SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF COMPUTING

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

# UNIT-IV –INTERNET SECURITY-SCS1316

# Internet Security

Email Security-PGP-S/MIME- Secured Electronic Transaction-IP Security Overview- IPSec Documents-IPSec Services, IPSec Architecture, IP Traffic Processing-Encapsulating Security Payload-Internet key Exchange- Firewalls- Stateful Packet Inspection-Application Gateways/Proxies- Hybrid Systems

# I. Electronic Mail Security

## Overview

1. Pretty Good Privacy (PGP)
2. S/MIME
3. DomainKeys Identified Mail (DKIM)

## Email Security Enhancements

1. Confidentiality: Protection from disclosure
2. Authentication: Of sender of message
3. Message integrity: Protection from modification
4. Non-repudiation of origin: Protection from denial by sender

### 1.1.PGP – Authentication and Confidentiality

2013, when the *NSA (United States National Security Agency) scandal* was leaked to the public, people started to opt for the services which can provide them a strong privacy for their data. Among the services people opted for, most particularly for Emails, were different plug-ins and extensions for their browsers. Interestingly, among the various plug-ins and extensions that people started to use, there were two main programs that were solely responsible for the complete email security that the people needed. One was S/MIME which we will see later and the other was PGP.

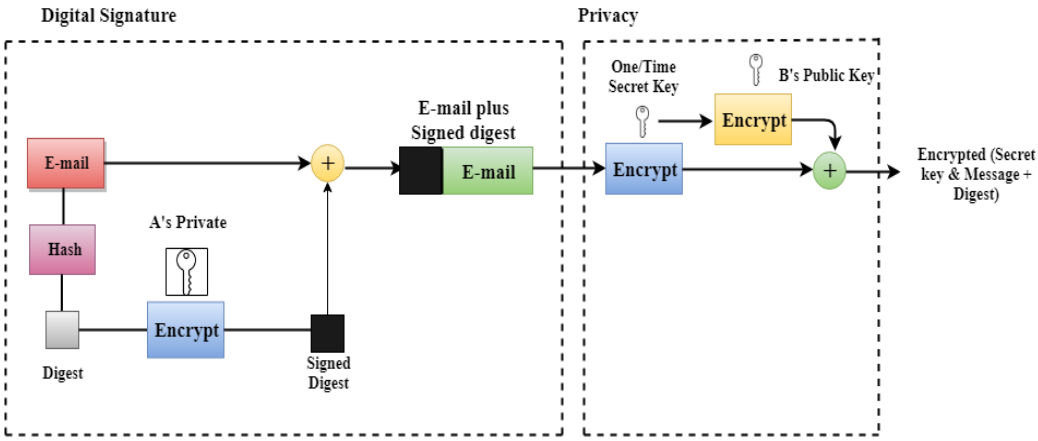
As said, PGP (Pretty Good Privacy), is a popular program that is used to provide confidentiality and authentication services for electronic mail and file storage. It was designed by Phil Zimmermann way back in 1991. He designed it in such a way, that the best cryptographic algorithms such as RSA, Diffie-Hellman key exchange, DSS are used for the public-key encryption (or) asymmetric encryption; CAST-128, 3DES, IDEA are used for symmetric encryption and SHA-1 is used for hashing purposes. PGP software is an open source one and is not dependent on either of the OS (Operating System) or the processor. The application is based on a few commands which are very easy to use.

- PGP uses a digital signature (a combination of hashing and public key encryption) to provide integrity, authentication, and non-repudiation. PGP uses a combination of secret key encryption and public key encryption to

provide privacy. Therefore, we can say that the digital signature uses one hash function, one secret key, and two private-public key pairs.

- PGP is an open source and freely available software package for email security.
- PGP provides authentication through the use of Digital Signature.
- It provides confidentiality through the use of symmetric block encryption.
- It provides compression by using the ZIP algorithm, and EMAIL compatibility using the radix-64 encoding scheme.

**PGP at the Sender site (A)**

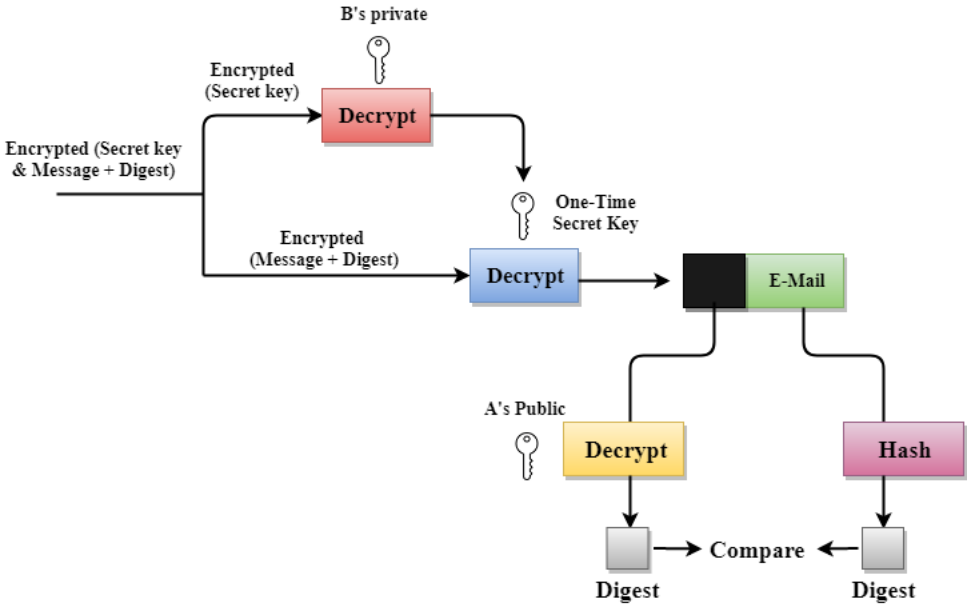



Following are the steps taken by PGP to create secure e-mail at the sender site

- The e-mail message is hashed by using a hashing function to create a digest.
- The digest is then encrypted to form a signed digest by using the sender's private key, and then signed digest is added to the original email message.
- The original message and signed digest are encrypted by using a one-time secret key created by the sender.
- The secret key is encrypted by using a receiver's public key.

  Both the encrypted secret key and the encrypted combination of message and digest are sent together.

**PGP at the Receiver site (B)**




Following are the steps taken to show how PGP uses hashing and a combination of three keys to generate the original message:

- The receiver receives the combination of encrypted secret key and message digest is received.
- The encrypted secret key is decrypted by using the sender's private key to get the one-time secret key.
- The secret key is then used to decrypt the combination of message and digest.
- The digest is decrypted by using the sender's public key, and the original message is hashed by using a hash function to create a digest.
- Both the digests are compared if both of them are equal means that all the aspects of security are preserved**.**

The following are the services offered by PGP:

1. Authentication
2. Confidentiality
3. Compression
4. Email Compatibility

5. Segmentation

1.1.1 Authentication:

Authentication basically means something that is used to validate something as true or real. To login into some sites sometimes we give our account name and password that is an authentication verification procedure.

In the email world, checking the authenticity of an email is nothing but to check *whether it actually came from the person it says*. In emails, authentication has to be checked as there are some people who spoof the emails or some spams and sometimes it can cause a lot of inconvenience. The Authentication service in PGP is provided as follows:

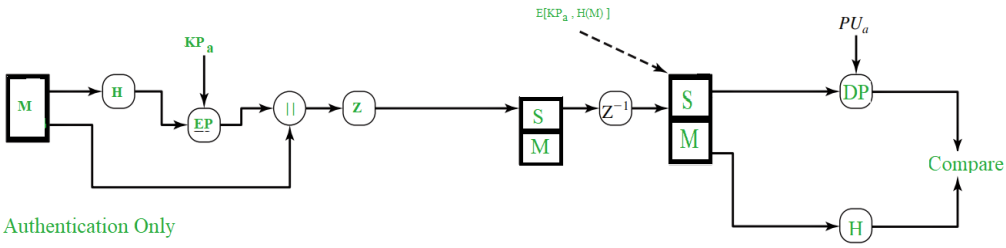



Figure 4.1 Authentication

As shown in the above figure, the Hash Function (H) calculates the Hash Value of the message. For the hashing purpose, SHA-1 is used and it produces a 160 bit output hash value. Then, using the sender's private key ($KP_a$), it is encrypted and it's called as Digital Signature. The Message is then appended to the signature. All the process happened till now, is sometimes described as *signing the message* . Then the message is compressed to reduce the transmission overhead and is sent over to the receiver.

At the receiver's end, the data is decompressed and the message, signature are obtained. The signature is then decrypted using the sender's public key($PU_a$) and the hash value is obtained. The message is again passed to hash function and it's hash value is calculated and obtained.

Both the values, one from signature and another from the recent output of hash function are compared and if both are same, it means that the email is actually sent from a known one and is legit, else it means that it's not a legit one.

2. Confidentiality:

Sometimes we see some packages labelled as 'Confidential', which means that those packages are not meant for all the people and only selected persons can see them. The same applies to the email confidentiality as well. Here, in the email service, only the sender and the receiver should be able to read the message, that means the contents have to be kept secret from every other person, except for those two.

PGP provides that Confidentiality service in the following manner:

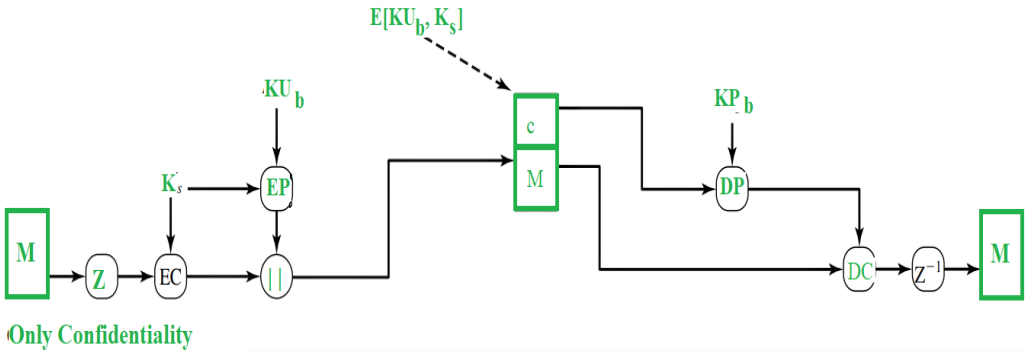



Figure 4.2 Confidentiality

The message is first compressed and a 128 bit session key ($K_s$), generated by the PGP, is used to encrypt the message through symmetric encryption. Then, the session key ($K_s$) itself gets encrypted through public key encryption (EP) using receiver's public key($KU_b$) . Both the encrypted entities are now concatenated and sent to the receiver.

As you can see, the original message was compressed and then encrypted initially and hence even if any one could get hold of the traffic, he cannot read the contents as they are not in readable form and they can only read them if they had the session key ($K_s$). Even though session key is transmitted to the receiver and hence, is in the traffic, it is in encrypted form and only the receiver's private key ($KP_b$)can be used to decrypt that and thus our message would be completely safe.

At the receiver's end, the encrypted session key is decrypted using receiver's private key ($KP_b$) and the message is decrypted with the obtained session key. Then, the message is decompressed to obtain the original message (M).

RSA algorithm is used for the public-key encryption and for the symmetric jey encryption, CAST-128(or IDEA or 3DES) is used.

Practically, both the Authentication and Confidentiality services are provided in

parallel as follows :

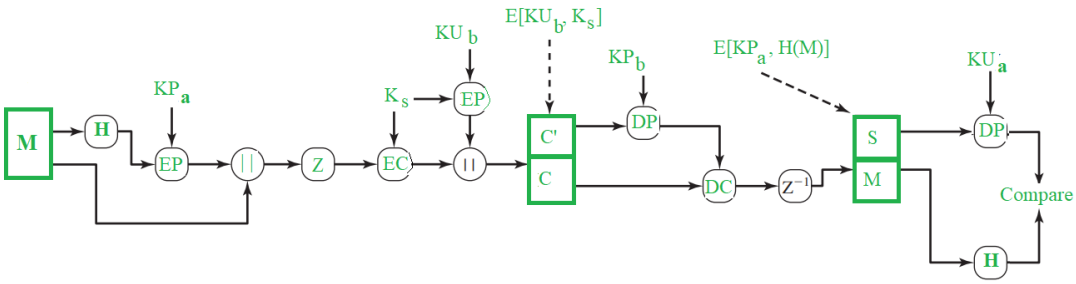



Figure 4.3 Authentication and Confidentiality

Note:
M – Message
H – Hash Function
$K_s$ – A random Session Key created for Symmetric Encryption purpose
DP – Public-Key Decryption Algorithm
EP – Public-Key Encryption Algorithm
DC – Asymmetric Encryption Algorithm
EC – Symmetric Encryption Algorithm
$KP_b$ – A private key of user B used in Public-key encryption process
$KP_a$ – A private key of user A used in Public-key encryption process
$PU_a$ – A public key of user A used in Public-key encryption process
$PU_b$ – A public key of user B used in Public-key encryption process
|| – Concatenation
Z – Compression Function
$Z^{-1}$ – Decompression Function

**PGP Operation – Compression**

- As a default, PGP compresses the message after applying the signature but before encryption
- This has the benefit of saving space both for e-mail transmission and for file storage
- The placement of the compression algorithm is critical

- Applying the hash function and signature after compression would constrain all PGP implementations to the same version of the compression algorithm
- Message encryption is applied after compression to strengthen cryptographic security
- The compression algorithm used is ZIP

**PGP E-mail Compatibility**

- Many electronic mail systems only permit the use of blocks consisting of ASCII text
- To accommodate this restriction, PGP provides the service of converting the raw 8-bit binary stream to a stream of printable ASCII characters
- The scheme used for this purpose is radix-64 conversion

- Each group of three octets of binary data is mapped into four ASCII characters ,This format also appends a CRC to detect transmission errors

**PGP segmentation**

- PGP segments messages if too big
- PGP produces binary (encrypted) data & appends a CRC
- Email was designed only for text ØNeed to encode binary into printable ASCII characters
- Uses radix-64 or base-64 algorithm
- Maps 3 bytes to 4 printable chars: 26 upper case alphabets, 26 lowercase alphabets, 10 numbers, +, \

**PGP Session Keys**

- Need a session key of varying sizes for each message:
- 56-bit DES,
- 168-bit Triple-DES
- 128-bit CAST (Carlisle Adams and Stafford Tavares)
- IDEA (International Data Encryption Algorithm)

Generated with CAST-128 using random inputs taken from previous uses and from

keystroke timing of user

**PGP Key Rings**

- each PGP user has a pair of key rings:
  - public-key ring contains all the public-keys of other PGP users known to this user, indexed by key ID
  - private-key ring contains the public/private key pair(s) for this user, indexed by key ID & encrypted keyed from a hashed passphrase

**Disadvantages of PGP Encryption**

- The Administration is difficult: The different versions of PGP complicate the administration.
- Compatibility issues: Both the sender and the receiver must have compatible versions of PGP. For example, if you encrypt an email by using PGP with one of the encryption technique, the receiver has a different version of PGP which cannot read the data.
- Complexity: PGP is a complex technique. Other security schemes use symmetric encryption that uses one key or asymmetric encryption that uses two different keys. PGP uses a hybrid approach that implements symmetric encryption with two keys. PGP is more complex, and it is less familiar than the traditional symmetric or asymmetric methods.
- No Recovery: Computer administrators face the problems of losing their passwords. In such situations, an administrator should use a special program to retrieve passwords. For example, a technician has physical access to a PC which can be used to retrieve a password. However, PGP does not offer such a special program for recovery; encryption methods are very strong so, it does not retrieve the forgotten passwords results in lost messages or lost files.

## 1.2.Secure/Multipurpose Internet Mail Extensions (S/MIME)

What is S/MIME

- S/MIME means Secure/Multipurpose Internet Mail Extensions.
- It is a technology that allows us to encrypt the content of our e-mails, so that

they are not vulnerable to cyber attacks.

- In other words, S/MIME keeps our e-mails safe and makes sure that the only person who reads them is the intended receiver.

S/MIME is a protocol for the secure exchange of e-mail and attached documents originally developed by RSA Security. Secure/Multipurpose Internet Mail Extensions (S/MIME) adds security to Internet e-mail based on the Simple Mail Transfer Protocol (SMTP) method and adds support for digital signatures and encryption to SMTP mail to support authentication of the sender and privacy of the communication. Note that because HTTP messages can transport MIME data, they can also use S/MIME.

**S/MIME Functions**

- Enveloped Data
  - Encrypted Content And Associated Keys
- Signed Data
  - Encoded Message + Signed Digest
- Clear-signed Data
  - Cleartext Message + Encoded Signed Digest
- Signed & Enveloped Data
  - Nesting Of Signed & Encrypted Entities

**S/MIME Cryptographic Algorithms**

- Hash functions: SHA-1 & MD5
- Digital signatures: DSS & RSA
- Session key encryption: D-H & RSA
- Message encryption: triple-des, RC2/40 and others
- MAC: HMAC with SHA-1
- Have a procedure to decide which algorithms to use

According to the capability of the receiving agent

**S/MIME Certificate Processing**

- S/MIME uses X.509 v3 certificates
- Managed using a hybrid of a strict X.509 CA hierarchy and enterprise's CAs
- Each client has a list of trusted CA's certificates and his own public/private key pairs & certificates
- Several types of certificates with different levels of checks:
- Class 1: Email and web browsing
- Class 2: Inter-company email
- Class 3: Banking, …

**S/MIME Enhanced Security Services**

- RFC2634 (1999) describes enhanced security services: Signed receipts: Request a signed receipt
- Security labels: Priority, which users (role) can access
- Secure mailing lists: Request a list processor to encrypt

**S/MIME Structure**

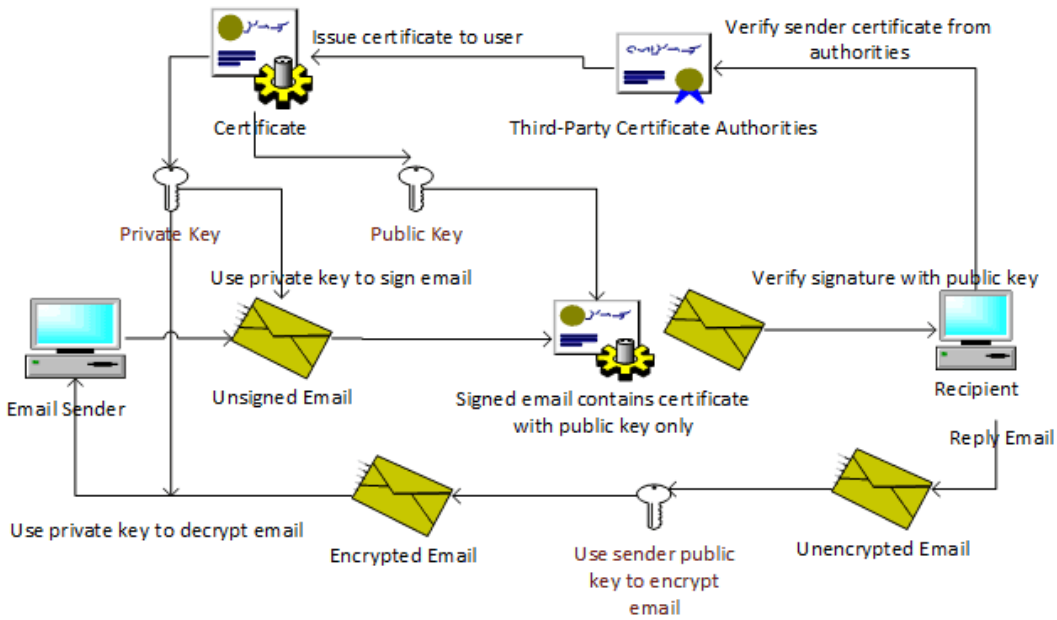


Figure 4.4 S/Mime Structure

How It Works

S/MIME is an extension of the widely implemented Multipurpose Internet Mail Extensions (MIME) encoding standard, which defines how the body portion of an SMTP message is structured and formatted. S/MIME uses the RSA public key cryptography algorithm along with the Data Encryption Standard (DES) or Rivest-Shamir-Adleman (RSA) encryption algorithm. In an S/MIME message, the MIME body section consists of a message in PKCS #7 format that contains an encrypted form of the MIME body parts. The MIME content type for the encrypted data is application/pkcs7-mime.

Understanding Digital Signatures

Digital signatures are the more commonly used service of S/MIME. As the name suggests, digital signatures are the digital counterpart to the traditional, legal signature on a paper document. As with a legal signature, digital signatures provide the following security capabilities:

- Authentication A signature serves to validate an identity. It verifies the answer to "who are you" by providing a means of differentiating that entity from all others and proving its uniqueness. Because there is no authentication in SMTP e-mail, there is no way to know who actually sent a message. Authentication in a digital signature solves this problem by allowing a recipient to know that a message was sent by the person or organization who claims to have sent the message.

- Nonrepudiation The uniqueness of a signature prevents the owner of the signature from disowning the signature. This capability is called nonrepudiation. Thus, the authentication that a signature provides gives the means to enforce nonrepudiation. The concept of nonrepudiation is most familiar in the context of paper contracts: a signed contract is a legally binding document, and it is impossible to disown an authenticated signature. Digital signatures provide the same function and, increasingly in some areas, are recognized as legally binding, similar to a signature on paper. Because SMTP e-mail does not provide a means of authentication, it cannot provide nonrepudiation. It is easy for a sender to disavow ownership of an SMTP e-mail message.

- Data integrity An additional security service that digital signatures provide is

data integrity. Data integrity is a result of the specific operations that make digital signatures possible. With data integrity services, when the recipient of a digitally signed e-mail message validates the digital signature, the recipient is assured that the e-mail message that is received is, in fact, the same message that was signed and sent, and has not been altered while in transit. Any alteration of the message while in transit after it has been signed invalidates the signature. In this way, digital signatures are able to provide an assurance that signatures on paper cannot, because it is possible for a paper document to be altered after it has been signed.

## 1.3.Secure Electronic Transaction (SET) Protocol

Secure Electronic Transaction or SET is a system which ensures security and integrity of electronic transactions done using credit cards in a scenario. SET is not some system that enables payment but it is a security protocol applied on those payments. It uses different encryption and hashing techniques to secure payments over internet done through credit cards. SET protocol was supported in development by major organizations like Visa, Mastercard, Microsoft which provided its Secure Transaction Technology (STT) and NetScape which provided technology of Secure Socket Layer (SSL).

SET protocol restricts revealing of credit card details to merchants thus keeping hackers and thieves at bay. SET protocol includes Certification Authorities for making use of standard Digital Certificates like X.509 Certificate.

Before discussing SET further, let’s see a general scenario of electronic transaction, which includes client, payment gateway, client financial institution, merchant and merchant financial institution.

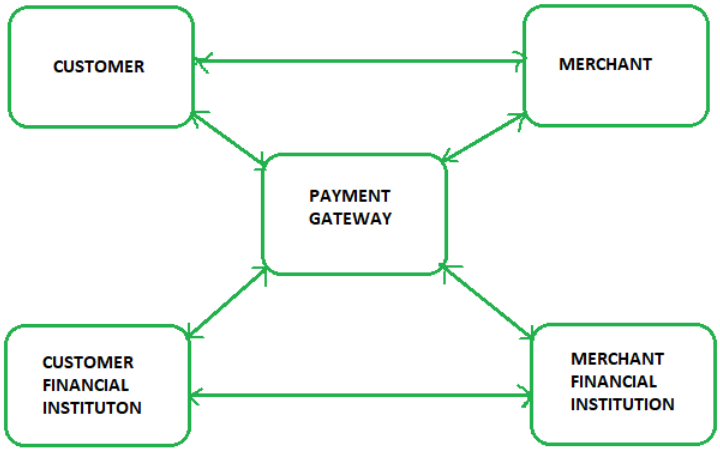



Figure 4.5 SET protocol

Requirements in SET :
SET protocol has some requirements to meet, some of the important requirements are :

- It has to provide mutual authentication i.e., customer (or cardholder) authentication by confirming if the customer is intended user or not and merchant authentication.
- It has to keep the PI (Payment Information) and OI (Order Information) confidential by appropriate encryptions.
- It has to be resistive against message modifications i.e., no changes should be allowed in the content being transmitted.
- SET also needs to provide interoperability and make use of best security mechanisms.

Participants in SET :
In the general scenario of online transaction, SET includes similar participants:

1. Cardholder – customer
2. Issuer – customer financial institution
3. Merchant

4. Acquirer – Merchant financial

5. Certificate authority – Authority which follows certain standards and issues certificates(like X.509V3) to all other participants.

SET functionalities :

- Provide Authentication

- Merchant Authentication – To prevent theft, SET allows customers to check previous relationships between merchant and financial institution. Standard X.509V3 certificates are used for this verification.

- Customer / Cardholder Authentication – SET checks if use of credit card is done by an authorized user or not using X.509V3 certificates.

- Provide Message Confidentiality : Confidentiality refers to preventing unintended people from reading the message being transferred. SET implements confidentiality by using encryption techniques. Traditionally DES is used for encryption purpose.

- Provide Message Integrity : SET doesn't allow message modification with the help of signatures. Messages are protected against unauthorized modification using RSA digital signatures with SHA-1 and some using HMAC with SHA-1,

Dual Signature :
The dual signature is a concept introduced with SET, which aims at connecting two information pieces meant for two different receivers :
Order Information (OI) for merchant
Payment Information (PI) for bank

You might think sending them separately is an easy and more secure way, but sending them in a connected form resolves any future dispute possible. Here is the generation of dual signature:

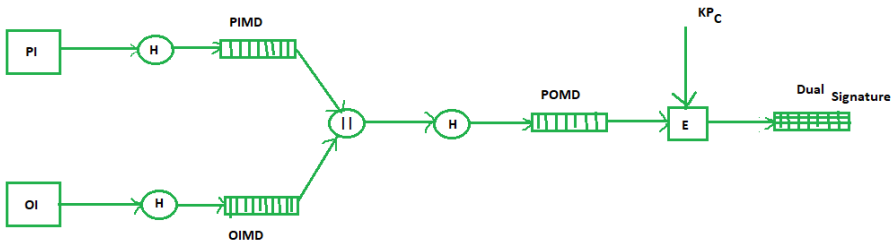



Figure 4.6 Generation of dual signature

Where,

PI stands for payment information

OI stands for order information

PIMD stands for Payment Information Message Digest

OIMD stands for Order Information Message Digest

POMD stands for Payment Order Message Digest

H stands for Hashing

E stands for public key encryption

KPc is customer's private key

|| stands for append operation

Dual signature, DS= E(KPc, [H(H(PI)||H(OI))])

Purchase Request Generation :

The process of purchase request generation requires three inputs:

- Payment Information (PI)
- Dual Signature
- Order Information Message Digest (OIMD)

The purchase request is generated as follows:

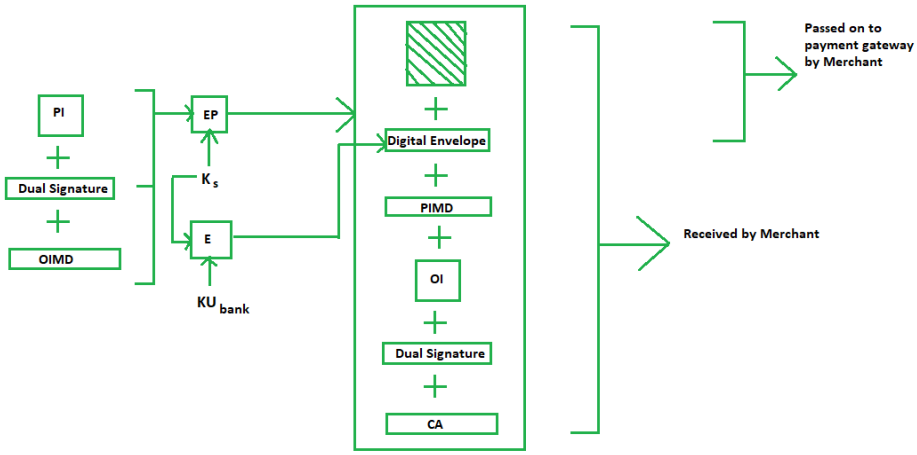



Figure 4.7 Purchase Request Generation

Here,

PI, OIMD, OI all have the same meanings as before.

The new things are :

EP which is symmetric key encryption

Ks is a temporary symmetric key

KUbank is public key of bank

CA is Cardholder or customer Certificate

Digital Envelope = E(KUbank, Ks)

Purchase Request Validation on Merchant Side :
The Merchant verifies by comparing POMD generated through PIMD hashing with POMD generated through decryption of Dual Signature as follows:

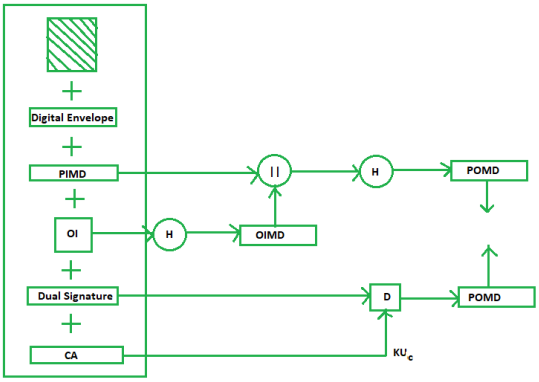



Figure 4.8 POMD generated through decryption of Dual Signature

Since we used Customer private key in encryption here we use KUc which is public key of customer or cardholder for decryption 'D'.

Payment Authorization and Payment Capture :
Payment authorization as the name suggests is the authorization of payment information by merchant which ensures payment will be received by merchant. Payment capture is the process by which merchant receives payment which includes again generating some request blocks to gateway and payment gateway in turn issues payment to merchant.

## 1.4. IP security (IPSec)

The IP security (IPSec) is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

Uses of IP Security –
IPsec can be used to do the following things:

- To encrypt application layer data.
- To provide security for routers sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.

- To protect network data by setting up circuits using IPsec tunneling in which all data is being sent between the two endpoints is encrypted, as with a Virtual Private Network(VPN) connection.

Components of IP Security –
It has the following components:

1. Encapsulating Security Payload (ESP) –

It provides data integrity, encryption, authentication and anti replay. It also provides authentication for payload.

2. Authentication Header (AH) –

It also provides data integrity, authentication and anti replay and it does not provide encryption. The anti replay protection, protects against unauthorized transmission of packets. It does not protect data's confidentiality.


Figure 4.9 Authentication Header

1. Internet Key Exchange (IKE)

It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication. The Key Management Protocol (ISAKMP) and Internet Security Association which provides a framework for authentication and key exchange. ISAKMP tells how the set up of the Security Associations (SAs) and how direct connections between two hosts that are using IPsec.

Internet Key Exchange (IKE) provides message content protection and also an open frame for implementing standard algorithms such as SHA and MD5. The algorithm's IP sec users produces a unique identifier for each packet. This identifier then allows a device to determine whether a packet has been correct or not. Packets which are not authorized are discarded and not given to receiver.

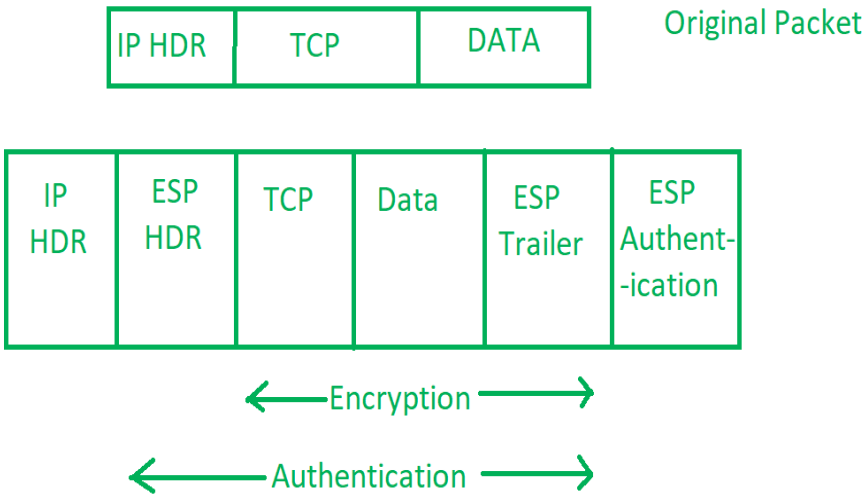



Figure 4.10 Internet Key Exchange

Working of IP Security –

1. The host checks if the packet should be transmitted using IPsec or not. These packet traffic triggers the security policy for themselves. This is done when the system sending the packet apply an appropriate encryption. The incoming packets are also checked by the host that they are encrypted properly or not.

2. Then the IKE Phase 1 starts in which the 2 hosts( using IPsec ) authenticate themselves to each other to start a secure channel. It has 2 modes. The Main mode which provides the greater security and the Aggressive mode which enables the host to establish an IPsec circuit more quickly.

3. The channel created in the last step is then used to securely negotiate the way the IP circuit will encrypt data accross the IP circuit.

4. Now, the IKE Phase 2 is conducted over the secure channel in which the two hosts negotiate the type of cryptographic algorithms to use on the session and agreeing on secret keying material to be used with those algorithms.

5. Then the data is exchanged across the newly created IPsec encrypted tunnel. These packets are encrypted and decrypted by the hosts using IPsec SAs.

6. When the communication between the hosts is completed or the session times out then the IPsec tunnel is terminated by discarding the keys by both the hosts.

IPSec Architecture

IPSec (IP Security) architecture uses two protocols to secure the traffic or data flow. These protocols are ESP (Encapsulation Security Payload) and AH (Authentication Header). IPSec Architecture include protocols, algorithms, DOI, and Key Management. All these components are very important in order to provide the three main services:

- Confidentiality
- Authentication
- Integirity

IP Security Architecture:

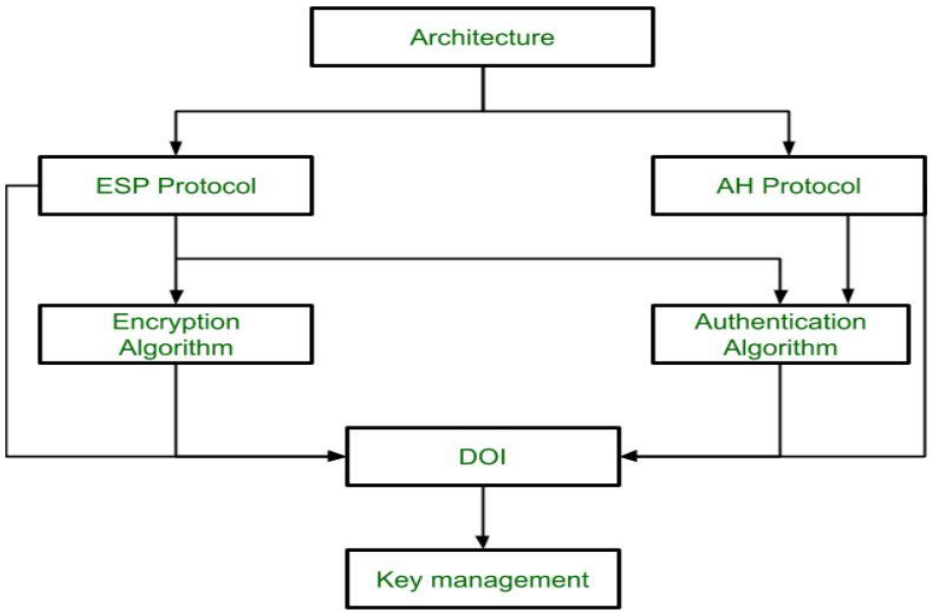



Figure 4.11 IP Security Architecture

1. Architecture:
Architecture or IP Security Architecture covers the general concepts, definitions, protocols, algorithms and security requirements of IP Security technology.

2. ESP Protocol:

ESP(Encapsulation Security Payload) provide the confidentiality service. Encapsulation Security Payload is implemented in either two ways:

- ESP with optional Authentication.
- ESP with Authentication.

Packet Format:

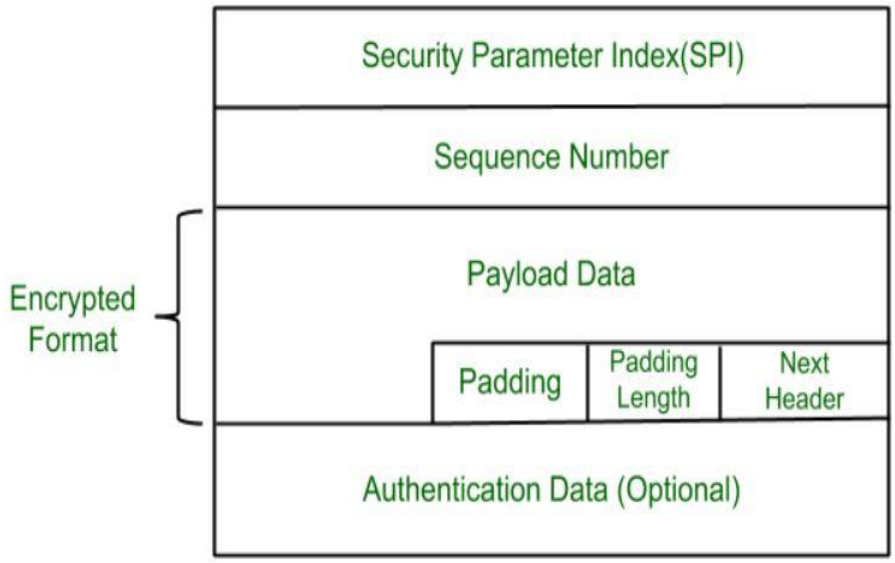



Figure 4.12 Packet Format

- Security Parameter Index(SPI):

This parameter is used in Security Association. It is used to give a unique number to the connection build between Client and Server.

- Sequence Number:

Unique Sequence number are allotted to every packet so that at the receiver side packets can be arranged properly.

- Payload Data:

Payload data means the actual data or the actual message. The Payload data is in encrypted format to achieve confidentiality.

- Padding:

Extra bits or space added to the original message in order to ensure confidentiality. Padding length is the size of the added bits or space in the original message.

- Next Header:

Next header means the next payload or next actual data.

- Authentication Data

This field is optional in ESP protocol packet format.

3. Encryption algorithm:

Encryption algorithm is the document that describes various encryption algorithm used for Encapsulation Security Payload.

4. AH Protocol:

AH (Authentication Header) Protocol provides both Authentication and Integrity service. Authentication Header is implemented in one way only: Authentication along with Integrity.

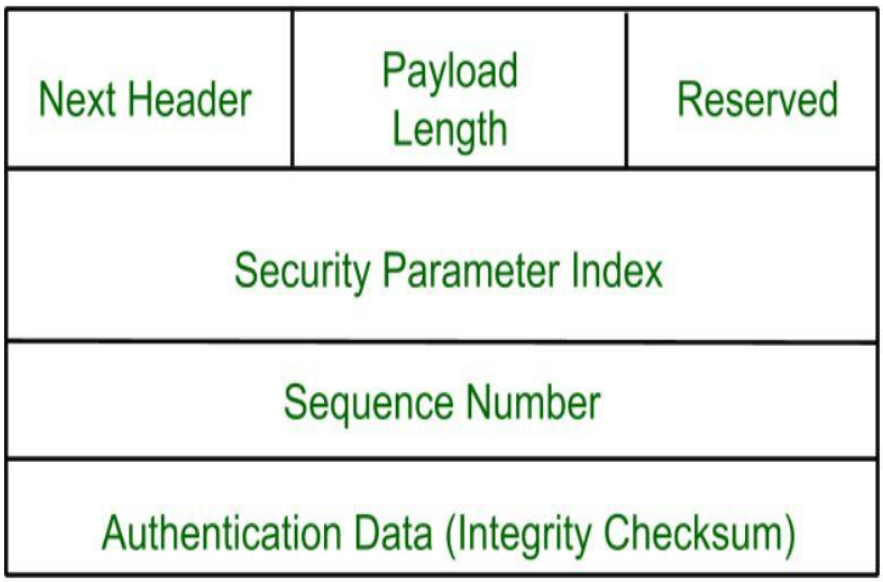



Figure 4.13 AH Protocol

Authentication Header covers the packet format and general issue related to the use of AH for packet authentication and integrity.

5. Authentication Algorithm:
Authentication Algorithm contains the set of the documents that describe authentication algorithm used for AH and for the authentication option of ESP.

6. DOI (Domain of Interpretation):
DOI is the identifier which support both AH and ESP protocols. It contains values needed for documentation related to each other.

7. Key Management:
Key Management contains the document that describes how the keys are exchanged between sender and receiver.

## 1.5.Encapsulating Security Payload (ESP)

Encapsulating Security Payload (ESP) is a member of the Internet Protocol Security (IPsec) set of protocols that encrypt and authenticate the packets of data between computers using a Virtual Private Network (VPN). The focus and layer on which ESP operates makes it possible for VPNs to function securely.

Being one of the most popular tools used in network security, Encapsulating Security Payload (abbreviated as ESP) offers the help we need in keeping the integrity, authenticity and confidentiality of the information we send across networks. Keep reading to learn more!

With the technological advancements, the way we conduct our business processes has changed immensely. Now, we heavily rely on the internet technologies and transfer massive amounts of data daily. For this data traffic, we often employ wireless and wired networks. As a result, network security and necessary cybersecurity measures gain importance each day.

Being one of the most popular tools used in network security, Encapsulating Security Payload (abbreviated as ESP) offers the help we need in keeping the integrity, authenticity and confidentiality of the information we send across networks. In this article, we will take a closer look at what Encapsulating Security Payload is. Keep reading to learn more.

What is Encapsulating Security Payload?

Encapsulating Security Payload (abbr. ESP) is a protocol within the scope of

the IPSec.

The information traffic on a network is provided with packets of data. In other words, when you want to send or receive a data through a network, it is turned into packets of information so that it can travel within the network. Similar to the data packages, payload is also sent through the network and it contains the 'actual' information, the intended message.

The Encapsulating Security Payload aims to offer necessary security measures for these packets of data and/or payloads. With the help of Encapsulating Security Payload, confidentiality, integrity and authentication of payloads and data packets in IPv4 and IPv6 networks.

How does the Encapsulating Security Payload work?

Also known as a transport layer security protocol, the Encapsulating Security Payload is able to function with both the IPv6 and IPv4 protocols. The way ESP operates is pretty straightforward: It is inserted between the Internet Protocol/IP header and upper layer protocols such as UDP, ICMP or TCP. In this position, the ESP takes the form of a header.

How can the Encapsulating Security Payload be used?

Although the Encapsulating Security Payload offers many benefits, it can be applied in only two ways: Tunnel mode and transport mode.

In the tunnel mode, a new IP header is created and used as the outermost IP header. It is followed by the Encapsulating Security Payload Header and original datagram. Tunnel mode is a must for the gateways.

In the transportation mode, the IP header is neither authenticated nor encrypted. As a result, your addressing information can potentially be leaked during the datagram transit. Transport mode often uses less processing, that is why most hosts prefer Encapsulating Security Payload in transport mode.

What are the benefits of the Encapsulating Security Payload?

The Encapsulating Security Payload offers all the functions of the Authentication Header, which are anti-replay protection, authentication and data integrity. On the other hand, the ESP differs from the Authentication Header in terms of data confidentiality: the ESP can provide data confidentiality while the Authentication Header cannot.

Moreover, the Encapsulating Security Protocol Payload aims to provide various services including but not limited to:

- Maintaining the confidentiality of datagrams with encryption
- Using security gateways to limit the traffic flow confidentiality
- Authenticating the origin of data using a public key encryption
- Providing antireplay services with the help of the sequence number mechanism given by the Authentication Header

In business environments, we use network technologies very often. They allow us to share resources and files, set communication protocols and such. As much as they streamline and accelerate our business processes, they can also pose a serious vulnerability for our cyber security. An intruder or a hacker can infiltrate into our networks, steal our valuable information or lock us out of our systems. That is why network security is one of the most important practices in cybersecurity.

Most organizations rely on firewalls for their network security needs. A firewall can be defined as a network security system that allows the cybersecurity professionals to monitor and control the network traffic. In other words, a firewall sets the boundary between the internal and external network. There are two main types of firewalls:

- Network-based firewalls: They are often positioned on the LANs, intranets or WANs of the gateway computers.
- Host-based firewalls: They are implemented on the network host itself in order to protect the entire network traffic. Host-based firewalls can be a part of the operating system or an agent application in order to offer an additional layer of security.

What is stateful inspection?

The term stateful inspection (also known as the dynamic packet filtering) refers to a distinguished firewall technology. It aims to monitor the active connections on a network. Moreover, the process of stateful inspection determines which network packets should be allowed through the firewall by utilizing the information regarding active connections.

Stateful inspection keeps track of each connection and constantly checks if they are valid. That is why it offers a better protection than its predecessors.

In a firewall where the stateful inspection is implemented, the network administrator can customise the parameters in order to meet the unique needs of the organization.

What is the benefit of implementing stateful inspection?

Before stateful inspection has become mainstream, similar technology called static packet filtering was in use. This older alternative only checks the headers of the packets in order to determine whether they should be allowed through the firewall. As a result, a hacker can simply indicate "reply" in the header in order to extract information from the network. On the contrary, stateful inspection aims to carry out a more sophisticated investigation. That is why it analyses the application layer of the packets. A dynamic packet filter like stateful inspection can offer a better security posture for networks through recording the session information like port numbers or IP addresses.

In other words, stateful inspection is better at keeping the intruders away from your network since it uses a more refined technology.

## 1.6.Internet key Exchange-

Internet Key Exchange (IKE) is a key management protocol standard used in conjunction with the Internet Protocol Security (IPSec) standard protocol. It provides security for virtual private networks' (VPNs) negotiations and network access to random hosts. It can also be described as a method for exchanging keys for encryption and authentication over an unsecured medium, such as the Internet.

IKE is a hybrid protocol based on:

- ISAKMP (RFC2408): Internet Security Association and Key Management Protocols are used for negotiation and establishment of security associations. This protocol establishes a secure connection between two IPSec peers.
- Oakley (RFC2412): This protocol is used for key agreement or key exchange. Oakley defines the mechanism that is used for key exchange over an IKE session. The default algorithm for key exchange used by this protocol is the Diffie-Hellman algorithm.
- SKEME: This protocol is another version for key exchange.

IKE enhances IPsec by providing additional features along with flexibility. IPsec, however, can be configured without IKE.

IKE has many benefits. It eliminates the need to manually specify all the IPSec security parameters at both peers. It allows the user to specify a particular lifetime for the IPsec security association. Furthermore, encryption can be changed during IPsec sessions. Moreover, it permits certification authority. Finally, it allows dynamic authentication of peers.

The IKE works in two steps. The first step establishes an authenticated communication channel between the peers, by using algorithms like the Diffie-Hellman key exchange, which generates a shared key to further encrypt IKE communications. The communication channel formed as a result of the algorithm is a bi-directional channel. The authentication of the channel is achieved by using a shared key, signatures, or public key encryption.

There are two modes of operation for the first step: main mode, which is utilized to protect the identity of the peers, and aggressive mode, which is used when the security of the identity of the peers is not an important issue. During the second step, the peers use the secure communication channel to set up security negotiations on behalf of other services like IPSec. These negotiation procedures give rise to two unidirectional channels of which one is inbound and the other outbound. The mode of operation for the second step is the Quick mode.

IKE provides three different methods for peer authentication: authentication using a pre-shared secret, authentication using RSA encrypted nonces, and authentication using RSA signatures. IKE uses the HMAC functions to guarantee the integrity of an IKE session. When an IKE session lifetime expires, a new Diffie-Hellman exchange is performed and the IKE SA is re-established.

## 1.7. Firewalls

## Introduction of Firewall

Firewall is a network device that isolates organization's internal network from larger outside network/Internet. It can be a hardware, software, or combined system that prevents unauthorized access to or from internal network.

A firewall is a network security device, either hardware or software-based, which

monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

Accept : allow the traffic
Reject : block the traffic but reply with an “unreachable error”
Drop : block the traffic with no reply

A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.

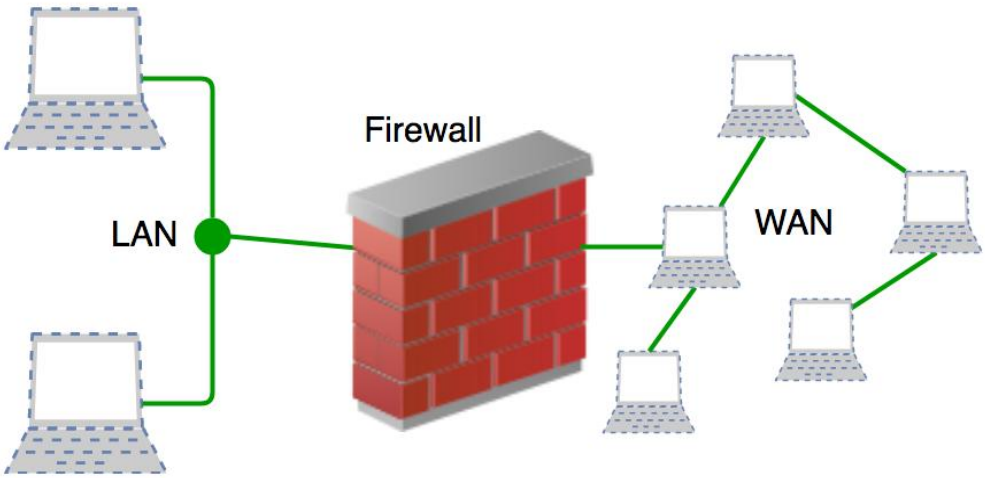



Figure 4.14 Basic Structure of Firewall

History and Need for Firewall

Before Firewalls, network security was performed by Access Control Lists (ACLs) residing on routers. ACLs are rules that determine whether network access should be granted or denied to specific IP address.
But ACLs cannot determine the nature of the packet it is blocking. Also, ACL alone does not have the capacity to keep threats out of the network. Hence, the Firewall was introduced.

Connectivity to the Internet is no longer optional for organizations. However, accessing the Internet provides benefits to the organization; it also enables the outside world to interact with the internal network of the organization. This creates a threat to the organization. In order to secure the internal network from unauthorized traffic, we

need a Firewall.

How Firewall Works

Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization. From the perspective of a server, network traffic can be either outgoing or incoming. Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication.
Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses *type code* instead of port number which identifies purpose of that packet.

Default policy: It is very difficult to explicitly cover every possible rule on the firewall. For this reason, the firewall must always have a default policy. Default policy only consists of action (accept, reject or drop).
Suppose no rule is defined about SSH connection to the server on the firewall. So, it will follow the default policy. If default policy on the firewall is set to *accept*, then any computer outside of your office can establish an SSH connection to the server. Therefore, setting default policy as *drop* (or reject) is always a good practice.

Generation of Firewall

Firewalls can be categorized based on its generation.

1. First Generation- Packet Filtering Firewall : Packet filtering firewall is used to control network access by monitoring outgoing and incoming packet and allowing them to pass or stop based on source and destination IP address, protocols and ports. It analyses traffic at the transport protocol layer (but mainly uses first 3 layers). Packet firewalls treat each packet in isolation. They have no ability to tell whether a packet is part of an existing stream of traffic. Only It can allow or deny the packets

based on unique packet headers.

1. Packet filtering firewall maintains a filtering table which decides whether the packet will be forwarded or discarded. From the given filtering table, the packets will be Filtered according to following rules:

| | Source IP | Dest. IP | Source Port | Dest. Port | Action |
|---|---|---|---|---|---|
| 1 | 192.168.21.0 | -- | -- | -- | deny |
| 2 | -- | -- | -- | 23 | deny |
| 3 | -- | 192.168.21.3 | -- | -- | deny |
| 4 | -- | 192.168.21.0 | -- | >1023 | Allow |

Figure 4.15 Sample packet Filter Firewall Rule

i. Incoming packets from network 192.168.21.0 are blocked.

ii. Incoming packets destined for internal TELNET server (port 23) are blocked.

iii. Incoming packets destined for host 192.168.21.3 are blocked.

iv. All well-known services to the network 192.168.21.0 are allowed.

2. Second Generation- Stateful Inspection Firewall : Stateful firewalls (performs Stateful Packet Inspection) are able to determine the connection state of packet, unlike Packet filtering firewall, which makes it more efficient. It keeps track of the state of networks connection travelling across it, such as TCP streams. So the filtering decisions would not only be based on defined rules, but also on packet's history in the state table.

3. Third Generation- Application Layer Firewall : Application layer firewall can inspect and filter the packets on any OSI layer, up to the application layer. It has the ability to block specific content, also recognize when certain application and protocols (like HTTP, FTP) are being misused.
In other words, Application layer firewalls are hosts that run proxy servers. A proxy firewall prevents the direct connection between either side of the firewall, each packet has to pass through the proxy. It can allow or block the traffic based on predefined

rules.

Note: Application layer firewalls can also be used as Network Address Translator(NAT).

4. Next Generation Firewalls (NGFW) : Next Generation Firewalls are being deployed these days to stop modern security breaches like advance malware attacks and application-layer attacks. NGFW consists of Deep Packet Inspection, Application Inspection, SSL/SSH inspection and many functionalities to protect the network from these modern threats.

## Firewalls are generally of two types: *Host-based* and *Network-based.*

1. Host- based Firewalls : Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.

2. Network-based Firewalls : Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.

Both types of firewall have their own advantages.

## Firewall is categorized into three basic types

- Packet filter (Stateless & Stateful)
- Application-level gateway
- Circuit-level gateway

These three categories, however, are not mutually exclusive. Modern firewalls have a mix of abilities that may place them in more than one of the three categories.

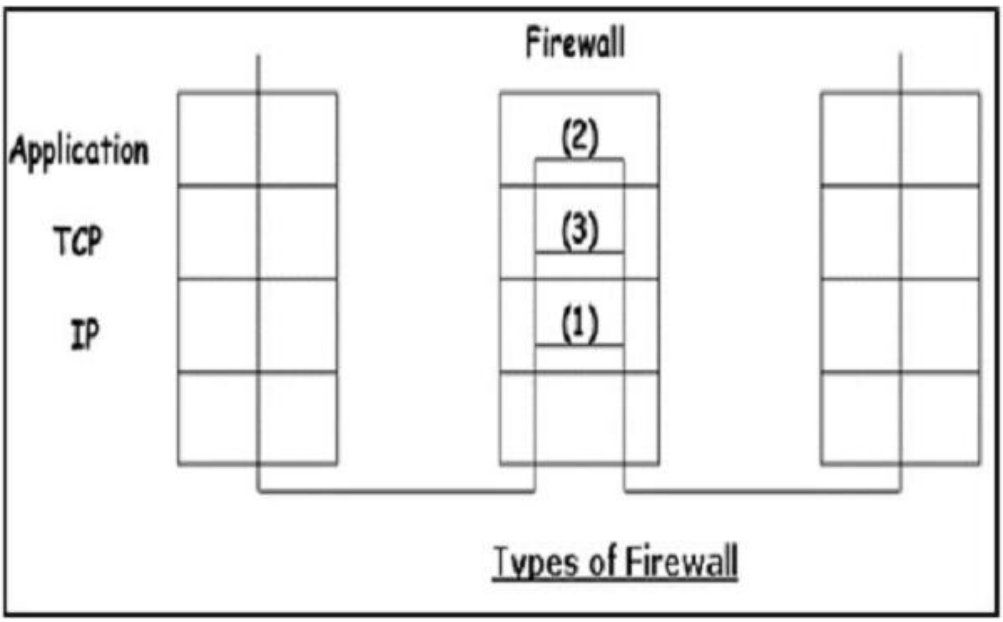



Figure 4.16 Types of firewall

Stateless & Stateful Packet Filtering Firewall

In this type of firewall deployment, the internal network is connected to the external network/Internet via a router firewall. The firewall inspects and filters data packet-by-packet.

Packet-filtering firewalls allow or block the packets mostly based on criteria such as source and/or destination IP addresses, protocol, source and/or destination port numbers, and various other parameters within the IP header.

The decision can be based on factors other than IP header fields such as ICMP message type, TCP SYN and ACK bits, etc.

Packet filter rule has two parts −

- Selection criteria − It is a used as a condition and pattern matching for decision making.
- Action field − This part specifies action to be taken if an IP packet meets the selection criteria. The action could be either block (deny) or permit (allow) the packet across the firewall.

Packet filtering is generally accomplished by configuring Access Control Lists (ACL) on routers or switches. ACL is a table of packet filter rules.

As traffic enters or exits an interface, firewall applies ACLs from top to bottom to each incoming packet, finds matching criteria and either permits or denies the individual packets.

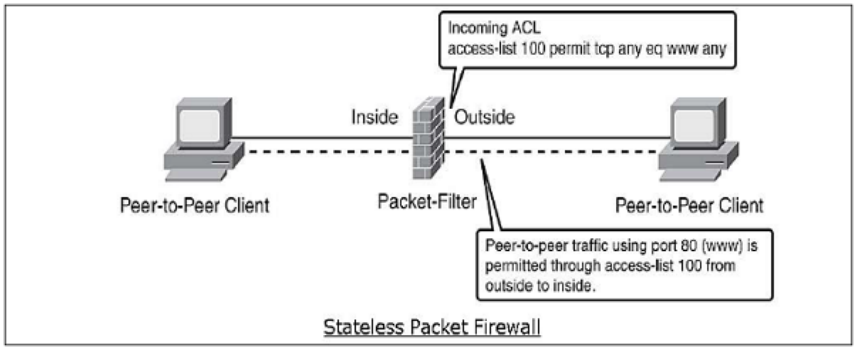



Figure 4.17 Stateless firewall

Stateless firewall is a kind of a rigid tool. It looks at packet and allows it if its meets the criteria even if it is not part of any established ongoing communication.

Hence, such firewalls are replaced by stateful firewalls in modern networks. This type of firewalls offer a more in-depth inspection method over the only ACL based packet inspection methods of stateless firewalls.

Stateful firewall monitors the connection setup and teardown process to keep a check on connections at the TCP/IP level. This allows them to keep track of connections state and determine which hosts have open, authorized connections at any given point in time.

They reference the rule base only when a new connection is requested. Packets belonging to existing connections are compared to the firewall's state table of open connections, and decision to allow or block is taken. This process saves time and provides added security as well. No packet is allowed to trespass the firewall unless it belongs to already established connection. It can timeout inactive connections at firewall after which it no longer admit packets for that connection.

Application Gateways

An application-level gateway acts as a relay node for the application-level traffic. They intercept incoming and outgoing packets, run proxies that copy and forward information across the gateway, and function as a *proxy server*, preventing any direct connection between a trusted server or client and an untrusted host.

The proxies are application specific. They can filter packets at the application layer of the OSI model.

Application-specific Proxies

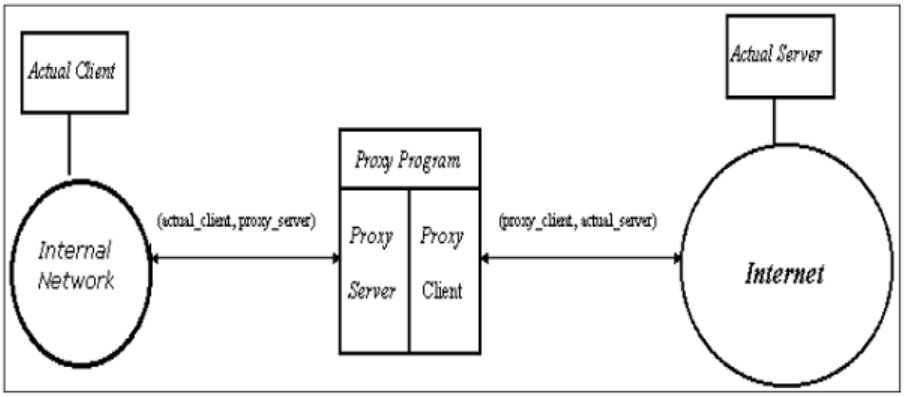



Figure 4.18 Application-specific Proxies

An application-specific proxy accepts packets generated by only specified application for which they are designed to copy, forward, and filter. For example, only a Telnet proxy can copy, forward, and filter Telnet traffic.

If a network relies only on an application-level gateway, incoming and outgoing packets cannot access services that have no proxies configured. For example, if a gateway runs FTP and Telnet proxies, only packets generated by these services can pass through the firewall. All other services are blocked.

Application-level Filtering

An application-level proxy gateway, examines and filters individual packets, rather than simply copying them and blindly forwarding them across the gateway. Application-specific proxies check each packet that passes through the gateway, verifying the contents of the packet up through the application layer. These proxies can filter particular kinds of commands or information in the application protocols.

Application gateways can restrict specific actions from being performed. For example, the gateway could be configured to prevent users from performing the 'FTP put' command. This can prevent modification of the information stored on the server by an attacker.

Transparent

Although application-level gateways can be transparent, many implementations require user authentication before users can access an untrusted network, a process that reduces true transparency. Authentication may be different if the user is from the internal network or from the Internet. For an internal network, a simple list of IP addresses can be allowed to connect to external applications. But from the Internet side a strong authentication should be implemented.

An application gateway actually relays TCP segments between the two TCP connections in the two directions (Client ↔ Proxy ↔ Server).

For outbound packets, the gateway may replace the source IP address by its own IP address. The process is referred to as Network Address Translation (NAT). It ensures that internal IP addresses are not exposed to the Internet.

Circuit-Level Gateway

The circuit-level gateway is an intermediate solution between the packet filter and the application gateway. It runs at the transport layer and hence can act as proxy for any application.

Similar to an application gateway, the circuit-level gateway also does not permit an end-to-end TCP connection across the gateway. It sets up two TCP connections and relays the TCP segments from one network to the other. But, it does not examine the application data like application gateway. Hence, sometime it is called as 'Pipe Proxy'.

**Hybrids Systems**: In an attempt combine the security of the application layer gateways with the flexibility and speed of packet filtering; some vendors have created systems that use the principle of both.

In some of these systems, new connections must be authenticated and approved at the application layer. Once this has been done, the remainder of the connection is passed down to the session layer, where packet filters watch the connection to ensure that only packets that are part of an on-going (already authenticated and approved) conversation are-being passed.

Other possibilities include using both packet filtering and application layer proxies. The benefits here include providing a measure of protection against the machines that provide services to the internet (such as a public web server), as well as provide the security of an application layer gateway to the internal network. Additionally, using this method, an attacker, in order to get to services on the internal network, will have to break through the access router, the bastion host, and the choke router.

**Important Aspects of Effective Firewalls**

Regardless of which security design logic or packet screening method is chosen, two important aspects of the firewall's implementation can determine whether or not a firewall solution will be effective:

First, the device or host system on which the firewall solution resides must be secure. If the system can be compromised, then the firewall can also be compromised. If thefirewalls you choose is based on a well-known network operating system, make sure the operating system is fully patched and all security updates have been applied. .

Second, for a firewall to be effective, all traffic to and from your network must pass through it. If a firewall can be physically or logically bypassed, there is no guarantee that the trusted network is safe. The architecture used for the firewall solution is very important.

Since firewall solutions can be configured using a single system or multiple systems,. the architecture used to implement the solution can be simple or complex. When deciding on a specific architecture keep in mind that the most effective firewall solutions are implemented to all network traffic passes through them. This implementation characteristic is evident in the following commonly identified firewall architectures.

REFERENCES

[1] :Willliam Stallings," Network System Essentials "-4th Edition Copyright © 2011 Pearson education, Inc., publishing as [Prentice Hall,

[2] 2. Atul Khahate, "Cryptography and network security",3rd Edition, Copyright © 2013 TMH Publishing

[3] 3. Kuldeep Singh Kohar", Network Security", revised reprint 2011.Vayu Education of India, New Delhi.Hall, 1983.

## Questions

Part A

1. List the services offered by PGP
2. Define is S/MIME
3. Explain the requirements in SET protocol
4. List the components of IP Security
5. Draw the IP Security Architecture
6. What is Encapsulating Security Payload?
7. How does the Encapsulating Security Payload work?
8. How can the Encapsulating Security Payload be used?
9. What is stateful inspection?
10. What is the benefit of implementing stateful inspection?
11. Define Internet Key Exchange
12. Explain different methods for peer authentication of IKE.
13. Explain the Need for Firewall
14. Define Firewall
15. What are the categories of Firewall

Part B

16. Demonstrate SECURE ELECTRONIC TRANSACTION (SET) with suitable example
17. Illustrate the steps involved in working of PGP
18. Explain in detail about Multipurpose Internet Mail Extensions
19. Organise the architectute of IP Security Overview and explain
20. Distinguish different types of Firewalls