COMPUTER SECURITY
KIBERDROŠĪBA

Author: **Lauris Glīzds**, e-mail: vova456@inbox.lv, 27165715
Scientific supervisor: **Artis Teilāns, Dr.sc.ing. profesors,** e-mail: artis.teilans@rta.lv
Rezekne Academy of Technologies, Atbrivosanas aleja 115, Rezekne

Abstract. *The paper contains information about hacking types and systems which they are suffered the most cyber attack. The main goal is to introduce people how to protect your systems from several cyber attacks following by special guidelines.*

Keywords: *computer security, cyber security, IT security.*

Introduction

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

It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection[2], and due to malpractice by operators, whether intentional, accidental, or due to them being tricked into deviating from secure procedures[3].

The field is of growing importance due to the increasing reliance on computer systems and the Internet in most societies[4], wireless networks such as Bluetooth and Wi-Fi – and the growth of "smart" devices, including smart phones, televisions and tiny devices as part of the Internet of Things.

Materials and methods

A vulnerability is a system susceptibility or flaw. 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].

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:

Backdoors

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.

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

http://dx.doi.org/10.17770/het2017.21.3588

techniques are possible including reflection and amplification attacks, where innocent systems are fooled into sending traffic to the victim.

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.

Spoofing

Spoofing, in general, is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver. Spoofing is most prevalent in communication mechanisms that lack a high level of security[7].

Tampering

Tampering describes a malicious modification of products. So-called "Evil Maid" attacks and security services planting of surveillance capability into routers[8] are examples.

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. So 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.

Phishing

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details directly from users[9]. 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.

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.

Social engineering

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[10].

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[11].

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[12].

Systems at risk

Computer security is critical in almost any industry which uses computers. Currently, most electronic devices such as computers, laptops and cellphones come with built in firewall security software, but despite this, computers are not 100 percent accurate and dependable to protect our data (Smith, Grabosky & Urbas, 2004.) There are many different ways of hacking into computers. It can be done through a network system, clicking into unknown links, connecting to unfamiliar Wi-Fi, downloading software and files from unsafe sites, power consumption, electromagnetic radiation waves, and many more. However, computers can be protected through well built software and hardware. By having strong internal interactions of properties, software complexity can prevent software crash and security failure[13].

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[14]. In-store payment systems and ATMs have also been tampered with in order to gather customer account data and PINs.

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 to physical damage caused by malicious commands sent to industrial equipment (in that case uranium enrichment centrifuges) which are infected via removable media. In 2014, the Computer Emergency Readiness Team, a division of the Department of Homeland Security, investigated 79 hacking incidents at energy companies[15]. Vulnerabilities in smart meters (many of which use local radio or cellular communications) can cause problems with billing fraud[16].

Consumer devices

Desktop computers and laptops are commonly infected with malware either 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 also become targets and many of these 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[17].

Home automation devices such as the Nest thermostat are also potential targets[17].

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[18], Staples[19], and Target Corporation[20]. 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[21].

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[22, 23], and Sony Pictures was attacked in 2014 where the motive appears to have been to embarrass with data leaks, and cripple the company by wiping workstations and servers[24, 25].

Government

Government and military computer systems are commonly attacked by activists[26, 27, 28, 29] and foreign powers[30, 31, 32, 33]. Local and regional government infrastructure such as traffic light controls, police and intelligence agency communications, personnel records, student records[34], 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.

Summary

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[35, 36, 37].

Some common countermeasures are listed in the following sections:

Security 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.

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"[38].

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[39]:

- 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.

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[40, 41].

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"[42]. 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.

Hardware protection mechanisms

While hardware may be a source of insecurity, such as with microchip vulnerabilities maliciously introduced during the manufacturing process[43, 44], 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[45], 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)[46]. In addition, a USB dongle can be configured to lock or unlock a computer[47].
- 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[48].
- 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[49]. Tools exist specifically for encrypting external drives as well[50].
- 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[51].
- 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[52].

Secure operating systems

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"[53] 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[54] and several military jets[55].

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[56]; important for cryptographic protocols for example.

Bibliography

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". csa.gov.sg. Retrieved 12 November 2014.
7. "What is Spoofing? - Definition from Techopedia".
8. Gallagher, Sean (May 14, 2014). "Photos of an NSA "upgrade" factory show Cisco router getting implant". Ars Technica. Retrieved August 3, 2014.
9. "Identifying Phishing Attempts". Case.
10. Arcos Sergio. "Social Engineering" (PDF).
11. Scannell, Kara (24 Feb 2016). "CEO email scam costs companies $2bn". Financial Times (25 Feb 2016). Retrieved 7 May 2016.
12. "Bucks leak tax info of players, employees as result of email scam". Associated Press. 20 May 2016. Retrieved 20 May 2016.
13. J. C. Willemssen, "FAA Computer Security". GAO/T-AIMD-00-330. Presented at Committee on Science, House of Representatives, 2000.
14. "Financial Weapons of War". Minnesota Law Review. 2016. SSRN 2765010.
15. Pagliery, Jose. "Hackers attacked the U.S. energy grid 79 times this year". CNN Money. Cable News Network. Retrieved 16 April 2015.
16. "Vulnerabilities in Smart Meters and the C12.12 Protocol". SecureState. 2012-02-16. Retrieved 4 November 2016.
17. "Is Your Watch Or Thermostat A Spy? Cybersecurity Firms Are On It". NPR.org. 6 August 2014.
18. Melvin Backman (18 September 2014). "Home Depot: 56 million cards exposed in breach". CNNMoney.
19. "Staples: Breach may have affected 1.16 million customers' cards". Fortune.com. December 19, 2014. Retrieved 2014-12-21.
20. "Target security breach affects up to 40M cards". Associated Press via Milwaukee Journal Sentinel. 19 December 2013. Retrieved 21 December 2013.
21. Jim Finkle (23 April 2014). "Exclusive: FBI warns healthcare sector vulnerable to cyber attacks". Reuters. Retrieved 23 May 2016.
22. Bright, Peter (February 15, 2011). "Anonymous speaks: the inside story of the HBGary hack". Arstechnica.com. Retrieved March 29, 2011.
23. Anderson, Nate (February 9, 2011). "How one man tracked down Anonymous—and paid a heavy price". Arstechnica.com. Retrieved March 29, 2011.
24. Palilery, Jose (December 24, 2014). "What caused Sony hack: What we know now". CNN Money. Retrieved January 4, 2015.
25. 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.
26. "Internet strikes back: Anonymous' Operation Megaupload explained". RT. 20 January 2012. Archived from the original on 5 May 2013. Retrieved May 5, 2013.
27. "Gary McKinnon profile: Autistic 'hacker' who started writing computer programs at 14". The Daily Telegraph. London. 23 January 2009.
28. "Gary McKinnon extradition ruling due by 16 October". BBC News. September 6, 2012. Retrieved September 25, 2012.
29. 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
30. "NSA Accessed Mexican President's Email", October 20, 2013, Jens Glüsing, Laura Poitras, Marcel Rosenbach and Holger Stark, spiegel.de
31. Sanders, Sam (4 June 2015). "Massive Data Breach Puts 4 Million Federal Employees' Records At Risk". NPR. Retrieved 5 June 2015.
32. Liptak, Kevin (4 June 2015). "U.S. government hacked; feds think China is the culprit". CNN. Retrieved 5 June 2015.
33. Sean Gallagher. "Encryption "would not have helped" at OPM, says DHS official".
34. "Schools Learn Lessons From Security Breaches". Education Week. 19 October 2015. Retrieved 23 May 2016.
35. RFC 2828 Internet Security Glossary
36. CNSS Instruction No. 4009 dated 26 April 2010
37. InfosecToday Glossary

38. Definitions: IT Security Architecture. SecurityArchitecture.org, Jan, 2006
39. Jannsen, Cory. "Security Architecture". Techopedia. Janalta Interactive Inc. Retrieved 9 October 2014.
40. "Cybersecurity at petabyte scale".
41. Woodie, Alex (9 May 2016). "Why ONI May Be Our Best Hope for Cyber Security Now". Retrieved 13 July 2016.
42. "Firms lose more to electronic than physical theft". Reuters.
43. "The Hacker in Your Hardware: The Next Security Threat". Scientific American.
44. Waksman, Adam; Sethumadhavan, Simha (2010), "Tamper Evident Microprocessors"(PDF), Proceedings of the IEEE Symposium on Security and Privacy, Oakland, California
45. "Sentinel HASP HL". E-Spin. Retrieved 2014-03-20.
46. "Token-based authentication". SafeNet.com. Retrieved 2014-03-20.
47. "Lock and protect your Windows PC". TheWindowsClub.com. Retrieved 2014-03-20.
48. James Greene (2012). "Intel Trusted Execution Technology: White Paper" (PDF). Intel Corporation. Retrieved 2013-12-18.
49. "SafeNet ProtectDrive 8.4". SCMagazine.com. 2008-10-04. Retrieved 2014-03-20.
50. "Secure Hard Drives: Lock Down Your Data". PCMag.com. 2009-05-11.
51. "Top 10 vulnerabilities inside the network". Network World. 2010-11-08. Retrieved 2014-03-20.
52. "Forget IDs, use your phone as credentials". Fox Business Network. 2013-11-04. Retrieved 2014-03-20.
53. 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.
54. Kelly Jackson Higgins (2008-11-18). "Secure OS Gets Highest NSA Rating, Goes Commercial". Dark Reading. Retrieved 2013-12-01.
55. "Board or bored? Lockheed Martin gets into the COTS hardware biz". VITA Technologies Magazine. December 10, 2010. Retrieved 9 March 2012.
56. Sanghavi, Alok (21 May 2010). "What is formal verification?". EE Times_Asia.