CSCI368 Network Security - Comprehensive Exam Notes

Course Overview

- **Instructor**: Dr. Khoa Nguyen (khoa@uow.edu.au)
- **Focus**: Wide range of computer network security topics
- **Prerequisites**: Basic cryptography, computer networks, programming (C/C++/Java)

Course Aims

1. Understand network vulnerabilities and network-based attacks
2. Apply network security technologies for securing networks
3. Use security standards and tools to enhance distributed system security
4. Evaluate, compare, and recommend network security applications and systems

---

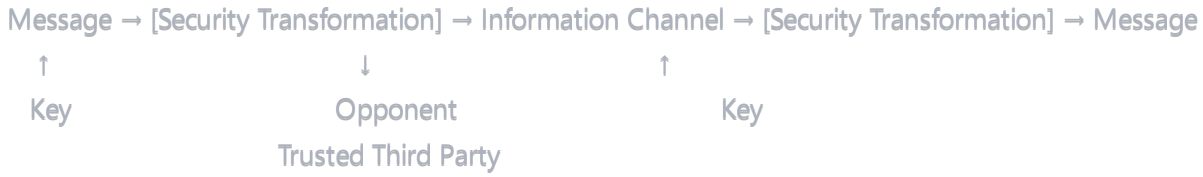
Topic 1: Introduction, Network Basics, Cryptography Basics

Network Security Fundamentals

Why Network Security Matters:

- Computer networks are vulnerable to attackers
- Computers rely on networks for communication
- Critical for: e-commerce, distributed computing, cloud computing, mobile communications, IoT

Abstract Communication Model:



Security Requirements (CIA+A)

1. **Confidentiality**: Information accessible only by authorized parties
2. **Integrity**: Protection from unauthorized modification, alteration, insertion, or deletion
3. **Authenticity**: Assurance of message origin
4. **Availability**: Information accessible to authorized parties when needed

Security Issues & Attack Types

Security Issues:

- **Interruption**: Attack on availability (Active)
- **Interception**: Attack on confidentiality (Passive)
- **Modification**: Attack on integrity (Active)
- **Fabrication**: Attack on authenticity (Active)

Common Attacks:

Passive Attacks:

- Eavesdropping communications and message release
- Traffic analysis (identities, locations, frequency of communications)

Active Attacks:

- Masquerade (impersonation) attacks
- Message modification
- Denial of Service (DoS)
- Replay attacks
- Man-in-the-middle attacks

Cryptography Basics

Encryption Types:

1. **Symmetric Cryptosystems (Secret Key):**
   - Same key for encryption and decryption
   - Examples: AES, DES, RC4
   - Fast but key distribution problem
2. **Asymmetric Cryptosystems (Public Key):**
   - Different keys for encryption and decryption
   - Examples: RSA, ElGamal, ECC
   - Slower but solves key distribution

Digital Signatures:

- Algorithms: RSA, DSS, ElGamal

- Provides authentication and non-repudiation
- Uses private key to sign, public key to verify

Hash Functions:

- Examples: MD5, SHA-1/2/3, HMAC
- Create fixed-size digest from variable input
- Used for integrity checking
- Keyed hash (HMAC) provides authentication

Topic 2: Public Key Infrastructure (PKI)

PKI Components

- **Certificate Authority (CA)**: Issues and manages digital certificates
- **Registration Authority (RA)**: Verifies certificate requests
- **Digital Certificates**: Bind public keys to entities
- **Certificate Repository**: Stores and distributes certificates
- **Certificate Revocation Lists (CRL)**: Lists revoked certificates

X.509 Certificates

- Standard format for digital certificates
- Contains: subject info, public key, issuer info, validity period, signature

Trust Models

- **Hierarchical**: Tree structure with root CA
- **Web of Trust**: Peer-to-peer trust relationships
- **Hybrid**: Combination of both approaches

Topic 3: Secure Message Transmission & Email Security

Email Security Threats

- Message interception
- Message modification
- Identity spoofing
- Denial of service

Email Security Solutions

Pretty Good Privacy (PGP):

- Hybrid cryptosystem
- Uses RSA for key exchange, symmetric encryption for message
- Digital signatures for authentication
- Web of trust model

S/MIME (Secure/Multipurpose Internet Mail Extensions):

- Standard for secure email
- Uses PKI infrastructure
- Supports encryption and digital signatures
- MIME-based format

Topic 4: Authentication & Key Establishment Protocols

Authentication Mechanisms

1. **Something you know** (passwords)
2. **Something you have** (tokens, cards)
3. **Something you are** (biometrics)
4. **Multi-factor authentication** (combination)

Key Establishment Protocols

Diffie-Hellman Key Exchange:

- Allows secure key agreement over insecure channel
- Based on discrete logarithm problem
- Vulnerable to man-in-the-middle attacks

Authenticated Key Agreement:

- Combines key establishment with authentication
- Protocols: Station-to-Station (STS), MQV

Protocol Security Properties

- **Entity Authentication**: Verify identity of communicating party
- **Key Authentication**: Assurance that key is known only to authorized parties
- **Key Freshness**: Ensure keys are not reused
- **Perfect Forward Secrecy**: Compromise of long-term keys doesn't affect past sessions

---

Topic 5: Centralized Authentication Systems & Kerberos

Kerberos Overview

- Network authentication protocol
- Uses symmetric key cryptography
- Trusted third-party authentication service
- Prevents password transmission over network

Kerberos Components

- **Key Distribution Center (KDC)**
- **Authentication Server (AS)**
- **Ticket Granting Server (TGS)**
- **Principals**: Users and services

Kerberos Protocol Flow

1. **AS Exchange**: Client requests ticket-granting ticket (TGT)
2. **TGS Exchange**: Client uses TGT to request service ticket
3. **Client-Server Exchange**: Client uses service ticket to access server

Kerberos Security Features

- Mutual authentication
- Ticket-based access control
- Time-limited tickets
- Replay attack prevention

Topic 6: Internet Protocol Security (IPSec) & Internet Key Exchange (IKE)

IPSec Overview

- Framework for securing IP communications

- Operates at network layer
- Provides confidentiality, integrity, and authentication

IPSec Protocols

1. **Authentication Header (AH)**: Provides authentication and integrity
2. **Encapsulating Security Payload (ESP)**: Provides confidentiality, authentication, and integrity

IPSec Modes

- **Transport Mode**: Protects payload only
- **Tunnel Mode**: Protects entire IP packet

Security Associations (SA)

- Unidirectional security relationship
- Defined by: Security Parameter Index (SPI), destination IP, security protocol
- Stored in Security Association Database (SAD)

Internet Key Exchange (IKE)

- Protocol for establishing IPSec security associations
- Two phases:
    1. **Phase 1**: Establish secure channel (IKE SA)
    2. **Phase 2**: Negotiate IPSec SAs

Topic 7: SSL/TLS & SSH

SSL/TLS Overview

- Secure communication protocol for web
- Operates between transport and application layers
- Provides confidentiality, integrity, and authentication

TLS Handshake Process

1. **Client Hello**: Client initiates connection
2. **Server Hello**: Server responds with certificate
3. **Key Exchange**: Establish shared secret
4. **Finished**: Confirm handshake completion

TLS Record Protocol

- Handles data fragmentation, compression, encryption
- Uses symmetric encryption after handshake

Secure Shell (SSH)

- Secure remote login protocol
- Replaces insecure protocols like Telnet, rlogin
- Uses public key authentication
- Provides encrypted communication channel

Topic 8: Wireless & Mobile Security

Wireless Security Challenges

- Broadcast nature of wireless medium
- Mobility of devices
- Resource constraints
- Easier eavesdropping

Wi-Fi Security Evolution

WEP (Wired Equivalent Privacy):

- Original Wi-Fi security protocol
- Uses RC4 encryption
- Seriously flawed and deprecated

WPA/WPA2 (Wi-Fi Protected Access):

- Improved security over WEP
- Uses TKIP (WPA) or AES (WPA2)
- Pre-shared key or enterprise authentication

WPA3:

- Latest Wi-Fi security standard
- Enhanced encryption and authentication
- Protection against offline attacks

Mobile Security Considerations

- **GSM Security**: A5 encryption algorithm
- **3GPP Security**: Enhanced authentication and key agreement
- **Mobile Device Management (MDM)**
- **Application security**

Security Protocols Summary

Key Security Protocols

- **VPN**: Virtual Private Networks for secure remote access
- **SSL/TLS**: Secure web communications
- **Kerberos**: Network authentication
- **IPSec**: Network layer security
- **SSH**: Secure remote access
- **WPA/WPA2/WPA3**: Wireless security

Exam Preparation Tips

Key Areas to Focus On

1. **Fundamental Security Concepts**: CIA triad, attack types
2. **Cryptographic Algorithms**: Symmetric vs asymmetric, hash functions
3. **Protocol Details**: Understand how each protocol works
4. **Security Analysis**: Identify vulnerabilities and countermeasures
5. **Practical Applications**: Real-world implementation scenarios

Common Exam Question Types

- Compare and contrast different security protocols
- Analyze security protocol vulnerabilities
- Design secure communication systems
- Evaluate security requirements for given scenarios
- Explain cryptographic mechanisms and their applications

Important Formulas and Concepts

- Remember key sizes and algorithm strengths
- Understand protocol message flows
- Know security properties of different systems
- Understand trust models and certificate validation

Assessment Information

- **Assignment 1**: Programming (20%)
- **Assignment 2**: Protocol design & analysis (20%)
- **Final Exam**: 60% (minimum 40% required to pass)
- Late penalty: 5% per day (including weekends)
- Maximum 4 days late accepted