ISSN 2348 - 7968

An Overview On Network Security

Ms Asiya Jaleel

M.Tech, Dept of CSE, Hyderabad.

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 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. Many businesses secure themselves from the internet by means of firewalls and encryption mechanisms.

This paper mainly Emphasis on Network Security and threats associated with it where 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. Security for networks with internet access
4. Current development in network security hardware and software

Based on this research, the future of network security is forecasted. New trends that are emerging will also be considered to understand where network security is secured.

Keywords: Ipv4, Ipv6, QoS, OSI, IPsec.

INTRODUCTION

System and network technology is a key technology for a wide variety of applications. Security is crucial to networks and applications. 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. The protocols of different layers can be easily combined to create stacks which allow modular development. The implementation of individual layers can be changed later without making other adjustments, allowing flexibility in development. 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, and decrypt it and re-insert a false message. Securing the network is just as important as securing the computers and encrypting the message. When developing a secure network, the following need to be considered:

1. Access – authorized users are provided the means to communicate to and from 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.

“Intranets” are connected to the internet and reasonably protected from it. The internet architecture itself leads to vulnerabilities in the network. Understanding the security issues of the internet greatly assists in developing new security technologies and approaches for networks with internet access and internet security itself.

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

1. HISTORY OF NETWORK SECURITY

The birth of the Internet takes place in 1969 when Advanced Research Projects

Agency Network (ARPANET) is commissioned by the department of Defence (DoD) for research in networking. The ARPANET is a success from the very beginning. Although originally designed to allow scientists to share data and access remote computers, e-mail quickly becomes the most popular application. 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. 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. For the first time the loose collection of networks which made up the ARPANET is seen as an "Internet", and the Internet as we know it today is born. The mid-80s marks a boom in the personal computer and super-minicomputer industries. The combination of inexpensive desktop machines and powerful, network-ready servers allows many companies to join the Internet for the first time. Corporations begin to use the Internet to communicate with each other and with their customers. In the 1990s, the internet began to become available to the public. The World Wide Web was born. Netscape and Microsoft were both competing on developing a browser for the internet. Internet continues to grow and surfing the internet has become equivalent to TV viewing for many users

2. INTERNET ARCHITECTURE AND VULNERABLE SECURITY ASPECTS OF THE INTERNET:

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. 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.

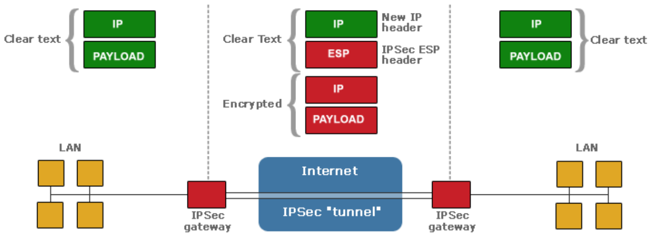

Figure1: IPsec contains a gateway and a tunnel in order to secure communications.

IPv4 Architecture :

The IPv4 architecture has an address that is 32 bits Wide. 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. Routing is a problem for this protocol because the routing tables are constantly increasing in size. The maximum theoretical size of the global routing tables was 2.1 million entries. 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. This eases configuration hassles for the user but not the network’s administrators. The lack of embedded security within the IPv4 protocol has led to the many attacks seen today. Mechanisms to secure IPv4 do exist, but there are no requirements for their use. 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. 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.

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. The address bits are used less efficiently in this protocol because it simplifies addressing configuration. The IPv6 routing system is more efficient and enables smaller global routing tables. The host configuration is also simplified. Hosts can automatically configure themselves. This new design allows ease of configuration for the user as well as network administrator. The security architecture of the IPv6 protocol is of great interest. 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. The quality of service problem is handled with IPv6. The internet protocol allows for special handling of certain packets with a higher quality of service. From a high-level view, the major benefits of IPv6 are its scalability and increased security. It must be emphasized that after researching IPv6 and its security features, it is not necessarily more secure than IPv4.

3. 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. There does not necessarily have to be any access from the organization's internal network to the Internet itself. 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.

Intranets have a place within agencies. But for broader data sharing, it might be better 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 email attachments
4. Encryption for all connections and data transfers
5. Authentication by synchronized, timed passwords or security certificates

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 2 is a graphical representation of an organization and VPN network.

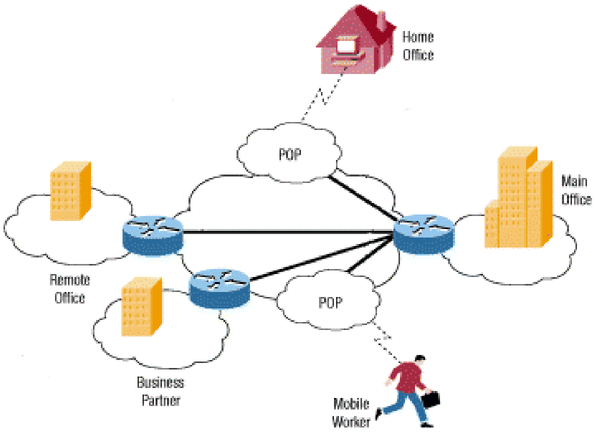

Figure 2: A typical VPN might have a main LAN at the corporate headquarters of a company, other LANs at remote offices or facilities and individual users connecting from out in the field.

4. CURRENT DEVELOPMENT IN NETWORK SECURITY HARDWARE AND SOFTWARE

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 cost of hardware devices is one thing that may lead to the widespread use of voice biometric security identification, especially among companies and organizations on a low budget. Hardware device such as computer mice with built in thumbprint readers would be the next step up. These devices would be more expensive to implement on several computers, as each machine would require its own hardware device. The advantage of voice recognition software is that it can be centralized, thus reducing the cost of implementation per machine. 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. 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. Very often people write their password down and keep it near their computer. This is of course completely undermines any effort at network security. Biometrics can replace this security identification method. The use of biometric identification stops this problem and while it may be expensive to set up at first, these devices save on administration and user assistance costs. 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. 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. It may seem that smart cards are nothing more than a repository for storing passwords. Obviously, someone can easily steal a smart card from someone else. Fortunately, there are safety features built into smart cards to prevent someone from using a stolen card. 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. 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. But the interesting thing is what happens when the user inputs the PIN. The PIN is verified from inside the smart card. Because the PIN is never transmitted across the network, there's absolutely no danger of it being intercepted. The main benefit, though, is that the PIN is useless without the smart card, and the smart card is useless without the PIN. There are other security issues of the smart card. The smart card is cost-effective but not as secure as the biometric identification devices.

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. 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. 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.

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. 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.

Future:

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.

References:

1. **www.google.com.**
2. **www.wikipedia.org/wiki/Network_security.**
3. **www.redhat.com/docs/manuals/enterprise/RHE.**
   www.nist.gov/.../AT-T_APENDIX_A_ATTSecurity_Customer_Refere...
4. **www.vtcif.telstra.com.au/info/security.html**
5. **http://www.cert.org/tech_tips, 2006**
6. **http://www.interhack.net/pubs/network-security.http://www.howstuffworks.com/vpn.htm .**
7. **www3.baylor.edu/~Sharon_P_Johnson/etg/inthistory.**