Study Guide for Chapter 1

March 6, 2025

1 Computer Security Concepts

1.1 Definition of Computer Security

Computer security is defined as the protection afforded to an automated information system to preserve the integrity, availability, and confidentiality of information system resources. These resources include hardware, software, firmware, information/data, and telecommunications.

1.2 Key Objectives of Computer Security

The three key objectives of computer security are:

- **Confidentiality**: Ensures that private or confidential information is not disclosed to unauthorized individuals. It includes data confidentiality and privacy.
- **Integrity**: Ensures that information and programs are changed only in a specified and authorized manner. It includes data integrity and system integrity.
- **Availability**: Ensures that systems work promptly and service is not denied to authorized users.

These objectives are often referred to as the **CIA triad**.

1.3 Additional Security Concepts

- **Authenticity**: Ensures that the origin of a message or data is verified and trusted.
- **Accountability**: Ensures that actions of an entity can be traced uniquely to that entity.

1.4 Examples of Security Requirements

Examples of applications illustrating confidentiality, integrity, and availability requirements are provided, with impact levels (low, moderate, high) defined in FIPS 199.

2 Threats, Attacks, and Assets

2.1 Threats and Attacks

- **Threat**: A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.
- **Attack**: A threat that is carried out and, if successful, leads to an undesirable violation of security.
- **Types of Attacks**:
  - **Active Attack**: Attempts to alter system resources or affect their operation.
  - **Passive Attack**: Attempts to learn or make use of information from the system without affecting system resources.

2.2 Threat Consequences

- **Unauthorized Disclosure**: Threat to confidentiality.
- **Deception**: Threat to integrity.
- **Disruption**: Threat to availability.
- **Usurpation**: Threat to system integrity.

2.3 Assets

The assets of a computer system can be categorized as:

- **Hardware**: Vulnerable to theft, damage, and availability threats.
- **Software**: Vulnerable to deletion, modification, and piracy.
- **Data**: Vulnerable to unauthorized access, modification, and destruction.
- **Communication Lines and Networks**: Vulnerable to passive and active attacks.

3 Security Functional Requirements

The FIPS 200 standard enumerates 17 security-related areas for protecting the confidentiality, integrity, and availability of information systems. These areas include:

- Access Control
- Awareness and Training
- Audit and Accountability
- Certification, Accreditation, and Security Assessments
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Planning
- Personnel Security
- Risk Assessment
- Systems and Services Acquisition
- System and Communications Protection
- System and Information Integrity

4 Fundamental Security Design Principles

The following are fundamental security design principles:

- **Economy of Mechanism**: Keep the design simple and small.
- **Fail-Safe Defaults**: Default to lack of access.
- **Complete Mediation**: Check every access against the access control mechanism.
- **Open Design**: Security mechanisms should be open to public scrutiny.

- **Separation of Privilege**: Require multiple conditions to grant access.
- **Least Privilege**: Every process and user should operate with the least set of privileges necessary.
- **Least Common Mechanism**: Minimize functions shared by different users.
- **Psychological Acceptability**: Security mechanisms should not unduly interfere with user work.
- **Isolation**: Isolate public access systems from critical resources.
- **Encapsulation**: Encapsulate procedures and data objects in a protected domain.
- **Modularity**: Develop security functions as separate, protected modules.
- **Layering**: Use multiple, overlapping protection approaches.
- **Least Astonishment**: A program or user interface should respond in the least surprising way.

5 Attack Surfaces and Attack Trees

5.1 Attack Surfaces

An attack surface consists of the reachable and exploitable vulnerabilities in a system. Attack surfaces can be categorized as:

- **Network Attack Surface**: Vulnerabilities over a network.
- **Software Attack Surface**: Vulnerabilities in application, utility, or operating system code.
- **Human Attack Surface**: Vulnerabilities created by personnel or outsiders.

5.2 Attack Trees

An attack tree is a branching, hierarchical data structure that represents a set of potential techniques for exploiting security vulnerabilities. The root node represents the goal of the attack, and the leaf nodes represent different ways to initiate an attack.

6 Computer Security Strategy

A comprehensive security strategy involves:

- **Security Policy**: A formal statement of rules and practices that specify how a system provides security services.
- **Security Implementation**: Involves prevention, detection, response, and recovery.
- **Assurance and Evaluation**: Assurance is the degree of confidence that security measures work as intended, and evaluation is the process of examining a system with respect to certain criteria.

7 Multiple Choice Questions

1. Which of the following is NOT one of the key objectives of computer security?
   - (a) Confidentiality
   - (b) Integrity
   - (c) Availability
   - (d) Authenticity

2. What is the primary goal of a passive attack?
   - (a) To alter system resources
   - (b) To learn or make use of information from the system
   - (c) To disrupt system services
   - (d) To gain unauthorized access to a system

3. Which of the following is an example of a threat to data integrity?
   - (a) Unauthorized disclosure of information
   - (b) Modification of data files
   - (c) Denial of service
   - (d) Theft of hardware

4. What is the principle of least privilege?
   - (a) Every process and user should operate with the least set of privileges necessary.
   - (b) Security mechanisms should be open to public scrutiny.
   - (c) Every access must be checked against the access control mechanism.
   - (d) The design of security measures should be as simple and small as possible.

5. Which of the following is a characteristic of an active attack?
   - (a) It attempts to learn or make use of information from the system.
   - (b) It attempts to alter system resources or affect their operation.
   - (c) It is difficult to detect because it does not involve any alteration of the data.
   - (d) It is typically prevented by encryption.

6. What is the purpose of an attack tree?
   (a) To represent a set of potential techniques for exploiting security vulnerabilities.
   (b) To define the security policy of a system.
   (c) To implement security mechanisms in a system.
   (d) To evaluate the effectiveness of security measures.
7. Which of the following is a fundamental security design principle?
   (a) Economy of Mechanism
   (b) Fail-Safe Defaults
   (c) Complete Mediation
   (d) All of the above
8. What is the primary focus of a network attack surface?
   (a) Vulnerabilities in application code.
   (b) Vulnerabilities over a network.
   (c) Vulnerabilities created by personnel.
   (d) Vulnerabilities in operating system code.
9. Which of the following is an example of a security functional requirement?
   (a) Access Control
   (b) Awareness and Training
   (c) Audit and Accountability
   (d) All of the above
10. What is the main goal of a security policy?
    (a) To define the rules and practices for providing security services.
    (b) To implement security mechanisms in a system.
    (c) To evaluate the effectiveness of security measures.
    (d) To detect and respond to security attacks.
11. Which of the following is a threat to system integrity?
    (a) Unauthorized disclosure of information
    (b) Modification of data files
    (c) Denial of service
    (d) Theft of hardware

Answer Key

1. D
2. B
3. B
4. A
5. B
6. A
7. D
8. B
9. D
10. A
11. B