CHAPTER 5: SECURITY

5.1 ENCRYPTION AND ENCRYPTION PROTOCOLS

5.1.1 Encryption Concepts

Plain Text: Original data before encryption.

Cipher Text: Result of applying encryption algorithm to data.

Encryption: Process of making cipher text from plain text.

Key: Value used by encryption/decryption algorithm.

5.1.2 Symmetric Key Encryption

Definition: Same key used for encryption and decryption.

Process:

1. Sender and receiver share secret key
2. Sender encrypts plain text with key → cipher text
3. Cipher text transmitted
4. Receiver decrypts with same key → plain text

Advantages:

- Fast
- Simple

Disadvantages:

- Key distribution problem
- Multiple keys needed for multiple recipients

Examples:

- AES (Advanced Encryption Standard)
- DES (Data Encryption Standard)

5.1.3 Asymmetric Key Encryption

Definition: Different keys for encryption and decryption.

Public Key:

- Shared with everyone
- Used for encryption
- Used for signature verification

Private Key:

- Kept secret
- Used for decryption
- Used for digital signatures

Sending Private Message:

1. Receiver sends public key to sender
2. Sender encrypts message with public key
3. Only receiver (with private key) can decrypt

Sending Verified Message:

1. Sender encrypts with private key
2. Anyone can decrypt with public key
3. Message verified as from sender

5.1.4 Digital Signatures

Process:

1. Calculate hash of message (digest)
2. Encrypt digest with sender's private key → digital signature
3. Send message + signature
4. Receiver decrypts signature with public key → digest
5. Receiver calculates hash of message

6. If digests match → message authentic

5.1.5 Digital Certificates

Purpose: Verify that public key belongs to claimed entity.

Certificate Contents:

- Entity's public key
- Entity's identity information
- CA's digital signature

Obtaining Certificate:

1. Entity contacts Certification Authority (CA)
2. CA confirms entity's identity
3. CA creates certificate with entity's public key
4. CA signs certificate with its private key
5. Entity posts certificate on website

5.1.6 SSL/TLS Protocol

Purpose: Provide secure communication between client and server.

Uses:

- Online shopping
- Online banking
- HTTPS websites

Process:

1. Client connects to server (port 443)
2. Server sends certificate
3. Client validates certificate
4. Client generates session key
5. Client encrypts session key with server's public key
6. Server decrypts session key
7. Secure session begins

5.2 MALWARE AND RESTRICTION METHODS

5.2.1 Types of Malware

Type	Description	Exploits
Virus	Replicates inside executable files	Executable files
Worm	Runs independently, propagates to networks	Shared networks
Spyware	Collects and transmits information	Background processes
Phishing	Emails requesting confidential info	User trust
Pharming	Bogus website redirects	Website appearance

5.2.2 Restriction Methods

Malware	Restriction Method
Virus	Anti-virus software with daily scans
Worm	Firewall protection
Spyware	Real-time anti-spyware
Phishing	Check sender email address
Pharming	Verify website URL

Revision #1
Created 2026-03-16 12:16:40 UTC by Samuel Lee
Updated 2026-03-16 12:16:53 UTC by Samuel Lee