1

History and Generations of Security Protocols

Bright Keswani[1†], Poonam Keswani[2*] and Rakhi Purohit[3‡]

[1]Department of Computer Applications, Suresh Gyan Vihar University, Jaipur, India
[2]Akashdeep PG College, Jaipur, India
[3]Global Institute of Technology, Jaipur, India

Abstract

For personal computers, organizations and military users, network security has become more important. Due to the recent arrival of the internet in network, and security now a key issue, the safety record maybe availability as well all people understand very good requirements security technologies in communications. Knowing the attack method can generate enough security. Many companies testing protection auto using some techniques of the network internet through download programs firewalls and some mechanisms encryption in itself company origin it has a special internal network known as "Intranet" to maintain in contact internet access from outside also safe from any threatening state. All the security of the network is huge as well in stage specific development for evaluation. It is a theme that consists of date summary for the security that shows in internet assets security, as well development internet current techniques security. To understand the ongoing investigation, understand previous for the internet, and level his from weak points from attacks, and also methods attack different via network internet known, as well security technologies what they are very mission a lot they are need as well to be reviewed and analysis.

***Keywords*:** Network security, security protocols, attacks collective, security techniques

**Corresponding author*: poonamkeswani777@gmail.com
†Corresponding author: kbright@rediffmail.com
‡Corresponding author: rakhimutha@gmail.com

Dinesh Goyal, S. Balamurugan, Sheng-Lung Peng and O.P. Verma (eds.) Design and Analysis of Security Protocol for Communication, (1–28) © 2020 Scrivener Publishing LLC

1.1 Introduction

Due to advent of the Internet and ever changing network technologies, the world is increasingly interconnected day by day. There are many personal, commercial, military, and government information in the creation of infrastructure networks around the world. Network security has become very important because intellectual property can be easily accessible via the efficient use of Internet and related tools. Although there are various types of networks but two fundamentally different networks, i.e., data networks and synchronous networks consisting of switches. The Internet is seen as a data network. From its current data network, information can be obtained through special procedures by router-based computers such as planting in the router "Trojan Horse". Data is not stored by switches of a synchronous network; therefore it is not compromised by attackers. That is why security is emphasized in data networks such as the Internet, as well as in various aspects of the Internet connection proposed by other networks.

For clear understanding, this chapter is divided into the following Sections. Further, each section is discussed in brief.

1. Network Security
2. The History and Security of the Network
3. Common Methods of Attack
4. Network Security Technology
5. Evolution of Network Security Protocols
6. Network Security Protocol

1.2 Network Security

When thinking about network security, we should know that the network should be a secure place. The network security does not affect the security of the client computers at any of the point of the connection chain [2]. So, when transferring the data from the communications channel which does not be attacked, there will be a potential intruder can indicate to a specific communication channel, which access data and decrypt and also re-encrypt the message, which is falsified. The task of repairing a network is as important as obtaining a computer and encrypting a message.

The system and some network technologies are the key technologies for various applications in network. Network security is critical for the specific network and the applications of network [1]. Network security is a

prerequisite for emerging networks; also it is easy to implement a very secure approach for networking.

At time of development of secure network, there are some of the factors considered accordingly, i.e., "Access", which provide authorized users with the methods to communicate with specific network; "Confidentiality", which ensures that information/data flow on the network will remains private; "Authentication", which makes sure that the users of the network are what they call people; "Integrity", which feature makes sure that the message is not modified during transmission, and "Do not repudiate", which makes sure that the user does not refute their use of the network [1].

The crimes committed by Kevin Mitnick have fueled the recent interest in security. Kevin Mitnick committed the greatest cybercrime in the history of the United States [3]. Losses of property and intellectual property of several companies amount to $80 million [3]. Since then, information security has become the focus of attention. The public network is called to provide personal as well as financial information. Security of such information must also evolve due to the development of information which is available online. Due to an attack Kevin Mitnick, The Company emphasizes the security of system. The Internet always works as main part behind data security.

Development of an effective security plan on the Internet require to address primarily to understand security issues, about the potential attackers, the level of security required, and about various factors that make the network insecure and vulnerable. Following are the steps to learn how to configure a secure network, the Internet, or other aspects during the search process.

In order to minimize the weaknesses from one device to another, many products are available which includes various tools for encryption of data and information, effective mechanisms for user authentication, intrusion detection and, security management. Companies around the world use a variety of these tools. The intranet connects and protects The Internet in a reasonable way. The same structure of the Internet may create weaknesses in the network. Internet security has greatly improved the development of new security mechanism and methods for networks including Internet as well as Intranet access.

It is also necessary to study the types of attacks online so that they can detect and prevent these attacks. Intrusion detection systems rely on the most common types of attacks.

Previous Internet protocols were not developed for assurance. In the TCP/IP communication stack, no security protocol is applied. This led to an attack on the Internet. Due to advancement in the Internet architecture information communications became more secure.

1.3 Historical Background of Network Security and Network Timeline

The Internet was first introduced in 1969, when the Department of Defense (ARPANET) conducted a network survey. Since the beginning of the year, ARPANET has been successful. The original design was intended easy access to remote computers so that scientists to share data and, it will become one of the most popular email for ARPANET to become a high-speed digital communication, which can be used to research various topics of interest and discuss. Collaboration in international network work is the first of many rules for entities that operate a growing network. He was the first president of INWG of Winton Joseph and became known as the "father of the Internet."

In the 1980s, TCP/IP was created by Bob Kent and Winton Joseph who were the main members of the TCP/IP team. TCP/IP is the general language for all computers to connect to the Internet. The loose network that makes the ARPANET known as today's "Internet". During 1980s, this kind of boom appeared in the computer industry. Combining low-cost desktops with powerful servers allows companies to communicate with their customers and business partners with the use of Internet.

In 1990, due to advent of World Wide Web [WWW] the Internet made accessible to everyone. Netscape Navigator and Microsoft Internet Explorer like search engines came into existence. Many important events have contributed to the development of computer security and networks. The timetable can be started in advance in 1930 to invent a Polish programmer's jigsaw machine in 1918 to convert simple information into cipher text. In 1930, the shocking mathematician Alan Turing broke the Enigma code. Make sure the connection is very important to the images of World War II. In 1960, it was launched by many students at the Massachusetts Institute of Technology (MIT) and the Department of Defense in the term "piracy", which is a popular electronic data and information exchange pipeline [3]. Telnet protocol was developed in 1970s. This led to the widespread use of data networks, initially limited to government contractors and academic researchers [3]. In the 1980s, online piracy and cybercrime began to emerge. After nine days of carnival, the authorities conducted an accidental search and penetrated into a highly confidential system. The 1986, Act of Fraud and Abuse was created, and computer crime Ian Murphy stole information from military computers. After graduation, Robert Morris was judged to launch more than 6,000 weak computers connected to the Internet. In the 1990s, the Internet became public and security issues increased dramatically. Today, about 950 million people worldwide use the Internet [3]. On any given day, there are approximately 225 important security violations [3]. These security breaches

can also result in significant financial losses. For large organizations and the average user, priority should be given to investing in appropriate security.

In 1975, the first malware was invented by two researchers who started the Xerox Company. It is called a "Worm" and looks for a lazy computer processor as an attempt to improve it. The creators of the simple diagnostic tool inadvertently created the first malware and created terms that are commonly used in multiple malware applications.

Many important events have contributed to the birth and development of computer security and networks. The program began in the 1930s, when Polish programmers invented a machine in 1918 to convert simple encrypted text messages. In 1930, the shocking mathematician Alan Turing broke the Enigma code ensuring that contact was crucial during the Second World War.

In 1960, he created the term "hacker" for many students at the Massachusetts Institute of Technology (MIT) and launched the Arpanet Department of Defense, which is popular as a channel for electronic exchange of data and information [3]. This paves the way for today's carrier network called the Internet. In 1970, the Telnet protocol was developed. This led to the widespread use of data networks, initially limited to government contractors and academic researchers [3].

In the 1980s, online piracy and cybercrime began to emerge. After 9 days of carnival, the authorities conducted an accidental search and penetrated into a highly confidential system. The 1986 Act of Fraud and Abuse was created, and computer crime Ian Murphy stole information from military computers. After graduation, Robert Morris was judged to launch more than 6,000 weak computers connected to the Internet. The Emergency Response Team (CERT) alerts computer users to cyber security issues based on concerns that Morris may repeat.

In the 1990s, the Internet became public and security issues increased dramatically. Today, about 950 million people worldwide use the Internet [3]. On 1 day, there were about 225 major security incidents [3]. These security breaches can also result in significant financial losses. For large organizations and the average user, priority should be given to investing in appropriate security.

1.4 Internet Architecture and Security Aspects

Fear of Internet security vulnerabilities has led companies to use private networks or protected internal networks. Security mechanisms in multiple layers of the Internet Protocol suite allow for logical protection of packet data sent over the network [11].

Analyze existing and new versions of the Internet Protocol to determine security risks. Although there may be security in the protocol, some attacks cannot be protected. Analyze these attacks to determine other security mechanisms that may be needed.

The Internet security architecture is called the Internet Safe security standard [19]. IPsec IP security covers next-generation IP (IPv6) (current version) (IPv4) although the development of new technologies such as IPsec does not seem to be sufficient to overcome the most common flaws on the Internet. A visual representation of IPsec provides a secure connection. IPSec is a peer-to-peer protocol that includes partial code and another part of decryption. The two parties share the key or key. IPSec can be used in two modes, transport mode and tunneling.

1.4.1 IPv4 and IPv6 Architecture

IPv4 was designed in 1980 to replace the NCP protocol in ARPANET. Twenty years later, IPv4 has many limitations [6]. IPv6 defect protocol design IPv4 is required. IPv6 is not a complete IPv4 packet protocol; instead, it is a new design. Internet protocols are designed to be very broad and cannot be fully covered. A key part of the security architecture is discussed in detail.

1.4.1.1 Structure of IPv4

The agreement contains several aspects that can cause problems when in use. Not all of these issues are related to security. It is worth noting that there is a full understanding of the Internet Protocol and its shortcomings. The reasons for the protocol issue are:

1. Address space
2. Routing
3. Configuration
4. Security
5. Quality of service

The IPv4 structure contains a 32-bit wide address [6]. This limits the maximum number of computers that can connect to the Internet. A 32-bit address can provide up to 2 billion computers connected to the Internet. No other issues are expected when the protocol is created. It facilitates malicious code distribution in IPv4 address space [5].

Routing is a problem with this protocol because the size of the routing table is constantly increasing. The maximum theoretical size input for the Global Positioning Table is 2 million [6]. Some methods have been used to

reduce the number of entries in the routing table. This is useful in a short amount of time, but major changes are required to resolve this issue.

A TCP/IP IPv4-based network is required to provide users with some data to configure the network. Some of the required information is the IP gateway, subnet mask and DNS server [4]. The simplicity of network configuration is not clear in the IPv4 protocol. The user can request the appropriate network configuration from the central server [6]. This is very useful.

For many of today's attacks, insecurity leads to the IPv4 protocol [9]. There is a mechanism to ensure IPv4, but not necessarily. IPsec is a specific protocol protection mechanism. Load the packet with encryption protection space. It provides confidentiality and ipsec integrity and authentication. This protection does not take into account pirate experts who can crack the encryption method and obtain the key.

When creating the Internet, QoS is based on the QoS of information sent over the network. The delivery of the original message is primarily dependent on the text. With the expansion of the Internet and the development of technology, other forms of communication have begun to spread on the Internet. For standard text, the quality of service for transmitting video and music is different. This protocol does not include QoS features. Dynamics vary depending on the type of data being sent [6].

1.4.1.2 IPv6 Architecture

In the development of IPv6, various aspects of the Protocol have been highlighted IPv4 address. It should be improved. Development efforts include the following areas:

1. Routing and addressing
2. Multi-protocol architecture
3. Safety Engineering
4. Traffic control

Extend the IPv6 address space by accepting a 128-bit address. The protocol uses a 128-bit address and supports up to three and four 10^38 devices. In this protocol, the use of address bits is less efficient because it simplifies the addressing configuration. The routing system is more efficient IPv6 and provides a smaller global routing table. The host configuration has also been simplified. The host can be configured automatically. This new design allows users and network administrators to easily configure.

The security architecture of the IPv6 protocol was born. Of great interest is that IPsec is integrated into the IPv6 protocol. IPsec IPv4 and IPv6 have the same function. The only difference is that IPv6 can use security

mechanisms along the way [6]. IPv6 addresses the issue of quality of service. IP allows special handling of certain packets with higher quality of service. You must confirm this after verifying IPv6. Its security features are not necessarily more secure than IPv4. Better security, not overall improvement.

1.4.2 Attack Through IPv4

Computer security has four main characteristics. The approach mentioned earlier is slightly different, but he rethinks comfort and attention. These security features are confidential, complete, private, and usable. Confidentiality and integrity remain the same. Availability means that authorized employees have access to computer assets [8]. Privacy is the right to protect personal secrets [8]. There are four attack methods associated with these four security features. Table 1.1 shows the attack methods and solutions.

A brief discussion of common attack techniques and security techniques will be provided. Not all methods are discussed in the table above. The current understanding of the techniques used to handle attacks is to understand the research and development of current secure hardware and software.

1.4.2.1 Internet Attacks Common Methods

There are several common methods of Internet attack. Some attacks gain system knowledge or personal information, such as spyware and phishing.

Table 1.1 Attack methods and security technology.

Computer security attributes	Attack methods	Technology for internet security
Privacy	Email bombing, Spamming, Hacking, Virus, Worms, IP Spoofing and DoS.	IDS, Firewall, anti-malware software, IPSec and SSl.
Integrity	Trojans, Virus, Worms, IP Spoofing and DoS.	IDS, Firewall, Anti-Malware Software, IPSec and SSl
Confidentiality	DoS, Eavesdropping, Phishing and IP Spoofing	IDS, Firewall, Cryptographic Systems, IPSec and SSL
Availability	DoS, Email, Bombing, Spamming and System Boot Record Infectors	IDS, Anti-Malware Software and Firewall.

Attacks can also interfere with the intended function of the system, such as viruses, worms, and Trojan horses. Another form of attack is the consumption of system resources, which may be the result of a denial of service attack. There are other forms of network intrusion, such as ground attacks, bomb attacks, and tear gas attacks. These attacks are not known in the name of two attacks, but they are used in some way even if they are not mentioned.

1.4.2.1.1 Listen Closely

Unauthorized interception of communications is known as illegal listening. Passive listening means that a person secretly listens to only network messages. Active spies, on the other hand, mean that intruders listen to certain content and listen to traffic. This can cause message distortion. Sensitive information can be stolen in this way [8].

1.4.2.1.2 Virus

A virus is a self-replicating program that uses file transfer and transmission [8]. Once the file is opened, the virus will be activated within the system.

1.4.2.1.3 Worm

Worms are considered viruses because they are repeated, but worms do not need files that allow them to spread [8]. There are two main types of worms and network identification worms and worms. A large number of email viruses use email as a means of infecting other computers. Network-sensitive worms are a major problem on the Internet. The target worm identifies the target network and once the worm reaches the target host, it is infected by a Trojan horse or other worm.

1.4.2.1.4 Trojan Horse

Trojan horses seem to be benign to users, but in reality they have some malicious targets. Trojan horses usually carry some goods, just like viruses.

1.4.2.1.5 Phishing

Phishing is an attempt to obtain confidential information from individuals, groups, or organizations. Deceive fraudulent users in detection. Personal information such as credit card numbers, online banking vouchers and other confidential information.

1.4.2.1.6 IP Spoofing Attack IP

It means that the address reflects the trusted address of the computer accessing other computers. The identity of intruders is hidden by a variety of means, making detection and prevention difficult and unable to delete fake IP (IP) packets by the use of current IP technology.

1.4.2.1.7 Denial of Service

A denial of service is considered an attack when a system that receives a large number of requests cannot reconnect with the applicant. The system then consumes resources waiting for the exchange to complete. Finally, the system is unable to respond to other unanswered requests.

1.4.2.2 Internet Security Technology

While information can be accessed and transmitted over the Internet, online threats will remain a major problem in the world. They developed various security and exploration measures to address these attacks.

1.4.2.2.1 Encryption System

Encryption is a useful tool widely used in current security architectures, including the use of code and passwords to transform information into model data to understand it.

1.4.2.2.2 Firewall

A firewall is a mechanism for controlling model boundaries or protecting perimeters. The goal of the firewall is to avoid traffic from outside, but it can also be used to avoid traffic from inside. The firewall is the first line of defense against hackers. It is a system designed to prevent unauthorized access or access from a private network. The firewall can be implemented in hardware or software, or a combination of the two.

1.4.2.2.3 Intrusion Detection System

An intrusion detection system is an additional measure to prevent intrusion into a computer. It can be an IDS system, which is software and hardware that detects attacks. IDS products are used to monitor connections and determine if an attack has been initiated. Some IDS systems only monitor and alert attacks, while others try to block attacks.

1.4.2.2.4 Software Methods and Anti-Malware

Viruses, worms, and Trojan horses are examples of malware or malware. Special anti-software tools are used to detect and process infected systems.

1.4.2.2.5 Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) is a set of protocols that is a standard way to achieve a high level of security between a web browser and a website. SSL is designed to create a secure tunnel or tunnel between a web browser and a web server to protect any information shared in a secure tunnel. SSL uses a certificate to provide client authentication for the server. The client sends the certificate to the server for identification.

1.4.3 IPv6 IP Security Issues

From a security perspective, IPv6 has made significant progress in IPv4 IP. Although IPv6 has a strong security mechanism, it is still weak. There are still potential security issues with certain aspects of the IPv6 protocol.

The new Internet protocol does not prevent properly configured servers, poorly designed applications, or protected sites.

Security issues may occur for the following reasons:

1. Problems in the management process
2. Flood problem
3. Liquidity issues

Due to the built-in IPsec function, there is a problem with the spindle operation [7]. The extension header avoids some of the common sources of attack caused by head operations. The problem is that the steering guide must be processed through all the stacks, which can result in a long series of steering heads. A large number of attachments may be confused by a knot, which is a form of attack if deliberate. Tradition remains a threat to IPv6 security.

When the entire network portion is resolved while searching for a possible destination with an open service, an attack type called port check [5] occurs. The IPv6 protocol address space is large, but the protocol is not threatened by such attacks.

Navigation is a new feature integrated with IPv6. This feature requires special security measures. Network administrators should be aware of these security requirements when using IPv6 Mobility.

1.5 Different Aspects of Security of the Network

The company currently uses a range of protection, encryption, and authentication mechanisms to create an Internet-connected intranet, but it is also protected.

An intranet is a dedicated computer network that uses the Internet protocol [12]. The difference between an intranet and an "external network" is that the first is usually limited to the employees of the organization, while the external network is usually available to customers, suppliers, or other authorized parties.

The company intranet does not require Internet access. This access is usually done through gateway and user authentication with a secure server, message encryption, usually using a virtual private network (VPN).

Although the intranet can be quickly configured to share data in a controlled environment, this information is still at risk unless there is strict security [12]. The downside of intranet networks is that important data may not reach the people who need it. The intranet has a place in multiple organizations. However, for a wider range of data exchanges, it is best to keep the network open and have the following security measures:

1. Detect and report whether the firewall has an intrusion attempt
2. Check for complex viruses in the firewall
3. Open the rules for additional employee emails
4. Encrypt all communication and data transmission
5. Authenticate by synchronization, password synchronization, or security certificate

If the intranet wants to access the Internet, it typically uses a virtual private network [13, 14]. Interfaces in multiple locations usually work on separate leased lines, or you can use the updated VPN method. The following technologies are different

1. Encryption system
2. Firewall
3. Intrusion detection system
4. Malignant and scanning procedures
5. Secure Sockets Layer (SSL) SSL

The network security zone continues on the same path. Use the same method and add biometric data. Biometric technology provides better

authentication than passwords, which can greatly reduce unauthorized access to the security system. New technologies such as smart cards are emerging in the field of Internet security research. The sidebar security network is very dynamic. A new firewall and encryption system is being implemented.

1.6 Evolution of Security Protocols for Network

The evolution of the network security protocol can be divided into three age groups [10]:

1. Filter packaging
2. Check the meeting
3. Application control

Although the development of anything is a continuous process, it is not a matter of cleaning up the next cycle. The spiritual perspective can determine certain characteristics that people lead in time.

This shows how the basic concepts of the Internet have changed the security and analysis of the five most advanced Internet security systems that must work in every network assessment.

1. Next Generation Firewall (NGFW)
2. Secure Web Portal (SWG)
3. Network Access Control (NAC)
4. Malware protection program
5. Secure access to the intermediary (CASB)

There are some network security systems, NGFW, NAC, and SWG, which have been developed for many years to accommodate the latest security threats. Other tools, such as sandbox protection and CASB, have some new concepts in the Public Safety Act.

1.6.1 Understanding the Key Components of Network Security

Traditional firewalls have been the most important and important line of defense for decades. Most corporate structures require secure servers at the edge of the core network to connect to other networks, especially if other networks are managed by a third party or are considered less centralized and secure.

This typically involves using a firewall to partition Internet connections, external networks, and remote WAN sites. The original firewall has no state, which means the firewall has no intelligence to monitor the data flow. As a result, the first wall of the fire was hit by a suicide bomber, and the attackers indicated that they were entering the rules allowed by the firewall.

Powerful firewalls are becoming common because they can monitor and track traffic between two devices that communicate with each other through a firewall. The state table not only controls the correct transport stream, but also ensures that the transmitted and received packets are connected to the original device. This is done by examining the network layer, the packets on OSI Layers 3 and 4, and tracking the IP address data. The TCP serial number and port number are processed. When transmitting a confirmed firewall packet, this information falsifies the hardware firewall to receive more harmful packets in the perimeter.

Although traditional firewalls are only designed to allow certain ports and protocols, they are not sure whether the visited site is harmful or inappropriate. This leaves a big gap, especially in terms of network traffic. The firewall can only allow or deny any traffic; it cannot selectively or see the upper layer protocol. This led to the creation of the SWG.

The first generation of SWGs had only one feature: filtering URLs. In most applications, Web Gateway is used to block access to websites that are included in a predefined blacklist. The company is responsible for maintaining SWG manufacturers, usually a blacklist database that is regularly updated on the gateway's network equipment. The administrator can choose which blacklist category to apply. There are some blacklist categories that include sites that include pornography, gambling, and hate groups, as well as sites that are often referred to as malware.

1.6.2 A Deep Defense Strategy

Over the years, network security systems such as traditional firewalls and secure web portals have run independently and performed different security functions [16]. Although this structure is better than nothing, it only provides a layer of defense for any threat. In order to add some extra layers of protection, there are some concepts of deep defense strategies. Our idea is to implement an interlocking security system to expose risks to multiple security measures designed to prevent malicious behavior.

Firewalls and traditional security gates are used for the Internet, email, and intrusion prevention systems (IPS). Protecting the infrastructure boundaries of an infrastructure company typically involves accessing cloud resources. All data entering and exiting the network is filtered through

firewalls and IPS. All traffic and email on the Internet will then be sent to the relevant security portal for further review to identify possible attachments contained in email attachments and malware.

With proper tuning and maintenance, deep defense engineering strategies using these components provide strong security. However, hackers began to discover that the network could find cracks between each system it entered. There are three main reasons for this. First of all, some security systems are difficult to fully implement. Usually, only some of the security features available in production are implemented.

Second, the security system cannot be maintained and updated correctly. For example, you must periodically update your firewall software to fix newly discovered vulnerabilities. Security portals and databases are often reviewed and sometimes require manual intervention updates.

Finally, while these systems overlap and provide multiple layers of protection, they work independently and are not shared and can be used to discover information between systems that have difficulty detecting threats.

1.6.3 How Does the Next Generation Network Security System Work Best

The next generation of security tools not only goes deeper into defense strategies, but goes further with tightly integrated and improved systems. Integrated with next-generation firewall capabilities to monitor and detect legacy firewalls, revealing regular IPS functionality by identifying signatures that contain known attack patterns. It is also known as NGFW for applications that use the firewall feature to check the deep technology package you are using. This allows the firewall to check the package not only by loading the subsidiary but also by the application to which the package belongs. This policy allows NGFW to securely interact with IPS and web portals by providing multiple layers of protection.

The web security gateway uses standard URL filtering for standards and direct protection against malware. The SWG acts as an IPS, focusing on web-based exceptions and virus signatures. When the new company discovers these signatures, it is automatically sent to the SWG device. Another new feature of most WWG groups is the ability to access global threat sensor networks. The threat of these sensors is typically maintained through security, identifying new threats and SWG groups locally and globally to better protect against real-time web threats. This type of security is an effective blow to increase rescue attacks.

Malware protection is a relatively new security tool for security administrators in many organizations. A limited number of malware environments

are designed to create an isolated environment simulation test environment that allows the system to perform multiple tests on suspicious packets. This approach sets a serious burden and hinders access to the production environment. The protective case can detect other tools such as NGFW and SWG. You can ignore this threat. Some malware installations require a sandbox filter. All data sandboxes are responsible for repairing suspicious downloads. In other designs, the limited malware environment relies on NGFW and SWG to classify the load as suspicious and then move it to the basement for further testing.

Next-generation networks are also beginning to rely on greater control over network access than their predecessors. I created a BYOD explosion. Concerns about cyber security vulnerabilities, rather than security personnel in the network, are very serious in identifying, evaluating, approving, and monitoring personnel who have access to network resources for production.

The NAC user and the correct device must be properly selected before allowing access to the network. If authenticated, the user or device receives a user access policy. Access policies provide access to resources that are accessible in the production network. In addition, you can access and follow resources. This is used to understand potential theft. In fact suspicious behavior refers to intellectual property or may be another harmful behavior.

The Internet was born in a military and academic environment. In this environment, users are always reliable and work together to make technology mutually beneficial. Therefore, IP and standard IP applications are safe from the start. Today, unsecure IP is still at the heart of Internet operations, with a range of long-term IP services such as:

1. Search Name—DNS Domain Name Service
2. File Transfer—FTP (FTP)
3. Email: SMTP Simple Mail Transfer Protocol (SMTP)
4. Web browsing: Hypertext Transfer Protocol (HTTP)

When the Internet was first developed, the basic technology running on the Internet was more secure than the trust era. However, the Internet has grown tremendously, with millions of people, many of whom are unreliable. Internet crime, corruption, espionage, extortion, etc., are getting bigger and bigger.

Therefore, Internet users must pay attention to managing their data security needs. Various unwelcome people roam the streets of the Internet without protection, so they must have strong defenses, valuable data, and services. Over the years, as the value of data and services on the Internet has grown, so does the current threat and the network industry has developed

a range of hardware and security software to address threats for network security in three eras.

1.7 Network Security Protocols

Due to the advancement and continuous growth of Internet, personal as well as business communication has increased the need for "Privacy" and "Information Security" for Eastern digital communication channels [18].

Both are critical to continuing personal communications and e-commerce that thrive in the Internet world Calls, security and privacy have come up with many security protocols and standards. These include Secure Communication Layer SSL Protocol (Transport Layer Security) TLS); IP Security (IPSec); HTTP Security (S-HTTP), Secure Email (PGP and S/MIME), DNDSEC, SSH, etc.

We will discuss these protocols and standards in a network protocol cluster in the following ways:

1.7.1 Application Layer

1. PGP
2. S / MIME
3. S-HTTP
4. HTTPS
5. SET
6. Kerberos

1.7.1.1 Good Privacy (PGP)

The Sensitive communications should not be underestimated. The best way to protect this type of information so far is to encrypt it. Email and any other form of communication encryption are critical to everyone's personal information. This is where you come from PGP, which is why PGP is very popular today. Phil Zimmermann is a public key encryption system for PGP. This feature creates the circle of trust between users. In such circle of trust, the two primary users are the loops of the public key pairs stored by each user and using keys in a person's keychain.

Unlike basic PKI infrastructure keys, such circle contains potential vulnerabilities and it can be exploited by hackers. In PGP there is a digital signature for verifying documents or files. This helps ensure that emails or

files that have just been received from the Internet are secure and will not change.

1.7.1.2 Email/Multipurpose Security (S/MIME)

Expand Multipurpose Internet Mail Extensions/Security Protocol Multipurpose Internet Mail Extensions (MIME) when adding digital signatures and encryption. MIME is communication protocols for transmission of multimedia data, which includes sound, images, and video. The reader must be interested in RFC protocol. MIME returns RFC 1521. Because web content (files), including hyperlinks to other hypertext links, describe the protocol message as MIME, you must state any type of relationship. This is what the MIME server does every time a client requests a web document. When the web server sends the requested file to the client browser, it adds a MIME header to the document and moves it. So, online email consists of following two parts, i.e., the "address" and the "body". In "address" part, there is information about MIME type and subtype. The MIME type describes the type of file that transfers the content type, such as images, sounds, applications, etc. Subtypes contain certain types of files, such as jpeg/GIF/tiff.

The development of S/MIME is the most lack of security services. Add two encryption elements: Encrypt and Encrypt Digital Encryption S/MIME. It supports three types of encryption algorithms, using common encryption keys for message navigation: Davey–Holman, RSA, and Triple DES. Digital signatures generate summary messages for SHA-1 or MD5 decentralized functions.

1.7.1.3 HTTP Secure (S-HTTP)

Secure HTTP (HTTP S-HTTP) is very simple for web development when developing HTTP. I do not have dynamic graphics. I did not need to encrypt the hard drive at the time. From end to end, it was developed for trading.

As the network becomes more popular in the company, users realize that if HTTP Current still represents the backbone of e-commerce, it needs additional improvements in encryption and graphics.

Each encrypted file of S-HTTP contains a digital certificate. A secure connection between the client and the HTTP server, especially business transactions is done through a various mechanisms to provide security when separating policies from mechanisms. It consists of a two-part HTTP

message: the message title and text. This address contains a description of how the message text (browser and server) is processed in the transaction, client, and browser. HTTP negotiation will be used to transfer the actual format of the desired information.

It uses other S-HTTP headers to encrypt digital mail, certificates, and HTTP authentication, and provides instructions about how to decrypt the text of the message.

1.7.1.4 Hypertext Transfer Protocol (HTTPS) in Secure Sockets Layer

Secure Sockets Layer (SSL) uses HTTPS as a subset of HTTP commonly used in the application layer. Also known as a protocol that transfers hypertext documents to HTTPS (HTTPS) or HTTP-based HTTP protocols.

A web protocol named HTTPS developed by Netscape. To encrypt and decrypt requests for user/web pages, it is integrated with the browser software. Port 443 in place of HTTP 80 port uses by the HTTPS protocol to interact with lower layer TCP/IP.

1.7.1.5 Secure E-Commerce (SET)

SET is an encryption protocol developed by companies such as Visa, Microsoft, IBM, RSA, Netscape, and MasterCard. These complex specifications are contained in three books on book introduction, a highly specialized system, and a programmer's guide, giving three formal instructions to the Convention. The SET sends services for each transaction, i.e. authentication, confidentiality, message integrity, and SET connection. Use public key cryptography and certificate signing to identify everyone involved in the transaction and allow each communication between them to be private.

1.7.1.6 Kerberos

The Kerberos network authentication protocol is designed to allow users, clients, and servers to authenticate each other. Verification process is accomplished by encrypting the keys because some keys are mutually authenticated over an insecure network connection. After verifying identity with the client and Kerberos server, the connection between both the parties can be secure. From this issue, you can communicate

between future encryptions to ensure the privacy and integrity of your data.

Client/Server Authentication requirements are as follows,

1. Security: Kerberos is no longer powerful enough to prevent potential spies from seeing it as a weak link.
2. Reliability: The Kerberos server architecture is distributed in large quantities with the support of other servers. This means that the Kerberos system is secure, which means a slight deterioration.
3. Transparency: In addition to providing a password, the user does not know that the HE will be authenticated.
4. Scalability: Kerberos is accepted. It identifies new clients and servers.

To meet above mentioned requirements, the stylist came to Kerberos. It is a trusted external authentication service for arbitration when mutual authentication occurs between the client and the server.

1.7.2 Transport Layer

These protocols are located below the application layer. The SSET unit IETF is measured after the consortium Netscape, and the IETF Engineering. Engineering Working Group IETF is modified by TLS.

1.7.2.1 Secure Sockets Layer (SSL)

SSL is also an encryption system which is used in Internet search engines like Netscape and Explorer provides an encrypted data path between the endpoint, client, and server. Data encryption, server authentication, message integrity, and authentication over TCP, LDAP, or POP3 clients provide a secure and authenticated service application layer compete with S-HTTP.

These giants have many common networks. First, S-HTTP is only available for the Web protocol. Since the SSL in the network group is smaller than S-HTTP, it can run on many other network protocols. In addition, second, in terms of implementation, because SSL is lower than S-HTTP. Replace applications that require a secure connection, such as a socket interface. On the other hand, it places the S-HTTT in the previous data in the named text field in the HTTP header.

Although SSL was introduced in a wide range of browsers, the Netscape S-HTTP browser was introduced in a smaller, narrower NCSA interface. This unfortunate choice condemns the fate of the S-HTTP SSL handshake.

There must be approximately three contact addresses before creating any TCP connections between the client and the service and working with SSL. This process is also known as a protocol for linking SSL. During the connection agreement, the client and server perform the following tasks: Set the encryption set to use. The server-enforced authentication provides a server that sends the certificate to the client to verify that the server certificate is signed by a trusted certificate authority. If necessary, provide the client with optional client authentication, which sends its own certificate to the server to verify that the client certificate is signed by a trusted certificate authority.

When using public key encryption, the primary information is exchanged after authentication, which causes the client to create a session key (usually a random number) that is used to negotiate all subsequent encryption or decryption. The client encrypts the session key using the commercial server's public key (from the merchant certificate). The server retrieves the session key by decrypting the session key using its private key. Both parties now use this symmetric key for all subsequent connections.

1.7.2.2 Transport Layer Security (TLS)

TLS is the result of the Internet Engineering Task Force (IETF). In 1996, you were trying to unify secure network communication. In 1999, RFC 2246 formed a new protocol named "Transport Layer Security" [TLS]. It is responsible for providing security and data integrity in the transport layer between two applications [4]. "Interoperability" is an additional features which have been added in the basic version means any party exchanges the capability parameter TLS without anyone having to understand the implementation details of TLS to the other party, and "Expandability", i.e., plan for future expansion and adapt to new engagements.

1.7.3 Network Layer

1. IP security
2. VPN

Above mentioned protocols are also address Internet communications security issues. These protocols include IPSec and VPN.

1.7.3.1 Internet Protocol Security (IPSec)

IP Security is the Internet Engineering Task Force Group (IETF) designed and developed to address the lack of inherent security protocols, authentication, and encryption based on Internet protocols [18]. IPSec is a very complex set of protocols described in many documents, including RFC 2401 and 2411. Although designed to run on a new version of Internet Protocol IP Version 6 (IPv6), it is also correctly implemented in the previous IPv4.

Try to provide IPSec protection by providing the following services at the network layer:

1. Access Control: Prevent unauthorized access to resources.
2. Security without connection: Make sure that the traffic is not modified in any way.
3. Confidentiality: Ensure that unauthorized third parties do not investigate Internet traffic. This requires encrypting the data fields of all packets IP, TCP, UDP, ICMP, or any other data field.
4. Verification: Especially the verification of key elements, so when the server receives the target IP for the specific purpose of the data source IP, it can ensure that the IP datagram is indeed created by the server with the source IP address to avoid this fake IP address.
5. Copy protection: Make sure that each package is different between the two.

These goals achieved by the IPSec protocol with dividing it into two protocols: the header AH authentication protocol i.e. the security of the protocol and the protection of the surrounding ESP, which provides the integrity of the source and data authentication protocol AH, but does not provide confidentiality. Provide ESP authentication, data integrity, and confidentiality. Any data unit in the source must be protected with AH or ESP. There are two ways to run IPSec, i.e., Transport and Tunneling. Transport mode provides host-to-host protection for top-level protocols between IPv4 and IPv6 hosts. Tunnel mode provides complete IP data mapping protection in AH and ESP between IPSec gateways because new IP headers have been added to both IPv4 and YIPv6. Between the two ports, the datagram is secure and has an IP address. The original is also very safe.

Data units may not be safe abroad. This protection is created when an IPSec gateway is created. First to encapsulate the data planner (including your IP address) into a new set of compelling data that is titled a new

IP gateway with IP security. At the receiving gateway, the new packet is unpacked and returned to the original data map.

1.7.3.2 Virtual Private Network (VPN)

VPN private networks add security measures through secure communication channels, leveraging public communication infrastructure data such as the Internet. Security measures including encryption are implemented using a tunneling protocol. There are two types of virtual private networks (VPNs) [13, 14]. Remote access allows one user to connect to a protected corporate network and a site that supports connections between two protected network networks. In any case, VPN technology is available. The cost of a private leasing company is much lower when using a public infrastructure such as the Internet.

The two components of a VPN are: These two terms are programs or devices. It implements encryption, decryption and authentication services. It also includes information. Tunnel: The endpoint is connected. A tunnel is a secure connection between an endpoint and a network, such as the Internet. In fact, this tunnel is actually created from the endpoint.

You must do the following:

1. IP packaging: Includes a TCP/IP packet contained in another package that contains the IP address of the firewall or the server acting as a VPN endpoint. This package helps hide host IP address hosts.
2. Encryption: The data portion of the package. Like SSL, encryption can be done in transport mode, which encrypts data as it is created, or encrypts and decrypts data by encrypting data and headers during transmission.
3. Authentication: Includes the creation of an encrypted domain that includes authentication of computers and packets using regular encryption.

Technical security is divided into three types of VPNs: Trust VP N; VPN security and hybrid VPN.

Trusted VPN: In these VPNs, customers rely on VPN providers to protect their privacy and security while maintaining the integrity of their components. This security depends on trust.

Secure VPN: Virtual Private Network (VPN) not only provides virtual security, so there are still security issues in VPN. To solve these problems, any other data encrypted by the Internet source or mobile traffic is

similar to the data used to decrypt when accessing the corporate network or host protocol.

In this way, encrypted traffic seems to have passed through the tunnel between the two networks. Initially and destination, although the data is clear, the attacker can see the transfer but still cannot read it. The recipient does not change the traffic that cannot be changed, so you can see a lot and will be rejected. The created network is called Secure VPN Encryption. VPN Secure is more secure than trusted VPN.

Hybrid VPN: Hybrid VPN is the latest Internet VPN technology that can be used as an alternative to a telephone system. Fixed VPN component VPNs do not provide new security, but provide customers with a way to easily create a network chip for the WAN. WAN On the other hand, components can control VPN VPN from one place, and QoS is usually guaranteed by the provider.

1.7.4 Data Link Layer

1. PPP
2. Radio
3. TACACS +

Link layer and LANS security There are several protocols used in the data link layer, such as PPP and RADIO AND TACAS +.

1.7.4.1 Point-to-Point Protocol (PPP)

This is the old agreement for Internet users to use the modem and PPP to dial the Internet. This protocol is limited to a single data link. Each call goes directly to the Remote Access Server (RAS). This feature is used to verify the call when a call is received.

The PPP connection containing the link protocol begins to negotiate between the client and the RAS to send and resolve security issues before the data begins to be sent.

These negotiations are performed using the LCP Link Control Protocol. Negotiations can result in approval or disapproval because purchasing power parity does not require approval.

1.7.4.2 Remote Authentication User Service (RADIO)

RADIO is a server for remote user authentication and accounting. Class-based online class security protocols, including Password Authentication

Protocol (PAP) and Challenge Identification Authentication Protocol (CHAP). It is primarily used by Internet Service Providers (ISPs) to provide authentication. Consider a remote user. It can also be used in private networks for authentication and accounting services in a centralized network to serve all dial-up connections. It has two main components: authentication and accounting.

1.7.4.3 Terminal System Access Control Access Control Equipment (TACACS +)

This protocol is called the "tac-plus" authentication protocol and is a common method. It is a powerful protocol for providing tags: Verifies any changes in authentication and content duration, allowing for many authentication mechanisms. Therefore, auditing: Recording the work done by users in TACASCS + has two purposes: to consider the services used by security auditing equipment.

1.8 Current Evolution of Red Security

The network security zone continues on the same path. Use the same method and add biometric data. Biometric technology provides better authentication than passwords, which can greatly reduce unauthorized access to the security system. New technologies such as smart cards have emerged in cyber security research. The security aspects of network software are very dynamic. A new firewall and encryption system is being implemented. The research carried out helps to understand current developments and predict future developments in the field.

1.8.1 Hardware Development

The development of this device has not developed rapidly. Dynamic systems and smart cards are the only new hardware technologies that have a major impact on security.

The most obvious use of cyber security biometrics is to start recording secure workstations from networked workstations. Each workstation requires some software support to dynamically identify the user and identify some of the biometric devices used. Hardware costs are a cause of widespread use of biometric measurements, especially for companies and institutions that offer low budgets. The next step will

be the next device, such as a computer mouse with a built-in fingerprint reader. Because each device requires its own device, deploying it to multiple computers is more expensive. The price of biometric mice and the software they support is about $120 in the United States. UU speech recognition programs are controlled to reduce the cost of implementation per device. At the top of the series, biometric bio packages cost $50,000, but you can manage secure registrations for up to 5,000 devices.

The primary use of biometric network security is to replace existing encryption systems. Keeping passwords safe is an important task even for small businesses. The password must be changed every few months, and people will forget the password or enter the password multiple times to remove the password from the system. People usually type in a password and store it near a computer. Of course, this completely undermines any effort in cyber security. Biometric technology can replace this method for secure identification. By using biometrics to solve this problem, although this is the first time cost-effective, these devices can provide management costs and user assistance.

Smart cards are usually digital electronic media-sized credit cards. The card itself is used to store encryption keys and other authentication and identity information. The main idea behind smart cards is to provide undeniable user identification. From logging in to your network to protect secure network connections and email transactions, smart cards can be used for a variety of purposes.

It seems that the smart card is just a repository for storing passwords. Someone can easily steal someone else's smart card. Fortunately, smart cards include built-in security features that prevent anyone from using stolen cards. Smart cards require anyone to use a PIN before granting access to any level of the system. It looks like the PIN code used by ATM.

When the user inserts the smart card into the card reader, the smart card user is required to enter the PIN code. When the boss card is sent to the user, the administrator sets a password for the user. Because the PIN number is short and the number is pure, the user must not face any problems in the ticket sales, so it is impossible to write the PIN.

But what is interesting is what happens when the user enters a PIN. The PIN code is verified in the smart card. Since the PIN is not transmitted over the network, there is no risk of intercepting the PIN. However, the main benefit is that if there is no smart card, the PIN is inefficient and the smart card is used without code. There are other security issues with PIN smart cards. Smart cards are profitable, but they are not as secure as biometric devices.

1.8.2 Software Development

Every aspect of the cyber security program is very broad including firewall, anti-virus, VPN, intrusion detection, and so on. It is currently not possible to search all security software. The goal is to achieve the goals of the security plan based on current priorities [17].

Improvements to the standard safety plan remain unchanged. Antivirus software is updated to protect against these threats when new viruses appear. The firewall process is the same as the intrusion detection system. Many of the research papers developed are based on an analysis of attack patterns to create smarter security programs [17].

When a security service enters biometrics, the program also needs to be able to use this information appropriately. Study safety procedures using neural networks. The purpose of this study was to use neural network face recognition software.

Many small and complex devices can connect to the Internet. Most security algorithms are currently highly computational and require a lot of processing power. However, this power is not suitable for small devices such as sensors. Therefore, it is necessary to design a lightweight security algorithm. Research in this area is ongoing.

1.9 Future Security Trends

What will improve Internet security is the most important set of applications [15]. The future may be similar to the immune system. The immune system can fight attacks and fight against powerful enemies. Similarly, cyber security can act as an immune system. The trend in biotechnology development may not be long ago, but it seems that it has not been effectively implemented. Many ongoing security developments are part of the same security technology with minor modifications.

References

1. Dowd, P.W. and McHenry, J.T., Network security: It's time to take it seriously. *Computer*, 31, 9, 24–28, 1998.
2. Kartalopoulos, S.V., Differentiating Data Security and Network Security, Communications, ICC '08. *IEEE International Conference on*, 19–23, pp. 1469–1473, 2008.

3. Security Overview, www.redhat.com/docs/manuals/enterprise/RHEL-4- Manual/security-guide/ch-sgs-ov.html, 2011.
4. Molva, R. and Institut Eurecom, Internet Security Architecture. *Computer Networks & ISDN Systems Journal*, 31, 787–804, 1999.
5. Sotillo, S. and East Carolina University, IPv6 security issues, www.infosecwriters.com/text_resources/pdf/IPv6_SSot illo.pdf, 2006.
6. Andress, J., IPv6: The Next Iinternet Protocol, www.usenix.com/publications/login/2005-04/pdfs/andress0504.pdf, 2005.
7. Warfield, M., Security Implications of IPv6, Internet Security Systems White Paper, documents.iss.net/whitepapers/IPv6.pdf, 2003.
8. Adeyinka, O., Internet Attack Methods and Internet Security Technology, Modeling & Simulation, AICMS 08, *Second Asia International Conference on*, 13–15, pp. 77–82, 2008.
9. Marin, G.A., Network security basics, Security & Privacy. *IEEE*, 3, 6, 68–72, 2005.
10. Internet History Timeline, https://www.baylor.edu/cms/index.php?id=93716, 2011.
11. Landwehr, C.E. and Goldschlag, D.M., Security issues in networks with Internet access. *Proc. IEEE*, 85, 12, 2034–2051, 1997.
12. "Intranet" Wikipedia, The Free Encyclopedia. 23 Jun 2008, 10:43 UTC. Wikimedia Foundation, Inc. <http://en.wikipedia.org/w/index.php?title=Intranet&oldid=221174244>, 2008.
13. Virtual private network. Wikipedia, The Free Encyclopedia. 30 Jun 2008, 19:32 UTC. Wikimedia Foundation, Inc. <http://en.wikipedia.org/w/index.php?title=Virtual_private_network&oldid=222715612>, 2008.
14. Tyson, J., How Virtual private networks work, http://www.howstuffworks.com/vpn.htm, 2014.
15. Al-Salqan, Y.Y., Future trends in Internet security, Distributed Computing Systems, *Proceedings of the Sixth IEEE Computer Society Workshop on Future Trends of*, 29–31, pp. 216–217, 1997.
16. Curtin, M., Introduction to Network Security, http://www.interhack.net/pubs/network-security, 1997.
17. Improving Security, http://www.cert.org/tech_tips, 2006.
18. Serpanos, D.N. and Voyiatzis, A.G., Secure network design: A layered approach, Autonomous Decentralized System, *The 2nd International Workshop on*, 6–7, 2002, pp. 95–100, 2002.
19. Ohta, T. and Chikaraishi, T., Network security model, Networks, *International Conference on Information Engineering '93. 'Communications and Networks for the Year 2000', Proceedings of IEEE Singapore International Conference on,* 2, 6–11, pp. 507–511, 1993.