Web Security

Need Of Security

- Security is required because the widespread use of data processing equipment, the security of information felt to be valuable to an organization was provided primarily by physical and administrative means.

WEB SECURITY :

- Measures to protect data during their transmission over a collection of interconnected networks.
- The World Wide Web is fundamentally a client/server application running over the internet and TCP/IP intranets.

Web security Requirement

- The web is very visible.
- The WWW is widely used by:-
- Business, Government agencies and many individuals.
- These can be described as passive attacks including eavesdropping on network traffic between browser and gaining access to information on a website that is supposed to be restricted.
- Active attacks including impersonating another user, altering information on a website.
- The web needs added security mechanisms to address these threats .

Web Security Threats

- Various approaches are used for providing security web. One of the examples is IP-security.

Parameter	Threats	Consequences	Counter Measures
INTEGRTY	1.Modification of user data, memory, message traffic in transmit.. 2.Trojan horse browser.	1.Loss of information . 2.Compromise of machine. 3.Vulnerability to all other threats.	Cryptographic checksums.
Confidentiality	1. Eavesdropping on the net. 2. Theft of information and data from server and client.	Loss of information and privacy.	Encryption, Web proxies.

(continue.....)

Parameter	Threats	Consequences	Counter Measures
Denial of service	1. Killing of user threads. 2. Flooding machine with bogus requests. 3. Filling up disk or memory. 4. Isolating machine by DNS attacks	1. Disupptive 2. Annoying 3. Prevent user from getting work done.	Difficult to prevent.
Authentication	1. Impersonation of legitimate users. 2. Data forgery.	1. Misrepresentation of user. 2. Belief that false information is valid.	Cryptographic techniques.

Web Traffic security Approaches

- A number of approaches to providing web security are possible. figure illustrates this difference.

1. Network level
2. Transport level
3. Application level

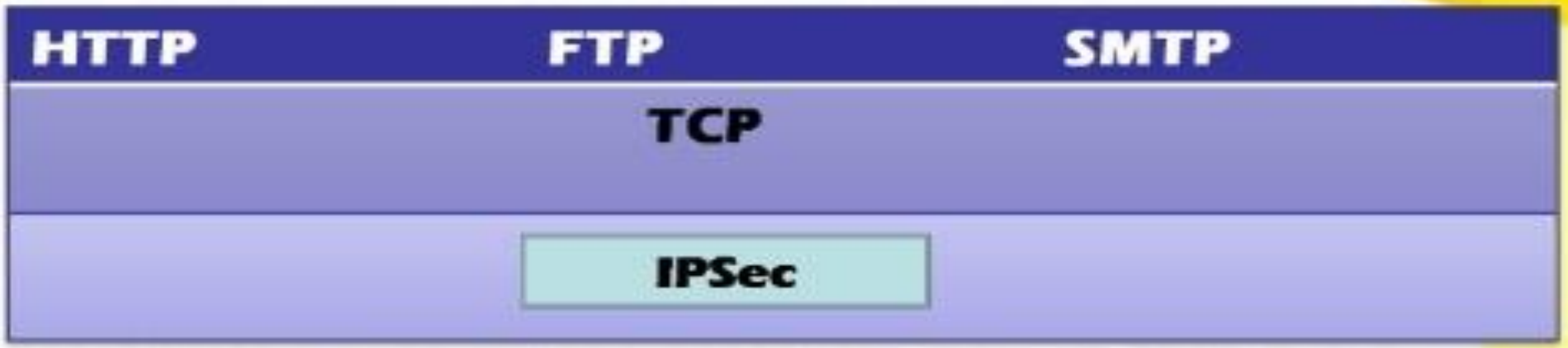


Fig: Network level

(continue.....)

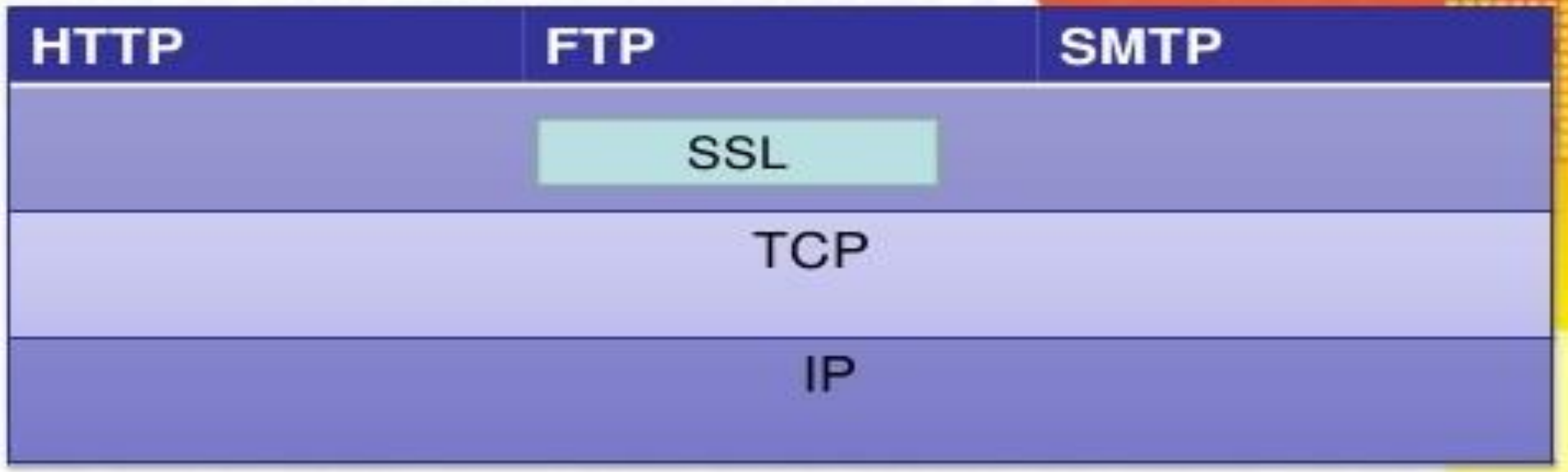


Fig: Transport level

Fig: Application level

Secure Socket Layer[SSL]

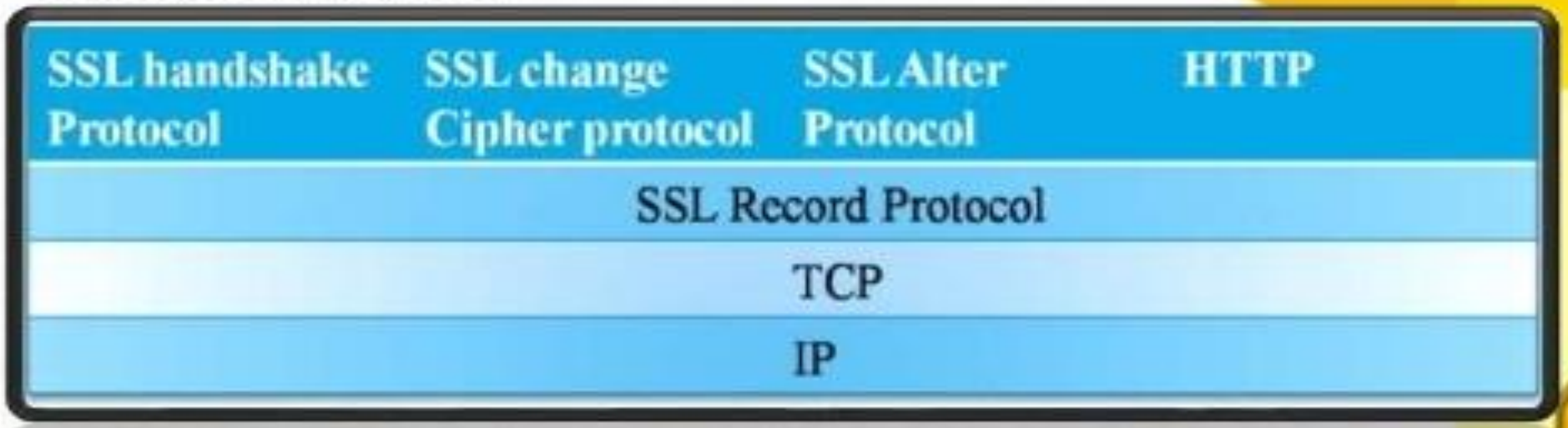
- SSL protocol is an internet protocol for secure exchange of information between a web browser and a web server.
- SSL is designed to make user of TCP to provide a reliable end to end secure service.
- SSL provides security services between TCP and application that use TCP.
- The SSL protocol is an internet protocol for secure exchange of information between a web browser and a web server.

Features of SSL

1. SSL server authentication , allowing a user to confirm a server's identity.
2. SSL client authentication , allowing a server to confirm a user's identity.
3. An encrypted SSL session , in which all information sent between browser and server is encrypted by a sending software and decrypted by the receiving software.
4. SSL supports multiple cryptographic algorithms.

SSL Architecture:-

- SSL uses TCP to provide reliable end-to-end secure service.
- SSL consists of two sub protocols , one for establishing a secure connection and other for using it. Figure shows SSL protocol stack.



[Figure : SSL protocol stack]

(continue.....)

HTTP:

- Provides the transfer services for web client/server interaction.

SSL Handshake Protocol , SSl change cipher protocol:

- Management of SSL exchanges.SSL Alert Protocol .

SSL Record Protocol:

- It provide basic security services to various higher layer protocols.
- 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 from a message authentication code(MAC).

Comparison between IPSec and SSL

Sr no.	Parameters	IP-Security	SSL
1.	Position in the OSI model	Internet layer	Between the transport and application layers.
2.	Configuration	Complex	Simple
3.	NAT	Problematic	No problem
4.	Software location	Kernel area	User area
5.	Firewall	Not friendly	Friendly
6.	Installation	Vender non-specific	Vender specific
7.	Interoperability	Yes	No
8.	Deploy	More expensive to deploy support and maintain.	Less costly to deploy and maintain.