Proceedings of International Web Conference "Cyber Security"
30th November 2022, Organized by Sbyte Technologies
Sponsored by INFISUM, USA.

A Review Study On Some Cyber Security Related Topics

S.SAHANA
Asst System Engineer Trainee-TCS
sahayesyes@gmail.com

Abstract: **It is the protection of computer systems and networks from information disclosure, theft of, or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. The field has become of significance due to the expanded reliance on computer systems, the Internet and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of smart devices, including smartphones, televisions, and the various devices that constitute the Internet of things (IoT). Cybersecurity is also one of the significant challenges in the contemporary world, due to the complexity of information systems, both in terms of political usage and technology. Its primary goal is to ensure the system's dependability, integrity, and data privacy**

Key words: **Network; Cyber Attacks; Multi Tenancy; Sensitive Information; Threat Factors;**

INTRODUCTION

A vulnerability is a weakness in design, implementation, operation, or internal control. Most of the vulnerabilities that have been discovered 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. Vulnerabilities can be researched, reverse-engineered, hunted, or exploited using automated tools or customized scripts. 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 these categories below:

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 many reasons, including original design or 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. Backdoors can be very hard to detect, and backdoors are usually discovered by someone who has access to application source code or intimate knowledge of the operating system of the computer.

Denial-of-service attack

Denial of service attacks (DoS) are designed to make a machine or network resource unavailable to its intended users. Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim's 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 or from a range of other possible techniques, including reflection and amplification attacks, where innocent systems are fooled into sending traffic to the victim.

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 microphones. Even when the system is protected by standard security measures, these may be bypassed 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.

Eavesdropping

Eavesdropping is the act of surreptitiously listening to a private computer "conversation" (communication), typically between hosts on a network. For instance, programs such as Carnivore and NarusInSight have been used by the Federal Bureau of Investigation (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 by monitoring the faint

electromagnetic transmissions generated by the hardware. TEMPEST is a specification by the NSA referring to these attacks.

Multi-vector, polymorphic attacks

Surfacing in 2017, a new class of multi-vector, polymorphic cyber threats combined several types of attacks and changed form to avoid cybersecurity controls as they spread.

Phishing

An example of a phishing email, disguised as an official email from a (fictional) bank. The sender is attempting to trick the recipient into revealing confidential information by "confirming" it at the phisher's website. Note the misspelling of the words received and discrepancy as recieved and discrepency, respectively. Although the URL of the bank's webpage appears to be legitimate, the hyperlink points at the phisher's webpage. Phishing is the attempt of acquiring sensitive information such as usernames, passwords, and credit card details directly from users by deceiving the users. 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. The fake website often asks for personal information, such as login details and passwords. This information can then be used to gain access to the individual's real account on the real website. Preying on a victim's trust, phishing can be classified as a form of social engineering. Attackers are using creative ways to gain access to real accounts. A common scam is for attackers to send fake electronic invoices to individuals showing that they recently purchased music, apps, or others, and instructing them to click on a link if the purchases were not authorized. A more strategic type of phishing is spear-phishing which leverages personal or organization-specific details to make the attacker appear like a trusted source. Spear-phishing attacks target specific individuals, rather than the broad net cast by phishing attempts.

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 exploit a vulnerability in the system to gain access to restricted data; or even become "root" and have full unrestricted access to a system.

Reverse engineering

Reverse engineering is the process by which a man-made object is deconstructed to reveal its designs, code, and architecture, or to extract knowledge from the object; similar to scientific research, the only difference being that scientific research is about a natural phenomenon.

Side-channel attack

Any computational system affects its environment in some form. This effect it has on its environment, includes a wide range of criteria, which can range from electromagnetic radiation, to residual effect on RAM cells which as a consequent make a Cold boot attack possible, to hardware implementation faults that allow for access and or guessing of other values that normally should be inaccessible. In Side-channel attack scenarios, the attacker would gather such information about a system or network to guess its internal state and as a result access the information which is assumed by the victim to be secure.

Social engineering

Social engineering, in the context of computer security, aims to convince a user to disclose secrets such as passwords, card numbers, etc. or grant physical access by, for example, impersonating a senior executive, bank, a contractor, or a customer. This generally involves exploiting peoples trust, and relying on their cognitive biases. A common scam involves emails sent to accounting and finance department personnel, impersonating their CEO and urgently requesting some action. In early 2016, the FBI reported that such "business email compromise" (BEC) scams had cost US businesses more than $2 billion in about two years. 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.

Spoofing

Spoofing is an act of masquerading as a valid entity through the falsification of data (such as an IP address or username), in order to gain access to information or resources that one is otherwise unauthorized to obtain. There are several types of spoofing, including:

- Email spoofing, is where an attacker forges the sending (From, or source) address of an email.
- IP address spoofing, where an attacker alters the source IP address in a network packet to

hide their identity or impersonate another computing system.

- MAC spoofing, where an attacker modifies the Media Access Control (MAC) address of their network interface controller to obscure their identity, or to pose as another.
- Biometric spoofing, where an attacker produces a fake biometric sample to pose as another user.

Tampering

Tampering describes a malicious modification or alteration of data. So-called Evil Maid attacks and security services planting of surveillance capability into routers are examples.

Malware

Malicious software (malware) installed on a computer can leak any information, such as personal information, business information and passwords, can give control of the system to the attacker, and can corrupt or delete data permanently.

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 toward information security within an organization. Information security culture is the "...totality of patterns of behavior in an organization that contributes to the protection of information of all kinds." Andersson and Reimers (2014) found that employees often do not see themselves as part of their organization's information security effort and often take actions that impede organizational changes. Indeed, the Verizon Data Breach Investigations Report 2020, which examined 3,950 security breaches, discovered 30% of cybersecurity incidents involved internal actors within a company. 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.

- Pre-evaluation: To identify the awareness of information security within employees and to analyze the current security policies.
- Strategic planning: To come up with a better awareness program, clear targets need to be set. Assembling a team of skilled professionals is helpful to achieve it.
- Operative planning: A good security culture can be established based on internal communication, management buy-in, security awareness and a training program.
- Implementation: Four stages should be used to implement the information security culture.

They are:

1. Commitment of the management
2. Communication with organizational members
3. Courses for all organizational members
4. Commitment of the employees

- Post-evaluation: To assess the success of the planning and implementation, and to identify unresolved areas of concern.

Systems at risk

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

Financial systems

The computer systems of financial regulators and financial institutions like the U.S. Securities and Exchange Commission, SWIFT, investment banks, and commercial banks are prominent hacking targets for cybercriminals interested in manipulating markets and making illicit gains. Websites and apps that accept or store credit card numbers, brokerage accounts, and bank account information are also prominent hacking targets, because of the potential for immediate financial gain from transferring money, making purchases, or selling the information on the black market. 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. In 2014, the Computer Emergency

Readiness Team, a division of the Department of Homeland Security, investigated 79 hacking incidents at energy companies.

Aviation

The aviation industry is very reliant on a series of complex systems which could be attacked. A simple power outage at one airport can cause repercussions worldwide, much of the system relies on radio transmissions which could be disrupted, and controlling aircraft over oceans is especially dangerous because radar surveillance only extends 175 to 225 miles offshore. There is also potential for attack from within an aircraft. In Europe, with the (Pan-European Network Service) and NewPENS, and in the US with the NextGen program, 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.

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. Smartphones, 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. The increasing number of home automation devices such as the Nest thermostat are also potential targets.

Large corporations

Large corporations are common targets . In many cases attacks are aimed at financial gain through identity theft and involve data breaches. Examples include the loss of millions of clients' credit card details by Home Depot, Staples, Target Corporation, and the most recent breach of Equifax. Medical records have been targeted in general identify theft, health insurance fraud, and impersonating patients to obtain prescription drugs for recreational purposes or resale. Although cyber threats continue to increase, 62% of all organizations did not increase security training for their business in 2015. Not all attacks are financially motivated, however: 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, and Sony Pictures was hacked in 2014 with the apparent dual motive of embarrassing the company through data leaks and crippling the company by wiping workstations and servers.

Automobiles

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 WiFi and Bluetooth to communicate with onboard consumer devices and the cell phone network. 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. Simple examples of risk include a malicious compact disc being used as an attack vector, 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 and in a widely publicized 2015 test, hackers remotely carjacked a vehicle from 10 miles away and drove it into a ditch. Manufacturers are reacting in numerous ways, with Tesla in 2016 pushing out some security fixes "over the air" into its cars' computer systems. 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.

Government

Government and military computer systems are commonly attacked by activists and foreign powers. Local and regional government infrastructure such as traffic light controls, police and intelligence agency communications, personnel records, student records, 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.

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. Concerns have been raised that this is being developed without appropriate consideration of the

security challenges involved. While the IoT creates opportunities for more direct integration of the physical world into computer-based systems, it also provides opportunities for misuse. In particular, as the Internet of Things spreads widely, cyberattacks are likely to become an increasingly physical (rather than simply virtual) threat. 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. An attack that targets physical infrastructure and/or human lives is sometimes referred to as a cyber-kinetic attack. As IoT devices and appliances gain currency, cyber-kinetic attacks can become pervasive and significantly damaging.

Medical systems

Medical devices have either been successfully attacked or had potentially deadly vulnerabilities demonstrated, including both in-hospital diagnostic equipment and implanted devices including pacemakers and insulin pumps. There are many reports of hospitals and hospital organizations getting hacked, including ransomware attacks, Windows XP exploits, viruses, and data breaches of sensitive data stored on hospital servers. 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.

Energy sector

In distributed generation systems, the risk of a cyber attack is real, according to Daily Energy Insider. An attack could cause a loss of power in a large area for a long period of time, and such an attack could have just as severe consequences as a natural disaster. The District of Columbia is considering creating a Distributed Energy Resources (DER) Authority within the city, with the goal being for customers to have more insight into their own energy use and giving the local electric utility, Pepco, the chance to better estimate energy demand. The D.C. proposal, however, would "allow third-party vendors to create numerous points of energy distribution, which could potentially create more opportunities for cyber attackers to threaten the electric grid."

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."

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).

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. Additionally, recent attacker motivations can be traced back to extremist organizations seeking to gain political advantage or disrupt social agendas. The growth of the internet, mobile technologies, and inexpensive computing devices have led to a rise in capabilities but also to the risk to environments that are deemed as vital to operations. All critical targeted environments are susceptible to compromise and this has led to a series of proactive studies on how to migrate the risk by taking into consideration motivations by these types of actors. Several stark differences exist between the hacker motivation and that of nation state actors seeking to attack based on an ideological preference. A standard part of threat modeling 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.

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.

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 only have 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 track 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".

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:

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

Practicing security architecture provides the right foundation to systematically address business, IT and security concerns in an organization.

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 and 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, the complete destruction of the compromised system is favored, as it may happen that not all the compromised resources are detected.

Today, computer security consists mainly of "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. However, relatively few organizations maintain computer systems with effective detection systems, and fewer still have organized response mechanisms in place. As a 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". The primary obstacle to effective eradication of cybercrime 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.

In order to ensure adequate security, the confidentiality, integrity and availability of a network, better known as the CIA triad, must be protected and is considered the foundation to information security. To achieve those objectives, administrative, physical and technical security measures should be employed. The amount of security afforded to an asset can only be determined when its value is known.

ACKNOWLEDGEMENTS

Author hereby thanks Dr.Sridhar Seshadri, Ex.Vice-Chancellor, for his continuous support, guidance and mentorship. His comments while reviewing this paper for publication are highly appreciable and well taken to modify this final version .

REFERENCES

[1]. Lai, T. L.; Liao, S.-W.; Wong, S. P. S.; Xu, H. (2020). "Statistical models and stochastic optimization in financial technology and investment science" (PDF). Annals of Mathematical Sciences and Applications. **5** (2): 317-345. doi:10.4310/AMSA.2020.v5.n2.a5. S2CID 240302839.

[2]. Lai, T. L.; Liao, S.-W.; Wong, S. P. S.; Xu, H. (2020). "Statistical models and stochastic optimization in financial technology and investment science" (PDF). Annals of Mathematical Sciences and Applications. **5** (2): 317-345. doi:10.4310/AMSA.2020.v5.n2.a5. S2CID 240302839.

[3]. Laqueur, Walter; C., Smith; Spector, Michael (2002). Cyberterrorism. Facts on File. pp. 52–53. ISBN 9781438110196.

[4]. Larabel, Michael (28 December 2017). "Syzbot: Google Continuously Fuzzing The Linux Kernel". www.phoronix.com/. Retrieved 25 March 2021.

[5]. Law, Laurie; Sabett, Susan; Solinas, Jerry (11 January 1997). "How to Make a Mint: The Cryptography of Anonymous Electronic Cash". American University Law Review. **46** (4). Archived from the original on 12 January 2018. Retrieved 11 January 2018

[6]. Lazarus, Ari (23 February 2018). "Phishers send fake invoices". Consumer Information. Retrieved 17 February 2020.

[7]. Lehman, Jeffrey; Phelps, Shirelle (2005). West's Encyclopedia of American Law, Vol. 3 (2 ed.). Detroit: Thomson/Gale. p. 137. ISBN 9780787663742.

[8]. Leigland, R (September 2004). "A Formalization of Digital Forensics" (PDF).

[9]. Lewis, James (February 2018). "Economic Impact of Cybercrime - No Slowing Down" (PDF).

[10]. Lieber, Ron (April 11, 2014). "Financial Advice for People Who Aren't Rich". The New York Times.(subscription required)

[11]. Liu, Jinan; Rahman, Sajjadur; Serletis, Apostolos (2020). "Cryptocurrency Shocks". SSRN Electronic Journal. doi:10.2139/ssrn.3744260. ISSN 1556-5068. S2CID 233751995.

[12]. Malvino, Albert P., & Brown, Jerald A. (1993). Digital Computer Electronics, 3rd Edition. New York, New York: Glencoe McGraw-Hill

[13]. Matteo D'Agnolo. "All you need to know about Bitcoin". timesofindia-economictimes. Archived from the original on 26 October 2015.

[14]. Michael G. Noblett; Mark M. Pollitt; Lawrence A. Presley (October 2000). "Recovering and examining computer forensic evidence". Retrieved 26 July 2010.

[15]. Millman, Renee (15 December 2017). "New polymorphic malware evades three-quarters of AV scanners". SC Magazine UK.

[16]. Milutinović, Monia (2018). "Cryptocurrency". Ekonomika. **64** (1): 105–122. doi:10.5937/ekonomika1801105M. ISSN 0350-137X.

[17]. Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.

[18]. Nakashima, Ellen (26 January 2008). "Bush Order Expands Network Monitoring: Intelligence Agencies to Track Intrusions". The Washington Post. Retrieved 8 February 2021.

[19]. Null, Linda, & Lobur, Julia. (2019). The Essentials of Computer Organization and Architecture. 5th Edition. Burlington, Massachusetts: Jones and Bartlett Learning.

[20]. Pagliery, Jose (2014). Bitcoin: And the Future of Money. Triumph Books. ISBN 978-1629370361. Archived from the original on 21 January 2018. Retrieved 20 January 2018.

[21]. Parker D (1983) Fighting Computer Crime, U.S.: Charles Scribner's Sons.

[22]. Patt, Yale N., & Patel, Sanjay J. (2020). Introduction to Computing Systems: From Bits and Gates to C and Beyond, 3rd Edition. New York, New York: McGraw Hill Education.

[23]. Pernice, Ingolf G. A.; Scott, Brett (20 May 2021). "Cryptocurrency". Internet Policy Review. **10** (2). doi:10.14763/2021.2.1561. ISSN 2197-6775.

[24]. Perrin, Chad (30 June 2008). "The CIA Triad". techrepublic.com. Retrieved 31 May 2012.

[25]. Petzold, Charles. (2009). Code: The Hidden Language of Computer Hardware and Software. Redmond, Washington: Microsoft Press.

