Volume: 08, Issue: 05 Pages: 120-123 (2017) Special Issue

Network Security, A Challenge

Jenani. M,
Department of Computer Science, Government Arts College For Women, Ramanathapuram.
Email: rnd.jenani@gmail.com

ABSTRACT

The Internet is growing with a tremendous speed so as to keep the security of the network is an important aspect. This paper outlines that the basic ideas of network security requirements and the overview of the vulnerabilities of the network. Network security consists of the policies and practices adopted to prevent and monitor the unauthorized access, misuse, alteration, or denial of service. Security management for networks is different for all kinds of situations and there are may be a lots of security attacks to breach the security. Network Security can be referred as protecting websites domains from various forms of attack. If we have the knowledge of how various attacks are executed we can protect ourselves from the violations. For these reasons, Network security is more challenging than ever, as today's corporate networks become increasingly both fascinate and complex.

Keywords: **Availability, Authenticity, Confidentiality, Denial of Service, Integrity, Network Security.**

1. INTRODUCTION

Security means considering vulnerabilities, threats, attacks, countermeasures, and acceptable risks. Security is a broad topic and covers a multitude of sins. In its simplest form, it is ensured unauthorized people cannot read or modify messages intended for other authorized recipients. Most security problems are intentionally caused by malicious people trying to gain some benefit, get attention, or to harm someone.

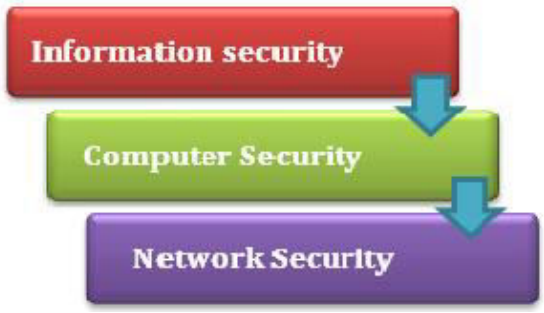

Figure 1: Introduction of Network Security

Information is an asset of any individuals or organization so the requirement of information security shortened 'infosec' plays an important role which is the process of protecting information from unauthorized parties. The broad use of computers leads to computer security which is the protection of computer system from theft or damage to the hardware, software and the data of them. In the advent of distributed systems, Network security becoming more complex. It refers a specialized field in computer networking infrastructure. Network security typically handled by a network administrator who implements the security of network software and hardware needed to protect a network and the resources accessed through the network.

2. REQUIREMENTS OF THE NETWORK SECURITY

Network security is the process through which we can protect the digital information within the system and also during the transmission.

Figure 2: CIA Traid

The objective of network security is to ensure "Confidentiality-Integrity-Availability" traid.

2.1. CONFIDENTIALITY

The information must be accessed only by the authorized individuals or parties. It is related to data privacy means that an individual controls the information which are related to them are collected and stored. Data encryption, User Ids and passwords, biometric verifications are some of the methods used to achieve confidentiality.

2.2. INTEGRITY

The information must be modified only by the authorized individuals or parties. It means that only authorized user can have the rights for modification. It has two levels:

2.2.1. DATA INTEGRITY: Assurance for data is changed only by the authorized user.

2.2.2. SYSTEM INTEGRITY: Assurance that system performs it function consistently without any damage. Hashing the data you receive and comparing it with the hash of original message is another method to ensure data integrity.

2.3. AVAILABILITY
Data must be accessible and available to the authorized persons at all the time. Assures that the system works punctual manner and the service is not denied to authorized users.
It can be ensured by rigorously maintaining all hardware, preparing hardware repairs immediately and maintaining a correctly functioning operating system environment.

3. LOSS OF SECURITY

Federal Information Processing Standards (FIPS) 199 provides the definition and loss of security in each constraint.

3.1. INTERCEPTION
The loss of confidentiality is known as "Interception" which is the unauthorized disclosure of information.

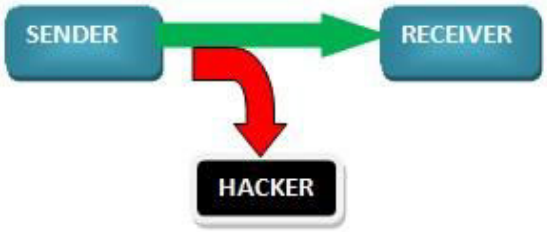

Figure 2: Interception

3.2. MODIFICATION
The loss of integrity is called as "Modification" means that intruders changed the information, after the sender sends it and before it reaches to the intended recipient.

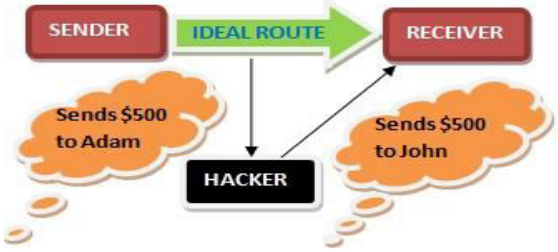

Figure 3: Modification

3.3. INTERRUPTION
The loss of availability is named as "Interruption" which is the disruption of information leads to DoS (Denial of Service).

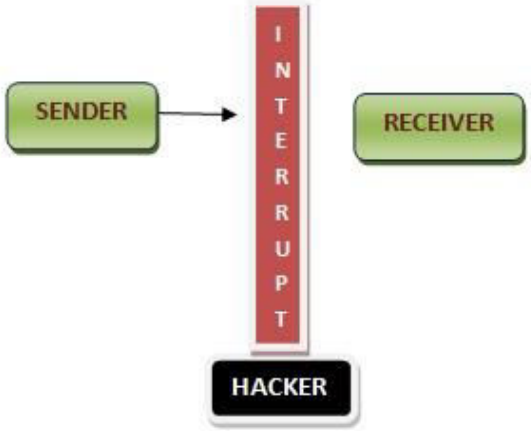

Figure 4: Interruption

3.4. FABRICATION
Authenticity is a mechanism used to verify whether the user is authorized or not. It checks the validity of the user, transmission and the information. In other words, it is the mechanism to establish the proof of identities. The loss of authenticity is entitled as "Fabrication" means that an intruder can act as an authorized user and get the access the information.

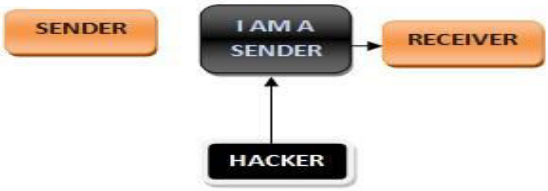

Figure 5: Fabrication

4. SECURITY ATTACKS

All networks contain many vulnerabilities, it is the responsibility of the network administrator to keep the network secure from malicious software, threats and attacks. A threat is a possible danger that might exploit vulnerability. It may exist when there is a circumstance, action or event that could breach security and cause them. An attack is an intelligent threat that deliberately attempt to violate security policies and services. The classification of various attacks is as follows:

Figure 6: Categories of Security attacks

4.1. GENERAL VIEW ATTACKS:
In this point of view, attacks are divided into four categories:

4.1.1. CRIMINAL ATTACKS: It is done for illegally get financial gain from society. It may denote by various ways:
Fraud: Attacks through credit cards, debit cards, ATM and electronic money etc.
Scam: Attacks had done by tempting people to send money in return of great profits but finally leads to losing their money.
Destruction: Attacks done for some other motives.
Identity Theft: Attacker doesn't steal money from the user rather they acts as a legitimate user. It also leads to Brand theft which is to setup a fake product that look like a real one.
Intellectual Property Theft: Stealing company's trade secrets, databases, auction's quotes, software and electronic documents.

4.1.2. PUBLICITY ATTACKS: This type of attacks done for publicity only and not for other aspects. The attackers want to see their name and photo on social media's and get publicity. They are not criminals and may be students of universities and employee of popular organizations**.** They give free solutions to their attacks.

4.1.3. LEGAL ATTACKS: This is unique attack that it aims to exploit the weakness of the technology. The attacker tries to make the tester doubtful about the security of the system.

4.1.4. ACCIDENTAL ATTACKS: It has no intention that the legitimate user unknowingly or accidently choose some options that may cause some undesirable things.

4.2. TECHNICAL VIEW ATTACKS:
From the technical point of view, attacks are classified into two categories:

Figure 7: Types of Technical view attacks

4.2.1. PASSIVE ATTACKS:
This type of attacks attempt to learn or make the use of confidential information but does not affect the system resource. It does not involve any modifications, these are hard to detect so it may want to prevent it. The attacker monitors for the open ports or vulnerabilities to gain the information about the target without changing it on the target machine. Passive attacks are only affect confidentiality. There are two main types of passive attacks:

4.2.1.1. RELEASE OF MESSAGE CONTENTS: In this type of attack, it monitors the content of transmission either it is a telephonic conversation, an e-mail or a transferred file that contains the confidential information. Attacker may take the copy of the information.

4.2.1.2. TRAFFIC ANALYSIS: This method also attack the confidentiality but it is little complicated than previous one. That is, using encryption we can able to eliminate the Release of Message Contents but in this traffic analysis, attacker may observe the pattern of encryption also. It is very subtle and hard to detect if we had a way to hide the information on a message and the hacker still viewed the hided information.

4.2.2. ACTIVE ATTACKS:
Active attacks attempt to obtain, alter the information and affect the system resources and operations. It tries to change the original message and intentionally create fake or fault messages. Comparing to passive attacks, active attacks are quite easy to detect but recovery is very difficult. This type of attacks affects not only the confidentiality but also the integrity, availability and authenticity. The active attacks are subdivided into different categories:

4.2.2.1. MASQUERADE ATTACKS: The intruder pretends to be a legitimate user of the network system so that he/she can gain the access or some privileges that the user is authorized for. This attack is attempted through the use of stolen login Ids and passwords.

4.2.2.2. REPLAY ATTACK: The hacker can capture the original message and make some modifications and then retransmit it to the receiver repeatedly to cause unauthorized effect. Replay attack is also known as a "man-in-the-middle attack". It can be prevented by using strong digital signatures.

4.2.2.3. MODIFICATION OF MESSAGES: In this type of attack the intruder alters the confidential information. This can be done by two different ways to modify the message either the attacker will alter the packet header addresses to direct a message to a different destination or will modify that data on the target machine so that an unauthorized effect can be produced.

4.2.2.4. DENIAL OF SERVICE (DOS): This is the major security threat to network security because it is very hard to prevent it. The attacker is disrupted the network by increasing the traffic through overloading the network.

4.2.2.5. DISTRIBUTED DENIAL OF SERVICE (DDOS): DDoS is a type of DoS attack where multiple compromised systems which are often infected with a Trojan horse, are used to target a single system causing a Denial of Service (DoS) attack.

4.3. PRACTICAL VIEW ATTACKS:
In this point of view, security attacks are classified into two levels:

4.3.1. APPLICATION LEVEL: This type of attacks is happened at application layer of the network. It attempts to access or modify the information at application level.

4.3.2. NETWORK LEVEL: This type of attacks is happened at network level, aims to reduce the capability of the network even to halt the system.

5. LEVELS OF IMPACTS ON SECURITY LOSS

The security loss can be expected to have the various effects on organizational operations, assets and individuals. The effects may leads to the following:

- Cause effect on degradation in mission capability to perform organizational primary operations
- Damage on organizational assets
- Financial loss
- Harm to individuals.

Table 1: Levels of Impacts on Security Loss

Levels	Effects	Loss
Low	Limited adverse	Minor
Moderate	Serious adverse	Significant
High	Severe adverse	Major

6. CHALLEGES OF NETWORK SECURITY

The requirement for network security is quite difficult.

- ✓ Developing Security mechanisms should consider various types of attacks it may leads to complexity.
- ✓ Determine the location where the security mechanisms is to be used either in physical or logical.
- ✓ Combination of more than one security mechanisms or protocols leads to contradiction of functioning.
- ✓ Always there may be a hard war between an attacker and the designer exists.
- ✓ Requires regular monitoring which is not able due to overload of the work.
- ✓ Need high level of investment.
- ✓ Does not guaranty for user-friendly and convenience.

7. CONCLUSION

Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. The construction of infrastructure of the computer network is quite expensive we want to protect it from the loss. Network security is a challenge for network administrator and internet service providers in order to prevent it from the attack of intruders. This paper simply describes the importance as well as the complication of the network security and also outlines the challenges that involve to it. The main objective is to create the awareness about the different kinds of security violations among network administrators. We should perform the regular monitoring and advanced technologies to prevent it.

8. REFERENCES

[1] Carle E. Landwehr, "*Security Issues in Networks with Internet Access*", Member, IEEE.

[2] Siddharth Ghansela, "*Network Security: Attacks, Tools and Techniques*", vol. 3, Issue 6, June 2013.

[3] Kartikey Agarwal, "*Network Security: Attacks and Defence*", vol. 1, Issue 3, August 2014.

[4] 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014), Mouna Jouini

[5] Eric Cole, (2009), *"Network Security, Bible"*, 2nd Edition.

[6] Prakhar Golchha,"*A Review on Network Security Threats and Solutions*", 2347:3878, 2014.

[7] Inam Mohammad, "*A Review of types of Security Attacks and Malicious Software in Network security*", Vol. 4, Issue 5, May 2014.

[8] Bhavya Daya, "*Network Security: History, Importance, and Future*", University of Florida Department of Electrical and Computer Engineering.

[9] https://powermore.dell.com/technology/network-security-three-biggest-challenges/

[10] William Stalings, "*Network Security and Cryptography*", 5th Edition.