Transport-Layer Security Exam Questions

Table of Contents

Multiple Choice Questions (MCQs)

TCP/UDP Fundamentals

1. Which of the following is NOT a characteristic of TCP? a) Connection-oriented b) Reliable delivery c) Low latency d) Ordered delivery

2. In TCP, what is the purpose of the sequence number field? a) To identify the destination port b) To indicate the index of the first byte in the segment c) To specify the protocol version d) To control flow rate

3. UDP is preferred over TCP for which type of application? a) File transfers b) Email communication c) Online gaming d) Web browsing

4. What is the size of the UDP header? a) 20 bytes b) 8 bytes c) 12 bytes d) 16 bytes

5. Which attack exploits the TCP three-way handshake process? a) UDP amplification attack b) SYN flooding attack c) Man-in-the-middle attack d) Buffer overflow attack

TLS Protocol

6. What is the correct order of the first three messages in a TLS 1.2 handshake? a) ClientHello → ServerHello → Certificate b) ClientHello → Certificate → ServerHello c) ServerHello → ClientHello → Certificate d) Certificate → ClientHello → ServerHello

7. Which TLS protocol component is responsible for encrypting application data? a) Handshake Protocol b) Alert Protocol c) Record Protocol d) Change Cipher Spec Protocol

8. What is the purpose of the Change Cipher Spec Protocol? a) To negotiate cipher suites b) To signal transition to new encryption settings c) To handle error messages d) To authenticate the server

9. In TLS key generation, what comes first in the process? a) Master secret b) Shared keys c) Pre-master secret d) Session keys

10. HTTPS uses which port number? a) 80 b) 443 c) 22 d) 25

DTLS Protocol

11. What is the main reason DTLS includes a HelloVerifyRequest message? a) To improve encryption strength b) To prevent DoS attacks c) To reduce latency d) To ensure packet ordering

12. Which characteristic of UDP makes it challenging to implement TLS directly over it? a) High bandwidth usage b) Complex header structure c) Unreliable transmission d) Limited port numbers

13. In DTLS, what must the client include in its second ClientHello message? a) Certificate b) Cookie c) Sequence number d) Timestamp

QUIC Protocol

14. Which company originally developed QUIC? a) Microsoft b) Apple c) Google d) Mozilla

15. What problem does QUIC solve that TCP+TLS cannot? a) Encryption strength b) Head-of-line blocking c) Certificate validation d) Port allocation

16. In the protocol comparison matrix, which combination of features does QUIC achieve? a) Reliable + Fast + Secure b) Reliable + Secure only c) Fast + Secure only d) Fast only

17. What is a potential disadvantage of QUIC mentioned in the material? a) Poor encryption b) DoS vulnerability in ClientHello c) Slow handshake process d) Limited platform support

Attack Vectors

18. In a UDP amplification attack, what does the attacker spoof? a) The destination port b) The packet size c) The source IP address d) The protocol version

19. Which mitigation technique prevents TCP SYN flooding by not allocating resources immediately? a) TCP filtering b) SYN cookies c) Rate limiting d) Packet inspection

20. What was the peak traffic volume of the 2018 Memcached DDoS attack? a) 1.3 Tbps b) 1.7 Tbps c) 2.1 Tbps d) 2.5 Tbps

---

Short Answer Questions (SAQs)

TCP/UDP Concepts

21. Explain the three-way handshake process in TCP. What happens if the final ACK is not received?

22. List four key differences between TCP and UDP protocols.

23. Describe how data segmentation works when a packet exceeds the Maximum Transmission Unit (MTU).

24. What is the purpose of port numbers in TCP/UDP communication? Provide an example.

TLS Security

25. Explain the role of each of the four main TLS protocols (Handshake, Record, Alert, Change Cipher Spec).

26. What information is included in a TLS cipher suite? Provide an example and break down its components.

27. Describe the key generation process in TLS, starting from pre-master secret to final shared keys.

28. Why is the Finished message in TLS sent encrypted rather than in plaintext?

DTLS Implementation

29. Explain why TLS cannot be directly implemented over UDP and what modifications DTLS makes.

30. What is the purpose of the cookie mechanism in DTLS? How does it work?

31. Describe three specific challenges that DTLS must address due to UDP's characteristics.

QUIC Innovation

32. How does QUIC solve the head-of-line blocking problem present in TCP?

33. What is meant by "early data transmission" in QUIC and why is it beneficial?

34. Explain how QUIC achieves both reliability and speed simultaneously.

Security Attacks

35. Describe the step-by-step process of a UDP amplification attack.

36. What is a SYN flood attack and how do SYN cookies mitigate it?

37. List three mitigation strategies for UDP amplification attacks from the victim's perspective.

Evaluation Questions

Protocol Assessment

38. Evaluate the trade-offs between using TCP and UDP for a real-time video streaming application. Consider latency, reliability, and user experience in your assessment.

39. Assess the security implications of using HTTPS vs HTTP for an e-commerce website. What specific threats does TLS protect against?

40. Evaluate the effectiveness of the cookie mechanism in DTLS for preventing DoS attacks. What are its limitations?

41. Analyze the performance overhead introduced by TLS in web applications. Is the security benefit worth the cost?

Design Evaluation

42. A company is experiencing frequent TCP SYN flood attacks on their web servers. Evaluate the effectiveness of implementing SYN cookies vs. increasing server resources. Which approach would you recommend and why?

43. Evaluate the decision to develop QUIC as a new protocol rather than improving existing TCP+TLS implementations. Was this the right approach?

44. Assess the vulnerability of QUIC to DoS attacks through ClientHello flooding. How serious is this threat compared to TCP SYN flooding?

Implementation Evaluation

45. Evaluate the challenges a developer would face when implementing a secure chat application using DTLS vs. TLS. Consider both technical and practical aspects.

46. Analyze the certificate management burden in TLS implementations. How does this affect small businesses vs. large enterprises?

47. Evaluate the claim that QUIC provides the "best of all worlds" (reliable, fast, secure). Are there any significant compromises?

Comparison Questions

Protocol Comparisons

48. Compare and contrast TCP and UDP in terms of:

- Connection establishment
- Reliability mechanisms
- Performance characteristics
- Suitable applications
- Header overhead

49. Create a detailed comparison between TLS and DTLS covering:

- Handshake process differences
- Security features
- Performance implications
- Attack vectors and mitigations
- Use case scenarios

50. Compare the evolution from TCP+TLS to QUIC. What specific problems did QUIC solve that the previous combination couldn't address?

Security Comparisons

51. Compare SYN flooding attacks and UDP amplification attacks in terms of:

- Attack mechanism
- Resource requirements for attacker
- Impact on victim
- Detection methods
- Mitigation strategies

52. Compare the security models of TLS 1.2 and TLS 1.3. What improvements were made in the newer version?

Performance Comparisons

53. Compare the handshake efficiency between:

- TCP three-way handshake
- TLS 1.2 handshake
- DTLS handshake
- QUIC handshake

54. Create a performance comparison matrix for all discussed protocols (TCP, UDP, TLS, DTLS, QUIC) across these dimensions:

- Latency
- Throughput
- CPU overhead
- Memory usage
- Network efficiency

Application Comparisons

55. Compare the suitability of different protocols for these applications:

- Web browsing
- Video conferencing
- File downloads
- Online gaming
- IoT sensor data transmission

Recommendation Questions

Protocol Selection

56. A startup is developing a multiplayer online game that requires real-time communication between players. The game will handle player positions, chat messages, and game state updates. Recommend the most appropriate protocol(s) and justify your choice.

57. A financial services company needs to implement secure communication for their trading platform that processes thousands of transactions per second. Time is critical, but security cannot be compromised. What protocol would you recommend and why?

58. A healthcare organization wants to implement a telemedicine platform that includes video calls, file sharing, and patient data transmission. Recommend a communication architecture considering both security and performance requirements.

Security Implementation

59. A small e-commerce website is experiencing both TCP SYN flood and UDP amplification attacks. The company has limited resources. Recommend a comprehensive defense strategy prioritizing the most critical protections.

60. A company is migrating from HTTP to HTTPS for their public website. They're concerned about performance impact and certificate costs. Provide recommendations for a smooth transition while maintaining security.

Architecture Design

61. A social media platform wants to implement real-time messaging that works across web browsers, mobile apps, and desktop applications. They need to handle millions of concurrent users. Recommend a protocol architecture and explain your reasoning.

62. A gaming company is designing a new cloud gaming service where video streams and control inputs must have minimal latency. Security is important but cannot impact performance. What protocol stack would you recommend?

63. An IoT company is developing smart home devices that need to communicate securely with a central hub. The devices have limited processing power and battery life. Recommend appropriate protocols for different types of communication (sensor data, control commands, firmware updates).

Migration Strategy

64. A legacy application currently uses plain TCP for communication between distributed components. The company wants to add security without major architectural changes. Recommend a migration strategy considering minimal disruption and maximum security benefit.

65. A video streaming service currently uses TCP for content delivery but is experiencing quality issues during peak hours. They're considering QUIC implementation. Recommend a migration plan including testing strategy and rollback procedures.

Industry-Specific Recommendations

66. A autonomous vehicle manufacturer needs to implement secure communication between vehicles and infrastructure. The system must handle safety-critical messages, traffic updates, and entertainment content. Recommend a comprehensive communication protocol strategy.

67. A cryptocurrency exchange needs to implement secure, high-frequency trading capabilities. They require microsecond latency for market data and millisecond latency for order execution. Recommend a protocol architecture that balances speed and security.

68. A remote surgery system requires ultra-low latency communication between surgical instruments and control systems, with zero tolerance for data loss or security breaches. Recommend a communication protocol and explain your security considerations.

Answer Key

MCQ Answers

1. c) Low latency
2. b) To indicate the index of the first byte in the segment
3. c) Online gaming
4. b) 8 bytes
5. b) SYN flooding attack
6. a) ClientHello → ServerHello → Certificate
7. c) Record Protocol
8. b) To signal transition to new encryption settings
9. c) Pre-master secret
10. b) 443
11. b) To prevent DoS attacks
12. c) Unreliable transmission
13. b) Cookie
14. c) Google
15. b) Head-of-line blocking
16. a) Reliable + Fast + Secure
17. b) DoS vulnerability in ClientHello
18. c) The source IP address
19. b) SYN cookies
20. b) 1.7 Tbps

SAQ Key Points

21. TCP Three-Way Handshake:

- Step 1: Client sends SYN
- Step 2: Server responds with SYN-ACK
- Step 3: Client sends ACK
- If final ACK not received: Server times out and closes connection

22. TCP vs UDP Differences:

- Connection: TCP is connection-oriented, UDP is connectionless
- Reliability: TCP guarantees delivery, UDP doesn't
- Ordering: TCP ensures order, UDP doesn't
- Speed: UDP is faster, TCP has more overhead

23. Data Segmentation:

- Large data broken into smaller segments
- Each segment fits within MTU
- Receiving computer reassembles segments
- Sequence numbers ensure proper ordering

24. Port Numbers:

- Identify specific applications within a computer
- Act as addresses for application-to-application communication
- Example: Web server typically uses port 80 (HTTP) or 443 (HTTPS)

Evaluation Question Guidelines

38. Video Streaming Assessment:

- TCP: Reliable but introduces latency through retransmissions
- UDP: Fast but may lose packets affecting quality
- Recommendation: UDP for live streaming, TCP for on-demand
- Consider hybrid approaches and error correction

39. HTTPS vs HTTP Security:

- HTTPS protects against: eavesdropping, tampering, impersonation
- Encrypts: URLs, headers, content, cookies
- Trade-off: Security vs. performance overhead
- Essential for e-commerce due to sensitive data

40. DTLS Cookie Mechanism:

- Effective against basic DoS attacks
- Limitations: Can be bypassed with IP spoofing
- Doesn't prevent all types of DoS attacks

- Balances security and performance

Comparison Question Guidelines

48. TCP vs UDP Comparison: Focus on fundamental differences in design philosophy, use cases, and performance characteristics.

49. TLS vs DTLS Comparison: Emphasize the cookie mechanism, reliability handling, and application scenarios.

50. TCP+TLS to QUIC Evolution: Highlight head-of-line blocking solution, integrated security, and performance improvements.

Recommendation Question Guidelines

56. Gaming Protocol Recommendation:

- Recommend UDP for real-time updates (positions, actions)
- TCP for reliable data (chat, game state)
- Consider QUIC for modern implementations
- Justify based on latency requirements

57. Financial Trading Platform:

- Recommend QUIC for optimal balance
- Justify security requirements
- Consider regulatory compliance
- Address performance criticality

58. Telemedicine Platform:

- QUIC for video calls (low latency + security)
- TLS for file transfers (reliability + security)
- Consider different protocols for different functions
- Address healthcare compliance requirements