Tutorial Sheet – Unit IV

Transport-Level Security and Wireless Network Security

Part A: Short Answer Questions

Transport-Level Security

1. What is Transport-Level Security?
2. What are web security considerations?
3. Define SSL.
4. Expand SSL.
5. Define TLS.
6. Expand TLS.
7. What is the purpose of SSL/TLS?
8. What is HTTPS?
9. Expand HTTPS.
10. What is an SSL certificate?
11. What is the default port number of HTTPS?
12. What is a TLS handshake?
13. What is session encryption?
14. Define Secure Shell (SSH).
15. What is the default port number of SSH?
16. What are the main services provided by SSH?
17. Differentiate between HTTP and HTTPS.
18. Differentiate between SSL and TLS.
19. What is server authentication?
20. What is certificate validation?

Wireless Network Security

21. What is wireless security?
22. Why is wireless security important?
23. What is mobile device security?
24. Define WLAN.
25. Expand IEEE 802.11.
26. What is Wi-Fi?
27. What is an access point?
28. What is SSID?
29. What is IEEE 802.11i?
30. What is WPA?
31. What is WPA2?
32. What is WPA3?
33. What is authentication in WLAN?
34. What is encryption in wireless networks?
35. What is rogue access point?

36. What is MAC filtering?
37. What is wireless eavesdropping?
38. What is wardriving?
39. What is WPA2-Enterprise?
40. What is CCMP?

Part B: Long Answer Questions

Transport-Level Security

1. Explain the need for Transport-Level Security in modern networks.
2. Discuss various web security considerations and threats.
3. Explain the architecture and operation of SSL.
4. Describe the SSL Record Protocol.
5. Explain the SSL Handshake Protocol in detail.
6. Discuss the architecture and working of TLS.
7. Compare SSL and TLS.
8. Explain the TLS handshake process with a neat diagram.
9. Describe HTTPS and its operation.
10. Explain the role of digital certificates in HTTPS.
11. Discuss the advantages and limitations of HTTPS.
12. Explain Secure Shell (SSH) architecture and services.
13. Describe SSH authentication and connection establishment.
14. Compare SSH and SSL/TLS.
15. Explain how SSL/TLS ensures confidentiality, integrity, and authentication.

Wireless Network Security

16. Explain wireless security and its challenges.
17. Discuss common wireless network attacks and countermeasures.
18. Explain mobile device security and associated threats.
19. Describe the architecture of IEEE 802.11 Wireless LAN.
20. Explain the operation of IEEE 802.11 WLAN.
21. Discuss security vulnerabilities in wireless LANs.
22. Explain IEEE 802.11i Wireless LAN Security architecture.
23. Describe the authentication mechanisms used in IEEE 802.11i.
24. Explain WPA, WPA2, and WPA3 security protocols.
25. Discuss encryption techniques used in wireless LAN security.
26. Explain the role of CCMP in IEEE 802.11i.
27. Compare WEP, WPA, WPA2, and WPA3.
28. Explain enterprise wireless security using IEEE 802.1X and RADIUS.
29. Discuss best practices for securing wireless networks.
30. Explain how wireless security differs from wired network security.

Part C: Analytical and Conceptual Questions

1. Why is HTTPS preferred over HTTP for web communication?
2. Analyze the importance of SSL/TLS in e-commerce applications.
3. Why was SSL replaced by TLS?
4. Explain how TLS prevents man-in-the-middle attacks.
5. Compare SSH and HTTPS in terms of security and applications.
6. Why are wireless networks more vulnerable than wired networks?
7. Analyze the security weaknesses of WEP.
8. Why is WPA2 considered more secure than WPA?
9. Discuss the significance of IEEE 802.11i in wireless security.
10. Analyze the security risks associated with mobile devices.
11. Why is certificate management important in HTTPS?
12. Explain the role of authentication servers in enterprise WLANs.

Part D: Problem-Solving and Application Questions

SSL/TLS and HTTPS

1. Draw and explain the SSL architecture.
2. Illustrate the SSL handshake process with a flow diagram.
3. Explain the TLS handshake sequence between a client and server.
4. Demonstrate how HTTPS secures a web transaction.
5. Explain certificate verification during an HTTPS session.
6. Draw the protocol stack for SSL/TLS and HTTPS.

SSH

7. Explain the phases of SSH protocol operation.
8. Draw and explain SSH architecture.
9. Illustrate secure remote login using SSH.

Wireless Security

10. Draw the architecture of IEEE 802.11 WLAN.
11. Explain the authentication process in WPA2.
12. Draw the IEEE 802.11i security architecture.
13. Illustrate the operation of CCMP in wireless security.
14. Explain how WPA2-Enterprise authentication works.
15. Demonstrate how a wireless network can be protected against common attacks.

Part E: Multiple Choice Questions (MCQs)

1. HTTPS operates on port:
    - A) 20
    - B) 21
    - C) 80
    - D) 443

    Answer: D

2. TLS is the successor to:
    - A) SSH
    - B) SSL
    - C) IPsec
    - D) WPA

    Answer: B

3. SSH operates on port:
    - A) 22
    - B) 23
    - C) 25
    - D) 443

    Answer: A

4. HTTPS provides:
    - A) Confidentiality
    - B) Authentication
    - C) Integrity
    - D) All of the above

    Answer: D

5. IEEE 802.11 refers to:
    - A) Ethernet
    - B) Wireless LAN
    - C) Bluetooth
    - D) Optical Network

    Answer: B

6. IEEE 802.11i is related to:
    - A) Routing
    - B) WLAN Security
    - C) Switching
    - D) VPN

Answer: B

7. WPA2 uses:
   - A) DES
   - B) RC4
   - C) AES
   - D) RSA

   Answer: C

8. The insecure predecessor of WPA is:
   - A) WPA3
   - B) AES
   - C) WEP
   - D) TLS

   Answer: C

9. CCMP is based on:
   - A) AES
   - B) DES
   - C) RC4
   - D) Blowfish

   Answer: A

10. A rogue access point is:
    - A) Authorized AP
    - B) Unauthorized AP
    - C) Secure AP
    - D) VPN Server

    Answer: B

Part F: Assignment Questions

1. Study the evolution from SSL to TLS and prepare a comparative report.
2. Analyze the role of HTTPS in securing e-commerce transactions.
3. Study the SSH protocol and its applications in network administration.
4. Investigate common web security threats and their mitigation techniques.
5. Compare HTTP, HTTPS, SSL, TLS, and SSH.
6. Analyze the security weaknesses of WEP and improvements introduced in WPA2.
7. Study IEEE 802.11 WLAN architecture and prepare a report.
8. Compare WPA, WPA2, and WPA3 security mechanisms.

9. Investigate mobile device security threats and countermeasures.
10. Study IEEE 802.11i and explain its role in wireless LAN security.

Viva Questions

1. What is SSL?
2. What is TLS?
3. What is HTTPS?
4. What is the default port number of HTTPS?
5. What is the purpose of SSL/TLS?
6. What is SSH?
7. What is the default port number of SSH?
8. What is an SSL certificate?
9. What is a WLAN?
10. What is IEEE 802.11?
11. What is IEEE 802.11i?
12. What is WPA2?
13. What is WPA3?
14. What is CCMP?
15. What is an Access Point?
16. What is SSID?
17. What is wireless security?
18. What is a rogue access point?
19. What is mobile device security?
20. Why is HTTPS more secure than HTTP?

Important University Exam Questions (Frequently Asked)

10-Mark Questions

1. Explain SSL architecture and handshake protocol.
2. Discuss TLS architecture and operation.
3. Explain HTTPS and the role of digital certificates.
4. Describe SSH architecture and services.
5. Explain web security considerations and threats.
6. Discuss wireless security challenges and countermeasures.
7. Explain IEEE 802.11 WLAN architecture and operation.
8. Describe IEEE 802.11i Wireless LAN Security.
9. Compare WEP, WPA, WPA2, and WPA3.
10. Explain mobile device security and wireless network protection mechanisms.

5-Mark Questions

1. Compare SSL and TLS.
2. Explain HTTPS operation.
3. Explain SSH services.
4. Describe WLAN architecture.
5. Explain WPA2 security features.
6. Discuss wireless network threats.

This tutorial sheet covers the complete **Unit IV syllabus** with **2-mark, 5-mark, 8-mark, and 10-mark examination-oriented questions**, MCQs, assignments, viva questions, and important university exam questions.