*International Journal on Emerging Trends in Electronics & Communication Engineering*
*Vol. 3, Issue 1 - 2019*

# DEVELOPMENT OF NETWORK SECURITY, NEED AND PROBLEMS

**RAJEEV RANJAN SINGH***

## ABSTRACT

The computer network technology is developing rapidly, and the development of internet technology is more quickly, people more aware of the importance of the network security. Security is an important field that consists of the provisions made in underlying computer network infrastructure, policies adopted by the network administrator to protect the network, the network-accessible resources from unauthorized access and the effectiveness of these measures combined together. Network security is main issue of computing. Protecting computer and network security are critical issues. Information is an asset that must be protected. Network security is more challenging than ever, as today's corporate networks become increasingly complex

**KEYWORDS:** Need For Network Security, Problems In Network Security, Development In Network Security

## INTRODUCTION

Network security is a challenge for network operators and internet service providers in order to prevent it from the attack of intruders. It deals with the requirements needed for a company, organization or the network administrator to help in protecting the network. Computers, networks, and the Internet affect our lives every day or we can say that we are so much dependent on them to make our life comfortable. We all are connected to the internet without any boundary, so Network Security is essential in this environment because any organizational network is accessible from any computer in the world and, therefore, potential vulnerable to threats from individuals who do not require physical access to it. Network security starts with authorization, commonly with a username and a password. Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, modification in system, misuse, or denial of a computer network and network-accessible resources. Basically network security involves the authorization of access to data in a network, which is controlled by the network admin. It has become more important to personal computer users, and organizations. If this authorized, a firewall forces to access policies such as what services are allowed to be accessed for network users.

*Department of Computer Science, Niet College, Alwar-301001, India. ***Correspondence E-mail Id:*** editor@eurekajournals.com

 **ISSN: 2581-558X**

## NEED FOR NETWORK SECURITY

Network security is the process through which we can protect the digital information. It is so crucial for all networks must be protected from threats and the risks so that a business can achieve its fullest potential. The objective of network security is:

### TO PROTECT THE CONFIDENTIALITY

The data must be accessed and read only by the authorized individuals or parties. It is the protection of the personal information. We can compare confidentiality with privacy. Data encryption, User Ids and passwords, Biometrics verifications are some of the methods through which confidentiality can be protected.

### TO MAINTAIN INTEGRITY

It is the assurance of not only the information can be accessed or modifies by the authorized persons only but also the data must be accurate, consistent over its entire life cycle. Measures taken to ensure integrity include controlling the physical environment of networked terminals and servers, restricting access to data, and maintaining rigorous authentication practices.

### TO ENSURE AVAILABILITY

Data must be available to the authorized persons at the right time. It can be ensured by rigorously maintaining all hardware, preparing hardware repairs immediately and maintaining a correctly functioning operating system environment. Regular backup must be taken, for information services that are highly critical, redundancy is appropriate method to ensure availability.

## PROBLEMS IN NETWORK SECURITY

All network face one or more issues, it is the responsibility of the network administrator to keep the network secure for malicious software, worms, and threats and from other attacks. An attack is an information security threat through which the intruder attempt to obtain, alter, remove, implant or reveal confidential information without authorized access or permissions

## PASSIVE MONITORING OF COMMUNICATIONS (PASSIVE ATTACKS)

In this attack the disclosure of the confidential information or the files to an attacker without the consent of the authorized individual or an organization. The attacker monitors for the open ports or vulnerabilities to gain the information about the target without changing it on the target machine. There are two main types of passive attacks:

1. Release of Message Content: This is one of the easiest methods to grasp from its name and what it does it easily figured out also. 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.
2. Traffic Analysis: This method also attack the confidentiality but it is little complicated than other methods. 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.

### ACTIVE ATTACKS

In this type of attack the hacker attempt to make changes to the data on the target machine. It can be said as the attacker can modify the stream of bits or creation of false stream of bits but the goal is same and much more of the passive attack and that is to steal the confidential information of the individual or organization and also do harm to the network or network services which they are providing. The active attacks are subdivided into different categories:

1. **REPLAY ATTACK:** It is a breach of security in which the hacker can store the information

 ISSN: 2581-558X

and then retransmit it with a trick to the receiver with some unauthorized operations such as false identification or a duplicate transaction. Replay attack is also known as "man-in-the-middle attack".

2. **MASQUERADE ATTACKS:** The intruder pretends to be a particular user of the network system so that he 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.
3. **MODIFICATION OF MESSAGES:** In this type of attack the intruder can use two different ways to modify the message either he will alter the packet header addresses to direct a message to a different destination or he will modify that data on the target machine so that an unauthorized effect can be produced. This is a very common type of attacks that is used.
4. **DENIAL OF SERVICE (DOS):** Here users are deprived of access to the network or its resources. The entire network is disrupted by overloading the messages than it can handle to ruin its performance. DoS are the major threat to network security in today's scenario because they can be easily launched with some basic knowledge.
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 attack.

### INSIDER ATTACK

These attacks involve someone who has authorized access to the network with either an account on the server or having a physical access to the network. He can intentionally or accidentally attack the network from some malicious or non-malicious ways. Malicious insiders intentionally eavesdrop, steal, or damage the information and they can use this information in a fraudulent manner. They can also deny access to other authorized users. In the same way attacks can be non-malicious while performing the tasks in an organization like carelessness, lack of knowledge, or intentional circumvention of security. Internal Intrusion Detection System (IDS) protect organizations against insider attacks.

### CLOSE-IN ATTACK

When an individual or a group is trying to attain close proximity to networks, so that, they can modify, collect the information or deny the access to the information. One of the popular close-in attacks is social engineering, where the attacker compromises the network through social interaction through an e-mail or over the phone. The attacker will apply some tricks in the conversation so that the victim a reveal the secrets of the company and he attacker could gain unauthorized access to the network or to the system.

### PASSWORD ATTACK

Password attacks are the classic way to gain access to a computer system to find out the password and login Id. Their goals might differ, but they all tries to crack the passwords which are stored in a network account database or a password-protected file.

### EXPLOIT ATTACK

In this type of attack on the computer system the attacker takes the advantage of a particular vulnerability that system offers to the intruders when the intruder knows about the security problem within an operating system or in a piece of software.

## DEVELOPMENT IN NETWORK SECURITY

There are many dramatic changes in the technology of network security this is all because of new mobile Operating systems, growing use of

 **ISSN: 2581-558X**

personal devices an many more reasons. Day to day enhancements both in technology and infrastructure make all these developments possible. There are more remote users, faster network connections, and extensive upgrades to mobile networks which are some of the reasons for network security.

## HARDWARE SECURITY MODULE (HSM)

A hardware security module is a physical computing device that safeguards and manages digital keys for strong authentication and provides crypto processing. These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server. HSMs provide both logical and physical protection of these materials, including cryptographic keys, from non-authorized use and potential adversaries.

## BIOMETRICS

Biometrics use is obvious that is for secure workstation log in that is connected to a network. The primary advantage of this technology over others is that they really do what they should, i.e. they authenticate user by using human's physiological or behavioural characteristics to authenticate users. Biometric objects cannot be stolen as password, keys and cards.

## SMART CARDS

It is an Integrated Circuit Card (ICC) of a pocket-size that has embedded integrated circuits. They are made of plastics, generally polyvinyl chloride (PVC). Smart cards can provide personal identification, authentication, data storage, and application processing. Smart card can be stolen but there is a safety feature built into it. The authenticated uses have to enter a personal identification number (PIN) after using it. The PIN is verified from inside the smart card as it is never transmitted across the network, hence cannot be used if the smart card is stolen.

## INTRUSION DETECTION SYSTEM (IDS)

An IDS is a listen only device or software application the monitors network or system activities for malicious activities. Intrusion prevention system (IPS) extended IDS solutions by adding the ability to block threats in addition to detecting them. IDS are placed out-of-band out his network infrastructure that is not a real-time communication path between the sender and the receiver of the information.

## CONCLUSION

Network security isn't something you either have or don' t, it is a continual arms race against hackers. Fortunately, as attacks become more sophisticated, so too does the technology and practices used to protect the network. One of the biggest security concerns today is the insider threat. Another major security concern is lack of consistency in enforcing "acceptable use" policy. Most of the policies are badly written, out of date and poorly communicated. Securing the network is just as important as securing the computers and encrypting the message. In current scenario there are number of ways, which guarantee for the safety and security of the network but it cannot be said they will everlasting. We have to perform regular network security testing.

## REFERENCES

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

[2]. Harish singh, "Network Security, A challenge" IJARCCE Vol. 5, Issue 3, March 2016.

[3]. 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014), Mouna Jouini.

[4]. Anuradha, Mohan V. Pawar ,Network security and Types of Attacks, ICCC 2015.

 ISSN: 2581-558X

[5]. Kartikey Agarwal, "Network Security: Attacks and Defence", vol. 1, Issue 3, August 2014.
[6]. http://computernetworkingnotes.com/network-security-access-lists- standards-and-extended/types-of-attack.html.
[7]. http://whatis.techtarget.com/definition/Confidentiality-integrity- and- availability-CIA.
[8]. Inam Mohammad, "A Review of types of Security Attacks and Malicious Software in Network security", Vol. 4, Issue 5, May 2014.
[9]. Eric Cole, (2009), Network Security, Bible, 2nd Edition.

 **ISSN: 2581-558X**