iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** II **Month of publication:** February 2017

DOI: http://doi.org/10.22214/ijraset.2017.2050

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Flexible Data Access Using Network Security

K. Ramya[1], K. Pavithradevi[2], A. Satheesh[3], R. Shanavash[4]
[1,2]Assistant Professor, [3,4]Student, Department of MCA
Gnanamani College of Technology, Pachal, Namakkal.

Abstract - Network security has become more important to individual computer users, organizations, and the military worse. 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 Network 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. 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.
keywords - Network Security, WLAN, Data Security, IFTE, Network Protocol.

I. INTRODUCTION

The networking technology have a boom development in Now-a-days. There is a large amount of personal, commercial, military, and government information on networking infrastructures needed over the world. we can access the Network Security techniques is helps for intellectual propertycan easly acquired. 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.

A. Network security

System and network technology is a key technology for a wide variety of applications in over the world. 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.
When developing a secure network, the following need to be considered:
Access – authorized users are provided the means to communicate to and from a
particular network.
Confidentiality – Information in the network remains private
Authentication – Ensure the users of the network are who they say they are
Integrity – Ensure the message has not been modified in transit
Non-repudiation – Ensure the user does not refute that he used the network

B. 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

Volume 5 Issue II, February 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

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 network.

C. Internet architecture and vulnerable security aspects

Fear of security breaches on the Internet is causing organizations to use protected private networks or intranets [2]. The Internet Engineering Task Force (IETF) has introduced security mechanisms at various layers of the Internet Protocol Suite [8].
These security mechanisms allow for the logical protection of data units that are transferred across the network.
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, they seem to be insufficient [5].
Figure 1 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 used in two modes, namely transport and tunnel modes.

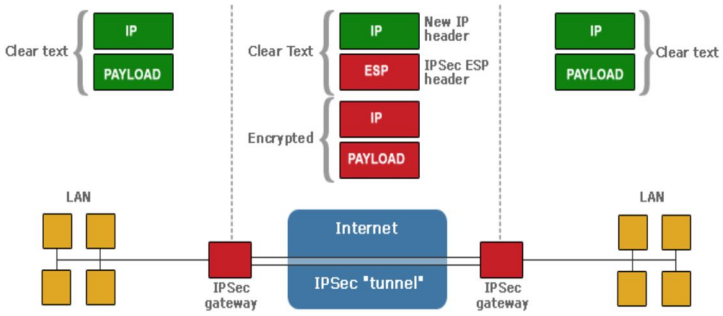


Figure 1: IPsec contains a gateway and a tunnel in order to secure communications.

D. 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 [2]. 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. The internet protocol's design is so vast and cannot be covered fully. The main parts of the architecture relating to security are discussed in detail.

1) 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:

Address Space Routing
Configuration Security Quality of Service

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 [5]. 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 [9]. 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.

2) 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:

Routing and addressing

Volume 5 Issue II, February 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Multi-protocol architecture
Security architecture
Traffic control

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. IP sec is embedded within the IPv6 protocol. IP sec functionality is the same for IPv4 and IPv6. The only difference is that IPv6 can utilize the security mechanism along the entire route.

3) *Attacks through the Current Internet Protocol IPv4:* There are four main computer security attributes. They were mentioned before in a slightly different form, but are restated for convenience and emphasis. These security attributes are confidentiality, integrity, privacy, and availability. Confidentiality and integrity still hold to the same definition. Availability means the computer assets can be accessed by authorized people [8]. Privacy is the right to protect personal secrets. Various attack methods relate to these four security attributes.

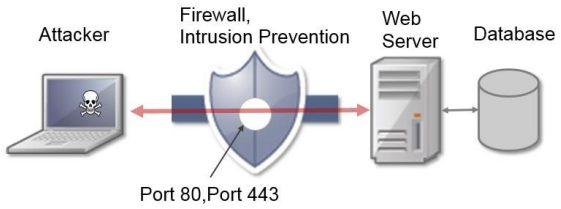


Table 1: Attack Methods and Security Technology

4) *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.

5) *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 intrude listens and inserts something into thecommunication stream. This can lead to the messages being distorted. Sensitive information can be stolen this way.

6) *Viruses:* Viruses are self-replication programs that use files to infect and propagate [2]. Once a file is opened, the virus will activate within the system.

7) *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 [9]. 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.

8) *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.

9) *Phishing:* Phishing is an attempt to obtain confidential information from an individual, group, or

organization. Phishers trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information.

10) *IP Spoofing Attacks:* Spoofing means to have the address of the computer mirror the address of a trustecomputer in order to gain access to other computers. The identity of the intruder is hidden by different

means m aking detection and prevention difficult. With the current IP protocol technology, IP spoofed packets cannot be eliminated.

11) *Denial of Service:* Denial of Service is an attack when the system receiving too many requests cannot return communication with the requestors [5]. The system then consumes resources waiting for the handshake to complete. Eventually, the system cannot respond to any more requests rendering it without service.

II. 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.

A. 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.

B. 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.

C. Intrusion Detection Systems

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.

III. 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[2]. 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:
Header manipulation issues
Flooding issues
Mobility issues

IV. 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:
Firewalls that detect and report intrusion attempts
Sophisticated virus checking at the firewall
Enforced rules for employee opening of email attachments
Encryption for all connections and data transfers
Authentication by synchronized, timed passwords or security certificates

Volume 5 Issue II, February 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

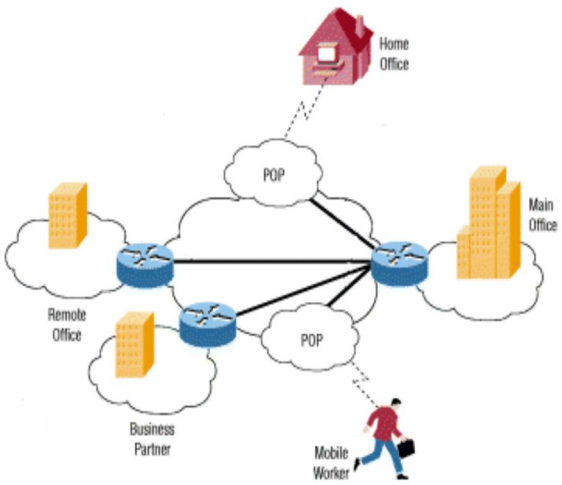


Figure 2: A typical VPN might have a main LAN at the corporate headquarters of a company, other LANs at remote offices or facilities and individual users connecting from out in the field.

A. 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. New technology such as the smart card is surfacing in research on network security. The software aspect of network security is very dynamic.Constantly new firewalls and encryption schemes are being implemented. The research being performed assists in understanding current development and projecting the futuredevelopments of the field.

B. 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.

C. 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. 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. Many research papers that have been skimmed were based on analyzing attack patterns in order to create smarter security software

.

D. In future trends 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.

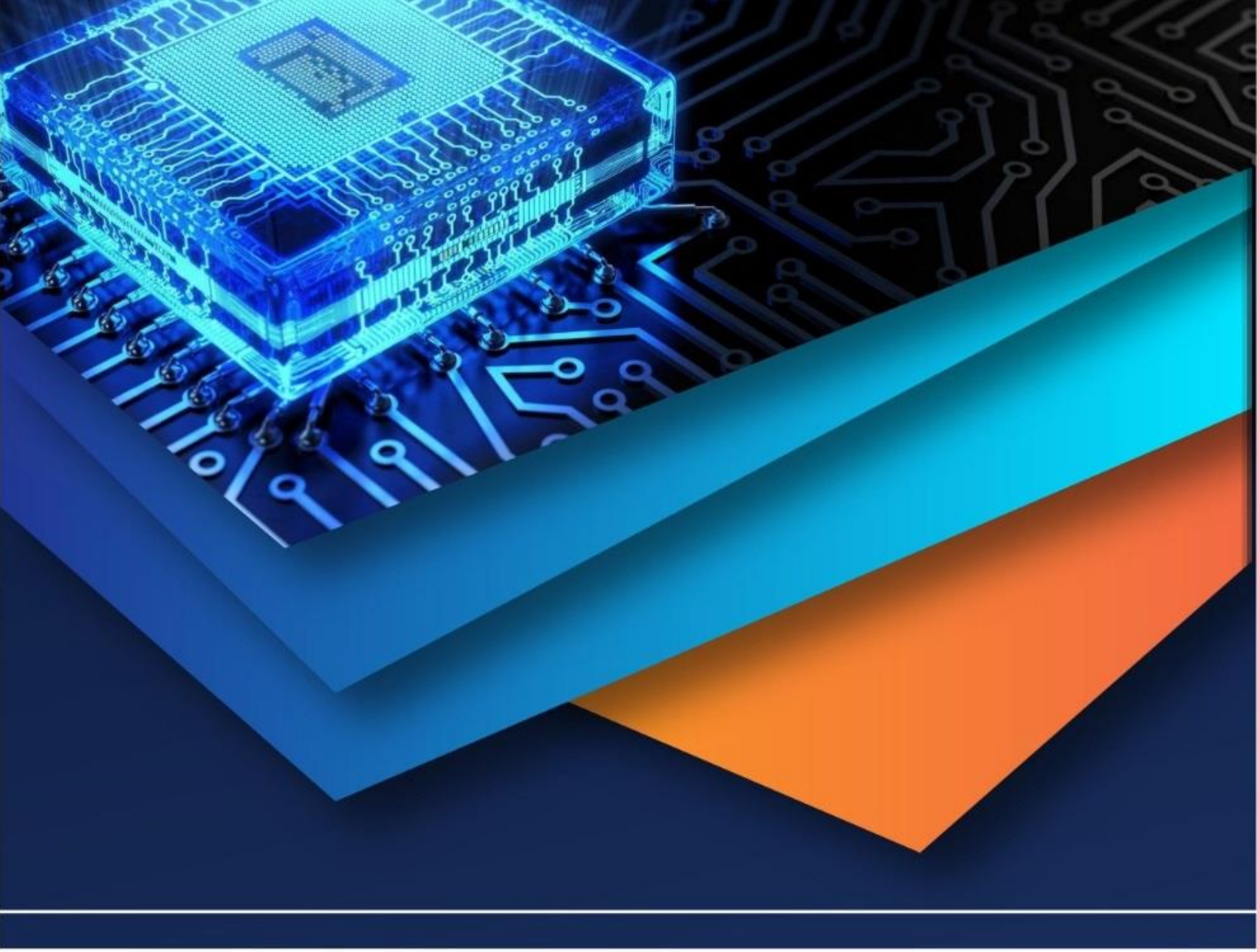
V. CONCLUSION

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.

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, 19-23May 2008
[2] K.Ramya and K.Pavithradevi "Effective Wireless Communication," International Journal of Advanced Research, volume4(12),pp. 1559-1562 Dec 2016.
[3] .C.Ganesh,B.Sathiyabama,T.Geetha"Fast Frequent Pattern Mining Using Vertical Data Format for Knowledge Discovery" International Journal of Emerging Research in Management and Technology",Vol 5,issue 5,2016
[4] Molva, R., Institut Eurecom,"Internet Security Architecture," in Computer Networks & ISDN Systems Journal, vol. 31, pp. 787-804, April 1999.
[5] L.Gomathi,K.Ramya "Data Mining Analysis using query Formulation In Aggregation Recommendation",Volume 2 Issue 1- October 2013.
[6] Sotillo, S., East Carolina University, "IPv6 security issues," August 2006, www.infosecwriters.com/text_resources/pdf/IPv6_SSotillo.pdf.
[7] Andress J., "IPv6: the next internet protocol,"April2005,www.usenix.com/publications/login/2005-04/pdfs/andress0504.pdf.
[8] Karthikeyan.R, Dr.Geetha.T ,Ramya.K ,Pavithradevi.K," A Survey on Sensor Networks", International journal for Research and Development in Technology, Volume 7,Issue 1 Jan 17.
[9] G.Arunachalam, K.Ramya, M.Vimala, M.Shanmugapriya, C.Krishnaveni,"Future Principle of TCP High-Speed Network "International Journal for Research & Development in Technology.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY