Midterm Exam

Mar. 29, 2022

Network Security Instructor: Prof. Shiuhpyng Shieh

Please write your answers **in order**. Five points will be deducted otherwise. **Make sure you explain your answer to each question**.

1. (20%) A Web browser may be supported by HTTP or HTTPS. (A) (5%) HTTPS uses port 80, 443, or 445? (B) (5%) HTTPS is supported by SSL, TLS, SSH, or any combination of them? Choose all that can apply. (C) (5%) When HTTPS is used, choose from the following elements of the communication that are encrypted: i) URL of the requested document, ii) Contents of the document, iii) Contents of TCP header, iv) Cookies sent from browser to server and from server to browser, v) Contents of HTTP header, (D) (5%) Can HTTPS prevent SQL Injection attack? Explain your answer.
2. (20%) In the SSL Handshake protocol, the following messages are exchanged between the client and the server: client_hello, server_hello, certificate, server_key_exchange, certificate request, server_hello_done, client_key_exchange, certificate_verify, change_cipher_spec, finished. CipherSpecs require a client write MAC secret, a server write MAC secret, a client write key, a server write key, a client write IV, and a server write IV which are generated from the master_secret. (A) (7%) How is master_secret derived? Give the formula that calculates master_secret. The inputs may include pre_master_secret, client_hello.random, and server_hello.random. (B) (7%) How is pre_master_secret derived? (C) (6%) How does both the client and the server know client_hello.random, and server_hello.random?
3. (20%) IEEE 802.1X Port-Based Network Access Control was designed to provide access control functions for LANs. The terms used in the IEEE 802.11standard: supplicant, network access point, and authentication server corresponding to the EAP peer, authenticator, and authentication server, respectively. Describe the operations of controlled port and uncontrolled port (A) before the supplicant is authenticated, and (B) after the supplicant is authenticated. (C) What is EAP? (D) Data in the cloud must be secured while at rest, in transit, and in use, and access to the data must be controlled. How to protect the data while data at rest, in transit, and in use, respectively?
4. (20%) (A) Given a X.509 CA hierarchy as the following figure, use the certificates listed in the figure to give a chain of certificates to show how X obtains B's public key. (B) What is OAuth?

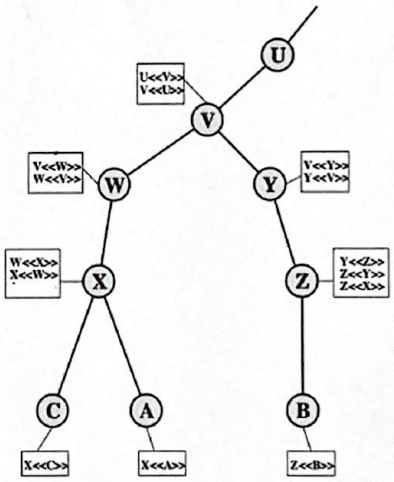

Figure 4.6 X.509 CA Hierarchy: a Hypothetical Example

5. (20%) (A) (7%) Give the Diffie-Hellman protocol. (B) (7%) Does the protocol support authentication, digital signature, key exchange, data encryption, or any combination of them? (C) (6%) Will the man-in-the-middle attack succeed against the Diffie Hellman protocol?