RESEARCH ARTICLE OPEN ACCESS

A Survey On Network Security Mechanism

Mulla Fathima Fouzia(Assistant Professor *
Shaik Munawar Sultana(Assistant Professor)**
Department of Computer Science And Engineering
Shadan College of Engineering and Technology

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. 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. In order to understand the research being performed today, background knowledge of the internet, its vulnerabilities, attack methods through the internet, and security technology is important and therefore they are reviewed.

INTRODUCTION

The world is becoming more interconnected with the advent of the 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 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. 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. History of security in networks
2. Internet architecture and vulnerable security aspects of the Internet
3. Types of internet attacks and security methods
4. Security for networks with internet access
5. 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 heading.

Network Security

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.

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 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. 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.

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, 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]:

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

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. To lessen the vulnerability of the computer to the network there are many products available. These tools are encryption, authentication mechanisms, intrusion-detection, security management and firewalls. 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 assists in developing new security technologies and approaches for networks with internet access and internet security itself. 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

The last reason for a network intrusion is most commonly guarded against and considered by most as the only intrusion motive. The other reasons mentioned need to be thwarted as well. Typical security currently exists on the computers connected to the network. Security protocols sometimes usually appear as part of a single layer of the OSI network reference model. Current work is being performed in using a layered approach to secure network design. The layers of the security model correspond to the OSI model layers. This security approach leads to an effective and efficient design which circumvents some of the common security problems.

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 ciphertext over a network, it is helpful to have a secure network. This will allow for the ciphertext 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 [2].

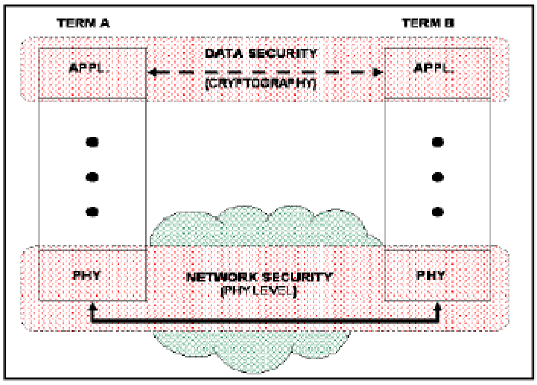


Figure 1: Based on the OSI model, data security and network security have a different security function

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 [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 countermeasure strategies [2].

HISTORY OF NETWORK SECURITY

Recent interest in security was fueled by the crime committed by Kevin Mitnick. Kevin Mitnick committed the largest computer-related crime in U.S. history [3]. The losses were eighty million dollars in U.S. intellectual property and source code from a variety of companies [3]. Since then, information security came into the spotlight. Public networks are being relied upon to deliver financial and personal information. Due to the evolution of information that is made available through the internet, information security is also required to evolve. Internet has been a driving force for data security improvement. Internet protocols in the past were not developed to secure themselves. Within the TCP/IP communication stack, security protocols are not implemented. This leaves the internet open to attacks. Modern developments in the internet architecture have made communication more secure.

1. Brief History of Internet

The birth of the interne takes place in 1969 when Advanced Research Projects Agency Network (ARPANet) is commissioned by the department of defense (DOD) for research in networking. 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. Security Timeline

Several key events contributed to the birth and evolution of computer and network security. The timeline can be started as far back as the 1930s.Polish cryptographers created an enigma machine in 1918 that converted plain messages to encrypted text. In 1930, Alan Turing, a brilliant mathematician broke the code for the Enigma. Securing communications was essential in World War II. In the 1990s, Internet became public and the security concerns increased tremendously. Approximately 950 million people use the internet today worldwide [3]. On any day, there are approximately 225 major incidences of a security breach [3]. These security breaches could also result in monetary losses of a large degree. Investment in proper security should be a priority for large organizations as well as common users.

INTERNET ARCHITECTURE AND VULNERABLE SECURITY ASPECTS

Fear of security breaches on the Internet is causing organizations to use protected private networks or intranets [4]. 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.

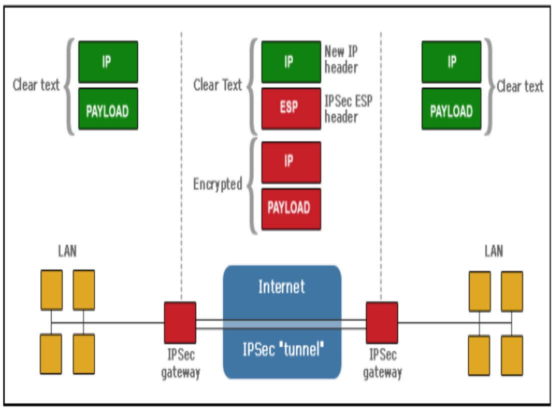


Figure 2: IPsec contains a gateway and a tunnel in order to secure communications.

The current version and new version of the Internet Protocol are analyzed to determine the security implications. Although security may exist within the protocol, certain attacks cannot be guarded against. These attacks are analyzed to determine other security mechanisms that may be necessary. 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.

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 [6]. 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.

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:

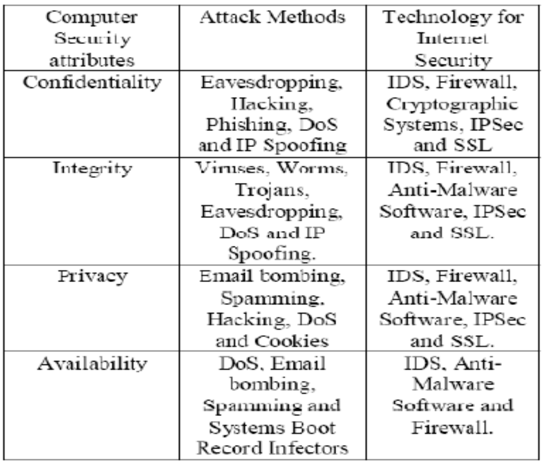
1. Address Space
2. Routing
3. Configuration
4. Security
5. Quality of Service

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

From a high-level view, the major benefits of IPv6 are its scalability and increased security. IPv6 also offers other interesting features that are beyond the scope of this paper. It must be emphasized that after researching IPv6 and its security features, it is not necessarily more secure than IPv4.



Computer Security attributes	Attack Methods	Technology for Internet Security
Confidentiality	Eavesdropping, Hacking, Phishing, DoS and IP Spoofing	IDS, Firewall, Cryptographic Systems, IPSec and SSL
Integrity	Viruses, Worms, Trojans, Eavesdropping, DoS and IP Spoofing.	IDS, Firewall, Anti-Malware Software, IPSec and SSL.
Privacy	Email bombing, Spamming, Hacking, DoS and Cookies	IDS, Firewall, Anti-Malware Software, IPSec and SSL.
Availability	DoS, Email bombing, Spamming and Systems Boot Record Infectors	IDS, Anti-Malware Software and Firewall.

Table 1: Attack Methods and Security Technology

Common Internet Attack Methods

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

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 eavesdropping is 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].

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.

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.

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].

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.

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].

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.

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

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.

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 front line 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].

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.

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.

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.

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 [5]:

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. Spoofing continues to be a security threat on IPv6 protocol. 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.

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. 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.

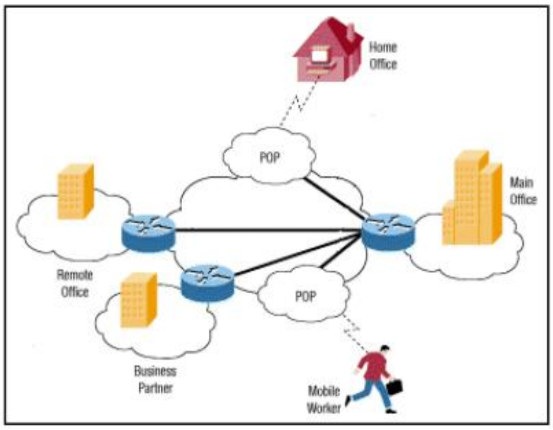


Figure 3: A typical VPN might have a main LAN at the corporate headquarters of a company, other LANs at remote offices or facilities and individual users connecting from out in the field

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. The software aspect of network security is very dynamic. Constantly new firewalls and encryption schemes are being implemented.

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 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.

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.

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 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.

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. Research in this area is currently being performed.

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.

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. Originally it was assumed that with the importance of the network security field, new approaches to security, both hardware and software, would be actively researched. It was a surprise to see most of the development taking place in the same technologies being currently used. The embedded security of the new internet protocol IPv6 may provide many benefits to internet users. Although some security issues were observed, the IPv6 internet 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.24- 28, Sep 2008

[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] "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 *Computer Networks & ISDN Systems Journal*, vol. 31, pp. 787-804, April 2011

[5] Sotillo, S., East Carolina University, "IPv6 security issues," August 2012,

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