed to be mainly military and political assignments around Southeast Asia and the South China Sea and the attackers are believed to be of Indian origin and gathering intelligence from influential parties.*[61]*[62]

Kyrgyzstan

In 2007 the website of the Central Electoral Commission of Kyrgyzstan was defaced during its election. The message left on the website read “This site has been hacked by Dream of Estonian organization”. During the election campaigns and riots preceding the election, there were cases of Denial-of-service attacks against the Kyrgyz ISPs.*[63]

Philippines

The Chinese are being blamed after a cybersecurity company, F-Secure Labs, found a malware, NanHaiShu, which targeted the Philippines Department of Justice. It sent information in an infected machine to a server with a Chinese IP address. The malware which is considered particularly sophisticated in nature was introduced by phishing emails that were designed to look like they were coming from an authentic sources. The information sent is believed to be relating to the South China Sea legal case.*[64]

Russia

Main article: Cyberwarfare in Russia

When Russia was still the Soviet Union in 1982, a portion of its Trans-Siberia pipeline within its territory exploded, allegedly due to computer malware implanted in the pirated Canadian software by the Central Intelligence Agency. The malware caused the SCADA system running the pipeline to malfunction. The “Farewell Dossier” provided information on this attack, and wrote that compromised computer chips would become a part of Soviet military equipment, flawed turbines would be placed in the gas pipeline, and defective plans would disrupt the output of chemical plants and a tractor factor. This caused the “most monumental nonnuclear explosion and fire ever seen from space.” However, the Soviet Union did not blame the United States for the attack.*[65]

Russian, South Ossetian, Georgian and Azerbaijani sites were attacked by hackers during the 2008 South Ossetia War.*[66]

Russian-led cyberattacks

Main articles: 2007 cyberattacks on Estonia, Cyberattacks during the 2008 South Ossetia war, and Russian intervention in the 2016 United States presidential election

It has been claimed that Russian security services organized a number of denial of service attacks as a part of their cyber-warfare against other countries,*[67] most notably the 2007 cyberattacks on Estonia and the 2008 cyberattacks on Russia, South Ossetia, Georgia, and Azerbaijan.*[68] One identified young Russian hacker said that he was paid by Russian state security services to lead hacking attacks on NATO computers. He was studying computer sciences at the *Department of the Defense of Information*. His tuition was paid for by the FSB.*[69]

South Korea

Main article: 2013 South Korea cyberattack

In July 2009, there were a series of coordinated denial of service attacks against major government, news media, and financial websites in South Korea and the United States.*[70] While many thought the attack was directed by North Korea, one researcher traced the attacks to the United Kingdom.*[71]

In July 2011, the South Korean company SK Communications was hacked, resulting in the theft of the personal details (including names, phone numbers, home and email addresses and resident registration numbers) of up to 35 million people. A trojaned software update was used to gain access to the SK Communications network. Links exist between this hack and other malicious activity and it is believed to be part of a broader, concerted hacking effort.*[72]

With ongoing tensions on the Korean Peninsula, South Korea's defense ministry stated that South Korea was going to improve cyber-defense strategies in hopes of preparing itself from possible cyber attacks. In March 2013, South Korea's major banks – Shinhan Bank, Woori Bank and NongHyup Bank – as well as many broadcasting stations – KBS, YTN and MBC – were hacked and more than 30,000 computers were affected; it is one of the biggest attacks

South Korea has faced in years.*[73] Although it remains uncertain as to who was involved in this incident, there has been immediate assertions that North Korea is connected, as it threatened to attack South Korea's government institutions, major national banks and traditional newspapers numerous times – in reaction to the sanctions it received from nuclear testing and to the continuation of **Foal Eagle**, South Korea's annual joint military exercise with the United States. North Korea's cyber warfare capabilities raise the alarm for South Korea, as North Korea is increasing its manpower through military academies specializing in hacking. Current figures state that South Korea only has 400 units of specialized personnel, while North Korea has more than 3,000 highly trained hackers; this portrays a huge gap in cyber warfare capabilities and sends a message to South Korea that it has to step up and strengthen its Cyber Warfare Command forces. Therefore, in order to be prepared from future attacks, South Korea and the United States will discuss further about deterrence plans at the Security Consultative Meeting (SCM). At SCM, they plan on developing strategies that focuses on accelerating the deployment of ballistic missiles as well as fostering its defense shield program, known as the Korean Air and Missile Defense.*[74]

3.4.2 Europe

Estonia

In April 2007, Estonia came under cyber attack in the wake of relocation of the Bronze Soldier of Tallinn.*[75] The largest part of the attacks were coming from Russia and from official servers of the authorities of Russia.*[76] In the attack, ministries, banks, and media were targeted.*[77]*[78] This attack on Estonia, a seemingly small Baltic nation, was so effective because of how most of the nation is run online. Estonia has implemented an e-government, where bank services, political elections and taxes are all done online. This attack really hurt Estonia's economy and the people of Estonia. At least 150 people were injured on the first day due to riots in the streets.*[79]

Germany

In 2013, Germany revealed the existence of their 60-person Computer Network Operation unit.*[80] The German intelligence agency, BND, announced it was seeking to hire 130 "hackers" for a new "cyber defence station" unit. In March 2013, BND president **Gerhard Schindler** announced that his agency had observed up to five attacks a day on government authorities, thought mainly to originate in China. He confirmed the attackers had so far only accessed data and expressed concern that the stolen information could be used as the basis of future sabotage attacks against arms manufacturers, telecommunications companies and government and military agencies.*[81] Shortly after **Edward Snowden** leaked details of the U.S. National Security Agency's cyber surveillance system, German Interior Minister **Hans-Peter Friedrich** announced that the BND would be given an additional budget of 100 million Euros to increase their cyber surveillance capability from 5% of total internet traffic in Germany to 20% of total traffic, the maximum amount allowed by German law.*[82]

Netherlands

See also: **Cozy Bear** § Dutch ministries (2017)

In the Netherlands, Cyber Defense is nationally coordinated by the National Cyber Security Centrum (NCSC).*[83] The Dutch Ministry of Defense laid out a cyber strategy in 2011.*[84] The first focus is to improve the cyber defense handled by the Joint IT branch (JIVC). To improve intel operations the intel community in the Netherlands (including the military intel organization MIVD) has set up the Joint Sigit Cyber Unit (JSCU). The ministry of Defense is furthermore setting up an offensive cyber force, called Defensie Cyber Command (DCC),*[85] which will be operational in the end of 2014.

Norway

See also: **Cozy Bear** § Norwegian Government (2017)

Sweden

In January 2017, Sweden's armed forces were subjected to a cyber-attack that caused them to shutdown a so-called Caxcis IT system used in military exercises.*[86]

Ukraine

According to CrowdStrike from 2014 to 2016, the Russian APT Fancy Bear used Android malware to target the Ukrainian Army's Rocket Forces and Artillery. They distributed an infected version of an Android app whose original purpose was to control targeting data for the D-30 Howitzer artillery. The app, used by Ukrainian officers, was loaded with the X-Agent spyware and posted online on military forums. The attack was claimed by CrowdStrike to be successful, with more than 80% of Ukrainian D-30 Howitzers destroyed, the highest percentage loss of any artillery pieces in the army (a percentage that had never been previously reported and would mean the loss of nearly the entire arsenal of the biggest artillery piece of the Ukrainian Armed Forces*[87]).*[88] According to the Ukrainian army this number is incorrect and that losses in artillery weapons “were way below those reported” and that that these losses “have nothing to do with the stated cause”.*[89]

In 2014, the Russians were suspected to use a cyber weapon called “Snake”, or “Ouroboros,” to conduct a cyber attack on Ukraine during a period of political turmoil. The Snake tool kit began spreading into Ukrainian computer systems in 2010. It performed Computer Network Exploitation (CNE), as well as highly sophisticated Computer Network Attacks (CNA).*[90]

On December 23, 2015 the BlackEnergy malware was used in a cyberattack on Ukraine's powergrid that left more than 200,000 people temporarily without power. A mining company and a large railway operator were also victims of the attack.*[91]

United Kingdom

MI6 reportedly infiltrated an Al Qaeda website and replaced the instructions for making a pipe bomb with the recipe for making cupcakes.*[92]

In October 2010, Iain Lobban, the director of the Government Communications Headquarters (GCHQ), said the UK faces a “real and credible” threat from cyber attacks by hostile states and criminals and government systems are targeted 1,000 times each month, such attacks threatened the UK's economic future, and some countries were already using cyber assaults to put pressure on other nations.*[93]

On 12 November 2013, financial organisations in London conducted cyber war games dubbed 'Waking Shark 2'*[94] to simulate massive internet-based attacks against bank and other financial organisations. The Waking Shark 2 cyber war games followed a similar exercise in Wall Street.*[95]

3.4.3 Middle East

Iran

Main article: Cyberwarfare in Iran

See also: Iranian Cyber Army

Further information: Operation Olympic Games, Operation Ababil, Operation Cleaver, and Operation Newscaster

Iran has been both victim and predator of several cyberwarfare operations. Iran is considered an emerging military power in the field.*[96]

In September 2010, Iran was attacked by the Stuxnet worm, thought to specifically target its Natanz nuclear enrichment facility. The worm is said to be the most advanced piece of malware ever discovered and significantly increases the profile of cyberwarfare.*[97]*[98]

Israel

In the 2006 war against Hezbollah, Israel alleges that cyber-warfare was part of the conflict, where the **Israel Defense Forces** (IDF) intelligence estimates several countries in the Middle East used Russian hackers and scientists to operate on their behalf. As a result, Israel attached growing importance to cyber-tactics, and became, along with the U.S., France and a couple of other nations, involved in cyber-war planning. Many international high-tech companies are now locating research and development operations in Israel, where local hires are often veterans of the IDF's elite computer units.^{*[99]} Richard A. Clarke adds that “our Israeli friends have learned a thing or two from the programs we have been working on for more than two decades.”^{*[1]*:8}

In September 2007, Israel carried out an airstrike on Syria dubbed Operation Orchard. U.S. industry and military sources speculated that the Israelis may have used cyberwarfare to allow their planes to pass undetected by radar into Syria.^{*[100]*[101]}

3.4.4 North America

United States

Main article: Cyberwarfare in the United States

Cyberwarfare in the United States is a part of the American military strategy of proactive cyber defence and the use of cyberwarfare as a platform for attack.^{*[102]} The new United States military strategy makes explicit that a cyberattack is *casus belli* just as a traditional act of war.^{*[103]}

In 2013 Cyberwarfare was, for the first time, considered a larger threat than Al Qaeda or terrorism, by many U.S. intelligence officials.^{*[104]} In 2017, Representative Mike Rogers, chairman of the U.S. House Permanent Select Committee on Intelligence, for instance, said that “We are in a cyber war in this country, and most Americans don't know it. And we are not necessarily winning. We have got huge challenges when it comes to cybersecurity.”^{*[105]}

U.S. government security expert Richard A. Clarke, in his book *Cyber War* (May 2010), defines “cyberwarfare” as “actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption.”^{*[1]*:6} *The Economist* describes cyberspace as “the fifth domain of warfare,”^{*[106]} and William J. Lynn, U.S. Deputy Secretary of Defense, states that “as a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain in warfare . . . [which] has become just as critical to military operations as land, sea, air, and space.”^{*[7]}

In 2009, president Barack Obama declared America's digital infrastructure to be a “strategic national asset,” and in May 2010 the Pentagon set up its new U.S. Cyber Command (USCYBERCOM), headed by General Keith B. Alexander, director of the National Security Agency (NSA), to defend American military networks and attack other countries' systems. The EU has set up ENISA (European Union Agency for Network and Information Security) which is headed by Prof. Udo Helmbrecht and there are now further plans to significantly expand ENISA's capabilities. The United Kingdom has also set up a cyber-security and “operations centre” based in Government Communications Headquarters (GCHQ), the British equivalent of the NSA. In the U.S. however, Cyber Command is only set up to protect the military, whereas the government and corporate infrastructures are primarily the responsibility respectively of the Department of Homeland Security and private companies.^{*[106]}

In February 2010, top American lawmakers warned that the “threat of a crippling attack on telecommunications and computer networks was sharply on the rise.”^{*[107]} According to The Lipman Report, numerous key sectors of the U.S. economy along with that of other nations, are currently at risk, including cyber threats to public and private facilities, banking and finance, transportation, manufacturing, medical, education and government, all of which are now dependent on computers for daily operations.^{*[107]} In 2009, president Obama stated that “cyber intruders have probed our electrical grids.”^{*[108]}

The Economist writes that China has plans of “winning informationised wars by the mid-21st century”. They note that other countries are likewise organizing for cyberwar, among them Russia, Israel and North Korea. Iran boasts of having the world's second-largest cyber-army.^{*[106]} James Gosler, a government cybersecurity specialist, worries that the U.S. has a severe shortage of computer security specialists, estimating that there are only about 1,000 qualified people in the country today, but needs a force of 20,000 to 30,000 skilled experts.^{*[109]} At the July 2010 Black Hat computer security conference, Michael Hayden, former deputy director of national intelligence, challenged thousands of attendees to help devise ways to “reshape the Internet's security architecture”, explaining, “You guys made the

cyberworld look like the north German plain.” *[110]

In January 2012, Mike McConnell, the former director of national intelligence at the National Security Agency under president George W. Bush told the Reuters news agency that the U.S. has already launched attacks on computer networks in other countries.*[111] McConnell did not name the country that the U.S. attacked but according to other sources it may have been Iran.*[111] In June 2012 *the New York Times* reported that president Obama had ordered the cyber attack on Iranian nuclear enrichment facilities.*[112]

In August 2010, the U.S. for the first time warned publicly about the Chinese military's use of civilian computer experts in clandestine cyber attacks aimed at American companies and government agencies. The Pentagon also pointed to an alleged China-based computer spying network dubbed GhostNet that was revealed in a research report last year.*[113] The Pentagon stated:

The People's Liberation Army is using “information warfare units” to develop viruses to attack enemy computer systems and networks, and those units include civilian computer professionals. Commander Bob Mehal, will monitor the PLA's buildup of its cyberwarfare capabilities and will continue to develop capabilities to counter any potential threat.*[114]

The United States Department of Defense sees the use of computers and the Internet to conduct warfare in cyberspace as a threat to national security. The United States Joint Forces Command describes some of its attributes:

Cyberspace technology is emerging as an “instrument of power” in societies, and is becoming more available to a country's opponents, who may use it to attack, degrade, and disrupt communications and the flow of information. With low barriers to entry, coupled with the anonymous nature of activities in cyberspace, the list of potential adversaries is broad. Furthermore, the globe-spanning range of cyberspace and its disregard for national borders will challenge legal systems and complicate a nation's ability to deter threats and respond to contingencies.*[115]

In February 2010, the United States Joint Forces Command released a study which included a summary of the threats posed by the internet:*[115]

With very little investment, and cloaked in a veil of anonymity, our adversaries will inevitably attempt to harm our national interests. Cyberspace will become a main front in both irregular and traditional conflicts. Enemies in cyberspace will include both states and non-states and will range from the unsophisticated amateur to highly trained professional hackers. Through cyberspace, enemies will target industry, academia, government, as well as the military in the air, land, maritime, and space domains. In much the same way that airpower transformed the battlefield of World War II, cyberspace has fractured the physical barriers that shield a nation from attacks on its commerce and communication. Indeed, adversaries have already taken advantage of computer networks and the power of information technology not only to plan and execute savage acts of terrorism, but also to influence directly the perceptions and will of the U.S. Government and the American population.

On 6 October 2011, it was announced that Creech AFB's drone and Predator fleet's command and control data stream had been keylogged, resisting all attempts to reverse the exploit, for the past two weeks.*[116] The Air Force issued a statement that the virus had “posed no threat to our operational mission” .*[117]

On 21 November 2011, it was widely reported in the U.S. media that a hacker had destroyed a water pump at the Curran-Gardner Township Public Water District in Illinois.*[118] However, it later turned out that this information was not only false, but had been inappropriately leaked from the Illinois Statewide Terrorism and Intelligence Center.*[119]

According to the *Foreign Policy* magazine, NSA's Tailored Access Operations (TAO) unit “has successfully penetrated Chinese computer and telecommunications systems for almost 15 years, generating some of the best and most reliable intelligence information about what is going on inside the People's Republic of China.” *[120]*[121]

On 24 November 2014. The Sony Pictures Entertainment hack was a release of confidential data belonging to Sony Pictures Entertainment (SPE).

In June 2015, the United States Office of Personnel Management (OPM) announced that it had been the target of a data breach targeting the records of as many as four million people.*[122] Later, FBI Director James Comey put the

number at 18 million.*[123] The *Washington Post* has reported that the attack originated in China, citing unnamed government officials.*[124]

In 2016, Jeh Johnson the United States Secretary of Homeland Security and James Clapper the U.S. Director of National Intelligence issued a joint statement accusing Russia of interfering with the 2016 United States presidential election.*[125] The New York Times reported the Obama administration has formally accused Russia of stealing and disclosing Democratic National Committee emails.*[126] Under U.S. law (50 U.S.C. Title 50 – War and National Defense, Chapter 15 – National Security, Subchapter III Accountability for Intelligence Activities *[127]) there must be a formal *Presidential finding* prior to authorizing a covert attack. U.S. vice president Joe Biden said on the American news interview program *Meet The Press* that the United States will respond.*[128] The New York Times noted that Biden's comment "seems to suggest that Mr. Obama is prepared to order —or has already ordered —some kind of covert action".*[129] On December 29 the United States imposed the most extensive sanctions against Russia since the Cold War,*[130] expelling 35 Russian diplomats from the United States.*[131]*[132]

The United States has used cyberattacks for tactical advantage in Afghanistan.*[133]

In 2014 Barack Obama ordered an intensification of cyberwarfare against North Korea's missile program for sabotaging test launches in their opening seconds.*[134] In 2016 President Barack Obama authorized the planting of cyber weapons in Russian infrastructure in the final weeks of his presidency in response to Moscow's alleged interference in the 2016 presidential election.*[135]

In March 2017, WikiLeaks has published more than 8,000 documents on the CIA. The confidential documents, codenamed Vault 7 and dated from 2013–2016, include details on CIA's software capabilities, such as the ability to compromise cars, smart TVs,*[136] web browsers (including Google Chrome, Microsoft Edge, Mozilla Firefox, and Opera Software ASA),*[137]*[138]*[139] and the operating systems of most smartphones (including Apple's iOS and Google's Android), as well as other operating systems such as Microsoft Windows, macOS, and Linux.*[140]

"Kill switch bill"

On 19 June 2010, United States Senator Joe Lieberman (I-CT) introduced a bill called "Protecting Cyberspace as a National Asset Act of 2010",*[141] which he co-wrote with Senator Susan Collins (R-ME) and Senator Thomas Carper (D-DE). If signed into law, this controversial bill, which the American media dubbed the "*Kill switch bill*", would grant the president emergency powers over parts of the Internet. However, all three co-authors of the bill issued a statement that instead, the bill "[narrowed] existing broad presidential authority to take over telecommunications networks".*[142]

3.5 Cyberpeace

See also: Cyberweapon § Control and disarmament

The German civil rights panel FIFF runs a campaign for cyberpeace – for the control of cyberweapons and surveillance technology and against the militarization of cyberspace and the development and stockpiling of offensive exploits and malware.*[143]*[144]*[145]*[146] Measures for cyberpeace include policymakers developing new rules and norms for warfare, individuals and organizations building new tools and secure infrastructures, promoting open source, the establishment of cyber security centers, auditing of critical infrastructure cybersecurity, obligations to disclose vulnerabilities, disarmament, defensive security strategies, decentralization, education and widely applying relevant tools and infrastructures, encryption and other cyberdefenses.*[143]*[147]*[148]*[149]

Cyberpeacemaking may also refer to new ways of using cyberspace to strengthen or bring about general peace.*[150]

3.6 Cyber counterintelligence

Cyber counter-intelligence are measures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions.*[151]

- On 7 April 2009, The Pentagon announced they spent more than \$100 million in the last six months responding to and repairing damage from cyber attacks and other computer network problems.*[152]

- On 1 April 2009, U.S. lawmakers pushed for the appointment of a White House cyber security “czar” to dramatically escalate U.S. defenses against cyber attacks, crafting proposals that would empower the government to set and enforce security standards for private industry for the first time.*[153]
- On 9 February 2009, the White House announced that it will conduct a review of the nation's cyber security to ensure that the Federal government of the United States cyber security initiatives are appropriately integrated, resourced and coordinated with the United States Congress and the private sector.*[154]
- In the wake of the 2007 cyberwar waged against Estonia, NATO established the Cooperative Cyber Defence Centre of Excellence (CCD CoE) in Tallinn, Estonia, in order to enhance the organization's cyber defence capability. The center was formally established on 14 May 2008, and it received full accreditation by NATO and attained the status of International Military Organization on 28 October 2008.*[155] Since Estonia has led international efforts to fight cybercrime, the United States Federal Bureau of Investigation says it will permanently base a computer crime expert in Estonia in 2009 to help fight international threats against computer systems.*[156]
- In 2015, the Department of Defense released an updated cyber strategy memorandum detailing the present and future tactics deployed in the service of defense against cyberwarfare. In this memorandum, three cybermissions are laid out. The first cybermission seeks to arm and maintain existing capabilities in the area of cyberspace, the second cybermission focuses on prevention of cyberwarfare, and the third cybermission includes strategies for retaliation and preemption (as distinguished from prevention).*[9]

One of the hardest issues in cyber counterintelligence is the problem of attribution. Unlike conventional warfare, figuring out who is behind an attack can be very difficult.*[157] However Defense Secretary Leon Panetta has claimed that the United States has the capability to trace attacks back to their sources and hold the attackers “accountable”.*[158]

3.7 Controversy over terms

There is debate on whether the term “cyberwarfare” is accurate.

Eugene Kaspersky, founder of Kaspersky Lab, concludes that “cyberterrorism” is a more accurate term than “cyber-war”. He states that “with today's attacks, you are clueless about who did it or when they will strike again. It's not cyber-war, but cyberterrorism.”*[159] He also equates large-scale cyber weapons, such as Flame and NetTraveler which his company discovered, to biological weapons, claiming that in an interconnected world, they have the potential to be equally destructive.*[159]*[160]

In October 2011 the *Journal of Strategic Studies*, a leading journal in that field, published an article by Thomas Rid, “Cyber War Will Not Take Place” which argued that all politically motivated cyber attacks are merely sophisticated versions of sabotage, espionage, or subversion*[161] – and that it is unlikely that cyber war will occur in the future.

Howard Schmidt, an American cybersecurity expert, argued in March 2010 that “there is no cyberwar... I think that is a terrible metaphor and I think that is a terrible concept. There are no winners in that environment.”*[33]

Other experts, however, believe that this type of activity already constitutes a war. The warfare analogy is often seen intended to motivate a militaristic response when that is not necessarily appropriate. Ron Deibert, of Canada's Citizen Lab, has warned of a “militarization of cyberspace”.*[162]

The European cybersecurity expert Sandro Gaycken argued for a middle position. He considers cyberwar from a legal perspective an unlikely scenario, due to the reasons lined out by Rid (and, before him, Sommer),*[163] but the situation looks different from a strategic point of view. States have to consider military-led cyber operations an attractive activity, within and without war, as they offer a large variety of cheap and risk-free options to weaken other countries and strengthen their own positions. Considered from a long-term, geostrategic perspective, cyber offensive operations can cripple whole economies, change political views, agitate conflicts within or among states, reduce their military efficiency and equalize the capacities of high-tech nations to that of low-tech nations, and use access to their critical infrastructures to blackmail them.*[164]

3.8 Legality, rules

Various parties have attempted to come up with international legal frameworks to clarify what is and is not acceptable, but none have yet to be widely accepted.

The Tallinn Manual, published in 2013, is an academic, non-binding study on how international law, in particular the *jus ad bellum* and *international humanitarian law*, apply to cyber conflicts and *cyber warfare*. It was written at the invitation of the Tallinn-based **NATO Cooperative Cyber Defence Centre of Excellence** by an international group of approximately twenty experts between 2009 and 2012.

The **Shanghai Cooperation Organisation** (members of which include China and Russia) defines cyberwar to include dissemination of information “harmful to the spiritual, moral and cultural spheres of other states”. In September 2011, these countries proposed to the UN Secretary General a document called “International code of conduct for information security”. *[165]

In contrast, the United States' approach focuses on physical and economic damage and injury, putting political concerns under freedom of speech. This difference of opinion has led to reluctance in the West to pursue global cyber arms control agreements.*[166] However, American General **Keith B. Alexander** did endorse talks with Russia over a proposal to limit military attacks in cyberspace.*[167] In June 2013, Barack Obama and **Vladimir Putin** agreed to install a secure *Cyberwar-Hotline* providing “a direct secure voice communications line between the US cybersecurity coordinator and the Russian deputy secretary of the security council, should there be a need to directly manage a crisis situation arising from an **ICT** security incident” (White House quote).*[168]

A Ukrainian professor of International Law, Alexander Merezhko, has developed a project called the International Convention on Prohibition of Cyberwar in Internet. According to this project, cyberwar is defined as the use of Internet and related technological means by one state against the political, economic, technological and information sovereignty and independence of another state. Professor Merezhko's project suggests that the Internet ought to remain free from warfare tactics and be treated as an international landmark. He states that the Internet (cyberspace) is a “common heritage of mankind”. *[169]

On the February 2017 RSA Conference Microsoft president Brad Smith suggested global rules – a “Digital Geneva Convention” – for cyber attacks that “ban the nation-state hacking of all the civilian aspects of our economic and political infrastructures”. He also stated that an independent organization could investigate and publicly disclose evidence that attributes nation-state attacks to specific countries. Furthermore, he said that the technology sector should collectively and neutrally work together to protect Internet users and pledge to remain neutral in conflict and not aid governments in offensive activity and to adopt a coordinated disclosure process for software and hardware vulnerabilities.*[170]*[171]

3.9 In films

Documentaries

Main page: Category:Documentary films about cyberwarfare

- *Cyber War Threat* (2015)
- *Darknet, Hacker, Cyberwar**[172] (2017)
- *Zero Days* (2016)

3.10 See also

- Cash machine
- Computer security organizations
- Cyber-arms industry
- Cyber-collection

- Cyber spying
- Cyber terrorism
- Duqu
- Fifth Dimension Operations
- IT risk
- iWar
- List of cyber attack threat trends
- List of cyber-attacks
- Penetration test
- Proactive cyber defence
- Signals intelligence
- Virtual war
- United States Cyber Command
 - Air Force Cyber Command
 - United States Army Cyber Command
 - Fleet Cyber Command
 - Marine Corps Cyberspace Command

3.11 References

Notes

- [1] Clarke, Richard A. *Cyber War*, HarperCollins (2010) ISBN 9780061962233
- [2] Blitz, James (1 November 2011). “Security: A huge challenge from China, Russia and organised crime” . Financial Times. Retrieved 6 June 2015.
- [3] Arquilla, John (1999). “Can information warfare ever be just?”. *Ethics and Information Technology*. **1** (3): 203–212. doi:10.1023/A:1010066528521.
- [4] Collins, Sean (April 2012). “Stuxnet: the emergence of a new cyber weapon and its implications” . *Journal of Policing, Intelligence and Counter Terrorism*. **7** (1). Retrieved 6 June 2015.
- [5] “Critical infrastructure vulnerable to attack, warned cyber security expert” . *gsnmagazine.com*. Government Security News. 2014. Retrieved 6 June 2015.
- [6] Maniscalchi, Jago (4 September 2011). “What is Cyberwar?”. Retrieved 6 June 2015.
- [7] Lynn, William J. III. “Defending a New Domain: The Pentagon's Cyberstrategy” , *Foreign Affairs*, Sept/Oct. 2010, pp. 97–108
- [8] Clapper, James R. “Worldwide Threat Assessment of the US Intelligence Community ”, Senate Armed Services Committee, 26 February 2015 p. 1
- [9] Lisa Lucile Owens, Justice and Warfare in Cyberspace, *The Boston Review* (2015), available at
- [10] Poole-Robb, Stuart. “Turkish blackout sparks fears of cyber attack on the West” , ITProPortal.com, 19 May 2015
- [11] USAF HQ, Annex 3–12 Cyberspace Ops, U.S. Air Force, 2011
- [12] James P. Farwell and Rafael Rohozinski, Stuxnet and the future of cyber war, *Survival*, 2011
- [13] “Cyberattacks, Terrorism Top U.S. Security Threat Report” . *NPR.org*. 12 March 2013.

- [14] “A Note on the Laws of War in Cyberspace”, James A. Lewis, April 2010
- [15] Rayman, Noah (18 December 2013). “Merkel Compared NSA To Stasi in Complaint To Obama”. *Time*. Retrieved 1 February 2014.
- [16] Devereaux, Ryan; Greenwald, Glenn; Poitras, Laura (19 May 2014). “Data Pirates of the Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas”. *The Intercept*. First Look Media. Retrieved 21 May 2014.
- [17] Schonfeld, Zach (23 May 2014). “The Intercept Wouldn’t Reveal a Country the U.S. Is Spying On, So WikiLeaks Did Instead”. *Newsweek*. Retrieved 26 May 2014.
- [18] Bodmer, Kilger, Carpenter, & Jones (2012). Reverse Deception: Organized Cyber Threat Counter-Exploitation. New York: McGraw-Hill Osborne Media. ISBN 0071772499, ISBN 978-0071772495
- [19] Sanders, Sam (4 June 2015). “Massive Data Breach Puts 4 Million Federal Employees’ Records at Risk”. *NPR*. Retrieved 5 June 2015.
- [20] Liptak, Kevin (4 June 2015). “U.S. government hacked; feds think China is the culprit”. *CNN*. Retrieved 5 June 2015.
- [21] “Clarke: More defense needed in cyberspace” HometownAnnapolis.com, 24 September 2010
- [22] “Malware Hits Computerized Industrial Equipment”. *The New York Times*, 24 September 2010
- [23] Singer, P.W.; Friedman, Allan (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press. p. 156. ISBN 978-0-19-991809-6.
- [24] Shiels, Maggie. (9 April 2009) BBC: Spies 'infiltrate US power grid'. BBC News. Retrieved 8 November 2011.
- [25] Meserve, Jeanne (8 April 2009). “Hackers reportedly have embedded code in power grid”. CNN. Retrieved 8 November 2011.
- [26] “US concerned power grid vulnerable to cyber-attack”. In.reuters.com (9 April 2009). Retrieved 8 November 2011.
- [27] Gorman, Siobhan. (8 April 2009) Electricity Grid in U.S. Penetrated By Spies. *The Wall Street Journal*. Retrieved 8 November 2011.
- [28] NERC Public Notice. (PDF). Retrieved 8 November 2011.
- [29] Xinhua: China denies intruding into the U.S. electrical grid. 9 April 2009
- [30] 'China threat' theory rejected. *China Daily* (9 April 2009). Retrieved 8 November 2011.
- [31] ABC News: Video. ABC News. (20 April 2009). Retrieved 8 November 2011.
- [32] Disconnect electrical grid from Internet, former terror czar Clarke warns. The Raw Story (8 April 2009). Retrieved 8 November 2011.
- [33] “White House Cyber Czar: ‘There Is No Cyberwar’”. *Wired*, 4 March 2010
- [34] Kim Zetter (3 March 2016). “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid”. *Wired*.
- [35] Evan Perez (12 February 2016). “U.S. official blames Russia for power grid attack in Ukraine”. CNN.
- [36] “Cyber-War Nominee Sees Gaps in Law”, *The New York Times*, 14 April 2010
- [37] Cyber ShockWave Shows U.S. Unprepared For Cyber Threats. Bipartisanpolicy.org. Retrieved 8 November 2011.
- [38] Drogin, Bob (17 February 2010). “In a doomsday cyber attack scenario, answers are unsettling”. *Los Angeles Times*.
- [39] Ali, Sarmad (16 February 2010). “Washington Group Tests Security in ‘Cyber ShockWave’”. *The Wall Street Journal*.
- [40] Cyber ShockWave CNN/BPC wargame: was it a failure?. *Computerworld* (17 February 2010). Retrieved 8 November 2011.
- [41] Steve Ragan Report: The Cyber ShockWave event and its aftermath. *The Tech Herald*. 16 February 2010
- [42] Lee, Andy (1 May 2012). “International Cyber Warfare: Limitations and Possibilities”. Jeju Peace Institute.
- [43] U.S. Navy Recruiting – Cyber Warfare Engineer.
- [44] Denning, D. E. (2008). The ethics of cyber conflict. *The Handbook of Information and Computer Ethics*. 407–429.
- [45] Financial Weapons of War, 100 Minnesota Law Review 1377 (2016)

- [46] "Google Attack Is Tip Of Iceberg" , McAfee Security Insights, 13 January 2010
- [47] Government-sponsored cyberattacks on the rise, McAfee says. *Network World* (29 November 2007). Retrieved 8 November 2011.
- [48] "China's Hacker Army". *Foreign Policy*. March 3, 2010.
- [49] "US embassy cables: China uses access to Microsoft source code to help plot cyber warfare, US fears" . *The Guardian*. London. 4 December 2010. Retrieved 31 December 2010.
- [50] "How China will use cyber warfare to leapfrog in military competitiveness" . *Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies*. 8 (1 October 2008). p. 37. Retrieved January 2013. Check date values in: laccess-date= (help)
- [51] "China to make mastering cyber warfare A priority (2011)". Washington, D.C.: NPR. Retrieved January 2013. Check date values in: laccess-date= (help)
- [52] "How China will use cyber warfare to leapfrog in military competitiveness" . *Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies*. 8 (1 October 2008). p. 42. Retrieved January 2013. Check date values in: laccess-date= (help)
- [53] "How China will use cyber warfare to leapfrog in military competitiveness" . *Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies*. 8 (1 October 2008). p. 43. Retrieved January 2013. Check date values in: laccess-date= (help)
- [54] "Washington, Beijing in Cyber-War Standoff" . Yahoo! News. 12 February 2013. Retrieved January 2013. Check date values in: laccess-date= (help)
- [55] Etzioni, Amitai (September 20, 2013). "MAR: A Model for US-China Relations" , *The Diplomat*.
- [56] Jim Finkle (3 August 2011). "State actor seen in "enormous" range of cyber attacks" . Reuters. Retrieved 3 August 2011.
- [57] "Beware of the bugs: Can cyber attacks on India's critical infrastructure be thwarted?". *BusinessToday*. Retrieved January 2013. Check date values in: laccess-date= (help)
- [58] "5 lakh cyber warriors to bolster India's e-defence" . *The Times of India*. India. 16 October 2012. Retrieved 18 October 2012.
- [59] "36 government sites hacked by 'Indian Cyber Army'" . *The Express Tribune*. Retrieved 8 November 2011.
- [60] "Hacked by 'Pakistan cyber army', CBI website still not restored" . Ndtv.com (4 December 2010). Retrieved 8 November 2011.
- [61] Pauli, Darren. "Copy paste slacker hackers pop corp locks in ode to stolen code" . The Register.
- [62] "APT Group 'Patchwork' Cuts-and-Pastes a Potent Attack" . Threatpost. 7 July 2016. Retrieved 2 January 2017.
- [63] Website of Kyrgyz Central Election Commission hacked by Estonian hackers, Regnum, 14 December 2007
- [64] https://www.f-secure.com/documents/996508/1030745/nanhaihu_whitepaper.pdf
- [65] Mazanec, Brian M. (2015). *The Evolution of Cyber War*. USA: University of Nebraska Press. pp. 235–236. ISBN 9781612347639.
- [66] Danchev, Dancho (11 August 2008). "Coordinated Russia vs Georgia cyberattack" . ZDNet. Retrieved 25 November 2008.
- [67] Cyberspace and the changing nature of warfare. Strategists must be aware that part of every political and military conflict will take place on the internet, says Kenneth Geers.
- [68] "www.axisglobe.com". Retrieved 1 August 2016.
- [69] Andrew Meier, *Black Earth*. W. W. Norton & Company, 2003, ISBN 0-393-05178-1, pages 15–16.
- [70] Sudworth, John. (9 July 2009) "New cyberattacks hit South Korea" . BBC News. Retrieved 8 November 2011.
- [71] Williams, Martin. UK, Not North Korea, Source of DDOS Attacks, Researcher Says. *PC World*.
- [72] "SK Hack by an Advanced Persistent Threat" (PDF). Command Five Pty Ltd. Retrieved 24 September 2011.

- [73] Lee, Se Young. “South Korea raises alert after hackers attack broadcasters, banks” . *Global Post*. Retrieved 6 April 2013.
- [74] Kim, Eun-jung. “S. Korean military to prepare with U.S. for cyber warfare scenarios” . Yonhap News Agency. Retrieved 6 April 2013.
- [75] “War in the fifth domain. Are the mouse and keyboard the new weapons of conflict?”. *The Economist*. 1 July 2010. Retrieved 2 July 2010. Important thinking about the tactical and legal concepts of cyber-warfare is taking place in a former Soviet barracks in Estonia, now home to NATO's “centre of excellence” for cyber-defence. It was established in response to what has become known as “Web War 1”, a concerted denial-of-service attack on Estonian government, media and bank web servers that was precipitated by the decision to move a Soviet-era war memorial in central Tallinn in 2007.
- [76] Estonia accuses Russia of 'cyber attack'. *The Christian Science Monitor*. (17 May 2007). Retrieved 8 November 2011.
- [77] Ian Traynor, “Russia accused of unleashing cyberwar to disable Estonia” , *The Guardian*, 17 May 2007
- [78] Boyd, Clark. (June 17, 2010) “Cyber-war a growing threat warn experts” . BBC News. Retrieved 8 November 2011.
- [79] Scott J. Shackelford, From Nuclear War to Net War: Analogizing Cyber Attacks in International Law, 27 Berkeley J. Int'l Law. 192 (2009).
- [80] “Germany's 60-person Computer Network Operation (CNO) unit has been practicing for cyber war for years.”
- [81] “Hackers wanted to man front line in cyber war” , *The Local*, 24 March 2013
- [82] “Germany to invest 100 million euros on internet surveillance: report” , Kazinform, 18 June 2013
- [83] “National Cyber Security Centrum – NCSC” .
- [84] “Defensie Cyber Strategie” .
- [85] “Cyber commando” .
- [86] Ringstrom, Anna (January 25, 2017). Goodman, David, ed. “Swedish forces exposed to extensive cyber attack: Dagens Nyheter” . Reuters. Archived from the original on January 25, 2017. Sweden's armed forces were recently exposed to an extensive cyber attack that prompted them to shut down an IT system used in military exercises, daily newspaper Dagens Nyheter reported on Wednesday. The attack that affected the Caxcis IT system was confirmed to the Swedish newspaper by armed forces spokesman Philip Simon.
- [87] Ukraine's military denies Russian hack attack , Yahoo! News (6 January 2017)
- [88] “Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units” . CrowdStrike. 22 December 2016.
- [89] Defense ministry denies reports of alleged artillery losses because of Russian hackers' break into software, Interfax-Ukraine (6 January 2017)
- [90] Mazanec, Brain M. (2015). *The Evolution of Cyber War*. USA: University of Nebraska Press. pp. 221–222. ISBN 9781612347639.
- [91] “BlackEnergy malware activity spiked in runup to Ukraine power grid takedown” . The Register. Retrieved 26 December 2016.
- [92] “Al Qaeda rocked by apparent cyberattack. But who did it?”. *The Chris Science Monitor*.
- [93] Britain faces serious cyber threat, spy agency head warns. *The Globe and Mail* (13 October 2010). Retrieved 8 November 2011.
- [94] “Attack the City: why the banks are 'war gaming'".
- [95] “Wall Street banks learn how to survive in staged cyber attack” . Reuters. 21 October 2013.
- [96] “Iran's military is preparing for cyber warfare” . Flash//CRITIC Cyber Threat News. Retrieved 18 March 2015.
- [97] AFP (1 October 2010). Stuxnet worm brings cyber warfare out of virtual world. Google. Retrieved 8 November 2011.
- [98] Ralph Langner: Cracking Stuxnet, a 21st-century cyber weapon | Video on. Ted.com. Retrieved 8 November 2011.
- [99] “Israel Adds Cyber-Attack to IDF” , Military.com, 10 February 2010
- [100] Fulghum, David A. "Why Syria's Air Defenses Failed to Detect Israelis", *Aviation Week & Space Technology*, 3 October 2007. Retrieved 3 October 2007.

- [101] Fulghum, David A. "Israel used electronic attack in air strike against Syrian mystery target", *Aviation Week & Space Technology*, 8 October 2007. Retrieved 8 October 2007.
- [102] American Forces Press Service: Lynn Explains U.S. Cybersecurity Strategy. Defense.gov. Retrieved 8 November 2011.
- [103] "Pentagon to Consider Cyberattacks Acts of War". *The New York Times*. 31 May 2006
- [104] Dilanian, Ken. "Cyber-attacks a bigger threat than Al Qaeda, officials say", *Los Angeles Times*, 12 March 2013
- [105] Nikita Vladimirov, Ex-House intel chairman: US 'not necessarily winning' the cyber war, *The Hill* (February 19, 2017).
- [106] "Cyberwar: War in the Fifth Domain" *Economist*, 1 July 2010
- [107] The Lipman Report, 15 October 2010
- [108] Clarke, Richard. "China's Cyberassault on America", *The Wall Street Journal*, 15 June 2011
- [109] "Cyberwarrior Shortage Threatens U.S. Security". NPR, 19 July 2010
- [110] "U.S. military cyberwar: What's off-limits?" CNET, 29 July 2010
- [111] "US Launched Cyber Attacks on Other Nations". RT, 26 January 2012.
- [112] Sanger, David E. "Obama Order Sped Up Wave of Cyberattacks Against Iran." *The New York Times*, 1 June 2012.
- [113] ANNUAL REPORT TO CONGRESS Military and Security Developments Involving the People's Republic of China 2010. US Defense Department (PDF). Retrieved 8 November 2011.
- [114] AP: Pentagon takes aim at China cyber threat Archived 23 August 2010 at the Wayback Machine.
- [115] "The Joint Operating Environment", Joint Forces Command, 18 February 2010, pp. 34–36
- [116] U.S. drone and predator fleet is being keylogged. *Wired*, October 2011. Retrieved 6 October 2011
- [117] Hennigan, W.J. "Air Force says drone computer virus poses 'no threat'". *Los Angeles Times*, 13 October 2011.
- [118] Mathew J. Schwartz (21 November 2011). "Hacker Apparently Triggers Illinois Water Pump Burnout". *InformationWeek*.
- [119] Kim Zetter (30 November 2011). "Exclusive: Comedy of Errors Led to False 'Water-Pump Hack' Report". *Wired*.
- [120] "U.S. NSA Unit 'TAO' Hacking China For Years". Business Insider. June 11, 2013
- [121] "Secret NSA hackers from TAO Office have been pwning China for nearly 15 years". *Computerworld*. June 11, 2013.
- [122] Barrett, Devlin (5 June 2015). "U.S. Suspects Hackers in China Breached About four (4) Million People's Records, Officials Say". *Wall Street Journal*. Retrieved 5 June 2015.
- [123] "U.S. gov't hack may be four (4) times larger than first reported".
- [124] Sanders, Sam (4 June 2015). "Massive Data Breach Puts 4 Million Federal Employees' Records At Risk". *NPR*.
- [125] "Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security". Department Of Homeland Security and Office of the Director of National Intelligence on Election Security. October 7, 2016. Retrieved 15 October 2016.
- [126] "U.S. Says Russia Directed Hacks to Influence Elections". NYT. Oct 7, 2016.
- [127] "Presidential approval and reporting of covert actions". *gpo.gov*. United States Code. Retrieved 16 October 2016.
- [128] "VP Biden Promises Response to Russian Hacking". NBC News Meet the Press. Oct 14, 2016.
- [129] "Biden Hints at U.S. Response to Russia for Cyberattacks". NYT. Oct 15, 2016.
- [130] Lee, Carol E.; Sonne, Paul (December 30, 2016). "U.S. Sanctions Russia Over Election Hacking; Moscow Threatens to Retaliate" – via Wall Street Journal.
- [131] "U.S. imposes sanctions on Russia over election interference". CBS News. December 29, 2016. Retrieved December 29, 2016.
- [132] "US expels 35 Russian diplomats, closes two compounds: report". *DW.COM*. December 29, 2016. Retrieved December 29, 2016.
- [133] Satter, Raphael. "US general: We hacked the enemy in Afghanistan.". Associated Press, 24 August 2012.

- [134] Sanger, David E.; Broad, William J. (4 March 2017). “Trump Inherits a Secret Cyberwar Against North Korean Missiles” . *The New York Times*. Retrieved 4 March 2017.
- [135] Greg Miller, Ellen Nakashima, Adam Entous: Obama’s secret struggle to retaliate against Putin’s election interference, *Washington Post*, 23. June 2017
- [136] Shane, Scott; Mazzetti, Mark; Rosenberg, Matthew (7 March 2017). “WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents” . *The New York Times*. Retrieved 7 March 2017.
- [137] Greenberg, Andy (2017-03-07). “How the CIA Can Hack Your Phone, PC, and TV (Says WikiLeaks)”. *WIRED*. Retrieved 2017-04-08.
- [138] Murdock, Jason (2017-03-07). “Vault 7: CIA hacking tools were used to spy on iOS, Android and Samsung smart TVs” . *International Business Times UK*. Retrieved 2017-04-08.
- [139] “WikiLeaks posts trove of CIA documents detailing mass hacking” . *CBS News*. 2017-03-07. Retrieved 2017-04-08.
- [140] “Vault 7: Wikileaks reveals details of CIA’s hacks of Android, iPhone Windows, Linux, MacOS, and even Samsung TVs”. *Computing*. 7 March 2017.
- [141] A Bill. To amend the Homeland Security Act of 2002 and other laws to enhance the security and resiliency of the cyber and communications infrastructure of the United States.. Senate.gov. 111th Congress 2D Session
- [142] Senators Say Cybersecurity Bill Has No 'Kill Switch', *Information Week*, 24 June 2010. Retrieved 25 June 2010.
- [143] Hofkirchner, Wolfgang; Burgin, Mark. *The Future Information Society: Social and Technological Problems*. World Scientific. ISBN 9789813108981. Retrieved 22 May 2017.
- [144] “Abrüstung statt „Cyberwar“: Forderungen nach WannaCry” . *netzpolitik.org* (in German). 22 May 2017. Retrieved 22 May 2017.
- [145] “WannaCry ist ein Kollateralschaden des Cyberwar - Pressenza” . *Pressenza* (in German). Pressenza. 18 May 2017. Retrieved 22 May 2017.
- [146] “"Cyberpeace"-Kampagne engagierter InformatikerInnen wird gefördert” . *heise online* (in German). Retrieved 22 May 2017.
- [147] “Eric Schmidt and Jared Cohen: We Must Prepare Ourselves for the Cyberwars of the Future” . Time. Retrieved 22 May 2017.
- [148] Friesinger, Günther; Herwig, Jana. *The Art of Reverse Engineering: Open - Dissect - Rebuild*. transcript Verlag. ISBN 9783839425039. Retrieved 22 May 2017.
- [149] Grady, Mark F.; Parisi, Francesco. *The Law and Economics of Cybersecurity*. Cambridge University Press. ISBN 9781139446969. Retrieved 22 May 2017.
- [150] Ramsbotham, Oliver; Miall, Hugh; Woodhouse, Tom. *Contemporary Conflict Resolution*. Polity. ISBN 9780745649740. Retrieved 22 May 2017.
- [151] DOD – Cyber Counterintelligence. Dtac.mil. Retrieved 8 November 2011.
- [152] Pentagon Bill To Fix Cyber Attacks: ,0M. CBS News. Retrieved 8 November 2011.
- [153] “Senate Legislation Would Federalize Cybersecurity” . *The Washington Post*. Retrieved 8 November 2011.
- [154] “White House Eyes Cyber Security Plan” . CBS News (10 February 2009). Retrieved 8 November 2011.
- [155] CCD COE – Cyber Defence. Ccdcoe.org. Retrieved 8 November 2011.
- [156] Associated Press (11 May 2009) FBI to station cybercrime expert in Estonia. *Boston Herald*. Retrieved 8 November 2011.
- [157] Reed, John. “Is the 'holy grail' of cyber security within reach?”. *Foreign Policy Magazine*, 6 September 2012.
- [158] Carroll, Chris. “US can trace cyberattacks, mount pre-emptive strikes, Panetta says” . *Stars and Stripes*, 11 October 2012.
- [159] “Latest viruses could mean 'end of world as we know it,' says man who discovered Flame” , *The Times of Israel*, 6 June 2012
- [160] “Cyber espionage bug attacking Middle East, but Israel untouched —so far” , *The Times of Israel*, 4 June 2013
- [161] Rid, Thomas (October 2011). “Cyber War Will Not Take Place” . *Journal of Strategic Studies*. 35: 5–32. doi:10.1080/01402390.2011.608939. Retrieved 21 October 2011.

- [162] Deibert, Ron (2011). “Tracking the emerging arms race in cyberspace” . *Bulletin of the Atomic Scientists*. **67** (1): 1–8. doi:10.1177/0096340210393703.
- [163] Sommer, Peter (January 2011). “Reducing Systemic Cybersecurity Risk” (PDF). *OECD Multi-Disciplinary Issues*. Retrieved 21 May 2012.
- [164] Gaycken, Sandro (2010). “Cyberwar – Das Internet als Kriegsschauplatz” .
- [165] Russian Embassy to the UK . Retrieved 25 May 2012.
- [166] Tom Gjelten (23 September 2010). “Seeing The Internet As An 'Information Weapon'" . NPR. Retrieved 23 September 2010.
- [167] Gorman, Siobhan. (4 June 2010) WSJ: U.S. Backs Talks on Cyber Warfare. *The Wall Street Journal*. Retrieved 8 November 2011.
- [168] Sean Gallagher, *US, Russia to install “cyber-hotline” to prevent accidental cyberwar*, ArsTechnica, 18 June 2013
- [169] Український центр політичного менеджменту – Зміст публікації – Конвенция о запрещении использования кибервойны. Politik.org.ua. Retrieved 8 November 2011.
- [170] "Digital Geneva Convention' needed to deter nation-state hacking: Microsoft president" . Reuters. 14 February 2017. Retrieved 20 February 2017.
- [171] Kaspersky, Eugene. “A Digital Geneva Convention? A Great Idea.” . Forbes. Retrieved 20 February 2017.
- [172] “Darknet, Hacker, Cyberwar – Der geheime Krieg im Netz” (in German). Retrieved 3 April 2017.

Further reading

- Andress, Jason. Winterfeld, Steve. (2011). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Syngress. ISBN 1-59749-637-5
- Bodmer, Kilger, Carpenter, & Jones (2012). *Reverse Deception: Organized Cyber Threat Counter-Exploitation*. New York: McGraw-Hill Osborne Media. ISBN 0071772499, "ISBN 978-0071772495"
- Brenner, S. (2009). *Cyber Threats: The Emerging Fault Lines of the Nation State*. Oxford University Press. ISBN 0-19-538501-2
- Carr, Jeffrey. (2010). *Inside Cyber Warfare: Mapping the Cyber Underworld*. O'Reilly. ISBN 978-0-596-80215-8
- Cordesman, Anthony H., Cordesman, Justin G. *Cyber-threats, Information Warfare, and Critical Infrastructure Protection*, Greenwood Publ. (2002)
- Costigan, Sean S.; Perry, Jake (2012). *Cyberspaces and global affairs*. Farnham, Surrey: Ashgate. ISBN 9781409427544.
- Gaycken, Sandro. (2012). *Cyberwar – Das Wettrüsten hat längst begonnen*. Goldmann/Randomhouse. ISBN 978-3442157105
- Geers, Kenneth. (2011). *Strategic Cyber Security*. NATO Cyber Centre. *Strategic Cyber Security*, ISBN 978-9949-9040-7-5, 169 pages
- Shane Harris (2014). *@War: The Rise of the Military-Internet Complex*. Eamon Dolan/Houghton Mifflin Harcourt. ISBN 978-0544251793.
- Hunt, Edward (2012). “US Government Computer Penetration Programs and the Implications for Cyberwar” . *IEEE Annals of the History of Computing*. **34** (3): 4–21. doi:10.1109/mahc.2011.82.
- Janczewski, Lech; Colarik, Andrew M. *Cyber Warfare and Cyber Terrorism* IGI Global (2008)
- Rid, Thomas (2011) “Cyber War Will Not Take Place,” *Journal of Strategic Studies*, doi:10.1080/01402390.2011.608939
- Ventre, D. (2007). *La guerre de l'information*. Hermes-Lavoisier. 300 pages
- Ventre, D. (2009). *Information Warfare*. Wiley – ISTE. ISBN 978-1-84821-094-3

- Ventre, D. (Edit.) (2010). *Cyberguerre et guerre de l'information. Stratégies, règles, enjeux*. Hermes-Lavoisier. ISBN 978-2-7462-3004-0
- Ventre, D. (2011). *Cyberespace et acteurs du cyberconflit*. Hermes-Lavoisier. 288 pages
- Ventre, D. (Edit.) (2011). *Cyberwar and Information Warfare*. Wiley. 460 pages
- Ventre, D. (2011). *Cyberattaque et Cyberdéfense*. Hermes-Lavoisier. 336 pages
- Ventre, D. (Edit.) (2012). *Cyber Conflict. Competing National Perspectives*. Wiley-ISTE. 330 pages
- Woltag, Johann-Christoph: 'Cyber Warfare' in Rüdiger Wolfrum (Ed.) *Max Planck Encyclopedia of Public International Law* (Oxford University Press 2012).

3.12 External links

- NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)
- Cyberwar Twitter feed from Richard Stiennon
- Cyberwar News community by Reza Rafati

Videos

- “Sabotaging the System” video, “60 Minutes”, 8 November 2009, CBS News, 15 minutes

Articles

- ABC: Former White House security advisor warns of cyber war
- Wall Street Journal: Fighting Wars in Cyberspace
- Will There Be An Electronic Pearl Harbor, PC World by Ira Winkler, 1 December 2009
- Senate panel: 80 percent of cyberattacks preventable, Wired, 17 November 2009
- Consumer Reports Online Security Guide
- Cyberwarfare reference materials
- Duncan Gardham, 26 June 2009, Hackers recruited to fight 'new cold war', Telegraph UK
- Stefano Mele, Jan 2016, Cyber Strategy & Policy Brief (Volume 01 – January 2016)
- Stefano Mele, Jun 2013, Cyber-Weapons: Legal and Strategic Aspects (version 2.0)
- Stefano Mele, Sep 2010, Cyberwarfare and its damaging effects on citizens
- History of Cyber Warfare
- Cybersecurity: Authoritative Reports and Resources, US Congressional Research Service
- Why the USA is Losing The Cyberwar Against China, by Joseph Steinberg, VentureBeat, 9 November 2011
- Michael Riley and Ashlee Vance, 20 July 2011, Cyber Weapons: The New Arms Race
- The Digital Arms Race: NSA Preps America for Future Battle, *Der Spiegel*, January 2015

Chapter 4

Computer security

Computer security, also known as **cyber security** or **IT security**, is the protection of computer systems from the theft or damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide.^{*[1]}

Cyber security includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection.^{*[2]} Also, due to malpractice by operators, whether intentional, accidental, IT security is susceptible to being tricked into deviating from secure procedures through various methods.^{*[3]}

The field is of growing importance due to the increasing reliance on computer systems and the Internet,^{*[4]} wireless networks such as Bluetooth and Wi-Fi, and the growth of “smart” devices, including smartphones, televisions and tiny devices as part of the Internet of Things.

4.1 Vulnerabilities and attacks

Main article: [Vulnerability \(computing\)](#)

A vulnerability is a weakness in design, implementation, operation or internal control. As they are discovered many vulnerabilities are documented in the [Common Vulnerabilities and Exposures \(CVE\) database](#).

An *exploitable* vulnerability is one for which at least one working attack or "exploit" exists.^{*[5]} Vulnerabilities are often hunted or exploited with the aid of [automated tools](#).

To secure a computer system, it is important to understand the attacks that can be made against it, and these threats can typically be classified into one of the categories below:

4.1.1 Backdoor

A backdoor in a computer system, a [cryptosystem](#) or an algorithm, is any secret method of bypassing normal authentication or security controls. They may exist for a number of reasons, including by original design or from poor configuration. They may have been added by an authorized party to allow some legitimate access, or by an attacker for malicious reasons; but regardless of the motives for their existence, they create a vulnerability.

4.1.2 Denial-of-service attack

Denial of service attacks (DoS) are designed to make a machine or network resource unavailable to its intended users.^{*[6]} Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim account to be locked, or they may overload the capabilities of a machine or network and block all users at once. While a network attack from a single IP address can be blocked by adding a new firewall rule, many forms of [Distributed denial of service \(DDoS\)](#) attacks are possible, where the attack comes from a large number of points – and defending is much more difficult. Such attacks can originate from the [zombie](#)

computers of a botnet, but a range of other techniques are possible including reflection and amplification attacks, where innocent systems are fooled into sending traffic to the victim.

4.1.3 Direct-access attacks

An unauthorized user gaining physical access to a computer is most likely able to directly copy data from it. They may also compromise security by making operating system modifications, installing software worms, keyloggers, covert listening devices or using wireless mice.* [7] Even when the system is protected by standard security measures, these may be able to be by-passed by booting another operating system or tool from a CD-ROM or other bootable media. Disk encryption and Trusted Platform Module are designed to prevent these attacks.

4.1.4 Eavesdropping

Eavesdropping is the act of surreptitiously listening to a private conversation, typically between hosts on a network. For instance, programs such as Carnivore and NarusInsight have been used by the FBI and NSA to eavesdrop on the systems of internet service providers. Even machines that operate as a closed system (i.e., with no contact to the outside world) can be eavesdropped upon via monitoring the faint electro-magnetic transmissions generated by the hardware; TEMPEST is a specification by the NSA referring to these attacks.

4.1.5 Spoofing

Spoofing, in general, is a fraudulent or malicious practice in which communication is disguised as a source known to the receiver. Spoofing is most prevalent in communication mechanisms that lack a high level of security.* [8]

4.1.6 Tampering

Tampering describes a malicious modification of products. So-called “Evil Maid” attacks and security services planting of surveillance capability into routers* [9] are examples.

4.1.7 Privilege escalation

Privilege escalation describes a situation where an attacker with some level of restricted access is able to, without authorization, elevate their privileges or access level. For example, a standard computer user may be able to fool the system into giving them access to restricted data; or even to "become root" and have full unrestricted access to a system.

4.1.8 Phishing

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details directly from users.* [10] Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Preying on a victim's trust, phishing can be classified as a form of social engineering.

4.1.9 Clickjacking

Clickjacking, also known as “UI redress attack” or “User Interface redress attack”, is a malicious technique in which an attacker tricks a user into clicking on a button or link on another webpage while the user intended to click on the top level page. This is done using multiple transparent or opaque layers. The attacker is basically “hijacking” the clicks meant for the top level page and routing them to some other irrelevant page, most likely owned by someone else. A similar technique can be used to hijack keystrokes. Carefully drafting a combination of stylesheets, iframes, buttons and text boxes, a user can be led into believing that they are typing the password or other information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

4.1.10 Social engineering

Main article: Social engineering (security)
 See also: Category:Cryptographic attacks

Social engineering aims to convince a user to disclose secrets such as passwords, card numbers, etc. by, for example, impersonating a bank, a contractor, or a customer.*[11]

A common scam involves fake CEO emails sent to accounting and finance departments. In early 2016, the FBI reported that the scam has cost US businesses more than \$2bn in about two years.*[12]

In May 2016, the Milwaukee Bucks NBA team was the victim of this type of cyber scam with a perpetrator impersonating the team's president Peter Feigin, resulting in the handover of all the team's employees' 2015 W-2 tax forms.*[13]

4.2 Information security culture

Employee behavior can have a big impact on information security in organizations. Cultural concepts can help different segments of the organization work effectively or work against effectiveness towards information security within an organization."Exploring the Relationship between Organizational Culture and Information Security Culture" provides the following definition of information security culture: "ISC is the totality of patterns of behavior in an organization that contribute to the protection of information of all kinds."*[14]

Andersson and Reimers (2014) found that employees often do not see themselves as part of the organization Information Security "effort" and often take actions that ignore organizational Information Security best interests.*[15] Research shows Information security culture needs to be improved continuously. In "Information Security Culture from Analysis to Change", authors commented, "It's a never ending process, a cycle of evaluation and change or maintenance." To manage the information security culture, five steps should be taken: Pre-evaluation, strategic planning, operative planning, implementation, and post-evaluation.*[16]

- Pre-Evaluation: to identify the awareness of information security within employees and to analyze the current security policy.
- Strategic Planning: to come up with a better awareness program, clear targets need to be set. Clustering people is helpful to achieve it.
- Operative Planning: a good security culture can be established based on internal communication, management-buy-in, and security awareness and a training program.*[16]
- Implementation: four stages should be used to implement the information security culture. They are commitment of the management, communication with organizational members, courses for all organizational members, and commitment of the employees.*[16]

4.3 Systems at risk

The growth in the number of computer systems, and the increasing reliance upon them of individuals, businesses, industries and governments means that there are an increasing number of systems at risk.

4.3.1 Financial systems

Web sites and apps that accept or store credit card numbers, brokerage accounts, and bank account information are prominent hacking targets, because of the potential for immediate financial gain from transferring money, making purchases, or selling the information on the black market.*[17] In-store payment systems and ATMs have also been tampered with in order to gather customer account data and PINs.

4.3.2 Utilities and industrial equipment

Computers control functions at many utilities, including coordination of telecommunications, the power grid, nuclear power plants, and valve opening and closing in water and gas networks. The Internet is a potential attack vector for such machines if connected, but the Stuxnet worm demonstrated that even equipment controlled by computers not connected to the Internet can be vulnerable. In 2014, the Computer Emergency Readiness Team, a division of the Department of Homeland Security, investigated 79 hacking incidents at energy companies.*[18] Vulnerabilities in smart meters (many of which use local radio or cellular communications) can cause problems with billing fraud.*[19]

4.3.3 Aviation

The aviation industry is very reliant on a series of complex system which could be attacked.*[20] A simple power outage at one airport can cause repercussions worldwide,*[21] much of the system relies on radio transmissions which could be disrupted,*[22] and controlling aircraft over oceans is especially dangerous because radar surveillance only extends 175 to 225 miles offshore.*[23] There is also potential for attack from within an aircraft.*[24]

In Europe, with the (Pan-European Network Service)*[25] and NewPENS,*[26] and in the US with the NextGen program,*[27] air navigation service providers are moving to create their own dedicated networks.

The consequences of a successful attack range from loss of confidentiality to loss of system integrity, air traffic control outages, loss of aircraft, and even loss of life.

4.3.4 Consumer devices

Desktop computers and laptops are commonly targeted to gather passwords or financial account information, or to construct a botnet to attack another target. Smart phones, tablet computers, smart watches, and other mobile devices such as quantified self devices like activity trackers have sensors such as cameras, microphones, GPS receivers, compasses, and accelerometers which could be exploited, and may collect personal information, including sensitive health information. Wifi, Bluetooth, and cell phone networks on any of these devices could be used as attack vectors, and sensors might be remotely activated after a successful breach.*[28]

The increasing number of home automation devices such as the Nest thermostat are also potential targets.*[28]

4.3.5 Large corporations

Large corporations are common targets. In many cases this is aimed at financial gain through identity theft and involves data breaches such as the loss of millions of clients' credit card details by Home Depot,*[29] Staples,*[30] and Target Corporation.*[31] Medical records have been targeted for use in general identify theft, health insurance fraud, and impersonating patients to obtain prescription drugs for recreational purposes or resale.*[32]

Not all attacks are financially motivated however; for example security firm HBGary Federal suffered a serious series of attacks in 2011 from hacktivist group Anonymous in retaliation for the firm's CEO claiming to have infiltrated their group,*[33]*[34] and in the Sony Pictures attack of 2014 the motive appears to have been to embarrass with data leaks, and cripple the company by wiping workstations and servers.*[35]*[36]

4.3.6 Automobiles

See also: Autonomous car § Potential disadvantages, Automated driving system § Risks and liabilities, and Automotive hacking

Vehicles are increasingly computerized, with engine timing, cruise control, anti-lock brakes, seat belt tensioners, door locks, airbags and advanced driver-assistance systems on many models. Additionally, connected cars may use Wi-Fi and bluetooth to communicate with onboard consumer devices and the cell phone network.*[37] Self-driving cars are expected to be even more complex.

All of these systems carry some security risk, and such issues have gained wide attention.*[38]*[39]*[40] Simple examples of risk include a malicious compact disc being used as an attack vector,*[41] and the car's onboard microphones being used for eavesdropping. However, if access is gained to a car's internal controller area network, the

danger is much greater^{*[37]} – and in a widely publicised 2015 test, hackers remotely carjacked a vehicle from 10 miles away and drove it into a ditch.^{*[42]*[43]}

Manufacturers are reacting in a number of ways, with Tesla in 2016 pushing out some security fixes “over the air” into its cars’ computer systems.^{*[44]}

In the area of autonomous vehicles, in September 2016 the United States Department of Transportation announced some initial safety standards, and called for states to come up with uniform policies.^{*[45]*[46]}

4.3.7 Government

Government and military computer systems are commonly attacked by activists^{*[47]*[48]*[49]*[50]} and foreign powers.^{*[51]*[52]*[53]*[54]} Local and regional government infrastructure such as traffic light controls, police and intelligence agency communications, personnel records, student records,^{*[55]} and financial systems are also potential targets as they are now all largely computerized. Passports and government ID cards that control access to facilities which use RFID can be vulnerable to cloning.

4.3.8 Internet of things and physical vulnerabilities

The Internet of things (IoT) is the network of physical objects such as devices, vehicles, and buildings that are embedded with electronics, software, sensors, and network connectivity that enables them to collect and exchange data^{*[56]} – and concerns have been raised that this is being developed without appropriate consideration of the security challenges involved.^{*[57]*[58]}

While the IoT creates opportunities for more direct integration of the physical world into computer-based systems,^{*[59]*[60]} it also provides opportunities for misuse. In particular, as the Internet of Things spreads widely, cyber attacks are likely to become an increasingly physical (rather than simply virtual) threat.^{*[61]} If a front door’s lock is connected to the Internet, and can be locked/unlocked from a phone, then a criminal could enter the home at the press of a button from a stolen or hacked phone. People could stand to lose much more than their credit card numbers in a world controlled by IoT-enabled devices. Thieves have also used electronic means to circumvent non-Internet-connected hotel door locks.^{*[62]}

Medical systems

See also: Medical device hijack and Medical data breach

Medical devices have either been successfully attacked or had potentially deadly vulnerabilities demonstrated, including both in-hospital diagnostic equipment^{*[63]} and implanted devices including pacemakers^{*[64]} and insulin pumps.^{*[65]} There are many reports of hospitals and hospital organizations getting hacked, including ransomware attacks,^{*[66]*[67]*[68]*[69]} Windows XP exploits,^{*[70]*[71]} viruses,^{*[72]*[73]*[74]} and data breaches of sensitive data stored on hospital servers.^{*[75]*[67]*[76]*[77]*[78]} On 28 December 2016 the US Food and Drug Administration released its recommendations for how medical device manufacturers should maintain the security of Internet-connected devices – but no structure for enforcement.^{*[79]*[80]}

4.4 Impact of security breaches

Serious financial damage has been caused by security breaches, but because there is no standard model for estimating the cost of an incident, the only data available is that which is made public by the organizations involved. “Several computer security consulting firms produce estimates of total worldwide losses attributable to virus and worm attacks and to hostile digital acts in general. The 2003 loss estimates by these firms range from \$13 billion (worms and viruses only) to \$226 billion (for all forms of covert attacks). The reliability of these estimates is often challenged; the underlying methodology is basically anecdotal.”^{*[81]}

However, reasonable estimates of the financial cost of security breaches can actually help organizations make rational investment decisions. According to the classic Gordon-Loeb Model analyzing the optimal investment level in information security, one can conclude that the amount a firm spends to protect information should generally be only a

small fraction of the expected loss (i.e., the **expected value** of the loss resulting from a cyber/information security breach).^{*} [82]

4.5 Attacker motivation

As with **physical security**, the motivations for breaches of computer security vary between attackers. Some are thrill-seekers or vandals, some are activists, others are criminals looking for financial gain. State-sponsored attackers are now common and well resourced, but started with amateurs such as **Markus Hess** who hacked for the **KGB**, as recounted by **Clifford Stoll**, in *The Cuckoo's Egg*.

A standard part of **threat modelling** for any particular system is to identify what might motivate an attack on that system, and who might be motivated to breach it. The level and detail of precautions will vary depending on the system to be secured. A home personal computer, bank, and classified military network face very different threats, even when the underlying technologies in use are similar.

4.6 Computer protection (countermeasures)

In computer security a countermeasure is an action, device, procedure, or technique that reduces a **threat**, a **vulnerability**, or an **attack** by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.^{*} [83]^{*} [84]^{*} [85]

Some common countermeasures are listed in the following sections:

4.6.1 Security by design

Main article: **Secure by design**

Security by design, or alternately **secure by design**, means that the software has been designed from the ground up to be secure. In this case, security is considered as a main feature.

Some of the techniques in this approach include:

- The **principle of least privilege**, where each part of the system has only the privileges that are needed for its function. That way even if an attacker gains access to that part, they have only limited access to the whole system.
- **Automated theorem proving** to prove the correctness of crucial software subsystems.
- **Code reviews** and **unit testing**, approaches to make modules more secure where formal correctness proofs are not possible.
- **Defense in depth**, where the design is such that more than one subsystem needs to be violated to compromise the integrity of the system and the information it holds.
- Default secure settings, and design to “fail secure” rather than “fail insecure” (see **fail-safe** for the equivalent in **safety engineering**). Ideally, a secure system should require a deliberate, conscious, knowledgeable and free decision on the part of legitimate authorities in order to make it insecure.
- **Audit trails** tracking system activity, so that when a security breach occurs, the mechanism and extent of the breach can be determined. Storing audit trails remotely, where they can only be appended to, can keep intruders from covering their tracks.
- **Full disclosure** of all vulnerabilities, to ensure that the “window of vulnerability” is kept as short as possible when bugs are discovered.

4.6.2 Security architecture

The Open Security Architecture organization defines IT security architecture as “the design artifacts that describe how the security controls (security countermeasures) are positioned, and how they relate to the overall information technology architecture. These controls serve the purpose to maintain the system's quality attributes: confidentiality, integrity, availability, accountability and assurance services”.^{*[86]}

Techopedia defines security architecture as “a unified security design that addresses the necessities and potential risks involved in a certain scenario or environment. It also specifies when and where to apply security controls. The design process is generally reproducible.” The key attributes of security architecture are:^{*[87]}

- the relationship of different components and how they depend on each other.
- the determination of controls based on risk assessment, good practice, finances, and legal matters.
- the standardization of controls.

4.6.3 Security measures

A state of computer “security” is the conceptual ideal, attained by the use of the three processes: threat prevention, detection, and response. These processes are based on various policies and system components, which include the following:

- User account access controls and **cryptography** can protect systems files and data, respectively.
- **Firewalls** are by far the most common prevention systems from a network security perspective as they can (if properly configured) shield access to internal network services, and block certain kinds of attacks through packet filtering. Firewalls can be both hardware- or software-based.
- **Intrusion Detection System (IDS)** products are designed to detect network attacks in-progress and assist in post-attack forensics, while **audit trails** and **logs** serve a similar function for individual systems.
- “Response” is necessarily defined by the assessed security requirements of an individual system and may cover the range from simple upgrade of protections to notification of **legal authorities**, counter-attacks, and the like. In some special cases, a complete destruction of the compromised system is favored, as it may happen that not all the compromised resources are detected.

Today, computer security comprises mainly “preventive” measures, like firewalls or an **exit procedure**. A firewall can be defined as a way of filtering network data between a host or a network and another network, such as the **Internet**, and can be implemented as software running on the machine, hooking into the network stack (or, in the case of most **UNIX**-based operating systems such as **Linux**, built into the operating system **kernel**) to provide real time filtering and blocking. Another implementation is a so-called “physical firewall”, which consists of a separate machine filtering network traffic. Firewalls are common amongst machines that are permanently connected to the **Internet**.

Some organizations are turning to big data platforms, such as **Apache Hadoop**, to extend data accessibility and machine learning to detect **advanced persistent threats**.^{*[88]*[89]}

However, relatively few organisations maintain computer systems with effective detection systems, and fewer still have organised response mechanisms in place. As result, as Reuters points out: “Companies for the first time report they are losing more through electronic theft of data than physical stealing of assets”.^{*[90]} The primary obstacle to effective eradication of cyber crime could be traced to excessive reliance on firewalls and other automated “detection” systems. Yet it is basic evidence gathering by using **packet capture appliances** that puts criminals behind bars.

4.6.4 Vulnerability management

Main article: **Vulnerability management**

Vulnerability management is the cycle of identifying, and remediating or mitigating **vulnerabilities**,^{*[91]} especially in **software** and **firmware**. Vulnerability management is integral to computer security and network security.

Vulnerabilities can be discovered with a **vulnerability scanner**, which analyzes a computer system in search of known vulnerabilities,^{*}[92] such as **open ports**, insecure software configuration, and susceptibility to **malware**

Beyond vulnerability scanning, many organisations contract outside security auditors to run regular penetration tests against their systems to identify vulnerabilities. In some sectors this is a contractual requirement.^{*}[93]

4.6.5 Reducing vulnerabilities

While **formal verification** of the correctness of computer systems is possible,^{*}[94]^{*}[95] it is not yet common. Operating systems formally verified include **seL4**,^{*}[96] and **SYSGO's PikeOS**^{*}[97]^{*}[98] – but these make up a very small percentage of the market.

Cryptography properly implemented is now virtually impossible to directly break. Breaking them requires some non-cryptographic input, such as a stolen key, stolen plaintext (at either end of the transmission), or some other extra cryptanalytic information.

Two factor authentication is a method for mitigating unauthorized access to a system or sensitive information. It requires “something you know”; a password or PIN, and “something you have”; a card, dongle, cellphone, or other piece of hardware. This increases security as an unauthorized person needs both of these to gain access.

Social engineering and direct computer access (physical) attacks can only be prevented by non-computer means, which can be difficult to enforce, relative to the sensitivity of the information. Training is often involved to help mitigate this risk, but even in a highly disciplined environments (e.g. military organizations), social engineering attacks can still be difficult to foresee and prevent.

Enoculation, derived from **Inoculation theory**, seeks to prevent social engineering and other fraudulent tricks or traps by instilling a resistance to persuasion attempts through exposure to similar or related attempts.^{*}[99]

It is possible to reduce an attacker's chances by keeping systems up to date with security patches and updates, using a security scanner or/and hiring competent people responsible for security. The effects of data loss/damage can be reduced by careful **backing up** and **insurance**.

4.6.6 Hardware protection mechanisms

See also: Computer security compromised by hardware failure

While hardware may be a source of insecurity, such as with microchip vulnerabilities maliciously introduced during the manufacturing process,^{*}[100]^{*}[101] hardware-based or assisted computer security also offers an alternative to software-only computer security. Using devices and methods such as **dongles**, **trusted platform modules**, intrusion-aware cases, drive locks, disabling USB ports, and mobile-enabled access may be considered more secure due to the physical access (or sophisticated **backdoor access**) required in order to be compromised. Each of these is covered in more detail below.

- **USB dongles** are typically used in software licensing schemes to unlock software capabilities,^{*}[102] but they can also be seen as a way to prevent unauthorized access to a computer or other device's software. The dongle, or key, essentially creates a secure encrypted tunnel between the software application and the key. The principle is that an encryption scheme on the dongle, such as **Advanced Encryption Standard (AES)** provides a stronger measure of security, since it is harder to hack and replicate the dongle than to simply copy the native software to another machine and use it. Another security application for dongles is to use them for accessing web-based content such as cloud software or **Virtual Private Networks (VPNs)**.^{*}[103] In addition, a USB dongle can be configured to lock or unlock a computer.^{*}[104]
- **Trusted platform modules (TPMs)** secure devices by integrating cryptographic capabilities onto access devices, through the use of microprocessors, or so-called computers-on-a-chip. TPMs used in conjunction with server-side software offer a way to detect and authenticate hardware devices, preventing unauthorized network and data access.^{*}[105]
- **Computer case intrusion detection** refers to a push-button switch which is triggered when a computer case is opened. The firmware or BIOS is programmed to show an alert to the operator when the computer is booted up the next time.

- Drive locks are essentially software tools to encrypt hard drives, making them inaccessible to thieves.*[106] Tools exist specifically for encrypting external drives as well.*[107]
- Disabling USB ports is a security option for preventing unauthorized and malicious access to an otherwise secure computer. Infected USB dongles connected to a network from a computer inside the firewall are considered by the magazine Network World as the most common hardware threat facing computer networks.*[108]
- Mobile-enabled access devices are growing in popularity due to the ubiquitous nature of cell phones. Built-in capabilities such as Bluetooth, the newer Bluetooth low energy (LE), Near field communication (NFC) on non-iOS devices and biometric validation such as thumb print readers, as well as QR code reader software designed for mobile devices, offer new, secure ways for mobile phones to connect to access control systems. These control systems provide computer security and can also be used for controlling access to secure buildings.*[109]

4.6.7 Secure operating systems

Main article: Security-evaluated operating system

One use of the term “computer security” refers to technology that is used to implement secure operating systems. In the 1980s the United States Department of Defense (DoD) used the “Orange Book” *[110] standards, but the current international standard ISO/IEC 15408, “Common Criteria” defines a number of progressively more stringent Evaluation Assurance Levels. Many common operating systems meet the EAL4 standard of being “Methodically Designed, Tested and Reviewed”, but the formal verification required for the highest levels means that they are uncommon. An example of an EAL6 (“Semiformally Verified Design and Tested”) system is Integrity-178B, which is used in the Airbus A380*[111] and several military jets.*[112]

4.6.8 Secure coding

Main article: Secure coding

In software engineering, secure coding aims to guard against the accidental introduction of security vulnerabilities. It is also possible to create software designed from the ground up to be secure. Such systems are "secure by design". Beyond this, formal verification aims to prove the correctness of the algorithms underlying a system;*[113] important for cryptographic protocols for example.

4.6.9 Capabilities and access control lists

Main articles: Access control list and Capability (computers)

Within computer systems, two of many security models capable of enforcing privilege separation are access control lists (ACLs) and capability-based security. Using ACLs to confine programs has been proven to be insecure in many situations, such as if the host computer can be tricked into indirectly allowing restricted file access, an issue known as the confused deputy problem. It has also been shown that the promise of ACLs of giving access to an object to only one person can never be guaranteed in practice. Both of these problems are resolved by capabilities. This does not mean practical flaws exist in all ACL-based systems, but only that the designers of certain utilities must take responsibility to ensure that they do not introduce flaws.

Capabilities have been mostly restricted to research operating systems, while commercial OSs still use ACLs. Capabilities can, however, also be implemented at the language level, leading to a style of programming that is essentially a refinement of standard object-oriented design. An open source project in the area is the E language.

The most secure computers are those not connected to the Internet and shielded from any interference. In the real world, the most secure systems are operating systems where security is not an add-on.

4.6.10 Response to breaches

Responding forcefully to attempted security breaches (in the manner that one would for attempted physical security breaches) is often very difficult for a variety of reasons:

- Identifying attackers is difficult, as they are often in a different jurisdiction to the systems they attempt to breach, and operate through proxies, temporary anonymous dial-up accounts, wireless connections, and other anonymising procedures which make backtracing difficult and are often located in yet another jurisdiction. If they successfully breach security, they are often able to delete logs to cover their tracks.
- The sheer number of attempted attacks is so large that organisations cannot spend time pursuing each attacker (a typical home user with a permanent (e.g., cable modem) connection will be attacked at least several times per day, so more attractive targets could be presumed to see many more). Note however, that most of the sheer bulk of these attacks are made by automated vulnerability scanners and computer worms.
- Law enforcement officers are often unfamiliar with information technology, and so lack the skills and interest in pursuing attackers. There are also budgetary constraints. It has been argued that the high cost of technology, such as DNA testing, and improved forensics mean less money for other kinds of law enforcement, so the overall rate of criminals not getting dealt with goes up as the cost of the technology increases. In addition, the identification of attackers across a network may require logs from various points in the network and in many countries, the release of these records to law enforcement (with the exception of being voluntarily surrendered by a network administrator or a system administrator) requires a search warrant and, depending on the circumstances, the legal proceedings required can be drawn out to the point where the records are either regularly destroyed, or the information is no longer relevant.

4.7 Notable attacks and breaches

Further information: [List of cyber-attacks](#) and [List of data breaches](#)

Some illustrative examples of different types of computer security breaches are given below.

4.7.1 Robert Morris and the first computer worm

Main article: [Morris worm](#)

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers – the first internet "computer worm".*[114] The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.*[114]

4.7.2 Rome Laboratory

In 1994, over a hundred intrusions were made by unidentified crackers into the Rome Laboratory, the US Air Force's main command and research facility. Using trojan horses, hackers were able to obtain unrestricted access to Rome's networking systems and remove traces of their activities. The intruders were able to obtain classified files, such as air tasking order systems data and furthermore able to penetrate connected networks of National Aeronautics and Space Administration's Goddard Space Flight Center, Wright-Patterson Air Force Base, some Defense contractors, and other private sector organizations, by posing as a trusted Rome center user.*[115]

4.7.3 TJX customer credit card details

In early 2007, American apparel and home goods company TJX announced that it was the victim of an unauthorized computer systems intrusion*[116] and that the hackers had accessed a system that stored data on credit card, debit card, check, and merchandise return transactions.*[117]

4.7.4 Stuxnet attack

The computer worm known as Stuxnet reportedly ruined almost one-fifth of Iran's nuclear centrifuges* [118] by disrupting industrial programmable logic controllers (PLCs) in a targeted attack generally believed to have been launched by Israel and the United States* [119]* [120]* [121]* [122] – although neither has publicly admitted this.

4.7.5 Global surveillance disclosures

Main article: Global surveillance disclosures (2013–present)

In early 2013, documents provided by Edward Snowden were published by *The Washington Post* and *The Guardian** [123]* [124] exposing massive the scale of NSA global surveillance. It was also revealed that the NSA had deliberately inserted a backdoor in a NIST standard for encryption* [125] and tapped the links between Google's data centres.* [126]

4.7.6 Target and Home Depot breaches

In 2013 and 2014, a Russian/Ukrainian hacking ring known as “Rescator” broke into Target Corporation computers in 2013, stealing roughly 40 million credit cards,* [127] and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers.* [128] Warnings were delivered at both corporations, but ignored; physical security breaches using self checkout machines are believed to have played a large role. “The malware utilized is absolutely unsophisticated and uninteresting,” says Jim Walter, director of threat intelligence operations at security technology company McAfee – meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

4.7.7 Office of Personnel Management data breach

In April 2015, the Office of Personnel Management discovered it had been hacked more than a year earlier in a data breach, resulting in the theft of approximately 21.5 million personnel records handled by the office.* [129] The Office of Personnel Management hack has been described by federal officials as among the largest breaches of government data in the history of the United States.* [130] Data targeted in the breach included personally identifiable information such as Social Security Numbers,* [131] names, dates and places of birth, addresses, and fingerprints of current and former government employees as well as anyone who had undergone a government background check.* [132] It is believed the hack was perpetrated by Chinese hackers but the motivation remains unclear.* [133]

4.7.8 Ashley Madison breach

Main article: Ashley Madison Data Breach

In July 2015, a hacker group known as “The Impact Team” successfully breached the extramarital relationship website Ashley Madison. The group claimed that they had taken not only company data but user data as well. After the breach, The Impact Team dumped emails from the company's CEO, to prove their point, and threatened to dump customer data unless the website was taken down permanently. With this initial data release, the group stated “Avid Life Media has been instructed to take Ashley Madison and Established Men offline permanently in all forms, or we will release all customer records, including profiles with all the customers' secret sexual fantasies and matching credit card transactions, real names and addresses, and employee documents and emails. The other websites may stay online.” * [134] When Avid Life Media, the parent company that created the Ashley Madison website, did not take the site offline, The Impact Group released two more compressed files, one 9.7GB and the second 20GB. After the second data dump, Avid Life Media CEO Noel Biderman resigned, but the website remained functional.

4.8 Legal issues and global regulation

Conflict of laws in cyberspace has become a major cause of concern for computer security community. Some of the main challenges and complaints about the antivirus industry are the lack of global web regulations, a global base of common rules to judge, and eventually punish, **cyber crimes** and cyber criminals. There is no global cyber law and cyber security treaty that can be invoked for enforcing global cyber security issues.

International legal issues of cyber attacks are complicated in nature. Even if an antivirus firm locates the cybercriminal behind the creation of a particular **virus** or piece of **malware** or form of **cyber attack**, often the local authorities cannot take action due to lack of laws under which to prosecute.*[135]*[136] Authorship attribution for cyber crimes and cyber attacks is a major problem for all law enforcement agencies.

"[Computer viruses] switch from one country to another, from one jurisdiction to another – moving around the world, using the fact that we don't have the capability to globally police operations like this. So the Internet is as if someone [had] given free plane tickets to all the online criminals of the world." * [135] Use of **dynamic DNS**, **fast flux** and **bullet proof servers** have added own complexities to this situation.

4.9 Role of government

The role of the government is to make **regulations** to force companies and organizations to protect their systems, infrastructure and information from any **cyber-attacks**, but also to protect its own national infrastructure such as the **national power-grid**.*[137]

The question of whether the government should intervene or not in the regulation of the **cyberspace** is a very polemical one. Indeed, for as long as it has existed and by definition, the **cyberspace** is a **virtual space** free of any government intervention. Where everyone agrees that an improvement on **cyber security** is more than vital, is the government the best actor to solve this issue? Many government officials and experts think that the government should step in and that there is a crucial need for regulation, mainly due to the failure of the private sector to solve efficiently the **cybersecurity** problem. R. Clarke said during a panel discussion at the **RSA Security Conference** in San Francisco, he believes that the "industry only responds when you threaten regulation. If the industry doesn't respond (to the threat), you have to follow through." *[138] On the other hand, executives from the private sector agree that improvements are necessary, but think that the government intervention would affect their ability to innovate efficiently.

4.10 International actions

Many different teams and organisations exist, including:

- The Forum of Incident Response and Security Teams (FIRST) is the global association of CSIRTs.*[139] The US-CERT, AT&T, Apple, Cisco, McAfee, Microsoft are all members of this international team.*[140]
- The Council of Europe helps protect societies worldwide from the threat of cybercrime through the Convention on Cybercrime.*[141]
- The purpose of the Messaging Anti-Abuse Working Group (MAAWG) is to bring the messaging industry together to work collaboratively and to successfully address the various forms of messaging abuse, such as spam, viruses, denial-of-service attacks and other messaging exploitations.*[142] France Telecom, Facebook, AT&T, Apple, Cisco, Sprint are some of the members of the MAAWG.*[143]
- ENISA : The European Network and Information Security Agency (ENISA) is an agency of the European Union with the objective to improve network and information security in the European Union.

4.10.1 Europe

CSIRTs in Europe collaborate in the **TERENA** task force TF-CSIRT. **TERENA**'s Trusted Introducer service provides an accreditation and certification scheme for CSIRTs in Europe. A full list of known CSIRTs in Europe is available from the Trusted Introducer website.

4.11 National actions

4.11.1 Computer emergency response teams

Main article: Computer emergency response team

Most countries have their own computer emergency response team to protect network security.

4.11.2 Canada

On October 3, 2010, Public Safety Canada unveiled Canada's Cyber Security Strategy, following a Speech from the Throne commitment to boost the security of Canadian cyberspace.*[144]*[145] The aim of the strategy is to strengthen Canada's "cyber systems and critical infrastructure sectors, support economic growth and protect Canadians as they connect to each other and to the world."*[145] Three main pillars define the strategy: securing government systems, partnering to secure vital cyber systems outside the federal government, and helping Canadians to be secure online.*[145] The strategy involves multiple departments and agencies across the Government of Canada.*[146] The Cyber Incident Management Framework for Canada outlines these responsibilities, and provides a plan for co-ordinated response between government and other partners in the event of a cyber incident.*[147] The Action Plan 2010–2015 for Canada's Cyber Security Strategy outlines the ongoing implementation of the strategy.*[148]

Public Safety Canada's Canadian Cyber Incident Response Centre (CCIRC) is responsible for mitigating and responding to threats to Canada's critical infrastructure and cyber systems. The CCIRC provides support to mitigate cyber threats, technical support to respond and recover from targeted cyber attacks, and provides online tools for members of Canada's critical infrastructure sectors.*[149] The CCIRC posts regular cyber security bulletins on the Public Safety Canada website.*[150] The CCIRC also operates an online reporting tool where individuals and organizations can report a cyber incident.*[151] Canada's Cyber Security Strategy is part of a larger, integrated approach to critical infrastructure protection, and functions as a counterpart document to the National Strategy and Action Plan for Critical Infrastructure.*[146]

On September 27, 2010, Public Safety Canada partnered with STOP.THINK.CONNECT, a coalition of non-profit, private sector, and government organizations dedicated to informing the general public on how to protect themselves online.*[152] On February 4, 2014, the Government of Canada launched the Cyber Security Cooperation Program.*[153] The program is a \$1.5 million five-year initiative aimed at improving Canada's cyber systems through grants and contributions to projects in support of this objective.*[154] Public Safety Canada aims to begin an evaluation of Canada's Cyber Security Strategy in early 2015.*[146] Public Safety Canada administers and routinely updates the GetCyberSafe portal for Canadian citizens, and carries out Cyber Security Awareness Month during October.*[155]

4.11.3 China

China's Central Leading Group for Internet Security and Informatization (Chinese: 中央网络安全和信息化领导小组) was established on February 27, 2014. This Leading Small Group (LSG) of the Communist Party of China is headed by General Secretary Xi Jinping himself and is staffed with relevant Party and state decision-makers. The LSG was created to overcome the incoherent policies and overlapping responsibilities that characterized China's former cyberspace decision-making mechanisms. The LSG oversees policy-making in the economic, political, cultural, social and military fields as they relate to network security and IT strategy. This LSG also coordinates major policy initiatives in the international arena that promote norms and standards favored by the Chinese government and that emphasize the principle of national sovereignty in cyberspace.*[156]

4.11.4 Germany

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) Nationales Cyber-Abwehrzentrum located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) Bundesamt für Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt für den Militärischen Ab-

schirmdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organization founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.

4.11.5 India

Some provisions for cyber security have been incorporated into rules framed under the Information Technology Act 2000.

The National Cyber Security Policy 2013 is a policy framework by Ministry of Electronics and Information Technology (MeitY) which aims to protect the public and private infrastructure from cyber attacks, and safeguard “information, such as personal information (of web users), financial and banking information and sovereign data” .

The Indian Companies Act 2013 has also introduced cyber law and cyber security obligations on the part of Indian directors.

4.11.6 Portugal

O CNCS em Portugal promove a utilização do ciberespaço de uma forma livre, confiável e segura, através da melhoria contínua da cibersegurança nacional e da cooperação internacional. —Cyber Security Services, Nano IT Security is a Portuguese company specialized in cyber security, pentesting and vulnerability analyses.

4.11.7 Pakistan

Cyber-crime has risen rapidly in Pakistan. There are about 34 million Internet users with 133.4 million mobile subscribers in Pakistan. According to Cyber Crime Unit (CCU), a branch of Federal Investigation Agency, only 62 cases were reported to the unit in 2007, 287 cases in 2008, ratio dropped in 2009 but in 2010, more than 312 cases were registered. However, there are many unreported incidents of cyber-crime.*[157]

“Pakistan's Cyber Crime Bill 2007”, the first pertinent law, focuses on electronic crimes, for example cyber-terrorism, criminal access, electronic system fraud, electronic forgery, and misuse of encryption.*[157]

National Response Centre for Cyber Crime (NR3C) – FIA is a law enforcement agency dedicated to fighting cyber crime. Inception of this Hi-Tech crime fighting unit transpired in 2007 to identify and curb the phenomenon of technological abuse in society.*[158] However, certain private firms are also working in cohesion with the government to improve cyber security and curb cyber attacks.*[159]

People in Pakistan can now report terrorist and extremist online content on Surfsafe® Pakistan web portal. Surfsafe® is an initiative by CODEPAK. Tier3 Cyber Security Pakistan led the development of the Surfsafe® e-system which includes reporting portal and Surfsafe® e-Scouts system. The National Counter Terrorism Authority (NACTA) of Pakistan provides the leadership for the Surfsafe® Campaign.*[160]

4.11.8 South Korea

Following cyber attacks in the first half of 2013, when the government, news media, television station, and bank websites were compromised, the national government committed to the training of 5,000 new cybersecurity experts by 2017. The South Korean government blamed its northern counterpart for these attacks, as well as incidents that occurred in 2009, 2011,*[161] and 2012, but Pyongyang denies the accusations.*[162]

4.11.9 United States

Legislation

The 1986 18 U.S.C. § 1030, more commonly known as the Computer Fraud and Abuse Act is the key legislation. It prohibits unauthorized access or damage of “protected computers” as defined in 18 U.S.C. § 1030(e)(2).

Although various other measures have been proposed, such as the “Cybersecurity Act of 2010 – S. 773” in 2009, the “International Cybercrime Reporting and Cooperation Act – H.R.4962” *[163] and “Protecting Cyberspace as a National Asset Act of 2010 – S.3480” *[164] in 2010 – none of these has succeeded.

Executive order 13636 *Improving Critical Infrastructure Cybersecurity* was signed February 12, 2013.

Agencies

The Department of Homeland Security has a dedicated division responsible for the response system, risk management program and requirements for cybersecurity in the United States called the National Cyber Security Division.*[165]*[166] The division is home to US-CERT operations and the National Cyber Alert System.*[166] The National Cybersecurity and Communications Integration Center brings together government organizations responsible for protecting computer networks and networked infrastructure.*[167]

The third priority of the Federal Bureau of Investigation (FBI) is to: “*Protect the United States against cyber-based attacks and high-technology crimes*”, *[168] and they, along with the National White Collar Crime Center (NW3C), and the Bureau of Justice Assistance (BJA) are part of the multi-agency task force, The Internet Crime Complaint Center, also known as IC3.*[169]

In addition to its own specific duties, the FBI participates alongside non-profit organizations such as InfraGard.*[170]*[171]

In the criminal division of the United States Department of Justice operates a section called the Computer Crime and Intellectual Property Section. The CCIPS is in charge of investigating computer crime and intellectual property crime and is specialized in the search and seizure of digital evidence in computers and networks.*[172]

The United States Cyber Command, also known as USCYBERCOM, is tasked with the defense of specified Department of Defense information networks and “*ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.*” *[173] It has no role in the protection of civilian networks.*[174]*[175]

The U.S. Federal Communications Commission's role in cybersecurity is to strengthen the protection of critical communications infrastructure, to assist in maintaining the reliability of networks during disasters, to aid in swift recovery after, and to ensure that first responders have access to effective communications services.*[176]

The Food and Drug Administration has issued guidance for medical devices,*[177] and the National Highway Traffic Safety Administration*[178] is concerned with automotive cybersecurity. After being criticized by the Government Accountability Office,*[179] and following successful attacks on airports and claimed attacks on airplanes, the Federal Aviation Administration has devoted funding to securing systems on board the planes of private manufacturers, and the Aircraft Communications Addressing and Reporting System.*[180] Concerns have also been raised about the future Next Generation Air Transportation System.*[181]

Computer emergency readiness team

“Computer emergency response team” is a name given to expert groups that handle computer security incidents. In the US, two distinct organization exist, although they do work closely together.

- US-CERT: part of the National Cyber Security Division of the United States Department of Homeland Security.*[182]
- CERT/CC: created by the Defense Advanced Research Projects Agency (DARPA) and run by the Software Engineering Institute (SEI).

4.12 Modern warfare

Main article: Cyberwarfare

There is growing concern that cyberspace will become the next theater of warfare. As Mark Clayton from the *Christian Science Monitor* described in an article titled “The New Cyber Arms Race”:

In the future, wars will not just be fought by soldiers with guns or with planes that drop bombs. They will also be fought with the click of a mouse a half a world away that unleashes carefully weaponized

computer programs that disrupt or destroy critical industries like utilities, transportation, communications, and energy. Such attacks could also disable military networks that control the movement of troops, the path of jet fighters, the command and control of warships.*[183]

This has led to new terms such as *cyberwarfare* and *cyberterrorism*. The United States Cyber Command was created in 2009*[184] and many other countries have similar forces.

4.13 Job market

Cybersecurity is a fast-growing*[185] field of IT concerned with reducing organizations' risk of hack or data breach. According to research from the Enterprise Strategy Group, 46% of organizations say that they have a “problematic shortage” of cybersecurity skills in 2016, up from 28% in 2015.*[186] Commercial, government and non-governmental organizations all employ cybersecurity professionals. The fastest increases in demand for cybersecurity workers are in industries managing increasing volumes of consumer data such as finance, health care, and retail.*[187] However, the use of the term “cybersecurity” is more prevalent in government job descriptions.*[188]

Cybersecurity is increasingly affected by Department of Defense (DoD) Dir. 8570.1M and 8140. Dir. 8570.1 was enacted in 2004 and mandates specific industry credentials for certain [positions with DoD or any contractor working for DoD. Research on college students and high school students has been done to determine whether relevant Information Technology industry certification is an asset to the teaching profession as they appear to be in the business world. [Andersson, D. (2009), Information Technology Industry Certification’s Impact on Undergraduate Student Perception of Instructor Effectiveness., UMI Dissertation Publishing Group, Volume 7005A. Publication No. 3358241] [Reimers, K. (2009), Impact of Information Technology (IT) Industry Certification on the Achievement of High School Students Enrolled in Technology Courses]. Andersson and Reimers found that CIS/IT students were keenly aware if their instructors had them. For example, certain certifications DOD 8570.1M are the only commercial certifications that the Department of Defense will accept towards meeting their Information Assurance hiring requirements.

*[189]

Typical cyber security job titles and descriptions include:*[190]

Security analyst Analyzes and assesses vulnerabilities in the infrastructure (software, hardware, networks), investigates using available tools and countermeasures to remedy the detected vulnerabilities, and recommends solutions and best practices. Analyzes and assesses damage to the data/infrastructure as a result of security incidents, examines available recovery tools and processes, and recommends solutions. Tests for compliance with security policies and procedures. May assist in the creation, implementation, or management of security solutions.

Security engineer

Performs security monitoring, security and data/logs analysis, and forensic analysis, to detect security incidents, and mounts the incident response. Investigates and utilizes new technologies and processes to enhance security capabilities and implement improvements. May also review code or perform other security engineering methodologies.

Security architect

Designs a security system or major components of a security system, and may head a security design team building a new security system.

Security administrator

Installs and manages organization-wide security systems. May also take on some of the tasks of a security analyst in smaller organizations.

Chief Information Security Officer (CISO)

A high-level management position responsible for the entire information security division/staff. The position may include hands-on technical work.

Chief Security Officer (CSO)

A high-level management position responsible for the entire security division/staff. A newer position now deemed needed as security risks grow.

Security Consultant/Specialist/Intelligence

Broad titles that encompass any one or all of the other roles or titles tasked with protecting computers, networks, software, data or information systems against viruses, worms, spyware, malware, intrusion detection, unauthorized access, denial-of-service attacks, and an ever increasing list of attacks by hackers acting as individuals or as part of organized crime or foreign governments.

Student programs are also available to people interested in beginning a career in cybersecurity.*[191]*[192] Meanwhile, a flexible and effective option for **information security** professionals of all experience levels to keep studying is online security training, including webcasts.*[193]*[194]*[195]

4.14 Terminology

The following terms used with regards to engineering secure systems are explained below.

- Access authorization restricts access to a computer to the group of users through the use of authentication systems. These systems can protect either the whole computer – such as through an interactive **login** screen – or individual services, such as an **FTP** server. There are many methods for identifying and authenticating users, such as **passwords**, **identification cards**, and, more recently, **smart cards** and **biometric systems**.
- **Anti-virus** software consists of computer programs that attempt to identify, thwart and eliminate **computer viruses** and other malicious software (**malware**).
- Applications are **executable code**, so general practice is to disallow users the power to install them; to install only those which are known to be reputable – and to reduce the **attack surface** by installing as few as possible. They are typically run with **least privilege**, with a robust process in place to identify, test and install any released security patches or updates for them.
- **Authentication** techniques can be used to ensure that communication end-points are who they say they are.]
- **Automated theorem proving** and other verification tools can enable critical algorithms and code used in secure systems to be mathematically proven to meet their specifications.
- **Backups** are one or more copies kept of important computer files. Typically multiple copies, (e.g. daily weekly and monthly), will be kept in different location away from the original, so that they are secure from damage if the original location has its security breached by an attacker, or is destroyed or damaged by natural disasters.
- **Capability and access control list** techniques can be used to ensure privilege separation and mandatory access control. This section discusses their use.
- **Chain of trust** techniques can be used to attempt to ensure that all software loaded has been certified as authentic by the system's designers.
- **Confidentiality** is the nondisclosure of information except to another authorized person.*[196]
- **Cryptographic** techniques can be used to defend data in transit between systems, reducing the probability that data exchanged between systems can be intercepted or modified.
- **Cyberwarfare** is an internet-based conflict that involves politically motivated attacks on information and information systems. Such attacks can, for example, disable official websites and networks, disrupt or disable essential services, steal or alter classified data, and cripple financial systems.
- **Data integrity** is the accuracy and consistency of stored data, indicated by an absence of any alteration in data between two updates of a data record.*[197]

This is secret stuff, PSE do not...

5a0 (k\$hQ% ...

This is secret stuff, PSE do not...

Cryptographic techniques involve transforming information, scrambling it so it becomes unreadable during transmission. The intended recipient can unscramble the message; ideally, eavesdroppers cannot.

- Encryption is used to protect the message from the eyes of others. Cryptographically secure ciphers are designed to make any practical attempt of breaking infeasible. Symmetric-key ciphers are suitable for bulk encryption using shared keys, and public-key encryption using digital certificates can provide a practical solution for the problem of securely communicating when no key is shared in advance.
- Endpoint security software helps networks to prevent exfiltration (data theft) and virus infection at network entry points made vulnerable by the prevalence of potentially infected portable computing devices, such as laptops and mobile devices, and external storage devices, such as USB drives.^{*}[198]
- Firewalls serve as a gatekeeper system between networks, allowing only traffic that matches defined rules. They often include detailed logging, and may include intrusion detection and intrusion prevention features. They are near-universal between company local area networks and the Internet, but can also be used internally to impose traffic rules between networks if network segmentation is configured.
- Honey pots are computers that are intentionally left vulnerable to attack by crackers. They can be used to catch crackers and to identify their techniques.
- Intrusion-detection systems can scan a network for people that are on the network but who should not be there or are doing things that they should not be doing, for example trying a lot of passwords to gain access to the network.
- A microkernel is an approach to operating system design which has only the near-minimum amount of code running at the most privileged level – and runs other elements of the operating system such as device drivers, protocol stacks and file systems, in the safer, less privileged user space.
- Pinging. The standard “ping” application can be used to test if an IP address is in use. If it is, attackers may then try a port scan to detect which services are exposed.
- A port scan is used to probe an IP address for open ports, and hence identify network services running there.
- Social engineering is the use of the use of deception to manipulate individuals to breach security.

4.15 Scholars

- Ross J. Anderson
- Annie Anton
- Adam Back
- Daniel J. Bernstein
- Matt Blaze
- Stefan Brands
- L. Jean Camp

- Lance Cottrell
- Lorrie Cranor
- Dorothy E. Denning
- Peter J. Denning
- Cynthia Dwork
- Deborah Estrin
- Joan Feigenbaum
- Ian Goldberg
- Shafi Goldwasser
- Lawrence A. Gordon
- Peter Gutmann
- Paul Kocher
- Monica S. Lam
- Butler Lampson
- Brian LaMacchia
- Carl Landwehr
- Kevin Mitnick
- Peter G. Neumann
- Susan Nycum
- Roger R. Schell
- Bruce Schneier
- Dawn Song
- Gene Spafford
- Joseph Steinberg
- Salvatore J. Stolfo
- Willis Ware
- Moti Yung

4.16 See also

- Attack tree
- CAPTCHA
- CertiVox
- Cloud computing security
- Common Criteria
- Comparison of antivirus software

- Computer security model
- Content Disarm & Reconstruction
- Content security
- Countermeasure (computer)
- Cyber hygiene
- Cyber-Insurance
- Cyber security standards
- Cyber self-defense
- Dancing pigs
- Data security
- Differentiated security
- Disk encryption
- Exploit (computer security)
- Fault tolerance
- Hardware security
- Human–computer interaction (security)
- Identity management
- Identity theft
- Identity-based security
- Information security awareness
- Internet privacy
- IT risk
- Kill chain
- List of computer security certifications
- MySecureCyberspace
- Open security
- Outline of computer security
- OWASP
- Penetration test
- Physical information security
- Presumed security
- Privacy software
- Proactive cyber defence
- Risk cybernetics
- Sandbox (computer security)
- Separation of protection and security
- Software Defined Perimeter

4.17 References

- [1] Gasser, Morrie (1988). *Building a Secure Computer System* (PDF). Van Nostrand Reinhold. p. 3. ISBN 0-442-23022-2. Retrieved 6 September 2015.
- [2] “Definition of computer security” . *Encyclopedia*. Ziff Davis, PCMag. Retrieved 6 September 2015.
- [3] Rouse, Margaret. “Social engineering definition” . TechTarget. Retrieved 6 September 2015.
- [4] “Reliance spells end of road for ICT amateurs” , May 07, 2013, The Australian
- [5] “Computer Security and Mobile Security Challenges” (pdf). *researchgate.net*. Retrieved 2016-08-04.
- [6] “Distributed Denial of Service Attack” . *cса.gov.sg*. Retrieved 12 November 2014.
- [7] Wireless mouse leave billions at risk of computer hack: cyber security firm
- [8] “What is Spoofing? – Definition from Techopedia” .
- [9] Gallagher, Sean (May 14, 2014). “Photos of an NSA “upgrade” factory show Cisco router getting implant” . Ars Technica. Retrieved August 3, 2014.
- [10] “Identifying Phishing Attempts” . Case.
- [11] Arcos Sergio. “Social Engineering” (PDF).
- [12] Scannell, Kara (24 Feb 2016). “CEO email scam costs companies \$2bn” . *Financial Times* (25 Feb 2016). Retrieved 7 May 2016.
- [13] “Bucks leak tax info of players, employees as result of email scam” . *Associated Press*. 20 May 2016. Retrieved 20 May 2016.
- [14] Lim, Joo S., et al. “Exploring the Relationship between Organizational Culture and Information Security Culture.” Australian Information Security Management Conference.
- [15]
- [16] Schlienger, Thomas; Teufel, Stephanie (2003). “Information security culture-from analysis to change” . *South African Computer Journal*. 31: 46–52.
- [17] “Financial Weapons of War” . *Minnesota Law Review*. 2016. SSRN 2765010 
- [18] Pagliery, Jose. “Hackers attacked the U.S. energy grid 79 times this year” . *CNN Money*. Cable News Network. Retrieved 16 April 2015.
- [19] “Vulnerabilities in Smart Meters and the C12.12 Protocol” . SecureState. 2012-02-16. Retrieved 4 November 2016.
- [20] P. G. Neumann, “Computer Security in Aviation,” presented at International Conference on Aviation Safety and Security in the 21st Century, White House Commission on Safety and Security, 1997.
- [21] J. Zellan, *Aviation Security*. Hauppauge, NY: Nova Science, 2003, pp. 65–70.
- [22] “Air Traffic Control Systems Vulnerabilities Could Make for Unfriendly Skies [Black Hat] - SecurityWeek.Com” .
- [23] “Hacker Says He Can Break Into Airplane Systems Using In-Flight Wi-Fi” . *NPR.org*. 4 August 2014.
- [24] Jim Finkle (4 August 2014). “Hacker says to show passenger jets at risk of cyber attack” . *Reuters*.
- [25] “Pan-European Network Services (PENS) - Eurocontrol.int” .
- [26] “Centralised Services: NewPENS moves forward - Eurocontrol.int” .
- [27] “NextGen Data Communication” . FAA.
- [28] “Is Your Watch Or Thermostat A Spy? Cybersecurity Firms Are On It” . *NPR.org*. 6 August 2014.
- [29] Melvin Backman (18 September 2014). “Home Depot: 56 million cards exposed in breach” . CNNMoney.
- [30] “Staples: Breach may have affected 1.16 million customers' cards” . Fortune.com. December 19, 2014. Retrieved 2014-12-21.

- [31] “Target security breach affects up to 40M cards” . *Associated Press via Milwaukee Journal Sentinel*. 19 December 2013. Retrieved 21 December 2013.
- [32] Jim Finkle (23 April 2014). “Exclusive: FBI warns healthcare sector vulnerable to cyber attacks” . *Reuters*. Retrieved 23 May 2016.
- [33] Bright, Peter (February 15, 2011). “Anonymous speaks: the inside story of the HBGary hack” . Arstechnica.com. Retrieved March 29, 2011.
- [34] Anderson, Nate (February 9, 2011). “How one man tracked down Anonymous—and paid a heavy price” . Arstechnica.com. Retrieved March 29, 2011.
- [35] Palilery, Jose (December 24, 2014). “What caused Sony hack: What we know now” . CNN Money. Retrieved January 4, 2015.
- [36] James Cook (December 16, 2014). “Sony Hackers Have Over 100 Terabytes Of Documents. Only Released 200 Gigabytes So Far” . *Business Insider*. Retrieved December 18, 2014.
- [37] Timothy B. Lee (18 January 2015). “The next frontier of hacking: your car” . Vox.
- [38] Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk (PDF) (Report). 2015-02-06. Retrieved November 4, 2016.
- [39] Staff, AOL. “Cybersecurity expert: It will take a 'major event' for companies to take this issue seriously” . AOL.com. Retrieved 22 January 2017.
- [40] “The problem with self-driving cars: who controls the code?”. The Guardian. 23 December 2015. Retrieved 22 January 2017.
- [41] Stephen Checkoway; Damon McCoy; Brian Kantor; Danny Anderson; Hovav Shacham; Stefan Savage; Karl Koscher; Alexei Czeskis; Franziska Roesner; Tadayoshi Kohno (2011). *Comprehensive Experimental Analyses of Automotive Attack Surfaces* (PDF). SEC'11 Proceedings of the 20th USENIX conference on Security. Berkeley, CA, US: USENIX Association. pp. 6–6.
- [42] Greenberg, Andy. “Hackers Remotely Kill a Jeep on the Highway—With Me in It” . WIRED. Retrieved 22 January 2017.
- [43] “Hackers take control of car, drive it into a ditch” . The Independent. 22 July 2015. Retrieved 22 January 2017.
- [44] “Tesla fixes software bug that allowed Chinese hackers to control car remotely” . The Telegraph. Retrieved 22 January 2017.
- [45] Kang, Cecilia (19 September 2016). “Self-Driving Cars Gain Powerful Ally: The Government” . The New York Times. Retrieved 22 January 2017.
- [46] “Federal Automated Vehicles Policy” (PDF). Retrieved 22 January 2017.
- [47] “Internet strikes back: Anonymous' Operation Megaupload explained” . RT. 20 January 2012. Archived from the original on 5 May 2013. Retrieved May 5, 2013.
- [48] “Gary McKinnon profile: Autistic 'hacker' who started writing computer programs at 14” . The Daily Telegraph. London. 23 January 2009.
- [49] “Gary McKinnon extradition ruling due by 16 October” . BBC News. September 6, 2012. Retrieved September 25, 2012.
- [50] Law Lords Department (30 July 2008). “House of Lords – Mckinnon V Government of The United States of America and Another” . Publications.parliament.uk. Retrieved 30 January 2010. 15. …alleged to total over \$700,000
- [51] “NSA Accessed Mexican President's Email” , October 20, 2013, Jens Glüsing, Laura Poitras, Marcel Rosenbach and Holger Stark, spiegel.de
- [52] Sanders, Sam (4 June 2015). “Massive Data Breach Puts 4 Million Federal Employees' Records At Risk” . NPR. Retrieved 5 June 2015.
- [53] Liptak, Kevin (4 June 2015). “U.S. government hacked; feds think China is the culprit” . CNN. Retrieved 5 June 2015.
- [54] Sean Gallagher. “Encryption ‘would not have helped’ at OPM, says DHS official” .
- [55] “Schools Learn Lessons From Security Breaches” . Education Week. 19 October 2015. Retrieved 23 May 2016.

- [56] “Internet of Things Global Standards Initiative” . *ITU*. Retrieved 26 June 2015.
- [57] Singh, Jatinder; Pasquier, Thomas; Bacon, Jean; Ko, Hajoon; Eyers, David (2015). “Twenty Cloud Security Considerations for Supporting the Internet of Things” . *IEEE Internet of Things Journal*: 1–1. doi:10.1109/JIOT.2015.2460333.
- [58] Chris Clearfield. “Why The FTC Can't Regulate The Internet Of Things” . *Forbes*. Retrieved 26 June 2015.
- [59] “Internet of Things: Science Fiction or Business Fact?” (PDF). *Harvard Business Review*. Retrieved 4 November 2016.
- [60] Ovidiu Vermesan; Peter Friess. “Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems” (PDF). River Publishers. Retrieved 4 November 2016.
- [61] Christopher Clearfield “Rethinking Security for the Internet of Things” Harvard Business Review Blog, 26 June 2013/
- [62] “Hotel room burglars exploit critical flaw in electronic door locks” . *Ars Technica*. Retrieved 23 May 2016.
- [63] “Hospital Medical Devices Used As Weapons In Cyberattacks” . *Dark Reading*. Retrieved 23 May 2016.
- [64] Jeremy Kirk (17 October 2012). “Pacemaker hack can deliver deadly 830-volt jolt” . *Computerworld*. Retrieved 23 May 2016.
- [65] “How Your Pacemaker Will Get Hacked” . *The Daily Beast*. Retrieved 23 May 2016.
- [66] Leetaru, Kalle. “Hacking Hospitals And Holding Hostages: Cybersecurity In 2016” . *Forbes*. Retrieved 29 December 2016.
- [67] “Cyber-Angriffe: Krankenhäuser rücken ins Visier der Hacker” . Wirtschafts Woche. Retrieved 29 December 2016.
- [68] “Hospitals keep getting attacked by ransomware —Here's why” . *Business Insider*. Retrieved 29 December 2016.
- [69] “MedStar Hospitals Recovering After 'Ransomware' Hack” . *NBC News*. Retrieved 29 December 2016.
- [70] Pauli, Darren. “US hospitals hacked with ancient exploits” . *The Register*. Retrieved 29 December 2016.
- [71] Pauli, Darren. “Zombie OS lurches through Royal Melbourne Hospital spreading virus” . *The Register*. Retrieved 29 December 2016.
- [72] “Grimsby hospital computer attack: 'No ransom has been demanded'" . *Grimsby Telegraph*. 31 October 2016. Retrieved 29 December 2016.
- [73] “Hacked Lincolnshire hospital computer systems 'back up'" . *BBC News*. 2 November 2016. Retrieved 29 December 2016.
- [74] “Lincolnshire operations cancelled after network attack” . *BBC News*. 31 October 2016. Retrieved 29 December 2016.
- [75] “Legion cyber-attack: Next dump is sansad.nic.in, say hackers” . *The Indian Express*. 12 December 2016. Retrieved 29 December 2016.
- [76] “15k patients’ info shared on social media from NH Hospital data breach” . *RT International*. Retrieved 29 December 2016.
- [77] “Former New Hampshire Psychiatric Hospital Patient Accused Of Data Breach” . *CBS Boston*. Retrieved 29 December 2016.
- [78] “Texas Hospital hacked, affects nearly 30,000 patient records” . *Healthcare IT News*. 4 November 2016. Retrieved 29 December 2016.
- [79] Becker, Rachel (27 December 2016). “New cybersecurity guidelines for medical devices tackle evolving threats” . *The Verge*. Retrieved 29 December 2016.
- [80] “Postmarket Management of Cybersecurity in Medical Devices” (PDF). 28 December 2016. Retrieved 29 December 2016.
- [81] Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). The Economic Impact of Cyber-Attacks. Congressional Research Service, Government and Finance Division. Washington DC: The Library of Congress.
- [82] Gordon, Lawrence; Loeb, Martin (November 2002). “The Economics of Information Security Investment” . *ACM Transactions on Information and System Security*. 5 (4): 438–457. doi:10.1145/581271.581274.
- [83] RFC 2828 Internet Security Glossary
- [84] CNSS Instruction No. 4009 dated 26 April 2010

- [85] InfosecToday Glossary
- [86] Definitions: IT Security Architecture. SecurityArchitecture.org, Jan, 2006
- [87] Jannsen, Cory. “Security Architecture” . *Techopedia*. Janalta Interactive Inc. Retrieved 9 October 2014.
- [88] “Cybersecurity at petabyte scale” .
- [89] Woodie, Alex (9 May 2016). “Why ONI May Be Our Best Hope for Cyber Security Now” . Retrieved 13 July 2016.
- [90] “Firms lose more to electronic than physical theft” . Reuters.
- [91] Foreman, P: *Vulnerability Management*, page 1. Taylor & Francis Group, 2010. ISBN 978-1-4398-0150-5
- [92] Anna-Maija Juuso and Ari Takanen *Unknown Vulnerability Management*, Codenomicon whitepaper, October 2010 .
- [93] Alan Calder and Geraint Williams. *PCI DSS: A Pocket Guide, 3rd Edition*. ISBN 978-1-84928-554-4. network vulnerability scans at least quarterly and after any significant change in the network
- [94] Harrison, J. (2003). “Formal verification at Intel”: 45–54. doi:10.1109/LICS.2003.1210044.
- [95] Umrigar, Zerkis D.; Pitchumani, Vijay (1983). “Formal verification of a real-time hardware design” . *Proceeding DAC '83 Proceedings of the 20th Design Automation Conference*. IEEE Press. pp. 221–7. ISBN 0-8186-0026-8.
- [96] “Abstract Formal Specification of the seL4/ARMv6 API” (PDF). Archived from the original (PDF) on 21 May 2015. Retrieved May 19, 2015.
- [97] Christoph Baumann, Bernhard Beckert, Holger Blasum, and Thorsten Bormer Ingredients of Operating System Correctness? Lessons Learned in the Formal Verification of PikeOS
- [98] “Getting it Right” by Jack Ganssle
- [99] Treglia, J., & Delia, M. (2017). Cyber Security Inoculation. Presented at NYS Cyber Security Conference, Empire State Plaza Convention Center, Albany, NY, June 3–4.
- [100] “The Hacker in Your Hardware: The Next Security Threat” . *Scientific American*.
- [101] Waksman, Adam; Sethumadhavan, Simha (2010), “Tamper Evident Microprocessors” (PDF), *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, California
- [102] “Sentinel HASP HL” . E-Spin. Retrieved 2014-03-20.
- [103] “Token-based authentication” . SafeNet.com. Retrieved 2014-03-20.
- [104] “Lock and protect your Windows PC” . TheWindowsClub.com. Retrieved 2014-03-20.
- [105] James Greene (2012). “Intel Trusted Execution Technology: White Paper” (PDF). Intel Corporation. Retrieved 2013-12-18.
- [106] “SafeNet ProtectDrive 8.4” . SCMagazine.com. 2008-10-04. Retrieved 2014-03-20.
- [107] “Secure Hard Drives: Lock Down Your Data” . PCMag.com. 2009-05-11.
- [108] “Top 10 vulnerabilities inside the network” . Network World. 2010-11-08. Retrieved 2014-03-20.
- [109] “Forget IDs, use your phone as credentials” . Fox Business Network. 2013-11-04. Retrieved 2014-03-20.
- [110] Lipner, Steve (2015). “The Birth and Death of the Orange Book” . *IEEE Annals of the History of Computing*. 37 (2): 19–31. doi:10.1109/MAHC.2015.27.
- [111] Kelly Jackson Higgins (2008-11-18). “Secure OS Gets Highest NSA Rating, Goes Commercial” . Dark Reading. Retrieved 2013-12-01.
- [112] “Board or bored? Lockheed Martin gets into the COTS hardware biz” . VITA Technologies Magazine. December 10, 2010. Retrieved 9 March 2012.
- [113] Sanghavi, Alok (21 May 2010). “What is formal verification?” . *EE Times_Aisia*.
- [114] Jonathan Zittrain, ‘The Future of The Internet’, Penguin Books, 2008
- [115] Information Security. United States Department of Defense, 1986

- [116] “THE TJX COMPANIES, INC. VICTIMIZED BY COMPUTER SYSTEMS INTRUSION; PROVIDES INFORMATION TO HELP PROTECT CUSTOMERS” (Press release). The TJX Companies, Inc. 2007-01-17. Retrieved 2009-12-12.
- [117] Largest Customer Info Breach Grows. MyFox Twin Cities, 29 March 2007.
- [118] “The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought” . Business Insider. 20 November 2013.
- [119] Reals, Tucker (24 September 2010). “Stuxnet Worm a U.S. Cyber-Attack on Iran Nukes?”. CBS News.
- [120] Kim Zetter (17 February 2011). “Cyberwar Issues Likely to Be Addressed Only After a Catastrophe” . Wired. Retrieved 18 February 2011.
- [121] Chris Carroll (18 October 2011). “Cone of silence surrounds U.S. cyberwarfare” . Stars and Stripes. Retrieved 30 October 2011.
- [122] John Bumgarner (27 April 2010). “Computers as Weapons of War” (PDF). IO Journal. Retrieved 30 October 2011.
- [123] Greenwald, Glenn. “NSA collecting phone records of millions of Verizon customers daily” . *The Guardian*. Retrieved August 16, 2013. Exclusive: Top secret court order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama
- [124] Seipel, Hubert. “Transcript: ARD interview with Edward Snowden” . *La Foundation Courage*. Retrieved 11 June 2014.
- [125] Newman, Lily Hay (9 October 2013). “Can You Trust NIST?”. *IEEE Spectrum*.
- [126] “New Snowden Leak: NSA Tapped Google, Yahoo Data Centers” , Oct 31, 2013, Lorenzo Franceschi-Bicchieri, mashable.com
- [127] Michael Riley; Ben Elgin; Dune Lawrence; Carol Matlack. “Target Missed Warnings in Epic Hack of Credit Card Data – Businessweek” . *Businessweek.com*.
- [128] “Home Depot says 53 million emails stolen” . *CNET*. CBS Interactive. 6 November 2014.
- [129] “Millions more Americans hit by government personnel data hack” . *Reuters*. 2017-07-09. Retrieved 2017-02-25.
- [130] Barrett, Devlin. “U.S. Suspects Hackers in China Breached About four (4) Million People's Records, Officials Say” . *The Wall Street Journal*.
- [131] Risen, Tom (5 June 2015). “China Suspected in Theft of Federal Employee Records” . *US News & World Report*. Archived from the original on 2015-06-06.
- [132] Zengerle, Patricia (2015-07-19). “Estimate of Americans hit by government personnel data hack skyrockets” . *Reuters*.
- [133] Sanger, David (5 June 2015). “Hacking Linked to China Exposes Millions of U.S. Workers” . *New York Times*.
- [134] Mansfield-Devine, Steve (2015-09-01). “The Ashley Madison affair” . *Network Security*. 2015 (9): 8–16. doi:10.1016/S1353-4858(15)30080-5.
- [135] “Mikko Hypponen: Fighting viruses, defending the net” . TED.
- [136] “Mikko Hypponen – Behind Enemy Lines” . Hack In The Box Security Conference.
- [137] “Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information” . Government Accountability Office. Retrieved November 3, 2015.
- [138] Kirby, Carrie (June 24, 2011). “Former White House aide backs some Net regulation / Clarke says government, industry deserve 'F' in cyber security” . *The San Francisco Chronicle*.
- [139] “FIRST website” .
- [140] “First members” .
- [141] “European council” .
- [142] “MAAWG” .
- [143] “MAAWG” .
- [144] “Government of Canada Launches Canada's Cyber Security Strategy” . *Market Wired*. 3 October 2010. Retrieved 1 November 2014.

- [145] “Canada's Cyber Security Strategy” . *Public Safety Canada*. Government of Canada. Retrieved 1 November 2014.
- [146] “Action Plan 2010–2015 for Canada's Cyber Security Strategy” . *Public Safety Canada*. Government of Canada. Retrieved 3 November 2014.
- [147] “Cyber Incident Management Framework For Canada” . *Public Safety Canada*. Government of Canada. Retrieved 3 November 2014.
- [148] “Action Plan 2010–2015 for Canada's Cyber Security Strategy” . *Public Safety Canada*. Government of Canada. Retrieved 1 November 2014.
- [149] “Canadian Cyber Incident Response Centre” . *Public Safety Canada*. Retrieved 1 November 2014.
- [150] “Cyber Security Bulletins” . *Public Safety Canada*. Retrieved 1 November 2014.
- [151] “Report a Cyber Security Incident” . *Public Safety Canada*. Government of Canada. Retrieved 3 November 2014.
- [152] “Government of Canada Launches Cyber Security Awareness Month With New Public Awareness Partnership” . *Market Wired*. Government of Canada. 27 September 2012. Retrieved 3 November 2014.
- [153] “Cyber Security Cooperation Program” . *Public Safety Canada*. Retrieved 1 November 2014.
- [154] “Cyber Security Cooperation Program” . *Public Safety Canada*.
- [155] “GetCyberSafe” . *Get Cyber Safe*. Government of Canada. Retrieved 3 November 2014.
- [156] “6.16 Internet security: National IT independence and China’s cyber policy,” in: Sebastian Heilmann, editor, *China’s Political System*, Lanham, Boulder, New York, London: Rowman & Littlefield Publishers (2017) ISBN 978-1442277342
- [157] “Cyber Security” . *Tier3 — Cyber Security Services Pakistan*.
- [158] “National Response Centre For Cyber Crime” .
- [159] “Tier3 – Cyber Security Services Pakistan” . *Tier3 – Cyber Security Services Pakistan*.
- [160] “Surfsafe® Pakistan” . *Surfsafe® Pakistan-report terrorist and extremist online-content*.
- [161] “South Korea seeks global support in cyber attack probe” . *BBC Monitoring Asia Pacific*. 7 March 2011.
- [162] Kwanwoo Jun (23 September 2013). “Seoul Puts a Price on Cyberdefense” . *Wall Street Journal*. Dow Jones & Company, Inc. Retrieved 24 September 2013.
- [163] “Text of H.R.4962 as Introduced in House: International Cybercrime Reporting and Cooperation Act – U.S. Congress” . OpenCongress. Retrieved 2013-09-25.
- [164] Archived 20 January 2012 at the Wayback Machine.
- [165] “National Cyber Security Division” . U.S. Department of Homeland Security. Archived from the original on 11 June 2008. Retrieved June 14, 2008.
- [166] “FAQ: Cyber Security R&D Center” . U.S. Department of Homeland Security S&T Directorate. Retrieved June 14, 2008.
- [167] AFP-JiJi, “U.S. boots up cybersecurity center” , October 31, 2009.
- [168] “Federal Bureau of Investigation – Priorities” . Federal Bureau of Investigation.
- [169] “Internet Crime Complaint Center (IC3) – Home” .
- [170] “Infragard, Official Site” . *Infragard*. Retrieved 10 September 2010.
- [171] “Robert S. Mueller, III – InfraGard Interview at the 2005 InfraGard Conference” . *Infragard (Official Site) – “Media Room”* . Archived from the original on 17 June 2011. Retrieved 9 December 2009.
- [172] “CCIPS” .
- [173] “U.S. Department of Defense, Cyber Command Fact Sheet” . *stratcom.mil*. May 21, 2010. Archived from the original on 3 July 2017.
- [174] “Speech:”. Defense.gov. Retrieved 2010-07-10.

- [175] Shachtman, Noah. “Military’s Cyber Commander Swears: “No Role” in Civilian Networks”, The Brookings Institution, 23 September 2010.
- [176] “FCC Cybersecurity” . FCC.
- [177] “Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication” . Retrieved 23 May 2016.
- [178] “Automotive Cybersecurity – National Highway Traffic Safety Administration (NHTSA)”. Retrieved 23 May 2016.
- [179] “U.S. GAO – Air Traffic Control: FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen” . Retrieved 23 May 2016.
- [180] Aliya Sternstein (4 March 2016). “FAA Working on New Guidelines for Hack-Proof Planes” . *Nextgov*. Retrieved 23 May 2016.
- [181] Bart Elias (18 June 2015). “Protecting Civil Aviation from Cyberattacks” (PDF). Retrieved 4 November 2016.
- [182] Verton, Dan (January 28, 2004). “DHS launches national cyber alert system” . *Computerworld*. IDG. Retrieved 2008-06-15.
- [183] Clayton, Mark. “The new cyber arms race” . *The Christian Science Monitor*. Retrieved 16 April 2015.
- [184] Nakashima, Ellen (September 13, 2016). “Obama to be urged to split cyberwar command from NSA” . *The Washington Post*. Archived from the original on September 14, 2016.
- [185] “Burning Glass Technologies, “Cybersecurity Jobs, 2015””. July 2015. Retrieved 11 June 2016.
- [186] Olsik, Jon. “Cybersecurity Skills Shortage Impact on Cloud Computing” . *Network World*. Retrieved 2016-03-23.
- [187] Burning Glass Technologies, “Demand for Cybersecurity Workers Outstripping Supply,” July 30, 2015, accessed 2016-06-11
- [188] de Silva, Richard (11 Oct 2011). “Government vs. Commerce: The Cyber Security Industry and You (Part One)”. Defence IQ. Retrieved 24 Apr 2014.
- [189] <http://iase.disa.mil/iawip/Pages/iabaseline.aspx>
- [190] “Department of Computer Science” . Retrieved April 30, 2013.
- [191] “(Information for) Students” . NICCS (US National Initiative for Cybercareers and Studies). Retrieved 24 April 2014.
- [192] “Current Job Opportunities at DHS” . U.S. Department of Homeland Security. Retrieved 2013-05-05.
- [193] “Cybersecurity Training & Exercises” . U.S. Department of Homeland Security. Retrieved 2015-01-09.
- [194] “Cyber Security Awareness Free Training and Webcasts” . MS-ISAC (Multi-State Information Sharing & Analysis Center). Retrieved 9 January 2015.
- [195] “Security Training Courses” . LearnQuest. Retrieved 2015-01-09.
- [196] “Confidentiality” . Retrieved 2011-10-31.
- [197] “Data Integrity” . Retrieved 2011-10-31.
- [198] “Endpoint Security” . Retrieved 2014-03-15.

Anderson, D., Reimers, K. and Barreto, C. (March 2014). Post-Secondary Education Network Security: Results of Addressing the End-User Challenge. publication date Mar 11, 2014 publication description INTED2014 (International Technology, Education, and Development Conference)

4.18 Further reading

- Wu, Chwan-Hwa (John); Irwin, J. David (2013). *Introduction to Computer Networks and Cybersecurity*. Boca Raton: CRC Press. ISBN 978-1466572133.
- Lee, Newton (2015). *Counterterrorism and Cybersecurity: Total Information Awareness* (2nd ed.). Springer. ISBN 978-3-319-17243-9.
- Singer, P. W.; Friedman, Allan (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press. ISBN 978-0199918119.
- Kim, Peter (2014). *The Hacker Playbook: Practical Guide To Penetration Testing*. Seattle: CreateSpace Independent Publishing Platform. ISBN 978-1494932633.

4.19 External links

Media related to Computer security at Wikimedia Commons

- Computer security at DMOZ
- Computer Security Resource

Chapter 5

Mobile security

This article is about security threats to mobile devices. For using mobile devices for secure system access, see Computer security § Hardware protection mechanisms.

Mobile security or **mobile phone security** has become increasingly important in mobile computing. Of particular concern is the security of personal and business information now stored on smartphones.

More and more users and businesses use smartphones to communicate, but also to plan and organize their users' work and also private life. Within companies, these technologies are causing profound changes in the organization of information systems and therefore they have become the source of new risks. Indeed, smartphones collect and compile an increasing amount of sensitive information to which access must be controlled to protect the privacy of the user and the intellectual property of the company.

All smartphones, as computers, are preferred targets of attacks. These attacks exploit weaknesses inherent in smartphones that can come from the communication mode—like Short Message Service (SMS, aka text messaging), Multimedia Messaging Service (MMS), wifi, Bluetooth and GSM, the *de facto* global standard for mobile communications. There are also exploits that target software vulnerabilities in the browser or operating system. And some malicious software relies on the weak knowledge of an average user. According to a finding by McAfee in 2008, 11.6% users had heard of someone else being affected by mobile malware, but only 2.1% had personal experience on such problem.*[1] However, this number is expected to grow.

Security countermeasures are being developed and applied to smartphones, from security in different layers of software to the dissemination of information to end users. There are good practices to be observed at all levels, from design to use, through the development of operating systems, software layers, and downloadable apps.

5.1 Challenges of mobile security

5.1.1 Threats

A smartphone user is exposed to various threats when they use their phone. In just the last two-quarters of 2012, the number of unique mobile threats grew by 261%, according to ABI Research.*[2] These threats can disrupt the operation of the smartphone, and transmit or modify user data. So applications must guarantee privacy and integrity of the information they handle. In addition, since some apps could themselves be malware, their functionality and activities should be limited (for example, restricting the apps from accessing location information via GPS, blocking access to the user's address book, preventing the transmission of data on the network, sending SMS messages that are billed to the user, etc.).

There are three prime targets for attackers:*[3]

- Data: smartphones are devices for data management, and may contain sensitive data like credit card numbers, authentication information, private information, activity logs (calendar, call logs);
- Identity: smartphones are highly customizable, so the device or its contents can easily be associated with a specific person. For example, every mobile device can transmit information related to the owner of the mobile

phone contract, and an attacker may want to steal the identity of the owner of a smartphone to commit other offenses;

- Availability: attacking a smartphone can limit access to it and deprive the owner of its use.

The source of these attacks are the same actors found in the non-mobile computing space:^{*[3]}

- Professionals, whether commercial or military, who focus on the three targets mentioned above. They steal sensitive data from the general public, as well as undertake industrial espionage. They will also use the identity of those attacked to achieve other attacks;
- Thieves who want to gain income through data or identities they have stolen. The thieves will attack many people to increase their potential income;
- Black hat hackers who specifically attack availability.^{*[4]} Their goal is to develop viruses, and cause damage to the device.^{*[5]} In some cases, hackers have an interest in stealing data on devices.
- Grey hat hackers who reveal vulnerabilities.^{*[6]} Their goal is to expose vulnerabilities of the device.^{*[7]} Grey hat hackers do not intend on damaging the device or stealing data.^{*[8]}

5.1.2 Consequences

When a smartphone is infected by an attacker, the attacker can attempt several things:

- The attacker can manipulate the smartphone as a zombie machine, that is to say, a machine with which the attacker can communicate and send commands which will be used to send unsolicited messages (spam) via sms or email;^{*[9]}
- The attacker can easily force the smartphone to make phone calls. For example, one can use the API (library that contains the basic functions not present in the smartphone) PhoneMakeCall by Microsoft, which collects telephone numbers from any source such as yellow pages, and then call them.^{*[9]} But the attacker can also use this method to call paid services, resulting in a charge to the owner of the smartphone. It is also very dangerous because the smartphone could call emergency services and thus disrupt those services;^{*[9]}
- A compromised smartphone can record conversations between the user and others and send them to a third party.^{*[9]} This can cause user privacy and industrial security problems;
- An attacker can also steal a user's identity, usurp their identity (with a copy of the user's sim card or even the telephone itself), and thus impersonate the owner. This raises security concerns in countries where smartphones can be used to place orders, view bank accounts or are used as an identity card;^{*[9]}
- The attacker can reduce the utility of the smartphone, by discharging the battery.^{*[10]} For example, they can launch an application that will run continuously on the smartphone processor, requiring a lot of energy and draining the battery. One factor that distinguishes mobile computing from traditional desktop PCs is their limited performance. Frank Stajano and Ross Anderson first described this form of attack, calling it an attack of "battery exhaustion" or "sleep deprivation torture";^{*[11]}
- The attacker can prevent the operation and/or be starting of the smartphone by making it unusable.^{*[12]} This attack can either delete the boot scripts, resulting in a phone without a functioning OS, or modify certain files to make it unusable (e.g. a script that launches at startup that forces the smartphone to restart) or even embed a startup application that would empty the battery;^{*[11]}
- The attacker can remove the personal (photos, music, videos, etc.) or professional data (contacts, calendars, notes) of the user.^{*[12]}

5.2 Attacks based on communication

5.2.1 Attack based on SMS and MMS

Some attacks derive from flaws in the management of **SMS** and **MMS**.

Some mobile phone models have problems in managing binary SMS messages. It is possible, by sending an ill-formed block, to cause the phone to restart, leading to the denial of service attacks. If a user with a **Siemens S55** received a text message containing a Chinese character, it would lead to a denial of service.* [13] In another case, while the standard requires that the maximum size of a Nokia Mail address is 32 characters, some Nokia phones did not verify this standard, so if a user enters an email address over 32 characters, that leads to complete dysfunction of the e-mail handler and puts it out of commission. This attack is called “curse of silence” . A study on the safety of the SMS infrastructure revealed that SMS messages sent from the **Internet** can be used to perform a distributed denial of service (**DDoS**) attack against the mobile telecommunications infrastructure of a big city. The attack exploits the delays in the delivery of messages to overload the network.* [14]

Another potential attack could begin with a phone that sends an MMS to other phones, with an attachment. This attachment is infected with a virus. Upon receipt of the MMS, the user can choose to open the attachment. If it is opened, the phone is infected, and the virus sends an MMS with an infected attachment to all the contacts in the address book. There is a real-world example of this attack: the virus Commwarrior* [12] uses the address book and sends MMS messages including an infected file to recipients. A user installs the software, as received via MMS message. Then, the virus began to send messages to recipients taken from the address book.

5.2.2 Attacks based on communication networks

Attacks based on the GSM networks

The attacker may try to break the encryption of the mobile network. The **GSM** network encryption algorithms belong to the family of algorithms called **A5**. Due to the policy of **security through obscurity** it has not been possible to openly test the robustness of these algorithms. There were originally two variants of the algorithm: **A5/1** and **A5/2** (stream ciphers), where the former was designed to be relatively strong, and the latter was designed to be weak on purpose to allow easy cryptanalysis and eavesdropping. **ETSI** forced some countries (typically outside Europe) to use **A5/2**. Since the encryption algorithm was made public, it was proved it was possible to break the encryption: **A5/2** could be broken on the fly, and **A5/1** in about 6 hours . * [15] In July 2007, the 3GPP approved a change request to prohibit the implementation of **A5/2** in any new mobile phones, which means that it has been decommissioned and is no longer implemented in mobile phones. Stronger public algorithms have been added to the **GSM** standard, the **A5/3** and **A5/4** (block ciphers), otherwise known as **KASUMI** or **UEA1*** [16] published by the **ETSI**. If the network does not support **A5/1**, or any other **A5** algorithm implemented by the phone, then the base station can specify **A5/0** which is the null-algorithm, whereby the radio traffic is sent unencrypted. Even in case mobile phones are able to use **3G** or **4G** which have much stronger encryption than **2G GSM**, the base station can downgrade the radio communication to **2G GSM** and specify **A5/0** (no encryption) . * [17] This is the basis for eavesdropping attacks on mobile radio networks using a fake base station commonly called an **IMSI catcher**.

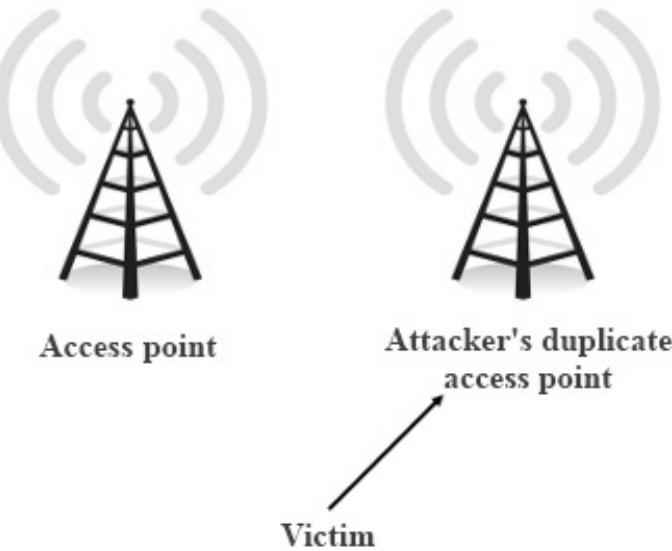
In addition, tracing of mobile terminals is difficult since each time the mobile terminal is accessing or being accessed by the network, a new temporary identity (TMSI) is allocated to the mobile terminal. The TMSI is used as the identity of the mobile terminal the next time it accesses the network. The TMSI is sent to the mobile terminal in encrypted messages.

Once the encryption algorithm of **GSM** is broken, the attacker can intercept all unencrypted communications made by the victim's smartphone.

Attacks based on Wi-Fi

See also: **Wi-Fi § Network_security**

An attacker can try to eavesdrop on **Wi-Fi** communications to derive information (e.g. username, password). This type of attack is not unique to smartphones, but they are very vulnerable to these attacks because very often the **Wi-Fi** is the only means of communication they have to access the internet. The security of wireless networks (WLAN) is thus an important subject. Initially, wireless networks were secured by **WEP** keys. The weakness of WEP is a short encryption key which is the same for all connected clients. In addition, several reductions in the search space of the keys have been found by researchers. Now, most wireless networks are protected by the **WPA** security protocol. WPA is based on the "Temporal Key Integrity Protocol (TKIP)" which was designed to allow migration from WEP to



Access Point spoofing

WPA on the equipment already deployed. The major improvements in security are the dynamic encryption keys. For small networks, the WPA is a "pre-shared key" which is based on a shared key. Encryption can be vulnerable if the length of the shared key is short. With limited opportunities for input (i.e. only the numeric keypad), mobile phone users might define short encryption keys that contain only numbers. This increases the likelihood that an attacker succeeds with a brute-force attack. The successor to WPA, called **WPA2**, is supposed to be safe enough to withstand a brute force attack.

As with GSM, if the attacker succeeds in breaking the identification key, it will be possible to attack not only the phone but also the entire network it is connected to.

Many smartphones for wireless LANs remember they are already connected, and this mechanism prevents the user from having to re-identify with each connection. However, an attacker could create a WIFI access point twin with the same parameters and characteristics as the real network. Using the fact that some smartphones remember the networks, they could confuse the two networks and connect to the network of the attacker who can intercept data if it does not transmit its data in encrypted form.*[18]*[19]*[20]

Lasco is a worm that initially infects a remote device using the **SIS** file format.*[21] SIS file format (Software Installation Script) is a script file that can be executed by the system without user interaction. The smartphone thus believes the file to come from a trusted source and downloads it, infecting the machine.*[21]

Principle of Bluetooth-based attacks

Main article: Bluetooth § Security

See also: Bluesnarfing and Bluebugging

Security issues related to **Bluetooth** on mobile devices have been studied and have shown numerous problems on different phones. One easy to exploit **vulnerability**: unregistered services do not require authentication, and vulnerable applications have a virtual serial port used to control the phone. An attacker only needed to connect to the port to take full control of the device.*[22] Another example: a phone must be within reach and Bluetooth in discovery mode. The attacker sends a file via Bluetooth. If the recipient accepts, a virus is transmitted. For example: **Cabir** is a worm

that spreads via Bluetooth connection.* [12] The worm searches for nearby phones with Bluetooth in discoverable mode and sends itself to the target device. The user must accept the incoming file and install the program. After installing, the worm infects the machine.

5.3 Attacks based on vulnerabilities in software applications

Other attacks are based on flaws in the OS or applications on the phone.

5.3.1 Web browser

See also: [Browser security](#)

The mobile web browser is an emerging attack vector for mobile devices. Just as common Web browsers, [mobile web](#) browsers are extended from pure web navigation with widgets and plug-ins, or are completely native mobile browsers.

Jailbreaking the [iPhone](#) with firmware 1.1.1 was based entirely on vulnerabilities on the web browser.* [23] As a result, the exploitation of the vulnerability described here underlines the importance of the Web browser as an attack vector for mobile devices. In this case, there was a vulnerability based on a stack-based buffer overflow in a library used by the web browser ([Libtiff](#)).

A vulnerability in the web browser for [Android](#) was discovered in October 2008. As the iPhone vulnerability above, it was due to an obsolete and vulnerable [library](#). A significant difference with the iPhone vulnerability was Android's [sandboxing](#) architecture which limited the effects of this vulnerability to the Web browser process.

Smartphones are also victims of classic piracy related to the web: [phishing](#), malicious websites, etc. The big difference is that smartphones do not yet have strong antivirus software available.

5.3.2 Operating system

See also: [Operating_system § Security](#)

Sometimes it is possible to overcome the security safeguards by modifying the operating system itself. As real-world examples, this section covers the manipulation of [firmware](#) and malicious signature certificates. These attacks are difficult.

In 2004, vulnerabilities in virtual machines running on certain devices were revealed. It was possible to bypass the bytecode verifier and access the native underlying operating system. The results of this research were not published in detail. The firmware security of Nokia's [Symbian](#) Platform Security Architecture (PSA) is based on a central configuration file called SWIPolicy. In 2008 it was possible to manipulate the Nokia firmware before it is installed, and in fact in some downloadable versions of it, this file was human readable, so it was possible to modify and change the image of the firmware.* [24] This vulnerability has been solved by an update from Nokia.

In theory smartphones have an advantage over hard drives since the [OS](#) files are in [ROM](#), and cannot be changed by [malware](#). However, in some systems it was possible to circumvent this: in the Symbian OS it was possible to overwrite a file with a file of the same name.* [24] On the Windows OS, it was possible to change a pointer from a general configuration file to an editable file.

When an application is installed, the [signing](#) of this application is verified by a series of [certificates](#). One can create a valid [signature](#) without using a valid certificate and add it to the list.* [25] In the Symbian OS all certificates are in the directory: c:\resource\swicertstore\dat. With firmware changes explained above it is very easy to insert a seemingly valid but malicious certificate.

5.4 Attacks based on hardware vulnerabilities

5.4.1 Electromagnetic Waveforms

In 2015, researchers at the French government agency Agence nationale de la sécurité des systèmes d'information (ANSSI) demonstrated the capability to trigger the voice interface of certain smartphones remotely by using “specific electromagnetic waveforms”.^{*[26]} The exploit took advantage of antenna-properties of headphone wires while plugged into the audio-output jacks of the vulnerable smartphones and effectively spoofed audio input to inject commands via the audio interface.^{*[26]}

5.4.2 Juice Jacking

See also: [Juice_jacking](#)

Juice Jacking is a physical or hardware vulnerability specific to mobile platforms. Utilizing the dual purpose of the USB charge port, many devices have been susceptible to having data exfiltrated from, or malware installed onto a mobile device by utilizing malicious charging kiosks set up in public places or hidden in normal charge adapters.

5.5 Password cracking

In 2010, researcher from the University of Pennsylvania investigated the possibility of cracking a device's password through a [smudge attack](#) (literally imaging the finger smudges on the screen to discern the user's password).^{*[27]} The researchers were able to discern the device password up to 68% of the time under certain conditions.^{*[27]} Outsiders may perform over-the-shoulder on victims, such as watching specific keystrokes or pattern gestures, to unlock device password or passcode.

5.6 Malicious software (malware)

See also: [Malware](#)

As smartphones are a permanent point of access to the internet (mostly on), they can be compromised as easily as computers with malware. A [malware](#) is a computer program that aims to harm the system in which it resides. [Trojans](#), [worms](#) and [viruses](#) are all considered malware. A Trojan is a program that is on the smartphone and allows external users to connect discreetly. A worm is a program that reproduces on multiple computers across a network. A virus is malicious software designed to spread to other computers by inserting itself into legitimate programs and running programs in parallel. However, it must be said that the malware are far less numerous and important to smartphones as they are to computers.

^{*[28]}

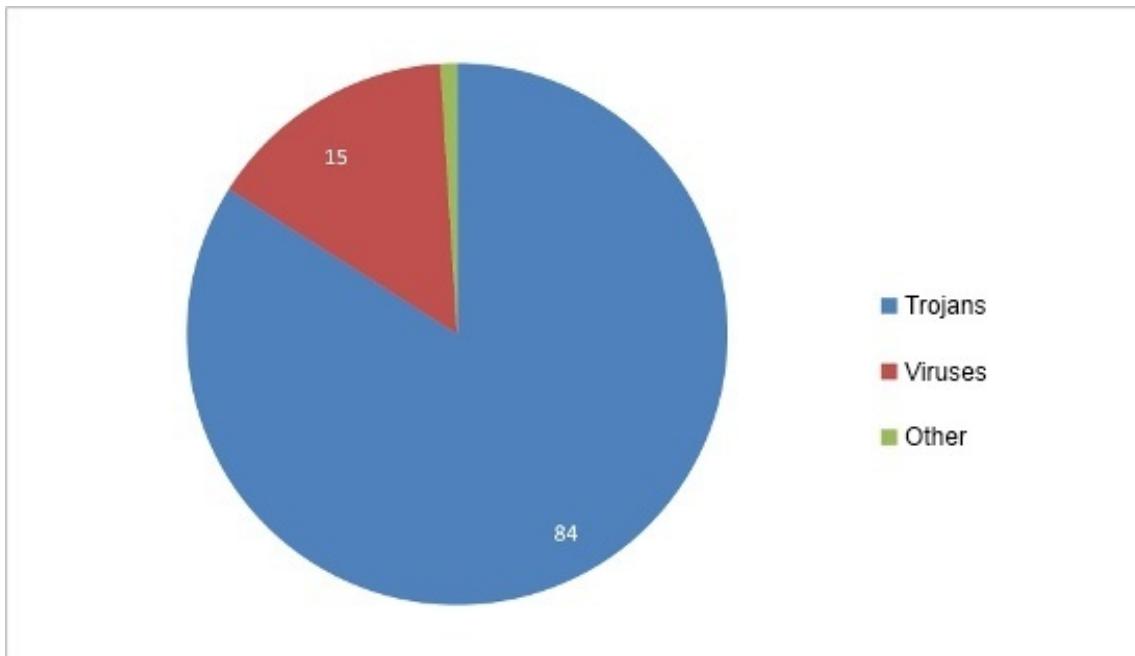
Nonetheless, recent studies show that the evolution of malware in smartphones have rocketed in the last few years posing a threat to analysis and detection.^{*[29]}

5.6.1 The three phases of malware attacks

Typically an attack on a smartphone made by malware takes place in 3 phases: the infection of a host, the accomplishment of its goal, and the spread of the malware to other systems. Malware often uses the resources offered by the infected smartphones. It will use the output devices such as Bluetooth or infrared, but it may also use the address book or email address of the person to infect the user's acquaintances. The malware exploits the trust that is given to data sent by an acquaintance.

Infection

Infection is the means used by the malware to get into the smartphone, it can either use one of the faults previously presented or may use the gullibility of the user. Infections are classified into four classes according to their degree of user interaction:^{*[30]}



Types of malware based on their number of smartphones in 2009

Explicit permission the most benign interaction is to ask the user if it is allowed to infect the machine, clearly indicating its potential malicious behavior. This is typical behavior of a proof of concept malware.

Implied permission this infection is based on the fact that the user has a habit of installing software. Most trojans try to seduce the user into installing attractive applications (games, useful applications etc.) that actually contain malware.

Common interaction this infection is related to a common behavior, such as opening an MMS or email.

No interaction the last class of infection is the most dangerous. Indeed, a worm that could infect a smartphone and could infect other smartphones without any interaction would be catastrophic.

Accomplishment of its goal

Once the malware has infected a phone it will also seek to accomplish its goal, which is usually one of the following: monetary damage, damage data and/or device, and concealed damage:^{*}[31]

Monetary damages the attacker can steal user data and either sell them to the same user or sell to a third party.

Damage malware can partially damage the device, or delete or modify data on the device.

Concealed damage the two aforementioned types of damage are detectable, but the malware can also leave a backdoor for future attacks or even conduct wiretaps.

Spread to other systems

Once the malware has infected a smartphone, it always aims to spread one way or another:^{*}[32]

- It can spread through proximate devices using Wi-Fi, Bluetooth and infrared;
- It can also spread using remote networks such as telephone calls or SMS or emails.

5.6.2 Examples of malware

Here are various malware that exist in the world of smartphones with a short description of each.

Viruses and trojans

Main article: Mobile virus

- Cabir (also known as Caribe, SybmOS/Cabir, Symbian/Cabir and EPOC.cabir) is the name of a computer worm developed in 2004, designed to infect mobile phones running Symbian OS. It is believed to have been the first computer worm that can infect mobile phones
- Commwarrior, found March 7, 2005, was the first worm that can infect many machines from MMS.*[12] It is sent as COMMWARRIOR.ZIP containing the file COMMWARRIOR.SIS. When this file is executed, Commwarrior attempts to connect to nearby devices by Bluetooth or infrared under a random name. It then attempts to send MMS message to the contacts in the smartphone with different header messages for each person, who receive the MMS and often open them without further verification.
- Phage is the first Palm OS virus discovered.*[12] It transfers to the Palm from a PC via synchronization. It infects all applications in the smartphone and embeds its own code to function without the user and the system detecting it. All that the system will detect is that its usual applications are functioning.
- RedBrowser is a Trojan based on java.*[12] The Trojan masquerades as a program called “RedBrowser” which allows the user to visit WAP sites without a WAP connection. During application installation, the user sees a request on their phone that the application needs permission to send messages. If the user accepts, RedBrowser can send SMS to paid call centers. This program uses the smartphone's connection to social networks (Facebook, Twitter, etc.) to get the contact information for the user's acquaintances (provided the required permissions have been given) and will send them messages.
- WinCE.PmCryptic.A is malicious software on Windows Mobile which aims to earn money for its authors. It uses the infestation of memory cards that are inserted in the smartphone to spread more effectively.*[33]
- CardTrap is a virus that is available on different types of smartphone, which aims to deactivate the system and third party applications. It works by replacing the files used to start the smartphone and applications to prevent them from executing.*[34] There are different variants of this virus such as Cardtrap.A for SymbOS devices. It also infects the memory card with malware capable of infecting Windows.
- Ghost Push is malicious software on Android OS which automatically roots the android device and installs malicious applications directly to system partition then unroots the device to prevent users from removing the threat by master reset (The threat can be removed only by reflashing). It cripples the system resources, executes quickly, and is hard to detect.

Ransomware

Mobile ransomware is a type of malware that locks users out of their mobile devices in a pay-to-unlock-your-device ploy, it has grown by leaps and bounds as a threat category since 2014.*[35] Specific to mobile computing platforms, users are often less security-conscious, particularly as it pertains to scrutinizing applications and web links trusting the native protection capability of the mobile device operating system. Mobile ransomware poses a significant threat to businesses reliant on instant access and availability of their proprietary information and contacts. The likelihood of a traveling businessman paying a ransom to unlock their device is significantly higher since they are at a disadvantage given inconveniences such as timeliness and less likely direct access to IT staff.

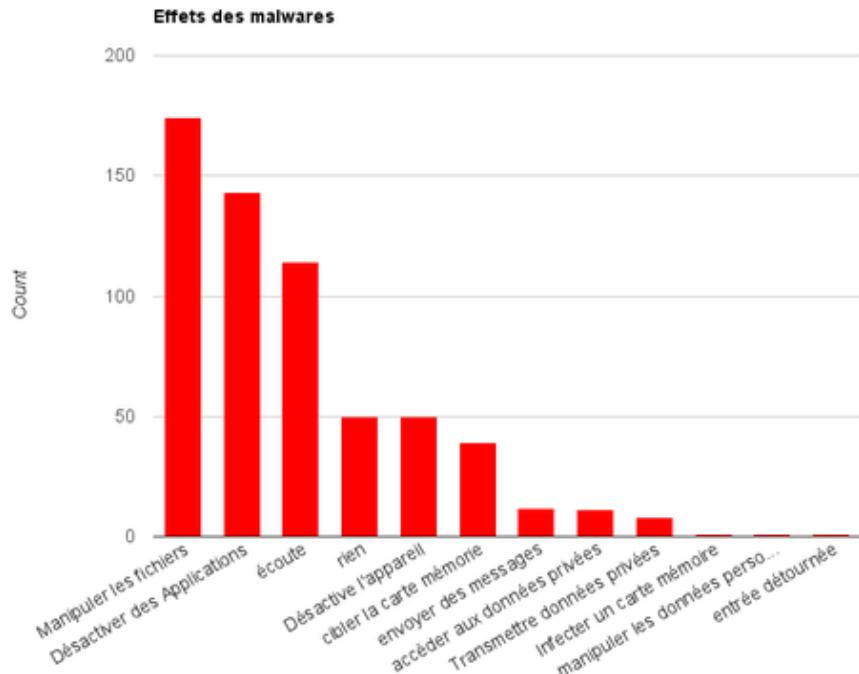
Spyware

Main article: Spyware

- Flexispy is an application that can be considered as a trojan, based on Symbian. The program sends all information received and sent from the smartphone to a Flexispy server. It was originally created to protect children and spy on adulterous spouses.*[12]

Number of malware

Below is a diagram which loads the different behaviors of smartphone malware in terms of their effects on smartphones:^{*} [28]



Effects of Malware

We can see from the graph that at least 50 malwares exhibit no negative behavior, except their ability to spread.^{*} [28]

5.6.3 Portability of malware across platforms

There is a multitude of malware. This is partly due to the variety of operating systems on smartphones. However attackers can also choose to make their malware target multiple platforms, and malware can be found which attacks an OS but is able to spread to different systems.

To begin with, malware can use runtime environments like Java virtual machine or the .NET Framework. They can also use other libraries present in many operating systems.^{*} [36] Other malware carry several executable files in order to run in multiple environments and they utilize these during the propagation process. In practice, this type of malware requires a connection between the two operating systems to use as an attack vector. Memory cards can be used for this purpose, or synchronization software can be used to propagate the virus.

5.7 Countermeasures

The security mechanisms in place to counter the threats described above are presented in this section. They are divided into different categories, as all do not act at the same level, and they range from the management of security by the operating system to the behavioral education of the user. The threats prevented by the various measures are not the same depending on the case. Considering the two cases mentioned above, in the first case one would protect the system from corruption by an application, and in the second case the installation of a suspicious software would be prevented.

5.7.1 Security in operating systems

The first layer of security in a smartphone is the **operating system (OS)**. Beyond needing to handle the usual roles of an operating system (e.g. resource management, scheduling processes) on the device, it must also establish the protocols for introducing external applications and data without introducing risk.

A central paradigm in mobile operating systems is the idea of a **sandbox**. Since smartphones are currently designed to accommodate many applications, they must have mechanisms to ensure these applications are safe for the phone itself, for other applications and data on the system, and for the user. If a malicious program reaches a mobile device, the vulnerable area presented by the system must be as small as possible. Sandboxing extends this idea to compartmentalize different processes, preventing them from interacting and damaging each other. Based on the history of operating systems, sandboxing has different implementations. For example, where **iOS** will focus on limiting access to its public API for applications from the **App Store** by default, **Managed Open In** allows you to restrict which apps can access which types of data. **Android** bases its sandboxing on its legacy of **Linux** and **TrustedBSD**.

The following points highlight mechanisms implemented in operating systems, especially **Android**.

Rootkit Detectors The intrusion of a **rootkit** in the system is a great danger in the same way as on a computer. It is important to prevent such intrusions, and to be able to detect them as often as possible. Indeed, there is concern that with this type of malicious program, the result could be a partial or complete bypass of the device security, and the acquisition of administrator rights by the attacker. If this happens, then nothing prevents the attacker from studying or disabling the safety features that were circumvented, deploying the applications they want, or disseminating a method of intrusion by a rootkit to a wider audience.*[37]*[38] We can cite, as a defense mechanism, the **Chain of trust** in **iOS**. This mechanism relies on the signature of the different applications required to start the operating system, and a certificate signed by Apple. In the event that the signature checks are inconclusive, the device detects this and stops the boot-up.*[39] If the Operating System is compromised due to **Jailbreaking**, root kit detection may not work if it is disabled by the **Jailbreak** method or software is loaded after **Jailbreak** disables Rootkit Detection.

Process isolation **Android** uses mechanisms of user process isolation inherited from **Linux**. Each application has a user associated with it, and a tuple (**UID**, **GID**). This approach serves as a **sandbox**: while applications can be malicious, they can not get out of the sandbox reserved for them by their identifiers, and thus cannot interfere with the proper functioning of the system. For example, since it is impossible for a process to end the process of another user, an application can thus not stop the execution of another.*[37]*[40]*[41]*[42]*[43]

File permissions From the legacy of **Linux**, there are also **filesystem permissions** mechanisms. They help with sandboxing: a process can not edit any files it wants. It is therefore not possible to freely corrupt files necessary for the operation of another application or system. Furthermore, in **Android** there is the method of locking memory permissions. It is not possible to change the permissions of files installed on the SD card from the phone, and consequently it is impossible to install applications.*[44]*[45]*[46]

Memory Protection In the same way as on a computer, **memory protection** prevents privilege escalation. Indeed, if a process managed to reach the area allocated to other processes, it could write in the memory of a process with rights superior to their own, with **root** in the worst case, and perform actions which are beyond its permissions on the system. It would suffice to insert function calls are authorized by the privileges of the malicious application.*[43]

Development through runtime environments Software is often developed in high-level languages, which can control what is being done by a running program. For example, **Java Virtual Machines** continuously monitor the actions of the execution threads they manage, monitor and assign resources, and prevent malicious actions. Buffer overflows can be prevented by these controls.*[47]*[48]*[43]

5.7.2 Security software

Above the operating system security, there is a layer of security software. This layer is composed of individual components to strengthen various vulnerabilities: prevent malware, intrusions, the identification of a user as a human, and user authentication. It contains software components that have learned from their experience with computer security; however, on smartphones, this software must deal with greater constraints (see limitations).

Antivirus and firewall An antivirus software can be deployed on a device to verify that it is not infected by a known threat, usually by signature detection software that detects malicious executable files. A **firewall**, meanwhile, can watch over the existing traffic on the network and ensure that a malicious application does not seek to communicate through it. It may equally verify that an installed application does not seek to establish suspicious communication, which may prevent an intrusion attempt.*[49]*[50]*[51]*[38]

Visual Notifications In order to make the user aware of any abnormal actions, such as a call they did not initiate, one can link some functions to a visual notification that is impossible to circumvent. For example, when a call is triggered, the called number should always be displayed. Thus, if a call is triggered by a malicious application, the user can see, and take appropriate action.

Turing test In the same vein as above, it is important to confirm certain actions by a user decision. The **Turing test** is used to distinguish between a human and a virtual user, and it often comes as a **captcha**.

Biometric identification Another method to use is **biometrics**.* [52] Biometrics is a technique of identifying a person by means of their **morphology**(by recognition of the eye or face, for example) or their behavior (their signature or way of writing for example). One advantage of using biometric security is that users can avoid having to remember a password or other secret combination to authenticate and prevent malicious users from accessing their device. In a system with strong biometric security, only the primary user can access the smartphone.

5.7.3 Resource monitoring in the smartphone

When an application passes the various security barriers, it can take the actions for which it was designed. When such actions are triggered, the activity of a malicious application can be sometimes detected if one monitors the various resources used on the phone. Depending on the goals of the malware, the consequences of infection are not always the same; all malicious applications are not intended to harm the devices on which they are deployed. The following sections describe different ways to detect suspicious activity.*[53]

Battery Some malware is aimed at exhausting the energy resources of the phone. Monitoring the energy consumption of the phone can be a way to detect certain malware applications.*[37]

Memory usage Memory usage is inherent in any application. However, if one finds that a substantial proportion of memory is used by an application, it may be flagged as suspicious.

Network traffic On a smartphone, many applications are bound to connect via the network, as part of their normal operation. However, an application using a lot of bandwidth can be strongly suspected of attempting to communicate a lot of information, and disseminate data to many other devices. This observation only allows a suspicion, because some legitimate applications can be very resource-intensive in terms of network communications, the best example being **streaming video**.

Services One can monitor the activity of various services of a smartphone. During certain moments, some services should not be active, and if one is detected, the application should be suspected. For example, the sending of an SMS when the user is filming video: this communication does not make sense and is suspicious; malware may attempt to send SMS while its activity is masked.*[54]

The various points mentioned above are only indications and do not provide certainty about the legitimacy of the activity of an application. However, these criteria can help target suspicious applications, especially if several criteria are combined.

5.7.4 Network surveillance

Network traffic exchanged by phones can be monitored. One can place safeguards in network routing points in order to detect abnormal behavior. As the mobile's use of network protocols is much more constrained than that of a computer, expected network data streams can be predicted (e.g. the protocol for sending an SMS), which permits detection of anomalies in mobile networks.

Spam filters As is the case with email exchanges, we can detect a spam campaign through means of mobile communications (SMS, MMS). It is therefore possible to detect and minimize this kind of attempt by filters deployed on network infrastructure that is relaying these messages.

Encryption of stored or transmitted information Because it is always possible that data exchanged can be intercepted, communications, or even information storage, can rely on **encryption** to prevent a malicious entity from using any data obtained during communications. However, this poses the problem of key exchange for encryption algorithms, which requires a secure channel.

Telecom network monitoring The networks for SMS and MMS exhibit predictable behavior, and there is not as much liberty compared with what one can do with protocols such as TCP or UDP. This implies that one cannot predict the use made of the common protocols of the web; one might generate very little traffic by consulting simple pages, rarely, or generate heavy traffic by using video streaming. On the other hand, messages exchanged via mobile phone have a framework and a specific model, and the user does not, in a normal case, have the freedom to intervene in the details of these communications. Therefore, if an abnormality is found in the flux of network data in the mobile networks, the potential threat can be quickly detected.

5.7.5 Manufacturer surveillance

In the production and distribution chain for mobile devices, it is the responsibility of manufacturers to ensure that devices are delivered in a basic configuration without vulnerabilities. Most users are not experts and many of them are not aware of the existence of security vulnerabilities, so the device configuration as provided by manufacturers will be retained by many users. Below are listed several points which manufacturers should consider.

Remove debug mode Phones are sometimes set in a debug mode during manufacturing, but this mode must be disabled before the phone is sold. This mode allows access to different features, not intended for routine use by a user. Due to the speed of development and production, distractions occur and some devices are sold in debug mode. This kind of deployment exposes mobile devices to exploits that utilize this oversight.*[55]*[56]

Default settings When a smartphone is sold, its default settings must be correct, and not leave security gaps. The default configuration is not always changed, so a good initial setup is essential for users. There are, for example, default configurations that are vulnerable to denial of service attacks.*[37]*[57]

Security audit of apps Along with smart phones, appstores have emerged. A user finds themselves facing a huge range of applications. This is especially true for providers who manage appstores because they are tasked with examining the apps provided, from different points of view (e.g. security, content). The security audit should be particularly cautious, because if a fault is not detected, the application can spread very quickly within a few days, and infect a significant number of devices.*[37]

Detect suspicious applications demanding rights When installing applications, it is good to warn the user against sets of permissions that, grouped together, seem potentially dangerous, or at least suspicious. Frameworks like such as Kirin, on Android, attempt to detect and prohibit certain sets of permissions.*[58]

Revocation procedures Along with appstores appeared a new feature for mobile apps: remote revocation. First developed by Android, this procedure can remotely and globally uninstall an application, on any device that has it. This means the spread of a malicious application that managed to evade security checks can be immediately stopped when the threat is discovered.*[59]*[60]

Avoid heavily customized systems Manufacturers are tempted to overlay custom layers on existing operating systems, with the dual purpose of offering customized options and disabling or charging for certain features. This has the dual effect of risking the introduction of new bugs in the system, coupled with an incentive for users to modify the systems to circumvent the manufacturer's restrictions. These systems are rarely as stable and reliable as the original, and may suffer from phishing attempts or other exploits.

Improve software patch processes New versions of various software components of a smartphone, including operating systems, are regularly published. They correct many flaws over time. Nevertheless, manufacturers often do not deploy these updates to their devices in a timely fashion, and sometimes not at all. Thus, vulnerabilities persist when they could be corrected, and if they are not, since they are known, they are easily exploitable.*[58]

5.7.6 User awareness

Much malicious behavior is allowed by the carelessness of the user. From simply not leaving the device without a password, to precise control of permissions granted to applications added to the smartphone, the user has a large responsibility in the cycle of security: to not be the vector of intrusion. This precaution is especially important if the user is an employee of a company that stores business data on the device. Detailed below are some precautions that a user can take to manage security on a smartphone.

A recent survey by internet security experts BullGuard showed a lack of insight into the rising number of malicious threats affecting mobile phones, with 53% of users claiming that they are unaware of security software for Smartphones. A further 21% argued that such protection was unnecessary, and 42% admitted it hadn't crossed their mind ("Using APA," 2011). These statistics show consumers are not concerned about security risks because they believe it is not a serious problem. The key here is to always remember smartphones are effectively handheld computers and are just as vulnerable.

Being skeptical A user should not believe everything that may be presented, as some information may be phishing or attempting to distribute a malicious application. It is therefore advisable to check the reputation of the application that they want to buy before actually installing it.*[61]

Permissions given to applications The mass distribution of applications is accompanied by the establishment of different permissions mechanisms for each operating system. It is necessary to clarify these permissions mechanisms to users, as they differ from one system to another, and are not always easy to understand. In addition, it is rarely possible to modify a set of permissions requested by an application if the number of permissions is too great. But this last point is a source of risk because a user can grant rights to an application, far beyond the rights it needs. For example, a note taking application does not require access to the geolocation service. The user must ensure the privileges required by an application during installation and should not accept the installation if requested rights are inconsistent.*[62]*[57]*[63]

Be careful Protection of a user's phone through simple gestures and precautions, such as locking the smartphone when it is not in use, not leaving their device unattended, not trusting applications, not storing sensitive data, or encrypting sensitive data that cannot be separated from the device.*[64]*[65]

Ensure data Smartphones have a significant memory and can carry several gigabytes of data. The user must be careful about what data it carries and whether they should be protected. While it is usually not dramatic if a song is copied, a file containing bank information or business data can be more risky. The user must have the prudence to avoid the transmission of sensitive data on a smartphone, which can be easily stolen. Furthermore, when a user gets rid of a device, they must be sure to remove all personal data first.*[66]

These precautions are measures that leave no easy solution to the intrusion of people or malicious applications in a smartphone. If users are careful, many attacks can be defeated, especially phishing and applications seeking only to obtain rights on a device.

5.7.7 Centralized storage of text messages

One form of mobile protection allows companies to control the delivery and storage of text messages, by hosting the messages on a company server, rather than on the sender or receiver's phone. When certain conditions are met, such as an expiration date, the messages are deleted.*[67]

5.7.8 Limitations of certain security measures

The security mechanisms mentioned in this article are to a large extent inherited from knowledge and experience with computer security. The elements composing the two device types are similar, and there are common measures that can be used, such as antivirus software and firewalls. However, the implementation of these solutions is not necessarily possible or at least highly constrained within a mobile device. The reason for this difference is the technical resources offered by computers and mobile devices: even though the computing power of smartphones is becoming faster, they have other limitations than their computing power.

- **Single-task system:** Some operating systems, including some still commonly used, are single-tasking. Only the foreground task is executed. It is difficult to introduce applications such as antivirus and firewall on such systems, because they could not perform their monitoring while the user is operating the device, when there would be most need of such monitoring.
- **Energy autonomy:** A critical one for the use of a smartphone is energy autonomy. It is important that the security mechanisms not consume battery resources, without which the autonomy of devices will be affected dramatically, undermining the effective use of the smartphone.
- **Network** Directly related to battery life, network utilization should not be too high. It is indeed one of the most expensive resources, from the point of view of energy consumption. Nonetheless, some calculations may need to be relocated to remote servers in order to preserve the battery. This balance can make implementation of certain intensive computation mechanisms a delicate proposition.*[68]

Furthermore, it should be noted that it is common to find that updates exist, or can be developed or deployed, but this is not always done. One can, for example, find a user who does not know that there is a newer version of the operating system compatible with the smartphone, or a user may discover known vulnerabilities that are not corrected until the end of a long development cycle, which allows time to exploit the loopholes.*[56]

5.7.9 Next Generation of mobile security

There is expected to be four mobile environments that will make up the security framework:

Rich operating system In this category will fall traditional Mobile OS like Android, iOS, Symbian OS or Windows Phone. They will provide the traditional functionality and security of an OS to the applications.

Secure Operating System (Secure OS) A secure kernel which will run in parallel with a fully featured Rich OS, on the same processor core. It will include drivers for the Rich OS (“normal world”) to communicate with the secure kernel (“secure world”). The trusted infrastructure could include interfaces like the display or keypad to regions of PCI-E address space and memories.

Trusted Execution Environment (TEE) Made up of hardware and software. It helps in the control of access rights and houses sensitive applications, which need to be isolated from the Rich OS. It effectively acts as a firewall between the “normal world” and “secure world” .

Secure Element (SE) The SE consists of tamper resistant hardware and associated software. It can provide high levels of security and work in tandem with the TEE. The SE will be mandatory for hosting proximity payment applications or official electronic signatures.

5.8 See also

- Browser security
- Computer security
- Information security
- Mobile Malware
- Mobile secure gateway
- Phone hacking
- Telephone tapping
- Wireless Public Key Infrastructure (WPKI)
- Wireless security

5.9 Notes

- [1] Steven., Furnell, (2009-01-01). *Mobile security*. IT Governance Pub. ISBN 9781849280204. OCLC 704518497.
- [2] BYOD and Increased Malware Threats Help Driving Billion Dollar Mobile Security Services Market in 2013, ABI Research
- [3] Bishop 2004.
- [4] Olson, Parmy. "Your smartphone is hackers' next big target" . CNN. Retrieved August 26, 2013.
- [5] (PDF) <http://www.gov.mu/portal/sites/cert/files/Guide%20on%20Protection%20Against%20Hacking.pdf>. Missing or empty |title= (help)
- [6] Lemos, Robert. "New laws make hacking a black-and-white choice" . CNET News.com. Retrieved September 23, 2002.
- [7] McCaney, Kevin. "'Unknowns' hack NASA, Air Force, saying 'We're here to help'" . Retrieved May 7, 2012.
- [8] Bilton 2010.
- [9] Guo, Wang & Zhu 2004, p. 3.
- [10] Dagon, Martin & Starger 2004, p. 12.
- [11] Dixon & Mishra 2010, p. 3.
- [12] Töyssy & Helenius 2006, p. 113.
- [13] Siemens 2010, p. 1.
- [14] "Brookstone spy tank app" . limormoyal.com. Retrieved 2016-08-11.
- [15] Gendrullis 2008, p. 266.
- [16] European Telecommunications Standards Institute 2011, p. 1.
- [17] Jøsang, Miralabé & Dallet 2015.
- [18] Roth, Polak & Rieffel 2008, p. 220.
- [19] Gittleson, Kim (28 March 2014) Data-stealing Snoopy drone unveiled at Black Hat BBC News, Technology, Retrieved 29 March 2014
- [20] Wilkinson, Glenn (25 September 2012) Snoopy: A distributed tracking and profiling framework Sensepost, Retrieved 29 March 2014
- [21] Töyssy & Helenius 2006, p. 27.
- [22] Mulliner 2006, p. 113.
- [23] Dunham, Abu Nimeh & Becher 2008, p. 225.
- [24] Becher 2009, p. 65.
- [25] Becher 2009, p. 66.
- [26] Kasmi C, Lopes Esteves J (13 August 2015). "IEMI Threats for Information Security: Remote Command Injection on Modern Smartphones" . *IEEE Transactions on Electromagnetic Compatibility*. doi:10.1109/TEMC.2015.2463089. Lay summary – WIRED (14 October 2015). 
- [27] Aviv, Adam J.; Gibson, Katherine; Mossop, Evan; Blaze, Matt; Smith, Jonathan M. *Smudge Attacks on Smartphone Touch Screens* (PDF). 4th USENIX Workshop on Offensive Technologies.
- [28] Schmidt et al. 2009a, p. 3.
- [29] Suarez-Tangil, Guillermo; Juan E. Tapiador; Pedro Peris-Lopez; Arturo Ribagorda (2014). "Evolution, Detection and Analysis of Malware in Smart Devices" (PDF). *IEEE Communications Surveys & Tutorials*.
- [30] Becher 2009, p. 87.
- [31] Becher 2009, p. 88.
- [32] Mickens & Noble 2005, p. 1.

- [33] Raboin 2009, p. 272.
- [34] Töyssy & Helenius 2006, p. 114.
- [35] Haas, Peter D. (2015-01-01). “Ransomware goes mobile: An analysis of the threats posed by emerging methods” . UTICA COLLEGE.
- [36] Becher 2009, p. 91-94.
- [37] Becher 2009, p. 12.
- [38] Schmidt, Schmidt & Clausen 2008, p. 5-6.
- [39] Halbronn & Sigwald 2010, p. 5-6.
- [40] Ruff 2011, p. 127.
- [41] Hogben & Dekker 2010, p. 50.
- [42] Schmidt, Schmidt & Clausen 2008, p. 50.
- [43] Shabtai et al. 2009, p. 10.
- [44] Becher 2009, p. 31.
- [45] Schmidt, Schmidt & Clausen 2008, p. 3.
- [46] Shabtai et al. 2009, p. 7-8.
- [47] Pandya 2008, p. 15.
- [48] Becher 2009, p. 22.
- [49] Becher et al. 2011, p. 96.
- [50] Becher 2009, p. 128.
- [51] Becher 2009, p. 140.
- [52] Thirumathyam & Derawi 2010, p. 1.
- [53] Schmidt, Schmidt & Clausen 2008, p. 7-12.
- [54] Becher 2009, p. 126.
- [55] Becher et al. 2011, p. 101.
- [56] Ruff 2011, p. 11.
- [57] Hogben & Dekker 2010, p. 45.
- [58] Becher 2009, p. 13.
- [59] Becher 2009, p. 34.
- [60] Ruff 2011, p. 7.
- [61] Hogben & Dekker 2010, p. 46-48.
- [62] Ruff 2011, p. 7-8.
- [63] Shabtai et al. 2009, p. 8-9.
- [64] Hogben & Dekker 2010, p. 43.
- [65] Hogben & Dekker 2010, p. 47.
- [66] Hogben & Dekker 2010, p. 43-45.
- [67] Charlie Sorrel (2010-03-01). “TigerText Deletes Text Messages From Receiver's Phone” . *Wired*. Archived from the original on 2010-10-17. Retrieved 2010-03-02.
- [68] Becher 2009, p. 40.

5.10 References

5.10.1 Books

- Bishop, Matt (2004). *Introduction to Computer Security*. Addison Wesley Professional. ISBN 978-0-321-24744-5.
- Dunham, Ken; Abu Nimeh, Saeed; Becher, Michael (2008). *Mobile Malware Attack and Defense*. Syngress Media. ISBN 978-1-59749-298-0.
- Rogers, David (2013). *Mobile Security: A Guide for Users*. Copper Horse Solutions Limited. ISBN 978-1-291-53309-5.

5.10.2 Articles

- Becher, Michael (2009). *Security of Smartphones at the Dawn of Their Ubiquitousness* (PDF) (Dissertation). Mannheim University.
- Becher, Michael; Freiling, Felix C.; Hoffmann, Johannes; Holz, Thorsten; Uellenbeck, Sebastian; Wolf, Christopher (May 2011). *Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices* (PDF). 2011 IEEE Symposium on Security and Privacy. pp. 96–111. ISBN 978-1-4577-0147-4. doi:10.1109/SP.2011.29.
- Bilton, Nick (26 July 2010). “Hackers With Enigmatic Motives Vex Companies” . *The New York Times*. p. 5.
- Cai, Fangda; Chen, Hao; Wu, Yuanyi; Zhang, Yuan (2015). *AppCracker: Widespread Vulnerabilities in User and Session Authentication in Mobile Apps* (PDF) (Dissertation). University of California, Davis.
- Crussell, Johnathan; Gibler, Clint; Chen, Hao (2012). *Attack of the Clones: Detecting Cloned Applications on Android Markets* (PDF) (Dissertation). University of California, Davis.
- Dagon, David; Martin, Tom; Starger, Thad (October–December 2004). “Mobile Phones as Computing Devices: The Viruses are Coming!”. *IEEE Pervasive Computing*. 3 (4): 11. doi:10.1109/MPRV.2004.21.
- Dixon, Bryan; Mishra, Shivakant (June–July 2010). *On and Rootkit and Malware Detection in Smartphones* (PDF). 2010 International Conference on Dependable Systems and Networks Workshops (DSN-W). ISBN 978-1-4244-7728-9.
- Gendrullis, Timo (November 2008). *A real-world attack breaking A5/1 within hours*. Proceedings of CHES ’08. Springer. pp. 266–282. doi:10.1007/978-3-540-85053-3_17.
- Guo, Chuanxiong; Wang, Helen; Zhu, Wenwu (November 2004). *Smart-Phone Attacks and Defenses* (PDF). ACM SIGCOMM HotNets. Association for Computing Machinery, Inc. Retrieved March 31, 2012.
- Halbronn, Cedric; Sigwald, John (2010). *Vulnerabilities & iPhone Security Model* (PDF). HITB SecConf 2010.
- Hogben, Giles; Dekker, Marnix (December 2010). “Smartphones: Information security Risks, Opportunities and Recommendations for users” . ENISA.
- Jøsang, Audun; Miralabé, Laurent; Dallot, Léonard (2015). “Vulnerability by Design in Mobile Network Security” (PDF). *Journal of Information Warfare (JIF)*. 14 (4). ISSN 1445-3347.
- Mickens, James W.; Noble, Brian D. (2005). *Modeling epidemic spreading in mobile environments*. WiSe ’05 Proceedings of the 4th ACM workshop on Wireless security. Association for Computing Machinery, Inc. pp. 77–86. doi:10.1145/1080793.1080806.
- Mulliner, Collin Richard (2006). *Security of Smart Phones* (PDF) (M.Sc. thesis). University of California, Santa Barbara.
- Pandya, Vaibhav Ranchhoddas (2008). *Iphone Security Analysis* (PDF) (Thesis). San Jose State University.

- Raboin, Romain (December 2009). *La sécurité des smartphones* (PDF). Symposium sur la sécurité des technologies de l'information et des communications 2009. SSTIC09 (in French).
- Racic, Radmilo; Ma, Denys; Chen, Hao (2006). *Exploiting MMS Vulnerabilities to Stealthily Exhaust Mobile Phone's Battery* (PDF) (Dissertation). University of California, Davis.
- Roth, Volker; Polak, Wolfgang; Rieffel, Eleanor (2008). *Simple and Effective Defense Against Evil Twin Access Points*. ACM SIGCOMM HotNets. ISBN 978-1-59593-814-5. doi:10.1145/1352533.1352569.
- Ruff, Nicolas (2011). *Sécurité du système Android* (PDF). Symposium sur la sécurité des technologies de l'information et des communications 2011. SSTIC11 (in French).
- Ruggiero, Paul; Foote, Jon. *Cyber Threats to Mobile Phones* (PDF) (thesis). US-CERT.
- Schmidt, Aubrey-Derrick; Schmidt, Hans-Gunther; Clausen, Jan; Yüksel, Kamer Ali; Kiraz, Osman; Camtepe, Ahmet; Albayrak, Sahin (October 2008). *Enhancing Security of Linux-based Android Devices* (PDF). Proceedings of 15th International Linux Kongress.
- Schmidt, Aubrey-Derrick; Schmidt, Hans-Gunther; Batyuk, Leonid; Clausen, Jan Hendrik; Camtepe, Seyit Ahmet; Albayrak, Sahin (April 2009a). *Smartphone Malware Evolution Revisited: Android Next Target?* (PDF). 4th International Conference on Malicious and Unwanted Software (MALWARE). ISBN 978-1-4244-5786-1. Retrieved 2010-11-30.
- Shabtai, Asaf; Fledel, Yuval; Kanonov, Uri; Elovici, Yuval; Dolev, Shlomi (2009). “Google Android: A State-of-the-Art Review of Security Mechanisms”. *CoRR*. arXiv:0912.5101v1 
- Thirumathyam, Rubathas; Derawi, Mohammad O. (2010). *Biometric Template Data Protection in Mobile Device Using Environment XML-database*. 2010 2nd International Workshop on Security and Communication Networks (IWSCN). ISBN 978-1-4244-6938-3.
- Töyssy, Sampo; Helenius, Marko (2006). “About malicious software in smartphones”. *Journal in Computer Virology*. Springer Paris. 2 (2): 109–119. doi:10.1007/s11416-006-0022-0. Retrieved 2010-11-30.

5.10.3 Websites

- European Telecommunications Standards Institute (2011). “3GPP Confidentiality and Integrity Algorithms & UEA1 UIA1”. Archived from the original on 12 May 2012.
- Siemens (2010). “Series M Siemens SMS DoS Vulnerability” .

5.11 Further reading

- CIGREF (October 2010). “Sécurisation de la mobilité” (PDF) (in French).
- Chong, Wei Hoo (November 2007). *iDEN Smartphone Embedded Software Testing* (PDF). Fourth International Conference on Information Technology, 2007. ITNG '07. ISBN 0-7695-2776-0. doi:10.1109/ITNG.2007.103.
- Jansen, Wayne; Scarfone, Karen (October 2008). “Guidelines on Cell Phone and PDA Security: Recommendations of the National Institute of Standards and Technology” (PDF). National Institute of Standards and Technology. Retrieved April 21, 2012.
- Lee, Sung-Min; Suh, Sang-bum; Jeong, Bokdeuk; Mo, Sangdok (January 2008). *A Multi-Layer Mandatory Access Control Mechanism for Mobile Devices Based on Virtualization*. 5th IEEE Consumer Communications and Networking Conference, 2008. CCNC 2008. ISBN 978-1-4244-1456-7. doi:10.1109/ccnc08.2007.63. Archived from the original on May 16, 2013.
- Li, Feng; Yang, Yinying; Wu, Jie (March 2010). *CPMC: An Efficient Proximity Malware Coping Scheme in Smartphone-based Mobile Networks* (PDF). INFOCOM, 2010 Proceedings IEEE. doi:10.1109/INFCOM.2010.5462113.
- Ni, Xudong; Yang, Zhimin; Bai, Xiaole; Champion, Adam C.; Xuan, Dong (October 2009). *Distribute: Differentiated User Access Control on Smartphones* (PDF). 6th IEEE International Conference on Mobile Adhoc and Periodic Sensor Systems, 2009. MASS '09. ISBN 978-1-4244-5113-5.

- Ongtang, Machigar; McLaughlin, Stephen; Enck, William; Mcdaniel, Patrick (December 2009). *Semantically Rich Application-Centric Security in Android* (PDF). Annual Computer Security Applications Conference, 2009. ACSAC '09. ISSN 1063-9527.
- Schmidt, Aubrey-Derrick; Bye, Rainer; Schmidt, Hans-Gunther; Clausen, Jan; Kiraz, Osman; Yüksel, Kamer A.; Camtepe, Seyit A.; Albayrak, Sahin (2009b). *Static Analysis of Executables for Collaborative Malware Detection on Android* (PDF). IEEE International Conference Communications, 2009. ICC '09. ISSN 1938-1883.
- Yang, Feng; Zhou, Xuehai; Jia, Gangyong; Zhang, Qiyuan (2010). *A Non-cooperative Game Approach for Intrusion Detection Systems in Smartphone systems*. 8th Annual Communication Networks and Services Research Conference. ISBN 978-1-4244-6248-3. doi:10.1109/CNSR.2010.24. Archived from the original on May 16, 2013.

Chapter 6

Network security

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a **computer network** and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

6.1 Network Security concept

Network security starts with **Authentication**, commonly with a username and a password. Since this requires just one detail authenticating the user name—i.e., the password—this is sometimes termed one-factor authentication. With two-factor authentication, something the user 'has' is also used (e.g., a **security token** or 'dongle', an ATM card, or a mobile phone); and with three-factor authentication, something the user 'is' is also used (e.g., a **fingerprint** or **retinal scan**).

Once authenticated, a **firewall** enforces access policies such as what services are allowed to be accessed by the network users.*[1] Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as **computer worms** or **Trojans** being transmitted over the network. **Anti-virus software** or an **intrusion prevention system (IPS)***[2] help detect and inhibit the action of such malware. An anomaly-based **intrusion detection system** may also monitor the network like **wireshark traffic** and may be logged for audit purposes and for later high-level analysis. Newer systems combining unsupervised **machine learning** with full network traffic analysis can detect active network attackers from malicious insiders or targeted external attackers that have compromised a user machine or account.*[3]

Communication between two hosts using a network may be encrypted to maintain privacy.

Honeypots, essentially **decoy** network-accessible resources, may be deployed in a network as surveillance and early-warning tools, as the honeypots are not normally accessed for legitimate purposes. Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new **exploitation techniques**. Such analysis may be used to further tighten security of the actual network being protected by the honeypot. A honeypot can also direct an attacker's attention away from legitimate servers. A honeypot encourages attackers to spend their time and energy on the decoy server while distracting their attention from the data on the real server. Similar to a honeypot, a **honeynet** is a network set up with intentional vulnerabilities. Its purpose is also to invite attacks so that the attacker's methods can be studied and that information can be used to increase network security. A honeynet typically contains one or more honeypots.*[4]

6.2 Security managements

Security management for networks is different for all kinds of situations. A home or small office may only require basic security while large businesses may require high-maintenance and advanced software and hardware to prevent malicious attacks from **hacking** and **spamming**.

6.2.1 Types of Attacks

Networks are subject to **attacks** from malicious sources. **Attacks** can be from two categories: “Passive” when a network intruder intercepts data traveling through the network, and “Active” in which an intruder initiates commands to disrupt the network’s normal operation or to conduct reconnaissance and lateral movement to find and gain access to assets available via the network.*[5]

Types of attacks include:*[6]

- Passive
 - Network
 - Wiretapping
 - Port scanner
 - Idle scan
 - Encryption
 - Traffic Analysis
- Active:
 - Virus
 - Eavesdropping
 - Data Modification
 - Denial-of-service attack
 - DNS spoofing
 - Man in the middle
 - ARP poisoning
 - VLAN hopping
 - Smurf attack
 - Buffer overflow
 - Heap overflow
 - Format string attack
 - SQL injection
 - Phishing
 - Cross-site scripting
 - CSRF
 - Cyber-attack

6.3 See also

- Cloud computing security
- Crimeware

- Cyber security standards
- Data loss prevention software
- Greynet
- Identity-based security
- Metasploit Project
- Mobile security
- Netsentron
- Network Security Toolkit
- TCP Gender Changer
- TCP sequence prediction attack
- Timeline of computer security hacker history
- Wireless security
- Dynamic secrets
- Low Orbit Ion Cannon
- High Orbit Ion Cannon

6.4 References

- [1] A Role-Based Trusted Network Provides Pervasive Security and Compliance - interview with Jayshree Ullal, senior VP of Cisco
- [2] Dave Dittrich, *Network monitoring/Intrusion Detection Systems (IDS)*, University of Washington.
- [3] “Dark Reading: Automating Breach Detection For The Way Security Professionals Think” . October 1, 2015.
- [4] ""Honeypots, Honeynets"". Honeypots.net. 2007-05-26. Retrieved 2011-12-09.
- [5] Wright, Joe; Jim Harmening (2009) “15” Computer and Information Security Handbook Morgan Kaufmann Publications Elsevier Inc p. 257
- [6] http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

6.5 Further reading

- *Case Study: Network Clarity*, SC Magazine 2014
- Cisco. (2011). What is network security?. Retrieved from cisco.com
- Security of the Internet (*The Froehlich/Kent Encyclopedia of Telecommunications vol. 15*. Marcel Dekker, New York, 1997, pp. 231–255.)
- *Introduction to Network Security*, Matt Curtin.
- *MPLS, SD-WAN and Network Security'*, Yishay Yovel.
- *Security Monitoring with Cisco Security MARS*, Gary Halleen/Greg Kellogg, Cisco Press, Jul. 6, 2007.
- *Self-Defending Networks: The Next Generation of Network Security*, Duane DeCapite, Cisco Press, Sep. 8, 2006.
- *Security Threat Mitigation and Response: Understanding CS-MARS*, Dale Tesch/Greg Abelar, Cisco Press, Sep. 26, 2006.

- *Securing Your Business with Cisco ASA and PIX Firewalls*, Greg Abelar, Cisco Press, May 27, 2005.
- *Deploying Zone-Based Firewalls*, Ivan Pepelnjak, Cisco Press, Oct. 5, 2006.
- *Network Security: PRIVATE Communication in a PUBLIC World*, Charlie Kaufman | Radia Perlman | Mike Speciner, Prentice-Hall, 2002. ISBN .
- *Network Infrastructure Security*, Angus Wong and Alan Yeung, Springer, 2009.

Chapter 7

Cybercrime

Cyber crime, or **computer related crime**, is crime that involves a computer and a network.^{*[1]} The computer may have been used in the commission of a crime, or it may be the target.^{*[2]} Cybercrimes can be defined as: “Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS).”^{*[3]} Cybercrime may threaten a person or a nation's security and financial health.^{*[4]} Issues surrounding these types of crimes have become high-profile, particularly those surrounding **hacking**, **copyright infringement**, **unwarranted mass-surveillance**, **child pornography**, and **child grooming**. There are also problems of **privacy** when confidential information is intercepted or disclosed, lawfully or otherwise. Debarati Halder and K. Jaishankar further define cybercrime from the perspective of gender and defined 'cybercrime against women' as “Crimes targeted against women with a motive to intentionally harm the victim psychologically and physically, using modern telecommunication networks such as internet and mobile phones”.^{*[3]} Internationally, both governmental and non-state actors engage in cybercrimes, including **espionage**, **financial theft**, and other cross-border crimes. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as **cyberwarfare**.

A report (sponsored by **McAfee**) estimates that the annual damage to the global economy is at \$445 billion;^{*[5]} however, a Microsoft report shows that such survey-based estimates are “hopelessly flawed” and exaggerate the true losses by orders of magnitude.^{*[6]} Approximately \$1.5 billion was lost in 2012 to online credit and debit card fraud in the US.^{*[7]} In 2016, a study by Juniper Research estimated that the costs of cybercrime could be as high as 2.1 trillion by 2019.^{*[8]}

7.1 Classification

Computer crime encompasses a broad range of activities.

7.1.1 Fraud and financial crimes

Main article: **Internet fraud**

Computer fraud is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss. In this context, the fraud will result in obtaining a benefit by:

- Altering in an unauthorized way. This requires little technical expertise and is common form of theft by employees altering the data before entry or entering false data, or by entering unauthorized instructions or using unauthorized processes;
- Altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions. This is difficult to detect;
- Altering or deleting stored data;

Other forms of fraud may be facilitated using computer systems, including bank fraud, carding, identity theft, extortion, and theft of classified information.

A variety of internet scams, many based on phishing and social engineering, target consumers and businesses.

7.1.2 Cyberterrorism

Main article: Cyberterrorism

Government officials and information technology security specialists have documented a significant increase in Internet problems and server scans since early 2001. But there is a growing concern among federal officials that such intrusions are part of an organized effort by cyberterrorists, foreign intelligence services, or other groups to map potential security holes in critical systems. A cyberterrorist is someone who intimidates or coerces a government or an organization to advance their political or social objectives by launching a computer-based attack against computers, networks, or the information stored on them.

Cyberterrorism in general can be defined as an act of terrorism committed through the use of cyberspace or computer resources (Parker 1983). As such, a simple propaganda piece in the Internet that there will be bomb attacks during the holidays can be considered cyberterrorism. There are also hacking activities directed towards individuals, families, organized by groups within networks, tending to cause fear among people, demonstrate power, collecting information relevant for ruining peoples' lives, robberies, blackmailing etc.*[9]

7.1.3 Cyberextortion

Main article: Extortion

Cyberextortion occurs when a website, e-mail server, or computer system is subjected to or threatened with repeated denial of service or other attacks by malicious hackers. These hackers demand money in return for promising to stop the attacks and to offer "protection". According to the Federal Bureau of Investigation, cyberextortionists are increasingly attacking corporate websites and networks, crippling their ability to operate and demanding payments to restore their service. More than 20 cases are reported each month to the FBI and many go unreported in order to keep the victim's name out of the public domain. Perpetrators typically use a distributed denial-of-service attack.*[10]

An example of cyberextortion was the attack on Sony Pictures of 2014.*[11]

7.1.4 Cyberwarfare

Main article: Cyberwarfare

The U.S. Department of Defense (DoD) notes that the cyberspace has emerged as a national-level concern through several recent events of geo-strategic significance. Among those are included, the attack on Estonia's infrastructure in 2007, allegedly by Russian hackers. "In August 2008, Russia again allegedly conducted cyberattacks, this time in a coordinated and synchronized kinetic and non-kinetic campaign against the country of Georgia. Fearing that such attacks may become the norm in future warfare among nation-states, the concept of cyberspace operations impacts and will be adapted by warfighting military commanders in the future.*[12]

7.1.5 Computer as a target

These crimes are committed by a selected group of criminals. Unlike crimes using the computer as a tool, these crimes require the technical knowledge of the perpetrators. As such, as technology evolves, so too does the nature of the crime. These crimes are relatively new, having been in existence for only as long as computers have—which explains how unprepared society and the world in general is towards combating these crimes. There are numerous crimes of this nature committed daily on the internet:

Crimes that primarily target computer networks or devices include:



Sailors analyze, detect and defensively respond to unauthorized activity within U.S. Navy information systems and computer networks

- Computer viruses
- Denial-of-service attacks
- Malware (malicious code)

7.1.6 Computer as a tool

Main articles: Internet fraud, Spamming, Phishing, and Carding (fraud)

When the individual is the main target of cybercrime, the computer can be considered as the tool rather than the target. These crimes generally involve less technical expertise. Human weaknesses are generally exploited. The damage dealt is largely psychological and intangible, making legal action against the variants more difficult. These are the crimes which have existed for centuries in the offline world. Scams, theft, and the likes have existed even before the development in high-tech equipment. The same criminal has simply been given a tool which increases his potential pool of victims and makes him all the harder to trace and apprehend.*[13]

Crimes that use computer networks or devices to advance other ends include:

- Fraud and identity theft (although this increasingly uses malware, hacking and/or phishing, making it an example of both “computer as target” and “computer as tool” crime)
- Information warfare
- Phishing scams
- Spam
- Propagation of illegal obscene or offensive content, including harassment and threats

The unsolicited sending of bulk email for commercial purposes (**spam**) is unlawful in some jurisdictions.

Phishing is mostly propagated via email. Phishing emails may contain links to other websites that are affected by malware.* [14] Or, they may contain links to fake online banking or other websites used to steal private account information.

Obscene or offensive content

The content of websites and other electronic communications may be distasteful, obscene or offensive for a variety of reasons. In some instances these communications may be legal.

The extent to which these communications are unlawful varies greatly between countries, and even within nations. It is a sensitive area in which the courts can become involved in arbitrating between groups with strong beliefs.

One area of Internet pornography that has been the target of the strongest efforts at curtailment is child pornography.



Various aspects needed to be considered when understanding harassment online.

Harassment See also: Cyberbullying, Online predator, Cyberstalking, and Internet troll

Whereas content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, sexual orientation. This often occurs in chat rooms, through newsgroups, and by sending hate e-mail to interested parties. Harassment on the internet also includes revenge porn.

There are instances where committing a crime using a computer can lead to an enhanced sentence. For example, in the case of *United States v. Neil Scott Kramer*, Kramer was served an enhanced sentence according to the U.S. Sentencing Guidelines Manual §2G1.3(b)(3)*[15] for his use of a cell phone to “persuade, induce, entice, coerce, or facilitate the travel of, the minor to engage in prohibited sexual conduct.” Kramer argued that this claim was insufficient because his charge included persuading through a computer device and his cellular phone technically is not a computer. Although Kramer tried to argue this point, U.S. Sentencing Guidelines Manual states that the term computer “means an electronic, magnetic, optical, electrochemically, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”*[16]

Connecticut was the U.S. state to pass a statute making it a criminal offense to harass someone by computer. Michigan, Arizona, and Virginia and South Carolina* [17] have also passed laws banning harassment by electronic means.*[18]*[19]

Harassment as defined in the U.S. computer statutes is typically distinct from cyberbullying, in that the former usually relates to a person's “use a computer or computer network to communicate obscene, vulgar, profane, lewd, lascivious, or indecent language, or make any suggestion or proposal of an obscene nature, or threaten any illegal or immoral act,” while the latter need not involve anything of a sexual nature.

Although freedom of speech is protected by law in most democratic societies (in the US this is done by the First Amendment), it does not include all types of speech. In fact spoken or written “true threat” speech/text is criminalized because of “intent to harm or intimidate”, that also applies for online or any type of network related threats in written text or speech.*[20] The US Supreme Court definition of “true threat” is “statements where the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group”.*[20]

Drug trafficking

Darknet markets are used to buy and sell recreational drugs online. Some drug traffickers use encrypted messaging tools to communicate with drug mules. The dark web site Silk Road was a major online marketplace for drugs before it was shut down by law enforcement (then reopened under new management, and then shut down by law enforcement again). After Silk Road 2.0 went down, Silk Road 3 Reloaded emerged. However, it was just an older marketplace named Diabolus Market, that used the name for more exposure from the brand's previous success.*[21]

7.2 Documented cases

- One of the highest profiled banking computer crime occurred during a course of three years beginning in 1970. The chief teller at the Park Avenue branch of New York's Union Dime Savings Bank embezzled over \$1.5 million from hundreds of accounts.*[22]
- A hacking group called MOD (Masters of Deception), allegedly stole passwords and technical data from Pacific Bell, Nynex, and other telephone companies as well as several big credit agencies and two major universities. The damage caused was extensive, one company, Southwestern Bell suffered losses of \$370,000 alone.*[22]
- In 1983, a nineteen-year-old UCLA student used his PC to break into a Defense Department international communications system.*[22]
- Between 1995 and 1998 the NewsCorp satellite pay to view encrypted SKY-TV service was hacked several times during an ongoing technological arms race between a pan-European hacking group and NewsCorp. The original motivation of the hackers was to watch Star Trek re-runs in Germany; which was something which NewsCorp did not have the copyright to allow.*[23]
- On 26 March 1999, the Melissa worm infected a document on a victim's computer, then automatically sent that document and a copy of the virus spread via e-mail to other people.
- In February 2000, an individual going by the alias of MafiaBoy began a series denial-of-service attacks against high-profile websites, including Yahoo!, Amazon.com, Dell, Inc., E*TRADE, eBay, and CNN. About fifty computers at Stanford University, and also computers at the University of California at Santa Barbara, were amongst the zombie computers sending pings in DDoS attacks. On 3 August 2000, Canadian federal prosecutors charged MafiaBoy with 54 counts of illegal access to computers, plus a total of ten counts of mischief to data for his attacks.
- The Russian Business Network (RBN) was registered as an internet site in 2006. Initially, much of its activity was legitimate. But apparently the founders soon discovered that it was more profitable to host illegitimate activities and started hiring its services to criminals. The RBN has been described by VeriSign as “the baddest of the bad”.*[24] It offers web hosting services and internet access to all kinds of criminal and objectionable activities, with an individual activities earning up to \$150 million in one year. It specialized in and in some cases monopolized personal identity theft for resale. It is the originator of MPack and an alleged operator of the now defunct Storm botnet.
- On 2 March 2010, Spanish investigators arrested 3 in infection of over 13 million computers around the world. The “botnet” of infected computers included PCs inside more than half of the Fortune 1000 companies and more than 40 major banks, according to investigators.
- In August 2010 the international investigation Operation Delevo, operating under the aegis of the Department of Homeland Security, shut down the international pedophile ring Dreamboard. The website had approximately 600 members, and may have distributed up to 123 terabytes of child pornography (roughly equivalent to 16,000 DVDs). To date this is the single largest U.S. prosecution of an international child pornography ring; 52 arrests were made worldwide.*[25]

- In January 2012 Zappos.com experienced a security breach after as many as 24 million customers' credit card numbers, personal information, billing and shipping addresses had been compromised.*[26]
- In June 2012 LinkedIn and eHarmony were attacked, compromising 65 million password hashes. 30,000 passwords were cracked and 1.5 million eHarmony passwords were posted online.*[27]
- December 2012 Wells Fargo website experienced a denial of service attack. Potentially compromising 70 million customers and 8.5 million active viewers. Other banks thought to be compromised: Bank of America, J. P. Morgan U.S. Bank, and PNC Financial Services.*[28]
- April 23, 2013 saw the Associated Press' Twitter account's hacked - the hacker posted a hoax tweet about fictitious attacks in the White House that they claimed left President Obama injured.*[29] This hoax tweet resulted in a brief plunge of 130 points from the Dow Jones Industrial Average, removal of \$136 billion from S&P 500 index,*[30] and the temporary suspension of AP's Twitter account. The Dow Jones later restored its session gains.
- In May 2017, 74 countries logged a ransomware cybercrime, called "WannaCry"*[31]

7.3 Combating computer crime

7.3.1 Diffusion of cybercrime

The broad diffusion of cybercriminal activities is an issue in computer crimes detection and prosecution. According to Jean-Loup Richet (Research Fellow at ESSEC ISIS), technical expertise and accessibility no longer act as barriers to entry into cybercrime.*[32] Indeed, hacking is much less complex than it was a few years ago, as hacking communities have greatly diffused their knowledge through the Internet. Blogs and communities have hugely contributed to information sharing: beginners could benefit from older hackers' knowledge and advice. Furthermore, Hacking is cheaper than ever: before the cloud computing era, in order to spam or scam one needed a dedicated server, skills in server management, network configuration, and maintenance, knowledge of Internet service provider standards, etc. By comparison, a mail software-as-a-service is a scalable, inexpensive, bulk, and transactional e-mail-sending service for marketing purposes and could be easily set up for spam.*[33] Jean-Loup Richet explains that cloud computing could be helpful for a cybercriminal as a way to leverage his attack – brute-forcing a password, improve the reach of a botnet, or facilitating a spamming campaign.*[34]

7.3.2 Investigation

A computer can be a source of evidence (see digital forensics). Even where a computer is not directly used for criminal purposes, it may contain records of value to criminal investigators in the form of a logfile. In most countries Internet Service Providers are required, by law, to keep their logfiles for a predetermined amount of time. For example; a European wide Data Retention Directive (applicable to all EU member states) states that all E-mail traffic should be retained for a minimum of 12 months.

- Methodology of cybercrime investigation

There are many ways for cybercrime to take place, and investigations tend to start with an IP Address trace, however that is not necessarily a factual basis upon which detectives can solve a case. Different types of high-tech crime may also include elements of low-tech crime, and vice-versa, making cybercrime investigators an indispensable part of modern law-enforcement. Methodology of cybercrime detective work is dynamic and is constantly improving, whether in closed police units, or in international cooperation framework.*[35]

7.3.3 Legislation

Due to easily exploitable laws, cybercriminals use developing countries in order to evade detection and prosecution from law enforcement. In developing countries, such as the Philippines, laws against cybercrime are weak or sometimes nonexistent. These weak laws allow cybercriminals to strike from international borders and remain undetected. Even when identified, these criminals avoid being punished or extradited to a country, such as the United States, that

has developed laws that allow for prosecution. While this proves difficult in some cases, agencies, such as the FBI, have used deception and subterfuge to catch criminals. For example, two Russian hackers had been evading the FBI for some time. The FBI set up a fake computing company based in Seattle, Washington. They proceeded to lure the two Russian men into the United States by offering them work with this company. Upon completion of the interview, the suspects were arrested outside of the building. Clever tricks like this are sometimes a necessary part of catching cybercriminals when weak legislation makes it impossible otherwise.*[36]

President Barack Obama released in an executive order in April 2015 to combat cybercrime. The executive order allows the United States to freeze assets of convicted cybercriminals and block their economic activity within the United States. This is some of the first solid legislation that combats cybercrime in this way.*[37]

The European Union adopted directive 2013/40/EU. All offences of the directive, and other definitions and procedural institutions are also in the Council of Europe's Convention on Cybercrime.*[38]

7.3.4 Penalties

Penalties for computer related crimes in New York State can range from a fine and a short period of jail time for a Class A misdemeanor such as unauthorized use of a computer up to computer tampering in the first degree which is a Class C felony and can carry 3 to 15 years in prison.

However, some **hackers** have been hired as **information security experts** by private companies due to their inside knowledge of computer crime, a phenomenon which theoretically could create **perverse incentives**. A possible counter to this is for courts to ban convicted hackers from using the Internet or computers, even after they have been released from prison – though as computers and the Internet become more and more central to everyday life, this type of punishment may be viewed as more and more harsh and draconian. However, nuanced approaches have been developed that manage cyberoffender behavior without resorting to total computer and/or Internet bans.*[39] These approaches involve restricting individuals to specific devices which are subject to computer monitoring and/or computer searches by probation and/or parole officers.*[40]

7.3.5 Awareness

As technology advances and more people rely on the internet to store sensitive information such as banking or credit card information, criminals are going to attempt to steal that information. Cyber-crime is becoming more of a threat to people across the world. Raising awareness about how information is being protected and the tactics criminals use to steal that information is important in today's world. According to the FBI's Internet Crime Complaint Center in 2014 there were 269,422 complaints filed. With all the claims combined there was a reported total loss of \$800,492,073. But yet cyber-crime doesn't seem to be on the average person's radar. There are 1.5 million cyber-attacks annually, that means that there are over 4,000 attacks a day, 170 attacks every hour, or nearly three attacks every minute, with studies showing us that only 16% of victims had asked the people who were carrying out the attacks to stop.*[41] Anybody who uses the internet for any reason can be a victim, which is why it is important to be aware of how one is being protected while online.

7.4 Agencies

- Australian High Tech Crime Centre
- National White Collar Crime Center

7.5 See also

- Computer Fraud and Abuse Act
- Computer trespass
- Cyber defamation law
- Cyber-

- Cyberheist
- Domain hijacking
- Economic and industrial espionage
- FBI
- Illegal drop catching
- Immigration and Customs Enforcement (ICE)
- Internet homicide
- Internet suicide pact
- Legal aspects of computing
- List of computer criminals
- Metasploit Project
- National Crime Agency (NCA)
- Penetration test
- Police National E-Crime Unit
- Protected computer
- Techno-thriller
- Trespass to chattels
- United States Secret Service
- White collar crime

7.6 References

- [1] Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.
- [2] Warren G. Kruse, Jay G. Heiser (2002). *Computer forensics: incident response essentials*. Addison-Wesley. p. 392. ISBN 0-201-70719-5.
- [3] • Halder, D., & Jaishankar, K. (2011) *Cyber crime and the Victimization of Women: Laws, Rights, and Regulations*. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9
- [4] Steve Morgan (January 17, 2016). "Cyber Crime Costs Projected To Reach \$2 Trillion by 2019" . *Forbes*. Retrieved September 22, 2016.
- [5] "Cyber crime costs global economy \$445 billion a year: report" . Reuters. 2014-06-09. Retrieved 2014-06-17.
- [6] "Sex, Lies and Cybercrime Surveys" (PDF). Microsoft. 2011-06-15. Retrieved 2015-03-11.
- [7] "#Cybercrime—what are the costs to victims - North Denver News" . *North Denver News*. Retrieved 16 May 2015.
- [8] "Cybercrime will Cost Businesses Over \$2 Trillion by 2019" (Press release). Juniper Research. Retrieved May 21, 2016.
- [9] "Cybercriminals Need Shopping Money in 2017, Too! - SentinelOne" . *sentinelone.com*. Retrieved 2017-03-24.
- [10] Lepofsky, Ron. "Cyberextortion by Denial-of-Service Attack" (PDF). Archived from the original (PDF) on July 6, 2011.
- [11] Mohanta, Abhijit (6 December 2014). "Latest Sony Pictures Breach : A Deadly Cyber Extortion" . Retrieved 20 September 2015.
- [12] Dennis Murphy (February 2010). "War is War? The utility of cyberspace operations in the contemporary operational environment" (PDF). Center for Strategic Leadership. Archived from the original (PDF) on 20 March 2012.

- [13] “Cyber Crime definition” .
- [14] “Save browsing” . *google*.
- [15] “2011 U.S. Sentencing Guidelines Manual § 2G1.3(b)(3)”.
- [16] “United States of America v. Neil Scott Kramer” . Retrieved 2013-10-23.
- [17] “South Carolina” . Retrieved 16 May 2015.
- [18] “1. In Connecticut , harassment by computer is now a crime” . Nerac Inc. February 3, 2003. Archived from the original on April 10, 2008.
- [19] “Section 18.2-152.7:1” . *Code of Virginia*. Legislative Information System of Virginia. Retrieved 2008-11-27.
- [20] Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace*, ABC-CLIO, 2010, pp. 91
- [21] “We talked to the opportunist imitator behind Silk Road 3.0” . 2014-11-07. Retrieved 2016-10-04.
- [22] Weitzer, Ronald (2003). *Current Controversies in Criminology*. Upper Saddle River, New Jersey: Pearson Education Press. p. 150.
- [23] David Mann And Mike Sutton (2011-11-06). “>>Netcrime” . Bjc.oxfordjournals.org. Retrieved 2011-11-10.
- [24] “A walk on the dark side” . The Economist. 2007-09-30.
- [25] “DHS: Secretary Napolitano and Attorney General Holder Announce Largest U.S. Prosecution of International Criminal Network Organized to Sexually Exploit Children” . Dhs.gov. Retrieved 2011-11-10.
- [26] DAVID K. LI (January 17, 2012). “Zappos cyber attack” . *New York Post*.
- [27] Salvador Rodriguez (June 6, 2012). “Like LinkedIn, eHarmony is hacked; 1.5 million passwords stolen” . *Los Angeles Times*.
- [28] Rick Rothacker (Oct 12, 2012). “Cyber attacks against Wells Fargo ‘significant,’ handled well: CFO” . *Reuters*.
- [29] “AP Twitter Hack Falsely Claims Explosions at White House” . Samantha Murphy. April 23, 2013. Retrieved April 23, 2013.
- [30] “Fake Tweet Erasing \$136 Billion Shows Markets Need Humans” . Bloomberg. April 23, 2013. Retrieved April 23, 2013.
- [31] hermesauto (13 May 2017). “Unprecedented cyber attacks wreak global havoc” .
- [32] Richet, Jean-Loup (2013). “From Young Hackers to Crackers” . *International Journal of Technology and Human Interaction*. 9 (1).
- [33] Richet, Jean-Loup (2011). “Adoption of deviant behavior and cybercrime 'Know how' diffusion” . *York Deviancy Conference*.
- [34] Richet, Jean-Loup (2012). “How to Become a Black Hat Hacker? An Exploratory Study of Barriers to Entry Into Cybercrime.” . *17th AIM Symposium*.
- [35] http://www.unafei.or.jp/english/pdf/RS_No79/No79_15RC_Group2.pdf
- [36] Kshetri, Nir. “Diffusion and Effects of Cyber Crime in Developing Countries” .
- [37] Northam, Jackie. “U.S. Creates First Sanctions Program Against Cybercriminals” .
- [38] Adrian Cristian MOISE (2015). “Analysis of Directive 2013/40/EU on attacks against information systems in the context of approximation of law at the European level” (PDF). *Journal of Law and Administrative Sciences*. Archived from the original (PDF) on December 8, 2015.
- [39] “Managing the Risks Posed by Offender Computer Use - Perspectives” (PDF). December 2011.
- [40] Bowker, Art (2012). *The Cybercrime Handbook for Community Corrections: Managing Risk in the 21st Century*. Springfield: Thomas. ISBN 9780398087289.
- [41] Feinberg, T (2008). “Whether it happens at school or off-campus, cyberbullying disrupts and affects.” . *Cyberbullying*: 10.

7.7 Further reading

- Balkin, J., Grimmelmann, J., Katz, E., Kozlofski, N., Wagman, S. & Zarsky, T. (2006) (eds) *Cybercrime: Digital Cops in a Networked Environment*, New York University Press, New York.
- Bowker, Art (2012) “The Cybercrime Handbook for Community Corrections: Managing Risk in the 21st Century” Charles C. Thomas Publishers, Ltd. Springfield.
- Brenner, S. (2007) *Law in an Era of Smart Technology*, Oxford: Oxford University Press
- Broadhurst, R., and Chang, Lennon Y.C. (2013) "Cybercrime in Asia: trends and challenges", in B. Hebberton, SY Shou, & J. Liu (eds), Asian Handbook of Criminology (pp. 49–64). New York: Springer (ISBN 978-1-4614-5217-1)
- Chang, L.Y. C. (2012) *Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention across the Taiwan Strait*. Cheltenham: Edward Elgar. (ISBN 978-0-85793-667-7)
- Chang, Lennon Y.C., & Grabosky, P. (2014) "Cybercrime and establishing a secure cyber world", in M. Gill (ed) Handbook of Security (pp. 321–339). NY: Palgrave.
- Csonka P. (2000) Internet Crime; the Draft council of Europe convention on cyber-crime: A response to the challenge of crime in the age of the internet? *Computer Law & Security Report* Vol.16 no.5.
- Easttom C. (2010) *Computer Crime Investigation and the Law*
- Fafinski, S. (2009) *Computer Misuse: Response, regulation and the law* Cullompton: Willan
- Glenny, Misha, *DarkMarket : cyberthieves, cybergangs, and you*, New York, NY : Alfred A. Knopf, 2011. ISBN 978-0-307-59293-4
- Grabosky, P. (2006) *Electronic Crime*, New Jersey: Prentice Hall
- Halder, D., & Jaishankar, K. (2016). *Cyber Crimes against Women in India*. New Delhi: SAGE Publishing. ISBN 978-9385985775.
- Halder, D., & Jaishankar, K. (2011) *Cyber crime and the Victimization of Women: Laws, Rights, and Regulations*. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9
- Jaishankar, K. (Ed.) (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal behavior*. Boca Raton, FL, USA: CRC Press, Taylor and Francis Group.
- McQuade, S. (2006) *Understanding and Managing Cybercrime*, Boston: Allyn & Bacon.
- McQuade, S. (ed) (2009) *The Encyclopedia of Cybercrime*, Westport, CT: Greenwood Press.
- Parker D (1983) *Fighting Computer Crime*, U.S.: Charles Scribner's Sons.
- Pattavina, A. (ed) *Information Technology and the Criminal Justice System*, Thousand Oaks, CA: Sage.
- Paul Taylor. *Hackers: Crime in the Digital Sublime* (November 3, 1999 ed.). Routledge; 1 edition. p. 200. ISBN 0-415-18072-4.
- Robertson, J. (2010, March 2). Authorities bust 3 in infection of 13m computers. Retrieved March 26, 2010, from Boston News: [Boston.com](#)
- Walden, I. (2007) *Computer Crimes and Digital Investigations*, Oxford: Oxford University Press.
- Rolón, Darío N. Control, vigilancia y respuesta penal en el ciberespacio, Latin American's New Security Thinking, Clacso, 2014, pp. 167/182
- Richet, J.L. (2013) From Young Hackers to Crackers, *International Journal of Technology and Human Interaction (IJTHI)*, 9(3), 53-62.
- Wall, D.S. (2007) *Cybercrimes: The transformation of crime in the information age*, Cambridge: Polity.
- Williams, M. (2006) *Virtually Criminal: Crime, Deviance and Regulation Online*, Routledge, London.
- Yar, M. (2006) *Cybercrime and Society*, London: Sage.

7.8 External links

- Centre for Cyber Victim Counselling (CCVC)
- The American Society of Digital Forensics & eDiscovery – Cybercrime Information
- A Guide to Computer Crime from legal.practitioner.com
- Virtual Forum Against Cybercrime
- Cyber Crime Law Complete Information
- CyberCrime Asia Research Center – Information about computer crime, Internet fraud and CyberTerrorism in Asia
- Information and Research Center for Cybercrime Germany
- International Journal of Cyber Criminology

7.8.1 Government resources

- Cybercrime.gov from the United States Department of Justice
- National Institute of Justice Electronic Crime Program from the United States Department of Justice
- FBI Cyber Investigators home page
- US Secret Service Computer Fraud
- Australian High Tech Crime Centre

Chapter 8

Vulnerability (computing)

In computer security, a **vulnerability** is a weakness which allows an attacker to reduce a system's information assurance. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.^{*[1]} To exploit a vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame, vulnerability is also known as the attack surface.

Vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities.^{*[2]} This practice generally refers to software vulnerabilities in computing systems. Using vulnerability as a method of criminal activity or to create civil unrest falls under US Code Chapter 113B on terrorism^{*[3]}

A security risk may be classified as a vulnerability. The use of vulnerability with the same meaning of risk can lead to confusion. The risk is tied to the potential of a significant loss. Then there are vulnerabilities without risk: for example when the affected asset has no value. A vulnerability with one or more known instances of working and fully implemented attacks is classified as an exploitable vulnerability—a vulnerability for which an exploit exists. The **window of vulnerability** is the time from when the security hole was introduced or manifested in deployed software, to when access was removed, a security fix was available/deployed, or the attacker was disabled—see zero-day attack.

Security bug (security defect) is a narrower concept: there are vulnerabilities that are not related to software: hardware, site, personnel vulnerabilities are examples of vulnerabilities that are not software security bugs.

Constructs in programming languages that are difficult to use properly can be a large source of vulnerabilities.

8.1 Definitions

ISO 27005 defines **vulnerability** as:^{*[4]}

A weakness of an asset or group of assets that can be exploited by one or more threats

where an *asset* is anything that has value to the organization, its business operations and their continuity, including information resources that support the organization's mission^{*[5]}

IETF RFC 2828 define **vulnerability** as:^{*[6]}

A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy

The Committee on National Security Systems of United States of America defined **vulnerability** in CNSS Instruction No. 4009 dated 26 April 2010 National Information Assurance Glossary:^{*[7]}

Vulnerability — Weakness in an IS, system security procedures, internal controls, or implementation that could be exploited

Many NIST publications define **vulnerability** in IT contest in different publications: FISMApedia^{*[8]} term^{*[9]} provide a list. Between them SP 800-30,^{*[10]} give a broader one:

A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

ENISA defines **vulnerability** in^{*}[11] as:

The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event [G.11] compromising the security of the computer system, network, application, or protocol involved.(ITSEC)

The Open Group defines **vulnerability** in^{*}[12] as:

The probability that threat capability exceeds the ability to resist the threat.

Factor Analysis of Information Risk (FAIR) defines **vulnerability** as:^{*}[13]

The probability that an asset will be unable to resist the actions of a threat agent

According FAIR vulnerability is related to Control Strength, i.e. the strength of a control as compared to a standard measure of force and the threat Capabilities, i.e. the probable level of force that a threat agent is capable of applying against an asset.

ISACA defines **vulnerability** in Risk It framework as:

A weakness in design, implementation, operation or internal control

Data and Computer Security: Dictionary of standards concepts and terms, authors Dennis Longley and Michael Shain, Stockton Press, ISBN 0-935859-17-9, defines **vulnerability** as:

1) In computer security, a weakness in automated systems security procedures, administrative controls, Internet controls, etc., that could be exploited by a threat to gain unauthorized access to information or to disrupt critical processing. 2) In computer security, a weakness in the physical layout, organization, procedures, personnel, management, administration, hardware or software that may be exploited to cause harm to the ADP system or activity. 3) In computer security, any weakness or flaw existing in a system. The attack or harmful event, or the opportunity available to a threat agent to mount that attack.

Matt Bishop and Dave Bailey^{*}[14] give the following definition of computer **vulnerability**:

A computer system is composed of states describing the current configuration of the entities that make up the computer system. The system computes through the application of state transitions that change the state of the system. All states reachable from a given initial state using a set of state transitions fall into the class of authorized or unauthorized, as defined by a security policy. In this paper, the definitions of these classes and transitions is considered axiomatic. A vulnerable state is an authorized state from which an unauthorized state can be reached using authorized state transitions. A compromised state is the state so reached. An attack is a sequence of authorized state transitions which end in a compromised state. By definition, an attack begins in a vulnerable state. A vulnerability is a characterization of a vulnerable state which distinguishes it from all non-vulnerable states. If generic, the vulnerability may characterize many vulnerable states; if specific, it may characterize only one...

National Information Assurance Training and Education Center defines **vulnerability**: ^{*}[15]^{*}[16]

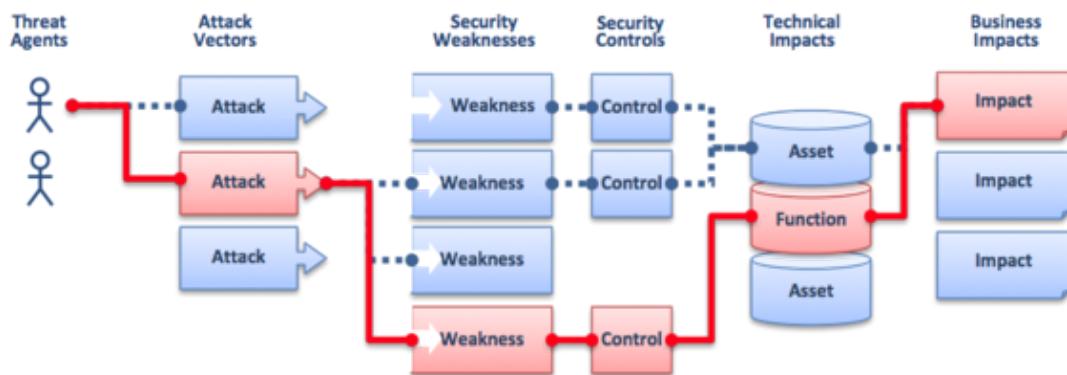
A weakness in automated system security procedures, administrative controls, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing. 2. A weakness in system security procedures, hardware design, internal controls, etc. , which could be exploited to gain unauthorized access to classified or sensitive information. 3. A weakness in the physical layout, organization, procedures, personnel, management, administration, hardware, or software

that may be exploited to cause harm to the ADP system or activity. The presence of a vulnerability does not in itself cause harm; a vulnerability is merely a condition or set of conditions that may allow the ADP system or activity to be harmed by an attack. 4. An assertion primarily concerning entities of the internal environment (assets); we say that an asset (or class of assets) is vulnerable (in some way, possibly involving an agent or collection of agents); we write: $V(i, e)$ where: e may be an empty set. 5. Susceptibility to various threats. 6. A set of properties of a specific internal entity that, in union with a set of properties of a specific external entity, implies a risk. 7. The characteristics of a system which cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment.

8.2 Vulnerability and risk factor models

A resource (either physical or logical) may have one or more vulnerabilities that can be exploited by a threat agent in a threat action. The result can potentially compromise the confidentiality, integrity or availability of resources (not necessarily the vulnerable one) belonging to an organization and/or other parties involved (customers, suppliers). The so-called CIA triad is the basis of Information Security.

An attack can be *active* when it attempts to alter system resources or affect their operation, compromising integrity or availability. A "passive attack" attempts to learn or make use of information from the system but does not affect system resources, compromising confidentiality.*[6]



OWASP: relationship between threat agent and business impact

OWASP (see figure) depicts the same phenomenon in slightly different terms: a threat agent through an attack vector exploits a weakness (vulnerability) of the system and the related security controls, causing a technical impact on an IT resource (asset) connected to a business impact.

The overall picture represents the risk factors of the risk scenario.*[17]

8.3 Information security management system

A set of policies concerned with information security management, the information security management system (ISMS), has been developed to manage, according to Risk management principles, the countermeasures in order to ensure the security strategy is set up following the rules and regulations applicable in a country. These countermeasures are also called Security controls, but when applied to the transmission of information they are called security services.*[18]

8.4 Classification

Vulnerabilities are classified according to the asset class they are related to.*[4]

- hardware
 - susceptibility to humidity
 - susceptibility to dust
 - susceptibility to soiling
 - susceptibility to unprotected storage
- software
 - insufficient testing
 - lack of audit trail
- network
 - unprotected communication lines
 - insecure network architecture
- personnel
 - inadequate recruiting process
 - inadequate security awareness
- physical site
 - area subject to flood
 - unreliable power source
- organizational
 - lack of regular audits
 - lack of continuity plans
 - lack of security

8.5 Causes

- Complexity: Large, complex systems increase the probability of flaws and unintended access points* [19]
- Familiarity: Using common, well-known code, software, operating systems, and/or hardware increases the probability an attacker has or can find the knowledge and tools to exploit the flaw* [20]
- Connectivity: More physical connections, privileges, ports, protocols, and services and time each of those are accessible increase vulnerability* [13]
- Password management flaws: The computer user uses weak passwords that could be discovered by brute force.* [21] The computer user stores the password on the computer where a program can access it. Users re-use passwords between many programs and websites.* [19]
- Fundamental operating system design flaws: The operating system designer chooses to enforce suboptimal policies on user/program management. For example, operating systems with policies such as default permit grant every program and every user full access to the entire computer.* [19] This operating system flaw allows viruses and malware to execute commands on behalf of the administrator.* [22]
- Internet Website Browsing: Some internet websites may contain harmful Spyware or Adware that can be installed automatically on the computer systems. After visiting those websites, the computer systems become infected and personal information will be collected and passed on to third party individuals.* [23]
- Software bugs: The programmer leaves an exploitable bug in a software program. The software bug may allow an attacker to misuse an application.* [19]

- **Unchecked user input:** The program assumes that all user input is safe. Programs that do not check user input can allow unintended direct execution of commands or SQL statements (known as Buffer overflows, SQL injection or other non-validated inputs).*[19]
- Not learning from past mistakes:*[24]*[25] for example most vulnerabilities discovered in IPv4 protocol software were discovered in the new IPv6 implementations.*[26]

The research has shown that the most vulnerable point in most information systems is the human user, operator, designer, or other human:*[27] so humans should be considered in their different roles as asset, threat, information resources. **Social engineering** is an increasing security concern.

8.6 Vulnerability consequences

The impact of a security breach can be very high. The fact that IT managers, or upper management, can (easily) know that IT systems and applications have vulnerabilities and do not perform any action to manage the **IT risk** is seen as a misconduct in most legislations. **Privacy law** forces managers to act to reduce the impact or likelihood of that security risk. **Information technology security audit** is a way to let other independent people certify that the IT environment is managed properly and lessen the responsibilities, at least having demonstrated the good faith. **Penetration test** is a form of verification of the weakness and countermeasures adopted by an organization: a **White hat** hacker tries to attack an organization's information technology assets, to find out how easy or difficult it is to compromise the IT security. *[28] The proper way to professionally manage the IT risk is to adopt an **Information Security Management System**, such as ISO/IEC 27002 or **Risk IT** and follow them, according to the security strategy set forth by the upper management. *[18]

One of the key concept of information security is the principle of **defence in depth**: i.e. to set up a multilayer defence system that can:

- prevent the exploit
- detect and intercept the attack
- find out the threat agents and prosecute them

Intrusion detection system is an example of a class of systems used to detect attacks.

Physical security is a set of measures to protect physically the information asset: if somebody can get physical access to the information asset, it is quite easy to make resources unavailable to its legitimate users.

Some sets of criteria to be satisfied by a computer, its operating system and applications in order to meet a good security level have been developed: **ITSEC** and **Common criteria** are two examples.

8.7 Vulnerability disclosure

Responsible disclosure (many now refer to it as 'coordinated disclosure' because the first is a biased word) of vulnerabilities is a topic of great debate. As reported by The Tech Herald in August 2010, "Google, Microsoft, TippingPoint, and Rapid7 have recently issued guidelines and statements addressing how they will deal with disclosure going forward." *[29]

A responsible disclosure first alerts the affected vendors confidentially before alerting **CERT** two weeks later, which grants the vendors another 45-day grace period before publishing a security advisory.

Full disclosure is done when all the details of vulnerability is publicized, perhaps with the intent to put pressure on the software or procedure authors to find a fix urgently.

Well respected authors have published books on vulnerabilities and how to exploit them: **Hacking: The Art of Exploitation Second Edition** is a good example.

Security researchers catering to the needs of the **cyberwarfare** or **cybercrime** industry have stated that this approach does not provide them with adequate income for their efforts.*[30] Instead, they offer their exploits privately to enable **Zero day attacks**.

The never ending effort to find new vulnerabilities and to fix them is called Computer insecurity.

In January 2014 when Google revealed a Microsoft vulnerability before Microsoft released a patch to fix it, a Microsoft representative called for coordinated practices among software companies in revealing disclosures.* [31]

8.7.1 Vulnerability inventory

Mitre Corporation maintains a list of disclosed vulnerabilities in a system called Common Vulnerabilities and Exposures, where vulnerability are classified (scored) using Common Vulnerability Scoring System (CVSS).

OWASP collects a list of potential vulnerabilities with the aim of educating system designers and programmers, therefore reducing the likelihood of vulnerabilities being written unintentionally into the software.* [32]

8.8 Vulnerability disclosure date

The time of disclosure of a vulnerability is defined differently in the security community and industry. It is most commonly referred to as “a kind of public disclosure of security information by a certain party”. Usually, vulnerability information is discussed on a mailing list or published on a security web site and results in a security advisory afterward.

The **time of disclosure** is the first date a security vulnerability is described on a channel where the disclosed information on the vulnerability has to fulfill the following requirement:

- The information is freely available to the public
- The vulnerability information is published by a trusted and independent channel/source
- The vulnerability has undergone analysis by experts such that risk rating information is included upon disclosure

8.9 Identifying and removing vulnerabilities

Many software tools exist that can aid in the discovery (and sometimes removal) of vulnerabilities in a computer system. Though these tools can provide an auditor with a good overview of possible vulnerabilities present, they can not replace human judgment. Relying solely on scanners will yield false positives and a limited-scope view of the problems present in the system.

Vulnerabilities have been found in every major operating system including Windows, macOS, various forms of Unix and Linux, OpenVMS, and others. The only way to reduce the chance of a vulnerability being used against a system is through constant vigilance, including careful system maintenance (e.g. applying software patches), best practices in deployment (e.g. the use of firewalls and access controls) and auditing (both during development and throughout the deployment lifecycle).

8.10 Examples of vulnerabilities

Vulnerabilities are related to:

- physical environment of the system
- the personnel
- management
- administration procedures and security measures within the organization
- business operation and service delivery
- hardware

- software
- communication equipment and facilities
- and their combinations.

It is evident that a pure technical approach cannot even protect physical assets: one should have administrative procedure to let maintenance personnel to enter the facilities and people with adequate knowledge of the procedures, motivated to follow it with proper care. See [Social engineering \(security\)](#).

Four examples of vulnerability exploits:

- an attacker finds and uses an overflow weakness to install malware to export sensitive data;
- an attacker convinces a user to open an email message with attached malware;
- an insider copies a hardened, encrypted program onto a thumb drive and cracks it at home;
- a flood damages one's computer systems installed at ground floor.

8.10.1 Software vulnerabilities

Common types of software flaws that lead to vulnerabilities include:

- Memory safety violations, such as:
 - Buffer overflows and over-reads
 - Dangling pointers
- Input validation errors, such as:
 - Format string attacks
 - SQL injection
 - Code injection
 - E-mail injection
 - Directory traversal
 - Cross-site scripting in web applications
 - HTTP header injection
 - HTTP response splitting
- Race conditions, such as:
 - Time-of-check-to-time-of-use bugs
 - Symlink races
- Privilege-confusion bugs, such as:
 - Cross-site request forgery in web applications
 - Clickjacking
 - FTP bounce attack
- Privilege escalation
- User interface failures, such as:
 - Warning fatigue^{*}[33] or user conditioning.
 - Blaming the Victim Prompting a user to make a security decision without giving the user enough information to answer it^{*}[34]
 - Race Conditions^{*}[35]^{*}[36]

- Side-channel attack
 - Timing attack

Some set of coding guidelines have been developed and a large number of static code analysers has been used to verify that the code follows the guidelines.

8.11 See also

- Browser security
- Computer emergency response team
- Information security
- Internet security
- Mobile security
- Vulnerability scanner

8.12 References

- [1] "The Three Tenets of Cyber Security" . U.S. Air Force Software Protection Initiative. Retrieved 2009-12-15.
- [2] Foreman, P: *Vulnerability Management*, page 1. Taylor & Francis Group, 2010. ISBN 978-1-4398-0150-5
- [3] <https://www.law.cornell.edu/uscode/text/18/part-I/chapter-113B>
- [4] ISO/IEC, "Information technology -- Security techniques-Information security risk management"ISO/IEC FIDIS 27005:2008
- [5] British Standard Institute, Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management BS ISO/IEC 13335-1-2004
- [6] Internet Engineering Task Force RFC 2828 Internet Security Glossary
- [7] CNSS Instruction No. 4009 dated 26 April 2010
- [8] "FISMAPedia" . fismapedia.org.
- [9] "Term:Vulnerability". fismapedia.org.
- [10] NIST SP 800-30 Risk Management Guide for Information Technology Systems
- [11] "Glossary" . europa.eu.
- [12] Technical Standard Risk Taxonomy ISBN 1-931624-77-1 Document Number: C081 Published by The Open Group, January 2009.
- [13] "An Introduction to Factor Analysis of Information Risk (FAIR)", Risk Management Insight LLC, November 2006;
- [14] Matt Bishop and Dave Bailey. A Critical Analysis of Vulnerability Taxonomies. Technical Report CSE-96-11, Department of Computer Science at the University of California at Davis, September 1996
- [15] Schou, Corey (1996). Handbook of INFOSEC Terms, Version 2.0. CD-ROM (Idaho State University & Information Systems Security Organization)
- [16] NIATEC Glossary
- [17] ISACA THE RISK IT FRAMEWORK (registration required) Archived July 5, 2010, at the Wayback Machine.
- [18] Wright, Joe; Harmening, Jim (2009). "15" . In Vacca, John. *Computer and Information Security Handbook*. Morgan Kaufmann Publications. Elsevier Inc. p. 257. ISBN 978-0-12-374354-1.

- [19] Kakareka, Almantas (2009). “23” . In Vacca, John. *Computer and Information Security Handbook*. Morgan Kaufmann Publications. Elsevier Inc. p. 393. ISBN 978-0-12-374354-1.
- [20] Krsul, Ivan (April 15, 1997). “Technical Report CSD-TR-97-026” . The COAST Laboratory Department of Computer Sciences, Purdue University. CiteSeerX 10.1.1.26.5435 ⓘ.
- [21] Pauli, Darren (16 January 2017). “Just give up: 123456 is still the world's most popular password” . *The Register*. Retrieved 2017-01-17.
- [22] “The Six Dumbest Ideas in Computer Security” . *ranum.com*.
- [23] “The Web Application Security Consortium / Web Application Security Statistics” . *webappsec.org*.
- [24] Ross Anderson. Why Cryptosystems Fail. Technical report, University Computer Laboratory, Cambridge, January 1994.
- [25] Neil Schlager. When Technology Fails: Significant Technological Disasters, Accidents, and Failures of the Twentieth Century. Gale Research Inc., 1994.
- [26] Hacking: The Art of Exploitation Second Edition
- [27] Kiountouzis, E. A.; Kokolakis, S. A. *Information systems security: facing the information society of the 21st century*. London: Chapman & Hall, Ltd. ISBN 0-412-78120-4.
- [28] Bavisi, Sanjay (2009). “22” . In Vacca, John. *Computer and Information Security Handbook*. Morgan Kaufmann Publications. Elsevier Inc. p. 375. ISBN 978-0-12-374354-1.
- [29] “The new era of vulnerability disclosure - a brief chat with HD Moore” . *The Tech Herald*.
- [30] “Browse - Content - SecurityStreet” . *rapid7.com*.
- [31] Betz, Chris (11 Jan 2015). “A Call for Better Coordinated Vulnerability Disclosure - MSRC - Site Home - TechNet Blogs” . *blogs.technet.com*. Retrieved 12 January 2015.
- [32] "Category:Vulnerability". *owasp.org*.
- [33] “Warning Fatigue” . *freedom-to-tinker.com*.
- [34] Archived October 21, 2007, at the Wayback Machine.
- [35] “Jesse Ruderman » Race conditions in security dialogs” . *squarefree.com*.
- [36] “lcamtuf’s blog” . *lcamtuf.blogspot.com*.

8.13 External links

- Security advisories links from the Open Directory http://www.dmoz.org/Computers/Security/Advisories_and_Patches/

Chapter 9

Eavesdropping



Cardinals eavesdropping in the Vatican. A painting by Henri Adolphe Laissement, 1895

Eavesdropping is secretly listening to the private conversation of others without their consent, as defined by *Black's Law Dictionary*.^{* [1]} The practice is commonly believed to be unethical.

9.1 Etymology

The verb *eavesdrop* is a back-formation from the noun *eavesdropper* (“a person who eavesdrops”), which was formed from the unrelated noun *eavesdrop* (“the dripping of water from the eaves of a house; the ground on which such water falls”).

An eavesdropper was someone who stands at the eavesdrop (where the water drops, i.e., next to the house) so as to hear what is said within. The PBS documentaries, *Inside the Court of Henry VIII* (April 8, 2015)^{* [2]} and *Secrets of*



"Belly-buster" hand-crank audio drill, used during the late 1950s and early 1960s to drill holes into masonry for implanting audio devices

Henry VIII's Palace (June 30, 2013) include segments that display and discuss "eavedrops", carved wooden figures Henry VIII had built into the eaves (overhanging edges of the beams in the ceiling) of **Hampton Court** to discourage unwanted gossip or dissension from the King's wishes and rule, to foment paranoia and fear,^{*[3]} and demonstrate that everything said there was being overheard; literally, that the walls had ears.^{*[4]}

9.2 Techniques

Eavesdropping can also be done over **telephone** lines, **email**, and other methods of **instant messaging** considered private. (If a message is broadcast, it is not considered eavesdropping.) **VoIP** communications software is also vulnerable to electronic eavesdropping via infections such as **trojans**.

9.3 Network attacks

Network eavesdropping is a network layer attack that focuses on capturing small *packets* from the network transmitted by other computers and reading the data content in search of any type of information. This type of network attack is generally one of the most effective as a lack of encryption services are used. It is also linked to the collection of metadata. Those who perform this type of attack are generally black hat hackers; however, government agencies, such as the National Security Agency, have also been connected.

9.4 See also

- Computer surveillance
- ECHELON
- Espionage
- Fiber tapping
- *Katz v. United States* (1967)
- Keystroke logging

- Magic (cryptography)
- Man-in-the-middle attack
- Mass surveillance
- NSA warrantless surveillance controversy (December 2005 – 2006)
- Opportunistic encryption
- People watching
- Privacy
- Secure communication
- Surveillance
- Telephone tapping
- Ultra
- United States eavesdropping

9.5 References

- [1] Garner, p. 550
- [2] *Inside the Court of Henry VIII*. Public Broadcasting Service. April 8, 2016.
- [3] *Inside the Court of Henry VIII*. Public Broadcasting Service. April 8, 2016.
- [4] Stollznow, Karen (August 7, 2014). “Eavesdropping: etymology, meaning, and some creepy little statues” . *KarenStollznow.com*.

9.6 External links

- The dictionary definition of [eavesdropping](#) at Wiktionary
- Media related to [Eavesdropping](#) at Wikimedia Commons

Chapter 10

Exploit (computer security)

An **exploit** (from the English verb *to exploit*, meaning “to use something to one’s own advantage”) is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a **bug** or **vulnerability** to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized). Such behavior frequently includes things like gaining control of a computer system, allowing **privilege escalation**, or a **denial-of-service** (DoS or related DDoS) attack.

10.1 Classification

There are several methods of classifying exploits. The most common is by how the exploit contacts the vulnerable software. A *remote exploit**[1] works over a network and exploits the security vulnerability without any prior access to the vulnerable system.

A *local exploit**[2] requires prior access to the vulnerable system and usually increases the privileges of the person running the exploit past those granted by the system administrator. Exploits against client applications also exist, usually consisting of modified servers that send an exploit if accessed with a client application.

Exploits against client applications may also require some interaction with the user and thus may be used in combination with the social engineering method. Another classification is by the action against the vulnerable system; unauthorized data access, arbitrary code execution, and denial of service are examples.

Many exploits are designed to provide superuser-level access to a computer system. However, it is also possible to use several exploits, first to gain low-level access, then to escalate privileges repeatedly until one reaches the highest administrative level (often called “root”).

After an exploit is made known to the authors of the affected software, the vulnerability is often fixed through a patch and the exploit becomes unusable. That is the reason why some **black hat hackers** as well as military or intelligence agencies hackers do not publish their exploits but keep them private.

Exploits unknown to everyone but the people that found and developed them are referred to as *zero day exploits*.

10.1.1 Types

Exploits are commonly categorized and named*[3]*[4] by the type of vulnerability they exploit (see vulnerabilities for a list), whether they are local/remote and the result of running the exploit (e.g. EoP, DoS, spoofing).

10.1.2 Pivoting

Pivoting refers to a method used by penetration testers that uses the compromised system to attack other systems on the same network to avoid restrictions such as **firewall** configurations, which may prohibit direct access to all machines. For example, if an attacker compromises a web server on a corporate network, the attacker can then use the compromised web server to attack other systems on the network. These types of attacks are often called multi-layered attacks. Pivoting is also known as *island hopping*.

Pivoting can further be distinguished into proxy pivoting and **VPN** pivoting. **Proxy pivoting** generally describes the practice of channeling traffic through a compromised target using a proxy payload on the machine and launching attacks from the computer.*[5] This type of pivoting is restricted to certain **TCP** and **UDP** ports that are supported by the proxy.

VPN pivoting enables the attacker to create an encrypted layer to tunnel into the compromised machine to route any network traffic through that target machine, for example, to run a vulnerability scan on the internal network through the compromised machine, effectively giving the attacker full network access as if they were behind the firewall.

Typically, the proxy or VPN applications enabling pivoting are executed on the target computer as the **payload** (software) of an exploit.

Pivoting is usually done by infiltrating a part of a network infrastructure (as an example, a vulnerable printer or thermostat) and using a scanner to find other devices connected to attack them. By attacking a vulnerable piece of networking, an attacker could infect most or all of a network and gain complete control.

10.2 See also

- Computer security
- Computer virus
- Crimeware
- Exploit kit
- *Hacking: The Art of Exploitation* (second edition)
- IT risk
- Metasploit
- Shellcode
- w3af

10.3 Notes

- [1] “Remote Exploits - Exploit Database” . www.exploit-db.com.
- [2] “Privilege Escalation and Local Exploits - Exploit Database” . www.exploit-db.com.
- [3] “Exploits Database by Offensive Security” . www.exploit-db.com.
- [4] “Exploit Database | Rapid7” . www.rapid7.com.
- [5] “Metasploit Basics – Part 3: Pivoting and Interfaces” . *Digital Bond*.

10.4 References

- Kahsari Alhadi, Milad. Metasploit Penetration Tester's Guide, ISBN 978-600-7026-62-5.

Chapter 11

Trojan horse (computing)

For other uses, see Trojan horse (disambiguation).

In computing, **Trojan horse**, or **Trojan**, is any malicious computer program which misleads users of its true intent. The term is derived from the Ancient Greek story of the deceptive wooden horse that led to the fall of the city of Troy.^{*[1]*[2]*[3]*[4]*[5]}

Trojans are generally spread by some form of social engineering, for example where a user is duped into executing an e-mail attachment disguised to be unsuspicious, (e.g., a routine form to be filled in), or by drive-by download. Although their payload can be anything, many modern forms act as a backdoor, contacting a controller which can then have unauthorized access to the affected computer.^{*[6]} Trojans may allow an attacker to access users' personal information such as banking information, passwords, or personal identity (IP address). Ransomware attacks are often carried out using a Trojan.

Unlike computer viruses and worms, Trojans generally do not attempt to inject themselves into other files or otherwise propagate themselves.^{*[7]}

11.1 Destructive

- Crashing the computer or device.
- Modification or deletion of files; even critical system files may be affected.
- Data corruption.
- Block any anti-virus program.
- Block any installation process.
- Formatting disks, destroying all contents.
- Spreading malware across the network.
- Spying on user activities and access sensitive information.
- Any security Can be breached with these Infections.

11.2 Use of resources or identity

- Use of the machine as part of a botnet (e.g. to perform automated spamming or to distribute Denial-of-service attacks)
- Using computer resources for mining cryptocurrencies
- Using the infected computer as proxy for illegal activities and/or attacks on other computers.
- Infecting other connected devices on the network.

11.3 Money theft, ransom

- Electronic money theft
- Installing ransomware such as CryptoLocker

11.4 Data theft

- Data theft, including for industrial espionage
- User passwords or payment card information
- User personally identifiable information
- Trade secrets

11.5 Spying, surveillance or stalking

- Keystroke logging
- Watching the user's screen
- Viewing the user's webcam
- Controlling the computer system remotely

11.6 Operation of a Trojan horse

If installed or run with elevated privileges a Trojan will generally have unlimited access. What it does with this power depends on the motives of the attacker.

Trojan horses in this way may require interaction with a malicious controller (not necessarily distributing the Trojan horse) to fulfill their purpose. It is possible for those involved with Trojans to scan computers on a network to locate any with a Trojan horse installed, which the hacker can then control. *[8]

Some Trojans take advantage of a security flaw in older versions of Internet Explorer and Google Chrome to use the host computer as an anonymizer proxy to effectively hide Internet usage,*[9] enabling the controller to use the Internet for illegal purposes while all potentially incriminating evidence indicates the infected computer or its IP address. The host's computer may or may not show the internet history of the sites viewed using the computer as a proxy. The first generation of anonymizer Trojan horses tended to leave their tracks in the page view histories of the host computer. Later generations of the Trojan horse tend to “cover” their tracks more efficiently. Several versions of Sub7 have been widely circulated in the US and Europe and became the most widely distributed examples of this type of Trojan horse.*[8]

In German-speaking countries, spyware used or made by the government is sometimes called *govware*. Govware is typically a trojan horse software used to intercept communications from the target computer. Some countries like Switzerland and Germany have a legal framework governing the use of such software.*[10]*[11] Examples of govware trojans include the Swiss MiniPanzer and MegaPanzer*[12] and the German “state trojan” nicknamed R2D2.*[10]

Due to the popularity of botnets among hackers and the availability of advertising services that permit authors to violate their users' privacy, Trojan horses are becoming more common. According to a survey conducted by BitDefender from January to June 2009, “Trojan-type malware is on the rise, accounting for 83-percent of the global malware detected in the world.” Trojans have a relationship with worms, as they spread with the help given by worms and travel across the internet with them.*[13] BitDefender has stated that approximately 15% of computers are members of a botnet, usually recruited by a Trojan infection.*[14]

11.7 Notable examples

11.7.1 Private and governmental

- FinFisher – Lench IT solutions / Gamma International
- DaVinci / Galileo RCS – HT S.r.l. (*hacking team*)
- 0zapftis / r2d2 StaatsTrojaner – DigiTask
- TAO QUANTUM/FOXACID – NSA
- Magic Lantern – FBI
- WARRIOR PRIDE – GCHQ

11.7.2 Publicly available

- Netbus – 1998 (published)
- Sub7 by Mobman – 1999 (published)
- Back Orifice – 1998 (published)
- Beast – 2002 (published)
- Bifrost Trojan – 2004 (published)
- DarkComet – 2008 (published)
- Blackhole exploit kit – 2012 (published)
- Gh0st RAT – 2009 (published)
- MegaPanzer BundesTrojaner – 2009 (published)^{*}[15]^{*}[16]

11.7.3 Detected by security researchers

- Clickbot.A – 2006 (discovered)
- Zeus – 2007 (discovered)
- Flashback Trojan – 2011 (discovered)
- ZeroAccess – 2011 (discovered)
- Koobface – 2008 (discovered)
- Vundo – 2009 (discovered)
- Meredrop – 2010 (discovered)
- Coreflood – 2010 (discovered)
- Tiny Banker Trojan – 2012 (discovered)
- Shedun Android malware – 2015 (discovered) ^{*}[17]^{*}[18]^{*}[19]^{*}[20]^{*}[21]^{*}[22]

11.8 See also

- Botnet
- Computer security
- Remote administration
- Remote administration software
- Cyber spying
- Dancing pigs
- Exploit (computer security)
- Industrial espionage
- Malware
- Principle of least privilege
- Privacy-invasive software
- Reverse connection
- Rogue security software
- Timeline of computer viruses and worms
- Zombie (computer science)

11.9 References

- Carnegie Mellon University (1999): “CERT Advisory CA-1999-02 Trojan Horses” , ЎЦ
- [1] Landwehr, C. E; A. R Bull; J. P McDermott; W. S Choi (1993). *A taxonomy of computer program security flaws, with examples*. DTIC Document. Retrieved 2012-04-05.
- [2] “Trojan Horse Definition” . Retrieved 2012-04-05.
- [3] “Trojan horse” . *Webopedia*. Retrieved 2012-04-05.
- [4] “What is Trojan horse? – Definition from Whatis.com” . Retrieved 2012-04-05.
- [5] “Trojan Horse: [coined By MIT-hacker-turned-NSA-spook Dan Edwards] N.” . Retrieved 2012-04-05.
- [6] “What is the difference between viruses, worms, and Trojans?”. Symantec Corporation. Retrieved 2009-01-10.
- [7] “VIRUS-L/comp.virus Frequently Asked Questions (FAQ) v2.00 (Question B3: What is a Trojan Horse?)”. 9 October 1995. Retrieved 2012-09-13.
- [8] Jamie Crapanzano (2003): “Deconstructing SubSeven, the Trojan Horse of Choice” , SANS Institute, Retrieved on 2009-06-11
- [9] Vincentas (11 July 2013). “Trojan Horse in SpyWareLoop.com” . Spyware Loop. Retrieved 28 July 2013.
- [10] Basil Cupa, Trojan Horse Resurrected: On the Legality of the Use of Government Spyware (Govware), LISS 2013, pp. 419–428
- [11] “Dokument nicht gefunden!”. Federal Department of Justice and Police. Archived from the original on May 6, 2013.
- [12] “Swiss coder publicises government spy Trojan – Techworld.com” . News.techworld.com. Retrieved 2014-01-26.
- [13] BitDefender.com Malware and Spam Survey
- [14] Datta, Ganesh. “What are Trojans?”. *SecurAid*.

- [15] “Mega-Panzer” .
- [16] “Mini-Panzer” .
- [17] “Trojanized adware family abuses accessibility service to install whatever apps it wants - Lookout Blog” .
- [18] “Shedun trojan adware is hitting the Android Accessibility Service - TheINQUIRER” .
- [19] “Lookout discovers new trojanized adware; 20K popular apps caught in the crossfire - Lookout Blog” .
- [20] “Shuanet, ShiftyBug and Shedun malware could auto-root your Android” . 5 November 2015.
- [21] Times, Tech (9 November 2015). “New Family Of Android Malware Virtually Impossible To Remove: Say Hello To Shedun, Shuanet And ShiftyBug” .
- [22] “Android adware can install itself even when users explicitly reject it” .

11.10 External links

- Trojan Horses at DMOZ

Chapter 12

Computer virus

Not to be confused with computer worm or Trojan horse (computing).

0 00 00-6D 73 62 6C	msbl
0 6A 75-73 74 20 77	ast.exe I just w
9 20 4C-4F 56 45 20	ant to say LOUE
0 62 69-6C 6C 79 20	YOU SAN!! billy
0 64 6F-20 79 6F 75	gates why do you
3 20 70-6F 73 73 69	make this possi
0 20 6D-61 6B 69 6E	ble ? Stop makin
E 64 20-66 69 78 20	g money and fix
7 61 72-65 21 21 00	your software!!
0 00 00-7F 00 00 00	♣ ♦► H ▲
0 00 00-01 00 01 00	♦_♦_ Q Q Q
0 00 00-00 00 00 46	á@ L F
C C9 11-9F E8 08 00	♦]êèù-ñ◀fp♦
0 00 03-10 00 00 00	►H`@ ♣ ♦►
3 00 00-01 00 04 00	p@ ð ♦ Q ♦

Hex dump of the Blaster worm, showing a message left for Microsoft co-founder Bill Gates by the worm's programmer

A **computer virus** is a type of malicious software program ("malware") that, when executed, replicates itself by modifying other computer programs and inserting its own code.*[1] Infected computer programs can include, as well, data files, or the "boot" sector of the hard drive. When this replication succeeds, the affected areas are then said to be "infected" with a computer virus.*[2]*[3]*[4]

Virus writers use social engineering deceptions and exploit detailed knowledge of security vulnerabilities to initially infect systems and to spread the virus. The vast majority of viruses target systems running Microsoft Windows,*[5]*[6]*[7] employing a variety of mechanisms to infect new hosts,*[8] and often using complex anti-detection/stealth strategies to evade antivirus software.*[9]*[10]*[11]*[12] Motives for creating viruses can include seeking profit (e.g., with ransomware), desire to send a political message, personal amusement, to demonstrate that a vulnerability exists in software, for sabotage and denial of service, or simply because they wish to explore cybersecurity issues, artificial life and evolutionary algorithms.*[13]

Computer viruses currently cause billions of dollars' worth of economic damage each year,*[14] due to causing system failure, wasting computer resources, corrupting data, increasing maintenance costs, etc. In response, free, open-source antivirus tools have been developed, and an industry of antivirus software has cropped up, selling or freely

distributing virus protection to users of various operating systems.* [15] As of 2005, even though no currently existing antivirus software was able to uncover all computer viruses (especially new ones), computer security researchers are actively searching for new ways to enable antivirus solutions to more effectively detect emerging viruses, before they have already become widely distributed.* [16]

The term “virus” is also commonly, but erroneously, used to refer to other types of malware. “Malware” encompasses computer viruses along with many other forms of malicious software, such as computer “worms”, ransomware, trojan horses, keyloggers, rootkits, spyware, adware, malicious Browser Helper Object (BHOs) and other malicious software. The majority of active malware threats are actually trojan horse programs or computer worms rather than computer viruses. The term computer virus, coined by Fred Cohen in 1985, is a misnomer.* [17] Viruses often perform some type of harmful activity on infected host computers, such as acquisition of hard disk space or central processing unit (CPU) time, accessing private information (e.g., credit card numbers), corrupting data, displaying political or humorous messages on the user's screen, spamming their e-mail contacts, logging their keystrokes, or even rendering the computer useless. However, not all viruses carry a destructive “payload” and attempt to hide themselves—the defining characteristic of viruses is that they are self-replicating computer programs which modify other software without user consent.

12.1 Historical development

See also: Timeline of notable computer viruses and worms

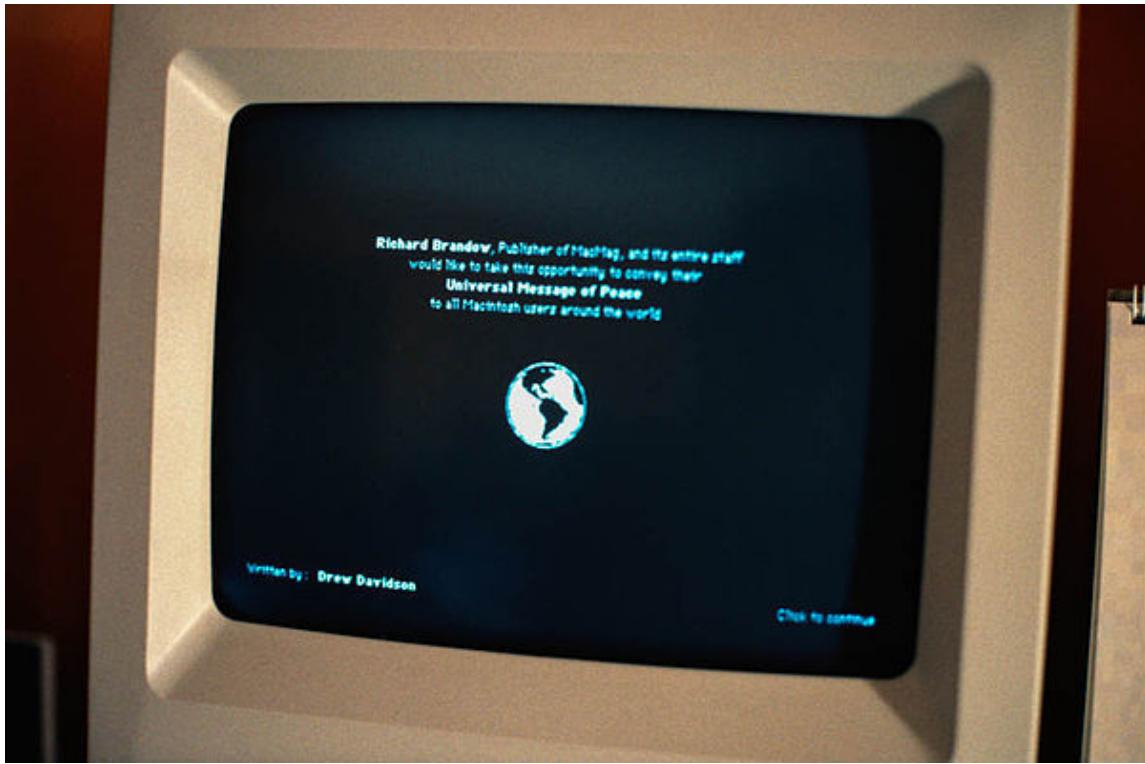
12.1.1 Early academic work on self-replicating programs

The first academic work on the theory of self-replicating computer programs* [18] was done in 1949 by John von Neumann who gave lectures at the University of Illinois about the “Theory and Organization of Complicated Automata”. The work of von Neumann was later published as the “Theory of self-reproducing automata”. In his essay von Neumann described how a computer program could be designed to reproduce itself.* [19] Von Neumann's design for a self-reproducing computer program is considered the world's first computer virus, and he is considered to be the theoretical “father” of computer virology.* [20] In 1972, Veith Risak, directly building on von Neumann's work on self-replication, published his article “Selbstreproduzierende Automaten mit minimaler Informationsübertragung” (Self-reproducing automata with minimal information exchange).* [21] The article describes a fully functional virus written in assembler programming language for a SIEMENS 4004/35 computer system. In 1980 Jürgen Kraus wrote his diplom thesis “Selbstreproduktion bei Programmen” (Self-reproduction of programs) at the University of Dortmund.* [22] In his work Kraus postulated that computer programs can behave in a way similar to biological viruses.

12.1.2 First examples

The Creeper virus was first detected on ARPANET, the forerunner of the Internet, in the early 1970s.* [23] Creeper was an experimental self-replicating program written by Bob Thomas at BBN Technologies in 1971.* [24] Creeper used the ARPANET to infect DEC PDP-10 computers running the TENEX operating system.* [25] Creeper gained access via the ARPANET and copied itself to the remote system where the message, “I'm the creeper, catch me if you can!” was displayed. The Reaper program was created to delete Creeper.* [26] In fiction, the 1973 Michael Crichton sci-fi movie *Westworld* made an early mention of the concept of a computer virus, being a central plot theme that causes androids to run amok.* [27] Alan Oppenheimer's character summarizes the problem by stating that "...there's a clear pattern here which suggests an analogy to an infectious disease process, spreading from one...area to the next.” To which the replies are stated: “Perhaps there are superficial similarities to disease” and, “I must confess I find it difficult to believe in a disease of machinery.”* [28] (Crichton's earlier work, the 1969 novel *The Andromeda Strain* and 1971 film version of it were about a biological virus-like disease that threatened the human race.)

In 1982, a program called "Elk Cloner" was the first personal computer virus to appear “in the wild”—that is, outside the single computer or [computer] lab where it was created.* [29] Written in 1981 by Richard Skrenta while in the ninth grade at Mount Lebanon High School near Pittsburgh, it attached itself to the Apple DOS 3.3 operating system and spread via floppy disk.* [29]* [30] This virus, created as a practical joke when Skrenta was still in high school, was



The MacMag virus 'Universal Peace', as displayed on a Mac in March 1988

injected in a game on a floppy disk. On its 50th use the Elk Cloner virus would be activated, infecting the personal computer and displaying a short poem beginning “Elk Cloner: The program with a personality.” In 1984 Fred Cohen from the University of Southern California wrote his paper “Computer Viruses – Theory and Experiments”.* [31] It was the first paper to explicitly call a self-reproducing program a “virus”, a term introduced by Cohen’s mentor Leonard Adleman. In 1987, Fred Cohen published a demonstration that there is no algorithm that can perfectly detect all possible viruses.* [32] Fred Cohen’s theoretical compression virus* [33] was an example of a virus which was not malicious software (malware), but was putatively benevolent (well-intentioned). However, antivirus professionals do not accept the concept of “benevolent viruses”, as any desired function can be implemented without involving a virus (automatic compression, for instance, is available under the Windows operating system at the choice of the user). Any virus will by definition make unauthorised changes to a computer, which is undesirable even if no damage is done or intended. On page one of *Dr Solomon’s Virus Encyclopaedia*, the undesirability of viruses, even those that do nothing but reproduce, is thoroughly explained.* [34]

An article that describes “useful virus functionalities” was published by J. B. Gunn under the title “Use of virus functions to provide a virtual APL interpreter under user control” in 1984.* [35] The first IBM PC virus in the “wild” was a boot sector virus dubbed (c)Brain,* [36] created in 1986 by the Farooq Alvi Brothers in Lahore, Pakistan, reportedly to deter unauthorized copying of the software they had written.* [37] The first virus to specifically target Microsoft Windows, WinVir was discovered in April 1992, two years after the release of Windows 3.0.* [38] The virus did not contain any Windows API calls, instead relying on DOS interrupts. A few years later, in February 1996, Australian hackers from the virus-writing crew VLAD created the Bizatch virus (also known as “Boza” virus), which was the first known virus to target Windows 95. In late 1997 the encrypted, memory-resident stealth virus Win32.Cabanas was released—the first known virus that targeted Windows NT (it was also able to infect Windows 3.0 and Windows 9x hosts).* [39]

Even home computers were affected by viruses. The first one to appear on the Commodore Amiga was a boot sector virus called SCA virus, which was detected in November 1987.* [40] The first social networking virus, Win32.5-0-1, was created by Matt Larose on August 15, 2001.* [41] The virus specifically targeted users of MSN Messenger and online bulletin boards. Users would be required to click on a link to activate the virus, which would then send an email containing user data to an anonymous email address, which was later found to be owned by Larose. Data sent would contain items such as user IP address and email addresses, contacts, website browsing history, and commonly used phrases. In 2008, larger websites used part of the Win32.5-0-1 code to track web users advertising-related interests.

12.2 Operations and functions

12.2.1 Parts

A viable computer virus must contain a **search routine**, which locates new files or new disks which are worthwhile targets for infection. Secondly, every computer virus must contain a routine to copy itself into the program which the search routine locates.* [42] The three main virus parts are:

Infection mechanism

Infection mechanism (also called 'infection vector'), is how the virus spreads or propagates. A virus typically has a search routine, which locates new files or new disks for infection.* [43]

Trigger

The trigger, which is also known as logic bomb, is the **compiled version** that could be activated any time an **executable file** with the virus is run that determines the event or condition for the malicious "**payload**" to be activated or delivered* [44] such as a particular date, a particular time, particular presence of another program, capacity of the disk exceeding some limit,* [45] or a double-click that opens a particular file.* [46]

Payload

The "**payload**" is the actual body or data that perform the actual malicious purpose of the virus. Payload activity might be noticeable (e.g., because it causes the system to slow down or "freeze"), as most of the time the "**payload**" itself is the harmful activity,* [43] or some times non-destructive but distributive, which is called **Virus hoax**.* [47]

12.2.2 Phases

Virus phases is the **life cycle** of the computer virus, described by using an analogy to **biology**. This life cycle can be divided into four phases:

Dormant phase

The virus program is idle during this stage. The virus program has managed to access the target user's computer or software, but during this stage, the virus does not take any action. The virus will eventually be activated by the "trigger" which states which event will execute the virus, such as a date, the presence of another program or file, the capacity of the disk exceeding some limit or the user taking a certain action (e.g., double-clicking on a certain icon, opening an e-mail, etc.). Not all viruses have this stage.* [43]

Propagation phase

The virus starts propagating, that is multiplying and replicating itself. The virus places a copy of itself into other programs or into certain system areas on the disk. The copy may not be identical to the propagating version; viruses often "morph" or change to evade detection by IT professionals and anti-virus software. Each infected program will now contain a **clone** of the virus, which will itself enter a propagation phase.* [43]

Triggering phase

A dormant virus moves into this phase when it is activated, and will now perform the function for which it was intended. The triggering phase can be caused by a variety of system events, including a count of the number of times that this copy of the virus has made copies of itself.* [43]

Execution phase

This is the actual work of the virus, where the “payload” will be released. It can be destructive such as deleting files on disk, crashing the system, or corrupting files or relatively harmless such as popping up humorous or political messages on screen.*[43]

12.3 Infection targets and replication techniques

Computer viruses infect a variety of different subsystems on their host computers and software.*[48] One manner of classifying viruses is to analyze whether they reside in **binary executables** (such as **.EXE** or **.COM** files), data files (such as **Microsoft Word** documents or **PDF** files), or in the **boot sector** of the host's **hard drive** (or some combination of all of these).*[49]*[50]

12.3.1 Resident vs. non-resident viruses

A *memory-resident virus* (or simply “resident virus”) installs itself as part of the **operating system** when executed, after which it remains in **RAM** from the time the computer is booted up to when it is shut down. Resident viruses overwrite **interrupt handling** code or other **functions**, and when the operating system attempts to access the target file or disk sector, the virus code intercepts the request and redirects the **control flow** to the replication module, infecting the target. In contrast, a *non-memory-resident virus* (or “non-resident virus”), when executed, scans the disk for targets, infects them, and then exits (i.e. it does not remain in memory after it is done executing).*[51]*[52]*[53]

12.3.2 Macro viruses

Many common applications, such as **Microsoft Outlook** and **Microsoft Word**, allow **macro programs** to be embedded in documents or emails, so that the programs may be run automatically when the document is opened. A *macro virus* (or “document virus”) is a virus that is written in a **macro language**, and embedded into these documents so that when users open the file, the virus code is executed, and can infect the user's computer. This is one of the reasons that it is dangerous to open unexpected or suspicious **attachments** in e-mails.*[54]*[55] While not opening attachments in e-mails from unknown persons or organizations can help to reduce the likelihood of contracting a virus, in some cases, the virus is designed so that the e-mail appears to be from a reputable organization (e.g., a major bank or credit card company).

12.3.3 Boot sector viruses

Boot sector viruses specifically target the **boot sector** and/or the **Master Boot Record***[56] (MBR) of the host's **hard drive** or removable storage media (flash drives, floppy disks, etc.).*[49]*[57]*[58]

12.3.4 Email virus

Email virus – A virus that specifically, rather than accidentally, uses the email system to spread. While virus infected files may be accidentally sent as **email attachments**, email viruses are aware of email system functions. They generally target a specific type of email system (Microsoft's Outlook is the most commonly used), harvest email addresses from various sources, and may append copies of themselves to all email sent, or may generate email messages containing copies of themselves as attachments.*[59]

12.4 Stealth strategies

In order to avoid detection by users, some viruses employ different kinds of **deception**. Some old viruses, especially on the **MS-DOS** platform, make sure that the “last modified” date of a host file stays the same when the file is infected by the virus. This approach does not fool antivirus software, however, especially those which maintain and date **cyclic redundancy checks** on file changes.*[60] Some viruses can infect files without increasing their sizes or

damaging the files. They accomplish this by overwriting unused areas of executable files. These are called *cavity viruses*. For example, the CIH virus, or Chernobyl Virus, infects Portable Executable files. Because those files have many empty gaps, the virus, which was 1 KB in length, did not add to the size of the file.*[61] Some viruses try to avoid detection by killing the tasks associated with antivirus software before it can detect them (for example, Conficker). In the 2010s, as computers and operating systems grow larger and more complex, old hiding techniques need to be updated or replaced. Defending a computer against viruses may demand that a file system migrate towards detailed and explicit permission for every kind of file access.*[62]

12.4.1 Read request intercepts

While some antivirus software employ various techniques to counter stealth mechanisms, once the infection occurs any recourse to “clean” the system is unreliable. In Microsoft Windows operating systems, the NTFS file system is proprietary. This leaves antivirus software little alternative but to send a “read” request to Windows OS files that handle such requests. Some viruses trick antivirus software by intercepting its requests to the Operating system (OS). A virus can hide by intercepting the request to read the infected file, handling the request itself, and returning an uninfected version of the file to the antivirus software. The interception can occur by code injection of the actual operating system files that would handle the read request. Thus, an antivirus software attempting to detect the virus will either not be given permission to read the infected file, or, the “read” request will be served with the uninfected version of the same file.*[63]

The only reliable method to avoid “stealth” viruses is to “boot” from a medium that is known to be “clean”. Security software can then be used to check the dormant operating system files. Most security software relies on virus signatures, or they employ heuristics.*[64]*[65] Security software may also use a database of file “hashes” for Windows OS files, so the security software can identify altered files, and request Windows installation media to replace them with authentic versions. In older versions of Windows, file cryptographic hash functions of Windows OS files stored in Windows—to allow file integrity/authenticity to be checked—could be overwritten so that the System File Checker would report that altered system files are authentic, so using file hashes to scan for altered files would not always guarantee finding an infection.*[66]

12.4.2 Self-modification

See also: Self-modifying code

Most modern antivirus programs try to find virus-patterns inside ordinary programs by scanning them for so-called *virus signatures*.*[67] Unfortunately, the term is misleading, in that viruses do not possess unique signatures in the way that human beings do. Such a virus “signature” is merely a sequence of bytes that an antivirus program looks for because it is known to be part of the virus. A better term would be “search strings”. Different antivirus programs will employ different search strings, and indeed different search methods, when identifying viruses. If a virus scanner finds such a pattern in a file, it will perform other checks to make sure that it has found the virus, and not merely a coincidental sequence in an innocent file, before it notifies the user that the file is infected. The user can then delete, or (in some cases) “clean” or “heal” the infected file. Some viruses employ techniques that make detection by means of signatures difficult but probably not impossible. These viruses modify their code on each infection. That is, each infected file contains a different variant of the virus.

Encrypted viruses

One method of evading signature detection is to use simple encryption to encipher (encode) the body of the virus, leaving only the encryption module and a static cryptographic key in cleartext which does not change from one infection to the next.*[68] In this case, the virus consists of a small decrypting module and an encrypted copy of the virus code. If the virus is encrypted with a different key for each infected file, the only part of the virus that remains constant is the decrypting module, which would (for example) be appended to the end. In this case, a virus scanner cannot directly detect the virus using signatures, but it can still detect the decrypting module, which still makes indirect detection of the virus possible. Since these would be symmetric keys, stored on the infected host, it is entirely possible to decrypt the final virus, but this is probably not required, since self-modifying code is such a rarity that it may be reason for virus scanners to at least “flag” the file as suspicious.*[69] An old but compact way will be the use of arithmetic operation like addition or subtraction and the use of logical conditions such as

XORing,^{*}[70] where each byte in a virus is with a constant, so that the exclusive-or operation had only to be repeated for decryption. It is suspicious for a code to modify itself, so the code to do the encryption/decryption may be part of the signature in many virus definitions.^{*}[69] A simpler older approach did not use a key, where the encryption consisted only of operations with no parameters, like incrementing and decrementing, bitwise rotation, arithmetic negation, and logical NOT.^{*}[70] Some viruses will employ a means of encryption inside an executable in which the virus is encrypted under certain events, such as the virus scanner being disabled for updates or the computer being rebooted. This is called **cryptovirology**. At said times, the executable will decrypt the virus and execute its hidden runtimes, infecting the computer and sometimes disabling the antivirus software.

Polymorphic code

Polymorphic code was the first technique that posed a serious threat to virus scanners. Just like regular encrypted viruses, a polymorphic virus infects files with an encrypted copy of itself, which is decoded by a decryption module. In the case of polymorphic viruses, however, this decryption module is also modified on each infection. A well-written polymorphic virus therefore has no parts which remain identical between infections, making it very difficult to detect directly using “signatures”.^{*}[71]^{*}[72] Antivirus software can detect it by decrypting the viruses using an emulator, or by statistical pattern analysis of the encrypted virus body. To enable polymorphic code, the virus has to have a polymorphic engine (also called “mutating engine” or “mutation engine”) somewhere in its encrypted body. See **polymorphic code** for technical detail on how such engines operate.^{*}[73]

Some viruses employ polymorphic code in a way that constrains the mutation rate of the virus significantly. For example, a virus can be programmed to mutate only slightly over time, or it can be programmed to refrain from mutating when it infects a file on a computer that already contains copies of the virus. The advantage of using such slow polymorphic code is that it makes it more difficult for antivirus professionals and investigators to obtain representative samples of the virus, because “bait” files that are infected in one run will typically contain identical or similar samples of the virus. This will make it more likely that the detection by the virus scanner will be unreliable, and that some instances of the virus may be able to avoid detection.

Metamorphic code

To avoid being detected by emulation, some viruses rewrite themselves completely each time they are to infect new executables. Viruses that utilize this technique are said to be in **metamorphic code**. To enable metamorphism, a “metamorphic engine” is needed. A metamorphic virus is usually very large and complex. For example, **W32/Simile** consisted of over 14,000 lines of **assembly language** code, 90% of which is part of the metamorphic engine.^{*}[74]^{*}[75]

12.5 Vulnerabilities and infection vectors

12.5.1 Software bugs

As software is often designed with security features to prevent unauthorized use of system resources, many viruses must exploit and manipulate **security bugs**, which are **security defects** in a system or application software, to spread themselves and infect other computers. **Software development** strategies that produce large numbers of “bugs” will generally also produce potential exploitable “holes” or “entrances” for the virus.

12.5.2 Social engineering and poor security practices

In order to replicate itself, a virus must be permitted to execute code and write to memory. For this reason, many viruses attach themselves to **executable files** that may be part of legitimate programs (see **code injection**). If a user attempts to launch an infected program, the virus' code may be executed simultaneously.^{*}[76] In operating systems that use **file extensions** to determine program associations (such as Microsoft Windows), the extensions may be hidden from the user by default. This makes it possible to create a file that is of a different type than it appears to the user. For example, an executable may be created and named “picture.png.exe”, in which the user sees only “picture.png” and therefore assumes that this file is a **digital image** and most likely is safe, yet when opened, it runs the executable on the client machine.^{*}[77]

12.5.3 Vulnerability of different operating systems

The vast majority of viruses target systems running Microsoft Windows. This is due to Microsoft's large market share of desktop computer users.*[78] The diversity of software systems on a network limits the destructive potential of viruses and malware.*[79] Open-source operating systems such as Linux allow users to choose from a variety of desktop environments, packaging tools, etc., which means that malicious code targeting any of these systems will only affect a subset of all users. Many Windows users are running the same set of applications, enabling viruses to rapidly spread among Microsoft Windows systems by targeting the same exploits on large numbers of hosts.*[5]*[6]*[7]*[80]

While Linux and Unix in general have always natively prevented normal users from making changes to the operating system environment without permission, Windows users are generally not prevented from making these changes, meaning that viruses can easily gain control of the entire system on Windows hosts. This difference has continued partly due to the widespread use of administrator accounts in contemporary versions like Windows XP. In 1997, researchers created and released a virus for Linux—known as "Bliss".*[81] Bliss, however, requires that the user run it explicitly, and it can only infect programs that the user has the access to modify. Unlike Windows users, most Unix users do not log in as an administrator, or "root user", except to install or configure software; as a result, even if a user ran the virus, it could not harm their operating system. The Bliss virus never became widespread, and remains chiefly a research curiosity. Its creator later posted the source code to Usenet, allowing researchers to see how it worked.*[82]

12.6 Countermeasures

See also: [Vulnerability to malware](#), [Anti-malware strategies](#), and [Browser hardening](#)

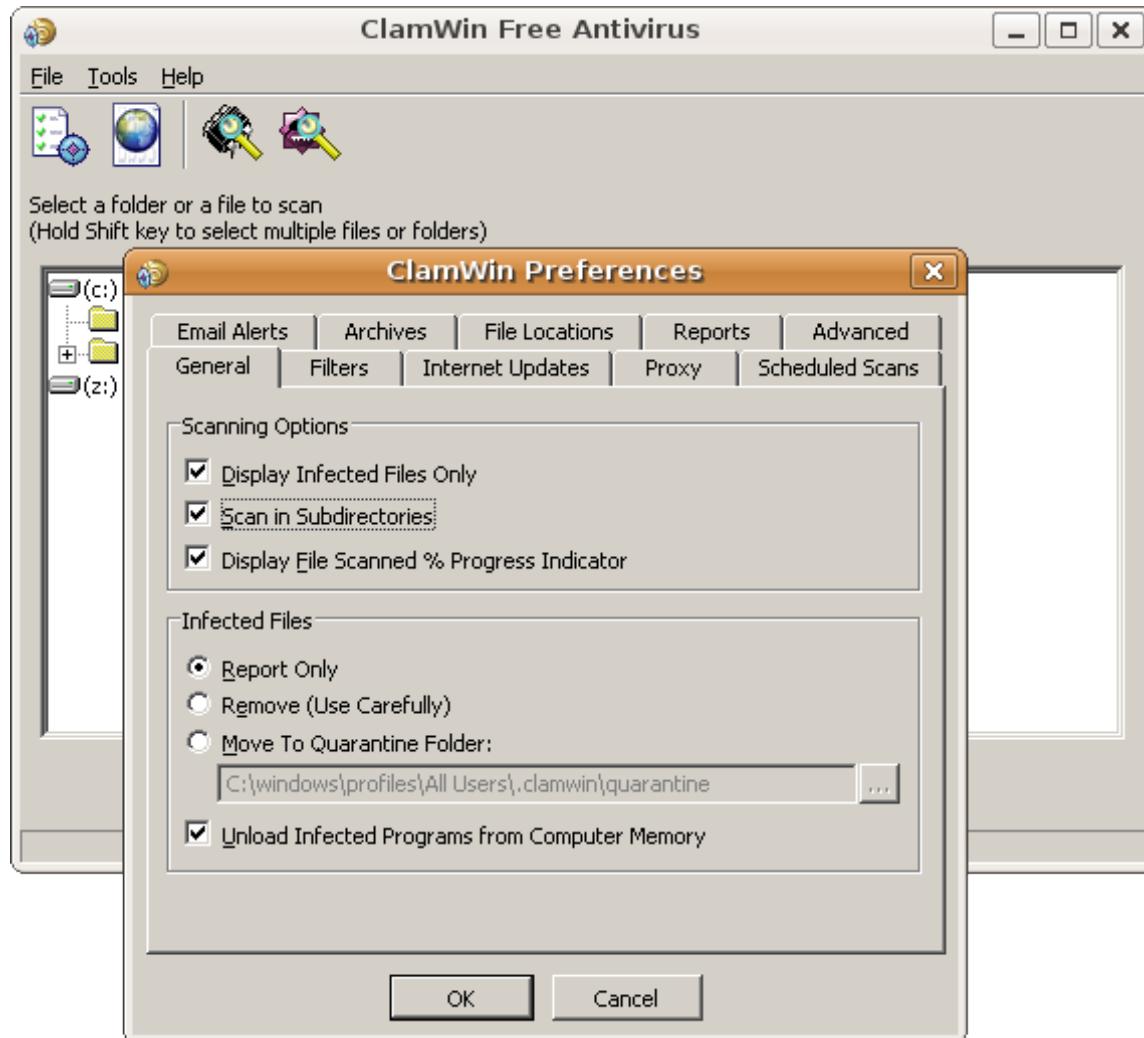
12.6.1 Antivirus software

Many users install antivirus software that can detect and eliminate known viruses when the computer attempts to download or run the executable file (which may be distributed as an email attachment, or on USB flash drives, for example). Some antivirus software blocks known malicious websites that attempt to install malware. Antivirus software does not change the underlying capability of hosts to transmit viruses. Users must update their software regularly to patch security vulnerabilities ("holes"). Antivirus software also needs to be regularly updated in order to recognize the latest threats. This is because malicious hackers and other individuals are always creating new viruses. The German AV-TEST Institute publishes evaluations of antivirus software for Windows*[\[83\]](#) and Android.*[\[84\]](#)

Examples of Microsoft Windows anti virus and anti-malware software include the optional Microsoft Security Essentials*[\[85\]](#) (for Windows XP, Vista and Windows 7) for real-time protection, the Windows Malicious Software Removal Tool*[\[86\]](#) (now included with Windows (Security) Updates on "Patch Tuesday", the second Tuesday of each month), and Windows Defender (an optional download in the case of Windows XP).*[87] Additionally, several capable antivirus software programs are available for free download from the Internet (usually restricted to non-commercial use).*[88] Some such free programs are almost as good as commercial competitors.*[\[89\]](#) Common security vulnerabilities are assigned CVE IDs and listed in the US National Vulnerability Database. Secunia PSI*[\[90\]](#) is an example of software, free for personal use, that will check a PC for vulnerable out-of-date software, and attempt to update it. Ransomware and phishing scam alerts appear as press releases on the Internet Crime Complaint Center noticeboard. Ransomware is a virus that posts a message on the user's screen saying that the screen or system will remain locked or unusable until a ransom payment is made. Phishing is a deception in which the malicious individual pretends to be a friend, computer security expert, or other benevolent individual, with the goal of convincing the targeted individual to reveal passwords or other personal information.

Other commonly used preventative measures include timely operating system updates, software updates, careful Internet browsing (avoiding shady websites), and installation of only trusted software.*[\[91\]](#) Certain browsers flag sites that have been reported to Google and that have been confirmed as hosting malware by Google.*[\[92\]](#)*[\[93\]](#)

There are two common methods that an antivirus software application uses to detect viruses, as described in the antivirus software article. The first, and by far the most common method of virus detection is using a list of virus signature definitions. This works by examining the content of the computer's memory (its Random Access Memory (RAM), and boot sectors) and the files stored on fixed or removable drives (hard drives, floppy drives, or USB flash drives), and comparing those files against a database of known virus "signatures". Virus signatures are just strings



Screenshot of the open source ClamWin antivirus software running in Wine on Ubuntu Linux

of code that are used to identify individual viruses; for each virus, the antivirus designer tries to choose a unique signature string that will not be found in a legitimate program. Different antivirus programs use different “signatures” to identify viruses. The disadvantage of this detection method is that users are only protected from viruses that are detected by signatures in their most recent virus definition update, and not protected from new viruses (see “zero-day attack”).*[94]

A second method to find viruses is to use a heuristic algorithm based on common virus behaviors. This method has the ability to detect new viruses for which antivirus security firms have yet to define a “signature”, but it also gives rise to more **false positives** than using signatures. False positives can be disruptive, especially in a commercial environment, because it may lead to a company instructing staff not to use the company computer system until IT services has checked the system for viruses. This can slow down productivity for regular workers.

12.6.2 Recovery strategies and methods

One may reduce the damage done by viruses by making regular **backups** of data (and the operating systems) on different media, that are either kept unconnected to the system (most of the time, as in a hard drive), **read-only** or not accessible for other reasons, such as using different file systems. This way, if data is lost through a virus, one can start again using the backup (which will hopefully be recent).*[95] If a backup session on optical media like CD and DVD is closed, it becomes read-only and can no longer be affected by a virus (so long as a virus or infected file was not copied onto the **CD/DVD**). Likewise, an operating system on a bootable CD can be used to start the computer if the installed operating systems become unusable. Backups on removable media must be carefully inspected before restoration. The Gammima virus, for example, propagates via removable **flash drives**.*[96]*[97]

Virus removal

Many websites run by antivirus software companies provide free online virus scanning, with limited “cleaning” facilities (after all, the purpose of the websites is to sell antivirus products and services). Some websites—like Google subsidiary **VirusTotal.com**—allow users to upload one or more suspicious files to be scanned and checked by one or more antivirus programs in one operation.*[98]*[99] Additionally, several capable antivirus software programs are available for free download from the Internet (usually restricted to non-commercial use).*[100] Microsoft offers an optional free antivirus utility called **Microsoft Security Essentials**, a **Windows Malicious Software Removal Tool** that is updated as part of the regular Windows update regime, and an older optional anti-malware (malware removal) tool **Windows Defender** that has been upgraded to an antivirus product in Windows 8.

Some viruses disable **System Restore** and other important Windows tools such as **Task Manager** and **CMD**. An example of a virus that does this is **CiaDoor**. Many such viruses can be removed by rebooting the computer, entering Windows “safe mode” with networking, and then using system tools or **Microsoft Safety Scanner**.*[101] **System Restore** on **Windows Me**, **Windows XP**, **Windows Vista** and **Windows 7** can restore the registry and critical system files to a previous checkpoint. Often a virus will cause a system to “hang” or “freeze”, and a subsequent hard reboot will render a system restore point from the same day corrupted. Restore points from previous days should work, provided the virus is not designed to corrupt the restore files and does not exist in previous restore points.*[102]*[103]

Operating system reinstallation

Microsoft's **System File Checker** (improved in Windows 7 and later) can be used to check for, and repair, corrupted system files.*[104] Restoring an earlier “clean” (virus-free) copy of the entire partition from a **cloned disk**, a **disk image**, or a **backup** copy is one solution—restoring an earlier backup disk “image” is relatively simple to do, usually removes any malware, and may be faster than “disinfecting” the computer—or reinstalling and reconfiguring the operating system and programs from scratch, as described below, then restoring user preferences.*[95] Reinstalling the operating system is another approach to virus removal. It may be possible to recover copies of essential user data by booting from a **live CD**, or connecting the hard drive to another computer and booting from the second computer's operating system, taking great care not to infect that computer by executing any infected programs on the original drive. The original hard drive can then be reformatted and the OS and all programs installed from original media. Once the system has been restored, precautions must be taken to avoid reinfection from any restored **executable files**.*[105]

12.6.3 Viruses and the Internet

See also: **Computer worm**

Before computer networks became widespread, most viruses spread on **removable media**, particularly **floppy disks**. In the early days of the **personal computer**, many users regularly exchanged information and programs on floppies. Some viruses spread by infecting programs stored on these disks, while others installed themselves into the **disk boot sector**, ensuring that they would be run when the user booted the computer from the disk, usually inadvertently. Personal computers of the era would attempt to boot first from a floppy if one had been left in the drive. Until floppy disks fell out of use, this was the most successful infection strategy and boot sector viruses were the most common in the “wild” for many years. Traditional computer viruses emerged in the 1980s, driven by the spread of personal computers and the resultant increase in **bulletin board system** (BBS), **modem** use, and software sharing. **Bulletin board**—driven software sharing contributed directly to the spread of **Trojan horse** programs, and viruses were written to infect popularly traded software. **Shareware** and **bootleg** software were equally common **vectors** for viruses on BBSs.*[106]*[107]*[108] Viruses can increase their chances of spreading to other computers by infecting files on a **network file system** or a **file system** that is accessed by other computers.*[109]

Macro viruses have become common since the mid-1990s. Most of these viruses are written in the scripting languages for Microsoft programs such as **Microsoft Word** and **Microsoft Excel** and spread throughout **Microsoft Office** by infecting documents and **spreadsheets**. Since Word and Excel were also available for **Mac OS**, most could also spread to **Macintosh computers**. Although most of these viruses did not have the ability to send infected **email messages**, those viruses which did take advantage of the **Microsoft Outlook Component Object Model** (COM) interface.*[110]*[111] Some old versions of Microsoft Word allow macros to replicate themselves with additional blank lines. If two macro viruses simultaneously infect a document, the combination of the two, if also self-replicating, can appear as a “mating” of the two and would likely be detected as a virus unique from the “parents”.*[112]

A virus may also send a web address link as an instant message to all the contacts (e.g., friends and colleagues' e-mail addresses) stored on an infected machine. If the recipient, thinking the link is from a friend (a trusted source) follows the link to the website, the virus hosted at the site may be able to infect this new computer and continue propagating.*[113] Viruses that spread using cross-site scripting were first reported in 2002,*[114] and were academically demonstrated in 2005.*[115] There have been multiple instances of the cross-site scripting viruses in the “wild”, exploiting websites such as MySpace (with the Samy worm) and Yahoo!.

12.7 See also

- Botnet
- Comparison of computer viruses
- Computer insecurity
- Crimeware
- *Core Wars*—an early computer game featuring virus-like competitors
- Cryptovirology
- Infection control
- Keystroke logging
- Malware
- Multipartite virus
- Spam (electronic)
- Trojan horse (computing)
- Virus hoax
- Windows 7 File Recovery
- Windows Action Center (Security Center)
- Zombie (computer science)

12.8 References

- [1] Stallings, William (2012). *Computer security : principles and practice*. Boston: Pearson. p. 182. ISBN 978-0-13-277506-9.
- [2] Aycock, John (2006). *Computer Viruses and Malware*. Springer. p. 14. ISBN 978-0-387-30236-2.
- [3] <http://vx.netlux.org/lib/aas10.html>
- [4] “Alan Solomon 'All About Viruses' (VX heavens)”. Web.archive.org. 2011-06-14. Archived from the original on January 17, 2012. Retrieved 2014-07-17.
- [5] Mookhey, K.K. et al. (2005). *Linux: Security, Audit and Control Features*. ISACA. p. 128. ISBN 9781893209787.
- [6] Toxen, Bob (2003). *Real World Linux Security: Intrusion Prevention, Detection, and Recovery*. Prentice Hall Professional. p. 365. ISBN 9780130464569.
- [7] Noyes, Katherine (Aug 3, 2010). “Why Linux Is More Secure Than Windows” . *PCWorld*.
- [8] Skoudis, Edward (2004). “Infection mechanisms and targets” . *Malware: Fighting Malicious Code*. Prentice Hall Professional. pp. 31–48. ISBN 9780131014053.
- [9] Aycock, John (2006). *Computer Viruses and Malware*. Springer. p. 27. ISBN 978-0-387-30236-2.

- [10] Ludwig, Mark A. (1996). *The Little Black Book of Computer Viruses: Volume I, The Basic Technologies*. pp. 16–17. ISBN 0-929408-02-0.
- [11] Harley, David et al. (2001). *Viruses Revealed*. McGraw-Hill. p. 6. ISBN 0-07-222818-0.
- [12] Filoli, Eric (2005). *Computer viruses:from theory to applications*. Springer. p. 8. ISBN 978-2-287-23939-7.
- [13] Bell, David J. et al, eds. (2004). “Virus” . *Cyberculture: The Key Concepts*. Routledge. p. 154. ISBN 9780203647059.
- [14] “Viruses that can cost you” .
- [15] Granneman, Scott. “Linux vs. Windows Viruses” . The Register. Retrieved September 4, 2015.
- [16] Kaspersky, Eugene (November 21, 2005). “The contemporary antivirus industry and its problems” . SecureLight.
- [17] Ludwig, Mark (1998). *The giant black book of computer viruses*. Show Low, Ariz: American Eagle. p. 13. ISBN 978-0-929408-23-1.
- [18] The term “computer virus” was not used at that time.
- [19] von Neumann, John (1966). “Theory of Self-Reproducing Automata” (PDF). *Essays on Cellular Automata*. University of Illinois Press: 66–87. Retrieved June 10, 2010.
- [20] Éric Filoli, *Computer viruses: from theory to applications, Volume 1*, Birkhäuser, 2005, pp. 19–38 ISBN 2-287-23939-1.
- [21] Risak, Veith (1972), “Selbstreproduzierende Automaten mit minimaler Informationsübertragung”, *Zeitschrift für Maschinenbau und Elektrotechnik*
- [22] Kraus, Jürgen (February 1980), *Selbstreproduktion bei Programmen* (PDF)
- [23] “Virus list” . Retrieved 2008-02-07.
- [24] Thomas Chen, Jean-Marc Robert (2004). “The Evolution of Viruses and Worms” . Retrieved 2009-02-16.
- [25] Parikka, Jussi (2007). *Digital Contagions: A Media Archaeology of Computer Viruses*. New York: Peter Lang. p. 50. ISBN 978-0-8204-8837-0.
- [26] Russell, Deborah & Gangemi, G.T. (1991). *Computer Security Basics*. O'Reilly. p. 86. ISBN 0-937175-71-4.
- [27] IMDB synopsis of Westworld. Retrieved November 28, 2015.
- [28] Michael Crichton (November 21, 1973). *Westworld* (movie). 201 S. Kinney Road, Tucson, Arizona, USA: Metro-Goldwyn-Mayer. Event occurs at 32 minutes. And there's a clear pattern here which suggests an analogy to an infectious disease process, spreading from one resort area to the next.” ... “Perhaps there are superficial similarities to disease.” “I must confess I find it difficult to belief in a disease of machinery.
- [29] Anick Jesdanun (1 September 2007). “School prank starts 25 years of security woes” . CNBC. Retrieved April 12, 2013.
- [30] “The anniversary of a nuisance” .
- [31] Cohen, Fred (1984), *Computer Viruses – Theory and Experiments*
- [32] Cohen, Fred, *An Undetectable Computer Virus*, 1987, IBM
- [33] Burger, Ralph, 1991. *Computer Viruses and Data Protection*, pp. 19–20
- [34] Dr. Solomon's Virus Encyclopedia, 1995. ISBN 1-897661-00-2. Abstract. Archived August 4, 2008, at the Wayback Machine.
- [35] Gunn, J.B. (June 1984). “Use of virus functions to provide a virtual APL interpreter under user control” . *ACM SIGAPL APL Quote Quad archive*. ACM New York, NY, USA. **14** (4): 163–168. ISSN 0163-6006. doi:10.1145/384283.801093.
- [36] “Boot sector virus repair” . Antivirus.about.com. 2010-06-10. Retrieved 2010-08-27.
- [37] “Amjad Farooq Alvi Inventor of first PC Virus post by Zagham” . YouTube. Retrieved 2010-08-27.
- [38] “winvir virus” . Retrieved 10 June 2016.
- [39] Grimes, Roger (2001). *Malicious Mobile Code: Virus Protection for Windows*. O'Reilly. pp. 99–100. ISBN 9781565926820.
- [40] “SCA virus” . Virus Test Center, University of Hamburg. 1990-06-05. Retrieved 2014-01-14.
- [41] <http://5-0-1.webs.com>

- [42] Ludwig, Mark (1998). *The giant black book of computer viruses*. Show Low, Ariz: American Eagle. p. 15. ISBN 978-0-929408-23-1.
- [43] Stallings, William (2012). *Computer security : principles and practice*. Boston: Pearson. p. 183. ISBN 978-0-13-277506-9.
- [44] Ludwig, Mark (1998). *The giant black book of computer viruses*. Show Low, Ariz: American Eagle. p. 292. ISBN 978-0-929408-23-1.
- [45] "www.cs.colostate.edu" (PDF). Retrieved 2016-04-25.
- [46] Gregory, Peter (2004). *Computer viruses for dummies* (in Danish). Hoboken, NJ: Wiley Pub. p. 210. ISBN 0-7645-7418-3.
- [47] Szor, Peter (2005). *The art of computer virus research and defense*. Upper Saddle River, NJ: Addison-Wesley. p. 43. ISBN 0-321-30454-3.
- [48] Serazzi, Giuseppe & Zanero, Stefano (2004). “Computer Virus Propagation Models” . In Calzarossa, Maria Carla & Gelenbe, Erol. *Performance Tools and Applications to Networked Systems* (PDF). Lecture Notes in Computer Science. Vol. 2965. pp. 26–50.
- [49] Avoine, Gildas et al. (2007). *Computer System Security: Basic Concepts and Solved Exercises*. EPFL Press / CRC Press. pp. 21–22. ISBN 9781420046205.
- [50] Brain, Marshall; Fenton, Wesley. “How Computer Viruses Work” . HowStuffWorks.com. Retrieved 16 June 2013.
- [51] Grimes, Roger (2001). *Malicious Mobile Code: Virus Protection for Windows*. O'Reilly. pp. 37–38. ISBN 9781565926820.
- [52] Salomon, David (2006). *Foundations of Computer Security*. Springer. pp. 47–48. ISBN 9781846283413.
- [53] Polk, William T. (1995). *Antivirus Tools and Techniques for Computer Systems*. William Andrew (Elsevier). p. 4. ISBN 9780815513643.
- [54] Grimes, Roger (2001). “Macro Viruses” . *Malicious Mobile Code: Virus Protection for Windows*. O'Reilly. ISBN 9781565926820.
- [55] Aycock, John (2006). *Computer Viruses and Malware*. Springer. p. 89. ISBN 9780387341880.
- [56] “What is boot sector virus?”. Retrieved 2015-10-16.
- [57] Anonymous (2003). *Maximum Security*. Sams Publishing. pp. 331–333. ISBN 9780672324598.
- [58] Skoudis, Edward (2004). “Infection mechanisms and targets” . *Malware: Fighting Malicious Code*. Prentice Hall Professional. pp. 37–38. ISBN 9780131014053.
- [59] Dave Jones. 2001 (December 2001). “Building an e-mail virus detection system for your network. Linux J. 2001, 92, 2-.” .
- [60] editor-in-chief, Béla G. Lipták, (2002). *Instrument engineers' handbook*. (3rd ed.). Boca Raton: CRC Press. p. 874. ISBN 9781439863442. Retrieved September 4, 2015.
- [61] “Computer Virus Strategies and Detection Methods” (PDF). Retrieved 2 September 2008.
- [62] *Internet Communication*. PediaPress. pp. 163–. GGKEY:Y43AS5T4TFD. Retrieved 16 April 2016.
- [63] Szor, Peter (2005). *The Art of Computer Virus Research and Defense*. Boston: Addison-Wesley. p. 285. ISBN 0-321-30454-3.
- [64] Fox-Brewster, Thomas. “Netflix Is Dumping Anti-Virus, Presages Death Of An Industry” . Forbes. Retrieved September 4, 2015.
- [65] “How Anti-Virus Software Works” . Stanford University. Retrieved September 4, 2015.
- [66] "www.sans.org". Retrieved 2016-04-16.
- [67] Jacobs, Stuart (2015-12-01). *Engineering Information Security: The Application of Systems Engineering Concepts to Achieve Information Assurance*. John Wiley & Sons. ISBN 9781119104711.
- [68] Bishop, Matt (2003). *Computer Security: Art and Science*. Addison-Wesley Professional. p. 620. ISBN 9780201440997.
- [69] *Internet Communication*. PediaPress. pp. 165–. GGKEY:Y43AS5T4TFD.
- [70] John Aycock (19 September 2006). *Computer Viruses and Malware*. Springer. pp. 35–36. ISBN 978-0-387-34188-0.

- [71] Kizza, Joseph M. (2009). *Guide to Computer Network Security*. Springer. p. 341. ISBN 9781848009165.
- [72] Eilam, Eldad (2011). *Reversing: Secrets of Reverse Engineering*. John Wiley & Sons. p. 216. ISBN 9781118079768.
- [73] “Virus Bulletin : Glossary – Polymorphic virus” . Virusbtn.com. 2009-10-01. Retrieved 2010-08-27.
- [74] Perriot, Fredrick; Peter Ferrie; Peter Szor (May 2002). “Striking Similarities” (PDF). Retrieved September 9, 2007.
- [75] “Virus Bulletin : Glossary —Metamorphic virus” . Virusbtn.com. Retrieved 2010-08-27.
- [76] “Virus Basics” . US-CERT.
- [77] “Virus Notice: Network Associates' AVERT Discovers First Virus That Can Infect JPEG Files, Assigns Low-Profiled Risk” . Retrieved 2002-06-13.
- [78] “Operating system market share” . netmarketshare.com. Retrieved 2015-05-16.
- [79] This is analogous to how genetic diversity in a population decreases the chance of a single disease wiping out a population in biology
- [80] Raggi, Emilio et al. (2011). *Beginning Ubuntu Linux*. Apress. p. 148. ISBN 9781430236276.
- [81] “McAfee discovers first Linux virus” (Press release). McAfee, via Axel Boldt. 5 February 1997.
- [82] Boldt, Axel (19 January 2000). “Bliss, a Linux 'virus'”.
- [83] “Detailed test reports—(Windows) home user” . AV-Test.org.
- [84] “Detailed test reports —Android mobile devices” . AV-Test.org.
- [85] “Microsoft Security Essentials” . Retrieved June 21, 2012.
- [86] “Malicious Software Removal Tool” . Archived from the original on June 21, 2012. Retrieved June 21, 2012.
- [87] “Windows Defender” . Retrieved June 21, 2012.
- [88] Rubenking, Neil J. (Feb 17, 2012). “The Best Free Antivirus for 2012” . pcmag.com.
- [89] Rubenking, Neil J. (Jan 10, 2013). “The Best Antivirus for 2013” . pcmag.com.
- [90] Rubenking, Neil J. “Secunia Personal Software Inspector 3.0 Review & Rating” . PCMag.com. Retrieved 2013-01-19.
- [91] “10 Step Guide to Protect Against Viruses” . GrnLight.net. Retrieved 23 May 2014.
- [92] “Google Safe Browsing” .
- [93] “Report malicious software (URL) to Google” .
- [94] Zhang, Yu et al. (2008). “A Novel Immune Based Approach For Detection of Windows PE Virus” . In Tang, Changjie et al. *Advanced Data Mining and Applications: 4th International Conference, ADMA 2008, Chengdu, China, October 8-10, 2008, Proceedings*. Springer. p. 250. ISBN 9783540881919.
- [95] “Good Security Habits | US-CERT” . Retrieved 2016-04-16.
- [96] “W32.Gammima.AG” . Symantec. Retrieved 2014-07-17.
- [97] Category: Computer Articles. “Viruses! In! Space!” . GrnLight.net. Retrieved 2014-07-17.
- [98] “VirusTotal.com (a subsidiary of Google)” .
- [99] “VirScan.org” .
- [100] Rubenking, Neil J. “The Best Free Antivirus for 2014” . pcmag.com.
- [101] “Microsoft Safety Scanner” .
- [102] “Virus removal -Help” . Retrieved 2015-01-31.
- [103] “W32.Gammima.AG Removal —Removing Help” . Symantec. 2007-08-27. Retrieved 2014-07-17.
- [104] “support.microsoft.com” . Retrieved 2016-04-16.
- [105] “www.us-cert.gov” (PDF). Retrieved 2016-04-16.

- [106] David Kim; Michael G. Solomon (17 November 2010). *Fundamentals of Information Systems Security*. Jones & Bartlett Publishers. pp. 360-. ISBN 978-1-4496-7164-8.
- [107] “1980s – Securelist – Information about Viruses, Hackers and Spam” . Retrieved 2016-04-16.
- [108] *Internet Communication*. PediaPress. pp. 160-. GGKEY:Y43AS5T4TFD.
- [109] “What is a Computer Virus?”. Actlab.utexas.edu. 1996-03-31. Retrieved 2010-08-27.
- [110] Realtimepublishers.com (1 January 2005). *The Definitive Guide to Controlling Malware, Spyware, Phishing, and Spam*. Realtimepublishers.com. pp. 48-. ISBN 978-1-931491-44-0.
- [111] Eli B. Cohen (2011). *Navigating Information Challenges*. Informing Science. pp. 27-. ISBN 978-1-932886-47-4.
- [112] Vesselin Bontchev. “Macro Virus Identification Problems” . *FRISK Software International*.
- [113] “Facebook 'photo virus' spreads via email.” . Retrieved 2014-04-28.
- [114] Berend-Jan Wever. “XSS bug in hotmail login page” . Retrieved 2014-04-07.
- [115] Wade Alcorn. “The Cross-site Scripting Virus” . bindshell.net. Retrieved 2015-10-13.

12.9 Further reading

- Burger, Ralf (16 February 2010) [1991]. *Computer Viruses and Data Protection*. Abacus. p. 353. ISBN 978-1-55755-123-8.
- Granneman, Scott (6 October 2003). “Linux vs. Windows Viruses” . *The Register*.
- Ludwig, Mark (1993). *Computer Viruses, Artificial Life and Evolution*. Tucson, Arizona 85717: American Eagle Publications, Inc. ISBN 0-929408-07-1. Archived from the original on July 4, 2008.
- Mark Russinovich (November 2006). *Advanced Malware Cleaning video* (Web (WMV / MP4)). Microsoft Corporation. Retrieved 24 July 2011.
- Parikka, Jussi (2007). *Digital Contagions. A Media Archaeology of Computer Viruses*. Digital Formations. New York: Peter Lang. ISBN 978-0-8204-8837-0.

12.10 External links

- Viruses at DMOZ (DMOZ)
- Microsoft Security Portal
- US Govt CERT (Computer Emergency Readiness Team) site
- 'Computer Viruses – Theory and Experiments' – The original paper by Fred Cohen, 1984
- Hacking Away at the Counterculture by Andrew Ross (On hacking, 1990)
- VX Heaven - the biggest library computer viruses

Chapter 13

Computer worm

This article is about coding of a worm. For the data storage device, see [Write Once Read Many](#). For other uses, see [worm \(disambiguation\)](#).

A **computer worm** is a standalone malware computer program that replicates itself in order to spread to other

0 00 00-6D	73 62 6C	msbl
0 6A 75-73	74 20 77	ast.exe I just w
9 20 4C-4F	56 45 20	ant to say LOVE
0 62 69-6C	6C 79 20	YOU SAN!! billy
0 64 6F-20	79 6F 75	gates why do you
3 20 70-6F	73 73 69	make this possi
0 20 6D-61	6B 69 6E	ble ? Stop makin
E 64 20-66	69 78 20	g money and fix
7 61 72-65	21 21 00	your software!!
0 00 00-7F	00 00 00	♣ ♦► H ▲
0 00 00-01	00 01 00	♦_♦_ @ @ @
0 00 00-00	00 00 46	á@ L F
C C9 11-9F	E8 08 00	♦ Jêèù-ñfp♦
0 00 03-10	00 00 00	►H `@ ♣ ♦►
3 00 00-01	00 04 00	♣ Õ ♦@ @ ♦

Hex dump of the Blaster worm, showing a message left for Microsoft CEO Bill Gates by the worm programmer

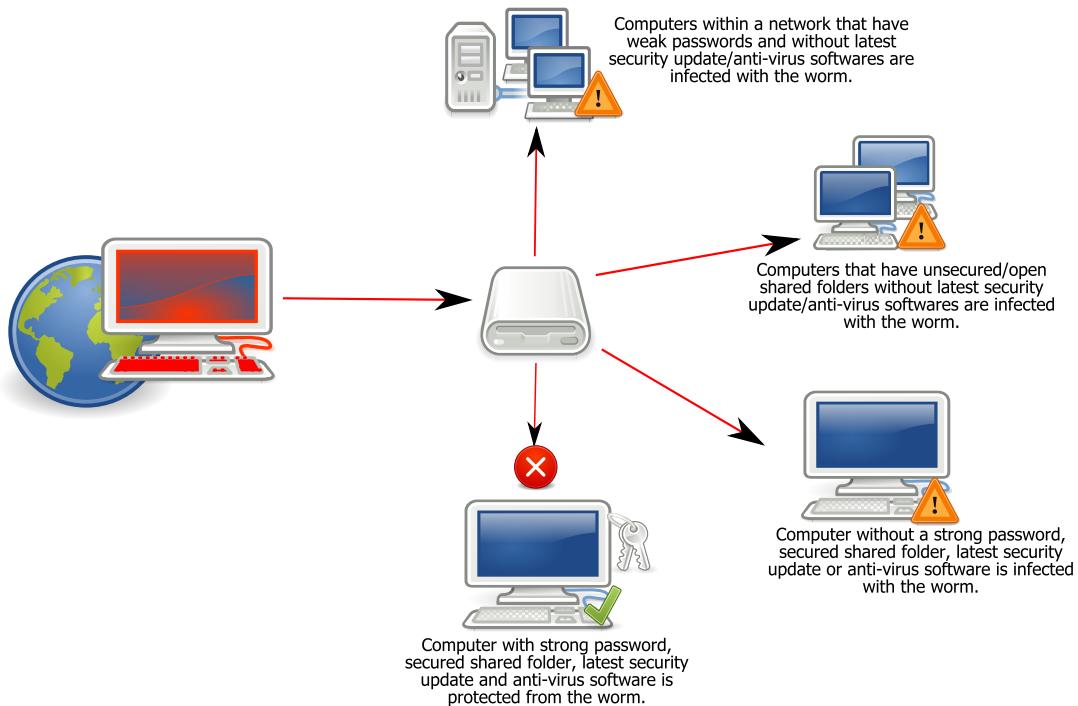
computers.* [1] Often, it uses a **computer network** to spread itself, relying on security failures on the target computer to access it. Worms almost always cause at least some harm to the network, even if only by consuming **bandwidth**, whereas viruses almost always corrupt or modify files on a targeted computer.

Many worms that have been created are designed only to spread, and do not attempt to change the systems they pass through. However, as the **Morris worm** and **Mydoom** showed, even these “payload-free” worms can cause major disruption by increasing network traffic and other unintended effects.

13.1 History

The actual term “worm” was first used in John Brunner's 1975 novel, *The Shockwave Rider*. In that novel, Nicholas Haflinger designs and sets off a data-gathering worm in an act of revenge against the powerful men who run a national electronic information web that induces mass conformity. “You have the biggest-ever worm loose in the net, and it

Worm:Win32 Conficker



Spread of Conficker worm

automatically sabotages any attempt to monitor it... There's never been a worm with that tough a head or that long a tail!"* [2]

On November 2, 1988, Robert Tappan Morris, a Cornell University computer science graduate student, unleashed what became known as the **Morris worm**, disrupting a large number of computers then on the Internet, guessed at the time to be one tenth of all those connected* [3] During the Morris appeal process, the U.S. Court of Appeals estimated the cost of removing the virus from each installation was in the range of \$200–53,000, and prompting the formation of the CERT Coordination Center* [4] and Phage mailing list.* [5] Morris himself became the first person tried and convicted under the 1986 Computer Fraud and Abuse Act.* [6]

13.2 Harm

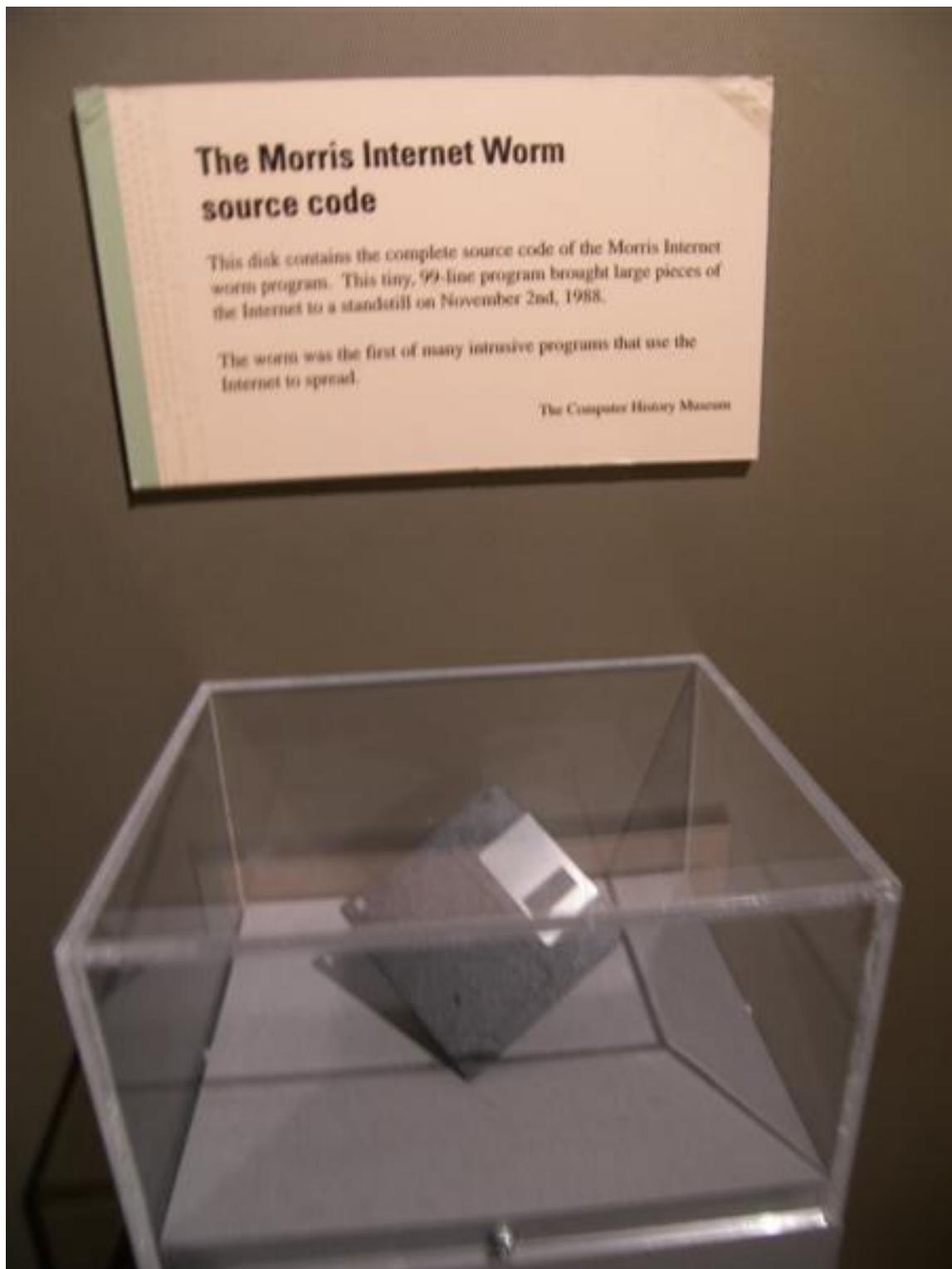
Any code designed to do more than spread the worm is typically referred to as the "payload". Typical malicious payloads might delete files on a host system (e.g., the **ExploreZip** worm), encrypt files in a **ransomware** attack, or exfiltrate data such as confidential documents or passwords.

Probably the most common payload for worms is to install a **backdoor**. This allows the computer to be remotely controlled by the worm author as a "zombie". Networks of such machines are often referred to as **botnets** and are very commonly used for a range of malicious purposes, including sending **spam** or performing **DoS** attacks.* [7]* [8]* [9]* [10]* [11]

13.3 Countermeasures

Worms spread by exploiting vulnerabilities in operating systems. Vendors with security problems supply regular security updates* [12] (see "**Patch Tuesday**"), and if these are installed to a machine then the majority of worms are unable to spread to it. If a vulnerability is disclosed before the security patch released by the vendor, a **zero-day** attack is possible.

Users need to be wary of opening unexpected email,* [13]* [14] and should not run attached files or programs, or visit



Morris worm source code floppy diskette at the Computer History Museum

web sites that are linked to such emails. However, as with the ILOVEYOU worm, and with the increased growth and efficiency of **phishing** attacks, it remains possible to trick the end-user into running malicious code.

Anti-virus and anti-spyware software are helpful, but must be kept up-to-date with new pattern files at least every few days. The use of a firewall is also recommended.

In the April–June 2008 issue of *IEEE Transactions on Dependable and Secure Computing*, computer scientists described a new and potentially effective way to combat internet worms. The researchers discovered how to contain

worms that scanned the Internet randomly, looking for vulnerable hosts to infect. They found that the key was to use software to monitor the number of scans that machines on a network send out. When a machine started to send out too many scans, it was a sign that it has been infected, which allowed administrators to take it off line and check it for malware.*[15]*[16] In addition, machine learning techniques can be used to detect new worms, by analyzing the behavior of the suspected computer.*[17]

Users can minimize the threat posed by worms by keeping their computers' operating system and other software up to date, avoiding opening unrecognized or unexpected emails and running **firewall** and antivirus software.*[18]

Mitigation techniques include:

- ACLs in routers and switches
- Packet-filters
- TCP Wrapper/ACL enabled network service daemons
- Nullroute

13.4 Worms with good intent

Main article: Helpful worm

Beginning with the very first research into worms at Xerox PARC, there have been attempts to create useful worms. Those worms allowed testing by John Shoch and Jon Hupp of the Ethernet principles on their network of Xerox Alto computers. The **Nachi** family of worms tried to download and install patches from Microsoft's website to fix vulnerabilities in the host system—by exploiting those same vulnerabilities.*[19] In practice, although this may have made these systems more secure, it generated considerable network traffic, rebooted the machine in the course of patching it, and did its work without the consent of the computer's owner or user. Regardless of their payload or their writers' intentions, most security experts regard all worms as **malware**.

Several worms, like **XSS worms**, have been written to research how worms spread. For example, the effects of changes in social activity or user behavior. One study proposed what seems to be the first computer worm that operates on the second layer of the OSI model (Data link Layer), it utilizes topology information such as Content-addressable memory (CAM) tables and Spanning Tree information stored in switches to propagate and probe for vulnerable nodes until the enterprise network is covered.*[20]

13.5 See also

- Botnet
- Code Shikara (Worm)
- Computer and network surveillance
- Computer virus
- Email spam
- Self-replicating machine
- Timeline of computer viruses and worms
- Trojan horse (computing)
- XSS worm
- Zombie (computer science)

13.6 References

- [1] Barwise, Mike. “What is an internet worm?”. BBC. Retrieved 9 September 2010.
- [2] Brunner, John (1975). *The Shockwave Rider*. New York: Ballantine Books. ISBN 0-06-010559-3.
- [3] “The Submarine” .
- [4] “Security of the Internet” . CERT/CC.
- [5] “Phage mailing list” . securitydigest.org.
- [6] Dressler, J. (2007). “United States v. Morris” . *Cases and Materials on Criminal Law*. St. Paul, MN: Thomson/West. ISBN 978-0-314-17719-3.
- [7] Ray, Tiernan (February 18, 2004). “Business & Technology: E-mail viruses blamed as spam rises sharply” . *The Seattle Times*.
- [8] McWilliams, Brian (October 9, 2003). “Cloaking Device Made for Spammers” . *Wired*.
- [9] “Mydoom Internet worm likely from Russia, linked to spam mail: security firm” . www.channelnewsasia.com. 31 January 2004. Archived from the original on 2006-02-19.
- [10] “Uncovered: Trojans as Spam Robots” . *Hiese online*. 2004-02-21. Archived from the original on 2009-05-28. Retrieved 2012-11-02.
- [11] “Hacker threats to bookies probed” . *BBC News*. February 23, 2004.
- [12] “USN list” . Ubuntu. Retrieved 2012-06-10.
- [13] Threat Description Email-Worm
- [14] Threat Description Email-Worm: VBS/LoveLetter
- [15] Sellke, S. H.; Shroff, N. B.; Bagchi, S. (2008). “Modeling and Automated Containment of Worms” . *IEEE Transactions on Dependable and Secure Computing*. 5 (2): 71–86. doi:10.1109/tdsc.2007.70230. Archived from the original on 25 May 2015.
- [16] “A New Way to Protect Computer Networks from Internet Worms” . *Newswise*. Retrieved July 5, 2011.
- [17] Moskovich R., Elovici Y., Rokach L. (2008), "Detection of unknown computer worms based on behavioral classification of the host", *Computational Statistics and Data Analysis*, 52(9):4544–4566, doi:10.1016/j.csda.2008.01.028
- [18] “Computer Worm Information and Removal Steps” . Veracode. Retrieved 2015-04-04.
- [19] “Virus alert about the Nachi worm” . Microsoft.
- [20] Al-Salloum, Z. S.; Wolthusen, S. D. (2010). “A link-layer-based self-replicating vulnerability discovery agent” . *The IEEE symposium on Computers and Communications*. p. 704. ISBN 978-1-4244-7754-8. doi:10.1109/ISCC.2010.5546723.

13.7 External links

- Malware Guide – Guide for understanding, removing and preventing worm infections on Vernalex.com.
- “The 'Worm' Programs – Early Experience with a Distributed Computation” , John Shoch and Jon Hupp, *Communications of the ACM*, Volume 25 Issue 3 (March 1982), pages 172–180.
- “The Case for Using Layered Defenses to Stop Worms” , Unclassified report from the U.S. National Security Agency (NSA), 18 June 2004.
- Worm Evolution, paper by Jago Maniscalchi on Digital Threat, 31 May 2009.

Chapter 14

Denial-of-service attack

“DoS” redirects here. For the computer operating system, see DOS. For other uses, see DoS (disambiguation).

In computing, a **denial-of-service attack (DoS attack)** is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.*[1]

In a **distributed denial-of-service attack (DDoS attack)**, the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source.

A DoS or DDoS attack is analogous to a group of people crowding the entry door or gate to a shop or business, and not letting legitimate parties enter into the shop or business, disrupting normal operations.

Criminal perpetrators of DoS attacks often target sites or services hosted on high-profile web servers such as banks or credit card payment gateways. Revenge, blackmail*[2]*[3]*[4] and activism*[5] can motivate these attacks.

14.1 History

Court testimony shows that the first demonstration of DoS attack was made by Khan C. Smith in 1997 during a DEF CON event disrupting Internet access to the Las Vegas Strip for over an hour and the release of sample code during the event led to the online attack of Sprint, EarthLink, E-Trade, and other major corporations in the year to follow.*[6]

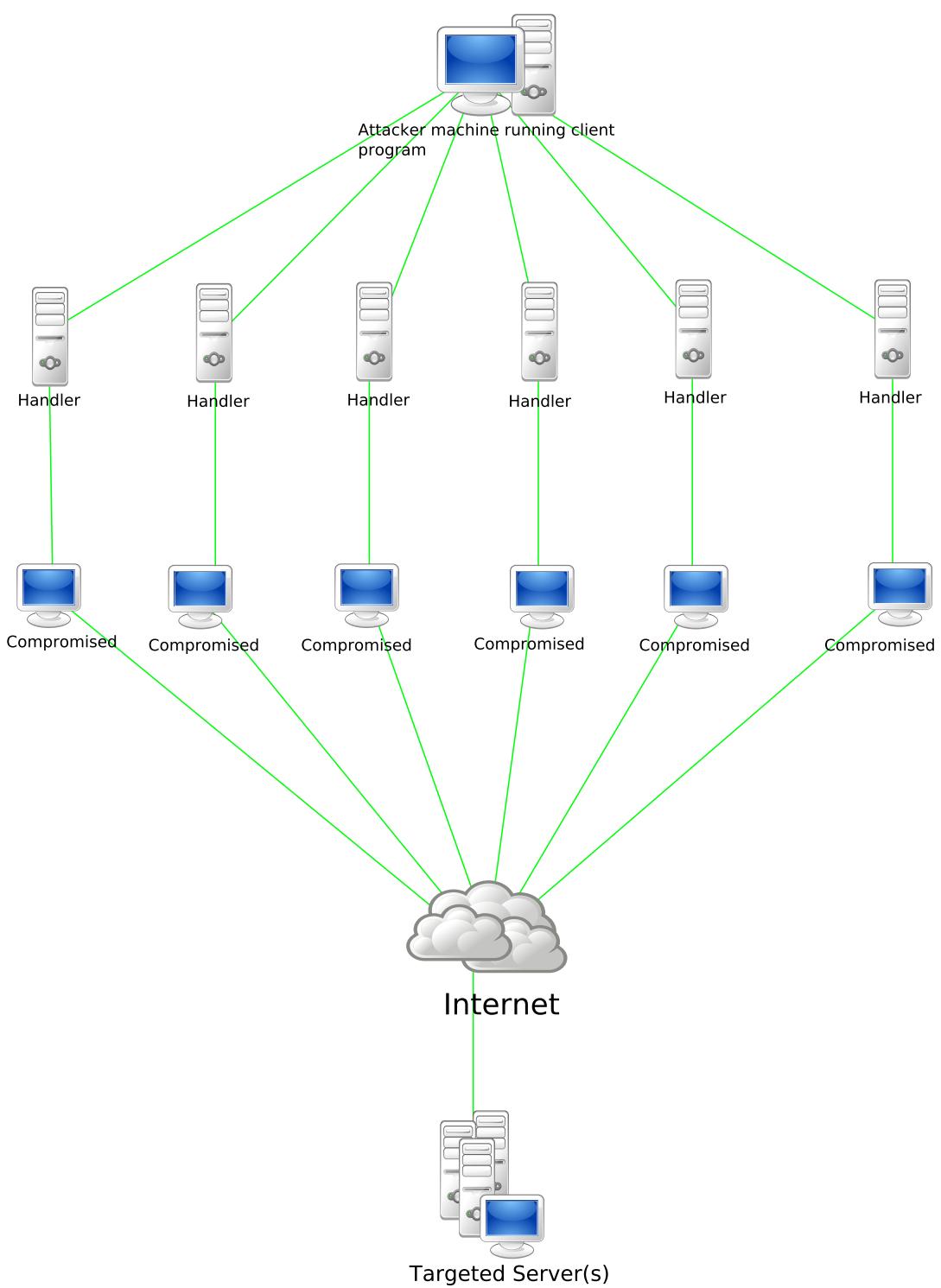
14.2 Types

Denial-of-service attacks are characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. In a distributed denial-of-service (DDoS) attack, the incoming traffic flooding the victim originates from many different sources – potentially hundreds of thousands or more. This effectively makes it impossible to stop the attack simply by blocking a single IP address; plus, it is very difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin. There are two general forms of DoS attacks: those that crash services and those that flood services. The most serious attacks are distributed.*[7] Many attacks involve forging of IP sender addresses (IP address spoofing) so that the location of the attacking machines cannot easily be identified and so that the attack cannot be easily defeated using ingress filtering.

14.2.1 Distributed DoS

See also: October 2016 Dyn cyberattack, IP address spoofing, and Hop (networking)

A **distributed denial-of-service (DDoS)** is a cyber-attack where the perpetrator uses more than one unique IP address, often thousands of them. The scale of DDoS attacks has continued to rise over recent years, by 2016



DDoS Stacheldraht attack diagram.

exceeding a terabit per second.*[8] *[9]

14.2.2 Application layer attacks

An **application layer DDoS attack** (sometimes referred to as **layer 7 DDoS attack**) is a form of DDoS attack where attackers target the **application layer** of the **OSI model**.^{*[10]*[11]} The attack over-exercises specific functions or features of a website with the intention to disable those functions or features. This application-layer attack is different from an entire network attack, and is often used against financial institutions to distract IT and security personnel from security breaches.^{*[12]} As of 2013, application layer DDoS attacks represent 20% of all DDoS attacks.^{*[13]} According to research by the company Akamai, there have been “51 percent more application layer attacks” from Q4 2013 to Q4 2014 and “16 percent more” from Q3 2014 over Q4 2014.^{*[14]}

Application layer

Main article: **OSI model**

The Open Systems Interconnection (OSI) model (ISO/IEC 7498-1) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO). The model groups similar communication functions into one of seven logical layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal connection on that layer.

Main article: **Application layer**

In the **OSI model**, the definition of its application layer is narrower in scope. The OSI model defines the application layer as being the user interface. The OSI application layer is responsible for displaying data and images to the user in a human-recognizable format and to interface with the presentation layer below it.

Method of attack

An application layer DDoS attack is done mainly for specific targeted purposes, including disrupting transactions and access to databases. It requires less resources and often accompanies network layer attacks.^{*[15]} An attack is disguised to look like legitimate traffic, except it targets specific application packets.^{*[13]} The attack on the application layer can disrupt services such as the retrieval of information or search function^{*[13]} as well as web browser function, email services and photo applications. In order to be deemed a *distributed* denial of service attack, more than around 3–5 nodes on different networks should be used; using fewer than 3–5 nodes qualifies as a **Denial-of-service attack** and not a DDoS.^{*[11]*[16]}

Defending application layer DDoS attacks

Defending against an application layer DDoS attack requires **DDoS mitigation**. Success of mitigation requires correctly identifying incoming traffic to separate human traffic from human-like bots and hijacked browsers.

14.2.3 Advanced persistent DoS

An **advanced persistent DoS** (APDoS) is more likely to be perpetrated by an **advanced persistent threat** (APT): actors who are well-resourced, exceptionally skilled and have access to substantial commercial grade computer resources and capacity. APDoS attacks represent a clear and emerging threat needing specialised monitoring and incident response services and the defensive capabilities of specialised DDoS mitigation service providers.

This type of attack involves massive network layer DDoS attacks through to focused application layer (HTTP) floods, followed by repeated (at varying intervals) SQLi and XSS attacks.^{*[17]} Typically, the perpetrators can simultaneously use from 2 to 5 attack vectors involving up to several tens of millions of requests per second, often accompanied by large SYN floods that can not only attack the victim but also any service provider implementing any sort of managed DDoS mitigation capability. These attacks can persist for several weeks- the longest continuous period noted so far lasted 38 days. This APDoS attack involved approximately 50+ petabits (50,000+ terabits) of malicious traffic.

Attackers in this scenario may (or often will) tactically switch between several targets to create a diversion to evade defensive DDoS countermeasures but all the while eventually concentrating the main thrust of the attack onto a single victim. In this scenario, threat actors with continuous access to several very powerful network resources are capable of sustaining a prolonged campaign generating enormous levels of un-amplified DDoS traffic.

APDoS attacks are characterised by:

- advanced reconnaissance (pre-attack OSINT and extensive decoyed scanning crafted to evade detection over long periods)
- tactical execution (attack with a primary and secondary victims but focus is on primary)
- explicit motivation (a calculated end game/goal target)
- large computing capacity (access to substantial computer power and network bandwidth resources)
- simultaneous multi-threaded OSI layer attacks (sophisticated tools operating at layers 3 through 7)
- persistence over extended periods (utilising all the above into a concerted, well managed attack across a range of targets^{*}[18]).

14.2.4 Denial-of-service as a service

Some vendors provide so-called “booter” or “stresser” services, which have simple web-based front ends, and accept payment over the web. Marketed and promoted as stress-testing tools, they can be used to perform unauthorized denial-of-service attacks, and allow technically unsophisticated attackers access to sophisticated attack tools without the need for the attacker to understand their use.^{*}[19]

14.3 Symptoms

The United States Computer Emergency Readiness Team (US-CERT) has identified symptoms of a denial-of-service attack to include:^{*}[20]

- unusually slow network performance (opening files or accessing web sites)
- unavailability of a particular web site
- inability to access any web site
- dramatic increase in the number of spam emails received (this type of DoS attack is considered an e-mail bomb).

Additional symptoms may include:

- disconnection of a wireless or wired internet connection
- long-term denial of access to the web or any internet services.

If the attack is conducted on a sufficiently large scale, entire geographical regions of Internet connectivity can be compromised without the attacker's knowledge or intent by incorrectly configured or flimsy network infrastructure equipment.

14.4 Attack techniques

A wide array of programs are used to launch DoS-attacks.

14.4.1 Attack tools

In cases such as **MyDoom** the tools are embedded in malware, and launch their attacks without the knowledge of the system owner. **Stacheldraht** is a classic example of a DDoS tool. It utilizes a layered structure where the attacker uses a client program to connect to handlers, which are compromised systems that issue commands to the zombie agents, which in turn facilitate the DDoS attack. Agents are compromised via the handlers by the attacker, using automated routines to exploit vulnerabilities in programs that accept remote connections running on the targeted remote hosts. Each handler can control up to a thousand agents.*[21]

In other cases a machine may become part of a DDoS attack with the owner's consent, for example, in **Operation Payback**, organized by the group **Anonymous**. The **LOIC** has typically been used in this way. Along with **HOIC** a wide variety of DDoS tools are available today, including paid and free versions, with different features available. There is an underground market for these in hacker related forums and IRC channels.

UK's **GCHQ** has tools built for DDoS, named **PREDATORS FACE** and **ROLLING THUNDER**.*[22]

14.4.2 Application-layer floods

Various DoS-causing exploits such as buffer overflow can cause server-running software to get confused and fill the disk space or consume all available memory or **CPU time**.

Other kinds of DoS rely primarily on brute force, flooding the target with an overwhelming flux of packets, over-saturating its connection bandwidth or depleting the target's system resources. Bandwidth-saturating floods rely on the attacker having higher bandwidth available than the victim; a common way of achieving this today is via distributed denial-of-service, employing a **botnet**. Another target of DDoS attacks may be to produce added costs for the application operator, when the latter uses resources based on **Cloud Computing**. In this case normally application used resources are tied to a needed Quality of Service level (e.g. responses should be less than 200 ms) and this rule is usually linked to automated software (e.g. Amazon CloudWatch*[23]) to raise more virtual resources from the provider in order to meet the defined QoS levels for the increased requests. The main incentive behind such attacks may be to drive the application owner to raise the elasticity levels in order to handle the increased application traffic, in order to cause financial losses or force them to become less competitive. Other floods may use specific packet types or connection requests to saturate finite resources by, for example, occupying the maximum number of open connections or filling the victim's disk space with logs.

A “banana attack” is another particular type of DoS. It involves redirecting outgoing messages from the client back onto the client, preventing outside access, as well as flooding the client with the sent packets. A **LAND** attack is of this type.

An attacker with shell-level access to a victim's computer may slow it until it is unusable or crash it by using a **fork bomb**.

A kind of application-level DoS attack is **XDoS** (or XML DoS) which can be controlled by modern web application firewalls (WAFs).

14.4.3 Degradation-of-service attacks

“Pulsing” zombies are compromised computers that are directed to launch intermittent and short-lived floodings of victim websites with the intent of merely slowing it rather than crashing it. This type of attack, referred to as “degradation-of-service” rather than “denial-of-service”, can be more difficult to detect than regular zombie invasions and can disrupt and hamper connection to websites for prolonged periods of time, potentially causing more disruption than concentrated floods.*[24]*[25] Exposure of degradation-of-service attacks is complicated further by the matter of discerning whether the server is really being attacked or under normal traffic loads.*[26]

14.4.4 Denial-of-service Level II

The goal of DoS L2 (possibly DDoS) attack is to cause a launching of a defense mechanism which blocks the network segment from which the attack originated. In case of distributed attack or IP header modification (that depends on the kind of security behavior) it will fully block the attacked network from the Internet, but without system crash.*[17]

14.4.5 Distributed DoS attack

A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers.^{*[7]} Such an attack is often the result of multiple compromised systems (for example, a botnet) flooding the targeted system with traffic. A botnet is a network of zombie computers programmed to receive commands without the owners' knowledge.^{*[27]} When a server is overloaded with connections, new connections can no longer be accepted. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track and shut down. These attacker advantages cause challenges for defense mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply add more attack machines. This, after all, will end up completely crashing a website for periods of time.

Malware can carry DDoS attack mechanisms; one of the better-known examples of this was MyDoom. Its DoS mechanism was triggered on a specific date and time. This type of DDoS involved hardcoding the target IP address prior to release of the malware and no further interaction was necessary to launch the attack.

A system may also be compromised with a trojan, allowing the attacker to download a zombie agent, or the trojan may contain one. Attackers can also break into systems using automated tools that exploit flaws in programs that listen for connections from remote hosts. This scenario primarily concerns systems acting as servers on the web. Stacheldraht is a classic example of a DDoS tool. It utilizes a layered structure where the attacker uses a client program to connect to handlers, which are compromised systems that issue commands to the zombie agents, which in turn facilitate the DDoS attack. Agents are compromised via the handlers by the attacker, using automated routines to exploit vulnerabilities in programs that accept remote connections running on the targeted remote hosts. Each handler can control up to a thousand agents.^{*[21]} In some cases a machine may become part of a DDoS attack with the owner's consent, for example, in Operation Payback, organized by the group Anonymous. These attacks can use different types of internet packets such as: TCP, UDP, ICMP etc.

These collections of systems compromisers are known as botnets / rootservers. DDoS tools like Stacheldraht still use classic DoS attack methods centered on IP spoofing and amplification like smurf attacks and fraggle attacks (these are also known as bandwidth consumption attacks). SYN floods (also known as resource starvation attacks) may also be used. Newer tools can use DNS servers for DoS purposes. Unlike MyDoom's DDoS mechanism, botnets can be turned against any IP address. Script kiddies use them to deny the availability of well known websites to legitimate users.^{*[28]} More sophisticated attackers use DDoS tools for the purposes of extortion – even against their business rivals.^{*[29]}

Simple attacks such as SYN floods may appear with a wide range of source IP addresses, giving the appearance of a well distributed DoS. These flood attacks do not require completion of the TCP three way handshake and attempt to exhaust the destination SYN queue or the server bandwidth. Because the source IP addresses can be trivially spoofed, an attack could come from a limited set of sources, or may even originate from a single host. Stack enhancements such as syn cookies may be effective mitigation against SYN queue flooding, however complete bandwidth exhaustion may require involvement.

If an attacker mounts an attack from a single host it would be classified as a DoS attack. In fact, any attack against availability would be classed as a denial-of-service attack. On the other hand, if an attacker uses many systems to simultaneously launch attacks against a remote host, this would be classified as a DDoS attack.

It has been reported that there are new attacks from internet of things which have been involved in denial of service attacks.^{*[30]} In one noted attack that was made peaked at around 20,000 requests per second which came from around 900 CCTV cameras.^{*[31]}

UK's GCHQ has tools built for DDoS, named PREDATORS FACE and ROLLING THUNDER.^{*[22]}

See also: DDoS mitigation

14.4.6 DDoS extortion

In 2015, DDoS botnets such as DD4BC grew in prominence, taking aim at financial institutions.^{*[32]} Cyber-extortionists typically begin with a low-level attack and a warning that a larger attack will be carried out if a ransom is not paid in Bitcoin.^{*[33]} Security experts recommend targeted websites to not pay the ransom. The attackers tend to get into an

extended extortion scheme once they recognize that the target is ready to pay.*[34]

14.4.7 HTTP POST DoS attack

First discovered in 2009, the HTTP POST attack sends a complete, legitimate **HTTP POST** header, which includes a 'Content-Length' field to specify the size of the message body to follow. However, the attacker then proceeds to send the actual message body at an extremely slow rate (e.g. 1 byte/110 seconds). Due to the entire message being correct and complete, the target server will attempt to obey the 'Content-Length' field in the header, and wait for the entire body of the message to be transmitted, which can take a very long time. The attacker establishes hundreds or even thousands of such connections, until all resources for incoming connections on the server (the victim) are used up, hence making any further (including legitimate) connections impossible until all data has been sent. It is notable that unlike many other (D)DoS attacks, which try to subdue the server by overloading its network or CPU, a HTTP POST attack targets the *logical* resources of the victim, which means the victim would still have enough network bandwidth and processing power to operate.*[35] Further combined with the fact that **Apache** will, by default, accept requests up to 2GB in size, this attack can be particularly powerful. HTTP POST attacks are difficult to differentiate from legitimate connections, and are therefore able to bypass some protection systems. **OWASP**, an open source web application security project, has released a testing tool to test the security of servers against this type of attacks.

14.4.8 Internet Control Message Protocol (ICMP) flood

A **smurf attack** relies on misconfigured network devices that allow packets to be sent to all computer hosts on a particular network via the **broadcast address** of the network, rather than a specific machine. The attacker will send large numbers of **IP** packets with the source address faked to appear to be the address of the victim. The network's bandwidth is quickly used up, preventing legitimate packets from getting through to their destination.*[36]

Ping flood is based on sending the victim an overwhelming number of **ping** packets, usually using the "ping" command from **Unix-like** hosts (the -t flag on **Windows** systems is much less capable of overwhelming a target, also the -l (size) flag does not allow sent packet size greater than 65500 in Windows). It is very simple to launch, the primary requirement being access to greater bandwidth than the victim.

Ping of death is based on sending the victim a malformed ping packet, which will lead to a system crash on a vulnerable system.

The **BlackNurse** attack is an example of an attack taking advantage of the required Destination Port Unreachable ICMP packets.

14.4.9 Nuke

A **Nuke** is an old denial-of-service attack against **computer networks** consisting of fragmented or otherwise invalid **ICMP** packets sent to the target, achieved by using a modified **ping** utility to repeatedly send this corrupt data, thus slowing down the affected computer until it comes to a complete stop.

A specific example of a nuke attack that gained some prominence is the **WinNuke**, which exploited the vulnerability in the **NetBIOS** handler in **Windows 95**. A string of out-of-band data was sent to **TCP** port 139 of the victim's machine, causing it to lock up and display a **Blue Screen of Death** (BSOD).

14.4.10 Peer-to-peer attacks

Main article: Direct Connect (protocol) § Direct Connect used for DDoS attacks

Attackers have found a way to exploit a number of bugs in **peer-to-peer** servers to initiate DDoS attacks. The most aggressive of these peer-to-peer-DDoS attacks exploits **DC++**. With peer-to-peer there is no botnet and the attacker does not have to communicate with the clients it subverts. Instead, the attacker acts as a "puppet master," instructing clients of large **peer-to-peer** file sharing hubs to disconnect from their peer-to-peer network and to connect to the victim's website instead.*[37]*[38]*[39]

14.4.11 Permanent denial-of-service attacks

Permanent denial-of-service (PDoS), also known loosely as phlashing,^{*}[40] is an attack that damages a system so badly that it requires replacement or reinstallation of hardware.^{*}[41] Unlike the distributed denial-of-service attack, a PDoS attack exploits security flaws which allow remote administration on the management interfaces of the victim's hardware, such as routers, printers, or other networking hardware. The attacker uses these vulnerabilities to replace a device's firmware with a modified, corrupt, or defective firmware image—a process which when done legitimately is known as *flashing*. This therefore "bricks" the device, rendering it unusable for its original purpose until it can be repaired or replaced.

The PDoS is a pure hardware targeted attack which can be much faster and requires fewer resources than using a botnet or a root/vserver in a DDoS attack. Because of these features, and the potential and high probability of security exploits on Network Enabled Embedded Devices (NEEDs), this technique has come to the attention of numerous hacking communities.

PhlashDance is a tool created by Rich Smith (an employee of Hewlett-Packard's Systems Security Lab) used to detect and demonstrate PDoS vulnerabilities at the 2008 EUsecWest Applied Security Conference in London.^{*}[42]

14.4.12 Reflected / spoofed attack

A distributed denial-of-service attack may involve sending forged requests of some type to a very large number of computers that will reply to the requests. Using Internet Protocol address spoofing, the source address is set to that of the targeted victim, which means all the replies will go to (and flood) the target. (This reflected attack form is sometimes called a "DRDOS".^{*}[43])

ICMP Echo Request attacks (Smurf attack) can be considered one form of reflected attack, as the flooding host(s) send Echo Requests to the broadcast addresses of mis-configured networks, thereby enticing hosts to send Echo Reply packets to the victim. Some early DDoS programs implemented a distributed form of this attack.

Amplification

Amplification attacks are used to magnify the bandwidth that is sent to a victim. This is typically done through publicly accessible DNS servers that are used to cause congestion on the target system using DNS response traffic. Many services can be exploited to act as reflectors, some harder to block than others.^{*}[44] US-CERT have observed that different services implies in different amplification factors, as you can see below:^{*}[45]

DNS amplification attacks involve a new mechanism that increased the amplification effect, using a much larger list of DNS servers than seen earlier. The process typically involves an attacker sending a DNS name look up request to a public DNS server, spoofing the source IP address of the targeted victim. The attacker tries to request as much zone information as possible, thus amplifying the DNS record response that is sent to the targeted victim. Since the size of the request is significantly smaller than the response, the attacker is easily able to increase the amount of traffic directed at the target.^{*}[48]^{*}[49] SNMP and NTP can also be exploited as reflector in an amplification attack.

An example of an amplified DDoS attack through NTP is through a command called monlist, which sends the details of the last 600 people who have requested the time from that computer back to the requester. A small request to this time server can be sent using a spoofed source IP address of some victim, which results in 556.9 times the amount of data that was requested back to the victim. This becomes amplified when using botnets that all send requests with the same spoofed IP source, which will send a massive amount of data back to the victim.

It is very difficult to defend against these types of attacks because the response data is coming from legitimate servers. These attack requests are also sent through UDP, which does not require a connection to the server. This means that the source IP is not verified when a request is received by the server. In order to bring awareness of these vulnerabilities, campaigns have been started that are dedicated to finding amplification vectors which has led to people fixing their resolvers or having the resolvers shut down completely.

14.4.13 R-U-Dead-Yet? (RUDY)

RUDY attack targets web applications by starvation of available sessions on the web server. Much like Slowloris, RUDY keeps sessions at halt using never-ending POST transmissions and sending an arbitrarily large content-length header value.

14.4.14 Shrew attack

The shrew attack is a denial-of-service attack on the Transmission Control Protocol. It uses short synchronized bursts of traffic to disrupt TCP connections on the same link, by exploiting a weakness in TCP's retransmission timeout mechanism.* [50]

14.4.15 Slow Read attack

Slow Read attack sends legitimate application layer requests but reads responses very slowly, thus trying to exhaust the server's connection pool. Slow reading is achieved by advertising a very small number for the TCP Receive Window size and at the same time by emptying clients' TCP receive buffer slowly. That naturally ensures a very low data flow rate.

14.4.16 Sophisticated low-bandwidth Distributed Denial-of-Service Attack

A sophisticated low-bandwidth DDoS attack is a form of DoS that uses less traffic and increases their effectiveness by aiming at a weak point in the victim's system design, i.e., the attacker sends traffic consisting of complicated requests to the system.* [51] Essentially, a sophisticated DDoS attack is lower in cost due to its use of less traffic, is smaller in size making it more difficult to identify, and it has the ability to hurt systems which are protected by flow control mechanisms.* [51]*[52]

14.4.17 (S)SYN flood

See also: SYN flood

A SYN flood occurs when a host sends a flood of TCP/SYN packets, often with a forged sender address. Each of these packets are handled like a connection request, causing the server to spawn a half-open connection, by sending back a TCP/SYN-ACK packet (Acknowledge), and waiting for a packet in response from the sender address (response to the ACK Packet). However, because the sender address is forged, the response never comes. These half-open connections saturate the number of available connections the server can make, keeping it from responding to legitimate requests until after the attack ends.* [53]

14.4.18 Teardrop attacks

A teardrop attack involves sending mangled IP fragments with overlapping, oversized payloads to the target machine. This can crash various operating systems because of a bug in their TCP/IP fragmentation re-assembly code.* [54] Windows 3.1x, Windows 95 and Windows NT operating systems, as well as versions of Linux prior to versions 2.0.32 and 2.1.63 are vulnerable to this attack.

(Although in September 2009, a vulnerability in Windows Vista was referred to as a “teardrop attack”, this targeted SMB2 which is a higher layer than the TCP packets that teardrop used).* [55]*[56]

One of the fields in an IP header is the “fragment offset” field, indicating the starting position, or offset, of the data contained in a fragmented packet relative to the data in the original packet. If the sum of the offset and size of one fragmented packet differs from that of the next fragmented packet, the packets overlap. When this happens, a server vulnerable to teardrop attacks is unable to reassemble the packets - resulting in a denial-of-service condition.

14.4.19 Telephony denial-of-service (TDoS)

Voice over IP has made abusive origination of large numbers of telephone voice calls inexpensive and readily automated while permitting call origins to be misrepresented through caller ID spoofing.

According to the US Federal Bureau of Investigation, telephony denial-of-service (TDoS) has appeared as part of various fraudulent schemes:

- A scammer contacts the victim's banker or broker, impersonating the victim to request a funds transfer. The banker's attempt to contact the victim for verification of the transfer fails as the victim's telephone lines are being flooded with thousands of bogus calls, rendering the victim unreachable.*[57]
- A scammer contacts consumers with a bogus claim to collect an outstanding payday loan for thousands of dollars. When the consumer objects, the scammer retaliates by flooding the victim's employer with thousands of automated calls. In some cases, displayed caller ID is spoofed to impersonate police or law enforcement agencies.*[58]
- A scammer contacts consumers with a bogus debt collection demand and threatens to send police; when the victim balks, the scammer floods local police numbers with calls on which caller ID is spoofed to display the victim's number. Police soon arrive at the victim's residence attempting to find the origin of the calls.

Telephony denial-of-service can exist even without Internet telephony. In the 2002 New Hampshire Senate election phone jamming scandal, telemarketers were used to flood political opponents with spurious calls to jam phone banks on election day. Widespread publication of a number can also flood it with enough calls to render it unusable, as happened with multiple +1-area code—867-5309 subscribers inundated by hundreds of misdialed calls daily in response to the song 867-5309/Jenny.

TDoS differs from other telephone harassment (such as prank calls and obscene phone calls) by the number of calls originated; by occupying lines continuously with repeated automated calls, the victim is prevented from making or receiving both routine and emergency telephone calls.

Related exploits include SMS flooding attacks and black fax or fax loop transmission.

14.5 Defense techniques

Defensive responses to denial-of-service attacks typically involve the use of a combination of attack detection, traffic classification and response tools, aiming to block traffic that they identify as illegitimate and allow traffic that they identify as legitimate.*[59] A list of prevention and response tools is provided below:

14.5.1 Application front end hardware

Application front-end hardware is intelligent hardware placed on the network before traffic reaches the servers. It can be used on networks in conjunction with routers and switches. Application front end hardware analyzes data packets as they enter the system, and then identifies them as priority, regular, or dangerous. There are more than 25 bandwidth management vendors.

14.5.2 Application level Key Completion Indicators

In order to meet the case of application level DDoS attacks against cloud-based applications, approaches may be based on an application layer analysis, to indicate whether an incoming traffic bulk is legitimate or not and thus enable the triggering of elasticity decisions without the economical implications of a DDoS attack.*[60] These approaches mainly rely on an identified path of value inside the application and monitor the macroscopic progress of the requests in this path, towards the final generation of profit, through markers denoted as Key Completion Indicators.*[61]

In essence, this technique is a statistical method of assessing the behavior of incoming requests to detect if something unusual or abnormal is going on. Imagine if you were to observe the behavior of normal, paying customers at a brick-and-mortar department store. On average, they would spend in aggregate a known percentage of time on different activities such as picking up items and examining them, putting them back on shelves, trying on clothes, filling a basket, waiting in line, paying for their purchases, and leaving. These high-level activities correspond to the Key Completion Indicators in a service or site, and once normal behavior is determined, abnormal behavior can be identified. For example, if a huge number of customers arrive and spend all their time picking up items and setting them down, but never making any purchases, this can be flagged as unusual behavior.

In the case of elastic cloud services where a huge and abnormal additional workload may incur significant charges from the cloud service provider, this technique can be used to stop or even scale back the elastic expansion of server availability in order to protect from economic loss. In the example analogy, imagine that the department store had

the ability to bring in additional employees on a few minutes' notice and routinely did this during “rushes” of unusual customer volume. If a mob shows up that never does any buying, after a relatively short time of paying for the additional employee costs, the store can scale back the number of employees, understanding that the non-buying customers provide no profit for the store and thus should not be serviced. While this may prevent the store from making sales to legitimate customers during the period of attack, it saves the potentially ruinous cost of calling up huge numbers of employees to service an illegitimate load.

14.5.3 Blackholing and sinkholing

With **blackhole routing**, all the traffic to the attacked DNS or IP address is sent to a “black hole” (null interface or a non-existent server). To be more efficient and avoid affecting network connectivity, it can be managed by the ISP.*[62]

A **DNS sinkhole** routes traffic to a valid IP address which analyzes traffic and rejects bad packets. Sinkholing is not efficient for most severe attacks.

14.5.4 IPS based prevention

Intrusion prevention systems (IPS) are effective if the attacks have signatures associated with them. However, the trend among the attacks is to have legitimate content but bad intent. Intrusion-prevention systems which work on content recognition cannot block behavior-based DoS attacks.*[17]

An **ASIC** based IPS may detect and block denial-of-service attacks because they have the **processing power** and the granularity to analyze the attacks and act like a **circuit breaker** in an automated way.*[17]

A **rate-based IPS (RBIIPS)** must analyze traffic granularly and continuously monitor the traffic pattern and determine if there is traffic anomaly. It must let the legitimate traffic flow while blocking the DoS attack traffic.*[63]

14.5.5 DDS based defense

More focused on the problem than IPS, a DoS defense system (DDS) can block connection-based DoS attacks and those with legitimate content but bad intent. A DDS can also address both protocol attacks (such as teardrop and ping of death) and rate-based attacks (such as ICMP floods and SYN floods).

14.5.6 Firewalls

In the case of a simple attack, a **firewall** could have a simple rule added to deny all incoming traffic from the attackers, based on protocols, ports or the originating IP addresses.

More complex attacks will however be hard to block with simple rules: for example, if there is an ongoing attack on port 80 (web service), it is not possible to drop all incoming traffic on this port because doing so will prevent the server from serving legitimate traffic.*[64] Additionally, firewalls may be too deep in the network hierarchy, with routers being adversely affected before the traffic gets to the firewall.

14.5.7 Routers

Similar to switches, routers have some rate-limiting and **ACL** capability. They, too, are manually set. Most routers can be easily overwhelmed under a DoS attack. **Cisco IOS** has optional features that can reduce the impact of flooding.*[65]

14.5.8 Switches

Most switches have some rate-limiting and **ACL** capability. Some switches provide automatic and/or system-wide rate limiting, traffic shaping, delayed binding (TCP splicing), deep packet inspection and Bogon filtering (bogus IP filtering) to detect and remediate DoS attacks through automatic rate filtering and WAN Link failover and balancing.*[17]

These schemes will work as long as the DoS attacks can be prevented by using them. For example, SYN flood can be prevented using delayed binding or TCP splicing. Similarly content based DoS may be prevented using deep packet inspection. Attacks originating from **dark addresses** or going to dark addresses can be prevented using **bogon filtering**. Automatic rate filtering can work as long as set rate-thresholds have been set correctly. Wan-link failover will work as long as both links have DoS/DDoS prevention mechanism.*[17]

14.5.9 Upstream filtering

All traffic is passed through a “cleaning center” or a “scrubbing center” via various methods such as proxies, tunnels, digital cross connects, or even direct circuits, which separates “bad” traffic (DDoS and also other common internet attacks) and only sends good traffic beyond to the server. The provider needs central connectivity to the Internet to manage this kind of service unless they happen to be located within the same facility as the “cleaning center” or “scrubbing center”.*[66]

Examples of providers of this service:

- Akamai Technologies*[67]
- CloudFlare*[68]
- Level 3 Communications*[69]
- Radware*[70]
- Arbor Networks*[71]
- AT&T*[72]
- F5 Networks*[73]
- Incapsula*[74]
- Neustar Inc*[75]
- Tata Communications*[76]
- Verisign*[77]
- Verizon*[78]*[79]

14.6 Unintentional denial-of-service

An unintentional denial-of-service can occur when a system ends up denied, not due to a deliberate attack by a single individual or group of individuals, but simply due to a sudden enormous spike in popularity. This can happen when an extremely popular website posts a prominent link to a second, less well-prepared site, for example, as part of a news story. The result is that a significant proportion of the primary site's regular users – potentially hundreds of thousands of people – click that link in the space of a few hours, having the same effect on the target website as a DDoS attack. A VIPDoS is the same, but specifically when the link was posted by a celebrity.

When Michael Jackson died in 2009, websites such as Google and Twitter slowed down or even crashed.*[80] Many sites' servers thought the requests were from a virus or spyware trying to cause a denial-of-service attack, warning users that their queries looked like “automated requests from a computer virus or spyware application”.*[81]

News sites and link sites – sites whose primary function is to provide links to interesting content elsewhere on the Internet – are most likely to cause this phenomenon. The canonical example is the **Slashdot effect** when receiving traffic from **Slashdot**. It is also known as “the **Reddit hug of death**” and “the **Digg effect**”.

Routers have also been known to create unintentional DoS attacks, as both **D-Link** and **Netgear** routers have overloaded NTP servers by flooding NTP servers without respecting the restrictions of client types or geographical limitations.

Similar unintentional denials-of-service can also occur via other media, e.g. when a URL is mentioned on television. If a server is being indexed by Google or another search engine during peak periods of activity, or does not have a lot of available bandwidth while being indexed, it can also experience the effects of a DoS attack.*[17]

Legal action has been taken in at least one such case. In 2006, Universal Tube & Rollform Equipment Corporation sued YouTube: massive numbers of would-be youtube.com users accidentally typed the tube company's URL, utube.com. As a result, the tube company ended up having to spend large amounts of money on upgrading their bandwidth.*[82] The company appears to have taken advantage of the situation, with utube.com now containing ads for advertisement revenue.

In March 2014, after Malaysia Airlines Flight 370 went missing, DigitalGlobe launched a crowdsourcing service on which users could help search for the missing jet in satellite images. The response overwhelmed the company's servers.*[83]

An unintentional denial-of-service may also result from a prescheduled event created by the website itself, as was the case of the Census in Australia in 2016. This could be caused when a server provides some service at a specific time. This might be a university website setting the grades to be available where it will result in many more login requests at that time than any other.

14.7 Side effects of attacks

14.7.1 Backscatter

See also: Backscatter (email) and Internet background noise

In computer network security, backscatter is a side-effect of a spoofed denial-of-service attack. In this kind of attack, the attacker spoofs (or forges) the source address in IP packets sent to the victim. In general, the victim machine cannot distinguish between the spoofed packets and legitimate packets, so the victim responds to the spoofed packets as it normally would. These response packets are known as backscatter.*[84]

If the attacker is spoofing source addresses randomly, the backscatter response packets from the victim will be sent back to random destinations. This effect can be used by network telescopes as indirect evidence of such attacks.

The term “backscatter analysis” refers to observing backscatter packets arriving at a statistically significant portion of the IP address space to determine characteristics of DoS attacks and victims.

14.8 Legality

See also: Computer crime

Many jurisdictions have laws under which denial-of-service attacks are illegal.

- In the US, denial-of-service attacks may be considered a federal crime under the Computer Fraud and Abuse Act with penalties that include years of imprisonment.*[85] The Computer Crime and Intellectual Property Section of the US Department of Justice handles cases of (D)DoS.
- In European countries, committing criminal denial-of-service attacks may, as a minimum, lead to arrest.*[86] The United Kingdom is unusual in that it specifically outlawed denial-of-service attacks and set a maximum penalty of 10 years in prison with the Police and Justice Act 2006, which amended Section 3 of the Computer Misuse Act 1990.*[87]

On January 7, 2013, Anonymous posted a petition on the whitehouse.gov site asking that DDoS be recognized as a legal form of protest similar to the Occupy protests, the claim being that the similarity in purpose of both are same.*[88]*[89]

14.9 See also

- Application layer DDoS attack
- BASHLITE
- Billion laughs
- Botnet
- Blaster (computer worm)
- DDoS mitigation
- Dendroid (malware)
- Fork bomb
- High Orbit Ion Cannon (HOIC)
- Hit-and-run DDoS
- Industrial espionage
- Infinite loop
- Intrusion detection system
- Low Orbit Ion Cannon (LOIC)
- Network intrusion detection system
- October 2016 Dyn cyberattack
- Project Shield
- ReDoS
- Resource exhaustion attack
- SlowDroid
- Slowloris (computer security)
- UDP Unicorn
- Virtual sit-in
- Warzapping
- Wireless signal jammer
- XML denial-of-service attack
- Xor DDoS
- Zemra
- Zombie (computer science)

14.10 References

- [1] “Understanding Denial-of-Service Attacks” . US-CERT. 6 February 2013. Retrieved 26 May 2016.
- [2] Prince, Matthew (25 April 2016). “Empty DDoS Threats: Meet the Armada Collective” . *CloudFlare*. Retrieved 18 May 2016.
- [3] “Brand.com President Mike Zammuto Reveals Blackmail Attempt” . 5 March 2014. Archived from the original on 11 March 2014.
- [4] “Brand.com’s Mike Zammuto Discusses Meetup.com Extortion” . 5 March 2014. Archived from the original on 13 May 2014.
- [5] “The Philosophy of Anonymous” . Radicalphilosophy.com. 2010-12-17. Retrieved 2013-09-10.
- [6] Smith, Steve. “5 Famous Botnets that held the internet hostage” . tqawebly. Retrieved November 20, 2014.
- [7] Taghavi Zargar, Saman (November 2013). “A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks” (PDF). IEEE COMMUNICATIONS SURVEYS & TUTORIALS. pp. 2046–2069. Retrieved 2014-03-07.
- [8] Goodin, Dan (28 September 2016). “Record-breaking DDoS reportedly delivered by >145k hacked cameras” . Ars Technica. Archived from the original on 2 October 2016.
- [9] Khandelwal, Swati (26 September 2016). “World’s largest 1 Tbps DDoS Attack launched from 152,000 hacked Smart Devices” . The Hacker News. Archived from the original on 30 September 2016.
- [10] Lee, Newton (2013). *Counterterrorism and Cybersecurity: Total Information Awareness*. Springer. ISBN 9781461472056.
- [11] “Layer Seven DDoS Attacks” . Infosec Institute.
- [12] “Gartner Says 25 Percent of Distributed Denial of Services Attacks in 2013 Will Be Application - Based” . Gartner. 21 February 2013. Retrieved 28 January 2014.
- [13] Ginovsky, John (27 January 2014). “What you should know about worsening DDoS attacks” . ABA Banking Journal. Retrieved 28 January 2014.
- [14] “Q4 2014 State of the Internet - Security Report: Numbers - The Akamai Blog” . blogs.akamai.com.
- [15] Higgins, Kelly Jackson (17 October 2013). “DDoS Attack Used ‘Headless’ Browser In 150-Hour Siege” . Dark Reading. InformationWeek. Archived from the original on January 22, 2014. Retrieved 28 January 2014.
- [16] Raghavan, S.V. (2011). *An Investigation into the Detection and Mitigation of Denial of Service (DoS) Attacks*. Springer. ISBN 9788132202776.
- [17] Kiyuna and Conyers (2015). *Cyberwarfare Sourcebook*. ISBN 1329063945.
- [18] Gold, Steve (21 August 2014). “Video games company hit by 38-day DDoS attack” . SC Magazine UK. Retrieved 4 February 2016.
- [19] Krebs, Brian (August 15, 2015). “Stress-Testing the Booter Services, Financially” . Krebs on Security. Retrieved 2016-09-09.
- [20] McDowell, Mindi (November 4, 2009). “Cyber Security Tip ST04-015 - Understanding Denial-of-Service Attacks” . United States Computer Emergency Readiness Team. Archived from the original on 2013-11-04. Retrieved December 11, 2013.
- [21] Dittrich, David (December 31, 1999). “The “stacheldraht” distributed denial of service attack tool” . University of Washington. Retrieved 2013-12-11.
- [22] Glenn Greenwald (2014-07-15). “HACKING ONLINE POLLS AND OTHER WAYS BRITISH SPIES SEEK TO CONTROL THE INTERNET” . The Intercept_. Retrieved 2015-12-25.
- [23] “Amazon CloudWatch” . Amazon Web Services, Inc.
- [24] Encyclopaedia Of Information Technology. Atlantic Publishers & Distributors. 2007. p. 397. ISBN 81-269-0752-5.
- [25] Schwabach, Aaron (2006). *Internet and the Law*. ABC-CLIO. p. 325. ISBN 1-85109-731-7.
- [26] Lu, Xicheng; Wei Zhao (2005). *Networking and Mobile Computing*. Birkhäuser. p. 424. ISBN 3-540-28102-9.

- [27] “Has Your Website Been Bitten By a Zombie?”. Cloudbric. 3 August 2015. Retrieved 15 September 2015.
- [28] Boyle, Phillip (2000). “SANS Institute – Intrusion Detection FAQ: Distributed Denial of Service Attack Tools: n/a” . SANS Institute. Retrieved 2008-05-02.
- [29] Leyden, John (2004-09-23). “US credit card firm fights DDoS attack” . *The Register*. Retrieved 2011-12-02.
- [30] Swati Khandelwal (23 October 2015). “Hacking CCTV Cameras to Launch DDoS Attacks” . *The Hacker News*.
- [31] Zeifman, Igal; Gayer, Ofer; Wilder, Or (21 October 2015). “CCTV DDoS Botnet In Our Own Back Yard” . *incapsula.com*.
- [32] “Who’s Behind DDoS Attacks and How Can You Protect Your Website?”. Cloudbric. 10 September 2015. Retrieved 15 September 2015.
- [33] Solon, Olivia (9 September 2015). “Cyber-Extortionists Targeting the Financial Sector Are Demanding Bitcoin Ransoms” . Bloomberg. Retrieved 15 September 2015.
- [34] Greenberg, Adam (14 September 2015). “Akamai warns of increased activity from DDoS extortion group” . SC Magazine. Retrieved 15 September 2015.
- [35] “OWASP Plan - Strawman - Layer_7_DDOS.pdf” (PDF). *Open Web Application Security Project*. 18 March 2014. Retrieved 18 March 2014.
- [36] “Types of DDoS Attacks” . *Distributed Denial of Service Attacks(DDoS) Resources, Pervasive Technology Labs at Indiana University*. Advanced Networking Management Lab (ANML). December 3, 2009. Archived from the original on 2010-09-14. Retrieved December 11, 2013.
- [37] Paul Sop (May 2007). “Prolexic Distributed Denial of Service Attack Alert” . Prolexic Technologies Inc. Prolexic Technologies Inc. Archived from the original on 2007-08-03. Retrieved 2007-08-22.
- [38] Robert Lemos (May 2007). “Peer-to-peer networks co-opted for DOS attacks” . SecurityFocus. Retrieved 2007-08-22.
- [39] Fredrik Ullner (May 2007). “Denying distributed attacks” . DC++: Just These Guys, Ya Know?. Retrieved 2007-08-22.
- [40] Leyden, John (2008-05-21). “Phlashing attack thrashes embedded systems” . *The Register*. Retrieved 2009-03-07.
- [41] Jackson Higgins, Kelly (May 19, 2008). “Permanent Denial-of-Service Attack Sabotages Hardware” . Dark Reading. Archived from the original on December 8, 2008.
- [42] “EUSecWest Applied Security Conference: London, U.K.” . EUSecWest. 2008. Archived from the original on 2009-02-01.
- [43] Rossow, Christian (February 2014). “Amplification Hell: Revisiting Network Protocols for DDoS Abuse” (PDF). Internet Society. Retrieved 4 February 2016.
- [44] Paxson, Vern (2001). “An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks” . ICIR.org.
- [45] “Alert (TA14-017A) UDP-based Amplification Attacks” . US-CERT. July 8, 2014. Retrieved 2014-07-08.
- [46] van Rijswijk-Deij, Roland (2014). “DNSSEC and its potential for DDoS attacks - a comprehensive measurement study” . ACM Press.
- [47] Adamsky, Florian (2015). “P2P File-Sharing in Hell: Exploiting BitTorrent Vulnerabilities to Launch Distributed Reflective DoS Attacks” .
- [48] Vaughn, Randal; Evron, Gadi (2006). “DNS Amplification Attacks” (PDF). ISOTF. Archived from the original (PDF) on 2010-12-14.
- [49] “Alert (TA13-088A) DNS Amplification Attacks” . US-CERT. July 8, 2013. Retrieved 2013-07-17.
- [50] Yu Chen; Kai Hwang; Yu-Kwong Kwok (2005). “Filtering of shrew DDoS attacks in frequency domain” . *The IEEE Conference on Local Computer Networks 30th Anniversary (LCN'05)*. pp. 8 pp. ISBN 0-7695-2421-4. doi:10.1109/LCN.2005.70.
- [51] Ben-Porat, U.; Bremler-Barr, A.; Levy, H. (2013-05-01). “Vulnerability of Network Mechanisms to Sophisticated DDoS Attacks” . *IEEE Transactions on Computers*. **62** (5): 1031–1043. ISSN 0018-9340. doi:10.1109/TC.2012.49.
- [52] orbitalsatelite. “Slow HTTP Test” . SourceForge.
- [53] “RFC 4987 – TCP SYN Flooding Attacks and Common Mitigations” . Tools.ietf.org. August 2007. Retrieved 2011-12-02.

- [54] “CERT Advisory CA-1997-28 IP Denial-of-Service Attacks” . CERT. 1998. Retrieved July 18, 2014.
- [55] “Windows 7, Vista exposed to ‘teardrop attack’”. ZDNet. September 8, 2009. Retrieved 2013-12-11.
- [56] “Microsoft Security Advisory (975497): Vulnerabilities in SMB Could Allow Remote Code Execution” . Microsoft.com. September 8, 2009. Retrieved 2011-12-02.
- [57] “FBI —Phony Phone Calls Distract Consumers from Genuine Theft” . FBI.gov. 2010-05-11. Retrieved 2013-09-10.
- [58] “Internet Crime Complaint Center’s (IC3) Scam Alerts January 7, 2013” . IC3.gov. 2013-01-07. Retrieved 2013-09-10.
- [59] Loukas, G.; Oke, G. (September 2010) [August 2009]. “Protection Against Denial of Service Attacks: A Survey” (PDF). *Comput. J.* **53** (7): 1020–1037. doi:10.1093/comjnl/bxp078.
- [60] Alqahtani, S.; Gamble, R. F. (1 January 2015). “DDoS Attacks in Service Clouds” . *2015 48th Hawaii International Conference on System Sciences (HICSS)*: 5331–5340. doi:10.1109/HICSS.2015.627.
- [61] Kousiouris, George (2014). “KEY COMPLETION INDICATORS:minimizing the effect of DoS attacks on elastic Cloud-based applications based on application-level markov chain checkpoints” . *CLOSER Conference*. Retrieved 2015-05-24.
- [62] Patrikakis, C.; Masiros, M.; Zouraraki, O. (December 2004). “Distributed Denial of Service Attacks” . *The Internet Protocol Journal*. **7** (4): 13–35.
- [63] Abante, Carl (March 2, 2013). “Relationship between Firewalls and Protection against DDoS” . *Ecommerce Wisdom*. Retrieved 2013-05-24.
- [64] Froutan, Paul (June 24, 2004). “How to defend against DDoS attacks” . *Computerworld*. Retrieved May 15, 2010.
- [65] Suzen, Mehmet. “Some IoT tips for Internet Service (Providers)” (PDF). Archived from the original (PDF) on 2008-09-10.
- [66] “DDoS Mitigation via Regional Cleaning Centers (Jan 2004)” (PDF). SprintLabs.com. Sprint ATL Research. Archived from the original (PDF) on 2008-09-21. Retrieved 2011-12-02.
- [67] Lunden, Ingrid (December 2, 2013). “Akamai Buys DDoS Prevention Specialist Prolexic For \$370M To Ramp Up Security Offerings For Enterprises” . TechCrunch. Retrieved September 23, 2014.
- [68] Gallagher, Sean. “Biggest DDoS ever aimed at Cloudflare’s content delivery network” . Ars Technica. Retrieved 18 May 2016.
- [69] “Level 3 DDoS Mitigation” . level3.com. Retrieved 9 May 2016.
- [70] “Defensepipe” . radware.com. Retrieved 9 November 2015.
- [71] “Clean Pipes DDoS Protection and Mitigation from Arbor Networks & Cisco” . ArborNetworks.com. 8 August 2013.
- [72] “AT&T Internet Protect Distributed Denial of Service Defense” (PDF). ATT.com (Product brief). 16 October 2012.
- [73] “Silverline DDoS Protection service” . f5.com. Retrieved 24 March 2015.
- [74] “Infrastructure DDos Protection” . incapsula.com. Retrieved 10 June 2015.
- [75] “DDoS Protection” . Neustar.biz. Retrieved 13 November 2014.
- [76] “DDoS Protection with Network Agnostic Option” . Tatacommunications.com. 7 September 2011.
- [77] “VeriSign Rolls Out DDoS Monitoring Service” . Darkreading.com. 11 September 2009. Retrieved 2 December 2011.
- [78] “Security: Enforcement and Protection” . Verizon.com. Retrieved 10 January 2015.
- [79] “Verizon Digital Media Services Launches Cloud-Based Web Application Firewall That Increases Defenses Against Cyberattacks” . Verizon.com. Retrieved 10 January 2015.
- [80] Shiels, Maggie (2009-06-26). “Web slows after Jackson’s death” . BBC News.
- [81] “We’re Sorry. Automated Query error” . Google Product Forums > Google Search Forum. Google.com. October 20, 2009. Retrieved 2012-02-11.
- [82] “YouTube sued by sound-alike site” . BBC News. 2006-11-02.
- [83] Bill Chappell (12 March 2014). “People Overload Website, Hoping To Help Search For Missing Jet” . NPR. Retrieved 4 February 2016.

- [84] "Backscatter Analysis (2001)". *Animations* (video). Cooperative Association for Internet Data Analysis. Retrieved December 11, 2013.
- [85] "United States Code: Title 18,1030. Fraud and related activity in connection with computers | Government Printing Office" . www.gpo.gov. 2002-10-25. Retrieved 2014-01-15.
- [86] "International Action Against DD4BC Cybercriminal Group" . EUROPOL. 12 January 2016.
- [87] "Computer Misuse Act 1990" . legislation.gov.uk —The National Archives, of UK. 10 January 2008.
- [88] "Anonymous DDoS Petition: Group Calls On White House To Recognize Distributed Denial Of Service As Protest." . HuffingtonPost.com. 2013-01-12.
- [89] "DDOS Attack: crime or virtual sit-in?". RT.com. YouTube.com. October 6, 2011.

14.11 Further reading

- Ethan Zuckerman; Hal Roberts; Ryan McGrady; Jillian York; John Palfrey (December 2011). "Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites" (PDF). The Berkman Center for Internet & Society at Harvard University. Archived from the original (PDF) on 2011-03-02. Retrieved 2011-03-02.
- "DDOS Public Media Reports" . Harvard. Archived from the original on 2011-03-02.
- PC World - Application Layer DDoS Attacks are Becoming Increasingly Sophisticated

14.12 External links

- RFC 4732 Internet Denial-of-Service Considerations
- Akamai State of the Internet Security Report - Quarterly Security and Internet trend statistics
- W3C The World Wide Web Security FAQ
- cert.org CERT's Guide to DoS attacks. (historic document)
- ATLAS Summary Report – Real-time global report of DDoS attacks.
- Low Orbit Ion Cannon - The Well Known Network Stress Testing Tool
- High Orbit Ion Cannon - A Simple HTTP Flooder
- LOIC SLOW An Attempt to Bring SlowLoris and Slow Network Tools on LOIC

Chapter 15

Malware

Malware, short for **malicious software**, is an umbrella term used to refer to a variety of forms of hostile or intrusive software,^{*[1]} including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software.^{*[2]} Malware is defined by its malicious intent, acting against the requirements of the computer user - and so does not include software that causes unintentional harm due to some deficiency.

Programs supplied officially by companies can be considered malware if they secretly act against the interests of the computer user. An example is the **Sony rootkit**, a Trojan horse embedded into **CDs** sold by **Sony**, which silently installed and concealed itself on purchasers' computers with the intention of preventing illicit copying; it also reported on users' listening habits, and unintentionally created vulnerabilities that were exploited by unrelated malware.^{*[3]}

Software such as **anti-virus** and **firewalls** are used to protect against activity identified as malicious, and to recover from attacks.^{*[4]}

15.1 Purposes

Many early infectious programs, including the **first Internet Worm**, were written as experiments or pranks. Today, malware is used by both **black hat hackers** and governments, to steal personal, financial, or business information.^{*[5]*[6]}

Malware is sometimes used broadly against government or corporate websites to gather guarded information,^{*[7]} or to disrupt their operation in general. However, malware is often used against individuals to gain information such as personal identification numbers or details, bank or credit card numbers, and passwords.

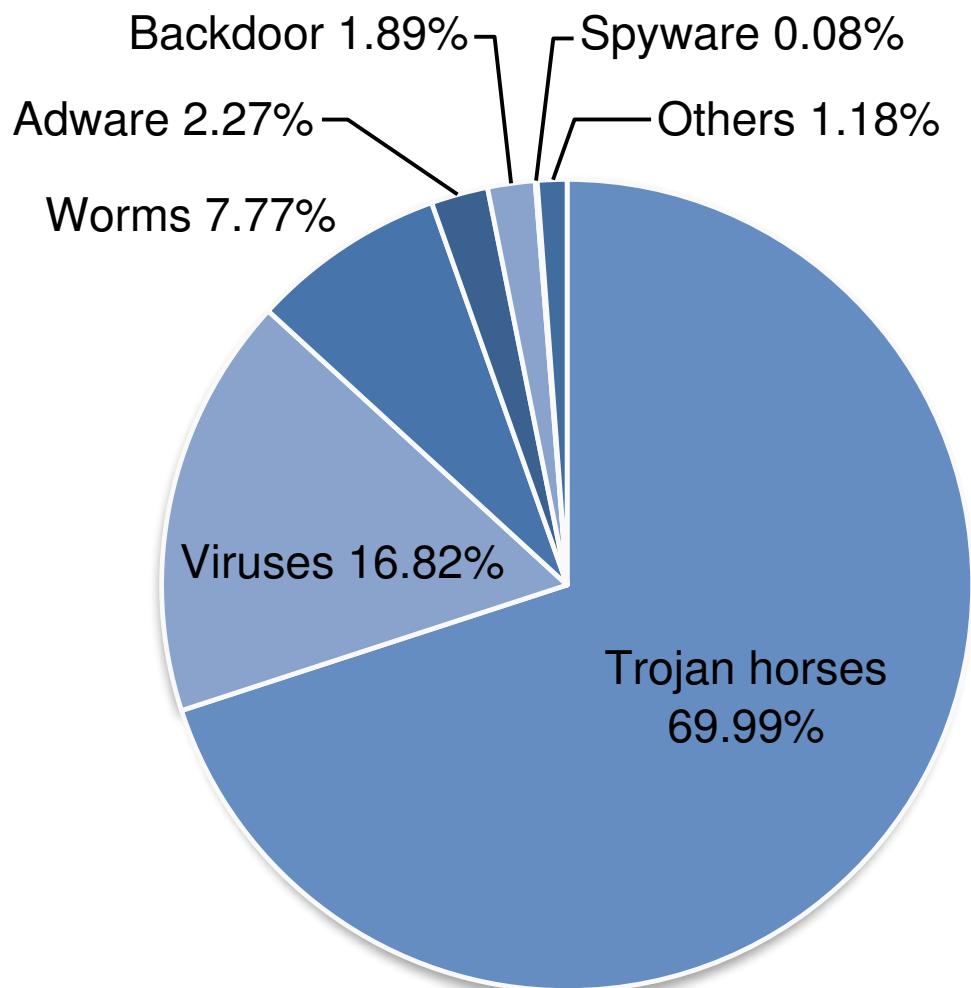
Since the rise of widespread **broadband Internet access**, malicious software has more frequently been designed for profit. Since 2003, the majority of widespread **viruses** and **worms** have been designed to take control of users' computers for illicit purposes.^{*[8]} Infected "zombie computers" are used to send **email spam**, to host contraband data such as **child pornography**,^{*[9]} or to engage in **distributed denial-of-service attacks** as a form of extortion.^{*[10]}

Programs designed to monitor users' web browsing, display unsolicited advertisements, or redirect affiliate marketing revenues are called **spyware**. Spyware programs do not spread like viruses; instead they are generally installed by exploiting security holes. They can also be hidden and packaged together with unrelated user-installed software.^{*[11]}

Ransomware affects an infected computer in some way, and demands payment to reverse the damage. For example, programs such as **CryptoLocker** encrypt files securely, and only decrypt them on payment of a substantial sum of money.

Some malware is used to generate money by **click fraud**, making it appear that the computer user has clicked an advertising link on a site, generating a payment from the advertiser. It was estimated in 2012 that about 60 to 70% of all active malware used some kind of **click fraud**, and 22% of all ad-clicks were fraudulent.^{*[12]}

In addition to criminal money-making, malware can be used for sabotage, often for political motives. **Stuxnet**, for example, was designed to disrupt very specific industrial equipment. There have been politically motivated attacks that have spread over and shut down large computer networks, including massive deletion of files and corruption of master boot records, described as "computer killing". Such attacks were made on Sony Pictures Entertainment (25



Malware by categories

March 16, 2011

Malware by categories on 16 March 2011.

November 2014, using malware known as **Shamoon** or W32.Disttrack) and Saudi Aramco (August 2012).^{*[13]}^{*[14]}

15.2 Infectious malware

Main articles: Computer virus and Computer worm

The best-known types of malware, **viruses** and **worms**, are known for the manner in which they spread, rather than any specific types of behavior. The term **computer virus** is used for a program that embeds itself in some other **executable** software (including the operating system itself) on the target system without the user's consent and when that is run causes the virus to spread to other **executables**. On the other hand, a **worm** is a stand-alone malware program that *actively* transmits itself over a **network** to infect other computers. These definitions lead to the observation that a virus requires the user to run an infected program or operating system for the virus to spread, whereas a worm spreads itself.^{*[15]}

15.3 Concealment

These categories are not mutually exclusive, so malware may use multiple techniques.*[16] This section only applies to malware designed to operate undetected, not sabotage and ransomware.

See also: [Polymorphic packer](#)

15.3.1 Viruses

Main article: [Computer virus](#)

A computer program usually hidden within another seemingly innocuous program that produces copies of itself and inserts them into other programs or files, and that usually performs a malicious action (such as destroying data).*[17]

15.3.2 Trojan horses

Main article: [Trojan horse \(computing\)](#)

A Trojan horse is a malicious computer program which misrepresents itself to appear useful, routine, or interesting in order to persuade a victim to install it. The term is derived from the Ancient Greek story of the Trojan horse used to invade the city of Troy by stealth.*[18]*[19]*[20]*[21]*[22]

Trojan horses are generally spread by some form of social engineering, for example where a user is duped into executing an e-mail attachment disguised to be unsuspicious, (e.g., a routine form to be filled in), or by drive-by download. Although their payload can be anything, many modern forms act as a backdoor, contacting a controller which can then have unauthorized access to the affected computer.*[23] While Trojan horses and backdoors are not easily detectable by themselves, computers may appear to run slower due to heavy processor or network usage.

Unlike computer viruses and worms, Trojan horses generally do not attempt to inject themselves into other files or otherwise propagate themselves.*[24]

15.3.3 Rootkits

Main article: [Rootkit](#)

Once a malicious program is installed on a system, it is essential that it stays concealed, to avoid detection. Software packages known as *rootkits* allow this concealment, by modifying the host's operating system so that the malware is hidden from the user. Rootkits can prevent a malicious process from being visible in the system's list of processes, or keep its files from being read.*[25]

Some malicious programs contain routines to defend against removal, not merely to hide themselves. An early example of this behavior is recorded in the Jargon File tale of a pair of programs infesting a Xerox CP-V time sharing system:

Each ghost-job would detect the fact that the other had been killed, and would start a new copy of the recently stopped program within a few milliseconds. The only way to kill both ghosts was to kill them simultaneously (very difficult) or to deliberately crash the system.*[26]

15.3.4 Backdoors

Main article: [Backdoor \(computing\)](#)

A backdoor is a method of bypassing normal authentication procedures, usually over a connection to a network such as the Internet. Once a system has been compromised, one or more backdoors may be installed in order to allow access in the future,*[27] invisibly to the user.

The idea has often been suggested that computer manufacturers preinstall backdoors on their systems to provide technical support for customers, but this has never been reliably verified. It was reported in 2014 that US government agencies had been diverting computers purchased by those considered “targets” to secret workshops where software or hardware permitting remote access by the agency was installed, considered to be among the most productive operations to obtain access to networks around the world.*[28] Backdoors may be installed by Trojan horses, worms, implants, or other methods.*[29]*[30]

15.3.5 Evasion

Since the beginning of 2015, a sizable portion of malware utilizes a combination of many techniques designed to avoid detection and analysis.*[31]

- The most common evasion technique is when the malware evades analysis and detection by fingerprinting the environment when executed.*[32]
- The second most common evasion technique is confusing automated tools' detection methods. This allows malware to avoid detection by technologies such as signature-based antivirus software by changing the server used by the malware.*[33]
- The third most common evasion technique is timing-based evasion. This is when malware runs at certain times or following certain actions taken by the user, so it executes during certain vulnerable periods, such as during the boot process, while remaining dormant the rest of the time.
- The fourth most common evasion technique is done by obfuscating internal data so that automated tools do not detect the malware.*[34]
- An increasingly common technique is adware that uses stolen certificates to disable anti-malware and virus protection; technical remedies are available to deal with the adware.*[35]

Nowadays, one of the most sophisticated and stealthy ways of evasion is to use information hiding techniques, namely stegomalware.

15.4 Vulnerability

Main article: [Vulnerability \(computing\)](#)

- In this context, and throughout, what is called the “system” under attack may be anything from a single application, through a complete computer and operating system, to a large network.
- Various factors make a system more vulnerable to malware:

15.4.1 Security defects in software

Malware exploits security defects (security bugs or vulnerabilities) in the design of the operating system, in applications (such as browsers, e.g. older versions of Microsoft Internet Explorer supported by Windows XP*[36]), or in vulnerable versions of browser plugins such as Adobe Flash Player, Adobe Acrobat or Reader, or Java SE.*[37]*[38] Sometimes even installing new versions of such plugins does not automatically uninstall old versions. Security advisories from plug-in providers announce security-related updates.*[39] Common vulnerabilities are assigned CVE IDs and listed in the US National Vulnerability Database. Secunia PSI*[40] is an example of software, free for personal use, that will check a PC for vulnerable out-of-date software, and attempt to update it.

Malware authors target bugs, or loopholes, to exploit. A common method is exploitation of a buffer overrun vulnerability, where software designed to store data in a specified region of memory does not prevent more data than the buffer can accommodate being supplied. Malware may provide data that overflows the buffer, with malicious executable code or data after the end; when this payload is accessed it does what the attacker, not the legitimate software, determines.

15.4.2 Insecure design or user error

Early PCs had to be booted from **floppy disks**. When built-in hard drives became common, the **operating system** was normally started from them, but it was possible to boot from another **boot device** if available, such as a floppy disk, **CD-ROM**, **DVD-ROM**, **USB flash drive** or **network**. It was common to configure the computer to boot from one of these devices when available. Normally none would be available; the user would intentionally insert, say, a CD into the optical drive to boot the computer in some special way, for example, to install an operating system. Even without booting, computers can be configured to execute software on some media as soon as they become available, e.g. to autorun a CD or USB device when inserted.

Malicious software distributors would trick the user into booting or running from an infected device or medium. For example, a virus could make an infected computer add autorunnable code to any USB stick plugged into it. Anyone who then attached the stick to another computer set to autorun from USB would in turn become infected, and also pass on the infection in the same way.*[41] More generally, any device that plugs into a USB port - even lights, fans, speakers, toys, or peripherals such as a digital microscope - can be used to spread malware. Devices can be infected during manufacturing or supply if quality control is inadequate.*[41]

This form of infection can largely be avoided by setting up computers by default to boot from the internal hard drive, if available, and not to autorun from devices.*[41] Intentional booting from another device is always possible by pressing certain keys during boot.

Older email software would automatically open **HTML email** containing potentially malicious **JavaScript** code. Users may also execute disguised malicious email attachments and infected executable files supplied in other ways.

15.4.3 Over-privileged users and over-privileged code

Main article: principle of least privilege

In computing, **privilege** refers to how much a user or program is allowed to modify a system. In poorly designed computer systems, both users and programs can be assigned more privileges than they should be, and malware can take advantage of this. The two ways that malware does this is through overprivileged users and overprivileged code.

Some systems allow all users to modify their internal structures, and such users today would be considered **over-privileged users**. This was the standard operating procedure for early microcomputer and home computer systems, where there was no distinction between an **administrator** or **root**, and a regular user of the system. In some systems, **non-administrator** users are over-privileged by design, in the sense that they are allowed to modify internal structures of the system. In some environments, users are over-privileged because they have been inappropriately granted administrator or equivalent status.

Some systems allow code executed by a user to access all rights of that user, which is known as **over-privileged code**. This was also standard operating procedure for early microcomputer and home computer systems. Malware, running as over-privileged code, can use this privilege to subvert the system. Almost all currently popular operating systems, and also many **scripting applications** allow code too many privileges, usually in the sense that when a user **executes** code, the system allows that code all rights of that user. This makes users vulnerable to malware in the form of **e-mail attachments**, which may or may not be disguised.

15.4.4 Use of the same operating system

- Homogeneity can be a vulnerability. For example, when all computers in a network run the same operating system, upon exploiting one, one **worm** can exploit them all.*[42] In particular, **Microsoft Windows** or **Mac OS X** have such a large share of the market that an exploited vulnerability concentrating on either operating system could subvert a large number of systems. Introducing diversity purely for the sake of robustness, such as adding **Linux** computers, could increase short-term costs for training and maintenance. However, as long as all the nodes are not part of the same **directory service** for authentication, having a few diverse nodes could deter total shutdown of the **network** and allow those nodes to help with recovery of the infected nodes. Such separate, functional redundancy could avoid the cost of a total shutdown, at the cost of increased complexity and reduced usability in terms of **single sign-on** authentication.

15.5 Anti-malware strategies

Main article: Antivirus software

As malware attacks become more frequent, attention has begun to shift from viruses and spyware protection, to malware protection, and programs that have been specifically developed to combat malware. (Other preventive and recovery measures, such as backup and recovery methods, are mentioned in the computer virus article).

15.5.1 Anti-virus and anti-malware software

A specific component of anti-virus and anti-malware software, commonly referred to as an on-access or real-time scanner, hooks deep into the operating system's core or kernel and functions in a manner similar to how certain malware itself would attempt to operate, though with the user's informed permission for protecting the system. Any time the operating system accesses a file, the on-access scanner checks if the file is a 'legitimate' file or not. If the file is identified as malware by the scanner, the access operation will be stopped, the file will be dealt with by the scanner in a pre-defined way (how the anti-virus program was configured during/post installation), and the user will be notified. This may have a considerable performance impact on the operating system, though the degree of impact is dependent on how well the scanner was programmed. The goal is to stop any operations the malware may attempt on the system before they occur, including activities which might exploit bugs or trigger unexpected operating system behavior.

Anti-malware programs can combat malware in two ways:

1. They can provide real time protection against the installation of malware software on a computer. This type of malware protection works the same way as that of antivirus protection in that the anti-malware software scans all incoming network data for malware and blocks any threats it comes across.
2. Anti-malware software programs can be used solely for detection and removal of malware software that has already been installed onto a computer. This type of anti-malware software scans the contents of the Windows registry, operating system files, and installed programs on a computer and will provide a list of any threats found, allowing the user to choose which files to delete or keep, or to compare this list to a list of known malware components, removing files that match.*[43]

Real-time protection from malware works identically to real-time antivirus protection: the software scans disk files at download time, and blocks the activity of components known to represent malware. In some cases, it may also intercept attempts to install start-up items or to modify browser settings. Because many malware components are installed as a result of browser exploits or user error, using security software (some of which are anti-malware, though many are not) to "sandbox" browsers (essentially isolate the browser from the computer and hence any malware induced change) can also be effective in helping to restrict any damage done.

Examples of Microsoft Windows antivirus and anti-malware software include the optional Microsoft Security Essentials* [44] (for Windows XP, Vista, and Windows 7) for real-time protection, the Windows Malicious Software Removal Tool* [45] (now included with Windows (Security) Updates on "Patch Tuesday", the second Tuesday of each month), and Windows Defender (an optional download in the case of Windows XP, incorporating MSE functionality in the case of Windows 8 and later).* [46] Additionally, several capable antivirus software programs are available for free download from the Internet (usually restricted to non-commercial use).* [47] Tests found some free programs to be competitive with commercial ones.* [47] Microsoft's System File Checker can be used to check for and repair corrupted system files.

Some viruses disable System Restore and other important Windows tools such as Task Manager and Command Prompt. Many such viruses can be removed by rebooting the computer, entering Windows safe mode with networking* [48], and then using system tools or Microsoft Safety Scanner.* [49]

Hardware implants can be of any type, so there can be no general way to detect them.

15.5.2 Website security scans

As malware also harms the compromised websites (by breaking reputation, blacklisting in search engines, etc.), some websites offer vulnerability scanning.* [50]* [51]* [52]* [53] Such scans check the website, detect malware, may note

outdated software, and may report known security issues.

15.5.3 “Air gap”isolation or “Parallel Network”

As a last resort, computers can be protected from malware, and infected computers can be prevented from disseminating trusted information, by imposing an “air gap” (i.e. completely disconnecting them from all other networks). However, malware can still cross the air gap in some situations. For example, removable media can carry malware across the gap. In December 2013 researchers in Germany showed one way that an apparent air gap can be defeated.*[54]

“AirHopper”,*[55] “BitWhisper”,*[56] “GSMem” *[57] and “Fansmitter” *[58] are four techniques introduced by researchers that can leak data from air-gapped computers using electromagnetic, thermal and acoustic emissions.

15.6 Grayware

See also: Privacy-invasive software and Potentially unwanted program

Grayware is a term applied to unwanted applications or files that are not classified as malware, but can worsen the performance of computers and may cause security risks.*[59]

It describes applications that behave in an annoying or undesirable manner, and yet are less serious or troublesome than malware. Grayware encompasses spyware, adware, fraudulent dialers, joke programs, remote access tools and other unwanted programs that harm the performance of computers or cause inconvenience. The term came into use around 2004.*[60]

Another term, potentially unwanted program (PUP) or potentially unwanted application (PUA),*[61] refers to applications that would be considered unwanted despite often having been downloaded by the user, possibly after failing to read a download agreement. PUPs include spyware, adware, and fraudulent dialers. Many security products classify unauthorised key generators as grayware, although they frequently carry true malware in addition to their ostensible purpose.

Software maker Malwarebytes lists several criteria for classifying a program as a PUP.*[62] Some adware (using stolen certificates) disables anti-malware and virus protection; technical remedies are available.*[35]

15.7 History of viruses and worms

Before Internet access became widespread, viruses spread on personal computers by infecting the executable boot sectors of floppy disks. By inserting a copy of itself into the machine code instructions in these executables, a virus causes itself to be run whenever a program is run or the disk is booted. Early computer viruses were written for the Apple II and Macintosh, but they became more widespread with the dominance of the IBM PC and MS-DOS system. Executable-infecting viruses are dependent on users exchanging software or boot-able floppies and thumb drives so they spread rapidly in computer hobbyist circles.

The first worms, network-borne infectious programs, originated not on personal computers, but on multitasking Unix systems. The first well-known worm was the Internet Worm of 1988, which infected SunOS and VAX BSD systems. Unlike a virus, this worm did not insert itself into other programs. Instead, it exploited security holes (vulnerabilities) in network server programs and started itself running as a separate process.*[63] This same behavior is used by today's worms as well.*[64]

With the rise of the Microsoft Windows platform in the 1990s, and the flexible macros of its applications, it became possible to write infectious code in the macro language of Microsoft Word and similar programs. These *macro viruses* infect documents and templates rather than applications (executables), but rely on the fact that macros in a Word document are a form of executable code.

15.8 Academic research

Main article: Malware research

The notion of a self-reproducing computer program can be traced back to initial theories about the operation of complex automata.*[65] John von Neumann showed that in theory a program could reproduce itself. This constituted a plausibility result in computability theory. Fred Cohen experimented with computer viruses and confirmed Neumann's postulate and investigated other properties of malware such as detectability and self-obfuscation using rudimentary encryption. His doctoral dissertation was on the subject of computer viruses.*[66] The combination of cryptographic technology as part of the payload of the virus, exploiting it for attack purposes was initialized and investigated from the mid 1990s, and includes initial ransomware and evasion ideas.*[67]

15.9 See also

- Botnet
- Browser hijacking
- Comparison of antivirus software
- Computer security
- Cyber spying
- File binder
- Identity theft
- Industrial espionage
- Linux malware
- Malvertising
- Phishing
- Riskware
- Security in Web apps
- Social engineering (security)
- Targeted threat
- Typosquatting
- Web server overload causes
- Zombie (computer science)

15.10 References

- [1] “Defining Malware: FAQ” . technet.microsoft.com. Retrieved 10 September 2009.
- [2] “An Undirected Attack Against Critical Infrastructure” (PDF). United States Computer Emergency Readiness Team(Us-cert.gov). Retrieved 28 September 2014.
- [3] Russinovich, Mark (2005-10-31). “Sony, Rootkits and Digital Rights Management Gone Too Far”. *Mark's Blog*. Microsoft MSDN. Retrieved 2009-07-29.
- [4] “Protect Your Computer from Malware” . OnGuardOnline.gov. Retrieved 26 August 2013.
- [5] “Malware” . FEDERAL TRADE COMMISSION- CONSUMER INFORMATION. Retrieved 27 March 2014.

- [6] Hernandez, Pedro. “Microsoft Vows to Combat Government Cyber-Spying” . eWeek. Retrieved 15 December 2013.
- [7] Kovacs, Eduard. “MiniDuke Malware Used Against European Government Organizations” . Softpedia. Retrieved 27 February 2013.
- [8] “Malware Revolution: A Change in Target” . March 2007.
- [9] “Child Porn: Malware's Ultimate Evil” . November 2009.
- [10] PC World – Zombie PCs: Silent, Growing Threat.
- [11] “Peer To Peer Information” . NORTH CAROLINA STATE UNIVERSITY. Retrieved 25 March 2011.
- [12] “Another way Microsoft is disrupting the malware ecosystem” . Retrieved 18 February 2015.
- [13] “Shamoon is latest malware to target energy sector” . Retrieved 18 February 2015.
- [14] “Computer-killing malware used in Sony attack a wake-up call” . Retrieved 18 February 2015.
- [15] “computer virus – Encyclopædia Britannica” . Britannica.com. Retrieved 28 April 2013.
- [16] All about Malware and Information Privacy
- [17] “What are viruses, worms, and Trojan horses?”. Indiana University. The Trustees of Indiana University. Retrieved 23 February 2015.
- [18] Landwehr, C. E; A. R Bull; J. P McDermott; W. S Choi (1993). *A taxonomy of computer program security flaws, with examples*. DTIC Document. Retrieved 2012-04-05.
- [19] “Trojan Horse Definition” . Retrieved 2012-04-05.
- [20] “Trojan horse” . Webopedia. Retrieved 2012-04-05.
- [21] “What is Trojan horse? – Definition from Whatis.com” . Retrieved 2012-04-05.
- [22] “Trojan Horse: [coined By MIT-hacker-turned-NSA-spook Dan Edwards] N.” . Retrieved 2012-04-05.
- [23] “What is the difference between viruses, worms, and Trojan horses?”. Symantec Corporation. Retrieved 2009-01-10.
- [24] “VIRUS-L/comp.virus Frequently Asked Questions (FAQ) v2.00 (Question B3: What is a Trojan Horse?)”. 9 October 1995. Retrieved 2012-09-13.
- [25] McDowell, Mindi. “Understanding Hidden Threats: Rootkits and Botnets” . US-CERT. Retrieved 6 February 2013.
- [26] “Catb.org” . Catb.org. Retrieved 15 April 2010.
- [27] Vincentas (11 July 2013). “Malware in SpyWareLoop.com” . Spyware Loop. Retrieved 28 July 2013.
- [28] Staff, SPIEGEL. “Inside TAO: Documents Reveal Top NSA Hacking Unit” . SPIEGEL. Retrieved 23 January 2014.
- [29] Edwards, John. “Top Zombie, Trojan Horse and Bot Threats” . IT Security. Retrieved 25 September 2007.
- [30] Appelbaum, Jacob. “Shopping for Spy Gear:Catalog Advertises NSA Toolbox” . SPIEGEL. Retrieved 29 December 2013.
- [31] Evasive malware
- [32] Kirat, Dhilung; Vigna, Giovanni; Kruegel, Christopher (2014). *Barecloud: bare-metal analysis-based evasive malware detection*. ACM. pp. 287–301. ISBN 978-1-931971-15-7.
- [33] The Four Most Common Evasive Techniques Used by Malware. April 27, 2015.
- [34] Young, Adam; Yung, Moti (1997). “Deniable Password Snatching: On the Possibility of Evasive Electronic Espionage” . *Symp. on Security and Privacy*. IEEE. pp. 224–235. ISBN 0-8186-7828-3.
- [35] Casey, Henry T. (25 November 2015). “Latest adware disables antivirus software” . Tom's Guide. Yahoo.com. Retrieved 25 November 2015.
- [36] “Global Web Browser... Security Trends” (PDF). Kaspersky lab. November 2012.
- [37] Rashid, Fahmida Y. (27 November 2012). “Updated Browsers Still Vulnerable to Attack if Plugins Are Outdated” . pcmag.com.

- [38] Danchev, Dancho (18 August 2011). “Kaspersky: 12 different vulnerabilities detected on every PC” . pcmag.com.
- [39] “Adobe Security bulletins and advisories” . Adobe.com. Retrieved 19 January 2013.
- [40] Rubenking, Neil J. “Secunia Personal Software Inspector 3.0 Review & Rating” . PCMag.com. Retrieved 19 January 2013.
- [41] “USB devices spreading viruses” . CNET. CBS Interactive. Retrieved 18 February 2015.
- [42] “LNCS 3786 – Key Factors Influencing Worm Infection” , U. Kanlayasiri, 2006, web (PDF): SL40-PDF.
- [43] “How Antivirus Software Works?”. Retrieved 2015-10-16.
- [44] “Microsoft Security Essentials” . Microsoft. Retrieved 21 June 2012.
- [45] “Malicious Software Removal Tool” . Microsoft. Archived from the original on 21 June 2012. Retrieved 21 June 2012.
- [46] “Windows Defender” . Microsoft. Archived from the original on 22 June 2012. Retrieved 21 June 2012.
- [47] Rubenking, Neil J. (8 January 2014). “The Best Free Antivirus for 2014” . pcmag.com.
- [48] “How do I remove a computer virus?”. Microsoft. Retrieved 26 August 2013.
- [49] “Microsoft Safety Scanner” . Microsoft. Retrieved 26 August 2013.
- [50] “An example of a website vulnerability scanner” . Unmaskparasites.com. Retrieved 19 January 2013.
- [51] “Redleg's File Viewer. Used to check a webpage for malicious redirects or malicious HTML coding” . Aw-snap.info. Retrieved 19 January 2013.
- [52] “Example Google.com Safe Browsing Diagnostic page” . Google.com. Retrieved 19 January 2013.
- [53] “Safe Browsing (Google Online Security Blog)”. Retrieved 21 June 2012.
- [54] Hanspach, Michael; Goetz, Michael (November 2013). “On Covert Acoustical Mesh Networks in Air” . *Journal of Communications*. doi:10.12720/jcm.8.11.758-767.
- [55] M. Guri, G. Kedma, A. Kachlon and Y. Elovici, “AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies,” *Malicious and Unwanted Software: The Americas (MALWARE), 2014 9th International Conference on*, Fajardo, PR, 2014, pp. 58-67.
- [56] M. Guri, M. Monitz, Y. Mirski and Y. Elovici, “BitWhisper: Covert Signaling Channel between Air-Gapped Computers Using Thermal Manipulations,” *2015 IEEE 28th Computer Security Foundations Symposium*, Verona, 2015, pp. 276-289.
- [57] GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies. Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, and Yuval Elovici, *Ben-Gurion University of the Negev; USENIX Security Symposium 2015*
- [58] <https://arxiv.org/ftp/arxiv/papers/1606/1606.05915.pdf>
- [59] Vincentas (11 July 2013). “Grayware in SpyWareLoop.com” . Spyware Loop. Archived from the original on 15 July 2014. Retrieved 28 July 2013.
- [60] “Threat Encyclopedia – Generic Grayware” . Trend Micro. Retrieved 27 November 2012.
- [61] “Rating the best anti-malware solutions” . ArsTechnica. Retrieved 28 January 2014.
- [62] “PUP Criteria” . malwarebytes.org. Retrieved 13 February 2015.
- [63] William A Hendric (4 September 2014). “Computer Virus history” . *The Register*. Retrieved 29 March 2015.
- [64] “Malware: Types, Protection, Prevention, Detection & Removal - Ultimate Guide” . EasyTechGuides.
- [65] John von Neumann, “Theory of Self-Reproducing Automata” , Part 1: Transcripts of lectures given at the University of Illinois, December 1949, Editor: A. W. Burks, University of Illinois, USA, 1966.
- [66] Fred Cohen, “Computer Viruses” , PhD Thesis, University of Southern California, ASP Press, 1988.
- [67] Young, Adam; Yung, Moti (2004). *Malicious cryptography - exposing cryptovirology*. Wiley. pp. 1–392. ISBN 978-0-7645-4975-5.

15.11 External links

- Malicious Software at DMOZ
- Further Reading: Research Papers and Documents about Malware on IDMARCH (Int. Digital Media Archive)
- Advanced Malware Cleaning – a Microsoft video

Chapter 16

Payload (computing)

In computing and telecommunications, the **payload** is the part of transmitted data that is the actual intended message. The payload excludes any headers or metadata sent solely to facilitate payload delivery.*[1]*[2]

The term is borrowed from transportation, where "payload" refers to the part of the load that *pays* for transportation.

16.1 Security

In computer security, the payload is the part of malware such as worms or viruses which performs the malicious action; deleting data, sending spam or encrypting data.*[3] In addition to the payload, such malware also typically has overhead code aimed at simply spreading itself, or avoiding detection.

16.2 Programming

In computer programming, the most common usage of the term is in the context of message protocols, to differentiate the protocol overhead from the actual data. For example, a JSON web service response might be:

```
{ "data":{ "message":"Hello, world!" } }
```

The string "Hello, world!" is the payload, while the rest is protocol overhead.

16.3 Networks

In the computer networking, data to be transmitted is the payload, but is almost always encapsulated in some type of a "frame" composed of framing bits and a frame check sequence.*[4]*[5] Examples are Ethernet frames, Point-to-Point Protocol (PPP) frames, Fibre Channel frames, and V.42 modem frames.

16.4 See also

- Service data unit

16.5 References

- [1] "Payload definition" . Pcmag.com. 1994-12-01. Retrieved 2012-02-07.
- [2] "Payload definition" . Techterms.com. Retrieved 2012-02-07.
- [3] "Payload definition" . Securityfocus.com. Retrieved 2012-02-07.

- [4] “*RFC 1122: Requirements for Internet Hosts —Communication Layers*” . IETF. October 1989. p. 18. RFC 1122. <https://tools.ietf.org/html/rfc1122#page-18>. Retrieved 2010-06-07.
- [5] “Data Link Layer (Layer 2)”. The TCP/IP Guide. 2005-09-20. Retrieved 2010-01-31.

Chapter 17

Rootkit

A **rootkit** is a collection of computer software, typically malicious, designed to enable access to a computer or areas of its software that would not otherwise be allowed (for example, to an unauthorized user) and often masks its existence or the existence of other software.^{*[1]} The term *rootkit* is a concatenation of "root" (the traditional name of the privileged account on Unix-like operating systems) and the word "kit" (which refers to the software components that implement the tool). The term "rootkit" has negative connotations through its association with malware.^{*[1]}

Rootkit installation can be automated, or an attacker can install it once they've obtained root or Administrator access. Obtaining this access is a result of direct attack on a system, i.e. exploiting a known vulnerability (such as privilege escalation) or a password (obtained by cracking or social engineering tactics like "phishing"). Once installed, it becomes possible to hide the intrusion as well as to maintain privileged access. The key is the root or administrator access. Full control over a system means that existing software can be modified, including software that might otherwise be used to detect or circumvent it.

Rootkit detection is difficult because a rootkit may be able to subvert the software that is intended to find it. Detection methods include using an alternative and trusted operating system, behavioral-based methods, signature scanning, difference scanning, and memory dump analysis. Removal can be complicated or practically impossible, especially in cases where the rootkit resides in the kernel; reinstallation of the operating system may be the only available solution to the problem.^{*[2]} When dealing with firmware rootkits, removal may require hardware replacement, or specialized equipment.

17.1 History

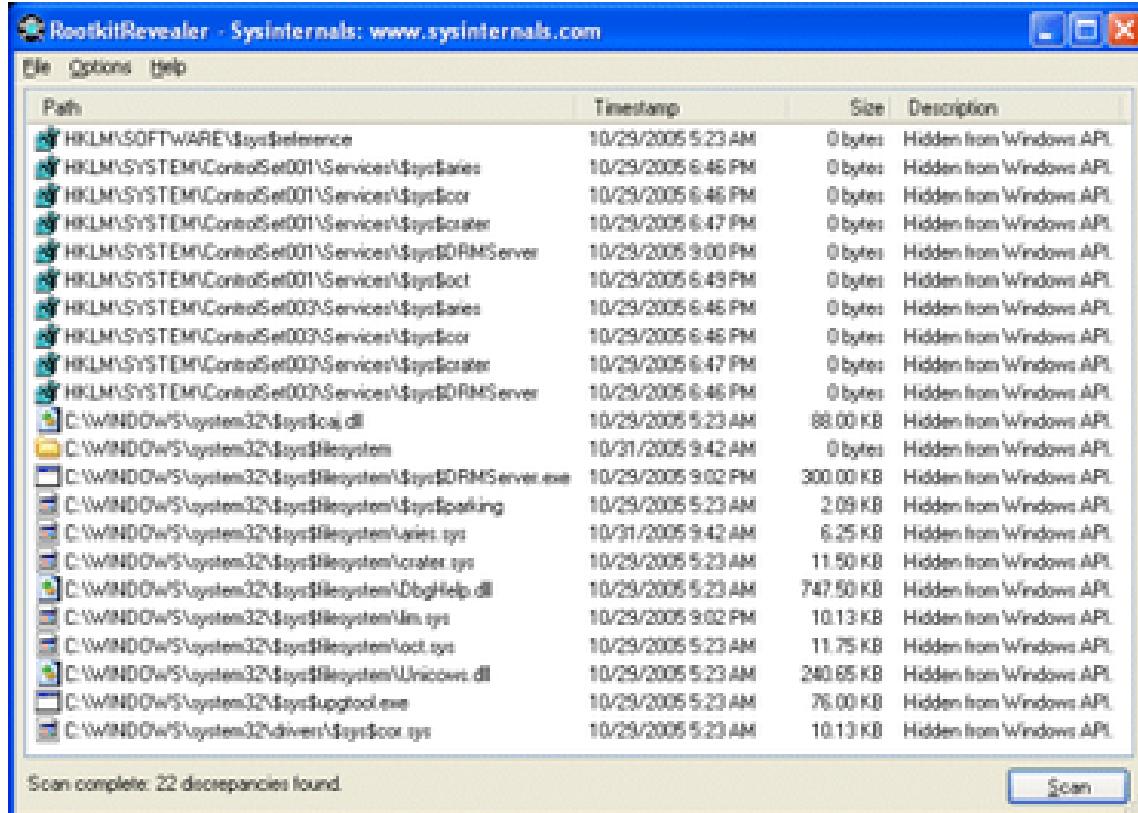
The term *rootkit* or *root kit* originally referred to a maliciously modified set of administrative tools for a Unix-like operating system that granted "root" access.^{*[3]} If an intruder could replace the standard administrative tools on a system with a rootkit, the intruder could obtain root access over the system whilst simultaneously concealing these activities from the legitimate system administrator. These first-generation rootkits were trivial to detect by using tools such as *Tripwire* that had not been compromised to access the same information.^{*[4]*[5]} Lane Davis and Steven Dake wrote the earliest known rootkit in 1990 for Sun Microsystems' SunOS UNIX operating system.^{*[6]} In the lecture he gave upon receiving the Turing award in 1983, Ken Thompson of Bell Labs, one of the creators of Unix, theorized about subverting the C compiler in a Unix distribution and discussed the exploit. The modified compiler would detect attempts to compile the Unix login command and generate altered code that would accept not only the user's correct password, but an additional "backdoor" password known to the attacker. Additionally, the compiler would detect attempts to compile a new version of the compiler, and would insert the same exploits into the new compiler. A review of the source code for the login command or the updated compiler would not reveal any malicious code.^{*[7]} This exploit was equivalent to a rootkit.

The first documented computer virus to target the personal computer, discovered in 1986, used cloaking techniques to hide itself: the Brain virus intercepted attempts to read the boot sector, and redirected these to elsewhere on the disk, where a copy of the original boot sector was kept.^{*[1]} Over time, DOS-virus cloaking methods became more sophisticated, with advanced techniques including the hooking of low-level disk INT 13H BIOS interrupt calls to hide unauthorized modifications to files.^{*[1]}

The first malicious rootkit for the Windows NT operating system appeared in 1999: a trojan called *NTRootkit* created

by Greg Hoglund.* [8] It was followed by *HackerDefender* in 2003.* [1] The first rootkit targeting Mac OS X appeared in 2009,* [9] while the Stuxnet worm was the first to target programmable logic controllers (PLC).* [10]

17.1.1 Sony BMG copy protection rootkit scandal



Screenshot of RootkitRevealer, showing the files hidden by the Extended Copy Protection rootkit

Main article: Sony BMG copy protection rootkit scandal

In 2005, Sony BMG published CDs with copy protection and digital rights management software called Extended Copy Protection, created by software company First 4 Internet. The software included a music player but silently installed a rootkit which limited the user's ability to access the CD.* [11] Software engineer Mark Russinovich, who created the rootkit detection tool RootkitRevealer, discovered the rootkit on one of his computers.* [1] The ensuing scandal raised the public's awareness of rootkits.* [12] To cloak itself, the rootkit hid from the user any file starting with "\$sys\$". Soon after Russinovich's report, malware appeared which took advantage of that vulnerability of affected systems.* [1] One BBC analyst called it a "public relations nightmare."* [13] Sony BMG released patches to uninstall the rootkit, but it exposed users to an even more serious vulnerability.* [14] The company eventually recalled the CDs. In the United States, a class-action lawsuit was brought against Sony BMG.* [15]

17.1.2 Greek wiretapping case 2004–05

Main article: Greek wiretapping case 2004–05

The Greek wiretapping case of 2004–05, also referred to as Greek Watergate,* [16] involved the illegal telephone tapping of more than 100 mobile phones on the Vodafone Greece network belonging mostly to members of the Greek government and top-ranking civil servants. The taps began sometime near the beginning of August 2004 and were removed in March 2005 without discovering the identity of the perpetrators. The intruders installed a rootkit targeting Ericsson's AXE telephone exchange. According to *IEEE Spectrum*, this was "the first time a rootkit has been observed on a special-purpose system, in this case an Ericsson telephone switch."* [17] The rootkit was designed to patch the

memory of the exchange while it was running, enable wiretapping while disabling audit logs, patch the commands that list active processes and active data blocks, and modify the data block checksum verification command. A “backdoor” allowed an operator with sysadmin status to deactivate the exchange’s transaction log, alarms and access commands related to the surveillance capability.*[17] The rootkit was discovered after the intruders installed a faulty update, which caused SMS texts to be undelivered, leading to an automated failure report being generated. Ericsson engineers were called in to investigate the fault and discovered the hidden data blocks containing the list of phone numbers being monitored, along with the rootkit and illicit monitoring software.

17.2 Uses

Modern rootkits do not elevate access,*[3] but rather are used to make another software payload undetectable by adding stealth capabilities.*[8] Most rootkits are classified as malware, because the payloads they are bundled with are malicious. For example, a payload might covertly steal user passwords, credit card information, computing resources, or conduct other unauthorized activities. A small number of rootkits may be considered utility applications by their users: for example, a rootkit might cloak a CD-ROM-emulation driver, allowing video game users to defeat anti-piracy measures that require insertion of the original installation media into a physical optical drive to verify that the software was legitimately purchased.

Rootkits and their payloads have many uses:

- Provide an attacker with full access via a backdoor, permitting unauthorized access to, for example, steal or falsify documents. One of the ways to carry this out is to subvert the login mechanism, such as the /bin/login program on Unix-like systems or GINA on Windows. The replacement appears to function normally, but also accepts a secret login combination that allows an attacker direct access to the system with administrative privileges, bypassing standard authentication and authorization mechanisms.
- Conceal other malware, notably password-stealing key loggers and computer viruses.*[18]
- Appropriate the compromised machine as a zombie computer for attacks on other computers. (The attack originates from the compromised system or network, instead of the attacker’s system.) “Zombie” computers are typically members of large botnets that can launch denial-of-service attacks, distribute e-mail spam, conduct click fraud, etc.
- Enforcement of digital rights management (DRM).

In some instances, rootkits provide desired functionality, and may be installed intentionally on behalf of the computer user:

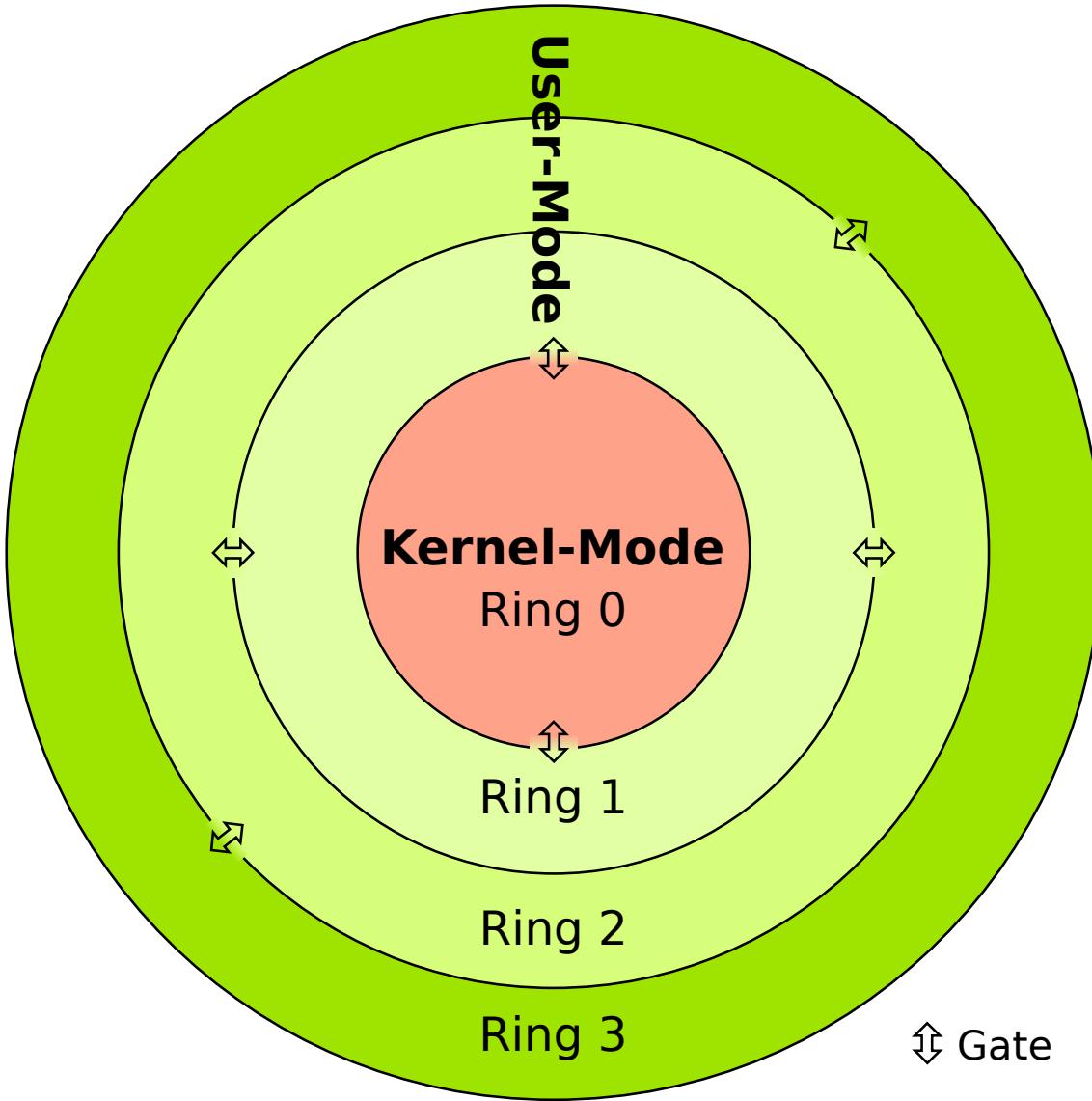
- Conceal cheating in online games from software like Warden.*[19]
- Detect attacks, for example, in a honeypot.*[20]
- Enhance emulation software and security software.*[21] Alcohol 120% and Daemon Tools are commercial examples of non-hostile rootkits used to defeat copy-protection mechanisms such as SafeDisc and SecuROM. Kaspersky antivirus software also uses techniques resembling rootkits to protect itself from malicious actions. It loads its own drivers to intercept system activity, and then prevents other processes from doing harm to itself. Its processes are not hidden, but cannot be terminated by standard methods (It can be terminated with Process Hacker).
- Anti-theft protection: Laptops may have BIOS-based rootkit software that will periodically report to a central authority, allowing the laptop to be monitored, disabled or wiped of information in the event that it is stolen.*[22]
- Bypassing Microsoft Product Activation* [23]

17.3 Types

Further information: Ring (computer security)

There are at least five types of rootkit, ranging from those at the lowest level in firmware (with the highest privileges), through to the least privileged user-based variants that operate in Ring 3. Hybrid combinations of these may occur spanning, for example, user mode and kernel mode.*[24]

17.3.1 User mode



Computer security rings (Note that Ring -1 is not shown)

User-mode rootkits run in Ring 3, along with other applications as user, rather than low-level system processes.*[25] They have a number of possible installation vectors to intercept and modify the standard behavior of application programming interfaces (APIs). Some inject a dynamically linked library (such as a .DLL file on Windows, or a .dylib file on Mac OS X) into other processes, and are thereby able to execute inside any target process to spoof it; others with sufficient privileges simply overwrite the memory of a target application. Injection mechanisms include:*

- Use of vendor-supplied application extensions. For example, Windows Explorer has public interfaces that allow third parties to extend its functionality.
- Interception of messages.
- Debuggers.

- Exploitation of **security vulnerabilities**.
- Function hooking or patching of commonly used APIs, for example, to hide a running process or file that resides on a filesystem.*[26]

...since user mode applications all run in their own memory space, the rootkit needs to perform this patching in the memory space of every running application. In addition, the rootkit needs to monitor the system for any new applications that execute and patch those programs' memory space before they fully execute.

—Windows Rootkit Overview, Symantec*[3]

17.3.2 Kernel mode

Kernel-mode rootkits run with the highest operating system privileges (Ring 0) by adding code or replacing portions of the core operating system, including both the **kernel** and associated **device drivers**. Most operating systems support kernel-mode device drivers, which execute with the same privileges as the operating system itself. As such, many kernel-mode rootkits are developed as device drivers or loadable modules, such as **loadable kernel modules** in Linux or **device drivers** in Microsoft Windows. This class of rootkit has unrestricted security access, but is more difficult to write.*[27] The complexity makes bugs common, and any bugs in code operating at the kernel level may seriously impact system stability, leading to discovery of the rootkit.*[27] One of the first widely known kernel rootkits was developed for Windows NT 4.0 and released in Phrack magazine in 1999 by Greg Hoglund.*[28]*[29]*[30] Kernel rootkits can be especially difficult to detect and remove because they operate at the same **security level** as the operating system itself, and are thus able to intercept or subvert the most trusted operating system operations. Any software, such as **antivirus software**, running on the compromised system is equally vulnerable.*[31] In this situation, no part of the system can be trusted.

A rootkit can modify data structures in the Windows kernel using a method known as *direct kernel object manipulation* (DKOM).* [32] This method can be used to hide processes. A kernel mode rootkit can also hook the **System Service Descriptor Table** (SSDT), or modify the gates between user mode and kernel mode, in order to cloak itself.*[3] Similarly for the **Linux** operating system, a rootkit can modify the *system call table* to subvert kernel functionality.*[33] It's common that a rootkit creates a hidden, encrypted filesystem in which it can hide other malware or original copies of files it has infected.*[34] Operating systems are evolving to counter the threat of kernel-mode rootkits. For example, 64-bit editions of Microsoft Windows now implement mandatory signing of all kernel-level drivers in order to make it more difficult for untrusted code to execute with the highest privileges in a system.*[35]

Bootkits

A kernel-mode rootkit variant called a **bootkit**, it can infect startup code like the **Master Boot Record** (MBR), **Volume Boot Record** (VBR) or **boot sector**, and in this way, can be used to attack **full disk encryption** systems.

An example of such an attack on disk encryption is the “Evil Maid Attack”, in which an attacker installs a bootkit on an unattended computer, replacing the legitimate **boot loader** with one under their control. Typically the malware loader persists through the transition to **protected mode** when the kernel has loaded, and is thus able to subvert the kernel.*[36]*[37]*[38]*[39] For example, the “Stoned Bootkit” subverts the system by using a compromised boot loader to intercept encryption keys and passwords.*[40] More recently, the Alureon rootkit has successfully subverted the requirement for 64-bit kernel-mode driver signing in **Windows 7** by modifying the **master boot record**.* [41] Although not malware in the sense of doing something the user doesn't want, certain “Vista Loader” or “Windows Loader” software works in a similar way by injecting an **ACPI SLIC** (System Licensed Internal Code) table in the RAM-cached version of the BIOS during boot, in order to defeat the **Windows Vista** and **Windows 7** activation process.*[42]*[43] This vector of attack was rendered useless in the (non-server) versions of **Windows 8**, which use a unique, machine-specific key for each system, that can only be used by that one machine.*[44] Many antivirus companies provide free utilities and programs to remove bootkits.

17.3.3 Hypervisor level

Rootkits have been created as Type II **Hypervisors** in academia as proofs of concept. By exploiting hardware virtualization features such as **Intel VT** or **AMD-V**, this type of rootkit runs in Ring –1 and hosts the target operating

system as a virtual machine, thereby enabling the rootkit to intercept hardware calls made by the original operating system.* [5] Unlike normal hypervisors, they do not have to load before the operating system, but can load into an operating system before promoting it into a virtual machine.* [5] A hypervisor rootkit does not have to make any modifications to the kernel of the target to subvert it; however, that does not mean that it cannot be detected by the guest operating system. For example, timing differences may be detectable in CPU instructions.* [5] The “SubVirt” laboratory rootkit, developed jointly by Microsoft and University of Michigan researchers, is an academic example of a virtual machine-based rootkit (VMBR),* [45] while Blue Pill software is another. In 2009, researchers from Microsoft and North Carolina State University demonstrated a hypervisor-layer anti-rootkit called Hooksafe, which provides generic protection against kernel-mode rootkits.* [46] Windows 10 introduced a new feature called “Device Guard”, that takes advantage of virtualization to provide independent external protection of an operating system against rootkit-type malware.* [47]

17.3.4 Firmware and hardware

A firmware rootkit uses device or platform firmware to create a persistent malware image in hardware, such as a router, network card,* [48] hard drive, or the system BIOS.* [25]* [49] The rootkit hides in firmware, because firmware is not usually inspected for code integrity. John Heasman demonstrated the viability of firmware rootkits in both ACPI firmware routines* [50] and in a PCI expansion card ROM.* [51] In October 2008, criminals tampered with European credit card-reading machines before they were installed. The devices intercepted and transmitted credit card details via a mobile phone network.* [52] In March 2009, researchers Alfredo Ortega and Anibal Sacco published details of a BIOS-level Windows rootkit that was able to survive disk replacement and operating system re-installation.* [53]* [54]* [55] A few months later they learned that some laptops are sold with a legitimate rootkit, known as Absolute CompuTrace or Absolute LoJack for Laptops, preinstalled in many BIOS images. This is an anti-theft technology system that researchers showed can be turned to malicious purposes.* [22]

Intel Active Management Technology, part of Intel vPro, implements out-of-band management, giving administrators remote administration, remote management, and remote control of PCs with no involvement of the host processor or BIOS, even when the system is powered off. Remote administration includes remote power-up and power-down, remote reset, redirected boot, console redirection, pre-boot access to BIOS settings, programmable filtering for inbound and outbound network traffic, agent presence checking, out-of-band policy-based alerting, access to system information, such as hardware asset information, persistent event logs, and other information that is stored in dedicated memory (not on the hard drive) where it is accessible even if the OS is down or the PC is powered off. Some of these functions require the deepest level of rootkit, a second non-removable spy computer built around the main computer. Sandy Bridge and future chipsets have “the ability to remotely kill and restore a lost or stolen PC via 3G”. Hardware rootkits built into the chipset can help recover stolen computers, remove data, or render them useless, but they also present privacy and security concerns of undetectable spying and redirection by management or hackers who might gain control.

17.4 Installation and cloaking

Rootkits employ a variety of techniques to gain control of a system; the type of rootkit influences the choice of attack vector. The most common technique leverages security vulnerabilities to achieve surreptitious privilege escalation. Another approach is to use a Trojan horse, deceiving a computer user into trusting the rootkit's installation program as benign—in this case, social engineering convinces a user that the rootkit is beneficial.* [27] The installation task is made easier if the principle of least privilege is not applied, since the rootkit then does not have to explicitly request elevated (administrator-level) privileges. Other classes of rootkits can be installed only by someone with physical access to the target system. Some rootkits may also be installed intentionally by the owner of the system or somebody authorized by the owner, e.g. for the purpose of employee monitoring, rendering such subversive techniques unnecessary.* [56] The installation of malicious rootkits is commercially driven, with a pay-per-install (PPI) compensation method typical for distribution.* [57]* [58]

Once installed, a rootkit takes active measures to obscure its presence within the host system through subversion or evasion of standard operating system security tools and application programming interface (APIs) used for diagnosis, scanning, and monitoring. Rootkits achieve this by modifying the behavior of core parts of an operating system through loading code into other processes, the installation or modification of drivers, or kernel modules. Obfuscation techniques include concealing running processes from system-monitoring mechanisms and hiding system files and other configuration data.* [59] It is not uncommon for a rootkit to disable the event logging capacity of an operating

system, in an attempt to hide evidence of an attack. Rootkits can, in theory, subvert *any* operating system activities.^{*[60]} The “perfect rootkit” can be thought of as similar to a “perfect crime”: one that nobody realizes has taken place. Rootkits also take a number of measures to ensure their survival against detection and “cleaning” by antivirus software in addition to commonly installing into Ring 0 (kernel-mode), where they have complete access to a system. These include **polymorphism** (changing so their “signature” is hard to detect), stealth techniques, regeneration, disabling or turning off anti-malware software.^{*[61]} and not installing on **virtual machines** where it may be easier for researchers to discover and analyze them.

17.5 Detection

The fundamental problem with rootkit detection is that if the operating system has been subverted, particularly by a kernel-level rootkit, it cannot be trusted to find unauthorized modifications to itself or its components.^{*[60]} Actions such as requesting a list of running processes, or a list of files in a directory, cannot be trusted to behave as expected. In other words, rootkit detectors that work while running on infected systems are only effective against rootkits that have some defect in their camouflage, or that run with lower user-mode privileges than the detection software in the kernel.^{*[27]} As with **computer viruses**, the detection and elimination of rootkits is an ongoing struggle between both sides of this conflict.^{*[60]} Detection can take a number of different approaches, including looking for virus “signatures” (e.g. antivirus software), integrity checking (e.g. **digital signatures**), difference-based detection (comparison of expected vs. actual results), and behavioral detection (e.g. monitoring CPU usage or network traffic).

For kernel-mode rootkits, detection is considerably more complex, requiring careful scrutiny of the System Call Table to look for hooked functions where the malware may be subverting system behavior,^{*[62]} as well as forensic scanning of memory for patterns that indicate hidden processes. Unix rootkit detection offerings include Zeppoo,^{*[63]} chkrootkit, rkHunter and OSSEC. For Windows, detection tools include Microsoft Sysinternals RootkitRevealer,^{*[64]} Avast! Antivirus, Sophos Anti-Rootkit,^{*[65]} F-Secure,^{*[66]} Radix,^{*[67]} GMER,^{*[68]} and WindowsSCOPE. Any rootkit detectors that prove effective ultimately contribute to their own ineffectiveness, as malware authors adapt and test their code to escape detection by well-used tools.^{*[Notes 1]} Detection by examining storage while the suspect operating system is not operational can miss rootkits not recognised by the checking software, as the rootkit is not active and suspicious behavior is suppressed; conventional anti-malware software running with the rootkit operational may fail if the rootkit hides itself effectively.

17.5.1 Alternative trusted medium

The best and most reliable method for operating-system-level rootkit detection is to shut down the computer suspected of infection, and then to check its **storage** by **booting** from an alternative trusted medium (e.g. a “rescue” CD-ROM or **USB flash drive**).^{*[69]} The technique is effective because a rootkit cannot actively hide its presence if it is not running.

17.5.2 Behavioral-based

The behavioral-based approach to detecting rootkits attempts to infer the presence of a rootkit by looking for rootkit-like behavior. For example, by profiling a system, differences in the timing and frequency of API calls or in overall CPU utilization can be attributed to a rootkit. The method is complex and is hampered by a high incidence of **false positives**. Defective rootkits can sometimes introduce very obvious changes to a system: the **Alureon** rootkit crashed Windows systems after a security update exposed a design flaw in its code.^{*[70]}^{*[71]} Logs from a **packet analyzer**, **firewall**, or **intrusion prevention system** may present evidence of rootkit behaviour in a networked environment.^{*[24]}

17.5.3 Signature-based

Antivirus products rarely catch all viruses in public tests (depending on what is used and to what extent), even though security software vendors incorporate rootkit detection into their products. Should a rootkit attempt to hide during an antivirus scan, a stealth detector may notice; if the rootkit attempts to temporarily unload itself from the system, signature detection (or “fingerprinting”) can still find it. This combined approach forces attackers to implement counterattack mechanisms, or “retro” routines, that attempt to terminate antivirus programs. Signature-based de-

tection methods can be effective against well-published rootkits, but less so against specially crafted, custom-root rootkits.*[60]

17.5.4 Difference-based

Another method that can detect rootkits compares “trusted” raw data with “tainted” content returned by an API. For example, binaries present on disk can be compared with their copies within operating memory (in some operating systems, the in-memory image should be identical to the on-disk image), or the results returned from file system or Windows Registry APIs can be checked against raw structures on the underlying physical disks*[60]*[72]—however, in the case of the former, some valid differences can be introduced by operating system mechanisms like memory relocation or shimming. A rootkit may detect the presence of a such difference-based scanner or virtual machine (the latter being commonly used to perform forensic analysis), and adjust its behaviour so that no differences can be detected. Difference-based detection was used by Russinovich's *RootkitRevealer* tool to find the Sony DRM rootkit.*[1]

17.5.5 Integrity checking

Code signing uses public-key infrastructure to check if a file has been modified since being digitally signed by its publisher. Alternatively, a system owner or administrator can use a cryptographic hash function to compute a “fingerprint” at installation time that can help to detect subsequent unauthorized changes to on-disk code libraries.*[73] However, unsophisticated schemes check only whether the code has been modified since installation time; subversion prior to that time is not detectable. The fingerprint must be re-established each time changes are made to the system: for example, after installing security updates or a service pack. The hash function creates a *message digest*, a relatively short code calculated from each bit in the file using an algorithm that creates large changes in the message digest with even smaller changes to the original file. By recalculating and comparing the message digest of the installed files at regular intervals against a trusted list of message digests, changes in the system can be detected and monitored—as long as the original baseline was created before the malware was added.

More-sophisticated rootkits are able to subvert the verification process by presenting an unmodified copy of the file for inspection, or by making code modifications only in memory, rather than on disk. The technique may therefore be effective only against unsophisticated rootkits—for example, those that replace Unix binaries like "ls" to hide the presence of a file. Similarly, detection in firmware can be achieved by computing a cryptographic hash of the firmware and comparing it to a whitelist of expected values, or by extending the hash value into Trusted Platform Module (TPM) configuration registers, which are later compared to a whitelist of expected values.*[74] The code that performs hash, compare, or extend operations must also be protected—in this context, the notion of an *immutable root-of-trust* holds that the very first code to measure security properties of a system must itself be trusted to ensure that a rootkit or bootkit does not compromise the system at its most fundamental level.*[75]

17.5.6 Memory dumps

Forcing a complete dump of virtual memory will capture an active rootkit (or a kernel dump in the case of a kernel-mode rootkit), allowing offline forensic analysis to be performed with a debugger against the resulting dump file, without the rootkit being able to take any measures to cloak itself. This technique is highly specialized, and may require access to non-public source code or debugging symbols. Memory dumps initiated by the operating system cannot always be used to detect a hypervisor-based rootkit, which is able to intercept and subvert the lowest-level attempts to read memory*[5]—a hardware device, such as one that implements a non-maskable interrupt, may be required to dump memory in this scenario.*[76]*[77] Virtual machines also make it easier to analyze the memory of a compromised machine from the underlying hypervisor, so some rootkits will avoid infecting virtual machines for this reason.

17.6 Removal

Manual removal of a rootkit is often too difficult for a typical computer user,*[25] but a number of security-software vendors offer tools to automatically detect and remove some rootkits, typically as part of an antivirus suite. As of 2005, Microsoft's monthly Windows Malicious Software Removal Tool is able to detect and remove some classes of

```

Terminal — bash — bash (ttyp1) — 96x50 — %1

Your system contains some unknown version numbers. Please run Rootkit Hunter
with the --update parameter or fill in the contact form (www.rootkit.nl)

Security advisories
* Check: Groups and Accounts
  Searching for /etc/passwd...
  Checking users with UID '0' (root)... [ Found ] [ OK ]
* Check: SSH
  Searching for sshd_config...
  Found /etc/sshd_config
  Checking for allowed root login... Watch out Root login possible. Possible risk!
    info:
    Hint: See logfile for more information about this issue
  Checking for allowed protocols... [ Warning (SSH v1 allowed) ]
* Check: Events and Logging
  Search for syslog configuration...
  Checking for running syslog slave...
  Checking for logging to remote system...
    info: install.@

[Press <ENTER> to continue]

----- Scan results -----
MD5
MD5 compared: 0
Incorrect MD5 checksums: 0

File scan
Scanned files: 342
Possible infected files: 0

Application scan
Vulnerable applications: 0

Scanning took 129 seconds

-----
Do you have some problems, undetected rootkits, false positives, ideas
or suggestions?
Please e-mail me by filling in the contact form (http://www.rootkit.nl)
-----
```

The *rkhunter* utility uses *SHA-1* hashes to verify the integrity of system files.

rootkits.*[78]*[79] Also, Windows Defender Offline can remove rootkits, as it runs from a trusted environment before the operating system starts. Some antivirus scanners can bypass file system APIs, which are vulnerable to manipulation by a rootkit. Instead, they access raw filesystem structures directly, and use this information to validate the results from the system APIs to identify any differences that may be caused by a rootkit.*[Notes 2]*[80]*[81]*[82]*[83] There are experts who believe that the only reliable way to remove them is to re-install the operating system from trusted media.*[84]*[85] This is because antivirus and malware removal tools running on an untrusted system may be ineffective against well-written kernel-mode rootkits. Booting an alternative operating system from trusted media can allow an infected system volume to be mounted and potentially safely cleaned and critical data to be copied off—or, alternatively, a forensic examination performed.*[24] Lightweight operating systems such as Windows PE, Windows Recovery Console, Windows Recovery Environment, BartPE, or Live Distros can be used for this purpose, allowing the system to be “cleaned”. Even if the type and nature of a rootkit is known, manual repair may be impractical,

while re-installing the operating system and applications is safer, simpler and quicker.*[84]

17.7 Public availability

Like much malware used by attackers, many rootkit implementations are shared and are easily available on the Internet. It is not uncommon to see a compromised system in which a sophisticated, publicly available rootkit hides the presence of unsophisticated worms or attack tools apparently written by inexperienced programmers.*[24] Most of the rootkits available on the Internet originated as exploits or as academic “proofs of concept” to demonstrate varying methods of hiding things within a computer system and of taking unauthorized control of it.*[86] Often not fully optimized for stealth, such rootkits sometimes leave unintended evidence of their presence. Even so, when such rootkits are used in an attack, they are often effective. Other rootkits with keylogging features such as GameGuard are installed as part of online commercial games.

17.8 Defenses

System **hardening** represents one of the first layers of defence against a rootkit, to prevent it from being able to install.*[87] Applying security patches, implementing the principle of least privilege, reducing the attack surface and installing antivirus software are some standard security best practices that are effective against all classes of malware.*[88] New secure boot specifications like **Unified Extensible Firmware Interface** have been designed to address the threat of bootkits, but even these are vulnerable if the security features they offer are not utilized.*[49] For server systems, remote server attestation using technologies such as Intel Trusted Execution Technology (TXT) provide a way of validating that servers remain in a known good state. For example, Microsoft Bitlocker encrypting data-at-rest validates servers are in a known “good state” on bootup. PrivateCore vCage is a software offering that secures data-in-use (memory) to avoid bootkits and rootkits by validating servers are in a known “good” state on bootup. The PrivateCore implementation works in concert with Intel TXT and locks down server system interfaces to avoid potential bootkits and rootkits.

17.9 See also

- Computer security conference
- Host-based intrusion detection system
- Man-in-the-middle attack
- *The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System*

17.10 Notes

- [1] The process name of Sysinternals RootkitRevealer was targeted by malware; in an attempt to counter this countermeasure, the tool now uses a randomly generated process name.
- [2] In theory, a sufficiently sophisticated kernel-level rootkit could subvert read operations against raw filesystem data structures as well, so that they match the results returned by APIs.

17.11 References

- [1] “Rootkits, Part 1 of 3: The Growing Threat” (PDF). McAfee. 2006-04-17. Archived from the original (PDF) on 2006-08-23.
- [2] <http://www.technibble.com/how-to-remove-a-rootkit-from-a-windows-system/>
- [3] “Windows Rootkit Overview” (PDF). Symantec. 2006-03-26. Retrieved 2010-08-17.

- [4] Sparks, Sherri; Butler, Jamie (2005-08-01). "Raising The Bar For Windows Rootkit Detection" . *Phrack*. **0xb** (0x3d).
- [5] Myers, Michael; Youndt, Stephen (2007-08-07). "An Introduction to Hardware-Assisted Virtual Machine (HVM) Rootkits" . Crucial Security. CiteSeerX: 10.1.1.90.8832.
- [6] Andrew Hay; Daniel Cid; Rory Bray (2008). *OSSEC Host-Based Intrusion Detection Guide*. Syngress. p. 276. ISBN 1-59749-240-X.
- [7] Thompson, Ken (August 1984). "Reflections on Trusting Trust" (PDF). *Communications of the ACM*. **27** (8): 761. doi:10.1145/358198.358210.
- [8] Greg Hoglund; James Butler (2006). *Rootkits: Subverting the Windows kernel*. Addison-Wesley. p. 4. ISBN 0-321-29431-9.
- [9] Dai Zovi, Dino (2009-07-26). *Advanced Mac OS X Rootkits* (PDF). Blackhat. Endgame Systems. Retrieved 2010-11-23.
- [10] "Stuxnet Introduces the First Known Rootkit for Industrial Control Systems" . Symantec. 2010-08-06. Retrieved 2010-12-04.
- [11] "Spyware Detail: XCP.Sony.Rootkit" . Computer Associates. 2005-11-05. Archived from the original on 2010-08-18. Retrieved 2010-08-19.
- [12] Russinovich, Mark (2005-10-31). "Sony, Rootkits and Digital Rights Management Gone Too Far" . *TechNet Blogs*. Microsoft. Retrieved 2010-08-16.
- [13] "Sony's long-term rootkit CD woes" . BBC News. 2005-11-21. Retrieved 2008-09-15.
- [14] Felton, Ed (2005-11-15). "Sony's Web-Based Uninstaller Opens a Big Security Hole; Sony to Recall Discs" .
- [15] Knight, Will (2005-11-11). "Sony BMG sued over cloaking software on music CD" . *New Scientist*. Sutton, UK: Reed Business Information. Retrieved 2010-11-21.
- [16] Kyriakidou, Dina (March 2, 2006). ""Greek Watergate" Scandal Sends Political Shockwaves" . Reuters. Retrieved 2007-11-24.
- [17] Vassilis Prevelakis; Diomidis Spinellis (July 2007). "The Athens Affair" .
- [18] Russinovich, Mark (June 2005). "Unearthing Root Kits" . Windows IT Pro. Retrieved 2010-12-16.
- [19] "World of Warcraft Hackers Using Sony BMG Rootkit" . The Register. 2005-11-04. Retrieved 2010-08-23.
- [20] Steve Hanna (September 2007). "Using Rootkit Technology for Honeypot-Based Malware Detection" (PDF). CCEID Meeting.
- [21] Russinovich, Mark (6 February 2006). "Using Rootkits to Defeat Digital Rights Management" . *Winternals*. SysInternals. Archived from the original on 31 August 2006. Retrieved 2006-08-13.
- [22] Ortega, Alfredo; Sacco, Anibal (2009-07-24). *Deactivate the Rootkit: Attacks on BIOS anti-theft technologies* (PDF). Black Hat USA 2009 (PDF). Boston, MA: Core Security Technologies. Retrieved 2014-06-12.
- [23] Kleissner, Peter (2009-09-02). "Stoned Bootkit: The Rise of MBR Rootkits & Bootkits in the Wild" (PDF). Retrieved 2010-11-23.
- [24] Anson, Steve; Bunting, Steve (2007). *Mastering Windows Network Forensics and Investigation*. John Wiley and Sons. pp. 73–74. ISBN 0-470-09762-0.
- [25] "Rootkits Part 2: A Technical Primer" (PDF). McAfee. 2007-04-03. Archived from the original (PDF) on 2008-12-05. Retrieved 2010-08-17.
- [26] Kdm. "NTIllusion: A portable Win32 userland rootkit" . *Phrack*. **62** (12).
- [27] "Understanding Anti-Malware Technologies" (PDF). Microsoft. 2007-02-21. Retrieved 2010-08-17.
- [28] Hoglund, Greg (1999-09-09). "A *REAL* NT Rootkit, Patching the NT Kernel". *Phrack*. **9** (55). Retrieved 2010-11-21.
- [29] Shevchenko, Alisa (2008-09-01). "Rootkit Evolution" . *Help Net Security*. Help Net Security.
- [30] Chuvakin, Anton (2003-02-02). An Overview of Unix Rootkits (PDF) (Report). Chantilly, Virginia: iDEFENSE. Retrieved 2010-11-21.
- [31] Butler, James; Sparks, Sherri (2005-11-16). "Windows Rootkits of 2005, Part Two" . *Symantec Connect*. Symantec. Retrieved 2010-11-13.

- [32] Butler, James; Sparks, Sherri (2005-11-03). "Windows Rootkits of 2005, Part One" . *Symantec Connect*. Symantec. Retrieved 2010-11-12.
- [33] Burdach, Mariusz (2004-11-17). "Detecting Rootkits And Kernel-level Compromises In Linux" . Symantec. Retrieved 2010-11-23.
- [34] Marco Giuliani (11 April 2011). "ZeroAccess – An Advanced Kernel Mode Rootkit" (PDF). Webroot Software. Retrieved 10 August 2011.
- [35] "Driver Signing Requirements for Windows" . Microsoft. Retrieved 2008-07-06.
- [36] Soeder, Derek; Permeh, Ryan (2007-05-09). "Bootroot" . eEye Digital Security. Archived from the original on 2013-08-17. Retrieved 2010-11-23.
- [37] Schneier, Bruce (2009-10-23). "'Evil Maid' Attacks on Encrypted Hard Drives" . Retrieved 2009-11-07.
- [38] Kumar, Nitin; Kumar, Vipin (2007). *Vbootkit: Compromising Windows Vista Security* (PDF). Black Hat Europe 2007.
- [39] "BOOT KIT: Custom boot sector based Windows 2000/XP/2003 Subversion" . NVlabs. 2007-02-04. Archived from the original on June 10, 2010. Retrieved 2010-11-21.
- [40] Kleissner, Peter (2009-10-19). "Stoned Bootkit" . Peter Kleissner. Retrieved 2009-11-07.
- [41] Goodin, Dan (2010-11-16). "World's Most Advanced Rootkit Penetrates 64-bit Windows" . The Register. Retrieved 2010-11-22.
- [42] Peter Kleissner, "The Rise of MBR Rootkits And Bootkits in the Wild" , Hacking at Random (2009) - text; slides
- [43] Windows Loader - Software Informer. This is the loader application that's used by millions of people worldwide
- [44] Microsoft tightens grip on OEM Windows 8 licensing
- [45] King, Samuel T.; Chen, Peter M.; Wang, Yi-Min; Verbowski, Chad; Wang, Helen J.; Lorch, Jacob R. (2006-04-03). International Business Machines (ed.), ed. *SubVirt: Implementing malware with virtual machines* (PDF). 2006 IEEE Symposium on Security and Privacy. Institute of Electrical and Electronics Engineers. ISBN 0-7695-2574-1. doi:10.1109/SP.2006.38. Retrieved 2008-09-15.
- [46] Wang, Zhi; Jiang, Xuxian; Cui, Weidong; Ning, Peng (2009-08-11). "Countering Kernel Rootkits with Lightweight Hook Protection" (PDF). In Al-Shaer, Ehab (General Chair). *Proceedings of the 16th ACM Conference on Computer and Communications Security*. CCS 2009: 16th ACM Conference on Computer and Communications Security. Jha, Somesh; Keromytis, Angelos D. (Program Chairs). New York: ACM New York. ISBN 978-1-60558-894-0. doi:10.1145/1653662.1653728. Retrieved 2009-11-11.
- [47] [https://msdn.microsoft.com/en-us/library/dn986865\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/dn986865(v=vs.85).aspx)
- [48] Delugré, Guillaume (2010-11-21). *Reversing the Broacom NetExtreme's Firmware* (PDF). hack.lu. Sogeti. Retrieved 2010-11-25.
- [49] <http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-uses-uefi-bios-rootkit-to-keep-rcs-9-agent-in-target-systems/>
- [50] Heasman, John (2006-01-25). *Implementing and Detecting an ACPI BIOS Rootkit* (PDF). Black Hat Federal 2006. NGS Consulting. Retrieved 2010-11-21.
- [51] Heasman, John (2006-11-15). "Implementing and Detecting a PCI Rootkit" (PDF). Next Generation Security Software. CiteSeerX: 10.1.1.89.7305. Retrieved 2010-11-13.
- [52] Modine, Austin (2008-10-10). "Organized crime tampers with European card swipe devices: Customer data beamed overseas" . *The Register*. Situation Publishing. Retrieved 2008-10-13.
- [53] Sacco, Anibal; Ortéga, Alfredo (2009). *Persistent BIOS infection* (PDF). CanSecWest 2009. Core Security Technologies. Retrieved 2010-11-21.
- [54] Goodin, Dan (2009-03-24). "Newfangled rootkits survive hard disk wiping" . *The Register*. Situation Publishing. Retrieved 2009-03-25.
- [55] Sacco, Anibal; Ortéga, Alfredo (2009-06-01). "Persistent BIOS Infection: The Early Bird Catches the Worm" . *Phrack*. 66 (7). Retrieved 2010-11-13.
- [56] Ric Vieler (2007). *Professional Rootkits*. John Wiley & Sons. p. 244. ISBN 9780470149546.

- [57] Matrosov, Aleksandr; Rodionov, Eugene (2010-06-25). “TDL3: The Rootkit of All Evil?” (PDF). Moscow: ESET. p. 3. Retrieved 2010-08-17.
- [58] Matrosov, Aleksandr; Rodionov, Eugene (2011-06-27). “The Evolution of TDL: Conquering x64” (PDF). ESET. Retrieved 2011-08-08.
- [59] Brumley, David (1999-11-16). “Invisible Intruders: rootkits in practice” . USENIX. USENIX.
- [60] Davis, Michael A.; Bodmer, Sean; LeMasters, Aaron (2009-09-03). “Chapter 10: Rootkit Detection” (PDF). *Hacking Exposed Malware & Rootkits: Malware & rootkits security secrets & solutions* (PDF). New York: McGraw Hill Professional. ISBN 978-0-07-159118-8. Retrieved 2010-08-14.
- [61] Trlokom (2006-07-05). “Defeating Rootkits and Keyloggers” (PDF). Trlokom. Retrieved 2010-08-17.
- [62] Dai Zovi, Dino (2011). “Kernel Rootkits” . Archived from the original on September 10, 2012. Retrieved 13 Sep 2012.
- [63] “Zeppo” . SourceForge. 18 July 2009. Retrieved 8 August 2011.
- [64] Cogswell, Bryce; Russinovich, Mark (2006-11-01). “RootkitRevealer v1.71” . Microsoft. Retrieved 2010-11-13.
- [65] “Sophos Anti-Rootkit” . Sophos. Retrieved 8 August 2011.
- [66] “BlackLight” . F-Secure. Retrieved 8 August 2011.
- [67] “Radix Anti-Rootkit” . usec.at. Retrieved 8 August 2011.
- [68] “GMER” . Retrieved 8 August 2011.
- [69] Harriman, Josh (2007-10-19). “A Testing Methodology for Rootkit Removal Effectiveness” (PDF). Dublin, Ireland: Symantec Security Response. Retrieved 2010-08-17.
- [70] Cuibotariu, Mircea (2010-02-12). “Tidserv and MS10-015” . Symantec. Retrieved 2010-08-19.
- [71] “Restart Issues After Installing MS10-015” . Microsoft. 2010-02-11. Retrieved 2010-10-05.
- [72] “Strider GhostBuster Rootkit Detection” . Microsoft Research. 2010-01-28. Retrieved 2010-08-14.
- [73] “Signing and Checking Code with Authenticode” . Microsoft. Retrieved 2008-09-15.
- [74] “Stopping Rootkits at the Network Edge” (PDF). Beaverton, Oregon: Trusted Computing Group. January 2007. Retrieved 2008-07-11.
- [75] “TCG PC Specific Implementation Specification, Version 1.1” (PDF). Trusted Computing Group. 2003-08-18. Retrieved 2010-11-22.
- [76] “How to generate a complete crash dump file or a kernel crash dump file by using an NMI on a Windows-based system” . Microsoft. Retrieved 2010-11-13.
- [77] Seshadri, Arvind; et al. (2005). “Pioneer: Verifying Code Integrity and Enforcing Untampered Code Execution on Legacy Systems” . Carnegie Mellon University.
- [78] Dillard, Kurt (2005-08-03). “Rootkit battle: Rootkit Revealer vs. Hacker Defender” .
- [79] “The Microsoft Windows Malicious Software Removal Tool helps remove specific, prevalent malicious software from computers that are running Windows 7, Windows Vista, Windows Server 2003, Windows Server 2008, or Windows XP” . Microsoft. 2010-09-14.
- [80] Hultquist, Steve (2007-04-30). “Rootkits: The next big enterprise threat?”. *InfoWorld*. IDG. Retrieved 2010-11-21.
- [81] “Security Watch: Rootkits for fun and profit” . CNET Reviews. 2007-01-19. Archived from the original on 2012-10-08. Retrieved 2009-04-07.
- [82] Bort, Julie (2007-09-29). “Six ways to fight back against botnets” . PCWorld. San Francisco: PCWorld Communications. Retrieved 2009-04-07.
- [83] Hoang, Mimi (2006-11-02). “Handling Today's Tough Security Threats: Rootkits” . *Symantec Connect*. Symantec. Retrieved 2010-11-21.
- [84] Danseglio, Mike; Bailey, Tony (2005-10-06). “Rootkits: The Obscure Hacker Attack” . Microsoft.
- [85] Messmer, Ellen (2006-08-26). “Experts Divided Over Rootkit Detection and Removal” . *NetworkWorld.com*. Framingham, Mass.: IDG. Retrieved 2010-08-15.

- [86] Stevenson, Larry; Altholz, Nancy (2007). *Rootkits for Dummies*. John Wiley and Sons Ltd. p. 175. ISBN 0-471-91710-9.
- [87] Skoudis, Ed; Zeltser, Lenny (2004). *Malware: Fighting Malicious Code*. Prentice Hall PTR. p. 335. ISBN 0-13-101405-6.
- [88] Hannel, Jeromey (2003-01-23). “Linux RootKits For Beginners - From Prevention to Removal” . SANS Institute. Archived from the original (PDF) on October 24, 2010. Retrieved 2010-11-22.

17.12 Further reading

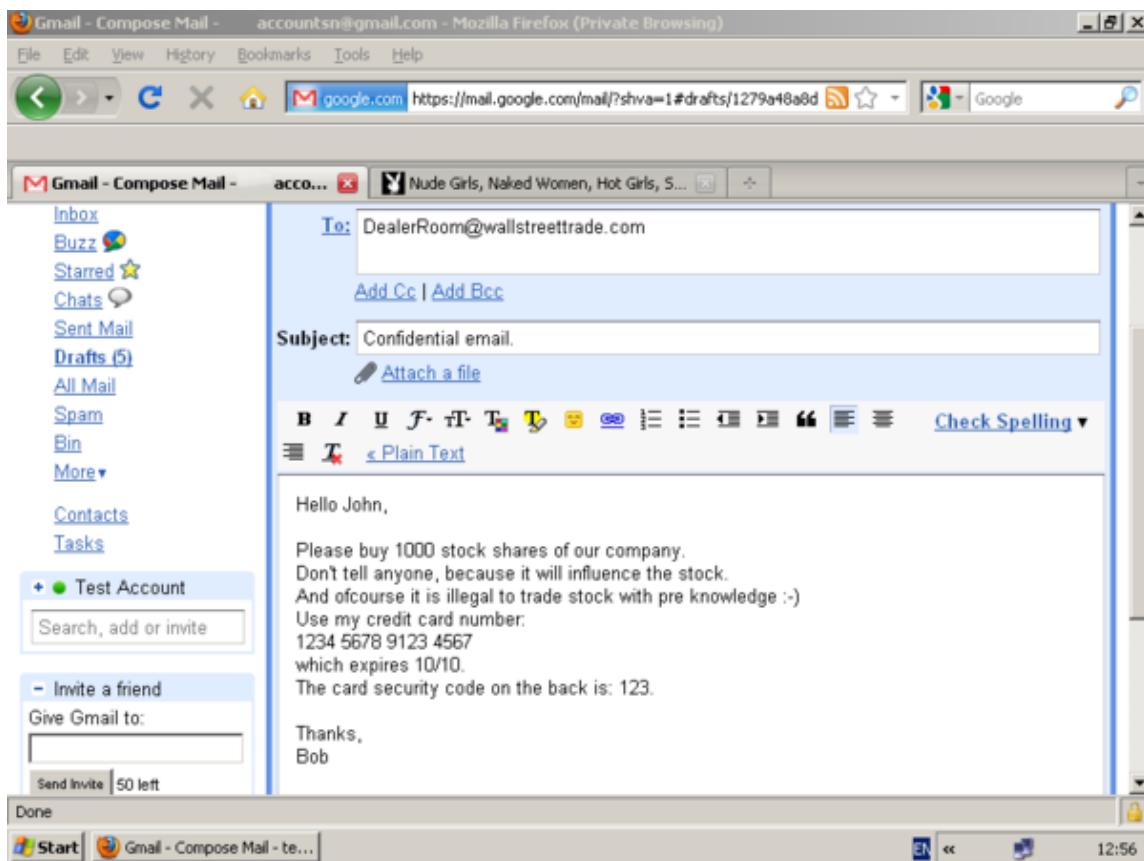
- Blunden, Bill (2009). *The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System*. Wordware. ISBN 978-1-59822-061-2.
- Hoglund, Greg; Butler, James (2005). *Rootkits: Subverting the Windows Kernel*. Addison-Wesley Professional. ISBN 0-321-29431-9.
- Grampp, F. T.; Morris, Robert H., Sr. (October 1984). “The UNIX System: UNIX Operating System Security” . *AT&T Bell Laboratories Technical Journal*. AT&T. **62** (8): 1649–1672.
- Kong, Joseph (2007). *Designing BSD Rootkits*. No Starch Press. ISBN 1-59327-142-5.
- Veiler, Ric (2007). *Professional Rootkits*. Wrox. ISBN 978-0-470-10154-4.

17.13 External links

- Rootkit Analysis: Research and Analysis of Rootkits
- Even Nastier: Traditional RootKits
- Sophos Podcast about rootkit removal
- Rootkit research in Microsoft
- Testing of antivirus/anti-rootkit software for the detection and removal of rootkits, Anti-Malware Test Lab, January 2008
- Testing of anti-rootkit software, InformationWeek, January 2007
- Security Now! Episode 9, Rootkits, Podcast by Steve Gibson/GRC explaining Rootkit technology, October 2005

Chapter 18

Keystroke logging



A keylogger example of a screencapture, which holds potentially confidential and private information. The image below holds the corresponding keylogger text result.

Keystroke logging, often referred to as **keylogging** or **keyboard capturing**, is the action of recording (logging) the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored.*[1] Keylogging can also be used to study human-computer interaction. Numerous keylogging methods exist: they range from hardware and software-based approaches to acoustic analysis.

18.1 Application

```

C:\Program Files\PyKeylogger\logs\detailed_log\Keylogger-software-logfile-example.txt - Notepad++
File Edit Search View Encoding Language Settings Macro Run TextFX Plugins Window ?
Keylogger-software-logfile-example.txt

1 20100326|1239|C:\WINDOWS\Explorer.EXE|327786|SoftwareInstall|Run| Commando in run window
2 20100326|1239|C:\WINDOWS\Explorer.EXE|393322|SoftwareInstall|Run|https://www.gmail.com[KeyName:Return]
3 20100326|1240|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Private Browsing - Mozilla Firefox (Private Browsing)|https://www.gmail.com[KeyName:Return]
4 20100326|1240|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail: Email from Google - Mozilla Firefox (Private Browsing)|accounts.n@gmail.com[KeyName:Return]
5 20100326|1241|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail - Compose Mail - accountsn@gmail.com - Mozilla Firefox (Private Browsing)| Hello John [KeyName:Home] Dealer Room @wallstreettrade.com Confidential email. Hello,
6 20100326|1242|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail - Compose Mail - accountsn@gmail.com - Mozilla Firefox (Private Browsing)|ck.[KeyName:Return] And ofcourse it is illegal to trade stock with pre knovledge : _0ESSESS :- )[KeyName:Return] Use my credit card number : [KeyName:Return]1234 5678 9123 4567[KeyName:Return]which
7 20100326|1243|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Gmail - Compose Mail - accountsn@gmail.com - Mozilla Firefox (Private Browsing)|0ESSESSwhich expires 10/10.[KeyName:Return] The card security code on the back is :
123.[KeyName:Return][KeyName:Return] Thanks,[KeyName:Return] Bob
8 20100326|1243|C:\Program Files\Mozilla Firefox\firefox.exe|262710|SoftwareInstall|Mozilla Firefox (Private Browsing)|www.playboy.com[KeyName:Return]

```

A *logfile* from a software-based keylogger, based on the screencapture above.

18.1.1 Software-based keyloggers

These are computer programs designed to work on the target computer's software.^{*} [2] Keyloggers are used in IT organizations to troubleshoot technical problems with computers and business networks. Families and business people use keyloggers legally to monitor network usage without their users' direct knowledge. Even Microsoft publicly admitted that Windows 10 operation system has a built-in keylogger in its final version "to improve typing and writing services".^{*[3]} However, malicious individuals can use keyloggers on public computers to steal passwords or credit card information. Most keyloggers are not stopped by **HTTPS** encryption because that only protects data in transit between computers, thus the threat being from the user's computer.

From a technical perspective there are several categories:

- **Hypervisor-based:** The keylogger can theoretically reside in a **malware hypervisor** running underneath the operating system, which thus remains untouched. It effectively becomes a **virtual machine**. **Blue Pill** is a conceptual example.
- **Kernel-based:** A program on the machine obtains root access to hide itself in the OS and intercepts keystrokes that pass through the kernel. This method is difficult both to write and to combat. Such keyloggers reside at the **kernel level**, which makes them difficult to detect, especially for user-mode applications that don't have root access. They are frequently implemented as **rootkits** that subvert the operating system kernel to gain unauthorized access to the hardware. This makes them very powerful. A keylogger using this method can act as a keyboard **device driver**, for example, and thus gain access to any information typed on the keyboard as it goes to the operating system.
- **API-based:** These keyloggers **hook** keyboard **APIs** inside a running application. The keylogger registers keystroke events, as if it was a normal piece of the application instead of malware. The keylogger receives an event each time the user presses or releases a key. The keylogger simply records it.
 - Windows APIs such as `GetAsyncKeyState()`, `GetForegroundWindow()`, etc. are used to poll the state of the keyboard or to subscribe to keyboard events.^{*[4]} A more recent example simply polls the **BIOS** for pre-boot authentication **PINs** that have not been cleared from memory.^{*[5]}

- **Form grabbing based:** Form grabbing-based keyloggers log web form submissions by recording the web browsing on submit events. This happens when the user completes a form and submits it, usually by clicking a button or hitting enter. This type of keylogger records form data before it is passed over the Internet.
- **Javascript-based:** A malicious script tag is injected into a targeted web page, and listens for key events such as onKeyUp(). Scripts can be injected via a variety of methods, including cross-site scripting, man-in-the-browser, man-in-the-middle, or a compromise of the remote web site.*[6]
- **Memory injection based:** Memory Injection (MitB)-based keyloggers perform their logging function by altering the memory tables associated with the browser and other system functions. By patching the memory tables or injecting directly into memory, this technique can be used by malware authors to bypass Windows UAC (User Account Control). The Zeus and SpyEye trojans use this method exclusively.*[7] Non-Windows systems have analogous protection mechanisms that the keylogger must thwart.⁷ with an added feature that allows access to locally recorded data from a remote location. Remote communication may be achieved when one of these methods is used:
 - Data is uploaded to a website, database or an FTP server.
 - Data is periodically emailed to a pre-defined email address.
 - Data is wirelessly transmitted by means of an attached hardware system.
 - The software enables a remote login to the local machine from the Internet or the local network, for data logs stored on the target machine.

Keystroke logging in writing process research

Keystroke logging is now an established research method for the study of writing processes.*[8]*[9] Different programs have been developed to collect online process data of writing activities,*[10] including Inputlog, Scriptlog, and Translog.

Keystroke logging is legitimately used as a suitable research instrument in a number of writing contexts. These include studies on cognitive writing processes, which include

- descriptions of writing strategies; the writing development of children (with and without writing difficulties),
- spelling,
- first and second language writing, and
- specialist skill areas such as translation and subtitling.

Keystroke logging can be used to research writing, specifically. It can also be integrated in educational domains for second language learning, programming skills, and typing skills.

Related features

Software keyloggers may be augmented with features that capture user information without relying on keyboard key presses as the sole input. Some of these features include:

- Clipboard logging. Anything that has been copied to the clipboard can be captured by the program.
- Screen logging. Screenshots are taken to capture graphics-based information. Applications with screen logging abilities may take screenshots of the whole screen, of just one application, or even just around the mouse cursor. They may take these screenshots periodically or in response to user behaviours (for example, when a user clicks the mouse). A practical application that is used by some keyloggers with this screen logging ability, is to take small screenshots around where a mouse has just clicked; thus defeating web-based keyboards (for example, the web-based screen keyboards that are often used by banks), and any web-based on-screen keyboard without screenshot protection.
- Programmatically capturing the text in a control. The Microsoft Windows API allows programs to request the text 'value' in some controls. This means that some passwords may be captured, even if they are hidden behind password masks (usually asterisks).*[11]

- The recording of every program/folder/window opened including a screenshot of each and every website visited.
- The recording of search engines queries, instant messenger conversations, FTP downloads and other Internet-based activities (including the bandwidth used).

18.1.2 Hardware-based keyloggers

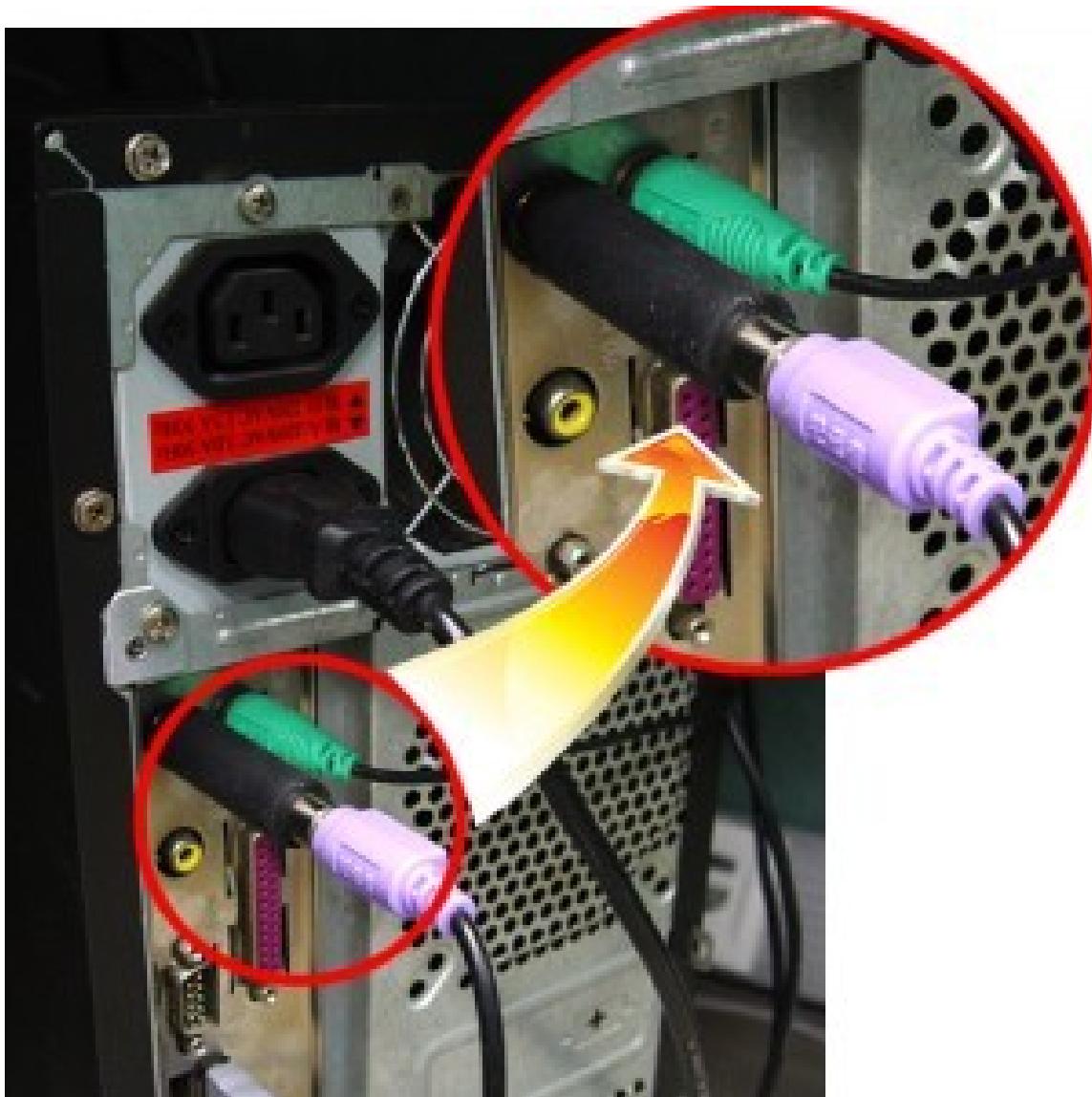


A hardware-based keylogger.

Main article: [Hardware keylogger](#)

Hardware-based keyloggers do not depend upon any software being installed as they exist at a hardware level in a computer system.

- Firmware-based: BIOS-level firmware that handles keyboard events can be modified to record these events as they are processed. Physical and/or root-level access is required to the machine, and the software loaded into the BIOS needs to be created for the specific hardware that it will be running on.*[12]
- Keyboard hardware: Hardware keyloggers are used for keystroke logging by means of a hardware circuit that is attached somewhere in between the computer keyboard and the computer, typically inline with the keyboard's cable connector. There are also USB connectors based Hardware keyloggers as well as ones for Laptop computers (the Mini-PCI card plugs into the expansion slot of a laptop). More stealthy implementations can be installed or built into standard keyboards, so that no device is visible on the external cable. Both types log all keyboard activity to their internal memory, which can be subsequently accessed, for example, by typing in a secret key sequence. A hardware keylogger has an advantage over a software solution: it is not dependent on being installed on the target computer's operating system and therefore will not interfere with any program running on the target machine or be detected by any software. However its physical presence may be detected if, for example, it is installed outside the case as an inline device between the computer and the keyboard. Some of these implementations have the ability to be controlled and monitored remotely by means of a wireless communication standard.*[13]
- Wireless keyboard and mouse sniffers: These passive sniffers collect packets of data being transferred from a wireless keyboard and its receiver. As encryption may be used to secure the wireless communications between



A connected hardware-based keylogger.

the two devices, this may need to be cracked beforehand if the transmissions are to be read. In some cases this enables an attacker to type arbitrary commands into a victim's computer.* [14]

- Keyboard overlays: Criminals have been known to use keyboard overlays on ATMs to capture people's PINs. Each keypress is registered by the keyboard of the ATM as well as the criminal's keypad that is placed over it. The device is designed to look like an integrated part of the machine so that bank customers are unaware of its presence.* [15]
- Acoustic keyloggers: **Acoustic cryptanalysis** can be used to monitor the sound created by someone typing on a computer. Each key on the keyboard makes a subtly different acoustic signature when struck. It is then possible to identify which keystroke signature relates to which keyboard character via statistical methods such as **frequency analysis**. The repetition frequency of similar acoustic keystroke signatures, the timings between different keyboard strokes and other context information such as the probable language in which the user is writing are used in this analysis to map sounds to letters.* [16] A fairly long recording (1000 or more keystrokes) is required so that a big enough **sample** is collected.* [17]
- Electromagnetic emissions: It is possible to capture the **electromagnetic emissions** of a wired keyboard from up to 20 metres (66 ft) away, without being physically wired to it.* [18] In 2009, Swiss researchers tested 11 different **USB**, **PS/2** and laptop keyboards in a semi-anechoic chamber and found them all vulnerable, primarily

because of the prohibitive cost of adding shielding during manufacture.* [19] The researchers used a wide-band receiver to tune into the specific frequency of the emissions radiated from the keyboards.

- Optical surveillance: Optical surveillance, while not a keylogger in the classical sense, is nonetheless an approach that can be used to capture passwords or PINs. A strategically placed camera, such as a hidden surveillance camera at an ATM, can allow a criminal to watch a PIN or password being entered.*[20]*[21]
- Physical evidence: For a keypad that is used only to enter a security code, the keys which are in actual use will have evidence of use from many fingerprints. A passcode of four digits, if the four digits in question are known, is reduced from 10,000 possibilities to just 24 possibilities (10^4 versus $4!$ (factorial of 4)). These could then be used on separate occasions for a manual “brute force attack”.
- Smartphone sensors: Researchers have demonstrated that it is possible to capture the keystrokes of nearby computer keyboards using only the commodity **accelerometer** found in smartphones.*[22] The attack is made possible by placing a smartphone near a keyboard on the same desk. The smartphone's accelerometer can then detect the vibrations created by typing on the keyboard, and then translate this raw accelerometer signal into readable sentences with as much as 80 percent accuracy. The technique involves working through probability by detecting pairs of keystrokes, rather than individual keys. It models “keyboard events” in pairs and then works out whether the pair of keys pressed is on the left or the right side of the keyboard and whether they are close together or far apart on the QWERTY keyboard. Once it has worked this out, it compares the results to a preloaded dictionary where each word has been broken down in the same way.*[23] Similar techniques have also been shown to be effective at capturing keystrokes on touchscreen keyboards*[24]*[25]*[26] while in some cases, in combination with gyroscope.*[27]*[28]

18.2 History

An early keylogger was written by Perry Kivolowitz and posted to the Usenet news group net.unix-wizards.net.sources on November 17, 1983.* [29] The posting seems to be a motivating factor in restricting access to /dev/kmem on Unix systems. The user-mode program operated by locating and dumping character lists (clists) as they were assembled in the Unix kernel.

In the 1970s, spies installed keystroke loggers in the US Embassy and Consulate buildings in Moscow and St Petersburg.*[30]*[31] They installed the bugs in Selectric II and Selectric III electric typewriters.*[32]

Soviet embassies used manual typewriters, rather than electric typewriters, for classified information—apparently because they are immune to such bugs.*[32] As of 2013, Russian special services still use typewriters.*[31]*[33]*[34]

18.3 Cracking

Writing simple software applications for keylogging can be trivial, and like any nefarious computer program, can be distributed as a **trojan horse** or as part of a **virus**. What is not trivial for an attacker, however, is installing a covert keystroke logger without getting caught and downloading data that has been logged without being traced. An attacker that manually connects to a host machine to download logged keystrokes risks being traced. A trojan that sends keylogged data to a fixed e-mail address or **IP address** risks exposing the attacker.

18.3.1 Trojans

Researchers devised several methods for solving this problem. They presented a deniable password snatching attack in which the keystroke logging trojan is installed using a virus or worm.*[35]*[36] An attacker who is caught with the virus or worm can claim to be a victim. The **cryptotrojan** asymmetrically encrypts the pilfered login/password pairs using the **public key** of the trojan author and covertly broadcasts the resulting **ciphertext**. They mentioned that the ciphertext can be **steganographically** encoded and posted to a public bulletin board such as **Usenet**.

18.3.2 Use by police

In 2000, the FBI used FlashCrest iSpy to obtain the PGP passphrase of Nicodemo Scarfo, Jr., son of mob boss Nicodemo Scarfo.*[37] Also in 2000, the FBI lured two suspected Russian cyber criminals to the US in an elaborate ruse, and captured their usernames and passwords with a keylogger that was covertly installed on a machine that they used to access their computers in Russia. The FBI then used these credentials to hack into the suspects' computers in Russia in order to obtain evidence to prosecute them.*[38]

18.4 Countermeasures

The effectiveness of countermeasures varies, because keyloggers use a variety of techniques to capture data and the countermeasure needs to be effective against the particular data capture technique. In the case of Windows 10 keylogging from Microsoft it is enough to change some privacy settings on your computer.*[39] For example, an on-screen keyboard will be effective against hardware keyloggers, transparency will defeat some—but not all—screenloggers and an anti-spyware application that can only disable hook-based keyloggers will be ineffective against kernel-based keyloggers.

Also, keylogger program authors may be able to update the code to adapt to countermeasures that may have proven to be effective against them.

18.4.1 Anti keyloggers

Main article: Anti keylogger

An anti keylogger is a piece of software specifically designed to detect keyloggers on a computer, typically comparing all files in the computer against a database of keyloggers looking for similarities which might signal the presence of a hidden keylogger. As anti keyloggers have been designed specifically to detect keyloggers, they have the potential to be more effective than conventional anti virus software; some anti virus software does not consider a keylogger to be a virus, as under some circumstances a keylogger can be considered a legitimate piece of software.*[40]

18.4.2 Live CD/USB

Rebooting the computer using a Live CD or write-protected Live USB is a possible countermeasure against software keyloggers if the CD is clean of malware and the operating system contained on it is secured and fully patched so that it cannot be infected as soon as it is started. Booting a different operating system does not impact the use of a hardware or BIOS based keylogger.

18.4.3 Anti-spyware / Anti-virus programs

Many anti-spyware applications are able to detect some software based keyloggers and quarantine, disable or cleanse them. However, because many keylogging programs are legitimate pieces of software under some circumstances, anti spyware often neglects to label keylogging programs as spyware or a virus. These applications are able to detect software-based keyloggers based on patterns in executable code, heuristics and keylogger behaviours (such as the use of hooks and certain APIs).

No software-based anti-spyware application can be 100% effective against all keyloggers. Also, software-based anti-spyware cannot defeat non-software keyloggers (for example, hardware keyloggers attached to keyboards will always receive keystrokes before any software-based anti-spyware application).

However, the particular technique that the anti-spyware application uses will influence its potential effectiveness against software keyloggers. As a general rule, anti-spyware applications with higher privileges will defeat keyloggers with lower privileges. For example, a hook-based anti-spyware application cannot defeat a kernel-based keylogger (as the keylogger will receive the keystroke messages before the anti-spyware application), but it could potentially defeat hook- and API-based keyloggers.

18.4.4 Network monitors

Network monitors (also known as reverse-firewalls) can be used to alert the user whenever an application attempts to make a network connection. This gives the user the chance to prevent the keylogger from "phoning home" with his or her typed information.

18.4.5 Automatic form filler programs

Main article: Form filler

Automatic form-filling programs may prevent keylogging by removing the requirement for a user to type personal details and passwords using the keyboard. Form fillers are primarily designed for web browsers to fill in checkout pages and log users into their accounts. Once the user's account and credit card information has been entered into the program, it will be automatically entered into forms without ever using the keyboard or clipboard, thereby reducing the possibility that private data is being recorded. However someone with physical access to the machine may still be able to install software that is able to intercept this information elsewhere in the operating system or while in transit on the network. (Transport Layer Security (TLS) reduces the risk that data in transit may be intercepted by network sniffers and proxy tools.)

18.4.6 One-time passwords (OTP)

Using one-time passwords may be keylogger-safe, as each password is invalidated as soon as it is used. This solution may be useful for someone using a public computer. However, an attacker who has remote control over such a computer can simply wait for the victim to enter his/her credentials before performing unauthorised transactions on their behalf while their session is active.

18.4.7 Security tokens

Use of smart cards or other security tokens may improve security against replay attacks in the face of a successful keylogging attack, as accessing protected information would require both the (hardware) security token *as well as* the appropriate password/passphrase. Knowing the keystrokes, mouse actions, display, clipboard etc. used on one computer will not subsequently help an attacker gain access to the protected resource. Some security tokens work as a type of hardware-assisted one-time password system, and others implement a cryptographic challenge-response authentication, which can improve security in a manner conceptually similar to one time passwords. Smartcard readers and their associated keypads for PIN entry may be vulnerable to keystroke logging through a so-called supply chain attack^{*[41]} where an attacker substitutes the card reader/PIN entry hardware for one which records the user's PIN.

18.4.8 On-screen keyboards

Most on-screen keyboards (such as the on-screen keyboard that comes with Windows XP) send normal keyboard event messages to the external target program to type text. Software key loggers can log these typed characters sent from one program to another.^{*[42]} Additionally, keylogging software can take screenshots of what is displayed on the screen (periodically, and/or upon each mouse click), which means that although certainly a useful security measure, an on-screen keyboard will not protect from all keyloggers.

18.4.9 Keystroke interference software

Keystroke interference software is also available.^{*[43]} These programs attempt to trick keyloggers by introducing random keystrokes, although this simply results in the keylogger recording more information than it needs to. An attacker has the task of extracting the keystrokes of interest—the security of this mechanism, specifically how well it stands up to cryptanalysis, is unclear.

18.4.10 Speech recognition

Similar to on-screen keyboards, speech-to-text conversion software can also be used against keyloggers, since there are no typing or mouse movements involved. The weakest point of using voice-recognition software may be how the software sends the recognized text to target software after the recognition took place.

18.4.11 Handwriting recognition and mouse gestures

Also, many PDAs and lately tablet PCs can already convert pen (also called stylus) movements on their touchscreens to computer understandable text successfully. Mouse gestures use this principle by using mouse movements instead of a stylus. Mouse gesture programs convert these strokes to user-definable actions, such as typing text. Similarly, graphics tablets and light pens can be used to input these gestures, however these are less common everyday.

The same potential weakness of speech recognition applies to this technique as well.

18.4.12 Macro expanders/recorders

With the help of many programs, a seemingly meaningless text can be expanded to a meaningful text and most of the time context-sensitively, e.g. “en.wikipedia.org” can be expanded when a web browser window has the focus. The biggest weakness of this technique is that these programs send their keystrokes directly to the target program. However, this can be overcome by using the ‘alternating’ technique described below, i.e. sending mouse clicks to non-responsive areas of the target program, sending meaningless keys, sending another mouse click to target area (e.g. password field) and switching back-and-forth.

18.4.13 Deceptive typing

Alternating between typing the login credentials and typing characters somewhere else in the focus window^{*[44]} can cause a keylogger to record more information than they need to, although this could easily be filtered out by an attacker. Similarly, a user can move their cursor using the mouse during typing, causing the logged keystrokes to be in the wrong order e.g., by typing a password beginning with the last letter and then using the mouse to move the cursor for each subsequent letter. Lastly, someone can also use context menus to remove, cut, copy, and paste parts of the typed text without using the keyboard. An attacker who is able to capture only parts of a password will have a smaller key space to attack if he chose to execute a brute-force attack.

Another very similar technique uses the fact that any selected text portion is replaced by the next key typed. e.g., if the password is “secret”, one could type “s”, then some dummy keys “asdfs” . Then, these dummies could be selected with the mouse, and the next character from the password “e” is typed, which replaces the dummies “asdfs” .

These techniques assume incorrectly that keystroke logging software cannot directly monitor the clipboard, the selected text in a form, or take a screenshot every time a keystroke or mouse click occurs. They may however be effective against some hardware keyloggers.

18.5 See also

- Anti keylogger
- Black-bag cryptanalysis
- Computer surveillance
- Digital footprint
- Hardware keylogger
- Reverse connection
- Spyware

- Trojan horse
- Virtual keyboard

18.6 References

- [1] “Keylogger” . Oxford dictionaries.
- [2] “What is a Keylogger?”. PC Tools.
- [3] Caleb Chen (2017-03-20). “Microsoft Windows 10 has a keylogger enabled by default – here’s how to disable it” .
- [4] “The Evolution of Malicious IRC Bots” (PDF). Symantec. 2005-11-26: 23–24. Retrieved 2011-03-25.
- [5] Jonathan Brossard (2008-09-03). “Bypassing pre-boot authentication passwords by instrumenting the BIOS keyboard buffer (practical low level attacks against x86 pre-boot authentication software)” (PDF). Iviz Technosolutions. Retrieved 2008-09-23. External link in |publisher= (help)
- [6] “Web-Based Keylogger Used to Steal Credit Card Data from Popular Sites” . Threatpost | The first stop for security news. 2016-10-06. Retrieved 2017-01-24.
- [7] “SpyEye Targets Opera, Google Chrome Users” . Krebs on Security. Retrieved 26 April 2011.
- [8] K.P.H. Sullivan & E. Lindgren (Eds., 2006), Studies in Writing: Vol. 18. Computer Key-Stroke Logging and Writing: Methods and Applications. Oxford: Elsevier.
- [9] V. W. Berninger (Ed., 2012), Past, present, and future contributions of cognitive writing research to cognitive psychology. New York/Sussex: Taylor & Francis. ISBN 9781848729636
- [10] Vincentas (11 July 2013). “Keystroke Logging in SpyWareLoop.com” . Spyware Loop. Archived from the original on 7 December 2013. Retrieved 27 July 2013.
- [11] Microsoft. “EM_GETLINE Message()”. Microsoft. Retrieved 2009-07-15.
- [12] “Apple keyboard hack” . Apple keyboard hack. Digital Society. Retrieved 9 June 2011.
- [13] “Keylogger Removal” . Keylogger Removal. SpyReveal Anti Keylogger. Archived from the original on 29 April 2011. Retrieved 25 April 2011.
- [14] “Keylogger Removal” . Keylogger Removal. SpyReveal Anti Keylogger. Retrieved 26 February 2016.
- [15] Jeremy Kirk (2008-12-16). “Tampered Credit Card Terminals” . IDG News Service. Retrieved 2009-04-19.
- [16] Andrew Kelly (2010-09-10). “Cracking Passwords using Keyboard Acoustics and Language Modeling” (PDF).
- [17] Sarah Young (14 September 2005). “Researchers recover typed text using audio recording of keystrokes” . UC Berkeley NewsCenter.
- [18] “Remote monitoring uncovered by American techno activists” . ZDNet. 2000-10-26. Retrieved 2008-09-23.
- [19] Martin Vuagnoux and Sylvain Pasini (2009-06-01). “Compromising Electromagnetic Emanations of Wired and Wireless Keyboards” . Lausanne: Security and Cryptography Laboratory (LASEC).
- [20] “ATM camera” . snopes.com. Retrieved 2009-04-19. External link in |publisher= (help)
- [21] Maggi, Federico; Volpatto, Alberto; Gasparini, Simone; Boracchi, Giacomo; Zanero, Stefano (2011). *A fast eavesdropping attack against touchscreens*. 7th International Conference on Information Assurance and Security. IEEE. doi:10.1109/ISIAS.2011.6122840.
- [22] Marquardt, Philip; Verma, Arunabh; Carter, Henry; Traynor, Patrick (2011). *(sp)iPhone: decoding vibrations from nearby keyboards using mobile phone accelerometers*. Proceedings of the 18th ACM conference on Computer and communications security. ACM. pp. 561–562. doi:10.1145/2046707.2046771.
- [23] “iPhone Accelerometer Could Spy on Computer Keystrokes” . Wired. 19 October 2011. Retrieved August 25, 2014. External link in |publisher= (help)
- [24] Owusu, Emmanuel; Han, Jun; Das, Sauvik; Perrig, Adrian; Zhang, Joy (2012). *ACCessory: password inference using accelerometers on smartphones*. Proceedings of the Thirteenth Workshop on Mobile Computing Systems and Applications. ACM. doi:10.1145/2162081.2162095.

- [25] Aviv, Adam J.; Sapp, Benjamin; Blaze, Matt; Smith, Jonathan M. (2012). *Practicality of accelerometer side channels on smartphones*. Proceedings of the 28th Annual Computer Security Applications Conference. ACM. doi:10.1145/2420950.2420957.
- [26] Cai, Liang; Chen, Hao (2011). *TouchLogger: inferring keystrokes on touch screen from smartphone motion* (PDF). Proceedings of the 6th USENIX conference on Hot topics in security. USENIX. Retrieved 25 August 2014.
- [27] Xu, Zhi; Bai, Kun; Zhu, Sencun (2012). *TapLogger: inferring user inputs on smartphone touchscreens using on-board motion sensors*. Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks. ACM. pp. 113–124. doi:10.1145/2185448.2185465.
- [28] Miluzzo, Emiliano; Varshavsky, Alexander; Balakrishnan, Suhrid; Choudhury, Romit Roy (2012). *Tapprints: your finger taps have fingerprints*. Proceedings of the 10th international conference on Mobile systems, applications, and services. ACM. pp. 323–336. doi:10.1145/2307636.2307666.
- [29] “The Security Digest Archives” . Retrieved 2009-11-22.
- [30] “Soviet Spies Bugged World's First Electronic Typewriters” . qccglobal.com.
- [31] Geoffrey Ingersoll. “Russia Turns To Typewriters To Protect Against Cyber Espionage” . 2013.
- [32] Sharon A. Maneki. “Learning from the Enemy: The GUNMAN Project” . 2012.
- [33] Agence France-Presse, Associated Press. “Wanted: 20 electric typewriters for Russia to avoid leaks” . inquirer.net.
- [34] Anna Arutunyan. “Russian security agency to buy typewriters to avoid surveillance” .
- [35] Young, Adam; Yung, Moti (1997). “Deniable Password Snatching: On the Possibility of Evasive Electronic Espionage” . *Proceedings of IEEE Symposium on Security and Privacy*. IEEE: 224–235. doi:10.1109/SECPRI.1997.601339.
- [36] Young, Adam; Yung, Moti (1996). “Cryptovirology: extortion-based security threats and countermeasures” . *Proceedings of IEEE Symposium on Security and Privacy*. IEEE: 129–140. doi:10.1109/SECPRI.1996.502676.
- [37] John Leyden (2000-12-06). “Mafia trial to test FBI spying tactics: Keystroke logging used to spy on mob suspect using PGP” . The Register. Retrieved 2009-04-19.
- [38] John Leyden (2002-08-16). “Russians accuse FBI Agent of Hacking” . The Register.
- [39] Alex Stim (2015-10-28). “3 methods to disable Windows 10 built-in Spy Keylogger” .
- [40] Theron, kristen (19 February 2016). “What is Anti Keylogger” .
- [41] Austin Modine (2008-10-10). “Organized crime tampers with European card swipe devices” . The Register. Retrieved 2009-04-18.
- [42] Scott Dunn (2009-09-10). “Prevent keyloggers from grabbing your passwords” . Windows Secrets. Retrieved 2014-05-10.
- [43] Christopher Ciabarra (2009-06-10). “Anti Keylogger” . Networkintercept.com. Archived from the original on 2010-06-26.
- [44] Cormac Herley and Dinei Florencio (2006-02-06). “How To Login From an Internet Cafe Without Worrying About Keyloggers” (PDF). Microsoft Research. Retrieved 2008-09-23.

18.7 External links

- Keyloggers at DMOZ

Chapter 19

Computer access control

In computer security, general access control includes identification, authorization, authentication, access approval, and audit. A more narrow definition of access control would cover only access approval, whereby the system makes a decision to grant or reject an access request from an already authenticated subject, based on what the subject is authorized to access. Authentication and access control are often combined into a single operation, so that access is approved based on successful authentication, or based on an anonymous access token. Authentication methods and tokens include **passwords**, biometric scans, physical **keys**, electronic keys and devices, hidden paths, social barriers, and monitoring by humans and automated systems.

those based on **capabilities** and those based on **access control lists (ACLs)**.

- In a capability-based model, holding an unforgeable reference or *capability* to an object provides access to the object (roughly analogous to how possession of one's house key grants one access to one's house); access is conveyed to another party by transmitting such a capability over a secure channel
- In an ACL-based model, a subject's access to an object depends on whether its identity appears on a list associated with the object (roughly analogous to how a bouncer at a private party would check an ID to see if a name appears on the guest list); access is conveyed by editing the list. (Different ACL systems have a variety of different conventions regarding who or what is responsible for editing the list and how it is edited.)

Both capability-based and ACL-based models have mechanisms to allow access rights to be granted to all members of a *group* of subjects (often the group is itself modeled as a subject).

19.1 Services

Access control systems provide the essential services of *authorization, identification and authentication (I&A), access approval, and accountability* where:

- authorization specifies what a subject can do
- identification and authentication ensure that only legitimate subjects can log on to a system
- access approval grants access during operations, by association of users with the resources that they are allowed to access, based on the authorization policy
- accountability identifies what a subject (or all subjects associated with a user) did

19.2 Authorization

Authorization involves the act of defining access-rights for subjects. An authorization policy specifies the operations that subjects are allowed to execute within a system.

Most modern operating systems implement authorization policies as formal sets of permissions that are variations or extensions of three basic types of access:

- Read (R): The subject can
 - Read file contents
 - List directory contents
- Write (W): The subject can change the contents of a file or directory with the following tasks:
 - Add
 - Update
 - Delete
 - Rename
- Execute (X): If the file is a program, the subject can cause the program to be run. (In Unix-style systems, the “execute” permission doubles as a “traverse directory” permission when granted for a directory.)

These rights and permissions are implemented differently in systems based on *discretionary access control* (DAC) and *mandatory access control* (MAC).

19.3 Identification and Authentication (I&A)

Main article: Authentication

Identification and Authentication^{*[1]} (I&A) is the process of verifying that an identity is bound to the entity that makes an assertion or claim of identity. The I&A process assumes that there was an initial validation of the identity, commonly called identity proofing. Various methods of identity proofing are available, ranging from in-person validation using government issued identification, to anonymous methods that allow the claimant to remain anonymous, but known to the system if they return. The method used for identity proofing and validation should provide an assurance level commensurate with the intended use of the identity within the system. Subsequently, the entity asserts an identity together with an authenticator as a means for validation. The only requirements for the identifier is that it must be unique within its security domain.

Authenticators are commonly based on at least one of the following four factors:

- *Something you know*, such as a password or a personal identification number (PIN). This assumes that only the owner of the account knows the password or PIN needed to access the account.
- *Something you have*, such as a smart card or security token. This assumes that only the owner of the account has the necessary smart card or token needed to unlock the account.
- *Something you are*, such as fingerprint, voice, retina, or iris characteristics.
- *Where you are*, for example inside or outside a company firewall, or proximity of login location to a personal GPS device.

19.4 Access approval

Access approval is the function that actually grants or rejects access during operations.^{*[2]}

During access approval, the system compares the formal representation of the authorization policy with the access request, to determine whether the request shall be granted or rejected. Moreover, the access evaluation can be done online/ongoing.^{*[3]}

19.5 Accountability

Accountability uses such system components as *audit trails* (records) and *logs*, to associate a subject with its actions. The information recorded should be sufficient to map the subject to a controlling user. Audit trails and logs are important for

- Detecting security violations
- Re-creating security incidents

If no one is regularly reviewing your logs and they are not maintained in a secure and consistent manner, they may not be admissible as evidence.

Many systems can generate automated reports, based on certain predefined criteria or thresholds, known as clipping levels. *For example, a clipping level may be set to generate a report for the following:*

- More than three failed logon attempts in a given period
- Any attempt to use a disabled user account

These reports help a system administrator or security administrator to more easily identify possible break-in attempts.

Definition of clipping level:^{*} [4] a disk's ability to maintain its magnetic properties and hold its content. A high-quality level range is 65–70%; low quality is below 55%.

19.6 Access control models

Access control models are sometimes categorized as either discretionary or non-discretionary. The three most widely recognized models are Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role Based Access Control (RBAC). MAC is non-discretionary.

19.6.1 Discretionary access control

Discretionary access control (DAC) is a policy determined by the owner of an object. The owner decides who is allowed to access the object, and what privileges they have.

Two important concepts in DAC are

- File and data ownership: Every object in the system has an *owner*. In most DAC systems, each object's initial owner is the subject that caused it to be created. The access policy for an object is determined by its owner.
- Access rights and permissions: These are the controls that an owner can assign to other subjects for specific resources.

Access controls may be discretionary in **ACL-based** or **capability-based** access control systems. (In capability-based systems, there is usually no explicit concept of 'owner', but the creator of an object has a similar degree of control over its access policy.)

19.6.2 Mandatory access control

Mandatory access control refers to allowing access to a resource if and only if rules exist that allow a given user to access the resource. It is difficult to manage, but its use is usually justified when used to protect highly sensitive information. Examples include certain government and military information. Management is often simplified (over what can be required) if the information can be protected using hierarchical access control, or by implementing sensitivity labels. What makes the method “mandatory” is the use of either rules or sensitivity labels.

- Sensitivity labels: In such a system subjects and objects must have labels assigned to them. A subject's sensitivity label specifies its level of trust. An object's sensitivity label specifies the level of trust required for access. In order to access a given object, the subject must have a sensitivity level equal to or higher than the requested object.
- Data import and export: Controlling the import of information from other systems and export to other systems (including printers) is a critical function of these systems, which must ensure that sensitivity labels are properly maintained and implemented so that sensitive information is appropriately protected at all times.

Two methods are commonly used for applying mandatory access control:

- Rule-based (or label-based) access control: This type of control further defines specific conditions for access to a requested object. A Mandatory Access Control system implements a simple form of rule-based access control to determine whether access should be granted or denied by matching:
 - An object's sensitivity label
 - A subject's sensitivity label
- Lattice-based access control: These can be used for complex access control decisions involving multiple objects and/or subjects. A lattice model is a mathematical structure that defines greatest lower-bound and least upper-bound values for a pair of elements, such as a subject and an object.

Few systems implement MAC; XTS-400 and SELinux are examples of systems that do.

19.6.3 Role-based access control

Role-based access control (RBAC) is an access policy determined by the system, not by the owner. RBAC is used in commercial applications and also in military systems, where multi-level security requirements may also exist. RBAC differs from DAC in that DAC allows users to control access to their resources, while in RBAC, access is controlled at the system level, outside of the user's control. Although RBAC is non-discretionary, it can be distinguished from MAC primarily in the way permissions are handled. MAC controls read and write permissions based on a user's clearance level and additional labels. RBAC controls collections of permissions that may include complex operations such as an e-commerce transaction, or may be as simple as read or write. A role in RBAC can be viewed as a set of permissions.

Three primary rules are defined for RBAC:

1. Role assignment: A subject can execute a transaction only if the subject has selected or been assigned a suitable role.
2. Role authorization: A subject's active role must be authorized for the subject. With rule 1 above, this rule ensures that users can take on only roles for which they are authorized.
3. Transaction authorization: A subject can execute a transaction only if the transaction is authorized for the subject's active role. With rules 1 and 2, this rule ensures that users can execute only transactions for which they are authorized.

Additional constraints may be applied as well, and roles can be combined in a hierarchy where higher-level roles subsume permissions owned by lower-level sub-roles.

Most IT vendors offer RBAC in one or more products.

19.6.4 Intent-based Access Control (IBAC)

Intent-based Access Control (IBAC),^{*[5]}^{*[6]} a novel access control model first proposed by Abdulaziz Almehmadi, is an access control system that detects the intention of the user requesting access answering the question "Why?" access is being requested as opposed to current access control systems that asks "Who?" is requesting access. IBAC is designed to prevent the insider threat as opposed to the current access control systems that are designed to prevent

the outsider threat. IBAC is a risk-based access control that assesses risk of access based on the detected intent and the motivation level towards executing that intent. IBAC takes advantage of the robustness of P300-based Concealed Information Test to detect an intent of access and uses the brain signals to detect the motivation level. The access control system has been used on 30 participants with 100% detected intentions of access and all mal-intent users being rejected access before they commit their mal-intended action.

19.6.5 Emotion-based Access Control (EBAC)

Emotion-based Access Control (EBAC),^{*[7]} a novel access control model first proposed by Abdulaziz Almehmadi, is an access control system that detects the emotion of the user requesting access in order to form an access decision. This form of access control adds the sensibility aspect to access control systems to further analyze the risk of granting an authorized user access. A user who has a high level of anger and might cause damage if granted access. As well as denying a malicious authorized user access can be useful, granting a non-authorized user who have good intentions of access can be useful as well (e.g. granting firefighters access to a facility in order to suppress damage).

In some cases, we would wish to deny access to authorized personals in the case that they request access to cause damage. On the other hand, we would wish to grant access to unauthorized individuals. who may suppress damage or prevent catastrophic incidents

EBAC uses emotion detection technology to supplement the access control systems by detecting the emotion of the person requesting access and using it as an additional authentication factor along with the recognized identity of the user as needed. The novelty of the approach is that access is granted based on the actual feelings of the users with regards to the requested resources. The approach is based on the detection of emotion based on the involuntary brain signals that are extremely hard to control or circumvent, and on using the detected emotion in the context of access control.

The EBAC system flow starts with the EEG signal acquisition. The EEG signals are sent via the Emotiv EPOC headset to a listener in the EBAC application. Signals are then analyzed and the emotion is detected with correspondence to the emotion level. The emotion and its rate are then categorized to be either positive or negative. Then data is sent to the decision maker to deny or grant access to the entity.

19.6.6 Attribute-based access control

In attribute-based access control (ABAC),^{*[8]*[9]} access is granted not based on the rights of the subject associated with a user after authentication, but based on attributes of the user. The user has to prove so-called claims about his attributes to the access control engine. An attribute-based access control policy specifies which claims need to be satisfied in order to grant access to an object. For instance the claim could be “older than 18”. Any user that can prove this claim is granted access. Users can be anonymous when authentication and identification are not strictly required. One does, however, require means for proving claims anonymously. This can for instance be achieved using **anonymous credentials**. XACML (extensible access control markup language) is a standard for attribute-based access control. XACML 3.0 was standardized in January 2013.^{*[10]}

19.6.7 Break-Glass Access Control Models

Traditionally, access has the purpose of restricting access, thus most access control models follow the “default deny principle”, i.e. if a specific access request is not explicitly allowed, it will be denied. This behavior might conflict with the regular operations of a system. In certain situations, humans are willing to take the risk that might be involved in violating an access control policy, if the potential benefit that can be achieved outweighs this risk. This need is especially visible in the health-care domain, where a denied access to patient records can cause the death of a patient. Break-Glass (also called break-the-glass) try to mitigate this by allowing users to override access control decision. Break-Glass can either be implemented in an access control specific manner (e.g. into RBAC),^{*[11]} or generic (i.e., independent from the underlying access control model).^{*[12]}

19.6.8 Access control based on the responsibility

In **Aligning Access Rights to Governance Needs with the Responsibility MetaModel (ReMMo) in the Frame of Enterprise Architecture**^{*[13]} an expressive Responsibility metamodel has been defined and allows representing

the existing responsibilities at the business layer and, thereby, allows engineering the access rights required to perform these responsibilities, at the application layer. A method has been proposed to define the access rights more accurately, considering the alignment of the responsibility and RBAC.

19.6.9 Host-based access control (HBAC)

The initialism HBAC stands for “host-based access control” .*[14]

19.7 References

- [1] “Unifying identity management and access control” . sourcesecurity.com. Retrieved 15 July 2013.
- [2] Dieter Gollmann. *Computer Security*, 3rd ed. Wiley Publishing, 2011, p. 387, bottom
- [3] Marcon, A. L.; Olivo Santin, A.; Stihler, M.; Bachtold, J., “A UCONabc Resilient Authorization Evaluation for Cloud Computing,” *Parallel and Distributed Systems, IEEE Transactions on*, vol. 25, no. 2, pp. 457–467, Feb. 2014 doi: 10.1109/TPDS.2013.113, bottom
- [4] “Definition of: clipping level” . PC Magazine.
- [5] Abdulaziz Almehmadi and Khalil El-Khatib, “On the Possibility of Insider Threat Prevention Using Intent-Based Access Control (IBAC)”, *Systems Journal, IEEE* , vol. PP, no. 99, pp. 1, 12, doi: 10.1109/JST.2015.2424677 URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7103286&isnumber=4357939>
- [6] Abdulaziz Almehmadi “Insider Threats Meet Access Control” , URL: https://www.amazon.com/gp/aw/d/1539772012/ref=mp_s_a_1_1?ie=UTF8&qid=1477837714&sr=8-1&pi=AC_SX280_SY350_FMwebp_QL65&keywords=almehmadi&dpPl=1&dpID=518-g2uTc0L&ref=plSrch
- [7] Abdulaziz Almehmadi and Khalil El-Khatib. 2013. “Authorized! access denied, unauthorized! access granted” . In *Proceedings of the 6th International Conference on Security of Information and Networks* (SIN '13).
- [8] Jin, Xin, Ram Krishnan, and Ravi Sandhu. “A unified attribute-based access control model covering dac, mac and rbac.” *Data and Applications Security and Privacy XXVI*. Springer Berlin Heidelberg, 2012. 41–55.
- [9] Hu, Vincent C.; Ferraiolo, David; Kuhn, Rick; Schnitzer, Adam; Sandlin, Kenneth; Miller, Robert; Scarfone, Karen. “Guide to Attribute Based Access Control (ABAC) Definition and Considerations” (PDF).
- [10] eXtensible Access Control Markup Language (XACML) V3.0 approved as an OASIS Standard, eXtensible Access Control Markup Language (XACML) V3.0 approved as an OASIS Standard.
- [11] Ferreira, Ana; Chadwick, David; Farinha, Pedro; Correia, Ricardo; Zao, Gansen; Chiro, Rui; Antunes, Luis (2009). “How to Securely Break into RBAC: The BTG-RBAC Model” . *Computer Security Applications Conference (ACSAC)*. IEEE. pp. 23–31. doi:10.1109/ACSAC.2009.12.
- [12] Brucker, Achim D.; Petritsch, Helmut (2009). “Extending Access Control Models with Break-glass.” . *ACM symposium on access control models and technologies (SACMAT)*. ACM Press. pp. 197–206. doi:10.1145/1542207.1542239.
- [13] Feltus C. (2014). *Aligning Access Rights to Governance Needs with the Responsibility MetaModel (ReMMo) in the Frame of Enterprise Architecture* (PDF).
- [14] Ballard, Ella Deon (2013). “Identity Management Guide: Managing Identity and Authorization Policies for Linux-Based Infrastructures” . Red Hat. Retrieved 2014-01-06. Any PAM service can be identified as to the host-based access control (HBAC) system in IdM.

Chapter 20

Application security

Application security encompasses measures taken to improve the security of an **application** often by finding, fixing and preventing security **vulnerabilities**.

Different techniques are used to surface such security **vulnerabilities** at different stages of an applications lifecycle such **design, development, deployment, upgrade, or maintenance**.

An always evolving but largely consistent set of common security flaws are seen across different applications, see **common flaws**

20.1 Terms

- **Asset.** A resource of value such as the data in a database, money in an account, file on the filesystem or any system resource.
- **Vulnerability.** A weakness or gap in security program that can be exploited by threats to gain unauthorized access to an asset.
- **Attack** (or exploit). An action taken to harm an asset.
- **Threat.** Anything that can exploit a vulnerability and obtain, damage, or destroy an asset.

20.2 Techniques

Different techniques will find different subsets of the security vulnerabilities lurking in an application and are most effective at different times in the software lifecycle. They each represent different tradeoffs of time, effort, cost and vulnerabilities found.

- Whitebox security review, or code review. This is a security engineer deeply understanding the application through manually reviewing the source code and noticing security flaws. Through comprehension of the application vulnerabilities unique to the application can be found.
- Blackbox security audit. This is only through use of an application testing it for security vulnerabilities, no source code required.
- Design review. Before code is written working through a **Threat_model** of the application. Sometimes alongside a spec or design document.
- Tooling. There exist many automated tools that test for security flaws, often with a higher false positive rate than having a human involved.

Utilizing these techniques appropriately throughout the **software development life cycle (SDLC)** to maximize security is the role of an application security team.

20.3 Application threats / attacks

According to the patterns & practices *Improving Web Application Security* book, the following are classes of common application security threats / attacks:

20.4 Mobile application security

Main article: Mobile security

The proportion of mobile devices providing open platform functionality is expected to continue to increase in future. The openness of these platforms offers significant opportunities to all parts of the mobile eco-system by delivering the ability for flexible program and service delivery= options that may be installed, removed or refreshed multiple times in line with the user's needs and requirements. However, with openness comes responsibility and unrestricted access to mobile resources and APIs by applications of unknown or untrusted origin could result in damage to the user, the device, the network or all of these, if not managed by suitable security architectures and network precautions. Application security is provided in some form on most open OS mobile devices ([Symbian OS](#), *[1] [Microsoft](#), [BREW](#), etc.). Industry groups have also created recommendations including the [GSM Association](#) and [Open Mobile Terminal Platform \(OMTP\)](#).*[2]

There are several strategies to enhance mobile application security including

- Application white listing
- Ensuring transport layer security
- Strong authentication and authorization
- Encryption of data when written to memory
- Sandboxing of applications
- Granting application access on a per-API level
- Processes tied to a user ID
- Predefined interactions between the mobile application and the OS
- Requiring user input for privileged/elevated access
- Proper session handling

20.5 Security testing for applications

Security testing techniques scour for vulnerabilities or security holes in applications. These vulnerabilities leave applications open to [exploitation](#). Ideally, security testing is implemented throughout the entire [software development life cycle](#) (SDLC) so that vulnerabilities may be addressed in a timely and thorough manner. Unfortunately, testing is often conducted as an afterthought at the end of the development cycle.

Vulnerability scanners, and more specifically web application scanners, otherwise known as penetration testing tools (i.e. ethical hacking tools) have been historically used by security organizations within corporations and security consultants to automate the security testing of http request/responses; however, this is not a substitute for the need for actual source code review. Physical code reviews of an application's source code can be accomplished manually or in an automated fashion. Given the common size of individual programs (often 500,000 lines of code or more), the human brain can not execute a comprehensive data flow analysis needed in order to completely check all circuitous paths of an application program to find vulnerability points. The human brain is suited more for filtering, interrupting and reporting the outputs of automated source code analysis tools available commercially versus trying to trace every possible path through a compiled code base to find the root cause level vulnerabilities.

The two types of automated tools associated with application vulnerability detection (application vulnerability scanners) are Penetration Testing Tools (often categorized as Black Box Testing Tools) and static code analysis tools (often categorized as White Box Testing Tools).

According to Gartner Research, *[3] "...next-generation modern Web and mobile applications requires a combination of SAST and DAST techniques, and new interactive application security testing (IAST) approaches have emerged that combine static and dynamic techniques to improve testing..." . Because IAST combines SAST and DAST techniques, the results are highly actionable, can be linked to the specific line of code, and can be recorded for replay later for developers.

Banking and large E-Commerce corporations have been the very early adopter customer profile for these types of tools. It is commonly held within these firms that both Black Box testing and White Box testing tools are needed in the pursuit of application security. Typically sited, Black Box testing (meaning Penetration Testing tools) are ethical hacking tools used to attack the application surface to expose vulnerabilities suspended within the source code hierarchy. Penetration testing tools are executed on the already deployed application. White Box testing (meaning Source Code Analysis tools) are used by either the application security groups or application development groups. Typically introduced into a company through the application security organization, the White Box tools complement the Black Box testing tools in that they give specific visibility into the specific root vulnerabilities within the source code in advance of the source code being deployed. Vulnerabilities identified with White Box testing and Black Box testing are typically in accordance with the OWASP taxonomy for software coding errors. White Box testing vendors have recently introduced dynamic versions of their source code analysis methods; which operates on deployed applications. Given that the White Box testing tools have dynamic versions similar to the Black Box testing tools, both tools can be correlated in the same software error detection paradigm ensuring full application protection to the client company.

The advances in professional Malware targeted at the Internet customers of online organizations has seen a change in Web application design requirements since 2007. It is generally assumed that a sizable percentage of Internet users will be compromised through malware and that any data coming from their infected host may be tainted. Therefore, application security has begun to manifest more advanced anti-fraud and heuristic detection systems in the back-office, rather than within the client-side or Web server code.*[4]

20.6 Security standards and regulations

- Sarbanes-Oxley Act (SOX)
- Health Insurance Portability and Accountability Act (HIPAA)
- ISO/IEC 27034-1:2011 *Information technology — Security techniques — Application security -- Part 1: Overview and concepts*
- ISO/IEC TR 24772:2013 *Information technology — Programming languages — Guidance to avoiding vulnerabilities in programming languages through language selection and use*
- Gramm-Leach-Bliley Act
- PCI Data Security Standardized (PCI DSS)

20.7 See also

- Countermeasure
- Data security
- Database security
- HERAS-AF
- Information security
- Trustworthy Computing Security Development Lifecycle

- Web application
- Web application framework

20.8 References

- [1] “Platform Security Concepts” , Simon Higginson.
- [2] Application Security Framework Archived March 29, 2009, at the Wayback Machine., Open Mobile Terminal Platform
- [3] http://www.gartner.com/technology/reprints.do?id=1-1GT3BKT&ct=130702&st=sb&mkt_tok=3RkMMJWWfF9wsRokvazAZKXonjHpf%252B4qX6WylMI%252F0ER3fOvrPUfGjI4CTsRmI%252BSLDwEYGJlv6SgFTbnFMbprzbgPUhA%253D
- [4] “Continuing Business with Malware Infected Customers” . Gunter Ollmann. October 2008.

20.9 External links

Chapter 21

Antivirus software

For medications concerning biological viruses, see [Antiviral](#).



ClamTk, an open source antivirus based on the ClamAV antivirus engine, originally developed by Tomasz Kojm in 2001.

Antivirus or **anti-virus** software (often abbreviated as **AV**), sometimes known as **anti-malware** software, is computer software used to prevent, detect and remove malicious software.* [1]

Antivirus software was originally developed to detect and remove computer viruses, hence the name. However, with the proliferation of other kinds of malware, antivirus software started to provide protection from other computer threats. In particular, modern antivirus software can protect from: malicious browser helper objects (BHOs), browser hijackers, ransomware, keyloggers, backdoors, rootkits, trojan horses, worms, malicious LSPs, dialers, fraudtools, adware and spyware.* [2] Some products also include protection from other computer threats, such as infected and malicious URLs, spam, scam and phishing attacks, online identity (privacy), online banking attacks, social engineering techniques, advanced persistent threat (APT) and botnet DDoS attacks.* [3]

21.1 History

See also: Timeline of notable computer viruses and worms

21.1.1 1949–1980 period (pre-antivirus days)

Although the roots of the computer virus date back as early as 1949, when the Hungarian scientist John von Neumann published the “*Theory of self-reproducing automata*”, *[4] the first known computer virus appeared in 1971 and was dubbed the “Creeper virus”.*[5] This computer virus infected Digital Equipment Corporation's (DEC) PDP-10 mainframe computers running the TENEX operating system.*[6]*[7]

The Creeper virus was eventually deleted by a program created by Ray Tomlinson and known as “The Reaper”.*[8] Some people consider “The Reaper” the first antivirus software ever written – it may be the case, but it is important to note that the Reaper was actually a virus itself specifically designed to remove the Creeper virus.*[8]*[9]*[10]

The Creeper virus was followed by several other viruses. The first known that appeared “in the wild” was “Elk Cloner”, in 1981, which infected Apple II computers.*[11]*[12]*[13]

In 1983, the term “*computer virus*” was coined by Fred Cohen in one of the first ever published academic papers on computer viruses.*[14] Cohen used the term “*computer virus*” to describe a program that: “*affect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of itself.*” *[15] (note that a more recent, and precise, definition of computer virus has been given by the Hungarian security researcher Péter Ször: “*a code that recursively replicates a possibly evolved copy of itself*” *[16]*[17])

The first IBM PC compatible “in the wild” computer virus, and one of the first real widespread infections, was “Brain” in 1986. From then, the number of viruses has grown exponentially.*[18]*[19] Most of the computer viruses written in the early and mid-1980s were limited to self-reproduction and had no specific damage routine built into the code. That changed when more and more programmers became acquainted with computer virus programming and created viruses that manipulated or even destroyed data on infected computers.*[20]

Before internet connectivity was widespread, computer viruses were typically spread by infected floppy disks. Antivirus software came into use, but was updated relatively infrequently. During this time, virus checkers essentially had to check executable files and the boot sectors of floppy disks and hard disks. However, as internet usage became common, viruses began to spread online.*[21]

21.1.2 1980–1990 period (early days)

There are competing claims for the innovator of the first antivirus product. Possibly, the first publicly documented removal of an “in the wild” computer virus (i.e. the “Vienna virus”) was performed by Bernd Fix in 1987.*[22]*[23]

In 1987, Andreas Lüning and Kai Figge founded G Data Software and released their first antivirus product for the Atari ST platform.*[24] Dubiously, they later also produced Virus Construction Kits.*[25] In 1987, the *Ultimate Virus Killer (UVK)* was also released.*[26] This was the de facto industry standard virus killer for the Atari ST and Atari Falcon, the last version of which (version 9.0) was released in April 2004. In 1987, in the United States, John McAfee founded the McAfee company (now part of Intel Security*|[27]) and, at the end of that year, he released the first version of *VirusScan*.*[28] In the meanwhile, in Czechoslovakia, Peter Paško, Rudolf Hrubý and Miroslav Trnka created the first version of NOD antivirus (albeit they established ESET after the communist period, as private ownership was not allowed in 1992).*[29]*[30]

In 1987, Fred Cohen wrote that *there is no algorithm that can perfectly detect all possible computer viruses*.*[31]

Finally, in the end of 1987, the first two heuristic antivirus utilities were released: *Flushot Plus* by Ross Greenberg*[32]*[33]*[34] and *Anti4us* by Erwin Lanting.*[35] In his O'Reilly book, *Malicious Mobile Code: Virus Protection for Windows*, Roger Grimes described Flushot Plus as “the first holistic program to fight MMC [malicious mobile code].” *[36]

However, the kind of heuristic used by early AV engines was totally different from those used today. The first product with a heuristic engine resembling modern ones was F-PROT in 1991.*[37] Early heuristic engines were based on dividing the binary in different sections: data section, code section (in a legitimate binary, it usually starts always from the same location). Indeed, the initial viruses re-organized the layout of the sections, or overrode the initial portion of section in order to jump to the very end of the file where malicious code was located—only going back to resume

execution of the original code. This was a very specific pattern, not used at the time by any legitimate software, which represented an elegant heuristic to catch suspicious code. Other kinds of more advanced heuristics were later added, such as suspicious section names, incorrect header size, regular expressions, and partial pattern in-memory matching.

In 1988, the growth of antivirus companies continued. In Germany, Tjark Auerbach founded **Avira** (*H+BEDV* at the time) and released the first version of **AntiVir** (named “*Luke Filewalker*” at the time). In Bulgaria, Dr. Vesselin Bontchev released his first freeware antivirus program (he later joined **FRISK Software**). Also Frans Veldman released the first version of **ThunderByte Antivirus**, also known as **TBAV** (he sold his company to **Norman Safeground** in 1998). In **Czech Republic**, Pavel Baudiš and Eduard Kučera started **avast!** (at the time *ALWIL Software*) and released their first version of **avast!** antivirus. In June 1988, in **South Korea**, Dr. Ahn Cheol-Soo released its first antivirus software, called **V1** (he founded **AhnLab** later in 1995). Finally, in the Autumn 1988, in **United Kingdom**, Alan Solomon founded **S&S International** and created his **Dr. Solomon's Anti-Virus Toolkit** (although he launched it commercially only in 1991 – in 1998 Dr. Solomon’s company was acquired by **McAfee**). In November 1988 a professor at the Panamerican University in Mexico City named Alejandro E. Carriles copyrighted the first antivirus software in Mexico under the name “*Byte Matabichos*” (*Byte Bugkiller*) to help solve the rampant virus infestation among students.*[38]

Also in 1988, a mailing list named **VIRUS-L***[39] was started on the **BITNET/EARN** network where new viruses and the possibilities of detecting and eliminating viruses were discussed. Some members of this mailing list were: Alan Solomon, Eugene Kaspersky (Kaspersky Lab), Friðrik Skúlason (FRISK Software), John McAfee (McAfee), Luis Corrons (Panda Security), Mikko Hyppönen (F-Secure), Péter Szőr, Tjark Auerbach (Avira) and Dr. Vesselin Bontchev (FRISK Software).*[39]

In 1989, in **Iceland**, Friðrik Skúlason created the first version of **F-PROT Anti-Virus** back in 1989 (he founded **FRISK Software** only in 1993). In the meanwhile, in **United States**, **Symantec** (founded by Gary Hendrix in 1982) launched its first **Symantec antivirus for Macintosh** (SAM).*[40]*[41] SAM 2.0, released March 1990, incorporated technology allowing users to easily update SAM to intercept and eliminate new viruses, including many that didn't exist at the time of the program's release.*[42]

In the end of the 1980s, in **United Kingdom**, Jan Hruska and Peter Lammer founded the security firm **Sophos** and began producing their first antivirus and encryption products. In the same period, in **Hungary**, also **VirusBuster** was founded (which has recently being incorporated by **Sophos**).

21.1.3 1990–2000 period (emergence of the antivirus industry)

In 1990, in **Spain**, Mikel Urizarbarrena founded **Panda Security** (*Panda Software* at the time).*[43] In **Hungary**, the security researcher Péter Szőr released the first version of **Pasteur** antivirus. In **Italy**, Gianfranco Tonello created the first version of **VirIT eXplorer** antivirus (he founded **TG Soft** one year later).*[44]

In 1990, the **Computer Antivirus Research Organization (CARO)** was founded. In 1991, CARO released the “*Virus Naming Scheme*”, originally written by Friðrik Skúlason and Vesselin Bontchev.*[45] Although this naming scheme is now outdated, it remains the only existing standard that most computer security companies and researchers ever attempted to adopt. **CARO** members includes: Alan Solomon, Costin Raiu, Dmitry Gryaznov, Eugene Kaspersky, Friðrik Skúlason, Igor Muttik, Mikko Hyppönen, Morton Swimmer, Nick Fitzgerald, Padgett Peterson, Peter Ferrie, Righard Zwienenberg and Dr. Vesselin Bontchev.*[46]*[47]

In 1991, in the **United States**, **Symantec** released the first version of **Norton Anti-Virus**. In the same year, in **Czechoslovakia**, Jan Gritzbach and Tomáš Hofer founded **AVG Technologies** (*Grisoft* at the time), although they released the first version of their **Anti-Virus Guard** (AVG) only in 1992. On the other hand, in **Finland**, **F-Secure** (founded in 1988 by Petri Allas and Risto Siilasmaa – with the name of Data Fellows) released the first version of their antivirus product. **F-Secure** claims to be the first antivirus firm to establish a presence on the World Wide Web.*[48]

In 1991, the **European Institute for Computer Antivirus Research (EICAR)** was founded to further antivirus research and improve development of antivirus software.*[49]*[50]

In 1992, in **Russia**, Igor Danilov released the first version of **SpiderWeb**, which later became **Dr. Web**.*[51]

In 1994, **AV-TEST** reported that there were 28,613 unique malware samples (based on MD5) in their database.*[52]

Over time other companies were founded. In 1996, in **Romania**, **Bitdefender** was founded and released the first version of **Anti-Virus eXpert (AVX)**.*[53] In 1997, in **Russia**, Eugene Kaspersky and Natalia Kaspersky co-founded security firm **Kaspersky Lab**.*[54]

In 1996, there was also the first “in the wild” **Linux** virus, known as “*Staog*”.*[55]

In 1999, AV-TEST reported that there were 98,428 unique malware samples (based on MD5) in their database.*[52]

21.1.4 2000–2005 period

In 2000, Rainer Link and Howard Fuhs started the first open source antivirus engine, called *OpenAntivirus Project*.*[56]

In 2001, Tomasz Kojm released the first version of ClamAV, the first ever open source antivirus engine to be commercialised. In 2007, ClamAV was bought by Sourcefire,*[57] which in turn was acquired by Cisco Systems in 2013.*[58]

In 2002, in United Kingdom, Morten Lund and Theis Søndergaard co-founded the antivirus firm BullGuard.*[59]

In 2005, AV-TEST reported that there were 333,425 unique malware samples (based on MD5) in their database.*[52]

21.1.5 2005 to 2014 period

In 2007, AV-TEST reported a number of 5,490,960 new unique malware samples (based on MD5) only for that year.*[52] In 2012 and 2013, antivirus firms reported a new malware samples range from 300,000 to over 500,000 per day.*[60]*[61]

Over the years it has become necessary for antivirus software to use several different strategies (e.g. specific email and network protection or low level modules) and detection algorithms, as well as to check an increasing variety of files, rather than just executables, for several reasons:

- Powerful macros used in word processor applications, such as Microsoft Word, presented a risk. Virus writers could use the macros to write viruses embedded within documents. This meant that computers could now also be at risk from infection by opening documents with hidden attached macros.*[62]
- The possibility of embedding executable objects inside otherwise non-executable file formats can make opening those files a risk.*[63]
- Later email programs, in particular Microsoft's Outlook Express and Outlook, were vulnerable to viruses embedded in the email body itself. A user's computer could be infected by just opening or previewing a message.*[64]

In 2005, F-Secure was the first security firm that developed an Anti-Rootkit technology, called *BlackLight*.

Given the consideration that most of the people is nowadays connected to the Internet round-the-clock, in 2008, Jon Oberheide first proposed a Cloud-based antivirus design.*[65]

In February 2008 McAfee Labs added the industry-first cloud-based anti-malware functionality to VirusScan under Artemis name. It was tested by AV-Comparatives in February 2008* [66] and officially unveiled in August 2008 in McAfee VirusScan.*[67]

Cloud AV created problems for comparative testing of security software – part of the AV definitions was out of testers control (on constantly updated AV company servers) thus making results non-repeatable. As a result, Anti-Malware Testing Standards Organisation (AMTSO) started working on methodology of testing cloud products which was adopted on May 7, 2009.*[68]

In 2011, AVG introduced a similar cloud service, called Protective Cloud Technology.*[69]

21.1.6 2014 to present (rise of next-gen)

More recently, following the 2014 release of the APT 1 report from Mandiant, the industry has seen a shift towards signature-less approaches to the problem capable of detecting and mitigating zero-day attacks. Numerous approaches to address these new forms of threats have appeared, including behavioral detection, artificial intelligence, machine learning, and cloud-based file detonation. According to Gartner, it is expected the rise of new entrants, such Carbon Black, Cylance and CrowdStrike will force EPP incumbents into a new phase of innovation and acquisition.*[70] One method from Bromium involves micro-virtualization to protect desktops from malicious code execution initiated by the end user. Another approach from SentinelOne and Carbon Black focuses on behavioral detection by building a full context around every process execution path in real time,*[71]*[72] while Cylance leverages an artificial intelligence

model based on machine learning.*[73] Increasingly, these signature-less approaches have been defined by the media and analyst firms as “next-generation” antivirus* [74] and are seeing rapid market adoption as certified antivirus replacement technologies by firms such as Coalfire and DirectDefense.* [75] In response, traditional antivirus vendors such as Trend Micro,* [76] Symantec and Sophos* [77] have responded by incorporating “next-gen” offerings into their portfolios as analyst firms such as Forrester and Gartner have called traditional signature-based antivirus “ineffective” and “outdated”.* [78]

21.2 Identification methods

One of the few solid theoretical results in the study of computer viruses is Frederick B. Cohen's 1987 demonstration that there is no algorithm that can perfectly detect all possible viruses.* [31] However, using different layers of defense, a good detection rate may be achieved.

There are several methods which antivirus engine can use to identify malware:

- **Sandbox detection:** is a particular behavioural-based detection technique that, instead of detecting the behavioural fingerprint at run time, it executes the programs in a virtual environment, logging what actions the program performs. Depending on the actions logged, the antivirus engine can determine if the program is malicious or not.* [79] If not, then, the program is executed in the real environment. Albeit this technique has shown to be quite effective, given its heaviness and slowness, it is rarely used in end-user antivirus solutions.* [80]
- **Data mining techniques:** are one of the latest approach applied in malware detection. Data mining and machine learning algorithms are used to try to classify the behaviour of a file (as either malicious or benign) given a series of file features, that are extracted from the file itself.* [81]* [82]* [83]* [84]* [85]* [86]* [87]* [88]* [89]* [90]* [91]* [92]*

21.2.1 Signature-based detection

Traditional antivirus software relies heavily upon signatures to identify malware.* [95]

Substantially, when a malware arrives in the hands of an antivirus firm, it is analysed by malware researchers or by dynamic analysis systems. Then, once it is determined to be a malware, a proper signature of the file is extracted and added to the signatures database of the antivirus software.* [96]

Although the signature-based approach can effectively contain malware outbreaks, malware authors have tried to stay a step ahead of such software by writing "oligomorphic", "polymorphic" and, more recently, "metamorphic" viruses, which encrypt parts of themselves or otherwise modify themselves as a method of disguise, so as to not match virus signatures in the dictionary.* [97]

21.2.2 Heuristics

Many viruses start as a single infection and through either mutation or refinements by other attackers, can grow into dozens of slightly different strains, called variants. Generic detection refers to the detection and removal of multiple threats using a single virus definition.* [98]

For example, the Vundo trojan has several family members, depending on the antivirus vendor's classification. Symantec classifies members of the Vundo family into two distinct categories, *Trojan.Vundo* and *Trojan.Vundo.B*.* [99]* [100]

While it may be advantageous to identify a specific virus, it can be quicker to detect a virus family through a generic signature or through an inexact match to an existing signature. Virus researchers find common areas that all viruses in a family share uniquely and can thus create a single generic signature. These signatures often contain non-contiguous code, using wildcard characters where differences lie. These wildcards allow the scanner to detect viruses even if they are padded with extra, meaningless code.* [101] A detection that uses this method is said to be “heuristic detection.”

21.2.3 Rootkit detection

Main article: Rootkit

Anti-virus software can attempt to scan for rootkits. A **rootkit** is a type of **malware** designed to gain administrative-level control over a computer system without being detected. Rootkits can change how the **operating system** functions and in some cases can tamper with the anti-virus program and render it ineffective. Rootkits are also difficult to remove, in some cases requiring a complete re-installation of the operating system.*[102]

21.2.4 Real-time protection

Real-time protection, on-access scanning, background guard, resident shield, autoprotect, and other synonyms refer to the automatic protection provided by most antivirus, anti-spyware, and other anti-malware programs. This monitors computer systems for suspicious activity such as computer viruses, spyware, adware, and other malicious objects in 'real-time', in other words while data loaded into the computer's active memory: when inserting a CD, opening an email, or browsing the web, or when a file already on the computer is opened or executed.*[103]

21.3 Issues of concern

21.3.1 Unexpected renewal costs

Some commercial antivirus software **end-user license agreements** include a clause that the **subscription** will be automatically renewed, and the purchaser's credit card automatically billed, at the renewal time without explicit approval. For example, **McAfee** requires users to unsubscribe at least 60 days before the expiration of the present subscription*^[104] while **BitDefender** sends notifications to unsubscribe 30 days before the renewal.*^[105] **Norton AntiVirus** also renews subscriptions automatically by default.*^[106]

21.3.2 Rogue security applications

Main article: **Rogue security software**

Some apparent antivirus programs are actually malware masquerading as legitimate software, such as **WinFixer**, **MS Antivirus**, and **Mac Defender**.*^[107]

21.3.3 Problems caused by false positives

A "false positive" or "false alarm" is when antivirus software identifies a non-malicious file as malware. When this happens, it can cause serious problems. For example, if an antivirus program is configured to immediately delete or quarantine infected files, as is common on **Microsoft Windows** antivirus applications, a false positive in an essential file can render the Windows **operating system** or some applications unusable.*^[108] Recovering from such damage to critical software infrastructure incurs technical support costs and businesses can be forced to close whilst remedial action is undertaken.*^[109]*^[110] For example, in May 2007 a faulty virus signature issued by **Symantec** mistakenly removed essential operating system files, leaving thousands of PCs unable to boot.*^[111]

Also in May 2007, the **executable file** required by **Pegasus Mail** on Windows was falsely detected by **Norton AntiVirus** as being a Trojan and it was automatically removed, preventing Pegasus Mail from running. Norton AntiVirus had falsely identified three releases of Pegasus Mail as malware, and would delete the Pegasus Mail installer file when that happened.*^[112] In response to this Pegasus Mail stated:

In April 2010, **McAfee VirusScan** detected svchost.exe, a normal Windows binary, as a virus on machines running **Windows XP** with Service Pack 3, causing a reboot loop and loss of all network access.*^[113]*^[114]

In December 2010, a faulty update on the **AVG** anti-virus suite damaged 64-bit versions of **Windows 7**, rendering it unable to boot, due to an endless boot loop created.*^[115]

In October 2011, **Microsoft Security Essentials** (MSE) removed the **Google Chrome** web browser, rival to Microsoft's own **Internet Explorer**. MSE flagged Chrome as a **Zbot** banking trojan.*^[116]

In September 2012, **Sophos'** anti-virus suite identified various update-mechanisms, including its own, as malware. If it was configured to automatically delete detected files, Sophos Antivirus could render itself unable to update, required manual intervention to fix the problem.*^[117]*^[118]

21.3.4 System and interoperability related issues

Running (the real-time protection of) multiple antivirus programs concurrently can degrade performance and create conflicts.*[119] However, using a concept called multiscanning, several companies (including G Data Software* [120] and Microsoft* [121]) have created applications which can run multiple engines concurrently.

It is sometimes necessary to temporarily disable virus protection when installing major updates such as Windows Service Packs or updating graphics card drivers.*[122] Active antivirus protection may partially or completely prevent the installation of a major update. Anti-virus software can cause problems during the installation of an operating system upgrade, e.g. when upgrading to a newer version of Windows “in place” —without erasing the previous version of Windows. Microsoft recommends that anti-virus software be disabled to avoid conflicts with the upgrade installation process.*[123]*[124]*[125]

The functionality of a few computer programs can be hampered by active anti-virus software. For example, TrueCrypt, a disk encryption program, states on its troubleshooting page that anti-virus programs can conflict with TrueCrypt and cause it to malfunction or operate very slowly.*[126] Anti-virus software can impair the performance and stability of games running in the Steam platform.*[127]

Support issues also exist around antivirus application interoperability with common solutions like SSL VPN remote access and network access control products.*[128] These technology solutions often have policy assessment applications which require that an up-to-date antivirus is installed and running. If the antivirus application is not recognized by the policy assessment, whether because the antivirus application has been updated or because it is not part of the policy assessment library, the user will be unable to connect.

21.3.5 Effectiveness

Studies in December 2007 showed that the effectiveness of antivirus software had decreased in the previous year, particularly against unknown or zero day attacks. The computer magazine *c’t* found that detection rates for these threats had dropped from 40–50% in 2006 to 20–30% in 2007. At that time, the only exception was the NOD32 antivirus, which managed a detection rate of 68%.*[129] According to the ZeuS tracker website the average detection rate for all variants of the well-known ZeuS trojan is as low as 40%.*[130]

The problem is magnified by the changing intent of virus authors. Some years ago it was obvious when a virus infection was present. The viruses of the day, written by amateurs, exhibited destructive behavior or pop-ups. Modern viruses are often written by professionals, financed by criminal organizations.*[131]

In 2008, Eva Chen, CEO of Trend Micro, stated that the anti-virus industry has over-hyped how effective its products are —and so has been misleading customers —for years.*[132]

Independent testing on all the major virus scanners consistently shows that none provide 100% virus detection. The best ones provided as high as 99.9% detection for simulated real-world situations, while the lowest provided 91.1% in tests conducted in August 2013. Many virus scanners produce false positive results as well, identifying benign files as malware.*[133]

Although methodologies may differ, some notable independent quality testing agencies include AV-Comparatives, ICSA Labs, West Coast Labs, Virus Bulletin, AV-TEST and other members of the Anti-Malware Testing Standards Organization.*[134]*[135]

21.3.6 New viruses

Anti-virus programs are not always effective against new viruses, even those that use non-signature-based methods that should detect new viruses. The reason for this is that the virus designers test their new viruses on the major anti-virus applications to make sure that they are not detected before releasing them into the wild.*[136]

Some new viruses, particularly ransomware, use polymorphic code to avoid detection by virus scanners. Jerome Segura, a security analyst with ParetoLogic, explained.*[137]

A proof of concept virus has used the Graphics Processing Unit (GPU) to avoid detection from anti-virus software. The potential success of this involves bypassing the CPU in order to make it much harder for security researchers to analyse the inner workings of such malware.*[138]

21.3.7 Rootkits

Detecting rootkits is a major challenge for anti-virus programs. Rootkits have full administrative access to the computer and are invisible to users and hidden from the list of running processes in the task manager. Rootkits can modify the inner workings of the operating system and tamper with antivirus programs.^{*[139]}

21.3.8 Damaged files

If a file has been infected by a computer virus, anti-virus software will attempt to remove the virus code from the file during disinfection, but it is not always able to restore the file to its undamaged state.^{*[140]*[141]} In such circumstances, damaged files can only be restored from existing backups or shadow copies (this is also true for ransomware^{*[142]}); installed software that is damaged requires re-installation^{*[143]} (however, see System File Checker).

21.3.9 Firmware issues

Active anti-virus software can interfere with a firmware update process.^{*[144]} Any writeable firmware in the computer can be infected by malicious code.^{*[145]} This is a major concern, as an infected BIOS could require the actual BIOS chip to be replaced to ensure the malicious code is completely removed.^{*[146]} Anti-virus software is not effective at protecting firmware and the motherboard BIOS from infection.^{*[147]} In 2014, security researchers discovered that USB devices contain writeable firmware which can be modified with malicious code (dubbed "BadUSB"), which anti-virus software cannot detect or prevent. The malicious code can run undetected on the computer and could even infect the operating system prior to it booting up.^{*[148]*[149]}

21.4 Performance and other drawbacks

Antivirus software has some drawbacks, first of which that it can impact a computer's performance.^{*[150]}

Furthermore, inexperienced users can be lulled into a false sense of security when using the computer, considering themselves to be invulnerable, and may have problems understanding the prompts and decisions that antivirus software presents them with. An incorrect decision may lead to a security breach. If the antivirus software employs heuristic detection, it must be fine-tuned to minimize misidentifying harmless software as malicious (false positive).^{*[151]}

Antivirus software itself usually runs at the highly trusted kernel level of the operating system to allow it access to all the potential malicious process and files, creating a potential avenue of attack.^{*[152]} The UK and US intelligence agencies, GCHQ and the National Security Agency (NSA), respectively, have been exploiting anti-virus software to spy on users.^{*[153]} Anti-virus software has highly privileged and trusted access to the underlying operating system, which makes it a much more appealing target for remote attacks.^{*[154]} Additionally anti-virus software is “years behind security-conscious client-side applications like browsers or document readers”, according to Joxean Koret, a researcher with Coseinc, a Singapore-based information security consultancy.^{*[154]}

21.5 Alternative solutions

Installed antivirus solutions, running on individual computers, although the most used, is only one method of guarding against malware. Other alternative solutions are also used, including: Unified Threat Management (UTM), hardware and network firewalls, Cloud-based antivirus and on-line scanners.

21.5.1 Hardware and network firewall

Network firewalls prevent unknown programs and processes from accessing the system. However, they are not antivirus systems and make no attempt to identify or remove anything. They may protect against infection from outside the protected computer or network, and limit the activity of any malicious software which is present by blocking incoming or outgoing requests on certain TCP/IP ports. A firewall is designed to deal with broader system threats that come from network connections into the system and is not an alternative to a virus protection system.

```

adama@~:~$ sudo freshclam
ClamAV update process started at Tue Aug 18 08:16:01 2009
main.cld is up to date (version: 51, sigs: 545035, f-level: 42, builder: sven)
daily.cld is up to date (version: 9709, sigs: 64749, f-level: 43, builder: ccordes)
adama@~:~$ clamscan ~/Virus/setup.exe
/home/adama/Virus/setup.exe: Trojan.Fakeav-104 FOUND

----- SCAN SUMMARY -----
Known viruses: 609137
Engine version: 0.95.2
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.02 MB
Data read: 0.02 MB (ratio 1.00:1)
Time: 2.443 sec (0 m 2 s)
adama@~:~$ 

```

The command-line virus scanner of *Clam AV 0.95.2*, an open source antivirus originally developed by Tomasz Kojm in 2001. Here running a virus signature definition update, scanning a file and identifying a Trojan.

21.5.2 Cloud antivirus

Cloud antivirus is a technology that uses lightweight agent software on the protected computer, while offloading the majority of data analysis to the provider's infrastructure.*[155]

One approach to implementing cloud antivirus involves scanning suspicious files using multiple antivirus engines. This approach was proposed by an early implementation of the cloud antivirus concept called CloudAV. CloudAV was designed to send programs or documents to a **network cloud** where multiple antivirus and behavioral detection programs are used simultaneously in order to improve detection rates. Parallel scanning of files using potentially incompatible antivirus scanners is achieved by spawning a virtual machine per detection engine and therefore eliminating any possible issues. CloudAV can also perform “retrospective detection,” whereby the cloud detection engine rescans all files in its file access history when a new threat is identified thus improving new threat detection speed. Finally, CloudAV is a solution for effective virus scanning on devices that lack the computing power to perform the scans themselves.*[156]

Some examples of cloud anti-virus products are Panda Cloud Antivirus, Crowdstrike, Cb Defense and Immunet. Comodo group has also produced cloud-based anti-virus.*[157]*[158]

21.5.3 Online scanning

Some antivirus vendors maintain websites with free online scanning capability of the entire computer, critical areas only, local disks, folders or files. Periodic online scanning is a good idea for those that run antivirus applications on their computers because those applications are frequently slow to catch threats. One of the first things that malicious software does in an attack is disable any existing antivirus software and sometimes the only way to know of an attack is by turning to an online resource that is not installed on the infected computer.*[159]

```
[ Rootkit Hunter version 1.3.6 ]

Checking rkhunter version...
This version : 1.3.6
Latest version: 1.3.8
Update available

Checking system commands...

Performing 'strings' command checks
  Checking 'strings' command [ OK ]

Performing 'shared libraries' checks
  Checking for preloading variables [ None found ]
  Checking for preloaded libraries [ None found ]
  Checking LD_LIBRARY_PATH variable [ Not found ]

Performing file properties checks
  Checking for prerequisites [ OK ]
  /bin/bash [ OK ]
  /bin/cat [ OK ]
  /bin/chmod [ OK ]
  /bin/chown [ OK ]
  /bin/cp [ OK ]
```

The command-line rkhunter scanner, an engine to scan for Linux rootkits. Here running the tool on Ubuntu.

21.5.4 Specialist tools

Virus removal tools are available to help remove stubborn infections or certain types of infection. Examples include Trend Micro's *Rootkit Buster*,^{*[160]} and *rkhunter* for the detection of rootkits, Avira's *AntiVir Removal Tool*,^{*[161]} *PCTools Threat Removal Tool*,^{*[162]} and AVG's Anti-Virus Free 2011.^{*[163]}

A rescue disk that is bootable, such as a CD or USB storage device, can be used to run antivirus software outside of the installed operating system, in order to remove infections while they are dormant. A bootable antivirus disk can be useful when, for example, the installed operating system is no longer bootable or has malware that is resisting all attempts to be removed by the installed antivirus software. Examples of some of these bootable disks include the *Avira AntiVir Rescue System*,^{*[161]} *PCTools Alternate Operating System Scanner*,^{*[164]} and *AVG Rescue CD*.^{*[165]} The AVG Rescue CD software can also be installed onto a USB storage device, that is bootable on newer computers.^{*[165]}

21.6 Usage and risks

According to an FBI survey, major businesses lose \$12 million annually dealing with virus incidents.^{*[166]} A survey by Symantec in 2009 found that a third of small to medium-sized business did not use antivirus protection at that time, whereas more than 80% of home users had some kind of antivirus installed.^{*[167]} According to a sociological survey conducted by G Data Software in 2010 49% of women did not use any antivirus program at all.^{*[168]}

21.7 See also

- Anti-virus and anti-malware software
- CARO, the Computer Antivirus Research Organization
- Comparison of antivirus software
- Comparison of computer viruses
- EICAR, the European Institute for Computer Antivirus Research

- Firewall software
- Internet security
- Linux malware
- Quarantine (computing)
- Sandbox (computer security)
- Timeline of computer viruses and worms
- Virus hoax

21.8 References

- [1] Naveen, Sharanya. “Anti-virus software” . Retrieved May 31, 2016.
- [2] Henry, Alan. “The Difference Between Antivirus and Anti-Malware (and Which to Use)” .
- [3] “What is antivirus software?”. Microsoft. Archived from the original on April 11, 2011.
- [4] von Neumann, John (1966) *Theory of self-reproducing automata*. University of Illinois Press.
- [5] Thomas Chen, Jean-Marc Robert (2004). “The Evolution of Viruses and Worms” . Retrieved February 16, 2009.
- [6] From the first email to the first YouTube video: a definitive internet history. Tom Meltzer and Sarah Phillips. *The Guardian*. October 23, 2009
- [7] *IEEE Annals of the History of Computing, Volumes 27–28*. IEEE Computer Society, 2005. 74: “[...]from one machine to another led to experimentation with the *Creeper* program, which became the world's first computer worm: a computation that used the network to recreate itself on another node, and spread from node to node.”
- [8] John Metcalf (2014). “Core War: Creeper & Reaper” . Retrieved May 1, 2014.
- [9] “Creeper – The Virus Encyclopedia” .
- [10] What was the First Antivirus Software?. Anti-virus-software-review.toptenreviews.com. Retrieved on January 3, 2017.
- [11] “Elk Cloner” . Retrieved December 10, 2010.
- [12] “Top 10 Computer Viruses: No. 10 – Elk Cloner” . Retrieved December 10, 2010.
- [13] “List of Computer Viruses Developed in 1980s” . Retrieved December 10, 2010.
- [14] Fred Cohen: “Computer Viruses – Theory and Experiments” (1983). Eecs.umich.edu (November 3, 1983). Retrieved on 2017-01-03.
- [15] Cohen, Fred (April 1, 1988). “Invited Paper: On the Implications of Computer Viruses and Methods of Defense” . *Computers & Security*. 7 (2): 167–184. doi:10.1016/0167-4048(88)90334-3 – via ACM Digital Library.
- [16] Szor, Peter (February 13, 2005). *The Art of Computer Virus Research and Defense*. Addison-Wesley Professional. ISBN 0321304543 – via Amazon.
- [17] “Virus Bulletin :: In memoriam: Péter Ször 1970–2013” .
- [18] “History of Viruses” .
- [19] Leyden, John (January 19, 2006). “PC virus celebrates 20th birthday” . *The Register*. Retrieved March 21, 2011.
- [20] “About computer viruses of 1980's” (PDF). Retrieved February 17, 2016.
- [21] Panda Security (April 2004). "(II) Evolution of computer viruses” . Archived from the original on August 2, 2009. Retrieved June 20, 2009.
- [22] Kaspersky Lab Virus list. viruslist.com
- [23] Wells, Joe (August 30, 1996). “Virus timeline” . IBM. Archived from the original on June 4, 2008. Retrieved June 6, 2008.

- [24] G Data Software AG (2011). “G Data presents security firsts at CeBIT 2010” . Retrieved August 22, 2011.
- [25] G Data Software AG (2016). “Virus Construction Set II” . Retrieved July 3, 2016.
- [26] Karsmakers, Richard (January 2010). “The ultimate Virus Killer Book and Software” . Retrieved July 6, 2016.
- [27] “McAfee Becomes Intel Security” . McAfee Inc. Retrieved January 15, 2014.
- [28] Cavendish, Marshall (2007). *Inventors and Inventions, Volume 4*. Paul Bernabeo. p. 1033. ISBN 0761477675.
- [29] “About ESET Company” .
- [30] “ESET NOD32 Antivirus” . Vision Square. February 16, 2016.
- [31] Cohen, Fred, An Undetectable Computer Virus (Archived), 1987, IBM
- [32] Yevics, Patricia A. “Flu Shot for Computer Viruses” . americanbar.org.
- [33] Strom, David (April 1, 2010). “How friends help friends on the Internet: The Ross Greenberg Story” . wordpress.com.
- [34] “Anti-virus is 30 years old” . spgedwards.com. April 2012.
- [35] “A Brief History of Antivirus Software” . techlineinfo.com.
- [36] Grimes, Roger A. (June 1, 2001). *Malicious Mobile Code: Virus Protection for Windows*. O'Reilly Media, Inc. p. 522. ISBN 9781565926820.
- [37] “F-PROT Tækniþjónusta – CYREN Iceland” . frisk.is.
- [38] Dirección General del Derecho de Autor, SEP, Mexico D.F. Registry 20709/88 Book 8, page 40, dated November 24, 1988.
- [39] “The 'Security Digest' Archives (TM) : www.phreak.org-virus_1” .
- [40] “Symantec Softwares and Internet Security at PCM” .
- [41] SAM Identifies Virus-Infected Files, Repairs Applications, *InfoWorld*, May 22, 1989
- [42] SAM Update Lets Users Program for New Viruses, *InfoWorld*, February 19, 1990
- [43] Naveen, Sharanya. “Panda Security” . Retrieved May 31, 2016.
- [44] <http://www.tgsoft.it>, TG Soft S.a.s. —. “Who we are – TG Soft Software House” .
- [45] “A New Virus Naming Convention (1991) – CARO – Computer Antivirus Research Organization” .
- [46] “CARO Members” . CARO. Retrieved June 6, 2011.
- [47] CAROids, Hamburg 2003 Archived November 7, 2014, at the Wayback Machine.
- [48] “F-Secure Weblog : News from the Lab” . F-secure.com. Retrieved September 23, 2012.
- [49] “About EICAR” . *EICAR official website*. Retrieved October 28, 2013.
- [50] David Harley, Lysa Myers & Eddy Willems. “Test Files and Product Evaluation: the Case for and against Malware Simulation” (PDF). AVAR2010 13th Association of anti Virus Asia Researchers International Conference. Archived from the original (PDF) on September 29, 2011. Retrieved June 30, 2011.
- [51] “Dr. Web LTD Doctor Web / Dr. Web Reviews, Best AntiVirus Software Reviews, Review Centre” . Reviewcentre.com. Retrieved February 17, 2014.
- [52] [In 1994, AV-Test.org reported 28,613 unique malware samples (based on MD5). “A Brief History of Malware; The First 25 Years”]
- [53] “BitDefender Product History” . Archived from the original on March 17, 2012.
- [54] “InfoWatch Management” . InfoWatch. Retrieved August 12, 2013.
- [55] “Linuxvirus – Community Help Wiki” .
- [56] “Sorry – recovering...” .

- [57] “Sourcefire acquires ClamAV” . ClamAV. August 17, 2007. Archived from the original on December 15, 2007. Retrieved February 12, 2008.
- [58] “Cisco Completes Acquisition of Sourcefire” . cisco.com. October 7, 2013. Retrieved June 18, 2014.
- [59] Der Unternehmer – brand eins online. Brandeins.de (July 2009). Retrieved on January 3, 2017.
- [60] Williams, Greg (April 2012). “The digital detective: Mikko Hypponen's war on malware is escalating” . Wired.
- [61] “Everyday cybercrime – and what you can do about it” .
- [62] Szor 2005, pp. 66–67
- [63] “New virus travels in PDF files” . August 7, 2001. Retrieved October 29, 2011.
- [64] Slipstick Systems (February 2009). “Protecting Microsoft Outlook against Viruses” . Archived from the original on June 2, 2009. Retrieved June 18, 2009.
- [65] “CloudAV: N-Version Antivirus in the Network Cloud” . usenix.org.
- [66] McAfee Artemis Preview Report. av-comparatives.org
- [67] McAfee Third Quarter 2008. corporate-ir.net
- [68] “AMTSO Best Practices for Testing In-the-Cloud Security Products » AMTSO” .
- [69] “TECHNOLOGY OVERVIEW” . AVG Security. Archived from the original on June 2, 2015. Retrieved February 16, 2015.
- [70] “Magic Quadrant Endpoint Protection Platforms 2016” . Gartner Research.
- [71] Messmer, Ellen. “Start-up offers up endpoint detection and response for behavior-based malware detection” . network-world.com.
- [72] “Homeland Security Today: Bromium Research Reveals Insecurity in Existing Endpoint Malware Protection Deployments” .
- [73] “Duelling Unicorns: CrowdStrike Vs. Cylance In Brutal Battle To Knock Hackers Out” . Forbes. July 6, 2016.
- [74] Potter, Davitt (June 9, 2016). “Is Anti-virus Dead? The Shift Toward Next-Gen Endpoints” .
- [75] “CylancePROTECT® Achieves HIPAA Security Rule Compliance Certification” . Cylance.
- [76] “Trend Micro-XGen” . Trend Micro. October 18, 2016.
- [77] “Next-Gen Endpoint” . Sophos.
- [78] The Forrester Wave™: Endpoint Security Suites, Q4 2016. Forrester.com (October 19, 2016). Retrieved on 2017-01-03.
- [79] Sandboxing Protects Endpoints | Stay Ahead Of Zero Day Threats. Enterprise.comodo.com (June 20, 2014). Retrieved on 2017-01-03.
- [80] Szor 2005, pp. 474–481
- [81] Kiem, Hoang; Thuy, Nguyen Yhanh and Quang, Truong Minh Nhat (December 2004) “A Machine Learning Approach to Anti-virus System” , *Joint Workshop of Vietnamese Society of AI, SIGKBS-JSAI, ICS-IPSJ and IEICE-SIGAI on Active Mining ; Session 3: Artificial Intelligence*, Vol. 67, pp. 61–65
- [82] *Data Mining Methods for Malware Detection*. ProQuest. 2008. pp. 15–. ISBN 978-0-549-88885-7.
- [83] Dua, Sumeet; Du, Xian (April 19, 2016). *Data Mining and Machine Learning in Cybersecurity*. CRC Press. pp. 1–. ISBN 978-1-4398-3943-0.
- [84] Firdausi, Ivan; Lim, Charles; Erwin, Alva; Nugroho, Anto Satriyo (2010). “Analysis of Machine learning Techniques Used in Behavior-Based Malware Detection” . *2010 Second International Conference on Advances in Computing, Control, and Telecommunication Technologies*. p. 201. ISBN 978-1-4244-8746-2. doi:10.1109/ACT.2010.33.
- [85] Siddiqui, Muazzam; Wang, Morgan C.; Lee, Joohan (2008). “A survey of data mining techniques for malware detection using file features” . *Proceedings of the 46th Annual Southeast Regional Conference on XX – ACM-SE 46*. p. 509. ISBN 9781605581057. doi:10.1145/1593105.1593239.

- [86] Deng, P.S.; Jau-Hwang Wang; Wen-Gong Shieh; Chih-Pin Yen; Cheng-Tan Tung (2003). "Intelligent automatic malicious code signatures extraction". *IEEE 37th Annual 2003 International Carnahan Conference on Security Technology, 2003. Proceedings*. p. 600. ISBN 0-7803-7882-2. doi:10.1109/CCST.2003.1297626.
- [87] Komashinskiy, Dmitriy; Kotenko, Igor (2010). "Malware Detection by Data Mining Techniques Based on Positionally Dependent Features". *2010 18th Euromicro Conference on Parallel, Distributed and Network-based Processing*. p. 617. ISBN 978-1-4244-5672-7. doi:10.1109/PDP.2010.30.
- [88] Schultz, M.G.; Eskin, E.; Zadok, F.; Stolfo, S.J. (2001). "Data mining methods for detection of new malicious executables". *Proceedings 2001 IEEE Symposium on Security and Privacy. S&P 2001*. p. 38. ISBN 0-7695-1046-9. doi:10.1109/SECPRI.2001.924286.
- [89] Ye, Yanfang; Wang, Dingding; Li, Tao; Ye, Dongyi (2007). "IMDS". *Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining – KDD '07*. p. 1043. ISBN 9781595936097. doi:10.1145/1281192.1281308.
- [90] Kolter, J. Zico; Maloof, Marcus A. (December 1, 2006). "Learning to Detect and Classify Malicious Executables in the Wild". *J*: 2721–2744.
- [91] Tabish, S. Momina; Shafiq, M. Zubair; Farooq, Muddassar (2009). "Malware detection using statistical analysis of byte-level file content". *Proceedings of the ACM SIGKDD Workshop on Cyber Security and Intelligence Informatics – CSI-KDD '09*. p. 23. ISBN 9781605586694. doi:10.1145/1599272.1599278.
- [92] Ye, Yanfang; Wang, Dingding; Li, Tao; Ye, Dongyi; Jiang, Qingshan (2008). "An intelligent PE-malware detection system based on association mining". *Journal in Computer Virology*. **4** (4): 323. doi:10.1007/s11416-008-0082-4.
- [93] Sami, Ashkan; Yadegari, Babak; Peiravian, Naser; Hashemi, Sattar; Hamze, Ali (2010). "Malware detection based on mining API calls". *Proceedings of the 2010 ACM Symposium on Applied Computing – SAC '10*. p. 1020. ISBN 9781605586397. doi:10.1145/1774088.1774303.
- [94] Shabtai, Asaf; Kanonov, Uri; Elovici, Yuval; Glezer, Chanan; Weiss, Yael (2011). ""Andromaly": A behavioral malware detection framework for android devices". *Journal of Intelligent Information Systems*. **38**: 161. doi:10.1007/s10844-010-0148-x.
- [95] Fox-Brewster, Thomas. "Netflix Is Dumping Anti-Virus, Presages Death Of An Industry". Forbes. Retrieved September 4, 2015.
- [96] Automatic Malware Signature Generation. (PDF) . Retrieved on January 3, 2017.
- [97] Szor 2005, pp. 252–288
- [98] "Generic detection". Kaspersky. Retrieved July 11, 2013.
- [99] Symantec Corporation (February 2009). "Trojan.Vundo". Archived from the original on April 9, 2009. Retrieved April 14, 2009.
- [100] Symantec Corporation (February 2007). "Trojan.Vundo.B". Archived from the original on April 27, 2009. Retrieved April 14, 2009.
- [101] "Antivirus Research and Detection Techniques". ExtremeTech. Archived from the original on February 27, 2009. Retrieved February 24, 2009.
- [102] "Terminology – F-Secure Labs".
- [103] Kaspersky Lab Technical Support Portal Archived February 14, 2011, at WebCite
- [104] Kelly, Michael (October 2006). "Buying Dangerously". Retrieved November 29, 2009.
- [105] Bitdefender (2009). "Automatic Renewal". Retrieved November 29, 2009.
- [106] Symantec (2014). "Norton Automatic Renewal Service FAQ". Retrieved April 9, 2014.
- [107] SpywareWarrior (2007). "Rogue/Suspect Anti-Spyware Products & Web Sites". Retrieved November 29, 2009.
- [108] Protalinski, Emil (November 11, 2008). "AVG incorrectly flags user32.dll in Windows XP SP2/SP3". Ars Technica. Retrieved February 24, 2011.
- [109] McAfee to compensate businesses for buggy update, retrieved December 2, 2010
- [110] Buggy McAfee update whacks Windows XP PCs, archived from the original on January 13, 2011, retrieved December 2, 2010

- [111] Tan, Aaron (May 24, 2007). “Flawed Symantec update cripples Chinese PCs” . *CNET Networks*. Retrieved April 5, 2009.
- [112] Harris, David (June 29, 2009). “January 2010 – Pegasus Mail v4.52 Release” . *Pegasus Mail*. Archived from the original on May 28, 2010. Retrieved May 21, 2010.
- [113] “McAfee DAT 5958 Update Issues” . April 21, 2010. Archived from the original on April 24, 2010. Retrieved April 22, 2010.
- [114] “Botched McAfee update shutting down corporate XP machines worldwide” . April 21, 2010. Archived from the original on April 22, 2010. Retrieved April 22, 2010.
- [115] Leyden, John (December 2, 2010). “Horror AVG update ballsup bricks Windows 7” . *The Register*. Retrieved December 2, 2010.
- [116] *MSE false positive detection forces Google to update Chrome*, retrieved October 3, 2011
- [117] *Sophos Antivirus Detects Itself as Malware, Deletes Key Binaries*, The Next Web, retrieved March 5, 2014
- [118] *Shh/Updater-B false positive by Sophos anti-virus products*, Sophos, retrieved March 5, 2014
- [119] “Plus! 98: How to Remove McAfee VirusScan” . Microsoft. January 2007. Archived from the original on April 8, 2010. Retrieved September 27, 2014.
- [120] Vamosi, Robert (May 28, 2009). “G-Data Internet Security 2010” . *PC World*. Retrieved February 24, 2011.
- [121] Higgins, Kelly Jackson (May 5, 2010). “New Microsoft Forefront Software Runs Five Antivirus Vendors' Engines” . *Darkreading*. Retrieved February 24, 2011.
- [122] “Steps to take before you install Windows XP Service Pack 3” . Microsoft. April 2009. Archived from the original on December 8, 2009. Retrieved November 29, 2009.
- [123] “Upgrading from Windows Vista to Windows 7” . Retrieved March 24, 2012. Mentioned within “Before you begin” .
- [124] “Upgrading to Microsoft Windows Vista recommended steps.” . Retrieved March 24, 2012.
- [125] “How to troubleshoot problems during installation when you upgrade from Windows 98 or Windows Millennium Edition to Windows XP” . May 7, 2007. Retrieved March 24, 2012. Mentioned within “General troubleshooting” .
- [126] “Troubleshooting” . Retrieved February 17, 2011.
- [127] “Spyware, Adware, and Viruses Interfering with Steam” . Retrieved April 11, 2013. Steam support page.
- [128] “Field Notice: FN – 63204 – Cisco Clean Access has Interoperability issue with Symantec Anti-virus – delays Agent start-up” .
- [129] Goodin, Dan (December 21, 2007). “Anti-virus protection gets worse” . *Channel Register*. Retrieved February 24, 2011.
- [130] “Zeus Tracker :: Home” .
- [131] Illett, Dan (July 13, 2007). “Hacking poses threats to business” . *Computer Weekly*. Retrieved November 15, 2009.
- [132] Espiner, Tom (June 30, 2008). “Trend Micro: Antivirus industry lied for 20 years” . *ZDNet*. Retrieved September 27, 2014.
- [133] AV Comparatives (December 2013). “Whole Product Dynamic “Real World” Production Test” (PDF). Archived (PDF) from the original on January 2, 2014. Retrieved January 2, 2014.
- [134] Kirk, Jeremy. “Guidelines released for antivirus software tests” .
- [135] Harley, David (2011). *AVIEN Malware Defense Guide for the Enterprise*. Elsevier. p. 487. ISBN 9780080558660.
- [136] Kotadia, Munir (July 2006). “Why popular antivirus apps 'do not work'" . Retrieved April 14, 2010.
- [137] The Canadian Press (April 2010). “Internet scam uses adult game to extort cash” . *CBC News*. Archived from the original on April 18, 2010. Retrieved April 17, 2010.
- [138] Exploit Code; Data Theft; Information Security; Privacy; Hackers; system, Security mandates aim to shore up shattered SSL; Reader, Adobe kills two actively exploited bugs in; stalker, Judge dismisses charges against accused Twitter. “Researchers up evilness ante with GPU-assisted malware” .

- [139] Iresh, Gina (April 10, 2010). “Review of Bitdefender Antivirus Security Software 2017 edition”. www.digitalgrog.com.au. Digital Grog. Retrieved November 20, 2016.
- [140] “Why F-PROT Antivirus fails to disinfect the virus on my computer?”. Retrieved August 20, 2015.
- [141] “Actions to be performed on infected objects” . Retrieved August 20, 2015.
- [142] “Cryptolocker Ransomware: What You Need To Know” . Retrieved March 28, 2014.
- [143] “How Anti-Virus Software Works” . Retrieved February 16, 2011.
- [144] “BT Home Hub Firmware Upgrade Procedure” . Archived from the original on May 12, 2011. Retrieved March 6, 2011.
- [145] “The 10 faces of computer malware” . July 17, 2009. Retrieved March 6, 2011.
- [146] “New BIOS Virus Withstands HDD Wipes” . March 27, 2009. Retrieved March 6, 2011.
- [147] “Phrack Inc. Persistent BIOS Infection” . June 1, 2009. Archived from the original on April 30, 2011. Retrieved March 6, 2011.
- [148] “Turning USB peripherals into BadUSB” . Retrieved October 11, 2014.
- [149] “Why the Security of USB Is Fundamentally Broken” . July 31, 2014. Retrieved October 11, 2014.
- [150] “How Antivirus Software Can Slow Down Your Computer” . Support.com Blog. Archived from the original on September 29, 2012. Retrieved July 26, 2010.
- [151] “Softpedia Exclusive Interview: Avira 10” . *Ionut Ilascu*. Softpedia. April 14, 2010. Retrieved September 11, 2011.
- [152] “Norton AntiVirus ignores malicious WMI instructions” . *Munir Kotadia*. CBS Interactive. October 21, 2004. Retrieved April 5, 2009.
- [153] “NSA and GCHQ attacked antivirus software so that they could spy on people, leaks indicate” . June 24, 2015. Retrieved October 30, 2016.
- [154] “Popular security software came under relentless NSA and GCHQ attacks” . *Andrew Fishman, Morgan Marquis-Boire*. June 22, 2015. Retrieved October 30, 2016.
- [155] Zeltser, Lenny (October 2010). “What Is Cloud Anti-Virus and How Does It Work?”. Archived from the original on October 10, 2010. Retrieved October 26, 2010.
- [156] Erickson, Jon (August 6, 2008). “Antivirus Software Heads for the Clouds” . *Information Week*. Retrieved February 24, 2010.
- [157] “Comodo Cloud Antivirus released” . wikipost.org. Retrieved May 30, 2016.
- [158] “Comodo Cloud Antivirus User Guideline PDF” (PDF). help.comodo.com. Retrieved May 30, 2016.
- [159] Krebs, Brian (March 9, 2007). “Online Anti-Virus Scans: A Free Second Opinion” . *Washington Post*. Retrieved February 24, 2011.
- [160] Naraine, Ryan (February 2, 2007). “Trend Micro ships free 'rootkit buster'” . *ZDNet*. Retrieved February 24, 2011.
- [161] Rubenking, Neil J. (March 26, 2010). “Avira AntiVir Personal 10” . *PC Magazine*. Retrieved February 24, 2011.
- [162] Rubenking, Neil J. (September 16, 2010). “PC Tools Spyware Doctor with AntiVirus 2011” . *PC Magazine*. Retrieved February 24, 2011.
- [163] Rubenking, Neil J. (October 4, 2010). “AVG Anti-Virus Free 2011” . *PC Magazine*. Retrieved February 24, 2011.
- [164] Rubenking, Neil J. (November 19, 2009). “PC Tools Internet Security 2010” . *PC Magazine*. Retrieved February 24, 2011.
- [165] Skinner, Carrie-Ann (March 25, 2010). “AVG Offers Free Emergency Boot CD” . *PC World*. Retrieved February 24, 2011.
- [166] “FBI estimates major companies lose \$12m annually from viruses” . January 30, 2007. Retrieved February 20, 2011.
- [167] Kaiser, Michael (April 17, 2009). “Small and Medium Size Businesses are Vulnerable” . *National Cyber Security Alliance*. Retrieved February 24, 2011.
- [168] Nearly 50% Women Don’t Use Anti-virus Software. Spamfighter.com (September 2, 2010). Retrieved on January 3, 2017.

21.9 Bibliography

- Szor, Peter (2005), *The Art of Computer Virus Research and Defense*, Addison-Wesley, ISBN 0-321-30454-3

21.10 External links

Chapter 22

Secure coding

Securing coding is the practice of developing computer software in a way that guards against the accidental introduction of security vulnerabilities. Defects, bugs and logic flaws are consistently the primary cause of commonly exploited software vulnerabilities.^{*[1]} Through the analysis of thousands of reported vulnerabilities, security professionals have discovered that most vulnerabilities stem from a relatively small number of common software programming errors. By identifying the insecure coding practices that lead to these errors and educating developers on secure alternatives, organizations can take proactive steps to help significantly reduce or eliminate vulnerabilities in software before deployment.

22.1 Buffer Overflow Prevention

Buffer overflows, a common software security vulnerability, happen when a process tries to store data beyond a fixed-length buffer. For example if you have 8 slots to store items in, and try to put 9 items you will end up with a problem. In computer memory the overflowed data may overwrite data in the next location which can result in a security vulnerability (stack smashing) or program termination (segmentation fault).^{*[1]}

An example of a C program prone to a buffer overflow is

```
int vulnerable_function(char * large_user_input) { char dst[SMALL]; strcpy(dst, large_user_input); }
```

If the user input is larger than the destination buffer, a buffer overflow will occur.

To fix this unsafe program, use strncpy to prevent a possible buffer overflow.

```
int secure_function(char * user_input) { char dst[BUF_SIZE]; //copy a maximum of BUF_SIZE bytes strncpy(dst, user_input,BUF_SIZE); }
```

Another secure alternative is to dynamically allocate memory on the heap using malloc.

```
char * secure_copy(char * src) { int len = strlen(src); char * dst = (char *) malloc(len + 1); if(dst != NULL){ strncpy(dst, src, len); //append null terminator dst[len] = '\0'; } return dst; }
```

In the above code snippet, the program attempts to copy the contents of *src* into *dst*, while also checking the return value of malloc to ensure that enough memory was able to be allocated for the destination buffer.

22.2 Format String Attack Prevention

A **Format String Attack** is when a malicious user supplies specific inputs that will eventually be entered as an argument to a function that performs formatting, such as printf(). The attack involves the adversary reading from or writing to the stack.

The C printf function writes output to stdout. If the parameter of the printf function is not properly formatted, several

security bugs can be introduced. Below is a program that is vulnerable to a format string attack.

```
int vulnerable_print(char * malicious_input) { printf(malicious_input); }
```

A malicious argument passed to the program could be “%s%s%s%s%s%s” , which can crash the program from improper memory reads.

22.3 Integer Overflow Prevention

Integer overflow occurs when an arithmetic operation results in an integer too large to be represented within the available space. A program which does not properly check for integer overflow introduces potential software bugs and exploits.

Below is a program which checks for overflow by confirming the sum is greater than or equal to x and y. If the sum did overflow, the sum would be less than x or less than y.

```
bool isValid(unsigned int x, unsigned int y) { unsigned int sum = x + y; return sum < MAX; }
```

If the sum of x and y are less than the defined MAX, the program will return true, otherwise isValid will return false. The problem with the code is it does not check for integer overflow on the addition operation. If the sum of x and y is greater than the available space to store the integer, the integer will overflow and “roll over” to a value less than MAX.

Below is a program which checks for overflow by confirming the sum is greater than or equal to x and y. If the sum did overflow, the sum would be less than x or less than y.

```
bool isValid(unsigned int x, unsigned int y) { unsigned int sum = x + y; return sum >= x && sum >= y && sum < MAX; }
```

22.4 See also

- Defensive programming
- Secure input and output handling
- Security bug

22.5 References

- [1] Viega, John; Gary McGraw (2001). *Building Secure Software: How to Avoid Security Problems the Right Way*. MAddison-Wesley Professional. p. 528. ISBN 978-0201721522.
- Taylor, Art; Brian Buege; Randy Layman (2006). *Hacking Exposed J2EE & Java*. McGraw-Hill Primis. p. 426. ISBN 0-390-59975-1.

22.6 External links

Chapter 23

Secure by design

Secure by design, in software engineering, means that the software has been designed from the ground up to be **secure**. Malicious practices are taken for granted and care is taken to minimize impact when a security vulnerability is discovered or on invalid user input.

Generally, designs that work well do not rely on being secret. It is not mandatory, but proper security usually means that everyone is allowed to know and understand the design *because it is secure*. This has the advantage that many people are looking at the code, and this improves the odds that any flaws will be found sooner ([Linus' law](#)). Of course, attackers can also obtain the code, which makes it easier for them to find vulnerabilities as well.

Also, it is important that everything works with the least amount of privileges possible (principle of least privilege). For example, a Web server that runs as the administrative user (root or admin) can have the privilege to remove files and users that do not belong to itself. Thus, a flaw in that program could put the entire system at risk. On the other hand, a Web server that runs inside an isolated environment and only has the privileges for required network and filesystem functions, cannot compromise the system it runs on unless the security around it is in itself also flawed.

23.1 Security by design in practice

Many things, especially input, should be distrusted by a secure design. A fault-tolerant program could even distrust its own internals.

Two examples of insecure design are allowing buffer overflows and format string vulnerabilities. The following C program demonstrates these flaws:

```
#include <stdio.h>
int main() {
    char a_chBuffer[100];
    printf("What is your name?\n");
    gets(a_chBuffer);
    printf("Hello, ");
    printf(a_chBuffer);
    printf("\n");
    return 0;
}
```

Because the `gets` function in the C standard library does not stop writing bytes into buffer until it reads a newline character or `EOF`, typing more than 99 characters at the prompt constitutes a buffer overflow. Allocating 100 characters for buffer with the assumption that almost any given name from a user is no longer than 99 characters doesn't prevent the user from actually *typing* more than 99 characters. This can lead to arbitrary machine code execution.

The second flaw is that the program tries to print its input by passing it directly to the `printf` function. This function prints out its first argument, replacing conversion specifications (such as "%s", "%d", et cetera) sequentially with other arguments from its call stack as needed. Thus, if a malicious user entered "%d" instead of his name, the program would attempt to print out a non-existent integer value, and undefined behavior would occur.

A related mistake in Web programming is for an online script not to validate its parameters. For example, consider a script that fetches an article by taking a filename, which is then read by the script and parsed. Such a script might use the following hypothetical URL to retrieve an article about dog food:

`http://www.example.net/cgi-bin/article.sh?name=dogfood.html`

If the script has no input checking, instead trusting that the filename is always valid, a malicious user could forge a URL to retrieve configuration files from the webserver:

`http://www.example.net/cgi-bin/article.sh?name=../../../../etc/passwd`

Depending on the script, this may expose the `/etc/passwd` file, which on Unix-like systems contains (among others) user IDs, their login names, home directory paths and shells. (See SQL injection for a similar attack.)

23.2 Server/client architectures

In server/client architectures, the program at the other side may not be an authorised client and the client's server may not be an authorised server. Even when they are, a man-in-the-middle attack could compromise communications.

Often the easiest way to break the security of a client/server system is not to go head on to the security mechanisms, but instead to go around them. A man in the middle attack is a simple example of this, because you can use it to collect details to impersonate a user. Which is why it is important to consider encryption, hashing, and other security mechanisms in your design to ensure that information collected from a potential attacker won't allow access.

Another key feature to client-server security design is good coding practices. For example, following a known software design structure such as client and broker can help in designing a well-built structure with a solid foundation. Furthermore, if the software is to be modified in the future, it is even more important that it follows a logical foundation of separation between the client and server. This is because if a programmer comes in and cannot clearly understand the dynamics of the program they may end up adding or changing something that can add a security flaw. Even with the best design this is always a possibility, but the better standardized the design the less chance there is of this occurring.

23.3 See also

- Computer security
- Cyber security standards
- Hardening
- Multiple Independent Levels of Security
- Secure by default
- Security through obscurity
- Software Security Assurance

23.4 External links

- Secure Programming for Linux and Unix HOWTO
- Secure UNIX Programming FAQ
- Top 10 Secure Coding Practices

Chapter 24

Security-focused operating system

This is a list of [operating systems](#) with a sharp security focus. Here, “security-focused” means that the project is devoted to increasing the security as a major goal. As such, something may be secure without being “security-focused.” For example, almost all of the operating systems mentioned here are faced with security bug fixes in their lifetime; however, they all strive consistently to approach all generic security flaws inherent in their design with new ideas in an attempt to create a secure computing environment. Security-focused does not mean [security-evaluated](#) operating system, which refers to operating systems that have achieved certification from an external security-auditing organization. An operating system that provides sufficient support for multilevel security and evidence of correctness to meet a particular set of government requirements is called a “[trusted operating system](#)”.

The list is alphabetical and does not imply a ranking.

24.1 Linux

The [Linux kernel](#) provides among other security features, the [Linux Security Module \(LSM\)](#), officially integrated with the mainline Linux kernel since 2003. However, there have been specialized distributions and projects that attempt to make Linux more secure in general or for particular scenarios.

24.1.1 openSUSE

openSUSE uses a stateful network packet filter (also known as *firewall*) and includes a feature called AppArmor which monitors running programs for unusual behavior). The YaST system configuration module is included to provide configuration and reporting for the firewall and other system components.

24.1.2 Debian

The “Securing Debian Manual” *[1] contains information for [Debian](#) administrators. Debian includes support for SELinux*[2] since version 5.0, as well as [AppArmor](#) and [Tomoyo](#). See also [Debian Security information and policy](#).

Kali Linux

[Kali Linux](#) is a Debian-derived Linux distribution designed for digital forensics and penetration testing, formerly known as Backtrack.

Tails

Tails is a security-focused Debian-based Linux distribution aimed at preserving privacy and anonymity.*[3]

Parrot Security OS

Parrot Security OS is a Cloud oriented GNU/Linux distribution based on Debian and designed to perform security and penetration tests, do forensic analysis, or act in anonymity. It uses the MATE Desktop Environment, Linux Kernel 4.6 or higher and it is available as a live lightweight installable ISO image for 32-bit, 64-bit and ARM processors with forensic options at boot, optimizations for programmers, and new custom pentesting tools.

24.1.3 Fedora

Fedora is a free, Red Hat-sponsored community-developed Linux distribution. Fedora is a mainstream distribution that makes significant efforts to improve security.*[4] As a consequence, it has a fully integrated SELinux MAC and fine-grained executable memory permission system (Exec Shield) and all binaries compiled with GCC's standard stack-smashing protection, as well as focusing on getting security updates into the system in a timely manner.

Qubes OS

Qubes OS is a desktop operating system based around the Xen hypervisor that allows grouping programs into a number of isolated sandboxes (virtual machines) to provide security. Windows for programs running within these sandboxes (“security domains”) can be color coded for easy recognition. The security domains are configurable, they can be transient (changes to the file system will not be preserved), and their network connection can be routed through special virtual machines (for example one that only provides Tor networking). The operating system provides secure mechanisms for copy and paste and for copying files between the security domains.*[5]

Red Hat Enterprise Linux

Red Hat Enterprise Linux offers the same security benefits as Fedora with the additional support of back-porting security fixes to the released versions of the packages (particularly the kernel) so the sys-admin does not have to perform a significant (and risky) upgrade to get a security fix.

24.1.4 Arch and Gentoo related

Hardened Gentoo

Hardened Gentoo is a sub-project of the Gentoo Linux project. Hardened Gentoo offers a ProPolice protected and position-independent executable base using exactly the same package tree as Gentoo. Executable space protection in Hardened Gentoo is handled by PaX. The Hardened Gentoo project is an extremely modular project, and also provides subprojects to integrate other intrusion-detection and mandatory access control systems into Gentoo. All of these can be optionally installed in any combination, with or without PaX and a ProPolice base.

Pentoo Project

Pentoo Penetration Testing Overlay and Livecd is a live CD and Live USB designed for penetration testing and security assessment. Based on Gentoo Linux, Pentoo is provided both as 32-bit and 64-bit installable live cd. Pentoo also is available as an overlay for an existing Gentoo installation. It features packet injection patched wifi drivers, GPGPU cracking software, and lots of tools for penetration testing and security assessment. The Pentoo kernel includes grsecurity and PAX hardening and extra patches – with binaries compiled from a hardened toolchain with the latest nightly versions of some tools available.

Tin Hat

Tin Hat Linux is derived from Hardened Gentoo Linux. It aims to provide a very secure, stable, and fast desktop environment that lives purely in RAM.*[6]

24.1.5 Mobile

CopperheadOS

CopperheadOS is a hardened FOSS operating system based on the Android mobile platform, which uses an unofficial port of PaX.*[7]*[8]*[9]

Replicant

Replicant is a FOSS operating system based on the Android mobile platform, which aims to replace all proprietary Android components with their free software counterparts. It is available for several smartphones and tablet computers.*[10]*[11]*[12]*[13]

In March 2014, the Replicant project announced the discovery of a backdoor present in a wide range of Samsung Galaxy products that allows the baseband processor to read and write the device's storage,*[14]*[15] sometimes with normal user privileges and sometimes as the root user, depending on device model.*[16] It is not generally known whether Samsung's proprietary firmware for the radio chip can be remotely instructed to use these access features and the intentions of creating such a backdoor.

24.1.6 Independent

Alpine Linux

Alpine Linux is a lightweight musl and BusyBox-based distribution. It uses PaX and grsecurity patches in the default kernel and compiles all packages with stack-smashing protection. Version 3.0 was released June 4, 2014.

Annvix

Annvix was originally forked from Mandriva to provide a security-focused server distribution that employs ProPolice protection, hardened configuration, and a small footprint. There were plans to include full support for the RSBAC mandatory access control system. However, Annvix is dormant, with the last version being released on December 30, 2007.

EnGarde Secure Linux

EnGarde Secure Linux is a secure platform designed for servers. It has had a browser-based tool for MAC using SELinux since 2003. Additionally, it can be accompanied with Web, DNS, and email enterprise applications, specifically focusing on security without any unnecessary software. The community platform of EnGarde Secure Linux is the bleeding-edge version freely available for download.

Immunix

Immunix was a commercial distribution of Linux focused heavily on security. They supplied many systems of their own making, including StackGuard; cryptographic signing of executables; race condition patches; and format string exploit guarding code. Immunix traditionally releases older versions of their distribution free for non-commercial use. The Immunix distribution itself is licensed under two licenses: The Immunix commercial and non-commercial licenses. Many tools within are GPL, however; as is the kernel.

Openwall Project

Solar Designer's Openwall Project (Owl) was the first distribution to have a non-executable userspace stack, /tmp race condition protection, and access control restrictions to /proc data, by way of a kernel patch. It also features a per-user tmp directory via the pam_mktemp PAM module, and supports Blowfish password encryption.

Subgraph OS

Subgraph OS is a Linux-based operating system designed to be resistant to surveillance and interference by sophisticated adversaries over the Internet. Subgraph OS is designed with features which aim to reduce the attack surface of the operating system, and increase the difficulty required to carry out certain classes of attack. This is accomplished through system hardening and a proactive, ongoing focus on security and attack resistance. Subgraph OS also places emphasis on ensuring the integrity of installed software packages through deterministic compilation.

Subgraph OS features a kernel hardened with the [Grsecurity](#) and [PaX](#) patchset, [Linux namespaces](#), and [Xpra](#) for application containment, mandatory file system encryption using [LUKS](#), resistance to cold boot attacks, and is configured by default to isolate network communications for installed applications to independent circuits on the [Tor anonymity network](#).

24.2 BSD

BSD is a family of [Unix](#) variants derived from a code base originating at the [University of California, Berkeley](#). All derived BSD operating systems are released under the terms of a [BSD-style license](#). There are several BSD variants, with only one being heavily focused on security.

24.2.1 Anonym.OS

Anonym.OS was a [Live CD](#) operating system based on OpenBSD 3.8 with strong encryption and anonymization tools. The goal of the project was to provide secure, anonymous [web browsing](#) access to everyday users.*[\[17\]](#) The project was discontinued after the release of Beta 4 (2006).

24.2.2 OpenBSD

See also: [OpenBSD security features](#)

OpenBSD is an open source BSD operating system that is known to be concerned heavily with security. The project has completed rigorous manual reviews of the code and addressed issues most systems have not.*[\[18\]](#) OpenBSD also supplies an executable space protection scheme known as [W^X](#) (memory is writeable [xor](#) executable), as well as a [ProPolice](#) compiled executable base. OpenBSD became the first mainstream operating system to support partial ASLR and to activate it by default; ASLR support was completed in 2008 when it added support for position-independent executable (PIE) binaries.

24.2.3 TrustedBSD

TrustedBSD is a sub-project of [FreeBSD](#) designed to add trusted operating system extensions, targeting the [Common Criteria for Information Technology Security Evaluation](#) (see also [Orange Book](#)). Its main focuses are working on access control lists, event auditing, extended attributes, mandatory access controls, and fine-grained capabilities. Since access control lists are known to be confronted with the confused deputy problem, capabilities are a different way to avoid this issue. As part of the TrustedBSD project, there is also a port of NSA's FLASK/TE implementation to run on FreeBSD. Many of these trusted extensions have been integrated into the main FreeBSD branch starting at 5.x.

24.2.4 HardenedBSD

HardenedBSD is a fork of FreeBSD by Oliver Pinter and Shawn Webb which focusses on exploit mitigation, using techniques such as ASLR, founded in 2014.*[\[19\]](#)

24.3 Solaris

Solaris is a Unix variant created by Sun Microsystems. Solaris itself is not inherently security-focused. The major portion of the Solaris source code has been released via the OpenSolaris project, mostly under the Common Development and Distribution License. Enhancements to OpenSolaris, both security related and others, are backported to the official Solaris when Sun certifies their quality.

24.3.1 Trusted Solaris

Trusted Solaris is a security-focused version of the Solaris Unix operating system. Aimed primarily at the government computing sector, Trusted Solaris adds detailed auditing of all tasks, pluggable authentication, mandatory access control, additional physical authentication devices, and fine-grained access control. Trusted Solaris is Common Criteria certified. (See [and](#)) The most recent version, Trusted Solaris 8 (released 2000), received the EAL4 certification level augmented by a number of protection profiles. Telnet was vulnerable to buffer overflow exploits until patched in April 2001.*[20]

24.3.2 Solaris 10 and trusted functionality

Trusted Solaris functionality has now been added to the mainstream version of Solaris. In the 11/06 update to Solaris 10, the *Solaris Trusted Extensions* feature adds mandatory access control and labelled security. Introduced in the same update, the *Secure by Default Networking* feature implements less services on by default compared to most previous releases that had most services enabled. RBAC, found in both mainstream Solaris and Trusted Solaris, dramatically lessens the need for using root directly by providing a way for fine grained control over various administrative tasks.

24.4 Microsoft Windows Server

Starting with Windows Server 2008, the server can run in “core” mode. In this mode of operation, the traditional graphical user interface is done away with, and replaced with a Windows command prompt. Roles and software for the server are then installed individually. This serves not only to lessen the strain on system resources produced by unwanted or unneeded applications, but also to reduce the overall “attack surface” of the operating system by virtue of excluding programs that may contain vulnerabilities.*[21]

24.5 Object-capability systems

These operating systems are all engineered around a different paradigm of security, **object-capabilities**, where instead of having the system deciding if an access request should be granted (usually through one or several access control lists), the bundling of authority and designation makes it impossible to request anything not legitimate.

- CapROS
- EROS
- Fiasco.OC
- KeyKOS
- seL4

24.6 See also

- Capabilities and access control lists
- Comparison of operating systems

- Damn Vulnerable Linux
- IX (operating system)
- OpenBSM
- Operating system (section Security)
- Security engineering
- Security-evaluated operating system
- Trusted operating system

24.7 References

- [1] “Securing Debian Manual” . *debian.org*. Retrieved 19 April 2015.
- [2] “SELinux” . *debian.org*. Retrieved 19 April 2015.
- [3] Vervloesem, Koen (2011-04-27). “The Amnesic Incognito Live System: A live CD for anonymity [LWN.net]”. *lwn.net*. Retrieved 2017-06-14.
- [4] “SELinux: бронежилет для корпоративного пингвина” [SELinux: bullet-proof vest for corporate penguin] (in Russian). 6 September 2011. Retrieved 26 October 2011.
- [5] “Redirecting...” . *qubes-os.org*. Retrieved 30 April 2017.
- [6] “Tin Hat” . D'Youville College.
- [7] Porup, J.M. (9 August 2016). “Copperhead OS: The startup that wants to solve Android's woeful security” . *arsTechnica.co.uk*. Ars Technica UK.
- [8] Corbet, Jonathan (17 February 2016). “CopperheadOS: Securing the Android” . *lwn.net*.
- [9] Linder, Brad (29 March 2016). “F-Droid, Copperhead, Guardian Project partner to create a security-focused, Android-based ecosystem” . *liliputing.com*.
- [10] “Overview - Replicant” . Redmine.replicant.us. Retrieved 2013-09-30.
- [11] Paul Kocialkowski (February 4, 2012). “WikiStart – Replicant” . Redmine.replicant.us. Retrieved 2013-09-30.
- [12] “Android and Users' Freedom - GNU Project - Free Software Foundation” . Gnu.org. Retrieved 2013-09-30.
- [13] “About” . Replicant project. Retrieved 2013-09-30.
- [14] Don Reisinger (13 March 2014). “Samsung Galaxy devices may have backdoor to user data, developer says” . CNET. Retrieved 25 April 2014.
- [15] Michael Larabel (12 March 2014). “Replicant Developers Find Backdoor In Android Samsung Galaxy Devices” . *Phoronix*. Retrieved 25 April 2014.
- [16] Paul Kocialkowski. “Samsung Galaxy Back-door” . *Replicant Wiki*. Archived from the original on 6 April 2014. Retrieved 25 April 2014.
- [17] Quinn Norton (January 14, 2006). “Anonytity on a Disc” . *Wired.com*. Retrieved November 6, 2011.
- [18] McIntire, Tim (8 August 2006). “Take a closer look at OpenBSD” . IBM. Archived from the original on January 27, 2007. Retrieved 19 February 2015.
- [19] Larabel, Michael (4 September 2014). “HardenedBSD: The Latest BSD Project That Aims To Boost Security” . Phoronix. Retrieved 4 July 2017.
- [20] “Sun Patch: Trusted Solaris 8 4/01: in.telnet patch” . 4 October 2002. Retrieved 13 August 2012. 4734086 in.telnetd vulnerable to buffer overflow ?? (Solaris bug 4483514)
- [21] “What is Server Core?”. *Microsoft TechNet*. Microsoft Corporation. Retrieved 17 October 2013.

24.8 External links

- HD Scania homepage, the author and only maintainer of *Nelson*
- Nelson: openSuSE and security based Cinnimalistic OS clan
- AIX
- OpenBSD
- Hardened Linux
- Qubes

Chapter 25

Authentication

For other uses of the terms “authentic” and “authenticity”, see [Authenticity](#).

Authentication (from Greek: αὐθεντικός *authentikos*, “real, genuine”, from αὐθέντης *authentes*, “author”) is the act of confirming the truth of an attribute of a single piece of data claimed true by an entity. In contrast with identification, which refers to the act of stating or otherwise indicating a claim purportedly attesting to a person or thing's identity, authentication is the process of actually confirming that identity. It might involve confirming the identity of a person by validating their [identity documents](#), verifying the authenticity of a website with a [digital certificate](#),^{* [1]} determining the age of an artifact by [carbon dating](#), or ensuring that a product is what its packaging and labeling claim to be. In other words, authentication often involves verifying the validity of at least one form of identification.

25.1 Methods

Main article: [Provenance](#)

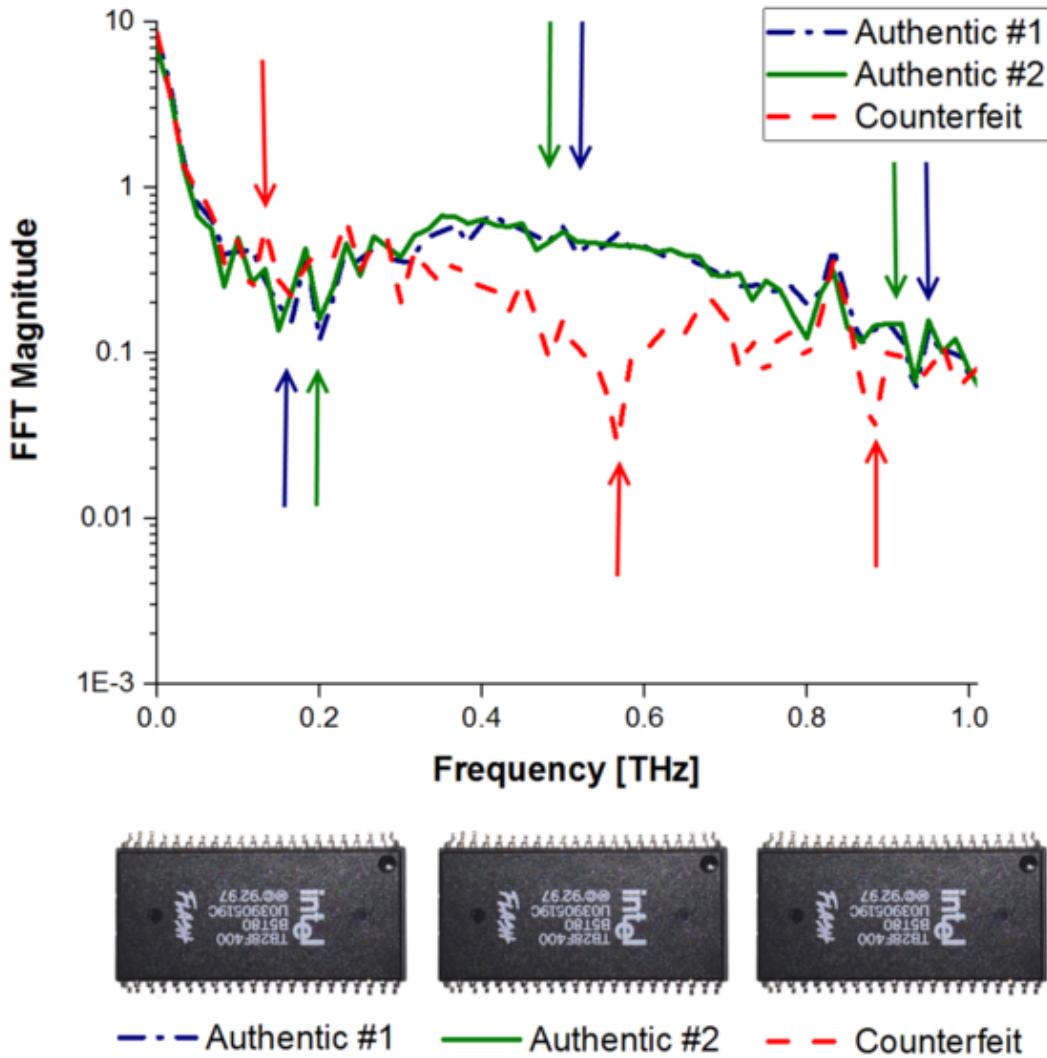
Authentication is relevant to multiple fields. In art, antiques and [anthropology](#), a common problem is verifying that a given artifact was produced by a certain person or in a certain place or period of history. In computer science, verifying a person's identity is often required to allow access to confidential data or systems.

Authentication can be considered to be of three types:

The **first type** of authentication is accepting proof of identity given by a credible person who has first-hand evidence that the identity is genuine. When authentication is required of art or physical objects, this proof could be a friend, family member or colleague attesting to the item's provenance, perhaps by having witnessed the item in its creator's possession. With autographed sports memorabilia, this could involve someone attesting that they witnessed the object being signed. A vendor selling branded items implies authenticity, while he or she may not have evidence that every step in the supply chain was authenticated. Centralized authority-based trust relationships back most secure internet communication through known public certificate authorities; decentralized peer-based trust, also known as a [web of trust](#), is used for personal services such as email or files ([pretty good privacy](#), [GNU Privacy Guard](#)) and trust is established by known individuals signing each other's [cryptographic key](#) at [Key signing parties](#), for instance.

The **second type** of authentication is comparing the attributes of the object itself to what is known about objects of that origin. For example, an art expert might look for similarities in the style of painting, check the location and form of a signature, or compare the object to an old photograph. An [archaeologist](#), on the other hand, might use [carbon dating](#) to verify the age of an artifact, do a chemical and spectroscopic analysis of the materials used, or compare the style of construction or decoration to other artifacts of similar origin. The physics of sound and light, and comparison with a known physical environment, can be used to examine the authenticity of audio recordings, photographs, or videos. Documents can be verified as being created on ink or paper readily available at the time of the item's implied creation.

Attribute comparison may be vulnerable to forgery. In general, it relies on the facts that creating a forgery indistinguishable from a genuine artifact requires expert knowledge, that mistakes are easily made, and that the amount of



Authentication using spectroscopic material analysis: The differences in constituent materials reveals the counterfeit item. [2]*

effort required to do so is considerably greater than the amount of profit that can be gained from the forgery.

In art and antiques, certificates are of great importance for authenticating an object of interest and value. Certificates can, however, also be forged, and the authentication of these poses a problem. For instance, the son of [Han van Meegeren](#), the well-known art-forgery, forged the work of his father and provided a certificate for its provenance as well; see the article [Jacques van Meegeren](#).

Criminal and civil penalties for [fraud](#), [forgery](#), and [counterfeiting](#) can reduce the incentive for falsification, depending on the risk of getting caught.

[Currency](#) and other financial instruments commonly use this second type of authentication method. Bills, coins, and [cheques](#) incorporate hard-to-duplicate physical features, such as fine printing or engraving, distinctive feel, watermarks, and [holographic imagery](#), which are easy for trained receivers to verify.

The **third type** of authentication relies on documentation or other external affirmations. In criminal courts, the rules of evidence often require establishing the [chain of custody](#) of evidence presented. This can be accomplished through a written evidence log, or by testimony from the police detectives and forensics staff that handled it. Some antiques are accompanied by certificates attesting to their authenticity. Signed sports memorabilia is usually accompanied by a certificate of authenticity. These external records have their own problems of forgery and [perjury](#), and are also vulnerable to being separated from the artifact and lost.

In computer science, a user can be given [access to secure systems](#) based on user credentials that imply authenticity. A network administrator can give a user a password, or provide the user with a key card or other access device to allow system access. In this case, authenticity is implied but not guaranteed.

Consumer goods such as pharmaceuticals, perfume, fashion clothing can use all three forms of authentication to prevent counterfeit goods from taking advantage of a popular brand's reputation (damaging the brand owner's sales and reputation). As mentioned above, having an item for sale in a reputable store implicitly attests to it being genuine, the first type of authentication. The second type of authentication might involve comparing the quality and craftsmanship of an item, such as an expensive handbag, to genuine articles. The third type of authentication could be the presence of a trademark on the item, which is a legally protected marking, or any other identifying feature which aids consumers in the identification of genuine brand-name goods. With software, companies have taken great steps to protect from counterfeiters, including adding holograms, security rings, security threads and color shifting ink.* [3]

25.2 Factors and identity

The ways in which someone may be authenticated fall into three categories, based on what are known as the factors of authentication: something the user *knows*, something the user *has*, and something the user *is*. Each **authentication factor** covers a range of elements used to authenticate or verify a person's identity prior to being granted access, approving a transaction request, signing a document or other work product, granting authority to others, and establishing a chain of authority.

Security research has determined that for a positive authentication, elements from at least two, and preferably all three, factors should be verified.* [4] The three factors (classes) and some of elements of each factor are:

- the **knowledge factors**: Something the user **knows** (e.g., a password, partial password, pass phrase, or personal identification number (PIN), challenge response (the user must answer a question, or pattern), Security question
- the **ownership factors**: Something the user **has** (e.g., wrist band, ID card, security token, cell phone with built-in hardware token, software token, or cell phone holding a software token)
- the **inherence factors**: Something the user **is** or **does** (e.g., fingerprint, retinal pattern, DNA sequence (there are assorted definitions of what is sufficient), signature, face, voice, unique bio-electric signals, or other biometric identifier).

25.2.1 Types

The most frequent types of authentication available in use for authenticating online users differ in the level of security provided by combining factors from the one or more of the three categories of factors for authentication:

Single-factor authentication

As the weakest level of authentication, only a single component from one of the three categories of factors is used to authenticate an individual's identity. The use of only one factor does not offer much protection from misuse or malicious intrusion. This type of authentication is not recommended for financial or personally relevant transactions that warrant a higher level of security.* [1]

Two-factor authentication

Main article: Two-factor authentication

When elements representing two factors are required for authentication, the term *two-factor authentication* is applied —e.g. a bankcard (something the user **has**) and a PIN (something the user **knows**). Business networks may require users to provide a password (knowledge factor) and a pseudorandom number from a **security token** (ownership factor). Access to a very-high-security system might require a **mantrap** screening of height, weight, facial, and fingerprint checks (several inherence factor elements) plus a PIN and a day code (knowledge factor elements), but this is still a two-factor authentication.



This is a picture of the front (top) and back (bottom) of an ID Card.

Multi-factor authentication

Instead of using two factors as used in 2FA, multiple authentication factors are used to enhance security of a transaction in comparison to the 2FA authentication process. [1]

Strong authentication

Main article: strong authentication

The U.S. government's National Information Assurance Glossary defines **strong authentication** as

layered authentication approach relying on two or more authenticators to establish the identity of an originator or receiver of information.

*[5] The European Central Bank (ECB) has defined *strong authentication* as “a procedure based on two or more of the three authentication factors”. The factors that are used must be mutually independent and at least one factor must be “non-reusable and non-replicable”, except in the case of an inherence factor and must also be incapable of being stolen off the Internet. In the European, as well as in the US-American understanding, strong authentication is very similar to multi-factor authentication or 2FA, but exceeding those with more rigorous requirements.*[1]*[6]

The Fast IDentity Online (FIDO) Alliance has been striving to establish technical specifications for strong authentication.*[7]

Continuous Authentication

Conventional computer systems authenticate users only at the initial log-in session, which can be the cause of a critical security flaw. To resolve this problem, systems need continuous user authentication methods that continuously monitor and authenticate users based on some biometric trait(s). A study used behavioural biometrics based in writing styles as a continuous authentication method.*[8]

25.3 Digital authentication



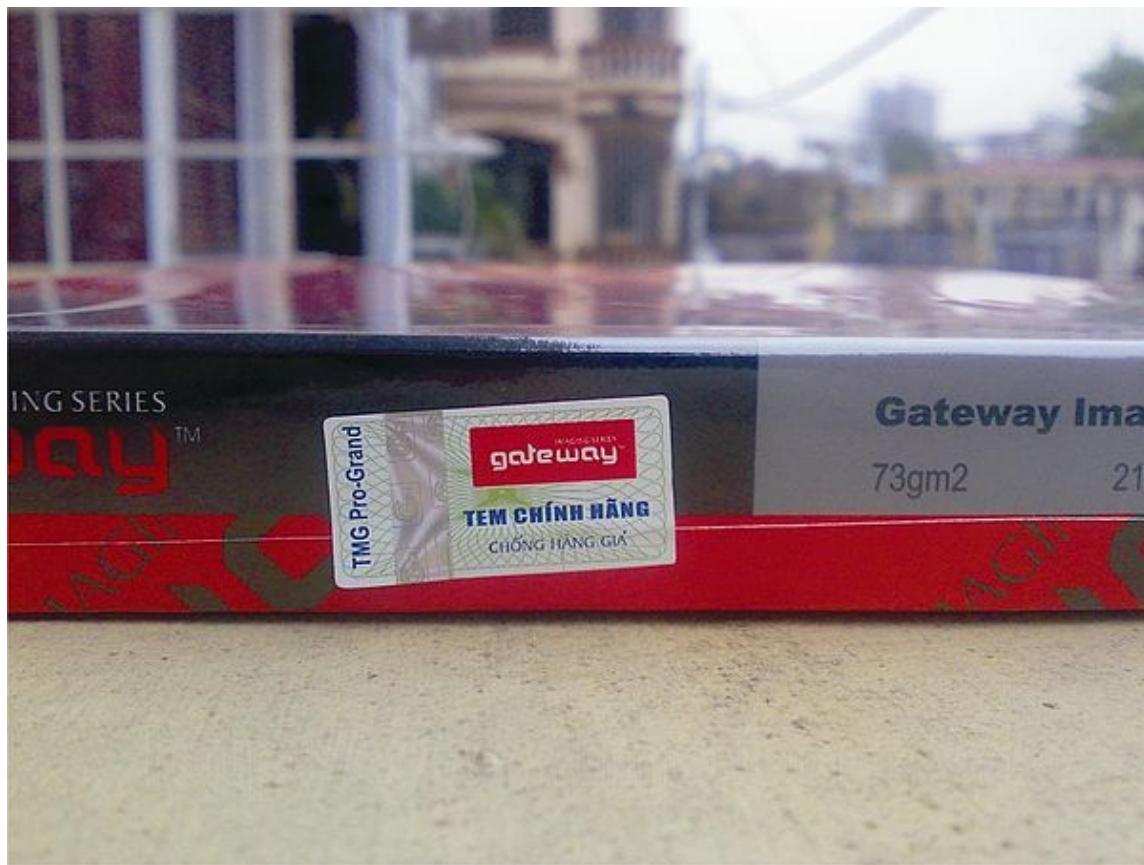
A High Level overview concerning identities and authenticity.

The authentication of information can pose special problems with electronic communication, such as vulnerability to man-in-the-middle attacks, whereby a third party taps into the communication stream, and poses as each of the two other communicating parties, in order to intercept information from each. Extra identity factors can be required to authenticate each party's identity.

The term *digital authentication* refers to a group of processes where the confidence for user identities is established and presented via electronic methods to an information system. It is also referred to as e-authentication. The digital authentication process creates technical challenges because of the need to authenticate individuals or entities remotely over a network. The American National Institute of Standards and Technology (NIST) has created a generic model for digital authentication that describes the processes that are used to accomplish secure authentication:

1. *Enrollment* – an individual applies to a credential service provider (CSP) to initiate the enrollment process. After successfully proving the applicant’s identity, the CSP allows the applicant to become a subscriber.
2. *Authentication* – After becoming a subscriber, the user receives an authenticator e.g., a token and credentials, such as a user name. He or she is then permitted to perform online transactions within an authenticated session with a relying party, where they must provide proof that he or she possesses one or more authenticators.
3. *Life-cycle maintenance* – the CSP is charged with the task of maintaining the user’s credential of the course of its lifetime, while the subscriber is responsible for maintaining his or her authenticator(s).^{*[1]*[9]}

25.4 Product authentication



A security hologram label on an electronics box for authentication

Counterfeit products are often offered to consumers as being authentic. Counterfeit consumer goods such as electronics, music, apparel, and counterfeit medications have been sold as being legitimate. Efforts to control the supply chain and educate consumers help ensure that authentic products are sold and used. Even security printing on packages, labels, and nameplates, however, is subject to counterfeiting.

A secure key storage device can be used for authentication in consumer electronics, network authentication, license management, supply chain management, etc. Generally the device to be authenticated needs some sort of wireless or wired digital connection to either a host system or a network. Nonetheless, the component being authenticated need not be electronic in nature as an authentication chip can be mechanically attached and read through a connector to the host e.g. an authenticated ink tank for use with a printer. For products and services that these secure coprocessors

can be applied to, they can offer a solution that can be much more difficult to counterfeit than most other options while at the same time being more easily verified.

25.4.1 Packaging

Packaging and labeling can be engineered to help reduce the risks of counterfeit consumer goods or the theft and resale of products.*[10]*[11] Some package constructions are more difficult to copy and some have pilfer-indicating seals. Counterfeit goods, unauthorized sales (diversion), material substitution and tampering can all be reduced with these anti-counterfeiting technologies. Packages may include authentication seals and use security printing to help indicate that the package and contents are not counterfeit; these too are subject to counterfeiting. Packages also can include anti-theft devices, such as dye-packs, **RFID** tags, or electronic article surveillance* [12] tags that can be activated or detected by devices at exit points and require specialized tools to deactivate. Anti-counterfeiting technologies that can be used with packaging include:

- Taggant fingerprinting – uniquely coded microscopic materials that are verified from a database
- Encrypted micro-particles – unpredictably placed markings (numbers, layers and colors) not visible to the human eye
- Holograms – graphics printed on seals, patches, foils or labels and used at point of sale for visual verification
- Micro-printing – second-line authentication often used on currencies
- Serialized barcodes
- UV printing – marks only visible under UV light
- Track and trace systems – use codes to link products to database tracking system
- Water indicators – become visible when contacted with water
- DNA tracking – genes embedded onto labels that can be traced
- Color-shifting ink or film – visible marks that switch colors or texture when tilted
- Tamper evident seals and tapes – destructible or graphically verifiable at point of sale
- 2d barcodes – data codes that can be tracked
- **RFID** chips
- **NFC** chips

25.5 Information content

Literary forgery can involve imitating the style of a famous author. If an original manuscript, typewritten text, or recording is available, then the medium itself (or its packaging – anything from a box to e-mail headers) can help prove or disprove the authenticity of the document. However, text, audio, and video can be copied into new media, possibly leaving only the informational content itself to use in authentication. Various systems have been invented to allow authors to provide a means for readers to reliably authenticate that a given message originated from or was relayed by them. These involve authentication factors like:

- A difficult-to-reproduce physical artifact, such as a seal, signature, watermark, special stationery, or fingerprint.
- A shared secret, such as a passphrase, in the content of the message.
- An electronic signature; public-key infrastructure is often used to cryptographically guarantee that a message has been signed by the holder of a particular private key.

The opposite problem is detection of plagiarism, where information from a different author is passed off as a person's own work. A common technique for proving plagiarism is the discovery of another copy of the same or very similar text, which has different attribution. In some cases, excessively high quality or a style mismatch may raise suspicion of plagiarism.

25.5.1 Factual verification

Determining the truth or factual accuracy of information in a message is generally considered a separate problem from authentication. A wide range of techniques, from detective work, to fact checking in journalism, to scientific experiment might be employed.

25.5.2 Video authentication

It is sometimes necessary to authenticate the veracity of video recordings used as evidence in judicial proceedings. Proper chain-of-custody records and secure storage facilities can help ensure the admissibility of digital or analog recordings by a court.

25.5.3 Literacy and literature authentication

In literacy, authentication is a readers' process of questioning the veracity of an aspect of literature and then verifying those questions via research. The fundamental question for authentication of literature is – Does one believe it? Related to that, an authentication project is therefore a reading and writing activity which students documents the relevant research process (*[13]). It builds students' critical literacy. The documentation materials for literature go beyond narrative texts and likely include informational texts, primary sources, and multimedia. The process typically involves both internet and hands-on library research. When authenticating historical fiction in particular, readers consider the extent that the major historical events, as well as the culture portrayed (e.g., the language, clothing, food, gender roles), are believable for the period.*[14]

25.6 History and state-of-the-art



NSA KAL-55B Tactical Authentication System used by the U.S. military during the Vietnam War – National Cryptologic Museum

Historically, fingerprints have been used as the most authoritative method of authentication, but court cases in the US and elsewhere have raised fundamental doubts about fingerprint reliability. Outside of the legal system as well, fingerprints have been shown to be easily spoofable, with British Telecom's top computer-security official noting that "few" fingerprint readers have not already been tricked by one spoof or another.*[15] Hybrid or two-tiered authentication methods offer a compelling solution, such as private keys encrypted by fingerprint inside of a USB device.

In a computer data context, cryptographic methods have been developed (*see* digital signature and challenge-response authentication) which are currently not spoofable **if and only if** the originator's key has not been compromised. That the originator (or anyone other than an attacker) knows (or doesn't know) about a compromise is irrelevant. It is not known whether these cryptographically based authentication methods are provably secure, since unanticipated mathematical developments may make them vulnerable to attack in future. If that were to occur, it may call into question much of the authentication in the past. In particular, a digitally signed contract may be questioned when a new attack on the cryptography underlying the signature is discovered.

25.7 Authorization

Main article: Authorization

The process of authorization is distinct from that of authentication. Whereas authentication is the process of verifying



A soldier checks a driver's identification card before allowing her to enter a military base.

that “you are who you say you are”, authorization is the process of verifying that “you are permitted to do what you are trying to do”. This does not mean authorization presupposes authentication; an anonymous agent could be authorized to a limited action set.

For example, a client showing proper identification credentials to a bank teller is asking to be authenticated that he really is the one whose identification he is showing. A client whose authentication request is approved becomes authorized to access the accounts of that account holder, but no others.

However note that if a stranger tries to access someone else's account with his own identification credentials, the stranger's identification credentials will still be successfully authenticated because they are genuine and not counterfeit; however, the stranger will not be successfully authorized to access the account, as the stranger's identification credentials had not been previously set to be eligible to access the account, even if valid (i.e. authentic).

Similarly when someone tries to log on a computer, they are usually first requested to identify themselves with a login name and support that with a password. Afterwards, this combination is checked against an existing login-password validity record to check if the combination is authentic. If so, the user becomes authenticated (i.e. the identification he supplied in step 1 is valid, or authentic). Finally, a set of pre-defined permissions and restrictions for that particular login name is assigned to this user, which completes the final step, authorization.

To distinguish “authentication” from the closely related “authorization”, the shorthand notations **A1** (authentication), **A2** (authorization) as well as **AuthN / AuthZ (AuthR)** or **Au / Az** are used in some communities.*[16]

Normally delegation was considered to be a part of authorization domain. Recently authentication is also used for various type of delegation tasks. Delegation in IT network is also a new but evolving field.*[17]

25.8 Access control

Main article: Access control

One familiar use of authentication and authorization is **access control**. A computer system that is supposed to be used only by those authorized must attempt to detect and exclude the unauthorized. Access to it is therefore usually controlled by insisting on an authentication procedure to establish with some degree of confidence the identity of the user, granting privileges established for that identity. One such procedure involves the usage of **Layer 8** which allows IT administrators to identify users, control Internet activity of users in the network, set user based policies and generate reports by username. Common examples of access control involving authentication include:

- Asking for photoID when a contractor first arrives at a house to perform work.
- Using **captcha** as a means of asserting that a user is a human being and not a computer program.
- By using a one-time password (OTP), received on a tele-network enabled device like mobile phone, as an authentication password or PIN
- A computer program using a **blind credential** to authenticate to another
- Entering a country with a **passport**
- Logging into a computer
- Using a confirmation E-mail to verify ownership of an e-mail address
- Using an **Internet banking** system
- Withdrawing cash from an **ATM**

In some cases, ease of access is balanced against the strictness of access checks. For example, the **credit card** network does not require a **personal identification number** for authentication of the claimed identity, and a small transaction usually does not require a signature of the authenticated person for proof of authorization of the transaction. The security of the system is maintained by limiting distribution of credit card numbers, and by the threat of punishment for fraud.

Computer security experts argue that it is impossible to prove the identity of a computer user with absolute certainty. It is only possible to apply one or more tests which, if passed, have been previously declared to be sufficient to proceed. The problem is to determine which tests are sufficient, and many such are inadequate. Any given test can be **spoofed** one way or another, with varying degrees of difficulty.

Computer security experts are now also recognising that despite extensive efforts, as a business, research and network community, we still do not have a secure understanding of the requirements for authentication, in a range of circumstances. Lacking this understanding is a significant barrier to identifying optimum methods of authentication. major questions are:

- What is authentication for?
- Who benefits from authentication/who is disadvantaged by authentication failures?
- What disadvantages can effective authentication actually guard against?

25.9 See also

- Access Control Service
- AssureID
- Atomic authorization
- Authentication Open Service Interface Definition
- Authenticity in art
- Authorization
- Basic access authentication
- Biometrics
- CAPTCHA
- Chip Authentication Program
- Closed-loop authentication
- Diameter (protocol)
- Digital identity
- EAP
- Electronic authentication
- Encrypted key exchange (EKE)
- Fingerprint Verification Competition
- Geolocation
- Global Trust Center
- Hash-based message authentication code
- Identification (information)
- Java Authentication and Authorization Service
- Kantara Initiative
- Kerberos
- Multi-factor authentication
- Needham–Schroeder protocol
- OAuth – an open standard for authorization
- OpenAthens
- OpenID Connect – an authentication method for the web
- OpenID – an authentication method for the web
- Provenance
- Public-key cryptography
- RADIUS
- Reliance authentication

- Secret sharing
- Secure Remote Password protocol (SRP)
- Secure Shell
- Security printing
- SQRL
- Strong authentication
- Tamper-evident technology
- TCP Wrapper
- Time-based authentication
- Two-factor authentication
- Usability of web authentication systems
- Woo–Lam

25.10 References

- [1] Turner, Dawn M. "Digital Authentication: The Basics" . Cryptomathic. Retrieved 9 August 2016.
- [2] Ahi, Kiarash (May 26, 2016). "Advanced terahertz techniques for quality control and counterfeit detection" . *Proc. SPIE 9856, Terahertz Physics, Devices, and Systems X: Advanced Applications in Industry and Defense, 98560G*. doi:10.1117/12.2228684. Retrieved May 26, 2016.
- [3] "How to Tell – Software" . microsoft.com. Retrieved 11 December 2016.
- [4] Federal Financial Institutions Examination Council (2008). "Authentication in an Internet Banking Environment" (PDF). Retrieved 2009-12-31.
- [5] Committee on National Security Systems. "National Information Assurance (IA) Glossary" (PDF). National Counter-intelligence and Security Center. Retrieved 9 August 2016.
- [6] European Central Bank. "Recommendations for the Security of Internet Payments" (PDF). European Central Bank. Retrieved 9 August 2016.
- [7] "FIDO Alliance Passes 150 Post-Password Certified Products" . InfoSecurity Magazine. 2016-04-05. Retrieved 2016-06-13.
- [8] Brocardo ML, Traore I, Woungang I, Obaidat MS. "Authorship verification using deep belief network systems". *Int J Commun Syst*. 2017. doi:10.1002/dac.3259
- [9] "Draft NIST Special Publication 800-63-3: Digital Authentication Guideline" . National Institute of Standards and Technology, USA. Retrieved 9 August 2016.
- [10] Eliasson, C; Matousek (2007). "Noninvasive Authentication of Pharmaceutical Products through Packaging Using Spatially Offset Raman Spectroscopy" . *Analytical Chemistry*. **79** (4): 1696–1701. PMID 17297975. doi:10.1021/ac062223z. Retrieved 9 Nov 2014.
- [11] Li, Ling (March 2013). "Technology designed to combat fakes in the global supply chain" . *Business Horizons*. **56** (2): 167–177. doi:10.1016/j.bushor.2012.11.010. Retrieved 9 Nov 2014.
- [12] How Anti-shoplifting Devices Work" , HowStuffWorks.com
- [13] Norton, D. E. (2004). *The effective teaching of language arts*. New York: Pearson/Merrill/Prentice Hall.
- [14] McTigue, E.; Thornton, E.; Wiese, P. (2013). "Authentication Projects for Historical Fiction: Do you believe it?". *The Reading Teacher*. **66**: 495–505. doi:10.1002/trtr.1132.
- [15] *The Register*, UK; Dan Goodin; 30 March 2008; *Get your German Interior Minister's fingerprint, here*. Compared to other solutions, "It's basically like leaving the password to your computer everywhere you go, without you being able to control it anymore" , one of the hackers comments.

- [16] “AuthN, AuthZ and Gluecon – CloudAve” . *cloudave.com*. 26 April 2010. Retrieved 11 December 2016.
- [17] A mechanism for identity delegation at authentication level, N Ahmed, C Jensen – *Identity and Privacy in the Internet Age* – Springer 2009

25.11 External links

- National Institute of Standards and Technology, U.S. Department of Commerce (August 2013). “Electronic Authentication Guideline – NIST Special Publication 800-63-2” (PDF).
- " New NIST Publications Describe Standards for Identity Credentials and Authentication Systems"

Chapter 26

Multi-factor authentication

Multi-factor authentication (MFA) is a method of computer access control in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are).^{*[1]*[2]}

Two-factor authentication (also known as **2FA**) is a method of confirming a user's claimed identity by utilizing a combination of *two* different components. Two-factor authentication is a type of multi-factor authentication.

A good example from everyday life is the withdrawing of money from a cash machine; only the correct combination of a **bank card** (something that the user possesses) and a PIN (**personal identification number**, something that the user knows) allows the transaction to be carried out.

26.1 Authentication factors

The use of multiple authentication factors to prove one's identity is based on the premise that an unauthorized actor is unlikely to be able to supply the factors required for access. If, in an authentication attempt, at least one of the components is missing or supplied incorrectly, the user's identity is not established with sufficient certainty and access to the asset (e.g., a building, or data) being protected by multi-factor authentication then remains blocked. The authentication factors of a multi-factor authentication scheme may include:

- some physical object in the possession of the user, such as a USB stick with a secret token, a bank card, a key, etc.
- some secret known to the user, such as a password, PIN, TAN, etc.
- some physical characteristic of the user (biometrics), such as a fingerprint, eye iris, voice, typing speed, pattern in key press intervals, etc.^{*[3]}

26.1.1 Knowledge factors

Knowledge factors are the most commonly used form of authentication. In this form, the user is required to prove knowledge of a secret in order to authenticate.

A **password** is a secret word or string of characters that is used for user authentication. This is the most commonly used mechanism of authentication. Many multi-factor authentication techniques rely on password as one factor of authentication.^{*[4]} Variations include both longer ones formed from multiple words (a **passphrase**) and the shorter, purely numeric, **personal identification number** (PIN) commonly used for **ATM** access. Traditionally, passwords are expected to be memorized.

Many **secret questions** such as “Where were you born?” are poor examples of a knowledge factor because they may be known to a wide group of people, or be able to be researched.

26.1.2 Possession factors

Possession factors (“something only the user has”) have been used for authentication for centuries, in the form of a key to a lock. The basic principle is that the key embodies a secret which is shared between the lock and the key, and the same principle underlies possession factor authentication in computer systems. A **security token** is an example of a possession factor.

Disconnected tokens



RSA SecurID token, an example of a disconnected token generator.

Disconnected tokens have no connections to the client computer. They typically use a built-in screen to display the generated authentication data, which is manually typed in by the user.*[5]

Connected tokens

Connected tokens are devices that are physically connected to the computer to be used, and transmit data automatically.*[6] There are a number of different types, including card readers, wireless tags and USB tokens.*[6]

26.1.3 Inherence factors

These are factors associated with the user, and are usually bio-metric methods, including fingerprint readers, retina scanners or voice recognition.

26.2 Mobile phone two-factor authentication

The major drawback of authentication performed including something that the user possesses is that the physical token (the USB stick, the bank card, the key or similar) must be carried around by the user, practically at all times. Loss and theft are a risk. Many organisations forbid USB and electronic devices being carried in or out owing to malware and data theft risks, and most important machines do not have USB ports for the same reason. Physical tokens do not scale, typically requiring a new token for each new account and system. There are also costs involved in procuring and subsequently replacing tokens of this kind. In addition, there are inherent conflicts and unavoidable trade-offs*^[7] between usability and security.

Mobile phone two-factor authentication, where devices such as mobile phones and smartphones serve as “something that the user possesses”, was developed to provide an alternative method that would avoid such issues. To authenticate themselves, people can use their personal access license (i.e. something that only the individual user knows) plus a one-time-valid, dynamic passcode consisting of digits. The code can be sent to their mobile device by **SMS** or via a special app. The advantage of this method is that there is no need for an additional, dedicated token, as users tend to carry their mobile devices around at all times anyway.

Some professional two-factor authentication solutions also ensure that there is always a valid passcode available for users. If one has already used a sequence of digits (passcode), this is automatically deleted and the system sends a new code to the mobile device. And if the new code is not entered within a specified time limit, the system automatically replaces it. This ensures that no old, already used codes are left on mobile devices. For added security, it is possible to specify how many incorrect entries are permitted before the system blocks access.*^[8]

Security of the mobile-delivered security tokens fully depends on the mobile operator's operational security and can be easily breached by wiretapping or **SIM cloning** by national security agencies.*^[9]

Advantages of mobile phone two-factor authentication

- No additional tokens are necessary because it uses mobile devices that are (usually) carried all the time.
- As they are constantly changed, dynamically generated passcodes are safer to use than fixed (static) log-in information.
- Depending on the solution, passcodes that have been used are automatically replaced in order to ensure that a valid code is always available; acute transmission/reception problems do not therefore prevent logins.
- The option to specify a maximum permitted number of incorrect entries reduces the risk of attacks by unauthorized persons.
- It is user friendly.

Disadvantages of mobile phone two-factor authentication

- The mobile phone must be carried by the user, charged, and kept in range of a cellular network whenever authentication might be necessary. If the phone is unable to display messages, such as if it becomes damaged or shuts down for an update or due to temperature extremes (e.g. winter exposure), access is often impossible without backup plans.
- The user must share their personal mobile number with the provider, reducing personal privacy and potentially allowing **spam**.
- The user may be charged by their mobile carrier for messaging fees.*^[10]
- Text messages to mobile phones using **SMS** are insecure and can be intercepted. The token can thus be stolen and used by third parties.*^[11]
- Text messages may not be delivered instantly, adding additional delays to the authentication process.
- Account recovery typically bypasses mobile phone two-factor authentication.*^[12]
- Modern smart phones are used both for browsing email and for receiving SMS. Email is usually always logged in. So if the phone is lost or stolen, all accounts for which the email is the key can be hacked as the phone can receive the second factor. So smart phones combine the two factors into one factor.

- Mobile phones can be stolen, potentially allowing the thief to gain access into the user's accounts.
- SIM cloning gives hackers access to mobile phone connections. Social engineering attacks against mobile operator companies resulted in handing over duplicate SIM cards to criminals.*[13]

26.2.1 Advances in mobile two-factor authentication

Advances in research of two-factor authentication for mobile devices consider different methods in which a second factor can be implemented while not posing a hindrance to the user. With the continued use and improvements in the accuracy of mobile hardware such as GPS,*[14] microphone,*[15] and gyro/accelerometer,*[16] the ability to use them as a second factor of authentication is becoming more trustworthy. For example, by recording the ambient noise of the user's location from a mobile device and comparing it with the recording of the ambient noise from the computer in the same room on which the user is trying to authenticate, one is able to have an effective second factor of authentication.*[17] This also reduces the amount of time and effort needed to complete the process.

26.3 Legislation

26.3.1 United States

Regulation

Details for authentication in the USA are defined with the Homeland Security Presidential Directive 12 (HSPD-12).*[18]

Existing authentication methodologies involve the explained three types of basic “factors”. Authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods.*[19]

IT regulatory standards for access to Federal Government systems require the use of multi-factor authentication to access sensitive IT resources, for example when logging on to network devices to perform administrative tasks*[20] and when accessing any computer using a privileged login.*[21]

Guidance

NIST Special Publication 800-63-2 discusses various forms of two-factor authentication and provides guidance on using them in business processes requiring different levels of assurance.*[22]

In 2005, the United States' Federal Financial Institutions Examination Council issued guidance for financial institutions recommending financial institutions conduct risk-based assessments, evaluate customer awareness programs, and develop security measures to reliably authenticate customers remotely accessing online financial services, officially recommending the use of authentication methods that depend on more than one factor (specifically, what a user knows, has, and is) to determine the user's identity.*[23] In response to the publication, numerous authentication vendors began improperly promoting challenge-questions, secret images, and other knowledge-based methods as “multi-factor” authentication. Due to the resulting confusion and widespread adoption of such methods, on August 15, 2006, the FFIEC published supplemental guidelines—which states that by definition, a “true” multi-factor authentication system must use distinct instances of the three factors of authentication it had defined, and not just use multiple instances of a single factor.*[24]

26.4 Security

According to proponents, multi-factor authentication could drastically reduce the incidence of online identity theft and other online fraud, because the victim's password would no longer be enough to give a thief permanent access to their information. However, many multi-factor authentication approaches remain vulnerable to phishing,*[25] man-in-the-browser, and man-in-the-middle attacks.*[26]

Multi-factor authentication may be ineffective against modern threats, like ATM skimming, phishing, and malware.*[27]

In May 2017 O2 Telefónica, a German mobile service provider, confirmed that cybercriminals had exploited SS7 vulnerabilities to bypass two-factor authentication (2FA) to do unauthorized withdrawals from users bank accounts. The criminals first infected the account holder's computers in an attempt to steal their bank account credentials and phone numbers. Then the attackers purchased access to a fake telecom provider and set-up a redirect for the victim's phone number to a handset controlled by them. Finally the attackers logged into victims' online bank accounts and requested for the money on the accounts to be withdrawn to accounts owned by the criminals. 2FA confirmation codes were routed to phone numbers controlled by the attackers and the criminals transferred the money out.*[28]

26.5 Industry regulation

26.5.1 Payment Card Industry Data Security Standard (PCI-DSS)

The Payment Card Industry (PCI) Data Security Standard, requirement 8.3, requires the use of MFA for all remote network access that originates from outside the network to a Card Data Environment (CDE).*[29] Beginning with PCI-DSS version 3.2, the use of MFA is required for all administrative access to the CDE, even if the user is within a trusted network.*[30]

26.6 Implementation considerations

Many multi-factor authentication products require users to deploy client software to make multi-factor authentication systems work. Some vendors have created separate installation packages for network login, Web access credentials and VPN connection credentials. For such products, there may be four or five different software packages to push down to the client PC in order to make use of the token or smart card. This translates to four or five packages on which version control has to be performed, and four or five packages to check for conflicts with business applications. If access can be operated using web pages, it is possible to limit the overheads outlined above to a single application. With other multi-factor authentication solutions, such as "virtual" tokens and some hardware token products, no software must be installed by end users.

There are drawbacks to multi-factor authentication that are keeping many approaches from becoming widespread. Some consumers have difficulty keeping track of a hardware token or USB plug. Many consumers do not have the technical skills needed to install a client-side software certificate by themselves. Generally, multi-factor solutions require additional investment for implementation and costs for maintenance. Most hardware token-based systems are proprietary and some vendors charge an annual fee per user. Deployment of hardware tokens is logically challenging. Hardware tokens may get damaged or lost and issuance of tokens in large industries such as banking or even within large enterprises needs to be managed. In addition to deployment costs, multi-factor authentication often carries significant additional support costs. A 2008 survey*[31] of over 120 U.S. credit unions by the *Credit Union Journal* reported on the support costs associated with two-factor authentication. In their report, software certificates and software toolbar approaches were reported to have the highest support costs.

26.7 Examples

Several popular web services employ multi-factor authentication, usually as an optional feature that is deactivated by default.*[32]

- Two-factor authentication
- Many Internet services (among them: Google, Amazon AWS) use open Time-based One-time Password Algorithm (TOTP) to support multi-factor or two-factor authentication

26.8 See also

- Comparison of authentication solutions

- Identity management
- Mutual authentication
- Reliance authentication
- Strong authentication

26.9 References

- [1] "Two-factor authentication: What you need to know (FAQ) – CNET" . *CNET*. Retrieved 2015-10-31.
- [2] "How to extract data from an iCloud account with two-factor authentication activated" . *iphonebackupextractor.com*. Retrieved 2016-06-08.
- [3] "What is 2FA?". Retrieved 19 February 2015.
- [4] "Securevoy – what is 2 factor authentication?". Retrieved April 3, 2015.
- [5] de Borde, Duncan. "Two-factor authentication" (PDF). Archived from the original (PDF) on January 12, 2012.
- [6] van Tilborg, Henk C.A.; Jajodia, Sushil, eds. (2011). *Encyclopedia of Cryptography and Security, Volume 1*. Springer Science & Business Media. p. 1305. ISBN 9781441959058.
- [7] <http://eprint.iacr.org/2014/135.pdf>
- [8] "Mobile Two Factor Authentication" (PDF). *securevoy.com*. Retrieved August 30, 2016. 2012 copyright
- [9] "How Russia Works on Intercepting Messaging Apps – bellingcat" . *bellingcat*. 2016-04-30. Retrieved 2016-04-30.
- [10] "Standard Vs. Premium Text Message Charges" . Retrieved 2017-07-12.
- [11] SSMS – A Secure SMS Messaging Protocol for the M-Payment Systems, Proceedings of the 13th IEEE Symposium on Computers and Communications (ISCC'08), pp. 700–705, July 2008 arXiv:1002.3171
- [12] Rosenblatt, Seth; Cipriani, Jason (June 15, 2015). "Two-factor authentication: What you need to know (FAQ)". *CNET*. Retrieved 2016-03-17.
- [13] tweet_btn(), Shaun Nichols in San Francisco 10 Jul 2017 at 23:31. "Two-factor FAIL: Chap gets pwned after 'AT&T falls for hacker tricks'". Retrieved 2017-07-11.
- [14] "Location Authentication - Inside GNSS" . www.insidegnss.com.
- [15] "Continuous voice authentication for a mobile device" .
- [16] "DARPA presents: Continuous Mobile Authentication - Behaviosec" . 22 October 2013.
- [17] "Sound-Proof: Usable Two-Factor Authentication Based on Ambient Sound | USENIX" . www.usenix.org. Retrieved 2016-02-24.
- [18] US Security Directive as issued on August 12, 2007 Archived September 16, 2012, at the Wayback Machine.
- [19] "Frequently Asked Questions on FFIEC Guidance on Authentication in an Internet Banking Environment" , August 15, 2006
- [20] "SANS Institute, Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches"
- [21] "SANS Institute, Critical Control 12: Controlled Use of Administrative Privileges" .
- [22] "Electronic Authentication Guide" (PDF). *Special Publication 800-63-2*. NIST. 2013. Retrieved 2014-11-06.
- [23] "FFIEC Press Release" . 2005-10-12. Retrieved 2011-05-13.
- [24] FFIEC (2006-08-15). "Frequently Asked Questions on FFIEC Guidance on Authentication in an Internet Banking Environment" (PDF). Retrieved 2012-01-14.
- [25] Brian Krebs (July 10, 2006). "Security Fix – Citibank Phish Spoofs 2-Factor Authentication" . Washington Post. Retrieved 20 September 2016.

- [26] Bruce Schneier (March 2005). “The Failure of Two-Factor Authentication”. *Schneier on Security*. Retrieved 20 September 2016.
- [27] “The Failure of Two-Factor Authentication – Schneier on Security” . *schneier.com*. Retrieved 23 October 2015.
- [28] Khandelwal, Swati. “Real-World SS7 Attack —Hackers Are Stealing Money From Bank Accounts” . *The Hacker News*. Retrieved 2017-05-05.
- [29] “Official PCI Security Standards Council Site – Verify PCI Compliance, Download Data Security and Credit Card Security Standards” . *www.pcisecuritystandards.org*. Retrieved 2016-07-25.
- [30] “For PCI MFA Is Now Required For Everyone | Centrify Blog” . *blog.centrify.com*. Retrieved 2016-07-25.
- [31] “Study Sheds New Light On Costs, Affects Of Multi-Factor” .
- [32] GORDON, WHITSON (3 September 2012). “Two-Factor Authentication: The Big List Of Everywhere You Should Enable It Right Now” . *LifeHacker*. Australia. Retrieved 1 November 2012.

26.10 Further reading

- Brandom, Russell (July 10, 2017). “Two-factor authentication is a mess” . *The Verge*. Retrieved July 10, 2017.

26.11 External links

- Attackers breached the servers of RSA and stole information that could be used to compromise the security of two-factor authentication tokens used by 40 million employees (register.com, 18 Mar 2011)
- Banks to Use Two-factor Authentication by End of 2006, (slashdot.org, 20 Oct 2005)
- List of commonly used websites and whether or not they support Two-Factor Authentication
- Microsoft to abandon passwords, Microsoft preparing to dump passwords in favour of two-factor authentication in forthcoming versions of Windows (vnu.net.com, 14 Mar 2005)

Chapter 27

Authorization

“Authorized” redirects here. For the 2007 Epsom Derby winner, see [Authorized \(horse\)](#).

Authorization is the function of specifying access rights to resources related to [information security](#) and [computer security](#) in general and to [access control](#) in particular. More formally, “to authorize” is to define an access policy. For example, [human resources](#) staff is normally authorized to access employee records and this policy is usually formalized as access control rules in a computer system. During operation, the system uses the access control rules to decide whether access requests from ([authentication](#)) shall be approved (granted) or disapproved (rejected). Resources include individual files or an item’s [data](#), [computer programs](#), computer devices and functionality provided by computer applications. Examples of consumers are computer users, computer [Software](#) and other [Hardware](#) on the computer.

27.1 Overview

Access control in [computer systems](#) and [networks](#) rely on access [policies](#). The access control process can be divided into the following phases: policy definition phase where access is authorized, and policy enforcement phase where access requests are approved or disapproved. Authorization is the function of the policy definition phase which precedes the policy enforcement phase where access requests are approved or disapproved based on the previously defined authorizations.

Most modern, multi-user operating systems include access control and thereby rely on authorization. Access control also uses [authentication](#) to verify the [identity](#) of consumers. When a consumer tries to access a resource, the access control process checks that the consumer has been authorized to use that resource. Authorization is the responsibility of an authority, such as a department manager, within the application domain, but is often delegated to a custodian such as a [system administrator](#). Authorizations are expressed as access policies in some types of “policy definition application”, e.g. in the form of an [access control list](#) or a [capability](#), on the basis of the “[principle of least privilege](#)”: consumers should only be authorized to access whatever they need to do their jobs. Older and single user operating systems often had weak or non-existent authentication and access control systems.

“Anonymous consumers” or “guests”, are consumers that have not been required to authenticate. They often have limited authorization. On a distributed system, it is often desirable to grant access without requiring a unique identity. Familiar examples of access [tokens](#) include keys and tickets: they grant access without proving identity.

Trusted consumers are often authorized for unrestricted access to resources on a system, but must be authenticated so that the access control system can make the access approval decision. “Partially trusted” and guests will often have restricted authorization in order to protect resources against improper access and usage. The access policy in some operating systems, by default, grant all consumers full access to all resources. Others do the opposite, insisting that the administrator explicitly authorizes a consumer to use each resource.

Even when access is controlled through a combination of authentication and [access control lists](#), the problems of maintaining the authorization data is not trivial, and often represents as much administrative burden as managing authentication credentials. It is often necessary to change or remove a user’s authorization: this is done by changing or deleting the corresponding access rules on the system. Using [atomic](#) authorization is an alternative to per-system authorization management, where a trusted third party securely distributes authorization information.

27.2 Related interpretations

27.2.1 Public policy

In public policy, authorization is a feature of **trusted systems** used for security or social control.

27.2.2 Banking

In banking, an **authorization** is a hold placed on a customer's account when a purchase is made using a **debit card** or **credit card**.

27.2.3 Publishing

In publishing, sometimes public lectures and other freely available texts are published without the approval of the author. These are called unauthorized texts. An example is the 2002 '*The Theory of Everything: The Origin and Fate of the Universe*', which was collected from Stephen Hawking's lectures and published without his permission as per copyright law.

27.3 See also

- Access control
- Authentication
- Authorization hold
- Authorization OSID
- Computer security
- Kerberos (protocol)
- OpenID Connect
- OpenID
- Operating system
- Privilege escalation
- Security engineering
- Usability of web authentication systems
- WebFinger
- WebID
- XACML

Chapter 28

Data-centric security

Data-centric security is an approach to security that emphasizes the security of the **data** itself rather than the security of networks, servers, or applications. Data-centric security is evolving rapidly as enterprises increasingly rely on digital information to run their business and **big data** projects become mainstream.* [1]* [2] Data-centric security also allows organizations to overcome the disconnect between IT security technology and the objectives of business strategy by relating security services directly to the data they implicitly protect; a relationship that is often obscured by the presentation of security as an end in itself.* [3]

28.1 Key concepts

Common processes in a data-centric security model include: * [4]

- Discover: the ability to know what data is stored where including sensitive information.
- Manage: the ability to define access policies that will determine if certain data is accessible, editable, or blocked from specific users, or locations.
- Protect: the ability to defend against data loss or unauthorized use of data and prevent sensitive data from being sent to unauthorized users or locations.
- Monitor: the constant monitoring of data usage to identify meaningful deviations from normal behavior that would point to possible malicious intent.

From a technical point of view, information(data)-centric security relies on the implementation of the following: * [5]

- Information (data) that is self-describing and defending.
- Policies and controls that account for business context.
- Information that remains protected as it moves in and out of applications and storage systems, and changing business context.
- Policies that work consistently through the different data management technologies and defensive layers implemented.

28.2 Technology

28.2.1 Data access controls and policies

Data access control is the selective restriction of access to data. Accessing may mean viewing, editing, or using. Defining proper access controls requires to map out the information, where it resides, how important it is, who it is important to, how sensitive the data is and then designing appropriate controls.*[6]

28.2.2 Encryption

Main article: [Encryption](#)

Encryption is a proven data-centric technique to address the risk of data theft in smartphones, laptops, desktops and even servers, including the cloud. One limitation is that encryption becomes useless once a network intrusion has occurred and cybercriminals operate with stolen valid user credentials.*[7]

28.2.3 Data masking

Main article: [Data masking](#)

Data Masking is the process of hiding specific data within a database table or cell to ensure that data security is maintained and that sensitive information is not exposed to unauthorized personnel. This may include masking the data from users, developers, third-party and outsourcing vendors, etc. Data masking can be achieved multiple ways: by duplicating data to eliminate the subset of the data that needs to be hidden or by obscuring the data dynamically as users perform requests.

28.2.4 Auditing

Main article: [Security audit](#)

Monitoring all activity at the data layer is a key component of a data-centric security strategy. It provides visibility into the types of actions that users and tools have requested and been authorized to on specific data elements. Continuous monitoring at the data layer combined with precise access control can contribute significantly to the real-time detection of data breaches, limits the damages inflicted by a breach and can even stop the intrusion if proper controls are in place. A 2016 survey*[8] shows that most organizations still don't assess database activity continuously and lack the capability to identify database breaches in a timely fashion.

28.3 Cloud computing

Cloud computing is an evolving paradigm with tremendous momentum, but its unique aspects exacerbate security and privacy challenges. Heterogeneity and diversity of cloud services and environments demand fine-grained access control policies and services that should be flexible enough to capture dynamic, context, or attribute-based access requirements and data protection.*[9]

28.3.1 Data-centric security in the public cloud environments

In recent decade many organizations rely on managing database services in public clouds such [Amazon_Web_Services](#) or [Microsoft_Azure](#) to organize their data. Such approach has its own limitations on what users can do with managing security of their sensitive data. For instance, hardware security appliances or agents running on the database servers are no longer the option. This requires innovative way to secure data and databases such as using reverse proxy sitting between clients / applications and database servers. The requirements such supporting a load balancing, high availability and fail-over in data-centric security brings additional challenges that database security vendors must to meet.*[10]

28.4 See also

- Data masking
- Data security
- Defense in depth (computing)
- Information security
- Information security policies

28.5 References

- [1] Gartner Group (2014). “Gartner Says Big Data Needs a Data-Centric Security Focus” .
- [2] SANS Institute (2015). “Data-Centric Security Needed to Protect Big Data Implementations” .
- [3] IEEE (2007). “Elevating the Discussion on Security Management: The Data Centric Paradigm” .
- [4] Wired Magazine (2014). “Information-Centric Security: Protect Your Data From the Inside-Out” .
- [5] Mogull, Rich (2014). “The Information-Centric Security Lifecycle” (PDF).
- [6] Federal News Radio (2015). “NASA Glenn becoming more data-centric across many fronts” .
- [7] MIT Technology Review (2015). “Encryption Wouldn’t Have Stopped Anthem’s Data Breach” .
- [8] Dark Reading (2016). “Databases Remain Soft Underbelly Of Cybersecurity” .
- [9] IEEE (2010). “Security and Privacy Challenges in Cloud Computing Environments” (PDF).
- [10] DataSunrise (2017). “Data-centric database security in the public clouds” .

Chapter 29

Firewall (computing)

In computing, a **firewall** is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.*[1] A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed not to be secure or trusted.*[2]

Firewalls are often categorized as either *network firewalls* or *host-based firewalls*. Network firewalls filter traffic between two or more networks; they are either software appliances running on general purpose hardware, or hardware-based firewall computer appliances. Host-based firewalls provide a layer of software on one host that controls network traffic in and out of that single machine.*[3]*[4]

Firewall appliances may also offer other functionality to the internal network they protect, such as acting as a DHCP*[5]*[6] or VPN*[7]*[8]*[9]*[10] server for that network.*[11]*[12]

29.1 History

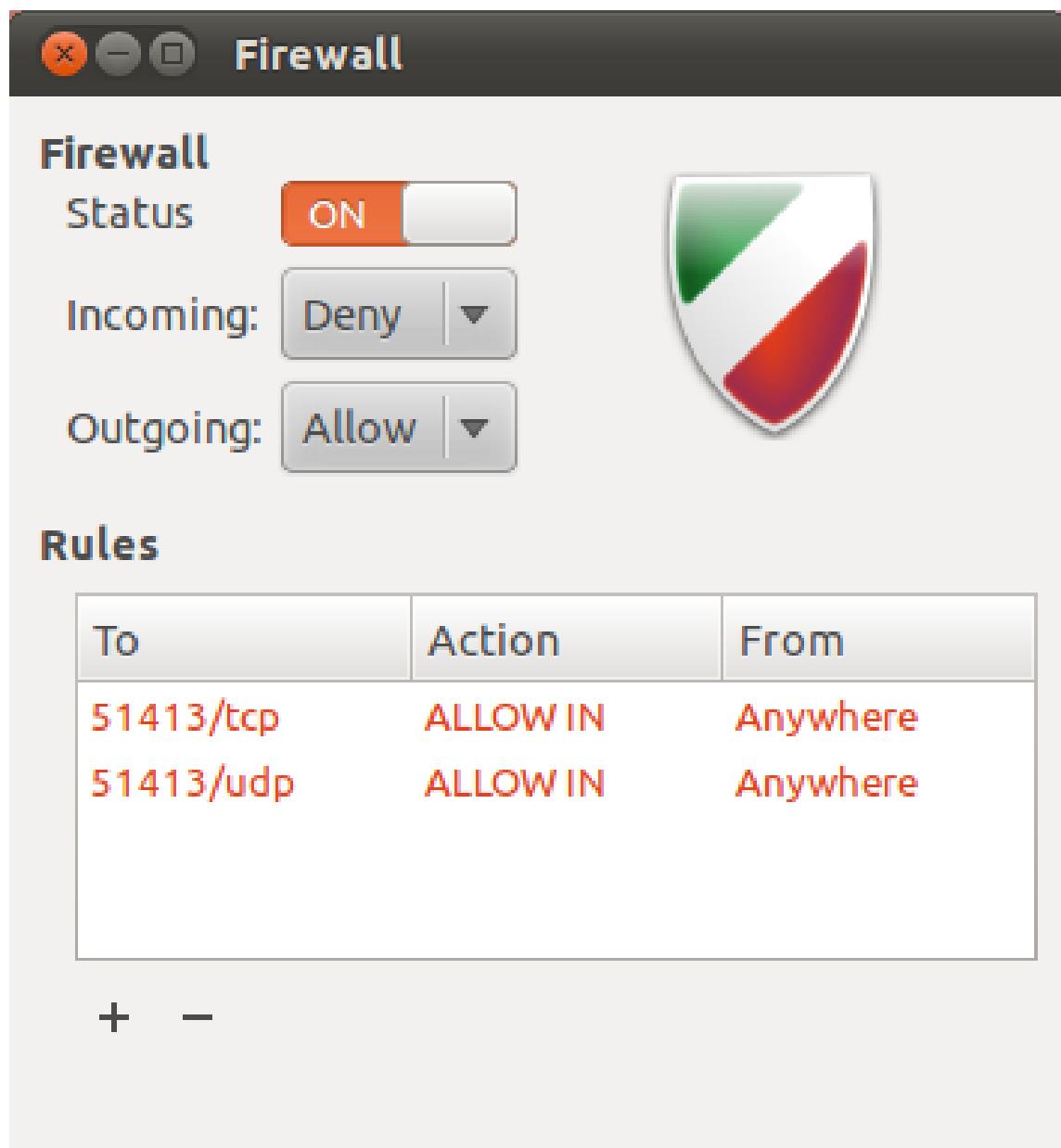
The term *firewall* originally referred to a wall intended to confine a fire or potential fire within a building.*[13] Later uses refer to similar structures, such as the metal sheet separating the engine compartment of a vehicle or aircraft from the passenger compartment.

The term was applied in the late 1980s to network technology that emerged when the Internet was fairly new in terms of its global use and connectivity.*[14] The predecessors to firewalls for network security were the routers used in the late 1980s.*[15]

29.1.1 First generation: packet filters

The first type of network firewall was the packet filter which would look at network addresses and ports of the packet to determine if that packet should be allowed or blocked.*[16] The first paper published on firewall technology was in 1988, when engineers from Digital Equipment Corporation (DEC) developed filter systems known as packet filter firewalls. This fairly basic system was the first generation of what is now a highly involved and technical internet security feature. At AT&T Bell Labs, Bill Cheswick and Steve Bellovin were continuing their research in packet filtering and developed a working model for their own company based on their original first generation architecture.*[17]

Packet filters act by inspecting the “packets” which are transferred between computers on the Internet. If a packet does not match the packet filter’s set of filtering rules, the packet filter will drop (silently discard) the packet or reject it (discard it, and send “error responses” to the source). Conversely, if the packet matches one or more of the programmed filters, the packet is allowed to pass. This type of packet filtering pays no attention to whether a packet is part of an existing stream of traffic (i.e. it stores no information on connection “state”). Instead, it filters each packet based only on information contained in the packet itself (most commonly using a combination of the packet’s source and destination address, its protocol, and, for TCP and UDP traffic, the port number). TCP and UDP protocols constitute most communication over the Internet, and because TCP and UDP traffic by convention uses well known ports for particular types of traffic, a “stateless” packet filter can distinguish between, and thus control, those types of traffic (such as web browsing, remote printing, email transmission, file transfer), unless the machines on each side of the packet filter are both using the same non-standard ports.*[18]



Screenshot of *Gufw*: The firewall shows its settings for incoming and outgoing traffic.

Packet filtering firewalls work mainly on the first three layers of the OSI reference model, which means most of the work is done between the network and physical layers, with a little bit of peeking into the transport layer to figure out source and destination port numbers.^{*[19]} When a packet originates from the sender and filters through a firewall, the device checks for matches to any of the packet filtering rules that are configured in the firewall and drops or rejects the packet accordingly. When the packet passes through the firewall, it filters the packet on a protocol/port number basis (GSS). For example, if a rule in the firewall exists to block telnet access, then the firewall will block the TCP protocol for port number 23.^{*[20]}

29.1.2 Second generation: “stateful”filters

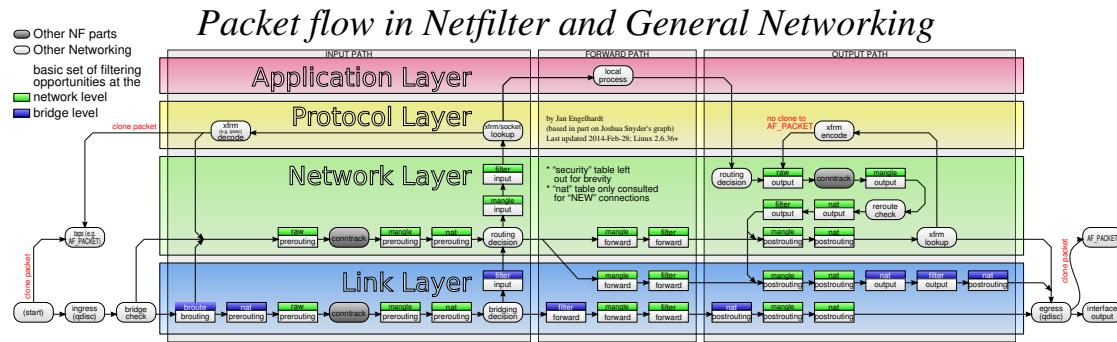
Main article: Stateful firewall

From 1989–1990 three colleagues from AT&T Bell Laboratories, Dave Presotto, Janardan Sharma, and Kshitij Nigam, developed the second generation of firewalls, calling them circuit-level gateways.^{*[21]}

Second-generation firewalls perform the work of their first-generation predecessors but operate up to layer 4 (transport layer) of the OSI model. This is achieved by retaining packets until enough information is available to make a judgement about its state.* [22] Known as **stateful packet inspection**, it records all connections passing through it and determines whether a packet is the start of a new connection, a part of an existing connection, or not part of any connection.* [23] Though static rules are still used, these rules can now contain *connection state* as one of their test criteria.

Certain denial-of-service attacks bombard the firewall with thousands of fake connection packets in an attempt to overwhelm it by filling its connection state memory.* [24]

29.1.3 Third generation: application layer



Flow of network packets through Netfilter, a Linux kernel module

Main article: Application level firewall

Marcus Ranum, Wei Xu, and Peter Churchyard developed an application firewall known as Firewall Toolkit (FWTK). In June 1994, Wei Xu extended the FWTK with the kernel enhancement of IP filter and socket transparent. This was known as the first transparent application firewall, released as a commercial product of Gauntlet firewall at Trusted Information Systems. Gauntlet firewall was rated one of the top firewalls during 1995–1998.

The key benefit of application layer filtering is that it can “understand” certain applications and protocols (such as File Transfer Protocol (FTP), Domain Name System (DNS), or Hypertext Transfer Protocol (HTTP)). This is useful as it is able to detect if an unwanted application or service is attempting to bypass the firewall using a protocol on an allowed port, or detect if a protocol is being abused in any harmful way.

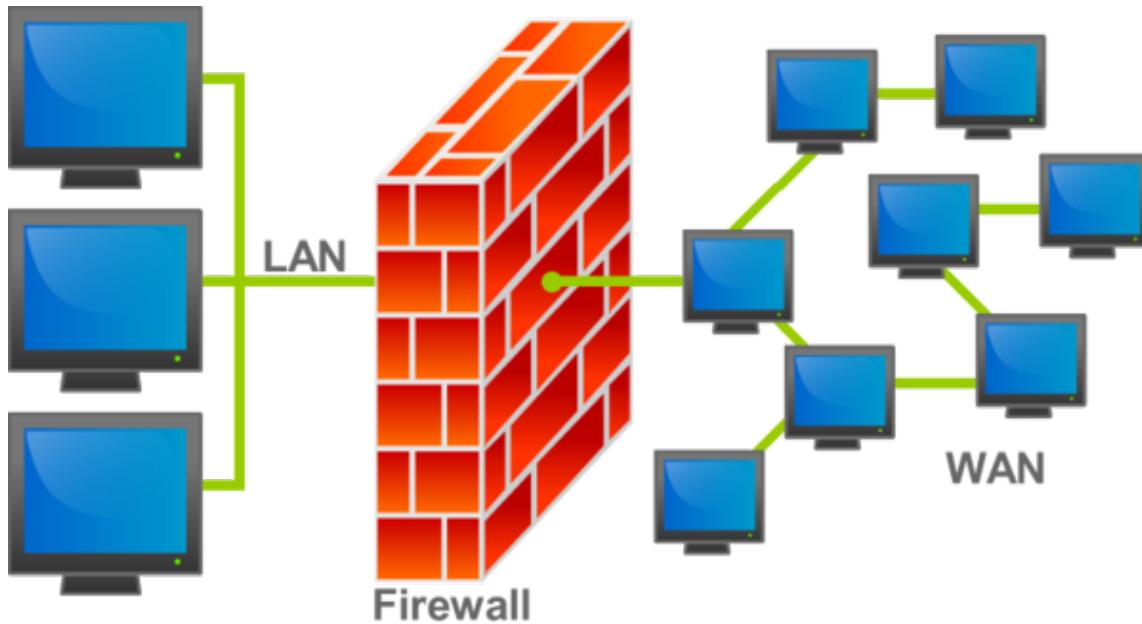
As of 2012, the so-called next-generation firewall (NGFW) is nothing more than the “wider” or “deeper” inspection at application stack. For example, the existing deep packet inspection functionality of modern firewalls can be extended to include

- Intrusion prevention systems (IPS)
- User identity management integration (by binding user IDs to IP or MAC addresses for “reputation”)
- Web application firewall (WAF). WAF attacks may be implemented in the tool “WAF Fingerprinting utilizing timing side channels” (WAFFle)* [25]

29.2 Types

Firewalls are generally categorized as network-based or host-based. Network-based firewalls are positioned on the gateway computers of LANs, WANs and intranets. Host-based firewalls are positioned on the network node itself. The host-based firewall may be a **daemon** or **service** as a part of the **operating system** or an agent application such as **endpoint security** or protection. Each has advantages and disadvantages. However, each has a role in layered security.

Firewalls also vary in type depending on where communication originates, where it is intercepted, and the state of communication being traced.* [26]



An illustration of where a firewall would be located in a network

29.2.1 Network layer or packet filters

Network layer firewalls, also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set. The firewall administrator may define the rules; or default rules may apply. The term “packet filter” originated in the context of BSD operating systems.

Network layer firewalls generally fall into two sub-categories, stateful and stateless. Stateful firewalls maintain context about active sessions, and use that “state information” to speed packet processing. Any existing network connection can be described by several properties, including source and destination IP address, UDP or TCP ports, and the current stage of the connection’s lifetime (including session initiation, handshaking, data transfer, or completion connection). If a packet does not match an existing connection, it will be evaluated according to the ruleset for new connections. If a packet matches an existing connection based on comparison with the firewall’s state table, it will be allowed to pass without further processing.

Stateless firewalls require less memory, and can be faster for simple filters that require less time to filter than to look up a session. They may also be necessary for filtering stateless network protocols that have no concept of a session. However, they cannot make more complex decisions based on what stage communications between hosts have reached.

Newer firewalls can filter traffic based on many packet attributes like source IP address, source port, destination IP address or port, destination service like HTTP or FTP. They can filter based on protocols, TTL values, network block of the originator, of the source, and many other attributes.

Commonly used packet filters on various versions of Unix are *ipfw* (FreeBSD, Mac OS X (< 10.7)), *NPF* (NetBSD), *PF* (Mac OS X (> 10.4), OpenBSD, and some other BSDs), *iptables/ipchains* (Linux) and *IPFilter*.

29.2.2 Application-layer

Main article: Application layer firewall

Application-layer firewalls work on the application level of the TCP/IP stack (i.e., all browser traffic, or all telnet or FTP traffic), and may intercept all packets traveling to or from an application. They block other packets (usually dropping them without acknowledgment to the sender).

On inspecting all packets for improper content, firewalls can restrict or prevent outright the spread of networked computer worms and Trojans. The additional inspection criteria can add extra latency to the forwarding of packets

to their destination.

Application firewalls function by determining whether a process should accept any given connection. Application firewalls accomplish their function by hooking into socket calls to filter the connections between the application layer and the lower layers of the OSI model. Application firewalls that hook into socket calls are also referred to as socket filters. Application firewalls work much like a packet filter but application filters apply filtering rules (allow/block) on a per process basis instead of filtering connections on a per port basis. Generally, prompts are used to define rules for processes that have not yet received a connection. It is rare to find application firewalls not combined or used in conjunction with a packet filter.*[27]

Also, application firewalls further filter connections by examining the process ID of data packets against a rule set for the local process involved in the data transmission. The extent of the filtering that occurs is defined by the provided rule set. Given the variety of software that exists, application firewalls only have more complex rule sets for the standard services, such as sharing services. These per-process rule sets have limited efficacy in filtering every possible association that may occur with other processes. Also, these per-process rule sets cannot defend against modification of the process via exploitation, such as memory corruption exploits. Because of these limitations, application firewalls are beginning to be supplanted by a new generation of application firewalls that rely on mandatory access control (MAC), also referred to as **sandboxing**, to protect vulnerable services.*[28]

29.2.3 Proxies

Main article: Proxy server

A proxy server (running either on dedicated hardware or as software on a general-purpose machine) may act as a firewall by responding to input packets (connection requests, for example) in the manner of an application, while blocking other packets. A proxy server is a gateway from one network to another for a specific network application, in the sense that it functions as a proxy on behalf of the network user.*[2]

Proxies make tampering with an internal system from the external network more difficult, so that misuse of one internal system would not necessarily cause a security breach exploitable from outside the firewall (as long as the application proxy remains intact and properly configured). Conversely, intruders may hijack a publicly reachable system and use it as a proxy for their own purposes; the proxy then **masquerades** as that system to other internal machines. While use of internal address spaces enhances security, crackers may still employ methods such as **IP spoofing** to attempt to pass packets to a target network.

29.2.4 Network address translation

Main article: Network address translation

Firewalls often have **network address translation** (NAT) functionality, and the hosts protected behind a firewall commonly have addresses in the “private address range”, as defined in **RFC 1918**. Firewalls often have such functionality to hide the true address of protected hosts. Originally, the NAT function was developed to address the limited number of IPv4 routable addresses that could be used or assigned to companies or individuals as well as reduce both the amount and therefore cost of obtaining enough public addresses for every computer in an organization. Although NAT on its own is not considered a security feature, hiding the addresses of protected devices has become an often used defense against **network reconnaissance**.*[29]

29.3 See also

- Access control list
- Air gap (networking)
- Bastion host
- Comparison of firewalls
- Computer security

- De-perimeterisation
- Distributed firewall
- Egress filtering
- End-to-end principle
- Firewall pinhole
- Firewalls and Internet Security
- Golden Shield Project
- Guard (information security)
- Identity-based security
- IP fragmentation attacks
- List of Unix-like router or firewall distributions
- Mangled packet
- Mobile security § Security software
- Next-Generation Firewall
- Personal firewall
- Screened-subnet firewall
- Unidirectional network
- Unified threat management
- Virtual firewall
- Vulnerability scanner
- Windows Firewall

29.4 References

- [1] Boudriga, Noureddine (2010). *Security of mobile communications*. Boca Raton: CRC Press. pp. 32–33. ISBN 0849379423.
- [2] Oppliger, Rolf (May 1997). “Internet Security: FIREWALLS and BEYOND” . *Communications of the ACM*. **40** (5): 94. doi:10.1145/253769.253802.
- [3] Vacca, John R. (2009). *Computer and information security handbook*. Amsterdam: Elsevier. p. 355. ISBN 9780080921945.
- [4] “What is Firewall?”. Retrieved 2015-02-12.
- [5] “Firewall as a DHCP Server and Client” . *Palo Alto Networks*. Retrieved 2016-02-08.
- [6] “DHCP” . *www.shorewall.net*. Retrieved 2016-02-08.
- [7] “What is a VPN Firewall? - Definition from Techopedia” . *Techopedia.com*. Retrieved 2016-02-08.
- [8] “VPNs and Firewalls” . *technet.microsoft.com*. Retrieved 2016-02-08.
- [9] “VPN and Firewalls (Windows Server)”. *Resources and Tools for IT Professionals | TechNet*.
- [10] “Configuring VPN connections with firewalls” .
- [11] Andrés, Steven; Kenyon, Brian; Cohen, Jody Marc; Johnson, Nate; Dolly, Justin (2004). Birkholz, Erik Pack, ed. *Security Sage's Guide to Hardening the Network Infrastructure*. Rockland, MA: Syngress. pp. 94–95. ISBN 9780080480831.
- [12] Naveen, Sharanya. “Firewall” . Retrieved 7 June 2016.

- [13] Canavan, John E. (2001). *Fundamentals of Network Security* (1st ed.). Boston, MA: Artech House. p. 212. ISBN 9781580531764.
- [14] Liska, Allan (Dec 10, 2014). *Building an Intelligence-Led Security Program*. Syngress. p. 3. ISBN 0128023708.
- [15] Ingham, Kenneth; Forrest, Stephanie (2002). "A History and Survey of Network Firewalls" (PDF). Retrieved 2011-11-25.
- [16] Peltier, Justin; Peltier, Thomas R. (2007). *Complete Guide to CISM Certification*. Hoboken: CRC Press. p. 210. ISBN 9781420013252.
- [17] Ingham, Kenneth; Forrest, Stephanie (2002). "A History and Survey of Network Firewalls" (PDF). p. 4. Retrieved 2011-11-25.
- [18] TCP vs. UDP By Erik Rodriguez
- [19] William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin (2003). "Google Books Link". *Firewalls and Internet Security: repelling the wily hacker*
- [20] Aug 29, 2003 Virus may elude computer defenses by Charles Duhigg, Washington Post
- [21] *Proceedings of National Conference on Recent Developments in Computing and Its Applications, August 12–13, 2009*. I.K. International Pvt. Ltd. 2009-01-01. Retrieved 2014-04-22.
- [22] Conway, Richard (204). *Code Hacking: A Developer's Guide to Network Security*. Hingham, Massachusetts: Charles River Media. p. 281. ISBN 1-58450-314-9.
- [23] Andress, Jason (May 20, 2014). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice* (2nd ed.). Elsevier Science. ISBN 9780128008126.
- [24] Chang, Rocky (October 2002). "Defending Against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial" . *IEEE Communications Magazine*. **40** (10): 42–43. doi:10.1109/mcom.2002.1039856.
- [25] "WAFFle: Fingerprinting Filter Rules of Web Application Firewalls" . 2012.
- [26] "Firewalls" . MemeBridge. Retrieved 13 June 2014.
- [27] "Software Firewalls: Made of Straw? Part 1 of 2" . Symantec Connect Community. 2010-06-29. Retrieved 2014-03-28.
- [28] "Auto Sandboxing" . Comodo Inc. Retrieved 2014-08-28.
- [29] "Advanced Security: Firewall" . Microsoft. Retrieved 2014-08-28.

29.5 External links

- Internet Firewalls: Frequently Asked Questions, compiled by Matt Curtin, Marcus Ranum and Paul Robertson.
- Firewalls Aren't Just About Security - Cyberoam Whitepaper focusing on Cloud Applications Forcing Firewalls to Enable Productivity.
- Evolution of the Firewall Industry - Discusses different architectures and their differences, how packets are processed, and provides a timeline of the evolution.
- A History and Survey of Network Firewalls - provides an overview of firewalls at the various ISO levels, with references to the original papers where first firewall work was reported.
- Software Firewalls: Made of Straw? Part 1 and Software Firewalls: Made of Straw? Part 2 - a technical view on software firewall design and potential weaknesses

Chapter 30

Intrusion detection system

An **intrusion detection system (IDS)** is a device or software application that monitors a network or systems for malicious activity or policy violations. Any detected activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources, and uses alarm filtering techniques to distinguish malicious activity from false alarms.

There is a wide spectrum of IDS, varying from antivirus software to hierarchical systems that monitor the traffic of an entire backbone network. The most common classifications are **network intrusion detection systems (NIDS)** and **host-based intrusion detection systems (HIDS)**. A system that monitors important operating system files is an example of a HIDS, while a system that analyzes incoming network traffic is an example of a NIDS. It is also possible to classify IDS by detection approach: the most well-known variants are signature-based detection (recognizing bad patterns, such as malware) and anomaly-based detection (detecting deviations from a model of “good” traffic, which often relies on machine learning). Some IDS have the ability to respond to detected intrusions. Systems with response capabilities are typically referred to as an **intrusion prevention system**.

30.1 Comparison with firewalls

Though they both relate to network security, an IDS differs from a **firewall** in that a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls limit access between networks to prevent intrusion and do not signal an attack from inside the network. An IDS evaluates a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system. This is traditionally achieved by examining network communications, identifying **heuristics** and patterns (often known as signatures) of common computer attacks, and taking action to alert operators. A system that terminates connections is called an intrusion prevention system, and is another form of an **application layer firewall**.

30.2 Classifications

IDS can be classified by where detection takes place (network or host) and the detection method that is employed.

30.2.1 Analyzed activity

Network intrusion detection systems

Network intrusion detection systems (NIDS) are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. It performs an analysis of passing traffic on the entire **subnet**, and matches the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator. An example of an NIDS would be installing it on the subnet where firewalls are located in order to see if someone is trying to break into the firewall. Ideally one would scan all inbound and outbound traffic, however doing so might create a bottleneck that would impair the overall speed of the network. OPNET and NetSim are commonly used tools for simulation network intrusion

detection systems. NID Systems are also capable of comparing signatures for similar packets to link and drop harmful detected packets which have a signature matching the records in the NIDS. When we classify the design of the NIDS according to the system interactivity property, there are two types: on-line and off-line NIDS, often referred to as inline and tap mode, respectively. On-line NIDS deals with the network in real time. It analyses the Ethernet packets and applies some rules, to decide if it is an attack or not. Off-line NIDS deals with stored data and passes it through some processes to decide if it is an attack or not.*[1]

Host intrusion detection systems

Main article: Host-based intrusion detection system

Host intrusion detection systems (HIDS) run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator if suspicious activity is detected. It takes a snapshot of existing system files and matches it to the previous snapshot. If the critical system files were modified or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission critical machines, which are not expected to change their configurations.

Intrusion detection systems can also be system-specific using custom tools and honeypots.

30.2.2 Detection method

Signature-based

Signature-based IDS refers to the detection of attacks by looking for specific patterns, such as byte sequences in network traffic, or known malicious instruction sequences used by malware.*[2] This terminology originates from anti-virus software, which refers to these detected patterns as signatures. Although signature-based IDS can easily detect known attacks, it is impossible to detect new attacks, for which no pattern is available.

Anomaly-based

Anomaly-based intrusion detection systems were primarily introduced to detect unknown attacks, in part due to the rapid development of malware. The basic approach is to use machine learning to create a model of trustworthy activity, and then compare new behavior against this model. Although this approach enables the detection of previously unknown attacks, it may suffer from false positives: previously unknown legitimate activity may also be classified as malicious.

New types of what could be called anomaly-based intrusion detection systems are being viewed by Gartner as User and Entity Behavior Analytics (UEBA)*[3] (an evolution of the user behavior analytics category) and network traffic analysis (NTA).*[4] In particular, NTA deals with malicious insiders as well as targeted external attacks that have compromised a user machine or account. Gartner has noted that some organizations have opted for NTA over more traditional IDS.*[5]

30.3 Intrusion prevention

Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization.*[6]

IDPSes typically record information related to observed events, notify security administrators of important observed events and produce reports. Many IDPSes can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content.*[6]

Intrusion prevention systems (IPS), also known as **intrusion detection and prevention systems (IDPS)**, are network security appliances that monitor network or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, report it and attempt to block or stop it.*[7].

Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent or block intrusions that are detected.*[8]*:273*[9]*:289 IPS can take such actions as sending an alarm, dropping detected malicious packets, resetting a connection or blocking traffic from the offending IP address.*[10] An IPS also can correct cyclic redundancy check (CRC) errors, defragment packet streams, mitigate TCP sequencing issues, and clean up unwanted transport and network layer options.*[8]*:278*[11].

30.3.1 Classification

Intrusion prevention systems can be classified into four different types: * [7]*[12]

1. **Network-based intrusion prevention system (NIPS)**: monitors the entire network for suspicious traffic by analyzing protocol activity.
2. **Wireless intrusion prevention systems (WIPS)**: monitor a wireless network for suspicious traffic by analyzing wireless networking protocols.
3. **Network behavior analysis (NBA)**: examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware and policy violations.
4. **Host-based intrusion prevention system (HIPS)**: an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host.

30.3.2 Detection methods

The majority of intrusion prevention systems utilize one of three detection methods: signature-based, statistical anomaly-based, and stateful protocol analysis.*[9]*:301*[13]

1. **Signature-Based Detection**: Signature based IDS monitors packets in the Network and compares with pre-configured and pre-determined attack patterns known as signatures.
2. **Statistical anomaly-based detection**: An IDS which is anomaly based will monitor network traffic and compare it against an established baseline. The baseline will identify what is “normal” for that network – what sort of bandwidth is generally used and what protocols are used. It may however, raise a False Positive alarm for legitimate use of bandwidth if the baselines are not intelligently configured.*[14]
3. **Stateful Protocol Analysis Detection**: This method identifies deviations of protocol states by comparing observed events with “predetermined profiles of generally accepted definitions of benign activity” .*[9]

30.4 Limitations

- **Noise** can severely limit an intrusion detection system's effectiveness. Bad packets generated from software bugs, corrupt DNS data, and local packets that escaped can create a significantly high false-alarm rate.*[15]
- It is not uncommon for the number of real attacks to be far below the number of false-alarms. Number of real attacks is often so far below the number of false-alarms that the real attacks are often missed and ignored.*[15]
- Many attacks are geared for specific versions of software that are usually outdated. A constantly changing library of signatures is needed to mitigate threats. Outdated signature databases can leave the IDS vulnerable to newer strategies.*[15]
- For signature-based IDSEs there will be lag between a new threat discovery and its signature being applied to the IDS. During this lag time the IDS will be unable to identify the threat.*[14]

- It cannot compensate for a weak identification and authentication mechanisms or for weaknesses in network protocols. When an attacker gains access due to weak authentication mechanism then IDS cannot prevent the adversary from any malpractice.
- Encrypted packets are not processed by most intrusion detection devices. Therefore, the encrypted packet can allow an intrusion to the network that is undiscovered until more significant network intrusions have occurred.
- Intrusion detection software provides information based on the network address that is associated with the IP packet that is sent into the network. This is beneficial if the network address contained in the IP packet is accurate. However, the address that is contained in the IP packet could be faked or scrambled.
- Due to the nature of NIDS systems, and the need for them to analyse protocols as they are captured, NIDS systems can be susceptible to same protocol based attacks that network hosts may be vulnerable. Invalid data and TCP/IP stack attacks may cause an NIDS to crash.*[16]

30.5 Evasion techniques

Main article: [Intrusion detection system evasion techniques](#)

There are a number of techniques which attackers are using, the following are considered 'simple' measures which can be taken to evade IDS:

- Fragmentation: by sending fragmented packets, the attacker will be under the radar and can easily bypass the detection system's ability to detect the attack signature.
- Avoiding defaults: The TCP port utilised by a protocol does not always provide an indication to the protocol which is being transported. For example, an IDS may expect to detect a trojan on port 12345. If an attacker had reconfigured it to use a different port the IDS may not be able to detect the presence of the trojan.
- Coordinated, low-bandwidth attacks: coordinating a scan among numerous attackers (or agents) and allocating different ports or hosts to different attackers makes it difficult for the IDS to correlate the captured packets and deduce that a network scan is in progress.
- Address spoofing/proxying: attackers can increase the difficulty of the ability of Security Administrators to determine the source of the attack by using poorly secured or incorrectly configured proxy servers to bounce an attack. If the source is spoofed and bounced by a server then it makes it very difficult for IDS to detect the origin of the attack.
- Pattern change evasion: IDSs generally rely on 'pattern matching' to detect an attack. By changing the data used in the attack slightly, it may be possible to evade detection. For example, an Internet Message Access Protocol (IMAP) server may be vulnerable to a buffer overflow, and an IDS is able to detect the attack signature of 10 common attack tools. By modifying the payload sent by the tool, so that it does not resemble the data that the IDS expects, it may be possible to evade detection.

30.6 Development

The earliest preliminary IDS concept was delineated in 1980 by James Anderson at the National Security Agency and consisted of a set of tools intended to help administrators review audit trails.*[17] User access logs, file access logs, and system event logs are examples of audit trails.

Fred Cohen noted in 1987 that it is impossible to detect an intrusion in every case, and that the resources needed to detect intrusions grow with the amount of usage.*[18]

Dorothy E. Denning, assisted by Peter G. Neumann, published a model of an IDS in 1986 that formed the basis for many systems today.*[19] Her model used statistics for anomaly detection, and resulted in an early IDS at SRI International named the Intrusion Detection Expert System (IDES), which ran on Sun workstations and could consider both user and network level data.*[20] IDES had a dual approach with a rule-based Expert System to detect known types of intrusions plus a statistical anomaly detection component based on profiles of users, host systems, and target

systems. Lunt proposed adding an Artificial neural network as a third component. She said all three components could then report to a resolver. SRI followed IDES in 1993 with the Next-generation Intrusion Detection Expert System (NIDES).^{*[21]}

The Multics intrusion detection and alerting system (MIDAS), an expert system using P-BEST and Lisp, was developed in 1988 based on the work of Denning and Neumann.^{*[22]} Haystack was also developed in that year using statistics to reduce audit trails.^{*[23]}

In 1986 the National Security Agency started an IDS research transfer program under Rebecca Bace. Bace later published the seminal text on the subject, *Intrusion Detection*, in 2000.^{*[24]}

Wisdom & Sense (W&S) was a statistics-based anomaly detector developed in 1989 at the Los Alamos National Laboratory.^{*[25]} W&S created rules based on statistical analysis, and then used those rules for anomaly detection.

In 1990, the Time-based Inductive Machine (TIM) did anomaly detection using inductive learning of sequential user patterns in Common Lisp on a VAX 3500 computer.^{*[26]} The Network Security Monitor (NSM) performed masking on access matrices for anomaly detection on a Sun-3/50 workstation.^{*[27]} The Information Security Officer's Assistant (ISOA) was a 1990 prototype that considered a variety of strategies including statistics, a profile checker, and an expert system.^{*[28]} ComputerWatch at AT&T Bell Labs used statistics and rules for audit data reduction and intrusion detection.^{*[29]}

Then, in 1991, researchers at the University of California, Davis created a prototype Distributed Intrusion Detection System (DIDS), which was also an expert system.^{*[30]} The Network Anomaly Detection and Intrusion Reporter (NADIR), also in 1991, was a prototype IDS developed at the Los Alamos National Laboratory's Integrated Computing Network (ICN), and was heavily influenced by the work of Denning and Lunt.^{*[31]} NADIR used a statistics-based anomaly detector and an expert system.

The Lawrence Berkeley National Laboratory announced Bro in 1998, which used its own rule language for packet analysis from libpcap data.^{*[32]} Network Flight Recorder (NFR) in 1999 also used libpcap.^{*[33]} APE was developed as a packet sniffer, also using libpcap, in November, 1998, and was renamed Snort one month later. APE has since become the world's largest used IDS/IPS system with over 300,000 active users.^{*[34]}

The Audit Data Analysis and Mining (ADAM) IDS in 2001 used tcpdump to build profiles of rules for classifications.^{*[35]} In 2003, Yongguang Zhang and Wenke Lee argue for the importance of IDS in networks with mobile nodes.^{*[36]}

In 2015, Viegas and his colleagues^{*[37]} proposed an anomaly-based intrusion detection engine, aiming System-on-Chip (SoC) for applications in Internet of Things (IoT), for instance. The proposal applies machine learning for anomaly detection, providing energy-efficiency to a Decision Tree, Naive-Bayes, and k-Nearest Neighbors classifiers implementation in an Atom CPU and its hardware-friendly implementation in a FPGA.^{*[38]}^{*[39]} In the literature, this was the first work that implement each classifier equivalently in software and hardware and measures its energy consumption on both. Additionally, it was the first time that was measured the energy consumption for extracting each features used to make the network packet classification, implemented in software and hardware.^{*[40]}

30.7 Free and open source systems

- ACARM-ng
- AIDE
- Bro NIDS
- Fail2ban
- OSSEC HIDS
- Prelude Hybrid IDS
- Sagan
- Samhain
- Snort
- Suricata

30.8 See also

- Application protocol-based intrusion detection system (APIDS)
- Artificial immune system
- Bypass switch
- Denial-of-service attack
- DNS analytics
- Intrusion Detection Message Exchange Format
- Protocol-based intrusion detection system (PIDS)
- Real-time adaptive security
- Security management
- Software-defined protection

30.9 References

- [1] Abdullah A. Mohamed, “Design Intrusion Detection System Based On Image Block Matching”, International Journal of Computer and Communication Engineering, IACSIT Press, Vol. 2, No. 5, September 2013.
- [2] Brandon Lokesak (December 4, 2008). “A Comparison Between Signature Based and Anomaly Based Intrusion Detection Systems” (PPT). www.iup.edu.
- [3] “Gartner report: Market Guide for User and Entity Behavior Analytics”. September 2015.
- [4] “Gartner: Hype Cycle for Infrastructure Protection, 2016” .
- [5] “Gartner: Defining Intrusion Detection and Prevention Systems” . Retrieved September 20, 2016.
- [6] Scarfone, Karen; Mell, Peter (February 2007). “Guide to Intrusion Detection and Prevention Systems (IDPS)” (PDF). *Computer Security Resource Center*. National Institute of Standards and Technology (800–94). Retrieved 1 January 2010.
- [7] “NIST – Guide to Intrusion Detection and Prevention Systems (IDPS)” (PDF). February 2007. Retrieved 2010-06-25.
- [8] Robert C. Newman (19 February 2009). *Computer Security: Protecting Digital Resources*. Jones & Bartlett Learning. ISBN 978-0-7637-5994-0. Retrieved 25 June 2010.
- [9] Michael E. Whitman; Herbert J. Mattord (2009). *Principles of Information Security*. Cengage Learning EMEA. ISBN 978-1-4239-0177-8. Retrieved 25 June 2010.
- [10] Tim Boyles (2010). *CCNA Security Study Guide: Exam 640-553*. John Wiley and Sons. p. 249. ISBN 978-0-470-52767-2. Retrieved 29 June 2010.
- [11] Harold F. Tipton; Micki Krause (2007). *Information Security Management Handbook*. CRC Press. p. 1000. ISBN 978-1-4200-1358-0. Retrieved 29 June 2010.
- [12] John R. Vacca (2010). *Managing Information Security*. Syngress. p. 137. ISBN 978-1-59749-533-2. Retrieved 29 June 2010.
- [13] Engin Kirda; Somesh Jha; Davide Balzarotti (2009). *Recent Advances in Intrusion Detection: 12th International Symposium, RAID 2009, Saint-Malo, France, September 23–25, 2009, Proceedings*. Springer. p. 162. ISBN 978-3-642-04341-3. Retrieved 29 June 2010.
- [14] nitin.; Mattord, verma (2008). *Principles of Information Security*. Course Technology. pp. 290–301. ISBN 978-1-4239-0177-8.
- [15] Anderson, Ross (2001). *Security Engineering: A Guide to Building Dependable Distributed Systems*. New York: John Wiley & Sons. pp. 387–388. ISBN 978-0-471-38922-4.
- [16] <http://www.giac.org/paper/gsec/235/limitations-network-intrusion-detection/100739>

- [17] Anderson, James P., "Computer Security Threat Monitoring and Surveillance," Washing, PA, James P. Anderson Co., 1980.
- [18] David M. Chess; Steve R. White (2000). "An Undetectable Computer Virus". *Proceedings of Virus Bulletin Conference*.
- [19] Denning, Dorothy E., "An Intrusion Detection Model," Proceedings of the Seventh IEEE Symposium on Security and Privacy, May 1986, pages 119–131
- [20] Lunt, Teresa F., "IDES: An Intelligent System for Detecting Intruders," Proceedings of the Symposium on Computer Security; Threats, and Countermeasures; Rome, Italy, November 22–23, 1990, pages 110–121.
- [21] Lunt, Teresa F., "Detecting Intruders in Computer Systems," 1993 Conference on Auditing and Computer Technology, SRI International
- [22] Sebring, Michael M., and Whitehurst, R. Alan., "Expert Systems in Intrusion Detection: A Case Study," The 11th National Computer Security Conference, October, 1988
- [23] Smaha, Stephen E., "Haystack: An Intrusion Detection System," The Fourth Aerospace Computer Security Applications Conference, Orlando, FL, December, 1988
- [24] McGraw, Gary (May 2007). "Silver Bullet Talks with Becky Bace" (PDF). *IEEE Security & Privacy Magazine*. 5 (3): 6–9. doi:10.1109/MSP.2007.70. Retrieved 18 April 2017.
- [25] Vaccaro, H.S., and Liepins, G.E., "Detection of Anomalous Computer Session Activity," The 1989 IEEE Symposium on Security and Privacy, May, 1989
- [26] Teng, Henry S., Chen, Kaihu, and Lu, Stephen C-Y, "Adaptive Real-time Anomaly Detection Using Inductively Generated Sequential Patterns," 1990 IEEE Symposium on Security and Privacy
- [27] Heberlein, L. Todd, Dias, Gihan V., Levitt, Karl N., Mukherjee, Biswanath, Wood, Jeff, and Wolber, David, "A Network Security Monitor," 1990 Symposium on Research in Security and Privacy, Oakland, CA, pages 296–304
- [28] Winkeler, J.R., "A UNIX Prototype for Intrusion and Anomaly Detection in Secure Networks," The Thirteenth National Computer Security Conference, Washington, DC., pages 115–124, 1990
- [29] Dowell, Cheri, and Ramstedt, Paul, "The ComputerWatch Data Reduction Tool," Proceedings of the 13th National Computer Security Conference, Washington, D.C., 1990
- [30] Snapp, Steven R, Brentano, James, Dias, Gihan V., Goan, Terrance L., Heberlein, L. Todd, Ho, Che-Lin, Levitt, Karl N., Mukherjee, Biswanath, Smaha, Stephen E., Grance, Tim, Teal, Daniel M. and Mansur, Doug, "DIDS (Distributed Intrusion Detection System) -- Motivation, Architecture, and An Early Prototype," The 14th National Computer Security Conference, October, 1991, pages 167–176.
- [31] Jackson, Kathleen, DuBois, David H., and Stallings, Cathy A., "A Phased Approach to Network Intrusion Detection," 14th National Computing Security Conference, 1991
- [32] Paxson, Vern, "Bro: A System for Detecting Network Intruders in Real-Time," Proceedings of The 7th USENIX Security Symposium, San Antonio, TX, 1998
- [33] Amoroso, Edward, "Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response," *Intrusion.Net Books*, Sparta, New Jersey, 1999, ISBN 0-9666700-7-8
- [34] Kohlenberg, Toby (Ed.), Alder, Raven, Carter, Dr. Everett F. (Skip), Jr., Esler, Joel., Foster, James C., Jonkman Marty, Raffael, and Poor, Mike, "Snort IDS and IPS Toolkit," Syngress, 2007, ISBN 978-1-59749-099-3
- [35] Barbara, Daniel, Couto, Julia, Jajodia, Sushil, Popyack, Leonard, and Wu, Ningning, "ADAM: Detecting Intrusions by Data Mining," Proceedings of the IEEE Workshop on Information Assurance and Security, West Point, NY, June 5–6, 2001
- [36] Intrusion Detection Techniques for Mobile Wireless Networks, ACM WINET 2003 <<http://www.cc.gatech.edu/~{}wenke/papers/winet03.pdf>>
- [37] Viegas, E.; Santin, A. O.; Fran?a, A.; Jasinski, R.; Pedroni, V. A.; Oliveira, L. S. (2017-01-01). "Towards an Energy-Efficient Anomaly-Based Intrusion Detection Engine for Embedded Systems". *IEEE Transactions on Computers*. 66 (1): 163–177. ISSN 0018-9340. doi:10.1109/TC.2016.2560839.
- [38] Fran a, A. L.; Jasinski, R.; Cemin, P.; Pedroni, V. A.; Santin, A. O. (2015-05-01). "The energy cost of network security: A hardware vs. software comparison". *2015 IEEE International Symposium on Circuits and Systems (ISCAS)*: 81–84. doi:10.1109/ISCAS.2015.7168575.

- [39] França, A. L. P. d; Jasinski, R. P.; Pedroni, V. A.; Santin, A. O. (2014-07-01). “Moving Network Protection from Software to Hardware: An Energy Efficiency Analysis” . *2014 IEEE Computer Society Annual Symposium on VLSI*: 456–461. doi:10.1109/ISVLSI.2014.89.
- [40] “Towards an Energy-Efficient Anomaly-Based Intrusion Detection Engine for Embedded Systems” (PDF). *SecPLab*.

This article incorporates public domain material from the National Institute of Standards and Technology document “Guide to Intrusion Detection and Prevention Systems, SP800-94” by Karen Scarfone, Peter Mell (retrieved on 1 January 2010).

30.10 Further reading

- Bace, Rebecca Gurley (2000). *Intrusion Detection*. Indianapolis, IN: Macmillan Technical. ISBN 1578701856.
- Bezroukov, Nikolai (11 December 2008). “Architectural Issues of Intrusion Detection Infrastructure in Large Enterprises (Revision 0.82)”. Softpanorama. Retrieved 30 July 2010.
- P.M. Mafra and J.S. Fraga and A.O. Santin (2014). “Algorithms for a distributed IDS in MANETs” . *Journal of Computer and System Sciences*. **80** (3): 554–570. doi:10.1016/j.jcss.2013.06.011.
- Hansen, James V.; Benjamin Lowry, Paul; Meservy, Rayman; McDonald, Dan (2007). “Genetic programming for prevention of cyberterrorism through dynamic and evolving intrusion detection” . *Decision Support Systems (DSS)*. **43** (4): 1362–1374. SSRN 877981  doi:10.1016/j.dss.2006.04.004.
- Scarfone, Karen; Mell, Peter (February 2007). “Guide to Intrusion Detection and Prevention Systems (IDPS)” (PDF). *Computer Security Resource Center*. National Institute of Standards and Technology (800-94). Retrieved 1 January 2010.
- Saranya, J.; Padmavathi, G. (2015). “A Brief Study on Different Intrusions and Machine Learning-based Anomaly Detection Methods in Wireless Sensor Networks” (PDF). *Avinashilingam Institute for Home Science and Higher Education for Women* (6(4)). Retrieved 4 April 2015.
- Singh, Abhishek. “Evasions In Intrusion Prevention Detection Systems” . Virus Bulletin. Retrieved 1 April 2010.

30.11 External links

- Intrusion Detection Systems at DMOZ
- Common vulnerabilities and exposures (CVE) by product
- NIST SP 800-83, Guide to Malware Incident Prevention and Handling
- NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS)
- Study by Gartner “Magic Quadrant for Network Intrusion Prevention System Appliances”

Chapter 31

Mobile secure gateway

Mobile secure gateway (MSG) is an industry term for the software or hardware appliance that provides secure communication between a mobile application and respective backend resources typically within a corporate network. It addresses challenges in the field of **mobile security**.

MSG is typically composed of two components - Client library and Gateway. The client is a library that is linked with the mobile application. It establishes secure connectivity to Gateway using cryptographic protocol typically **SSL/TLS**. This represents a secured channel used for communication between the mobile application and hosts. Gateway separates internal IT infrastructure from the Internet, allowing only an authorized client requests to reach a specific set of hosts inside restricted network.

31.1 Client library

The Client **library** is linked with the corresponding **mobile application**, and that provides secure access via the **Gateway** to the set of Hosts. The Client library exposes public **API** to the mobile application, mimicking platform default **HTTP** client library. The application uses this API to communicate with the desired hosts in a secure way.

31.2 Gateway

Gateway is a server or **daemon** typically installed onto physical or virtual appliance placed into **DMZ**. Gateway public interface is exposed to the Internet (or other untrusted network) and accepts **TCP/IP** connections from mobile applications. It operates on **IPv4** and/or **IPv6** networks. Incoming client connections typically use **SSL/TLS** to provide security for the network communication and a mutual trust of communicating peers. Communication protocol is typically based on **HTTP**.*[1]

31.3 Host

Gateway forwards requests from connected apps to a collection of configured hosts. These are typically **HTTP** or **HTTPS** servers or services within an internal network. The response from a host is sent back to the respective mobile app.

31.4 References

[1] “Mobile Security” . www.peerlyst.com. Retrieved 6 May 2016.

31.5 External links

- Mobile Secure Gateway description on TeskaLabs.
- Mobile Secure Gateway description on Symantec.

31.6 Text and image sources, contributors, and licenses

31.6.1 Text

- **Information security Source:** https://en.wikipedia.org/wiki/Information_security?oldid=794455860 *Contributors:* Tuxisuaa, The Anome, Khendon, William Avery, Ant, Hephaestos, Edward, Madvenu, JohnOwens, Michael Hardy, Kku, SebastianHelm, Ronz, Angela, Marteau, Nikai, Andrewman327, Itai, LMB, ZeWrestler, Chrisbrown, Joy, Vaceituno, Kimvais, Saqib (usurped)-enwiki, Chealer, Fredrik, Rurus, Adhemar, HaeB, Centrx, Inkling, Peruvianllama, Wikibob, Falcon Kirtaran, Matt Crypto, Edcolins, Utcursh, Andycjp, LiDaobing, Alex Cohn, Sfoskett, Sam Hocevar, Xinconnu, Imjustmatthew, Ohka-, Klemen Kocjancic, Mike Rosoft, Shiftchange, Rich Farmbrough, Rhobite, Wrp103, Sperling, Pnevares, Violetriga, Danakil, MBisanz, El C, Spearhead, Bobo192, John Vandenberg, Wiki-Ed, Giraffedata, Grutness, Guy Harris, Davebailey, Revmachine21, Sutch, Wtmitchell, Suruena, Amorymeltzer, RainbowOfLight, SteinbDJ, Chris Brown, Kbolino, Bobrayner, Nuno Tavares, Woohookitty, Mindmatrix, Tabletop, SDC, Btyner, Mandarax, Graham87, BD2412, Qwertytus, Foulter, Rjwilmsi, Pleiotrop3, The wub, Aapo Laitinen, JdforresterBot, GüniX, RexNL, Intgr, Lmatt, DVdm, Bgwhite, GroupOne, YurikBot, Borgx, RobotE, RussBot, Stephenb, Gaius Cornelius, Ptomes, Rsrikanth05, AlMac, Irishguy, DeadEyeArrow, Mitte, Mcicogni, Bill.martin, Awillcox, Closedmouth, CharlesHBennett, GraemeL, Rearden9, Ajuk, Whouk, Tom Morris, SmackBot, Glavin, Grye, CommodoCast, Bburton, Mauls, Ohnoitsjamie, JorgePeixoto, Chris the speller, Chris Ulbrich, MK8, George Rodney Maruri Game, Wikipediatrix, Kungming2, DHN-bot-enwiki, Colonies Chris, CelebritySecurity, JonHarder, Addshore, Jdlambert, Richard001, Mistress Selina Kyle, KizzoGirl, Kuru, Noah Salzman, Kvng, Hu12, DouglasCalvert, Iridescent, Xsmith, Wilcho, IvanLanin, Mlichter, CmdrObot, Ale jrb, Alexconlin, Gfragkos, Mike0131, Robwhitcher, John Yesberg, Puntarenus, UncleBubba, Riker2000, Tenbergen, Alucard (Dr.), Dancer, Nunewsco, Csrcyborg, Epbr123, RickinBaltimore, Wmasterj, Dawnseeker2000, Jpluser, AntiVandalBot, Widefox, Obiwankenobi, Seaphoto, Rossj81, Eddy Scott, Esmond.pitt, MikeLynch, JAnDbot, MER-C, Kitdaddio, Tqbf, Magioladitis, Ishikawa Minoru, Dekimasu, Ged fi, Think outside the box, Richard Bartholomew, Nyttend, Aka042, Morpheus063, AlephGamma, Brwriter2, Thireus, Gomm, Kozmando, JaGa, CliffC, Jim.henderson, Jstaryuk, Ranman45, Anaxial, CommonsDelinker, Fellwalker57, Ali, Uncle Dick, Theo Mark, INFOSECFORCE, Mathglot, BrWriter2006, Adamdaley, Evb-wiki, Yakheart, Cralar, Soliloquial, Emergentchaos, NoticeBored, WideClyde, HansWDaniel, Sa ashok, Happyrose, UriBraun, Beta7, Aclyon, OKMInfoSec, Liko81, Shanata, Falcon8765, Enviroboy, Truesestate, Cartermichael, Rgalexander, Farcaster, Finnring, Amatriain, Rlendog, Derekslater, Gerakibot, Ml-crest, MerileeNC, Sephiroth storm, Alanpc1, JohnManuel, Flyer22 Reborn, JCLately, ObscurO, Corp Vision, Vbscript2, Kieraf-enwiki, Denisarona, Martarius, ClueBot, Shonharris, Kl4m, Huther, Vinodvmenon, The Thing That Should Not Be, Donalcampbell, Plastiksfolk, Little saturn, VQuakr, Mild Bill Hiccup, PolarYukon, V1ntage318, Ktr101, Eekster, Sun Creator, WalterGR, Colemannick, Prokopenya Viktor, DanielPharos, Aitias, Scgilardi, Portal60, Bearsona, XLinkBot, FTsafe, Scottdimmick, Sakura Cartelet, Wingfamily, Cupids wings, Addbot, Nitinbhogan, Stuartfost, PatrickFlaherty, Open4Ever-enwiki, Leszek Jałczuk, MrOllie, Jmligram, Gpdhillon2, Sbilly, Ramfoss, Tassedethe, Calm reason, SasiSasi, Jarble, Fryed-peach, Sfoak, Luckas-bot, Yobot, Fraggie81, Idumont, Cfim001, Evans1982, Canoruo, Sweerek, Stevedaily, AnomieBOT, Cdschuett, DemocraticLuntz, Jim1138, Piano non troppo, Elieb001, Apau98, Quantumseven, Materialscientist, Citation bot, Aneah, Eumolpo, Stationcall, RealityApologist, LilHelpa, Delmundo.averganzado, Fancy steve, Grantgw, GrouchoBot, Favertama, Aron.j.j, Prunesqualer, Mattg82, Kernel.package, Mathonius, Choibg, TarseeRota, Shadowjams, Umbrussels, Breadtk, Thehelpfulbot, Cascadeuse, Srandaman, FrescoBot, Nageh, Itusg15q4user, Ionutmovie, Nainawalli, Haeinous, Raed abu farha, JIK1975, Infinitesteps, I dream of horses, Abductive, Shawne, Cpaidhrin, Feldermouse, Hoo man, MastiBot, Mdjang, Hnguyen322, FoxBot, Dobradavid, Prowriter16, Lotje, Himugk, Brian the Editor, DARTH SIDIOUS 2, Mean as custard, RjwilmsiBot, Docpd, VernoWhitney, Alexandru47, DRAGON BOOSTER, Ioliver2, MeS2135, EmausBot, John of Reading, AChrisTurner, WikitanvirBot, امدادج, Timtempleton, Abyss of enchantment, Akjar13, Dkosutic, Primefac, Inthenet, GoingBatty, Klbrain, Cmlloyd1969, K6ka, Mz7, Vanished user wijnm4oj3t8hsafclkwhd2l4tg4, Manasprakash79, Mattatpredictive, Kilopi, Staszek Lem, TyA, Dcressb, 111Alpha, Donner60, Alexttcn, Puffin, Pastore Italy, GrayFullbuster, Bzwas, Jramio, ClueBot NG, Satellizer, MosaicSecurity, Frietjes, Sonakshi87, Itscepardis, Asukite, Saluki2001, Widr, Helpful Pixie Bot, Strike Eagle, Wbm1058, BG19bot, Vdmerwe.johann, JaredPoepelman, Jobin RV, Saurav kashyap, Richu jose, BattyBot, BKD-Banker\$, Pratyaya Ghosh, MSS. Selina Kyle, Dtruonggwhs, Cyberbot II, ChrisGualtieri, Pspagnoletti, Scar123, BooleanMaybe, Dexbot, Codename Lisa, Mogism, 2edsphere, RazrRekr201, Patrick.bausemer, Pete Mahen, Lugia2453, Aperks1811, Anotherderelict, Me, Myself, and I are Here, Phamnhatkhanh, Param21, Zeromadcowz, Shebang42, Pdecalculus, Rakomwolvesbane, Kolbeinik, Tentinator, Postonm, Tsarihan, Pkleinr, Mldisch, Reenaiit, Sparkau, JWNoctis, Malmoe7, Rons corner, Sukhamoyana, Fixture, Ittybittytittykitty, Wikilubina, Desire cilow, Saectar, Kate Lynn, Amgauna, Monkbot, Neilcame9978, Greedo8, S166865h, VeniVidiVikipedia, Hannasnow, ScienceGuard, Amatimoldwiki, 405Duke, Nitinkathuria80, Thetechgirl, TranquilHope, Manish9050, Raaj.ajm, Datasecurity, Julietdeltalima, Meletisb, Eeethan, Samkel95, Manikaran.singh, Godfarther48, Supdiop, Informationsecurityprofessional, Informationsystemgeeks, Oluwa2Chainz, DarkSocrates, Latosh Boris, RSTumber, InternetArchiveBot, Lo.tiffany97, GreenC bot, SamsungflWSamsung, Gulumeemee, RainFall, Bullaful, Walangtao, Cookiestan, Murkl, Hossainjubayer, Gere-myBenkirane, Jamal Millwood and Anonymous: 558
- **Internet security Source:** https://en.wikipedia.org/wiki/Internet_security?oldid=793529303 *Contributors:* Aarontay, Evgeni Sergeev, ZeWrestler, Tuomas, HaeB, Frencheigh, AlistairMcMillan, Matt Crypto, SWAdair, Wmahan, CaribDigita, Elroch, TonyW, Discospinster, Rich Farmbrough, KneeLess, Xezbeth, JoeSmack, CanisRufus, *drew, MBisanz, Apollo2011, La goutte de pluie, Minghong, Pearle, Smoothy, Wtmitchell, Jim Mikulak, Versageek, Bsdlogical, Johntex, Mindmatrix, Deltabeignet, Kevinkinnett, Willangford, Vary, Gurch, Vec, Intgr, Chobot, DVdm, Bgwhite, Peterl, Elf guy, Wavelength, Argav, Alan216, Phantomsteve, Sarranduin, Akamat, Stephenb, Pseudomonas, Moa Epsilon, Amcfreely, HopeSeekr of xMule, S33k3r, KGasso, Th1rt3en, GraemeL, Thespian, DoriSmith, LSnK, Carlosguitar, Draicone, KnowledgeOfSelf, McGeddon, Verne Equinox, Jjalexand, Thumperward, N2f, Baa, Can't sleep, clown will eat me, Frap, Tewolf, Nixeagle, JonHarder, Rrburke, Parent5446, Ianmacm, Mistress Selina Kyle, Ninnnu-enwiki, A. Parrot, Beetstra, Ehheh, A Clown in the Dark, Mere Mortal, FleetCommand, CmdrObot, Equendil, Cydebot, Gogo Dodo, Tiger williams, ErrantX, Wikid77, Edupedro, Mojo Hand, John254, Dawnseeker2000, Obiwankenobi, Jerrypcj, SiobhanHansa, Raanoo, Io Katai, Magioladitis, Gstroot, JohnLai, 28421u2232nfencenc, Gomm, Stephenchou0722, CliffC, Sjjupadhyay-enwiki, Lutz.hausmann, Trusilver, Jessant13, Dbiel, JudyJohn, WikiBone, Karrade, Sbunker, Wiki-ay, Philip Trueman, Oshawah, Zifert, Natg 19, Bryan.dollery, Dirkbb, Mr Nic, LittleBenW, Debog, Kbrose, SieBot, WereSpielChequers, Caltas, DaBler, Bananastalktome, Oxymoron83, Jruderman, Fornaeffe, Yuva raju raj, ClueBot, DavidGGG, The Thing That Should Not Be, EoGuy, Mild Bill Hiccup, Anapazapa, Excirial, Dcampbell30, Spock of Vulcan, Arjayay, La Pianista, Versus22, DumZiBoT, XLinkBot, Mitch Ames, Good Olfactory, Addbot, Xp54321, Mortense, Grayfell, Debsalmi, Kongr43gen, CanadianLinuxUser, Chzz, Yobot, QueenCake, AnomieBOT, DemocraticLuntz, lexec1, JDavis680, AdjustShift, Bestija11, Ulric1313, Materialscientist, Waltzmoore66, Citation bot, ArthurBot, Itbuddy, LilHelpa, TheAMmollusc, Mgf12rw, Nasnema, Craftyminion, BritishWatcher, S0aaasd2sf, Seldridge99, Fjollig arme, FrescoBot, Nageh, Chevymontecarlo, D'ohBot, A little insignificant, HamburgerRadio, Singaporesuperboy, DrilBot, Smeago, Jusses2, In3go, Piandcompany, Jujutacular, Cnwilliams, Intsafetycenter,

Train2104, Lotje, Vrenator, TBloemink, DARTH SIDIOUS 2, Mean as custard, VernoWhitney, EmausBot, WikitanvirBot, Timtempleton, Andyyype, Zollerriia, Dcirovic, K6ka, MathMaven, 30, Riittaajo, Fæ, Zloyvolsheb, Enikuo, SporkBot, Rameez-NJITWILL, W163, Sbmeirow, Donner60, Autoerrant, Tyros1972, ChuispastonBot, Humanetwork, Makeet, 28bot, ClueBot NG, Snocman, Cntras, Widr, Karl 334, Helpful Pixie Bot, Electriccatfish2, Titodutta, Jeraphine Gryphon, BG19bot, Mleoking, Muneeb2000, Altaïr, Valentinocourt, Cin316, RroccoMaroc, BKoteska, MeanMotherJr, Motta.allo, David.moreno72, Cyberbot II, Sakmaz, Dexbot, وَنْ اَبْشِرِي, Corn cheese, Palmbeachguy, The Mol Man, Tentinator, Wuerzele, Matty.007, PCRepairGuy, Gaodong, Mickel1982, Chenthilvelmurugana, SiavooshPayandehAzad, Thisara1990, BrettofMoore, Mitzi.humphrey, SandorSchwartz, Joewalter, Greenmow, XamieA, Mathewherz, Adam9007, AmberHenely, Chenthil Vel, Srilekha selva, Sharanyanaveen, Simplexity22, DatGuy, Qzd, Philipheight, Thinusnua, GreenC bot, Robrobrob2, Neetiwariesh, Bender the Bot, Antoicaiza, PrimeBOT, GenericDNA, Nevint, Phi11ip, BreakerOfChainz and Anonymous: 334

- **Cyberwarfare** *Source:* <https://en.wikipedia.org/wiki/Cyberwarfare?oldid=794312385> *Contributors:* The Anome, Edward, Paul A, Conti, Tpbradbury, Jredmond, Donreed, Nurg, Ancheta Wis, Tom harrison, Gracefool, Utcursch, Slowking Man, Beland, AndrewKeenan-Richardson, Neutrality, Orange Goblin, Openfly, Rich Farmbrough, Wikiacc, Kzzl, Bender235, Pk2000, TheMile, Devil Master, Bobo192, Giraffedata, Obradovic Goran, YDZ, Dominic, H2g2bob, Johntex, Bobrayner, Richard Arthur Norton (1958-), Woohookitty, Mindmatrix, Rbcwa, JeffUK, Plrk, Paxsimius, BD2412, Rjwilmsi, Friejose, Qqqqqq, Nihiltres, Vsion, Lmatt, Chobot, Benlisquare, Bgwhite, Wavelength, RussBot, WritersCramp, ONEder Boy, CecilWard, Neil.steiner, Neurotoxic, Tony1, Deku-shrub, Eclipsed, Kal-El, Inter-shark, Gregzeng, Arthur Rubin, Geoffrey.landis, Katieh5584, SmackBot, Mmernex, Rtc, McGeddon, C.Fred, Chris the speller, Blue-bot, H2ppyme, Snori, Mordantkitten, Frap, Radagast83, Abmac, Yulia Romero, Uriel-238, Daveschroeder, Ohconfucius, WngLdr34, Mathiasrex, Robofish, NYCJosh, Hvn0413, DL2000, Hu12, Levineps, Iridescent, Kenef0618, Joseph Solis in Australia, Octane, Quod-fui, CmdrObot, Ale jrB, Zarex, TVC 15, Neelix, NathanDahlin, Old port, Bobblehead, Hcob, Nick Number, DPdH, Dawnseeker2000, Alphachimpbot, VictorAnyakin, NByz, ClassicSC, Turgidson, MER-C, SiobhanHansa, Geniac, Magioladitis, Bongwarrior, Flayer, Buckshot06, BilCat, XMog, Esanchez7587, Bytecount, Hbent, Atulsnischal, Sjjupadhyay-enwiki, CommonsDelinker, KTo288, Billy Pilgrim, Teh dave, Maurice Carbonaro, Theo Mark, Hodja Nasreddin, Octopus-Hands, Andareed, Tukkek, Hillock65, Jevansen, TopGun, BernardZ, Tkgd2007, Ashcroftgm, Fences and windows, Pmedema, WazzaMan, Saibod, LeaveSleaves, Rsnbrgr, Staka, Meters, Falcon8765, B.L.A.Z.E, Oth, Kevinfromhk, Boulainvilliers, Kbrose, Moonriddengirl, Rockstone35, BStarky, Flyer22 Reborn, Avaarga, WannabeAmatureHistorian, Oxymoron83, Skinny87, Jericho347, Dillard421, RJ CG, Deciwill, Martarius, Chessy999, Niceguyedc, Trivialist, MasterXC, Gordon Ecker, Excirial, Nymf, Bvlax2005, Rhododendrites, Arjayay, Light show, DumZiBoT, Kgcoleman, Emdarraj, XLinkBot, Avoided, Scostigan, Jaanusele, Addbot, Fgnievinski, AkhtaBot, StereotypicalWizard, MrOllie, Spy-Ops, Green Squares, Blaylockjam10, Golf2232, 5 albert square, Myk60640, Lightbot, Jarble, Goodmanjoon, Suwa, آशीष મટનાગર, Luckas-bot, Yobot, Tohd8BohaithuGh1, Bruce404, Waqashsn, Millinski, AnomieBOT, Apollo1758, FeelSunny, 1exec1, Bsimmmons666, Jim1138, Mbeimcik, Ulric1313, Materialscientist, Aneah, ArthurBot, LilHelpa, Xqbot, Sionus, Capricorn42, Dondiw, DJWolfy, Alexander Mclean, Wdl1961, BritishWatcher, Miguelito Vieira, Irwick, Peace2keeper, Crzer07, Pradameinhoff, What99999999333, Howsa12, Gordonrox24, Vihelik, Tanagram, FrescoBot, Russian Rocky, Tobby72, Sidna, Stanszyk, Remdarraj, Jersey92, Deadhorseflogging, HamburgerRadio, Pinethicket, I dream of horses, RedBot, Rochdalehornet, Full-date unlinking bot, Xeworlebi, Utility Monster, Mahimahi42, NFS-reloaded, Jonkerz, Lotje, Collegeofgolf, Oliver H, Remiked, Woodlot, Jfmantis, RjwilmsiBot, TjBot, VernoWhitney, Beyond My Ken, Lopifalko, Techhead7890, 09lamin, EmausBot, John of Reading, Ghostofnemo, SoAuthentic, Hirsutism, Kaiser1935, Rail88, Dewritech, GoingBatty, P@ddington, Cybercitizen123, Cowfman, Wikipelli, Dcirovic, K6ka, 7th sojourn, Unmourned, Sabres87, ZéroBot, Prayer-fortheworld, EneMsty12, Cymru.lass, Erianna, Quantumor, Quite vivid blur, GermanJoe, Joesolo13, Pastore Italy, Boundto, Dawid2009, Zabanio, Cat10001a, Paddingtonbaer, Pymansorl, ClueBot NG, Antrim Kate, Satellizer, Rawkage, BrekekekexKoaxKoax, Frietjes, Rezabot, Helpful Pixie Bot, Dukes08, BG19bot, M0rphzone, Paganinip, Marcopacelle, Donzae, Utkal Ranjan Sahoo, Cyffann, Jassy pal, Jayadevp13, David.moreno72, Cyberbot II, FosterHaven, Khazar2, Jabotito48, Mogism, Freshjane0, Dileeppp89, Hellowns, Pahlevun, SFK2, ThatI guy77, Telfordbuck, Me, Myself, and I are Here, Dhruvpubby, Meltingwood, Kennethgeers, Madtee, Tentinator, Reziebear, TheJoeAlt, ArmbrustBot, Newuser2013, Rmj1, Wikiuser13, Reacher1989, Beastlymac, Kahtar, CFLaherty, Fixture, CrowJU2, Monkbot, Cybersecurity101, Arsonhussy99, Betyd, S166865h, ICPSGWU, ChamithN, Gragie123, Kashifs294, TheCoffeeAddict, Rubbish computer, Atvica, Kixean777, LCEwald, BlakeTS, Prinsgezinde, Nøkkenbuer, Alainsfeir2, Omancyd, RoadWarrior445, Barbara (WVS), Qzd, KGirTrucker81, GreenC bot, Hakuli, Bender the Bot, Callsignpink, 44alexsmith, Avataron, Tman1027, Drdiamond12, PvOberstein, Dividegeography, Magic links bot, AvalerionV and Anonymous: 273

- **Computer security** *Source:* https://en.wikipedia.org/wiki/Computer_security?oldid=793870428 *Contributors:* Tobias Hoevekamp, Derek Ross, Tuxisua, Brion VIBBER, Eloquence, Zardoz, Mav, Robert Merkel, The Anome, Stephen Gilbert, Taw, Arcade-enwiki, Graham Chapman, Dachshund, Arvindn, PierreAbbat, Fubar Obfuscō, SimonP, Ben-Zin-enwiki, Ant, Ark-enwiki, Heron, Dwheeler, Chuq, Iorek-enwiki, Frecklefoot, Edward, Michael Hardy, Pnm, Kku, Ixfd64, Dcljr, Dori, Arpingstone, CesarB, Haakon, Ronz, Snyoes, Yaronf, Nikai, Smatty, Qwert, Dwo, Mydogategodshat, Jengod, JidGom, Aarontay, Gingekerr, Taxman, Joy, Vaceituno, Khym Chanur, Pakaran, Robbot, Yas-enwiki, Fredrik, ZimZalaBim, Nur, Rursus, Texture, KellyCoinGuy, 2501-enwiki, Hadal, Tea2min, David Gerard, Honta, Wolf530, Tom harrison, Dratman, Mike40033, Siroxo, C17GMaster, Matt Crypto, SWAdair, Bobblewik, Wmahan, Mu, DavidBrooks, Geni, Antandrus, Beland, Mako098765, CSTAR, Thincat, GeoGreg, Marc Mongenet, Gcschoryu, Bobbyelliott, Joyous!, Bluefoxicy, Squash, Strbenjr, Mike Rosoft, Kmccoy, Shamino, Monkeyman, Pyrop, Rich Farmbrough, Rhobite, Leibniz, FT2, Jesper Laisen, ArnoldReinhold, YUL89YYZ, Jwalden, Zarutian, MeltBanana, Sperling, Bender235, ZeroOne, Moa3333, JoeSmack, Danakil, Omnifarious, Jensbn, El C, Joanjoc-enwiki, Marcok, Perspective, Spearhead, EurekaLott, Nigelj, Stesmo, Smalljim, Rvera-enwiki, Myria, Adrian-enwiki, Boredzo, ClementSeveillac, JohnnyDog, Poweroid, Alansohn, Quiggles, Arthena, Lightdarkness, Cdc, Mrholylebrain, Caesura, Gbeeker, Raarouf, Filx, Proton, M3tainfo, Suruena, HenkvD, 2mcm, Wikicaz, H2g2bob, Condor33-enwiki, Bsdlogical, John-tex, Dan100, Woohookitty, Daira Hopwood, Al E., Prashanthns, Zhen-Xjell, Palica, Kesla, Vininim, Graham87, Clapaucius, BD2412, Icey, Sjakkalle, Rjwilmsi, Seidenstud, Koavf, Guyd, DeadlyAssassin, Dookie-enwiki, Edgar, Oblivious, QuickFox, Kazrak, Ddawson, Ligulem, Smtuly, Aapo Laitinen, Ground Zero, GünniX, RexNL, Alvin-cs, BMF81, JonathanFreed, Jmorgan, J.Ammon, DVdm, Bgwhite, Hall Monitor, Digitalme, Gwernol, FrankTobia, Elf guy, Wavelength, NTBot-enwiki, Alan216, StuffOfInterest, Foxygirttamara, Stephenb, Gaius Cornelius, Ptomes, Morphh, Salsb, Wimt, Bachrach44, AlMac, Irishguy, Albedo, Rmky87, Amfreely, Deku-shrub, Romal, Peter Schmiedeskamp, Zzuuzz, Gorgonzilla, Papergrl, Arthur Rubin, Ka-Ping Yee, Juliano, GraemeL, Rlove, JoanneB, Whouk, NeilN, SkerHawx, SmackBot, Mmernex, Tripletmot, Reedy, KnowledgeOfSelf, TestPilot, Kosik, McGeddon, Stretch 135, Ccalvin, Man-junathbhatt, Zyxw, Yamaguchi 先生, Gilliam, Ohnoitsjamie, Skizzik, Lakshmin, Kurykh, Autarch, RDBrown, Snori, Miquonranger03, Deli nk, Jenny MacKinnon, Kungming2, Jonasyorg, Timothy Clemans, Frap, Ponnampalam, Nixeagle, KevM, JonHarder, Rrburke, Wine Guy, Cpt-enwiki, Krich, Ritchie333, Bslede, Richard001, Stor stark7, Newtonlee, Doug Bell, Harryboyles, Kuru, Geoinline, J 1982, Gobonobo, Disavian, Robofish, Joffeloff, Kwestin, Mr. Lefty, Beetstra, Jadams76, Ehheh, Boxflux, Kvng, Chadnibal, Wfgiuliano, Dthvt, IvanLaniin, DavidHOzAu, Lcamtuf, CmdrObot, Tional, ShelfSkewed, Michael B. Trausch, Phatom87, Cydebot, Mblumber, Future Perfect at Sunrise, Blackjackmagic, UncleBubba, Gogo Dodo, Anonymi, Anthonyhcole, GRevolution824, Clovis Sangrail, HitroMi-

lanese, SpK, Njan, Ebyabe, Thijs!bot, Epbr123, The Punk, Kpavery, Wistless, Oarchimondeo, Headbomb, RichardVeryard, EdJohnston, Nick Number, Druiloor, SusanLesch, Dawnseeker2000, I already forgot, Sheridbm, AntiVandalBot, Obiwankenobi, Shirt58, Marokwitz, Khhodges, Ellenaz, Manionc, Chill doubt, Dmerrill, SecurityGuy, JAnDbot, Jimothytrotter, Roving Wordslinger, Kaobear, Barek, MER-C, The Transhumanist, Technologyvoices, Tqbf, Dave Nelson, Acroterion, Raanoo, Magioladitis, VoABot II, Ukuser, JNW, Michi.bo, Szh~enwiki, Hubbardiae, Arcticf, Froid, JXS, AlephGamma, Rohasnagpal, Catgut, Whatamidoing, Marzoog, Gerrardperrett, Thireus, Devmem, Dharmadhyaksha, DerHexer, JaGa, Reseacord, XandroZ, Gwern, SolitaryWolf, CliffC, =JeffH, Sjjupadhyay~enwiki, Bertix, Booker.ercu, J.delanoy, Gam2121, Maurice Carbonaro, Theo Mark, Jesant13, Jreferee, JA.Davidson, Katalaveno, Gregbaker, Touisiau, Ansh1979, Toon05, Mufka, Largoplazo, Dubhe.sk, YoavD, Bonadea, Red Thrush, GrahamHardy, RJASE1, Cralar, Javeed Safai, ABF, Wiki-ay, Davidwr, Oshawah, Zifert, Crazypete101, Dictouray, Lollerwaffle, Shanata, Haseo9999, Falcon8765, Pctechbytes, Sapphic, Donnymo, FutureDomain, Farcaster, Smith bruce, Kbrose, JonnyJD, Lxicm, Whitehatnetizen, Jargonexpert, Laoris, SecurInfos~enwiki, Mi-crest, Immzw4, Sephiroth storm, Graceup, Yuxin19, Agilmore, JohnManuel, Flyer22 Reborn, Jojalozzo, Riya.agarwal, Corp Vision, Lightmouse, KathrynLybarger, Mscwriter, Soloxide, StaticGull, Capitalismojo, PabloStraub, Rinconsoleao, Denisarona, White Stealth, Ishisaka, WikipedianMarlith, Sfan00 IMG, Elassint, ClueBot, Shonharris, PipepBot, TransporterMan, Supertouch, Add32, Emantras, Tanglewood4, Mild Bill Hiccup, Niceguyedc, Dkonyko, Trivialist, Gordon Ecker, DragonBot, Dwcmsc, Excirial, Socrates2008, Dcampbell30, Moomoo987, Dr-Mx, Rbilesky, DanielPharos, Versus22, HarrivBOT, Fathisule, Raysecurity, XLinkBot, AgnosticPreachersKid, BodhisattvaBot, Solinym, Skarebo, Wingfamily, WikiDao, MystBot, Dsimic, JimWalker67, Jvtregli, Addbot, Non-dropframe, Cst17, MrOllie, Passport90, Favonian, Torla42, AgadaUrbanit, Tassedethe, Jarble, Ben Ben, Tartarus, Luckas-bot, Yobot, OrgasGirl, The Grumpy Hacker, Librsh, Cyanoa Crylate, DisillusionedBitterAndKnackered, Grammaton, THEN WHO WAS PHONE?, Dr Roots, Sweerek, AnomieBOT, JDavis680, Jim1138, Galoubet, Dwayne, Piano non troppo, AdjustShift, Rwhalb, Quantumseven, HRV, Vijay Varadharajan, Materialscientist, Aneah, Stationcall, ArthurBot, LilHelpa, Cameron Scott, Intelati, Securitywiki, Jsharpminor, Hi878, Coolkidmoa, Zarcillo, Mark Schierbecker, Pradameinhoff, Amaury, George1997, Architectchamp, =Josh.Harris, Shadowjams, President of hittin' that ass, FrescoBot, Bingo-101a, Nageh, Ionutzmovie, Cudwin, Expertour, Intelligentsium, Pinethicket, I dream of horses, Edderso, Access-bb, Jonesey95, Lluis tgn, Yahia.barie, RedBot, MastiBot, Wlalng123, Serols, Mentmic, Dac04, Banej, Dobradavid, Codemaster32, Tjmannos, Nitesh13579, Lotje, Sumone10154, Arkelweis, Ntlhui, Aoidh, Endpointsecurity, Diannaa, Tbhotch, Jesse V., DARTH SIDIOUS 2, Mean as custard, Ripchip Bot, Panda Madrid, DASHBot, Julie188, EmausBot, Timtempleton, Dewritech, Active Banana, P@ddington, Mitartep, Dcirovic, Jasonanaggie, Susfele, Dolovis, Cosmoskramer, Alxndrpaz, AvicAWB, Bar-abban, Ocaasi, Solipsys, Tolly4bolly, Sharpie66, DennisIsMe, Veryfoolish, Geohac, ChuispastonBot, GermanJoe, Pastore Italy, Tentontunic, Seper-sann, Gadgad1973, Rocketretro1960, Jramio, ClueBot NG, Catlemur, AArie142, Name Omitted, Enfceer, Iliketurtlesmeow, Saluki2001, Widr, Dougmcdonell, Helpful Pixie Bot, TechGeek70, Curb Chain, Calabe1992, BG19bot, Mollsieber, MOrphzone, Rubnum, Mohilekedar, Karlomagnus, IraChesterfield, Sburkeel, Gorthian, Zune0112, Venera Seyranyan, Wondervoll, Mihai.scridores, Jtlopez, Mathnerd314159, Nfirdosian, Alessandra Napolitano, Wannabemodel, Keeper03, BattyBot, David.moreno72, Popescualin, Arr4, Mrt3366, Cyberbot II, Khazar2, Peter A. Wolff, Soulparadox, Ilker Savas, Usernamekiran, BIG ISSUE LADY, Saturdayswiki, Dexbot, Jmitola, Mogism, Pete Mahen, TwoTwoHello, Lugia2453, Doopbridge, Sbhalotra, SFK2, Arjungiri, Jamesx12345, Me, Myself, and I are Here, ElinaSy, Patna01, Dr Dinosaur IV, TheFrog001, Atlazcrew, Pdecaculus, Mbmxpress, Idavies007, RaheemaHussain, Cyberlawjustin, Rkocher, MoHafesji, TJLaher123, ResearcherQ, Westonbowden, Peter303x, Whizz40, Stuntddude, Karinher, OccultZone, LukeJeremy, Robevans123, Fixture, Chima4mani, ClyderRakker46, Jonathan lampe, Ippcap, Leejung86, 7Sidz, Azulfiqar, IrvingCarR, Nyashinski, Monkbot, JessicaParrisWestbrook, Nitzy99, Carpalclip3, Fighy45, Nikolaihao, RicardoBanchez, Owais Khursheed, Kinetic37, Venividipedia, Neito Nossal, Oushee, 405Duke, BrettofMoore, A Great Catholic Person, Gr3yHatt001, Thetechgirl, ChamithN, Grage123, Crystallizedcarbon, Jjorgeliso, Fimatic, Hchaudh3, AndrewKin, JRPolicy, Pacguy, PrithviIDReddy, HVanIderstine, Leemily, FormerPatchEditor, JohnElliotV, Pixelized frog, 3 of Diamonds, Johngot, Anarchyte, Bmore84, BurritoSlayer, JJMC89, Information-systemgeeks, PardonTheComma, Nemoanon, JohnEvans79, Hatebott, Ajay Yankee, Nbyrd2000, Soderbounce, Stirmizi, Tejalpatel, Hdaackda, Chenthil Vel, Tonybdistil, Shedletskyy, Prshnktiik, Srilekha selva, Sharanyanaveen, Joanjoc, ZacharyKeeton, Aromelle, RS-Tumber, InternetArchiveBot, Clip History, Wendygreen11, Fuortu, Istbscott, GreenC bot, Osamamahood1, John "Hannibal" Smith, Iremmason, Micpou, Negocios&Deportes, Micheal Ethan, RainFall, Vkrishnaranda, Unisankar, Bminkus, Flying1monkey, Bender the Bot, 72, TriganaBob, Juliet Jolly, Bullaful, NoahPearson, Abdulmuneeb, Manavrungra123, Devanshumeel1234, KAP03, Shamgar2016, Mike Burshteyn, Shabeehammed, GrimmReaper, Kennethtrtan, Jessecbrown, AvinashBiswa19, Cookiestan, Its Gabe, Styledworkhorse, Galyon, Magic links bot, ChinaWatcher2016, Mitesh Gangaramani and Anonymous: 799

- **Mobile security Source:** https://en.wikipedia.org/wiki/Mobile_security?oldid=792504623 **Contributors:** Dreamyshade, Edward, Kku, Ronz, Phil Boswell, Bearcat, Bumm13, Richi, Giraffedata, Ceyockey, Feezo, Mindmatrix, Mattisha, Tabletop, Rjwilmsi, Ahunt, Bgwhite, Wavelength, Sarysa, Gilliam, Ohnoitsjamie, Chris the speller, Deli nk, Kwestin, Shritwod, Gogo Dodo, Drogers.uk, Dawnseeker2000, Visik, Obiwankenobi, Magioladitis, JamesBWatson, Elinruby, Cesarth~enwiki, Jesant13, Katharineamy, Bonadea, SylviaStanley, WereSpielChequers, Flyer22 Reborn, Capitalismojo, Josang, Socrates2008, Stypex, DanielPharos, Boleyn, Addbot, Grayfell, MrOllie, Yobot, Wiki-Dan61, AnomieBOT, Rubinbot, Mark Schierbecker, 78.26, January2009, FrescoBot, Vertago1, Biker Biker, Jonesey95, OMGWEEGEE2, Cnwilliams, Chris Caven, RjwilmsiBot, Rsmaah, EmausBot, John of Reading, WikitanvirBot, Timtempleton, K6ka, Midas02, Bamyers99, SporkBot, ClueBot NG, Pietrogpimu, Widr, Helpful Pixie Bot, Electriccatfish2, BG19bot, Lifeformnoho, Yash101, Cyberbot II, ChrisGualtieri, MikeD-NJITWILL, Dexbot, Rickbcaol, 967Bytes, Lugia2453, Me, Myself, and I are Here, Securevoicecalling, Gtangil, Mbqt31, Tsarihan, Dannyruthe, Dodi 8238, Monkbot, RicardoHeinz, Dsprc, Nitin93flanker, KH-1, Alesteska, Andreilow, Ujjwal Sahay, Anarchyte, Marieswiss12, Cmason1234, Lisahamilton90, Muhammad mobeen83, Chenthil Vel, Wikijagon, Bootsandmountains, GreenC bot, Peerlyst2016, SuperFetched777, AFFlannery, Briankennethswain, Bender the Bot, Grapeerjam, Hmsplsathish, RayBall, Its Gabe, Ealchemist, Sakshi Jhalani, Mary1783 and Anonymous: 52
- **Network security Source:** https://en.wikipedia.org/wiki/Network_security?oldid=794489975 **Contributors:** Ed Brey, ZimZalaBim, Mike Rosoft, Discospinster, Wrp103, Bobo192, Nsaa, Arthena, Woohookitty, Mindmatrix, Aarghdvaark, BD2412, Kbdank71, Seraphimblade, Twaring, Nivix, Ewlyahooocom, Intgr, Chobot, ADVm, Bgwhite, FrankTobia, Epabhith, Irishguy, Nick C, Deku-shrub, Vanished user 8488293, Zzuuzz, JonnyJinx, BorgQueen, Victor falk, SmackBot, Gilliam, Ohnoitsjamie, Rmosler2100, Deli nk, Kungming2, Rrburke, Radicle, Nakon, Weregerbil, Philpraxis~enwiki, Will Beback, Kuru, DavidBailey, Robofish, Gorgalore, Aqw3R, Ehheh, TastyPoutine, Kvng, Iridescent, Shoeofdeath, Dthvt, Cbrown1023, Leujohn, E smith2000, MaxEnt, Sutekh.destroyer, Shandon, Ayzmo, Thijs!bot, Epbr123, TheFearow, JustAGal, Michael A. White, Dawnseeker2000, AntiVandalBot, Obiwankenobi, Seaphoto, Marokwitz, Prolog, Ellenaz, AndreasWittenstein, ClassicSC, Andonic, PhilKnight, Tqbf, Raanoo, VoABot II, AuburnPilot, AlephGamma, Rohasnagpal, Elinruby, Stephenchou0722, STBot, CliffC, Jonathan Hall, R'n'B, Obscurans, Pharaoh of the Wizards, Jesant13, Ginsengbomb, Smyle.dips, ElectricValkyrie, DH85868993, Ken g6, Vanished user 39948282, CardinalDan, Wiki-ay, Philip Trueman, Oshawah, Mdeshon, M2petite, GidsR, Falcon8765, FlyingLeopard2014, SieBot, Liamoshan, RJaguar3, Quest for Truth, Flyer22 Reborn, Mscwriter, Dodger67, Hariva, ManOnPipes, ClueBot, Arcitsol, Donalcampbell, Drmies, Mild Bill Hiccup, Boing! said Zebedee, Krmashall, Sommo, Jswd, Eekster, Leonard^Bloom, Radiosband, Rhododendrites, Tnspartan, Ranjithsutari, Johnnuniq, SoxBot III, SF007, XLinkBot, Stickee, Nepenthes,

BaroloLover, Mitch Ames, ErkinBatu, Nakamura36, Sindbad72, HexaChord, Sweeper tamonten, Addbot, Willking1979, Dmsynx, Ron-hjones, TutterMouse, Jncraton, CanadianLinuxUser, T38291, Cst17, MrOllie, Download, Тиверополник, Tide rolls, Ghalleen, Bodies3819, Batman2472, CaliMan88, RoggerFerguson, Sgarchik, Pheebalicious, AnomieBOT, JDavis680, Dwayne, Piano non troppo, AdjustShift, Rwhalb, Ulric1313, Materialscientist, Aneah, Stationcall, ArthurBot, Xtremejames183, TheAMmollusc, Simsianity, Impakti, FreshBreak, Tedzdog, Pradameinhoff, SassoBot, SCARECROW, Seldridge99, Jcj04864, E0steven, Coffeerules9999, Citation bot 1, Farazy, FoxBot, Lotje, Vrenator, Dmuellenberg, Reach Out to the Truth, Mean as custard, RjwilmsiBot, Sundar.ciet, Ripchip Bot, Tremaster, Happyisenough, Timtempleton, Primefac, Sumsum2010, Take your time, Dcirovic, Yurisk, Ocaasi, Slimkaos, De.vos.katja, Donnen60, Orange Suede Sofa, TYelliot, Sepersann, Mjbmrbot, Eliwins, ClueBot NG, Girraj study, JetBlast, Jaket911, TZM.Tronix, Netsecurityauthors, Sn23-NJITWILL, Denningr, Rahubud, HMSSolent, Calabe1992, BG19bot, Hallows AG, Kyendell, Annapawiki, Mark Arsten, Piano1900, Nashrul Hakiem, Sheenaancy, Millennium bug, W.D., Mdann52, Mrt3366, Yy.sujin, YFdyh-bot, Prelude after noon, Jags707, SimonWiseman, Codename Lisa, Patrick.bausemer, Pete Mahen, Junkyardsparkle, Me, Myself, and I are Here, Vanischenu from public computers, Phamnhatkhanh, Csteinb, Jakec, Ahoora62, FockeWulf FW 190, Softwareguy2013, Hard ToOp, Monkbot, Tabowen, Owais Khursheed, Oushee, TerryAlex, Sin.akshat, Robbiegray-mv, KH-1, Greenmow, TheoMessin, Tmar877, Eroticgiraffe-selfies, Yoloswag1224, Mrs.Guidoisa (fill in the blank), Mrs. Guido is a (fill in the bank), RoadWarrior445, CAPTAIN RAJU, Ayogakar, Srilekha selva, Sharanyanaveen, Christy Max, Wendygreen11, TheMagnificentist, John "Hannibal" Smith, LanceRishad, Unisankar, Quinton Feldberg, Kristopher.a.lopez, SecurityPanther, Rkb82, Geetika saini, Saru1993, Em2449, Kendrickk56 and Anonymous: 333

- **Cybercrime** *Source:* <https://en.wikipedia.org/wiki/Cybercrime?oldid=794535904> *Contributors:* Damian Yerrick, Frecklefoot, Edward, D, Ixfd64, Sannse, Dori, Ihcoye, Ronz, Jebba, Darkwind, Andrew, Julesd, Andres, Kaihsu, GCarty, Ww, Greenrd, Zoicon5, Katana0182, Robbot, ZimZalaBim, Lowellian, Desmay, UtherSRG, Plandu, Alan Lifting, Everyking, Edcolins, Utcursch, Antandrus, Jorm, Beland, Reagle, Joyous!, Ta bu shi da yu, DanielCD, Discospinster, Rich Farmbrough, ArnoldReinhold, Atchom, Marks, Bender235, El-wikipedista~enwiki, Narcisse, Cmdrjameson, Elipongo, WikiLeon, Vishnu vijay, Timmywimmy, ADM, Zachlipton, Alansohn, Arthena, Snowolf, Wtmitchell, L33th4x0rguy, TaintedMustard, Harej, RainbowOfLight, H2g2bob, W7KyzmjT, Ringbang, You, Woohooikit, Mindmatrix, Scjessey, Wikiklrs, Prashanthns, BD2412, Galwhaa, Josh Parris, Rjwilmsi, Bill37212, Bruce lee, Bhadani, Amelio Vázquez, Ysangkok, Rabreu, Gunnix, Nivix, Gurch, Tieno007~enwiki, Czar, Intgr, Alphachimp, David91, Bgwhite, Wavelength, Phantomsteve, SpuriousQ, IanManka, Akamad, Stephenb, Markjx, NawlinWiki, Welsh, Renata3, Moe Epsilon, Deku-shrub, FoolsWar, Lippard, Zzu-uzz, Gtdp, Red Jay, Rurik, CWenger, NeilN, Tom Morris, Sardanaphalus, Crystallina, SmackBot, Reedy, Stifle, Canthusus, Nil Einne, Mauls, Gilliam, Skizzik, Jrkagan, Kurykh, JDCMAN, Dimonicquo, Silly rabbit, Octahedron80, WikiPedant, Mihairad, Tim Pierce, Jennica, ConMan, Expugilist, Savidan, RolandR, FlyHigh, Prehistoricmaster2, Kuru, Ocee, Shadowlynk, Joffeloff, IronGargoyle, Kirkconnell, Barrycarlyon, Beetstra, Invisifan, Hu12, MikeWazowski, Iridescent, Kencf0618, CapitalR, Sim8183, Tawkerbot2, Dlohcierekim, CmdrObot, Ale jr, JohnCD, Penbat, MrFish, Equendil, Anthonyhcole, DumbBOT, ErrantX, Heathniederee, Epbr123, Mojo Hand, Vertium, Esemono, Dawnseeker2000, The Legendary Ranger, Dzubint, I already forgot, AntiVandalBot, Oducado, QuiteUnusual, Paste, Joe Schmedley, Oddity-, Wayiran, Gilliantayloryoung, JAnDbot, Dustin gayler, Levitica, SiobhanHansa, VoABot II, Maheshkumaryadav, Joellee, Kiwimandy, Edper castro, DerHexer, JaGa, Mahnol, Cocytus, MartinBot, Lordmyx, Jeannealcid, Jim.henderson, Rhiltonjua, Psychoair, Keith D, Jerry teps, Bemsor, Nixonmahilum, Thirdright, JonBurrows, Jmm6f488, Kemiv, Semaja, Reno911, Boxmoor, Neon white, NYCRuss, Vanillagorillas, Tokyoyigrl79, Turner70, HiLo48, DadaNeem, Olegwiki, Druss666uk, Ja 62, Funandtrvl, Metalicaguy007, VolkovBot, Philip Trueman, MissionInn.Jim, Notecardforfree, Technopat, Sparkzy, Helppe, Jose figueredo, Sankalpdavid, Qxz, Anna Lincoln, The3stars, Tpk5010, Snowbot, Jlh, Milan Keršáger, Billinghurst, Enigmaman, Falcon8765, Justmeherenow, Noncompliant one, Cool110110, DeanC81, Yintan, LeadSongDog, Flyer22 Reborn, Jojalozzo, Jestypnugh, Oxymoron83, Harry-, Techman224, Manway, Millstream3, AMbot, Mr. Stradivarius, Barry Jameson, Denisarona, Jons63, Elassint, ClueBot, Kai-Hendrik, Binkster.net, The Thing That Should Not Be, Jotag14, Taraldo, Tomas e. Chris.tripledot, CounterVandalismBot, Niceguyedc, LizardJr8, Trivialist, PMDrive1061, Chaserx7, Canis Lupus, Jusdafax, Rhododendrites, Cenarium, Imaximax1, Vivon1, Jmaio2, Aleksd, Light show, Agilentis, Thingg, PCHS-NJROTC, Callinus, Johnnuniq, MBK-iPhone, BarretB, XLinkBot, Roxy the dog, Gonzonoir, Afpre, Charco2006, Bamford, Addbot, Some jerk on the Internet, Non-dropframe, Gpershing, MrOllie, Jgkjfdlsgkjd, Fatboy500, PranksterTurtle, Glane23, Debresser, Favonian, Jaydec, 5 albert square, Tide rolls, Bultro, Willondon, Jarble, HerculeBot, Matt.T, Albeiror24, Jackelfive, Ben Ben, Kurtis, Publicly Visible, Luckas-bot, Yobot, Legobot II, II MusLiM HyBRID II, Mdolphy, KamikazeBot, JackCoke, Lessandmore, IW.HG, Ircpresident, Vörös, Backslash Forwardslash, AnomieBOT, DemocraticLuntz, Kerfuffle, Jim1138, IRP, Darkblazikenex2, NickK, Materialscientist, ArthurBot, Quebec99, Justwiki, Xqbot, JimVC3, Capricorn42, RoodyAlien, Mrc1028, Srich32977, Pradameinhoff, Wikieditor1988, Tankrider, Lior1075, Shadowjams, FrescoBot, Weyes1, Yashansi, YOKOTA Kuniteru, Blockyeyes, Ka4, Buchana4, Dejan33, Sfafinski, Bobmack89x, Pinethicket, I dream of horses, Gajic32, Professional7, Tom.Reding, MJ94, Serols, Mentmic, Full-date unlinking bot, Merlion444, FoxBot, Lotje, Callanec, Vrenator, Aoidh, Reaper Eternal, ThinkEnemies, Reach Out to the Truth, Minimac, DARTH SIDIOUS 2, Fred11111111, Mean as custard, RjwilmsiBot, VernoWhitney, Agent Smith (The Matrix), Beccritical, EmausBot, John of Reading, Immunize, Sophie, Angrytoast, Katherine, Dewritech, RA0808, Minimac's Clone, RenamedUser01302013, Tommy2010, Wikipelli, Dcirovic, Ida Shaw, Pragnesh89, Josve05a, Jenks24, Michael Essmeyer, Empty Buffer, Forgottenking, Bustermythmonger, EneMsty12, Christina Silverman, Kjg0972, Erianna, Umni2, Donner60, Carmichael, Yulli67, ChuispastonBot, Trickmind, Gary Dee, Davey2010, Petrb, ClueBot NG, Mechanical digger, Sagaa2010, Gareth Griffith-Jones, Iii I I I, Catlemur, 6ii9, Hirai NJITWILL, Widr, Leeaar04, Helpful Pixie Bot, Aigendon, HMSSolent, Nightenbelle, Markthing Inc., Titodutta, KLBot2, BG19bot, VasundraTaneja, Jhanov1999, Ramesh Ramaiah, FxHVC, Najma El Shelhi, Frze, AvocatoBot, SusanBREN, Metricopolus, Mark Arsten, Lochfyneman, Dainomite, Harizotoh9, MrBill3, Glacialfox, Klildiplomus, Yasht101, Aisteco, CrimeWeb, Fylbecatulous, Agent 78787, Darylgolden, ~riley, Aristotle, Pratyaya Ghosh, Cyberbot II, Padenton, Khazar2, Abowker, Bamachick20, HelicopterLlama, Lugia2453, Frosty, Metalytics, FrostieFrost, Me, Myself, and I are Here, Mason Doering, PinkAmpersand, Greengreenred, Dddeege, LectriceDuSoir, Reziebear, Ugog Nizdast, Glaisher, Bullblade, EdynBliss, Ginsuloft, Jupitus Smart, Ibrahim Husain Meraj, Quenhitran, Cindy123456, Jnguyenx3, Keatonhouse, FockeWulf FW 190, M3osol1301, Fixture, Dodi 8238, JaconaFrere, Skr15081997, Kacyoconnor14, Lordinangel101, Altaythegooner, AKS.9955, Cybersecurity101, Addisnog, Pinklights2323, S166865h, StaceyHutter, Sumnist, Johnc123456, KH-1, Willhesucceed, Vanyaxd, Julietdeltalima, Hellys320, Hayman30, Destor918, Lymaniffy, Rishab Elangovan, Guegreen, FormerPatchEditor, DarthWyyrlok, Notnot9, Erosen15, CyanoTex, Drdebaratiwiki, KasparBot, Dmonshagen, Airplane Maniac, DebaratiH, ScottAvalon, Zackie1990, Priyadarshivishal23, Josh9791, Rahul Tibile, Mkm8dy, Tejalpatel, Pencilsharpener, Srilekha selva, Harshadp87, Harrisgideon2000, Layla, the remover, InternetArchiveBot, Wendygreen11, Parmenionofmacedon, ELHOUSAINT OUSBOUH3, Silas mololo, Peter SamFan, Saladin Saleem Bhatti, Suomi viro, KGirTrucker81, Chrissymad, John "Hannibal" Smith, Smooth G 89, Rand1990, Lennoneyc, Mona963, Sonuakkachu, Bender the Bot, BrianjCasciotta, Lassitude44, Alfie 09, SususRagey, Louiepug, KaplanAL, Ravi Kotwani, T shaffer09, Magic links bot, Gloveman7812, AvaleronV, Ykkalyan7, ChooseNoName, Toreightyone, DemGoofs, Shreyash Monkey, Spokane1977 and Anonymous: 779
- **Vulnerability (computing)** *Source:* [https://en.wikipedia.org/wiki/Vulnerability_\(computing\)?oldid=794192047](https://en.wikipedia.org/wiki/Vulnerability_(computing)?oldid=794192047) *Contributors:* Kku, Cesarb, Ronz, Joy, Eugene van der Pijll, Phil Boswell, ZimZalaBim, Waldo, Sdfisher, Jason Quinn, Wmahan, Utcursch, Beland, White-

Dragon, Quar!, FrozenUmbrella, Mozzerati, Discospinster, Xezbeth, Mani1, Guy Harris, Adequate~enwiki, InShaneee, Velella, Ceyockey, Mindmatrix, Ahouseholder, Ruud Koot, Macaddct1984, Mandarax, Tslocum, BD2412, Ketiltrot, Rjwilmsi, Jweiss11, ElKevbo, Naraht, Brownh2o, Chobot, YurikBot, Wavelength, Gardar Rurak, Gaius Cornelius, Irishguy, Gruffi~enwiki, Perry Middlemiss, Mugunth Kumar, Abune, SmackBot, Mmernex, AnOddName, Gilliam, PJTraill, Chris the speller, Persian Poet Gal, Manuc66~enwiki, JonHarder, Solarapex, Chris palmer, Mistress Selina Kyle, FlyHigh, Lambiam, Derek farn, Xandi, Beetstra, Ehheh, Nevuer, Dreftymac, JoeBot, Jbolden1517, Penbat, Vanished user fj0390923roktg4tlkm2plkd, Thijs!bot, EdJohnston, Dawnseeker2000, Obiwankenobi, Dman727, Eleschinski2000, S.C.F, Esanchez7587, CliffC, Fleetflame, Ash, Jesant13, Anant k, Sarveshbathija, Touisiau, Jramsey, Tanjstaffl, TXiKiBoT, Oshwah, Softtest123, Zhenqinl, Michaeldsuarez, Haseo9999, Swiki, LittleBenW, Sassy410, JuTiLiu, WereSpielChequers, Securityphreaks, Phe-bot, Cenzic, Jojalozzo, Jruderman, Ottawahitech, Dcampbell30, Liquifried, WalterGR, DanielPharos, PotentialDanger, Sensiblekid, Fathisules, Addbot, Yuma, SpBot, Tide rolls, Luckas-bot, BaldPark, Yobot, Djptechie, Sweerek, AnomieBOT, MistyHora, Blueraspberry, Materialscientist, ArthurBot, The Evil IP address, RobotBOT, Pradameinhoff, Bentisa, Erik9, FrescoBot, Kitaure, HamburgerRadio, Pinethicket, LittleWink, Guriaz, Serols, Tool789789, Dtang2, Lotje, DARTH SIDIOUS 2, VernoWhitney, EmausBot, John of Reading, T3dkjn89q00vl02Cxplkqs3x7, Timtempleton, Pastore Italy, ClueBot NG, Ptrb, Shajure, Emilyisdistinct, J23450N, AvocatoBot, Exercisephys, Mrebe1983, Partaj1, Mdann52, Mrt3366, Cyberbot II, Mediran, Codename Lisa, Mogism, Pharrel101, Pintoch, Wieldthespade, Krazy alice, OccultZone, Fixture, Pat power11, Monkbot, S166865h, Balancesheet, CodeCurmudgeon, Gamebuster, Greenmow, Gustasoz, GreenC bot, DisclosureBrain, PrimeBOT, D1975, Ehacknews, Bkr42 and Anonymous: 110

- **Eavesdropping** *Source:* <https://en.wikipedia.org/wiki/Eavesdropping?oldid=792180987> *Contributors:* Magnus Manske, Waveguy, Dan Koehl, Kku, Menchi, TakuyaMurata, Skysmith, Docu, Kingturtle, Kaihsu, John K, Lee M, DJ Clayworth, Kierant, Joy, Khym Chanur, Securiger, Postdlf, Wereon, Xanzzibar, Zigger, Abu el mot~enwiki, Jhs15681, Talkstosocks, Bender235, Longhair, Jag123, Pearle, Alansohn, Gargaj, AndreasPraefcke, Mangojuice, Stefanomione, BD2412, FlaBot, Ground Zero, CiaPan, YurikBot, Mikeblas, Occono, EEMIV, Elkman, Zzuuzz, Nikkimaria, Ekeb, Rearden9, Junglecat, SmackBot, Gilliam, Betacommand, Rmosler2100, Chris the speller, Bluebot, Shalom Yechiel, Ortzinator, Cybercobra, Givenez, Joystick74, Tazmaniacs, Loodog, Gobonobo, Ckatz, 16@r, Colonel Warden, Lord E, McQuack, JForget, CBM, Penbat, Halfor, Cydebot, Playtime, Clayquot, SimonDeDancer, MafiaCapo, M. B., Jr., Luigifan, RickinBaltimore, NigelR, Fayenatic london, Barek, Jaysweet, Froid, Escorial82, MartinBot, Morki, Keith D, LegendGamer, Pharaoh of the Wizards, Jeepday, Flatscan, KimiSan, Sağlamci, Beta7, Melsaran, SieBot, Dreamafter, Flyer22 Reborn, Kjtobo, Wahrmund, Pinkadelica, Denisarona, Sandy of the CSARs, Martarius, ClueBot, Stevehs, DionysosProteus, Mike Klaassen, Shaliya waya, BOTarate, Vigilius, Mitch Ames, Kbdankbot, Cewvero, Addbot, RFBugExpert, Ielvis, OmgDALE, SamatBot, Herr Gruber, Luckas Blade, Luckasbot, Yobot, AnomieBOT, Citation bot, Xqbot, Mononomic, Charles D. Ward, GrouchoBot, SassoBot, Thehelpfulbot, AlexanderKaras, Citation bot 1, Bsaldoval, Lotje, MrJackCole, Diannaa, Werirth, Youngeuropean, Cobaltcigs, ClueBot NG, Helpful Pixie Bot, BG19bot, Mark Arsten, StevenBeaupre, Spiculalinguae, Essam4002, Hume42, Frosty, Me, Myself, and I are Here, Anonz 8431, Flat Out, DavidLeighEllis, Dodi 8238, Abracombie, ChrisHF, Scarlettail, Suctioninfo2, Amortias, Mathjam, CAPTAIN RAJU, Saff V., Bumbum01, Jthomps1993 and Anonymous: 154
- **Exploit (computer security)** *Source:* [https://en.wikipedia.org/wiki/Exploit_\(computer_security\)?oldid=794450636](https://en.wikipedia.org/wiki/Exploit_(computer_security)?oldid=794450636) *Contributors:* AxelBoldt, Mav, Aldie, SimonP, Stevertigo, Michael Hardy, TakuyaMurata, Karada, Ronz, Nikai, Smaffy, RI, Enigmasoldier, Altenmann, Pengo, Alerante, Guanaco, SWAdair, Utcursch, Bluefoxicity, Discospinster, Rich Farmbrough, Pie4all88, Syp, El C, Matthe, Bobo192, La goutte de pluie, Ramsey, Walter Görlitz, Adequate~enwiki, Ringbang, Nuno Tavares, Mindmatrix, Georgia guy, Apokrif, Vargo0, MarquetteD, Mindfuq, RainR, FlaBot, Ground Zero, Latka, Arunkosh, Chobot, KDK, YurikBot, Hydragyrum, Stephenb, Pseudomonas, Dpakoha, Irishguy, Ugnius, Zwobot, Yudiweb, Raistolo, Papergrl, SmackBot, Pgk, Bomac, BiT, Mauls, Gilliam, Jerome Charles Potts, Abaddon314159, JonHarder, Sloverlord, Nakon, Tompsc, Pilotguy, Lambiam, Putnamehere3145, LebanonChild, Ehheh, Dreftymac, SkyWalker, Fabio-cots, Skittleys, Omicronpersei8, Ebrahim, Dreaded Walrus, PC Master, Zorro CX, Ghostwo, SpigotMap, Crakkpot, TXiKiBoT, Wolfrock, Jamespolco, Irsdl, Swiki, PeterCanthropus, Flyer22 Reborn, PabloStraub, ClueBot, Excirial, SchreiberBike, DanielPharos, Fathisules, SkyLined, GD 6041, MrOllie, Legobot, Luckas-bot, Amirobot, Nallimbot, Galoubet, ExploitSolutions, ArthurBot, Sionus, Boyrussia, Waterloox, Weltersmith, Omnipaediast, Pradameinhoff, Erik9, Erik9bot, HambugerRadio, Gurieu, Guriaz, PleaseStand, EmausBot, WikitanvirBot, Dewritech, ZéroBot, IGeMiNix, Pastore Italy, ClueBot NG, Neynt, BG19bot, Who.was.phone, Compfreak7, T2kien, Ueutyi, Kelly McDaniel, Comp.arch, W. P. Uzer, Fixture, Shellcode 64, Favone, In Harry Potter We Trust, TragicEnergy, FoxStudios, Pkutuzov314, Potayto, S166865h, CAPTAIN RAJU, Dya2shu, John "Hannibal" Smith, Wii Kate Pedia, Seba5tien, El cid, el campeador, Magic links bot, Hitchhiker4242 and Anonymous: 153
- **Trojan horse (computing)** *Source:* [https://en.wikipedia.org/wiki/Trojan_horse_\(computing\)?oldid=793945412](https://en.wikipedia.org/wiki/Trojan_horse_(computing)?oldid=793945412) *Contributors:* Damian Yerrick, Paul Drye, MichaelTinkler, LC~enwiki, Mav, Bryan Derksen, Zundark, Rjstott, Andre Engels, Gianfranco, Mincus, Heron, R Lowry, Michael Hardy, Voidvector, Pnm, Kku, Dori, Ahoerstemeier, Ronz, Darrell Greenwood, Julesd, Glenn, Jiang, Ryuukuro, Timwi, Andrevan, Ww, WhisperToMe, SEWilco, Chuunen Baka, Robbot, Kizor, Schutz, Altenmann, Puckly, Premeditated Chaos, Sunray, Tbutzon, Saforrest, Borislav, Miles, Splatt, HaeB, Cyrus, GreatWhiteNortherner, Giftlite, Fennec, Brian Kendig, No Guru, Wikibob, Leonard G., Zerolanvier, AlastairMcMillan, Fanf, Matt Crypto, PlatinumX, SWAdair, SoWhy, Knutux, SURIV, Antandrus, Tbjablin, Kesac, Asriel86, Bumm13, Trafton, Shiftchange, Monkeyman, A-giau, Discospinster, Sperling, Stereotek, JoeSmack, CanisRufus, Shanes, Sietse Snel, One-dimensional Tangent, Yono, Bobo192, Stesmo, Alexandre.tp, Cmdrjameson, Chirag, DCEdwards1966, Haham hanuka, Jjron, Ranveig, Alansohn, Anthony Appleyard, Guy Harris, Andrewpmk, M7, Riana, Sade, Ciaran H, Kesh, Danhash, Evil Monkey, BDD, Versageek, Brookie, Nuno Tavares, Woohookitty, Mindmatrix, TigerShark, Myleslong, Matey~enwiki, Briangotts, Pol098, WadeSim-Miser, Easys12c, Optichan, Gyrae, Mekong Bluesman, Graham87, Avram, Jclemens, Enzo Aquarius, Rjwilmsi, JoshuacUK, Blacktoxic, NeonMerlin, ElKevbo, Ttwaring, Aapo Laitinen, AySz88, Andrzej P, Wozniak, RainR, RobertG, Jifish, Bubbleboys, Ewlyahocom, AlexjohnC3, TheDJ, DevastatorHIC, Ben-w, Gr8dude, M7bot, Ahunt, Chobot, DVdm, Roboto de Ajvol, Angus Lepper, Sceptre, Ytg111, Kerownen, CambridgeBayWeather, Eleassar, Ptomes, Wimt, NawlinWiki, Wiki alf, Dialectric, RattleMan, Johann Wolfgang, Vincspenc, THB, Ugnius, Nick C, Kenkoo1987, T, Lockesdonkey, Wknigh94, Nigurath, Zzuuzz, E Wing, Jogers, GraemeL, Ethan Mitchell, NeilN, RandallZ, Airconswitch, Suburbancow, CIreland, Jayscholar, Slampaladino, J2xshandy, Scolaire, SmackBot, Kellen, Ashenai, Unschool, Narson, Bobet, Tarret, C.Fred, KocjoBot~enwiki, Delldot, KelleyCook, Jpvinal, Arsenaldc1988, Yamaguchi 先生, Gilliam, Ohnoitsjamie, Spamhuntrress, Snori, Tree Biting Conspiracy, Miquonranger03, Gareth, LaggedOnUser, Lexlex, DHN-bot~enwiki, Jeffreyarcand, Abaddon314159, Can't sleep, clown will eat me, MyNameIsVlad, Frap, Christian80, KaiserbBot, Rrburke, TKD, Emre D., Nibuod, Sljaxon, Drphilharmonic, HDow, LeoNomis, Richard0612, Clicketyclack, Neverender 899, SS2005, Kuru, Jidanni, Gobonobo, Sir Nicholas de Mimsy-Porpington, Evan Robidoux, UkNegative, IronGargoyle, 041744, JHunterJ, George The Dragon, Alethiophile, Waggers, Iridescent, Redskull619, IvanLanin, JoeE, Blehfu, Courcelles, Linkspamremover, Astral9, Mzub, ChrisCork, Switchercat, Skywalker, JForget, DJPhazer, CmdrObot, Wafulz, Makeemlighter, ParadoX, CWY2190, Rikva, Lishy Guy, Jesse Viviano, INVERTED, Neelix, Funnyfarmofdoom, Equentil, Slazenger, MC10, Gogo Dodo, Red Director, SnootyClaus, Strom, Mr. XYZ, Shirulashem, DumbBOT, UnDeRsCoRe, Rudá Almeida, Omicronpersei8, Rocket000, Thijs!bot, Epbr123, Blademaster313, N5iln, Laboye, Vertium,

John254, James086, Leon7, Danfreedman, EdJohnston, Mule Man, Dawnseeker2000, Mentifisto, AntiVandalBot, Luna Santin, Widefox, Seaphoto, Oducado, Karthik sripal, Rhuggins-ahammond, JAnDbot, Xhienne, El Dominio, Vaclon, HellDragon, Mishrankur, TAnthony, Freedomlinux, VoABot II, Nyq, Jrg7891, SineWave, GODHack~enwiki, Indon, Cailil, Esanchez7587, Shuini, DidierStevens, Charitwo, Gwern, Atulnischal, MartinBot, Axlq, Drewmutt, Jonathan Hall, R'n'B, JohnNapier, J.delanoy, Patsyanks06, Legoboy2000, Catmoongirl, Didgeman, Mccajor, McSly, RichJizz123, Demizh, Evils Dark, Gurchzilla, AntiSpamBot, Dividing, LeighvsOptimvsMaximvs, Shoessss, Cue the Strings, Andrewcmcardle, Darryl L James, Bonadea, Martial75, Ditre, Anapologetus, ThePointblank, CardinalDan, Burlywood, Deor, VolkovBot, ABF, Jeff G., Sulcage, Rtrace, VasilievVV, Jacroe, Ryan032, Philip Trueman, PGSONIC, Af648, Oshawah, Zidonuke, Dorcots, Floddinn, Drake Redcrest, Rei-bot, Crohnie, Arnon Chaffin, Warrush, Anna Lincoln, Clarince63, Undine235, LeaveSleaves, ^demonBot2, Lukes123, Skittles266, BotKung, Hurleyman, SpecMode, Darkness0110, Madhero88, Peteritism, Haseo9999, Lamro, Falcon8765, Envirobot, Insanity Incarnate, Why Not A Duck, Spitfire8520, LittleBenW, AlleborgoBot, Logan, PGWG, Numbuh48, Fire-foxobsession, Ramesseum, Softpile, Copana2002, SieBot, Teh nubkilr, BotMultichill, Krawi, Josh the Nerd, Caltas, Eagleal, RJaguar3, X-Fi6, Chiroz, Sephiroth storm, Yintan, Johnnyeagleisrocker, Happysailor, Flyer22 Reborn, Caith, Oxymoron83, Kosack, Hobartimus, Drsamgo, Bcrom, Hamiltondaniel, Spphilbrick, AtteOOIE, Snarkosis, The sunder king, Martarius, ClueBot, Jimmyrules1, Dammonkeyman889944, Avenged Eightfold, Binksternet, Artichoker, The Thing That Should Not Be, IceUnshattered, Lawrence Cohen, Ndennison, Wysprgr2005, Ascabastion, Freebullets, Zarkthehackeralliance, Mild Bill Hiccup, Piriczki, Infogaufire, CounterVandalismBot, Dandog77, Abrol19, Dennistang2007, Gunnar Kreitz, Somno, Aua, Excirial, Jusdafax, PixelBot, Eekster, Bde1982, Rhododendrites, Mac1202, Lunchscale, WalterGR, Doctor It, Jaizovic, DanielPharos, JaneGrey, Taranet, VIKIPEDIA IS AN ANUS!, 7, Ranjithsutari, Berean Hunter, Egmontaz, Alchemist Jack, Polemos~enwiki, XLinkBot, Spitfire, NieusLuna, Jovianeye, Sakura Cartelet, Parallelized, TFOWR, ErkinBatu, Mifter, Alexius08, Noctibus, Addbot, Some jerk on the Internet, Landon1980, A.qarta, Friginator, Markymann12, Ronhjones, Ashton1983, Nirajdoshi, MrOllie, Download, Morning277, Ericzhang789, London-infoman, D.c.camero, Glane23, Exor674, SamatBot, Arteyu, Theman98, Politoed666, Numbo3-bot, Tide rolls, Legion79, Krano, Apteva, Teles, Zorrobot, Jarble, Arbitrarily0, Fda-neels, Koru3, Legobot, Helpfulweasal, Yobot, WikiDan61, 2D, Fraggle81, Cfml001, Xxppivjtxxx, NERVUN, Nallimbot, QueenCake, Sujit.jhare, South Bay, AnomieBOT, KDS4444, DemocraticLuntz, Rubinbot, Captain Quirk, Jim1138, Chuckiesdad, Materialscientist, Arezey, Frankenpuppy, Xqbot, Capricorn42, Robot85, Liorma, Bihco, Jsharpminor, KrisBogdanov, FlightTime, S0aaasdf2sf, GrouchoBot, Alumnium, Megamoneyextreme, RibotBOT, SassoBot, TrueGlue, Amaury, JulianDelphiki, Shadowjams, SchnitzelMannGreek, Vanatom, Thehelpfulbot, Trojan1223, FrescoBot, Untilabout9am, Daerlun, Clubmaster3, Michael93555, Scottaucoin89, A little insignificant, Haein45, HamburgerRadio, Mitchell virus, Launchballer, Winterst, I dream of horses, Vicenarian, Edderso, Jacobdead, A8UDI, Rihdiugam, Serols, Ddspec, Robo Cop, Pcuser42, GWPSP090, Ksanex, DixonDBot, Lamarmote, Miiszmylove, MichaelRivers, Vrenator, Reaper Eternal, Jefffrd10, Specs112, Vanished user aoiowaiuyr894isdik43, Ciscorx, Minimac, Ameypersonsave, DARTH SIDIOUS 2, Mean as custard, MMS2013, Lowoox, SMARTCUTEFUNNYXD, Brandonprince00, NerdyScienceDude, Limited2fan, Slon02, Skamecrazy123, Smd75jr, DASHBot, EmausBot, Super48paul, Fly by Night, Dewritech, L235, Tommy2010, Wikipelli, Dcirovic, K6ka, TheGeomaster, Skaera, Ida Shaw, Dalek32, Traxs7, Eldruin, Newbiepedian, Kiwi128, EneMsty12, AndrewOne, Lolecat56734, Coasterlover1994, Sahimrobot, L Kensington, Donner60, Gary Dee, ClueBot NG, Cwmhiraeth, MufinMan999, Gareth Griffith-Jones, MelbourneStar, Bped1985, Augustalex, Muon, Braincricket, Mesoderm, Rezabot, Widr, OKIsItJustMe, Alan357319, Madpigeon12, Strike Eagle, Titodutta, W.andrea, Complol2234343, Robbieee2, Wiki13, TheGeneralUser, MusikAnimal, AvocatoBot, Desenagrator, Mark Arsten, Sbd01, Onewhohelps, Display name 99, Snow Blizzard, MrBill3, Glacialfox, Kelvinruttman, Millennium bug, Tutelary, David.moreno72, Niraj.adyyyy, Th4n3r, Hsr.rautela, Adhithyan15, Cyberbot II, ChrisGualtieri, MadGuy7023, JayMyers-NJT WILL, Ghostman1947, Dexbot, Rezonansowy, FoCuSandLeArN, SoledadKabocha, Djairhorn, Lugia2453, JoshLyman2012, Jc86035, Siravneetsingh, Soda drinker, Discuss-Dubious, Sourov0000, Telfordbuck, Cablewoman, Bugzeelboy, NimaBoscarino, RootSword, Dave Braunschweig, Epicgenius, CatBallSack, Eyesnore, Gaman0091, DavidLeighEllis, Ugog Nizdast, Khabir123, NottNott, Kushay titanium, Someone not using his real name, Manish2911, Oranjelo100, Dannyruthe, Sathishguru, FockeWulf FW 190, STH235SilverLover, Joseph 0515, Marp pro, Rkpayne, Monkbot, Sidharta.mallick, Filedelinkerbot, Abcdfeghtys, Laura J. Pyle, Bibliworm, TerryAlex, Classofthewise, MRD2014, Earthquake58, ChamithN, Crystallizedcarbon, HamadPervaiz, Eteethan, Helpguy77, BoxOfChickens, TQuentin, KasparBot, Ceannlann gorm, James the king12, Adam9007, JeremiahY, TeacherWikipedia, OldMcDonald12345, Sro23, CAPTAIN RAJU, Drakeblair08, Kurousagi, Majneeds2chill, Vansockslayer, Aditya3929, User0071987, Bradley190432754, Pa19602030fu, Montouesto, Srilekha selva, Simplexity22, Voidcube, QianCheng, Promestein, Marianna251, GreenC bot, Chrissymad, John "Hannibal" Smith, Lucifer, Prince.manjeet, Arshdeep Singh Bhatia, Miles315, Bender the Bot, Smithsam007, Paul!, Smdpls, Bennv3771, NiceNCrispyChip, STEAMY TACO, Shashankhrs31399, Razam sh, Aggarwalace, Samsmith123456, STUART123 and Anonymous: 1258

- **Computer virus** *Source:* https://en.wikipedia.org/wiki/Computer_virus?oldid=794487390 *Contributors:* Damian Yerrick, AxelBoldt, Peter Winnberg, The Cunctator, LC-enwiki, Lee Daniel Crocker, Brion VIBBER, Mav, Bryan Derksen, The Anome, Taw, Taral, Malcolm Farmer, Tim Chambers, Mark Ryan, Dragon Dave, Greg Lindahl, Fubar Obfusco, William Avery, SimonP, Ben-Zin~enwiki, Heron, Modemac, Frecklefoot, Edward, Michael Hardy, Nixdorf, Pnm, Liftarn, Smkatz, Wwwwolf, Ixfd64, Cyde, TakuyaMurata, Minesweeper, Egil, Ahoerstemeier, Jdforrester, Darkwind, Stefan-S, Rossami, Nikai, BOARShevik, Cratbro, Evercat, Smatty, Rob Hoot, Samuel~enwiki, GRAHAMUK, Hashar, Dblaissdel, Adam Bishop, Dcoetzee, RickK, Dysprosia, Doradus, WhisperToMe, Zoicon5, Tp-bradbury, Jake Nelson, Furrykef, Morwen, SEWilco, Omegatron, Morven, Wetman, Chrisjj, Pakaran, Secretlondon, Jamesday, Rossum-capek, Huangdi, David Stapleton, Chuunen Baka, Gromlakh, Robbot, Paranoid, Sander123, Fredrik, Kizor, RedWolf, Bernhard Bauer, Romanm, Kokiri, Lowellian, Merovingian, Academic Challenger, Goofyheadedpunk, Premeditated Chaos, DHN, Jondel, Hadal, Kostiq, HaeB, Mattflaschen, Cordell, Carnildo, Tea2min, David Gerard, Baloo Ursidae, Giftlite, DocWatson42, Marius~enwiki, Fennec, Jtg, Lethe, Tom harrison, Ferkelparade, Frevidar, Ayman, Noone~enwiki, Ds13, Guanaco, Patrickdavidson, Dmmaus, Mboverload, Siroxo, AlistairMcMillan, Matt Crypto, Adam McMaster, Utcursch, Knutux, Sonjaaa, Antandrus, Beland, Chinakow, Tbjablin, Wkdewey, Bumm13, Kevin B12, Thevaliant, Sam Hocevar, Cynical, Sillydragon, Crazyeddie, Nataliesiobhan, Joyous!, Jcw69, MakeRocketGoNow, Trafton, Grm wnr, Chmod007, M1ss1ontomars2k4, Kate, Mike Rosoft, Mormegil, Freaknurture, Monkeyman, Imroy, Jiy, Discospinster, Solitude, Rich Farmbrough, Agnitus, Rhobite, Qwerty1234, EliasAlucard, Lemontree, Stereotek, Bender235, Rubicon, ESkog, ZeroOne, TerraFrost, CMC, JoeSmack, MisterSheik, CanisRufus, Ginnsu, El C, Joanjoc~enwiki, PhilHibbs, Shanes, Sietse Snel, Roy-Boy, Jpgordon, Rpresser, Bobo192, Vanished user sdfkjertiwoi1212u5mcake, Stesmo, Smalljim, Clawson, Brendansa, John Vandenberg, Flxmghgvvk, Orbst, Jjk, Richi, La goutte de pluie, Jojit fb, Minghong, John Fader, Obradovic Goran, Wrs1864, Sam Korn, Pearle, Benbread, Jakew, Wayfarer, Alan Isherwood, Knucmo2, Jumbuck, Storm Rider, Alansohn, Andrewpmk, Riana, AzaToth, Kurt Shaped Box, Goldom, T-1000, Phocks, Hu, Malo, VladimirKorablin, GregLindahl, Snowolf, Marianocecowksi, PaePae, Wtmitchell, Tocsin, Fordan, TaintedMustard, Gdavidp, Paul1337, Docboat, Evil Monkey, TrollVandal, LFaraone, Bsadowski1, SteinbDJ, Alai, LukeSurl, Gofeel, Dan100, Ceyockey, Umapathy, Bruce89, Tom.k, Boothy443, Firsfron, Alvis, Reinoutr, Roboshed, Octernion, RHaworth, Uncle G, Kurzon, MattGiuci, Pol098, MONGO, Miss Madeline, Nearnley, Jok2000, Wayward, Prashanthns, Dysepsion, Seishirou Sakurazuka, Graham87, Marcg106, Magister Mathematicae, Cuchullain, BD2412, CivilCasualty, Kbdank71, FreplySpang, JIP, Jclemens, Reisio, Grammarbot, Zoz, Spot Color Process, Ketiltrout, Sjakkalie, Rjwilmsi, Whatcanbrowndo, Xgamer4, Koavf, Isaac Rabinovich,

Tarnas, Kinu, Adjusting, Collins.mc, Commander, Astronaut, Rillian, Tangotango, Bruce1ee, Authr, Raffaele Megabyte, Captain Disdain, ErikHaugen, Gudeldar, Frenchman113, Darksasami, Bubba73, Jdmurray, GregAsche, Sango123, DirkvdM, Antimatt, Leithp, Audunv, Munahaf, RainR, FlaBot, RobertG, Winhunter, Crazycomputers, JiFish, Nivix, RexNL, Gurch, AlexjohnC3, DevastatorIIC, Born2cycle, BitterMan, SteveBaker, Ahunt, Imagine&Engage, Superdude876, Chobot, Visor, Bornhj, Random user 39849958, Digitalme, Peterl, YurikBot, Wavelength, Sceptre, Hairy Dude, Huw Powell, Adam1213, Sigeng, Jtkiefer, WAvegetarian, Anonymous editor, SpuriousQ, Ukdragon37, RadioFan, Stephenb, Gaius Cornelius, CambridgeBayWeather, Wimt, Bullseye, Lusanaherandraton, Anomalocaris, Shanel, NawlinWiki, Wiki alf, Bachrach44, Dialectric, Tfine80, Jaxl, Harksaw, Dureo, Robert McClenon, Nick, Coderzombie, Raven4x4x, Ugnius, Froth, Amcfreely, FatM1ke, Zwobot, Slaad, Dlyons493, BrucevdB, Pblomartinez, DeadEyeArrow, Bota47, Haemo, JoshuaArgent, Romal, Wknight94, Jcvamp, Mugunth Kumar, FF2010, Zero1328, K.Nevelsteen, Zzuuzz, Imaninjapirate, Theda, Closed-mouth, Spondoolicks, Dspradau, BorgQueen, Petri Krohn, GraemeL, Rlove, JoanneB, Mario23, Pursin1, Chrishmt0423, SingDeep, LeonardoRob0t, Rex Nebular, Scoutersig, Amren, Kevin, AVazquezR, Spliffy, Curpsbot-unicodify, RunOrDie, RG2, Eptin, Tyomitch, GrinBot~enwiki, DVD R W, Theroachman, Rahul s55, タチコマ robot, So Hungry, SpLoT, Veinor, SmackBot, MattieTK, Fireworks, Thomas Ash, Khfan93, DreamTheEndless, KnowledgeOfSelf, TestPilot, Hydrogen Iodide, Aborlan, Chairman S., Frymaster, Ericwest, Onebravemonkey, Born2killx, Xaosflux, PeterSymonds, Macintosh User, Gilliam, Algont, Ohnoitsjamie, Oscarthechat, Skizzik, MikeVella, ERcheck, Bluebot, Hayson1991, Rkitko, Green meklar, MalafayaBot, Bolmedias, Danielmau, Delink, Jerome Charles Potts, EdgeOfEpsilon, DHN-bot~enwiki, The Moose, Sbharris, Hongooi, Brucedes, Antonrojo, Firetrap9254, Cancaseiro, WikiPedant, Can't sleep, clown will eat me, Frap, Ultra-Loser, Onorem, Avb, KevM, JonHarder, Yidisheryid, TKD, Manhattan Project 2000, Addshore, SundarBot, Name? I have no name., Maurice45, Sspecter, Krich, PiMaster3, Zrulli, Khukri, Decltype, Nakon, Savidan, Birdfluboy, TedE, Dreadstar, Warren, Insineratehymn, Weregerbil, Last Avenue, Hammer1980, RedViking, RichAromas, Wizardman, Ultraexactzz, Sigma 7, Ck lostsword, Pilotguy, DataGigolo, Kukini, Ged UK, Ugur Basak Bot~enwiki, The undertow, SashatoBot, TjOeNeR, Daishokaioshin, Acebrock, Srikeit, SS2005, Vanished user 9i39j3, Kuru, John, Edetic, Wtwilson3, Slowmover, Sfivaz, Lazylaces, Sir Nicholas de Mimsy-Porpington, Minna Sora no Shita, CaptainVindaloo, Aleenf1, IronGargoyle, Cbk1994, PseudoSudo, Ckatz, A. Parrot, AFOH, Andypandy.UK, Slakr, CommKing, Beetstra, Muadd, Boomshadow, LuYiSi, Martinp23, Mr Stephen, Gerardsylvester, Optakeover, Waggers, Doczilla, Riffic, Elb2000, Evadb, Ryanjunk, Zyborg, Vtt395, KJS77, Levineps, Alan.ca, BranStark, OnBeyondZebrax, Fredil Yupigo, ILovePlankton, Rigurat, Twas Now, MikeHobday, Courcelles, Astral9, Coffee Atoms, Fdp, Mzub, Tawkerbot2, Prophaniti, Chris55, Emote, Bleavitt, SkyWalker, Weird0, FleetCommand, Jorcoga, Ninetyone, KyraVixen, JohnCD, Jesse Viviano, Sree v, Lentower, Leujohn, Casper2k3, Kejoxen, Karenjc, Ricecake42, Nmacu, TJDay, Inzy, Cydebot, Ntsimp, Herd of Swine, Fl, Steel, Meno25, Michaelas10, Gogo Dodo, Hebrides, JFreeman, DarthSidious, Dancter, Tawkerbot4, DumbBOT, Enevile, Chrislk02, Phydend, Asenine, Optimist on the run, Omicronpersei8, Daniel Olsen, Lo2u, Bcohea, Gimmetrow, Dartharias, DarkMasterBob, Ebpr123, Hervegirod, Computafreak, Sagaciousuk, Andyjsmith, Ambulnick, Glennfcowan, Azkhiri, Hunan131, Oliver202, Philsp, Luigifan, Jojan, Radiokillplay, James086, Dooley, Java13690, Ddddgffff, Brainbox 112, Renamed user 5197261az5af96as6aa, Dfrg.msc, Philippe, Big Bird, Dawnseeker2000, Natalie Erin, Oldmanbiker, Dainis, Dzubint, Dantheman531, Mentisto, Porqin, AntiVandalBot, Fedayee, Luna Santin, Widefox, Ibigewald lcaven, MHoover, Oducado, Quintote, Jayron32, Qa Plar, TimVickers, Scenia, Petey21, Malcolm, Chill doubt, Ayrin83, Storkk, Myanw, Darrenhusted, Leuko, Kigali1, MER-C, Epeefleche, Avaya1, Jolmos, OhanaUnited, Tengfred, Xeno, Mullibok, Berkeley@gmail.com, Bookinvestor, Coopercmu, LittleOldMe, Acroterion, SteveSims, Tarif Ezaz, Akuyume, Magioladitis, WolfmanSF, KeKe, Pedro, Bongwarrior, VoABot II, MartinDK, Dragon Dan, Jetstreamer, JamesBWatson, Jrg7891, Master2841, Think outside the box, EhUpMother, Brewhaha@edmc.net, Twsx, Shankargiri, Avicennasis, Midgrid, Bubba hotep, Catgut, Aishwarya .s, Web-Crawling Stickler, Adrian J. Hunter, Allstarecho, Canyouhearmenor, Spellmaster, Omkarcp3, Davis W, Glen, Chris G, Der-Hexer, Eeera, Markc01, Glennforever, Connor Behan, Alu042, Leliro19, 0612, Murray paul, Stephenchou0722, Stealthound, Hdt83, MartinBot, CliffC, NAHID, Poeloq, Rhlitonjua, Rettetast, Mike6271, Draknfyre, Keith D, Bemsor, Jonathan Hall, Kostisl, R'n'B, Smial, WelshMatt, DarkGhost89, Siliconov, ItsProgrammable, Artaxiad, Shellwood, Paranoia, J.delanoy, MRFraga, Legitimate Editor, Carre, Rgoodermote, Bitthesilverbullet, Inspigeon, David sancho, Theo Mark, MrBell, Eliz81, 12dstring, RAF Regiment, Acalamari, Xbspiro, Ravi.shankar.kgr, JFKenn, Timpeiris, Gman124, SpigotMap, Compman12, Crakkpot, Skier Dude, Evils Dark, Gurchzilla, JayJasper, Bilbobee, Bubble94, Chriswiki, Psywavez, HiLo48, Kmoe333, Drahgo, TomasBat, NewEnglandYankee, Srpnor, Dougmarlowe, Ressel, Hennessey, Patrick, Hanacy, Darthpickle, Jackaranga, Black Hornet, Darr dude, RB972, Jamesontai, Jleske, GGenov, Vanished user 39948282, Anonymoususer, Sniper120, Kamote321, Gtg204y, RVJ, Jarry1250, Jay.rulzster, Squids and Chips, Specter01010, Praesidium~enwiki, Leethax, Wikieditor06, BauerJ24, Sacada2, Javeed Safai, VolkovBot, TreasuryTag, CWii, Bluegila, Jeff G., Alegjos, Philip Trueman, Qevlarr, TXiKiBoT, Oshwah, NoticeBored, BuickCenturyDriver, Technopat, Hqb, Yuma en, Miranda, Crazypete101, Lord Vaedeon, JayC, Qxz, Shindo9Hikaru, Mattinson, WraithTDK, Rfcrossp, Anna Lincoln, Codyjames7, Lradrama, Sanjivdinakar, Xaraikex, Tricky Wiki44, JhsBot, Phillyfan1111, Mind23, LeaveSleaves, Tpk5010, Peter Dontchev, Miketsa, Air-con noble, David in DC, Wiae, Csdorman, Da31989, Slipknotmetal, Madhero88, Lolroflomg, Jacky15, Aryeh Grosskopf, Lerdthenerd, Haseo9999, SQL, Tikuko, Gorank4, Falcon8765, Purgatory Fubar, LarsBK, Brianga, Mike4ty4, Bobo The Ninja, LittleBenW, AlleborgoBot, Kehrbykid, FlyingLeopard2014, Kpa4941, Wraithhart, ChipChamp, Repy, Sepetro, Copana2002, Anindianblogger, SieBot, Coffee, J800eb, Dino911, YonaBot, Euryalus, WereSpielChequers, Dawn Bard, Eagleal, BloodDoll, Triwbe, Kkrouni, Bmader, Sephiroth storm, Yintan, Falcofire, GrooveDog, Jerryobject, Keilana, Flyer22 Reborn, The Evil Spartan, Man It's So Loud In Here, Arbor to SJ, Travis Evans, Askild, Wheres my username, Oxymoron83, Antonio Lopez, KPH2293, Timothy Jacobs, Hobartimus, OKBot, Dillard421, Benji2210, Maelgwnbot, Vice regent, BruzerFox, Mminoche, Etchelon83, Miketoloo, Treekids, Jkonline, Denisarona, Lloydpick, Escape Orbit, Into The Fray, Guitaralex, ImageRemovalBot, Mx, Granger, Martarius, Humpet, ClueBot, Fyyer, The Thing That Should Not Be, TableManners, Vox-puppet, WakaWakaWoo20, Jan1nad, Seriousch, Jotag14, Wysprgr2005, Likepeas, Meekywiki, VQuakr, Mild Bill Hiccup, Boing! said Zebedee, Moniquehls, CounterVandalismBot, Jakebob2, Tumland, Blanchardb, LizardJr8, Bjbutton, Hitherebrian, Otolemur crassicaudatus, MrBosnia, Bfmv-rulez, Puchiko, Rockfang, MindstormsKid, Gunnar Kreitz, DragonBot, Campoftheamericas, Excirial, Alexbot, Jus-dafax, PixelBot, Winston365, Lartoven, Posix memalign, Rhododendrites, Cenarium, WalterGR, TheRedPenOfDoom, Tnxman307, Hans Adler, Frozen4322, SchreiberBike, Arvind007, ChrisHodgesUK, BOTarate, El bot de la dieta, DanielPharos, Thinggg, Aitias, Scalhotrod, Jester5x5, Versus22, PCHS-NJROTC, MelonBot, Vybr8, Qwfp, Johnuniq, Jpg1954, Egmontaz, Apparition11, Editor2020, SF007, Runefrost, DumZiBoT, Bones000sw, Gkaukonen, TheNameWithNoMan, XLinkBot, Stickee, Rror, Sakura Cartelet, Poosebag, Avoided, Mitch Ames, Skarebo, WikHead, SilvonenBot, Me, Myself, and I, SkyLined, Airplaneman, Imapoo, Thatguyflint, Nesky~enwiki, Wnzrf, CalumH93, Flixmhj321, Mojibz, Pacific ocean stiller ocean, Addbot, Xp54321, BreannaFirth, Nuno Brito, Willking1979, Clsdennis2007, Giftiger wunsch, StickRail11, Non-dropframe, DougsTech, Nz26, Ur nans, AlexWangombe, Ronjhones, Justinpwnz11233, Mr. Wheely Guy, GyroMagician, Ethanpet113, Ashton1983, Rynhom44, CanadianLinuxUser, Leszek Jafczuk, NumbNull, Download, Chamal N, CarsracBot, RTG, Glane23, AndersBot, Sumbuddi, Favonian, Comphelper12, Jasper Deng, 5 albert square, ACM2, Savetheozone, Last5, Tassedethe, Lolbombs, The hippy nerd, Tide rolls, Bfigura's puppy, Lightbot, C933103, Gail, Bro0010, Micke, Maverick1071, GloomyJD, Alexd18, Legobot, Worldbruce, Senator Palpatine, DisillusionedBitterAndKnackered, Washburnmav, Taxisfolder, THEN WHO WAS PHONE?, Golftheimer, KamikazeBot, Theornamentalist, Kablakang, 葵葵葵葵葵, Bility, Kmoultry, AnomieBOT, Amritasya-

Putra, Valueyou, La Corona, Rubinbot, 1exec1, ThaddeusB, Arzanish, Jim1138, Galoubet, Dwayne, Danielt998, AdjustShift, Kingpin13, Materialscientist, Racconish, Cameron Scott, Xqbot, Spidern, Cureden, What!?Why?Who?, Gilo1969, Gap9551, S0aasdf2sf, Coretheapple, Sci-Fi Dude, Basvb, Frosted14, Shas1194, Ute in DC, Wizardist, ProtectionTaggingBot, Shirik, Mark Schierbecker, ReformatMe, Amaury, Drvikaschahal, 1nt2, Aurush kazemini, N419BH, Mrbillgates, Lelapindore, Chaheel Riens, Erik9, Sesu Prime, Legobot III, FreeKnowledgeCreator, GliderMaven, Komitsuki, Kitaure, Jono20201, Zero Thrust, Scott A Herbert, HamburgerRadio, Intelligentium, Pinethicket, I dream of horses, Elockid, HRoestBot, Calmer Waters, Bejinhan, RedBot, Pearson, Serols, HaiyaTheWin, Footwarrior, Lineslarge, Reconsider the static, IJBall, Caramelldansener, 3centsoap, Xeroxli, FoxBot, Mercy11, Trappist the monk, LogAntiLog, Lotje, Callanec, Gejyspa, Vrenator, Singlemaltscotch, Zacker150, Extra999, January, Rudy16, Chimpso, Jeffrd10, Nazizombies!, Mufc ftw, Canuckian89, Suffusion of Yellow, Richardsaugust, Tbhotch, TheMesquito, DARTH SIDIOUS 2, Onel5969, Mean as custard, The Utahraptor, RjwilmsiBot, Bento00, Fletcher707, Regancy42, DRAGON BOOSTER, Chroniccommand, Ghymes21, NerdyScienceDude, Deagle AP, DASHBot, Deadlyops, EmausBot, Immunize, Never give in, Ajraddatz, Sevvie, Zerotonin, Dewritech, JuJitsuthirddan, GoingBatty, Ben10Joshua, Olof nord, RenamedUser01302013, Vanished user zq46pw21, Elee, Huctwitha, Tommy2010, Wikipelli, Soadfan112, K6ka, Kurena196, Papelbon467, Elison2007, Hejerik, Rajnish357, AvicBot, ZéroBot, Rhinestone42, Checkingfax, Fæ, Josve05a, Davemacc, Bryce Carmony, Sgerbic, Kiwi128, Alxndrpaz, Imtoocool9999, Mhammad-alkhalaf, Skate4life18, 2han3, Pan Brerus, K kisses, Bawx, Tyuioop, Jy0Gc3, Wayne Slam, Yabba67, Openstrings, Quantumor, Techpraveen, Donner60, Autoerrant, Bomazi, Mv Cristi, ChuispastonBot, GermanJoe, Pastore Italy, Dylan Flaherty, Czeror, SlowPhoton, Neil P. Quinn, Brad117, Mikitei, DASHBot-tAV, Fungo4shezzo, Myfunkypbear123456789, ClueBot NG, Horoporo, Matthiaspaul, This lousy T-shirt, Baseball Watcher, Mesoderm, Rezabot, Massly, Rukario-sama, Widr, Anupmehra, Helpful Pixie Bot, Alexbee2, Tailor-tinker, Lowercase sigmabot, BG19bot, Janendra, Kaltenmeyer, PatrickCarbone, AvocatoBot, Jobin RV, Tobias B. Besemer, Eman2129, Tony Tan, DPL bot, Agent190, Nap-sync, BattyBot, Biosthmors, Justincheng12345-bot, David.moreno72, Smileguy91, Cyberbot II, Codeh, Arcandam, Orioncaspar, Usernamekiran, Dexbot, Cwobel, Codename Lisa, 331dot, 967Bytes, Makecat-bot, Lugia2453, Frosty, Arrayoutofbounds, Andyhowlett, Athomeinkobe, Kevin12xd, Cdwn, Cadillac000, Palmbeachguy, Epicgenius, JamesmcMahon0, Ayush 691, Melonkelon, EvergreenFir, Ronburgandee, ElHef, DavidLeighEllis, QPT, Babitaarora, NorthBySouthBaranof, Ibrahim Husain Meraj, Sam Sailor, Dannyruthe, Averruncus, FockeWulf FW 190, Fixture, Digiwyse, JaconaFrere, Lakun.patra, 32RB17, Monkbot, Horseless Headman, Kosmosi, Happy Attack Dog, Thisiswikidome, Pantel, Eman235, Jazwal, Shuaibshaikh84, Virus victim, Amortias, Shahean Cozad, NQ, The Last Arietta, Suspender guy, Pariah24, Edityouranswer11, KH-1, ChamithN, Narky Blert, Crystallizedcarbon, WikiGopi, Cpt Wise, Eurodine, Vivek56, Charlotte Churche, অনিদ্রা, Abistevenson22, Julietdeltalima, Tech Aid, Pishcal, Juned kadri, IEditEncyclopedia, Jalen stephens, Wredants, Selim Abou Rahal, TheGracefulSlick, Chandrayadav227, Deanwall123, Hamza190949, Miniredeyes999, GeneralizationsAreBad, Amcann421, Ilikecakeandstuff, Bankofworld, KasparBot, Seanpatrickgray, Astolf0, Wugapodes, Gautamnarayan, MCFinest Anthony, Mac1817:-), CJwar, Santhosh Sankar, Mutaiyab Ahmad, JJMC89, TheGlatiator, My Chemistry romantic, DelugeRPG, Danya02, Entro3.14, PCMarcLondon, Viney P Sunu, Ameya Kanojia, CAPTAIN RAJU, Flashgermade99, MB, Imdnj, Koopa King 125, Chenthil Vel, Sharanyanaveen, Wikipedia Virus Page, Naeem chakera, Expert Computers, InternetArchiveBot, Entranced98, Creeperparty568, Promestein, Suresuba, John.smithm, KGirTrucker81, GreenC bot, Wpiuaaa, SkyWarrior, Ardral, RunnyAmiga, Chickadee46, Msearce, Srops, Joshuambruck1, Superchunk22, Bender the Bot, Pyrrhonist05, 72, Triptothecottage, L3X1, XxdarkwolfxFX, L07-IST816, KAP03, Groobfield, James P. Winchester, Tompop888, Gambler1478, NiceNCrispyChip, CapitalCapybara, Baconbob, Kityt, Magic links bot, Friteby, Hjuujuujuujuj and Anonymous: 2063

- **Computer worm** *Source:* https://en.wikipedia.org/wiki/Computer_worm?oldid=791408025 *Contributors:* LC~enwiki, Brion VIBBER, Mav, The Anome, Stephen Gilbert, Koyaanis Qatsi, Malcolm Farmer, PierreAbbat, Daniel Mahu, Paul~enwiki, Fubar Obfuscō, Patrick, Nixdorf, Pnm, Wwwwolf, CesarB, Ahoerstemeier, Cyp, Jebba, Jdforrester, UserGoogol, Andres, Evercat, GCarty, Gamma~enwiki, Dj ansi, Hashar, Agtx, Ww, Dysprosia, Fuzheado, WhisperToMe, Wik, Zoicon5, Furykef, Dcsohl, Wilinckx~enwiki, Robbot, Naddy, Yosri, Jondel, Seth Ilys, Tea2min, David Gerard, Alerante, DocWatson42, Fennec, Akadroid, Jtg, Noone~enwiki, Eequor, Fanf, Matt Crypto, Just Another Dan, Maximimax, Gscshoyru, Trafton, Grunt, Mike Rosoft, Monkeyman, Discospinster, Rich Farmbrough, Rhobite, KneeLess, YUL89YYZ, Bender235, ESkog, JoeSmack, RJHall, PhilHibbs, Sietse Snel, DavidSky, Smalljim, MITalum, Sam Korn, Nsaa, Alansohn, Andrewpmk, Jonathanriley, Staeiou, Bsadowski1, Pauli133, Bobrayner, Newnoise~enwiki, Roboshed, Woohookitty, Mindmatrix, Camw, Guy M, TomTheHand, Isnow, Kralizec!, Palica, RichardWeiss, Jclemens, Rjwilmsi, Matt.whitby, Syndicate, Mcmvanbree, Nguyen Thanh Quang, RainR, Jwkpiano1, Dan Guan, JiFish, GünniX, RexNL, Ewlyahoocom, King of Hearts, Pstevens, Daev, Chobot, AFA, Bornhj, DVdm, Mogh, YurikBot, Borgx, Kerowren, Barefootguru, Wimt, Wiki alf, Misza13, DeadEyeArrow, Bota47, Jkelly, WAS 4.250, Dspradau, Rs232, Kungfuadam, GrinBot~enwiki, Asterion, DVD R W, Rahul s55, SmackBot, Mmernex, Aim Here, Gamerzworld, David.Mestel, KelleyCook, Object01, Gilliam, Ohnoitsjamie, Martial Law, Biblioteqa, Bluebot, Snori, Miquonranger03, Pomegranite, DHN-bot~enwiki, Firetrap9254, Anabus, Tscabot, NYKevin, Can't sleep, clown will eat me, Yidisheryid, Rrburke, Addshore, Celarnor, Jaimie Henry, James McNally, Richard001, Wirbelwind, Weregerbil, SashatoBot, Ian Dalziel, Nic tan33, Ehheh, Optakeover, Waggers, Vernalex, Woodroar, Iridescent, Jason.grossman, Joseph Solis in Australia, Aeons, Mzub, Tawkerbot2, Dlohcierekim, Chetvorno, Makeemlighter, GHe, Jesse Viviano, Augrunt, Oden, Slazenger, Gogo Dodo, ST47, Luckyherb, HitroMilanese, Thij'sbot, Eprb123, Wikid77, Luigifan, Powellatlaw, Dawnseeker2000, Mentifisto, AntiVandalBot, Seaphoto, Oducado, Waerloeg, Jenny Wong, Clarker, JAnDbot, Leuko, MER-C, PubliusFL, Coopercmu, Superjag, SteveSims, Yixin1996, Bongwarrior, Rami R, Alekjds, Adrian J. Hunter, DerHexer, Shuini, NMaia, S3000, MartinBot, STBot, Ghatziki, Poeloq, Lilac Soul, Shellwood, Bitethesilverbullet, Herbythyme, Imfo, Uncle Dick, Yonidebot, Milo03, Crimson Instigator, Barts1a, Ignatzmice, Demizh, DJ1AM, Juliancolton, Beezhive, CardinalDan, Idioma-bot, Lights, Deor, Hersfold, Jeff G., Philip Trueman, Dindon~enwiki, Zifert, Technopat, Zman2000, Oxfordwang, LeaveSleaves, Tpk5010, BigDunc, RandomXYZb, MDfoo, Falcon8765, Enviroboy, Burntsauce, EJF, Barkeep, SieBot, BotMultichill, Itsme2000, DarkfireInferno, Sephiroth storm, Sat84, Happysailor, Mszegedy, Very cheap, Smaug123, Hello71, Miniapolis, Macy, OKBot, Amrishdubey2005, StaticGull, Mygerardromance, Hamiltondaniel, GioCM, Denisarona, Cellorelio, Minimosher, ClueBot, Traveler100, The Thing That Should Not Be, Lawrence Cohen, Fenwayguy, CrazyChemGuy, Eekster, Rhododendrites, WalterGR, Dekisugi, DanielPharos, Thingg, Aitias, VIKIPEDIA IS AN ANUS!, XXXSuperSnakeXXX, SoxBot III, Sensiblekid, DumZiBoT, XLinkBot, Skarebo, WikHead, PL290, Noctibus, ZooFari, Jabberwoch, Wnzrf, Addbot, Amanda2423, A.qarta, Fieldday-sunday, Leszek Jańczuk, CactusWriter, MrOllie, Protonk, Chzz, Favanian, Comphelper12, Jasper Deng, Yyaflkaj;fasd;kdfjk, Numbo3-bot, Craigjones, Tide rolls, Yobot, Amirobot, Nallimbot, Gunnar Hendrich, Tempodivalse, Souch3, A More Perfect Onion, Jim1138, Piano non troppo, Meatabex, Materialscientist, Neurolysis, ArthurBot, LilHelpa, MauritsBot, Xqbot, Useingwere, Capricorn42, UBJ 43X, Avastik, Khruner, Frosted14, RibotBOT, Ulm, AlanNShapiro, Crackitcert, WPANI, Rossd2oo5, DylanBigbear, HamburgerRadio, Uberian22, Intelligentium, Pinethicket, I dream of horses, Adlerbot, Serols, Subzerobubbles, Lotje, Fox Wilson, Vrenator, Wiwiwiwiwiwiwiwi, Nat-tippy99, Adi4094, Reach Out to the Truth, DARTH SIDIOUS 2, Hajatvrc, DASHBot, EmausBot, Orphan Wiki, Gfoley4, Bexz2000, Wikipelli, Jasonanaggie, JDDJS, Fæ, Kalin.KOZHUHAROV, A930913, Tolly4bolly, W163, MonoAV, DennisIsMe, ChuispastonBot, Gary Dee, Ziyad en, ClueBot NG, Henry Stanley, Borkificator, O.Koslowski, Widr, Helpful Pixie Bot, BG19bot, TheTrainEnthusiast, MusikAnimal, Tobias B. Besemer, Toccata quarta, Mantovanifabiomarco, Glacialfox, Derschueler, Anbu121, BattyBot, Johnthehero,

David.moreno72, Cyberbot II, ChrisGualtieri, EagerToddler39, Dexbot, Lal Thangzom, Codename Lisa, Webclient101, Djairhorn, Luga2453, HarJIT, Jamesx12345, Rossumund, Muhammadbarzman, Smileyss, Ginsuloft, Dannyruthe, FockeWulf FW 190, AntiCompositeNumber, Fixture, JaconaFrere, Satyajeet vit, Kjerish, KH-1, Julietdeltaalima, KasparBot, Gautamnarayan, RippleSax, Compassionate727, CaseyMillerWiki, Fakersenpaipls, Manav garg, Jamiejackherer, Sharanyanaveen, Jumblebumble12, Simplexity22, GreenC bot, ASire03, Getloader, NoToleranceForIntolerance, Bender the Bot and Anonymous: 539

- **Denial-of-service attack** *Source:* https://en.wikipedia.org/wiki/Denial-of-service_attack?oldid=792146882 *Contributors:* Magnus Manske, Derek Ross, Mav, The Anome, RobLa, Mark, Rjstott, Ed Poor, Yooden, PierreAbbat, Edward, Oystein, Michael Hardy, Mdupont, Ixfd64, Zanimum, Delirium, Looxix-enwiki, Ahoerstemeier, Baylink, Jebba, DropDeadGorgias, Julesd, Marco Krohn, Cyan, Evercat, Ghewgill, Agtx, Charles Matthews, Timwi, Pablo Mayrgunder, Kbkb, Jwrosenzweig, Fuzheado, WhisperToMe, Pedant17, Maximus Rex, Furykef, Taxman, Tempshill, Vedge, Thue, Bloodshedder, Mtcv, Olathe, Lothar Kimmeringer-enwiki, Carlossuarez46, Robbot, Fredrik, Korath, R3m0t, RedWolf, Nurg, Rfc1394, Wikibot, Victor, Lupo, Alanyst, Pengo, Tea2min, David Gerard, Ancheta Wis, Alerante, Centrx, Ryanrs, Wolfkeeper, HangingCurve, No Guru, Niteowlneils, Carlo.Ierna, Mboverload, Gracefool, Cloud200, Rchandra, Mckaysalisbury, SonicAD, Wmahan, Chowbok, Gdm, Antandrus, Beland, Mako098765, Piotrus, Wikimol, Rdsmith4, Gauss, Kigoe, Sam Hocevar, SamSim, Neutrality, Bluefoxicity, Stereo, Danc, Millisits, Wesha, Johan Elisson, Discospinster, Rich Farmbrough, Oliver Lineham, Mani1, Bender235, Andrejj, Violetriga, CanisRufus, Goto, Crukis, Smalljim, Mpeg4codec, Thewrite1, Giraffedata, Deryck Chan, Physicistjedi, Wrts1864, Krellis, Pearle, Alansohn, Godzig, Csabo, CyberSkull, Corporal, Andrewpmk, Echuck215, Lightdarkness, Ciaran H, Sligocki, Gblaz, Hu, Snowolf, Wtmitchell, Velella, BanyanTree, Xee, Bsdlogical, Redvers, Ceyockey, Walshga, Kenyon, DarTar, Gmaxwell, Woohookitty, Mindmatrix, Blacheagle, Peng~enwiki, Pol098, WadeSimMiser, Ocker3, Tckma, Scootey, Rchamberlain, Wayward, Prashanthns, Burfdl, Amechad, Graham87, Deltabeignet, Clapaucius, Kakaopor, Kbdank71, Kane5187, Josh Parris, Ketiltrot, Sjö, Rjwilmsi, Friejose, Nneoneo, ElKevbo, Goncalopp, Everton137, Scartol, Bhadani, Andrzej P, Wozniak, Drngrvy, Alliekins619, Wragge, FlaBot, VKokielov, Vegardw, Spaceman85, Who, Nivix, RevNL, Revolving Bugbear, RobyWayne, Intgr, Alphachimp, Malhonen, GreyCat, Chobot, Bwoodring, DVdm, Gwernol, Gimere, Kakurady, Mann Ltd-enwiki, Shaggyjacobs, YurikBot, Splintercellguy, Phantomsteve, RussBot, Sparky132, RedPen, Gardar Rurak, Hellbus, סְרִירָה, Gaius Cornelius, Shaddack, Rsrikanth05, The Cute Philosopher, NawlinWiki, Robertvan1, RattleMan, Escheffel, DavidH, Janarius, Gareth Jones, Catamorphism, Expensivehat, Irishguy, Anetode, Peter Delmonte, Rmky87, Mikeblas, Juanpdp, Bucketsofg, Nethgirb, BOT-Superzerocool, DeadEyeArrow, Darkfred, Yudiweb, Black Falcon, Romal, Sierra 1, WAS 4.250, Frankgerlach~enwiki, Delirium of disorder, Wikibert~enwiki, Msuzen, Raistolo, Closedmouth, Arthur Rubin, Fang Aili, Abune, Josh3580, Matt Casey, Sean Whitton, GraemeL, JoanneB, Vicarious, RenamedUser jaskldjslak904, Huds, ViperSnake151, SoulSkorpion, GrinBot~enwiki, KNHaw, One, SmackBot, Fireman biff, Unschoold, McGeddon, Raven 1959, Freekee, KVDP, Eskimbot, Edgar181, David Fuchs, Buck O'Nollege, Eiler7, Yamaguchi 先生, Aldor, Gilliam, Brianski, Gorman, Chris the speller, Fintler, Apankrat, Jcc1, Persian Poet Gal, Thumperward, Snori, Tree Biting Conspiracy, Elecnix, Nbarth, Sunholm, Emurphy42, Zsinj, Rogermw, Frap, Oscar Bravo, Kaishen~enwiki, OrphanBot, JonHarder, Wiredsoul, Rrburke, Midnightcomm, Artephius, XtAzY, Joomadeus, Shadow1, PPBlais, Paroxysm, Kleuske, SaintedLegion, Acdx, ElizabethFong, Vina-iwbot~enwiki, Bejnarn, Mdavids, Rosarinjroy, Nishkid64, JzG, Kuru, Shadowlynk, Mgiganteus1, IronGargoyle, Barrick, Slakr, Rofl, Dicklyon, Larrymcpc, Uuuuhuł, Romeu, Tuspm, NeoDeGenero, Manifestation, Vashtihorvat, Kvng, Xionbox, Hu12, Gevron, White Ash, JoeBot, Wjejske-newr, Andrew Hampe, Blehfu, Courcelles, Tawkerbot2, SkyWalker, Ddcc, CmdrObot, Boborok, Alan Taylor, KyraVixen, N3X15, TheMightyOrb, GHe, Lemmio, WeggeBot, Pgr94, MeekMark, T23c, Dan Fuhry, Equendil, Cydebot, W.F.Galway, Yehaa~enwiki, Galassi, MC10, Gogo Dodo, Carl Turner, Daenney, Tawkerbot4, Christian75, Pchachten, Zzsql, Ryammshea, Omicronpersei8, Click23, Thijs!bot, Edman274, Kubanczyk, Dschrader, Ultimus, Mbell, Loudsox, RLE64, Marek69, Woody, Bgaurav, JustAGal, Soma mishra, Dawnseeker2000, CTZMSC3, Escarbot, I already forgot, KrakatoaKatie, AntiVandalBot, Yonatan, Widefox, Darklord 205, Oducado, Ross cameron, QuiteUnusual, KP Botany, BenTremblay, DarkAudit, Jayron32, Cinnamon42, Davken1102, Oddity-, Mightywayne, Asmeurer, Ivan Velikii (2006-2008), MER-C, CosineKitty, Gmd1722, Blackmo, Livefastdieold, Hut 8.5, A.hawrylyshen, Geniac, Orpenn, Io Katai, Magioladitis, Ariel@compucall, Trigguh, Bongwarrior, VoABot II, Bradcis, Sarahj2107, Nytrend, Brusegadi, Fedevala, Bobkeyes, Web-Crawling Stickler, MetsBot, DarkMrFrank, A3nm, DerHexer, Shuini, Gwern, Stephanhou0722, Mmoneypenny, CliffC, Jeannealcid, Rhitonjua, Anaxial, Keith D, Bemsor, Krimanilo, R'n'B, Joelee.org, RockMFR, J.delanoy, Skidoo, Herbythyme, StewE17, Uncle Dick, Jesant13, Eliz81, Duzzyman, Cadence-, Andy5421, Ncmvocalist, Clerks, Crakkpot, Zedmelon, Silas S. Brown, Naniwako, Goarany, Mysterysociety, Zhouf12, Bushcarrot, Danr2k6, Liveste, JonNiola, Mufka, Cmichael, KylieTastic, DorganBot, Useight, Steel1943, Signalhead, Lights, Jhalkompwdr, CWii, Butwhatdoiknow, Lexein, Fences and windows, J-Baptiste, Philip Trueman, Oshawah, Vipinhari, Rei-bot, Anonymous Dissident, Liko81, Warrush, Anna Lincoln, Lradrama, TheJae, Broadbot, Canaima, LeaveSleaves, Ziounclesi, UnitedStatesian, Da31989, Haseo9999, Dark Tea, Spartytime, Plreicher, Monty845, Dsarma, Shree theultimate, DeanC81, Red, Hmwith, Lsi john, Drake144, SieBot, Madman, K. Annoyomous, Klaslop, ToePeu.bot, Dawn Bard, Sephiroth storm, Yintan, Alex9788, Softwaredude, Flyer22 Reborn, Xavier6984~enwiki, Bananastalktome, Drennick, Gopher23, Tmaufuer, Joey Eads, Harry the Dirty Dog, La Parka Your Car, Remocrevo, ChriStopher, Rjc34, Raoravikiran, Kortaggio, Denisarona, Atif.12, Martarius, Beeblebrox, ClueBot, LAX, NicDumZ, The Thing That Should Not Be, B1atv, Starkiller88, Antisof, Terry rodery, Lawrence Cohen, Keraunoscopia, Jotag14, R000t, Pwitham, SuperHamster, Melgomac, Boing! said Zebedee, PentiumMMX, Trivialist, William Ortiz, Cwagmire, Swearwolf666, Kitsunegami, Excirial, Jefflayman, Filovirus, Wilsone9, Zac439, Rhododendrites, Usbdriver, Mikae, Muro Bot, DanielPharos, Jcmcc450, MelonBot, SoxBot III, Egmontaz, Darkicebot, Bearsona, XLinkBot, Arnolddgibson, Rror, Xawieri~enwiki, WikHead, Findep, SilvonenBot, Alexius08, Dnrvfantj, Brento1499, IsmaelLuceno, Addbot, Chakkalokesh, Viperdeck PyTh0n, Ramu50, Mortense, WeatherFug, AlexanderDmitri, Stphnm, Astt100, Msick33, Tothwolf, Totakeke423, Ronjhones, Scientus, CanadianLinuxUser, Mjsa, Atif0321, O.neill.kid, MrOllie, Mcnaryxc, Ld100, Favonian, ChenzwBot, Getmoreatp, Chicken Quiet, Jasper Deng, Tide rolls, Jarble, Bartledan, Peter AUDEMG, Titi 3blood, Luckas-bot, Yobot, Hagoleshet, Ptbotgourou, Fraggie81, Donfbreed, Ojay123, Becky Sayles, THEN WHO WAS PHONE?, GateKeeper, MrBlueSky, Echtner, Eric-Wester, Magog the Ogre, Synchronism, AnomieBOT, BlackCatN, Thexelt, Kristen Eriksen, Deathwiki, Killiondude, Jim1138, IRP, Gascreed, AdjustShift, Ulric1313, Flewis, Materialscientist, Fffffrrrr, Nosperantos, Citation bot, Aneah, Armoraid, ArthurBot, LilHelpa, Xqbot, Addihockey10, Jeffrey Mall, Melkor, Tad Lincoln, Shulini, Silversam, Mechanic1c, Karlos77, Life Now, GrouchoBot, Frosted14, Monaarora84, Omnipaedita, MugabeeX, Sophus Bie, TakaGA, Smallman12q, Shadowjams, SchnitzelMannGreek, Teknopup, Samwb123, Shyish, GliderMaven, FrescoBot, Sandgem Addict, Balth3465, Galorr, JMS Old Al, Adnan Suomi, Zhangyongmei, Jamesrules90, Fiddler on the green, Drogonov, HamburgerRadio, I dream of horses, Haneef503, Modamoda, Tom.Reding, Anders K Berggren, Yaltaplace, Fat&Happy, RedBot, BrianHoef, Anonauthor, Île flottante, LiberatorG, Lines-large, Blstormo, Random1c, Cnwilliams, JackHenryDyson, FoxBot, Trappist the monk, Mwikieditor, Jrmurad, DixonDBot, Xiphidae, Demonkill101, Lotje, Lionaneesh, Gazzat5, N-david-l, Dinamik-bot, Toobulkeh, JOptionPane, Allen4names, Adarw, Xitrax, Merlin-sorca, Fastilysock (usurped), Gomangoman, Mean as custard, RjwilmsiBot, Ripchip Bot, Bossanoven, Enrico.cambiaso, VernoWhitney, Mchcopl, J36miles, EmausBot, Mjdtjm, Dewritech, Racerx11, GoingBatty, RA0808, RenamedUser01302013, NotAnonymous0, Qrs-dogg, L235, Klbrain, Solarra, Wikipelli, Dcirovic, K6ka, Euclidithalis, Mz7, OmidPLuS, QuentinUK, John Cline, Daonguyen95, Bon-goramsey, Josve05a, DannyFratella, Finnish Metal, Msamae83, Access Denied, EneMsty12, Wikfr, Whsazdfhnbfxgnh, FinalRapture,

Beatles2233, Ivhtbr, Erianna, Maccoat, EricWesBrown, Demiurge1000, TyA, Anne-Caroline~enwiki, Schnoatbrax, Donner60, Ryan-carpenter, Jak32797, Pastore Italy, Zabanio, Teapeat, Kellyk99, Paddingtonbaer, Petrb, ClueBot NG, TT-97976, Gareth Griffith-Jones, Manubot, Keegen123, MelbourneStar, Satellizer, Permalinks, Joefromrandb, Cogware, Stultiwikia, Lawandtech, Lasoraf, Sunndil, Tejasrnbr, Jormund, 123Hedgehog456, O.Koslowski, Vlhsrp, Popo41~enwiki, Widr, Souledric, Helpful Pixie Bot, Strike Eagle, BG19bot, Murler, Rpk74 lb, Tragic8, Vagobot, Fahmedch, Streakydl, Juro2351, Meoking, MadHaTTer666, Mfordth, Lloydus98, Adsf1234, MusikAnimal, Stogers, Kovo1cat, Mark Arsten, Op47, Rm1271, GGShinobi, Eduart.steiner, Writ Keeper, Jarrodmaddy, Junganghansik, Gtaguy235, Minhal Mehdi, Worldnewsinformant, Comfr, Skunk44, BattyBot, Abgelcartel, David.moreno72, AllenZh, RichardMills65, Mdann52, Cathairawr, Tonyxc600, Cyberbot II, Vinsanity123, Run4health, Chengshuotian, Eb15111, Dwnd4, Superkc, Team Blitz, Iciciliser, Kikue26, Dexbot, K7L, SoledadKabocha, 331dot, TonyJunak, Broadcasterxp, Lugia2453, Spicyitalianmeatball, UNOwen-NYC, Ascom99, Jmoss57, Leemon2010, Me, Myself, and I are Here, Palmbeachguy, Rogr101, JoshuaHall155065, Sid Shadesslayer, Epicgenius, Ashikali1607, Renoldsmartin, ExtremeRobot, HMGamerr, FrigidNinja, Melonkelon, Mbmxpress, JamesMoose, Tentinator, Sngs87, Marchino61, Webhostingtips, Johnhax, Ogh4x, Nodove, DavidLeighEllis, Dwgould, NiuWang, Reacher1989, Ginsuloft, ArmitageAmy, Henrychan123, Jianhui67, FockeWulf FW 190, UY Scuti, Quite savvy, YellowLawnChair, Akashksunny13, Meteor sandwich yum, Jeremyb-phone, PJone, Dodi 8238, Pvpmasters, XxWoLfxX115, JNKL, Lordangel101, Kazkade, Monkbot, Noahp15, Lucyloo10, Vieque, Jakupian, Jacobdunn82, Web20DOS, Muhammadabukar92, Cph12345, 365adventure, Frogteam, Orthogonal1, MRD2014, Bammie73, BlackCat1978, ApolloLV, Jjsantanna, Thetechgirl, Sam-the-droid, Cirflow, KH-1, Tommate789, ChamithN, Koen2014 7, Matia, V1n1 paresh, HoustonMade, Flated, Probincrux, ThatOneGuyGaming, Lizard Squadron, JohnZLegand, Delcooper11, Chiranjeev242, Restart32, Jokingrotten, Eslam Yosef, Infinite Guru, Haroly, Yasuo Miyakawa, Test, Murph9000, Risc64, Hazim116, Tom29739, Lemondoge, Kurousagi, UpsandDowns1234, Pandamaury, WannaBeEditor, Positronon, Misfoundings, Sharanyanaveen, Doulph88, Gmuenglishclass, JennishFernardis, Harmon758, InternetArchiveBot, DBZFan30, 奉艺政, For the lols haha, GayAlienZ, DevinP6576, GreenC bot, Exemplo347, JDWFC, John "Hannibal" Smith, Kainweir, Gluons12, Unkown934, Sarraalqahtani, DNS1999, 白點專業檳榔, BedrockPerson, Franck2, Dboylolz, Woolw0w, Bender the Bot, Bullaful, FL3SH, Max berlings, Zulu53, Necabi, Canjustgo, DanGonite, Mdikici4001, Clover100, Jamesede, Djrcuz94, Dmtschida, JasonJson, Laurdecl, Nutinmyfactsmydude, Wikiguruman, Gogogir77, Shakilbhuiyan.bd, Shreesudhu, Kiernaoneill, Edthat2, Userblogger1234, Unitell and Anonymous: 1346

- **Malware Source:** <https://en.wikipedia.org/wiki/Malware?oldid=793712823> **Contributors:** LC~enwiki, Mav, The Anome, PierreAbbat, Paul~enwiki, Fubar Ofbusco, Heron, Edward, Michael Hardy, David Martland, Pnm, Kku, Liftarn, Wwwwolf, Shoaler, (, CesarB, Ellywa, DavidWBrooks, CatherineMunro, Angela, Darkwind, Ciphergoth, Stefan-S, Evercat, GCarty, Etaoin, RodC, WhisperToMe, Radiojon, Tpbradbury, Bevo, Spikey, Khym Chanur, Finlay McWalter, Rossumcapek, Huangdi, Riddley, Donarreiskoffer, Pigsonthew, Fredrik, Vespristiano, JosephBarillari, Postdlf, Rfc1394, KellyCoinGuy, DHN, Mandel, HaeB, Lzur, Mdmcginn, David Gerard, Centrx, Fennec, Laudaka, Akadruid, Jtg, CarloZottmann, Mintleaf~enwiki, Everyking, Dratman, Mboverload, AlistairMcMillan, Matt Crypto, ChicXulub, Noe, Salasks, Piotrus, Quar!, Rdsmith4, Mikko Paananen, Kevin B12, Icairns, TonyW, Clemwang, Trafton, D6, Monkeyman, Discospinster, Rich Farmbrough, Guanabot, Vague Rant, Vsmith, Sperling, Night Gyr, Bender235, Sc147, JoeSmack, Elwikipedista~enwiki, Sietse Snel, Art LaPella, EurekaLott, One-dimensional Tangent, Xgravity23, Bobo192, Longhair, Billymac00, Smalljim, Unquietwiki, KBi, VBGFscJUn3, Visualize, Minghong, Hfguide, Espoo, Alansohn, Mickeyreiss, Tek022, Patrick Bernier, Arthena, T-1000, !melquiades, JeffreyAtW, Stephen Turner, Snowolf, Wtmitchell, Veabella, GL, Uucp, Danhash, Evil Monkey, RainbowOfLight, Xixtas, Dtobias, Richard Arthur Norton (1958-), OwenX, Mindmatrix, Camw, Pol098, Julyo, Zhen-Xjell, Palica, Allen3, Cuvtixo, Elvey, Chun-hian, Jclemens, Reisio, Dpv, Ketiltrout, Rjwilmsi, Collins.mc, Vary, Bruce1ee, Frenchman113, PrivaSeeCrusade, Connorhd, Yamamoto Ichiro, Andrzej P. Wozniak, RainR, FlaBot, Fragglet, Intgr, Chobot, Bornhj, Bdelisle, Cshay, Gwernol, RogerK, Siddhant, YurikBot, Wavelength, RattusMaximus, Aussie Evil, Phantomsteve, Ikesther, RussBot, DMahalko, TheDoober, Coyote376, Ptomes, Wimt, Thane, NawlinWiki, Hm2k, Krystyn Dominik, Trovatore, Cleared as filed, Coderzombie, Kingpomba, Ugnius, Amcfreely, Voidxor, Tony1, Alex43223, FlyingPenguins, Chriscool, Bota47, Groink, Yudiweb, User27091, Tigalch, Flipjargendy, Romal, American2, Nikkimaria, Theda, Closedmouth, Abune, PrivaSeeCrusader, Dspradau, GraemeL, Cffrost, RealityCheck, Rename-dUser jaskldjslak904, Allens, Jasón, NeilN, Mhardcastle, MacsBug, SmackBot, ManaUser, Mmernex, Hal Canary, Hydrogen Iodide, Bigbluefish, WookieInHeat, Stifle, KelleyCook, Bobzchemist, Ericwest, Ccole, HalfShadow, Yamaguchi 先生, Gilliam, Ohnoitsjamie, Skizzik, PJTraill, Larsroe, Appelshine, Father McKenzie, Jopson, Jprg1966, Thumperward, Snori, Pylori, Mitko, Fluri, SalemY, Ikiroid, Whispering, Ted87, Janipewter, Audriusa, Furby100, Berland, JonHarder, Rrburke, DR04, Mr.Z-man, Radagast83, Cybercobra, Warren, HarisM, URLwatcher02, Drphilharmonic, DMacks, Fredgoat, Salamurai, Kajk, Pilotguy, Clicketyclack, Ged UK, MaliNorway, CFLeon, Howdoesthiswo, Vanished user 9i39j3, OcarinaOfTime, Gobonobo, Robofish, Xaldafax, Nagle, Fernando S. Aldado~enwiki, Voceditenore, Ian Dalziel, 16@r, AndyPandy.UK, Slakr, NcSchu, Ehheh, Uuhuul, Vernalex, DI2000, Andreworkney, Fan-1967, Tomwood0, Iridescent, Dreftymac, NativeForeigner, Mere Mortal, UncleDouggie, Cbrown1023, Jitendrasinghjat, Astral9, Mzub, JForget, DJPhazer, Durito, FleetCommand, Americasrof, Powerpugg, Wikkid, Hezzy, JohnCD, Kris Schnee, Jesse Viviano, Xxovercastxx, Ke-joxen, Augrunt, Nnp, TheBigA, Cydebot, MC10, Besieged, Gogo Dodo, Pascal.Tesson, Medovina, Shirulashem, DumbBOT, Chrislk02, Optimist on the run, Kozuch, Drewjames, Vanished User jdksfajlasd, Tunheim, Legotech, Thijs!bot, Epbr123, Crockspot, Wikid77, Pstanton, Oldiowl, Technogreek43, Kharitonov, Headbomb, A3RO, Screen317, James086, SusanLesch, Dawnseeker2000, Escarbot, AntiVandalBot, Widefox, Seaphoto, Михајло Ајђелковић, SummerPhD, Quintote, Mack2, Storkk, Golgofrinchian, JAnDbot, Mac Lover, MelanieN, Andonic, Entgroupzd, MSBOT, Geniac, Bongwarrior, VoABot II, Kinston eagle, Tedickey, Sugarboogy phalanx, Nyttend, Rich257, Alekjds, 28421u2232nfencenc, LorenzoB, DerHexer, MKS, Calltech, XandroZ, Gwern, Kiminatheguardian, Atulsnischal, ClubOranje, MartinBot, CliffC, Ct280, BetBot~enwiki, Aladdin Sane, R'n'B, CommonsDelinker, LedgendGamer, J.delanoy, Svetovid, Phoenix1177, Herbythyme, A Nobody, Jaydge, Compman12, Fomalhaut71, Freejason, Demizh, HiLo48, Chiswick Chap, Kraftlos, Largoplazo, Cometstyles, Tiggerjay, Robert Adrian Dizon, Tiangua1830, Bonadea, Jarry1250, RiseAgainst01, Sacada2, Tftraserteacher, VolkovBot, Jeff G., NBurden, Satani, Wes Pacek, Philip Trueman, Teacherdude56, TXiKiBoT, Oshawah, Floddinn, Muro de Aguas, Zifert, PoM187, Rei-bot, Retiono Virginian, Jackfork, LeaveSleaves, Optigan13, Miketsa, BotKung, Wewillmeetagain, Tmalcomv, Blurpeace, RandomXYZb, Digita, LittleBenW, Logan, Fredthefrog, S.Örvarr.S, Adavel, Copana2002, Tom NM, Nubiotech, LarsHolmberg, Sephiroth storm, Yintan, Calabraxthis, Xelgen, Arda Xi, Bentogoa, Happysailor, Flyer22 Reborn, Jojalozzo, Nnkx00, Nosferatus2007, Evaluist, Miniapolis, Kljtech, Lightmouse, Helikophis, IdreamofJeanie, Correogsk, Stieg, Samker, Jacob.jose, BfMGH, Dabomb87, Denisaron, Ratemonth, Martarius, ClueBot, Muhammadsb1, NickCT, Vitor Cassol, The Thing That Should Not Be, VsBot, Lawrence Cohen, Wysprgr2005, Frmorrisson, Jwhibey, Sam Barsoom, Ottava Rima, Paulcmnt, Excirial, Jusdafax, Dcampbell30, Rhododendrites, Ejsilver26, Arjayay, WalterGR, 7&6=thirteen, Maniago, Jaizovic, Dekisugi, Xme, DanielPharos, Versus22, Callinus, Johnuniq, Rossen4, DumZiBoT, Darkicebot, XLinkBot, BodhisattvaBot, DaL33T, Avoided, Sogle, Mifter, Noctibus, CalumH93, Kei Jo, Addbot, Xp54321, Cxz111, Arcolz, Mortense, A.qarta, Otisjimmy1, Crazysane, TutterMouse, Ashton1983, CanadianLinuxUser, Leszek Jaćczuk, T38291, Noozgroop, CactusWriter, MrOllie, Download, LaaknorBot, Glane23, Ld100, AndersBot, Jasper Deng, Tassedeth, Eviledeathmath, Tide rolls, Krano, Teles, Gail, Jarble, Quantumobserver, Crt, Legobot, আর্জিষ মন্ত্রণালয়, Publicly Visible, Luckas-bot, Yobot, Philmikeyz, WikiDan61, Tohd8BohaithuGh1, Ptbotgourou, Fraggle81, Evans1982, Gjohnson9894, Dmarquard, AnomieBOT, DemocraticLuntz,

Rubinbot, Roman candles, Jim1138, IRP, Galoubet, RandomAct, Materialsscientist, CoMePrAdZ, RevelationDirect, Crimsonmargarine, Frankenpuppy, ArthurBot, Quebec99, Cameron Scott, Xqbot, TheAMmollusc, Mgaskins1207, Capricorn42, 12056, Avastik, Christopher Forster, Masonaxcte, S0aasdf2sf, Almabot, GrouchoBot, Monaorora84, Shirik, RibotBOT, PM800, Dougofborg, Luminique, Glider-Maven, Afromayun, Fingerz, FrescoBot, Vikasahil, Mitravaruna, Wikipe-tan, Sky Attacker, PickingGold12, WOULDshed, TurningWork, Jonathansuh, Romangralewicz, DrydenGeary, HamburgerRadio, Citation bot 1, SL93, Uberian22, Bobmack89x, Pinethicket, I dream of horses, Idemnow, Vicenarian, Rameshngbot, RedBot, Overkill82, Serols, Chan mike, Fumitol, Graham france, Javanx3d, FoxBot, Tgv8925, TobeBot, SchreyP, FFM784, Jesus Presley, TheStrayCat, Neutronrocks, Techienow, Lotje, Wikipandaeng, Dinamik-bot, Vrenator, Mirko051, Aoidh, KP000, Simonkramer, Tbhotch, Lord of the Pit, DARTH SIDIOUS 2, Whisky drinker, Mean as custard, Moshe1962, RjwilmsiBot, Colindiffer, Panda Madrid, Thunder238, Salvio giuliano, Enauspeaker, EmausBot, John of Reading, WikitanvirBot, Dewritech, The Mysterious El Willstro, Winner 42, Wikipelli, K6ka, Porque123, Elison2007, SocialAlex, Connoe, AvicBot, FlippyFlink, Bollyjeff, Df1gd, Azuris, H3llBot, EneMsty12, Simorjay, Paramecium13, Tyuioop, Tolly4bolly, Cit helper, Coasterlover1994, Techpraveen, Champion, Rigley, Capnjim123, Ankitcktd, Ego White Tray, Mv Cristi, Pastore Italy, Corb555, Mark Martinec, Helpsome, ClueBot NG, Cwmhiraeth, Rich Smith, PizzaMuncherMan, Lzeltsler, PwnFlakes, Matthiaspaul, MelbourneStar, Catlemur, Satellizer, Piast93, Steve dixon, MarsTheGrayAdept, Mesoderm, Widr, BrandoBraganza, Rubybaret, BBirke, Calabe1992, BG19bot, Kre-nair, Harmonicsonic, Vagobot, CityOfSilver, Sailing to Byzantium, Mahn98, PatrickCarbone, Hopsmatch, MusikAnimal, Mark Arsten, Michael Barera, Forbo, JZCL, 220 of Borg, AntanO, Partaj1, BattyBot, JC.Torpey, Spazz rabbit, Cimorus, Zhao Feng Li, MahdiBot, Stigmatella aurantiaca, Pauly72, BYagour, Verzer, Antonio.chuh, ChrisGaultieri, Tech77, Hassim1983, Hnetsec, MadGuy7023, JYBot, Ghostman1947, Toopepot, EagerToddler39, Dexbot, FoCuSandLeArN, FTLK, Codename Lisa, Joshy5.crane, Dothack111, Skullmak, 967Bytes, Webbanana1, Wiki nol ege, Rajalakshmi S Kothandaraman, Salwanmohsen, TwoTwoHello, CoLocate, Lugia2453, Himanshu Jha 07, Frosty, UNOwenNYC, SirkusSystems, Sourov0000, Corn cheese, Palmbeachguy, Gtangil, Epicgenius, Dr Dinosaur IV, TheFrog001, JimsWorld, Flashgamer001, Camayoc, Msumedh, Kap 7, Nonsenseferret, Bio pox, RonPaul573e, Madsteve 9, Kogmaw, Tankman98, Olivernina, ExtraBart, 38zu.cn, Mooman4158, DavidLeighEllis, Warl0ck, Kharkiv07, Ugog Nizdast, Melody Lavender, Swiftsectioner, Ginsuloft, Chris231989, Wifi router rootkits, Ban embedded cpus for networks, JohnMadden2009, Someone not using his real name, Wifi wiretapping, BornFearz, DannyRuthe, Noyster, FockeWulf FW 190, Ajitkumar.pu, Mickel1982, JaconaFrere, Vandraag, SnoozeKing, Newlywoos, Gatundr Burkllg, Alan24308, Worzzy, Justin15w, Lucius.the, Andrei Marzan, Joeleo123, MLP Eclipse, Stevebrown164, BrayLockBoy, Qwertyp2000, Andrdema, Degh96, A4frees, 1anamada, AnastasiiaGS, Olidog, Maxwell Verbeek, Oiyarbepsy, WikiGopi, Eurodyne, Jiten Dhandha, Shovelhead54, Spamer, Fimatic, Hvaara, Friendshipbracelet, Rubbish computer, Agent-Paradox, Gabiked, ToonLucas22, Nysrtup, Davenilk, Akstotz, M8b8f8, Supdiop, KasparBot, Tmar877, Marzan Chowdhury, Musik-Bot, Adam9007, JJMC89, Jasmineluv, ROMA1maro, Albaniakuov, Shreyassachdeva, Hearmewe, Salarmfd, Luis150902, Chenthil Vel, Kosherpenguinxperience, Phils234, Srilekha selva, Sharanyanaveen, Allthefoxes, InternetArchiveBot, Entranced98, Eno Lirpa, GreenC bot, Pranjal01, Gulumeemee, John "Hannibal" Smith, Atomicselection, Lynchkid101, Lmiller 22, Henull, NewByzantine, Dongboyxd, Bender the Bot, 72, Buchanan554, Mariahjanepeter, 2211nb, Zacikan, PrimeBOT, Christo Tomy, Prinsipe Ybarro, ZS5, Osadkfpdsdf, Someone4562345325645634674365, Abhisharif, Shieeet, TheDecider, Kanak Poddar and Anonymous: 955

- **Payload (computing)** *Source:* [https://en.wikipedia.org/wiki/Payload_\(computing\)?oldid=794115022](https://en.wikipedia.org/wiki/Payload_(computing)?oldid=794115022) *Contributors:* Kku, Robbot, Discospinster, H2g2bob, Pol098, GregorB, BertK, SmackBot, Snori, Hateless, Kvng, Neelix, Alaibot, Legotech, Pstanton, MikeLynch, The Transhumanist, Swpb, Tinucherian, Bogey97, Derekrorgerson, Synthebot, X-Fi6, Denisaron, Wwdw, WikHead, Addbot, Pradameinhoff, Erik9, Jonesey95, Oliverlyc, Jenks24, ClueBot NG, Daze21, Scarlettail, Mo5254, Wambuirwn, 0xF8E8, Buscopaz, Abhishekashyap092, Muhammad ismail johari, This-is-name and Anonymous: 37

- **Rootkit** *Source:* <https://en.wikipedia.org/wiki/Rootkit?oldid=788267298> *Contributors:* Zundark, Fubar Obfusc0, William Avery, SimonP, Stevertigo, Frecklefoot, JohnOwens, Nixdorf, Pnm, Kku, Liftarn, Zanimum, Pennmachine, Tregoweth, Ahoerstemeier, Haakon, Nikai, Schneelocke, Emperorbma, Timwi, Aarontay, Ww, Olego, Fuzheado, Markhurd, Echoray, Furykef, Taxman, Bevo, Rossum-capek, Phil Boswell, Robbot, Scott McNay, Henrygb, Auric, Zidane2k1, Paul G, Tea2min, Unfree, David Gerard, Alison, JimD, Ezhiki, Cloud200, AlistairMcMillan, Sauceman, Taka, Allobodig, Deewiant, Creidieki, Pascaly, Adashiel, Squash, Bri, EITyrant, Rich Farmbrough, Agnistus, Jayc, Bender235, CanisRufus, Twilight (renamed), Kwamikagami, PhillHibbs, Spoon!, Femto, Perfecto, Stesmo, Small-jim, Chasmo, Mpvdml, Adrian-enwiki, Giraffedata, Yonkie, Bawolff, Helix84, Espoo, Jhfrontz, Polarscribe, CyberSkull, JohnAlbertRigali, Hookysun, Phocks, BanyanTree, Danhash, Earpol, RJFJR, RainbowOfLight, Kazvorpal, RyanGerbil10, Japanese Searobin, Dtobias, Defixio, Alvis, CCooke, OwenX, Woohookitty, David Haslam, Steven Luo, Shevek, Pol098, Apokrif, Btmiller, Easyas12c, Midnightblaze, SDC, Umofomia, Xiong Chiamiov, RichardWeiss, Graham87, BD2412, Rjwilmsi, TitaniumDreads, Syndicate, Arisa, Randolph, RainR, Flarn2006, FlaBot, RobertG, Stoph, JiFish, Harmil, Mark Lusznak, Arunkoshy, Mordien, Intgr, Mimithethbrain, Dbpigeon, Bgwhite, Martin Hinks, Poorsod, FrankTobia, Elf guy, Uriah923, YurikBot, Wavelength, Hairy Dude, Diesonne, AVM, Chrisjustinparr, IByte, Hydrargyrum, NawlinWiki, Wiki alf, Mipadi, Ian Cheese, Ejdejz, Stephen e nelson, Cleared as filed, Nick, Raven4x4x, JackHe, Mysid, FoolsWar, Bota47, Nescio, Ninly, Maxwell's Demon, Mateo LeFou, Theda, Closedmouth, Arthur Rubin, Reyk, Roothorick, Anime-Janai, Solarusdude, Jacqui M, That Guy, From That Show!, SmackBot, Mmernex, Estoy Aquí, Reedy, Mate.tamasko, Unyoyoga, Kelley-Cook, Iph, SimonZerafa, Ohnoitsjamie, Chris the speller, Bluebot, Gspbeetle, Thumperward, Ben.the mole, Octahedron80, DARQ MX, DHN-bot-enwiki, Jmax-, 1(), Frap, Onorem, Tim Pierce, Sommers, Ukrained, Whpq, MichaelBillington, DMacks, J.Christopher.Wells, AndyBQ, A5b, Mitchumch, N-dy, Clicketyclack, FrostyBytes, Tasc, Tthtlc, Peyre, Simon Solts, Xionbox, OnBeyondZebrax, LAlawMedMBA, IvanLanin, CapitalR, Prpower, Phoenixrod, Courcelles, Tawkerbot2, Davidbspalding, FatalError, Zarex, Cyrus XIII, Megaboz, Jokes Free4Me, Jesse Viviano, Chrismo111, Racooper, Myasuda, Equendil, A876, GrahamGRA, Tryl, Pirate, Fetterinity, Mewsterus, Etaon, Ambulnick, Marek69, Tocharianne, Dawnseeker2000, AntiVandalBot, Widefox, Obiwankenobi, Czj, Sjledet, Lfstevens, Bscottbrown, AndreasWittenstein, TivicBot, Hiddenstealth, NapoliRoma, MER-C, Minitrue, QuantumEngineer, Karsini, BCube, Repku, Raanoo, Drugonot, Chevinki, Nyttend, Cl36666, Denorios, Stromdal, Alekjds, Hamiltonstone, Cpl Syx, XandroZ, Stephenhou0722, R27smith200245, MartinBot, Eshafto, CobraBK, Fethers, R'n'B, Nono64, Ash, Felipe1982, CraZ, Pharaoh of the Wizards, UBeR, Uncle Dick, Maurice Carbonaro, Theo Mark, Leeked, Andy5421, It Is Me Here, Peppergrower, Crakkpot, DavisNT, Wng z3r0, Marekz, Joshua Issac, Comet-styles, Gemini1980, ArneWynand, VolkovBot, Ashecan Rantings, Senachie, Soliloquial, TXiKiBoT, Sphinx2k, CanOfWorms, Miketsa, UnitedStatesian, Natg 19, Haseo9999, Willbrydo, Suzaku Medli, Ceranthor, Ggpur, MrChupon, SieBot, Technobreath, Sephirot storm, Edans.sandes, Windowsvistafan, Aly89, General Synopsis, Fyre, Clearshield, Capitalismoj, Bogwhistle, BfMGH, Guest141, Martarius, ClueBot, The Thing That Should Not Be, TheRasIsBack, Mild Bill Hiccup, Fossguy, Tai Ferret, Socrates2008, Crywalt, PixelBot, JunkyBox, Rhododendrites, Holden yo, NuclearWarfare, Mrkt23, Pinkevin, Htfiddler, DanielPharos, Floul1, Johnnuniq, SF007, Uuddii, Pelican eats pigeon, XLinkBot, Dsimic, Thatguyflint, Addbot, Willking1979, Kongr43gpen, Sergey AMTL, Elsenero, TutterMouse, Cst17, MrOllie, OlEnglish, Fiftyquid, Luckas-bot, Yobot, Fraggie81, GateKeeper, Golftheimer, Alipie42, AnomieBOT, NoKindOfName, Blueraspberry, Materialsscientist, Nutsterrt, Citation bot, ArthurBot, LilHelpa, Avastik, S0aasdf2sf, Notwej, Charlie Sanders, GrouchoBot, Kernel.package, Thearcher4, Trafford09, Sophus Bie, XLCior, Shadowjams, FrescoBot, WPANI, Ozhu, Wmcleod, HamburgerRadio, Citation bot 1, JoeSmoker, Winterst, Pinethicket, Jonesey95, Shultquist, Gim3x, OMGWEEGEE2, Rbt0, Trappist the monk, Techienow,

Vanished user aoiowaiuyr894isdik43, Onel5969, TjBot, Alph Bot, EmausBot, John of Reading, WikitanvirBot, Timtempleton, Hercules31, Dewritech, Janiko, P3+J3^u!, Dcirovic, ZéroBot, Herman Shurger, Basheersubei, Mike735150, IceCreamForEveryone, Bender17, Chicklette1, Dilflame, Macwhiz, Nhero2006, DASHBotAV, Pianosa, ClueBot NG, Biterankle, Morgankevinj huggle, Matthiaspaul, MelbourneStar, Zakblade2000, Barry McGuiness, Helpful Pixie Bot, BG19bot, Strovonsky, Rijinatwki, Abagi2, John davidthomas, BattlyBot, Tkbx, StarryGrandma, Cyberbot II, ChrisGaultier, Draculamilktoast, Cadava14, Dexbot, Codename Lisa, Noul Edge, Soledad-Kabocha, Cryptodd, CaSJer, A Certain Lack of Grandeur, Ginsuloft, Oranjelo100, FockeWulf FW 190, Dust482, Monkbot, Vieque, BethNaught, Verdana Bold, Ahollypak, KH-1, Shinydiscoball, Jithedran Subburaj, TQuentin, Azlan 6473, KasparBot, Ceannlann gorm, UpsandDowns1234, Montouestou, Sharanyanaveen, GreenC bot, Layra1mthew, Axelkai36 and Anonymous: 593

- **Keystroke logging** *Source:* https://en.wikipedia.org/wiki/Keystroke_logging?oldid=793880654 *Contributors:* Derek Ross, LC-enwiki, The Anome, SimonP, R Lowry, Edward, Lir, Pnm, Kku, Ixfd64, Ellywa, Ronz, Angela, Kingturtle, Aimaz, Rossami, Evercat, Samw, GCarty, Guaka, Aarontay, Ww, Dysprosia, WhisperToMe, Markhurd, Tschild, Furrykef, Nv8200pa, Omegatron, Jamesday, Catskul, Blugill, Lowellian, Hadal, Wereon, David Gerard, DavidCary, Laudaka, Jason Quinn, AlistairMcMillan, Solipsist, Antandrus, Beland, OverlordQ, Lynda Finn, Mike Rosoft, Discospinster, Rich Farmbrough, ArnoldReinhold, Xezbeth, ZeroOne, JoeSmack, Sietse Snel, RoyBoy, Femto, Adambro, Yono, Bobo192, Nigelj, Stesmo, Wisdom89, Dteare, Starchild, Alansohn, Danhash, Bobrayner, Woohookitty, Unixer, Armando, Pol098, WadeSimMiser, Firien, Dbutler1986, Graham87, JIP, Rjwilmsi, DickClarkMises, FlaBot, Weihao.chiu-enwiki, Latka, JiFish, Intgr, Runescape Dude, Salvatore Ingala, Peterl, Whosasking, Tiimage, YurikBot, Wavelength, Borgx, FlareNUKE, Lincolnite, Conscious, Hede2000, SpuriousQ, Rsrikanth05, Wimt, Mipadi, Bob Stromberg, Vivaldi, Tony1, Occono, Palpalpalpal, DeadEyeArrow, Closedmouth, GraemeL, Egumtown, Stefan favorsky, Baxil, Veinor, A bit iffy, SmackBot, Royalguard11, Hydrogen Iodide, Gnaragarra, J.J.Sagnella, Ohnoitsjamie, Skizzik, Chris the speller, Optikos, @modi, MK8, DHN-bot-enwiki, Colonies Chris, Firetrap9254, Ko-jieroSaske, SheeEttin, Frap, Skidude9950, Ww2ensor, Flask215, Khoikhoi, Engwar, Nakon, Gamgee, Kalathalan, Clicketyclack, James Allison, OcarinaOfTime, Ckatz, Tuanmd, Redboot, Ehheh, InedibleHulk, Njb, Mets501, H, Kvng, Mike Doughney, Pausic, Grendzy, Sander Säde, OnLine, Jeremy Banks, JForget, Dycedarg, Jesse Viviano, Gogo Dodo, CorpX, Alexdw, Odie5533, Tawkerbot4, Bposert, DumbBOT, SJ2571, Njan, Alexey M., Ebpr123, FTAAP, Snydley, RamiroB, Sheng.Long 200X, Druiloor, AntiVandalBot, Luna Santin, Seaphoto, Fayenatic london, Zorgkang, Spydex, Qwerty Binary, Dreaded Walrus, JANDBot, Thylacinus cynocephalus, Tony Myers, Barek, Bakasuprman, A1ecks, Hut 8.5, TAnthony, Isthistringon, Techie guru, .anacondabot, Magioladitis, Jaysweet, Ukuser, JNW, Cheezyd, Confiteordeo, Fedia, Wikivda, Wikire, MartinBot, STBot, CliffC, Jonathan.lampe@standardnetworks.com, Anaxial, Keith D, Nono64, Spider, Tresmius, Slash, J.delanoy, Pharaoh of the Wizards, Cyrus abdi, Renamed user 5417514488, Samtheboy, Noogenesis, VolkovBot, TreasuryTag, MemeGeneScene, Jeff G., Philip Trueman, TXiKiBoT, Mrdave2u, Zifert, A4bot, Glarosa, Isis4563, Madhero88, Dirkbb, Turgan, Jjjccc~enwiki, ChewyCaligari, Rock2e, Resurgent insurgent, Cool110110, SieBot, Triwbe, Sephiroth storm, Nmvwi, Arda Xi, OsamaBinLogin, Banditauren, Tombomp, Clearshield, Dillard421, ArchiSchmedes, ClueBot, Wilbur1337, The Thing That Should Not Be, AsympoteG, Garyzx, Dotmax, Blanchardb, Asalei, Socrates2008, Rhododendrites, Technobadger, Manasjyoti, Arjayay, Drwho-for, Shin-chan01, El bo de la dieta, DanielPharos, Berean Hunter, Johnuniq, SF007, Noname6562, Darkicebot, Against the current, XLinkBot, Spitfire, Stickee, Rror, Dom44, Lamantine, WikHead, Dsimic, Tustin2121, Addbot, Mortense, Movingboxes, Rhinostopper, MrOllie, Etracksys, Matt5075, Networkintercept, Favonian, ChenzwBot, Sureshot327, Tide rolls, Willondon, MuZemike, Luckas-bot, Yobot, 2D, Bigtophat, Navy blue84, AnomieBOT, Andrewrp, Kingpin13, Ulric1313, Materialscientist, Are you ready for IPv6?, Human, HkBattousai, GB fan, LilHelpa, Xqbot, Dragonshardz, Jeffrey Mall, Reallymoldycheese, Automaite, Ezen, S0aasdf2sf, Aceclub, RadiX, GrouchoBot, IslandLumberJack, Mark Schierbecker, Krypton3, 78.26, Aenus, Mountilee, Prari, FrescoBot, WPANI, Clubmaster3, DigitalMonster, PeramWiki, Nathancac, Waller540, HamburgerRadio, Italick, Redrose64, Tom.Reding, Rajtuhin, Serols, MKFI, Just a guy from the KP, AgentG, Reconsider the static, Ao5357, Lotje, Vrenator, Mean as custard, F11f12f13, Sloppyjosh, Forenti, DASH-Bot, J36miles, EmausBot, Manishfusion1, GoingBatty, Wikipelli, LinuxAngel, FlippyFlink, John Cline, Ida Shaw, Traxs7, S3cr3tos, Δ, Donner60, Ego White Tray, AlexNEAM, ClueBot NG, Matthiaspaul, O.Koslowski, Mactech1984, Lolpopz1234, Marsmore, Nbudden, BG19bot, IraChesterfield, Samiam111-enwiki, Guesst4094, Carliitaeliza, MeanMotherJr, BattyBot, Abelcartel, Jfd34, Millennium bug, David.moreno72, Lloydiske, EagerToddler39, Codename Lisa, Webclient101, Klabor74, Zhiweisun, Jaericsmith, Sourov0000, Corn cheese, Way2veers, Yuvalg9, MountRainier, JadeGuardian, Ugog Nizdast, Kennethaw88, Lvanwaes, Mover07, Jianhui67, Dannyruthe, NewWorldOdor, FockeWulf FW 190, Janeandrew01, Michael Dave, CNMall41, Jamesmakeon, Bobsd12, Wasill37, KH-1, Crystallized-carbon, Scyrusk, Hayman30, Zabshk, JoanaRivers, ScottDNelson, Jhfhey, Awmarks, Muhammad mobeen83, BD2412bot, Wikijagon, Sharanyanaveen, Ivory Dream, White Arabian Filly, Qzd, InternetArchiveBot, The Voidwalker, Chrisprice07, John "Hannibal" Smith, Phillipsreggie999, James Samwise Ganji, JAMES MCGUMMERY, Deshawn992, Deshawn991, Jameshardwell, Khorkhe, Luigiboy260, Richardparker119, Supportpc, Bender the Bot, CwestOak, Magic links bot, Jhen Daguinotas, Alex iv75 and Anonymous: 591
- **Computer access control** *Source:* https://en.wikipedia.org/wiki/Computer_access_control?oldid=779527209 *Contributors:* Kku, BD2412, Anomalocaris, DragonHawk, Headbomb, Jarble, Yobot, Timothyhouse1, Jasonanaggie, Frietjes, BG19bot, Cfeltus, Lagoset, Monkbot, Crystallizedcarbon, Alsaheri and Anonymous: 11
- **Application security** *Source:* https://en.wikipedia.org/wiki/Application_security?oldid=777602852 *Contributors:* SimonP, Kku, Charles Matthews, Psychonaut, DavidCary, Cloud200, Hillel, AliveFreeHappy, Discospinster, Rhobite, Enric Naval, JYolkowski, Bobrayner, OwenX, Mindmatrix, Halovivek, Vegaswikian, Pseudomonas, Welsh, Tjarrett, Slicing, NielsenGW, Rwww, Algae, Tyler Oderkirk, SmackBot, Ohnoitsjamie, Frap, JonHarder, IronGargoyle, Kvng, Iridescent, Sander Säde, Tedmarynicz, OnPatrol, Blackjackmagic, Njan, Aarnold200, Dawnseeker2000, Obiwankenobi, Dman727, Robina Fox, Toutoune25, JLEM, Grabon-enwiki, IronAlloy, JEMLA, DatabACE, Maurice Carbonaro, Maxgleeson, Alanfeld, Philip Trueman, Felmon, Pryder100, NEUrOO, M4gnun0n, Friendlydata, Dosco, Swtechwr, Wiscoplay, Dcunitied, Raysecurity, XLinkBot, Paulmnguyen, Dthomsen8, Mitch Ames, Ha runner, Bookbrad, MrOllie, Eheitzman, Jnarvey, Yobot, Fraggle81, Nickbell79, AnomieBOT, Fhuonder, Stationcall, Mwd, FrescoBot, Nageh, Geofhill, Amey.anekar, Hnguyen322, Trappist the monk, Vrenator, Mr.moyal, Super n1c, We hope, ClueBot NG, Aashbel-enwiki, Widr, RachidBM, BG19bot, MatthewJPJohnson, Swameticul, Xena77, Mdann52, Tohimanshu, Triomio, Isoron27000, Roberto Bagnara, Truehorizon, Securechecker1, Jpickel, MuscleheadNev, IagoQnsi, Chrisdmiller5, KH-1, Greenmow, Milan2377, Abigailw, Prugile, InternetArchiveBot, GreenC bot, Bjm243wiki, Collingreene, AvaleronV and Anonymous: 79
- **Antivirus software** *Source:* https://en.wikipedia.org/wiki/Antivirus_software?oldid=794071797 *Contributors:* Bryan Derksen, Zundark, Danny, Fubar Ofbusco, William Avery, DennisDaniels, Edward, Pnm, Kku, Tannin, Tgeorgescu, Minesweeper, CesarB, Ronz, Yaronf, Rlandmann, Whkoh, Stefan-S, Nikai, IMSoP, RickK, Pedant17, Furrykef, Tempshill, Omegatron, Pakaran, Shantavira, Robbot, Chealer, Boffy b, Calimero, RedWolf, Altenmann, KellyCoinGuy, Iaen, Delpino, Lzur, David Gerard, Fabiform, Graeme Bartlett, Laudaka, Eran, Noone-enwiki, Rick Block, AlistairMcMillan, Solipsist, Wmahan, Utcursh, SoWhy, Beland, Piotrus, Cynical, Gcschoyru, TonyW, Hobart, Eisnel, Discospinster, Rich Farmbrough, Bender235, ESkog, JoeSmack, Evice, Aecis, Chungy, PhilHibbs, Sietse Snel, Femto, Perfecto, Stesmo, Longhair, Orbst, Richi, TheProject, Troels Nybo-enwiki, Timsheridan, Hagerman, Alansohn, CyberSkull, Conan, PatrickFisher, Babajobu, Stephen Turner, Snowolf, Wtmitchell, Downlode, Rotring, Nightstallion, Umapathy, Woohookitty, Mindma-

trix, Armando, Robwingfield, Pol098, Urod, Isnow, Kralizec!, Pictureuploader, Palica, Matturn, Cuvtixo, Kbdank71, Yurik, Ryan Norton, Rjwilmsi, DirkvdM, RainR, FlaBot, JiFish, RexNL, Gurch, DavideAndrea, ChongDae, Born2cycle, Melancholie, Ahunt, Peterl, Gwerndl, YurikBot, Wavelength, Borgx, Grizzly37, Wfried, Arado, TheDoober, Pi Delport, SpuriousQ, Akhristov, Clunia, NawlinsWiki, Hm2k, Badagnani, Archnad, CecilWard, Vlad, Bota47, Bokonon~enwiki, BazookaJoe, GraemeL, Peter, Caballero1967, Fourfourfour, Hirebrand, Jaysbro, Eptin, タチコマ robot, Dunxd, Cumbiagermen, Firewall-guy, SmackBot, Although, JurgenHadley, J7, Dxco, Relaxing, Easygoeasycome, Gilliam, JorgePeixoto, Lakshmin, Gary09202000, Chris the speller, Egladkh, Morte, EncMstr, Jerome Charles Potts, Bigs slb, DHN-bot~enwiki, Uniwares, Darth Panda, Frap, JonHarder, Korinkami, 03vaseyj, SundarBot, Cybergobra, Valenciano, Mwtoews, Ihateregister, Oo7jeep, Gobonobo, Capmo, NongBot~enwiki, 16@r, Erotnl, Beetstra, Doczilla, Qu4rk, Cronos Warchild, Caiaffa, Hu12, DabMachine, SimonD, Phantomnecro, UncleDoggie, CapitalR, Kirill Chiryasov, Karunamon, Courcelles, Tawkerbot2, Fdssdf, FleetCommand, CmdrObot, BENNYSOFT, Jesse Viviano, NaBUru38, Chrisahn, Cydebot, Gogo Dodo, Xhopingtearsxxx, AcceleratorX, Tawkerbot4, Khattab01~enwiki, Ohadgliksman, The Mad Bomber, SpK, Neustradamus, Mikewax, TAG.Odessa, Dimo414, Thijs!bot, Jdivakarla, Leedeth, LemonMan, Saibo, Dalahäst, RickinBaltimore, TurboForce, Dawnseeker2000, Mentifisto, AntiVandal-Bot, Sjconrad-mchedrawe, Gökhane, Serpent's Choice, JAnDbot, Kaobear, Meinsla, MER-C, Tushard mwti, TAnthony, anacondabot, Raanoo, Penubag, Bongwarrior, Lotusv82, Proland, The Kinslayer, JohnLai, Gomm, Xeolyte, Chris G, DerHexer, Hdt83, Martin-Bot, STBot, CliffC, FDD, Icenine378, CommonsDelinker, Emilinho~enwiki, J.delanoy, Pharaoh of the Wizards, Dinoguy1000, Theo Mark, Jesant13, Turbulencepb, Neon white, Rippdog2121, Tokyogirl79, 5theye, Patrickjk, AntiSpamBot, Dougmarlowe, DadaNeem, Pandawelch, White 720, Jamesontai, Idioma-bot, Javeed Safai, Melovfemale, VolkovBot, AlnoktaBOT, Philip Trueman, DoorsAjar, TXiKiBot, Oshawah, Emedlin1, Mujidat61, Vipinhari, Technopat, Anonymous Dissident, Qxz, Corvus cornix, LeaveSleaves, Natg 19, Tmalcomv, Haseo9999, C45207, Ngantenguyen, LittleBenW, Fredtheflyingfrog, Lonwolve, Wrldwzrd89, Sahilm, Derekeslater, News-partnergroup, Swaq, Sephiroth storm, Yintan, Miremare, Mothmolevna, Jerryobject, Flyer22 Reborn, PolarBot, Nosferatus2007, Askild, Topicle, OKBot, Cameron Laird, Plati, Samker, PrimeYoshi, Sitoush, Escape Orbit, Arnos78, Martarius, Tanvir Ahmmmed, Leaht-wosaints, ClueBot, Kl4m, The Thing That Should Not Be, IceUnshattered, Trotline, Spuernase, Freebullets, Mild Bill Hiccup, Ka vijay, LizardJr8, ChandlerMapBot, Georgest23, Rockfang, DragonBot, Excirial, Socrates2008, Pavix, Tyler, Pladook, Aurora2698, Jotterbot, JamieS93, ChrisHodgesUK, DanielPharos, Versus22, Johnnuniq, SoxBot III, Apparition11, SF007, Sensiblekid, XLinkBot, Rror, Mavenkatesh, Svarya, HexaChord, Addbot, Xp54321, Wizho, Mortense, Nuno Brito, Softfreak, Sergey AMTL, Vatrena ptica, CanadianLinuxUser, Fluffernutter, Ankitguptajaipur, Kueensryche, NjardarBot, WorldlyWebster, MrOllie, CarsracBot, FluffyWhite-Cat, Womanitoba, ChenzwBot, Jasper Deng, Mike A Quinn, Katharine908, Tide rolls, Luckas Blade, Teles, Luckas-bot, Yobot, THEN WHO WAS PHONE?, Wonderfl, AnomieBOT, Jim1138, DMWuCg, Roastingpan, Blueraspberry, Materialscientist, Police267, Citation bot, Kalamkaa, Eumolpo, LilHelpa, Cameron Scott, Misi91, Avun, XZeroBot, Sputink, Rwmoeckoe, S0aaasd2sf, Frosted14, Sas-soBot, ReformatMe, Mathonius, VB.NETLover, TheRyan95, Shadowjams, Diablosblizz, Samwb123, G7yunghi, FrescoBot, GunAl-chemist, WPANI, Yuyujoke, Mi8ka, HJ Mitchell, Craig Pemberton, Franklin.online2006, Expertour, HamburgerRadio, Redrose64, SuperAntivirus, Marnegro, Pinethicket, HRoestBot, Skyerise, Paulsterne, A8UDI, Ma2001, Kostes32, One666, Seam123, AntonST, Σ, Meaghan, Salvidrim!, Ravensburg13, Cnwilliams, Trappist the monk, Lamarmote, Miiszmyle, LogAntiLog, Lotje, Callanec, Wikipandaeng, Vrenator, TBloemink, 777sms, Neshemah, Diannaa, Ivanvector, Hornlitz, Exeter, Teenboi001, Mean as custard, Rjwilmsi-Bot, Ripchip Bot, Panda Madrid, Enauspeaker, DASHBot, EmausBot, John of Reading, WikitanvirBot, Immunize, Philtweir, Hercules31, Dinh tuydzao, Ibbn, RA0808, Ryanxo, Tommy2010, Cmlloyd1969, Dcirovic, Emenid, Elison2007, Fæ, Mats131, MorbidEntree, ElationAviation, Makecat, Skyinfo, Yabbad7, Champion, Rickrap707, Difame, ChuispastonBot, GermanJoe, Pastore Italy, EdoBot, Kandr8, PetrB, ClueBot NG, Lzelts, TheKaneDestroyer, Jack Greenmaven, Satellizer, LK20, Dfarrell07, Multiwikiswat, Piyush1992, JuventiniFan, Malijinx, Widr, Hsinghsarao, Joseph843, Helpful Pixie Bot, Dwe0008, HMSSolent, Krenair, Jezal87, Janendra, Arturnyc, Carl.schutte, AvocatoBot, Thekillerpenguin, AngusWOOF, Teksquisite, Irfanshaharuddin, TheMw2Genius, Kremnin, Newmen1020304050, BattyBot, Justincheng12345-bot, David.moreno72, JC.Torpey, Divonnais, Farqad, IddiKlu, Nisha1987, Rohanek-nathshinde459, Garamond Lethe, JYBot, Dark Silver Crow, Codename Lisa, Cryptodd, Lelomark, Pegururu66, K1ngXSp3c1al, Lugia2453, RMCD bot, Kumarworld2, Sourov0000, Seo100, Me, Myself, and I are Here, M.R.V model, Gautamcool12, Faizan, I am One of Many, Ryan889, Matt.Sharp98, Jakec, EddyMc1, Ashajose0002, Assumption, Ginsulof, Quenhitran, Dannyruthe, Noyster, FockeWulf FW 190, MetalFusion81, Robevans123, Thinkcomputing, Monkbot, CodyHofstetter, TerryAlex, MRD2014, Xpasindu123, Thetechgirl, KH-1, Randomuser0122, ChamithN, WikiGopi, Jacbizer, DpkgDan, Puffle7275, Deanwalt123, Rom broke, Drop knowhow, Seanpatrickgray, Alfarish, Fluffyvoir, Natasha Miranda, TerraCodes, Chenthil Vel, Cyberstip, Chenthil Vel Murugan 1986, Srilekha selva, Sharanyanaveen, Dilipanch, XxXMinecraftProsnipzXXX, Mar11, InternetArchiveBot, GreenC bot, Satish0143, Lolo1299008, Guy4you, Plmnbcvcxz12, Lytebyte, Adeel02, Bender the Bot, SERVO SWAMI, Harshitgpt89, Rbenvenisti, Murkl, Shaikh Imran, Hr3r34t5ge3r4t4rf, Sapnamalik, Techsupportaustralia and Anonymous: 709

- **Secure coding** *Source:* https://en.wikipedia.org/wiki/Secure_coding?oldid=777741523 *Contributors:* AliveFreeHappy, H2g2bob, Bo-brayner, Malcolma, Cedar101, SmackBot, Frap, Alaibot, QuiteUnusual, Manionc, Fabrictramp, Susan118, Addbot, Elviscrc, Luckas-bot, Shantzg001, John of Reading, Bk314159, Helpful Pixie Bot, Richu jose, Monkbot, CodeCurmudgeon, Mkhaliil purdue and Anonymous: 5
- **Secure by design** *Source:* https://en.wikipedia.org/wiki/Secure_by_design?oldid=774917761 *Contributors:* Aeazram, Kku, LMB, Joy, Gracefool, Vadmium, AndrewKeenanRichardson, Sam Hocevar, Andreas Kaufmann, Sperling, Project2501a, Ciaran H, Mailer diablo, Pol098, Josh Parris, Koavf, Volfy, FlaBot, Quuxplusone, Tardis, Gardar Rurak, Ptomes, Bovineone, Mcicogni, Drable, Alex Ruddick, SmackBot, Mmernex, Mauls, Commander Keane bot, Chris the speller, Wonderstruck, Hu12, CmdrObot, Towopedia, Dawnseeker2000, Manionc, Dougher, Gwern, Nono64, Warut, Alecwh, Zoef1234, Goodone21, XLinkBot, Addbot, Luckas-bot, AnomieBOT, Teriyak-istix, LucienBOT, Sae1962, John of Reading, WikitanvirBot, TheSophera, Klbrain, はんぞう, Wes.turner, Gary Dee, Frijtjes and Anonymous: 22
- **Security-focused operating system** *Source:* https://en.wikipedia.org/wiki/Security-focused_operating_system?oldid=791822097 *Contributors:* The Anome, Kku, Graue, PatriceNeff, David Latapie, Dysprosia, Maximus Rex, Taxman, Joy, Finlay McWalter, Chealer, Hadal, Foot, Ricky~enwiki, Kusunose, Sam Hocevar, Bluefoxicity, DMG413, Projex, Till Ulen, FT2, MeltBanana, Sperling, Bender235, Spearhead, Miles Monroe~enwiki, NicM, Bobrayner, Pol098, Ruud Koot, Qwertyus, Dar-Ape, Nihiltres, Jrtayloriv, BMF81, Bgwhite, Ptomes, Etbe, Diaelectric, Mosquitopsu, Ilmaisin, Janizary, Allens, SmackBot, Gizmoguy, Izzy, Frap, JonHarder, Klimov, Vdanen, Harryboyles, La Cigale, MaxEnt, Nowhere man, Editor at Large, TurboForce, Widefox, Dougher, JonathanCross, NapoliRoma, Transcendence, Wkussmaul, Doc aberdeen, Cpiral, 83d40m, Dlewis7444, Penma, Benbucks, Allong, Maximillion Pegasus, Canaima, Toddst1, Jojalozzo, Mild Bill Hiccup, Xenon54, Ravaet, SF007, Useerup, Paulmnguyen, JamieGoebel, Addbot, Hybrasil, C933103, Yobot, AnomieBOT, ChristopheS, Ojakubcik, FrescoBot, NuclearWizard, Mdjango, David Hedlund, JumpDiscont, Diannaa, Wrix24x7, John of Reading, WikitanvirBot, GoingBatty, Peaceray, Wafelijzer, ClueBot NG, Solbu, BG19bot, WikiTryHardDieHard, Akuckartz, Gotimer, Unconventional2, Cyberbot II, NewGuy1001, MrFrety, EveningStarNM, Comp.arch, Oranjelo100, Ostree, Zakraye, Eclipses-

park, LoudLizard, Miraclexix, MrArsGravis, R3sJAP155M, Hail knowledge, GreenC bot, John "Hannibal" Smith, Michael Reed, Bender the Bot, Carlelliss, 妖魔鬼怪快啲走, Alexhaydock, Lj, Robot375623, WannaUnix and Anonymous: 105

- **Authentication** *Source:* <https://en.wikipedia.org/wiki/Authentication?oldid=793072289> *Contributors:* SJK, Mswake, Imran, Edward, Gbroiles, EvanProdromou, Pnm, MartinHarper, (, Pde, EntmootsOfTrolls, Smack, Edmilne, M0mms, Ww, Nickshanks, Altenmann, Nurg, Lowellian, Rholton, Tea2min, Mark.murphy, Tom-, Rchandra, Matt Crypto, Pgan002, Beland, Heavy chariot, Ablewisuk, Oneiros, Almit39, Rich Farmbrough, Tpokorra, ArnoldReinhold, Pavel Vozenilek, Goochelaar, Bender235, Szquirrel, Edward Z. Yang, Billymac00, John Vandenberg, SpeedyGonsales, Cherlin, HasharBot-enwiki, ClementSeveilliac, Johntinker, DreamGuy, H2g2bob, HenryLi, Ceyockey, Roland2~enwiki, Rodii, Woohookitty, Mindmatrix, RHaworth, Daira Hopwood, Kokoriko, Shonzilla, Bernburgerin, Jorunn, Rjwilmsi, Pdelong, Husky, Syced, Fish and karate, Emarsee, Margosbot-enwiki, LeCire-enwiki, YurikBot, Wavelength, RobotE, RussBot, Backburner001, DanMS, Theshadow27, Bachrach44, Cryptosmith, Leotohill, Bota47, PanchoS, Metadigital, Zzuuzz, GraemeL, SmackBot, Imz, EJVargas, KocjoBot-enwiki, Arny, Yamaguchi 先生, Ohnoitsjamie, Lakshmin, Chris the speller, Bluebot, DHNbot-enwiki, Tsca.bot, Skidude9950, JonHarder, Arnneisp, Radagast83, Tjcoppet, Luís Felipe Braga, Kuru, Spiel496, Nabeth, Kvng, Hu12, DouglasCalvert, Polly matzinger, Dan1679, WeggeBot, Thepofo, Ednar, Cydebot, Xemoi, UncleBubba, Bdpg, Jose.canedo, Dancer, AngoraFish, Lindenhills, Nuwesco, Thijs!bot, Epbr123, Sqying, EdJohnston, Dawnseeker2000, AntiVandalBot, Fedayee, Rshoham, Blmatthews, EJNorman, AndreasWittenstein, JAnDbot, Durrantm, Ingvar2000, Jheiv, Wilm, Technologyvoices, Darth Andy, Magiolditis, Rami R, AlephGamma, Gabriel Kielland, David Eppstein, User A1, Ludvikus, JaGa, STBot, Bnwick, Bertix, Rlsheehan, Syphertext, Nigelshaw, Homer Landskirty, Idioma-bot, VolkovBot, TXiKiBoT, NoticeBored, Technopat, Rei-bot, Aymath2, Steven J. Anderson, Jackfork, Mayahlynn, Double Dickel, SieBot, Euryalus, WereSpielChequers, Pkgx, Mdsam2~enwiki, Yerpo, Skippydo, Pinkadelica, Stlmh, Denisarona, Sfan00 IMG, ClueBot, Mild Bill Hiccup, Wikiodl1, Trivialist, Neverquick, Apelbaum, Jomsborg, Captipossum, The Founders Intent, Ykhwong, Primasz, BOTarate, Bludpojke, Versus22, Boozinf, Apparition11, XLinkBot, Dmg46664, Avoided, Dsimic, Addbot, Fyrael, Ronhjones, EconoPhysicist, Wireless friend, Yobot, PinkTeen, MarioS, THEN WHO WAS PHONE?, Pavanthatha, AnomieBOT, DemocraticLuntz, Galoubet, Materialscientist, ArthurBot, DSisypBot, Mywikiid99, GrouchoBot, Omnipaedista, RibotBOT, Dtodorov, Shadowjams, Talion86, Jmd wiki99, Id babe, Nageh, D'ohBot, Teux, WikiBenutzer, MastiBot, Littledogboy, Hnguyen322, Trappist the monk, Anavaman, Lotje, Ashdo, Mean as custard, Kiko4564, AnBuKu, EmausBot, Goldenbrook, WikitanvirBot, Timtempleton, Zollerriia, Active Banana, Clymbon, Tommy2010, ValC, Dcirovic, K6ka, FlippyFlink, Jahub, Quondum, Davy7891, Fakeshop, Donner60, Newstv11, ClueBot NG, MelbourneStar, Frietjes, 0x55534C, Curb Chain, Mahfudien, Mt 1985, Mike2learn, OnlinepresenceHID, MusikAnimal, CitationCleanerBot, Wikisafety, Daniel.N.Rollins, RockOrSomething, FoCuSandLeArN, Cryptodd, TwoTwoHello, Lugia2453, Maruleth, Pipat.poonP1, Kmaletsky, DavidLeighEllis, Ugoz Nizdast, UKAmerican, SoaringSouls, Sticky molasses, Monkbot, ScienceGuard, Mounikamm, Narky Blert, MarianneMiller, Ana286, Wrtr63, CAPTAIN RAJU, NewYorkActuary, Aiwlwttok, CLCStudent, Thinusnaa, Blue Edits, SarahSmith(Laser Eng), Bender the Bot, Adsiah, Satishkarry, Marcelo.brocardo, Aries-san, Leslie Tomlinson and Anonymous: 245
- **Multi-factor authentication** *Source:* https://en.wikipedia.org/wiki/Multi-factor_authentication?oldid=794360843 *Contributors:* Ant, Edward, Nealmcb, Pnm, William M. Connolley, Julesd, JimTheFrog, Pabouk, Cloud200, Alexf, Robert Brockway, AlexKilpatrick, ArnoldReinhold, Alexanderino, Mindmatrix, BD2412, Koavf, Czar, Intgr, Wavelength, Pontillo, ViperSnake151, SmackBot, McGeddon, Rojomeko, Xaosflux, Ohnoitsjamie, Thumperward, Snori, MovGPO, Jmnbatista, Kuru, Kvng, ETSkinner, Nick Number, Dawnseeker2000, Dougher, Froid, Firealwaysworks, David Eppstein, DGG, Bwranch, Krishnachandranvn, Atropos235, Cowillia, Edvvc, Softtest123, JL-Bot, Martarius, Niceguyedc, MarcelW, Dsimic, Addbot, Mortense, Otisjimmy1, MrOllie, Worch, Wireless friend, Yobot, MarioS, There'sNoTime, Sweerek, AnomieBOT, Bluerasberry, Materialscientist, LilHelpa, Supcmd, Biker Biker, Chris Caven, ItsZippy, Lotje, Anongork, GoingBatty, Bpburns88, HupHollandHup, Neil P. Quinn, Rocketrod1960, ClueBot NG, Snotbot, MerlIwBot, Lowercase sigmabot, BG19bot, Turtle595, Encyclopedant, Mark Arsten, CitationCleanerBot, BattyBot, David.moreno72, Suncatcher 13, Zhaofeng Li, Mdann52, Cyberbot II, Dicti0nary0, Hbiering, Radiochemist, Qxukhgiels, Dexbot, Codename Lisa, Gacelperfinian, Basilphilipsz, Me, Myself, and I are Here, Dave Braunschweig, Lsmll, BB609, MesaBoy77, Comrade pem, NickyLarson29, Kwaimind, Dudewhereismy-bike, Rosstaylor3b, Sticky molasses, Benforrest, Pfalcon2, Dylan-Evans-not-the-other-one, 19JKG96, Nyashinski, Vieque, Srijanshasti, KH-1, TheCoffeeAddict, Sinchdev, Baylott, Drahtloser, Joemates, Walter.Jessica, GreenC bot, Stuckfly, JimSullivan, Exception e, Bishop-9-Echo, Bloggingyan, Russcore, Ariessan, Magnushubner, PaulBoskabouter and Anonymous: 90
- **Authorization** *Source:* <https://en.wikipedia.org/wiki/Authorization?oldid=787317225> *Contributors:* Michael Hardy, Pnm, Kku, Mu-lad, PBS, Lowellian, Wikibot, Mark.murphy, Mark T, Tagishsimon, ArnoldReinhold, Lectionar, Cjcollier, Dave.Dunford, Ringbang, HenryLi, Rodii, Mindmatrix, BD2412, BMF81, RobotE, RussBot, Ru.spider, Gaius Cornelius, Theshadow27, Rupert Clayton, Bota47, Deville, GraemeL, SmackBot, Betacommand, JonHarder, MichaelBillington, Tjcoppet, Luís Felipe Braga, 16@r, DI2000, TwistOfCain, Rgrov, The Transhumanist, Anaxial, Emeraude, Metrax, NewEnglandYankee, Althepal, VolkovBot, Philip Trueman, TXiKiBoT, Oshawah, MrMelonhead, Mazarin07, Jamelan, Jaap3, Cnilep, SieBot, Gerakibot, Sean.hoyland, Josang, Niceguyedc, Socrates2008, SoxBot III, Ali farjami-enwiki, Dsimic, Addbot, Fyrael, MrOllie, Lightbot, Luckas-bot, Yobot, MacTire02, Materialscientist, Joining a hencing, Jordav, JimVC3, GrouchoBot, Omnipaedista, Nageh, Edajgi76, Danbalam, Just a guy from the KP, Hnguyen322, EmausBot, WikitanvirBot, Timtempleton, Akjar13, Sam Tomato, Winner 42, Ellisun, Shengzhongxie, Wbm1058, BattyBot, ChrisGaultieri, Kupiakos, Codename Lisa, JustBerry, GeoffreyT2000, Crystallizedcarbon, ARIENGGO ARIE, MB, Thinusnaa, AbdulrahmanMohammedYousef, Cici-lindholm and Anonymous: 69
- **Data-centric security** *Source:* https://en.wikipedia.org/wiki/Data-centric_security?oldid=790322945 *Contributors:* Kku, Shiftchange, ShakespeareFan00, Jytdog, Dekart, Idumont, SwisterTwister, BG19bot, DaltonCastle, Me, Myself, and I are Here, David.brossard and Anonymous: 1
- **Firewall (computing)** *Source:* [https://en.wikipedia.org/wiki/Firewall_\(computing\)?oldid=794225207](https://en.wikipedia.org/wiki/Firewall_(computing)?oldid=794225207) *Contributors:* Paul-enwiki, Nealmcb, Michael Hardy, Pnm, Egil, Ahoerstemeier, Copsewood, Haakon, Jebba, Sugarfish, Rl, Dcoetzee, Jay, DJ Clayworth, Taxman, Bevo, Topbanana, Joy, Khym Chanur, Robbot, ZimZalaBim, Danutz, Auric, Jondel, Hadal, Diberri, Tea2min, Pabouk, Giftlite, Yama, Everyking, Rchandra, AlistairMcMillan, Eequor, Matthäus Wander, Wiki Wikardo, DemonThing, Wmahan, Stevietheman, ConradPino, Antandrus, Ricky~enwiki, Mitaphane, Biot, Deewiant, Joyous!, Hax0rw4ng, Asquella, Mernen, IgnoredAmbience, Monkeyman, Discospinster, Fabioj, Wk muriithi, EliasAlucard, Smyth, YUL89YYZ, Deelkar, DonDiego, Pmetzger, El C, Mwanner, Dols, Spearhead, Linkoman, RoyBoy, Femto, Jpgordon, Bobo192, Smalljim, Enric Naval, Viriditas, Giraffedata, Danski14, Alansohn, Anthony Appleyard, Interiot, Malo, Wtmitchell, Velella, L33th4x0rguy, Rick Sidwell, IMeowbot, Henry W. Schmitt, TheCoffee, DSatz, Kenyon, Brookie, Zntrip, Andem, Nuno Tavares, Angr, OwenX, Woohookitty, Karnesky, Mindmatrix, Dzordzm, Bazsi-enwiki, Kralizec!, Prashanthns, DE-Siegel, Turnstep, Ashmoo, Graham87, Chun-hian, Kbdank71, FreplySpang, Jclemens, Rjwilmsi, OneWeirdDude, Eptalon, NeonMerlin, ElKevbo, Sferrier, Dmccreary, Gurch, DevastatorIIC, Intgr, Alphachimp, OpenToppedBus, Ahunt, Marcuswittig, DVdm, FeldBum, Bg-white, Theymos, YurikBot, Wavelength, Borgx, TexasAndroid, Quentin X, Sceptre, Alan216, MMuzammils, RussBot, Mattgibson, Lin-colnite, Pi Delport, Stephenb, Manop, Rsrikanth05, Wimt, Capi, NawlinWiki, ENeville, Trevor1, Rebel, Mortein, Cryptosmith, Jpbownen,

Voidxor, Bkil, Zwobot, Bucketsofg, Black Falcon, Mcicogni, CraigB, Nlu, Wknight94, Rwxrwxrwx, Dse, JonnyJinx, Closedmouth, E Wing, Pb30, ILRainyday, Chriswaterguy, Talyian, Cffrost, Anclation~enwiki, Maxamegalon2000, Bswilson, A13ean, SmackBot, Un-school, Rbmccutt, KnowledgeOfSelf, C.Fred, Od Mishehu, Eskimbot, Vilerage, Info lover, Xaosflux, Gilliam, Ohnoitsjamie, Lakshmin, Bluebot, DStoykov, Jprg1966, Thumperward, Mcj220, Snori, Oli Filth, Prasan21, Lubos, Elagatis, DavidChipman, DHN-bot~enwiki, Da Vynci, Anabus, Suicidalhamster, Abaddon314159, Can't sleep, clown will eat me, Frap, Chlewbot, JonHarder, Yorick8080, Fynali, Celarnor, Meandtheshell, Ntolkin, Aldaron, Nachico, Elcasc, HarisM, Skrewz~enwiki, Phoenix314, LeoNomis, FerzenR, Andrei Stroe, Ugur Basak Bot~enwiki, The undertow, Harryboyles, Eldrac0, Mattloaf1, Melody Concerto, Beetstra, Boomshadow, Feureau, Gondoleyley, Peyre, Kvng, Hu12, Hetal, BranStark, BananaFiend, Jhi247, Robbie Cook, Newone, GDallimore, Pmattos~enwiki, Tawkertbot2, Chetvorno, SkyWalker, JForget, FleetCommand, Ale jrb, Megaboz, JohnCD, Topsplnslams, Kgentryjr, Random name, Lazulilasher, WeggeBot, Josemi, Nnp, Eqwendil, Phatom87, Cydebot, T Houdijk, Mashby, UncleBubba, Gogo Dodo, Tbird1965, Hamzanaqvi, Guitardemon666, Ilrate, Omicronpersei8, Thijs!bot, Danhm, Epbr123, Barticus88, Kubanczyk, Dschrader, Pajz, Randilyn, Simeon H, Marek69, SGGH, Chrisdab, CharlotteWebb, Wai Wai, Dawnseeker2000, AntiVandalBot, RoMo37, Davidoff, Purpleslog, Isilanies, Vendettax, LegitimateAndEvenCompelling, Dougher, ShyShocker, DoogieConverted, Dman727, Deadbeef, Acrosser, JAnDbot, Sheridp, MER-C, Seddon, Lucy1981, Tushard mtwi, Kjwu, Jahoee, Raanoo, VoABot II, AtticusX, Maheshkumaryadav, Swpb, Djdancy, Hps@hps, Cellspark, Twsx, Dean14, AlephGamma, Gstroot, LeinaD natipaC, Hans Persson, Nposs, Greg Grahame, Just James, DerHexer, Rtouret, Hbent, Jalara, XandroZ, Seba5618, Tommysander, MartinBot, CliffC, LeonTang, R'n'B, Ash, PrestonH, Thirdright, J.delanoy, Night-Falcon90909, Shawniverson, Ans-mo, Jigesh, L'Aquatique, !Darkfire!6'28'14, Molly-in-md, KCinDC, STBotD, Equazcion, Red Thrush, Beezhive, Halmstad, SoCalSuperEagle, Idioma-bot, Zeroshell, Jramsey, Timotab, VolkovBot, Mike.batters, Jeff G., Indubitably, Al-noktaBOT, VasilievVV, Venom8599, Philip Trueman, Apy886, Oshawah, Jackrockstar, Cedric dlb, Ulrichlang, OlavN, Anna Lincoln, Corvus cornix, David.bar, Sanfrannman59, Justin20, Jackfork, LeaveSleaves, Seb az86556, Lolsalad, Yk Yk Yk, Phirenzie, Why Not A Duck, Brianga, MrChupon, JasonTWL, EmxBot, Hoods11, SieBot, EQ5afN2M, Jchandlerhall, YonaBot, Sephiroth storm, Yintan, Miremare, Calabraxthis, Milan Kerslager, Android Mouse, Hokiehead, JSpong, Hazawazawaza, Goodyhusband, Doctorfluffy, Oxy-moron83, Nuttycoconut, Tombomp, C'est moi, Mygerardromance, Altzinn, WikiLaurent, Bryon575, Ipostinouno, Berford, Escape Orbit, Loren.wilton, ClueBot, Rumping, Snigbrook, CorenSearchBot, The Thing That Should Not Be, Jan1nad, Enthusiast01, SecPHD, Arakunem, Jobeard, Njmanson, Niceguyedc, Blanchardbot, Harland1, ChandlerMapBot, Bencejoful, Jusdafax, Tim874536, Dcampbell30, Estirabot, Shiro jdn, Aurora2698, Peter.C, Mxbuck, Creed1928, ChrisHodgesUK, BOTarate, La Pianista, 9Nak, Aitias, Certes, Apparition11, Vanished user uih38riiw4hjlsd, Sensiblekid, DumZiBoT, BarretB, Wordwizz, Gnowor, Booster4324, Gonzoноir, Rror, NellieBly, SP1R1TM4N, Badgernet, Alexius08, Noctibus, WikiDao, Thatguyflint, Osarius, Wyatt915, Addbot, Wikialoft, RPHv, Some jerk on the Internet, Captain-tucker, Otisjimmy1, Crazysane, TutterMouse, Lets Enjoy Life, Vishnavia, CanadianLinuxUser, Leszek Jaiczuk, Sysy909, Cst17, MrOllie, Roseurey, Emailtonaved, Chzz, Debresser, Muheer, LinkFA-Bot, Tide rolls, Lightbot, OLEnglish, Krano, Iune, Bluebusy, WikiDreamer Bot, Shawnj99, Luckas-bot, Yobot, Terronis, Fraggie81, Amirobot, Fightingirishfan, AnomieBOT, JDavis680, Jlavepoze, Tcosta, Killiondude, Jim1138, Gascreed, Piano non troppo, Elieb001, Gc9580, Fahadsadah, Kylefaherty, Flewis, Materialscientist, Citation bot, Aneah, Neurolysis, Obersachsebot, Xqbot, TheAMmollusc, Duesseljan, Addihockey10, JimVC3, Capricorn42, CoolingGibbon, 4twenty42o, Jmptrice, Ched, GrouchoBot, Backpackadam, Prunesqualer, RibotBOT, SassoBot, EddieNiedzwiecki, Thearcher4, Doulos Christos, =Josh.Harris, Gnuish, Chaheel Riens, Jaraics, Dan6hell66, G7yunghi, Prari, FrescoBot, Nageh, WPANI, Kamathvasudev, Galorr, Smile4ever, Expertour, Lukevenegas, DivineAlpha, Graphit, Pinethicket, I dream of horses, HRoestBot, Serols, Fixer88, Meaghan, Richard, MrBenCai, December21st2012Freak, Cougar w, Weylimp, Danshelb, TobeBot, WilliamSun, FunkyBike1, Vrenator, Clarkcj12, Stephenman882, Bangowiki, Mwalsh34, Eponymosity, Tbhotch, Gaiterin, DARTH SIDIOUS 2, Hugger and kisser, Dbrooksgta, Teenboi001, Aviv007, Regancy42, VernoWhitney, DASHBot, Chuck369, EmausBot, WikitanvirBot, Timtempleton, Super48paul, Solarra, Winner 42, Dcirovic, K6ka, Aejr120, Shupzv3, Athn, Ebrambot, Kandarp.pande.kandy, Sg313d, Cit helper, IntelligentComputer, Rafiwiki, Flyinghatchet, OisinisiO, NTox, Cubbyhouse, Zabanio, DASHBotAV, Sepersann, 28bot, Socialservice, ClueBot NG, AAriel42, Lord Roem, Vakanuvis789, 123Hedgehog456, Vlhsrp, Widr, Johnny C. Morse, Debby5.0, HMSSolent, Titodutta, Kanwar47, Wbm1058, Wiki13, Silvrous, Dentalplanisa, Euphoria42, Zune0112, Paulwray97, Nprrakis, Klildiplomus, Sk8erPrince, David.moreno72, Cimorcus, Fastcatz, CGuerrero-NJITWILL, Cvarta, PhilipFoulkes, Dexbot, Sendar, Jmitola, SimonWiseman, Codename Lisa, Avinash7075, Namnatulko, Pete Mahen, CaSJ, Junkyardsparkle, Jamesx12345, Rob.bosch, VikiED, Palmbeachguy, Epicgenius, Camayoc, Melonkelon, Anupasinha.20, Praemonitus, SamoaBot, EvergreenFir, DavidLeighEllis, Indiesingh, Ginsuloft, SophisticatedSwampert, ScotXW, Harshad1310, Fixture, Winged Blades of Godric, Kylrh, Nyashinski, Monkbot, The Original Filfi, Dsprc, Darshansham, TJH2018, WikiGopi, Jeremy.8910, Hayman30, ScrapIronIV, Kenkuteng, AMLIMSON, Miraclexix, Amccann421, Jerodlycett, KasparBot, RippleSax, ProprioMe OW, Risc64, Natasha Miranda, Radhwann, 0600K078, Chenthil Vel, Sharanyanaveen, Entranced98, Marianna251, Dakshin t, Nishantpatil1995, El cid, el campeador, Bender the Bot, ErikBln, Aaron.lancaster, Wikishovel, Saru1993, Karan unagar and Anonymous: 1033

- Intrusion detection system** Source: https://en.wikipedia.org/wiki/Intrusion_detection_system?oldid=794064016 Contributors: Mav, Harperf, Michael Hardy, Willsmith, Kku, (, Ellywa, Ronz, Julesd, Smaffy, Schneelocke, Dwo, Hashar, Joy, Astronautics~enwiki, Tbutzon, Wereon, Tea2min, Lady Tenar, Gtrmp, Mintleaf~enwiki, Ngardiner, Rick Block, Cloud200, Falcon Kirtaran, Chowbok, Utcursch, Kusunose, Hellisp, Bluefoxicity, Olivier Debre, Aaryna, Sysy, Discospinster, Bender235, Sietse Snel, GattoRandagio, Tmh, Obradovic Goran, Espoo, Guy Harris, Denoir, Tje, Rick Sidwell, M3tainfo, H2g2bob, Btornado, Nuno Tavares, Krille, Isnow, Jclemens, Rjwilmsi, Aapo Laitinen, Margosbot~enwiki, Intrgr, Windharp, Chobot, Bgwhite, Joonga, Borgx, Michael@thelander.com, Wolfmankurd, Boonebytes, Msos, Falcon9x5, Abune, Josh3580, LeonardoRob0t, NeilN, SimmondP, SmackBot, Mmernex, JurgenHadley, Charlesrh, Yamaguchi 先生, Unforgettableid, Jprg1966, Mhecht, Frap, JonHarder, Midnightcomm, UU, Grover cleveland, Radagast83, Weregerbil, Kolmigabrouil, Drphilharmonic, DMacks, Kuru, Itsgeneb, Tomhubbard, MarkSutton, Slakr, Yms, Visnup, EdC~enwiki, Kvng, FleetCommand, Sir Vicious, Difference engine, Cydebot, Mikebrand, Studerby, Cs california, Malleus Fatuorum, Jojan, Dawnseeker2000, AndreasWittenstein, JAnDbot, PhilKnight, Caffeinepuppy, BigChicken, Ronbarak, Pete Wall, CliffC, Tamer ih~enwiki, CraigMonroe, Haiauphixu, NewEnglandYankee, Sgorton, Derekrogerson, Wilson.canadian, Wlgrin, VolkovBot, Tburket, Butseriouslyfolks, TXiKiBoT, Qxz, Ferengi, Clangin, Nitin.skd, Softtest123, Madhero88, Finity, Hotmixclass, Dremeda, Phisches, Shahmirj, Jerryobject, Blueclaw, South-Lake, Jasonhatwiki, ClueBot, Lokipro, PolarYukon, Foss guy, Anubis1055, Gunnar Kreitz, Excirial, CrazyChemGuy, Dcampbell30, Footballfan190, Pete71, SoxBot III, Miklosq, Jovianeye, Tackat, Addbot, Some jerk on the Internet, Ronhjones, J7387438, MrOllie, Chrismcnab, Oakleeman, Bond0088, Yobot, Omarmalali, AnomieBOT, Jim1138, Hiihammuk, Materialscientist, Aneah, Xqbot, Capricorn42, Kpcatch6, Jesse5656, Kernel.package, Locobot, Shadowjams, Aghsajjy, Weyesr1, Access-bb, Jonesey95, RedBot, Banej, Lotje, Dungeonscaper, Offnfopt, Lopifalko, Autumnalmonk, Ddasune, EmausBot, WikitanvirBot, Nick Moyes, Mjdtjm, Dewritech, RA0808, Qrsdogg, Thecheesykid, ZéroBot, Lamf 0009, Paklan, Boundary11, RISCO Group, Bomazi, Nero2006, Schvenn, Cgt, ClueBot NG, Andrew.philip.thomas, Alima86, Bernolákovčina, Rezabot, Widr, Helpful Pixie Bot, Karthikjain, Deltaray3, Titodutta, Wbm1058, BG19bot, NewsAndEventsGuy, W.andrea, PhnomPencil, Kagundu, CitationCleanerBot, RobVeggett, Archos331, Baszerr, Cristianocosta, Mogism, Cerabot~enwiki, Bgibbs2, Namnatulco, TwoTwoHello, Spicyitalianmeatball, Frosty, SFK2, Me, Myself, and I are Here, Jose Manuel

Caballero, KBhokray, Rajamca66, Acc12345acc, Ajpolino, Paul2520, Rsschomburg, Freddyap, Drkhataniar, Monkbot, Sofia Koutsouveli, S166865h, Malayks, GeoffreyT2000, 115ash, Crystallizedcarbon, Pblowry, Jchang301, CAPTAIN RAJU, Ahmed embedded, Pickyt, Pranuvinu1, NoToleranceForIntolerance, L3X1, Big Ray 999, SecurityPanther, L8 ManeValidus, Geetika saini, Magic links bot, Pradaswami, Tonn, AvalerionV and Anonymous: 327

- **Mobile secure gateway** *Source:* https://en.wikipedia.org/wiki/Mobile_secure_gateway?oldid=781801628 *Contributors:* Kku, Rathfelder, Frap, Kvng, Yobot, I dream of horses, Champion, BG19bot, BattyBot, Alesteska, P.enderle23, Fendilaru and Anonymous: 3

31.6.2 Images

- **File:1988-03_Universal_Peace_virus_on_my_Mac.jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/9/98/1988-03_Universal_Peace_virus_on_my_Mac.jpg *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* Mike Evangelist
 - **File:2010-T10-ArchitectureDiagram.png** *Source:* <https://upload.wikimedia.org/wikipedia/commons/8/86/2010-T10-ArchitectureDiagram.png> *License:* CC BY-SA 3.0 *Contributors:* <http://www.owasp.org/index.php/File:2010-T10-ArchitectureDiagram.png> *Original artist:* Neil Smithline
 - **File:Ambox_globe_content.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/b/bd/Ambox_globe_content.svg *License:* Public domain *Contributors:* Own work, using File:Information icon3.svg and File:Earth clip art.svg *Original artist:* penubag
 - **File:Ambox_important.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/b/b4/Ambox_important.svg *License:* Public domain *Contributors:* Own work based on: Ambox scales.svg *Original artist:* Dsmurat, penubag
 - **File:Ambox_rewrite.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/1/1c/Ambox_rewrite.svg *License:* Public domain *Contributors:* self-made in Inkscape *Original artist:* penubag
 - **File:Audio_drill.jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/a/a8/Audio_drill.jpg *License:* Public domain *Contributors:* ? *Original artist:* ?
 - **File:Authentication_Using_THz_Material_Analysis.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/f/f9/Authentication_Using_THz_Material_Analysis.png *License:* CC BY-SA 4.0 *Contributors:* Own work *Original artist:* SarahSmith(Laser Eng)
 - **File:CIAJMK1209.png** *Source:* <https://upload.wikimedia.org/wikipedia/commons/9/9a/CIAJMK1209.png> *License:* CC BY-SA 3.0 *Contributors:* Made and uploaded by John Manuel - JMK. *Original artist:* John M. Kennedy T.
 - **File:CPU_ring_scheme.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/2/25/CPU_ring_scheme.svg *License:* CC-BY-SA-3.0 *Contributors:* This vector image was created with Inkscape. *Original artist:* User:Sven, original Author User:Cljk
 - **File:ClamAV0.95.2.png** *Source:* <https://upload.wikimedia.org/wikipedia/commons/2/2f/ClamAV0.95.2.png> *License:* GPL *Contributors:* my PC running Ubuntu 9.04 *Original artist:* SourceFire
 - **File:ClamTK3.08.jpg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/2/26/ClamTK3.08.jpg> *License:* GPL *Contributors:* Own work (own screenshot) *Original artist:* Dave Maunori
 - **File:ClamWin_Wine_screenshot.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/0/08/ClamWin_Wine_screenshot.png *License:* GPL *Contributors:* Transferred from en.wikipedia to Commons by Mardus. *Original artist:* The original uploader was SF007 at English Wikipedia
 - **File:Closed_Access_logo_alternative.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/c/c1/Closed_Access_logo_alternative.svg *License:* CC0 *Contributors:* File:Open_Access_logo_PLoS_white.svg and own modification *Original artist:* Jakob Voß, influenced by original art designed at PLoS, modified by Wikipedia users Nina and Beao
 - **File:Commons-logo.svg** *Source:* <https://upload.wikimedia.org/wikipedia/en/4/4a/Commons-logo.svg> *License:* PD *Contributors:* ? *Original artist:* ?
 - **File:Conficker.svg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/5/53/Conficker.svg> *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* Gppande
 - **File:Crypto_key.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/6/65/Crypto_key.svg *License:* CC-BY-SA-3.0 *Contributors:* Own work based on image:Key-crypto-sideways.png by MisterMatt originally from English Wikipedia *Original artist:* MesserWoland
 - **File:Crystal_Clear_app_linnighborhood.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/f/f9/Crystal_Clear_app_linnighborhood.svg *License:* LGPL *Contributors:* All Crystal Clear icons were posted by the author as LGPL on kde-look; Derivative works of this file: of File:Banned proxys.svg *Original artist:* Everaldo Coelho and YellowIcon; User:Ch.Andrew, Notwist and Carport
 - **File:Crystal_Clear_device_cdrom_unmount.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/1/10/Crystal_Clear_device_cdrom_unmount.png *License:* LGPL *Contributors:* All Crystal Clear icons were posted by the author as LGPL on kde-look; *Original artist:* Everaldo Coelho and YellowIcon;
 - **File:Defense_In_Depth_-_Onion_Model.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/4/4c/Defense_In_Depth_-_Onion_Model.svg *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* ?
 - **File:Desktop_computer_clipart_-_Yellow_theme.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/d/d7/Desktop_computer_clipart_-_Yellow_theme.svg *License:* CC0 *Contributors:* <https://openclipart.org/detail/17924/computer> *Original artist:* AJ from openclipart.org
 - **File>Edit-clear.svg** *Source:* <https://upload.wikimedia.org/wikipedia/en/f/f2/Edit-clear.svg> *License:* Public domain *Contributors:* The Tango! Desktop Project. *Original artist:*
- The people from the Tango! project. And according to the meta-data in the file, specifically: “Andreas Nilsson, and Jakub Steiner (although minimally).”
- **File:Emoji_u1f4bb.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/d/d7/Emoji_u1f4bb.svg *License:* Apache License 2.0 *Contributors:* https://github.com/googlei18n/noto-emoji/blob/f2a4f72/svg/emoji_u1f4bb.svg *Original artist:* Google
 - **File:Encryption_-_decryption.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/b/bf/Encryption_-_decryption.svg *License:* CC-BY-SA-3.0 *Contributors:* based on png version originally uploaded to the English-language Wikipedia by mike40033, and moved to the Commons by MichaelDiederich. *Original artist:* odder

- **File:EvilTwinWireless_en.jpg** *Source:* https://upload.wikimedia.org/wikipedia/en/4/4a/EvilTwinWireless_en.jpg *License:* CC-BY-SA-3.0 *Contributors:*
I derived this from Thomas.Baguette's work, using Paint.NET to edit the strings with similar fonts. *Original artist:* User:sarysa
- **File:Firewall.png** *Source:* <https://upload.wikimedia.org/wikipedia/commons/5/5b/Firewall.png> *License:* CC BY-SA 3.0 *Contributors:* Feito por mim *Original artist:* Bruno Pedrozo
- **File:GatewayTracingHologramLabel.jpg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/d/da/GatewayTracingHologramLabel.jpg> *License:* CC BY-SA 3.0 *Contributors:* self-made http://www.tmg.com.vn *Original artist:* Newone http://www.tmg.com.vn
- **File:GraphiqueMalware_en.jpg** *Source:* https://upload.wikimedia.org/wikipedia/en/6/6b/GraphiqueMalware_en.jpg *License:* CC-BY-SA-3.0 *Contributors:*
I derived this from Thomas.Baguette's work, using Paint.NET to edit the strings with similar fonts. *Original artist:* User:sarysa
- **File:Gufw_10.04.4.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/b/ba/Gufw_10.04.4.png *License:* GPL *Contributors:* http://gufw.tuxfamily.org *Original artist:* ?
- **File:Henri_Adolphe_Laissement_Kardin%C3%A4le_im_Vorzimmer_1895.jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/7/7b/Henri_Adolphe_Laissement_Kardin%C3%A4le_im_Vorzimmer_1895.jpg *License:* Public domain *Contributors:* Hampel Kunstauktionen *Original artist:* Henri Adolphe Laissement (1854-1921)
- **File:ID-card-spain-(01).png** *Source:* <https://upload.wikimedia.org/wikipedia/commons/2/23/ID-card-spain-%2801%29.png> *License:* CC SA 1.0 *Contributors:* ? *Original artist:* ?
- **File:Identities-and-authenticity-HL-overview.png** *Source:* <https://upload.wikimedia.org/wikipedia/commons/8/89/Identities-and-authenticity-HL-overview.png> *License:* CC BY-SA 4.0 *Contributors:* Own work *Original artist:* FlippyFlink
- **File:Internet_map_1024.jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/d/d2/Internet_map_1024.jpg *License:* CC BY 2.5 *Contributors:* Originally from the English Wikipedia; description page is/was here. *Original artist:* The Opte Project
- **File:KAL-55B_Tactical_Authentication_System_(Vietnam_War_era)_-_National_Cryptologic_Museum_-_DSC08013.JPG** *Source:* https://upload.wikimedia.org/wikipedia/commons/f/fc/KAL-55B_Tactical_Authentication_System_%28Vietnam_War_era%29_-_National_Cryptologic_Museum_-_DSC08013.JPG *License:* CC0 *Contributors:* Own work *Original artist:* Daderot
- **File:Keylogger-hardware-PS2-example-connected.jpg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/d/dc/Keylogger-hardware-PS2-example.jpg> *License:* GFDL *Contributors:* <http://www.weboctopus.nl/webshop/img/p/59-430-large.jpg> *Original artist:* <http://www.weboctopus.nl>
- **File:Keylogger-hardware-PS2.jpg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/1/11/Keylogger-hardware-PS2.jpg> *License:* Copyrighted free use *Contributors:* http://www.keylogger-keyloggers.nl/images/keylogger_company_keylogger_hardware_PS2.jpg *Original artist:* www.keylogger-keyloggers.nl
- **File:Keylogger-screen-capture-example.png** *Source:* <https://upload.wikimedia.org/wikipedia/commons/2/22/Keylogger-screen-capture-example.png> *License:* MPL 1.1 *Contributors:* Own work *Original artist:* own work
- **File:Keylogger-software-logfile-example.jpg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/c/c4/Keylogger-software-logfile-example.jpg> *License:* GPL *Contributors:* Own work in combination with the keylogger program <http://pykeylogger.sourceforge.net/> and the text editor <http://notepad-plus.sourceforge.net/> *Original artist:* Own work
- **File:Lock-green.svg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/6/65/Lock-green.svg> *License:* CC0 *Contributors:* en: File:Free-to-read_lock_75.svg *Original artist:* User:Trappist the monk
- **File:MalwareEffect.png** *Source:* <https://upload.wikimedia.org/wikipedia/commons/a/a6/MalwareEffect.png> *License:* GFDL *Contributors:* reproduction et modification d'un graphique *Original artist:* jeff000
- **File:Malware_statics_2011-03-16-en.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/e/ec/Malware_statics_2011-03-16-en.svg *License:* CC BY-SA 3.0 *Contributors:*
Malware_statics_2011-03-16-es.svg *Original artist:* Malware_statics_2011-03-16-es.svg: Kizar
- **File:MediaWiki-logo.svg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/b/bb/MediaWiki-notext.svg> *License:* Public domain *Contributors:* Own work based on: Tournesol.png *Original artist:* User:Anthere (flower) and User:Eloquence (combination, concept), reworked by User:Aka, vectorized by User:Chrkl ; brackets fixed by guillom
- **File:Merge-arrows.svg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/5/52/Merge-arrows.svg> *License:* Public domain *Contributors:* ? *Original artist:* ?
- **File:Mergefrom.svg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/0/0f/Mergefrom.svg> *License:* Public domain *Contributors:* ? *Original artist:* ?
- **File:Monitor_padlock.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/7/73/Monitor_padlock.svg *License:* CC BY-SA 3.0 *Contributors:* Own work (Original text: self-made) *Original artist:* Lunarbunny (talk)
- **File:Morris_Worm.jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/b/b6/Morris_Worm.jpg *License:* CC BY-SA 2.0 *Contributors:* Museum of Science - Morris Internet Worm *Original artist:* Go Card USA from Boston, USA
- **File:Netfilter-packet-flow.svg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/3/37/Netfilter-packet-flow.svg> *License:* CC BY-SA 3.0 *Contributors:* Own work, Origin SVG PNG *Original artist:* Jan Engelhardt
- **File:Online_harassment_lit_review.jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/8/8a/Online_harassment_lit_review.jpg *License:* CC BY-SA 4.0 *Contributors:* Own work *Original artist:* Willowbl00
- **File:PalmPilot5000.jpg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/e/e7/PalmPilot5000.jpg> *License:* CC-BY-SA-3.0 *Contributors:* en.wikipedia.org: 00:35, 3. Jul 2004 . . Mfatic . . 220x296 (12719 Byte) (Palm Pilot 5000

This template will categorize into Category:Wikipedia license migration candidates. *I dug this out of a drawer and took the photo myself.) Original artist:* Mfatic

- **File:Privacy_International_2007_privacy_ranking_map.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/2/2c/Privacy_International_2007_privacy_ranking_map.png *License:* CC BY-SA 3.0 *Contributors:* own work, based on [Image:Privacy_International_2006_privacy_ranking_map.png](#) *Original artist:* Wüstling
- **File:Question_book-new.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/9/99/Question_book-new.svg *License:* Cc-by-sa-3.0 *Contributors:*
Created from scratch in Adobe Illustrator. Based on [Image:Question book.png](#) created by [User:Equazcion](#) *Original artist:* Tkgd2007
- **File:Rkhunter_Ubuntu.png** *Source:* https://upload.wikimedia.org/wikipedia/en/5/5c/Rkhunter_Ubuntu.png *License:* ? *Contributors:*
Screenshot taken in Ubuntu
Original artist:
Michael Boelen et al
- **File:Rkhunter_on_Mac_OS_X.png** *Source:* https://upload.wikimedia.org/wikipedia/commons/c/c0/Rkhunter_on_Mac_OS_X.png *License:* GPL *Contributors:* Transferred from en.wikipedia to Commons by IngerAlHaosului using CommonsHelper. *Original artist:* The original uploader was CyberSkull at English Wikipedia
- **File:RootkitRevealer.png** *Source:* <https://upload.wikimedia.org/wikipedia/en/9/9c/RootkitRevealer.png> *License:* Fair use *Contributors:* <http://blogs.technet.com/b/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx> *Original artist:* ?
- **File:Scale_of_justice_2.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/0/0e/Scale_of_justice_2.svg *License:* Public domain *Contributors:* Own work *Original artist:* DTR
- **File:SecureID_token_new.JPG** *Source:* https://upload.wikimedia.org/wikipedia/commons/8/8f/SecureID_token_new.JPG *License:* Public domain *Contributors:* Own work *Original artist:* Ocrho
- **File:Stachledraht_DDOS_Attack.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/3/3f/Stachledraht_DDOS_Attack.svg *License:* LGPL *Contributors:* All Crystal icons were posted by the author as LGPL on kde-look *Original artist:* Everaldo Coelho and YellowIcon
- **File:Text_document_with_red_question_mark.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/a/a4/Text_document_with_red_question_mark.svg *License:* Public domain *Contributors:* Created by bdesham with Inkscape; based upon [Text-x-generic.svg](#) from the Tango project. *Original artist:* Benjamin D. Esham (bdesham)
- **File:U.S._Navy_Cyber_Defense_Operations_Command_monitor.jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/d/d6/U.S._Navy_Cyber_Defense_Operations_Command_monitor.jpg *License:* Public domain *Contributors:* <http://www.navy.mil/management/photodb/photos/081203-N-2147L-390.jpg> *Original artist:* Mass Communications Specialist 1st Class Corey Lewis , U.S. Navy
- **File:US_Navy_050308-N-2385R-029_Master-at-Arms_Seaman_Carly_Farmer_checks_an_identification_card_(ID)_before_allowing_a_driver_to_enter_the_gate_at_U.S._Fleet_Activities_Sasebo,_Japan.jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/4/42/US_Navy_050308-N-2385R-029_Master-at-Arms_Seaman_Carly_Farmer_checks_an_identification_card_%28ID%29_before_allowing_a_driver_to_enter_the_gate_at_U.S._Fleet_Activities_Sasebo%2C_Japan.jpg *License:* Public domain *Contributors:*
This Image was released by the United States Navy with the ID 050308-N-2385R-029 (next). This tag does not indicate the copyright status of the attached work. A normal [copyright tag](#) is still required. See [Commons:Licensing](#) for more information.
Original artist: U.S. Navy photo by Photographer's Mate 3rd Class Yesenia Rosas
- **File:Virus_Blaster.jpg** *Source:* https://upload.wikimedia.org/wikipedia/commons/e/ec/Virus_Blaster.jpg *License:* Public domain *Contributors:* <http://nuevovirus.info/virus-blaster/> *Original artist:* admin
- **File:Wiki_letter_w.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/6/6c/Wiki_letter_w.svg *License:* Cc-by-sa-3.0 *Contributors:* ? *Original artist:* ?
- **File:Wiki_letter_w_cropped.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/1/1c/Wiki_letter_w_cropped.svg *License:* CC-BY-SA-3.0 *Contributors:* This file was derived from [Wiki letter w.svg](#):
Original artist: Derivative work by Thumperward
- **File:Wikibooks-logo-en-noslogan.svg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/d/df/Wikibooks-logo-en-noslogan.svg> *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* User:Bastique, User:Ramac et al.
- **File:Wikibooks-logo.svg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/f/fa/Wikibooks-logo.svg> *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* User:Bastique, User:Ramac et al.
- **File:Wikidata-logo.svg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/f/ff/Wikidata-logo.svg> *License:* Public domain *Contributors:* Own work *Original artist:* User:Planemad
- **File:Wikimedia_Community_Logo.svg** *Source:* https://upload.wikimedia.org/wikipedia/commons/7/75/Wikimedia_Community_Logo.svg *License:* Public domain *Contributors:* Own work *Original artist:*
pl.wiki: WarX
- **File:Wikiversity-logo-Snorky.svg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/1/1b/Wikiversity-logo-en.svg> *License:* CC BY-SA 3.0 *Contributors:* Own work *Original artist:* Snorky
- **File:Wiktionary-logo-en-v2.svg** *Source:* <https://upload.wikimedia.org/wikipedia/commons/9/99/Wiktionary-logo-en-v2.svg> *License:* CC-BY-SA-3.0 *Contributors:* ? *Original artist:* ?
- **File:Wiktionary-logo-v2.svg** *Source:* <https://upload.wikimedia.org/wikipedia/en/0/06/Wiktionary-logo-v2.svg> *License:* CC-BY-SA-3.0 *Contributors:* ? *Original artist:* ?

31.6.3 Content license

- Creative Commons Attribution-Share Alike 3.0