A Study of Cyber Security Issues and Challenges

Rohit Chivukula
School of Computing and Engineering
University of Huddersfield
Huddersfield, United Kingdom
rohit.chivukula.cse@gmail.com

T.Jaya Lakshmi
Department of Computer Science and Engineering
SRM University, AP
Adhra Pradesh, India.
jaya.phd.hcu@gmail.com

Lohith Ranganadha Reddy Kandula
Department of Computer Science and Engineering
SRM University, AP
Andhra Pradesh, India
lohith_ranganadhareddy@srmap.edu.in

Kalavathi Alla
Department of Information Technology
Vasireddy Vemkatadri Institute of Technology
Andhra Pradesh, India.
kalavathi_alla@yahoo.com

2021 IEEE Bombay Section Signature Conference (IBSSC) | 978-1-6654-1758-7/21/$31.00 ©2021 IEEE | DOI: 10.1109/IBSSC53889.2021.9673270

***Abstract*—Life has reached a stage where we cannot live without internet enabled technology. New devices and services are being invented continuously with the evolution of new technologies to improve our day-to-day lifestyle. At the same time, this opens many security vulnerabilities. There is a necessity for following proper security measures. Cybercrime may happen to any device/service at any time with worst ever consequences. In this study, an overview of the concept of cyber security has been presented. The paper first explains what cyber space and cyber security is. Then the costs and impact of cyber security are discussed. The causes of security vulnerabilities in an organization and the challenging factors of protecting an organization from cybercrimes are discussed in brief. Then a few common cyber-attacks and the ways to protect from them are specified. At last, a famous case study of Mirai's attack on a few high-profile victims and the impact is presented.**

***Index Terms*—Cyber space, cyber security, cost and impact of cyber security, cyber-attack, Mirai botmet.**

I. Introduction

Cyber security is concerned with keeping the cyber space safe. Cyber space is a virtual world driven by information systems. It is the virtual space, where digital information can be exchanged electronically with the help of communication networks. The need and scale of cyberspace is escalating day by day, to improve economic growth, because many tasks such as delivering governance to the people by governments, trade by business organizations, paying bills, playing games, banking transactions and communication between persons, businesses and governments are transformed to online mode. The current situation of pandemic has increased the requirement of digital education, not only delivering lectures, but also conducting workshops, seminars, and conferences online. The significance of collaborations between various medical experts across the globe facilitating sharing the knowledge, expertise and resources is understood. Cyber space has always been a target for digital criminals increasing likelihood of security breaches. These threats come in the form of intrusion, denial of service attacks and virus deployment.

Cyber security refers to a group of activities and measures, intended to protect the 'real geography' of cyber space. The main aim of cyber security is to protect online infrastructure and resources such as devices, software and the information, from all possible threats, attacks, damage and misuse. The next section discusses the types of cyber-attacks. Section III describes the causes of security vulnerabilities. The cyber-attacks severely impact organizations in terms of information loss as well as financial, which will be discussed in section IV. Sections V and VI briefly discuss challenges and protection against cyber-attacks. At last, an interesting case study is discussed, which is a clever application of a popular cyber-attack called Distributed Denial of Service (DDoS), by a warm called Mirai, which took unauthorized control of poorly secured "Internet of Things" (IoT) devices for attacking several high-profile online websites.

II. Types of Cyber Attacks

A cyberattack is an illegal move that targets computer hardware such as personal computers are computer networks, software or data such as information systems and infrastructures [1]. A cyber attacker may be a person or software that tries to access data or functions of the system without authorization with malicious intent [2]. The following are some of the popular cyber-attacks.

- Malware: This is a threat in Microsoft systems. It is a short form for malicious software. Malware is designed to damage a personal computer, network or server having Microsoft software installed in it. Worms, viruses, and trojans are different forms of malware. A worm reproduces itself and spreads from one computer to another. A virus is a code snippet that inserts itself within the code of another program, then enforces that program to do malicious action and spread itself. A trojan cannot reproduce itself but imitates as something the user wants and traps the user to activate it. Then it can damage and spreads.
- Phishing: Phishing is an act of creating fraud emails to users and provoke them to provide sensitive data like bank usernames, One Time Passcodes, credit card details etc.

978-1-6654-1758-7/21/$31.00 ©2021 IEEE

- Denial of service: A DoS attack is a brute-force technique that refuses an online service to users. For example, cyber criminals may send heavy traffic to a website or so many requests to a database which may overwhelm the system's functionality, keeping them busy and unavailable to users. A distributed denial of service (DDoS) attack uses a large number of computers, usually containing a malware which are controlled by cybercriminals, take over the traffic of the targets.
- Cryptojacking: Cryptojacking is an attack that gets access over victim's computer system to generate cryptocurrency. The attackers often install malware in the target's system to get their transactions done.
- Ransomware: Ransomware is a kind of malware that encrypts target system's files. The attacker then demands a ransom from the target to regain access to the data after payment. Victims will be given instructions of payment to get the decryption key. Costs vary from a few hundred to thousands of dollars and are generally demanded to be paid in cryptocurrency to cybercriminals.
- Botnet: A botnet is a network of devices collaborating to achieve a particular task. Botnets are used by cybercriminals to drive many attacks such as DoS. Botnets can steal passwords and other sensitive information and can spread viruses. A malicious bot bypasses organizational security firewall and infects large scale of devices in an organization and controls all of them remotely.
- Man in the middle: A man in the middle attack (MITM) is a way by which cybercriminals intrude between the user and a web service they target. For example, an attacker could configure a Wi-Fi network with a login screen designed to mimic a corporate networ. Once a user logs in, the attacker can access any information they submit, including bank passwords.
- SQL injection: SQL injection is an attack targets ownership on database owned by victim. Many databases operate with Structured Query Language (SQL). In a SQL injection attack, a cybercriminal may write some SQL commands into a web form to acquire personal information of users with a intent. This damages the credibility of the organization that owns the database.

III. Causes of Vulnerabilities

Cybersecurity problems can range from minor issues such as outdated software to large-scale struggles like a lack of support from management teams. Unsecured protocols, password flaws, missing system patches, outdated software and cross-site scripting are the top five most common enterprise vulnerabilities. However, phishing attacks have been identified as the gateway for attackers to infiltrate an organization at a deeper level. The following are a few other issues which make an organization vulnerable [3].

- Small organizations overlook the possibility that they can be targeted for cyber criminals.
- Many in house cyber security professionals are engaged in managing threats, training staff and meeting compliance requirements, but not much on proactively develop future strategies.
- Ignoring email security strategies.
- Not giving importance to data backup plans.
- Not taking bring your own device policies seriously.
- Absence of standardization in devices employed for internet access.
- Lack of national level architecture for Cybersecurity.
- Lack of awareness.

The organizations irrespective of size can be impacted severely by cyber-attacks. Next section discusses the impact of being affected by cyber threats and cost of various cyber security measures.

IV. Costs and Impact of Cyber Security

Cyber-attacks are most impactful global risks that impact businesses, government and other sectors [4]. Cyber criminals do not discriminate based on sixe of company or industry. Their objective is to obtain financial or political advantages from cybercrimes. Cybersecurity aims to protect one's business from threats like ransomware, data breaches, phishing attacks, DNS hijacking, crypto-jacking, insider threats, denial of service attacks etc. The expenses of cyber security fall into two categories: Products and Services.

A. Cyber Security Products

Cybersecurity products may be virtual or physical devices that protect data. The following are some security products:

- Firewalls: A security device that acts as the primary defence to protect network's important assets. It is usually a physical product, but it can also be available virtually. The firewall protects a network by filtering traffic and acting as a safeguard between organization's intra and inter networks. It also functions as a protective layer which can block malicious software.
- Endpoint Detection and Response: These are the tools used for identifying and examining suspicious activities on computers and servers in a business network.
- Antivirus: Manages fundamental cyber threats and watches activity from malicious web sites, documents and software. Often fails to identify advanced threats.
- Email protection: Email is the most general way malware enters organizational network. Email protection services use third party software that filters the emails before they are delivered.
- Two factor-authentication: Is a procedure that uses two credentials to be logged in. Paid two-factor authentication products can be used if an organization wants to monitor admin portals and enforce device trust policies. Table. I gives the costs of these cyber security products.

B. Cyber Security Services

These are the pprofessional services that protect organization from cyber-attacks. These types of services include:

TABLE I
COSTS OF CYBER SECURITY PRODUCTS

Product	Cost(monthly in $)
Firewall	1,500 -15,000 (annual)
Endpoint Detection and Response	5 - 8 per user 9 - 18 per server
Antivirus	3 - 5 per user 5 - 8 per server
Email protection	3 - 6 per user
Two factor authentication	0 - 10 per user

- Vulnerability assessment: This service helps an organization in assessing the mostly exposed areas the most significant risks of cyber-attacks.
- Penetration testing: This service offers a practice of testing a system or website pertaining to organizational network to identify vulnerabilities that a cybercriminal may exploit.
- Compliance auditing: Is the process to ensure the government that a business is following the rules and regulations of a specific agreement.

The report given by World Economic Forum emphasising Global security Risks in the year 2020 ranked cyber-attacks as top 5th most impactful global risk [4], [5]. Cybercrime costs more than $3.5 billion in USA as per 2019 FBI report [6]. Almost all sectors have been affected by cyber-attacks. Finance sector is the most affected, with annual costs crossing $18 million in 2018 [5]. Fig. 1 shows the average cost of cyber-attacks in various sectors.

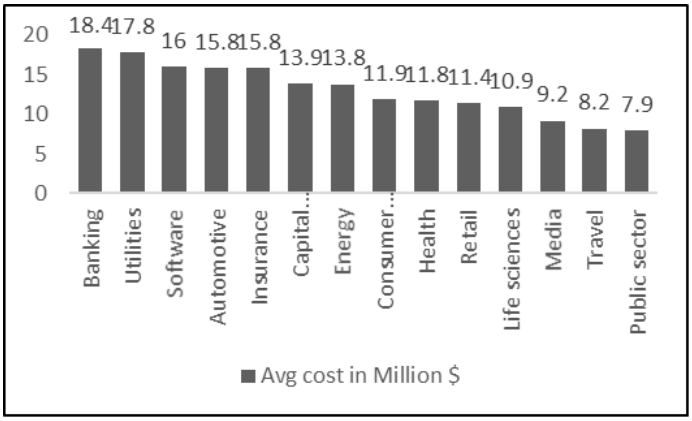

Fig. 1. Average cost of cyberattacks in various sectors.

Romanosky et al analyse around 12000 cybercrimes happened during the years 2004 to 2015, to find costs and composition of these crimes industry wise [7]. The authors consider four types of cybercrimes: data breaches, security incidents, privacy violations, and phishing. The observations of [7] are that data breaches and other cyberattacks have caused enormous losses to firms. Some cases of identity theft that triggers extreme harms to individuals are also reported. Information loss has been major impact of malware, Web-based attacks. Business disruption has been the consequences of Denial-of-Service (DOS) as well as Malicious insiders.

V. CYBER SECURITY DEFENCE STRATEGIES

There are many methods to get protected from cyber-attacks. Following are a few.

- To own a secure hardware which are protected and enabled with 2-way authentication. For instance, if one of the high-level employees' laptop is stolen and reaches to the hands of cyber criminals, then there will be tremendous information loss to the organization.
- Encryption of data wherever needed.
- Backing up important information.
- Training employees on the latest cybercrimes and the ways to protect helps organization to mitigate cyber risks.
- Analysing the sources of cybersecurity threats with the help of in house professional ethical hackers and taking corrective measures wherever security is weak.
- Using anti-malware, anti-virus and firewalls improves protection of organizational networks.
- The router best practices specified below can protect wireless sensor networks:
  - Changing admin passwords for new devices.
  - Setting wireless access point so that it does not broadcast its service set identifier (SSID)
  - Setting router to use Wi-Fi Protected Access 2 (WPA-2), with the Advanced Encryption Standard (AES) for encryption
  - Avoid using WEP (Wired-Equivalent Privacy).

VI. CYBER SECURITY CHALLENGES

Achieving cybersecurity is turning out to be difficult year by year, as cybercriminals discover new attacks, exploit new vulnerabilities constantly over time. Major cyber security challenges are as follows:

- Ransomware: In this kind of attack, a malware penetrates inside our system, it encrypts whole data. Then all the files in the system get locked. The decryption key is sent only after paying a ransom. [8].
- General Data Protection Regulation (GDPR): The GDPR is a document that covers the protection of personal data of EU citizens. Its implementation affects all companies that process data from customers or EU companies or that have an office in one of the EU countries. Many businesses will not try to conform to the regulations because the cost exceeds risks [9].
- Compromised IoT devices: Internet of things is group of digital devices that are connected to a network. This gives a control over majority of the connected devices from a single point of operation, which may lead to leads to increased risk of attacks. Some of the challenges regarding IoT are: Botnets, DDoS Attacks and Ransomware attacks [10].
- Cloud security issues: Cloud platforms store huge volume of sensitive data. Some of the challenges are cloud misconfigurations, spectre and meltdown vulnerabilities, usage of less secure APIs and data loss [11].

- AI and Machine learning enables attacks: Artificial Intelligence and Machine Learning may be used for performing various attacks like sending higher amount of spam messages using chatbots, password guessing [12].
- Blockchain Revolution: Crypto currency technologies are still in budding stage and many companies compromise on security controls. Some of the attacks in this category are Eclipse attack, Sybil attack, and DDoS attack [13].
- Sandbox-evading Malware: Sandboxing is a popular malware detection and prevention method. Cyber criminals find new ways to evade this technology. Core count and Lack of user input are two techniques that attackers use for bypassing sandboxing.

VII. Case Study: MIRAI IOT BOTNET [14]

The Mirai botnet, comprised of embedded and IoT devices, unleashed an internet storm in 2016 when it attacked several high-profile targets with DDoS attacks. A few high-profile victims suffered from attacks by Mirai:

- Krebs on Security : Krebs on Security is a blog maintained by Brian Krebs, who writes investigative articles on cyber-crime. This blog experienced 269 DDOS attacks between July 2012 and September 2016. The attack by Mirai was the largest, topping out at 623 Gbps.
- OVH attack: OVH is one of the largest European hosting providers. OVH hosts around 18 million apps, Wikileaks being one of their most controversial one. The Mirai attack lasted about 7 days and peaked at 1TBs and was done using 145,000 IoT devices.
- DYN attack: This attack targeted systems operated by DNS provider Dyn. This event refused the access to many websites including AirBnB, Amazon, Github, HBO, Netflix, Paypal and Twitter.
- Lonestar Cell, one of the largest Liberian telecom operators started to be targeted by Mirai on October 31. Over the next few months, it suffered 616 attacks, the most of any Mirai victim.
- Deutsche Telekom going dark: One of the largest German Internet provider, Deutsche Telekom has been targeted a vulnerability in a management interface present in routers used by many of its customers, with the intent of infecting the devices to make them part of a Mirai botnet. About 900,000 customers were impacted in the attack.

Mirai is a self-propagating worm, that duplicates itself on vulnerable IoT devices. It is also considered a botnet because the infected devices are controlled via a central set of command and control servers. These servers direct the next device to target, to the infected devices. Mirai has two parts: a replication module and an attack module. Fig. explains the two modules. The operation of Mirai is shown in Fig.2.

The replication module expands the botnet size by enslaving vulnerable IoT devices. It scans the entire internet for viable targets and reports them to the C&C servers to infect them with Mirai botnet. Mirai used a fixed set of 64 default login/password combinations that are generally used by IoT devices to compromise the vulnerable devices. The attack

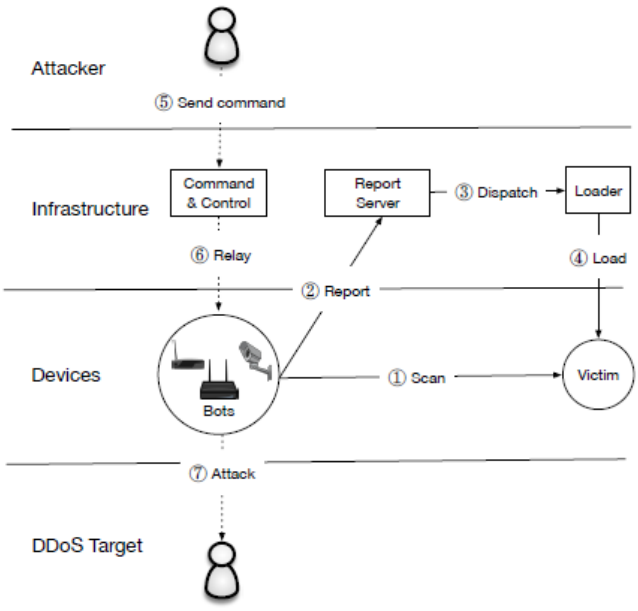

Fig. 2. The operation of Mirai [14]

module carried out DDoS attacks against the targets specified by the C&C servers. This module use DDoS techniques such as HTTP flooding, UDP flooding, and all TCP flooding options. These methods allowed Mirai to perform attacks, application-layer attacks, and TCP state-exhaustion attacks. In November 2016, the author of the Mirai botnet , Daniel Kaye was arrested.

A. Lessons to learn from case study

- Insecure IoT devices are easy targets of DDoS attacks.
- IoT vendors needs to follow security practices such as
  - Eliminate default credentials: This prevents cyber criminals from easy guessing of loin/password combinations to compromise IoT devices.
  - Make auto-patching mandatory: Take patches seriously. Automatic patching is the best option to ensure that no security breach like Deutsche Telekom shuts down a large part of the internet.
  - Enforce rate limiting: Enforcing login rate limiting can be a good option to reduce traffic. Another alternative would be using a captcha.

VIII. Future Research Directions

Security Analytics is one of the promising research directions in this area. There are several datasets extracted from cyber incidents, available online. Extracting hidden patterns or insights from this kind of data will be helpful in understanding and preventing various cyber threats. A plethora of scientific methods including machine learning and deep learning techniques can be used in this context which may supplement intelligent decision making for cybersecurity solutions [15]. Cyber security using Blockchain is another area to focus on. Blockchain is distributed ledger of records, called as

blocks, which are connected using cryptographic functions. Blockchain solutions can be effectively used to solve cyber security problems [13]. IoT devices are being used universally and cyber-attacks on such devices create severe adverse effects to the organizations. IoT security is a serious problem to address.

REFERENCES

[1] "International organization for stan-dardization (iso)." [Online]. Available: standards.iso.org

[2] "What is a cyber attack?" [Online]. Available: https://www.ibm.com/services/business-continuity/cyber-attack

[3] E. P. Dalziell, "Understanding the vulnerability of organisations," 2005.

[4] M. Taddeo, "Is cybersecurity a public good?" *Minds and Machines*, vol. 29, 10 2019.

[5] "Wthe global risks report 2020." [Online]. Available: https://www.weforum.org/reports/the-global-risks-report-2020

[6] T. R. Soomro and M. Hussain, "Social media-related cybercrimes and techniques for their prevention." *Appl. Comput. Syst.*, vol. 24, no. 1, pp. 9–17, 2019.

[7] S. Romanosky, "Examining the costs and causes of cyber incidents," *Journal of Cybersecurity*, vol. 2, no. 2, pp. 121–135, 2016.

[8] R. Richardson and M. M. North, "Ransomware: Evolution, mitigation and prevention," *International Management Review*, vol. 13, no. 1, p. 10, 2017.

[9] P. Voigt and A. Von dem Bussche, "The eu general data protection regulation (gdpr)," *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, vol. 10, p. 3152676, 2017.

[10] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Internet of things (iot): Taxonomy of security attacks," in *2016 3rd International Conference on Electronic Design (ICED)*. IEEE, 2016, pp. 321–326.

[11] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," *Journal of Network and Computer Applications*, vol. 79, pp. 88–115, 2017.

[12] N. Kaloudi and J. Li, "The ai-based cyber threat landscape: A survey," *ACM Computing Surveys (CSUR)*, vol. 53, no. 1, pp. 1–34, 2020.

[13] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo, "A systematic literature review of blockchain cyber security," *Digital Communications and Networks*, vol. 6, no. 2, pp. 147–156, 2020.

[14] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis *et al.*, "Understanding the mirai botnet," in *26th {USENIX} security symposium ({USENIX} Security 17)*, 2017, pp. 1093–1110.

[15] I. H. Sarker, A. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," *Journal of Big data*, vol. 7, no. 1, pp. 1–29, 2020.