Internet Attacking Methods and Network Security Issues using IP Protocols

Divyashree S
M tech II Sem
Kalpataru Institute of Technology, Tiptur.
divyashrees2008@gmail.com

Vidyashree M
M tech II Sem
Kalpataru Institute of Technology, Tiptur.
vidyashreem224@gmail.com

***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. Social networking sites such as Facebook and Twitter have gained more popularity in recent years. Because of its large user base, and large amount of information, they become a potential channel for attackers to exploit. The internet structure itself allowed for many security threats to occur. 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. The range of study encompasses a brief history dating back to internet's beginnings and the current development in network security.**

Keywords- Confidentiality; ARPANET; Intrusion Detection Systems; Secure Socket Layer.

I. INTRODUCTION

The world is becoming more interconnected with the advent of the Internet and new networking technology. 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.

Network security is becoming of great importance because of intellectual property that can be easily acquired through the internet. 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 synchronous network that consists of switches does not buffer data and therefore are not threatened by attackers.

II. OVERVIEW OF NETWORK SECURITY GOALS

The primary goal of network security is to provide controls at all points along the network perimeter which allow access to the network and only let traffic pass if that is authorized, valid and of acceptable risk. The purpose of network security is to protect networks, network devices and network messages from unauthorized access, usually by outsiders. To provide control all points along the network perimeter in order to block network traffic that is malicious, unauthorized or that otherwise presents risk to the network. To detect and respond to attempted and actual intrusions through the network. To prevent network messages that is sent across networks from being intercepted or modified.

System and network technology is a key technology for a wide variety of applications. Security is crucial to networks and applications. Although, network security is a critical requirement in emerging networks, there is a significant lack of security methods that can be easily implemented. When developing a secure network, the following need to be considered [1]:

- Access authorized
- Confidentiality Authentication
- Integrity
- Non-repudiation

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]. The steps involved in understanding the composition of a secure network, internet or otherwise, is followed throughout this research endeavor. The types of attacks through the internet need to also be studied to be able to detect and guard against them. Intrusion detection systems are established based on the types of attacks most commonly used. 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

A. 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. Even if this unintelligible data is intercepted, a key is needed to decode the message. This method of security is effective to a certain degree. 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. This will allow for the cipher text to be protected, so that it is less likely for many people to even attempt to break the code. A secure network will also prevent someone from inserting unauthorized messages into the, hard ciphers are needed as well as attack shard network. Therefore networks [2].

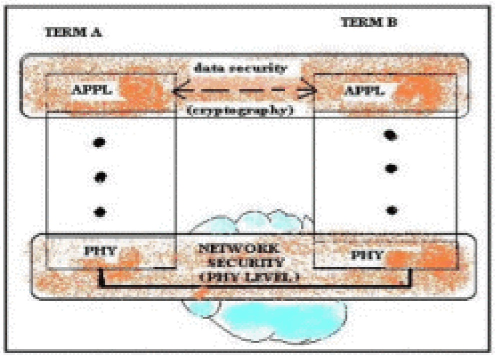

Fig.1. Based on the OSI model, data security and network security have a different security function [2].

The relationship of network security and data security to the OSI model is shown in Figure 1. It can be seen that the cryptography occurs at the application layer; therefore the application writers are aware of its existence. The user can possibly choose different methods of data security. Network security is mostly contained within the physical layer. Layers above the physical layer is also used to accomplish the network security required [2]. Authentication is performed on a layer above the physical layer. Network security in the physical layer requires failure detection, attack detection mechanisms, and intelligent counter measure strategies [2].

III. SECURITY ASPECTS AND INTERNET ARCHITECTURE

The security breaches on the Internet are causing organizations to use protected private networks or intranets [3]. The Internet Engineering Task Force (IETF) has introduced security mechanisms at various layers of the Internet Protocol Suite [3]. Network architecture is a set of high-level design principles that guide the technical design of a network, especially the engineering of its protocols and algorithms.

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 [4]. Figure 2 shows a visual representation of how IPsec is implemented to provide secure communications. IPsec is a point-to-point protocol, one side encrypts, the other decrypts and both sides share key or keys. IPsec can be used in two modes, namely transport mode and tunnel modes.

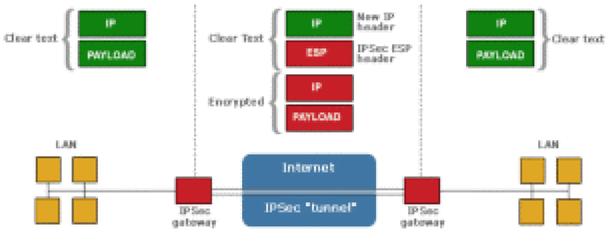

Fig.2. IPsec contains a gateway and a tunnel in order to secure communications.

A. 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 [5]. 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. The main parts of the architecture relating to security are discussed in detail.

Based on these considerations the proposed architecture will have the following points (see Fig. 3)

• *Network:* The network will work under Ethernet with a star topology which will be divided in two networks: Real-Time-IPv6 (RTV6) and Real- Time-V4 (RTV4). They will coexist by IPv4 tunnels.

• *Clients:* Clients in this model will be Laptops with Linux operating system that will be connected to the RTV6 network by a 1000 Mb switch (half duplex). These clients will have IPv6 addresses and clearance to access server information.

• *Tunneling:* Basically it will be an IPv4 tunnel which will connect our RTV6 router to the Campus' IPV6 router.

• *Application Software:* Software will consist of an application that will be monitoring in real time device activity via the SNMP protocol.

• *Security:* In this model a firewall will be used in the RTV6 router to control network access, also the IPSEC protocol could be used, for which IPv6 has special headers.

• *QoS:* One IPv6 advantage is that broadcast doesn't exist (rather multicasting is used). This avoids unnecessary traffic. Another advantage is that the use of label flow will considerably increase QoS.

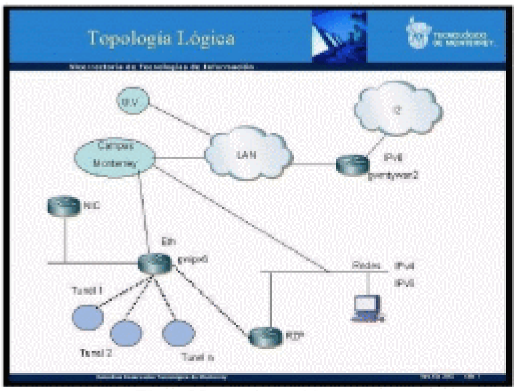

Fig.3. Network Architecture

a) *IPv4 Architecture*

The protocol contains a couple aspects which caused problems with its use. These problems do not all relate to security. They are mentioned to gain a comprehensive understanding of the internet protocol and its shortcomings. The causes of problems with the protocol are:

- Address Space
- Routing
- Configuration
- Security
- Quality of Service

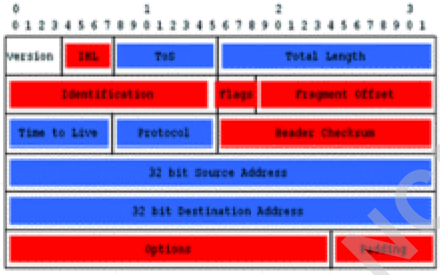

Fig.4. IPv4 Header Format

The IPv4 architecture is shown in Figure 4 has an address that is 32 bits wide [5]. This limits the maximum number of computers that can be connected to the internet. The 32 bit address provides for a maximum of two billions computers to be connected to the internet. The problem of exceeding that number was not foreseen when the protocol was created. The small address space of the IPv4 facilitates malicious code distribution [4].

Routing is a problem for this protocol because the routing tables are constantly increasing in size. Methods have been adopted to reduce the number of entries in the routing table. This is helpful for a short period of time, but drastic change needs to be made to address this problem.

The TCP/IP based networking of IPv4 requires that the user supplies some data in order to configure a network. Some of the information required is the IP address, routing gateway address, subnet mask, and DNS server. The simplicity of configuring the network is not evident in the IPv4 protocol. The user can request appropriate network configuration from a central server [5]. This eases configuration hassles for the user but not the network's administrators.

The lack of embedded security within the IPv4protocol has led to the many attacks seen today. Mechanisms to secure IPv4 do exist, but there are no requirements for their use [5]. 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 [5].This form of protection does not account for the skilled hacker who may be able to break the encryption method and obtain the key.

When internet was created, the quality of service(QoS) was standardized according to the information that was transferred across the network. The original transfer of information was mostly text based. As the internet expanded and technology evolved, other forms of communication began to be transmitted across the internet. The quality of service for streaming videos and music are much different than the standard text. The protocol does not have the functionality of dynamic QoS that changes based on the type of data being communicated [5].

b) *IPv6 Architecture*

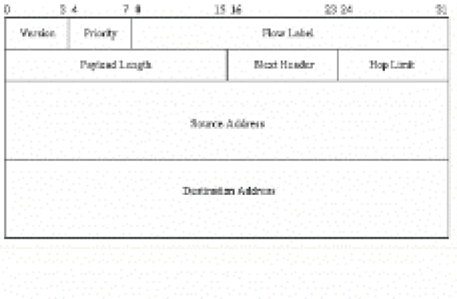

Fig.5. IPv6 Header Format

When IPv6 was being developed and shown in figure 5, emphasis was placed on aspects of the IPv4 protocol that needed to be improved. The development efforts were placed in the following areas:

- Routing and addressing
- Multi-protocol architecture
- Security architecture
- Traffic control

The security architecture of the IPv6 protocol is of great interest. IPsec is embedded within the IPv6protocol. IPsec functionality is the same for IPv4and IPv6. The only difference is that IPv6 can utilize the security mechanism along the entire route [5].The quality of service problem is handled with IPv6.

B. Attacks through the Current Internet Protocol IPv4

There are four main computer security attributes. They were mentioned before in a slightly different form, but are restated for convenience and emphasis. 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. Privacy is the right to protect personal secrets.

a) Common Internet Attack Methods

Common internet attacks methods are broken down into categories. Some attacks gain system knowledge or personal information, such as.

- *Eavesdropping*
- *Viruses*
- *Worms*
- *Trojans*
- *Phishing*
- *IP Spoofing Attacks*
- *Denial of Service*

b) 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.

- Cryptographic systems
- Firewall
- Intrusion Detection Systems
- Anti-Malware Software and scanners
- Secure Socket Layer (SSL)

c) 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. Some areas of the IPv6 protocol still pose a potential security issue. The new internet protocol does not protect against misconfigured servers, poorly designed applications, or poorly protected sites. The possible security problems emerge due to the following [4]:

- Header manipulation issues
- Flooding issues
- Mobility issues

Header manipulation issues arise due to the IPsec's embedded functionality [6]. Extension headers deter some common sources of attacks because of header manipulation. The problem is that extension headers need to be processed by all stacks, and this can lead to a long chain of extension headers.

A type of attack called port scanning occurs when a whole section of a network is scanned to find potential targets with open services [4]. The address space of the IPv6 protocol is large but the protocol is still not invulnerable to this type of attack. Mobility is a new feature that is incorporated in to the internet protocol IPv6.

IV. 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).

Although intranets can be set up quickly to share data in a controlled environment, that data is still at risk unless there is tight security. The disadvantage of a closed intranet is that vital data might not get into the hands of those who need it. Intranets have a place within agencies. But for broader data sharing, it might be better to keep the networks open, with these safeguards:

- Firewalls that detect and report intrusion attempts
- Sophisticated virus checking at the firewall
- Enforced rules for employee opening of email attachments

It was mentioned that if the intranet wanted access to the internet, virtual private networks are often used. Intranets that exist across multiple locations generally run over separate leased lines or a newer approach of VPN can be utilized. VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real world connection such as leased line, a VPN uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee. Figure 6 is a graphical representation of an organization and VPN network.

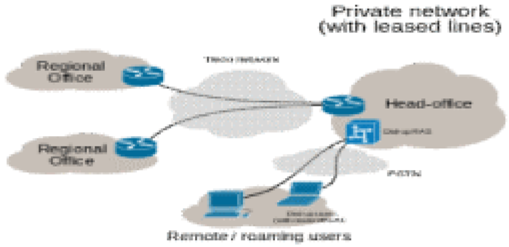

Fig.6. A typical VPN might have a main LAN at the corporate headquarters of a company, other LANs at remote offices or facilities and individual users connecting from out in the field.

V. NETWORK SECURITY IN CURRENT DEVELOPMENTS

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 h on network security.

A. Hardware Developments

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. Maintaining password security can be a major task for even a small organization.

Smart cards are usually a credit-card sized digital electronic media. The card itself is designed to store encryption keys and other information used in authentication and other identification processes. Smartcards can be used for everything from logging in to the network to providing secure Web communications and secure e-mail transactions.

PIN is similar to the PIN used by ATM machines .When a user inserts the smart card into the card reader, the smart card prompts the user for a PIN. This PIN was assigned to the user by the administrator at the time the administrator issued the card to the user. Because the PIN is short and purely numeric, the user should have no trouble remembering it and therefore would be unlikely to write the PIN down.

B. 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 improvement of the standard security software still remains the same. 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. 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.

VI. FUTURE TRENDS IN SECURITY

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. Similarly, the network security will be able to function as an immune system.

The trend towards biometrics could have taken place a while ago, but it seems that it isn't being actively pursued. Many security developments that are taking place are within the same set of security technology that is being used today with some minor adjustments.

VII. 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.

The embedded security of the new internet protocol IPv6 may provide many benefits to internet users. Although some security issues were observed, the IPv6internet protocol seems to evade many of the current popular attacks.

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.

REFERENCES

[1] Dowd, P.W.; McHenry, J.T., "Network security: it's time to take it seriously," Computer, vol.31, no.9, pp.2428, Sep 1998.

[2] Kartalopoulos, S. V., "Differentiating Data Security and Network Security," Communications, 2008. ICC '08.IEEE International Conference on, pp.14691473, 1923 May 2008.

[3] Molva, R., Institute Eurecom, Internet Security Architecture, in Computer Networks & ISDN Systems Journal, vol. 31, pp. 787804, April 1999.

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

[5] Andress J., IPv6: the next internet protocol, April2005, www.usenix.com/publications/login/200504/pdfs/andress0504.pdf.

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