THE ERA OF NETWORK SECURITY

Namratha J[1], M Likhith Varma[2]

[1,2] *IV sem CSE, RNS Institute of Technology*

[1]1rn19cs084.namrathaj@gmail.com, [2]1rn19cs083.mlikhithvarma@gmail.com

***Abstract*- The main aim of network security is to protect the applicability and integrity of data. These technologies include both hardware and software. It tackles a variety of threats. It is important to protect our devices from the attackers. Some of the crucial elements to be understood by the user include need for network security and CIA model which are briefly stated in this paper, followed by the types of security models offered. Network security attacks which include active and passive attacks and their further divisions are also explained. These attacks can be prevented by different types of network security methods offered.**

Keywords: Network security, CIA model, active and passive attacks, network security models

1. INTRODUCTION

Though plenty of measures are carried out to ensure that our network is secure, the threats never cease to exist. The significance of network security increases as information becomes more and more sensitive. Both individual computer systems and the Internet have been targeted on a day to day basis by cyber attackers. Due to the ubiquity of the Internet, network security plays a significant role and it can be defined as a policy related to the networks to ensure the safety of significant information, hardware and software resources. It not only monitors but also checks for illicit access, exploitation and undesired modifications in the networking system. Paradigm of security varies as time passes and most of the security solutions are driven by different solutions based on the user requirements. Security of information can be ensured by the CIA model: confidentiality, integrity and availability here the information is secured from hackers, protected from unwanted changes which are not initiated by the administrator and it is made available to the people approved by the administrator. Thus, the CIA model is the most important goal which is further discussed in this paper.

2. NEED FOR NETWORK SECURITY

With the rapid development in the era of the internet, network security should pay more attention in order to control unauthorized access and modifications in the network since the client's information security is extremely vital [1]. It covers a variety of computer networks, both public and private, that are used in conducting transactions and communications among businesses, government agencies and individuals [6]. Nonetheless, the internet has been implemented in our daily lives as we are in the era of digitalization. This has caused the hackers to become increasingly active and the networking systems are targeted by multiple virus attacks. Further, motives of such attackers may be either to have fun or to sabotage critical information of organizations [3]. In order to avoid this, the usual authentication process carried out is to allocate an unique ID and user password for authentication. Different security mechanisms find its application to enhance the security properties defined in a given security policy [5]. Abundant research is being performed in the network security domain to ensure that the data is secured.

3. PRINCIPLES OF SECURITY—The CIA Model

A highly used model of security is called the CIA Triad. The three principles it follows are confidentiality, integrity, and availability. The CIA Triad is applicable to the entire spectrum of security systems. Any loopholes among these principles will show dangerous consequences.

Confidentiality:

It stops unauthorized access of secret data which may be a company's confidential data. Confidentiality is the feature of security most often attacked. Examples to keep data transferred from one computer to another confidential are cryptography and encryption methods. Cryptography protects the sensitive data transmitting across the air. An attacker can hijack the packets transmitted in the air. He can find beneficial data [2]. Normally, the data that is encrypted is not understandable anymore until it is decrypted. Thus, encryption of the data can help protect the collected data from leaking even when they are attacked [4].

Integrity:

Integrity prevents unauthorized editing of data, thereby assuring the accuracy of the information. Man-in-the-middle is a very common security attack, where an intruder intercepts data in transfer and modifies it before it reaches the receiver. This causes several problems. The unintelligible packets will be dropped at the receiver, leading to a simple

Denial of Service (DoS) attack. If the attacker understands the packet format and the semantic meaning of the communication protocol serious damages can be done. The attacker changes the content so that the receiver obtains the wrong information [2]. MD5 or SHA are the cryptographic techniques to ensure that the lost data can be recovered immediately [4].

Availability:

Availability is the prevention of loss of access to the information. It is crucial that the information requested is available to the authorized users at any time. DoS is one of the many attacks that attempts to stop access to the user.

4. SECURITY MODELS

A crucial element in the design of security systems is the security model. It integrates the security policy that is enforced in the system. The security paradigm is a symbolic depiction of security policy. It summarizes the policy maker's requirements in a set of rules that a network system must follow.

There are three main types of Classic Security Models:

- Bell-LaPadula (BLM)
- BIBA model
- Clarke-Wilson Security Model

The BLM model, which is a multi-tiered model, was mainly introduced to protect the confidentiality of information in government and military applications. It has three basic rules: the simple company base, the star secret base, and the powerful star secret base.

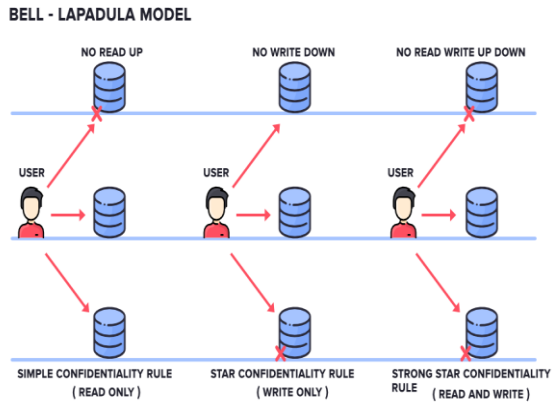

Fig.1 Diagrammatic representation of BLM Model (Courtesy: google)

The Biba model was invented by the scientist Kenneth J. Biba. It is the modification of the Bell-LaPadula model that gives importance to the integrity of the information within the system. Here, classification, users, and files are organized in an inseparable manner based on layers of secrecy. It has three rules: the simple rule of integrity, the rule of stellar integrity, and the rule of strong star safety.

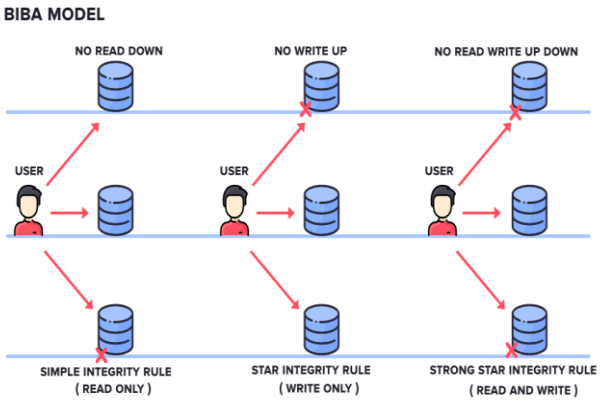

Fig.2 Diagrammatic representation of BIBA Model (Courtesy: google)

Clark-Wilson's model disables users from making unauthorized edits to data. This model introduces a three-dimensional system: a subject, a program, and an object. This model is highly secure. The components of the model are the transformation process and the integrity checking process.

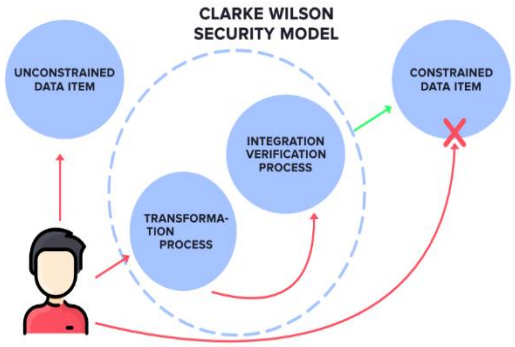

Fig.3 Diagrammatic representation of Clark-Wilson Model (Courtesy: google)

5. TYPES OF NETWORK SECURITY ATTACKS

Network threats are harmful, unlawful activities that take advantage of network susceptibility. Attackers aim at breaching, harming, sabotaging or gaining unauthorized access to confidential data in order to tailor to their needs. Types of attacks include active and passive attacks.

Passive attackers monitor sensitive data. However it doesn't affect system resources and the data remains unchanged. Some of the passive threats include releasing Message content (the hacker views the sensitive information received by the receiver) and Traffic analysis (Patter of the message is cracked by the hacker by the observation of network traffic). To protect the network from passive attacks, encryption keys can

be used to scramble messages or to convert them into unreadable format for any unauthorized recipients.

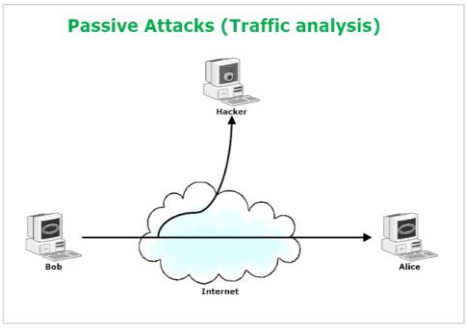

Fig.4 Demonstration of passive attack (Courtesy: google)

Active attackers aim at destroying the network as a whole and the systems linked with it. The information obtained during passive attacks is used during active attacks. These threats include Masquerade (pretending to be someone else), Replay (The hackers re-use the data repeatedly which was obtained previously for their own benefit), Modification of message content (change of address of the packet header to direct it to an unpurposeful destination or changing user data) and Denial of Service (overload server by giving false requests).

Though the users might know more about active attacks than passive attacks, it is difficult to find out the main reason behind it with improper monitoring and unprotected machine and human identities.

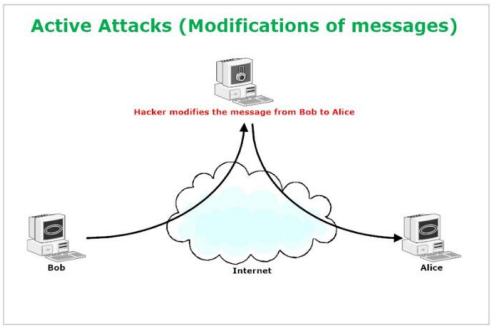

Fig. 5 Demonstration of active attack (Courtesy: google)

6. NETWORK SECURITY

Network security can be defined as layered defenses offered. Unlawful access, abuse or undesired changes to the network are monitored and controlled. Networks are accessed by authorized users, while malicious attackers are blocked. The world has currently been remodeled by digitalization, which has a greater influence on our day to day activities. Organizations have to implement network security to protect the network which is used to offer different services to employees and customers. Ultimately, the organization's reputation is held high.

Different Network Security services offered are Antivirus and Anti-malware Software, Application Security, Behavioral Analytics, Data Loss Prevention (DLP), Email Security, Firewalls, Mobile Device Security, Network Segmentation, Security Information and Event Management (SIEM), Virtual Private Network (VPN), Web Security, Wireless Security, Endpoint Security and Network Access Control (NAC).

They are explained below:

Anti-virus and anti-malware program: the protection software used to protect our system from viruses, trojan horse attacks, worms, etc. is an anti-virus and anti-malware program. This program scans the system and the network for malware and Trojan horse attacks every time a new file is inserted into the system. It also detects and fixes the problem, if it is found with any infected data or virus.

Application Security: All built applications are imperfect in one or the other way. Any application could have exploits or weaknesses that attackers could use to access the network. Hence, application security helps fill these gaps.

Behavioral Analytics: Abnormal behavior of the network can be discovered if the normal condition is known. Behavioral analytics tools can naturally differentiate abnormal activities from the normal activities. Thus, the security team can now efficiently detect the settlement indicators that can be dangerous and address the threats quickly.

DLP (Prevention of data loss): The employees must ensure not to send confidential data off the network. Consequently, DLP technologies and measures must be used so that no one other than the authorized people can download, forward, or print sensitive data.

Email Security: Virus or malware can be introduced by the attackers into the network through email. Hence, a proficient email security application is needed which scans the incoming messages for viruses and is able to filter skeptical information and control message flow to inhibit any kind of information loss to the system.

Firewalls: They act as a wall between two networks or between two devices. Basically, it is a

predefined set of guidelines that are used to protect the network from any unauthorized access. Firewalls are of two types, i.e. hardware and software. A program firewall is installed in systems to provide shields from various types of attacks as it filters, blocks, and fixes unwanted objects in the network. A hardware firewall acts as a gateway between two network systems so that only a user or predefined traffic can access the network and its resources.

Mobile Device Security: Cyber criminals can easily hack or attack cell phones using the data facility on phones, and they can access the device from any insecure resource link from the website. Hence, it is necessary to install an antivirus program on our machines and people should download or upload data from trusted sources and that also only from secure websites.

Segmentation of the network: From a security viewpoint, the software-based organization will divide its critical data into two to three fragments and store it in different places and over many devices. In the worst case, if data is corrupted or deleted due to a virus, the sources which were stored as a backup can now be used to rebuild the data.

SIEM(Information regarding system and event management): Products of SIEM which are available in virtual hardware, physical and server software forms, collect all the information required by the security team to detect and respond to threats.

VPN: Virtual Private Network efficiently encrypts the information during communication between an endpoint and a network over the Internet. Remote access VPNs generally use IPsec or SSL for authenticating the network and device connection.

Web Security: The ultimate web security solution helps the organisation to control employees' web usage, block the malignant websites.

Wireless Security: Wireless networks are not as secure as wired networks. It creates room for the attacker's entry. So it is imperative that wireless security is strengthened.

Endpoint Security: It is used to protect business networks when they are accessed on remote devices which includes laptops or any wireless devices. For example, seven layered defense offered by Comodo Advanced Endpoint Protection.

Network Access Control (NAC): It helps the users to control network access features. The users must be familiarized with all the devices and users related to their network to identify and protect from the attackers. Incompatible endpoint devices can only be granted restricted access or be blocked.

Technical network protection: It protects the data within the network. It protects stored and transmitted data from malware and unauthorized entities.

Physical Network Protection: This is designed to prevent unauthorized people from interfering manually with network components. Unique IDs are provided to ensure that the network components are protected.

Administrative Network Protection: Behavior of the user over the network is controlled via administrative network protection. A standard procedure for operation is provided to the IT officers which has to be used to perform some variations in the infrastructure.

7. CONCLUSION

Cyber security is crucial in the era of network security. Protecting our devices from these attacks are of great significance. Need for network security and the principles of security (CIA model) are crucial elements to be understood by the user. These are explained in this paper followed by the types of security models offered. Network systems are exposed to diverse attacks. These can be categorized as either passive or active attacks. This is further explained in the paper followed by the different types of network security methods offered.

REFERENCES

[1] Dr. Sandeep Tayal, Dr. Nipin Gupta, Dr. Pankaj Gupta, Deepak Goyal, Monika Goyal: A Review paper on Network Security and Cryptography, Advances in Computational Sciences and Technology ISSN 0973-6107 Volume 10, Number 5 (2017) pp. 763-770.Mohsin Nazir. Cloud Computing: Overview & Current Research Challenges. ISSN: 2278-0661, ISBN: 22788727Volume 8, Issue 1 (Nov. - Dec. 2012), PP 14-22.

[2] Shio Kumar Singh, M P Singh and D K Singh: A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks, International Journal of Computer Trends and Technology- May to June Issue 2011.Storage Networking Industry Association.Cloud Storage Reference Model,Jun.2009.

[3] Pranesh V. Kallapur and V. Geetha: Web Security: A Survey of Latest Trends in Security Attacks, Y. Wu (Ed.): Advances in Computer, Communication, Control &

Automation, LNEE 121, pp. 405–415. springerlink.com © Springer-Verlag Berlin Heidelberg 2011.

[4] Huaqing Lin, Zheng Yan, Yu Chen, and Lifang Zhang: A Survey on Network Security-Related Data Collection Technologies, VOLUME XX, 2017, 2169-3536 © 2017 IEEE.

[5] Christopher Kruegel, University of California: "Network Security and Secure Applications" ,0-8493-1985-4/05/$0.00+$1.50 © 2005 by CRC Press LLC pg 34 to 49 .

[6] Shyam Nandan Kumar: Review on Network Security and Cryptography, International Transaction of Electrical and Computer Engineers System, 2015, Vol. 3, No. 1, 1-11

.