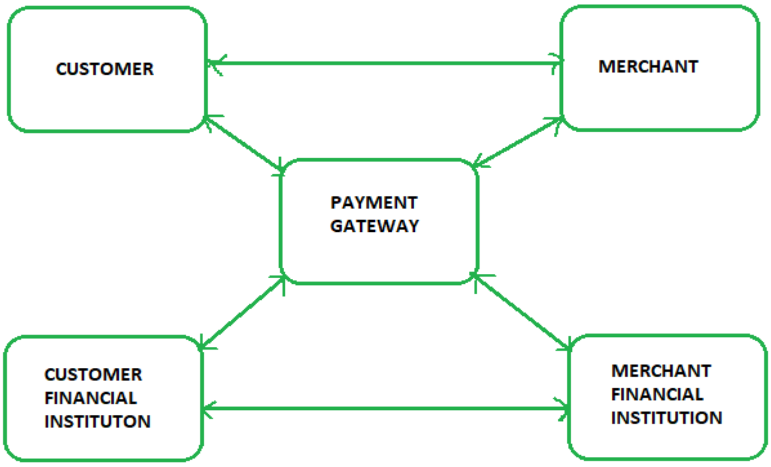
Unit – V

SET

SET (secure electronic transaction) functionalities

Secure Electronic Transaction or SET is a system that ensures the 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 to those payments. It uses different encryption and hashing techniques to secure payments over the internet done through credit cards. The SET protocol was supported in development by major organizations like Visa, Mastercard, and Microsoft which provided its Secure Transaction Technology (STT), and Netscape which provided the technology of Secure Socket Layer (SSL).
SET protocol restricts the revealing of credit card details to merchants thus keeping hackers and thieves at bay. The 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 transactions, which includes client, payment gateway, client financial institution, merchant, and merchant financial institution.



Requirements in SET: The 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 an 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 the best security mechanisms.

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

1. **Cardholder –** customer
2. **Issuer –** customer financial institution
3. **Merchant**
4. **Acquirer –** Merchant financial
5. **Certificate authority –** Authority that follows certain standards and issues certificates(like X.509V3) to all other participants.

SET functionalities:

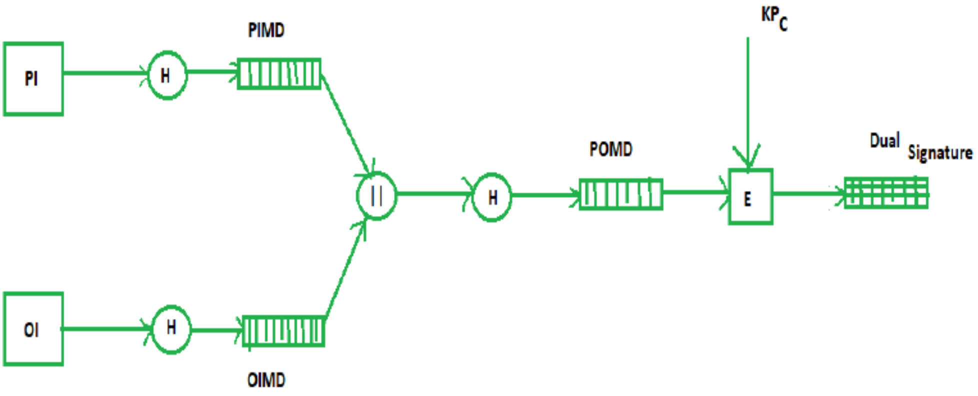
- **Provide Authentication**
    - **Merchant Authentication** – To prevent theft, SET allows customers to check previous relationships between merchants and financial institutions. Standard X.509V3 certificates are used for this verification.
    - **Customer / Cardholder Authentication** – SET checks if the use of a 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 purposes.
- **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:

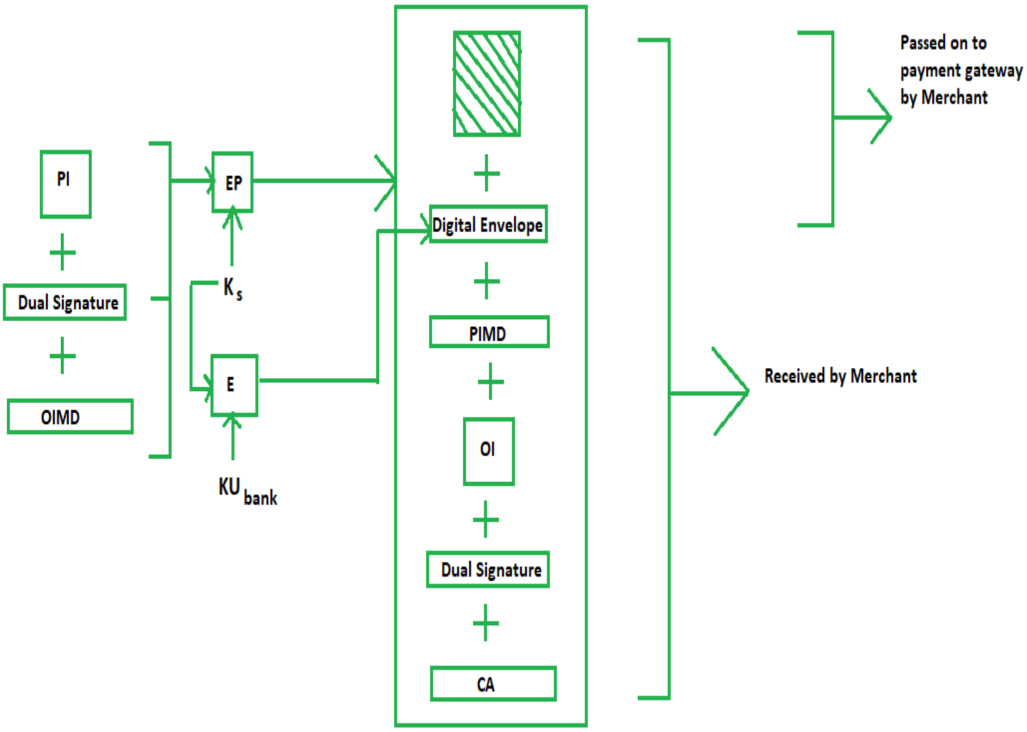


```
Where,

   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:

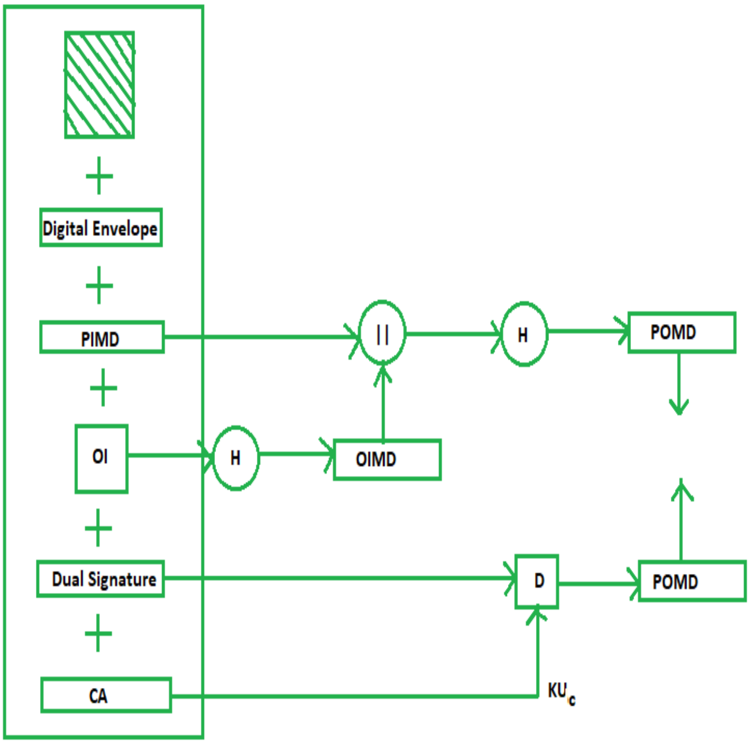
- Payment Information (PI)
- Dual Signature
- Order Information Message Digest (OIMD)

The purchase request is generated as follows:



```
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:



Since we used Customer’s private key in encryption here we use KUC which is the public key of the customer or cardholder for decryption ‘D’.

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

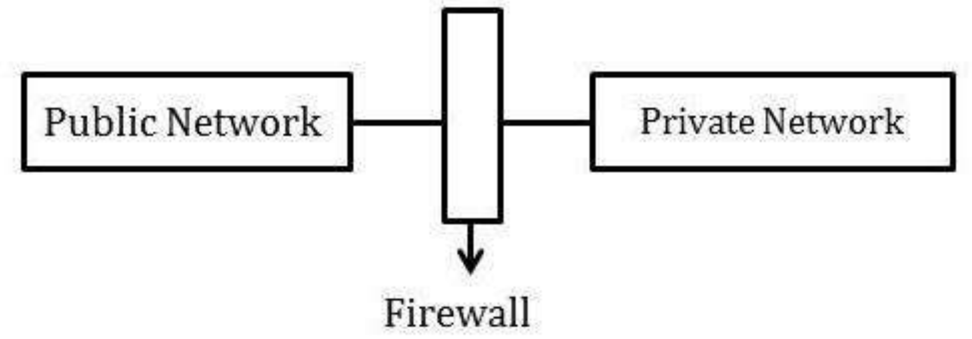
The disadvantages of Secure Electronic Exchange: At the point when SET was first presented in 1996 by the SET consortium (Visa, Mastercard, Microsoft, Verisign, and so forth), being generally taken on inside the following couple of years was normal. Industry specialists additionally anticipated that it would immediately turn into the key empowering influence of worldwide internet business. Notwithstanding, this didn’t exactly occur because of a few serious weaknesses in the convention.

The security properties of SET are better than SSL and the more current TLS, especially in their capacity to forestall web based business extortion. Be that as it may, the greatest downside of SET is its intricacy. SET requires the two clients and traders to introduce extraordinary programming – – card perusers and advanced wallets – – implying that exchange members needed to finish more jobs to carry out SET. This intricacy likewise dialed back the speed of web based business exchanges. SSL and TLS don’t have such issues.

The above associated with PKI and the instatement and enlistment processes additionally slowed down the far reaching reception of SET. Interoperability among SET items – – e.g., declaration interpretations and translations among entrusted outsiders with various endorsement strategies – – was likewise a huge issue with SET, which likewise was tested by unfortunate convenience and the weakness of PKI.

Firewalls

A firewall is a network security device; it is a protective layer for the server that monitors and filters all the incoming and outgoing network traffic. It uses a set of rules to determine whether to allow or block a specific network traffic. Firewalls can prevent unauthorized use before reaching the servers. Firewalls can be hardware or software-based.



Firewall Policies

To protect private networks and individual machines, a firewall can be employed to filter incoming or outgoing traffic based on a predefined set of rules known as *firewall policies*.

Packet flowing through a firewall can have one of the following three outcomes −

- **Accepted** − Permitted through the firewall.
- **Dropped** − Not allowed through with no indication of failure
- **Rejected** − Not allowed through accompanied by an attempt to inform the source that the packet was rejected.

Properties of the packets and the protocols are −

- TCP or UDP
- The source and destination IP address
- The source and destination ports

- The application-level payload of the packet

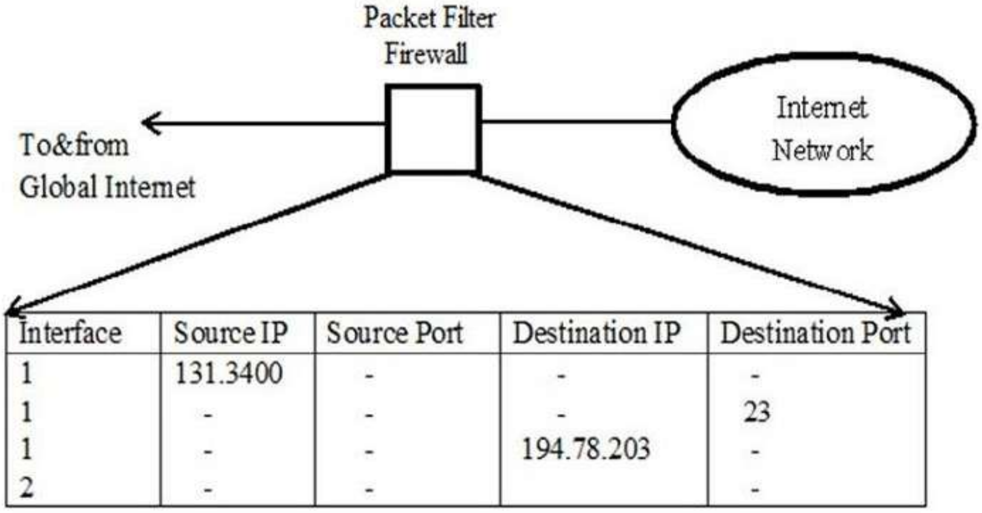
Types of Firewall

- **Packet Filters (Stateless Firewall)** − In the packet filters, if a packet matches then the packet filters set of rules and filters will drop or accept it.
- **Stateful firewall filters** − It is also known as a network firewall; this filter maintains a record of all the connections passing through. It can determine if a packet is either the start of a new connection or a part of an existing connection or is an invalid packet.
- **Application firewall** − A web application firewall is used for HTTP applications. There are sets of rules that are applied to monitor or block data packets from HTTP network traffic. For example, these rules can help block cross-site scripting (XSS) and SQL injections.

Packet Filter Firewall

A packet filter firewall can forward or block packets based on the information in the network layer and transport layer headers source and destination IP addresses, source, and destination port address, and type of protocol (TCP and UDP).

A packet filter firewall is a router that uses a filtering table to decide which packet must be discarded or not to forward. It filters at the network or transport layer.



Interface	Source IP	Source Port	Destination IP	Destination Port
1	131.3400	-	-	-
1	-	-	-	23
1	-	-	194.78.203	-
2	-	-		-

Proxy Based Firewall

A proxy-based firewall acts as an intermediary between the requested data by the end-users and the source servers. The proxy filters all the network traffic and will block or allow the traffic based on its rules and policies.

The proxy can also examine the entire network packet besides the network address and the port number. This type of firewall is labeled as the most secured, as it prevents direct network contact between the systems.

Firewall basing

A firewall is a critical component of any secure network system, and firewall basing is an important security practice that can help protect networks from malicious attacks. Firewall basing is the process of configuring and managing firewalls to allow only specific, predetermined traffic to enter or leave a network, while blocking potentially malicious traffic. Firewall basing makes use of rules and settings that can be configured to create a secure environment, and is a vital part of network security. It can also be used to monitor, analyze, and control network activity and access, giving administrators the ability to detect and prevent unauthorized use of network resources. By utilizing firewall basing, organizations can have greater control over the security of their networks, making them more secure and protected from malicious threats.

Bastion Host

A bastion host is a system identified by the firewall administrator as a critical strong point in the network's security.Typically, the bastion host serves as a platform for an application-level or circuit-level gateway. Common characteristics of a bastion host are as follows: • The bastion host hardware platform executes a secure version of its operating system, making it a hardened system. • Only the services that the network administrator considers essential are installed on the bastion host. These could include proxy applications for DNS, FTP, HTTP, and SMTP. • The bastion host may require additional authentication before a user is allowed access to the proxy services. In addition, each proxy service may require its own authentication before granting user access. • Each proxy is configured to support only a subset of the standard application's command set. • Each proxy is configured to allow access only to specific host systems. This means that the limited command/feature set may be applied only to a subset of systems on the protected network.

• Each proxy maintains detailed audit information by logging all traffic, each connection, and the duration of each connection. The audit log is an essential tool for discovering and terminating intruder attacks. • Each proxy module is a very small software package specifically designed for network security. Because of its relative simplicity, it is easier to check such modules for security flaws. For example, a typical UNIX mail application may contain over 20,000 lines of code, while a mail proxy may contain fewer than 1000. • Each proxy is independent of other proxies on the bastion host. If there is a problem with the operation of any proxy, or if a future vulnerability is discovered, it can be uninstalled without affecting the operation of the other proxy applications. Also, if the user population requires support for a new service, the network administrator can easily install the required proxy on the bastion host. • A proxy generally performs no disk access other than to read its initial configuration file. Hence, the portions of the file system containing executable code can be made read only. This makes it difficult for an intruder to install Trojan horse sniffers or other dangerous files on the bastion host. • Each proxy runs as a nonprivileged user in a private and secured directory on the bastion host.

Host-Based Firewalls

A host-based firewall is a software module used to secure an individual host. Such modules are available in many operating systems or can be provided as an add-on package. Like conventional stand-alone firewalls, host-resident firewalls filter and restrict the flow of packets. A common location for such firewalls is a server. There are several advantages to the use of a server-based or workstationbased firewall: • Filtering rules can be tailored to the host environment. Specific corporate security policies for servers can be implemented, with different filters for servers used for different application. • Protection is provided independent of topology. Thus both internal and external attacks must pass through the firewall. • Used in conjunction with stand-alone firewalls, the host-based firewall provides an additional layer of protection. A new type of server can be added to the network, with its own firewall, without the necessity of altering the network firewall configuration.

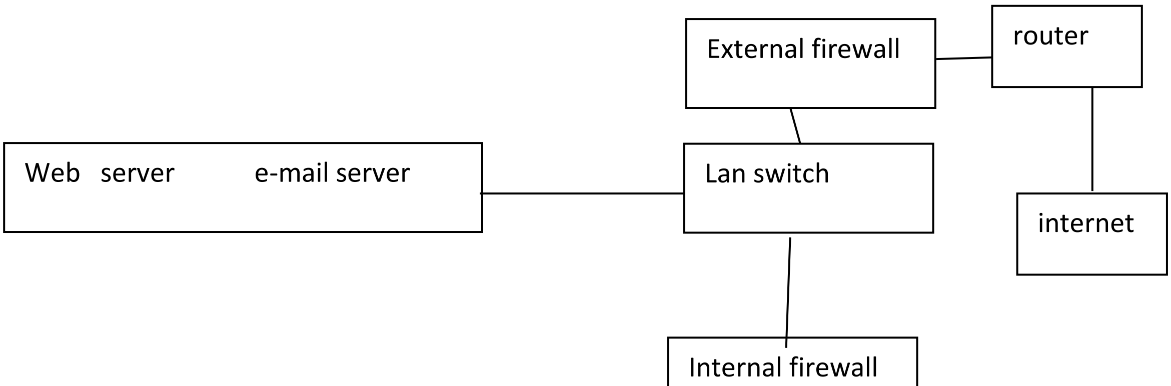
Firewall location and configuration

DMZ Networks suggests the most common distinction, that between an internal and an external firewall. An external firewall is placed at the edge of a local or enterprise network, just inside the boundary router that connects to the Internet or some wide area network (WAN). One or more internal firewalls protect the bulk of the enterprise network. Between these two types of firewalls are one or more networked devices in a region referred to as a DMZ (demilitarized zone) network. Systems that are externally accessible but need some protections are usually located on DMZ networks. Typically, the systems in the DMZ require or foster external connectivity, such as a corporate Web site, an e-mail server, or a DNS (domain name system) server. The external firewall provides a measure of access control and protection for the DMZ systems consistent with their need for external connectivity. The external firewall also provides a basic level of protection for the remainder of the enterprise network. In this type of configuration, internal firewalls serve three purposes:

1. The internal firewall adds more stringent filtering capability, compared to the external firewall, in order to protect enterprise servers and workstations from external attack.

2. The internal firewall provides two-way protection with respect to the DMZ. First, the internal firewall protects the remainder of the network from attacks launched from DMZ systems. Such attacks might originate from worms, rootkits, bots, or other malware lodged in a DMZ system. Second, an internal firewall can protect the DMZ systems from attack from the internal protected network.

3.Multiple internal firewalls can be used to protect portions of the internal network from each other. For example, firewalls can be configured so that internal servers are protected from internal workstations and vice versa. A common practice is to place the DMZ on a different network interface on the external firewall from that used to access the internal networks



E-mail Security

Nowadays, e-mail has become very widely used network application. Let's briefly discuss the e-mail infrastructure before proceeding to know about e-mail security protocols.

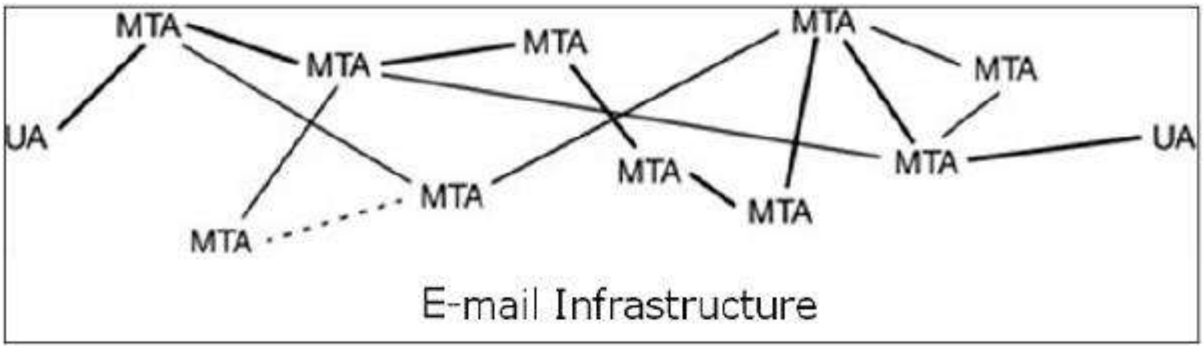
E-mail Infrastructure

The simplest way of sending an e-mail would be sending a message directly from the sender's machine to the recipient's machine. In this case, it is essential for both the machines to be running on the network simultaneously. However, this setup is impractical as users may occasionally connect their machines to the network.

Hence, the concept of setting up e-mail servers arrived. In this setup, the mail is sent to a mail server which is permanently available on the network. When the recipient's machine connects to the network, it reads the mail from the mail server.

In general, the e-mail infrastructure consists of a mesh of mail servers, also termed as **Message Transfer Agents** (MTAs) and client machines running an e-mail program comprising of User Agent (UA) and local MTA.

Typically, an e-mail message gets forwarded from its UA, goes through the mesh of MTAs and finally reaches the UA on the recipient's machine.



E-mail Infrastructure

The protocols used for e-mail are as follows −

- Simple mail Transfer Protocol (SMTP) used for forwarding e-mail messages.

- Post Office Protocol (POP) and Internet Message Access Protocol (IMAP) are used to retrieve the messages by recipient from the server.

MIME

Basic Internet e-mail standard was written in 1982 and it describes the format of e-mail message exchanged on the Internet. It mainly supports e-mail message written as text in basic Roman alphabet.

By 1992, the need was felt to improve the same. Hence, an additional standard *Multipurpose Internet Mail Extensions* (MIME) was defined. It is a set of extensions to the basic Internet E-mail standard. MIME provides an ability to send e-mail using characters other than those of the basic Roman alphabet such as Cyrillic alphabet (used in Russian), the Greek alphabet, or even the ideographic characters of Chinese.

Another need fulfilled by MIME is to send non-text contents, such as images or video clips. Due to this features, the MIME standard became widely adopted with SMTP for e-mail communication.

E-Mail Security Services

Growing use of e-mail communication for important and crucial transactions demands provision of certain fundamental security services as the following −

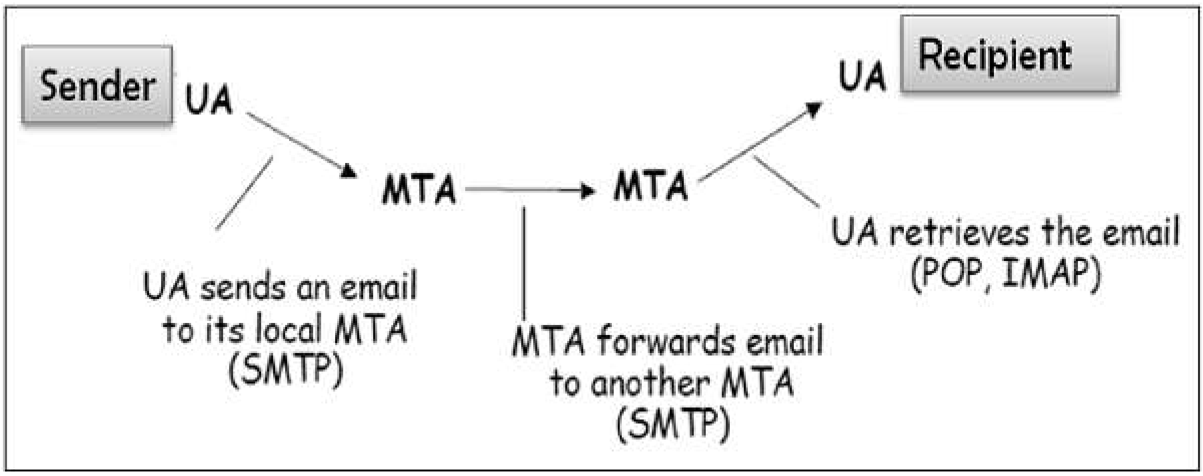
- **Confidentiality** − E-mail message should not be read by anyone but the intended recipient.
- **Authentication** − E-mail recipient can be sure of the identity of the sender.
- **Integrity** − Assurance to the recipient that the e-mail message has not been altered since it was transmitted by the sender.
- **Non-repudiation** − E-mail recipient is able to prove to a third party that the sender really did send the message.
- **Proof of submission** − E-mail sender gets the confirmation that the message is handed to the mail delivery system.
- **Proof of delivery** − Sender gets a confirmation that the recipient received the message.

Security services such as privacy, authentication, message integrity, and non-repudiation are usually provided by using public key cryptography.

Typically, there are three different scenarios of e-mail communication. We will discuss the methods of achieving above security services in these scenarios.

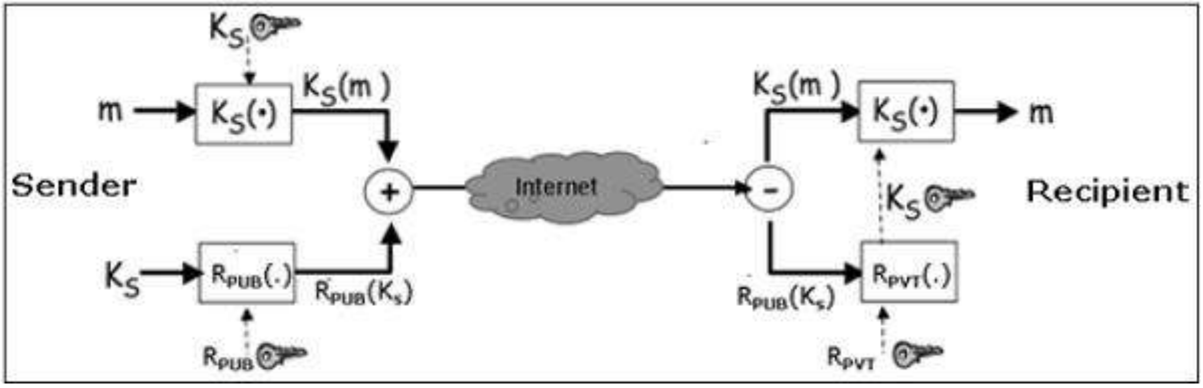
One-to-One E-mail

In this scenario, the sender sends an e-mail message to only one recipient. Usually, not more than two MTA are involved in the communication.


Sender
UA
MTA
MTA
UA
Recipient
UA sends an email to its local MTA (SMTP)
MTA forwards email to another MTA (SMTP)
UA retrieves the email (POP, IMAP)

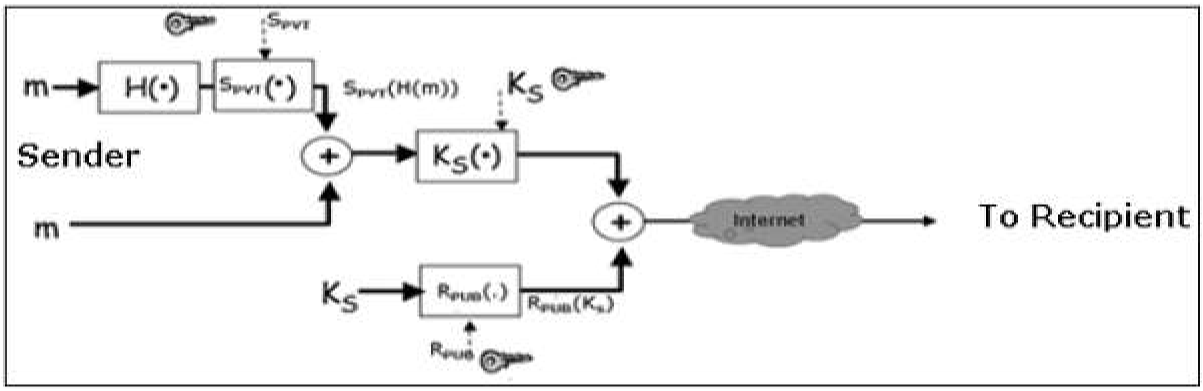
Let's assume a sender wants to send a confidential e-mail to a recipient. The provision of privacy in this case is achieved as follows −

- The sender and receiver have their private-public keys as (S_{PVT}, S_{PUB}) and (R_{PVT}, R_{PUB}) respectively.
- The sender generates a secret symmetric key, K_S for encryption. Though the sender could have used R_{PUB} for encryption, a symmetric key is used to achieve faster encryption and decryption.
- The sender encrypts message with key K_S and also encrypts K_S with public key of the recipient, R_{PUB}.
- The sender sends encrypted message and encrypted K_S to the recipient.
- The recipient first obtains K_S by decrypting encoded K_S using his private key, R_{PVT}.
- The recipient then decrypts message using the symmetric key, K_S.



If message integrity, authentication, and non-repudiation services are also needed in this scenario, the following steps are added to the above process.

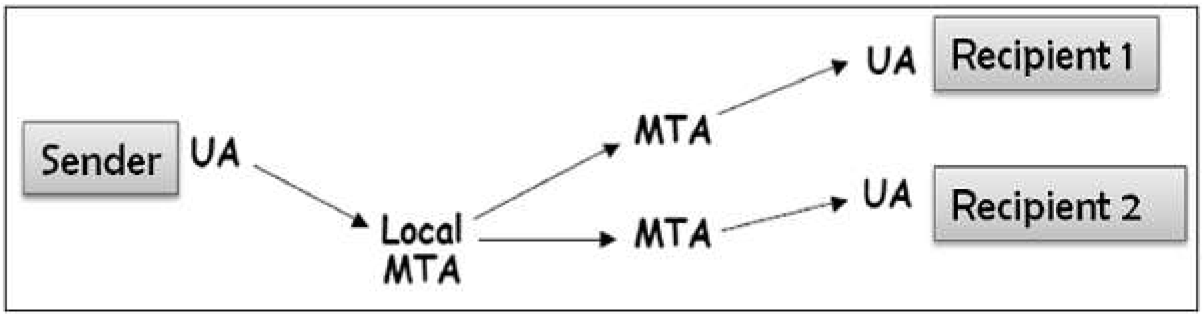
- The sender produces hash of message and digitally signs this hash with his private key, S_{PVT}.
- The sender sends this signed hash to the recipient along with other components.



- The recipient uses public key S_{PUB} and extracts the hash received under the sender's signature.
- The recipient then hashes the decrypted message and now compares the two hash values. If they match, message integrity is considered to be achieved.
- Also, the recipient is sure that the message is sent by the sender (authentication). And lastly, the sender cannot deny that he did not send the message (non-repudiation).

One-to-Multiple Recipients E-mail

In this scenario, the sender sends an e-mail message to two or more recipients. The list is managed by the sender's e-mail program (UA + local MTA). All recipients get the same message.



Let's assume, the sender wants to send confidential e-mail to many recipients (say R1, R2, and R3). The provision of privacy in this case is achieved as follows −

- The sender and all recipients have their own pair of private-public keys.
- The sender generates a secret symmetric key, K_s and encrypts the message with this key.
- The sender then encrypts K_S multiple times with public keys of R1, R2, and R3, getting $R1_{PUB}(K_S)$, $R2_{PUB}(K_S)$, and $R3_{PUB}(K_S)$.
- The sender sends encrypted message and corresponding encrypted K_S to the recipient. For example, recipient 1 (R1) receives encrypted message and $R1_{PUB}(K_S)$.
- Each recipient first extracts key K_S by decrypting encoded K_S using his private key.
- Each recipient then decrypts the message using the symmetric key, K_S.

For providing the message integrity, authentication, and non-repudiation, the steps to be followed are similar to the steps mentioned above in one-to-one e-mail scenario.

PGP

Pretty Good Privacy (PGP) is an e-mail encryption scheme. It has become the de-facto standard for providing security services for e-mail communication.

As discussed above, it uses public key cryptography, symmetric key cryptography, hash function, and digital signature. It provides −

- Privacy
- Sender Authentication
- Message Integrity
- Non-repudiation

Along with these security services, it also provides data compression and key management support. PGP uses existing cryptographic algorithms such as RSA, IDEA, MD5, etc., rather than inventing the new ones.

S / MIME

S/MIME stands for Secure Multipurpose Internet Mail Extension. S/MIME is a secure e-mail standard. It is based on an earlier non-secure e-mailing standard called MIME.

Working of S/MIME

S/MIME approach is similar to PGP. It also uses public key cryptography, symmetric key cryptography, hash functions, and digital signatures. It provides similar security services as PGP for e-mail communication.

The most common symmetric ciphers used in S/MIME are RC2 and TripleDES. The usual public key method is RSA, and the hashing algorithm is SHA-1 or MD5.

S/MIME specifies the additional MIME type, such as “application/pkcs7-mime”, for data enveloping after encrypting. The whole MIME entity is encrypted and packed into an object. S/MIME has standardized cryptographic message formats (different from PGP). In fact, MIME is extended with some keywords to identify the encrypted and/or signed parts in the message.

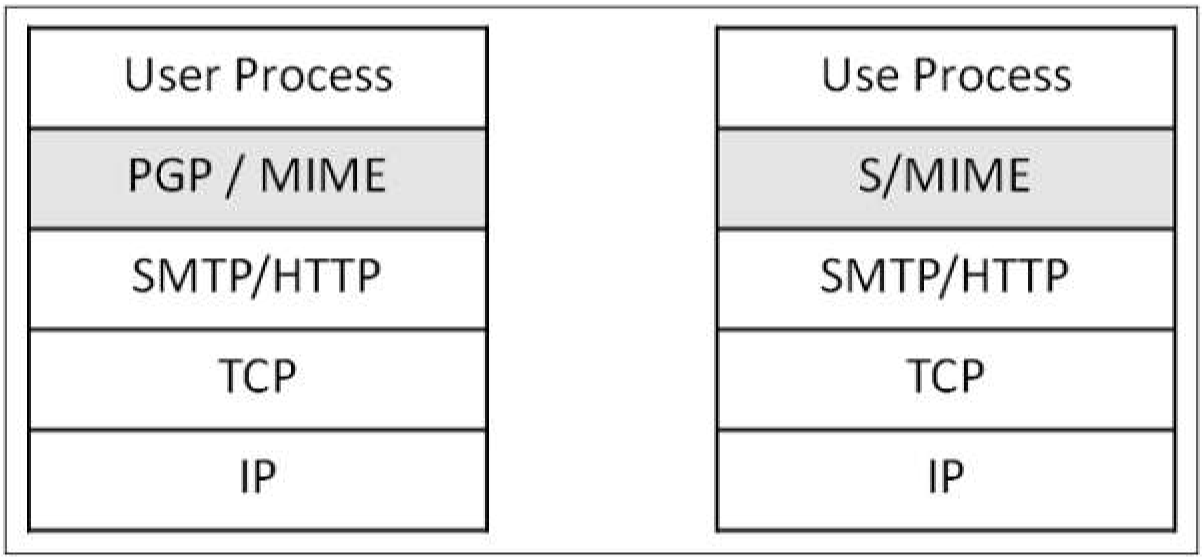
S/MIME relies on X.509 certificates for public key distribution. It needs top-down hierarchical PKI for certification support.

Employability of S/MIME

Due to the requirement of a certificate from certification authority for implementation, not all users can take advantage of S/MIME, as some may wish to encrypt a message, with a public/private key pair. For example, without the involvement or administrative overhead of certificates.

In practice, although most e-mailing applications implement S/MIME, the certificate enrollment process is complex. Instead PGP support usually requires adding a plug-in and that plug-in comes with all that is needed to manage keys. The Web of Trust is not really used. People exchange their public keys over another medium. Once obtained, they keep a copy of public keys of those with whom e-mails are usually exchanged.

Implementation layer in network architecture for PGP and S/MIME schemes is shown in the following image. Both these schemes provide application level security of for e-mail communication.



One of the schemes, either PGP or S/MIME, is used depending on the environment. A secure e-email communication in a captive network can be provided by adapting to PGP. For e-mail security over Internet, where mails are exchanged with new unknown users very often, S/MIME is considered as a good option.

DNS Security

In the first chapter, we have mentioned that an attacker can use DNS Cache Poisoning to carry out an attack on the target user. **Domain Name System Security Extensions** (DNSSEC) is an Internet standard that can foil such attacks.

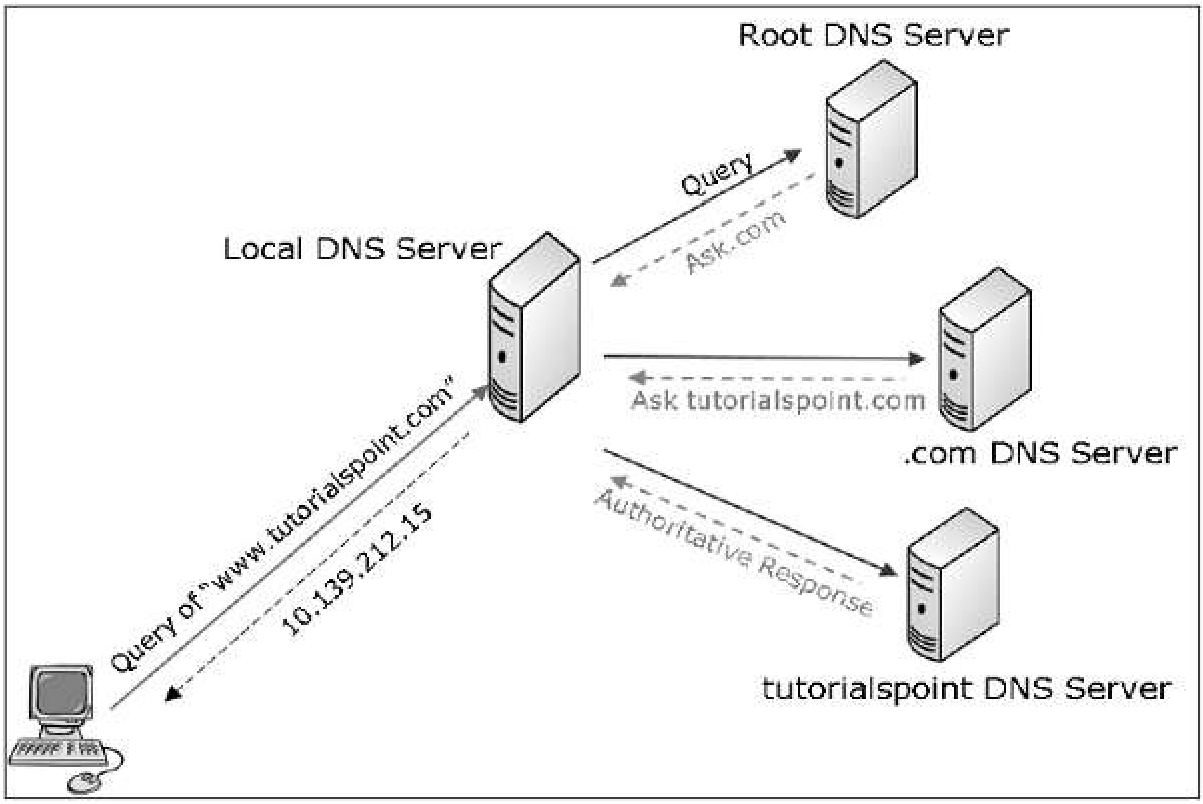
Vulnerability of Standard DNS

In a standard DNS scheme, whenever the user wants to connect to any domain name, his computer contacts the DNS server and looks up the associated IP address for that domain name. Once IP address is obtained, the computer then connects to that IP address.

In this scheme, there is no verification process involved at all. A computer asks its DNS server for the address associated with a website, the DNS server responds with an IP address, and your computer undoubtedly accepts it as legitimate response and connects to that website.

A DNS lookup actually happens in several stages. For example, when a computer asks for “www.tutorialspoint.com”, a DNS lookup is performed in several stages −

- The computer first asks the local DNS server (ISP provided). If ISP has this name in its cache, it responds else forwards the query to “root zone directory” where it can find “.com.” and root zone replies.
- Based on the reply, the computer then asks the “.com” directory where it can find “tutorialspoint.com.”
- Based on the information received, the computer inquires “tutorialspoint.com” where it can find www. tutorialspoint.com.



DNSSEC Defined

DNS lookup, when performed using DNSSEC, involves signing of replies by the responding entity. DNSSEC is based on public-key cryptography.

In DNSSEC standard, every DNS zone has a public/private key pair. All information sent by a DNS server is signed with the originating zone’s private key for ensuring authenticity. DNS clients need to know the zone’s public keys to check the signatures. Clients may be preconfigured with the public keys of all the top-level domains, or root DNS.

With DNSSEC, the lookup process goes as follows −

- When your computer goes to ask the root zone where it can find .com, the reply is signed by the root zone server.
- Computer checks the root zone’s signing key and confirms that it is the legitimate root zone with true information.
- In the reply, the root zone provides the information on the signing key of .com zone server and its location, allowing the computer to contact the .com directory and ensuring it is legitimate.
- The .com directory then provides the signing key and information for tutorialspoint.com, allowing it to contact google.com and verify that you are connected to the real tutorialspoint.com, as confirmed by the zones above it.
- The information sent is in the form of Resource Record Set (RRSets). The example of RRSet for domain “tutorialspoint.com” in top-level “.com” server is shown in the following table.

Domain Name	Time to live	Type	Value

tutorialspoint.com	86400	NS	dns.tutorialspoint.com
dns.tutorialspoint.com	86400	A	36..1.2.3
tutorialspoint.com	86400	KEY	3682793A7B73F731029CE2737D...
tutorialspoint.com	86400	SIG	86947503A8B848F5272E53930C...

- The KEY record is a public key of “tutorialspoint.com”.
- The SIG record is the top-level .com server's signed hash of the fields NS, A, and KEY records to verify their authenticity. Its value is $Kcom_{pvt}$(H(NS,A,KEY)).

Thus, it is considered that when DNSSEC is fully rolled out, the user’s computer is able to confirm that DNS responses are legitimate and true, and avoid DNS attacks launched through DNS cache poisoning.