Marks -

Page No. 118
Date

6) Application & Web Security

6.1 Application hardening and patches

Application hardening is a security feature designed to prevent exploitation of various types of vulnerabilities in software application. It can be done by changing default application configuration, implementing the latest software patches, hotfixes and updates, using the latest and secured versions of protocol and following procedures and ~~policies~~ policies to reduce attack and system down time.

Steps for hardening windows operating system / Guideline for securing windows operating system:

1. Rename administrator account
2. Password management
3. Use NTFS file system
4. Disable all unnecessary services
5. Permissions on file and access to registry
6. Remove unnecessary programs
7. Enable login
8. File Sharing
9. Apply latest patches and fixes
10. Remove unnecessary user accounts and ensure password guidelines are in place.

- Application Patch :- A patch is a piece of software designed to fix problem with, or update a computer program or its supporting data. This includes fixing security vulnerabilities and other bugs, and improving the usability and performance. They are most likely to be comming from the vendor that sells the application.

Application patches are likely to come in three varieties: hotfixes, patches and upgrades.

→ Hotfixes are usually small section of code designed to fix up a specific problem.

→ Patches are usually collection of fixes, and they are usually released on periodic basis.

→ The term upgrade has positive connotation - you are moving to a better, more functional and more secure application.

- Web servers :- A web server is a computer program that delivers content, such as web pages, using Hyper Text Transfer Protocol (HTTP) over the world wide web.
  A client, commonly a web browser or web crawler, initiates communication by making a request for a specific resource using HTTP and the server responds with the content of that resources, or an error message, if unable to do so.

- Active Directory :- An active directory is a directory structure used in Microsoft Windows based computers and servers to store information and data about networks and domains. It does variety of functions including ability to provide information on objects.

Terminologies used in active directory :-

① Object :- An object is any user, system, computer, resource or service tracked within Active directory.

② Domain :- Each object is placed into a domain, which can then used to control which users may access which objects. Each domain has its own security policies, administrative control, privilages and relationships to other domains.

③ Tree and forest :- A forest is a collection of trees; Trees are collection of one or more domains.

④ Trust relationship :- Under this concept, when a user authenticates sucessfully into one child domain, all other child parents under the same parent will accept the authentication as well, due to two-way trust system.

6.2 Web security :

The main types of threats to web systems are listed below;

① Physical :- Physical threats include loss or damage to equipment through fire, smoke, water and other fire supressants, dust, theft and physical impact.

② Malfunction :- Both equipment and software malfunction threats can impact upon the operations of the website or web application.

③ Malware :- It comes in many guises.

④ Spoofing :- It is where a computer assumes identity of another and masquerading where a user pretends to be other.

⑤ Scanning :- Scanning of web system, includes bruteforce and dictionery attacks on username, passwords and encryption keys.

⑥ Eavesdropping :- Monitoring of data may also used to uncover passwords or other sensetive data.

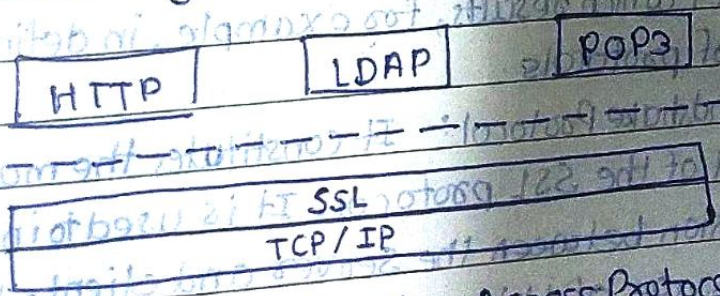
Web Traffic security Approaches :-

One way to provide web security is to use IP security (IpSec). The advantages of using IpSec are that it is transparent to end users and application and provides general purpose solution. IpSec includes a filtering capability so that only selected traffic need incur the overhead of IpSec processing.

Another relatively general purpose is to implement security just above TCP. The foremost example of this approach is the Secure Sockets Layer (SSL) and the follow on Internet standard known as Transport Layer Security (TLS)

Secure Sockets Layer (SSL) :-

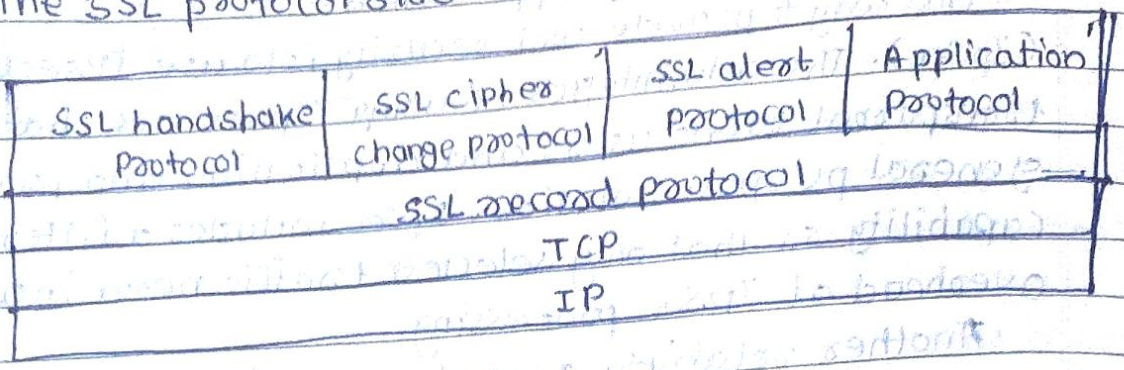
Secure Sockets Layer (SSL) is a protocol that provides security for communications over networks such as internet. It is used for establishing an encrypted link between a web server and a browser. The usage of SSL technology ensures that all data transmitted between the web server and browser remains encrypted.



LDAP :- Lightweight Directory Access Protocol
POP3 :- Post office Protocol - Version 3

Read

The SSL protocol stack:



* The SSL record protocol :- The SSL record protocol is used to transfer any data within a session - both messages and other SSL protocols, as well as for any application data.
* The Alert protocol :- It is used by parties to convey session messages associated with data exchange and functioning of the protocol. The first byte always takes the value, "warning" (1) or "fatal" (2), the determines the severity of message sent.
* The Change cipher Spec protocol :- It is the simplest SSL protocol. It consists of a single message that carries the value as 1. The sole purpose of this message is to cause the pending session state to be established as a fixed state, which results, for example, in defining the used set of protocols.
* The Handshake Protocol :- It constitutes the most complex part of the SSL protocol. It is used to initiate a session between the server and client. Within the message of this protocol, various components such as algorithms are keys used for data encryption are negotiated.

SSL benefits :-

* Data encayrtion
* Trust
* Private communication Channel
* Importance
* SSL certificate
* Authentication
* Message privacy
* Message integrity
* Incoesing business

limitations of SSL :-

* Complex installation
* Increased load
* No client identification

SSL applications :-

* SSL secured transactions with an e-commerce website
* Authenticated client access to an SSL - secured web site
* Remote access
* SWL access
* Email

TLS protocol :-

Transport Layer Security (TLS) protocol provides communication privacy over internet. The protocol allows client/server applications to communicate in a way that it is designed to prevent eavesdropping, tampering or message forgery.

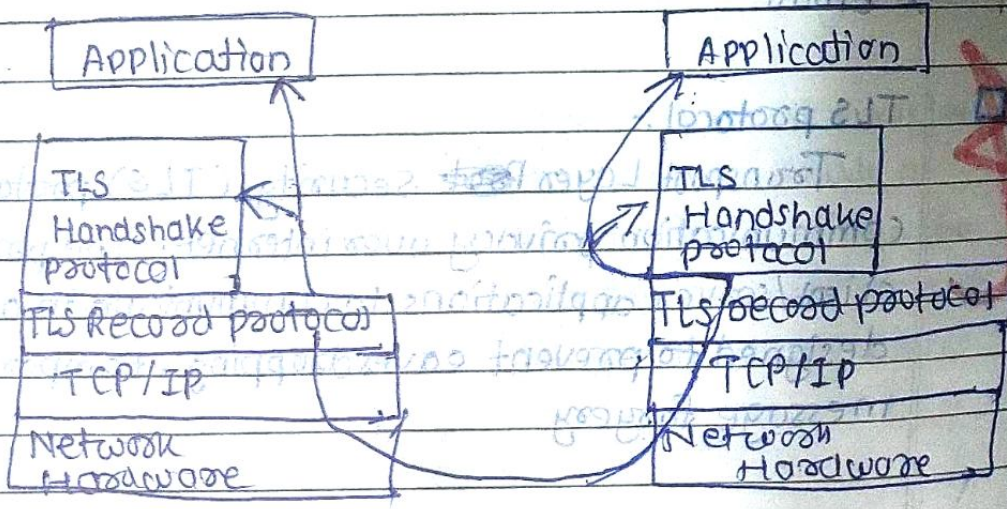
TLS protocol is composed of two layers :-

1. TLS Record protocol
2. TLS Handshake protocol

1. TLS Record protocol :- The TLS record protocol provides connection security that has two basic properties :-
   * The connection is private – The keys for this symmetric encryption are generated uniquely for each connection and are based on a secret negotiated by another protocol.
   * The connection is reliable – Message transports includes a message integrity check using a keyed MAC. Secure Hash functions are used for MAC computations

2. TLS Handshake protocol :- It allows server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data

Working of TLS :-



① The handshake beings with a client connects to a TLS enabled server requesting a secure connection, and presents a list of supported cipher suites.
② From this list, the server picks the strongest cipher and hash function that it also supports and notifies the client of decision.
③ The server sends back its identification in the form of a digital certificate. The certificate usually contains server name, the trusted certificate authority (CA), and the server's public encryption key.
④ The client may contact the server that issued the certificate and confirm that certificate is authentic before proceeding.
⑤ In order to generate the session keys used for secure connection, the client encrypts a random number (RN) with the server's public key (Pbk) and sends the result to the server. Only the server should be able to decrypt it with its private key (Pvk).
⑥ From the random number, both parties generate key material for encryption and decryption.

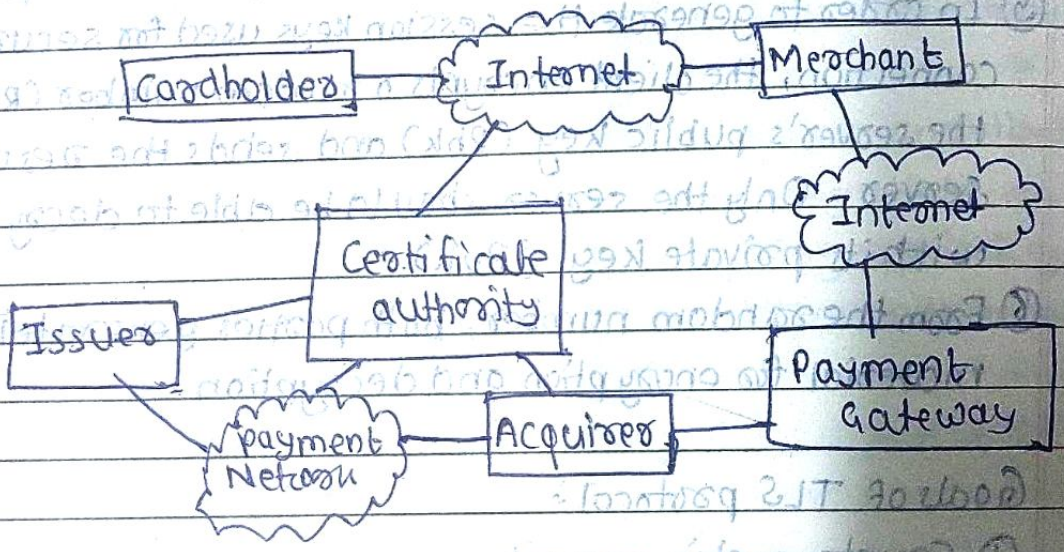
Goals of TLS protocol:
① Cryptographic security
② Interoperability
③ Extensibility
④ Relative efficiency.

Secure Electronic Transaction (SET):-

Secure Electronic Transactions (SET) is a system for ensuring the security of financial transactions on the network. It is not a payment system but rather a set of security protocols and format that enabled users to emply the existing credit card payment infrastructure on an open network in a secure fashion.

SET objectives:-

* To encrypt critical information over the internet
* To seperate the merchant from credit card information
* To link payment and order information



Working of SET:-

① The customer opens a Mastercard or Visa bank account. Any issuer of a credit card is some kind of bank.

② The customer receives a digital certificate. It includes a public key with an expiration date.

③ Third party merchants also receive certificates from the bank. The certificates include merchant's and bank's public key.

④ The customer places an order over a web page, by phone, or some other means.

(5) The customer's browser receives and confirms from the merchant's certificate that the merchant is valid
(6) The browser sends the order information. This message is encrypted with the merchants public key, the payment information, which is encrypted with the bank's public key, and information that ensures payment can only be used with this particular order.
(7) The merchant verifies the customer by checking digital signature on the customer's certicate.
(8) The merchant sends order message along to the bank. This includes the bank public key, customer's payment information, and the merchant's certificate
(9) The bank verifies the merchant and the message
(10) The bank digital signs and sends authorisation to the merchant, we can then fill the order.

Various participants in SET and their roles :-

* Cardholder :- A cardholder is an authorised holder of a payment card that has been issued by issuer.
* Merchant :- A merchant is a person or an organisation that wants to sell goods or services to card holders.
* Issuer :- The issuer is the financial institution (bank) that provides a payment card to the card holder.
* Acquirer :- This is a financial institution that has a relationship with merchants for processing payment card authorisation and payment.
* Payment gateway :- It processes the payment messages on behalf of the merchants. It acts as an interface between SET and existing card payment network for payment authorisations.
* Certification authority :- This is authority that is trusted to public key certificates to cardholders, merchants and payment gateways.