Unit- 5 Security Features in Operating System

OS Security. What does Operating System Security. Definition — What does Operating System Security (OS Security) mean? Operating system security (OS security) is the process of ensuring OS integrity, confidentiality and availability.

The operating system must identify each user who requests access and must ascertain that the user is actually who he or she purports to be. The most common authentication mechanism is password comparison. Memory protection. Each user's program must run in a portion of memory protected against unauthorized accesses.

Windows 7 Security Features 1 Date Execution Prevention (DEP) 2 Address Space Layout Randomization (ASLR) 3 Structured Exception Handler Overwrite Protection (SEHOP) 4 User Account Control (UAC) 5 DNS System Security Enhancements (DNSSEC) 6 Bitlocker 7 Improved Cryptography 8 Windows Firewall/Defender 9 Improved Authentication Mechanisms.

STANDARD BASIC SECURITY FEATURES. For the basic security features, Linux has password authentication, file system discretionary access control, and security auditing. These three fundamental features are necessary to achieve a security evaluation at the C2 level.

Objects to be Protected in Operating System:

Protection and security requires that computer resources such as **CPU, softwares, memory** etc. are protected. This extends to the operating system as well as the data in the system. This can be done by ensuring integrity, confidentiality and availability in the operating system.

Protection refers to a mechanism which controls the access of programs, processes, or users to the resources defined by a computer system. We can take protection as a helper to multi programming operating system, so that many users might safely share a common logical name space such as directory or files.

System Protection in Operating System. Protection refers to a mechanism which controls the access of programs, processes, or users to the resources defined by a computer system. We can take protection as a helper to multi programming operating system, so that many users might safely share a common logical name space.

Computer Science MCA Operating System Protection and security requires that computer resources such as CPU, softwares, memory etc. are protected. This extends to the operating system as well as the data in the system. This can be done by ensuring integrity, confidentiality and availability in the operating system.

The system must be protect against unauthorized access, viruses, worms etc. A threat is a program that is malicious in nature and leads to harmful effects for the system.

Protection Methods of Operating Systems:

Protection refers to a mechanism which controls the access of programs, processes, or users to the resources defined by a computer system. We can take protection as a helper to multi programming operating system, so that many users might safely share a common logical name space such as directory or files.

Need of Protection:

- To prevent the access of unauthorized users and
- To ensure that each active programs or processes in the system uses resources only as the stated policy,
- To improve reliability by detecting latent errors.

- **Role of Protection:**

  The role of protection is to provide a mechanism that implement policies which defines the uses of resources in the computer system.Some policies are defined at the time of design of the system, some are designed by management of the system and some are defined by the users of the system to protect their own files and programs.

- Every application has different policies for use of the resources and they may change over time so protection of the system is not only concern of the designer of the operating system. Application programmer should also design the protection mechanism to protect their system against misuse.

Now we are going to learn about hardware protection and it's the type. so first let's see the type of hardware which is used in a computer system. we know that a computer system contains the hardware like processor, monitor, RAM and many more, and one thing that the operating system ensures that these devices can not directly accessible by the user.

Basically, hardware protection is divided into 3 categories: CPU protection, Memory Protection, and I/O protection. These are explained as following below.

1. CPU Protection:

CPU protection is referred to as we can not give CPU to a process forever, it should be for some limited time otherwise other processes will not get the chance to execute the process. So for that, a timer is used to get over from this situation. which is basically give a certain amount of time a process and after the timer execution a signal will be sent to the process to leave the CPU. hence process will not hold CPU for more time.

2. Memory Protection:

In memory protection, we are talking about that situation when two or more processes are in memory and one process may access the other process memory. and to prevent this situation we are using two registers as:

1. Bare register

2. Limit register

So basically Bare register store the starting address of program and limit register store the size of the process, so when a process wants to access the memory then it is checked that it can access or can not access the memory.

3. I/O Protection:

So when we're ensuring the I/O protection then some cases will never have occurred in the system as:

1. Termination I/O of other process
2. View I/O of other process
3. Giving priority to a particular process I/O

File Protection:

In computer systems, alot of user’s information is stored, the objective of the operating system is to keep safe the data of the user from the improper access to the system. Protection can be provided in number of ways. For a single laptop system, we might provide protection by locking the computer in a desk drawer or file cabinet. For multi-user systems, different mechanisms are used for the protection.

Types of Access :

The files which have direct access of the any user have the need of protection. The files which are not accessible to other users doesn’t require any kind of protection. The mechanism of the protection provide the facility of the controlled access by just limiting the types of access to the file. Access can be given or not given to any user depends on several factors, one of which is the type of access required. Several different types of operations can be controlled:

- **Read –**

  Reading from a file.
- **Write –**

  Writing or rewriting the file.
- **Execute –**

  Loading the file and after loading the execution process starts.
- **Append –**

  Writing the new information to the already existing file, editing must be end at the end of the existing file.

- **Delete –**

  Deleting the file which is of no use and using its space for the another data.
- **List –**

  List the name and attributes of the file.

Operations like renaming, editing the existing file, copying; these can also be controlled. There are many protection mechanism. each of them mechanism have different advantages and disadvantages and must be appropriate for the intended application.

Access Control :

There are different methods used by different users to access any file. The general way of protection is to associate *identity-dependent access* with all the files and directories an list called access-control list (ACL) which specify the names of the users and the types of access associate with each of the user. The main problem with the access list is their length. If we want to allow everyone to read a file, we must list all the users with the read access. This technique has two undesirable consequences:

Constructing such a list may be tedious and unrewarding task, especially if we do not know in advance the list of the users in the system.

Previously, the entry of the any directory is of the fixed size but now it changes to the variable size which results in the complicates space management. These problems can be resolved by use of a condensed version of the access list. To condense the length of the access-control list, many systems recognize three classification of users in connection with each file:

- **Owner –**

  Owner is the user who has created the file.
- **Group –**

  A group is a set of members who has similar needs and they are sharing the same file.
- **Universe –**

  In the system, all other users are under the category called universe.

The most common recent approach is to combine access-control lists with the normal general owner, group, and universe access control scheme. For example: Solaris uses the three categories of access by default but allows access-control lists to be added to specific files and directories when more fine-grained access control is desired.

Other Protection Approaches:

The access to any system is also controlled by the password. If the use of password are is random and it is changed often, this may be result in limit the effective access to a file.

The use of passwords has a few disadvantages:

- The number of passwords are very large so it is difficult to remember the large passwords.
- If one password is used for all the files, then once it is discovered, all files are accessible; protection is on all-or-none basis.

User Authentication:

Authentication is the process of verifying the identity of user or information. User authentication is the process of verifying the identity of user when that user logs into a computer system.

The main objective of authentication is to allow authorized users to access the computer and to deny access to the unauthorized users. Operating Systems generally identifies/authenticates users using following 3 ways : Passwords, Physical identification, and Biometrics. These are explained as following below.

1. **Passwords :**
   Passwords verification is the most popular and commonly used authentication technique. A password is a secret text that is supposed to be known only to a user. In password based system, each user is assigned a valid username and password by the system administrator. System stores all username and Passwords. When a user logs in, its user name and password is verified by comparing it with stored login name and password. If the contents are same then the user is allowed to access the system otherwise it is rejected.

2. **Physical Identification :**
   This technique include machine readable badges(symbols), card or smart cards. In some companies, badges are required for employees to gain access to the organization's gate. In many system, identification is combined with the use of password i.e the user must insert the card and then supply his /her password. This kind of authentication is commonly

used with ATM. Smart card can enhance this scheme by keeping the user password within the card itself. This allow the authentication without storage of password in the computer system. The loss of such card can be dangerous.

3. **Biometrics :**

   This method of authentication is based on the unique biological characteristics of each user such as finger prints, voice or face recognition, signatures and eyes.

Biometric devices often consist of –

- A scanner or other devices to gather the necessary data about user.
- Software to convert the data into a form that can be compared and stored.
- A database that stores information for all authorized users.

A number of different types of physical characteristics are –

- **Facial Characteristics –**

  Humans are differentiated on the basis of facial characteristics such as eyes, nose, lips, eyebrows and chin shape.
- **Fingerprints –**

  Fingerprints are believed to he unique across the entire human population.
- **Hand Geometry –**

  Hand geometry systems identify features of hand that includes shape, length and width of fingers.

- **Retinal pattern –**

  It is concerned with the detailed structure of the eye.
- **Signature –**

  Every individual has a unique style of handwriting, and this feature is reflected in the signatures of a person.
- **Voice –**

  This method records the frequency pattern of the voice of an individual speaker.

One Time passwords:

One-time passwords provide additional security along with normal authentication. In One-Time Password system, a unique password is required every time user tries to login into the system. Once a one-time password is used, then it cannot be used again. One-time password is implemented in various ways. Some commercial applications send one-time passwords to user on registered mobile/ email which is required to be entered prior to login.

Web Security: Web Security Requirements

Security of a computer system is a crucial task. It is a process of ensuring confidentiality and integrity of the OS.

A system is said to be secure if its resources are used and accessed as intended under all the circumstances, but no system can guarantee absolute security from several of the various malicious threats and unauthorized access.

Security of a system can be threatened via two violations:

- **Threat:** A program which has the potential to cause serious damage to the system.
- **Attack:** An attempt to break security and make unauthorized use of an asset.

Security violations affecting the system can be categorized as malicious and accidental. **Malicious threats**, as the name suggests are a kind of harmful computer code or web script designed to create system vulnerabilities leading to back doors and security breaches. **Accidental Threats**, on the other hand, are comparatively easier to be protected against. Example: Denial of Service DDoS attack.

Security can be compromised via any of the breaches mentioned:

- **Breach of confidentiality:** This type of violation involves the unauthorized reading of data.
- **Breach of integrity:** This violation involves unauthorized modification of data.
- **Breach of availability:** It involves unauthorized destruction of data.
- **Theft of service:** It involves unauthorized use of resources.
- **Denial of service:** It involves preventing legitimate use of the system. As mentioned before, such attacks can be accidental in nature.

Security System Goals –

Henceforth, based on the above breaches, the following security goals are aimed:

1. **Integrity:**

   The objects in the system mustn't be accessed by any unauthorized user & any user not having sufficient rights should not be allowed to modify the important system files and resources.

2. **Secrecy:**

   The objects of the system must be accessible only to a limited number of authorized users. Not everyone should be able to view the system files.

3. **Availability:**

   All the resources of the system must be accessible to all the authorized users i.e only one user/process should not have the right to hog all the system resources. If such kind of situation occurs, denial of service could happen. In this kind of situation, a malware might hog the resources for itself & thus preventing the legitimate processes from accessing the system resources.

Threats can be classified into the following two categories:

1. **Program Threats:**

   A program written by a cracker to hijack the security or to change the behaviour of a normal process.

2. **System Threats:**

   These threats involve the abuse of system services. They strive to create a situation in which operating-system resources and user files are misused. They are also used as a medium to launch program threats.

Types of Program Threats –

1. **Virus:**

   An infamous threat, known most widely. It is a self-replicating and a malicious thread which attaches itself to a system file and then rapidly replicates itself, modifying and destroying essential files leading to a system breakdown.

   Further, Types of computer viruses can be described briefly as follows:

   – file/parasitic – appends itself to a file

   – boot/memory – infects the boot sector

   – macro – written in a high-level language like VB and affects MS Office files

   – source code – searches and modifies source codes

   – polymorphic – changes in copying each time

   – encrypted – encrypted virus + decrypting code

   – stealth – avoids detection by modifying parts of the system that can be used to detect it, like the read system
   call

   – tunneling – installs itself in the interrupt service routines and device drivers

   – multipartite – infects multiple parts of the system

2. **Trojan Horse:**

   A code segment that misuses its environment is called a Trojan Horse. They seem to be attractive and harmless cover program but are a really harmful hidden program which can be used as the virus carrier. In one of the versions of Trojan, User is fooled to enter its confidential login details on an application. Those details are stolen by a login emulator and can be further used as a way of information breaches.

Another variance is Spyware, Spyware accompanies a program that the user has chosen to install and downloads ads to display on the user's system, thereby creating pop-up browser windows and when certain sites are visited by the user, it captures essential information and sends it over to the remote server. Such attacks are also known as **Convert Channels**.

3. **Trap Door:**

   The designer of a program or system might leave a hole in the software that only he is capable of using, the Trap Door works on similar principles. Trap Doors are quite difficult to detect as to analyze them, one needs to go through the source code of all the components of the system.

4. **Logic Bomb:**

   A program that initiates a security attack only under a specific situation.

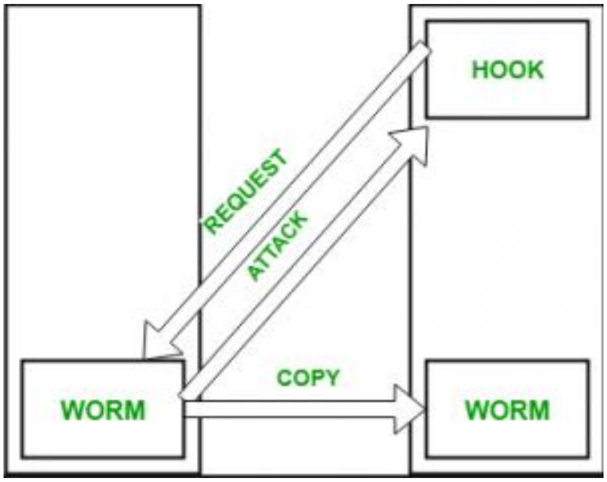
Types of System Threats –

Aside from the program threats, various system threats are also endangering the security of our system:

1. Worm:

An infection program which spreads through networks. Unlike a virus, they target mainly LANs. A computer affected by a worm attacks the target system and writes a small program “hook” on it. This hook is further used to copy the worm to the target computer. This process repeats recursively, and soon enough all the systems of the LAN are affected. It uses the spawn mechanism to duplicate itself. The worm spawns copies of itself, using up a majority of system resources and also locking out all other processes.

The basic functionality of a the worm can be represented as:



2. Port Scanning:

It is a means by which the cracker identifies the vulnerabilities of the system to attack. It is an automated process which involves creating a TCP/IP connection to a specific port. To protect the identity of the attacker, port scanning attacks are launched from **Zombie Systems**, that is systems which were previously independent systems that are also serving their owners while being used for such notorious purposes.

3. Denial of Service:

Such attacks aren’t aimed for the purpose of collecting information or destroying system files. Rather, they are used for disrupting the legitimate use of a system or facility.

These attacks are generally network based. They fall into two categories:

– Attacks in this first category use so many system resources that no useful work can be performed.

For example, downloading a file from a website that proceeds to use all available CPU time.

– Attacks in the second category involves disrupting the network of the facility. These attacks are a result of the abuse of some fundamental TCP/IP principles. the fundamental functionality of TCP/IP.

Security Measures Taken –

To protect the system, Security measures can be taken at the following levels:

- **Physical:**

  The sites containing computer systems must be physically secured against armed and malicious intruders. The workstations must be carefully protected.

- **Human:**

  Only appropriate users must have the authorization to access the system. Phishing(collecting confidential information) and Dumpster Diving(collecting basic information so as to gain unauthorized access) must be avoided.

- **Operating system:**

  The system must protect itself from accidental or purposeful security breaches.

- **Networking System:**

  Almost all of the information is shared between different systems via a network. Intercepting these data could be just as harmful as breaking into a computer. Henceforth, Network should be properly secured against such attacks.

Usually, Anti Malware programs are used to periodically detect and remove such viruses and threats. Additionally, to protect the system from the Network Threats, Firewall is also be used.

Web Security Requirements:

1. Is the Web service being used for EAI or B2Bi?

Web services can be used for two distinct domains—enterprise application integration (EAI) and business-to-business integration (B2Bi). The security requirements for the EAI domain are a subset of those for B2Bi since it is much easier to control, manage, find, execute, and maintain Web services within an intranet than to use them over the Internet across the corporate firewall. While Web services for EAI should have one level of authentication and rarely make use of encryption, Web services for B2Bi may involve multiple levels of authentication and should always use encryption. Furthermore, in the case of B2Bi domain, the messages corresponding to Web service request and response may need to be encrypted, using one or more of the following: cryptography, digital signatures, and secured socket layer (SSL). However, the use of SSL should be avoided, as far as possible, for Web services used within the corporate network for EAI projects. Lastly, nonrepudiation is useful for Web services in the B2Bi domain since it prevents a malicious sender from later disavowing having created and sent a specific message.

2. What's the purpose of the Web service?

If the Web service exposes just public information-oriented business process or data, such as today's weather in a city or a stock quote for a company, the security requirements are looser than those for a Web service that exposes private business information.

3. Who are the subscribers of the Web service?
Knowing who a Web service's subscribers are is important for determining the authorization and authentication features of the Web service.

4. Can the service be invoked over the Internet?
Is the Web service restricted to trusted trading partners, or can any company invoke the Web service over the Internet? This is critical to the authorization and authentication features of the Web service, apart from data protection and nonrepudiation features.

5. How secure is the underlying application?
What level of access does the Web service provide to the underlying application? Should the access be based on authorization and entitlements? The greater the access to underlying applications, the greater the authorization and authentication security requirements.

6. Is the Web service transaction-oriented?
The security threats will be higher if the transaction is distributed across multiple entities.

7. What protocol is utilized?

What network protocol handles the authentication and data transmission between the service requestor and provider? It’s important to know if there’s a need for data security since anyone can sniff the Web service request and response, which would be carried over the network as plain XML documents. If it is HTTPS, then there is no need for any additional encryption/decryption algorithms since HTTPS provides it.

8. Is there a need to verify sender/recipients?

Is there a need to guarantee that the sender of the Web service request and response message is the same as the creator of the message? This information might be needed for auditing purposes and ensuring that the sender and creator are the same entity. Nonrepudiation security requirements will typically be needed if the Web service is being used for B2Bi.

9. Who is involved in the service?

How many distinct entities are involved in the usage of the Web service; i.e., does the Web service have an entity-chaining feature? If there is more than one entity, it will require higher security features.

10. Is component chaining used?

Is there an application- and component-chaining feature in the implementation code of the Web service? If the application chaining spans the corporate firewall, the security requirements become stingier.

Secure Socket Layer (SSL):

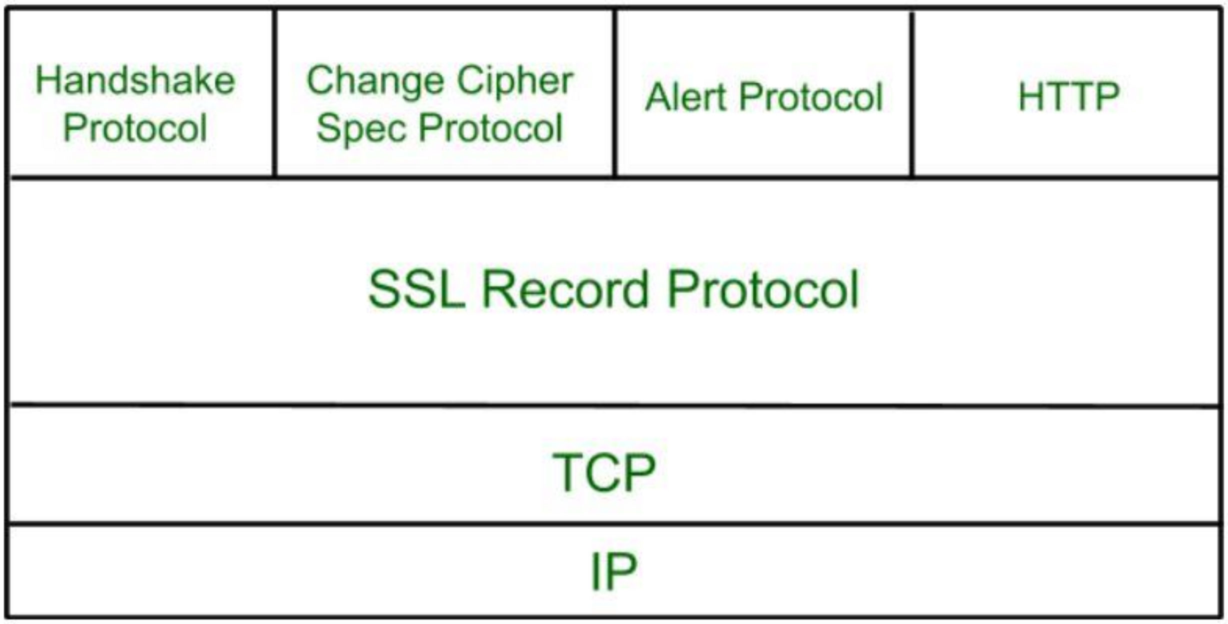
Secure Sockets Layer (SSL) Definition - What does Secure Sockets Layer (SSL) mean? Secure Sockets Layer (SSL) is a standard protocol used for the secure transmission of documents over a network. Developed by Netscape, SSL technology creates a secure link between a Web server and browser to ensure private and integral data transmission.

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:

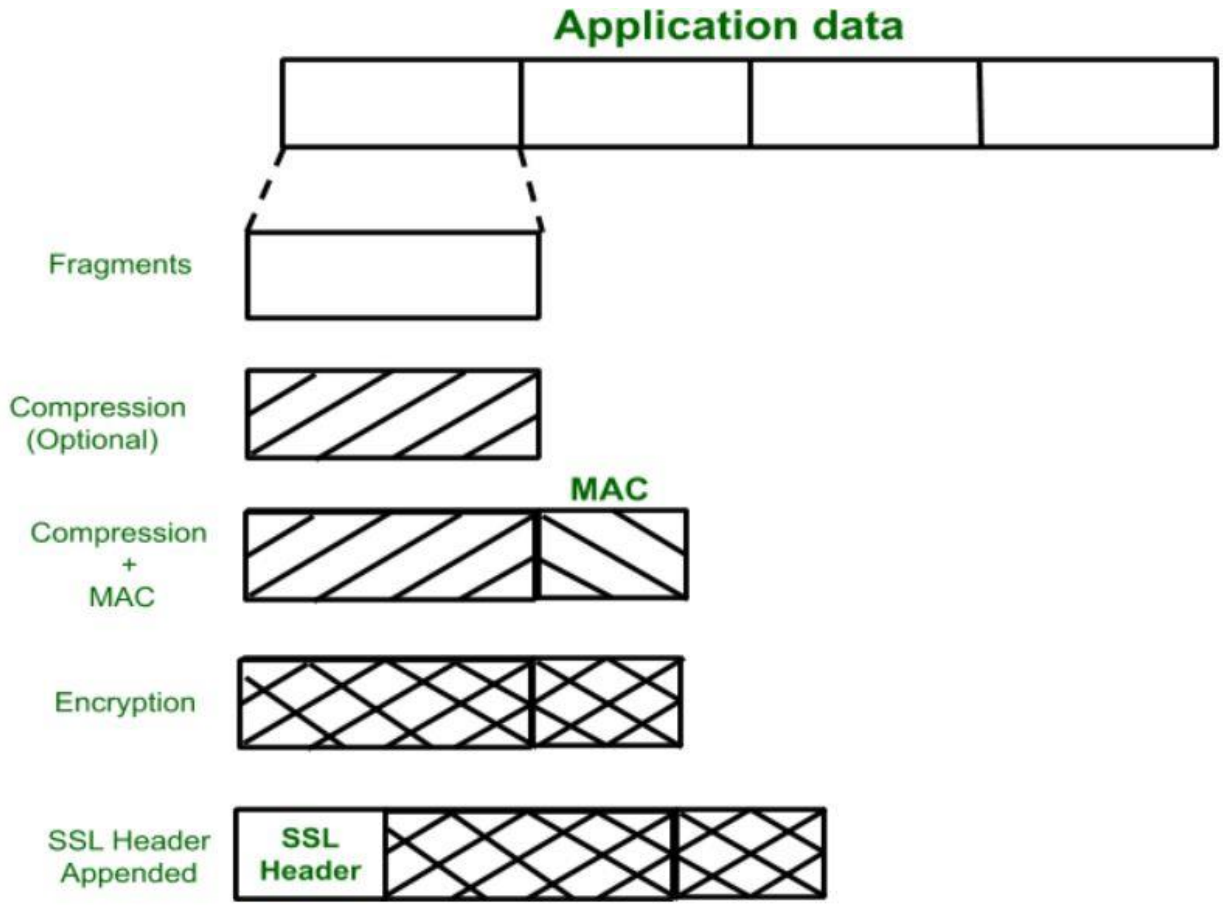


SSL Record Protocol:

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 reply 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.

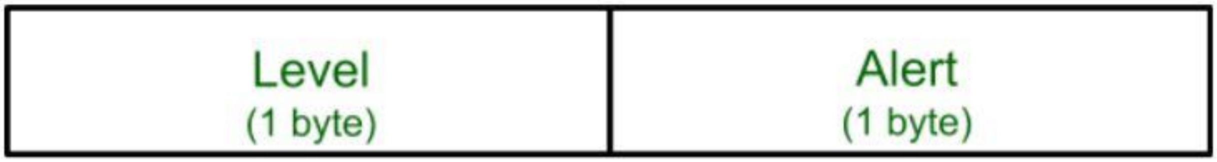
Change-cipher Protocol:

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 contain 2 bytes.



The level is further classified into two parts:

- **Warning:**

  This Alert has no impact on the connection between sender and receiver.

- **Fatal Error:**

  This Alert breaks the connection between sender and receiver.

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.

Transport Layer Security (TLS):

Transport Layer Securities (TLS) are designed to provide security at the transport layer. TLS was derived from a security protocol called Secure Service Layer (SSL). TLS ensures that no third party may eavesdrops or tampers with any message.

There are several benefits of TLS:

- **Encryption:**

  TLS/SSL can help to secure transmitted data using encryption.

- **Interoperability:**

  TLS/SSL works with most web browsers, including Microsoft Internet Explorer and on most operating systems and web servers.

- **Algorithm flexibility:**

  TLS/SSL provides operations for authentication mechanism, encryption algorithms and hashing algorithm that are used during the secure session.

- **Ease of Deployment:**

  Many applications TLS/SSL temporarily on a windows server 2003 operating systems.

- **Ease of Use:**

  Because we implement TLS/SSL beneath the application layer, most of its operations are completely invisible to client.

Working of TLS:

The client connects to server (using TCP), the client will be something. The client sends number of specifications:

1. Version of SSL/TLS.
2. which cipher suites, compression method it wants to use.

The server checks what the highest SSL/TLS version is that is supported by them both, picks a cipher suite from one of the client's options (if it supports one) and optionally picks a compression method. After this the basic setup is done, the server provides its certificate. This certificate must be trusted either by the client itself or a party that the client trusts. Having verified the certificate and being certain this server really is who he claims to be (and not a man in the middle), a key is exchanged. This can be a public key, “PreMasterSecret” or simply nothing depending upon cipher suite.

Both the server and client can now compute the key for symmetric encryption. The handshake is finished and the two hosts can communicate securely. To close a connection by finishing. TCP connection both sides will know the connection was improperly terminated. The connection cannot be compromised by this through, merely interrupted.

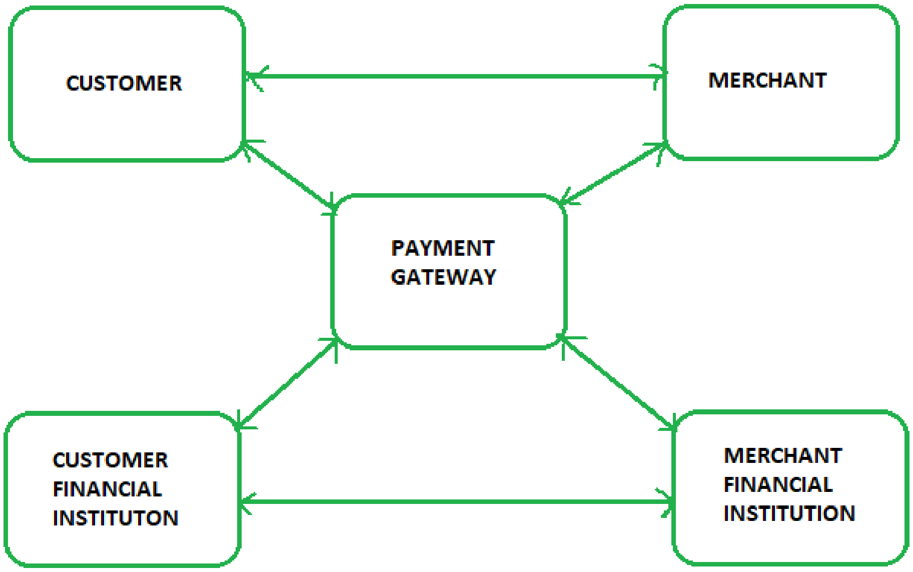
Secure Electronic Transaction (SET):

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,

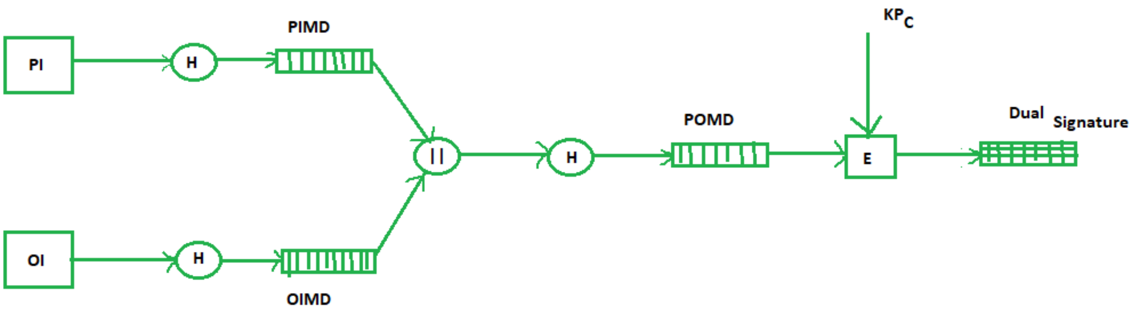
Dual Signature:

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

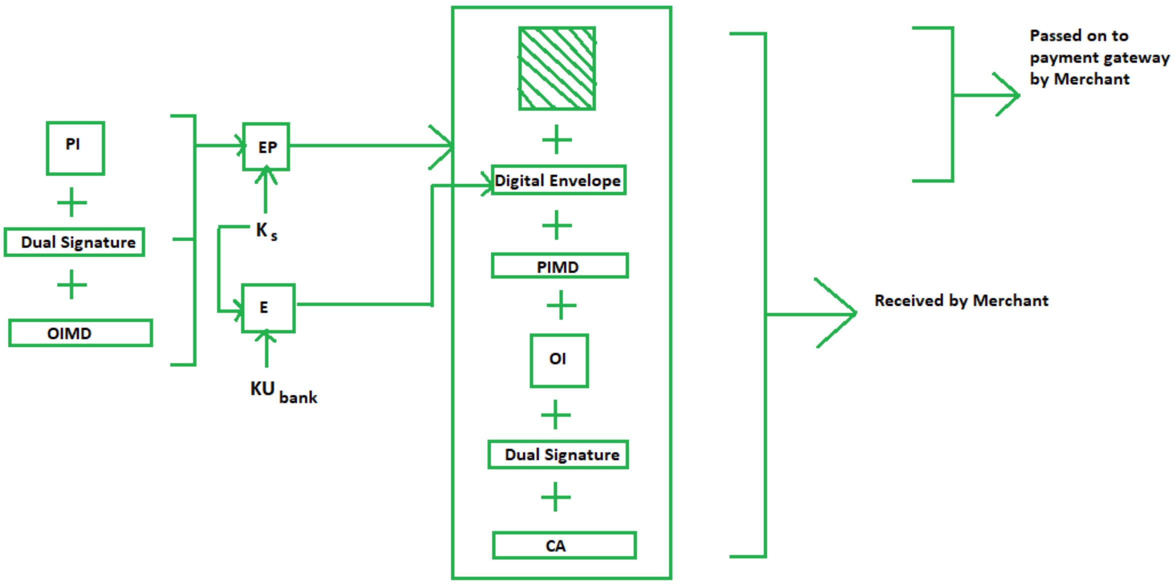
Dual signature, DS= E(KPc, [H(H(PI)||H(OI))])

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

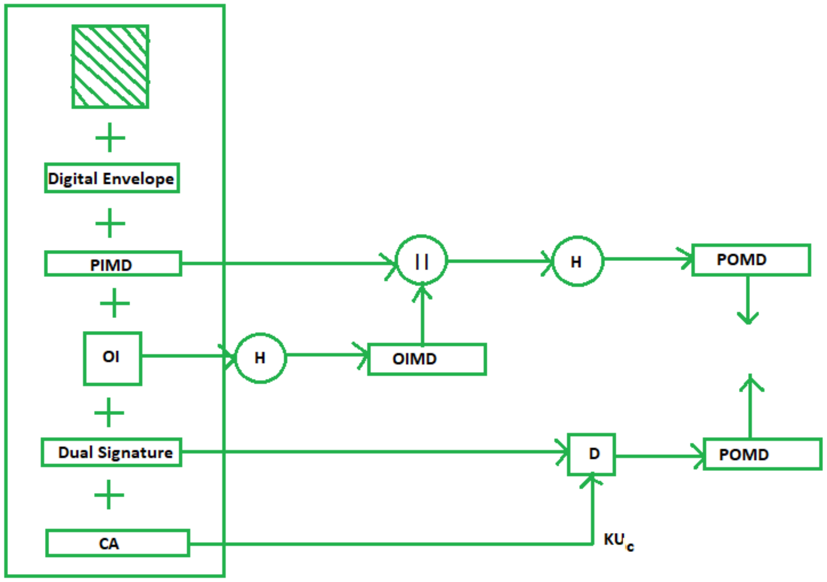
KUbank is public key of bank

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.