# Principles of Computer Security

Alvin Lin

January 2018 - May 2018

## Overview

This course is unique in that it is the only course with the presence of an adversary. We have to defend against all sorts of attacks, crude or not.

### Military Humor

Secure a building:

- Army: Put guards around the place
- Navy: Turn out the lights and lock the doors
- Air Force: Take out a 5-year lease with an option to buy
- Marines: Kill everyone inside and make it a command post

### What does it mean to secure a computer system?

- Kill every user who is using it?
- Turn off the computer?
- Prevent unauthorized access

### Important Reminders

- The final project is graded as a group but each individual may receive a different grade depending on effort.
- Email is not the best medium to contact the professor, use MyCourses. Each student will have a private channel to the professor.
- Let the professor know in advance if you will be missing class if possible.
- Do not send assignments by email.

### Discussion Question

Consider this claim:

- Security is only possible in a world in which everyone trusts everyone.
- Security is only possible in a world where no one trusts anyone.

## What is 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)." -NIST Computer Security Handbook.

A computer scientist is someone who can apply computer science theory and software development fundamentals to produce computing-based solutions. Security should be involved in all factors of being a computer scientist.

## Security: Knowledge Areas

| | |
|---|---|
| Data Security | Protection of data at rest, during processing, and in transit |
| Software Security | Development and use of software that reliably preserves the security properties of the protected information and systems |
| Component Security | The security aspects of the design, procurement, testing, analysis, and maintenance of components integrated into larger systems |
| Connection Security | Security of the connections between components, both physical and logical |
| System Security | Security aspects of systems that are composed of components and connections, and use software |
| Human Security | The study of human behavior in the context of data protection, privacy, and threat mitigation |
| Organizational Security | Protecting organizations from cybersecurity threats and managing risk to support the successful accomplishment of the organizations' missions |
| Societal Security | Aspects of cybersecurity that broadly impact society as a whole |

## C-I-A Pillar: Three Objectives

**Confidentiality:**

- Data confidentiality: private or confidential information is not made available or disclosed to unauthorized individuals.
- Privacy: assures that individuals can control or influence what information related to them may be collected/stored, and by whom, and to whom it may be disclosed.

**Integrity:**

- Data integrity: assures that information and programs are changed only in a specified and 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.

**Availability:**

- Assures that systems work promptly and service is never denied to authorized users.

## From CIA to CIANA

**Non-repudiation:**

- Assures that the system has the ablity to correlate, with high certainty, a recorded action with its originating individual or entity.

**Authentication:**

- Assures that the system has the ability to verify the identity of an individual or entity.

## Security Principles

- Least privilege: a subject should be given only those priveleges that it needs to complete its task.
- Fail-safe defaults: unless a subject is given explicit access to an object, it should be denied access to it.
- Economy of mechanism: security mechanisms should be as simple as possible.
- Complete mediation: all accesses to objects be checked to ensure that they are allowed.
- Open design: security of a mechanism must not depend on design/implementation secrecy.
- Separation of privilege: system must not grant permission based on a single condition.
- Least common mechanism: mechanisms for resource access must not be shared.
- Psychological acceptability: security mechanisms must not make resources more difficult to access than if they were not present.

## Security Breach Impact

FIPS 199: Standards for Security Categorization of Federal Information and Information Systems.
**Low**:

- Loss expected to have limited adverse effect on operations, assets, or individuals.
- Some degradation, minor asset damange, some financial loss, and minor individual harm.

**Moderate**:

- Serious adverse effect on operations, organizational assets, or individuals.
- Significant degradation, damage to assets, financial loss, or harm to individuals that does not involve loss of life or serious, life-threatening injuries.

**High**:

- Severe or catastrophic effect on operations, organization assets, or individuals.
- Organization is not able to perform one or more of its primary functions, or major damage to organizational assets, or major financial loss, or severe harm to individuals involving loss of life or serious life-threatening injuries.

You can find all my notes at `http://omgimanerd.tech/notes`. If you have any questions, comments, or concerns, please contact me at alvin@omgimanerd.tech