Basic Security Concepts

Amir Masoumzadeh

CSI 424/524

Aug. 28, 2025

UNIVERSITY AT ALBANY
State University of New York

Assets of a Computer System

- Data
- Software
- Hardware
- Communication facilities and networks

C/I/A Triad

- Confidentiality
- Integrity
- Availability

Exercise 02a: C/I/A

Which security service is primarily provided/compromised in each scenarios below?

1. A bank will only disclose financial standing of a company to authorized people from that company
2. A web server is unreachable (down)
3. A virus has deleted all the files on a hard disk
4. Correct PIN should be provided to withdraw money from an ATM
5. You browse CS department's website through HTTPS protocol, which is encrypted

Vulnerabilities, Threats, and Attacks

Vulnerabilities Intrinsic flaws that can be exploited to undermine security

Threats Capability of exploiting vulnerabilities

- Represents potential security harm to an asset

Attacks Threats carried out

- Insider/Outsider
- Passive/Active

Passive and Active Attacks

Passive Learn or make use of information from the system but does not affect system resources

Active Alter system resources or affect their operation

Threat Categories

- Unauthorized Disclosure
  - Exposure
  - Interception
  - Inference
- Deception
  - Masquerade
  - Falsification
  - Repudiation
- Disruption
  - Incapacitation
  - Corruption
  - Obstruction
- Usurpation
  - Misappropriation
  - Misuse

Threat Categories (Definitions)

Threat Consequences, and the Types of Threat Actions That Cause Each Consequence. Based on RFC 2828.

Threat Consequence	Threat Action (Attack)
Unauthorized Disclosure A circumstance or event whereby an entity gains access to data for which the entity is not authorized.	**Exposure:** Sensitive data are directly released to an unauthorized entity. **Interception:** An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations. **Inference:** A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or byproducts of communications. **Intrusion:** An unauthorized entity gains access to sensitive data by circumventing a system's security protections.
Deception A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.	**Masquerade:** An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity. **Falsification:** False data deceive an authorized entity. **Repudiation:** An entity deceives another by falsely denying responsibility for an act.
Disruption A circumstance or event that interrupts or prevents the correct operation of system services and functions.	**Incapacitation:** Prevents or interrupts system operation by disabling a system component. **Corruption:** Undesirably alters system operation by adversely modifying system functions or data. **Obstruction:** A threat action that interrupts delivery of system services by hindering system operation.
Usurpation A circumstance or event that results in control of system services or functions by an unauthorized entity.	**Misappropriation:** An entity assumes unauthorized logical or physical control of a system resource. **Misuse:** Causes a system component to perform a function or service that is detrimental to system security.

Source: Computer Security: Principles and Practice (3rd Edition), W. Stallings and L. Brown, 2014

Exercise 02b: Threats

Categorize the following threats:

1. A web server can become unreachable by potential attackers
2. A virus may delete all files on a hard disk
3. A sketchy financial website may deny that you have deposited money into your account
4. Someone may eavesdrop your chat messages as they are routed through your network

Policy and Mechanism

- Policy says what is, and is not, allowed
  - This defines "security" for the system
- Mechanisms (methods/tools/procedures) enforce policies

Goals of Security

- Prevention
  - Prevent attackers from violating security policy
- Detection
  - Detect attackers' violation of security policy
- Recovery
  - Stop attack, assess and repair damage
  - Continue to function correctly even if attack succeeds

Security Design Principles: Overview

- Simplicity
  - Less to go wrong
  - Fewer possible inconsistencies
  - Easy to understand
- Restriction
  - Minimize access
  - Inhibit communication

1. Least Privilege

- A subject should be given only those privileges necessary to complete its task
  - Function, not identity, controls
  - Rights added as needed, discarded after use
  - Minimal protection domain

2. Fail-Safe Defaults

- Default action is to deny access
- If action fails, system as secure as when action began

3. Economy of Mechanism

- Keep it as simple as possible
  - KISS principle
- Simpler means less can go wrong
  - And when errors occur, they are easier to understand and fix

4. Complete Mediation

- Check every access
- Usually done once, on first action
  - Unix: file access checked on open, not checked thereafter
  - If permissions change after, may get unauthorized access

5. Open Design

- Security should not depend on secrecy of design or implementation
  - "Security through obscurity"
  - Does not apply to information such as passwords or cryptographic keys
  - Popularly misunderstood to mean that source code should be public

6. Separation of Privilege

- Require multiple conditions to grant privilege
  - Separation of duty
  - Defense in depth

7. Least Common Mechanism

- Access mechanisms should not be shared
  - Information can flow along shared channels
  - Covert channels
- Isolation
  - Virtual machines
  - Sandboxes

8. Psychological Acceptability

- Security mechanisms should not add to difficulty of accessing resource
  - Hide complexity introduced by security mechanisms
  - Ease of installation, configuration, and use
  - Human factors are critical here

Exercise 02c: Design Principles

- You are responsible for securing a learning management system
  - Authorized Users: instructor, teaching assistant, and students
- For each of the statements below, select the two most important design principles (listed at the bottom).
  1. Users enter the system.
  2. Students submit their assignments.
  3. Assignments need to be graded by TA, and then grades need to be finalized by instructor.

Design Principles: Fail-Safe Defaults, Least Common Mechanism, Least Privilege, Separation of Privilege