# A Survey on Network Security Attacks and Defence

**Prof. Pranali R. Landge**

*Abstract-* **Network security is important in every field of today's world such as military, government, organizations and even in our daily lives. Having the knowledge of how the attacks are executed we can better protect ourselves. The internet structure itself allowed for many security threats to occur. The entire field of network security is vast and in an evolutionary stage. The range of study encompasses the current development in network security, attacks and methods through the internet.**

**This paper briefly outlines the concept of network security; the various attack methods which are used, as well as various defence mechanisms against them.**

**Keywords: Network Security, Security Attacks**

## I. INTRODUCTION

In this digital era more and more people becoming active on the Internet for their personal and professional, because of this internet is growing rapidly. But, along with the evolution of Networking and Internet, several threats attacks and Trojan Horses have also risen drastically. So the task of securing the network is now at the forefront of computer network related issues.

A network consists of routers from which information can be easily stolen by the use of malwares such as a "Trojan Horses". Network security is thus mainly focused on the data networks and on the devices which are used to link to the internet. Email is a widely used service today and it is also

3. Confidentiality – Data in the network remains private. This is done to ensure that the information can be viewed only by authenticated systems and it can be achieved using various encryption techniques.

4. Integrity – This ensures that the message has not been changed during transmission.

An effective network security plan is developed with the understanding of security issues, potential attackers, needed level of security, and factors that make a network vulnerable to attack

## II. HISTORY OF NETWORK SECURITY

Recent interest in security was fueled by the crime committed by Kevin Mitnick. Kevin Mitnick committed the largest computer-related crime in U.S. history[1] . The losses were eighty million dollars in U.S. intellectual property and source code from a variety of companies[1]. Since then, information security came into the spotlight. Public networks are being relied upon to deliver financial and personal information. Due to the evolution of information that is made available through the internet, information security is also required to evolve. Due to Kevin Mitnick's offense, companies are emphasizing security for the intellectual property. Internet has been a driving force for data security improvement. Internet protocols in the past were not developed to secure themselves. Within the TCP/IP communication stack, security protocols are not implemented. This leaves the internet open to attacks. Modern developments in the internet architecture have made communication more secure. contain many serious flaws, there is no system of authenticating the sender as well as the recipient, it is stored in multiple places during transmission and can be easily intercepted and changed.

Over the last few years, security threats to company have grown and changed significantly and so have the defences. Security is a vital requirement for network. When considering network security, it must be emphasized that the whole network is secure. Network security does not only concern the security in the computers at each end of the communication chain. When transmitting data the communication channel should not be vulnerable to attack. A possible hacker could target the communication channel, obtain the data, decrypt it and re-insert a false message. Securing the network is just as important as securing the computers and encrypting the message. While developing a secure network, the following need to be considered -

1. Access – Only authorized users are allowed to communicate to and from a particular network.

2. Authentication – This ensures that the users in the network are who they say they are. Actual flow of information can start only after the user has been authenticated and allowed to communicate to other systems in the network.

## III. NETWORK SECURITY TECHNOLOGIES

**1. Firewall technology:**

Firewall technology is an array of safety applications to exert mandatory access on external network by using predetermined safety facilities between network systems. Data transfer between two or more networks should follow certain safety measures to monitor the performance, determine whether the communication between the networks is allowed, and monitor the running of the network.

**2. Data encryption technology:**

Data encryption technology categories can be divided in data storage, data transfer, data integrity, authentication and key management techniques. Data encryption is stored in the memory in order to prevent data loss and destruction. The transmission process in the information encrypted is commonly in the form of circuit encryption and port encryption. Data integrity identification technology is to protect information transfer, storage, access, identification and confidential treatment of people and data. In this process, the system is characterized by the parameter value judgment on whether the input is in line with the set value. Data are subject to validation, and encryption enhanced the protection. Key management is a common encryption in many cases. Key management techniques include key generation, distribution, storage, and destruction, etc.

**3. Instrusion Detection Technique:**

Intrusion detection technology is to ensure the safety of the design and the rational allocation. Intrusion detection condition in the report. It can address and resolve system vulnerabilities in a timely manner. Technologies that are not in line with security policies are frequently used.

**4. Anti Virus Technology:**

Anti-virus technology not simply refers to anti-virus software technology. From the effects of its use, it can be classified into network anti-virus software and stand-alone anti-virus software. Online anti-virus software focuses on network connection against viruses. Once the virus has enter in the network or diffused to other network data, it will be promptly detected by online virus software, be killed and deleted.

## IV. Different Types Of Security Attacks

**1. Passive attacks:**

This type of attacks includes attempts to break the system using observed data. One of its example is plain text attack, where both the plain text and cipher text are already known to the attacker. Properties of passive attacks are as follows:

- **Interception:** The data passing through a network can be easily sniffed and thus attacking the confidentiality of the user, such as eavesdropping, "Man in the middle" attacks
- **Traffic analysis:** Also attacks confidentiality. It can include trace back on a network like a CRT radiation.

**2. Active Attacks**

In this attack the attacker sends data stream to one or both the parties involved or he can also completely cut off the data stream. Its attributes are as follows:

- **Interruption:** It prevents an authenticated user form accessing the site. It attacks availability. Such as DOS attacks.
- **Modification:** In this the data is modified mostly during transmission. It attacks integrity.
- **Fabrication:** Creating counterfeit items on a network without proper authorization. It attacks authentication.

**3. DOS Attack**

DOS attacks today have become a major threat to network security all over the world. They can be easily launched by anyone with the basic knowledge of network security. They don't require as much time and planning as some other attacks, in short they are cheap and efficient method of attacking networks. They can shutdown the company network by overflowing it with requests and thus affects availability of the network. With the help of easy to use network tools such as Trinoo, which can be easily downloaded of the internet any normal user can initiate an attack. DOS attacks usually works by exhausting the targeted network of bandwidth, TCP connections buffer, application/service buffer, CPU cycles, etc. DOS attacks use many users connected to a network known as zombies most of the time users are unaware of that their computer is infected[2] .Many attacks are used to perform a DOS attack so as to disable service. Some of which are as follows:

- TCP SYN Flooding
- ICMP Smurf Flooding
- UDP Flooding

## V. Types Of Network Security

The different types of network security are as follows[3] :

- **Security by Obscurity :**This works on stealth approach. Its basic working principle is that if no one knows the system exists then it won't be attacked. The problem with this approach is that it won't be a long term solution, and once the system is detected, it will be completely vulnerable.

- **The Perimeter Defence**: Organization harden the network security by using tools such as hiding the network behind a firewall, separating the network from an untrusted network. This method does nothing to stop an attack from inside. Once the perimeter system fails the inside system is completely left vulnerable.

- **Defence in Depth:** This is the best way to protect the system but also very difficult to implement. In this each system is hardened and is monitored thus acting like an island and it defends itself against the attacks. Even if one of the networks is compromised it won't affect the other networks. In this method internal networks are less susceptible to be compromised. With this system it can also detect hack attempts from the compromised systems.

## VI. Defence For Network Security

Many of the network attacks can be easily prevented by the network admin monitoring his network closely and applying the entire latest patch available from the vendor to his software. However this cannot prevent most of the attacks, to prevent them, the network requires configurations such as:

**1. Firewalls:**

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 authenticity 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.

**2. Configuration Management.**

Use safety tool and switch: Network management personnel identify 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. When designing a large-scale regional computer network, we need to ensure that the switch is connected to a network or in a separate network, so that the switch can form a separate management network. This will effectively reduce the number of network switches and narrow

the scope of failure. By using search and location, it is also convenient for network managers to quickly handle remote network accidents.

**3. Encrypting the World Wide Web (WWW)**

Network security can also be compared to human system. The human system can be taken as analogy, providing a protection at each point just like a body we can greatly improve the security. Using this mechanism we can spread our resources and prevent dependency on one system [5]. For the sake of privacy, confidentiality and availability our communications on the web should always be encrypted, this reduces the number of attacks and prevents anyone to view the ongoing transmissions. These can be achieved by putting together a system of encryption and employing a system of digital certificates. The most important way of encryption is the SSL protocol [4].

**4. Online Anti-Malware Software and scanners**

According to the characteristics of computer network virus, effective prevention on the virus is difficult and complex. Viruses, worms and Trojan horses are all examples of malicious software, or Malware for short. Special so-called anti-Malware tools are used to detect them and cure an infected system. As an effective solution to prevent it, the basic requirement is to meet the following demands:

1. Install anti-virus (Anti-Malware) 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(anti-malware) measures have emerged in order to effectively guarantee the network security. Network management personnel can install a complete set of antivirus 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."

**5. Thwart 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.

**6. Defence against DOS Attacks**

To prevent DDoS attack many technologies have been developed such as intrusion detection systems
(IDSs), firewalls, and enhanced routers. These things are used between the internet and servers. They
monitor incoming connections as well as outgoing connections and automatically take steps to protect the network. They have traffic analysis, access control, redundancy built into them [7].IDSs are make a log of both the incoming and outgoing connections. These logs can then be compared to baseline traffic to detect potential Dos attacks. If there is unusually high traffic on the server it can also alert of a possible ongoing DOS attack such as TCP SYN flooding [6].Firewalls can also be used as defence against DOS attacks with the required configuration. Firewalls can be used to allow or deny certain packets, ports and IP addresses etc. Security measures can also be employed in routers which can create another defence line away from the target, so even if a DOS attack takes place it won't affect the internal network. Service providers can also increase the service quality of infrastructure. Whenever a server fails a backup server can take its place, this will make effect of DOS attack negligible. If the service providers are able to distribute the heavy traffic of a DOS attack over a wide network quickly it can also prevent DOS attacks, however this method require computer and network resources and they can be very costly to provide on daily basis as a result only very big companies opt for this method.

## VII. PRESENT DEVELOPMENTS IN NETWORK SECURITY

Network security is being improved in two fields namely hardware and security in the following ways:

**1. Hardware Developments:**

Biometric systems and smart cards are the only new hardware technologies that are widely impacting security. The main use of Biometric network security will be to replace the current password system. Maintaining password security can be a major task for even a small organization. Biometric has very important use in the field of the network security, some obvious uses such a built in biometric scanner attached to a workstation can be used as an authentication mechanism which can be used as a login to the system, since two persons cannot have the same biometrics as the both persons, it is a full proof mechanism of login [11].People tend to forget their passwords and so they keep it near their workstation written on a slip or something else or even lock themselves out of their system by incorrectly entering it too many times. All this can be easily avoided by biometric systems as they provide users undeniable proof of identity. Smartcards are provided by companies to its workers, they only work when they are inserted in the computer and a pin issued the network administrator is entered, since the pin issued is only four characters and numeric, users don't forget it and don't write it down.

The smart card is cost-effective but not as secure as the biometric identification devices.

**2. Software Developments:**

The software aspect of network security is very vast. It includes firewalls, antivirus, VPN, intrusion
detection, and much more. The improvement of the standard security software still remains the same. When new viruses emerge, the antivirus is updated to be able to guard against those threats. This process is the same for firewalls and intrusion detection systems. Many research papers that have been skimmed were based on analyzing attack patterns in order to create smarter security software. As the security

hardware transitions to biometrics, the software also needs to be able to use the information appropriately. Antivirus works on a very basic principle; they scan a file and then matches its digital signature against the known malwares. If the signature is match in the database it reports it, delete it or even disinfect it depending on the user's setting. Current research is being performed on security software using neural networks. The objective of the research is to use neural networks for the facial recognition software. Many small and complex devices can be connected to the internet. Most of the current security algorithms are computational intensive and require substantial processing power. This power, however, is not available in small devices like sensors. Therefore, there is a need for designing light-weight security algorithms [8]. Research in this area is currently being performed.

## VIII. CONCLUSION

In this study different articles and conferences reviewed in order to provide detail view of Network security, the various attack methods which are used, as well as various defence mechanism against them. The security technology is mostly software based, but many common hardware devices are used. The current development in network security is not very impressive. Most of the attacks can be easily prevented, by following many simply methods as outlined in this paper. As new and more sophisticated attacks occur, researchers across the world find new methods to prevent them. Numerous advancements are being made in the field of network security both in the field of hardware and software

## REFERENCES

[1] Kartalopoulos, S. V., "Differentiating Data Security and Network Security," *Communications, 2008. ICC '08. IEEE International Conference on*, pp.1469-1473, 19-23 May 2008
[2] Q. Gu, Peng Liu, "Denial of Service Attacks," Texas State University, San Marcos.
[3] J. E. Canavan, Fundamentals of Network Security, Artech House Telecommunications Library, 2000.
[4] R. E. Mahan, "Introduction to Computer & Network Security," Washington State University, 2000.
[5] M. A. Shibli, "MagicNET: Human Immune System & Network Security," IJCSNS International Journal of Computer Science and Network Security, Vol. .9 No.1, January 2009.
[6] M. Kassim, "An Analysis on Bandwidth Utilization and Traffic Pattern," IACSIT Press, 2011.
[7] M. Eian, "Fragility of the Robust Security Network: 80211," Norwegian University of Science and Technology, 2011.
[8] B. Daya ,"Network Security: History, Importance, and Future ,"University of Florida Department of Electrical and Computer Engineering , 2013.
[9] Curtin, M. "Introduction to Network Security," http://www.interhack.net/pubs/network-security.
[10] http://web.mit.edu/~bdaya/www/Network%20Security.pdf
[11] Li CHEN,Web Security : Theory And Applications,School of Software,Sun Yat-sen University, China.
[12] Xiao Ze. Research on computer network security analysis model [J]. *Journal On Communications*, **2012**(3):267