Emerging Cybersecurity Threats and Trends in Electrical and Electronics Systems: An Empirical Analysis

Dr. V. Shobana [1], Dr. C. Maheswari [2], Dr. V. Balaji [3], Mr. A. Viswanath [4]

[1] Department of Computer Science with Cyber Security, Dr. N.G.P. Arts and Science College, Coimbatore.

[2,3,4] Department of Electrical and Electronics Engineering, PSG College of Technology, Coimbatore.

Abstract

The empirical analysis provides an overview of the emerging trends in cyber-attacks and cybersecurity. It examines the increasing sophistication of cyber threats, the evolving landscape of defensive technologies, and the implications for organizations and policymakers. The increasing integration of digital technologies in electrical and electronics systems has made these domains susceptible to a variety of cyber threats. This paper presents an empirical analysis of the emerging cybersecurity threats and trends within these systems. By examining case studies, recent incidents, and statistical data, we highlight the critical vulnerabilities and propose robust cybersecurity measures. The findings emphasize the need for continuous advancements in security protocols to safeguard critical infrastructure.

Keywords—Cyber-attacks, Cybersecurity, AI, Ransomware, Phishing, Zero Trust, Password less Authentication, Regulatory Compliance.

1. INTRODUCTION

Because of the existence of the internet over the past three decades, data is growing tremendously and the threat against those data is also rising. The Internet has now become the heart of every individual and it has become a part of their day-to-day activities. The number of users who are using the internet has crossed 3 billion worldwide which has seamlessly increased the cyber-attacks worldwide. Currently, most of the international relations, economic, commercial, cultural, social, and governmental exchanges between nations occur virtually at all levels, involving people, non-governmental groups, and governments and government institutions[1]. All the above stated things are carried out in cyber space. Most of the sensitive data and information are prone to attacks thus there should be a strong infrastructure which should be available to safeguard all these types of data. Cyber Space occupies most of the population data like sensitive financial transactions, interaction of people for most of the time also happened in this space. Thus, it becomes more crucial to protect all that data without exploiting that data to unwanted users. The strong and weak actors which includes governments, crime, terrorist groups and even individuals, have entered cyberspace due to its low entry cost, anonymity, unpredictable geographical location, dramatic impact and lack of public transparency. These actors are at risk from cyberwarfare, cybercrime, cyberterrorism, and cyberespionage. This study enhances us in knowing the different tools and emerging technologies that will aid in protecting all these data[2].

2. BASIC CONCEPTS

Cyber Security deals with protecting systems, programs, and networks from a set of digital attacks. These digital attacks are known as cyber-attacks where they target systems to change, manipulate, destroy, and access information which is very sensitive. These attacks are intended to gain money from users through ransom ware which will result in changing the schedule of the normal processes. Imagine a situation where an employee is working with his/her computer. A silent observer alias hacker will be stealing the information in background and will sell it to criminals. Those criminals will make hold of the company for a ransom profit. This is a common happening in Cyber space today. This is because cyber security has become more essential in almost all stages of business and the need for cyber security professionals is becoming more in demand. This study helps us to have knowledge on these aspects of hacking and the recent tools and techniques to eradicate them. Cyber security is a technology that is designed to protect systems and networks from unauthorized access. The following are the different sources where a cyber threat can emerge.

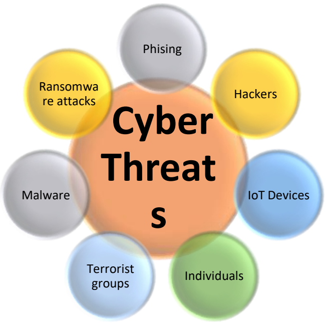

Fig I- Sources of Cyber Threats

The above listed are the different sources of threats where an unauthorized person can gain access to the information and use it for a ransom profit [3].

3. TYPES OF CYBER CRIMES

Cybercrime is a form of unauthorized access which involves a computer, maybe a network or device. They always look for companies or firms involving a huge number of transactions [1]. This will lead to hacking of sensitive information and there will be an increased number of Cyber Crimes. Cyber criminals will make a profit out of by using one of the following ways.

i. Unauthorized Access
ii. Cyber stalking
iii. Virus Attacks or Malware
iv. Denial of Service Attack
v. Salami Attacks
vi. Web Hijacking
vii. Cyber Defamation
viii. Email Bombing
ix. Data Diddling
x. Cyber Terrorism

The above are the topmost listed Cyber Crimes that are most common among the internet users. Let's have a look at each one of these in detail.

i. Unauthorized Access

Unauthorized access refers to gaining access to resources which have not been authorized [4]. It may be a password protected file, password of an online banking account or credit card information. Once they gain access to it, they can easily access sensitive information which is not intended for their use.

ii. Cyber Stalking

Generally stalking refers to the act of harassing or stalking a victim through digital means such as social media platforms, through messages that has been posted in a discussion forum, through messaging application [5]. Here both the victim and the harasser may be individuals. Posting offensive rude messages, sending threatening mails to victims, creating fake accounts are some of the examples of stalking. This may be taken as an extension of cyber bullying.

iii. Virus Attacks or Malware

A Computer virus may be termed as a software which is malicious that will be spreading across different computers and results in causing damage to systems. This will lead to misfunctioning of the systems, may result in operational failures and even data leakage or data loss. Some of the common types of virus attacks include XSS, Brute force attack, crypto jacking, Trojan Horse attack and Malicious URL's.

iv. Denial of Service Attack

This type of attack makes the system shutdown and will not be available for the intended users. This can be achieved by making a network traffic or by crashing the victim's machine by sending information.

v. Salami Attacks

This type of attack happens with a motive of financial fraud and taking amount from financial account. This attack happens by combining small minor attacks and will become a sturdy attack. This type of attack happens where the financial transactions are higher. Penny shaving and Salami Slicing are some of the types of Salami Attack [6].

vi. ***Web Hijacking***

Also known as browser hijacking, wherein a malware trying to access the browser setting of a user and redirecting the user who is using the website to some other links where they are not intended to visit. It is otherwise called a browser redirect virus.

vii. **Cyber Defamation**

It refers to the publication of defamatory or false information of an organization or individual in the Online platform. This may consist of statements such as forums, blogs, social media, or any other online means. This type of defamation may result in loss of reputation of an organization or an individual which leads to loss of business, emotional stress, or some other financial damage. The intention behind this type of attack is to spoil the reputation of an individual or an organization. The two types of defamation are *slander* which is done orally and *libel* which is written statement online [7].

viii. **Email Bombing**

This type of cybercrime consists of sending many emails to a particular email address which results in crashing the mail server and thus it disturbs the web portal or website and its functionality. It is one type of denial-of-service attack wherein the purpose is to overwhelm a particular email inbox.

ix. **Data Diddling**

This refers to the act of entering information which is not correct and thus leads to falsified information being entered. It often results in inflation when dealt with numbers such as salary or expenses. The data is being altered before it is coded into the machine [4].

x. **Cyber Terrorism**

This is targeted attack that has been made politically across nations to attack a country's military points, air traffic controls, banks, and telecommunication networks. This type of attack may happen for several reasons, and it is considered more powerful than the traditional methods used by terrorist.

4. MOTIVATION BEHIND CYBER CRIMINALS

The motivation behind cyber criminals is that they have to collapse the regular business activity and also, they try to manipulate the data that has been stolen to have a financial loss, to destroy the reputation of an individual. Some people just do this to test their knowledge and to have some fun. Some types of cyber criminals are Black hat hackers, Gray Hat Hackers, White hat hackers, script kiddies, Suicide hackers, state sponsored hackers, hacktivists, and cyber terrorists.

5. UKRAINE POWER GRID ATTACKS - CASE ANALYSIS

Overview

In December 2015 and again in 2016, Ukraine experienced significant power outages caused by cyberattacks on its power grid. These incidents are among the first known instances where cyberattacks successfully disrupted an electricity supply.

Attack Mechanism

Initial Access: The attackers gained access to the network through phishing emails containing malicious attachments, which allowed them to obtain credentials for the control systems.

Control System Manipulation: Using the stolen credentials, the attackers remotely accessed the Supervisory Control and Data Acquisition (SCADA) systems and manipulated circuit breakers to cut power.

Destructive Actions: The attackers deployed malware such as BlackEnergy3 and KillDisk to erase data from systems and render them inoperable, making recovery more difficult.

Impact

Power Outages: The 2015 attack caused outages affecting approximately 230,000 people for several hours. The 2016 attack, although smaller in scale, demonstrated increased sophistication.

Response and Recovery: The attacks highlighted the need for improved incident response and recovery plans. Ukraine had to manually restore power, a process that took several hours.

International Implications: These attacks underscored the potential for cyber warfare to disrupt critical infrastructure and prompted other nations to reevaluate their cybersecurity strategies for power grids [8].

6. TYPES OF CYBER SECURITY TOOLS

To captivate all the problems discussed above a set of tools are available to eradicate all these complaints by safeguarding the individual as well as an organization sensitive data. These tools will help us to protect the confidentiality and integrity of data. As far as information security or Cyber Security is concerned it follows three principles *a. Confidentiality b. Integrity* and *c. Availability[9].*

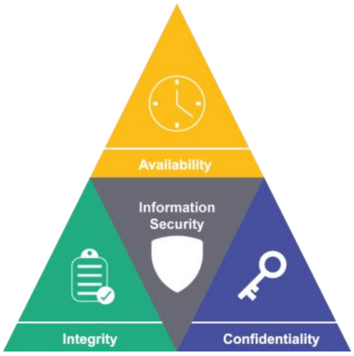

Fig- II. Security Triangle (CIA)

There are several tools available that are used by various organizations to safeguard their data. The different tools are.

Network security tools

This will help to manage and detect the intrusions happening in a network [10]. It is the responsibility of this tool to collect, analyze and escalate the occurring threats as soon as possible. Some of the tools which help in carrying out this task are listed below.

- ➢ Splunk- Fast versatile tool which monitors the network.
- ➢ POF- Monitors network without creating additional traffic.
- ➢ OSSEC-Open-Source Cyber Security tool which monitors intrusions.

Encryption tools

There are a number of encryption tools which primary concern is to protect our data by storing our data in a varied form. The data that has been encrypted will not be in original form once encryption is done. The following are some of the tools which are used for this encryption**.**

- Encryption Tools
    - ➢ TrueCrypt
    - ➢ Key Pass
    - ➢ Tor
- Web vulnerability tools
    - ➢ Nmap
    - ➢ Nikto
    - ➢ Burp Suite
- Network defense wireless-tools
    - ➢ Netstumbler
    - ➢ Aircrack-ng
    - ➢ KisMAC
- Packet sniffers
    - ➢ Cain and Abel
    - ➢ Wireshark
    - ➢ John the Ripper
- Firewalls
    - ➢ GlassWire Firewall
    - ➢ AVS Firewall
    - ➢ Mcafee Firewall
- PKI
- Antivirus software
    - ➢ Avast Business Antivirus
    - ➢ Bitdefender Endpoint Security
    - ➢ Kaspersky Endpoint Security
- Managed detection tools
    - ➢ Snort
    - ➢ Forcepoint
    - ➢ GFI LanGuard
- Penetration testing tools
    - ➢ Kali Linux
    - ➢ Metasploit

7. CONCLUSION

The empirical analysis highlights the dynamic nature of the cybersecurity landscape. Organizations must continuously adapt to emerging threats by leveraging advanced technologies and fostering collaborative efforts. Future research should focus on the long-term impact of these trends and the development of new defensive strategies. The case study presented highlights the need for comprehensive cybersecurity measures, continuous monitoring, and the development of resilient systems to protect critical infrastructure from cyber threats.

REFERENCES

[1] ISACA, "Securing the Future: Enhancing Cybersecurity in 2024 and Beyond," 2024. [Online]. Available: https://www.isaca.org.
[2] McKinsey, "Cybersecurity Trends: Looking Over the Horizon," 2024. [Online]. Available: https://www.mckinsey.com.
[3] Verizon, "Data Breach Investigations Report," 2023. [Online]. Available: https://www.verizon.com.
[4] VMware Security Blog, "Amid COVID-19, global orgs see a 148% spike in ransomware attacks: finance industry heavily targeted," Apr. 15, 2020. [Online]. Available: https://blogs.vmware.com.
[5] B. Carlson, "Top cybersecurity statistics, trends, and facts," CSO Online, Oct. 7, 2021. [Online]. Available: https://www.csoonline.com.
[6] J. Smith, "Zero Trust Security: A Comprehensive Overview," Int. Journal of Cyber Security., vol. 12, no. 2, pp. 112-125, 2023.
[7] A. Kumar, "Password less Authentication: A Future Without Passwords," J. Inf. Security., vol. 15, no. 4, pp. 256-267, 2023.
[8] D. Lee, "Behavioural Analytics in Cybersecurity: Detecting Insider Threats," Comput. Security., vol. 92, pp. 101745, 2024.
[9] S. Green, "Collaboration in Cybersecurity: Bridging the Gap Between Public and Private Sectors," Gov. Inf. Q., vol. 41, no. 1, pp. 98-108, 2024.
[10] M. Johnson, "Navigating Regulatory Compliance in Cybersecurity," J. Law Cyber Security., vol. 9, no. 1, pp. 45-59, 2024.