# System Security

Saranya Chandran
Amrita Center for Cybersecurity Systems & Networks

# Course Roadmap

- Security Goals
- Memory Exploits
- Vulnerabilities (SSL/TLS)
- Understanding threats
- Secure Coding Techniques for C program
- Fuzzing
- Trusted Execution Environment

# Grading

| Component | Weightage |
| --- | --- |
| Periodical1 | 10 |
| Periodical2 | 10 |
| Lab Exam 1 | 10 |
| Lab Exam2 | 10 |
| Assignment | 20 |
| End Sem | 40 |

# Computer Security

Definition by National Institute of Standards and Technology [NIST 95]

**Computer security :** The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

- Security is an attribute of a computer system
- Correctness
    - Ensures system behaves as specified under expected circumstances
    - Example Banking Website, Word processing software
- Security is concerned with preventing undesirable behavior
    - Takes into account an adversary who is actively and maliciously trying to circumvent protective measures you put in place.
- Correctness specifies what a system should do and security is about what a system should not do

# Security Goals

Key concepts

- Authentication
  - The property of being genuine, verifiable and trusted
  - E.g. Authenticating a user
  - Two factor authentication
- Authorization
- **Confidentiality**
- **Integrity**
- Accountability
- Non-repudiation
- **Availability**

# CIA

## Confidentiality

- Data Confidentiality: Assures that private or confidential information is not disclosed to unauthorized individuals

- Stealing Information - Corporate secrets , Credit card number e.t.c.

- Privacy: Assures that individuals control or influence what information related to them may be collected and stored by whom and to whom that information may be disclosed

# CIA contd..

## Integrity

- Data Integrity: Assures that information and programs are changed only in an authorized manner

- System Integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system
    - Installing unwanted software such as Spyware or Rootkits, Destroying records (logs, accounts)

# CIA contd..

## Availability

- Assures that systems work promptly and service is not denied to authorized users
- Stalling the ability to purchase products or access banking information

### CIA Triad

# Security Goals

Authenticity

- The property of being genuine, verifiable and trusted
- Authenticating a user or verifying the source of a message
- Use passwords
- E.g. ATM authenticates user using pin number

Authorization

- Act of checking whether a user has permission to conduct some action
- Use Access Control List : determine whether users are authorized to do different actions
- E.g. Cash withdrawal from ATM

Authentication is about verifying identity

Authorization is about verifying a user’s authority

# Security Goals

Accountability

- Protection against deniability
- It allows an entity to be traced uniquely
- Crucial in intrusion detection and and preventions systems
- Mentioned in Federal Information Processing Standards (FIPS) 199

Non-repudiation

- Guaranteeing message transmission between parties
- Ability to prove (at the receiver side) that the sender actually sent the data or the ability to prove (at the sender side) that the receiver actually received the data
- Use digital signatures, data hash

# Secure Design Principles

# Secure design principles

- The Principle of Least Privilege
  - User or computer program should be given the least amount of privileges necessary to accomplish a task.
  - E.g. valet
- Defense-in-Depth (Redundancy)
  - Multiple mechanisms help to achieve security
  - Prevent, Detect, Contain, and Recover
  - Password security
- Diversity in Defence
  - using multiple heterogeneous systems that do the same thing.
  - use of multiple operating systems within a corporation to mitigate the impact of viruses.

# Secure design principles

- Securing the Weakest Link
  - The weakest link is the part of a system that is the most vulnerable, susceptible, or easiest to attack.
  - Weak Passwords
  - People
  - Implementation vulnerabilities
- Fail-Safe Stance
  - designing a system in such a way that even if one or more components fail, we can still ensure some level of security.
  - Eg : failure of firewall
    - If a firewall ever fails, it should deny access by default and not let any traffic in
- Secure by Default
  - By default, system should be optimized for security wherever possible.
  - Enable only necessary features

# Secure design principles

- Simplicity
  - Keeping software as simple as possible
  - Complex software is likely to have many more bugs and security holes than simple software
- Usability
  - Users should be able to accomplish tasks that the software is meant to assist them in carrying out
  - Do not rely on documentation
  - Secure by default
  - Remember that users will often ignore security if given the choice
- Security Features Do Not Imply Security
  - One or more security features in a product does not ensure security
  - Depends on how security features used

# Reference


- Neil Daswani, Christopher Kern, Anita Kesavan, “Foundations of Security, What Every Programmer Needs to Know”,Apress, 2007