CSCI368 Network Security - Question Bank & Study Material

Multiple Choice Questions (MCQs)

Topic 1: Introduction & Cryptography Basics

1. Which of the following is NOT one of the fundamental security requirements? a) Confidentiality b) Integrity c) Authenticity d) Efficiency

Answer: d) Efficiency

2. A passive attack that involves monitoring communications to extract information is called: a) Masquerade b) Eavesdropping c) Denial of Service d) Message modification

Answer: b) Eavesdropping

3. Which cryptographic system uses the same key for both encryption and decryption? a) Asymmetric cryptography b) Public key cryptography c) Symmetric cryptography d) Hash functions

Answer: c) Symmetric cryptography

4. The security issue that represents an attack on availability is: a) Interception b) Modification c) Fabrication d) Interruption

Answer: d) Interruption

5. Which of the following is an example of an asymmetric cryptographic algorithm? a) AES b) DES c) RSA d) RC4

Answer: c) RSA

Topic 2: Public Key Infrastructure

6. In a PKI system, what is the primary role of a Certificate Authority (CA)? a) Encrypt messages b) Issue and manage digital certificates c) Store private keys d) Authenticate users directly

Answer: b) Issue and manage digital certificates

7. X.509 certificates contain all of the following EXCEPT: a) Subject's public key b) Subject's private key c) Issuer information d) Validity period

Answer: b) Subject's private key

8. In a hierarchical trust model, trust is established through: a) Peer-to-peer relationships b) A tree structure with a root CA c) Direct user validation d) Distributed consensus

Answer: b) A tree structure with a root CA

Topic 3: Email Security

9. Which email security standard uses the web of trust model? a) S/MIME b) PGP c) SMTP d) IMAP

Answer: b) PGP

10. S/MIME differs from PGP primarily in its: a) Encryption algorithms b) Trust model c) Message format d) Key size

Answer: b) Trust model

Topic 4: Authentication & Key Establishment

11. The Diffie-Hellman key exchange is vulnerable to which type of attack? a) Brute force b) Man-in-the-middle c) Replay d) Dictionary

Answer: b) Man-in-the-middle

12. Perfect Forward Secrecy ensures that: a) Keys are never compromised b) Past sessions remain secure even if long-term keys are compromised c) Future sessions are always secure d) All communications are encrypted

Answer: b) Past sessions remain secure even if long-term keys are compromised

Topic 5: Kerberos

13. In Kerberos, what does the client receive from the Authentication Server (AS)? a) Service ticket b) Session key c) Ticket Granting Ticket (TGT) d) Server's public key

Answer: c) Ticket Granting Ticket (TGT)

14. Kerberos prevents replay attacks by using: a) Encrypted passwords b) Time stamps c) Digital signatures d) Public key cryptography

Answer: b) Time stamps

Topic 6: IPSec & IKE

15. Which IPSec protocol provides only authentication and integrity (no confidentiality)? a) ESP b) AH c) IKE d) ISAKMP

Answer: b) AH

16. In IPSec tunnel mode: a) Only the payload is protected b) The entire IP packet is protected c) Only the headers are protected d) No protection is provided

Answer: b) The entire IP packet is protected

Topic 7: SSL/TLS & SSH

17. The TLS handshake process includes all of the following steps EXCEPT: a) Client Hello b) Server Hello c) Key Distribution d) Certificate Exchange

Answer: c) Key Distribution

18. SSH was designed to replace which insecure protocols? a) HTTP and HTTPS b) FTP and SFTP c) Telnet and rlogin d) SMTP and POP3

Answer: c) Telnet and rlogin

Topic 8: Wireless & Mobile Security

19. Which Wi-Fi security protocol is considered obsolete and should not be used? a) WPA b) WPA2 c) WPA3 d) WEP

Answer: d) WEP

20. WPA2 uses which encryption algorithm? a) RC4 b) AES c) DES d) TKIP

Answer: b) AES

Short Answer Questions (SAQs)

Topic 1: Fundamentals

1. Define the four fundamental security requirements and provide a brief example of each.

Answer:

- **Confidentiality**: Information accessible only by authorized parties (e.g., encrypted email)
- **Integrity**: Protection from unauthorized modification (e.g., digital signatures on documents)
- **Authenticity**: Assurance of message origin (e.g., certificate-based authentication)
- **Availability**: Information accessible when needed (e.g., redundant systems to prevent DoS)

2. Explain the difference between active and passive attacks, providing two examples of each.

Answer: Passive Attacks (no modification of data):

- Eavesdropping: Monitoring communications to extract information
- Traffic analysis: Analyzing communication patterns to infer relationships

Active Attacks (modification or disruption):

- Masquerade: Impersonating another entity
- Message modification: Altering transmitted data
- Denial of Service: Preventing legitimate access to resources

3. Describe the abstract communication model for secure communication.

Answer: The model includes:

- **Sender and Receiver**: Communicating parties
- **Security Transformations**: Encryption/decryption, signing/verification
- **Information Channel**: Potentially insecure communication medium
- **Keys**: Shared secrets for cryptographic operations
- **Opponent**: Potential attacker monitoring or manipulating communications
- **Trusted Third Party**: Entity that assists in key distribution or authentication

Topic 2: PKI

4. Explain the components of a Public Key Infrastructure and their roles.

Answer:

- **Certificate Authority (CA)**: Issues, manages, and revokes digital certificates
- **Registration Authority (RA)**: Verifies identity of certificate requesters
- **Digital Certificates**: Bind public keys to entities with CA's digital signature
- **Certificate Repository**: Stores and distributes certificates
- **Certificate Revocation Lists (CRL)**: Lists certificates that have been revoked

5. Compare hierarchical and web of trust models.

Answer: Hierarchical Model:

- Tree structure with root CA at top
- Centralized trust authority
- Easier to manage and validate
- Single point of failure

Web of Trust Model:

- Peer-to-peer trust relationships

- Decentralized trust establishment
- More resilient but complex
- Users validate each other's keys

Topic 3: Email Security

6. Explain how PGP achieves both confidentiality and authentication.

Answer: Confidentiality:

- Uses hybrid cryptosystem
- Generates random symmetric key for message encryption
- Encrypts symmetric key with recipient's public key

Authentication:

- Sender signs message with private key
- Recipient verifies signature with sender's public key
- Ensures message origin and integrity

7. What are the main differences between PGP and S/MIME?

Answer: PGP:

- Web of trust model
- Not tied to specific certificate authority
- Uses its own message format
- More flexible but less standardized

S/MIME:

- Hierarchical PKI model
- Relies on Certificate Authorities
- MIME-based standard format
- Better integration with email systems

Topic 4: Authentication & Key Establishment

8. Describe the Diffie-Hellman key exchange process and its main vulnerability.

Answer: Process:

1. Parties agree on public parameters (p, g)
2. Each party generates private key and computes public value
3. Parties exchange public values
4. Each computes shared secret using own private key and other's public value

Main Vulnerability:

- Susceptible to man-in-the-middle attacks
- No authentication of communicating parties
- Attacker can establish separate keys with each party

9. What is Perfect Forward Secrecy and why is it important?

Answer: Perfect Forward Secrecy ensures that compromise of long-term keys doesn't affect the security of past communication sessions. It's important because:

- Protects historical communications
- Limits damage from key compromise
- Uses ephemeral keys for each session
- Common in modern protocols like TLS 1.3

Topic 5: Kerberos

10. Explain the three-step Kerberos authentication process.

Answer: Step 1 - AS Exchange:

- Client requests Ticket Granting Ticket (TGT) from AS
- AS verifies client credentials and issues TGT

Step 2 - TGS Exchange:

- Client presents TGT to TGS to request service ticket
- TGS validates TGT and issues service ticket

Step 3 - Client-Server Exchange:

- Client presents service ticket to target server
- Server validates ticket and provides service

11. What security features does Kerberos provide?

Answer:

- **Mutual Authentication**: Both client and server verify each other
- **Single Sign-On**: One login provides access to multiple services
- **Ticket-based Access Control**: Time-limited access tokens
- **Replay Attack Prevention**: Using timestamps and sequence numbers
- **No Password Transmission**: Passwords never sent over network

Topic 6: IPSec

12. Compare IPSec AH and ESP protocols.

Answer: Authentication Header (AH):

- Provides authentication and integrity only
- No confidentiality (no encryption)
- Protects entire IP packet (in tunnel mode)
- Cannot work with NAT

Encapsulating Security Payload (ESP):

- Provides confidentiality, authentication, and integrity
- Encrypts payload data
- Can work in transport or tunnel mode
- More comprehensive protection

13. Explain the difference between IPSec transport and tunnel modes.

Answer: Transport Mode:

- Protects only the payload of IP packet
- Original IP headers remain unchanged
- Used for end-to-end communication
- More efficient but less secure

Tunnel Mode:

- Protects entire IP packet (header + payload)
- Creates new IP header for transmission
- Used for VPN connections

- More secure but higher overhead

Topic 7: SSL/TLS

14. Outline the key steps in the TLS handshake process.

Answer:

1. **Client Hello**: Client initiates connection, sends supported cipher suites
2. **Server Hello**: Server responds with chosen cipher suite and certificate
3. **Certificate Verification**: Client validates server certificate
4. **Key Exchange**: Establish pre-master secret using server's public key
5. **Finished Messages**: Both parties confirm handshake completion
6. **Secure Communication**: Begin encrypted data exchange

15. How does SSH provide secure remote access?

Answer:

- **Public Key Authentication**: Uses key pairs for user authentication
- **Encrypted Communication**: All data encrypted using symmetric keys
- **Integrity Protection**: Prevents tampering with transmitted data
- **Server Authentication**: Prevents man-in-the-middle attacks
- **Multiple Authentication Methods**: Supports password, public key, and other methods

Topic 8: Wireless Security

16. Explain the evolution of Wi-Fi security from WEP to WPA3.

Answer: WEP (Wired Equivalent Privacy):

- Used RC4 encryption with static keys
- Severe vulnerabilities (weak IV, key recovery attacks)
- Deprecated due to easy cracking

WPA (Wi-Fi Protected Access):

- Introduced TKIP for better key management
- Improved but still had vulnerabilities
- Interim solution while WPA2 was developed

WPA2:

- Uses AES encryption with CCMP
- Much stronger security than WEP/WPA
- Current standard for most networks

WPA3:

- Enhanced encryption and authentication
- Protection against offline attacks
- Improved security for open networks

17. What are the unique security challenges in wireless networks?

Answer:

- **Broadcast Medium**: Easier to intercept communications
- **Mobility**: Devices move between different security domains
- **Resource Constraints**: Limited processing power and battery
- **Physical Security**: Harder to control physical access
- **Interference**: Potential for jamming and disruption

Evaluation, Comparison, and Recommendation Questions

Question 1: Protocol Security Analysis

Scenario: A large corporation needs to secure communications between its headquarters and three branch offices. The company handles sensitive financial data and requires strong authentication, confidentiality, and integrity.

Evaluate and compare the following solutions: a) Site-to-site VPN using IPSec b) SSL/TLS-based application-level security c) Kerberos-based authentication with encrypted channels

Recommendation: Provide your recommendation with justification.

Sample Answer:

IPSec Site-to-Site VPN:

- **Strengths**: Network-layer security, transparent to applications, strong encryption, mutual authentication

- **Weaknesses**: Complex configuration, potential NAT issues, requires dedicated infrastructure
- **Suitability**: Excellent for securing all traffic between sites

SSL/TLS Application-Level Security:

- **Strengths**: Widely supported, works through firewalls/NAT, per-application control
- **Weaknesses**: Requires application modification, doesn't protect all traffic, endpoint dependency
- **Suitability**: Good for specific applications but not comprehensive

Kerberos with Encrypted Channels:

- **Strengths**: Centralized authentication, single sign-on, strong authentication
- **Weaknesses**: Single point of failure, time synchronization requirements, complex deployment
- **Suitability**: Excellent for authentication but needs additional encryption

Recommendation: Implement IPSec site-to-site VPN as the primary solution because:

- Provides comprehensive protection for all inter-site traffic
- Offers strong authentication and encryption
- Transparent to applications
- Suitable for financial data protection requirements
- Can be combined with Kerberos for enhanced authentication

Question 2: Email Security Evaluation

Scenario: A healthcare organization needs to secure email communications containing patient information to comply with privacy regulations.

Compare PGP and S/MIME for this use case. Consider:

- Ease of deployment and management
- Integration with existing email infrastructure
- Compliance requirements
- User experience
- Security features

Provide your recommendation with justification.

Sample Answer:

PGP Analysis:

- **Deployment**: More complex, requires user training on key management
- **Integration**: Limited integration with standard email clients
- **Compliance**: Provides required encryption but auditing is challenging
- **User Experience**: Steeper learning curve, manual key management
- **Security**: Strong encryption, web of trust model

S/MIME Analysis:

- **Deployment**: Easier with existing PKI infrastructure
- **Integration**: Native support in most email clients
- **Compliance**: Better audit trails, centralized management
- **User Experience**: More transparent, automatic certificate handling
- **Security**: Strong encryption, hierarchical trust model

Recommendation: S/MIME is recommended for healthcare organizations because:

- **Compliance**: Better audit trails and centralized management support regulatory requirements
- **Integration**: Native email client support reduces deployment complexity
- **Management**: PKI infrastructure provides centralized certificate management
- **User Experience**: Transparent operation increases user adoption
- **Security**: Adequate encryption strength for healthcare data protection

Question 3: Wireless Security Assessment

Scenario: A university is upgrading its campus wireless network. The network must support:

- Students with personal devices
- Faculty with university-issued laptops
- Guest access for visitors
- IoT devices for building automation

Evaluate the security implications and recommend an appropriate wireless security strategy.

Sample Answer:

Security Challenges:

- **Diverse Device Types**: Different security capabilities and requirements
- **Multiple User Categories**: Students, faculty, guests with different trust levels

- **IoT Devices**: Limited security features, potential vulnerabilities
- **Physical Access**: Open campus environment increases attack surface

Recommended Strategy:

1. Network Segmentation:

- Separate SSIDs for different user categories
- VLAN isolation between network segments
- Firewall rules between segments

2. Authentication Framework:

- **WPA3-Enterprise** for faculty and staff
- **WPA3-Personal** for students with strong pre-shared keys
- **Captive portal** for guest access with time limitations
- **Certificate-based authentication** for IoT devices

3. Additional Security Measures:

- **802.1X authentication** for enterprise users
- **MAC address filtering** for IoT devices
- **Regular security audits** and penetration testing
- **Intrusion detection systems** for wireless networks

4. Management and Monitoring:

- Centralized wireless controller
- Real-time monitoring and alerting
- Regular firmware updates
- User education programs

Justification: This multi-layered approach provides appropriate security for each user category while maintaining usability and supporting diverse device types.

Question 4: Authentication System Comparison

Scenario: A multinational corporation with 10,000 employees across 50 locations needs to implement a centralized authentication system.

Compare and evaluate: a) Kerberos-based authentication b) LDAP with SSL/TLS c) SAML-based federated authentication

Consider scalability, security, interoperability, and management overhead.

Sample Answer:

Kerberos Analysis:

- **Scalability**: Good for large organizations, realm-based architecture
- **Security**: Strong authentication, ticket-based access control
- **Interoperability**: Limited cross-platform support, time synchronization issues
- **Management**: Complex initial setup, ongoing maintenance required

LDAP with SSL/TLS:

- **Scalability**: Excellent scaling capabilities, distributed architecture
- **Security**: Good with proper SSL/TLS implementation
- **Interoperability**: Excellent cross-platform support
- **Management**: Simpler to implement and maintain

SAML Federated Authentication:

- **Scalability**: Excellent for geographically distributed organizations
- **Security**: Strong security with proper implementation
- **Interoperability**: Excellent, web-based standard
- **Management**: Moderate complexity, requires identity provider setup

Recommendation: Implement a hybrid approach:

- **Primary**: SAML-based federated authentication for web applications and cloud services
- **Secondary**: LDAP with SSL/TLS for internal directory services
- **Consideration**: Kerberos for specific high-security applications

Justification:

- Addresses multinational distribution requirements
- Provides flexibility for different application types
- Balances security with usability
- Supports modern cloud and web applications

Question 5: Network Security Architecture Design

Scenario: A financial services company is designing a new network security architecture. The company processes credit card transactions and must comply with PCI DSS requirements.

Design a comprehensive security architecture that includes:

- Network segmentation strategy
- Encryption requirements
- Authentication mechanisms
- Monitoring and auditing

Evaluate the security trade-offs and provide recommendations.

Sample Answer:

Network Segmentation Strategy:

- **DMZ**: Web servers and application gateways
- **Internal Network**: Employee workstations and internal services
- **Payment Processing Zone**: Isolated network for card data processing
- **Management Network**: Separate network for security management

Encryption Requirements:

- **Data in Transit**: TLS 1.3 for all external communications, IPSec for internal communications
- **Data at Rest**: AES-256 encryption for databases and file storage
- **Key Management**: Hardware Security Modules (HSMs) for key protection

Authentication Mechanisms:

- **Multi-factor Authentication**: Required for all administrative access
- **Certificate-based Authentication**: For system-to-system communications
- **Strong Password Policies**: Regular rotation and complexity requirements
- **Privileged Access Management**: Just-in-time access for administrative tasks

Monitoring and Auditing:

- **SIEM System**: Centralized log collection and analysis
- **Network Monitoring**: Real-time traffic analysis and anomaly detection
- **File Integrity Monitoring**: Detection of unauthorized changes

- **Regular Penetration Testing**: Quarterly security assessments

Security Trade-offs:

- **Security vs. Performance**: Encryption adds latency but necessary for compliance
- **Security vs. Usability**: Strong authentication may impact user experience
- **Security vs. Cost**: HSMs and monitoring systems require significant investment

Recommendation: Implement the comprehensive architecture with phased deployment:

1. **Phase 1**: Basic network segmentation and encryption
2. **Phase 2**: Advanced authentication and monitoring
3. **Phase 3**: Full compliance and optimization

This approach balances security requirements with operational feasibility while ensuring PCI DSS compliance.

Practice Questions for Self-Assessment

Quick Review Questions

1. What are the four types of security issues in network communications?
2. How does symmetric encryption differ from asymmetric encryption?
3. What is the purpose of a Certificate Revocation List (CRL)?
4. Why is Kerberos considered a trusted third-party authentication system?
5. What is the main advantage of IPSec tunnel mode over transport mode?
6. How does TLS ensure both confidentiality and integrity?
7. What makes WPA3 more secure than WPA2?
8. What is the difference between authentication and authorization?
9. How does Perfect Forward Secrecy protect against key compromise?
10. Why is network segmentation important in security architecture?

Critical Thinking Questions

1. Analyze the security implications of using public Wi-Fi for business communications.
2. Evaluate the effectiveness of multi-factor authentication in preventing unauthorized access.
3. Compare the security models of centralized vs. decentralized authentication systems.
4. Assess the impact of quantum computing on current cryptographic systems.

5. Design a security strategy for a small business transitioning to cloud services.

Exam Strategy Tips

Time Management

- **MCQs**: 1-2 minutes per question
- **SAQs**: 5-10 minutes per question
- **Long Questions**: 15-20 minutes per question
- **Review**: Leave 10-15 minutes for final review

Answer Strategies

- **MCQs**: Eliminate obviously wrong answers first
- **SAQs**: Structure answers with clear points
- **Long Questions**: Use diagrams where appropriate
- **Technical Terms**: Define key terms in your answers

Common Pitfalls to Avoid

- Don't confuse security properties (confidentiality vs. integrity)
- Remember the differences between similar protocols (SSL vs. TLS)
- Pay attention to specific protocol details (AH vs. ESP in IPSec)
- Consider practical implementation challenges in evaluation questions