

CS2107 Notes

Contents

1. Security Requirements
 - a. Introduction
 - b. CIA
 - c. Others
 - d. Breaches in Recent Security News
2. Key Concepts & Basic Mechanisms of Principal Protection Mechanisms
 - a. Cryptography & Encryption
 - i. Cryptography?
 - ii. Classical Ciphers
 1. Substitution Cipher
 2. Caesar Cipher
 3. Permutation Cipher
 4. One-time Pad
 - iii. Modern Ciphers
 - iv. Properties of Ciphers
 - v. Block Ciphers vs Stream Ciphers
 - vi. Attacks on Cryptosystem Implementations
 - vii. Kerckhoff's Principle vs Security through Obscurity
 - viii. Historical Facts
 - b. Authentication (Entity Authentication)
 - i. Password
 1. Stages
 2. Attacks
 3. Preventive Measures
 4. ATM and ATM Attacks
 - ii. Biometrics
 - iii. Multi-factor Authentication
 - c. Authentication and Cryptography (Data Origin Authentication)
 - i. Public Key Cryptography
 1. RSA
 - ii. Cryptographic Hash
 - iii. Data Integrity
 1. Unkeyed Hash
 - iv. Data-Origin Authenticity
 1. MAC
 2. Signature
 - v. Attacks and Pitfalls
 1. Birthday Attack on Hash
 2. Using Encryption for Authenticity
 3. Hashed and Salted Passwords
 - d. Cryptography Part 2
 - i. Public Key Distribution and Public Key Infrastructure
 - ii. Certificates
 1. Certificate Authority
 2. Certificate
 3. X.509 Digital Certificate Standard
 4. How to Get a Certificate
 - iii. Certificate Authority and Trust Relationship
 - iv. Limitations and Attacks
 - v. Strong Authentication
 1. Secret Key
 2. Public Key

- vi. Session Key
- e. Putting It All Together
 - i. Securing a Communication Channel
 - ii. HTTPS
- 3. Network Security
 - a. Network Layers
 - b. Network Attacks
 - i. Domain Name System Attacks
 - ii. Denial of Service Attacks
 - iii. Distributed Denial of Service Attacks
 - c. Useful Network Security Tools
 - d. Network Protection
 - i. Cryptography
 - ii. Firewall
 - iii. Network Security Management
- 4. Key Concepts 2
 - a. Access Control
- 5. Basic Security Tools & Linux Commands
- 6. Common Insecure Programming Practices & Suggestions

Appendix

- A. Terminology and Definitions