
Network Security: Private Communication in a Non-Private World

Chapter 1: Introduction

- **Secure communication**: Focus on how to communicate securely over insecure mediums.
- **Disclaimer**: Authors' opinions may not reflect their employers. Mentions of commercial products are for information only.
- **Design insights**: Offers insights that go beyond basic specifications.

Chapter 2: Introduction to Cryptography

- **Purpose**: Cryptography ensures:
    - **Confidentiality** (keeping communication private).
    - **Integrity** (ensuring messages are unaltered).
    - **Authentication** (verifying identity).
- **Types of Cryptographic Functions**:
    - **Hash functions**: Produce fixed-length outputs, hard to reverse.
    - **Secret key functions**: Same key for encryption and decryption.
    - **Public key functions**: Uses separate keys for encryption (public) and decryption (private); also supports digital signatures.
- **Cryptographic Attacks**:
    - **Ciphertext-only attack**.
    - **Known-plaintext attack**.
    - **Chosen-plaintext attack**.

Chapter 3: Secret Key Cryptography

- **Block ciphers**: Encrypt fixed-length blocks of plaintext.
- **Key/block size**: Must be large enough to prevent brute-force attacks.
- **Practical ciphers**: Often use multiple rounds of simpler ciphers.
- **Example**: DES (Data Encryption Standard) as a common block cipher.

Chapter 4: Modes of Operation

- **Encryption modes**:
    - **ECB (Electronic Code Book)**: Simple but insecure.
    - **CBC (Cipher Block Chaining)**: Adds security by chaining blocks.
    - **CTR (Counter mode)**: Encrypts a counter, XORs it with plaintext.
    - **XTS mode**: Designed for encrypting disk storage.
- **Length preservation**: Ciphertext stealing.
- **Message Authentication Codes (MACs)**:
    - **CBC-MAC**: Uses the last block of CBC encryption.
    - **CMAC**: A more secure variant of CBC-MAC.
    - **GCM (Galois/Counter Mode)**: Provides both encryption and authentication.

Chapter 5: Cryptographic Hashes

- **Hash functions**: Applications include:
    - Password hashing.
    - Message fingerprinting.
    - Digital signatures.
    - Data shorthand.
- **Key property**: Collision resistance.
- **Efficient structures**: Hash trees (Merkle trees).
- **Attack**: Append attack (vulnerability in hash constructions).
- **Examples**: SHA-3 and SHAKE (secure hash functions).

Chapter 6: First-Generation Public Key Algorithms

- **RSA**: Widely used for encryption and digital signatures.
- **Other algorithms**:
    - **ElGamal**, **DSA**, **ECDSA** (mainly for digital signatures).
    - **Diffie-Hellman**, **ECDH** (key exchange).

- **PKCS**: Standards for encoding RSA keys, signatures, and messages.

Chapter 7: Quantum Computing

- **Impact**: Quantum computers could break RSA and algorithms based on the discrete logarithm problem.

Chapter 8: Post-Quantum Cryptography

- **Resistant algorithms**: Designed to resist quantum attacks.
    - **Hash-based signatures**.
    - **Lattice-based cryptography**: Based on the difficulty of finding short lattice vectors.
    - **Code-based cryptography**: Utilizes error-correcting codes.
    - **Multivariate cryptography**: Based on polynomial equations.

Chapter 9: Authentication of People

- **Common methods**:

    - **Password-based authentication** (vulnerable to attacks).
    - **Strong password protocols**: Protect even if the server's database is compromised.

- **Example**: Lamport’s hash (one-time password scheme).

Chapter 10: Trusted Intermediaries

- **Kerberos**: A trusted third-party authentication system.
- **Public Key Infrastructure (PKI)**: Uses certificates to establish trust relationships.

Chapter 11: Communication Session Establishment

- **Secure session protocols**:
    - **One-way/mutual authentication**: Achieved using shared secrets or public keys.
    - **Session keys**: Protect data during communication.

- **Perfect forward secrecy (PFS)**: Ensures past communication is secure even if long-term secrets are compromised.

Chapter 12: IPsec

- **IPsec suite**: Secures IP communications.
  - **IKE (Internet Key Exchange)**: Establishes security associations and keys.
  - **AH (Authentication Header)**: Provides integrity protection.
  - **ESP (Encapsulating Security Payload)**: Provides encryption and optional integrity protection.

Chapter 13: SSL/TLS and SSH

- **SSL/TLS**: Protocol for securing web traffic.
- **SSH**: Protocol for secure remote login and file transfer.

Chapter 14: Electronic Mail Security

- **Email security**: Ensures confidentiality, integrity, and authenticity.
  - **Methods**: Digital signatures and encryption.

Chapter 15: Bitcoin

- **Bitcoin**: Cryptocurrency using blockchain to record transactions.
  - **Mining**: Verifies and adds transactions to the blockchain.

Chapter 16: Cryptographic Tricks

- **Cryptographic techniques**:
  - **Secret sharing**.
  - **Zero-knowledge proofs**.
  - **Oblivious transfer**.

Chapter 17: Folklore

- **Common practices**:

- **Key rollover**: Limits the impact of compromised keys.
- **Encryption + integrity**: Always combine encryption with integrity protection.