Network Security: Concepts and Various Aspects for Treating the Attacks

Dr. Pradosh Chandra Patnaik

Associate Professor and Head, Dept. of CSE,
Aurora's Scientific, Technological and Research Academy, Hyderabad.

***Abstract*: Personal computer users, companies, and the military are all becoming more concerned about network security. With the arrival of the internet, security became a major concern, and understanding the history of security provides a better understanding of the development of security technologies. Because of the internet's structure, several security problems can arise. If the internet's architecture is altered, the number of possible attacks that may be transmitted across the network is reduced. We can respond with proper protection if we understand the attack strategies. To protect themselves from the internet, several companies utilize firewalls and encryption measures. Businesses create an intranet to stay connected to the internet while guarding against potential threats. The field of network security is vast and ever-changing. To appreciate the study being undertaken today, background knowledge of the internet, its vulnerabilities, internet-based attack strategies, and security technology is required, and this knowledge is reviewed.**

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

I. INTRODUCTION

The world is getting increasingly interconnected as a result of the Internet and new networking technology. There is a multitude of personal, economic, military, and government data on networking infrastructures available around the world. Network security is becoming increasingly critical due to the ease with which intellectual property can be gained via the internet. Intellectual property rights could be infringed upon. Data networks and synchronous networks consisting of switches are two types of networks that are fundamentally different. A data network is what the internet is. Because the current data network is made up of computer-based routers, malicious software, such as "Trojan horses," can gain access to data. The synchronous network of switches is not vulnerable to attackers since it does not buffer data. That's why data networks like the internet, as well as other networks that connect to it, prioritise security. The wide topic of network security is investigated by investigating the following:

1. Internet architecture and vulnerable Internet security features
2. Internet attack types and protection measures
3. Network security for internet-connected networks
4. Recent advancements in network security hardware and software

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 vital necessity, there is a substantial dearth of security approaches that can be simply deployed. 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 procedure. Different layer protocols can be simply joined to form stacks that allow for modular development. Individual layer implementations can be altered later without affecting other layers, allowing for development flexibility. Secure network design, in contrast to network design, is not a well-developed procedure. There is no approach for dealing with the complexities of security requirements. The advantages of secure network design are not the same as those of network design. Network security does not include safeguarding both ends of the network. The communication channel should not be vulnerable to attack when transmitting data. A potential hacker may target the communication route, steal the encrypted data, decrypt it, and then reintroduce a fake message. It is just as critical to secure the intermediary network as it is to secure the computers and encrypt the communication.

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”

“With the understanding of security issues, potential attackers, needed level of security, and factors that make a network vulnerable to attack an effective network security plan is developed” [1]. There are numerous products available to make the PC less vulnerable to network attacks. These tools include encryption, firewalls, intrusion detection, security management, and authentication mechanisms. Businesses all across the world use a combination of several of these technologies. “Intranets” are both connected to and reasonably secured from the internet. The internet architecture inherently causes network vulnerabilities. Understanding internet security challenges tremendously aids in the development of safe solutions to protect networks from the internet.

The forms of internet attacks must also be understood in order to recognise and defend against them. Intrusion detection systems are built around the most frequent sorts of assaults. In network intrusions, packets are injected to cause issues for the following reasons:

Consuming resources ineffectively interfering with any system resource's intended purpose gaining system knowledge such as passwords and logins that can be abused in later attacks

III. DIFFERENTIATING DATA SECURITY AND NETWORK SECURITY

Data security is the feature of security that permits a client's data to be converted into incomprehensible data for transmission. Even if this nonsensical data is intercepted, decoding the message requires a key. To some extent, this security mechanism is effective. In the past, strong cryptography was easily broken; however, this is no longer the case. Due to the progress of hackers, cryptographic systems must always evolve in order to stay one step ahead.

It is advantageous to use a secure network while exchanging encrypted text over a network. This will secure the cypher text, making it less likely that many people will attempt to break the encryption. 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.

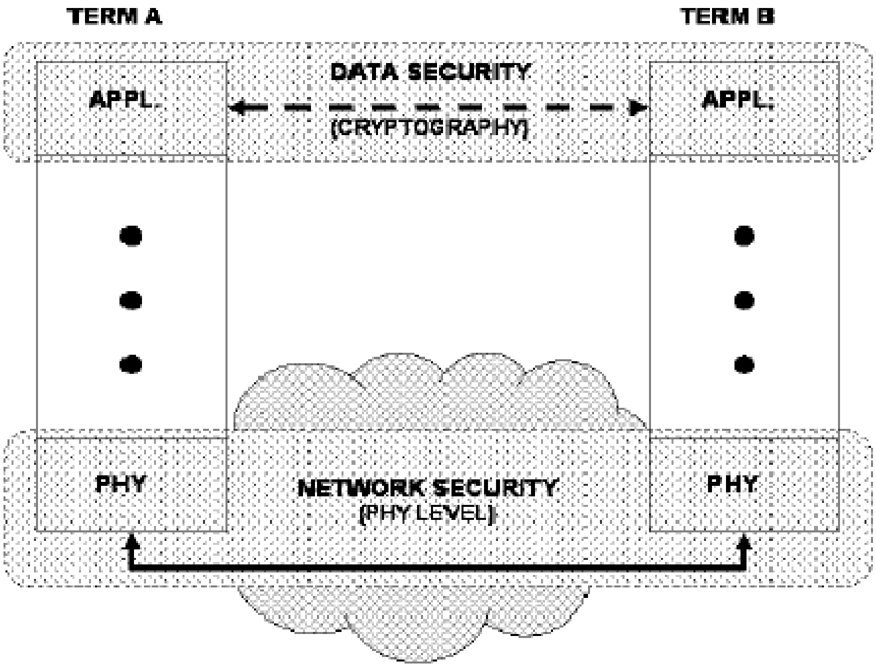

Fig.1: The relationship of network security and data security

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 measures. The physical layer is primarily responsible for network security. Layers above the physical layer are also utilised to achieve network security. “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].

IV. INTERNET ARCHITECTURE AND VULNERABLE SECURITY ASPECTS

“Fear of security breaches on the Internet is causing organizations to use protected private networks or intranets. The Internet Engineering Task Force (IETF) has introduced security mechanisms at various layers of the Internet Protocol Suite” [4]. These security measures provide the logical protection of data units as they travel through the network. The security implications of the present and new versions of the Internet Protocol are assessed. Although security exists inside the protocol, not all assaults are protected. These assaults are examined in order to determine whether additional security measures are required.

“The security architecture of the internet protocol known as IP Security is a standardization of internet security. IP security, IP sec, covers the new generation of IP (IPv6) as well as the current version (IPv4). Although new techniques, such as IP sec, have been developed to overcome internet’s best-known deficiencies, they seem to be insufficient” [5].

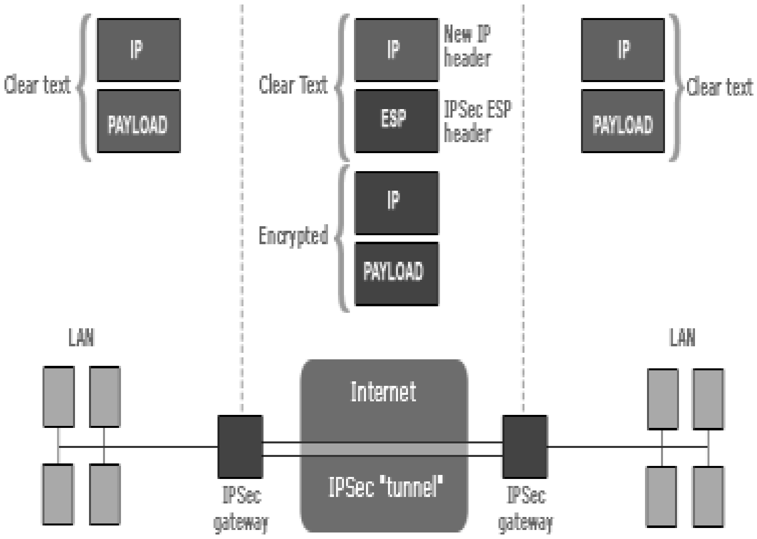

Fig. 2: Visual Representation of IPsec to Provide Secure Communications

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 THE CURRENT INTERNET PROTOCOL IPV4

1. Common Internet Attack Methods

The most common internet attack tactics are classified. Some attacks, such as eavesdropping and phishing, gather system knowledge or personal information. Viruses, worms, and trojans are examples of attacks that can disrupt the system's intended operation. The other type of assault is when the system's resources are wasted, which can be produced by a denial of service (DoS) attack. Other types of network intrusions include land attacks, surf attacks, and teardrop attacks. These attacks are not as well-known as DoS attacks, but they are utilised in some form or another even if they are not named.

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 eaves dropping are 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].

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.

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]. Worms are classified into two types: mass mailing worms and network aware worms. Email is used by mass mailing worms to infect other systems. Worms that are network aware are a serious issue for the Internet. A network aware worm chooses a target, and once inside the target host, it can infect it with a Trojan or otherwise.

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].

1.5 Phishing

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

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].

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.

2. Technology for Internet Security

Internet risks will continue to be a big concern in the global community as long as information can be accessed and exchanged via the Internet. To deal with these attacks, various defensive and detection techniques were created.

2.1 Cryptographic systems

Today, cryptography is a valuable and commonly utilised technology in security engineering. It entailed the use of codes and cyphers to convert information into incomprehensible data. As a result, this nonsensical data is safely transported across the network.

2.2 Firewall

A firewall is a common border control or perimeter defence system. A firewall's function is to restrict traffic from the outside, but it can also be used to block traffic from the inside. A firewall is the first line of defence against invaders. It's a system that prevents illegal access to or from a private network. “Firewalls can be implemented in both hardware and software, or a combination of both”[8].

2.3 Intrusion Detection Systems

An Intrusion Detection System (IDS) is an extra security mechanism that aids in the prevention of computer invasions. 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 conducted. Some intrusion detection systems (IDS) just monitor and alarm when an attack occurs, whilst others attempt to prevent the attack.

2.4 Anti-Malware Software and Scanners

Malware, sometimes known as malicious software, includes viruses, worms, and Trojan horses. To detect and treat an infected machine, certain anti Malware programs are used.

2.5 Secure Socket Layer (SSL)

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 establish a secure channel, or tunnel, between a web browser and a web server, ensuring that any information sent is secure within the secured tunnel. Through the use of certificates, SSL allows clients to authenticate to servers. To authenticate their identity, clients provide a certificate to the server.

VI. SECURITY ISSUES OF IP PROTOCOL IPV6

Everyone is talking about IPv6 right now. In terms of security, IPv6 is a significant advancement over the IPv4 internet protocol. However, despite its excellent security features, IPv6 remains vulnerable to threats. Some aspects of the IPv6 protocol continue to represent a security risk. The new internet protocol does not guard against incorrectly configured servers, poorly designed apps, or insecure websites.

The possible security problems emerge due to the following:

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

“Header manipulation issues arise due to the IPsec’s embedded functionality” [7]. 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. The large number of extension headers can overwhelm a certain node and is a form of attack if it is deliberate. 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]. The IPv6 protocol has a wide address space, yet it is still vulnerable to this type of attack. Mobility is a new feature built into the internet protocol IPv6. The feature necessitates additional security procedures. When utilizing IPv6's mobility capability, network managers must be aware of these security requirements.

VII. SECURITY IN DIFFERENT NETWORKS

Businesses today utilize a combination of firewalls, encryption, and authentication systems to build "intranets" that are both connected to and shielded from the internet. A private computer network that uses internet protocols is known as an intranet. Intranets differ from "Extranets" in that the former are often restricted to organisation workers, whereas extranets can be accessible by customers, suppliers, or other allowed parties. There does not have to be any access to the Internet from the organization's internal network. When such access is offered, it is normally through a gateway with a firewall, as well as user authentication, message encryption, and the use of virtual private networks (VPNs). Although intranets may be easily set up to share data in a controlled environment, such data is still at risk unless rigorous security is in place. The problem of a closed intranet is that essential data may not reach those who require it. Intranets have a position within organizations. However, for greater data sharing, it may be preferable to keep the networks open, with the following 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

It was claimed that virtual private networks are frequently utilized for intranet access to the internet. Intranets that span many sites are typically run via different leased lines, though a newer solution of VPN can be used. A VPN is a private network that connects remote sites or users via a public network (typically the Internet). A VPN uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee rather than a dedicated, real world connection such as a leased line.

VIII. CURRENT DEVELOPMENTS IN NETWORK SECURITY

The network security area is following in the footsteps of its predecessors. With the inclusion of biometric identification, the same approaches are applied. Biometrics is a more secure way of authentication than passwords. This might significantly limit illegal access to secure systems. The software side of network security is always evolving. New firewalls and encryption techniques are constantly being introduced. The research being conducted aids in comprehending present advances as well as anticipating future developments in the subject.

1. Hardware Developments

Hardware advancements are not occurring at a quick pace. The only new hardware innovations that have a significant impact on security are biometric systems and smart cards. The most obvious application of biometrics for network security is secure workstation logons for a network-connected workstation. Each workstation requires some software support for biometric identification of the user, as well as some hardware device, depending on the biometric being utilised. The affordability of hardware devices is one factor that may contribute to the widespread usage of speech biometric security identification, particularly among small and medium-sized businesses and organisations. The next step up would be hardware devices such as computer mice with built-in fingerprint readers. These devices would be more expensive to implement across multiple computers because each one would require its own hardware device.

2. Software Developments

The software side of network security is extremely broad. It includes firewalls, antivirus, VPN, intrusion detection, and a variety of other features. At present time, it is not viable to investigate the research and development of every security software. The goal is to have an understanding of where security software is heading based on current emphasis.

IX. FUTURE TRENDS IN SECURITY

More than anything else, the set of applications will drive Internet security. In the future, security could be analogous to an immune system. The immune system repels threats and prepares itself to face more difficult foes. Likewise, network security will be able to act as an immune system.

The trend toward biometrics may have begun some time ago, but it does not appear to be aggressively pursued. Many security developments are taking place inside the same set of security technology that is now in use, with minimal alterations.

X. 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 analysed. Although most security technology is software-based, numerous popular hardware devices are used. 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 realise 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., "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 1999
[5] Sotillo, S., East Carolina University, “IPv6 security issues,” August 2006, www.infosecwriters.com/text_resources/pdf/IPv6_SSot illo.pdf.
[6] Andress J., “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