Volume 5, No. 5, May-June 2014

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Advancing the Technology of Network Security by using Latest Cryptographic Schemes and Software Developments

Nikhil Singla[1], Puneet Gulati[2]

[1,2]Student (B.Tech 4th sem) Department of Computer Science Engineering

Dronacharya College of Engineering, Gurgaon-123506, India

Abstract : **Network security** consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password Network security has become more important to personal computer users, organizations, and the military. With all the work going on the internet, Security became a major concern and the history of security allows a better understanding of the emergence of security technology. The range of study includes a brief history dating back to internet's beginnings and the current development in network security. In order to understand their search 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.

Keywords: Firewalls, Encryption ,Intranet, Vulnerability

I. 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 which comprises 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. 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 [2].

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:

a. To consume resources uselessly.
b. To interfere with any system resource's intended function.
c. To gain system knowledge that can be exploited in later attacks.

II. DIFFERENTIATING BETWEEN NETWORK AND DATA SECURITY

Data security is the aspect of security that allows a client's data to be transformed into unidentifiable data for transmission. Even if this unidentifiable 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. 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.

In the OSI model the cryptography occurs at the application layer therefore the user can possibly choose different methods of data security. Network security is mostly contained within the physical layer. 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[4].

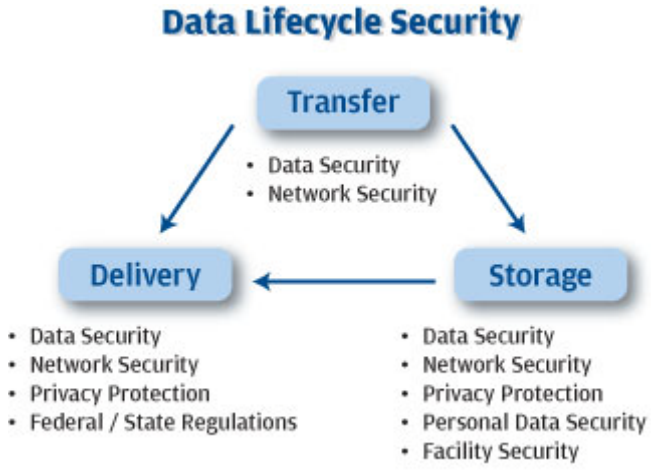

Figure 1: shows data security and network security have a different security function

III. HISTORY OF INTERNET

The birth of the internet took place in 1969 when Advanced Research Projects Agency Network (ARPAnet) was commissioned by the department of defense (DOD) for research in networking.

The Inter Networking Working Group becomes the first of several standards-setting entities to govern the growing network.

Vinton Cerf was elected the first chairman of the INWG, and later he was known as a "Father of the Internet."In the 1980s, Bob Kahn and Vinton Cerf are key members of a team that create TCP/IP, the common language of all Internet computers. For the first time the loose collection of networks which made up the ARPANET is seen as an "Internet", and the Internet as we know it today is born. In the 1990s,the World Wide Web was born. Netscape and Microsoft were both competing on developing a browser for the internet. In the 1960s, the term “hacker” is coined by a couple of Massachusetts Institute of Technology (MIT) students. The Computer Fraud and Abuse Act of 1986 was created because of Ian Murphy’s crime of stealing information from military computers. Most importantly , Kevin Mitnick (the first hacker of world) committed the largest computer-related crime in U.S. history . The losses were eighty million dollars in U.S. intellectual property and source code from a variety of companies. Since then, information security came into the spotlight.

IV. IPV4 ARCHITECTURE

The protocol contains a couple aspects which caused problems with its use.The causes of problems with the protocol are:

a. Address Space
b. Routing
c. Configuration
d. Security
e. 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.

Routing is a problem for this protocol because the routing tables are constantly increasing in size. 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. Some of the information required is the IP address, routing gateway address, subnet mask, and DNS server.

The lack of embedded security within the IPv4 protocol has led to the many attacks seen today. Mechanisms to secure IPv4 do exist, but there are no requirements for their use. IP sec is a specific mechanism used to secure the protocol.

When internet was created, the quality of service(QoS) was standardized according to the information that was transferred across the network. The original transfer of information was mostly text-based. As the internet expanded and technology evolved, other forms of communication began to be transmitted across the internet[6].

V. 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:

a. Routing and addressing
b. Multi-protocol architecture
c. Security architecture
d. Traffic control

The IPv6 protocol’s address space was extended by supporting 128 bit addresses. With 128 bit addresses, the protocol can support up to 3.4*(10)^38 machines[1].

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. IPsec is embedded within the IPv6 protocol. IPsec functionality is the same for IPv4and IPv6. The only difference is that IPv6 can utilize the security mechanism along the entire route[6].

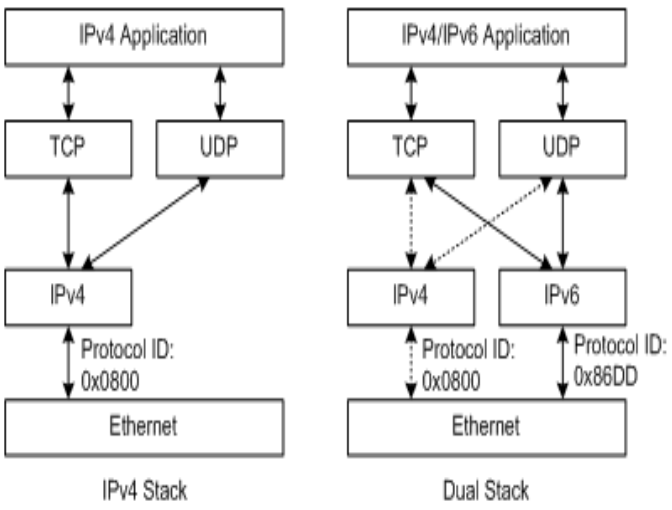

Figure 2: shows IPv4 and IPv6 Archietecture

VI. SOME COMMON INTERNET ATTACKS

A. Virus:

A **virus** is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected".

B. 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.

C. 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.

D. Denial of Service:

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

E. XSS Attack:

It's a vulnerability which is found very frequently in the websites which he enables the attacker to inject the clients id scripts into the website.

The Attacker sends the vulnerable website with his malicious script to the other user, when browser receives all the scripts, it assumes all the scripts have come from the trusted source and because of that victim gets compromised. Generally this vulnerability is found in the search box, shout box, comment box etc… It can be found by the same way we can find SQL Injections.

F. 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.

G. 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[3].

Table 1: Attack Methods and Security Technology

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.

VII. 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. Firewall:

A **firewall** is a software or hardware-based network security system that controls the incoming and outgoing network traffic by analyzing the data packets and determining whether they should be allowed through or not, based on applied rule set. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is not assumed to be secure and trusted.

B. Cryptographic Systems:

A cryptographic system is any computer system that involves cryptography. Such systems include for instance, a system for secure electronic mail which might include methods for digital signatures, cryptographic hash functions, key management techniques, and so on. Cryptographic systems are made up of cryptographic primitives and are usually rather complex. Because of this, breaking a cryptosystem is not restricted to breaking the underlying cryptographic algorithms - usually it is far easier to break the system as a whole, e.g., through the not uncommon misconceptions of users in respect to the cryptosystem. The systematic arrangement of cypher text can abide the security[7].

C. Anti-Malware Softwares:

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.

D. Secure Socket Layer(Ssl):

SSL (Secure Sockets Layer) is a standard security technology for establishing an encrypted link between a server and a client—typically a web server (website) and a browser; or a mail server and a mail client (e.g., Outlook). SSL allows sensitive information such as credit card numbers, social security numbers, and login credentials to be transmitted securely. Normally,data sent between browsers and web servers is sent in plain text—leaving you vulnerable to eavesdropping. If an attacker is able to intercept all data being sent between a browser and a web server they can see and use that information.

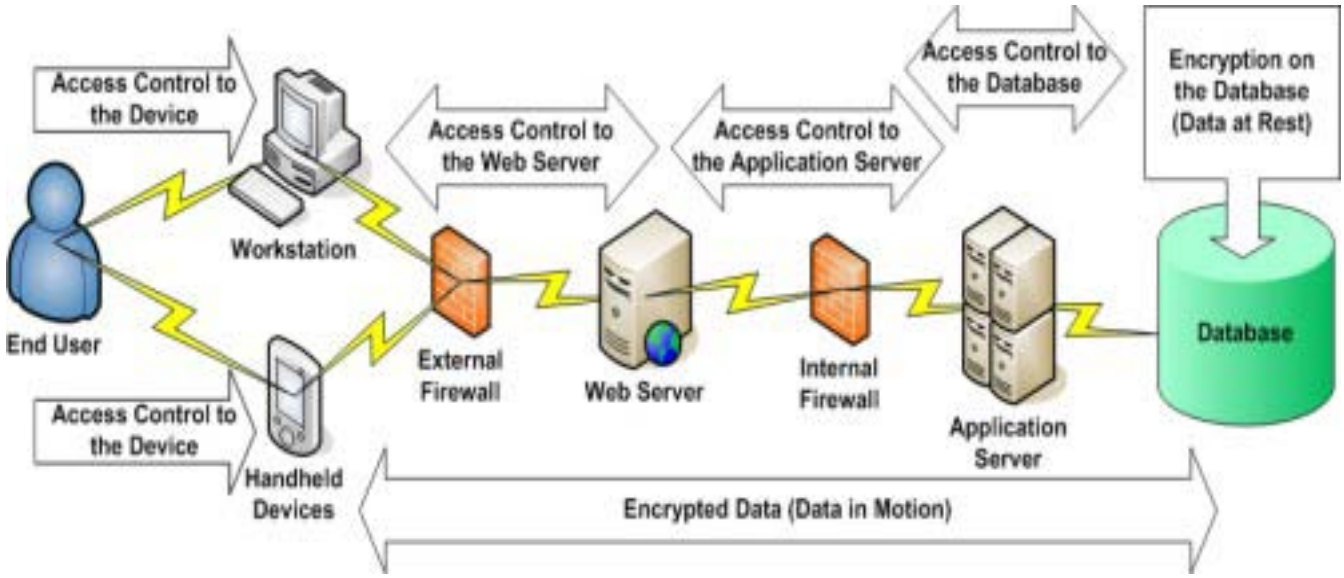

Figure 3: shows various technology for Network security

VIII. CURRENT DEVELOPMENTS IN NETWORK SECURITY

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.

A. 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.

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. 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. A biometric mouse, with the software to support it, is available from around $120 in the U.S. The advantage of voice recognition software is that it can be centralized, thus reducing the cost of implementation per machine. At top of the range a centralized voice biometric package can cost up to $50,000 but may be able to manage the secure log- in of up to 5000 machines.

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. Very often people write their password down and keep it near their computer. This is of course completely undermines any effort at network security. Biometrics can replace this security identification method. The use of biometric identification stops this problem and while it may be expensive to set up at first, these devices save on administration and user assistance costs.

IX. FUTURE SUGGESTIONS

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. 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.

X. 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.

XI. REFERENCES

[1] Andress J., "IPv6: the next internet protocol,"April 2005 ww.usenix.com/publications/login/2005-04/pdfs/andress0504.pdf.

[2] Curtin, M. "Introduction to Network Security," http://www.interhack.net/pubs/network-security.

[3] 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.

[4] Kartalopoulos, S. V., "Differentiating Data Security and Network Security," Communications, 2008. ICC '08. IEEE International Conference on, pp.1469-1473, 19-23 May 2008

[5] "Security Overview," www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/security-guide/ch-sgs-ov.html.

[6] Molva, R., Institut Eurecom,"Internet Security Architecture," in Computer Networks & ISDN Systems Journal, vol. 31, pp. 787-804, April 1999

[7] Detail about data encrytion, "http://www.cdc.gov/cancer/npcr/tools/security/encryption2.html.

[8] "Network Security" "http://web.mit.edu/~bdaya/www/Network%20Security.pdf".

