IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-6, Issue-8, Aug 2018 E-ISSN: 2347-2693

Mitigating Cyber Attacks Through Security Models and Networking Protocols

Pranav Chaudhary

Information Technology, Maharaja Agrasen, GGSIPU, New Delhi, India

Available online at: www.ijcseonline.org

Accepted: 17/Aug /2018, Published: 31/Aug/2018

***Abstract*—** With the increasing dependency of most of the organizations on technology in today's world, the aspect of information security is a major concern. A plethora of data, be it insignificant (like text messages) or vital (data of some government agency) is stored and transferred over the internet and is exposed to a variety of attacks by people with immoral intentions. Information security is therefore a vital aspect for any organization or government body which has to ensure that their data is not mutated by an attacker and reaches the intended recipient unchanged. This paper discusses various types of security models which are used in practice by the organizations and various cryptographic methods that are commonly used for the protection of data against undesirable breaches. A variety of algorithms have been developed in order to protect the data. Various types of keys which form an essential component of the encrypting algorithms are also discussed. There are several cyber-attacks which pose an austere threat to the organizations. These threats can be mitigated using various cryptographic algorithms and network protocols. These protocols also play an important role in mitigating the security breaches of sensitive data and are discussed towards the end of this paper.

***Keywords*—** Cyber Security, Cyber-attacks, Cypher Text, Cryptography, Phishing, Security Protocol.

I. INTRODUCTION

In the late 20th century, when computers and the internet were royalties of the government and the military, the risk of data breach was almost non-existent as the common people did not have the access to the computer and the internet. As time went on and production of computers became cheaper, they became available for a common man and they were no longer a royalty. This was a revolutionary change but it brought a lot of anomalies with it. The use of computers and internet was not limited to seeking information and knowledge but it expanded and the people with the wrong intentions got to lay their hands on immoral activities. This acted as a threat to the sensitive data over the internet as there were no cryptographic methods to protect data. Even if there were, they weren't strong enough and could easily be breached by potential attackers. This threat was a humungous one and the need to protect data from cyber-attacks came into picture. Many business organizations also began to exchange their data over the internet as it was much cheaper and convenient to send the data over the internet. As the internet consumption grew larger, the need for cyber security and various cryptographic methods arose in order to prevent the data from malicious attacks. Even today, despite of the development of a plethora of algorithms to prevent cyber-attacks, the data on the internet is still vulnerable to such attacks and may even fall in the wrong hands. There are people working to create algorithms which converts the plain text (normal data) into cypher text. A cypher text will not be understandable by someone who does not know the working of the algorithm that was used to convert the plain text into cypher text. The sender and the receiver have a particular "key" which helps the sender to convert the plain text into cypher text and the receiver is able to decipher the text using the key. This type of communication aims to achieve the security of data. The "key" along with an appropriate algorithm achieves the making of cypher text. The following figure represents this conversion process.

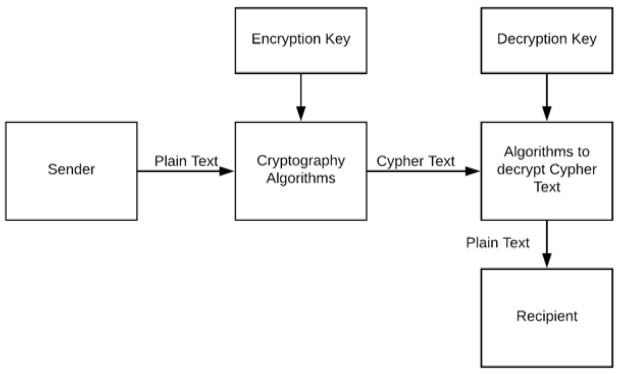

Figure 1: Conversion process of plain text to cypher text

Even though this process of encrypting the text and then decrypting it seems to be protective, a person could decipher the information in the cypher text if he/she gets a hold of the decryption key. Therefore, it is necessary to develop algorithms which are capable of creating keys in a way that their working is not easy to understand. If the attacker gets a hold of the working of the algorithm and understands how the key is used to encrypt data, he/she will get the access to sensitive information encrypted in the cypher text. The data or information that is prone to attacks can be classified in the following three forms. **Data at Rest** refers to the data that is stored on a local computer or a server. This data is generally stored in the hard drives, portable USB drives or in flash memory (SD cards) and can be in the form of pdf files, word files or data stored in folders. **Data in Motion** refers to the data which is being transmitted between the devices. This data could be in the form of text messages being sent over the internet, the credit card details being shared with a website or some data which is being downloaded. **Data in use** is referred to the data which is currently in use by the device. This type of data is stored in the volatile memory (Random Access Memory) of a device for a short period of time. Once the data is processed, it is removed from the RAM. In order to prevent the data attacks, one must ensure proper authentication as well as the authorization. Both of these terms define separate aspects of security. **Authentication** is the process which involves the verification of a user i.e. whether the user actually is who he/she claims to be. The two most common methods of authentication are PIN and passwords. However, certain methods like face detection and fingerprint detection may also be used for authentication. The process of **Authorization** is followed by authentication and it is used to verify the rights that a particular user has i.e. whether the user can only read the information or the user can read as well as modify the information. Authorization provides other rights depending on what permissions the user has been granted by the administration.

II. THE CYBER SECURITY MODELS

The model used in the information security field is the CIA-Confidentiality, Integrity and Availability. This model is [2] a benchmark which is used to evaluate the security of an organization. A more refined version of this model, called the RMIAS, is often used to address the recent security trends. Both the models are discussed below.

The CIA Model

CIA [2] is an acronym for Confidentiality, Integrity and Availability. This model defines the three main aspects which should be considered when designing any application (be it a computer software or a mobile application) to prevent it against the attackers. **Confidentiality** ensures that only the authorized users have access to the information and ensures that the information that is transmitted is not accessible to any of the unauthorized users. **Integrity** ensures the completeness and accuracy of the components. It also ensures that there are no unauthorized modifications to the components. **Availability** ensures that all the components and information is available to the authorized users whenever required.

The RMIAS Model

RMIAS stands for "A reference model of Information Assurance and Security". This model [5] has a broader scope than the CIA model and is based on the IAS- Information Assurance and Security. Information assurance is slightly different than information security. While information security does not put a lot of emphasis on the involved risks and costs, information assurance completely emphasizes on these. The focus of information assurance is to reduce the risks to the information and the information systems. It also focuses on various defensive and cost effective measures that can be put into place in order to minimize the impact of a cyber-attack.

III. CRYPTOGRAPHIC KEYS

Cryptographic keys are [4] are a string of bits that are used by a cryptographic algorithm in order to convert the plain text into cypher text or vice versa. The cryptographic keys may be symmetric or public (asymmetric) depending on how the data is to be encrypted. The use of cryptographic keys along with appropriate algorithms provide the necessary encryption and decryption of data. The two classifications of keys is discussed below.

SYMMETRIC KEYS

As the name suggests, symmetric keys [9] use a single key pattern for encryption as well as the decryption of data. This key is known to the sender as well as the recipient. These types of keys are generally used by government organizations or military. As these organizations prefer their data as well as the encryption techniques to be confidential, symmetric keys fit their needs very well. The algorithm used as well as the cryptographic key is only known within the organization. This classification of keys has several disadvantages. Since the algorithms and keys are only known within the organization (sender and the recipient), specialized engineers who have a lot of knowledge of cryptography and cyber security will not have the access to the symmetric keys and hence these keys would not be worked upon by them in order to make them more secure as per the modern norms. In order to overcome this problem, there is another type of key known as the "Public Key".

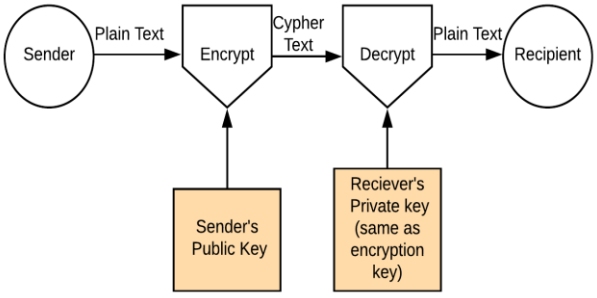

Figure 2: Working of symmetric key

PUBLIC KEYS

These type of keys have separate encryption and decryption keys. The encryption key is "public" and accessible by anyone. This type of keys uses algorithms which are public as well. The public nature of the keys and the algorithms help in their development and security because they are accessible by anyone. The security experts can get their hands on them and work on them to keep them up to date against potential threats posed by many criminal activities. The decryption key in this case does not have a public nature. It is only known by the recipient which ensures that only the recipient has the means to access the data encoded in the cypher text. The working of the public key is represented in the figure below.

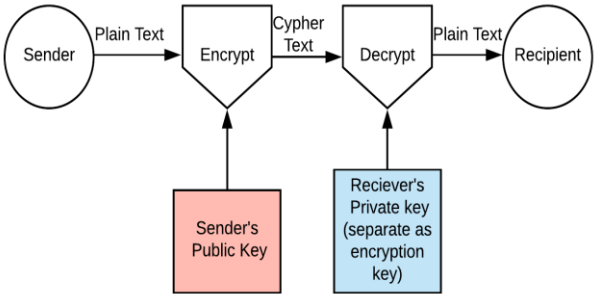

Figure 3: Working of Public Key

IV. CYBER ATTACKS

Depending upon the type of network which is being use, there are a variety of attacking methods used by the cyber attackers. When someone is connected to the network via a wired network, an attacker can gain access to the data being transferred by the user if he/she gets a hold to the server where the data is being transferred or the actual physical media through which the data is being transferred. If the connection is wireless, the attacker may connect to the same network (to which his victim user is connected) and may gain access to the data being transferred. As the transmission media in the case of wireless communication is air, the attacker (by using specific hardware/adopters) may track the signals and extract the sensitive information. This could be extremely dangerous as the data being extracted may contain login details, passwords, bank account numbers and other sensitive data. Various types of attacks are discussed below.

Denial of Service (DoS)

This is one of the most common cyber-attacks. In this, the attacker floods the target user (can be a computer or a server) with requests. This consumes all of the memory resources of the target machine and hence makes it incapable or serving the authorized users with any requests. The DOS attack can be put to a stop by blocking the attacker's IP address. This prevents the machine from taking any requests from this blocked source and hence preventing it from any further requests and makes the resources available again. However, a more severe version of this attack, called the Distributed Denial of Service (DDoS) is used more often than DoS.

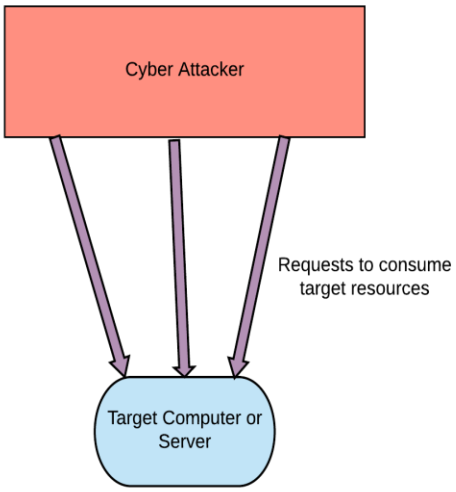

Figure 4: Depiction of a DoS attack

Distributed Denial of Service (DDoS)

The functioning of this attack is very similar to DoS but instead of a single node/source being used to utilize the resources of the victim, this attack makes the use of multiple nodes/sources in order to attack the victim. This type of attack [7] is austere and it becomes difficult for the victim to stop DDoS as the attacker uses multiple sources for the attack, making it almost impossible for the victim to block the requests as the sources from where the requests are coming are in a large number. The attacker uses **botnets** to carry these attacks. Botnets are nodes which have viruses and malwares installed on them. These viruses and malwares contaminate the victim's computer along with using all of its resources. A depiction of the working of these attacks is shown in the figure below.

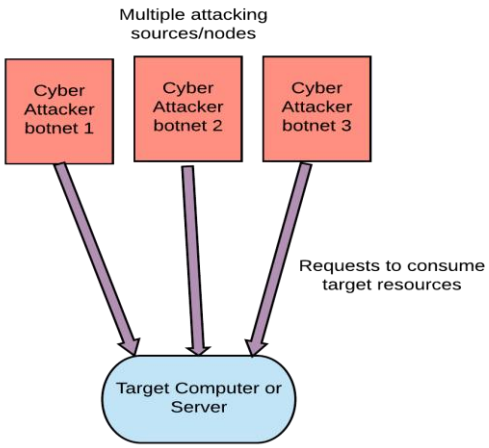

Figure 5: Depiction of DDoS attacks

Phishing

In this type of attack, the attacker [3] hosts a replica of a website (a bank website, a social media replica etc.) and asks the user to fill in their details like passwords, credit card numbers or other credentials. Since the website appears to be legitimate, the user provides the details asked by the attacker and hence gains sensitive data. This is a very common type of attack and is not just carried out on big organizations, but also normal users who have a bank account in a particular bank or a social media account on a social networking website.

The SQL Injection

SQL is a programming language which is used to perform various operations on the data stored in the database. IN SQL injection, the attacker [8] writes a malicious code in the SQL language and tries to run this code onto the target machine. This malicious code may allow the attacker to read, write or edit the sensitive data stored on the database. This may cause a permanent damage to the important information and hence is one of the most severe cyber-attacks.

V. SECURITY PROTOCOLS

A security protocol is a protocol which ensures that the data or the information being carried over the network transmits without any anomalies or any modifications from unauthorized resources. A security protocol can be defined as a set of rules that govern the secure transmission of the sensitive data. There are different types of protocols classified for various types of networks (wired or wireless). Keeping in mind the attacks discussed above, it is very important for these protocols to be implemented as any sort of vulnerability or loophole could allow the attacker to gain access to the sensitive data. Some of the network protocols, both for wireless (Wi-Fi based) and cellular modes of transfer are discussed below.

A. Wireless Data Communication Protocols

The WEP Protocol

WEP is an acronym for Wired Equivalent Privacy. This protocol [6] is used for the protection of data which is transmitted wirelessly. This protocol aims to achieve the same level of security for the data transferred wirelessly as the data transmitted using a wired media. Compared to the wired media which has physical protection of data (data transmitted through cables in enclosed buildings of an organization), the wireless data is in the form of radio waves. This data can be obtained by an attacker if he/she is equipped with a proper hardware (which allows to extract the data from these waves). WEP aims to achieve the same level of protection for data transferred wirelessly as the data transferred via a physical medium. It does so by encrypting the data at the sender's end and decrypting it at the designated receiver. There are several flaws with the existing model of the WEP protocol. The WEP protocol uses a shared key i.e. it sends over the same key along with all the packets across the network. If enough information is gathered by the attacker about this key, he/she can get access to the encrypted data within minutes. The WEP protocol has been replaced by safer protocols (WPA and WPA2) which are discussed below.

The WPA and WPA2 Protocol

WPA is an acronym for Wi-Fi protected access and was introduced to overcome the loopholes and problems with the WEP protocol. Just like WEP, WPA also uses encryption in order to protect the data which is being transferred wirelessly but unlike the WEP, it uses an encryption key which dynamically changes as the data is transferred over the network. This prevents the attackers from developing a key as the key changes itself and hence does not have the same structure at any point of time. The WPA is superior to the WEP but it's successor, the WPA2 is more secure, reliable and up to date with the industry standards.

The WPA2 [6] makes the use of stronger encryption methods for the data which is transferred over the network. The algorithm used by the WPA, the temporal key integration protocol (TKIP) has a few limitations and security loopholes. WPA2 does not make the use of this algorithm. It uses the AES algorithm, which is more secure and provides a stronger encryption of data as compared to the algorithm used by WPA.

B. Cellular Data Communication Protocols

The UMTS Network Protocol

UMTS network protocol ensures mutual authentication between the network and the user. This allows the device to determine whether the network it is connecting to is legitimate or not. This protocol also ensures the data integrity i.e. ensures that the data being received is complete and is

not modified or altered in any way. Integrity and Encryption are well assured by this protocol.

Long Term Evolution Network Protocol (LTE)

LTE (4^{th} generation) network is the most advanced cellular network being used today. It has most of the security features provided by the 2^{nd} and the 3^{rd} generation of networks. In addition to maintaining the integrity as well as ensuring proper encryption of the data, LTE keeps the sensitive information away from malicious attackers by narrowly defining the transfer of signals. The LTE network is being continuously worked upon to make it more secure as it is being used by most of the cellular devices across the world.

VI. CONCLUSION

Security plays a very important role in any organization, be it a million dollar one or a small company which has just started off. Security aspects of a product are often undermined by the organizations in order to provide quick delivery of a product or a software due to the competition with rival companies. This compromise may buy them some time to incorporate more features but may make the product prone to cyber-attacks which is bad for the reputation of the company. Therefore, security aspects of a product should never be taken for granted. A customer will certainly be satisfied with a feature loaded product but if the customer feels that his/her data is at risk, he/she may never use that organization's product again. There are various security models and security protocols which have become industry standards. Technology is evolving every single day and cyber security experts are coming with better solutions for the protection of sensitive data. But with this advancement of technology, the cyber attackers are coming up with better tools to attack the sensitive data too. We probably would never be able to eliminate the cyber threats completely but with the right approach, the cyber security experts will certainly explore ways to mitigate them.

REFERENCES

[1] Singh Anurag, Singh Brijmohan, "Cyber Security Policies for Digital India: Challenges & Opportunities", International Journal of Computer Sciences and Engineering, Vol.5, Issue.12, pp.164-168, 2017.

[2] Steve G. Walkins, "An Introduction to Information Security and ISO27001:2013: A Pocket Guide", IT Governance Publishing, pp. 21-42, 2013.

[3] Suganya V,"A Review on Phishing Attacks and Various Anti Phishing Techniques." International Journal of Computer Applications 139.1 (2016): 20-23.

[4] Amalraj, A. Joseph, and J. John Raybin Jose. "A survey paper on cryptography techniques." International Journal of Computer Science and Mobile Computing 5.8 (2016): 55-59.

[5] Cherdantseva, Yulia, and Jeremy Hilton. "A reference model of information assurance & security." 2013 International Conference on Availability, Reliability and Security. IEEE, 2013.

[6] Vipin Poddar, Hitesh Choudhary. "A Comparitive Analysis of Wireless Security Protocols (WEP and WPA2)", International Journal of AdHoc Networking Systems, Vol. 4, No. 3, July 2014.

[7] Mahjabin, Tasnuva, Yang Xiao, Guang Sun, and Wangdong Jiang. "A survey of distributed denial-of-service attack, prevention, and mitigation techniques." International Journal of Distributed Sensor Networks 13, no. 12, 2017.

[8] Mishra, Neha, and Sunita Gond. "Defenses to protect against SQL injection attacks." International Journal of Advanced Research in Computer and Communication Engineering 2.10 (2013).

[9] Ayushi. "A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications, Volume 1 – No. 15, 2010.

[10] Sanjay E. Pate, Bhojaraj H. Barhate, "*A survey of Possible Attacks on Text & Graphical Password Authentication Techniques*", International Journal of Scientific Research in Computer Science and Engineering, Vol.06, Issue.01, pp.77-80, 2018

[11] B. Bhasker, T. Jagadish kumar, M.V.Kamal, "*A Security Determination-Reaction Architecture for Heterogeneous Distributed Network*", International Journal of Scientific Research in Computer Science and Engineering, Vol.5, Issue.5, pp.26-34, 2017

[12] Poonam Devi , "*Attacks on Cloud Data: A Big Security Issue*", International Journal of Scientific Research in Network Security and Communication, Vol.6, Issue.2, pp.15-18, 2018

[13] Shailja Sharma, "*A Review of Vulnerabilities and Attacks in Mobile Ad-Hoc Network*", International Journal of Scientific Research in Network Security and Communication, Vol.6, Issue.2, pp.66-69, 2018

Authors Profile

Mr. Pranav Chaudhary is currently pursuing Bachelor of Information Technology from Maharaja Agrasen Institute of Technology, India. He has published several technical papers in reputed international journals. His main research work focuses on Cyber Security, Augmented Reality, Cloud Computing and Computer Networking.

