NETWORK SECURITY – THE RESEARCH

POOJA ANAND, SHIVAM MAHESHWARI

***Abstract*— For the first few decades of their existence, computer networks were primarily used. And In today's world, everyone is connected to a network in one way or the other and with the advancement of technology and user needs network security has became the major issue. Network security prevents the access to the unauthorized user. This paper discusses the concept of Network Security, its role, the types of network threats and how these can be managed.**

***Index Terms*— Network Security, attacks, network, Management.**

I. INTRODUCTION

Network Security is the major subject for the experienced experts which has been maintained till now. It consists of the authentication of the user for accessing the data that is controlled by the administrator. The authentication procedure includes the user to set the user name and password or some other kind of information that will only be accessible to the user. In the paper, Section 1 discusses about the network security which describes the term and its role. Section 2 of the paper describes the types of attacks that may affect the security. Section 3 of the paper describes the techniques used to manage the security and maintain it from various attacks. Section 4 discusses some of the devices that provide secure network environment to the user.

II. NETWORK SECURITY

Network security can be maintained for both public as well as for private networks used for daily communication purpose in one way or the other among various individuals, companies, businesses, government agencies. It protects the user data from any misuse, modification by any unauthorized process. The process of network security starts when the user assigns the username and password which is authenticated every time whenever user wants to access any information. For communication over a network, there are various protocols defined in OSI (Open Systems Interface) model described by ISO (International Standard of Organization). To achieve a secure communication in a network, the data should not be susceptible to attack and following things must be taken care of while communication.

- **Access** – The user must be authorized to communicate from a network.
- **Confidentiality** – Information shared must be private between the users.
- **Authentication** – The data must be shared among the authenticated user only.
- **Integrity** – The data shared over the network must not be modified.

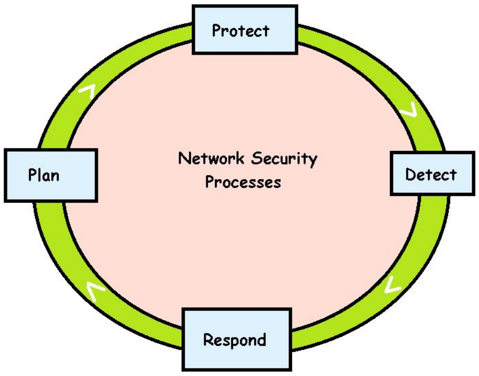

Figure 1: Network Security Processes

III. TYPES OF SECURITY ATTACKS

There are various malicious attacks that may occur to break the network security. These are as follows

- **Viruses, worms** – These are the programs that are used to infect the file of the user which replicate themselves if downloaded by the user accidently.
- **Spyware** – It is the technique in which the attacker places any malicious program in the software or program to the user and user downloads it unknowingly which corrupts the user system.
- **Adware** – These are the illegal copies of the original software by which the selling of original license decreases.
- **IP Spoofing** – It is the technique in which the attacker keeps the track of user's traffic and may manipulate the data for which the user contains no knowledge of this manipulation. According to the user, the information received is from the original source.
- **Denial of service** - Denial-of-Service (DOS) is a technique in which the user cannot deny the request of the attacker to send the packets. These are easy to run programs but very difficult to track. In this, the program simply connects the system of the user and attacks.
- **Data interception** – In this, the attacker uses the packets to corrupt or modify the data that are being transferred in a network from one user to another.
- **Phishing** – In phishing, the private information of the user is acquired by the phisher by tricking the user with their personal data such as online banking data, credit card number, and so on.

Manuscript received Sep 27, 2014.

POOJA ANAND, Department of Information Technology, Dronacharya College of Engineering, Gurgaon, India
SHIVAM MAHESHWARI, Department of Information Technology, Dronacharya College of Engineering, Gurgaon, India

- **ARP poisoning** – In this, the attacker replaces the destination IP Address with its own IP Address so that the sender receives the IP and MAC Address of the attacker and the user unintentionally sends the information to the attacker instead of the authenticated user at the destination end.
- **Cyber attack** – It is any offensive manner of tampering anyone's personal computer network or computer with an intention of stealing, destroying or altering any information.

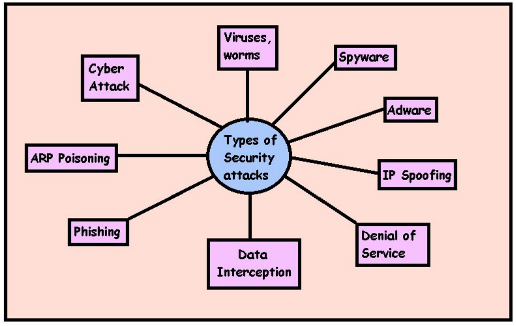

Figure 2: Types of Security Attacks

IV. Network Security Management

Management of security in a network is very different like in homes and small scale companies require less security but for large organization, security management requires advance software's for high security to prevent the data from any malicious attacks, hacker, or by any unauthorized user. Effective planning should be used for the maintaining the security. There are various methods that may be used to protect a network. These are

- **Firewalls -** Firewalls are commonly defined as the mechanism that is used to act as a hurdle between two networks. For maintaining security, various organizations use firewalls.
- **Access Control List (ACL) -** It is the list which consists of the address of the sender, address of the receiver, service port and various other details. It performs the function of controlling the routers.
- **Demilitarized Zone (DMZ) -** DMZ is a part of a firewall that is a network between the trusted and untrusted network. It functions in the layers of the internet and whenever any untrusted user tries to attack the user, it blocks the network.
- **Proxy -** Proxy is the process in which the host obtains the information from the internet by a proxy server in order to maintain security of data. This enables the user to access the resources without direct communication from internet.
- **Cryptographic Systems –** These are the systems that are used to transform the information into coded form or in the cipher form to secure the user data.

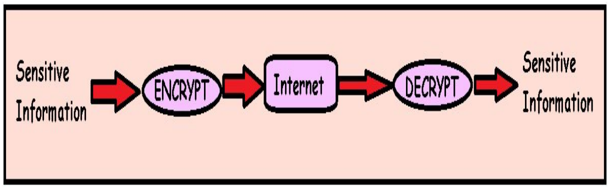

Figure 3: Encryption of Data

V. Secure Network Devices

- **Secure Modems** – These are the devices used for creating modem logs, read caller ID information and also controls the connectivity with the server. It also checks that unauthenticated user should not access its facility.
- **Crypto-Capable Routers –** The functioning of these routers are to encrypt the outgoing data and decrypt the incoming data to avoid the misuse of data from any unauthenticated user. For this, it uses many encryption techniques and algorithms such as AES, DES, RES, 3DES.
- **Virtual Private Networks –** Virtual private networks (VPN) are just like wide area network (Internet). It creates point-to-point connection between end users. It uses many tunneling protocol or traffic encryption techniques to send and receive data across network safely.

Conclusion

Security is very vast issue that may be of various kinds namely - network security, data security, computer security, internet security, and so on. The paper focuses on the network security, the security features, potential threats that may be used to break the security of the user information available over the network. This paper also discusses the measures and some secure devices that may be used to protect the network in an industry.

References

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

[2] Network Security Basics, www.syngress.com.

[3] Network Security ISOC NTW 2000, Cisco systems, www.cisco.com.

[4] Network Security, www.wikipedia.com.