Internet security

Internet security is a branch of computer security. It encompasses the Internet, browser security, web site security,[1] and network security as it applies to other applications or operating systems as a whole. Its objective is to establish rules and measures to use against attacks over the Internet.[2] The Internet is an inherently insecure channel for information exchange, with high risk of intrusion or fraud, such as phishing,[3] online viruses, trojans, ransomware and worms.

Many methods are used to combat these threats, including encryption and ground-up engineering.[4]

Contents

Threats

Malicious software

Malicious software comes in many forms, such as viruses, Trojan horses, spyware, and worms.

- Malware, a portmanteau of 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 unintentionally causes harm due to some deficiency. The term badware applies to both malware and unintentionally harmful software.
- A botnet is a network of computers that have been taken over by a robot or bot that performs large-scale malicious acts for its creator.
- Computer viruses are programs that can replicate their structures or effects by infecting other files or structures on a computer. The typical purpose of a virus is to take over a computer to steal data.
- Computer worms are programs that can replicate themselves throughout a computer network.
- Ransomware is a type of malware that restricts access to the computer system that it infects, and demands a ransom in order for the restriction to be removed.
- Scareware is a program of usually limited or no benefit, containing malicious payloads, that is sold via 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.
- One particular kind of spyware is key logging malware. Often referred to as keylogging or keyboard capturing, is the action of recording (logging) the keys struck on a keyboard.
- A Trojan horse, commonly known as a *Trojan*, is a general term for malware that pretends to be harmless, so that a user will be convinced to download it onto the computer.

Denial-of-service attacks

A denial-of-service attack (DoS) or distributed denial-of-service attack (DDoS) is an attempt to make a computer resource unavailable to its intended users. It works by making so many service requests at once that the system is overwhelmed and becomes unable to process any of them. DoS may target cloud computing systems.[5] According to business participants in an international security survey, 25% of respondents experienced a DoS attack in 2007 and another 16.8% in 2010.[6] DoS attacks often use bots (or a botnet) to carry out the attack.

Phishing

Phishing targets online users in an attempt to extract sensitive information such as passwords and financial information.[7] Phishing occurs when the attacker pretends to be a trustworthy entity, either via email or a web page. Victims are directed to web pages that appear to be legitimate, but instead route information to the attackers. Tactics such as email spoofing attempt to make emails appear to be from legitimate senders, or long complex URLs hide the actual website.[8][9] Insurance group RSA claimed that phishing accounted for worldwide losses of $10.8 billion in 2016.[10]

Application vulnerabilities

Applications used to access Internet resources may contain security vulnerabilities such as memory safety bugs or flawed authentication checks. Such bugs can give network attackers full control over the computer.[11][12]

A widespread web-browser application vulnerability is the cross-origin resource sharing (CORS) vulnerability - for maximum security and privacy, make sure to adopt adequate countermeasures against it (such as the patches provided for WebKit-based browsers).[13]

Countermeasures

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.[14]

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 Engineering Task Force (IETF). It provides security and authentication at the IP layer by transforming data using encryption. Two main types of transformation form the basis of IPsec: the Authentication Header (AH) and ESP. They provide data integrity, data origin authentication, and anti-replay services. These protocols can be used alone or in combination.

Basic components include:

- 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 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.

Threat modeling

Threat Modeling (https://foreseeti.com/threat-modeling/) tools helps you to proactively analyze the cyber security posture of a system or system of systems and in that way prevent security threats.

Multi-factor authentication

Multi-factor authentication (MFA) is an access control method of in which a user is granted access only after successfully presenting separate pieces of evidence to an authentication mechanism – two or more from the following categories: knowledge (something they know), possession (something they have), and inherence (something they are).[15][16] Internet resources, such as websites and email, may be secured using this technique.

Security token

Some online sites offer customers the ability to use a six-digit code which randomly changes every 30–60 seconds on a physical security token. The token has built-in computations and manipulates numbers based on the current time. This means that every thirty seconds only a certain array of numbers validate access. The website is made aware of that device's serial number and knows the computation and correct time to verify the number. After 30–60 seconds the device presents a new random six-digit number to log into the website.[17]

Electronic mail security

Background

Email messages are composed, delivered, and stored in a multiple step process, which starts with the message's composition. When a message is sent, it is transformed into a standard format according to RFC 2822.[18] Using a network connection, the mail client sends the sender's identity, the recipient list and the message content to the server. Once the server receives this information, it forwards the message to the recipients.

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:

- Digitally signing the message to ensure its integrity and confirm the sender's identity.
- Encrypting the message 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 them. For example, the organizations could establish a virtual private network (VPN) to encrypt communications between their mail servers.[19] Unlike methods that only encrypt a message body, a VPN can encrypt all communication over the connection, including email header information such as senders, recipients, and subjects. However, a VPN does not provide a message signing mechanism, nor can it provide protection for email messages along the entire route from sender to recipient.

Message Authentication Code

A Message authentication code (MAC) is a cryptography method that uses a secret key to digitally sign 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.[20]

Firewalls

A computer firewall controls access to a single computer. A network firewall controls access to an entire network. A firewall is a security device — computer hardware or software — that filters traffic and blocks outsiders. It generally consists of gateways and filters. Firewalls can also screen network traffic and block

traffic deemed unauthorized.

Web security

Firewalls restrict incoming and outgoing network packets. Only authorized traffic is allowed to pass through it. Firewalls create checkpoints between networks and computers. Firewalls can block traffic based on IP source and TCP port number. They can also serve as the platform for IPsec. Using tunnel mode, firewalls can implement VPNs. Firewalls can also limit network exposure by hiding the internal network from the public Internet.

Types of firewall

Packet filter

A packet filter 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 Interconnect (OSI) model and statically defines what traffic will be allowed. Circuit proxies forward network packets (formatted 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 internal information from the outside.

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.

Browser choice

Web browser market share predicts the share of hacker attacks. For example, Internet Explorer 6, which used to lead the market,[21] was heavily attacked.[22]

Protections

Antivirus

Antivirus software can protect a programmable device by detecting and eliminating malware.[23] A variety of techniques are used, such as signature-based, heuristics, rootkit, and real-time.

Password managers

A password manager is a software application that creates, stores and provides passwords to applications. Password managers encrypt passwords. The user only needs to remember a single master password to access the store.[24]

Security suites

Security suites were first offered for sale in 2003 (McAfee) and contain firewalls, anti-virus, anti-spyware and other components.[25] 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.[26]

History

At the National Association of Mutual Savings Banks (NAMSB) conference in January 1976, Atalla Corporation (founded by Mohamed Atalla) and Bunker Ramo Corporation (founded by George Bunker and Simon Ramo) introduced the earliest products designed for dealing with online security. Atalla later added its Identikey hardware security module, andj supported processing online transactions and network security. Designed to process bank transactions online, the Identikey system was extended to shared-facility operations. It was compatible with various switching networks, and was capable of resetting itself electronically to any one of 64,000 irreversible nonlinear algorithms as directed by card data information.[27] In 1979, Atalla introduced the first network security processor (NSP).[28]

See also

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

References

1. "What Is Internet Security? | McAfee" (https://www.mcafee.com/enterprise/en-us/security-awareness/cybersecurity/what-is-internet-security.html). *www.mcafee.com*. Retrieved 2021-09-05.
2. Gralla, Preston (2007). *How the Internet Works* (https://archive.org/details/howinternetworks00gral). Indianapolis: Que Pub. ISBN 978-0-7897-2132-7.
3. Rhee, M. Y. (2003). *Internet Security: Cryptographic Principles, Algorithms and Protocols*. Chichester: Wiley. ISBN 0-470-85285-2.

4. "101 Data Protection Tips: How to Keep Your Passwords, Financial & Personal Information Safe in 2020" (https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe). *Digital Guardian*. 2019-12-16. Retrieved 2020-10-23.
5. Yan, Q.; Yu, F. R.; Gong, Q.; Li, J. (2016). "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges". *IEEE Communications Surveys and Tutorials*. **18** (1): 602–622. doi:10.1109/COMST.2015.2487361 (https://doi.org/10.1109%2FCOMST.2015.2487361). S2CID 20786481 (https://api.semanticscholar.org/CorpusID:20786481).
6. "Information Sy-infographic". *University of Alabama at Birmingham Business Program*. Missing or empty `|url=` (help)
7. Izak, Belarua. "Welke virusscanners zijn het beste voor macOS High Sierra" (https://virusscannermac.nl/beste-virusscanner-voor-mac/). *Virusscanner MAC* (in Dutch). Retrieved 4 January 2018.
8. Ramzan, Zulfikar (2010). "Phishing attacks and countermeasures" (https://books.google.com/books?id=I-9P1EkTkigC&pg=PA433). In Stamp, Mark; Stavroulakis, Peter (eds.). *Handbook of Information and Communication Security*. Springer. ISBN 9783642041174.
9. van der Merwe, Alta; Loock, Marianne; Dabrowski, Marek (2005). "Characteristics and Responsibilities Involved in a Phishing Attack" (https://dl.acm.org/citation.cfm?id=1071800). *Proceedings of the 4th International Symposium on Information and Communication Technologies*. Trinity College Dublin: 249–254. Retrieved 4 January 2018.
10. Long, Mathew (February 22, 2017). "Fraud Insights Through Integration" (https://www.rsa.com/en-us/blog/2017-02/fraud-insights-integration). RSA. Retrieved October 20, 2018.
11. "Improving Web Application Security: Threats and Countermeasures" (https://msdn.microsoft.com/en-us/library/ms994920.aspx). *msdn.microsoft.com*. Retrieved 2016-04-05.
12. "Justice Department charges Russian spies and criminal hackers in Yahoo intrusion" (https://www.washingtonpost.com/world/national-security/justice-department-charging-russian-spies-and-criminal-hackers-for-yahoo-intrusion/2017/03/15/64b98e32-0911-11e7-93dc-00f9bdd74ed1_story.html?tid=ss_fb-bottom). *Washington Post*. Retrieved 15 March 2017.
13. "Unofficial WebKit CORS vulnerability patches" (http://webkit-cors-vulnerability.trentalancia.com/). *webkit-cors-vulnerability.trentalancia.com*. Retrieved 2021-05-01.
14. "Securing the Network Layer Against Malicious Attacks" (https://www.tdktech.com/tech-talks/securing-the-network-layer-against-malicious-attacks/). *TDK Technologies*. October 27, 2020.
15. "Two-factor authentication: What you need to know (FAQ) – CNET" (https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/). *CNET*. Retrieved 2015-10-31.
16. "How to extract data from an iCloud account with two-factor authentication activated" (https://www.iphonebackupextractor.com/blog/extract-data-two-factor-authentication/). *iphonebackupextractor.com*. Retrieved 2016-06-08.
17. Margaret Rouse (September 2005). "What is a security token?" (https://searchsecurity.techtarget.com/definition/security-token). SearchSecurity.com. Retrieved 2014-02-14.
18. Resnick, Peter W. "Internet Message Format" (https://tools.ietf.org/html/rfc2822.html). *tools.ietf.org*. Retrieved 2021-05-01.
19. "Virtual Private Network" (https://web.archive.org/web/20130603122059/http://itcd.hq.nasa.gov/networking-vpn.html). NASA. Archived from the original (http://itcd.hq.nasa.gov/networking-vpn.html) on 2013-06-03. Retrieved 2014-02-14.
20. "What Is a Message Authentication Code?" (http://www.wisegeek.com/what-is-a-message-authentication-code.htm). Wisegeek.com. Retrieved 2013-04-20.
21. "Browser Statistics" (https://www.w3schools.com/browsers/default.asp). W3Schools.com. Retrieved 2011-08-10.

22. Bradly, Tony. "It's Time to Finally Drop Internet Explorer 6" (https://www.pcworld.com/article/191356/its_time_to_finally_drop_internet_explorer_6.html). PCWorld.com. Retrieved 2010-11-09.
23. Larkin, Eric (2008-08-26). "Build Your Own Free Security Suite" (http://www.pcworld.com/article/150204/build_your_own_free_security_suite.html). Retrieved 2010-11-09.
24. "USE A FREE PASSWORD MANAGER" (https://web.archive.org/web/20160125015536/http://scsccbkk.org/Use%20a%20Password%20Manager%20for%20Security.pdf) (PDF). scsccbkk.org. Archived from the original (http://www.scsccbkk.org/Use%20a%20Password%20Manager%20for%20Security.pdf) (PDF) on 2016-01-25. Retrieved 2016-06-17.
25. Rebbapragada, Narasu. "All-in-one Security" (https://web.archive.org/web/20101027173353/http://www.pcworld.com/article/125817/allinone_security.html). PC World.com. Archived from the original (https://www.pcworld.com/article/125817/article.html) on October 27, 2010. Retrieved 2010-11-09.
26. "Free products for PC security" (https://www.comodo.com/products/free-products.php). 2015-10-08.
27. "Four Products for On-Line Transactions Unveiled" (https://books.google.com/books?id=3u9H-xL4sZAC&pg=PA3). *Computerworld*. IDG Enterprise. **10** (4): 3. 26 January 1976.
28. Burkey, Darren (May 2018). "Data Security Overview" (http://www.gtug.de/HotSpot2018/download/Presentation/C108-Burkey.pdf) (PDF). Micro Focus. Retrieved 21 August 2019.

External links

- National Institute of Standards and Technology (NIST.gov) (https://www.nist.gov/information-technology-portal.cfm) - Information Technology portal with links to computer- and cyber security
- National Institute of Standards and Technology (NIST.gov) (https://csrc.nist.gov/publications/detail/sp/800-45/version-2/final) -Computer Security Resource Center -Guidelines on Electronic Mail Security, version 2
- PwdHash Stanford University (https://crypto.stanford.edu/PwdHash/) - Firefox & IE browser extensions that transparently convert a user's password into a domain-specific password.
- Cybertelecom.org Security (https://www.cybertelecom.org/security/) - surveying federal Internet security work
- DSL Reports.com (https://www.dslreports.com/)- Broadband Reports, FAQs and forums on Internet security, est 1999