A Study on Network Security Aspects and Attacking Methods

P.Aruna Devi ,
Asst professor,
Dept of Computer Technology ,
Dr.SNS Rajalakshmi College of Arts and Science
Coimbatore-49.

S.Rani Laskhmi,
Asst professor,
Dept of Computer Technology ,
Dr.SNS Rajalakshmi College of Arts and Science
Coimbatore-49.

K.Sathiyavaishnavi,
Asst professor ,
Dept of Computer Technology ,
Dr.SNS Rajalakshmi College of Arts and Science
Coimbatore-49.

ABSTRACT

Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern and the history of security allows a better understanding of the emergence of security technology. The architecture of the internet, when modified can reduce the possible attacks that can be sent across the network. Knowing the attack methods, allows for the appropriate security to emerge. Many businesses secure themselves from the internet by means of firewalls and encryption mechanisms. The businesses create an "intranet" to remain connected to the internet but secured from possible threats. The entire field of network security is vast and in an evolutionary stage. In order to understand the research being performed today, background knowledge of the internet, its vulnerabilities, attack methods through the internet, and security technology is important and therefore they are reviewed.

KEYWORDS
Internet, Intranet, Attacks, Security, Open Systems Interface, Department of Defense, Denial Of Service, Secure Socket Layer, Virtual Private Networks, personal identification number

1. INTRODUCTION

The world is becoming more interconnected with the advent of the Internet and new networking technology. There is a large amount of personal, commercial, military, and government information on networking infrastructures worldwide.

There are currently two fundamentally different networks, data networks and synchronous network comprised of switches. The internet is considered a data network. Since the current data network consists of computer- based routers, information can be obtained by special programs, such as "Trojan horses," planted in the routers. The vast topic of network security is analyzed by researching the following:

1. History of security in networks
2. Internet architecture and vulnerable security aspects of the Internet
3. Types of internet attacks and security methods
4. Security for networks with internet access
5. Current development in network security hardware and software based on this research, the future of network security is forecasted

1.1 Network Security

System and network technology is a key technology for a wide variety of applications. Security is crucial to networks and applications. There exists a "communication gap" between the developers of security technology and developers of networks. Network design is a well- developed process that is based on the Open Systems Interface (OSI) model. The OSI model has several advantages when designing networks. It offers modularity, flexibility, ease- of- use, and standardization of protocols. When considering network security, it must be emphasized that the whole network is secure. When developing a secure network, the following need to be considered [1]:

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 who they say they are
4. Integrity – Ensure the message has not been modified in transit
5. Non repudiation – Ensure the user does not refute that he used the network.

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 [1].These tools are encryption, authentication mechanisms, intrusion- detection, security management and firewalls.

"Intranets" are both connected to the internet and reasonably protected from it.

Network intrusions consist of packets that are introduced to cause problems for the following reasons:

- To consume resources uselessly
- To interfere with any system resource's intended function
- To gain system knowledge that can be exploited in later attacks

1.2. Differentiating Data Security and Network Security

Data security is the aspect of security that allows a client's data to be transformed into unintelligible data for transmission. Strong cryptography in the past can be easily broken today. Cryptographic methods have to continue to advance due to the advancement of the hackers as well. When transferring cipher text over a network, it is helpful to have a secure network. A secure network will also prevent someone from inserting unauthorized messages into the network. Therefore, hard ciphers are needed as well as attack- hard networks [2].

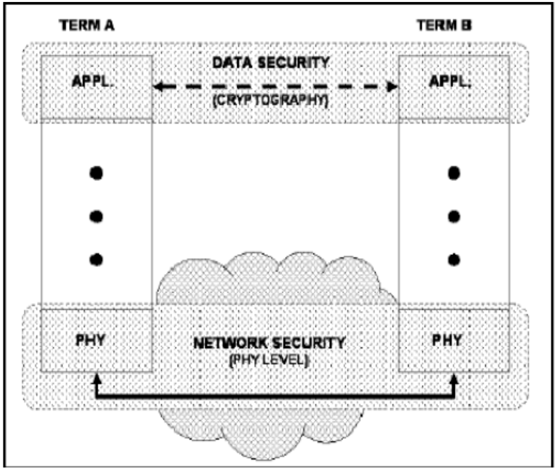


Figure 1: Based on the OSI model, data security and network security have a different security function [2].

The relationship of network security and data security to the OSI model is shown in Figure1.It can be seen that the cryptography occurs at the application layer; therefore the application writers are aware of its existence. Layers above the physical layers are also used to accomplish the network security required [2]. Authentication is performed on a layer above the physical layer.

2. 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 [3]. Public networks are being relied upon to deliver financial and personal information. 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.

2.1. Brief History of Internet

The birth of the internet takes place in 1969 when Advanced Research Projects Agency Network (ARPA Net) is commissioned by the Department of Defense (DOD) for research in networking. The ARPANET is a success from the very beginning. The ARPANET becomes a high- speed digital post office as people use it to collaborate on research projects and discuss topics of various interests. The Inter Networking Working Group becomes the first of several standards- setting entities to govern the growing network [10]. Vinton Cerf is elected the first chairman of the INWG, and later becomes known as a "Father of the Internet." [10] .In the 1980s, Bob Kahn and Vinton Cerf are key members of a team that create TCP/IP, the common language of all Internet computers.

2.2 Security Timeline

The timeline can be started as far back as the 1930s. Polish cryptographers created an enigma machine in 1918 that converted plain messages to encrypted text. In 1930, Alan Turing, a brilliant mathematician broke the code for the Enigma. In the 1960s, the term “hacker” is coined by a couple of Massachusetts Institute of Technology (MIT) students. The Department of Defense began the ARPA Net, which gains popularity as a conduit for the electronic exchange of data and information [3]. This paves the way for the creation of the carrier network known today as the Internet. During the 1970s, the Telnet protocol was developed.

In the 1990s, Internet became public and the security concerns increased tremendously. Approximately 950 million people use the internet today worldwide [3].

3. INTERNET ARCHITECTURE AND VULNERABLE SECURITY ASPECTS

Fear of security breaches on the Internet is causing organizations to use protected private networks or intranets [4]. The Internet Engineering Task Force (IETF) has introduced security mechanisms at various layers of the Internet Protocol Suite [4]. The security architecture of the internet protocol, known as IP Security, is a standardization of internet security. IP security, IPsec, covers the new generation of IP (IPv6) as well as the current version (IPv4). Although new techniques, such as IPsec, have been developed to overcome internet's best- known deficiencies, they seem to be insufficient [5]. Figure 2 shows a visual representation of how IPsec is implemented to provide secure communications.

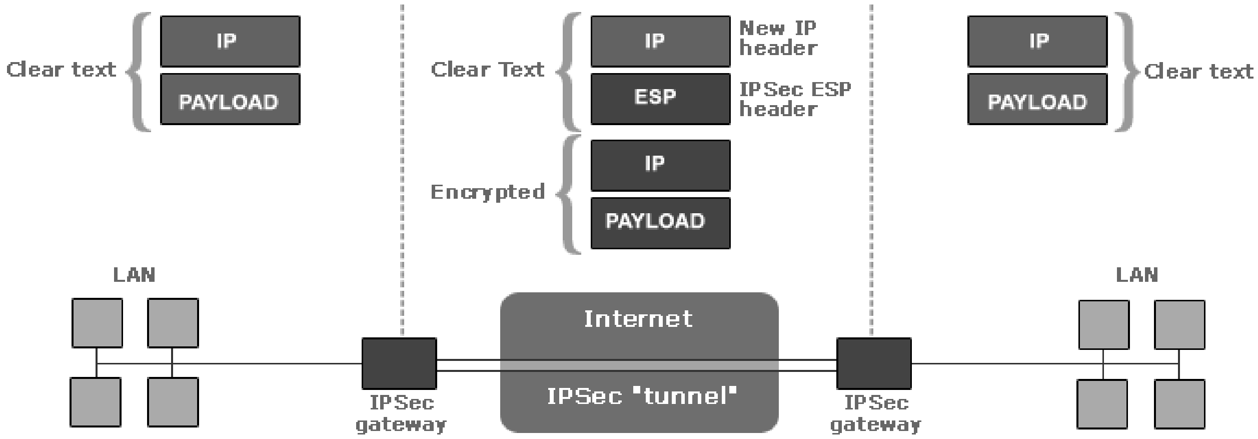


Figure 2: IPsec contains a gateway and a tunnel in order to secure communications.[17]

3.1. IPv4 and IPv6 Architectures

IPv4 was design in 1980 to replace the NCP protocol on the ARPANET. The IPv4 displayed many limitations after two decades [6]. The IPv6 protocol was designed with IPv4's shortcomings in mind. IPv6 is not a superset of the IPv4 protocol; instead it is a new design. The internet protocol's design is so vast and cannot be covered fully.

3.1.1 IPv4Architecture

The protocol contains a couple aspects which caused problems with its use. These problems do not all relate to security. The causes of problems with the protocol are:

1. Address Space
2. Routing
3. Configuration
4. Security
5. Quality of Service

The IPv4 architecture has an address that is 32 bits wide [6]. This limits the maximum number of computers that can be connected to the internet. The small address space of the IPv4 facilitates malicious code distribution [5].The maximum theoretical size of the global routing tables was 2.1 million entries [6].

The TCP/IP- based networking of IPv4 requires that the user supplies some data in order to configure a network. The user can request appropriate network configuration from a central server [6].IPsec is a specific mechanism used to secure the protocol. IPsec secures the packet payloads by means of cryptography. IPsec provides the services of confidentiality, integrity, and authentication [6].

3.1.2 IPv6 Architecture

When IPv6 was being developed, emphasis was placed on aspects of the IPv4 protocol that needed to be improved. The development efforts were placed in the following areas:

1. Routing and addressing
2. Multi- protocol architecture
3. Security architecture
4. Traffic control

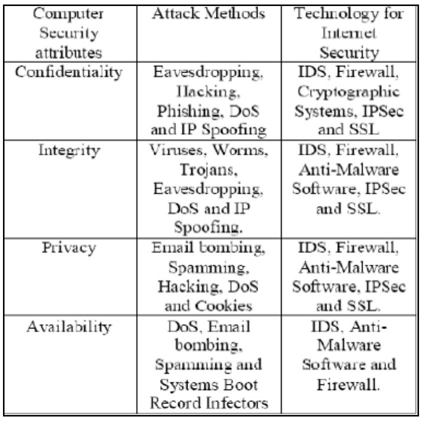
The IPv6 protocol's address space was extended by supporting 128 bit addresses. With 128 bit addresses, the protocol can support up to 3.4 *(10)^38 machines.

IPsec is embedded within the IPv6 protocol. IPsec functionality is the same for IPv4 and IPv6. The only difference is that IPv6 can utilize the security mechanism along the entire route [6].

4. ATTACKS THROUGH THE CURRENT INTERNET PROTOCOL IPV4

There are four main computer security attributes. These security attributes are confidentiality, integrity, privacy, and availability. Confidentiality and integrity still hold to the same definition. Availability means the computer assets can be accessed by authorized people [8]. Privacy is the right to protect personal secrets [8]. Various attack methods relate to these four security attributes. Table1 shows the attack methods and solutions.

Table 1: Attack Methods and Security Technology [8]



Computer Security attributes	Attack Methods	Technology for Internet Security
Confidentiality	Eavesdropping, Hacking, Phishing, DoS and IP Spoofing	IDS, Firewall, Cryptographic Systems, IPSec and SSL
Integrity	Viruses, Worms, Trojans, Eavesdropping, DoS and IP Spoofing.	IDS, Firewall, Anti-Malware Software, IPSec and SSL.
Privacy	Email bombing, Spamming, Hacking, DoS and Cookies	IDS, Firewall, Anti-Malware Software, IPSec and SSL.
Availability	DoS, Email bombing, Spamming and Systems Boot Record Infectors	IDS, Anti-Malware Software and Firewall.

4.1 Common Internet Attack Methods

Common internet attacks methods are broken down into categories. Some attacks gain system knowledge or personal information, such as eavesdropping and phishing. Attacks can also interfere with the system's intended function, such as viruses, worms and Trojans. The other form of attack is when the system's resources are consumes uselessly, these can be caused by Denial of Service (DoS) attack. Other forms of network intrusions also exist, such as land attacks, smurf attacks, and teardrop attacks. These attacks are not as well known as DoS attacks.

4.1.1 Eavesdropping

Interception of communications by an unauthorized party is called eavesdropping. Passive eavesdropping is when the person only secretly listens to the networked messages. On the other hand, active eavesdropping is when the intruder listens and inserts something into the communication stream. This can lead to the messages being distorted. Sensitive information can be stolen this way [8].

4.1.2 Viruses

Viruses are self- replication programs that use files to infect and propagate [8]. Once a file is opened, the virus will activate within the system.

4.1.3 Worms

A worm is similar to a virus because they both are self- replicating, but the worm does not require a file to allow it to propagate [8]. There are two main types of worms, mass- mailing worms and network- aware worms. Mass mailing worms use email as a means to infect other computers. Network- aware worms are a major problem for the Internet. A network- aware worm selects a target and once the worm accesses the target host, it can infect it by means of a Trojan or otherwise.

4.1.4 Trojans

Trojans appear to be benign programs to the user, but will actually have some malicious purpose. Trojans usually carry some payload such as a virus [8].

4.1.5 Phishing

Phishing is an attempt to obtain confidential information from an individual, group, or organization [9]. Phisher strick users into disclosing personal data, such as credit card numbers, online bank credentials, and other sensitive information.

4.1.6 IP Spoofing Attacks

Spoofing means to have the address of the Computer mirror the address of a trusted computer in order to gain access to other computers. The identity of the intruder is hidden by different means making detection and prevention difficult. With the current IP protocol technology, IP- spoofed packets cannot be eliminated [8].

4.1.7 Denial of Service

Denial of Service is an attack when the system receiving too many requests cannot return communication with the requestors [9]. The system then consumes resources waiting for the handshake to complete. Eventually, the system cannot respond to any more requests rendering it without service.

4.2 Technology for Internet Security

Internet threats will continue to be a major issue in the global world as long as information is accessible and transferred across the Internet. Different defense and detection mechanisms were developed to deal with these attacks.

4.2.1 Cryptographic systems

Cryptography is a useful and widely used tool in security engineering today. It involved the use of codes and ciphers to transform information into unintelligible data.

4.2.2 Firewall

A firewall is a typical border control mechanism or perimeter defense. The purpose of a firewall is to block traffic from the outside, but it could also be used to block traffic from the inside. A firewall is the front line defense mechanism against intruders.It is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both [8].

4.2.3 Intrusion Detection Systems

An Intrusion Detection System (IDS) is an additional protection measure that helps ward off computer intrusions. IDS systems can be software and hardware devices used to detect an attack. Some IDS systems just monitor and alert of an attack, whereas others try to block the attack.

4.2.4 Anti -Malware Software and scanners

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.

4.2.5 Secure Socket Layer (SSL)

The Secure Socket Layer (SSL) is a suite of protocols that is a standard way to achieve a good level of security between a web browser and a website. SSL is designed to create a secure channel, or tunnel, between a web browser and the web server, so that any information exchanged is protected within the secured tunnel. SSL provides authentication of clients to server through the use of certificates.

4.3. Security Issues of IP Protocol IPv6

From a security point of view, IPv6 is a considerable advancement over the IPv4 internet protocol. Despite the IPv6's great security mechanisms, it still continues to be vulnerable to threats. The possible security problems emerge due to the following [5]:

1. Header manipulation issues
2. Flooding issues
3. Mobility issues

Header manipulation issues arise due to the IPsec's embedded functionality [7]. Extension headers put off some common sources of attacks because of header manipulation.Spoofing continues to be a security threat on IPv6 protocol. A type of attack called port scanning occurs when a whole section of a network is scanned to find potential targets with open services [5].

5. SECURITY IN DIFFERENT NETWORKS

The businesses today use combinations of firewalls, encryption, and authentication mechanisms to create "intranets" that are connected to the internet but protected from it at the same time. Intranet is a private computer network that uses internet protocols. Intranets differ from "Extranets" in that the former are generally restricted to employees of the organization while extranets can generally be accessed by customers, suppliers, or other approved parties. When such access is provided it is usually through a gateway with a firewall, along with user authentication, encryption of messages, and often makes use of virtual private networks (VPNs).To keep the networks open, with these safeguards:

1. Firewalls that detect and report intrusion attempts
2. Sophisticated virus checking at the firewall
3. Enforced rules for employee opening of e- mail attachments
4. Encryption for all connections and data transfers
5. Authentication by synchronized, timed passwords or security certificates

VPN is a private network that uses a public network (usually the Internet)to connect remote sites or users together. Figure 3 is a graphical representation of an organization and VPN network.

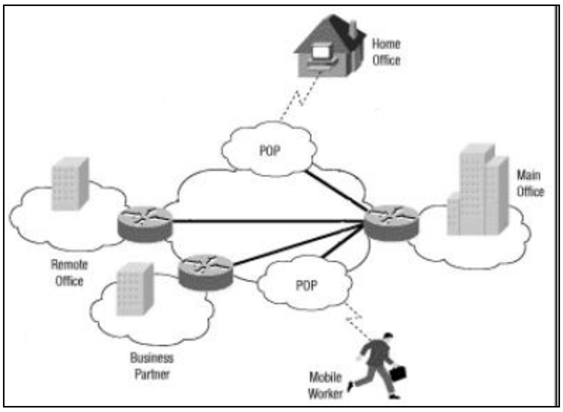


Figure 3: A typical VPN might have a main LAN at the corporate headquarters of a company, other LANs at remote offices or facilities and individual users connecting from out in the field.[14]

6. CURRENT DEVELOPMENTS IN NETWORK SECURITY

The network security field is continuing down the same route. The same methodologies are being used with the addition of biometric identification. 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.

6.1. Hardware Developments

Hardware developments are not developing rapidly. Biometric systems and smart cards are the only new hardware technologies that are widely impacting security. The most obvious use of biometrics for network security is for secure workstation logons for a workstation connected to a network. Each workstation requires some software support for biometric identification of the user as well as, depending on the biometric being used, some hardware device. The main use of Biometric network security will be to replace the current password system. Passwords have to be changed every few months and people forget their password or lock themselves out of the system by incorrectly entering their password repeatedly. Biometrics can replace this security identification method. Smart cards are usually a credit- card- sized digital electronic media. Smart cards can be used for everything from logging in to the network to providing secure Web communications and secure e- mail transactions. Smart cards require anyone who is using them to enter a personal identification number (PIN) before they'll be granted any level of access into the system. The PIN is similar to the PIN used by ATM machines. The PIN is verified from inside the smart card. The smart card is cost effective but not as secure as the biometric identification devices.

6.2. Software Developments

The software aspect of network security is very vast. It includes firewalls, antivirus, intrusion detection, and much more. The research development of all security software is not feasible to study at this point. The goal is to obtain a view of where the security software is heading based on emphasis being placed now. When new viruses emerge, the antivirus is updated to be able to guard against those threats.

7. FUTURE TRENDS IN SECURITY

What is going to drive the Internet security is the set of applications more than anything else. The future will possibly be that the security is similar to an immune system. The immune system fights off attacks and builds itself to fight tougher enemies. Many security developments that are taking place are within the same set of security technology that is being used today with some minor adjustments.

8. CONCLUSION

Network security is an important field that is increasingly gaining attention as the internet expands. The security threats and internet protocol were analyzed to determine the necessary security technology. The security technology is mostly software based, but many common hardware devices are used. The current development in network security is not very impressive. It was a surprise to see most of the development taking place in the same technologies being currently used. The embedded security of the new internet protocol IPv6 may provide many benefits to internet users. Combined use of IPv6 and security tools such as firewalls, intrusion detection, and authentication mechanisms will prove effective in guarding intellectual property for the near future. The network security field may have to evolve more rapidly to deal with the threats further in the future.

9. REFERENCES

[1] 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

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

[3] “Security Overview,” www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/security-guide/ch-sgs-ov.html.

[4] Molva, R., Institut Eurecom,“Internet Security Architecture,” in Computer Networks & ISDN Systems Journal, vol. 31, pp. 787-804, April 199913

[5] Sotillo, S., East Carolina University, “IPv6 security issues,” August 2006, www.infosecwriters.com/text_resources/pdf/IPv6_SSotillo.pdf.

[6] AndressJ., “IPv6:the next internet protocol,” April 2005, www.usenix.com/publications/login/2005-04/pdfs/andress0504.pdf.

[7] Warfield M., “Security Implications of IPv6,” Internet Security Systems White Paper,documents.iss.net/whitepapers/IPv6.pdf

[8] Adeyinka,O., "Internet Attack Methods and Internet Security Technology," Modeling&Simulation, 2008. AICMS 08. Second Asia International Conference on, vol., no., pp.77-82, 13-15 May 2008

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

[10] “Internet History Timeline,” www3.baylor.edu/~Sharon_P_Johnson/etg/inthistory.htm

[11] Landwehr, C.E.;Goldschlag,D.M., "Security issues in networks with Internet access," Proceedings of the IEEE, vol.85, no.12, pp.2034-2051,Dec 1997

[12] "Intranet." Wikipedia, The Free Encyclopedia. 23 Jun 2008, 10:43UTC. Wikimedia Foundation, Inc. 2 Jul 2008 <http://en.wikipedia.org/w/index.php?title=Intranet&oldid=221174244>.

[13] "Virtual private network."Wikipedia, The Free Encyclopedia. 30 Jun 2008, 19:32UTC. Wikimedia Foundation, Inc. 2 Jul 2008 <http://en.wikipedia.org/w/index.php?title=Virtual_private_network&oldid=222715612>.

[14] Tyson,J., ”How Virtual private networks work,” http://www.howstuffworks.com/vpn.htm.

[15] Al-Salqan, Y.Y., "Future trendsin Internet security," Distributed Computing Systems, 1997., Proceedings of the Sixth IEEE Computer Society Work shop on Future Trends of, vol., no., pp.216-217, 29-31Oct 1997

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

[17] “Improving Security,” Http://www.cert.org/tech_tips, 2006.

[18] Serpanos,D.N.; Voyiatzis, A.G., "Secure network design: A layered approach," Autonomous Decentralized System, 2002. The 2nd International Workshop on, vol., no., pp. 95-100, 6-7Nov. 2002

[19] Ohta, T.; Chikaraishi, T., "Network security model," Networks, 1993. International Conference on Information Engineering '93. 'Communications and Networks forthe Year 2000', Proceedings of IEEE Singapore International Conference on , vol.2, no., pp.507-511 vol.2, 6-11 Sep 1993