Improving Networks Security: Threats and Measures

Saurabh Patodi
Dept. of computer Science
S.J.H.S.Gujarati Innovative College,Indore(M.P) India

Richa Sharma
Dept. of computer Science
S.J.H.S.Gujarati Innovative College,Indore(M.P) India

Aniruddha Solank
Dept. of computer Science
S.J.H.S.Gujarati Innovative College,Indore(M.P) India

Abstract - Network security is now days becoming more and more important because people like to connect with each other all the time via internet. Personal computer users, employees of professional organizations, government servants, academicians, social workers, students, military peoples etc are very familiar to use network currently and all these people use the available network for most of their work. All these people keep their most important data on internet and also do the money related online transactions. The internet structure is itself such that there may be possibility of threats to occur. To secure our network we must have to know which type of security threats may occur and how? By knowing this we may able to find out security methods against these threats.

With the rapid development of computer technology, computer network continues to expand the scope of application with more and more users. Network security gradually attracts people's attention. This paper briefly introduces the concept of computer security, focuses on the threats of computer network security and discusses basic techniques. It proposes effective measures to improve the computer network security

Keywords- Network Security, Security Attacks, Security Issue, Security Measures

I. INTRODUCTION

Network security refers to any activities designed to protect your network. It consists of the technologies and processes that are deployed to protect networks from internal and external threats. Network security involves all activities that organizations, enterprises, and institutions undertake to protect the value and ongoing usability of assets and the integrity and continuity of operations. Effective network security targets a variety of threats and stops them from entering or spreading on your network.

II. NETWORK SECURITY OBJECTIVES

To provide a better as well as robust level of security, the objective about what should be done is main aspect, which is as follows -

- Analyze Network security level.
- To analyze security threats and provides mechanism against it.
- Discussing role of computer system assets in the area of security.

Various network security trends emerged which also studies and categorized under network security heading. System and network technology becomes a key aspect to provide wide variety of applications. Security is a crucial in networking aspect. While discussing about Network security, emphasize will be given for security of network.

Main part in network security is to provide security to data which is getting transferred over the communication channel.
When anyone wants to develop secure network, the following points should be kept in mind which needs to be considered:
1. Access - Only authorized users are able to access the assets or components available in the network.
2. Authentication - Only Authenticate or registered user is only able to gain access to system.
3. Privacy - The data on network should be kept private.

The effective and efficient data security plans can be developed with understanding of security issues and study of factors that make a network vulnerable to attack. To enhanced security of network components there are many tools are available such as encryption tools intrusion detection, security mechanisms and firewalls. Understanding the security issues of internet, provides valuable assistance in developing new security mechanisms and approaches for networks & internet security itself.

III. NETWORK SECURITY MODEL

A model for much of what we will be discussing is captured, in very general terms, in Figure 1. A message is to be transferred from one party to another across some sort of Internet service. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the Internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals. Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on. All of the techniques for providing security have two components:

1. A security-related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.

2. Some secret information shared by the two principals and, it is hoped, unknown to the opponent.
An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

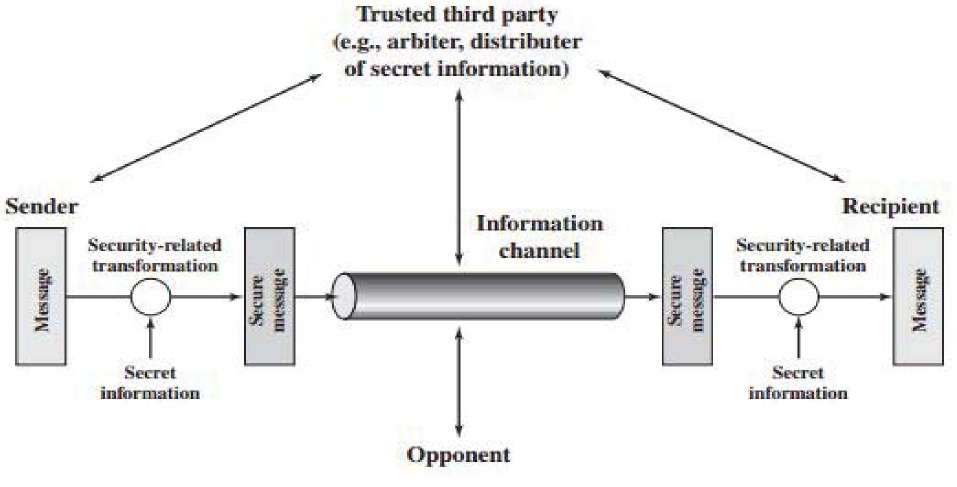


Fig. 1 Network Security Model

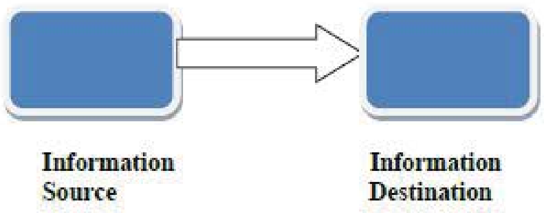
A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent. Or a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission. This general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information.
4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

IV. TYPES OF ATTACKS

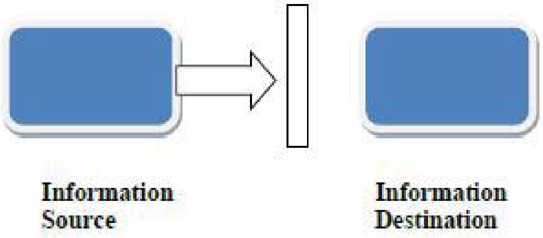
Types of attacks should be characterized by viewing their functions as well as the impact they will left on the data. In general , there is a normal flow from Information Source to Information Destination , which may disturbed when attacks has been done on the data which is to be transferred over communication channel .

1. Normal Flow:



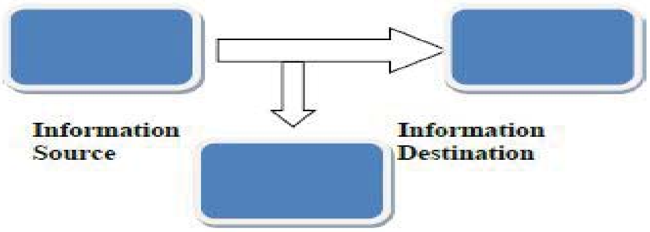
Data which is to be transferred over internet must follow the normal path as shown in figure 1. The information must be securely passed over communication channel without any obstacles.

2. Interruption:



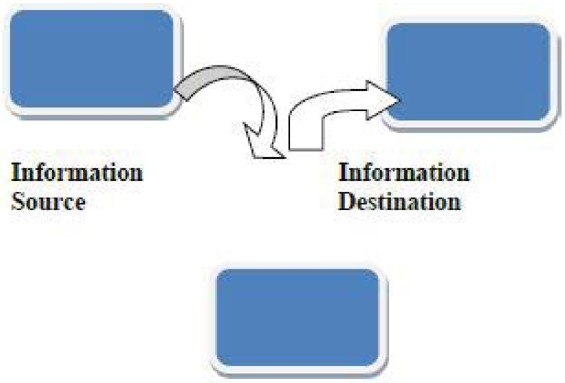
In Interruption, the normal flow of the data must be broken by the external intruders, which stops the data to reached to Destination as shown in Figure 2 .

3. Interception:



In Interception, the data which is getting transferred over internet should be reached to destination but intruders can gain the access of that data and must be getting information from that data.

4. Modifications:



In Modification, The intruders can access the data, make the modifications in it and resend the data to the destinations. This is nothing but the tampering of with the assets. Modification is shown in figure 4.

V. NETWORK SECURITY THREATS

- **Eavesdropping** - When any unauthorized party tries to listen to the communication, it is known as eavesdropping.
- **Viruses** - Viruses are software programs which can self-replicate on computers via computer networks. Virus programs are attached with other program files.
- **Worms** - A worm is also software programs which can self-replicate on computers via computer networks. There are two main types of worms, mass-mailing worms and network aware worms.
- **Trojans**- Trojan horse is a malicious or harmful code which is contained inside apparently harmless programming or data in such a way that it gets total control of your computer and can do anything with your computer. It can remove all data from your hard disk or it can run memory allocation table etc.
- **Spyware** - Spyware is a type of malware that is installed on a computer without the knowledge of the owner in order to collect the owner's private information.
- **Phishing** - Phishing is an attempt to obtain confidential information from an individual, group, or organization. Phishing is a technical term used for hacking personal data and these are generally in the form of e-mail messages. Phishers may tries to get personal data, such as credit card numbers, online banking credentials, and other sensitive information.
- **Spoofing Attacks** - Spoofing means to try to get the address of the computer in order to gain access to other computers so that data and other secret information can be stolen from those computers.
- **Denial of Service** - Denial of Service is an attack when the system receiving too many requests cannot return communication with the requestors. The system then consumes resources waiting for the handshake to complete. Eventually, the system cannot respond to any more requests rendering it without service.
- **IP spoofing** - In computer networking, the term IP address spoofing or IP spoofing refers to the creation of Internet Protocol (IP) packets with a forged source IP address, called spoofing, with the purpose of concealing the identity of the sender or impersonating another computing system.
- **Packet sniffing** - It is a program that can record all network packets that travel past a given network interface, on a given computer, on a network as well as to extract sensitive information from packets.

VI. MEASURES TO IMPROVE NETWORK SECURITY

A. Online anti-virus measures

According to the characteristics of computer network virus, effective prevention on the virus is difficult and complex. It is a daunting task for network managers to monitor the prevention work. Previous work is only limited to every client computer, in which every user needs to install anti-virus software and on your machine, such as

KV300 system, or Rising anti-virus software, etc. However, due to limited computer skill of users, this approach is hard to ensure the safety of the whole network system. As an effective solution to prevent the, the basic requirement is to meet the following demands:
1. Install anti-virus software on computers
2 Update the virus database in users' machines
3 Released the latest virus database upgrade file from the WAN connection
4 Coordination and management of remote users' virus scanning
5 Address user-reported problems timely
6 Download and preview scan report provided by users
7 Remote control user options
8 Improve the execution speed and zooming ability in large-scale networks
People are more capable of preventing online viruses. More anti-virus measures have emerged in order to effectively guarantee the network security. Network management personnel can install a complete set of virus software on any client server through one source server. As there are many types of software, network managers should take into account their own situation to achieve the "best use."

B. Measure to prevent hackers

The invasion and attack can be divided into subjective and objective security issues. Subjectivity security issue mainly refers to errors made by network management personnel. Objectivity security issue mainly refers to loopholes in computers and the network where hackers exploit these vulnerabilities to conduct various forms of attack.

C. Use safety tool

The above-mentioned basic techniques of computer network security can collect safety issues of host computers. Network management personnel identify these problems in a timely manner and install the patch. Network managers take the advantage of scanning tools (such as NAL's Cyber Cop Scanner) to scan host computers, learn about the weakness links take appropriate preventive and repair measures.

D.Firewall technology

Firewall technology is to prevent others from accessing your network device like a shield. There are three types of firewall technology, namely, packet filtering technology, agent technology, and status monitoring technology. Packet filtering technology is to verify the IP address by setting it. Those IP addresses that do not match those settings will be filtered by the firewall. But this is the first layer of protection. Agent technology is to verify the legitimacy of requests sent by accept client of proxy server to. This technology also involves with user authentication, login, simplified filtering criteria and shielding the internal IP addresses. Status monitoring technology is the third generation of network security technologies, which is effective for all levels of network monitoring. It makes it possible to make timely security decisions. Firewall technology can successfully prevent hacker from intrusion in the local network and protect the network.

VII. CURRENT DEVELOPMENT IN NETWORK SECURITY

Currently we are using biometric identification techniques in colleges and organizations. The biometric machines or hardware are connected with the computer so with the internet. Biometrics provides a better method of authentication than passwords. This might greatly reduce the unauthorized access of secure systems. New technology such as the smart card is surfacing in research on network security. The software aspect of network security is very dynamic. Constantly new firewalls and encryption schemes are being implemented.

1. Hardware Development

Smart cards are usually a credit-card-sized digital electronic media which stores digital information. The main idea behind smart cards is to provide undeniable proof of a user's identity. Smart cards can be used for everything from logging in to the network to providing secure Web communications and secure e-mail transactions. Smart card can be implemented with PIN number which is a personal identification number. If your smart card is misplaced, other person can't use it because it needs your PIN number to access the resources. We are also using PIN numbers in ATM cards.

2. Software Developments

Wide variety of advance software is available in market to get high degree of network security including firewalls, antivirus, intrusion detection, and much more. The research focuses on development of more sophisticated software, able to deal with any type of attack in most efficient way. When new viruses come into picture, the antivirus is updated to be able to fight against those threats. This process is the same for firewalls and intrusion detection systems.

VIII. CHALLENGES OF NETWORK SECURITY

The Challenges of Computer Security Computer and network security is both fascinating and complex. Some of the reasons include:

1. Security is not as simple as it might first appear to the novice. The requirements seem to be straightforward; indeed, most of the major requirements for security services can be given self-explanatory, one-word labels: confidentiality, authentication, non-repudiation, integrity. But the mechanisms used to meet those requirements can be quite complex, and understanding them may involve rather subtle reasoning.

2. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features. In many cases, successful attacks are designed by looking at the problem in a completely different way, therefore exploiting an unexpected weakness in the mechanism.

3. Security mechanisms typically involve more than a particular algorithm or protocol. They also require that participants be in possession of some secret information (e.g., an encryption key), which raises questions about the creation, distribution, and protection of that secret information. There also may be a reliance on communications protocols whose behavior may complicate the task of developing the security mechanism. For example, if the proper functioning of the security mechanism requires setting time limits on the transit time of a message from sender to receiver, then any protocol or network that introduces variable, unpredictable delays may render such time limits meaningless.

4. Computer and network security is essentially a battle of wits between a perpetrator who tries to find holes and the designer or administrator who tries to close them. The great advantage that the attacker has is that he or she need only find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security.

5. There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs.

6. Security requires regular, even constant, monitoring, and this is difficult in today’s short-term, overloaded environment.

7. Security is still too often an afterthought to be incorporated into a system after the design is complete rather than being an integral part of the design process.

VIII. CONCLUSION

Network Security is an important field gaining attention as the popularity of internet increases with the increase in communication strategies. Through the new approaches towards the communication strategies, network and data security gaining popularity. A number of security mechanisms are also invented to provide better access to network. With the development of computer network technology, computer network security problems happen all the time. Therefore, people hold worries towards the development of computer network technology. Since computer network security influences people’s life, researches to build a computer network security model must be continued.

REFERNCES

[1] Advanced Honeypot System for Analysing Network Security By Suruchi Narote and Sandeep Khanna(ISSN: 2347-3215 Volume 2 Number 4 (April-2014) pp. 65-70)

[2] Security Issues and Attacks in Wireless Sensor Network By Raja Waseem Anwar, Majid Bakhtiari, Anazida Zainal,Abdul Hanan Abdullah and Kashif Naseer Qureshi(World Applied Sciences Journal 30 (10): 1224-1227, 2014)

[3] Network Security : Attacks and Defence. Kartikey Agarwal*, Dr. Sanjay Kumar Dubey Amity University, Noida, Uttar Pradesh, India (International Journal of Advance Foundation and Research in Science & Engineering (IJAFRSE)Volume 1, Issue 3, August 2014.)

[4] A Survey on Different aspects of Network Security in Wired and Wireless Networks

[5] By- Bharti Chopra, Dr. Parminder Singh (ISSN: 2278-621X Vol. 4 Issue 2 July 2014)

[6] Network Security Issues and Solutions By - Mrs. Bhumika S. Zalavadia (ISSN : 2229-3345 Vol. 5 No. 06 Jun 2014)

[7] A Survey on Security Issue in Mobile Ad-Hoc Network and Solutions By - Mayank Kumar and Tanya Singh(E-ISSN: 2347-2693)

[8] Brenton, C. and Hunt, C. (2002): Mastering Network Security, Second Edition, Wiley

[9] Marin, G.A. (2005), “Network security basics”, In security & Privacy, IEEE, Issue 6, Vol. 3, pp. 68-72, 2005.

[10] McClure, S., Scambray J., Kurtz, G. (2009): Hacking Exposed: Network Security Secrets & Solutions, Sixth Edition, TMH.

[11] “Security Overview”. www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/security-guide

[12] Murray, P., Network Security, found at http://www.pandc.org/peter/presentations/ohio-tech-2004/Ohio-tech-security-handout.pdf

[13] Dowd, P.W.; McHenry, J.T., "Network security: it's time to take it seriously," Computer, vol.31, no.9, pp.24- 28, Sep 1998

[14] Kartalopoulos, S. V., "Differentiating Data Security and Network Security," Communications, 2008. ICC '08. IEEE International Conference on, pp.1469-1473, 19-23 May 2008

[15] Adeyinka, O., "Internet Attack Methods and Internet Security Technology," Modeling & Simulation, 2008. AICMS08. Second Asia International Conference on, vol., no., pp.77-82, 13-15 May 2008

[16] Marin, G.A., "Network security basics," Security & Privacy, IEEE , vol.3, no.6, pp. 68-72, Nov.-Dec. 2005

[17] Simmonds, A; Sandilands, P; van Ekert, L (2004) Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285, pp.317–323

[18] Curtin, M. “Introduction to Network Security,” http://www.interhack.net/pubs/network-security.