CS 454/654 Reliability and Security of Computing Systems

Final Exam Study Guide

---

1. Digital Signatures

- **Universal Forgery**: Understand how an attacker can forge a valid signature for any message without prior knowledge of the signature.
- **Selective Forgery**: Learn how an attacker can forge a valid signature for a specific message selected by the attacker.
- **Known Message Attack**: Study how attackers use known signed messages to discover weaknesses.
- **Direct Chosen Message Attack**: Understand how attackers gain access to a signing oracle to generate signatures for chosen messages.

Authenticity of University Web Applications:

- Methods to ensure secure data transmission and validation.
- Use of certificates and secure communication protocols.

2. Other Public Key Cryptosystems

Elliptic Curve Cryptography (ECC):

- Learn how ECC generates private and public keys using global parameters like the base point and prime modulus.

3. Message Authentication Codes

- **Hash-based Message Authentication Code (HMAC)**:
  - Study its structure using a cryptographic hash function combined with a secret key.
  - Understand its role in verifying both the integrity and authenticity of messages.
- **Cipher-based Message Authentication Code (CMAC)**:
  - Learn its structure using a block cipher instead of a hash function.

4. Cryptographic Key Management and Distribution

Certificate Revocation:

- Know the reasons for certificate revocation (e.g., private key compromise, CA compromise, or certificate expiration).

Public Announcements vs. Public Key Certificates:

- Understand how public announcements and certificates ensure authenticity and reliability.

- Compare the use of digital signatures in public key certificates to validate public keys.

5. TLS and SSH

TLS Session vs. TLS Connection:

- Differentiate between a session (stateful communication setup) and a connection (a single secure transmission within a session).

TLS Handshake:

- Review each step of the TLS handshake, including key exchange, authentication, and session key generation.
- Learn the purpose of messages like "ClientHello," "ServerHello," and "Finished."

TLS Pseudo-Random Function (PRF):

- Study how PRF generates secure keys using hash functions and shared secrets.

SSH User Authentication:

- Understand the message types:
  - **Authentication Request**: User sends credentials to the server.
  - **Authentication Failure**: Server denies authentication, requesting additional credentials.
  - **Authentication Success**: Server accepts the user and grants access.

6. IPSec

Security Associations and Databases:

- Understand the purpose of the Security Association (SA) in establishing shared security parameters.
- Learn the roles of the Security Association Database (SAD) and Security Policy Database (SPD).

Outbound Packet Processing:

- Review how IPSec applies the appropriate security policies to outgoing packets, including encryption and authentication.

7. IoT Ecosystem

- **Unique Characteristics**:
  - Learn about key attributes like heterogeneity, scalability, and resource constraints.
  - Understand the challenges in securing IoT devices and communication.

Good luck with your preparation!