FIT3031: Tutorial 5 Solutions

WEB SECURITY

Q1 What are the advantages of each of the three approaches shown in Figure 5.1? √

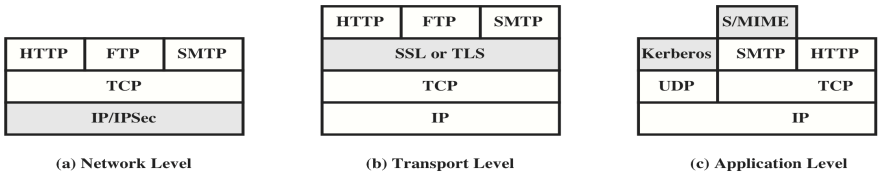

Figure 5.1 Relative Location of Security Facilities in the TCP/IP Protocol Stack

Ans: The advantage of using **IPSec** (Figure 5.1a) 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 5.1c) is that the service can be tailored to the specific needs of a given application.

Q2 What protocols comprise SSL? √

Ans: SSL handshake protocol; SSL change cipher spec protocol; SSL alert protocol; SSL record protocol.

Q3 What is the difference between an SSL connection and an SSL session? √

Ans: 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.

Q4 List and briefly define the parameters that define an SSL session state.

Ans: 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.

Q5 What services are provided by the SSL record Protocol? √

Ans: 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).

Q6 What steps are involved in the SSL record protocol transmission?

Ans: Fragmentation; compression; add MAC; encrypt; append SSL record header.

Q7 What is the purpose of HTTPS? √

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

Q8 For what applications is SSH useful? √

Ans: The initial version, SSH1 was focused on providing a secure remote logon facility to replace TELNET and other remote logon schemes that provided no security. SSH also provides a more general client/server capability and can be used for such network functions as file transfer and e-mail.

Q9 List and briefly define the SSH protocols. √

Ans: **Transport Layer Protocol**: Provides server authentication, data confidentiality, and data integrity with forward secrecy (i.e., if a key is compromised during one session, the knowledge does not affect the security of earlier sessions). The transport layer may optionally provide compression. **User Authentication Protocol**: Authenticates the user to the server. **Connection Protocol:** Multiplexes multiple logical communications channels over a single underlying SSH connection.

Problems: √

1. With SSL there is a distinction between a connection and a session. Explain how this distinction is related to the separation between the Handshake Protocol and the Change_Cipher_Spec Protocol.

   Ans: A given connection can persist over several sessions. By separating the two protocols, a change in a session can occur without having to renegotiate the entire connection. This is very useful, considering that the Change Cipher Spec message consists of a single byte compared to the complex Handshake protocol.

2. In SSL and TLS, why is there a separate Change Cipher Protocol rather than including a change_cipher_spec message in the Handshake Protocol?

   Ans: The change cipher spec protocol exists to signal transitions in ciphering strategies, and can be sent independent of the complete handshake protocol exchange.

3. What purpose does the MAC serve during the change cipher spec SSL exchange?

   Ans: To integrity protect the first set of messages where the cookies and crypto suite information is exchanged. This will prevent a man-in-the-middle attack in step 1 for instance, where someone can suppress the original message and send a weaker set of crypto suites.

4. Consider the following threats to Web security and describe how each one is countered by a particular feature of SSL.

   a. Brute-Force Cryptanalytic Attack: An exhaustive search of the key space for a conventional encryption algorithm.

      Brute Force Cryptanalytic Attack: The conventional encryption algorithms use key lengths ranging from 40 to 168 bits.

   b. Replay Attack: Earlier SSL handshake messages are replayed.

      Replay Attack: This is prevented by the use of nonces.

   c. Man-in-the-Middle Attack: An attacker interposes during key exchange, acting as the client to the server and as server to the client.

      Man-in-the-Middle Attack: This is prevented by the use of public-key certificates to authenticate the correspondents.

   d. Password Sniffing: Passwords in HTTP or other application traffic are eavesdropped.

      Password Sniffing: User data is encrypted.

5. For SSH packets, what is the advantage, if any, of not including the MAC in the scope of the packet encryption?

This allows for the message to be authenticated before attempting decryption, which may be more efficient.