Network Security: Present and Future Trends

Anand Chopra[1], Jaswinder Singh Walia[2] , Lalit Kumar[3]
Department Of Computer Science And Engineering
GZS-PTU Campus, Bathinda(Pb), India
[1]anand005chopra@gmail.com
[2]jassiwalia001@gmail.com
[3]lalitjindal1234@gmail.com

Abstract- *Network Security has become an important part for PC users, organizations , various companies and also for the military. With the growing use of internet, security has also become a major concern. This is due to rise in the use of digital based work. However we can say that internet itself is responsible for various security threats. To save internet from these attacks we need network security. The entire field of network security is huge and always in an growing stage. The range study shows it's emphasis on the brief history of internet and network security and the current scenario in the field of network security. In order to understand the current research being held we need to understand the background of network security and various technologies included in it to make it a success and to save internet and network communication from various types of illegal access.*

Keyword- *Network Security,Data Secrecy,Integrity*

I. INTRODUCTION

The world is becoming more interconnected with the world of the Internet and new networking technology and at a faster rate. There is a large amount networking infrastructure available worldwide for personal, commercial, military, and government information. Because of Intellectual property Network security is gaining great importance through the internet but it is also followed by several problems like data secrecy, integrity, authentication and digital signature problems[1]. Data secrecy and integrity are the problems of secret and reliable data communication between two communicating devices.

There are two types of fundamentally different networks: data networks and synchronous network which mainly comprises of switches. The internet is considered a data network.

The Synchronus network are not threatened by the attackers.The topic of network security is depicted by the following [2]:

1. History of network security.
2. Internet architecture and various vulnerable security aspects of the Internet.
3. Types of internet attacks.
4. Various methods for networking security.
5. Network Security with internet access.
6. Current development in network security on the basis of hardware and software.

What is Network Security?

System and network technology is a key technology for a wide variety of applications. Security is crucial to networks and applications. Network security is a critical requirement in emerging networks. When considering network security, we must take care that the whole network is secure. Network security concerns the security in the computers at each end of the communication chain. When transmitting data we must take care that the communication channel should not be vulnerable to any kind of attack. A hacker could target the communication channel, obtain the data, decrypt it and re-insert a false message. Thus, Securing the network is just as important as securing the computers and encrypting the message.

When developing a secure network, the following need is to be considered[3]:

1. Access– Authorized users are provided the means to communicate to and from a particular network.
2. Confidentiality– Information in the network remains private.
3. Authentication – Ensure the users of the network are having the right identity.
4. Integrity – Ensure the message has not been modified when transported.
5. Non-repudiation – Ensure the user does not disagree that he used the network.

To make the computer less vulnerable any kind of attack there are many products available. These tools are encryption, firewalls, intrusion-detection, and security management and authentication mechanisms.

Kevin Mitnick committed the largest computer-related crime in U.S. history. The loss was of eighty million dollars in U.S. intellectual property[2]. Since then, information security came into the consideration. For financial and personal information Public networks are being followed. Companies are emphasizing security due to Kevin Mitnick's offence. Internet has proved to be the power booster for data security. Security protocols are not implemented in the TCP/IP communication stack and due to this internet is prone to various types of attacks. Due to recent high class developments in the internet world communication has become more secure.

The birth of the internet took place in 1969 by Advanced Research Projects Agency Network (ARPANET). TCP/IP, the common language of all Internet computers was created in 1980s by Bob Kahn, Vinton Cerf and by their team members[2]. Internet as we know it today was born from the collection of loose networks famously known as the ARPANET.

II. INTERNET ARCHITECTURE AND VARIOUS VULNERABLE SECURITY ASPECTS

Fear of security contravention on the Internet is causing organizations to use private networks or intranets. The Internet Engineering Task Force (IETF) has introduced various security mechanisms at various levels/layers of the IP Suite. These security help in the logical protection of data units that are being transferred across a particular network. The security architecture of the internet protocol is known as IP Security and it covers the new generation of IP (IPv6) as well as the current version (IPv4). Although new techniques, such as IPSec has been developed to overcome various deficiencies of internet. IPSec mainly is a point-to-point protocol in which one side encrypts and the other side decrypts and both sides share keys. IPSec can be used in two modes namely transport mode and tunnel modes. Particularly to determine various security mechanisms we need to first analyze the attacks that occur[1].

III. COMPARISON BETWEEN IPV4 AND IPV6

- IPV4 has only 2^{32} possible ways to represent the address whereas the number changes to 2^{128} in IPV6[4].
- Basic header length in IPV4 and IPV6 is 20 and 40 bytes respectively.
- IPV6 offers stateful and stateless address auto-configuration but IPV4 includes only stateful auto-configuration.
- IPV6 requires compulsory IPSec support but it is optional in IPV4.
- Security is limited in IPV4 but IPV6 is mainly designed to handle increasing need of network security.

IV. VARIOUS TYPES OF ATTACKS IN THE FIELD OF INTERNET

There are various types of internet attacks but are divided into various types of categories.

It may be the case when various attacks interfere with the system's intended functions which include various types of viruses, trojans and worms.

Various types of internet attacks include:

A. Eavesdropping

Any kind of obstruction in communication caused by unauthorized party is eavesdropping. There are two types of eavesdropping: passive and active. Passive eavesdropping is when the attacker only secretly listens to the messages and Active eavesdropping is when the attacker listens and inserts something into the communication stream and this leads to distortion of message.

B. Viruses

Viruses are self-replicated programs that use files to infect the entire system. Once a file is opened, the virus will activate within the system and may have adverse effect on the functioning of the system.

C. Phishing

Phishing is an attempt to obtain the secret information from an individual, group, or organization about a particular thing which should be kept confidential. Sometimes fake people like Phishers fool out users to disclose their personal data such as credit card numbers, online banking credentials and other sensitive information and then use this information for their own benefit.

D. IP Spoofing

IP Spoofing is a hijacking technique in which the attacker pretends to be an authorized user to hijack browsers and gain access of the network. The identity of the attacker is hidden by different means making detection and prevention difficult.

E. Denial of Service

Denial of Service is an attack when the system receiving too many requests cannot return communication to the requestors. The resources are then being consumed by the system waiting for the handshake to complete and eventually the system cannot respond to any more requests translating it without any service.

F. 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 [7].

1.Different types of DOS attacks

Many attacks are used to perform a DOS attack so as to disable service. Some of which are as follows:

TCP SYN Flooding: When a client wants to connect to the server, the client first sends to an SYN message to the server. The server then responds to the client by sending a SYN-ACK message to the client. The client completes the connection by sending an ACK message. The connection is now established and data can be transferred easily. The problem arises when the connections remain half open and the server waits for the client side to send an ACK message. This takes system resources and the server will wait till the expiration date. The person exploiting the server will never send the ACK message and will keep on sending new connection demand, till the server is overloaded, thus cannot provide access [8].

ICMP Smurf Flooding: ICMP package is used to know whether the server is responding or not. The server replies with an ICMP echo command. In smurf attack the attacking host forges the ICMP echo requests having victims address as the source and the broadcast address of remote networks. These computers will then send back ICMP echo reply package to source, thus congesting victim's network.

UDP Flooding: Many networks now use TCP and ICMP protocols to prevent DOS attacks but a hacker can send large number of packages as UDP overloading the victim and preventing any new connection.

V. VARIOUS TECHNOLOGIES FOR INTERNET SECURITY

Various kinds of attacks will continue as long as exchange of information takes place across the globe with the help of internet.

However certain technologies have been introduced to control these attacks. These technologies include.

A. CRYPTOGRAPHY

Cryptography is a useful tool used for internet security. It involves various ways to disguise the messages in order to avoid the interception from an unauthorized user. It involves the usage of codes and ciphers in order to transform the data.

B. FIREWALL

Firewall the incoming and outgoing network traffic based on applied rule set. A firewall establishes a barrier between a trusted internal network and another network. It is a front line defense mechanism against the attackers.

C. Anti-Malware Software and scanners

Viruses, worms and Trojan horses are all examples Malware that is found in our systems.

Special anti-Malware tools are used to detect them and cure an infected system. These software scan the system and detect the malware and just vanishes them out from our system to make it secure and healthy.

D. Secure Socket Layer (SSL)

The Secure Socket Layer (SSL) includes various suite protocols used for security between a web browser and a website. SSL is made to create a secure channel between a web browser and the server, so that any information which is being exchanged is protected within the secured channel. SSL provides authentication of clients to server only through the use of certificates.

E. 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 [6].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 [5].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. Firewalls can also perform real time evaluation of the traffic and take the necessary steps to prevent the attack. 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.

VI. CURRENT DEVELOPMENTS IN NETWORK SECURITY

Network Security has been working on the same terminologies for a while now but the use of biometrics has provided with a better method of authentication as compared to passwords. New technology mainly includes E-Banking, Mobile Security, Smart Cards. In software approach few new firewalls and encryption schemes help to maintain internet security. Network Security has Hardware and Software approach for it's further development.

A. Hardware Development

Hardware is not developed at a faster rate but however includes biometric systems and smart cards. Biometrics are used to secure various workstations logon when a workstation is connected to a network. Smart Cards are usually a credit card that is designed itself to store the encryption keys. The main motive is to provide unavoidable proof of user's identity. The cost of hardware devices mainly adds to it's widespread among various companies and organizations.

B. Software Development

This approach is very widely developed and also is further developing at a faster rate. It includes addition of new firewalls, antivirus and VPNs. The main motive is to obtain a good software for security purposes. Various examples of software development include E-banking, Mobile security systems etc.

However there is still need of further developments to improve network security. We may certainly need light weight security algorithms to take network security at a new level of success.

VII. FUTURE TRENDS IN NETWORK SECURITY

Various sets of new applications happens to be the future of network security. In future we will see that everybody will need network security and it will be considered as the immune system of the system. Network Security will fight off various types of network attacks and will help to keep the system protected from various attackers.

A. Cognitive Sensing

These sensing networks are used for a adapting a large amount of information and protecting it by rejecting those networks that could harm the information in many ways.

B. Underwater Acoustic Sensor Systems
Various kinds of underwater sensors are used to trace different scientific data that need to protected from unauthorized access. A GPS free routing protocol such as DUCS(Distributed Underwater Clustering Scheme) is used to minimize this illegal act by protecting data.

C. Security Intelligence
It shows the characteristic which is distributed on the enterprise network and provides on with various kinds of security applications and devices used to protect the data.

D. Scanning Engines
These are deployed across the physical network with integrated visibility, administration management and policy management helps to detect illicit access.

VIII. CONCLUSION

Network Security serves to be an important part of internet and is now growing at a faster rate. The security technology involves both software and hardware approaches growing instantly a good speed. Network Security sees it's future growing and helping to make the system free from any kind of unauthorized access. However Network Security predictions are going to be widespread with unpleasant attacks and growing danger. Being passionate about educating the users about smart security measures may help to improve the performance of network security and encouraging users to focus on "visibility is security".

IX. REFERENCES

1. Sanghavi P., Mehta K., Soni S., 2013, "*Network Security*", International Journal Of Scientific And Research Publications, Vol(3).

2. Sharma A.K., Soni T., Sharma S., 2014, "*Study of Network Security System with Digital Signature For High Security*", International Journal Of Informative And Futuristic Research, Vol(1).

3. Devi P.A., Lakshmi S.R., Sathiyavaishnavi K., 2013, "*A Study On Network Security Aspects And Attacking Methods*", International Journal Of P2P Network Trends And Technology, Vol(3).

4. Dr. Sharma S., 2014, "*Computer Networks-II*", Published under S.K. Kataria And Sons.

5. M. Kassim, "*An Analysis on Bandwidth Utilization and Traffic Pattern*," IACSIT Press, 2011.

6. M. Eian, "*Fragility of the Robust Security Network: 80211*," Norwegian University of Science and Technology.

7. Q. Gu, Peng Liu, "*Denial of Service Attacks*," Texas State University, San Marcos.

8. J. E. Canavan, "*Fundamentals of Network Security*", Artech House Telecommunications Library,
2000.