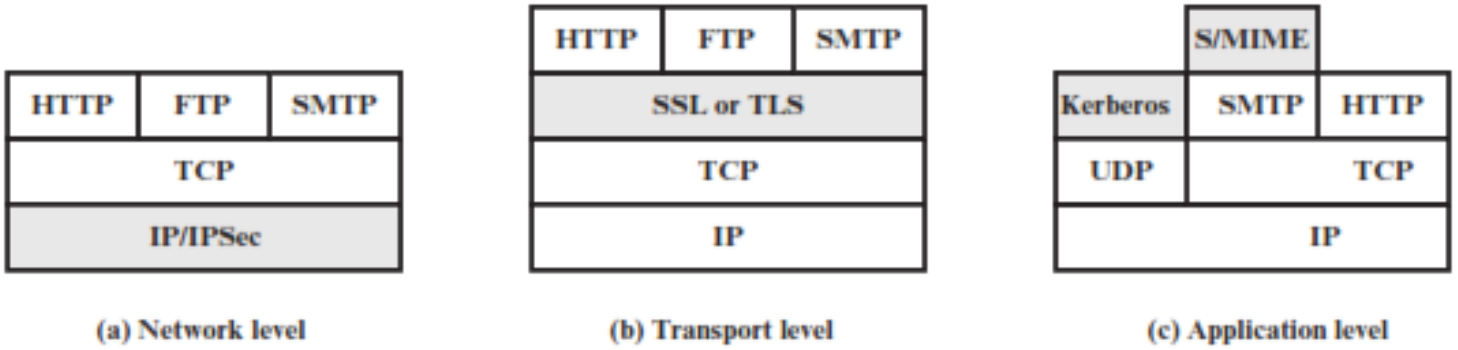
Questions

SSL

- What are the advantages of each of the three approaches shown in Figure 17.1?



- The advantage of using **IPSec (Figure 17.1a) is that it is transparent** to end users and applications and provides a general-purpose solution. Further, IPSec includes a filtering capability so that only selected traffic need incur the overhead of IPSec processing.

- The advantage of using **SSL is that it makes use of the reliability and flow control mechanisms** of TCP.
- The advantage of **application-specific security services** (Figure 17.1c) is that the service can be tailored to the specific needs of a given application.

- **What protocols comprise TLS?**
- SSL handshake protocol; SSL change cipher spec protocol; SSL alert protocol; SSL record protocol.

- What is the difference between a TLS connection and a TLS session?

- **Connection: A connection is a transport (in the OSI layering model** definition) that provides a suitable type of service. For SSL, such connections are peer-to-peer relationships. The connections are transient. Every connection is associated with one session.
- **Session:**
- An SSL session is an association between a client and a server. Sessions are created by the Handshake Protocol. Sessions define a set of cryptographic security parameters, which can be shared among multiple connections. Sessions are used to avoid the expensive negotiation of new security parameters for each connection.

- List and briefly define the parameters that define a TLS session state.

- **Session identifier: An arbitrary byte sequence chosen by the server** to identify an active or resumable session state. **Peer certificate: An** X509.v3 certificate of the peer. **Compression method: The algorithm** used to compress data prior to encryption. **Cipher spec: Specifies the** bulk data encryption algorithm (such as null, DES, etc.) and a hash algorithm (such as MD5 or SHA-1) used for MAC calculation. It also defines cryptographic attributes such as the hash_size. **Master secret: 48-byte secret shared between the client and server. Is resumable: A flag indicating whether the session can be used to** initiate new connections.

- List and briefly define the parameters that define a TLS session connection.
- **Server and client random: Byte sequences that are chosen by the** server and client for each connection. **Server write MAC secret: The** secret key used in MAC operations on data sent by the server. **Client**

- **write MAC secret: The secret key used in MAC operations on data**
- sent by the client. **Server write key: The conventional encryption key**
- for data encrypted by the server and decrypted by the client. **Client**
- **write key: The conventional encryption key for data encrypted by the**
- client and decrypted by the server. **Initialization vectors: When a**
- block cipher in CBC mode is used, an initialization vector (IV) is
- maintained for each key. This field is first initialized by the SSL
- Handshake Protocol. Thereafter the final ciphertext block from each
- record is preserved for use as the IV with the following record.
- **Sequence numbers: Each party maintains separate sequence**

- **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 form a message authentication code (MAC).

- HTTPS (HTTP over SSL) refers to the combination of HTTP and SSL to implement secure communication between a Web browser and a Web server.

- . SSl/TLS includes protocol mechanisms to enable two TCP users to determine the security mechanisms and services they will use.
- Sessions are used to avoid the expensive negotiation of new security parameters for each connection that shares security parameters.
- Microsoft Explorer originated SSL.

- T
- T
- F

- The World Wide Web is fundamentally a client/server application running over the Internet and TCP/IP intranets.
-
- One way to classify Web security threats is in terms of the location of the threat: Web server, Web browser, and network traffic between browser and server.
-
- The encryption of the compressed message plus the MAC must increase the content length by more than 1024 bytes.

- T
- T
- F

- The Change Cipher Spec Protocol is one of the three SSL-specific protocols that use the SSL Record Protocol.
-
- The SSL Record Protocol is used before any application data is transmitted.
-
- The first element of the CipherSuite parameter is the key exchange method.

- SSL Handshake Protocol
- SSL Record Layer Protocol
- SSL Change Cipher Spec
- SSL alert Protocol
- T
- F
- T

- The certificate message is required for any agreed on key exchange method except fixed Diffie-Hellman.
- The shared master secret is a one-time 48-byte value generated for a session by means of secure key exchange.
- The TLS Record Format is the same as that of the SSL Record Format.
- Server authentication occurs at the transport layer, based on the server possessing a public/private key pair.

- F
- T
- T
- T

- The The SSL Internet standard version is called _____ .
-
- A) SSH B) HTTP
-
- C) SLP D) TLS

- TLS

- The most complex part of SSL is the _____ .
-
- A) SSL Record Protocol B) Handshake Protocol
-
- C) Change Cipher Spec Protocol D) Alert Protocol

- The symmetric encryption key for data encrypted by the client and decrypted by
- the server is a _____ .
-
- A) server write key B) **client write key**
-
- C) sequence key D) master key

- _____ provides secure, remote logon and other secure client/server facilities.
-
- A) SLP B) HTTPS
-
- C) TLS D) SSH