CNS Assignment No. 5

Q.1 Why we need to provide the security in Operating System?

Ans. 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.

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.

Need of protection:

- To prevent the access of unauthorized users
- 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.

Q2. Explain memory protection process in details.

Ans: 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.

Q3. Define Web Security. What are the requirements that are needed to provide in Web Security?

Ans: 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.

Web services can be used for two distinct domains—

a)Enterprise Application Integration.

b)Business to Business Integration.

Requirements of Web Security are as follows:-

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

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

3. Who are the subscribers of the Web service?

4. Can the service be invoked over the Internet?

5. How secure is the underlying application?

6. Is the Web service transaction-oriented?

7. What protocol is utilized?

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

9.Who is involved in the service?

10. Is component chaining used?

Q4. Explain in Briefly:

i)Secure Socket Layer(SSL).

ii)Transport Layer Security(TLS).

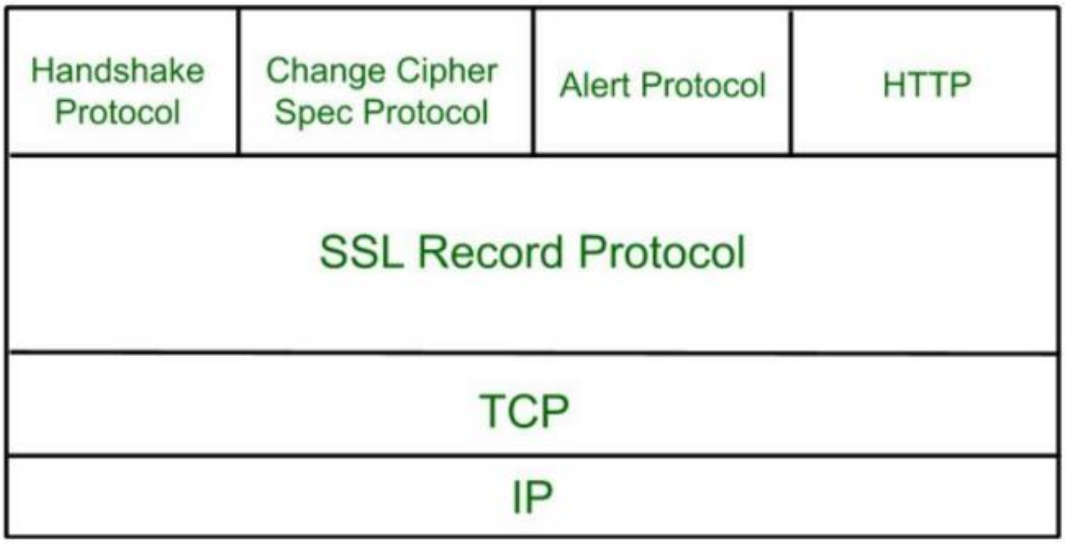
Ans:

i)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.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.



ii)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 Flexing:**
  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.

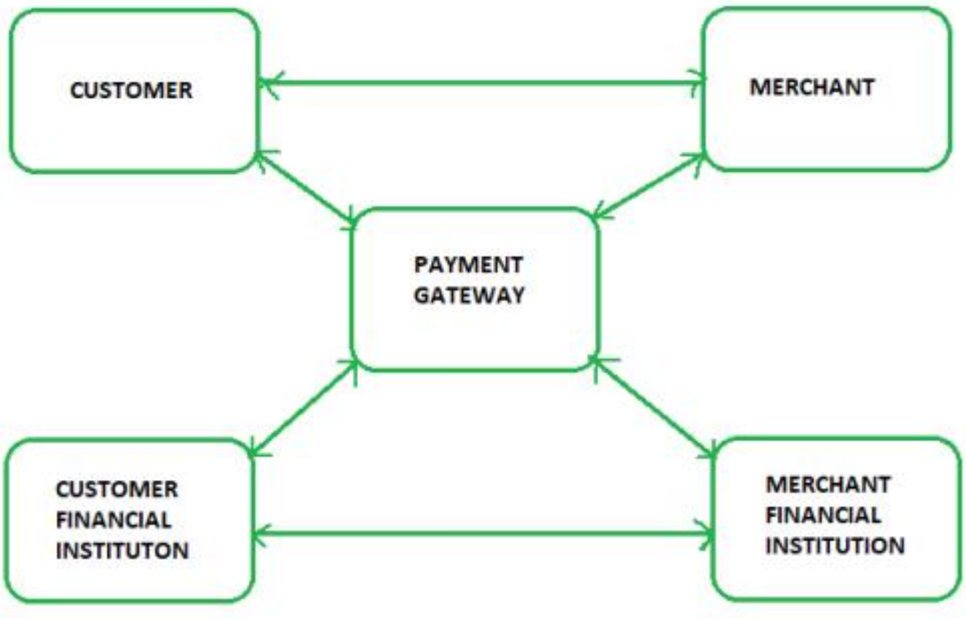
Q5. Explain Secure Electronic Transaction(SET) protocol in details.

Ans: 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.

a general scenario of electronic transactions, which includes client, payment gateway, client financial institution, merchant, and merchant financial institution.



Q6. What are the different types of threats in computing System?

Ans: Types of Threats:

1. Physical Threats: A physical danger to computer systems is a potential cause of an occurrence/event that could result in data loss or physical damage. It can be classified as:

- **Internal:** Short circuit, fire, non-stable supply of power, hardware failure due to excess humidity, etc. cause it.
- **External:** Disasters such as floods, earthquakes, landscapes, etc. cause it.
- **Human:** Destroying of infrastructure and/or hardware, thefts, disruption, and unintentional/intentional errors are among the threats.

2. Non-physical threats:

The non-physical threads can be commonly caused by:

(i) Malware: Malware ("malicious software") is a type of computer program that infiltrates and damages systems without the users' knowledge.

(ii) Virus: It is a program that replicates itself and infects your computer's files and programs, rendering them inoperable.

(iii) Spyware: Spyware is a type of computer program that tracks, records, and reports a user's activity (offline and online) without their permission for the purpose of profit or data theft.

(iv) Worms: Computer worms are similar to viruses in that they replicate themselves and can inflict similar damage.

(v) Trojan: A Trojan horse is malicious software that is disguised as a useful host program. When the host program is run, the Trojan performs a harmful/unwanted action.

(vi) Denial Of Service Attacks: A Denial of Service attack is one in which an attacker tries to prohibit legitimate users from obtaining information or services.

(vii) Phishing: Phishing is a type of attack that is frequently used to obtain sensitive information from users, such as login credentials and credit card details.

Q7. Which objects are need to be protected in Operating System?

Ans:

Objects to be Protected 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 such as directory or files. 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.

a)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.

b)Software Protection:-

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.

- To prevent the access of unauthorized users
- 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.

c) 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.