



A Review on Cyber Security and the Fifth Generation Cyberattacks

A. SARAVANAN¹ and S.SATHYA BAMA²

¹Department of MCA, Sree Saraswathi Thyagaraja College, Pollachi, India.

²483, Lawley Road, Coimbatore, Tamil Nadu, India.

Abstract

Cyberattacks has become quite common in this internet era. The cybercrimes are getting increased every year and the intensity of damage is also increasing. providing security against cyber-attacks becomes the most significant in this digital world. However, ensuring cyber security is an extremely intricate task as requires domain knowledge about the attacks and capability of analysing the possibility of threats. The main challenge of cyber security is the evolving nature of the attacks. This paper presents the significance of cyber security along with the various risks that are in the current digital era. The analysis made for cyber-attacks and their statistics shows the intensity of the attacks. Various cyber security threats are presented along with the machine learning algorithms that can be applied on cyberattacks detection. The need for the fifth generation cybersecurity architecture is discussed.



Article History

Received: 30 January 2019

Accepted: 24 May 2019

Keywords

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

Introduction

Due to the increasing trust and usage of the Internet, almost all the industries, government and even financial institutions has transformed their transactions to the cyber infrastructure. This makes the cyber system more vulnerable to cyberattacks. A cyberattack is a malicious attempt made by an individual or organization to breach the information system of another individual or organization. Most commonly, cyberattacks target the business


organization, military, government, or other financial institutions such as banking either for hacking secured information or for a ransom.

The volume and knowledge of the technology in cyberattack are increasing drastically. This become the important threats to the cyber world. According to Trustwave's 2015 Global Security Report, approximately, 98% of tested web applications were found vulnerable to cyber-attack. Based on the

CONTACT A. Saravanan ✉ ssathya21@gmail.com 📍 Department of MCA, Sree Saraswathi Thyagaraja College, Pollachi, India.



© 2018 The Author(s). Published by Oriental Scientific Publishing Company

This is an  Open Access article licensed under a Creative Commons license: Attribution 4.0 International (CC-BY).

Doi: <http://dx.doi.org/10.13005/ojst12.02.04>

Department of Business, Innovation and Skills' 2015 security survey 90% of the huge organization and 74 % of the small organization agonized from security breaches.¹ Thus the term cyber security has become the most prominent field under research. Cyber security ensures preserving confidentiality, integrity and availability of information in the Cyberspace². Though cybersecurity is a single term, to guarantee the security it involves the coordination of the various other domains. This relationship between various domain is depicted in Figure 1.

These domains are simply described below.

- Application security implementing various measures to improve the security of an application. This is often done by monitoring the application and finding, fixing and preventing security vulnerabilities.
- Information Security is a set of procedures or practices to maintain the confidentiality, integrity and availability of business data and information in various forms.
- Network security is a process designed to shield the usability and integrity of the network and its data and provide secured access towards the network. Network security always includes both hardware and software technologies.
- Operations security is a process of identifying and protecting unclassified critical information which are often attractive for the competitor or adversary to gain real information.
- Internet security involves various security

processes implemented for ensuring the security of online transactions. It involves protecting browsers, network, operating systems, and other applications from attacks by setting up precise rules and regulations.

- ICT security is the ability to protect the Confidentiality, Integrity and Availability of an organization's digital information assets.
- End-User Knowledge is most significant since people are the weakest link in the cybersecurity chain. The lack of user knowledge about cybersecurity risks is the reason for 50% of the cyberattack and almost 90% of cyberattacks are caused by human behaviour.

However, the attacks made by the cyber criminals are getting smarter and they use new methods and technology for successful attacks. They often find the security holes and breaches in the secured system and steal information or damage the system in less time.³ In this digital era, since people do all the major day to day activities online, there is an urgent need for the improved cyber security with new techniques. To neutralize the cyberattacks, equal growth in the cyber security as attacks is required. Though several new techniques are suggested by various researchers and many techniques are currently in use, the effect of an attack is still increasing.⁴ Cybersecurity has to protect any private, personal or government data from attacks by focusing on three main tasks.⁵

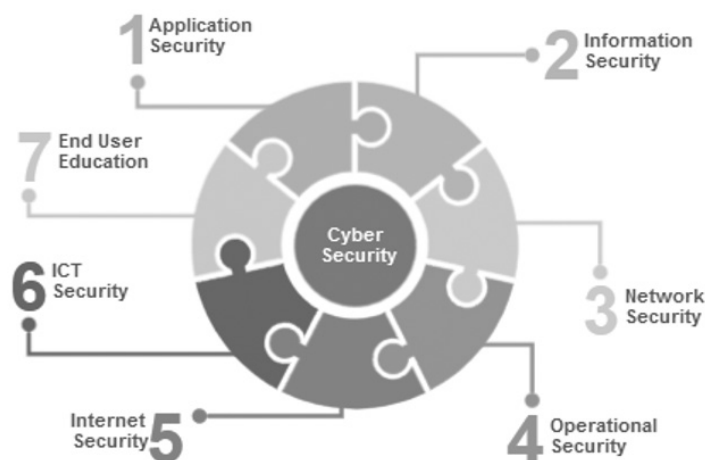


Fig. 1: Cyber Security and various domains

1. Taking measures to protect equipment, software and the information they contain.
2. Guaranteeing the state or quality of being protected from the several threats; and
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 the application security.⁶ Every year they identify and release the series of software vulnerabilities and describe the ten most important in their top ten project. 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.⁷

The cyber-attacks have emerged to fifth generation, though, 97%. Of organizations are using outdated security technologies and equipped for second and third generation attacks.⁸ The cyber security generations are elaborated in Figure 2.

Cyber Attack Statistics

The number of unique cyber incidents in the second quarter of 2018, as defined by Positive Technologies, was 47 percent higher than the number from just a year previous. In the third quarter of 2018, Kaspersky Labs the number of malicious mobile installation packages was up by nearly a third when compared

to just the previous few months. But there's an easy way to avoid those attacks, as Norton says that 99.9 percent of those packages come from unofficial "third party" app stores. The major cyberattacks for the year 2017 is represented as a timeline.

According to the report given by Atlanta Journal-Constitution newspaper – www.ajc.com, \$ 2.7 million spent by the City of Atlanta to repair damage from ransomware attack. A report given by 2018 IT Professionals Security Report Survey says that 76% of organizations experienced a phishing attack in the past year and 49% of organizations experienced a DDoS attack in the past year. The ‘AdultSwine’ malware was installed up to 7 million times across 60 Children’s Games Apps. Over 20% of organizations are impacted by Cryptojacking Malware every week and 40% of organizations were impacted by Cryptominers in 2018. (Check Point Research Blog).

Over 300 apps in the google play store contained malware and were downloaded by over 106 million users.⁹ 614 GB of data related to weapons, sensor and communication systems stolen from US Navy contractor, allegedly by Chinese government hackers. Check Point global attack sensors undergone a survey on the new vulnerabilities introduced in the past 8 years The values are depicted in Figure 3.¹⁰

Cyber Security Threats

The common goal of the cyberattacks is to disable or to gain access to the target system. The goal can be achieved by applying various attacks on the target system. Several cyberattacks exist and even evolve day by day. Some of the common cyberattacks are explained below:

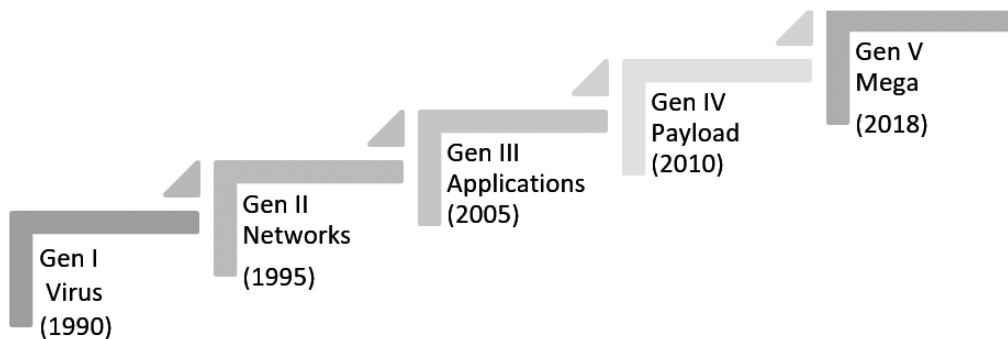


Fig. 2: Cyber Attack Generation

Malware

Malware is a malicious software that is designed to cause destruction to a single system or a network. Basic malevolent software such as worms, viruses, and trojans and recent malicious software such as spyware, ransomware belongs to this category. The malware infects the system or network when a user clicks a dangerous link, through email attachment or while installing risky software. The main point to be noted is that the malware reproduces or spreads when it interacts with other system or device. Some of the causes includes blocking access to the network, installs additional spiteful software, gathers information.

Phishing

Phishing is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email. The goal is to steal sensitive data like credit card and login information or to install malware on the victim's machine. Phishing is an increasingly common cyber threat.

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 exists that includes 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.

Cryptojacking

A specialized attack that involves getting someone else's computer to do the work of generating cryptocurrency for the target. The attackers will either install malware on the victim's computer to perform the necessary calculations, or sometimes run the code in JavaScript that executes in the victim's browser.

Denial-of-service Attack

A denial-of-service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to process the legitimate requests. Attackers can also use multiple compromised devices to launch this attack. Instead of launching single attacks, the attacker launches several attacks to the victim. This is known as a distributed-denial-of-service (DDoS) attack. 24% of companies have experienced a DDoS attack in the past year¹¹

SQL Injection

A Structured Query Language (SQL) injection is a quite common attack that occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not. An attacker could carry out a SQL injection simply by submitting malicious code into a vulnerable website search box.

Zero-Day Exploit

A zero-day exploit hits after a network vulnerability is announced but before a patch or solution is

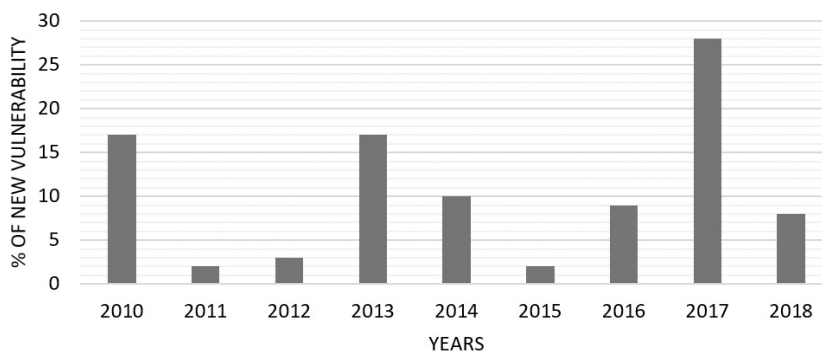


Fig. 3: Percentage of attacks that leveraged a new vulnerability

implemented. Attackers target the disclosed vulnerability during this window of time. Zero-day vulnerability threat detection requires constant awareness.

Spam

It an e-mail message that is unwanted.¹² Spam e-mails can be not only a time-consuming task for recipients but a source of Java applets that may execute automatically when the message is read.¹³

Apart from the above mentioned threats, SANS Institute identifies the following malicious spyware actions as the most frequent, malicious activities¹⁴:

- changing network settings,
- disabling antivirus and antispymware tools,
- turning off the Microsoft Security Center and/or automatic updates,
- installing rogue certificates,
- cascading file droppers,
- keystroke logging,
- URL monitoring, form scraping and screen scraping,
- turning on the microphone and/or camera,
- pretending to be an antispymware or antivirus tool,
- editing search results,
- acting as a spam relay,
- planting a rootkit or altering the system to prevent removal,
- installing a bot for attacker remote control,
- intercepting sensitive documents and exfiltrating them, or encrypting them for ransom,
- planting a sniffer.

Some of the fifth generation cyber-attacks includes Andromeda, AdvisorsBot, Cerber, CNRig, Cryptoloot, Fireball, HiddenMiner, Iotroop, Nivdort, NotPetya, RubyMiner, Trickbot, WannaCry, WannaMine, Ransomware, adultSwine, and cryptocurrency attacks. These are sophisticated attacks that cause severe damage.

Machine Learning and Cybersecurity

Numerous methods and procedures have been developed in the literature for the detection of threats in the cyberspace. Recently machine learning has contributed much in the cyber security. In case of spam detection, basically filters are used to analyse

the content to differentiate whether the message is spam or not. The machine learning algorithms such as Bayesian classifier,¹⁵ SVM,¹⁶ MapReduce,¹⁷ Behaviour-based spam detection using neural networks,¹⁸ Text detection method for image spam filtering¹⁹ were suggested.

Statistical analysis based malware detection was introduced in.²⁰ Malware detection using machine learning was suggested.²¹ Statistical and dynamical based malware detection was suggested by Shijo and Salim.²² detecting of internet worm malcodes using principal component analysis and multiclass support vector machine was introduced.²³ For detecting phishing email, random forest machine learning technique was employed.²⁴ Several supervised learning algorithms were introduced to detect the phishing sites.²⁵ Thus clustering algorithm and classification algorithms such as SVM, Random Forest, Naïve Bayes classifier, neural network, fuzzy based classifier is commonly used in detecting the security threats that includes spam detection, malware detection and phishing detection.

Moving to Fifth Generation Cyber Security Architecture

The rapid digital transformation of business places increasing demands on security. Current security architectures to manage all this are outdated and are the most common cause for unavailability and security issues that lead to failure. Thus there is a need for implementing fifth generation architecture that includes cloud infrastructure and Internet of Things, though, businesses can eliminate single points of failure by providing the necessary strength and resiliency to maintain operations and security under any circumstances.

This security architecture must build a consolidated, unified security architecture that manages and integrates with mobile, cloud and networks to protect against and prevent fifth generation cyberattacks. Integrated threat prevention also needs to work with a dynamic security policy across all platforms that expresses business needs, supports cloud demands with auto scaling and is able to flexibly integrate with third-party APIs. Furthermore, a unified and advanced multi-layered threat prevention environment must include CPU-Level sandbox prevention, threat extraction, anti-phishing and

anti-ransomware solutions to defend against known and unknown 'zero-day' attacks. In this way, having the right architecture upon which the entire security infrastructure operates is the only way to ensure a single, cohesive wall of protection to prevent fifth generation cyberattacks.²⁶

Conclusion

In the past 20 years, cyberattacks and the cybersecurity have advanced and evolved rapidly due to the technological advancement. Though this is the case, unfortunately, most organizations have not evolved and are still using second or third generation cyber security even after the evolution of the fifth generation of These fifth generation attacks are named as mega attacks as it large-scale and fast-moving attacks. These sophisticated attacks can effortlessly bypass the conventional, static detection-based security systems that are used by the most of the today's organizations. Thus to defend

the latest attacks, organizations should implement the fifth generation security architecture to protect their network infrastructure, cloud and mobile infrastructure. Thus to conclude, the awareness among the organizations and individuals about the cyberattacks and their effect along with the security solutions are to be increased. Everyone should use the technology only after analysing the pros and cons and the security breaches and care must be taken to secure their information. The future work aims at proposing the fifth generation security framework to protect the online digital infrastructure that includes cloud, mobile and network infrastructure.

Acknowledgements

This research has not received any specific grant from funding agencies in the public, commercial, or not-for-profit sectors. The authors declare no conflict of interest.

Reference

1. Trustwave Global Security. Report retrieved from: https://www2.trustwave.com/rs/815-RFM693/images/2015_TrustwaveGlobalSecurityReport.pdf
2. International Organization for Standardization. ISO/IEC 27032:2012. Information technology—Security techniques—Guidelines for cybersecurity. 2012
3. Chowdhury A. Recent cyber security attacks and their mitigation approaches—An Overview. In International conference on applications and techniques in information security, Springer, Singapore. 2016; pp 54-65.
4. Passeri P. Cyber Attacks Statistics Paolo Passeri, May 2016. <http://www.hackmageddon.com/category/security/cyber-attacks-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. The OWASP Foundation. 2018.
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/check-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/CheckPointSecurityReport2019_vol01.pdf
11. Check Point C-Level Perspective Survey. 2017. sample size: 59 C-Level Executives. Available Online: <https://www.checkpoint.com/downloads/product-related/report/2018-security-report.pdf>
12. Drucker H. Wu D. Vapnik VN. Support vector machines for spam categorization. *IEEE Trans Neural Netw Publ IEEE Neural Netw Counc* 1999; 10(5):1048–54

13. Cranor LF, Lamacchia BA. Spam!. Commun ACM. 1998; 41(8):74–83
14. SANS Institute. Top 15 Malicious Spyware Actions. 2018. Available Online: <https://www.sans.org/security-resources/>
15. Wang Z.J., Liu Y., Wang Z.J. E-mail filtration and classification based on variable weights of the Bayesian algorithm. Appl Mech Mater. 2014; 513–517:2111–2114.
16. Hsu W.C., Yu T.Y. E-mail spam filtering based on support vector machines with Taguchi method for parameter selection. J Converg Inf Technol 2010. 5(8):78–88.
17. Caruana G., Li M., Qi M. A MapReduce based parallel SVM for large scale spam filtering. In: IEEE 2011 eighth international conference on fuzzy systems and knowledge discovery (FSKD), 2011; pp 2659–2662.
18. 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. 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. Dhaya R., Poongodi M. Detecting software vulnerabilities in android using static analysis. 2015; pp 915–918.
21. 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. Shijo P.V., Salim A. Integrated static and dynamic analysis for malware detection. Procedia Comput Sci. 2015; 46:804–811.
23. Divya S., Padmavathi G. A novel method for detection of internet worm malcodes using principal component analysis and multiclass support vector machine. Int J Secur Appl. 2014; 8(5):391–402
24. Akinyelu A.A., Adewumi A.O. Classification of phishing email using random forest machine learning technique. J Appl Math 2014; pp 1–6.
25. Santhana Lakshmi V., Vijaya M.S. Efficient prediction of phishing websites using supervised learning algorithms. Procedia Eng. 2012; 30:798–805.
26. Check point 2018 security report. 2018. Available Online: <https://www.checkpoint.com/downloads/product-related/report/2018-security-report.pdf>.