A review on Cyber security

Salma Fauzia
Muffakham Jah College of Engineering and Technology,
Osmania University, INDIA.

Abstract. Cyber security is a practice of protecting devices connected to the internet. Security is of great concern of any organization/user and as more and more devices are becoming part of the internet and securing these devices is a challenge. This paper presents a review on cyber security.

Keywords: Security, IoT, attacks

1 Introduction

Ten billion devices are connected to the internet as on 2020 providing communication, ease of access and flexibility to the users but at the same time also raises the concern of security and privacy of data. Cyber security is the practice of protecting critical systems and sensitive information from digital attacks [1]. The attacks can be within an organization or from outside of an organization and cyber security deals with security of the networked devices/ systems. The limitation that gives a chance to the attackers to steal the information is called vulnerability and the information accessed in an unauthorized way is called as data breach.

The Common threats and attacks are

1. Malware: Malicious software that gets installed when a user clicks on a URL or opens a mail from unauthorized sources.
2. Ransomware: This is software that encrypts the data of a person and can be decrypted only in exchange for a ransom.
3. Phising: An attack that is launched through an email, instant message, or text message to steal credentials like credit card

information and banking details. The attacker poses as a trustworthy contact like a bank or other financial institutions.

4. Insider threats: An employee of the institute tries to leak the data intentionally or unintentionally.
5. Man in the middle: The attacker secretly relays the communications between two parties who believe that they are directly communicating with each other.
6. Distributed denial of service: A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic [2].

2. Challenges and strategy

Any device connected to the internet is vulnerable to attacks. Preventing these attacks is a challenge because Internet is a distributed set up connecting huge database across the globe. The attacks can be web based (eg. DNS spoofing, injection attacks) or system attacks (Virus, worm, Trojan). Lack of awareness of users of these devices is a major concern and poses a major challenge. The software is not updated by users as they find it unnecessary. Outdated or pirated version of software provides loopholes to attackers. The older hardware may also not be able to adapt itself to new updates. The security of a user/ organization should be very strong. The major goals of security in the area of networking are confidentiality, integrity and availability.

The various cyber security tools (strategy) that can be used are

I. Firewalls
II. Penetration testing
III. Antivirus software
IV. MDR services
V. PKI services
VI. Staff training etc

Data security can be ensured by having proper backups (Hard drives - personal or work computer, external hard drives, departmental or institution server), archival and suitable data disposable mechanisms (Eliminating the access and destroy the data and the device).

3. Cyber security in Internet of Things -IoT

The Internet of Things- IoT is an extension of the Internet into the physical world for interaction with physical entities from the surroundings [11] . Internet of Things is susceptible to cyber attacks as these networks are unattended by human being, wireless in nature and have less complex hardware which makes implementation of complex security algorithms difficult.

Internet of Things is an emerging field which has given rise to the concept of smart cities. Automatic controlling of traffic lights [3], water supply management [4], automatic vehicle parking, surveillance cameras [5], body area networking in hospitals are a few applications of IoT. A cyber attack on these types of applications is inevitable. In the year 2015, Kyiv (a Ukraine city) had a power outage caused by cyberattacks and this deprived the people of electricity for an hour approximately [6]. Vulnerability may exist in an IoT based system at the devices level, communication medium or at the software and application level. The security guidelines to be considered aree as follows [12]

I. Data should be accountable i.e servers and applications should be automated.
II. Usage of strong passwords, multifactor authentication along with encryption.
III. The organization's security strategy should be built on the assumption of compromise.
IV. Physical accessibility of IoT devices should be taken care of.

The Institute of Electrical and Electronics Engineers (IEEE) and the Internet Engineering Task Force (IETF) are the main bodies that are involved in designing security protocols and guidelines that will play an important role in protecting the global IoT network [7], [8]. Cyber security methods and techniques will ensure that IoT will be a

secure network for users and things connected to Internet. Role-Based Access Control (RBAC) is a method where real-time and dynamic data streams management systems are integrated in IoT to ensure the CIA triad i.e data authenticity, confidentiality, and integrity during transmission [9] [10]. Data encryption plays a major role in providing security to the things connected to IoT. The various areas identified where IoT security needs research is shown below.

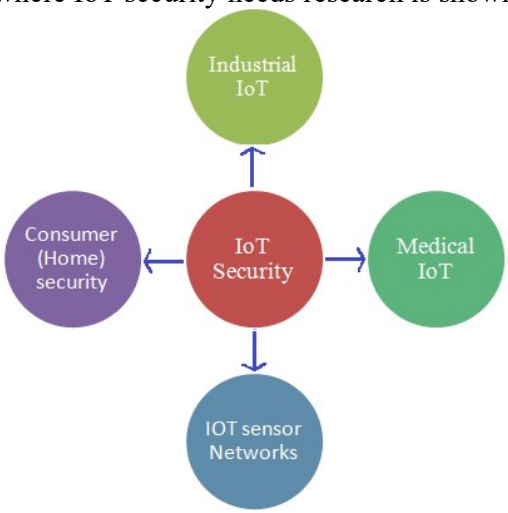

Fig 2: IoT security- Research areas

Iot security can be ensured with the help of security analytics, network segmentation, enabling network segmentation, device authentication etc, also the use of AI and ML can also play a significant role.

3. Opportunities

The different domains in the area of cyber security are

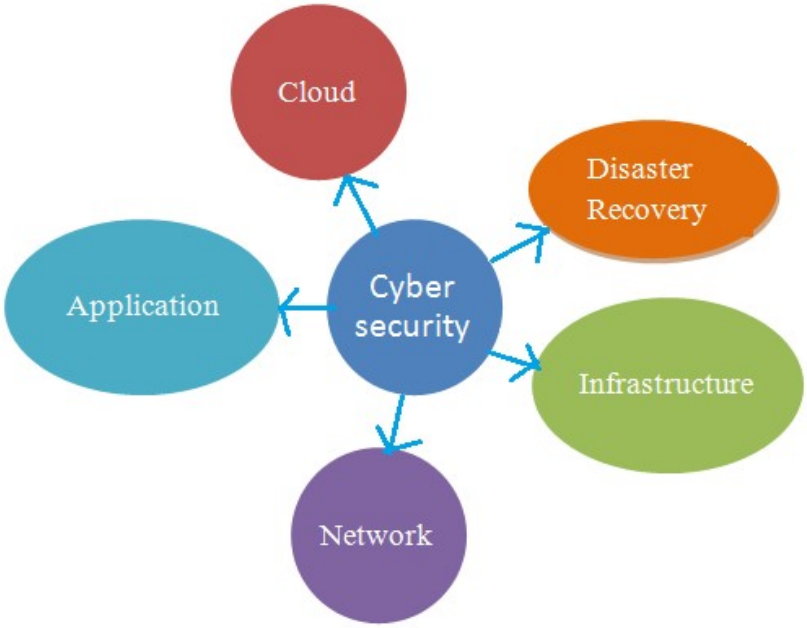

Fig 2: Cyber security- Opportunities

Certifications are available in different subjects ranging from forensic to intrusion to ethical hacking. They are typically administrated by independent accredited organizations such as CompTIA, EC Council, GIAC, ISACA, and (ISC) 2.

4. Conclusion

This paper presented a brief overview of cyber security attacks and its features. IoT security is equally important as it is directly related to smart devices closer to human beings. Risk analysis and testing can be two major factors in defending cyber attacks. Identifying the gaps in security and eliminating the risk to user is a major concern in cyber security. Developing an effective risk management plan and disaster recovery is a very strong impending area of research in the field of cyber security.

References

[1] https://www.ibm.com/topics/cybersecurity

[2] https://www.cloudflare.com/en-in/learning/ddos/what-is-a-ddos-attack/

[3] A Laszka, B. Potteiger, Y. Vorobeychik, S. Amin, and X. Koutsoukos,"Vulnerability of transportation networks to traffic-signal tampering," in Proc. ACM/IEEE 7th Int. Conf. Cyber-Phys. Syst. (ICCPS), Apr. 2016, pp. 1_10.

[4] S. Soltan, M. Yannakakis, and G. Zussman, "REACT to cyber attacks on power grids," IEEE Trans. Netw. Sci. Eng., vol. 6, no. 3, pp. 459_473,Jul. 2019.

[5] R. Taormina, S. Galelli, N. O. Tippenhauer, E. Salomons, and A. Ostfeld, "Characterizing cyber-physical attacks on water distribution systems," J. Water Resour. Planning Manage., vol. 143, no. 5, May 2017, Art. no. 04017009.

[6] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine cyber induced power outage: Analysis and practical mitigation strategies," in Proc. 70th Annu. Conf. Protective Relay Eng. (CPRE), Apr. 2017, pp. 1_8.

[7] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A survey of Existing Protocols and Open Research Issues," IEEE Commun. Survey Tuts. vol. 17, no. 3, pp. 1294–1312, 3rd Quart. 2015.

[8] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of Things," Ad Hoc Netw., vol. 32, pp. 17–31, Sep. 2015.

[9] R. Sandhu, E. J. Coyne, H. L. Feinstein, and C.E. Youman, "Role-based access control models," IEEE Computer, vol. 29, no. 2, pp. 38–47, 1996.

[10] R. V. Nehme, E. A. Rundensteiner, and E. Bertino, "A security punctuation framework for enforcing access control on streaming data," in ICDE, 2008.

[11] Mohamed Abomhara and Geir M. Køien "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks", Journal of cyber security and mobility, vol. 4, no. 1, 2015

[12] https://www.trendmicro.com/vinfo/mx/security/news/internet-of-things/the-iot-attack-surface-threats-and-security-solutions