NETWORKS, PROTOCOLS & SECURITY
23EC2210 R/A/E

TOPIC:
SECURE SOCKET LAYER

Session-39

AIM OF THE SESSION

To familiarize the students with the basic concept of the socket, Secure Socket Layer, and the working of the simple mail transfer protocol

INSTRUCTIONAL OBJECTIVES

The session is design to understand the:

1. Introduction of the concepts of socket
2. To understand the Secure Socket Layer and
3. To understand the concepts of the working of simple mail transfer protocol.

LEARNING OUTCOMES

At the end of this session, you should be able to:

1. Describe the concept of Socket.
2. Describe the Secure Socket Layer and
3. Describe the working of simple mail transfer protocol.

SYLLABUS

PREFACE OF SOCKET ,

SECURE SOCKET LAYER

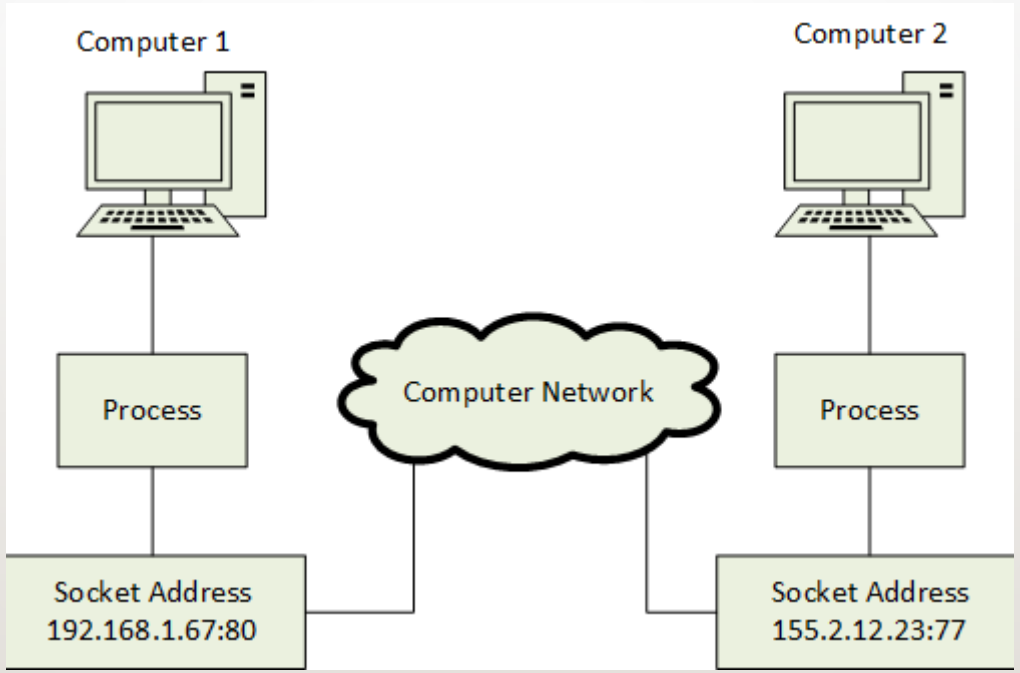
PREFACE TO THE SOCKET

- Sockets in computer networks are used for allowing the transmission of information between two processes of the same machines or different machines in the network.
- Sockets allow communication of two processes that are running on the same or different machines.
- Sockets are the end of two-way communication between two programs that are running on the networks.

PREFACE TO THE SOCKET

- Sockets are mostly used in client-server architecture for communication between multiple applications.
- The socket is created by the combination of the IP address and port number of the software. With this combination, the process knows the system address and address of the application where data is to be sent.
- : is used to separate IP address and port number. or e.g.: 192.168.1.67:80, 155.2.12.23:77, etc.

PREFACE TO THE SOCKET

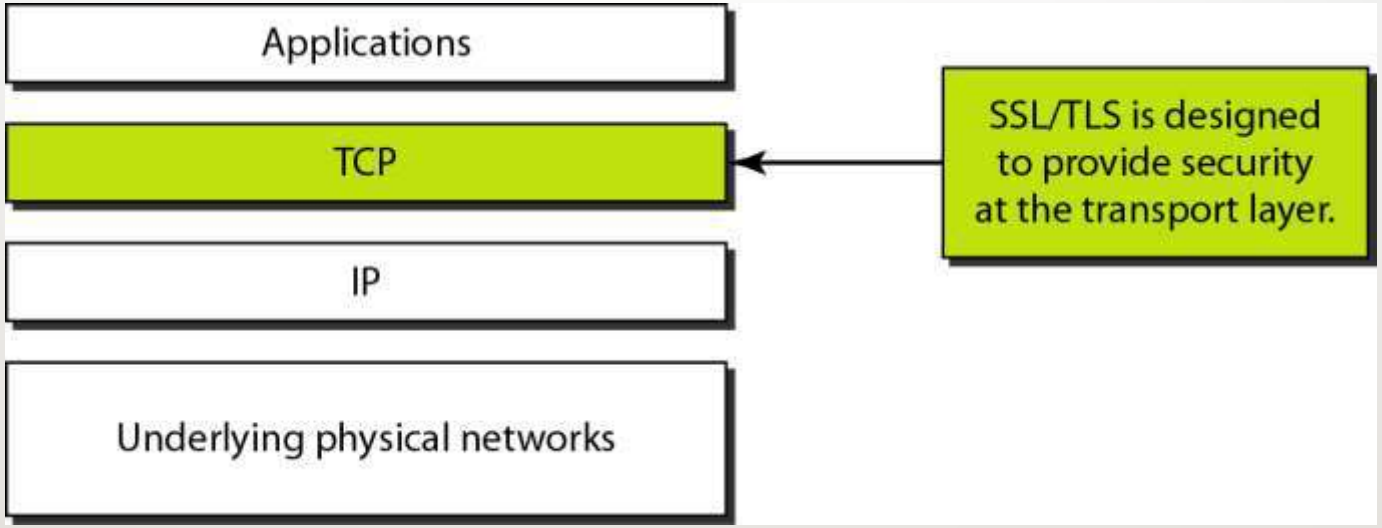


SECURE SOCKET LAYER (SSL)

- *Two protocols are dominant today for providing security at the transport layer: the Secure Sockets Layer (SSL) Protocol and the Transport Layer Security (TLS) Protocol. The latter is actually an IETF version of the former.*

SECURE SOCKET LAYER (SSL)

- Location of SSL and TSL in the Internet Model



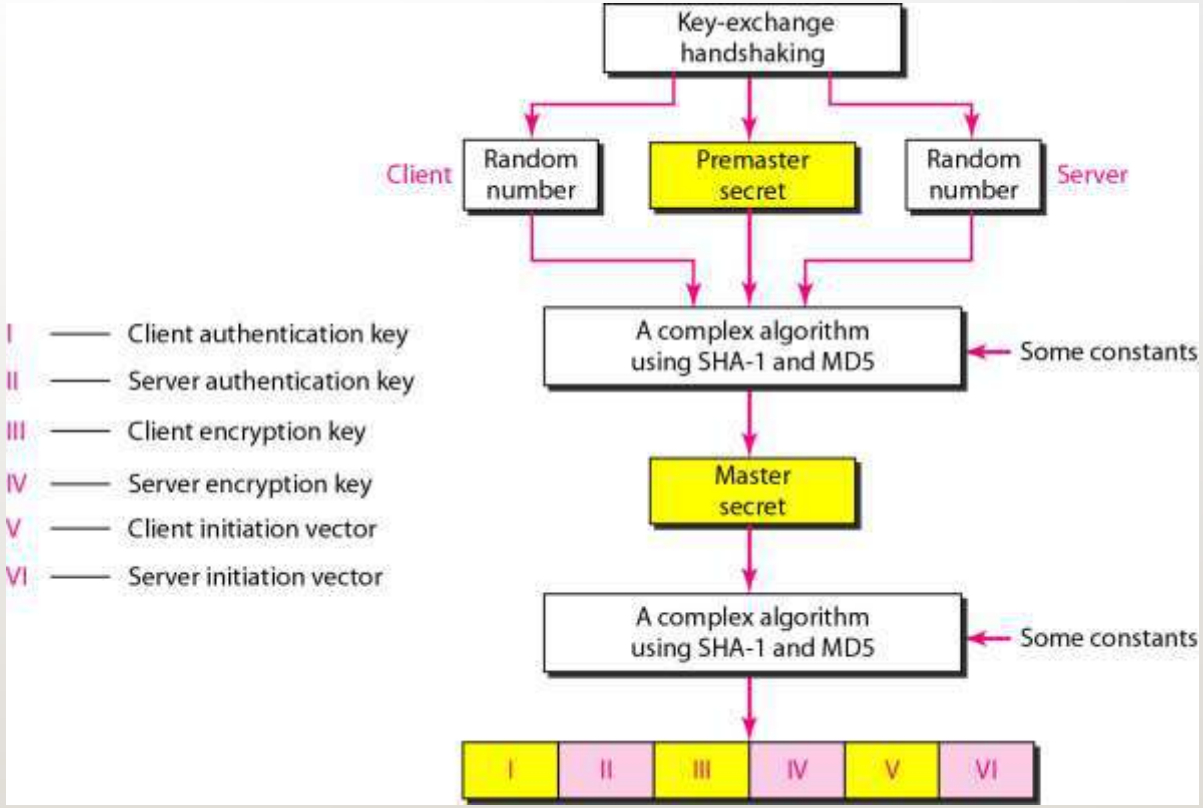
SECURE SOCKET LAYER (SSL)

- SSL cipher suit list

Cipher Suite	*Key Exchange Algorithm*	*Encryption Algorithm*	*Hash Algorithm*
SSL_DHE_RSA_*WITH*_DES_CBC_SHA	DHE_RSA	DES_CBC	SHA
SSL_DHE_RSA_*WITH*_3DES_EDE_CBC_SHA	DHE_RSA	3DES_EDE_CBC	SHA
SSL_DHE_DSS_*WITH*_DES_CBC_SHA	DHE_DSS	DES_CBC	SHA
SSL_DHE_DSS_*WITH*_3DES_EDE_CBC_SHA	DHE_DSS	3DES_EDE_CBC	SHA
SSL_DH_RSA_*WITH*_DES_CBC_SHA	DH_RSA	DES_CBC	SHA
SSL_DH_RSA_*WITH*_3DES_EDE_CBC_SHA	DH_RSA	3DES_EDE_CBC	SHA
SSL_DH_DSS_*WITH*_DES_CBC_SHA	DH_DSS	DES_CBC	SHA
SSL_DH_DSS_*WITH*_3DES_EDE_CBC_SHA	DH_DSS	3DES_EDE_CBC	SHA
SSL_FORTEZZA_DMS_*WITH*_NULL_SHA	FORTEZZA_DMS	NULL	SHA
SSL_FORTEZZA_DMS_*WITH*_FORTEZZA_CBC_SHA	FORTEZZA_DMS	FORTEZZA_CBC	SHA
SSL_FORTEZZA_DMS_*WITH*_RC4_128_SHA	FORTEZZA_DMS	RC4_128	SHA

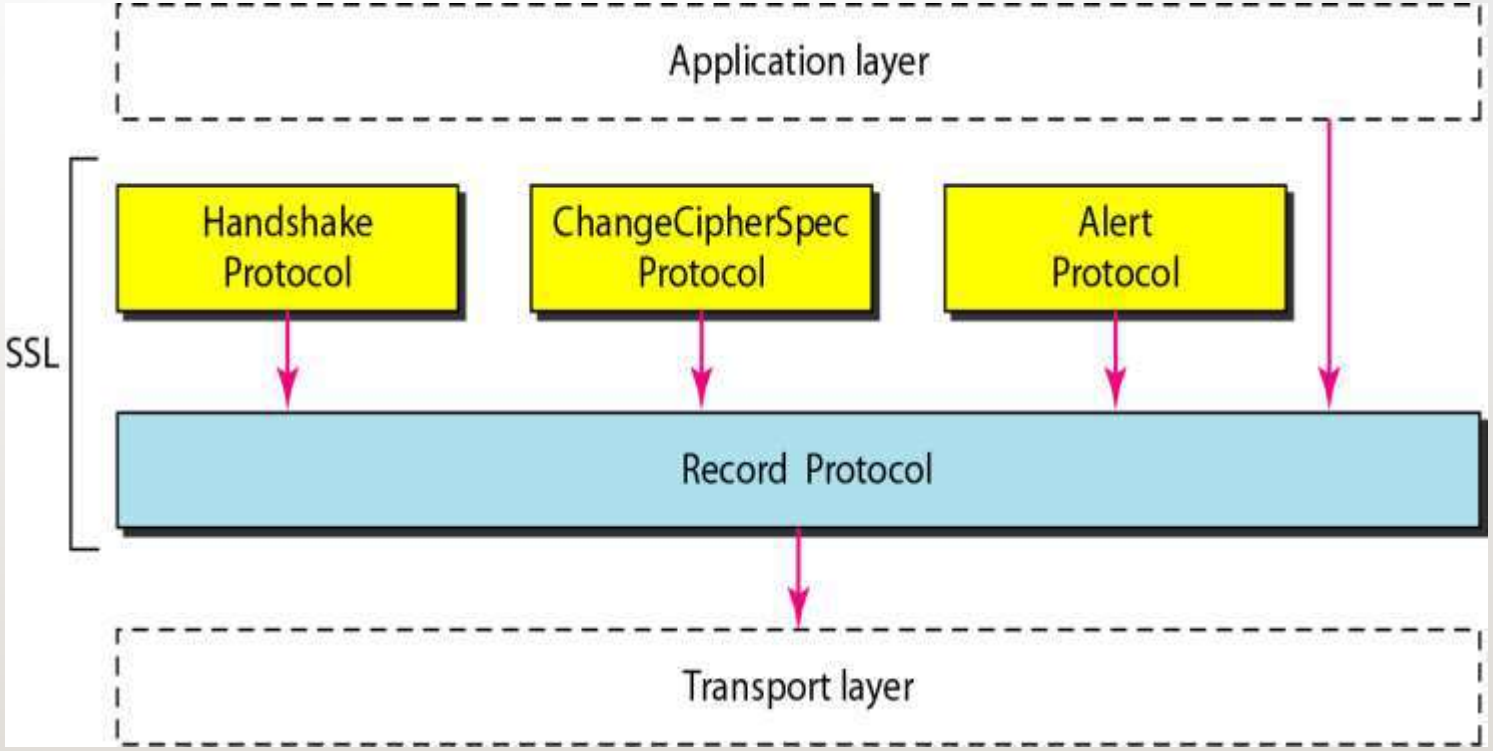
SECURE SOCKET LAYER (SSL)

- *The client and the server have six different cryptography secrets.*
- *Creation of cryptographic secrets in SSL*



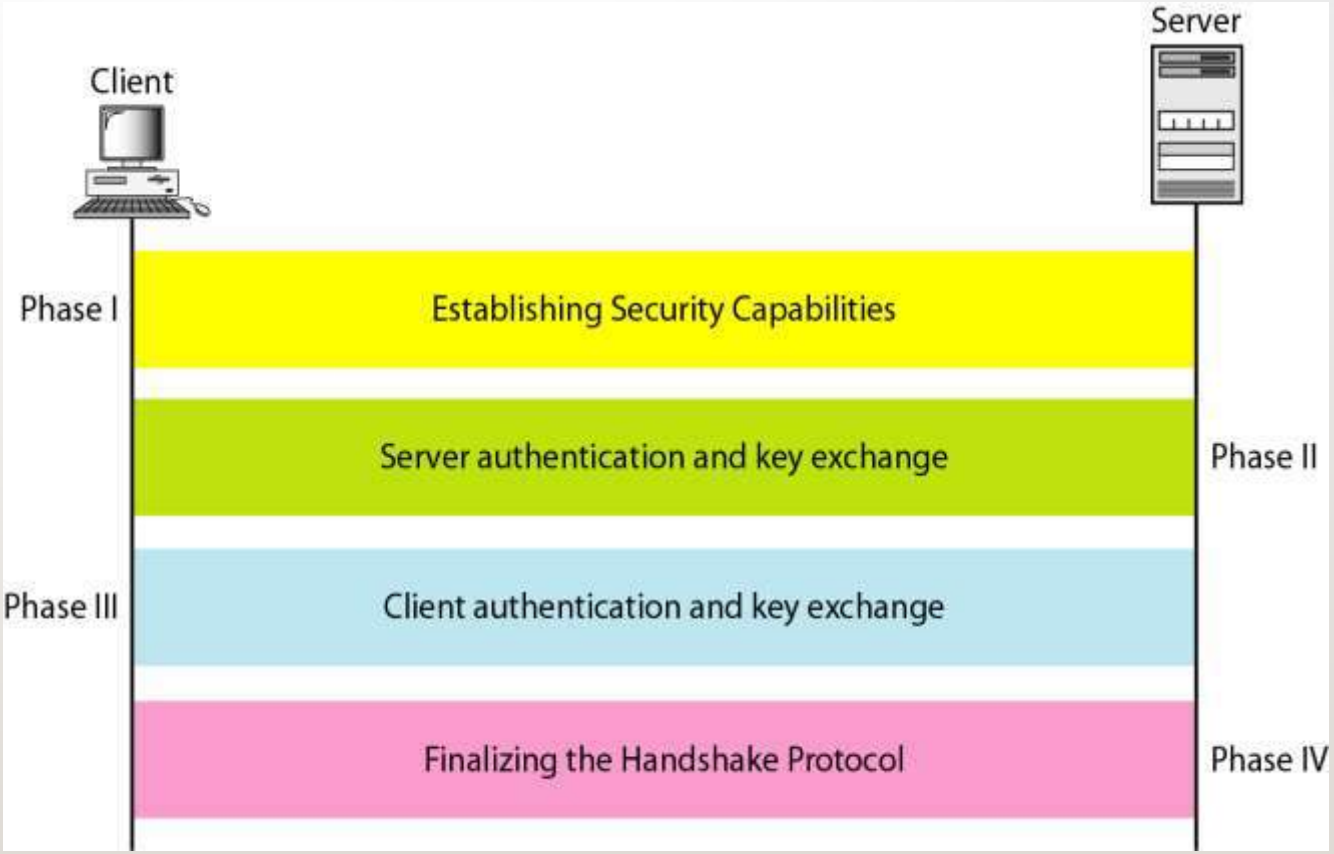
SECURE SOCKET LAYER (SSL)

- SSL Protocol suit



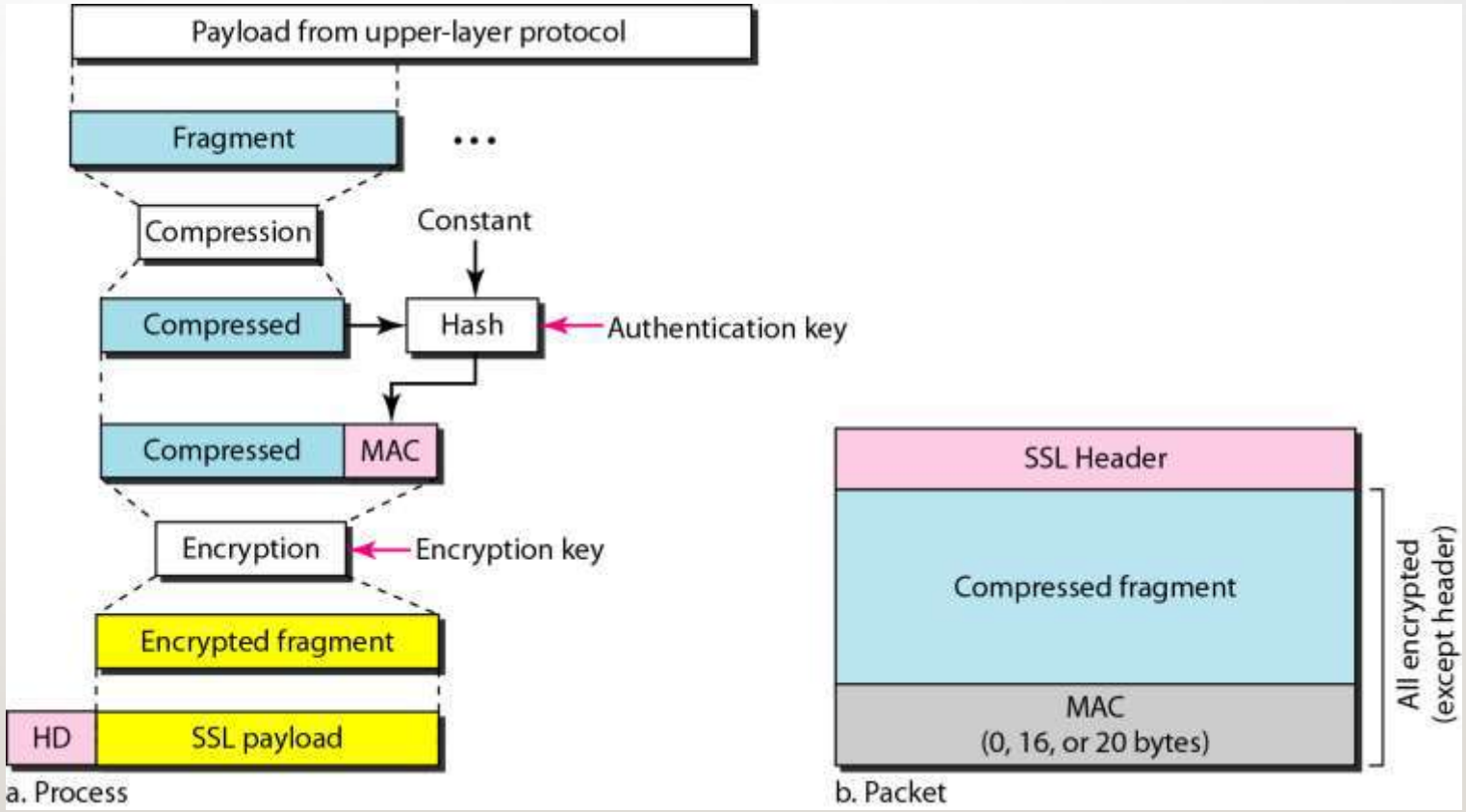
SECURE SOCKET LAYER (SSL)

- Hand shake Protocol



SECURE SOCKET LAYER (SSL)

- Processing done by the record Protocol



SELF LEARNING QUESTION

1. In the above figure from left to right, the correct order of the shaded levels are
   a) Network level, Application level, Transport level
   b) Application level, Network level, Transport level
   c) Transport level, Application level, Network level
   d) Network level, Transport level, Application level

Answer: d

Explanation: IP/IPSec is the Network level, SSL or TLS is the Transport Level, Kerberos and S/MIME are the Application level.

1. In the above figure, which of the above shaded block is transparent to end users and applications?
   a) IP/IPSec
   b) SSL
   c) Kerberos
   d) S/MIME

Answer: a

Explanation: IP/IPSec is the Network layer which is transparent to end users and applications.

REFERENCES FOR FURTHER LEARNING OF THE SESSION

Reference Books:

1. Data Communications and Networking (3rd Ed.) "–B. A. Ferouzan – TMH
2. Computer Networks (4th Ed.)", A. S. Tanenbaum – – Pearson Education/PHI

Sites and Web links:

1. https://www.scaler.com/topics/computer-network/socket-programming/
2. https://www.geeksforgeeks.org/socket-in-computer-network/
3. https://www.cloudflare.com/learning/ssl/what-is-ssl/
4. https://www.geeksforgeeks.org/secure-socket-layer-ssl/
5. https://www.javatpoint.com/simple-network-management-protocol
6. https://www.manageengine.com/network-monitoring/what-is-snmp.html

THANK YOU

TEAM –NETWORK PROTOCOLS & SECURITY (NPS)