HTTP Full Form

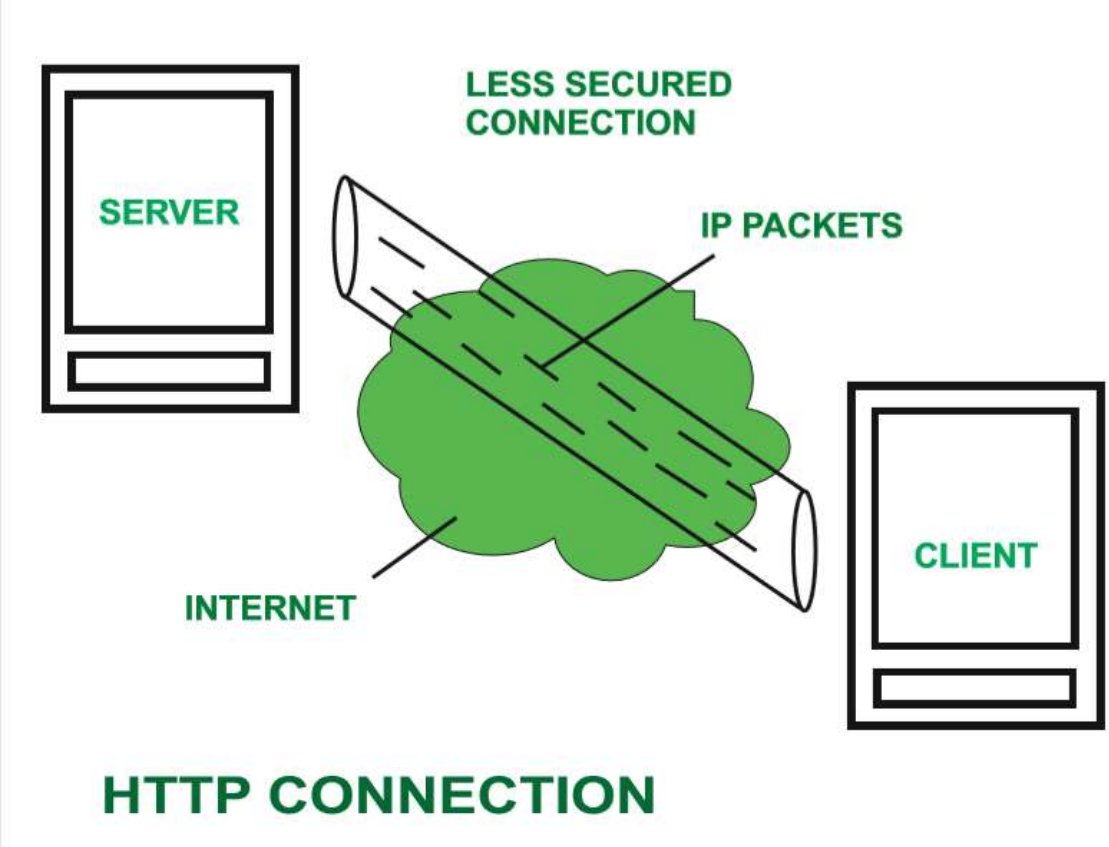
HTTP stands for HyperText Transfer Protocol. It is invented by **Tim Berner.** HyperText is the type of text which is specially coded with the help of some standard coding language called as HyperText Markup Language (HTML). **HTTP/2** is latest version of HTTP, which was published on May 2015. The protocols that are used to transfer hypertext between two computers is known as HyperText Transfer Protocol.

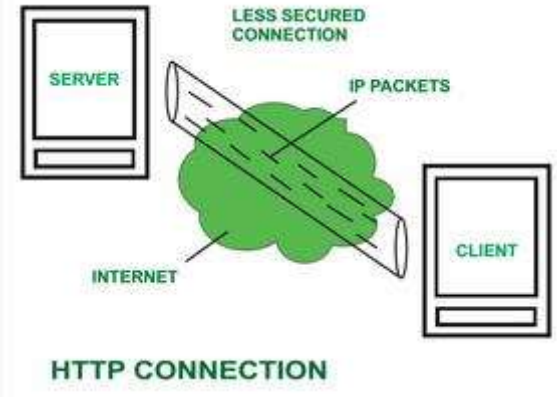
HTTP provides standard between a web browser and web server to establish communication. It is set of rules for transferring data from one computer to another. Data such as text, images, and other multimedia files are shared on the World Wide Web. Whenever a web user opens their web browser, user indirectly uses HTTP. It is an application protocol which is used for distributed, collaborative, hypermedia information systems.

How it works ?

First of all, whenever we want to open any website then first we open web browser after that we will type URL of that website (e.g., www.facebook.com). This URL is now sent to Domain Name Server (DNS). Then DNS first check records for this URL in their database, then DNS will return IP address to web browser corresponding to this URL. Now browser is able to sent request to actual server.

After server sends data to client, connection will be closed. If we want something else from server we should have to re-establish connection between client and server.





History ::

Tim Berners Lee and his team at CERN gets credit for inventing original HTTP and associated technologies.

1. **HTTP version 0.9 –**

   This was first version of HTTP which was introduced in 1991.

2. **HTTP version 1.0 –**
   In 1996, RFC 1945 (Request For Comments) was introduced in HTTP version 1.0.

3. **HTTP version 1.1 –**
   In January 1997, RFC 2068 was introduced in HTTP version 1.1. Improvements and updates to HTTP version 1.1 standard were released under RFC 2616 in June 1999.

4. **HTTP version 2.0 –**
   The HTTP version 2.0 specification was published as RFC 7540 on May 14, 2015.

5. **HTTP version 3.0 –**
   HTTP version 3.0 is based on previous RFC draft. It is renamed as HyperText Transfer Protocol QUIC which is a transport layer network protocol developed by Google.

Characteristics of HTTP: HTTP is IP based communication protocol which is used to deliver data from server to client or vice-versa.

1. Server processes a request, which is raised by client and also server and client knows each other only during current request and response period.
2. Any type of content can be exchanged as long as server and client are compatible with it.
3. Once data is exchanged then servers and client are no more connected with each other.
4. It is a request and response protocol based on client and server requirements.

5. It is connection less protocol because after connection is closed, server does not remember anything about client and client does not remember anything about server.
6. It is stateless protocol because both client and server does not expecting anything from each other but they are still able to communicate.

Advantages :

- Memory usage and CPU usage are low because of less simultaneous connections.
- Since there are few TCP connections hence network congestion are less.
- Since handshaking is done at initial connection stage, then latency is reduced because there is no further need of handshaking for subsequent requests.
- The error can be reports without closing connection.
- HTTP allows HTTP pipe-lining of request or response.

Disadvantages :

- HTTP requires high power to establish communication and transfer data.
- HTTP is less secure, because it does not uses any encryption method like https use TLS to encrypt normal http requests and response.
- HTTP is not optimized for cellular phone and it is too gabby.
- HTTP does not offer genuine exchange of data because it is less secure.
- Client does not close connection until it receives complete data from server and hence server needs to wait for data completion and cannot be available for other clients during this time.

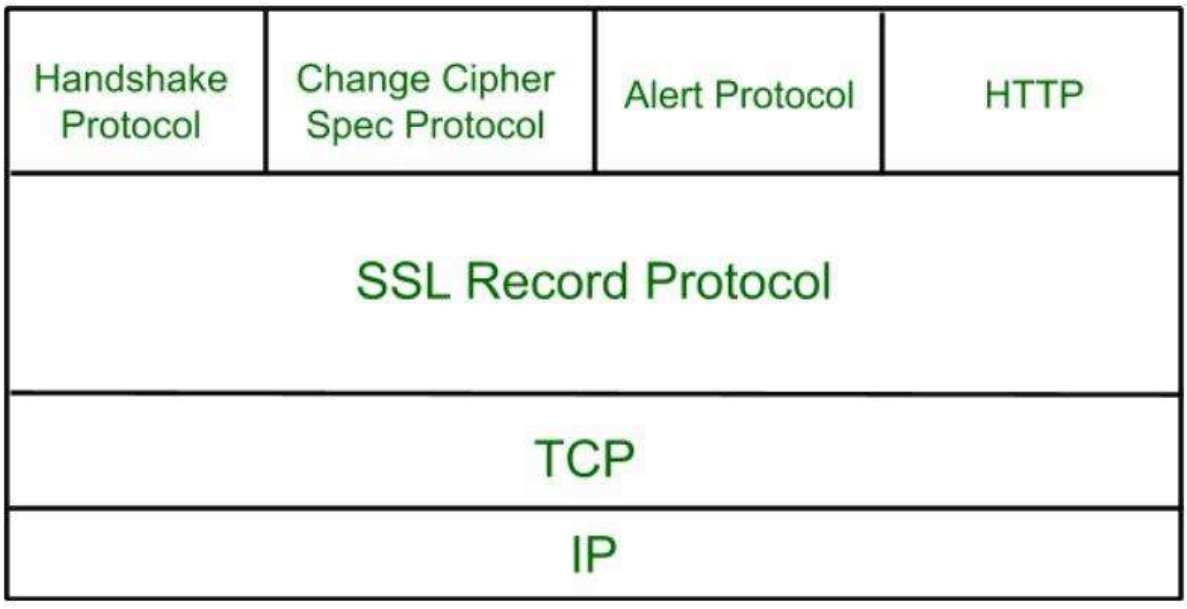
Secure Socket Layer (SSL)

Secure Socket Layer (SSL) provides security to the data that is transferred between web browser and server. SSL encrypts the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.

Secure Socket Layer Protocols:

- SSL record protocol
- Handshake protocol
- Change-cipher spec protocol
- Alert protocol

SSL Protocol Stack:

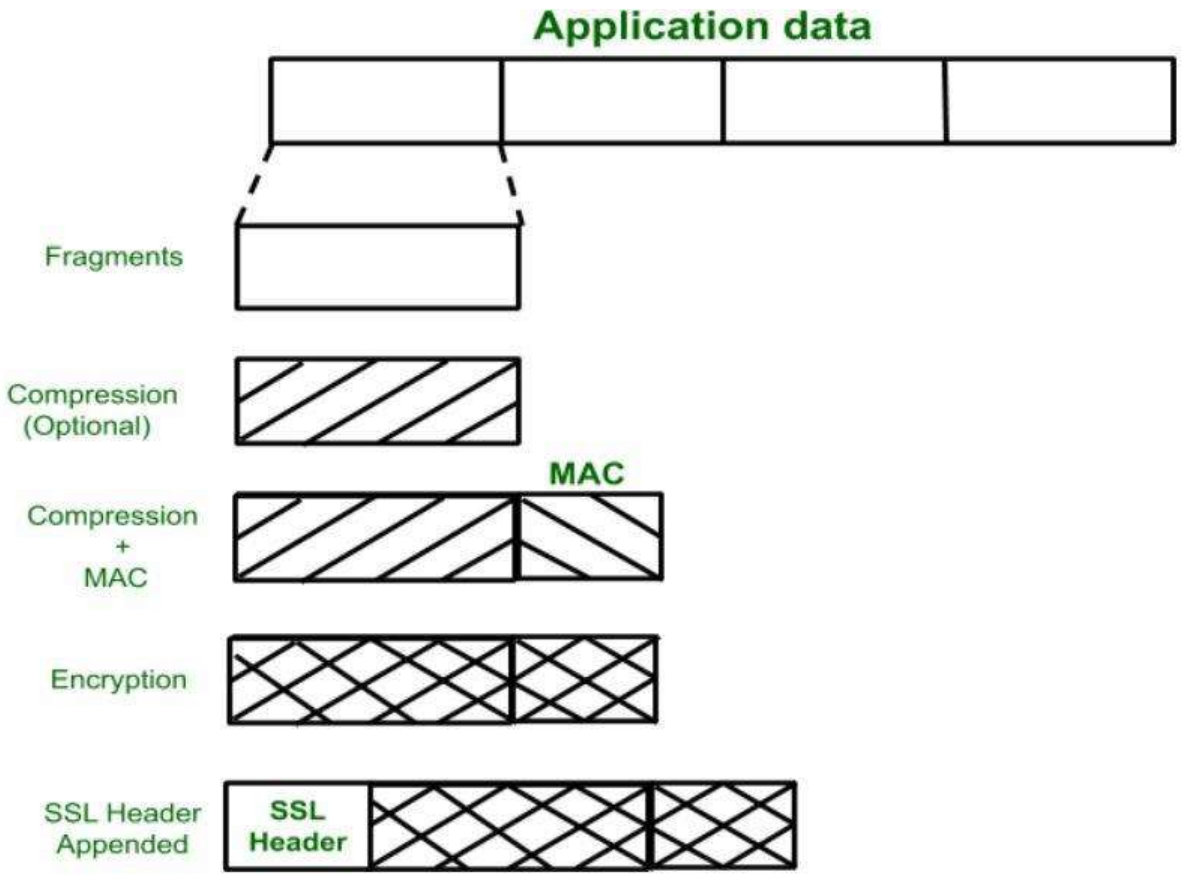


SSL Record Protocol:

SSL Record provides two services to SSL connection.

- Confidentiality
- Message Integrity

In the SSL Record Protocol application data is divided into fragments. The fragment is compressed and then encrypted MAC (Message Authentication Code) generated by algorithms like SHA (Secure Hash Protocol) and MD5 (Message Digest) is appended. After that encryption of the data is done and in last SSL header is appended to the data.



Handshake Protocol:

Handshake Protocol is used to establish sessions. This protocol allows the client and server to authenticate each other by sending a series of messages to each other. Handshake protocol uses four phases to complete its cycle.

- **Phase-1:** In Phase-1 both Client and Server send hello-packets to each other. In this IP session, cipher suite and protocol version are exchanged for security purposes.

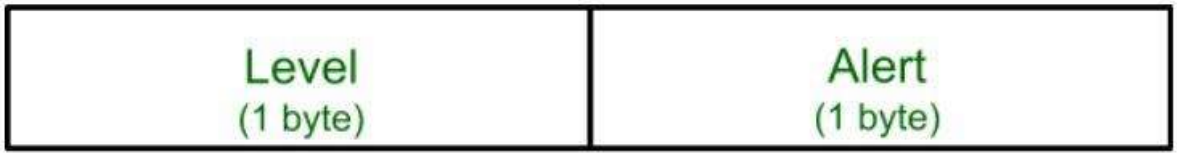
- **Phase-2:** Server sends his certificate and Server-key-exchange. The server end phase-2 by sending the Server-hello-end packet.
- **Phase-3:** In this phase, Client replies to the server by sending his certificate and Client-exchange-key.
- **Phase-4:** In Phase-4 Change-cipher suite occurred and after this Handshake Protocol ends.

Change-cipher Protocol:

This protocol uses the SSL record protocol. Unless Handshake Protocol is completed, the SSL record Output will be in a pending state. After handshake protocol, the Pending state is converted into the current state.
Change-cipher protocol consists of a single message which is 1 byte in length and can have only one value. This protocol's purpose is to cause the pending state to be copied into the current state.

Alert Protocol:

This protocol is used to convey SSL-related alerts to the peer entity. Each message in this protocol contains 2 bytes.



The level is further classified into two parts:

Warning (level = 1):
This Alert has no impact on the connection between sender and receiver. Some of them are:
Bad certificate: When the received certificate is corrupt.
No certificate: When an appropriate certificate is not available.
Certificate expired: When a certificate has expired.
Certificate unknown: When some other unspecified issue arose in processing the certificate, rendering it unacceptable.
Close notify: It notifies that the sender will no longer send any messages in the connection.

Fatal Error (level = 2):
This Alert breaks the connection between sender and receiver. Some of them are :

Handshake failure: When the sender is unable to negotiate an acceptable set of security parameters given the options available.
Decompression failure: When the decompression function receives improper input.
Illegal parameters: When a field is out of range or inconsistent with other fields.
Bad record MAC: When an incorrect MAC was received.
Unexpected message: When an inappropriate message is received.
The second byte in the Alert protocol describes the error.

Silent Features of Secure Socket Layer:

- The advantage of this approach is that the service can be tailored to the specific needs of the given application.
- Secure Socket Layer was originated by Netscape.

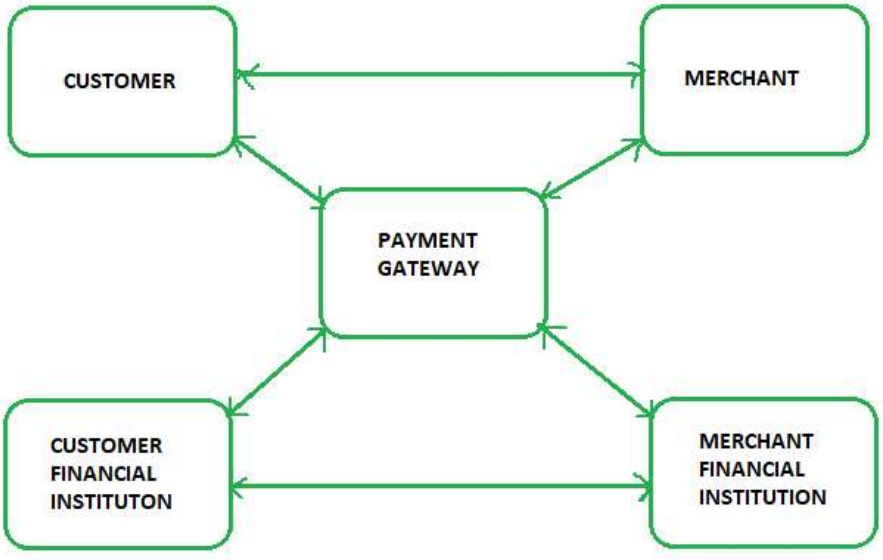
- SSL is designed to make use of TCP to provide reliable end-to-end secure service.
- This is a two-layered protocol.

Secure Electronic Transaction (SET) Protocol

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, 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,

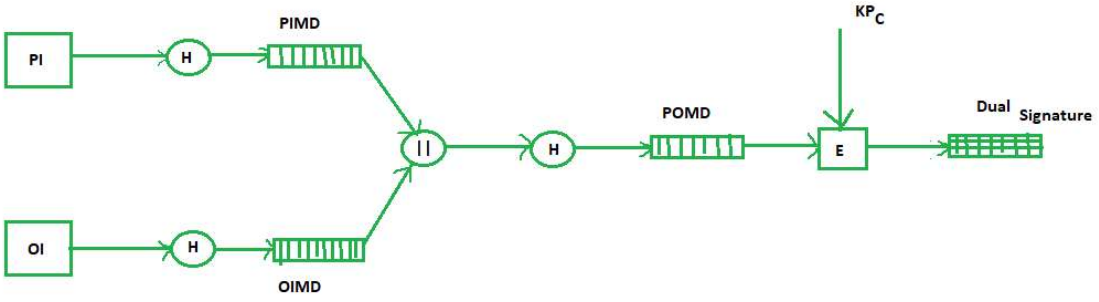
Dual Signature :

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,

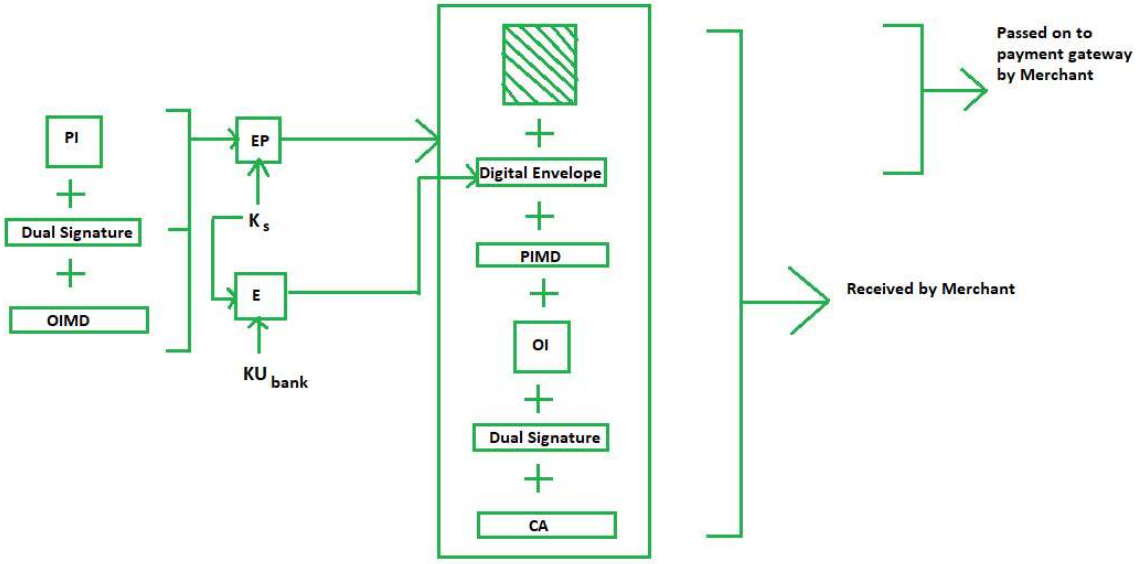
```
PI stands for payment information

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

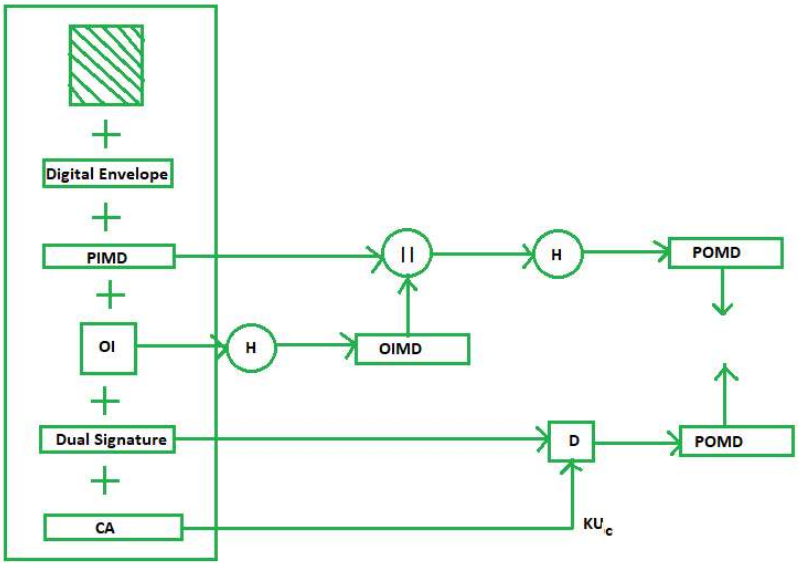
KUbank is public key of bank

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.

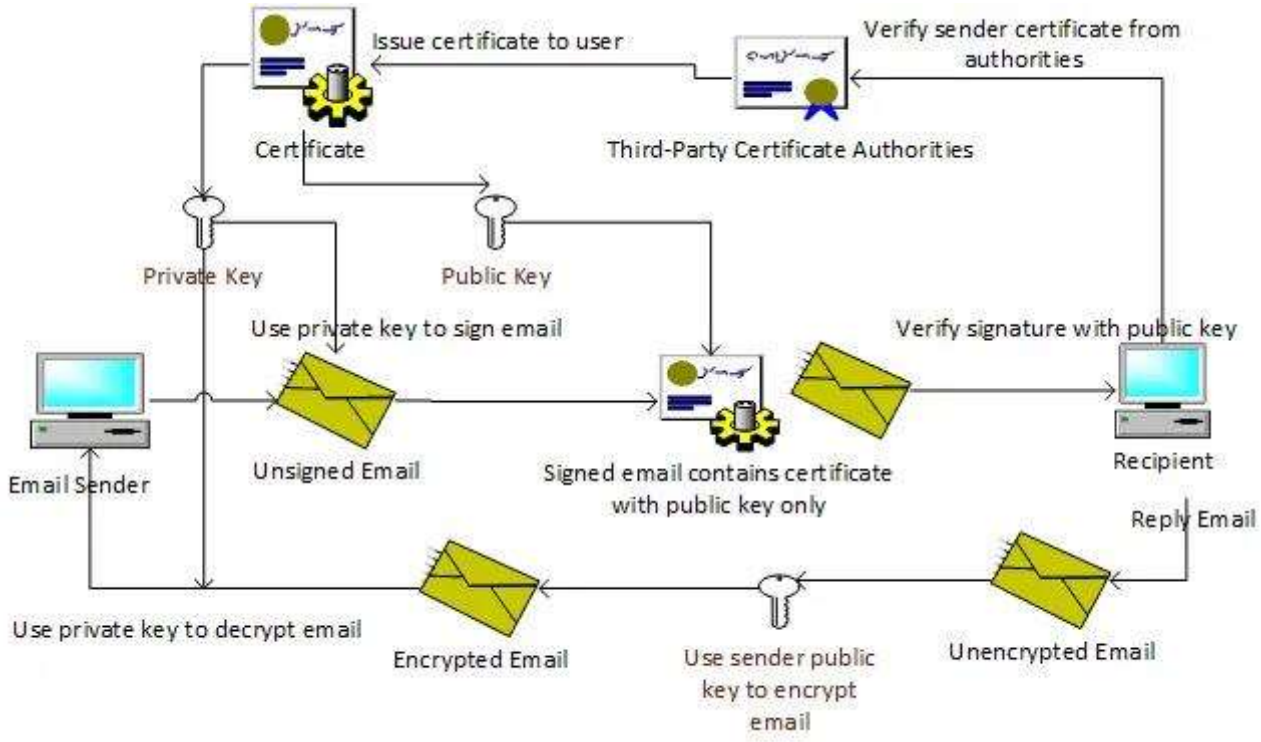
Secure/Multipurpose Internet Mail Extensions (S/MIME)

What is S/MIME (Secure/Multipurpose Internet Mail Extensions)?

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.

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.



S/Mime Structure

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

Privacy Enhanced Mail (PEM) and it's Working

Privacy Enhanced Mail (PEM) is an email security standard to provide secure electronic mail communication over the internet. Security of email messages has become extremely important nowadays. In order to deal with the security issues of emails the internet architecture board has adopted it.
The PEM mainly provides the following services –

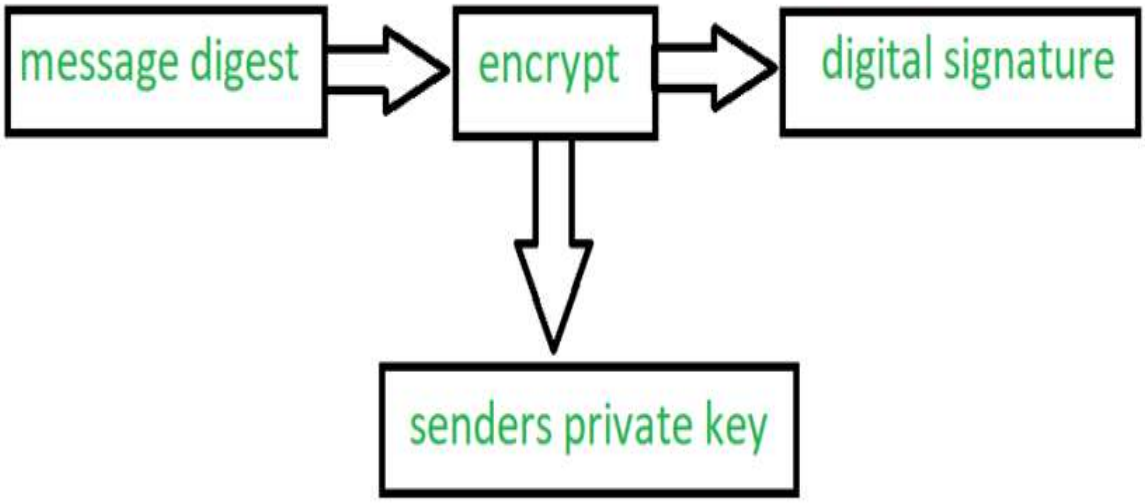
1. **Confidentiality –**
   Confidentiality refers to the act of preventing unauthorized access to the information hence protecting it. The confidentiality is obtained in PEM by encrypting the messages by using various standard algorithms such as Data Encryption Standard (DES). DES in cipher block chaining mode is being currently used by PEM.
2. **Integrity –**
   Data integrity refers to the consistency of data through out its life cycle. This is obtained by using a unique concept called as message digest where message digest is a hash function which converts the message into an image called digest on taking the message as input. PEM uses RSA encryption, MD2 and MD5 hash functions to generate the digests. An octet value is generated from the hash functions which is then encrypted which is then run against the message digest by the receiver assured of the integrity of the message that is transmitted.

Working of PEM :
The PEM works basically in 4 main steps.

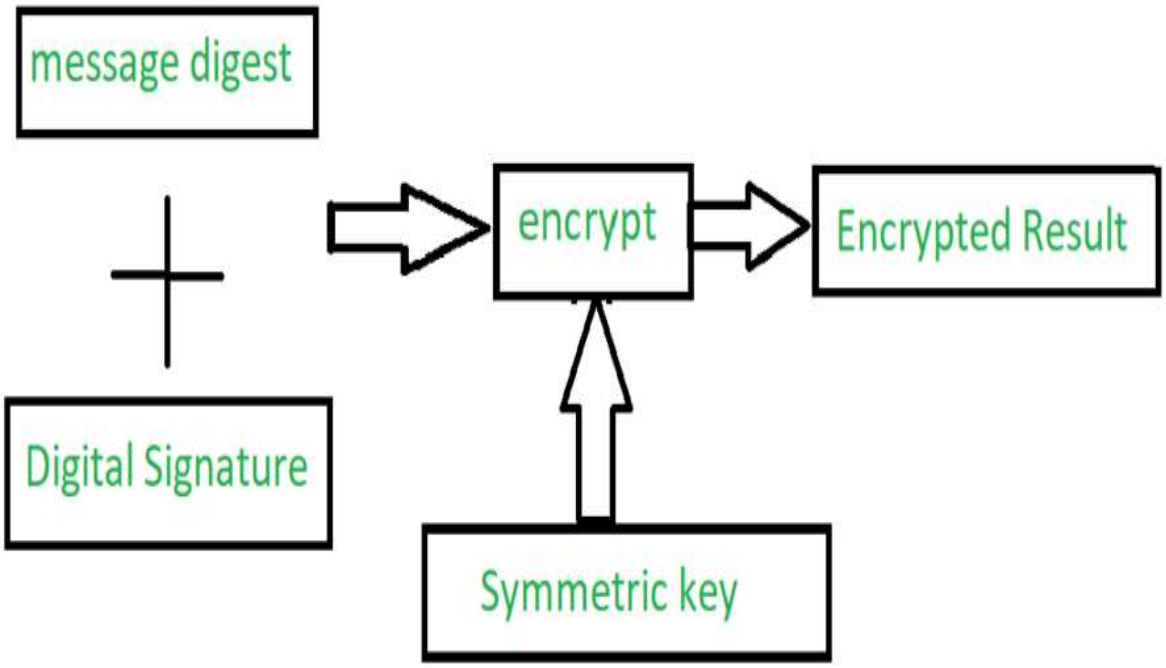
1. **Canonical Conversion –**
   This step involves the conversion of the message into a standard format that is independent of the computer architecture and the operation system of the sender and the receiver. If the sender and receiver has

different computer architecture or operating system. It may lead to generation of different message digest due to difference in their interpretation because of syntactical difference from one operating system to an other.

2. Digital Signature –
   In this step, the digital signature is generated by encrypting the message digest of an email message with the sender's private key.



3. Encryption –
   The encrypted message is generated by encrypting the original message and digital signature together along with the symmetric key as shown in the figure below.This step is very crucial in order to obtain the confidentiality.



4. **Base-64 Encoding –**

   This is the last step where the binary output is transformed into character output. The binary output which is 24 bits is divided into 4 equal sets and mapped with the 8 bit character output generating a decimal code. Now PEM uses a separate map table and each number from the code generated is mapped with its corresponding value from the mapping table and binary equivalent corresponding to the 8 bit ASCII of the character is written.

PGP – Authentication and Confidentiality

In 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.

The following are the services offered by PGP:

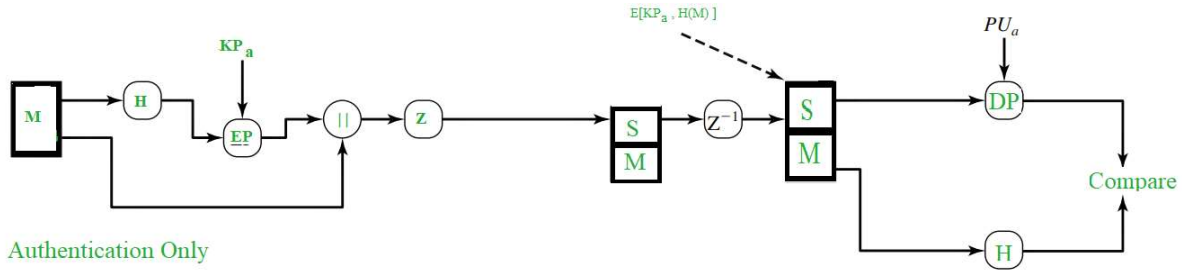
1. Authentication
2. Confidentiality
3. Compression
4. Email Compatibility
5. Segmentation

In this article, we will see about Authentication and Confidentiality.

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:



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.

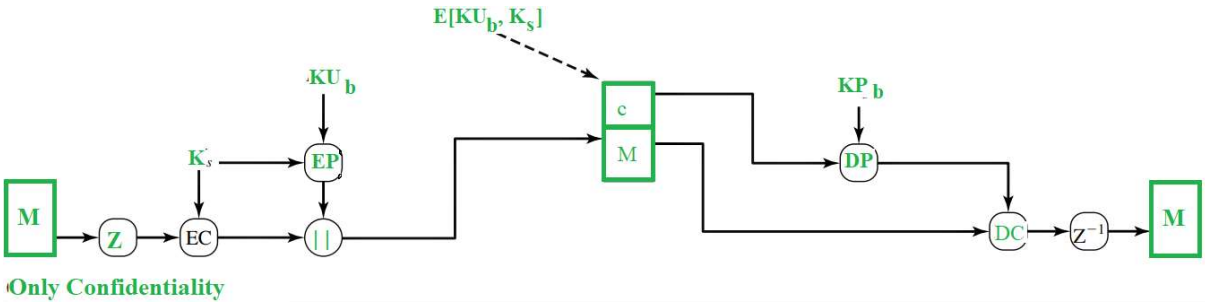
At the receiver's end, the data is decompressed and the message, signature are obtained. The signature is then decrypted using the sender's public key(PU_a) and the hash value is obtained. The message is again passed to hash function and it's hash value is calculated and obtained.

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:

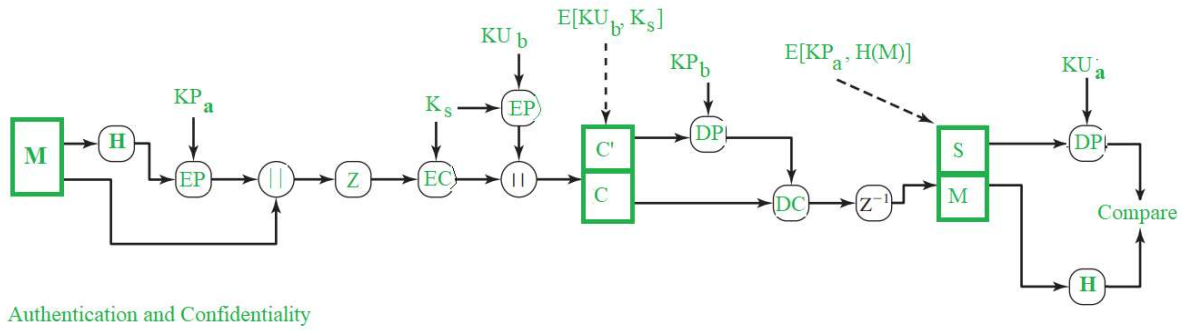


The message is first compressed and a 128 bit session key (K_s), generated by the PGP, is used to encrypt the message through symmetric encryption. Then, the session key (K_s) itself gets encrypted through public key encryption (EP) using receiver's public key(KU_b) . Both the encrypted entities are 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 key encryption, CAST-128(or IDEA or 3DES) is used.

Practically, **both** the Authentication and Confidentiality services are provided in parallel as follows :



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

Wireless Security (WEP)

Wireless Network provides various comfort to end users but actually they are very complex in their working. There are many protocols and technologies working behind to provide a stable connection to users. Data packets traveling through wire provide a sense of security to users as data traveling through wire probably not heard by eavesdroppers.

To secure the wireless connection, we should **focus on** the following areas –

- Identify endpoint of wireless network and end-users i.e., Authentication.
- Protecting wireless data packets from middleman i.e., Privacy.
- Keeping the wireless data packets intact i.e., Integrity.

We know that wireless clients form an association with Access Points (AP) and transmit data back and forth over the air. As long as all wireless devices follow 802.11 standards, they all coexist. But all wireless devices are not friendly and trustworthy, some rogue devices may be a threat to wireless security. Rogue devices can steal our important data or can cause the unavailability of the network.

Wireless security is **ensured by** following methods-

- Authentication
- Privacy and Integrity

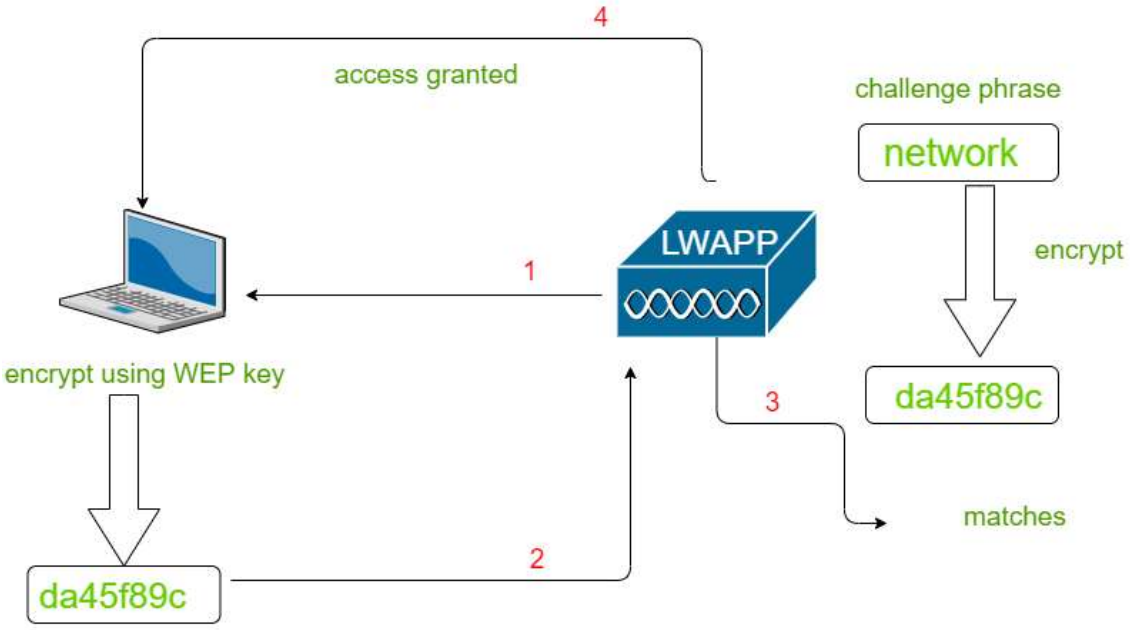
In this article, we talk about Authentication. There are broadly two types of Authentication process: Wired Equivalent Privacy (WEP), and Extensible Authentication Protocol (802.1x/EAP).
These are explained as following below.

1. Wired Equivalent Privacy (WEP) :

For wireless data transmitting over the air, open authentication provides no security.
WEP uses the RC4 cipher algorithm for making every frame encrypted. The RC4

cipher also encrypts data at the sender side and decrypt data at the receiving site, using a string of bits as key called WEP key.

WEP key can be used as an authentication method or encryption tool. A client can associate with AP only if it has the correct WEP key. AP tests the knowledge of the WEP key by using a challenge phrase. The client encrypts the phrase with his own key and send back to AP. AP compares the received encrypted frame with his own encrypted phrase. If both matches, access to the association is granted.



Working of WEP Authentication

2. Extensible Authentication Protocol (802.1x/EAP) :

In WEP authentication, authentication of the wireless clients takes place locally at AP. But Scenario gets changed with 802.1x. A dedicated authentication server is added to the infrastructure. There is the participation of three devices –

1. **Supplicant –**

   Device requesting access.
2. **Authenticator –**

   Device that provides access to network usually a Wlan controller (WLC).

3. **Authentication Server –**

   Device that takes client credentials and deny or grant access.

EAP is further of four types with some amendments over each other –

- LEAP
- EAP-FAST
- PEAP
- EAP-TLS

Wifi protected access (WPA)

The two security protocols and security certification programs are *Wi-Fi Protected Access (WPA)* and *Wi-Fi Protected Access II (WPA2)*. These are developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these protocols because of the serious weaknesses the researchers found in the previous system, Wired Equivalent Privacy (WEP). WPA also referred to as the draft IEEE 802.11i standard became available in 2003. The Wi-Fi Alliance made it as an intermediate measure in anticipation of the availability of the more secure and complex WPA2, which became available in 2004 which is a common shorthand for the full IEEE 802.11i (or IEEE 802.11i-2004) standard.

In January 2018, with several security improvements over WPA2 Wi-Fi Alliance announced the release of *WPA3*.

1. **WPA –**
   The WPA is an intermediate measure to take the place of WEP. WPA could be implemented through firmware upgrades on wireless network interface cards that were designed for WEP in 1999. However, since more changes were required in the wireless access points (APs) than those needed on the network cards, most pre-2003 APs could not be upgraded to support WPA.
   The WPA protocol implements almost all of the IEEE 802.11i standard. The Temporal Key Integrity Protocol (TKIP) was adopted for WPA. WEP used a 64-bit or 128-bit encryption key that must be manually entered on wireless access points and devices which once entered can never be changed. TKIP employs a per-packet key, which means that it dynamically generates a new 128-bit key for each packet and thus prevents the types of attacks that compromised WEP.

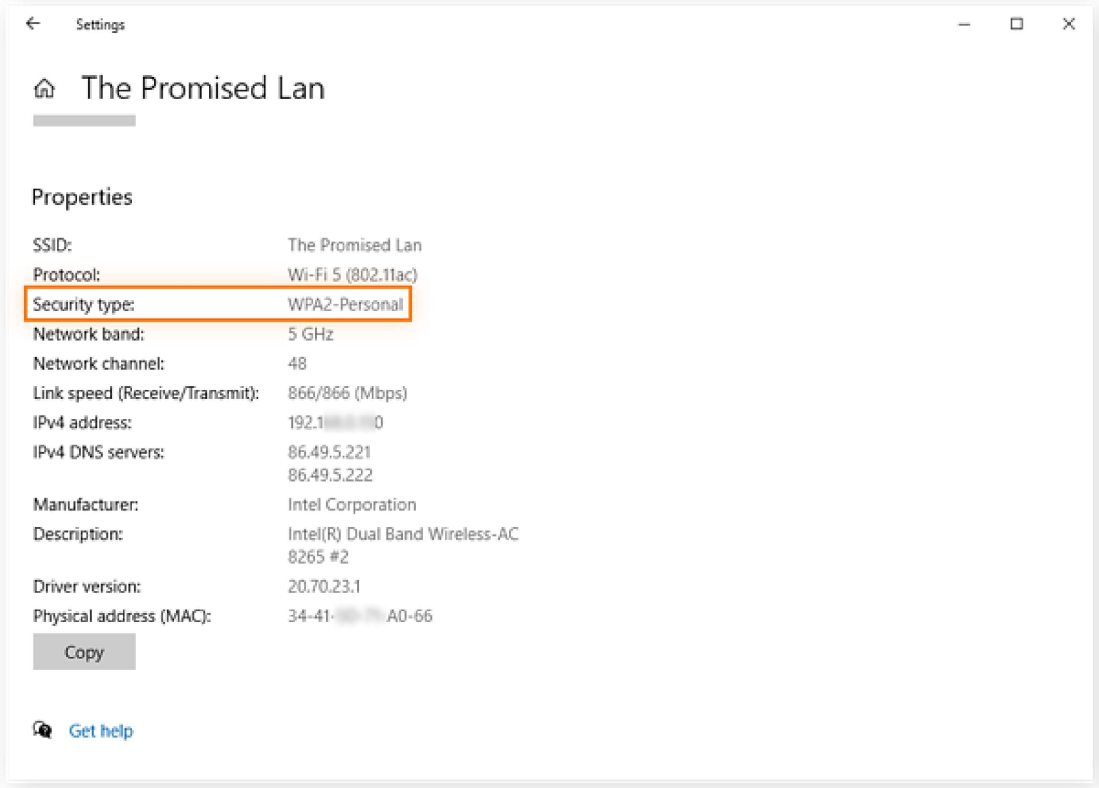
WPA included a Message Integrity Check, which is designed to prevent an attacker to alter or resend data packets. This replaced the cyclic redundancy check (CRC) that was used by the WEP standard. CRC's had a main flaw that it did not provide a sufficiently strong data integrity guarantee for the packets it handled. Well tested message authentication codes existed to solve these problems, but they required too much computation to be used on old network cards. WPA uses a message integrity check algorithm called TKIP to verify the integrity of the packets. TKIP is much stronger than a CRC, but the algorithm used in WPA2 is stronger. Researchers discovered a flaw in WPA similar to older weaknesses in WEP and the limitations of the message integrity code hash function, named Michael, that is used to retrieve the keystream from short packets to use for re-injection and spoofing.

2. **WPA2 –**

   WPA2 replaced WPA. WPA2, which requires testing and certification by the Wi-Fi Alliance, implemented the mandatory elements of IEEE 802.11i. Particularly, it included mandatory support for CCMP(Counter Mode CBC-MAC Protocol), an AES(Advanced Encryption Standard) based encryption mode. Certification began in September, 2004. WPA2 certification is mandatory for all new devices to bear the Wi-Fi trademark from March 13, 2006.

WPA 2

What is WPA2 network security?



WPA2 **ensures that data sent or received over your wireless network is encrypted, and only people with your network password have access to it**. A benefit of the WPA2 system was that it introduced the Advanced Encryption System (AES) to replace the more vulnerable TKIP system used in the original WPA protocol.

Security researchers[1] have discovered a major vulnerability in Wi-Fi Protected Access 2 (WPA2). WPA2 is a type of encryption used to secure the vast majority of Wi-Fi networks. A WPA2 network provides unique encryption keys for each wireless client that connects to it.

Think of **encryption** as a secret code that can only be deciphered if you have the "key," and a vital technology that helps keep digital data away from intruders and identity thieves.

The vulnerability, dubbed "KRACKs" (Key Reinstallation AttaCKs), is actually a group of multiple vulnerabilities that when successfully exploited, could allow attackers to intercept and steal data transmitted across a Wi-Fi network. Digital personal information that is

transmitted over the Internet or stored on your connected devices — such as your driver's license number, Social Security number, credit card numbers, and more — could be vulnerable. All of this personal information can be used toward committing identity theft, such as accessing your bank or investment accounts without your knowledge.

In some instances, attackers could also have the ability to manipulate web pages, turning them into fake websites to collect your information or to install malware on your devices.

What should you do?

Wi-Fi users should immediately update their Wi-Fi-enabled devices as soon as a software update is made available. Wi-Fi enabled devices are anything that connects to the Internet — from laptops, tablets, and smartphones to other smart devices such as wearables and home appliances.

Should you change your Wi-Fi password?

No. This vulnerability does not affect the password to your router's Wi-Fi network. Regardless of if your Wi-Fi network is password protected, this new vulnerability still puts your data at risk because it affects the devices and the Wi-Fi itself, not your home router, which is what the password protects.

The researchers who discovered this vulnerability state that the attack could be "especially catastrophic" against version 2.4 and above of wpa_supplicant, a Wi-Fi client commonly used on Linux and Android 6.0 and above.

If you are using an Android phone, you will need to go the manufacturer's website to see if there is a new patch available for this vulnerability.

Are hackers already exploiting this vulnerability?

Not yet. But as with many newly discovered vulnerabilities, it is only a matter of time before hackers find ways to exploit this weakness to their advantage.

What else can you do to help protect your connected devices while waiting for a software update?

Keep in mind that it may take some time for the manufacturer of your devices to come up with a security patch. In the meantime, there are extra steps you can take to help secure your devices.

We strongly recommend that users install and use a reputable VPN on all their mobile devices and computers before connecting to any Wi-Fi network. By using a secure virtual private network (VPN) on your smartphones and computers, your web traffic will be encrypted and your data will be safe from interception by a hacker. A VPN creates a "secure tunnel" where information sent over a Wi-Fi connection is encrypted, making data sent to and from your device more secure.

Norton Secure VPN uses bank-grade encryption by employing the same encryption technologies that leading banks deploy, so you can rest assured that your information stays secure and private. You can also browse anonymously and protect your privacy with Norton Secure VPN. Mask your online activities and location with this no-log VPN that encrypts your personal information but never stores your online activity or location.

By using a secure VPN (Virtual Private Network) such as Norton Secure VPN, your web traffic will be encrypted by additional means and will be protected against interception.

Additionally, only using HTTPS-enabled websites means your web traffic will also be encrypted by SSL and may be safer from this vulnerability. HTTPS browsing adds an extra layer of security by using encryption via the website you are visiting.

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 –

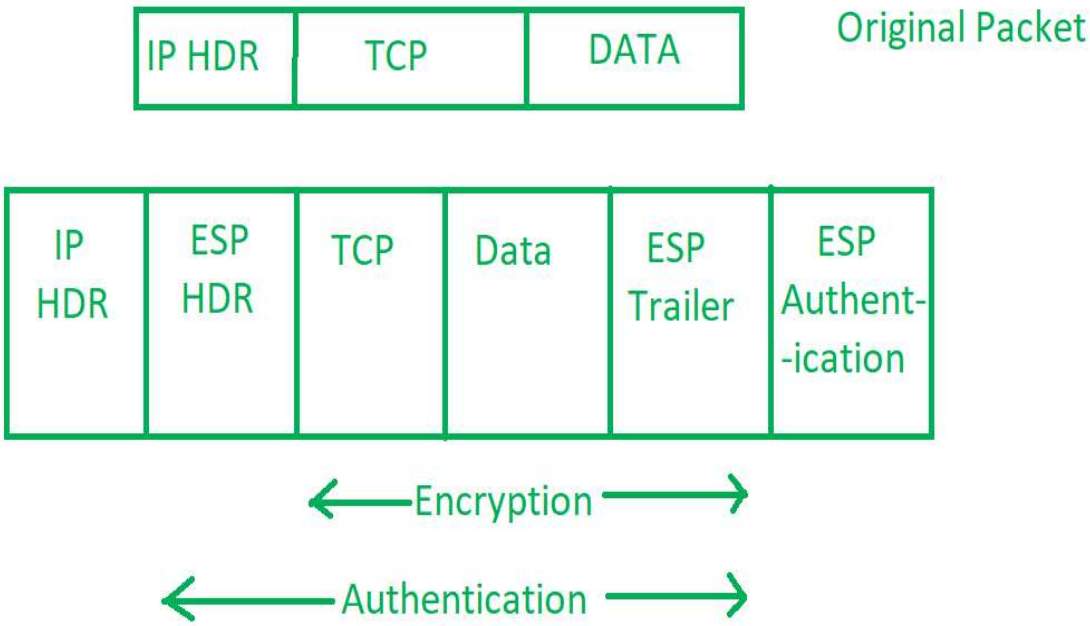
It has the following components:

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.

3. **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.



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 across 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.