International Journal of Wireless and Mobile Communication for Industrial Systems
Vol.6, No.1 (2019), pp.21-28
http://dx.doi.org/10.21742/ijwmcis.2019.6.1.03

A Detailed Review on Cyber Security and Its Challenges

N. Thirupathi Rao[1] and Debnath Bhattacharyya[2]

Department of Computer Science and Engineering, Vignan's Institute of Information Technology (A), Visakhapatnam 530049, AP, India
[1]nakkathiru@gmail.com, [2]debnathb@gmail.com

Abstract

The utilization of various electronic gadgets with data usage had increased a lot in recent days. The mostly used devices are like the mobile phones, laptops and other network-based working devices. As these devices are being used, the internet connectivity for these devices are mandatory and the utilization of internet connectivity to all the applications in those devices is becoming a serious problem. As these applications are connected with internet facility always and the data stored in such devices can be accessed easily by using various secret applications or any other patch files. The breaching of data in those devices or applications in those devices had become easier and can be tapped the data without the knowledge of the users of such devices. These applications and things are providing serious challenges to the users for keeping their devices safe and use those devices safe and secure. In the current article, an attempt had been made to provide the various cyber security challenges being faced by users and the latest trends and challenges being generated and faced by the users are given in detail.

Keywords: *Security, Networks, Nodes, Websites, Online banking, Hardware components, Modems*

1. Introduction

Cyber security is one of the major and important that was growing importance from day-to-day. As the technology is growing faster, the utilization of devices and their importance also increased a lot. Almost all the applications which were used in these models will work by utilizing the features of internet. In other words, it can be considered that without using the internet connectivity, these problems or network-based problems may not arise. As the utilization of these devices based on internet connectivity is growing, the people being using such sort of systems are also increasing a lot. As the number of people using these sorts of applications, the customers and the people who were being suffering from such events can be considered seriously and useful for the betterment of the applications and also for the betterment of the public utilization of these sorts of applications [1]. The devices which were used in these sorts of networks can be easily tampered in some cases and in some other cases, these devices can be easily hacked by tampering the electrical signals which were being produced by these devices. Most of these electronic devices are controlled by other types of devices from outside due to the reason that these electrically operated devices can be tapped or the signals can be tapped easily. As a result, the devices can be controlled form other locations or can be controlled by using other devices and also by replacing such devices with other sorts

Article history:
Received (August 15, 2019), Review Result (September 29, 2019), Accepted (November 18, 2019)

Print ISSN: 2205-8443, eISSN: 2207-5399 IJWMCIS

of crimes. As a result, the people can be cheated and the data or the applications can be hacked or misutilized.

Figure 1. A sample model of cyber security [2]

The other side important problems with these cyber-related issues is the online websites or the online purchasing websites and portals for buying goods through online. These sorts of websites are the easy targets for the people to target and can make the cybercrimes and can cheat the people. Nowadays, most of the people are depending on these commercial websites for shopping, purchasing and for other purposes. It is easy to get the data of the people who were using such websites and can be hacked easily. Once a customer was logged in and given his entire credentials and other bank details to the websites, the hackers or the cybercriminals may enter into the website and can access the bank credentials of the customers and can use the details for further shopping. By the time the actual owners or the customers identifies the activity and tries to complain or tries to change the credentials, the money can be hacked or misutilized. These sorts of cybercrimes are common in now a day. The people whoever is using such online portals or the websites for purchasing such items or things from websites and also tries to keep the bank login and other credentials in their own account. In normal cases, the people will be notified, but in some other cases it cannot be noticed also. By the time the customer knows, the crime had already might happened.

One should be very careful when they are creating some account details in a social websites or in commercial websites. The data which we are providing in those websites was one of the major sources for these sorts of people for getting better chances to cheat the public. The data from these websites can be hacked easily and can be used for various other problems. The data can be collected from these websites and misused for all these sorts of cybercrimes. The hardware components of the websites or the software components or the programs and other devices and their constituents can be used by these people by locating at various other locations in the same country or sometimes in some other countries too. By analyzing these sorts of crimes and other issues, the data can be analyzed and always tries to avoid such websites or the addresses which were given by these fake people with fake details. In the following sections, the various types of cyber-attacks that can happen or already happened somewhere and the preventive measures and other applications of these cyber models are discussed in detail.

2. Types of cyber threats

In the current section, some of the common problems that can be observed or noticed in the cybercrimes or some cyber threats are as follows.

2.1. Attack on integrity

This type of crimes or threats will happen to those applications or the problems which could be thought that they cannot be hacked or cannot be traced by the other people. The major happenings in this model are destroying the data, destroying the useful information to the applications. These attacks can happen where there is a trust and belief of the public on some applications and it can be sued for other purposes by the hackers or the criminals to misinterpret the data or misinterpret the common public and hack their personal details, data and some other financial benefits or the financial data.

2.2. Attacks on availability

This is another prone of the important attacks form or the mode of operation. Once the data is available, it can be used by any other people or the people whoever got the access to such data storages etc., when the data is available or stored in a particular place, several softwares are available in the market for the protection of such data. When the data is flooding to the network or to some particular in the network, the data can be protected securely by always sending the data batch by batch with proper utilization of these softwares and other techniques such that the data can be delivered securely at the end users. The data should be sent in such a way that it cannot be accessed by any other persons and even if he got the data, he cannot open it or he cannot understand the data format that we were sending to the end users.

2.3. Attacks on confidentiality

Confidentiality is one of the major issues or the important point to be considered for cyber-attacks or cybercrimes. The copying the others data or collection of data secretly from various other sources is also an important consideration for the common users. The people whoever is working for the same, all these people are ready to grasp the data of others and can misuse them at anytime. This may cause the serious problems to the people who had given or submitted the data for their accounts to get some other benefits from those websites.

2.4. Phishing attacks

In some cases, the best option for these people was to steal the password or to make some trick such that the data of the password or the other details can be tracked. Even in some other cases, the people well trained for such issues or against such issues also will be a prey for those people. Once, if the data related to such issues were hacked, the stealing of the valuable data or the valuable information regarding the person was stolen and it can be misused for various purposes. Most of the cases, the crimes are related with the financial issues. Financial issues that were related to the banks and the customers who were using such websites for the better usage of the websites for their business and also for their item purchasing and also for the better utilization of the resources.

3. Challenges of cyber security

In the recent days, the people who were prone to such threats and such severe issues are increasing day-to-day. As the people are taking special precautions and measures to keep their data or the details secretly or undisclosed to the public, the hackers are doing the reverse process of trying to access such data and they are getting success in some cases and in some other cases, they were failed or unable to break such security systems and cannot access the data. While doing all such security measures and steps for security, some of the serious steps or the precautions to be discussed in detail. Some of the challenges that were being faced by these sorts of problems are discussed in detail in the following sections as follows,

- Application Security
- Network Security
- Data Security
- Database and Infrastructure Security

3.1. Application security

Application security is one of the most important challenges to be done in cyber security related issues. The security features to be added to the application while it was in the phase of developing mode. It was tested at various levels such that these attacks cannot be done to these apps. But the fact is that the attackers always try to identify some bugs in the coding of the applications and can be processed. Lots of tools are available in the internet in order to make changes in the existing data or in various applications.

Figure 2. Application security model example [3]

Some tools are available such that the entire code can be changed for an application and it can be processed at various levels of the coding and at developing phases of the applications. The identification of these sorts of changes or errors to be incorporated into the program might have many issues related to such problems. The less time was taken to identify such issues in those applications, the amount of damage can be reduced to that extent. The steps to be followed

in the application development such that o avoid these sorts of problems are considered as follows. The first point to be considered was the verification of Open Web Application Security Project's (OWASP list) such that to identify the errors or the bugs that can be identified easily [6] It is always better for the developers and other makers of applications to follow these guidelines such that the attacks or the threats can be identified and avoided.

The next step to be followed was the training of the code developers such that they can develop the codes or the program the applications that cannot be opened or hacked by the user sort the hackers without proper login details with that the users can be caught with solid proofs of their thefts or crimes on the machines for the data. The next important step to be followed was to check the coding of the application and its functioning for the quality control of the applications developed before releasing it to the market outside. Also it is required to develop and analyze the applications such that to make the devices to withstand for these sorts of applications.

3.2. Network security

Network security is a combination of various technologies and other devices and their working. In simple words, common rules to be followed or designed to implement and also to protect the network related issues like the confidentiality of the network, accessibility of the network, both hardware and software related issues etc [7]. Every device or the component working or placed in any company or in any organization requires organizing the network models and the functioning of those networks will depends on the success or the failure of such model websites and data in such websites. Several measures to be considered and followed for the better functioning and better working of such models.

Figure 3. Network security model example [3]

The network architecture which was used for now a days is changes from time to time. The attackers always try to identify the network architecture such that to operate and track the details and can hack them. Some of the easy targets of the attackers are like the nodes in the network, modems in the network, number of nodes, number of areas in the network, users data, users location etc. The provision of network security can be imposed or can be worked in the form

of three types. They are physical network security, technical network security and administrative network security.

The physical network security deals with the sorts of issues like the devices which were connected and participating in the network with physical or real-time connections. These types of network models or the issues can be considered little bit serious and can be identified easily due to the malfunctioning or the wrong functioning of the devices used in the network [11]. The technical network security issues deals with the components and the items that were participating in the functioning of the network models and their functioning. The errors that were incorporated in the development of programming of such devices or applications include these sorts of problems. The other model of security was the administrative network security. The issues related to the network models in the level of administrative or administration was done so far.

3.3. Data security

Data security can also be known as computer security or information security. It refers to the provision of security to the various components of a computer or various peripherals of a computer or in some other cases, the peripheral of a laptop and other devices or the electronic gadgets [8][10]. The major concern or the important point to the considered here was the provision of security to the various components of the computers or laptops or other electronic gadgets was to provide security to these devices and also to protect the data which was lying in those devices and also the information that was very much sensible for others and also to restrict the access of unauthorized users to the data and databases.

Figure 4. An example for data analysis or analytics [4]

Some of the technologies being used or to be considered as some of the example technologies that were supporting the functionality or for the better functionality of the resources are like the Data Erase, Data masking and data backups. The process of masking was the major important consideration in the current day technologies. A large volume of data was being transferred from various sources of nodes to the other set of nodes located at various destination nodes. When the data is being transferred, the data needs to be encrypted for the safe transfer of data to the end user. The actual data was being encrypted such that only the source of destination

nodes and the receiver side nodes can receive the data and then after the decryption process will be started and then the actual data will be extracted from the source. The middle users can see the data is being transferred but, they don't know what sort of data is being transferred and how to extract the exact data from the messages being transferring.

3.4. Database and infrastructure security

The other important consideration to be given more importance and more weight during the working of these networks and especially with the security provisions to be considered for the applications in cyber security models or methods [9]. They are the provision of security to the databases and also to the best security to be provided for the infrastructure that had established for the better functioning of the established network structure and models. The provision of security to database was a major consideration due to the reason that almost all the data of the users or the companies or the firms will be stored in the databases and it should be given utmost security. The major concern can be considered is of avoiding the users utilization without proper credentials. The unauthorized access to the users will be brought down by strictly verifying the users credentials and restricting them to access of the databases.

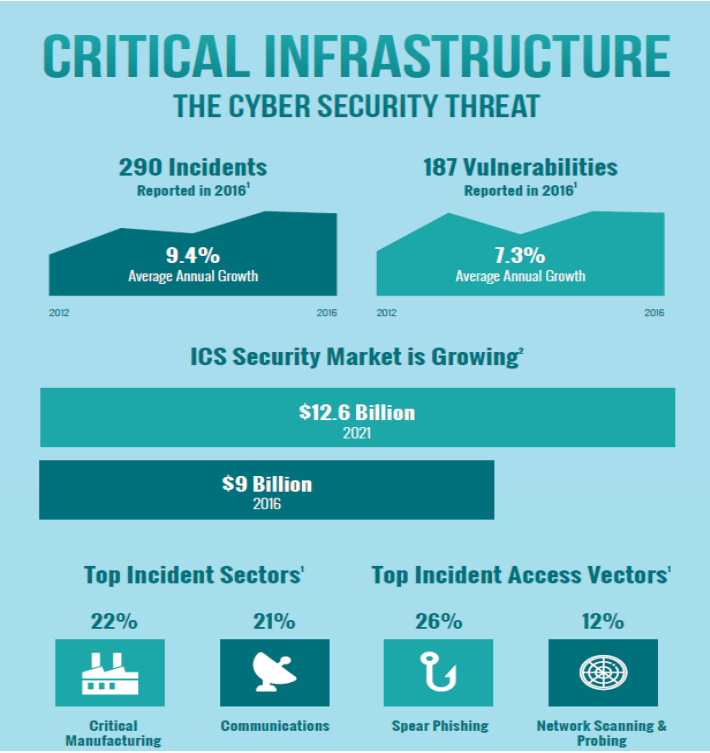

Figure 5. Infrastructure security example [5]

The security to the devices which were providing the facility in infrastructure facility is easily prone of cyber-attacks. The reason is very simple that almost all the devices used in the infrastructure are electronic-based devices. These devices easily prone of attacks or can easily be tampered with wrong data or with confusing data. The data can be processed at various levels of the sections and can be easily tampered at one device. The electromagnetic forces that these devices are facing will create the change in the functioning of these devices and hence

the actual target of these cybercriminals or the attacker's job was done easily by the process of these devices. As a result, the most important data that should not be leaked to anyone will be leaked or can be accessed by many other users and the data was misused by those people.

4. Conclusions

The problems being faced by the normal users and the technical people who were working on the machines, computer and laptops are facing the similar type of problems or threats like the data being stolen or the personal details of the users or the bank details of these users are being stolen. These problems and the people suffering with such problems are increasing a lot. The solutions are very easy to implement. In the current article, an attempt has been made to provide a light on some of the cyber-attacks that may create problems to the common users and the normal users of these computers. Some of the security problems that will create some issues to the users and the steps or the points to be followed or considered for avoiding such issues or to be safe from those sorts of issues are explained in detail in the current article. For providing the basic information about these threats to the normal users, the current article helpful to such users in detail.

References

[1] Thakur, Kutub, Qiu, Meikang, Gai, Keke, and Ali, Md., "An investigation on cyber security threats and security models," IEEE 2nd International Conference on Cyber Security and Cloud Computing (CSCloud 2015), At New York, USA, pp.25-36, **(2015)** DOI:10.1109/CSCloud

[2] MSc Cyber Security, https://www.york.ac.uk/study/postgraduate-taught/courses/msc-cyber-security, **(2019)**

[3] Jeffrey Roman ,"Application security: Four key steps," Bank Info Security, January, **(2015)**

[4] Cyber EDU, "What is network security? Network security defined, explained, and explored," FORCEPOINT, https://www.forcepoint.com/cyber-edu/network-security, **(2019)**

[5] Ravi kandala, "Security analytics-big data use case," Business Analytics, **(2014)**

[6] "Critical infrastructure: Recent cyber security threat incidents," https://www.oilandgasiq.com/events-oil-and-gas-cyber-security/downloads/critical-infrastructure-recent-cyber-security-threat-incidents, **(2019)**

[7] Feba Babu and Kishore Sebastian, "A review on cyber security threats and statistical models", IOP Conf. Series: Materials Science and Engineering, vol.396, pp.1-6, **(2018)** DOI:10.1088/1757-899X/396/1/012029.

[8] Kutub Thakur, Meikang Qiu, Keke Gai, and Md Liakat Ali, "An investigation on cyber security threats and security models," IEEE 2nd International Conference on Cyber Security and Cloud Computing, New York, NY, USA, **(2015)** DOI: 10.1109/CSCloud

[9] Yang Lu, "Cyber security research: A review of current research topics," Journal of Industrial Integration and Management, vol.3, no.4, pp.1-25, **(2018)** DOI: 10.1142/S2424862218500148

[10] N.Thirupathi Rao and Debnath Bhattacharyya, "Review on space and security issues in cloud computing," International Journal of Security and Its Applications, vol.13, no.2, pp.1-8 **(2019)**,

[11] N.Thirupathi Rao, "Security issues and routing challenges on mobile ad-Hoc networks: An extensive review," International Journal of Security and Its Applications, vol.12, no.6, pp.27-36, **(2018)**