International Journal of
Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: http://dx.doi.org/10.7324/IJASRE.2017.32508

Vol.3 (8) Sep - 2017

A PRIMER ON CYBERSECURITY

Matthew N. O. Sadiku, Shumon Alam, and Sarhan M. Musa
Roy G. Perry College of Engineering
Prairie View A&M University
Prairie View, TX 77446
Cajetan M. Akujuobi
Office of the Vice President for Research and Dean of Graduate School
Prairie View A&M University
Prairie View, TX 77446

ABSTRACT

Information technologies have become indispensable to the modern lifestyle and threats against the availability, integrity, and confidentiality of information can affect the very functioning of our societies. The act of protecting information systems is known as cybersecurity. Cybersecurity is a national and global phenomenon because the malicious use of cyberspace could hamper economic, public health, safety, and national security activities. It is becoming more and more important as more information is being made available on computer networks. This paper provides a primer on this existing field.

Key Words: Cybersecurity, Information Security, Internet Security.

1. INTRODUCTION

We are all connected to the Internet one way or the other. The Internet is used for everything from storing a company's confidential information to social networking. It has revolutionized the functioning of educational systems, businesses, economies, societies, and governments around the world. Although the Internet brings immeasurable opportunities, it also brings new risks. Because of its fast, cheap, and anonymous character, the Internet has become a place for various attacks and criminal activities.

By nature, cyberspace or the Internet is difficult to secure. Intruders exploit the vulnerabilities to steal information and money and perpetrate crimes. The crimes include child pornography, banking and financial fraud, and intellectual property violations. They may also include accessing government and defense confidential information, tampering with commercially sensitive data, and targeting supply chains. Companies are constantly bombarded from all types of sources: criminal syndicates, cyber vandals, intruders, and disgruntled insiders/employees.

Cybersecurity is the process of protecting computer networks from cyber attacks or unintended unauthorized access. Cybersecurity takes different forms including military, law enforcement, judicial, commerce, infrastructure, interior, intelligence, and information systems. The relationship between cybersecurity and other security domains is shown in Figure 1 [1].

2. CYBERSECURITY FEATURES

The cybersecurity is a dynamic, interdisciplinary field involving information systems, computer science, and criminology. The security objectives have been availability, authentication, confidentiality, non-repudiation, and integrity [2]:

- *Availability*: This refers to the availability of information and ensuring that authorized parties can access the information when needed. Attacks targeting availability of service generally leads to denial of service.

- *Authenticity*: This ensures that the identity of an individual user or system is the identity claimed. This usually involves using username and password to validate the identity of the user. It may also take the form of what you have such as a driver's license, an RSA token, or a smart card.

- *Integrity*: Data integrity means information is authentic and complete. This assures that data, devices, and processes are free from tampering. Data should be free from the injection, deletion, or corruption. When integrity is targeted, nonrepudiation is also affected

- *Confidentiality*: Confidentiality ensures that measures are taken to prevent sensitive information from reaching the wrong people. Data secrecy is important especially for privacy-sensitive data such as user personal information and meter readings.

- *Nonrepudiation*: This is an assurance of the responsibility to an action. The source should not be able to deny having sent a message, while the destination should not deny having received it. This security objective is essential for accountability and liability.

3. CYBER ATTACKS

Cyber attacks are threatening the operation of businesses, banks, companies, and government networks. They vary from the illegal crime of individual citizen (hacking) to actions of groups (terrorists). The following are typical examples of cyber attacks or threats [3]:

- *Malware*: This is a malicious software or code that includes traditional computer viruses, computer worms, and Trojan horse programs. Malware can infiltrate your network through the Internet, downloads, attachments, email, social media, and other platforms. Spyware is a type of malware that collects information without the victim's knowledge.
- *Phishing*: Criminals trick victims into handing over their personal information such as online passwords, social security number, and credit card numbers.
- *Denial-of-service attacks*: These are designed to make a network resource unavailable to its intended users. These can prevent the user from accessing email, websites, online accounts or other services.
- *Social Engineering Attacks*: A cyber criminal attempts to trick users to disclose sensitive information. A social engineer aims to convince a user through impersonation to disclose secrets such as passwords, card numbers, or social security number.
- *Man-In-the-Middle Attack*: This is a cyber attack where a malicious attacker secretly inserts him/herself into a conversation between two parties who believe they are directly communicating with each other. A common example of man-in-the-middle attacks is eavesdropping. The goal of such an attack is to steal personal information.

Cybersecurity involves reducing the risk of cyber attacks. It involves the collection of tools, policies, guidelines, risk management approaches, and best practices that can be used to protect the cyber environment and mitigate cyber attacks. Cyber crime prevention is a multifaceted issue. Cyber risks should be managed proactively by the management.

4. CYBERSECURITY GOVERNANCE

Cybersecurity is the joint responsibility of all relevant stakeholders including government, business, infrastructure owners and users. Governments and international organizations play a key role in cybersecurity issues. Securing the cyberspace is of high priority to the Department of Homeland Security (DHS). The DHS has a dedicated division responsible for risk management program and requirements for cybersecurity called the National Cyber Security Division. The Federal Communications Commission's role in cybersecurity is to strengthen the protection of critical computer networks and networked infrastructure. The

Computer Fraud and Abuse Act (CFAA) remains the most relevant applicable law expressing the U.S. proactive cybersecurity effort.

Other governments (such as the United Kingdom, Canada, Japan, Australia, and New Zealand) are introducing various security measures, enacting cybersecurity-related laws and regulations, and forging international cooperation on cybersecurity. Cybersecurity issues have been on the NATO agenda for a while due to its international nature. NATO redefined its cyber defense policy with its 2008 response to cyber attacks against Estonia [4].

5. CHALLENGES

6.

Cybersecurity policy faces a host of challenges and obstacles – political, bureaucratic, legal, political, financial, national, and international. Unfortunately, we lack proper scientific understanding of cybersecurity in order to tackle these challenges in a principled manner.

The first challenge cybersecurity faces is the confusion over its varied definitions [5]. Cybersecurity means different things to different people and there is lack of consensus among stakeholders. There is no uniform set of standards that cybersecurity professional must follow when implementing a cybersecurity program. Although there are several laws, regulations, and policies governing cybersecurity, compliance with such guidelines does not automatically guarantee network security.

Cybersecurity policy lags technological innovation. Information technology changes rapidly, with security technology and practices evolving even faster to keep pace with changing threats. Because cybersecurity is not well-understood by non-experts, the economics are hard to demonstrate, and effectiveness is difficult to measure. Minimizing our cybersecurity risks requires commitment on both technical and political fronts.

Security is no longer confined just to what users do with a computer. Through the Internet of Things (IoT), devices can gather, store, and transmit data that is capable of exposing sensitive information. The explosion in these and inherently insecure devices is shifting the security paradigm. IoT manufacturers must improve the security of their devices because good cybersecurity is good business [6].

Mobile technology and social networking bring new cybersecurity challenges. With the advent of such applications at an unprecedented scale, the privacy of the information is compromised to a larger extent.

Cybersecurity breaches cannot be stopped at a nation's borders since it is difficult to determine where the actual borders are in cyberspace. Thus, cybersecurity can become a supranational problem. To address cybersecurity threat, nations must collaborate among themselves [7].

7. CONCLUSION

Cyber security is a fast growing field concerned with reducing computer-related risks or data breaches. Cybersecurity issues are critical for information infrastructure such as a smart power grid. The current trend of integrating power systems with advanced communication technologies has introduced serious cybersecurity concerns.

Cybersecurity education and training are crucial towards protecting the nation's ever-increasing cyberinfrastructure. One way to do this is to integrate cybersecurity concepts to undergraduate programs in STEM and IT fields, which already offer the core technology skills [8].

The demand for cybersecurity professionals is expected to grow since weak cybersecurity endangers the country. Companies, government, and organizations all employ cybersecurity professionals [9].

REFERENCES

[1] A. Klimburg (ed.), *National Cyber Security Framework Manual*, NATO CCD COE Publication,Tallinn, 2012.

[2] M. N. O. Sadiku, M. Tembely, and S. M. Musa, "Smart grid cybersecurity," *Journal of Multidisciplinary Engineering Science and Technology* (JMEST), vol. 3, no. 9, September 2016, pp.5574-5576.

[3] FCC Small Biz Cyber Planning Guide, https://transition.fcc.gov/cyber/cyberplanner.pdf

[4] E. Tikk, "Global cybersecurity–Thinking about the niche for NATO," *SAIS Review*, vol. 30, no. 2, Summer-Fall 2010, pp. 105-119.

[5] K. Zeng, "Exploring cybersecurity requirements in the defense acquisition process," *Doctoral Dissertation*, Capitol Technology University, April 2016.

[6] K. L. Miller, "What we talk about when we talk about 'reasonable cybersecurity': A proactive and adaptive approach," *The Computer & Internet Lawyer,* vol. 34, no. 3, March 2017, pp. 1-8.

[7] H. de Bruijn and M. Janssen, "Building cybersecurity awareness: The need for evidence-based framing strategies," *Government Information Quarterly*, vol. 34, 2017, pp. 1–7.

[8] V. P. Janeja et al., " Cybersecurity workforce development: A peer mentoring approach," *Proceedings of IEEE Conference on Intelligence and Security Informatics* (ISI), September 2016, pp. 267-272.

[9] "Computer security," *Wikipedia*, the free encyclopedia
https://en.wikipedia.org/wiki/Computer_security

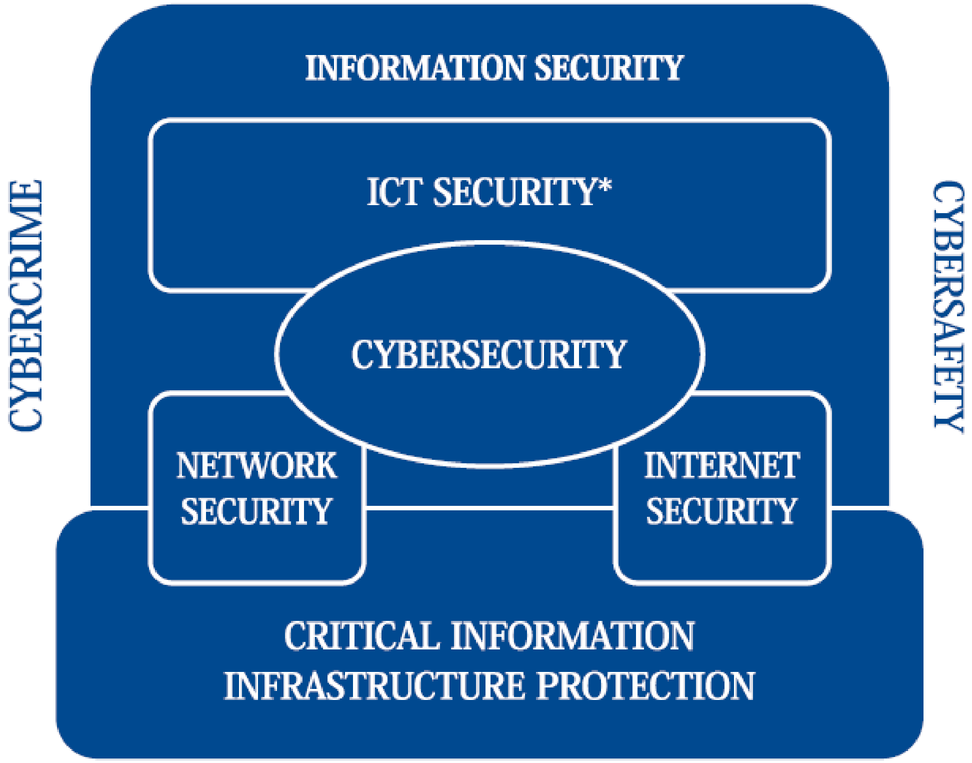

Figure 1. Relationship between cybersecurity and other security domains [1].

About the authors

Matthew N.O. Sadiku is a professor in the Department of Electrical and Computer Engineering at Prairie View A&M University, Texas. He is the author of several books and papers. His areas of research interests are in computational electromagnetic and computer networks. He is a fellow of IEEE.

Shumon Alam is the director and researcher at Center of Excellence of Communication Systems Technology Research (CECSTR) and SECURE Center of Excellence both at Prairie View A&M University. His research interests are in the areas of control, communication systems, networking, cybersecurity, and signal processing.

Sarhan M. Musa is a professor in the Department of Engineering Technology at Prairie View A&M University, Texas. He has been the director of Prairie View Networking Academy, Texas, since 2004. He is an LTD Spring and Boeing Welliver Fellow.