Auto-Evaluation Questions
(Transport Layer Security and HTTPS)

1. Consider a TCP/IP based stacks when we use TLS (or SSL), TLS or S/MIME (protectiojn of Email Messages). What are the advantages and drawbacks of each stack ?
2. What are the sub-protocols comprised in the TLS protocol stack?
3. What are the differences between TLS-session and TLS-connection? What TLS sub-protocols represent TLS-session sub-protocols and TLS-connection sub-protocols?
4. Explain briefly the security association parameters at the TLS-session state level approach?
5. Explain briefly the security association parameters at the TLS-connection state level approach?
6. What services and security properties are guaranteed in the TLS RLP sub-protocol?
7. Explain how TLS processes and protects messages sent by an application-level protocol, explaining the processing steps involved.
8. Briefly detail the different levels of awareness of connection in the HTTPS protocol.

   - - -

9. Considering the TLS sub-protocols, what sub-protocol must manage and process/validate certification chains and public-key certificates, as well as, public-key cryptographic methods?
10. From the following security properties, what property is not protected by TLS? Why?
    a. Message-Integrity
    b. Message-Confidentiality
    c. Connection-oriented confidentiality
    d. Connectionless confidentiality
    e. Connection-oriented integrity
    f. Connectionless integrity
    g. Message-Authentication
    h. Peer-Authentication
    i. Availability
11. What is the purpose of the TLS Alert sub-protocol?
12. What is the purpose of the TLS Heartbeat subprotocol?
13. Given a TLS flow (for example a flow intercepted by a tool like wireshark), how can you identify that the protocol is running with a mutual authentication setup?
14. Given a TLS flow (for example a flow intercepted by a tool like wireshark), how can you identify that the protocol is running with a client-only authentication setup?
15. Given a TLS flow (for example a flow intercepted by a tool like wireshark), how can you identify the ciphersuite selected in the end of the TLS handshake sub-protocol?
16. How can be identified in a TLS flow supporting a HTTPS connection to a web server that the web server suffer from the Heartbleed vulnerability ?
17. Considering the top ten OWASP vulnerabilities for Web Applications, which ones are related to TLS misconfigurations or TLS vulnerabilities induced by the setup of weak ciphersuites in the TLS handshake ?

18. What is the difference between a FIXED Diffie Hellman and Ephemeral Diffie-Hellman setups in the TLS protocol? What are the advantages/drawbacks of both setups?
19. To use a ECDH-ECDA ciphersuite in a mutual-authentication setup for TLS what kind of certificates must be used by the client and the server ?
20. Is it possible for the question 19 that the server and client can use a certification chain where the top level root certificate use RSA signatures? Explain.
21. In TLS, what is the endpoint that determines the chosen ciphertext for the TLS session ? The client or the server endpoint?
22. In TLS does the client know the type of public-key certificate that must be valid to be presented to the server, when mutual authentication is used? Why?
23. Why is danger the use of Anonymous Diffie-Hellman as a key-echange mode for TLS ? Explain.
24. The session key as well the Mac keys established after the TSL handshake is generated as a contributive key? Explain.
25. Is it possible to support TLS over UDP with the same security guarantees as studied for the TSL protocol? Why?
26. In TLS, in what consists a Poodle vulnerability?
27. In TLS, in what consists a BEAST vulnerability?
28. Why a vulnerability induced by PKI attacks can be a source of vulnerabilities for TLS?

- - -

29. From your analysis, why is relevant to have a separated Change Cipher Spec sub-protocol in the TLS stack, rather than including a change-cipher spec message type in the Handshake sub-protocol?
30. What is the purpose of the MAC computation during the change cipher spec TLS exchange?
31. Considering the following threats to Web Security, describe the counter-measures as features of TLS, provided to TLS-protected application-level traffic (ex., HTTPS, REST/HTTPS, etc):
    a. Brute Force Cryptoanalytic attack
    b. Known Plaintext Dictionary Attack
    c. Replay attacks
    d. Main in the Middle, interposing key-exchanges acting as the supposed client or the supposed server
    e. Password-Sniffing
    f. HTTP Basic Authentication using HTTPS/TLS
    g. IP-Spoofing with forged IP addresses to fool a host into accepting bogus data
    h. IP Hijacking, disrupting the communication between clients and servers, where the attacker (hijacker) takes the place of one of the hosts during the communication flow
    i. SYN flooding attacks for denial of TCP connections
    j. DNS-Attacks with forged DNS fully qualified names / IP mappings, for the attacker to take the place of a correct DNS name and respective public IP

mapping

32. Is it possible in TLS for a receiver to reorder TLS records (protected by the RLP sub-protocol) that can eventually arrive out-of-order? Or does the situation a consequence for the receiver to fire an Alert Message, ending the TLS established session?