Web Security and Email Security

Unit 8 [5 LH]

Topics

- Web security,
- Threats, SSL (Architecture, Handshake protocol, Handshake protocol action),
- overview of TLS and HTTPS,
- Secure Electronic Transaction overview,
- Dual Signature,
- Payment Processing,
- E-Mail, SMTP, PEM, PGP,
- Concept of Secure Email.

Web Security

- Web security is a set of procedures, practices, and technologies for assuring the reliable, predictable operation of web servers, web browsers, other programs that communicate with web servers, and the surrounding Internet infrastructure.
- Unfortunately, the sheer scale and complexity of the Web makes the problem of web security dramatically more complex than the problem of Internet security in general.

Web Security

- Today’s web security problem has three primary facets:
  - *Securing the web server and the data that is on it.*
  - *Securing information that travels between the web server and the user.*
  - *Securing the end user’s computer and other devices that people use to access the Internet.*

Web Security

Securing the web server and the data that is on it

- You need to be sure that the server can continue its operation, that the information on the server cannot be modified without authorization, and that the information is only distributed to those individuals to whom you want it distributed.

Web Security

Securing information that travels between the web server and the user

- You would like to assure that information the user supplies to the web server (usernames, passwords, financial information, the names of web pages visited, etc.) cannot be read, modified, or destroyed by any third parties.
- You want similar protection for the information that flows back from the web servers to the users.
- It is also important to assure that the link between the user and the web server cannot be easily disrupted.

Web Security

Securing the end user's computer and other devices that people use to access the Internet

- Finally, web security requires that the end user's computer be reasonably secured.
- Users need to run their web browsers and other software on a secure computing platform that is free of viruses and other hostile software.
- Users also need protections for their privacy and personal information, to make sure that it is not compromised either on their own computers or by their online services.

What do attackers want?

Nearly all attackers on the World Wide Web have the same goal: they want to make your computers do things that you don't want them to do. For example:

- They want to scan your system for confidential documents, which they will transmit to other systems.
- They want to corrupt the information on your computer, or even reformat your computer's hard disk drive.
- They want to use your system to store pirated software, MP3 music files, or images for later access by them and their friends.
- They want to modify your computer's operating system, leaving traps, creating new security holes, or simply causing your system to crash.
- They want to use home-banking applications or credit card numbers residing on your computer to transfer money from your bank account to theirs.
- They want to be able to selectively block access to your system as they wish, or use it in a coordinated attack to deny access to someone else.
- They want to install some form of server, such as an IRC (Internet Relay Chat) server they can access without slowing down their own machines..

Securing the server

- Securing the web server is a three-part process.
  - First, the computer itself must be secured using traditional computer security techniques.
  - Second, special programs that provide web service must be secured.
  - Finally, you need to examine the operating system and the web service to see if there are any unexpected interactions between the two that might compromise the system’s overall security.

Securing the information in transit

- There are many ways to protect information from eavesdropping as it travels through a network:
  - Physically secure the network, so that eavesdropping is impossible.
  - Hide the information that you wish to secure within information that appears innocuous (not harmful).
  - Encrypt the information so that it cannot be decoded by any party who is not in possession of the proper key.
- Of these techniques, encryption is the only technique that is practical on a large-scale public network.

Securing the User's Computer

- Protect from virus and worms
  - ILOVEYOU virus..

Web Security

- Web application security aims to address and fulfill the four conditions of security: confidentiality, integrity, availability and non-repudiation
- ***Confidentiality***: States that the sensitive data stored in the Web application should not be exposed under any circumstances.
- ***Integrity***: States that the data contained in the Web application is consistent and is not modified by an unauthorized user.
- ***Availability***: States that the Web application should be accessible to the genuine user within a specified period of time depending on the request.
- ***Non-repudiation***: States that the genuine user cannot deny modifying the data contained in the Web application and that the Web application can prove its identity to the genuine user.

Web Threats

- A web threat is any threat that uses the World Wide Web to facilitate Cybercrime.
- Web threats use multiple types of malware and fraud, all of which utilize HTTP or HTTPS protocols, but may also employ other protocols and components, such as links in email or Instant messages, or malware attachments or on servers that access the Web.
- They benefit cybercriminals by stealing information for subsequent sale and help absorb infected PCs into botnets.
- Web threats pose a broad range of risks, including financial damages, identity theft, loss of confidential information/data, theft of network resources, damaged brand/personal reputation, and erosion of consumer confidence in e-commerce and online banking.
- It is a type of threat related to information technology (IT). The IT risk, i.e. risk affecting has gained and increasing impact on society due to the spread of IT processes

Web Threats

- Web threats can be divided into two primary categories, based on delivery method – *push* and *pull*.
- ***Push attacks*** use phishing, DNS poisoning (or pharming), and other means to appear to originate from a trusted source and then collects information and/or injects malware.
- ***Pull-based web threats*** are often referred to as “drive-by” threats since they they can affect any website visitor. Cybercriminals infect legitimate websites, which unknowingly transmit malware to visitors or alter search results to take users to malicious websites. Upon loading the page, the user's browser passively runs a malware downloader in a hidden HTML frame (IFRAME) without any user interaction

	Threats	Consequences	Countermeasures
Integrity	• Modification of user data • Trojan horse browser • Modification of memory • Modification of message traffic in transit	• Loss of information • Compromise of machine • Vulnerabilty to all other threats	Cryptographic checksums
Confidentiality	• Eavesdropping on the net • Theft of info from server • Theft of data from client • Info about network configuration • Info about which client talks to server	• Loss of information • Loss of privacy	Encryption, Web proxies
Denial of Service	• Killing of user threads • Flooding machine with bogus requests • Filling up disk or memory • Isolating machine by DNS attacks	• Disruptive • Annoying • Prevent user from getting work done	Difficult to prevent
Authentication	• Impersonation of legitimate users • Data forgery	• Misrepresentation of user • Belief that false information is valid	Cryptographic techniques

Figure: A comparison of Threats on the Web.

Web Security Threat

- The types of security threats faced when using the Web can be grouped into two ways.
  - One way to group these threats is in terms of passive and active attacks. Passive attacks include eavesdropping on network traffic between browser and server and gaining access to information on a Web site that is supposed to be restricted. Active attacks include impersonating another user, altering messages in transit between client and server, and altering information on a Web site.
  - Another way to classify Web security threats is in terms of the location of the threat: Web server, Web browser, and network traffic between browser and server.

Web Traffic Security Approaches

- IP security (IPSec)
- Secure Socket Layer(SSL) or Transport Layer Security (TSL)
- Application Specific Security

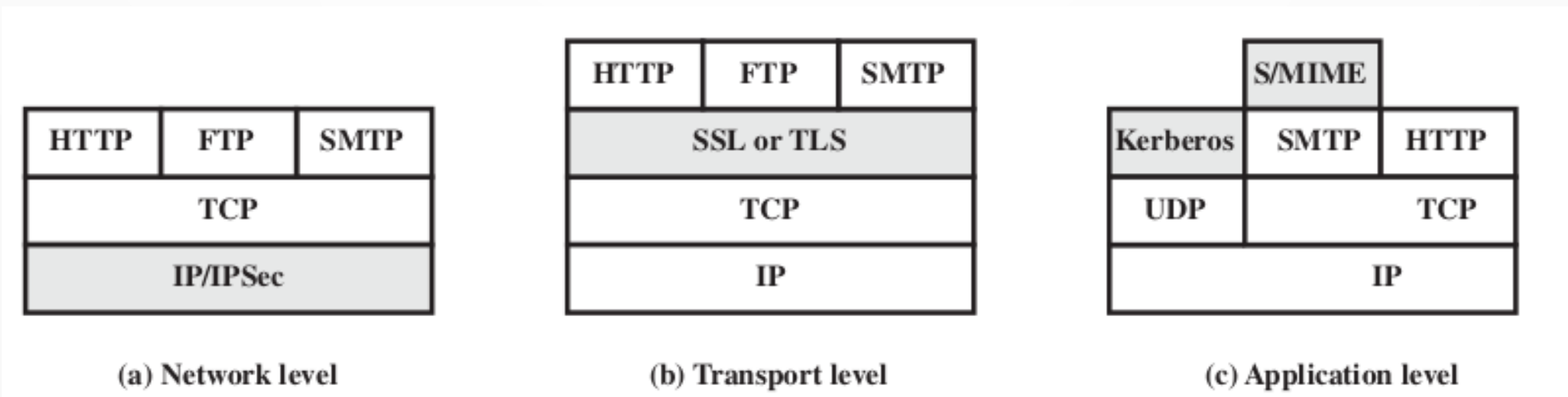


Figure: Relative location of facilities in the TCP/IP Protocol stack.

Secure Socket Layer (SSL)

- Secure Sockets Layer (SSL) is a standard protocol used for the secure transmission of documents over a network.
- Developed by Netscape, SSL technology creates a secure link between a Web Server and browser to ensure private and integral data transmission.
- SSL uses TCP for communication.
- In SSL, the word socket refers to the mechanism of transferring data between a client and server over a network.
- When using SSL for secure Internet transactions, a Web server needs an SSL certificate to establish a secure SSL connection.
- SSL encrypts network connection segments above the transport layer, which is a network connection component above the program layer.

SSL

- SSL follows an asymmetric cryptographic mechanism, in which a Web browser creates a public key and a private (secret) key.
- The public key is placed in a data file known as a certificate signing request (CSR). The private key is issued to the recipient only.
- The objective of SSL are:
  - ***Data Integrity***: Data is protected from tampering.
  - ***Data Privacy***: Data privacy is ensured through a series of protocols, including the SSL Record Protocol, SSL Handshake Protocol, SSL Change CipherSpec Protocol and SSL Alert Protocol.
  - ***Client-server authentication***: The SSL protocol uses standard cyrptographic technique to authenticate the client and server.
- SSL is the predecessor of Transport Layer Security (TLS), which is a cryptographic protocol for secure Internet data transmission.

SSL Architecture

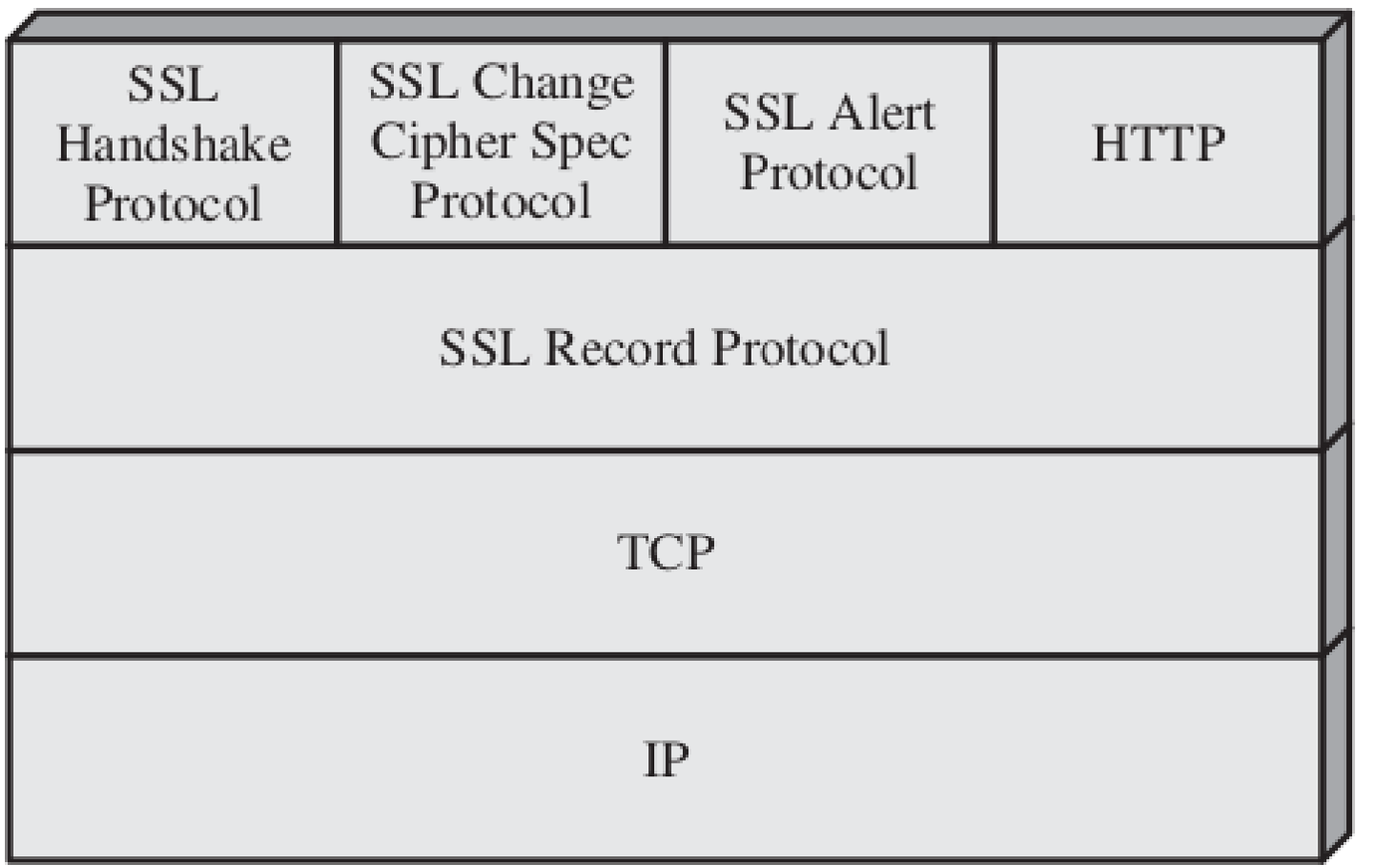


Figure: SSL protocol stack.

SSL Architecture

- SSL is designed to make use of TCP to provide a reliable end-to-end secure service.
- SSL is not a single protocol but rather two layers of protocols.
- The SSL Record Protocol provides basic security services to various higher layer protocols.
- In particular, the Hypertext Transfer Protocol (HTTP), which provides the transfer service for Web client/server interaction, can operate on top of SSL.
- Three higher-layer protocols are defined as part of SSL: the Handshake Protocol, The Change Cipher Spec Protocol, and the Alert Protocol.
- These SSL specific protocols are used in the management of SSL exchanges.
- Two important SSL concepts are the *SSL session* and the *SSL connection*.

SSL Architecture

- **SSL Connection**
  - A connection is a transport that provides a suitable type of service.
  - For SSL, such connections are peer-to-peer relationships.
  - Every connection is associated with one session.
- **SSL Session**
  - An SSL session is an association between a client and a server. Sessions are created by the Handshake Protocol.
  - Sessions define a set of cryptographic security parameters which can be shared among multiple connections.

SSL Architecture

SSL Record Protocol

- The SSL Record Protocol provides two services for SSL connections:
  - ***Confidentiality***: The Handshake Protocol defines a shared secret key that is used for conventional encryption of SSL payloads.
  - ***Message Integrity***: The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC).

SSL Architecture

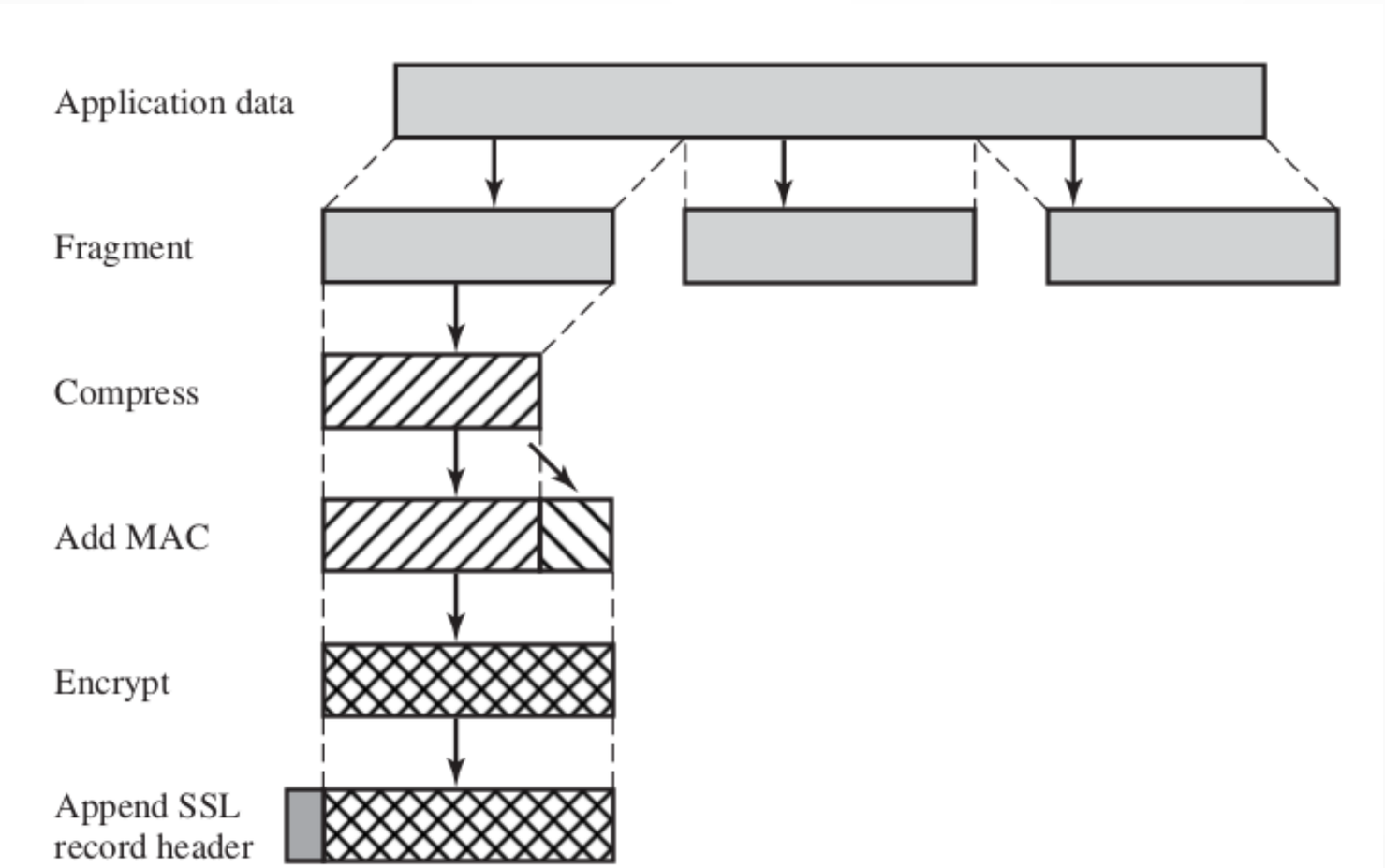


Figure: SSL Record Protocol Operation

SSL Architecture

Change Cipher Spec Protocol

- The Change Cipher Spec Protocol is one of the three SSL-specific protocols that usethe SSL Record Protocol, and it is the simplest.
- This protocol consists of a single message, which consists of a single byte with the value 1.
- The sole purpose of this message is to cause the pending state to be copied into the current state, which updates the cipher suite to be used on this connection.

SSL Architecture

SSL Alert Protocol

- The Alert Protocol is used to convey SSL-related alerts to the peer entity.
- As with other applications that use SSL, alert messages are compressed and encrypted, as specified by the current state.
- Each message in this protocol consists of two bytes. The first byte takes the value warning (1) or fatal (2) to convey the severity of the message.
  - If the level is fatal, SSL immediately terminates the connection. Other connections on the same session may continue, but no new connections on this session may be established.
  - The second byte contains a code that indicates the specific alert.

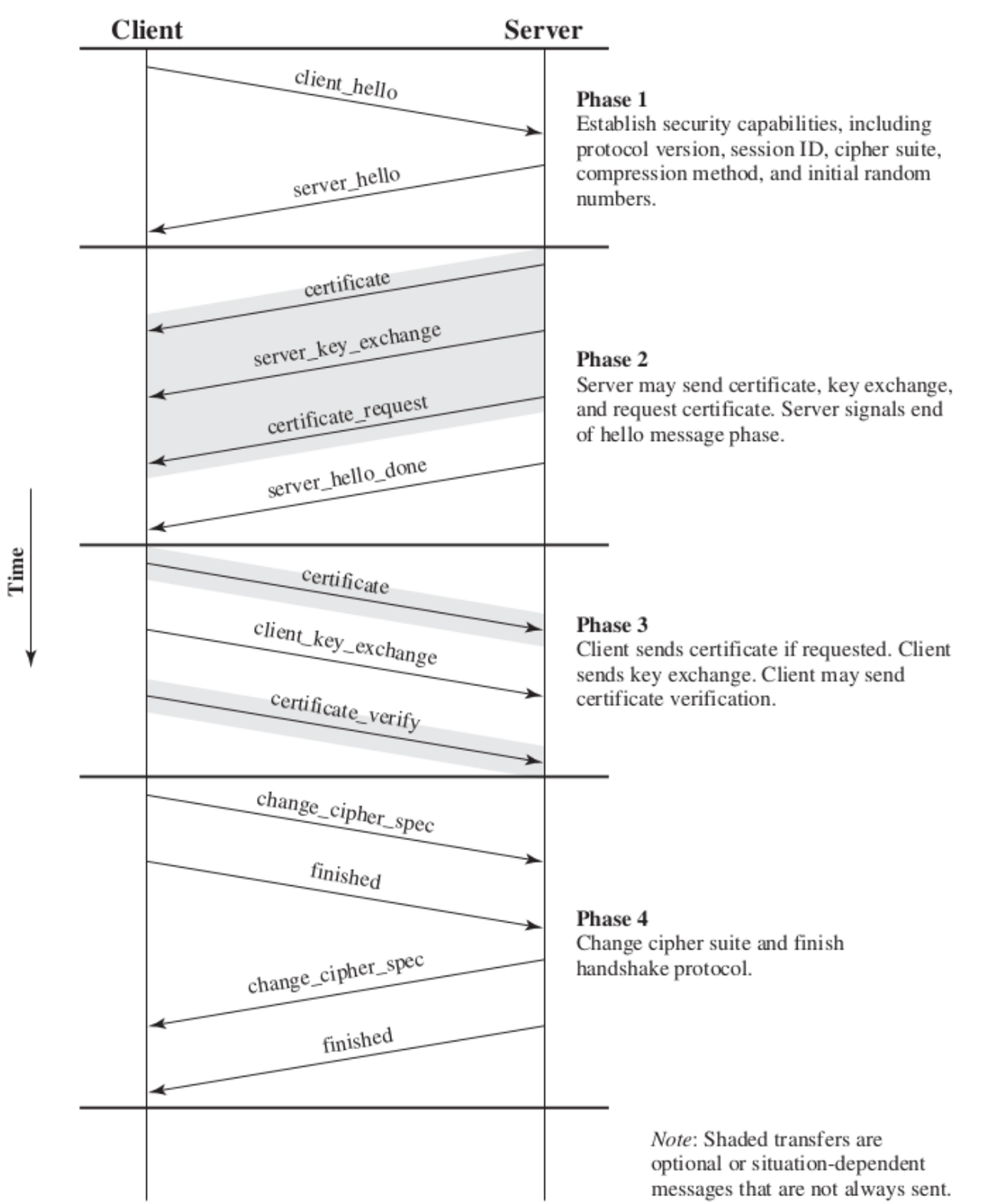


Figure: Handshake Protocol Action

Transport Layer Security

- TLS (Transport Layer Security) is just an updated, more secure, version of SSL.
- Transport layer security (TLS) is a protocol that provides communication security between client/server applications that communicate with each other over the Internet.
- It enables privacy, integrity and protection for the data that's transmitted between different nodes on the Internet.
- TLS primarily enables secure Web browsing, applications access, data transfer and most Internet-based communication.
- It prevents the transmitted/transported data from being eavesdropped or tampered.
- TLS is used to secure Web browsers, Web servers, VPNs, database servers and more.

Transport Layer Security

- TLS protocol consists of two different layers of sub-protocols:
  - **TLS Handshake Protocol**: Enables the client and server to authenticate each other and select a encryption algorithm prior to sending the data.
  - **TLS Record Protocol**: It works on top of the standard TCP protocol to ensure that the created connection is secure and reliable. It also provides data encapsulation and data encryption services

HTTP

- Hyper Text Transfer Protocol (HTTP) is an application layer protocol used primarily on the World Wide Web.
- HTTP uses a client-server model where the web browser is the client and communicates with the webserver that hosts the website.
- The browser uses HTTP, which is carried over TCP/IP to communicate to the server and retrieve Web content for the user.
- A basic HTTP request involves the following steps:
  - A connection to the HTTP server is opened.
  - A request is sent to the server.
  - Some processing is done by the server.
  - A response from the server is sent back.
  - The connection is closed.

Limitation of HTTP

- Integrity is not there, so someone can easily alter with the content.
- HTTP is insecure as there's no encryption methods for it. So, it's subjected towards man in the middle and eavesdropping of sensitive information.
- There's no authentication, so you will not have any clear idea with whom you are initiating a communication.
- Authentication is sent in the clear, anyone who intercepts the request and can know the username and passwords being used.

HTTPS

- HTTPS (HTTP over SSL) refers to the combination of HTTP and SSL to implement secure communication between a Web browser and a Web server.
- The HTTPS capability is built into all modern Web browsers.
- Its use depends on the Web server supporting HTTPS communication.
- The principal difference seen by a user of a Web browser is that URL (uniform resource locator) addresses begin with https:// rather than http://.
- A normal HTTP connection uses port 80. If HTTPS is specified, port 443 is used, which invokes SSL.

HTTPS

- When HTTPS is used, the following elements of the communication are encrypted:
  - URL of the requested document
  - Contents of the document
  - Contents of browser forms (filled in by browser user)
  - Cookies sent from browser to server and from server to browser
  - Contents of HTTP header

HTTPS: Connection Initiation

- For HTTPS, the agent acting as the HTTP client also acts as the TLS client.
- The client initiates a connection to the server on the appropriate port and then sends the TLS ClientHello to begin the TLS handshake.
- When the TLS handshake has finished, the client may then initiate the first HTTP request.
- All HTTP data is to be sent as TLS application data.

HTTPS: Connection Closure

- An HTTP client or server can indicate the closing of a connection by including the following line in an HTTP record: `Connection: close`.
- This indicates that the connection will be closed after this record is delivered.

Secure Electronic Transaction

- Secure electronic transaction (SET) was an early communications protocol used by e-commerce websites to secure electronic debit and credit card payments, launched in 1996.
- Secure electronic transaction was used to facilitate the secure transmission of consumer card information via electronic portals on the internet.
- Secure electronic transaction protocols were responsible for blocking out the personal details of card information, thus preventing merchants, hackers, and electronic thieves from accessing consumer information.

Secure Electronic Transaction

- Other standards for digital security for online debit and credit card transactions emerged after the protocols defined by secure electronic transactions were introduced in the mid-1990s.
- Visa was an early adopter of a new standard of security protocols, called 3-D Secure,1 which was eventually adopted in different forms by Mastercard, Discover, and American Express for securing customer’s digital payment.

- 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 includes Certification Authorities for making use of standard Digital Certificates like X.509 Certificate.

SET Working

- https://www.educba.com/secure-electronic-transaction/

Dual Signature

- Dual signature is the use of encryption with two electronic signatures as a security measure for delivering an electronic message in a Secure Electronic Transaction (SET).
- The purpose of the dual signature is *to link two messages that are intended for two different recipients*.
- In this case, the customer wants to send the ***order information (OI)*** to the merchant and the ***payment information (PI)*** to the bank.

Dual Signature

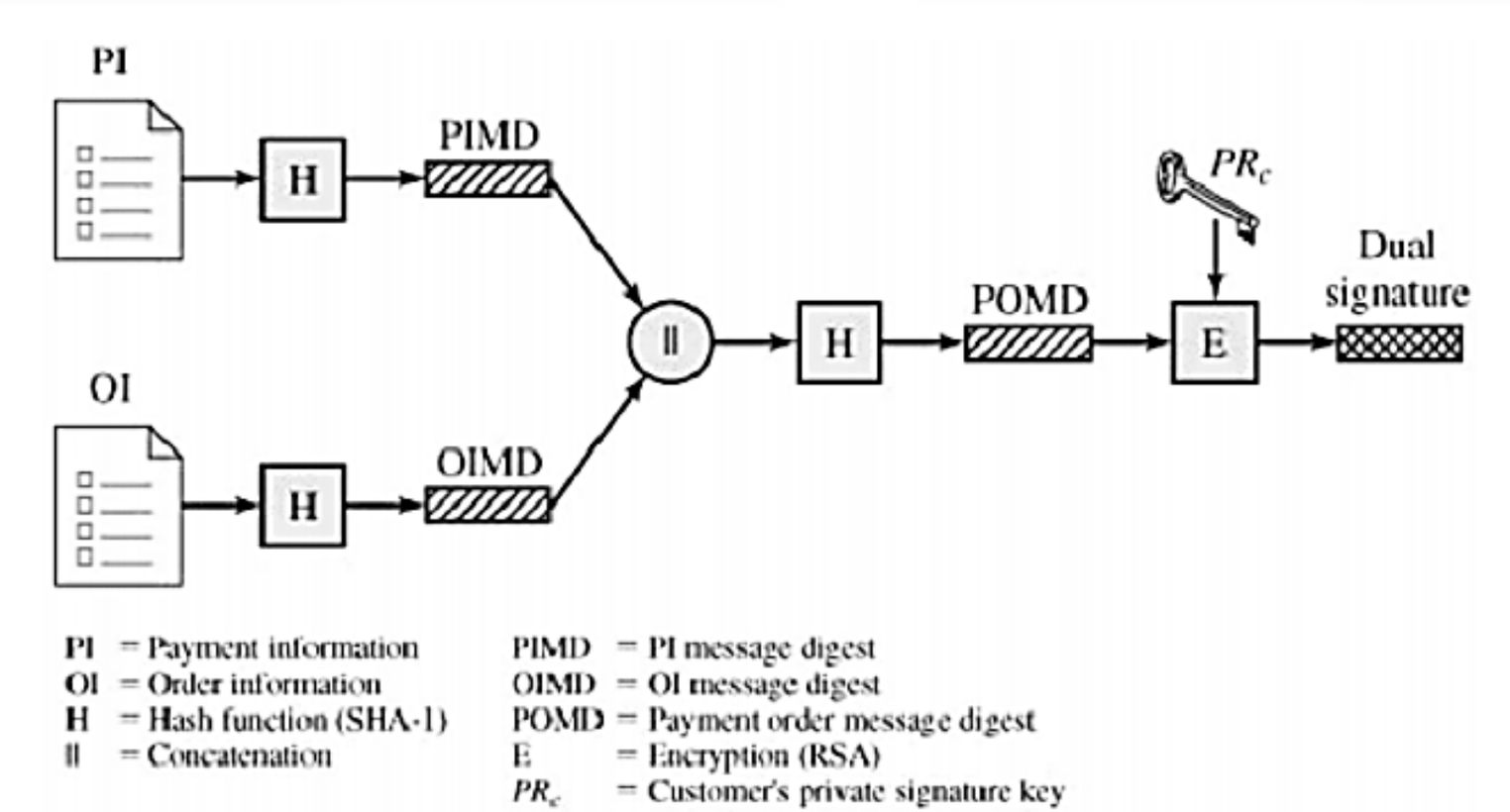


Figure: Construction of Dual Signature

Dual Signature

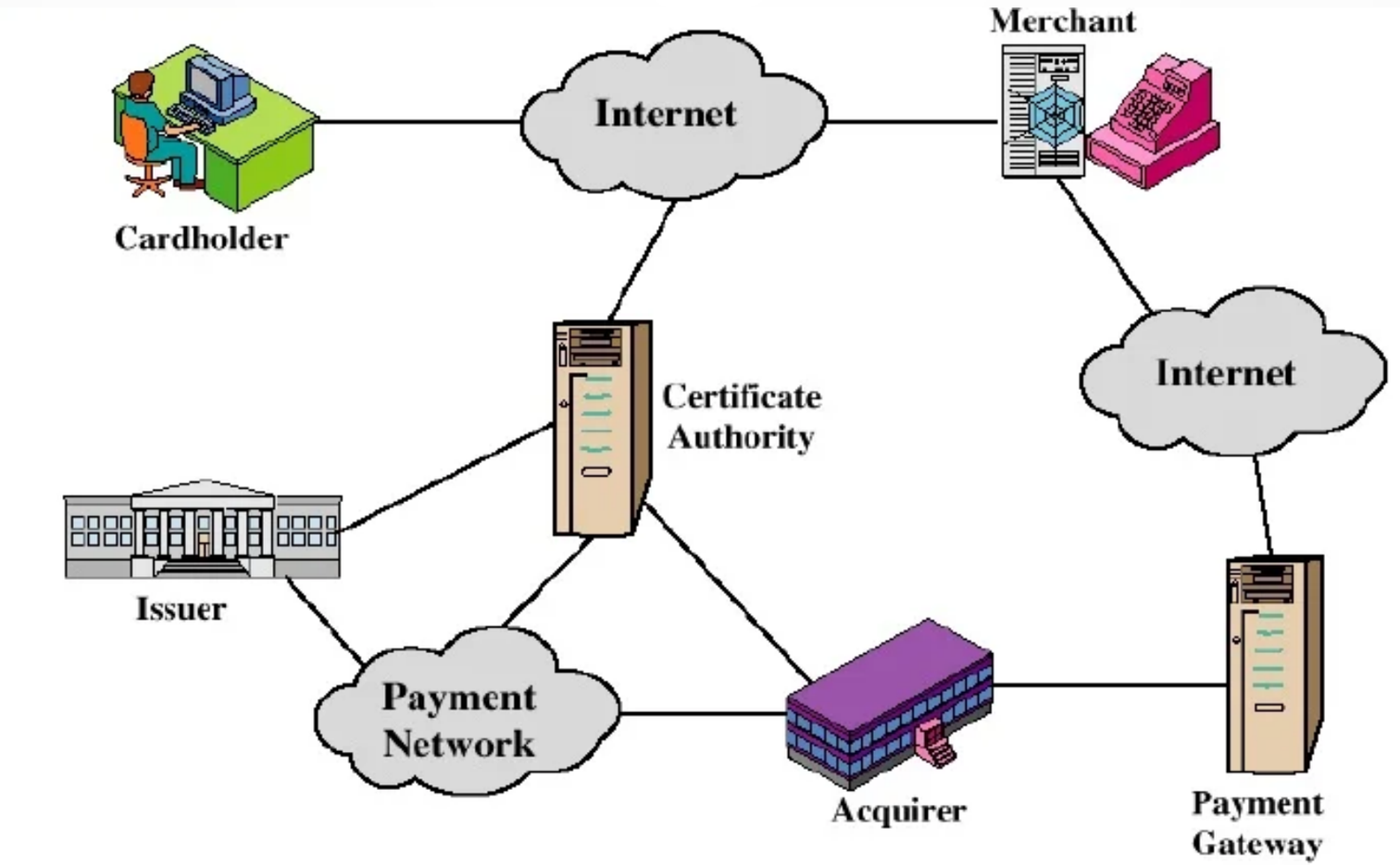
- The merchant does not need to know the customer's credit card number, and the bank does not need to know the details of the customer's order.
- The customer is afforded extra protection in terms of privacy by keeping these two items separate.
- The customer takes the hash (using SHA-1) of the PI and the hash of the OI.
- These two hashes are then concatenated and the hash of the result is taken.
- Finally, the customer encrypts the final hash with his or her private signature key, creating the dual signature

Payment Processing

- Payment processing is a series of steps required to authenticate and approve a transaction, followed by an additional set of steps that transfer funds from the transaction to the merchant and the various parties responsible for processing the transaction
- It is usually a third-party service that is actually a system of computer processes that process, verify, and accept or decline credit card transactions on behalf of the merchant through secure Internet connections.
- Payment processing is a service that allows websites to sell online by accepting payment via electronic methods such as credit cards, debit cards and bank transfers.
- Provided by payment service providers, payment processing is the technical connection or ‘gateway’ between a website and the financial institutions or ‘acquirers’ that govern different payment methods.

- https://www.merchantmaverick.com/what-is-payment-processing/

Participants in SET



Participants in SET System

- In the general scenario of online transactions, SET includes similar participants:
  1. **Cardholder** – customer
  2. **Issuer** – customer financial institution (e.g. bank) that issues the payment card
  3. **Merchant –** the seller
  4. **Acquirer** – A financial organization that processes payment authorization and facilitates electronic funds transfer to the merchant's account.
  5. **Certificate authority** – Authority that follows certain standards and issues certificates(like X.509V3) to all other participants.
  6. **Dual signature**: A guaranteed SET data integrity innovation that links two different recipient messages

Requirement 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.

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,

Email and Concept of Secure Email

- Electronic mail (email) is a digital mechanism for exchanging messages through Internet or intranet communication platforms.
- Email messages are relayed through email servers, which are provided by all Internet service providers (ISP).
- Emails are transmitted between two dedicated server folders: sender and recipient.
- A sender saves, sends or forwards email messages, whereas a recipient reads or downloads emails by accessing an email server.

Email and Concept of Secure Email

- ***Email security*** describes various techniques for keeping sensitive information in email communication and accounts secure against unauthorized access, loss, or compromise.
- Email is a popular medium for the spread of malware, spam, and phishing attacks, using deceptive messages to entice recipients to divulge sensitive information, open attachments or click on hyperlinks that install malware on the victim’s device.
- Email is also a common entry vector for attackers looking to gain a foothold in an enterprise network and breach valuable company data.

- Email security is necessary for both individual and business email accounts, and there are multiple measures organizations should take to enhance email security.

Email and Concept of Secure Email

- From an individual/end user standpoint, proactive email security measures include:
  - Strong passwords
  - Password rotations
  - Spam filters
  - Desktop-based anti-virus/anti-spam applications
- Similarly, a service provider ensures email security by using strong password and access control mechanisms on an email server; encrypting and digitally signing email messages when in the inbox or in transit to or from a subscriber email address.
- It also implements firewall and software-based spam filtering applications to restrict unsolicited, untrustworthy and malicious email messages from delivery to a user's inbox.
-

Simple Mail Transfer Agent (SMTP)

- Simple Mail Transfer Protocol (SMTP) is the standard protocol for email services on a TCP/IP network.
- SMTP provides the ability to send and receive email messages.
- It is an application-layer protocol that enables the transmission and delivery of email over the Internet.
- SMTP clients and servers have two main components.
  - *User agent*: prepares the messages, encloses it in an envelope
  - *Mail Transfer Agent*: transfers the mail across the internet.

Limitation of SMTP

- Transmission of executable files and binary files using SMTP is not possible without converting into text files. Use MIME to send mail in other format.
- It cannot transmit text data that contains national language characters.
- It is limited to 7-bit ASCII characters only.
- SMTP servers may reject mails beyond some specific length

Privacy-Enchanced Mail (PEM)

- Privacy-Enhanced Mail (PEM) is an Internet standard that provides for secure exchange of electronic mail.
- PEM employs a range of cryptographic techniques to allow for confidentiality, sender authentication, and message integrity.
- PEM provides mainly two services:
  - Confidentiality
  - Integrity

Service provided by PEM

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.

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.

Pretty Good Service

- PGP is an open-source, freely available software package for e-mail security.
- It provides authentication through the use of digital signature, confidentiality through the use of symmetric block encryption, compression using the ZIP algorithm, and e-mail compatibility using the radix-64 encoding scheme.
- PGP incorporates tools for developing a public-key trust model and public-key certificate management.
- S/MIME is an Internet standard approach to e-mail security that incorporates the same functionality as PGP.
- DKIM is a specification used by e-mail providers for cryptographically signing e-mail messages on behalf of the source domain.

Pretty Good Service (PGP)

- Pretty Good Privacy (PGP) is a methodology used for encrypting and decrypting digital files and communications over the Internet.
- PGP was initially designed for email security.
- PGP works on the public key cryptography mechanism, where users encrypt and decrypt data using their respective public and private keys.
- PGP uses a symmetric encryption key to encrypt messages, and a public key is used with each sent and received message.
- First, the receiver must use its private key to decrypt the key and then decrypt the message through the decrypted symmetric key.
- PGP also provides data/file integrity services by digitally signing messages, allowing receivers to learn whether or not message confidentiality is compromised.
- PGP is also used to encrypt files stored on a computer and/or complete hard disk drives.

Pretty Good Privacy (PGP)

- PGP can be used basically for 4 things:

1. Encrypting a message or file so that only the recipient can decrypt and read it.
2. Clear signing a plain text message guarantees that it can only have come from the sender and not an impostor.
3. Encrypting computer files so that they can't be decrypted by anyone other than the person who encrypted them.
4. Really deleting files (i.e. overwriting the content so that it can't be recovered and read by anyone else) rather than just removing the file name from a directory/folder.

Pretty Good Service

Function	Algorithms Used	Description
Digital signature	DSS/SHA or RSA/SHA	A hash code of a message is created using SHA-1. This message digest is encrypted using DSS or RSA with the sender's private key and included with the message.
Message encryption	CAST or IDEA or Three-key Triple DES with Diffie-Hellman or RSA	A message is encrypted using CAST-128 or IDEA or 3DES with a one-time session key generated by the sender. The session key is encrypted using Diffie-Hellman or RSA with the recipient's public key and included with the message.
Compression	ZIP	A message may be compressed for storage or transmission using ZIP.
E-mail compatibility	Radix-64 conversion	To provide transparency for e-mail applications, an encrypted message may be converted to an ASCII string using radix-64 conversion.

Figure: Summary of PGP Services