IPv4 Network Security

[1]Sujit Mehar, [2]Samikshya Mishra, [3]Laxmiparbati Das

[1]Assistant Professor in Dept. of Computer Science, GIET Gangapatna, Bhubaneswar
[2]Assistant Professor in Dept. of Computer Science, GIET Gangapatna, Bhubaneswar
[3]Assistant Professor in Dept. of Computer Science, GIET Gangapatna, Bhubaneswar

Abstract- The significance of network security has escalated for personal computer users, organizations, and military entities alike. With the proliferation of the internet, security has emerged as a paramount concern, and a retrospective analysis of security history provides valuable insights into the evolution of security technology. The inherent structure of the internet itself poses numerous security vulnerabilities, necessitating modifications to mitigate potential threats across the network. Understanding the various attack vectors empowers us to devise effective security measures. Many enterprises safeguard their digital assets from online threats by implementing firewalls and encryption protocols. They establish secure internal networks, commonly referred to as "intranets," to maintain connectivity with the internet while shielding against potential risks. The realm of network security is expansive and continually evolving. To grasp the ongoing research endeavors, it's imperative to possess foundational knowledge encompassing the internet's architecture, vulnerabilities, prevalent attack methodologies, and advancements in security technology. Consequently, these fundamental aspects are meticulously reviewed to inform contemporary research efforts in network security.

I. INTRODUCTION

The world is becoming more interconnected due to Internet and new networking technology. There is a large amount of personal, commercial, military, and government information on networking infrastructures worldwide. Network security is becoming of utmost importance because of intellectual property that can be easily acquired through the internet. There can be breach in intellectual property.

There are two types of 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. That is why security is emphasized in data networks, such as the internet, and other networks that link to the internet.

The vast topic of network security is analyzed by researching the following:

1. Internet architecture and vulnerable security aspects of the Internet
2. Types of internet attacks and security methods
3. Security for networks with internet access
4. Current development in network security hardware and software

II. NETWORK SECURITY

System and network technology is a key technology for a wide variety of applications. Networks and applications need security. Although, network security is a critical requirement, there is a significant lack of security methods that can be implemented easily.

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 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. In contrast to network design, secure network design is not a well-developed process. There isn’t a methodology to manage the complexity of security requirements. Secure network design does not contain the same advantages as network design.

Network security doesn’t mean securing both end computers. When transmitting data the communication channel should not be vulnerable to attack. A possible hacker could target the communication channel, obtain the encrypted data, and decrypt it and re-insert a false message. Securing the middle 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]:

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]. To make the computer less vulnerable to the network there are many products available. These tools are encryption, firewalls, intrusion-detection, and security management and authentication mechanisms. Businesses throughout the world are using a combination of some of these tools. "Intranets" are both 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 helps to develop secure solutions to protect the networks from the internet.

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 like passwords, logins that can be exploited in later attacks

III. 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. Due to advancement of hackers, cryptographic methods have to develop constantly to be one step ahead.

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 network. Therefore, hard ciphers are needed as well as attack-hard networks.

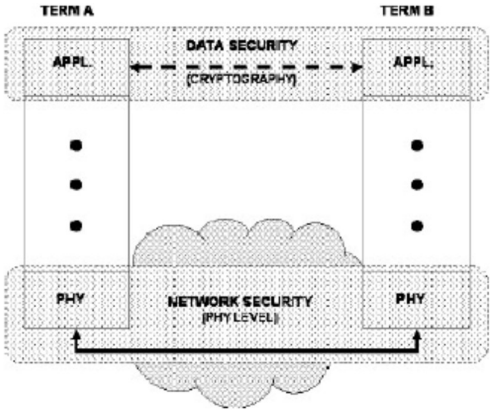

Figure 1

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 are also used to accomplish the network security required. 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 mechanisms allow for the logical protection of data units that are transferred across the network. The current version and new version of the Internet Protocol are analyzed to determine the security implications. Although security may exist within the protocol, not all attacks are guarded against. These attacks are analyzed to determine other security mechanisms that may be necessary.

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].

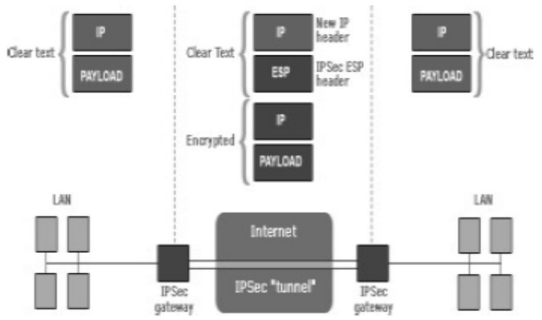

Figure 2: shows a visual representation of how IPsec is implemented to provide secure communications.

IP sec 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.

V. ATTACKS THROUGH THE CURRENT INTERNET PROTOCOL IPV4

1. Common Internet Attack Methods

Common internet attacks methods are broken down into categories. Some attacks gain system knowledge or personal information, such as eaves dropping 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, surf attacks, and teardrop attacks. These attacks are not as well-known as DoS attacks, but they are used in some form or another even if they aren't mentioned by name.

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]. 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.

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 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.

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. These unintelligible data is thus transferred in the network safely.

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 frontline 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].

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. IDS products are used to monitor connection in determining whether attacks are been launched. Some IDS systems just monitor and alert of an attack, whereas others try to block the attack.

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.

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. Clients present a certificate to the server to prove their identity.

VI. SECURITY ISSUES OF IP PROTOCOL IPV6

IPv6 is the next thing everyone's talking about. 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 is configure servers, poorly designed applications, or poorly protected sites.

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 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 into the internet protocol IPv6. The feature requires special security measures. Network administrators need to be aware of these security needs when using IPv6's mobility feature.

VII. 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. 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:

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 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.

VIII. 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. The software aspect of network security is very dynamic. Constantly new firewalls and encryption schemes are being implemented. The research being performed assist in understanding current development and projecting the future developments of the field.

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 work station 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.

2. Software Developments

The software aspect of network security is very vast. It includes firewalls, antivirus, VPN, 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.

IX. 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. 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.

X. CONCLUSION

"In the ever-expanding landscape of the internet, network security has emerged as a crucial field garnering increasing attention. Through meticulous analysis of security threats and internet protocols, we strive to discern the requisite adaptations in security technology. While predominantly software-centric, network security also relies on a plethora of hardware devices for robust implementation.

Regrettably, recent strides in network security development have not been as groundbreaking as anticipated. Despite the profound significance of this field, it's disconcerting to observe that much of the innovation is merely iterative, rather than transformative. Initially, there was an expectation that the paramount importance of network security would drive vigorous exploration of novel approaches in both hardware and software domains. However, the prevailing trend indicates a predilection for refining existing technologies rather than pioneering new paradigms.

Optimal security solutions often entail the judicious amalgamation of IPv6 alongside established security tools such as firewalls, intrusion detection systems, and authentication mechanisms. This synergistic integration holds promise in fortifying intellectual property protection in the foreseeable future. Nevertheless, as threats continue to evolve in sophistication and scale, there is an urgent imperative for the network security domain to foster a culture of rapid evolution and innovation to effectively address future challenges."

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