

CS2107 NOTES

AY19/20 Semester 1

Hanming Zhu

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
 - i. Network Models
 - ii. Addressing Schemes
 - iii. Hub, Switch and Router
 - b. Network Attacks
 - i. Name Resolution and Attacks
 - ii. Denial of Service Attacks
 - iii. Distributed Denial of Service Attacks
 - 1. Botnet
 - c. Useful Tools
 - d. Network Protection
 - i. Cryptography
 - 1. SSL/TLS
 - 2. WPA2
 - 3. IPsec
 - ii. Firewall
 - 1. Demilitarized Zone
 - iii. Network Security Management
- 4. Key Concepts Part II
 - a. Access Control
 - i. Layering Model in Computer System Design
 - ii. Access Control Model
 - iii. Specifying Access Rights
 - 1. Access Control Matrix
 - 2. Access Control List
 - 3. Capabilities
 - iv. Intermediate Control
 - 1. Privileges
 - 2. Role-based Access Control
 - 3. Bell-LaPadula Model
 - 4. Biba Model
 - v. Access Control in UNIX/Linux
 - 1. Terminology
 - 2. Password File Protection
 - 3. File System Permission
 - 4. Search Path Issues
 - vi. UNIX/Linux: Privilege Escalation (Controlled Invocation)
- 5. Software Security
 - a. Overview of Software Security
 - b. Computer Architecture
 - i. Code vs Data
 - ii. Control Flow and Program Counter
 - iii. Stack
 - iv. Control Flow Integrity
 - c. Attacks and Vulnerabilities
 - i. Printf() and Format String Vulnerability
 - ii. Data Representation & Security
 - iii. Buffer Overflow
 - iv. Integer Overflow
 - v. Code/Script Injection

- vi. Undocumented Access Points
 - vii. TOCTOU Race Condition
 - d. Defense and Preventive Measures
 - i. Filtering / Input Validation
 - ii. Safer Functions
 - iii. Bounds Checking and Type Safety
 - iv. Memory Protection
 - 1. Randomization
 - 2. Canary
 - v. Code Inspection / Taint Analysis
 - vi. Testing
 - vii. Principle of Least Privilege
 - viii. Patching
 - ix. Summary
- 6. Web Security
 - a. Background
 - b. Security Issues and Threat Models
 - i. Attackers as Another End Systems
 - ii. Attackers as a Man-in-the-Middle
 - c. Attacks on SSL/TLS
 - d. URL and Address Bar Insecurities
 - e. Cookies and Same-Origin Policy
 - f. Cross-Site Scripting (XSS)
 - g. Cross-Site Request Forgery (CSRF)
 - h. Other Web Attacks and Terminologies