ISSN No:-2456-2165

Computer Network Security

Narendra Kumar Chahar
Assistant Professor
Department of Computer Science and Engineering
Jayoti Vidyapeeth Women's University, Jaipur

Abstract:- Network security is becoming increasingly important to personal computer users, businesses, and the military. Security became a major concern with the advent of the internet, and understanding the history of security allows a better understanding of the emergence of security technology. Many security threats can occur due to the structure of the internet. If the internet's architecture is changed, it can reduce the number of possible attacks that can be sent across the network. Knowing the attack methods enables us to respond with adequate security. Many businesses use firewalls and encryption mechanisms to protect themselves from the internet. To stay connected to the internet, businesses create an "intranet."

Keywords:- *Data Security, Network Security, IPv4, IPv6, Internet Architecture.*

I. INTRODUCTION

Because of the Internet and new networking technology, the world is becoming more interconnected. Worldwide, there is a wealth of personal, commercial, military, and government information on networking infrastructures. Because of the ease with which intellectual property can be acquired via the internet, network security is becoming increasingly important. Intellectual property can be violated. There are two types of networks: data networks and synchronous networks comprised of switches.

The internet is classified as a data network. Because the current data network is made up of computer-based routers, special programmes, such as "Trojan horses," planted in the routers, can obtain information. Because the synchronous network, which is made up of switches, does not buffer data, it is not vulnerable to attackers. That is why data networks, such as the internet, and other networks that connect to the internet, place a premium on security.

The vast topic of network security is investigated by investigating the following:

- Internet architecture and vulnerable Internet security aspects
- Internet attack types and security measures
- Network security for internet-connected networks
- Current network security hardware and software development.

II. NETWORK SECURITY

System and network technology is essential for a wide range of applications. Security is required for networks and applications. Despite the fact that network security is a critical requirement, there is a significant lack of security methods that can be easily implemented.

There is a "communication gap" between security technology developers and network developers. The Open Systems Interface (OSI) model underpins network design, which is a well-developed process. Different layer protocols can be easily combined to form stacks that allow for modular development. Individual layer implementations can be changed later without affecting other layers, allowing for development flexibility. Secure network design, in contrast to network design, is not a well-developed process. There is no methodology for dealing with the complexities of security requirements. Secure network design does not provide the same benefits as network design.

Network security does not imply securing both ends of the network. The communication channel should not be vulnerable to attack when transmitting data. A potential hacker could target the communication channel, obtain the encrypted data, decrypt it, and then reintroduce a false message. It is just as important to secure the middle network as it is to secure the computers and encrypt the message.

When designing a secure network, the following factors must be considered:

- Access– Authorized users are given the ability to communicate to and from a specific network.
- Confidentiality– Data in the network is kept private.
- Authentication – Ensure that network users are who they claim to be.
- Integrity – Ensure that the message has not been altered in transit.
- Nonrepudiation – Ensure that the user does not deny using the network.

An effective network security plan is developed with an understanding of security issues, potential attackers, required level of security, and factors that make a network vulnerable to attack. There are numerous products available to make the computer less vulnerable to network attacks. Encryption, firewalls, intrusion detection, security management, and authentication mechanisms are examples of these tools. Businesses all over the world use a combination of some of these tools. "Intranets" are both connected to and reasonably protected from the internet.

The internet architecture itself is at the helm as a result of network flaws Understanding internet security issues

greatly aids in the development of secure solutions to protect networks from the internet.

The types of internet attacks must also be studied in order to detect and defend against them. Intrusion detection systems are built around the most common types of attacks. In network intrusions, packets are introduced to cause problems for the following reasons:

- Not a proper use of resources
- Interfering with the intended function of any system resource
- Gaining system knowledge such as passwords and logins that can be used in later attacks.

III. DIFFERENCE BETWEEN DATA SECURITY AND NETWORK SECURITY

Data security is the aspect of security that allows a client's data to be converted into incomprehensible data for transmission. Even if this unintelligible data is intercepted, decoding the message requires a key. To some extent, this security method is effective. In the past, strong cryptography was easily broken; however, this is no longer the case. Due to the advancement of hackers, cryptographic methods must constantly evolve in order to stay one step ahead.

It is advantageous to use a secure network when transferring cypher text over a network. This will protect the cypher text, making it less likely that many people will attempt to break the code. A secure network will also prevent unauthorized messages from being inserted into the network. As a result, hard cyphers and attack hard networks are required.

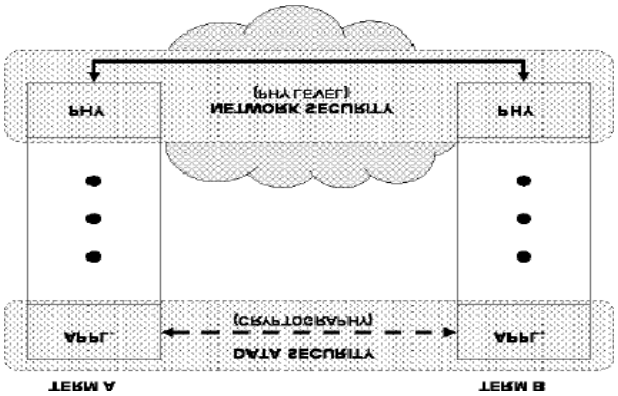

Fig. 1

Figure 1 depicts the relationship between network security and data security and the OSI model. Because cryptography takes place at the application layer, application writers are aware of its existence. The user may select from a variety of data security methods. The physical layer is primarily responsible for network security. Layers above the physical layer are also used to achieve the required network security. Authentication takes place on a layer that is above the physical layer. Physical layer network security necessitates failure detection, attack detection mechanisms, and intelligent countermeasure strategies.

IV. VULNERABLE SECURITY ASPECTS IN INTERNET ARCHITECTURE

Organizations are using protected private networks or intranets due to concerns about security breaches on the Internet. The Internet Engineering Task Force (IETF) has added security mechanisms to the Internet Protocol Suite at various layers. These security mechanisms enable the logical protection of data units as they travel across the network. The security implications of the current and new versions of the Internet Protocol are assessed. Although security exists within the protocol, not all attacks are protected. These attacks are examined in order to determine whether additional security measures are required.

The IP Security architecture of the internet protocol is a standardization of internet security. IP security, or IP sec, refers to both the new generation of IP (IPv6) and the current version (IPv4). Although new techniques, such as IP sec, have been developed to address some of the internet's most well-known shortcomings, they appear to be insufficient.

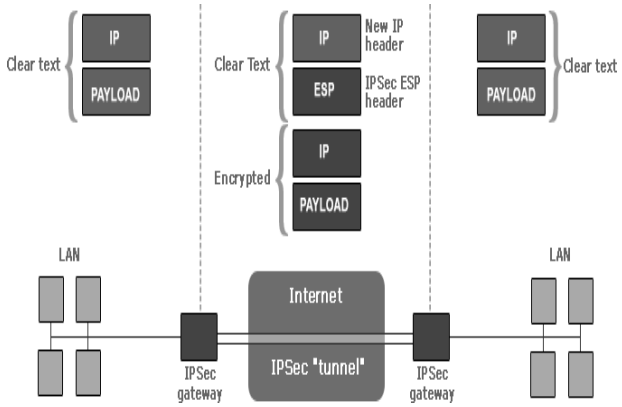

Fig. 2: Visual representation of IPsec implementation to provide secure communications

IPsec is a point-to-point protocol in which one side encrypts, the other side decrypts, and both sides share the same key or keys. IPsec has two modes of operation: transport mode and tunnel mode.

V. ATTACKS THROUGH IPV4 AND SECURITY ISSUES IN IPV6

A. Common Internet Attack Methods

The most common internet attack methods are classified. Some attacks, such as eavesdropping and phishing, gain system knowledge or personal information. Attacks are possible.

Viruses, worms, and trojans can also interfere with the system's intended function. Another type of attack is when the system's resources are used inefficiently, which can be caused by a denial of service (DoS) attack. Other types of network intrusions include land attacks, surf attacks, and teardrop attacks.

These attacks aren't as well-known as DoS attacks, but they're still used in some form or another, even if they're not mentioned by name.

- Viruses: Viruses are self-replicating programmes that infect and spread through files [8]. When a file is opened, the virus enters the system and becomes active.
- Trojans: Trojans may appear to the user to be harmless programmes, but they will actually serve a malicious purpose. Trojans typically transport a payload, such as a virus [8].
- Eavesdropping: Eavesdropping is the act of intercepting communications by an unauthorized party. Passive eavesdropping occurs when a person only listens in secret to networked messages. Active eavesdropping, on the other hand, occurs when the intruder listens and inserts something into the communication stream. As a result, the messages may become distorted. This method can be used to steal sensitive information [8].
- Phishing: The attempt to obtain confidential information from an individual, group, or organization is known as phishing [9]. Phishers trick users into disclosing sensitive information such as credit card numbers, online banking credentials, and other personal information.
- Denial of service: Denial of Service is an attack that occurs when a system receives an excessive number of requests and is unable to communicate with the requestors [9]. While waiting for the handshake to complete, the system consumes resources. Eventually, the system will be unable to respond to any further requests, rendering it inoperable.
- IP Spoofing: Spoofing means having the computer's address mirror the address of a trusted computer in order to gain access to other computers. The identity of the intruder is concealed in various ways, making detection and prevention difficult. IP spoofed packets cannot be eliminated with current IP protocol technology [8].

B. Internet Security Technologies

Internet threats will continue to be a major concern in the global community as long as information can be accessed and transferred via the Internet. To deal with these attacks, various defense and detection mechanisms were developed.

- Firewall: A firewall is a common border control or perimeter defense mechanism. A firewall's purpose is to block traffic from the outside, but it can also be used to block traffic from the inside. A firewall is the first line of defense against intruders. It's a system that prevents unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or in a hybrid of the two [8].
- Cryptographic Systems: Today, cryptography is a valuable and widely used tool in security engineering. It entailed the use of codes and cyphers to convert information into incomprehensible data. As a result, this unintelligible data is safely transferred across the network.
- Secure Socket Layer: The Secure Socket Layer (SSL) protocol suite is a standard method for achieving a high level of security between a web browser and a website. SSL is intended to create a secure channel, or tunnel, between a web browser and a web server, so that any information exchanged within the secured tunnel is protected. Through the use of certificates, SSL allows clients to authenticate to servers. To prove their identity, clients present a certificate to the server.
- Intrusion Detection System: An Intrusion Detection System (IDS) is an additional security measure that aids in the prevention of computer intrusions. IDS systems can be both software and hardware devices that detect attacks. IDS products are used to monitor connections in order to determine whether or not attacks have been launched. Some intrusion detection systems (IDS) simply monitor and alert when an attack occurs, whereas others attempt to prevent the attack.

VI. SECURITY IN COMPUTER NETWORK

The network security field is following in the footsteps of its predecessors. With the addition of biometric identification, the same methodologies are used. Biometrics is a more secure method of authentication than passwords. This could significantly reduce unauthorized access to secure systems. The software aspect of network security is constantly evolving. New firewalls and encryption schemes are constantly being implemented. The research being conducted aids in understanding current developments as well as projecting future developments in the field. There are two main deployments are defined in the network security as Software Deployment and Hardware Deployment.

VII. FUTURE SCOPE OF NETWORK SECURITY

The set of applications will influence Internet security more than anything else. In the future, security may resemble as an immune system. The immune system defends against attacks and prepares itself to face more difficult foes. Similarly, network security will be able to serve as an immune system.

The biometrics movement may have begun some time ago, but it does not appear to be aggressively pursued. Many security developments are occurring inside the same set of security technology that is now in use, with minimal alterations. After so many years of evolution, there are some loopholes i.e., bypassing or altering the security measures that needed to change and must be secured. Multiple levels of security measures can prevent them.

VIII. CONCLUSION

Network security is an essential area that is gaining traction as the internet grows in size. To evaluate the necessary changes in security technology, the security threats and internet protocol were analyzed. The majority of security technology is software-based, but several common hardware devices are included. The current state of network security is unimpressive.

With the importance of the network security area, it was believed that new approaches to security, both hardware and software, would be actively investigated. It was surprising to realize that the majority of the progress was taking place in the same technologies that are already in use.

In the near future, the combination of IPv6 and security measures such as firewalls, intrusion detection, and authentication procedures will be successful in protecting

intellectual property. To deal with future dangers, the network security area may need to evolve more quickly.

REFERENCES

[1.] Dowd,P.W.;McHenry,J.T.,"Networksecurity:it'stimetotakeitseriously,"Computer, vol.31,no.9, pp.24-28,Sep1998
[2.] Kartalopoulos, S. V., "Differentiating Data Security and Network Security,"Communications,2008.ICC'08.IEEEInternationalConferenceon,pp.1469-1473,19-23May2008
[3.] "SecurityOverview," www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/security-guide/ch-sgs-ov.html.
[4.] Molva, R., Institut Eurecom,"Internet Security Architecture," in ComputerNetworks&ISDNSystemsJournal, vol. 31,pp.787-804, April1999
[5.] Sotillo, S., East Carolina University, "IPv6 security issues," August 2006,www.infosecwriters.com/text_resources/pdf/IPv6_SSotillo.pdf.
[6.] Warfield M., "Security Implications of IPv6," Internet Security SystemsWhitePaper,documents.iss.net/whitepapers/IPv6.pdf
[7.] AndressJ.,"IPv6:thenextinternetprotocol,"April2005,www.usenix.com/publications/login/2005-04/pdfs/andress0504.pdf.
[8.] Adeyinka, O., "Internet Attack Methods and Internet Security Technology,"Modeling&Simulation,2008.AICMS08.SecondAsiaInternationalConferenceon,vol.,no.,pp.77-82,13-15May2008
[9.] Marin, G.A., "Network security basics," Security & Privacy, IEEE, vol.3,no.6,pp.68-72,Nov.-Dec.2005
[10.] Priyank Sanghavi, Kreena Mehta, "Network Security", IJSRP, http://www.ijsrp.org/research-paper-0813/ijsrp-p20131.pdf
[11.] Dr. Pradosh Chandra Patnaik, "Network Security: Concepts and Various Aspects for Treating the Attacks", IJSDR2102055