Cyber Security And The Fifth Generation Cyberattacks

Neha Kaushal, Ranvir kaur
Mca, Assistant Professor
Rayat Bahra University

Abstract

The prevalence of cyberattacks has surged in this era of interconnected ness. With each passing year, cybercrimes have witnessed a notable rise, accompanied by an escalation in the severity of their impact. Consequently, safeguarding against these malicious activities has emerged as an utmost priority in the digital realm. Yet, guaranteeing cybersecurity is an intricate undertaking, demanding expertise in attack vectors and the ability to analyze potential threats. The primary obstacle in the realm of cybersecurity lies in the ever-evolving nature of these attacks. This manuscript illuminates the profound importance of cybersecurity while shedding light on the diverse risks prevailing in the contemporary digital era.

Keywords

Cyberattacks;
Cybersecurity;
Fifth Generation;
Machine Learning Algorithm;
Security Threats.

Introduction

With the growing reliance on the Internet, virtually all industries,cyberspace. This paradigm shift has rendered the cyber infrastructure more susceptible to malicious cyberattacks. A cyberattack denotes a deliberate and malevolent endeavor undertaken by an individual or organization to infiltrate the information system of another entity. Business organizations, military establishments, governments, and financial institutions, particularly banks, are the primary targets of these cyber assaults, which aim to either gain unauthorized access to secure information or extort a ransom. The sheer scale and complexity of technology involved in cyberattacks have witnessed a drastic escalation, emerging as a significant menace to the cyber world. Trustwave's 2015 Global Security
Report provides insight into this pressing issue.

Acquiescent

A cyberattack refers to a malicious endeavor, conducted by individuals or organizations, with the intent to infiltrate the information system of another entity. Business organizations, military establishments, governments, and financial institutions, such as banks, are the primary targets of thesecyber assaults, which aim to either gain unauthorized access to secure information or extort a ransom. The proliferation of technology and the increasing knowledge base surrounding cyberattacks have resulted in a significant threat to the cyber world. Trustwave's 2015 Global Security Report revealed that approximately 98% of tested web applications were found to be vulnerable to cyberattacks. Furthermore, according to the Department of Business, Innovation and Skills' 2015 security survey, 90% of large organizations and 74% of small organizations experienced security breaches. These alarming statistics emphasize the urgency and importance of the field of cybersecurity as an area of research.

Cybersecurity encompasses measures to ensure the confidentiality, integrity, and availability of information in cyberspace. While it is a single term, achieving effective cybersecurity involves the coordination and integration of various domains. Figure 1 illustrates the internelationships between these domains, highlighting the complex nature
of cybersecurity. These domains can be described as follows:

1. Application Security: This domain focuses on implementing measures to enhance the security of applications. It involves monitoring applications, identifying and fixing security vulnerabilities, and implementing preventive measures.

2. Information Security: Information security encompasses procedures and practices to ensure the confidentiality, integrity, and availability of business data and information in various forms. It aims to protect sensitive information from unauthorized access, alteration, or destruction.

3. Network Security: Network security is designed to safeguard the usability and integrity of a network and its data. It involves employing hardware and software technologies to protect the network from unauthorized access, data breaches, and other security threats.

4. Operations Security: Operations security involves identifying and protecting critical, unclassified information that may be targeted by competitors or adversaries. It focuses on securing sensitive operational information and preventing unauthorized disclosure

5. Internet Security: Internet security encompasses a range of processes aimed at ensuring the security of online transactions. It involves protecting web browsers, networks, operating systems, and applications by establishing and enforcing rules and regulations to mitigate potential attacks.

6. ICT Security: ICT (Information and Communication Technology) security focuses on protecting the confidentiality, integrity, and availability of an organization's digital information assets. It involves implementing security measures for digital systems, networks, and communication channels.

7. End-User Knowledge: End-user knowledge is a critical aspect of cybersecurity since humans are often the weakest link in the chain. The lack of user knowledge about cybersecurity risks contributes to approximately 50% of cyberattacks, and nearly 90% of cyberattacks are caused by human behavior. Educating end-users about cybersecurity best practices and promoting awareness is essential to mitigate risks. However,cybercriminals continuously adapt and employ new methods and technologies for their attacks. They exploit security vulnerabilities and breaches in secured systems, rapidly stealing information or causing damage. In this digital era, where individuals conduct various daily activities online, there is an urgent need for enhanced cybersecurity with new techniques. To counter cyberattacks effectively, cybersecurity must evolve at an equal pace with the attacks themselves. Although numerous techniques have been suggested and implemented, the impact of cyberattacks continues to increase. Cybersecurity must focus on protecting private, personal, and government data by addressing three primary tasks:

1. Taking measures to protect equipment, software, and the information they contain.

2. Guaranteeing the state or quality of being protected from several threats; and protecting browsers, networks, operating systems, and applications.

3. Ensuring the confidentiality, integrity, and availability of information by implementing appropriate security measures.

Fig.1: Cyber Security and various Domains

3. Implementing and improving these activities.

In recent years, many non-profit organizations and projects have been carried out with the aim of facing security threats. The most popular organization is Open Web Application Security Project (OWASP), an international non-for- profit charitable organization that focuses on application security.6 Every year they identify and release the series of software vulnerabilities and describe the ten most important in their top ten projects. In the year of 2018, the top ten vulnerabilities listed by the OWASP are injection, broken authentication and session management, sensitive data exposure, XML External Entities (XXE), Broken Access control, Security misconfigurations, Cross-Site Scripting (XSS), Insecure Deserialization, Using Components with known vulnerabilities, Insufficient logging and monitoring.

Cyber Attack Statistics

In the second quarter of 2018, Positive Technologies reported a 47% increase in the number of unique cyber incidents compared to the previous year. Kaspersky Labs found that the number of malicious mobile installation packages in the third quarter of 2018 had risen by almost a third compared to the preceding months. Norton states that 99.9% of these packages originate from unofficial "third-party" app stores, highlighting the importance of avoiding such sources to

mitigate attacks. A timeline representing major cyberattacks in 2017 demonstrates the severity of the issue. As reported by the Atlanta Journal -Constitution, the City of Atlanta spent $2.7 million to repair damage caused by a ransomware attack. The 2018 IT Professionals Security Report Survey revealed that 76% of organizations experienced a phishing attack in the past year, while 49% faced a DDoS attack. The 'AdultSwine' malware infected up to 7 million devices through 60 Children's Games Apps. Additionally, Cryptolocker Malware impacted over 20% of organizations weekly, while 40% of organizations were affected by Cryptominers in 2018 (according to Check Point Research Blog). Further highlighting the widespread impact, over 300 apps on the Google Play Store contained malware and were downloaded by more than 106 million users. Moreover, Chinese government hackers allegedly stole 614 GB of data related to weapons, sensors, and communication systems from US Navy contractors. Check Point's global attack sensors conducted a survey on vulnerabilities introduced over the past eight years, revealing crucial findings. These incidents underscore the escalating threat landscape and the urgent need for robust cybersecurity measures
to protect individuals, organizations, and critical infrastructure from cyberattacks

Cyber Security Threats

The primary objective of cyberattacks is to either disable or gain unauthorized
access to the target system . Achieving this goal involves employing various attack

methods, which continue to evolve and become more sophisticated with each passing day. Here are explanations of some common cyber-attacks:

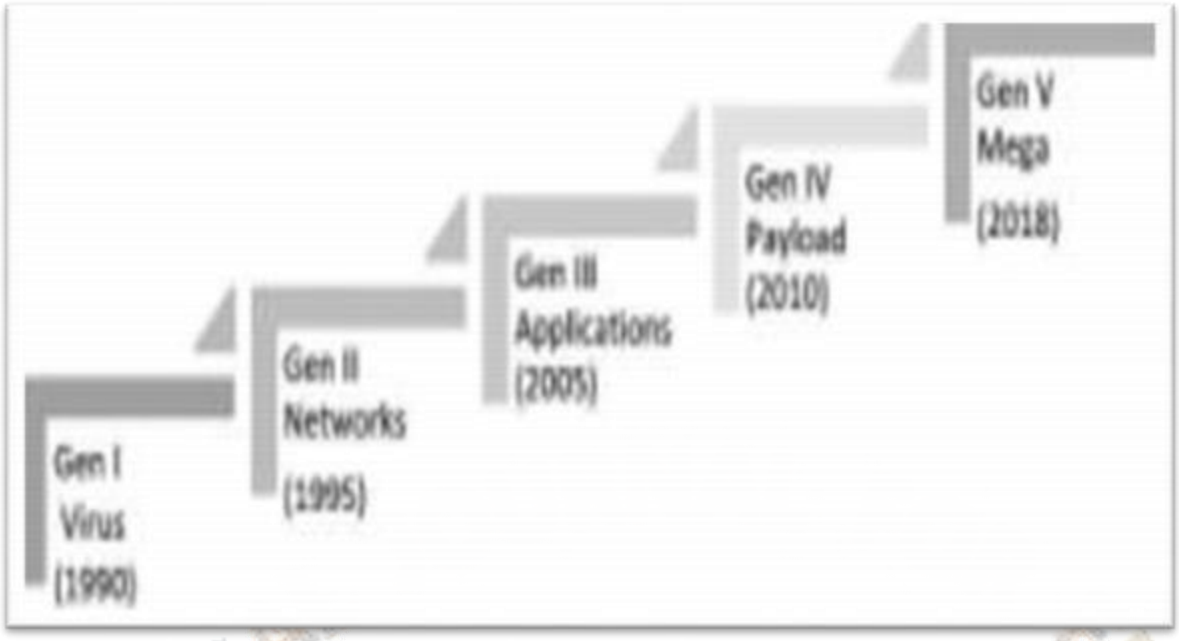

Fig. 2: Cyber Security attack generation

Man-in-the-middle-Attack

Man-in-the-middle (MitM) attacks occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data. It is normally known as eavesdropping attacks. Several variations of the MITM attack exist that include password stealing, credential forwarding, etc. Normally on an unsecure public Wi-Fi, attackers can insert themselves between a visitor's device and the network. Without knowing, the visitor passes all information through the attacker. In some cases, the attacker installs some software to gather the information about the victim through malware.

Zero-day-Exploit

A zero-day exploit hits after a network vulnerability is announced but before a patch or solution is implemented. Attackers target the disclosed vulnerability during this window of time. Zero-day vulnerability threat detection requires constant awareness.

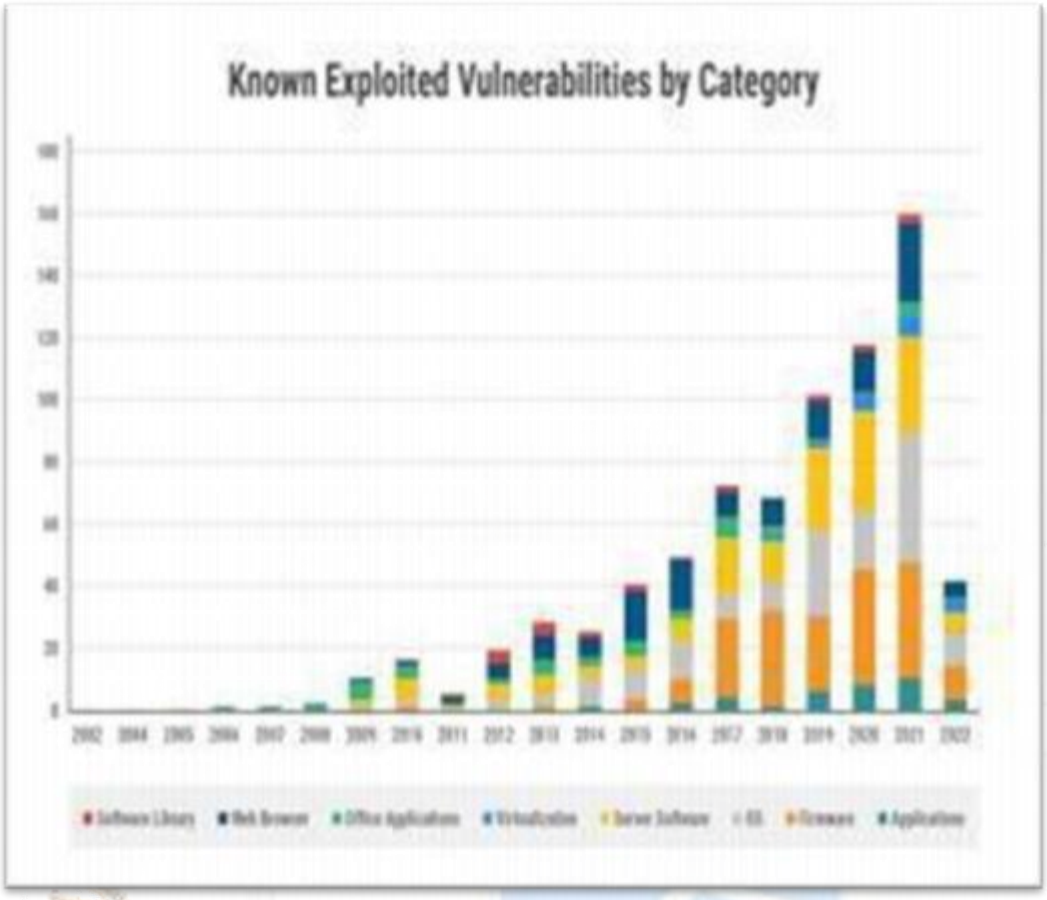

Fig. 3: Percentage of attacks that leveraged new vulnerability

Moving the fifth generation Cyber Scurity Architecture

The rapid digital transformation of businesses has placed increasing demands on security measures. However, current security architectures are often outdated and become the common cause of unavailability and security issues that lead to failures. Therefore, there is a pressing need to implement a fifth-generation architecture that incorporates c infrastructure and the Internet of Th (IoT). By doing so, businesses can elimi single points of failure and provide necessary strength and resiliency to en operations and security even under adv Circumstances. The proposed
security architecture sh establish a consolidated and un approach that integrates

and mana mobile, cloud, and network security. comprehensive strategy aims to pro against and prevent fifth-genera cyberattacks. Integrated threat prevention must w seamlessly with a dynamic security p across all platforms, aligning with busi needs and supporting cloud dema through auto scaling. It should also the flexibility to integrate with third-p APIs. Furthermore, a unified and advanced m layered threat prevention environmene ssential. It should encompass CPU- sandbox prevention, threat extraction, phishing, and anti-ransomwaresolution defend against both known and unk n "zero-day" attacks. By implementing right architecture, organizations
safeguard their network infrastruc cloud services, and mobile infrastruc effectively.

To conclude, there is a need to rawareness among organizations individuals about the impact cyberattacks and the available sec solutions. It is crucial for everyone to technology after analyzing its pros and cons while aking measures to secure their information. The future work in this area aims to propose a fifth-generation security framework to protect online digital infrastructure, including cloud, mobile, and network
infrastructure.

Conclusion

In summary, this cybersecurity review paper has shed light on the challenges and opportunities within the field. By synthesizing existing research, it provides a comprehensive overview of the current state of cybersecurity. The findings underscore the need for proactive measures, continuous education, and collaborative efforts to safeguard digital assets and protect against cyber threats. By leveraging these insights, policymakers, practitioners, and researchers can work together to build a more secure and resilient cyber landscape. Cybersecurity is one of the most important aspects of the fast-paced growing digital world. The threats of it are hard to deny, so it is crucial to learn how to defend from
them and teach others how to do it too. If you want to learn more about

what is cybersecurity and how to deal with cybercriminals, hop into our courses section and become a hero in the digital platforms. Organizations are finding themselves under the pressure of being forced to react quickly to the dynamically increasing number of cybersecurity threats. Since the attackers have been using an at lifecycle, organizations have also b forced to come up with a vul nera management lifecycle. The vulnera management lifecycle is designed counter the efforts made by the attac in the quickest and most effective way. This chapter has discussed the vulnerability management lifecycle in terms of the vulnerability management strategy. It has gone through the steps of asset inventory creation, the management of information flow, the assessment of risks, assessment of vulnerabilities, reporting, and remediation.

References

1. Trustwave Global Security. Report retrieves from:
https://www2.trustwave.com/rs/81critical web application security risks.
RFM693/images/2015_TrustwaveGlobalS The OWASP Foundation. 2018.
RityReport.pdf

2. International Organization for StandardIza ISO/IEC 27032:2012.
Information techno
— Security techniques — Guidelines cybersecurity. 2012

3. Chowdhury A. Recent cybersecurity attand their mitigation approaches - Overview In International conference application and techniques in information security, Springer, Singapore. 2016; pp 54

4. Passeri P. Cyber Attacks Statistics Paolo Passeri, May 2016.
http://www.hackmageddon.com/category/security/cyberattacks-statistics/. Accessed 07 October 2016

5. Fischer EA. Creating a national framework for cybersecurity: an analysis of issues and options. Technical report. Congressional Research Service. 2005.

6. The Open Web Application Security Project (OWASP). 2018. Available online:https://www.swascan.com/owasp/

7.The Open Web Application Security Project OWASP Top 10 — the ten most critical web application security risks.

8. Check Point Research Survey of IT Security Professionals, sample size: 443 participants. 2018.

9. Check Point Mobile Threat Research Publications. 2017. Available Online:https://research.checkpoint.com/chec k-point-mobile-research-team- looks-back 2017/

10. Cyber Attack Trends Analysis Key Insights to Gear Up for in 2019. Available Online: http://www.snt.hr/boxcontent/CheckP
ointSecurityReport2019_vol01.p

11. 56 SARAVANAN & BAMA, Orient. J. Comp. Sci. & Technol., Vol. 12(2) 50 56 (2019)13.

12. Wu C.H. Behavior-based spam detection using a hybrid method of rule- based techniques and neural networks. Expert Syst Appl. 2009: 36(3):4321 - 4330.19.

13. In: IEEE 2011 eighth international conference on fuzzy systems and knowledge discovery (FSKD), 2011; pp 2659-2662.18.

14. Wu C.H. Behavior-based spam detection using a hybrid method of rule- based techniques and neural networks. Expert Syst Appl. 2009: 36(3):4321 -4330.19

15. Hazza Z.M., Aziz N.A. A new efficient text detection method for image spam filtering. Int Rev Comput Softw. 2015; 10(1):1 -8.20.

16. Dhaya R., Poongod i M. Detecting software vulnerabilities in android using static analysis. 2015; pp 915-918.21

17. Markel Z., Bilzor M. Building a machine learning classifier for malware detection. In: Second workshop on anti-malware testing research (WATeR). IEEE. Canterbury. UK. 2015. 22.

18. Shijo P.V., Salim A. Integrated static and dynamic analysis for malware detection.