Cybersecurity information technology list

This is a **list of cybersecurity information technology**. Cybersecurity is security as it is applied to information technology. This includes all technology that stores, manipulates, or moves data, such as computers, data networks, and all devices connected to or included in networks, such as routers and switches. All information technology devices and facilities need to be secured against intrusion, unauthorized use, and vandalism. Additionally, the users of information technology should be protected from theft of assets, extortion, identity theft, loss of privacy and confidentiality of personal information, malicious mischief, damage to equipment, business process compromise, and the general activity of cybercriminals. The public should be protected against acts of cyberterrorism, such as the compromise or loss of the electric power grid.

Cybersecurity is a major endeavor of the IT industry. There are a number of professional certifications given for cybersecurity training and expertise.[1] Although billions of dollars are spent annually on cybersecurity, no computer or network is immune from attacks or can be considered completely secure. The single most expensive loss due to a cybersecurity exploit was the ILOVEYOU or Love Bug email worm of 2000, which cost an estimated 8.7 billion American dollars.[2]

This article attempts to list all the important Wikipedia articles about cybersecurity. There are a number of minor articles that can be reached by means of links in the listed articles.

General

Introductory articles about cybersecurity subjects:

- Security
- Computer security[3]
- Internet security[4]
- Network security[5]
- Information security, Data security[6]
- List of computer security certifications

Cryptography

The art of secret writing or code. A "plaintext" message is converted by the sender to "ciphertext" by means of a mathematical algorithm that uses a secret key. The receiver of the message then reverses the process and converts the ciphertext back to the original plaintext.[7]

- History of cryptography
- Enigma machine
- Alan Turing
- Cipher
- Substitution cipher
- One-time pad
- Beale ciphers
- The Codebreakers[8]
- Cryptanalysis
- Cryptographic primitive
- Cryptographic Service Provider
- Data Encryption Standard
- Advanced Encryption Standard
- International Data Encryption Algorithm
- HMAC
- HMAC-based One-time Password algorithm
- Cryptographic hash function
- Hash collision
- List of hash functions
- Comparison of cryptographic hash functions
- Hash-based cryptography
- SHA-1
- SHA-2
- SHA-3
- SHA-3 competition
- Cryptographic nonce
- Salt (cryptography)
- Cryptographic strength
- Block cipher
- Block cipher mode of operation
- Stream cipher
- Key (cryptography)
- Key size
- Cryptographic key types
- Symmetric-key algorithm

- Public-key cryptography
- Public-Key Cryptography (conference)
- Digital signature
- Non-repudiation
- Public key certificate
- Certificate authority
- X.509
- Public key fingerprint
- RSA (cryptosystem)
- Secret sharing
- Internet key exchange
- Pretty Good Privacy
- Strong cryptography

Steganography

The art of hidden writing. The secret message is hidden within another object, such as a digital photograph.[9]

- Steganography
- BPCS-Steganography
- Steganography tools
- Steganalysis
- OpenPuff
- Kristie Macrakis[10]

Authentication and access

The process by which a potential client is granted authorized use of an IT facility by proving its identity.[11]

- Authentication
- Login
- Password
- Passphrase
- Password strength
- One-time password
- Multi-factor authentication
- Identity management
- Identity management theory
- Identity management system
- Encrypting PIN Pad
- Shared secret
- Authorization
- Access control
- Principle of least privilege
- Cryptographic protocol
- Authentication protocol
- Public key infrastructure
- RADIUS
- Kerberos (protocol)
- OpenID
- OAuth
- Active Directory Federation Services
- Security Assertion Markup Language
- SAML-based products and services

Public Key Infrastructure (PKI)

A framework for managing digital certificates and encryption keys.

- Public key infrastructure
- X.509
- Root certificate
- Public key certificate
- Certificate authority
- Digital signature
- Certificate policy
- Certificate Practice Statement
- Certificate revocation list
- Online Certificate Status Protocol

Tools

Computerized utilities designed to study and analyze the security of IT facilities and/or break into them on an unauthorized and potentially criminal basis.[12]

- List of security assessment tools
- Kali
- Security Administrator Tool for Analyzing Networks
- Nessus (software)
- Vulnerability scanner
- Nessus Attack Scripting Language
- OpenVAS
- Yasca
- Metasploit project
- John the Ripper
- Smeg Virus Construction Kit
- Virus Creation Laboratory
- Exploit kit

Threats

Modes of potential attacks on IT facilities.[13]

- Cyberattack
- STRIDE (security)
- Vulnerability (computing)
- Common Vulnerabilities and Exposures
- Privilege escalation
- Social engineering (security)
- Malware
- Spyware
- Backdoor (computing)
- Computer virus
- Computer worm
- Macro virus
- Keystroke logging
- Trojan horse
- Hardware Trojan
- Eavesdropping
- Zombie
- Botnets
- Advanced persistent threat
- Man-in-the-middle attack
- Man-on-the-side attack
- Meet-in-the-middle attack
- Length extension attack
- Replay attack
- Pre-play attack
- Dictionary attack
- Biclique attack
- Denial-of-service attack

- Resource exhaustion attack
- Brute-force attack
- Watermarking attack
- Mangled packet
- Reverse connection
- Polymorphic code
- Password cracking
- Spoofing attack
- POODLE

Exploits

Violations of IT facilities.[14]

- Exploit (computer security)
- Timeline of computer viruses and worms
- Comparison of computer viruses
- Malware analysis
- XML denial-of-service attack
- Distributed denial-of-service attacks on root nameservers
- Linux malware
- Zero-day (computing)
- Virus hoax
- Pegasus
- Rogue security software
- List of rogue security software
- MS Antivirus (malware)
- AntiVirus Gold
- Spysheriff
- SpywareBot
- TheSpyBot
- ByteDefender
- Security Essentials 2010
- Email spam
- Phishing
- Tiny Banker Trojan
- Melissa (computer virus)
- Brain (computer virus)
- CIH (computer virus)
- ILOVEYOU
- Anna Kournikova (computer virus)
- Michelangelo (computer virus)
- Simile (computer virus)
- Stoned (computer virus)
- Acme (computer virus)
- AIDS (computer virus)
- AI (computer virus)
- Cascade (computer virus)
- Flame (computer virus)
- Abraxas (computer virus)
- 1260 (computer virus)
- SCA (computer virus)
- ReDoS
- SYN flood
- Billion laughs attack
- UDP flood attack
- Wi-Fi deauthentication attack
- Smurf attack
- Mydoom
- IP address spoofing
- Fork bomb
- WinNuke

Criminal activity

Violation of the law by means of breaking into and/or misusing IT facilities. Laws that attempt to prevent these crimes.[15]

- Computer misuse act
- Cyber-security regulation
- China Internet Security Law
- Computer Crime and Intellectual Property Section
- Cyber criminals
- Cybercrime
- Security hacker
- White hat (computer security)
- Black hat (computer security)
- Industrial espionage #Use of computers and the Internet
- Phreaking
- RDP shop
- Market for zero-day exploits
- 2600 magazine
- Phrack, Google search on "hacker magazine"
- Identity theft
- Identity fraud
- Cyberstalking
- Cyberbullying

Nation states

Countries and their governments that use, misuse, and/or violate IT facilities to achieve national goals.[16]

- Cyber-arms industry
- Computer and network surveillance
- List of government surveillance projects
- Clipper chip
- Targeted surveillance
- United States Cyber Command
- Cybersecurity and Infrastructure Security Agency
- National Cybersecurity and Communications Integration Center
- Bletchley Park
- NSO Group
- Hacking Team
- Unit 8200
- NSA
- Room 641A
- Narus (company)
- Equation group
- Tailored Access Operations
- XKeyscore
- PRISM (surveillance program)
- Stuxnet
- Carnivore (software)

End-point protection

The securing of networked computers, mobile devices and terminals.[17]

- Antivirus software
- Comparison of antivirus software
- Lookout (IT security)
- Windows Defender
- Kaspersky Lab
- Malwarebytes
- Avast Antivirus
- Norton AntiVirus
- AVG AntiVirus
- McAfee
- McAfee VirusScan
- Symantec Endpoint Protection
- Microsoft Safety Scanner
- Windows Malicious Software Removal Tool
- VirusTotal
- Application firewall
- Personal firewall
- SentinelOne

Network protection

The protection of the means by which data is moved from one IT facility to another.[18]

- Virtual private network
- IPsec
- Internet Key Exchange
- Internet Security Association and Key Management Protocol
- Kerberized Internet Negotiation of Keys
- Firewall (computing)
- Stateful firewall
- HTTPS
- HTTP Public Key Pinning
- Transport Layer Security
- TLS acceleration
- Network Security Services
- Off the record messaging
- Secure Shell
- Circuit-level gateway
- Intrusion detection system
- Intrusion Detection Message Exchange Format
- Security information management
- Security information and event management
- Security event manager
- Router (computing) #Security
- Security log
- Intranet #Enterprise private network
- Proxy server

Processing protection

The securing of IT facilities that manipulate data, such as computer servers, often by means of specialized cybersecurity hardware.[19]

- Hardware security module
- Secure cryptoprocessor
- Trusted Platform Module
- Unified Extensible Firmware Interface #Secure Boot
- Executable space protection

Storage protection

The protection of data in its non-moving state, usually on magnetic or optical media or in computer memory.[20]

- Disk encryption
- Disk encryption theory
- Disk encryption software
- Comparison of disk encryption software
- BitLocker
- Encrypting File System
- Filesystem-level encryption
- Disk encryption hardware
- Hardware-based full disk encryption
- Personal data
- General Data Protection Regulation
- Privacy policy
- Information security audit
- Information technology audit
- Information technology security audit

Management of security

The processes by which security technology is monitored for faults, deployed and configured, measured for its usage, queried for performance metrics and log files, and/or monitored for intrusions.[21]

- Information security management
- FCAPS #Security management

Standards, frameworks, & requirements

Officially agreed architectures and conceptual structures for designing, building, and conducting cybersecurity.[22][23]

- NIST Cybersecurity Framework[24][25]
- National Initiative for Cybersecurity Education[26][27]
- Center for Internet Security
- The CIS Critical Security Controls for Effective Cyber Defense[28]
- Cyber Risk Quantification
- Risk management framework[29]
- IT risk[30]
- Risk IT[31]
- ISO/IEC 27000-series
- Cyber-security regulation[32]
- Health Insurance Portability and Accountability Act #Security Rule

- Federal Information Security Management Act of 2002[33]

See also

- Outline of computer security https://witslb.com/

References

1. *"CompTIA Career Roadmap" (https://certification.comptia.org/why-certify/roadmap) . CompTIA. Retrieved 20 Aug 2019.*
2. *Ciampia, Mark (2018). Security+ Guide to Network Security Fundamentals. Cengage. ISBN 978-1337288781.*
3. *Stallings & Brown (2017). Computer Security: Principles and Practice (4 ed.). Pearson. ISBN 978-0134794105.*
4. *Stallings, William (1995). Network and Internetwork Security: Principles and Practice (https://archive.org/details/networkinternetw0000stal) . IEEE Press. ISBN 0-7803-1107-8.*
5. *The Open University (2016). Network security. Kindle.*
6. *Merkow & Breithaupt (2014). Information Security: Principles and Practice (2 ed.). Pearson. ISBN 978-0789753250.*
7. *Stallings, William (2016). Cryptography and Network Security (7th ed.). Pearson. ISBN 978-0134444284.*
8. *Kahn, David (1967). The Code Breakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. Scribner. ISBN 0-684-83130-9.*
9. *Fridrich, Jessica (2009). Steganography in Digital Media. Cambridge. ISBN 978-0521190190.*
10. *Macrakis, Kristie (2014). Prisoners, Lovers, and Spies: The Story of Invisible Ink from Herodotus to Al-Qaeda. Yale University Press. ISBN 978-0300179255.*
11. *Kao, I Lung (2019). Effective and Efficient Authentication and Authorization in Distributed Systems. University of Florida. ISBN 978-0530003245.*
12. *ICT School (2019). Hacking Tools for Computers. ICT School. ISBN 9781088521588.*
13. *Diogenes & Ozkaya (2018). Cybersecurity--Attack and Defense Strategies. Packt Publishing. ISBN 978-1-78847-529-7.*
14. *Andes, Thomas (8 April 2016). The Encyclopedia of Computer Security Exploits. ISBN 9781530944682.*
15. *Britz, Marjie (2013). Computer Forensics and Cyber Crime (3 ed.). Pearson. ISBN 978-0132677714.*

16. *Kaplan, Fred (2016). Dark Territory: The Secret History of Cyber War. Simon & Schuster. ISBN 978-1476763262.*
17. *Lopez & Setola (2012). Critical Infrastructure Protection. Springer-Verlog. ISBN 978-3642289194.*
18. *Stewart, Michael (2013). Network Security, Firewalls, and VPNs (2 ed.). James & Bartlett Learning. ISBN 978-1284031676.*
19. *Grasser, Michael (2008). Secure CPU: A Secure Processor Architecture for Embedded Systems. VDM Verlag. ISBN 978-3639027839.*
20. *Jacobs & Rudis (2014). Data-Driven Security. Wiley. ISBN 978-1118793725.*
21. *Campbell, T. (2016). Practical Information Security Management: A Complete Guide to Planning and Implementation (https://books.google.com/books?id=sbWiDQAAQBAJ&pg=PA1) . APress. ISBN 9781484216859.*
22. *Calder, Alan (28 September 2018). NIST Cybersecurity Framework: A Pocket Guide. IT Governance Publishing Ltd. ISBN 978-1787780422.*
23. *Alsmatti, Izzat (2019). The NICE Cybersecurity Framework. Springer. ISBN 978-3030023591.*
24. *NIST. "Framework for Improving Critical Infrastructure Cybersecurity v1.1" (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf) (PDF). NIST. Retrieved 19 Aug 2019.*
25. *NIST. "Cybersecurity Framework Page" (https://www.nist.gov/cyberframework) . NIST. Retrieved 19 Aug 2019.*
26. *NIST. "NIST SP 800-181: NICE Cybersecurrity Workforce Framework" (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf) (PDF). NIST. Retrieved 19 Aug 2019.*
27. *U.S. Congress. "Cybersecurity Enhancement Act of 2014" (https://www.congress.gov/bill/113th-congress/senate-bill/1353/text) . U.S. Congress. Retrieved 19 Aug 2019.*
28. *Center for Internet Security. CIS Controls V7.1.*
29. *NIST. Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf) (PDF).*
30. *Talabis & Martin (2013). Information Security Risk Assessment Toolkit. Syngress. ISBN 978-1597497350.*
31. *ISACA. The Risk IT Practitioner Guide.*
32. *Kosseff, Jeff (2017). Cyber Security Law. Wiley. ISBN 978-1119231509.*
33. *Taylor, Laura (2013). FISMA Compliance Handbook (2 ed.). Elsevier. ISBN 978-0124058712.*

Last edited 11 days ago **by** Bethoven999