FIT3031: Tutorial 5

WEB SECURITY

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

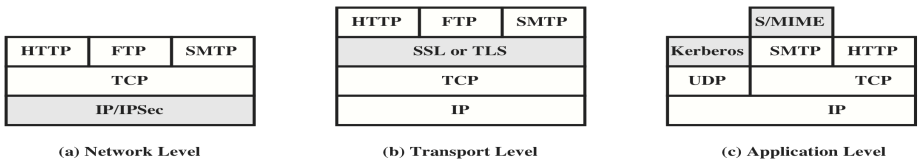

Figure 5.1 Relative Location of Security Facilities in the TCP/IP Protocol Stack

Q2 What protocols comprise SSL? √

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

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

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

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

Q7 What is the purpose of HTTPS? √

Q8 For what applications is SSH useful? √

Q9 List and briefly define the SSH protocols. √

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.

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?

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

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

- **a.** Brute-Force Cryptanalytic Attack: An exhaustive search of the key space for a conventional encryption algorithm.
- **b.** Replay Attack: Earlier SSL handshake messages are replayed.
- **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.
- **d.** Password Sniffing: Passwords in HTTP or other application traffic are eavesdropped.

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