ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (167-178), Month: April-June 2014, Available at: www.researchpublish.com

NETWORK SECURITY AND CRYPTOGRAPHY

Mr Ram Kumar[1], V.Sowmya[2]

Computer Science and Engineering, Saveetha School Of Engineering, Thandalam, Chennai, INDIA

Abstract: **This paper aims to provide a broad review of network security and cryptography, with particular regard to digital signatures. Network security and cryptography is a subject too wide ranging to coverage about how to protect information in digital form and to provide security services. However, a general overview of network security and cryptography is provided and various algorithms are discussed. A detailed review of the subject of network security and cryptography in digital signatures is then presented. The purpose of a digital signature is to provide a means for an entity to bind its identity to a piece of information. The common attack on digital signature was reviewed. The first method was the RSA signature scheme, which remains today one of the most practical and versatile techniques available. Fiat-Shamir signature schemes, DSA and related signature schemes are two other methods reviewed. Digital signatures have many applications in information security, including authentication, data integrity, and non-repudiation was reviewed.**

Keywords: **network security, cryptography, digital signatures.**

I. INTRODUCTION

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/ data, and telecommunications).

This definition introduces three key objectives that are at the heart of computer security:

• **Confidentiality:** This term covers two related concepts:

Data1 confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

• **Integrity:** This term covers two related concepts:

Data integrity: Assures that information and programs are changed only in a specified and authorized manner.

System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

• **Availability:** Assures that systems work promptly and service is not denied to authorized users.

These three concepts form what is often referred to as the CIA triad. The three concepts embody the fundamental security objectives for both data and for information and computing services. For example, the NIST standard FIPS 199 (*Standards for Security Categorization of Federal Information*

Confidentiality

Data, and services

Integrity

Availability

The Challenges of Computer Security

Computer and network security is both fascinating and complex. Some of the reasons follow:

1. Security is not as simple as it might first appear to the novice. The requirements seem to be straightforward; indeed, most of the major requirements for security services can be given self-explanatory, one-word labels: confidentiality, authentication, nonrepudiation, or integrity. But the mechanisms used to meet those requirements can be quite complex, and understanding them may involve rather subtle reasoning.

2. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features. In many cases, successful attacks are designed by looking at the problem in a completely different way,

therefore exploiting an unexpected weakness in the mechanism.

3. Because of point 2, the procedures used to provide particular services are often counterintuitive. Typically, a security mechanism is complex, and it is not obvious from the statement of a particular requirement that such elaborate measures are needed. It is only when the various aspects of the threat are considered that elaborate security mechanisms make sense.

4. Having designed various security mechanisms, it is necessary to decide where to use them. This is true both in terms of physical placement (e.g., at what points in a network are certain security mechanisms needed) and in a logical sense [e.g., at what layer or layers of an architecture such as TCP/IP (Transmission Control Protocol/Internet Protocol) should mechanisms be placed].

5. Security mechanisms typically involve more than a particular algorithm or protocol. They also require that participants be in possession of some secret information (e.g., an encryption key), which raises questions about the creation, distribution, and protection of that secret information. There also may be a reliance on communications protocols whose behavior may complicate the task of developing the security mechanism. For example, if the proper functioning of the security mechanism requires setting time limits on the transit time of a message from sender to receiver, then any protocol or network that introduces variable, unpredictable delays may render such time limits meaningless.

6. Computer and network security is essentially a battle of wits between a perpetrator who tries to find holes and the designer or administrator who tries to close them. The great advantage that the attacker has is that he or she need only find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security.

7. There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs.

8. Security requires regular, even constant, monitoring, and this is difficult in today's short-term, overloaded environment.

9. Security is still too often an afterthought to be incorporated into a system after the design is complete rather than being an integral part of the design process.

10. Many users and even security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information.

II. SECURITY ATTACKS

A useful means of classifying security attacks, used both in X.800 and RFC 2828, is in terms of *passive attacks* and *active attacks.* A passive attack attempts to learn or make use of information from the system but does not affect system resources. An active attack attempts to alter system resources or affect their operation.

Passive Attacks

Passive attacks are in the nature of eaves dropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are the release of message contents and traffic analysis.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (167-178), Month: April-June 2014, Available at: www.researchpublish.com

The release of message contents is easily understood. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

A second type of passive attack, traffic analysis, is subtler. Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption. If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

Passive attacks are very difficult to detect, because they do not involve any alteration of the data.Typically, the message traffic is sent and received in an apparently normal fashion, and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern. However, it is feasible to prevent the success of these attacks, usually by means of encryption.Thus, the emphasis in dealing with passive attacks is on prevention rather than detection

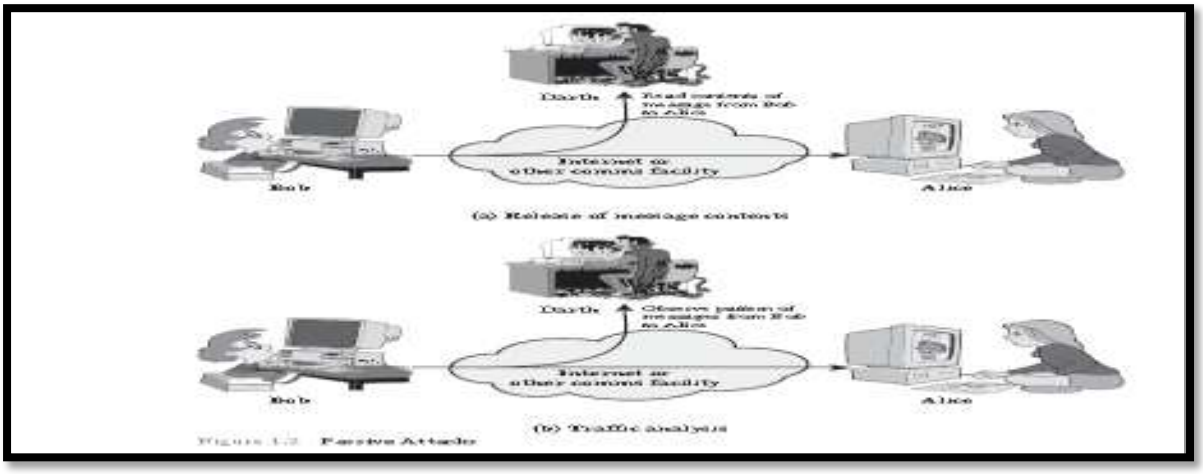
Active Attacks

Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

A masquerade takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges. Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect .

Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect . For example, a message meaning "Allow John Smith to read confidential file *accounts*" is modified to mean "Allow Fred Brown to read confidential file *accounts.*"

The denial of service prevents or inhibits the normal use or management of communications facilities . This attack may have a specific target.

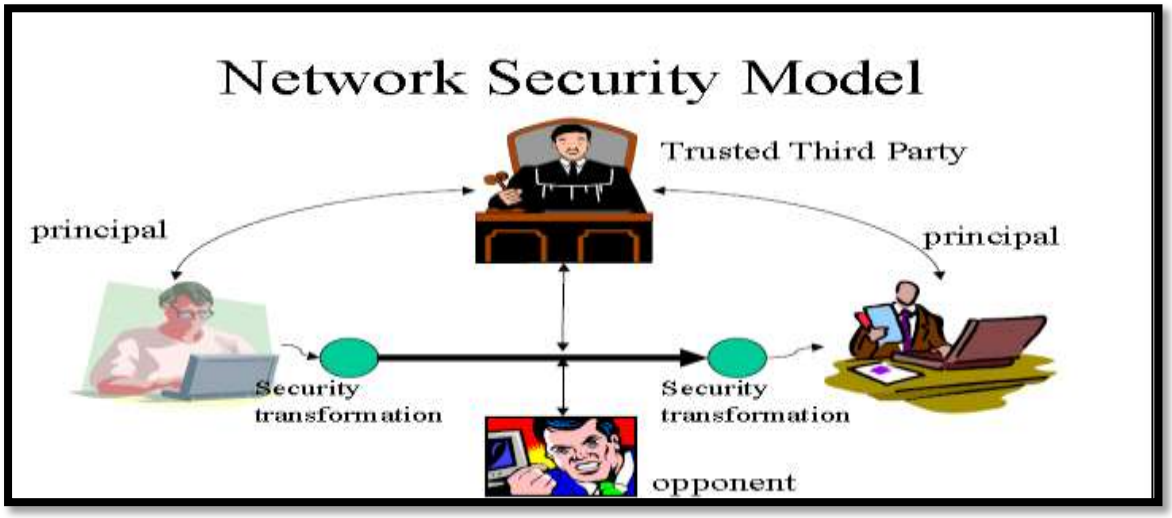


ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (167-178), Month: April-June 2014, Available at: www.researchpublish.com

III. A MODEL FOR NETWORK SECURITY

A model for much of what we will be discussing is captured, in very general terms. A message is to be transferred from one party to another across some sort of Internet service. The two parties, who are the *principals* in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the Internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals. Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on. All the techniques for providing security have two components:

• A security-related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.



IV. SYMMETRIC CIPHER MODEL

A symmetric encryption scheme has five ingredients

• *Plaintext:* This is the original intelligible message or data that is fed into the algorithm as input.

• Encryption algorithm: The encryption algorithm performs various substitutions and transformations on the plaintext.

• *Secret key:* The secret key is also input to the encryption algorithm.The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time.The exact substitutions and transformations performed by the algorithm depend on the key.

• *Ciphertext:* This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.

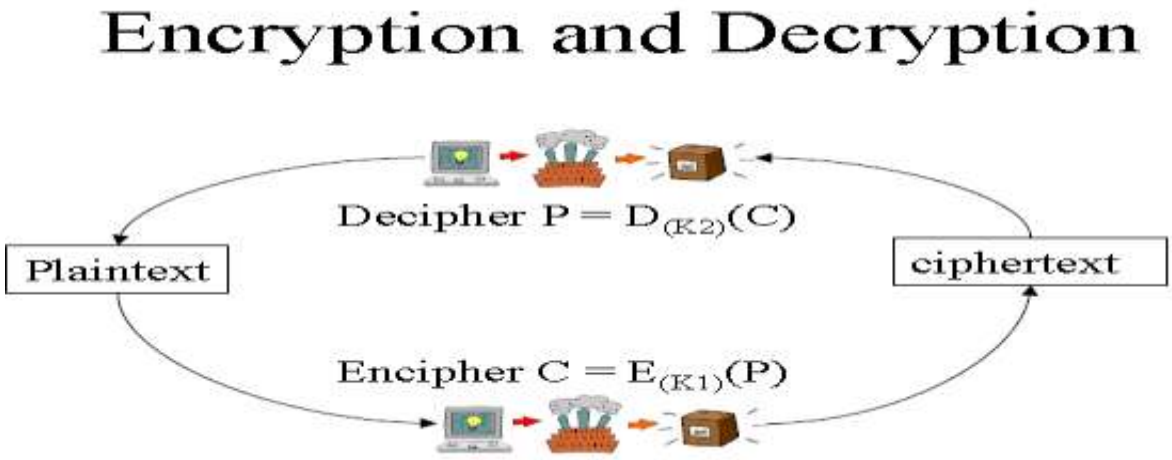
• *Decryption algorithm:* This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plain text.

There are two requirements for secure use of conventional encryption:

1. We need a strong encryption algorithm. At a minimum, we would like the algorithm to be such that an opponent who knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext or figure out the key. This requirement is usually stated in a stronger form. The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.

2. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm, all communication using this key is readable.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (167-178), Month: April-June 2014, Available at: www.researchpublish.com



V. STEGANOGRAPHY

We conclude with a discussion of a technique that (strictly speaking), is not encryption, namely, steganography.

A plaintext message may be hidden in one of two ways. The methods of steganography conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformations

of the text.10

A simple form of steganography, but one that is time-consuming to construct, is one in which an arrangement of words or letters within an apparently innocuous text spells out the real message. For example, the sequence of first letters of each

word of the overall message spells out the hidden message.

Various other techniques have been used historically; some examples are the following

• Character marking: Selected letters of printed or typewritten text are overwritten in pencil.The marks are ordinarily not visible unless the paper is held at an angle to bright light.

• Invisible ink: A number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.

Pin punctures: Small pin punctures on selected letters are ordinarily not visibleunless the paper is held up in front of a light.

• Typewriter correction ribbon: Used between lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light.

VI. WEB SECURITY CONSIDERATIONS

The World Wide Web is fundamentally a client/server application running over the Internet and TCP/IP intranets. As such, the security tools and approaches discussed, so far in this book are relevant to the issue of Web security. But, as pointed out in [GARF02], the Web presents new challenges not generally appreciated in the context of computer and network security.

• The Internet is two-way. Unlike traditional publishing environments—even electronic publishing systems involving teletext, voice response, or fax-back— the Web is vulnerable to attacks on the Web servers over the Internet.

• The Web is increasingly serving as a highly visible outlet for corporate and product information and as the platform for business transactions. Reputations can be damaged and money can be lost if the Web servers are subverted.

• Although Web browsers are very easy to use,Web servers are relatively easy to configure and manage, and Web content is increasingly easy to develop, the underlying software is extraordinarily complex. This complex software may hide many potential security flaws. The short history of the Web is filled with examples of new and upgraded systems, properly installed, that are vulnerable to a variety of security attacks.

• A Web server can be exploited as a launching pad into the corporation's or agency's entire computer complex. Once the Web server is subverted, an attacker may be able to gain access to data and systems not part of the Web itself but connected to the server at the local site.

• Casual and untrained (in security matters) users are common clients for Web-based services. Such users are not necessarily aware of the security risks that exist and do not have the tools or knowledge to take effective countermeasures.

Web Security Threats

One way to group these threats is in terms of passive and active attacks. Passive attacks include eavesdropping on network traffic between browser and server and gaining access to information on a Web site that is supposed to be restricted. Active attacks include impersonating another user, altering messages in transit between client and server, and altering information on a Web site.

Another way to classify Web security threats is in terms of the location of the threat: Web server, Web browser, and network traffic between browser and server.

Issues of server and browser security fall into the category of computer system security;

Web Traffic Security Approaches

A number of approaches to providing Web security are possible. The various approaches that have been considered are similar in the services they provide and, to some extent, in the mechanisms that they use, but they differ with respect to their scope of applicability and their relative location within the TCP/IP protocol stack. One way to provide Web security is to use IP security (IPsec) .The advantage of using IPsec is that it is transparent to end users and applications and provides a general-purpose solution. Furthermore, IPsec includes a filtering capability so that only selected traffic need incur the overhead of IPsec processing. Another relatively general-purpose solution is to implement security just above TCP . The foremost example of this approach is the Secure.

VII. WIRELESS LAN SECURITY

There are two characteristics of a wired LAN that are not inherent in a wireless LAN.

1. In order to transmit over a wired LAN, a station must be physically connected to the LAN. On the other hand, with a wireless LAN, any station within radio range of the other devices on the LAN can transmit. In a sense, there is a form of authentication with a wired LAN in that it requires some positive and presumably observable action to connect a station to a wired LAN.

2. Similarly, in order to receive a transmission from a station that is part of a wired LAN, the receiving station also must be attached to the wired LAN. On the other hand, with a wireless LAN, any station within radio range can receive. Thus, a wired LAN provides a degree of privacy, limiting reception of data to stations connected to the LAN.

These differences between wired and wireless LANs suggest the increased need for robust security services and mechanisms for wireless LANs. The original 802.11 specification included a set of security features for privacy and authentication that were quite weak. For privacy, 802.11 defined the Wired Equivalent Privacy (WEP) algorithm.The privacy portion of the 802.11 standard contained major weaknesses.

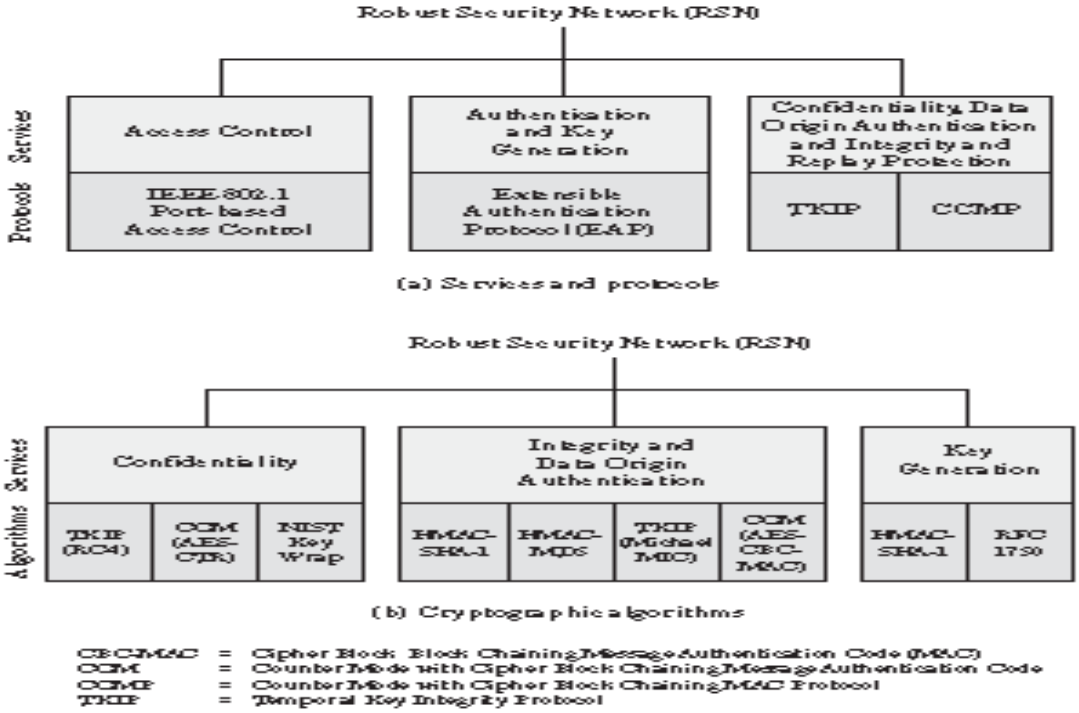
Subsequent to the development of WEP, the 802.11i task group has developed a set of capabilities to address the WLAN security issues. In order to accelerate the introduction of strong security into WLANs, the Wi-Fi Alliance promulgated Wi-Fi Protected Access (WPA) as a Wi-Fi standard.WPA is a set of security mechanisms that eliminates most 802.11 security issues and was based on the current state of the 802.11i standard. The final form of the 802.11i standard is referred to as Robust Security Network (RSN).The Wi-Fi Alliance certifies vendors in compliance with the full 802.11i specification under the WPA2 program.

• Authentication: A protocol is used to define an exchange between a user and an AS that provides mutual authentication and generates temporary keys tobe used between the client and the AP over the wireless link.

• Access control:1 This function enforces the use of the authentication function, routes the messages properly, and facilitates key exchange. It can work with a variety of authentication protocols.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (167-178), Month: April-June 2014, Available at: www.researchpublish.com

• Privacy with message integrity: MAC-level data (e.g., an LLC PDU) are encrypted along with a message integrity code that ensures that the data have not been altered.

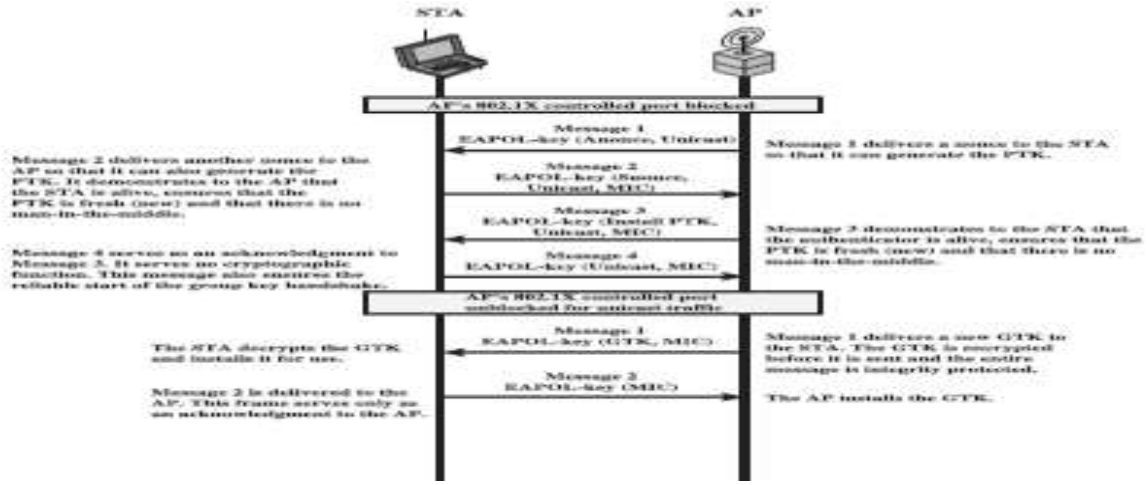


1. Two wireless stations in the same BSS communicating via the access point (AP) for that BSS.

2. Two wireless stations (STAs) in the same ad hoc IBSS communicating directly with each other.

3. Two wireless stations in different BSSs communicating via their respective APs across a distribution system.

4. A wireless station communicating with an end station on a wired network via its AP and the distribution system.



VIII. IP SECURITY OVERVIEW

In 1994, the Internet Architecture Board (IAB) issued a report titled "Security in the Internet Architecture" (RFC 1636). The report identified key areas for security mechanisms. Among these were the need to secure the network. Infrastructure from unauthorized monitoring and control of network traffic and the need to secure end-user-to-end-user traffic using authentication and encryption mechanisms. To provide security, the IAB included authentication and encryption as necessary security features in the next-generation IP, which has been issued as IPv6. Fortunately, these security capabilities were designed to be usable both with the current IPv4 and the future IPv6. This means that vendors can begin

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (167-178), Month: April-June 2014, Available at: www.researchpublish.com

offering these features now, and many vendors now do have some IPsec capability in their products. The IPsec specification now exists as a set of Internet standards.

Applications of IPsec

IPsec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet. Examples of its use include:

• Secure branch office connectivity over the Internet: A company can build a secure virtual private network over the Internet or over a public WAN. This enables a business to rely heavily on the Internet and reduce its need for private networks, saving costs and network management overhead.

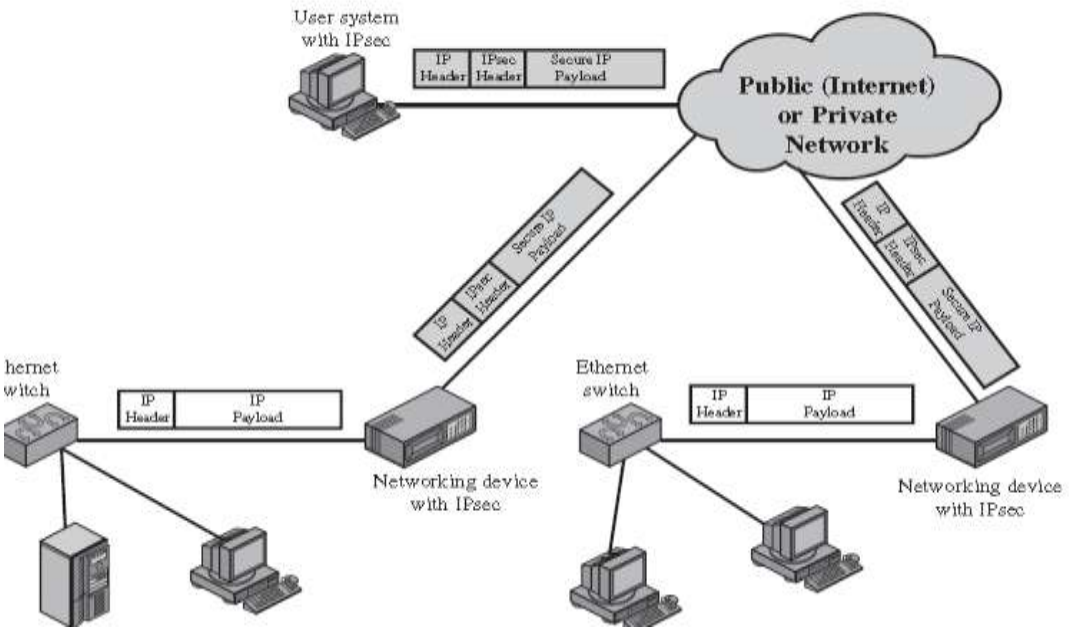
• Secure remote access over the Internet: An end user whose system is equipped with IP security protocols can make a local call to an Internet Service Provider (ISP) and gain secure access to a company network.This reduces the cost of toll charges for traveling employees and telecommuters.

• Establishing extranet and intranet connectivity with partners: IPsec can be used to secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism.

• Enhancing electronic commerce security: Even though some Web and electronic commerce applications have built-in security protocols, the use of IPsec enhances that security. IPsec guarantees that all traffic designated by the network administrator is both encrypted and authenticated, adding an additional layer of security to whatever is provided at the application layer.

The principal feature of IPsec that enables it to support these varied applications is that it can encrypt and/or authenticate *all* traffic at the IP level. Thus, all distributed applications (including remote logon, client/server, e-mail, file transfer,Web access, and so on) can be secured. An organization maintains LANs at dispersed locations. Nonsecure IP traffic is conducted on each LAN. For traffic offsite, through some sort of private or public WAN, IPsec protocols are used.

These protocols operate in networking devices, such as a router or firewall, that connect each LAN to the outside world. The IPsec networking device will typically encrypt and compress all traffic going into the WAN and decrypt and decompress traffic coming from the WAN; these operations are transparent to workstations and servers on the LAN. Secure transmission is also possible with individual users who dial into the WAN. Such user workstations must implement the IPsec protocols to provide security.



Benefits of IPsec

Some of the benefits of IPsec:

• When IPsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter.Traffic within a company or workgroup does not incur the overhead of security-related processing.

• IPsec in a firewall is resistant to bypass if all traffic from the outside must use IP and the firewall is the only means of entrance from the Internet into the organization.

• IPsec is below the transport layer (TCP, UDP) and so is transparent to applications.There is no need to change software on a user or server system when IPsec is implemented in the firewall or router. Even if IPsec is implemented in end systems, upper-layer software, including applications, is not affected.

• IPsec can be transparent to end users.There is no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material when users leave the organization.

• IPsec can provide security for individual users if needed.This is useful for offsite workers and for setting up a secure virtual subnetwork within an organization for sensitive applications.

IPsec Services

IPsec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services.Two protocols are used to provide security: an authentication protocol designated by the header of the protocol, Authentication Header (AH); and a combined encryption/authentication protocol designated by the format of the packet for that protocol, Encapsulating Security Payload (ESP). RFC 4301 lists the following services:

• Access control

• Connectionless integrity

• Data origin authentication

• Rejection of replayed packets (a form of partial sequence integrity)

• Confidentiality (encryption)

• Limited traffic flow confidentiality

IX. IMPORTANCE OF CRYPTOGRAPHY

In the information age, cryptography has become one of the major methods for protection in all applications.

Cryptography allows people to carry over the confidence found in the physical world to the electronic world. It allows people to do business electronically without worries of deceit and deception. In the distant past, cryptography was used to assure only secrecy. Wax seals, signatures, and other physical mechanisms were typically used to assure integrity of the message and authenticity of the sender.

When people started doing business online and needed to transfer funds electronically, the applications of cryptography for integrity began to surpass its use for secrecy. Hundreds of thousands of people interact electronically every day, whether it is through e-mail, e-commerce (business conducted over the Internet), ATM machines, or cellular phones. The constant increase of information transmitted electronically has lead to an increased reliance on cryptography and authentication.

During and before World War II, the main applications of cryptography were military. Both coding theory and cryptography originated with the seminal work of Claude Shannon in 1948. With the spread of computers and electronic communications after the war, the use of cryptographic schemes for passwords, banking transactions and various aspects of computer security proliferated. So did the uses of error-correcting codes in radio based communication systems and satellite communications. These uses and the evolving theory of codes generated much mathematical activity.

An obvious application of cryptography is the transformation of information to prevent other from observing its meaning. This is the classical concept of secrecy, wherein we attempt to prevent information from reaching an enemy in a usable form. Secrecy is viewed by many as the central issue in the field of information protection. Secure communication is the most straightforward use of cryptography. Two people may communicate securely by encrypting the messages sent between them. While secure communication has existed for centuries, the key management problem has prevented it from becoming commonplace. Thanks to the development of public-key cryptography, the tools exist to create a large-scale network of people who can communicate securely with one another even if they had never communicated before.

Cryptographic protocols: RSA

RSA is an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is an asymmetric algorithm that uses private and public keys, and is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Microsoft and Netscape. The mathematical details of the algorithm used in obtaining the public and private keys are available at the RSA Web site. Briefly, the algorithm involves multiplying two large prime numbers (a prime number is a number divisible only by that number and 1) and through additional operations deriving a set of two numbers that constitute the public key and the private key. Once the keys have been developed, the original prime numbers are no longer important and can be discarded. Both the public and the private keys are needed for encryption /decryption but only the owner of a private key ever needs to know it. Using the RSA system, the private key never needs to be sent across the Internet.

The private key is used to decrypt text that has been encrypted with the public key. Thus, if I send you a message, I can find out your public key (but not your private key) from a central administrator and encrypt a message to you using your public key. When you receive it, you decrypt it with your private key. In addition to encrypting messages (which ensures privacy), you can authenticate yourself to me (so I know that it is really you who sent the message) by using your private key to encrypt a digital signature. When I receive it, I can use your public key to decrypt (to verify) it.

A typical cryptographic protocol failure is encountered in the use of the RSA. It seems that if an attacker can choose the plaintext to be signed under an RSA signature system, observe the result of the signature, and then iterate the process, it is possible to get the signer to reveal the private key in a very small number of signatures (about 1 signature per bit of the key). Thus an unmodified RSA signature system requires a sound protocol to be safely used. However all commercial systems use the RSA encryption only for key exchange, while using a symmetric algorithm to sign the actual data - for example RC4.

SSL (Secure Sockets Layer)

The Secure Sockets Layer (SSL) is a commonly used protocol for managing the security of data transmission on the Internet. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.

SSL is most commonly used for securing website transactions. An SSL certificate enables encryption between the web server hosting the site and web browsers that connect to it. This ensures that nobody can intercept confidential information being sent between the site and the users - for example, credit card numbers, login names and passwords, and personal information.

SSL certificates are issued by Certificate Authorities (CAs) such as *Thawte* and VeriSign, who act as trusted third parties by verifying the identities of the companies that operate the web sites. This assists users/customers to be sure that they are dealing with a genuine real-world business and not a fake website.

The latest version of SSL is also known as TLS (Transaction Layer Security). A variation of TLS, WTLS or Wireless TLS, has been optimized for cell phones.

DES (Data Encryption Standard)

DES, an acronym for the Data EncryptionStandard, is the name of the Federal Information Processing Standard (FIPS) 46-3, which describes the data encryption algorithm (DEA). DES is an improvement of the algorithm Lucifer developed

by IBM in the early 1970s. While the algorithm was essentially designed by IBM, the NSA and NBS played a substantial role in the final stages of the development. DES has been extensively studied since its publication and is the best known and widely used symmetric algorithm in the world.

DES effectively only provides 56 bit encryption, which is now recognized to be too weak for effective security. Typical applications today use Triple DES, which uses three rounds of DES encryption to reinforce each other, resulting in an effective 112 bit key strength.

AES (Advanced Encryption Standard)

The AES is the Advanced Encryption Standard. The AES is intended to be issued as a FIPS standard and will replace DES. Most now agree that this DES is approaching the end of its useful life - it has not been reaffirmed as a federal standard. In January 1997 the AES initiative was announced and in September 1997 the public was invited to propose suitable block ciphers as candidates for the AES. After a two-stage selection process, the winner, Rijndael, was selected. NIST was looking for a cipher that will remain secure well into the next century.

Electronic Commerce

Cryptography makes secure web sites and electronic safe transmissions possible. For a web site to be secure all of the data transmitted between the computers where the data is kept and where it is received must be encrypted. This allows people to do online banking, online trading, and make online purchases with their credit cards, without worrying that any of their account information is being compromised. However, simply entering a credit card number on the Internet leaves one open to fraud. This level of activity could not be supported without cryptographic security. It has been said that one is safer using a credit card over the Internet than within a store or restaurant. This is true provided that the database of the e-commerce system has adequate protection to ensure that unauthorized people cannot simply harvest the information after the transactions have already been processed. These levels of security, give the means to strengthen the foundation with which e-commerce can grow. As more and more business is conducted over the Internet, the need for protection against fraud, theft, and corruption of vital information increases. Cryptography is very important to the continued growth of the Internet and electronic commerce.

E-mail

Cryptography is very important to the continued growth of the Internet and electronic commerce. People use e-mail to conduct personal and business matters on a daily basis. E-mail has no physical form and may exist electronically in more than one place at a time. This poses a potential problem as it increases the opportunity for an eavesdropper to get a hold of the transmission. Encryption protects e-mail by rendering it very difficult to read by any unintended party. Digital signatures can also be used to authenticate the origin and the content of an e-mail message. The concept of using cryptography for the electronic signing of documents has received increasing attention because of the legal recognition in various countries of electronic signatures to be equivalent to handwritten signatures on physical documents. The important aspects of these transformations are that a signature be an unforgivable and irrefutable certification of the agreement to which it is attached. This prevents harm which could result from forgery or attempts to back out of an agreement once signed.

Pretty Good Privacy (PGP) is a popular program used to encrypt and decrypt e-mail over the Internet. It can also be used to send an encrypted digital signature that lets the receiver verify the sender's identity and know that the message was not changed en route. PGP is the most widely used privacy-ensuring program by individuals and is also used by many corporations. Developed by Philip R. Zimmermann in 1991, PGP has become a de facto standard for e-mail security. PGP can also be used to encrypt files being stored so that they are unreadable by other users or intruders.

S/MIME (Secure Multi-Purpose Internet Mail Extensions) is a secure method of sending e-mail that uses the RSA encryption system. Like SSL, S/MIME uses digital certificates issued by Certificate Authorities like *Thawte* and VeriSign. The advantage of S/MIME over PGP is that it is already built into practically all major email software, including Microsoft Outlook/Outlook Express and Exchange, Netscape Messenger, Lotus Notes, Mozilla and Ximian Evolution.

Authentication

Authentication and identification are two widely used applications of cryptography.

Identification is the process of verifying something's or someone's identity. For example, when withdrawing money from a bank, a teller asks to see identification (for example, your ID document) to verify the identity of the owner of the bank account. This same process can be done electronically using cryptography. Every automatic teller machine (ATM) card is associated with a personal identification number (PIN), which connects the owner to the card and thus to the account. When the card is inserted into the ATM, the machine prompts the cardholder for the PIN. If the correct PIN is entered, the machine identifies that person as the rightful owner and grants access.

Authentication is similar to identification, in that both allow an entity access to resources (such as an Internet account), but authentication is broader because it does not necessarily involve identifying a person or entity. Banks use authentication codes almost exclusively as their means of protecting electronic funds transfers (EFTs) of many billions of dollars per day. Authentication merely determines whether that person or entity is authorized for whatever is in question.

Regulated access

Cryptography is also used to regulate access to satellite television. However, the satellite TV companies do not have a direct connection to each individual subscriber's home. This means that anyone with a satellite dish can pick up the signals. To alleviate the problem of people getting free TV, they use cryptography. The trick is to allow only those who have paid for their service to unscramble the transmission; this is done with receivers ("unscramblers"). Each subscriber is given a receiver; the satellite transmits signals that can only be unscrambled by such a receiver (ideally).

X. CONCLUSION

Security in the Internet is improving. The increasing use of the Internet for commerce is improving the deployed technology to protect the financial transactions. Extension of the basic technologies to protect multicast communications is possible and can be expected to be deployed as multicast becomes more widespread.

Control over routing remains the basic tool for controlling access to streams. Implementing particular policies will be possible as multicast routing protocols improve. Cryptography is a tool which may alleviate many of the perceived problems of using the Internet for communications. However, cryptography requires the safe implementation of complex mathematical equations and protocols, and there are always worries about bad implementations. A further worry is that users are integral to securing communications, since they must provide appropriate keys. As the founders of First Virtual point out [#!cybercommerce!#] a safe application of cryptographic technology will pay close attention to how public keys are associated with user identities, how stolen keys are detected and revoked and how long a stolen key is useful to a criminal.

Cryptography may be groovy technology, but since security is a human issue, cryptography is only as good as the practices of the people who use it. Users leave keys lying around, choose easily remembered keys, don't change keys for years. The complexity of cryptography effectively puts it outside the understanding of most people and so motivation for the practices of cryptographic security is not available