# Lecture 1
# September 24, 2025

ECS 235A, Computer and Information Security

# Administrative Stuff: Instructors

- Instructor: Matt Bishop, mabishop@ucdavis.edu
  - Office Hours: TuTh 11:00–11:50am in 2203 Watershed Sciences; W 2:10–3:00pm on Zoom (see Canvas announcement for link information)
  - When you send email, please put "ECS 235A" in the subject so I will know it is class related
- TA: Muwei Zheng, mzheng@ucdavis.edu
  - Office Hours and location: *to be arranged*

# Goals

- Understand what computer security is and learn its basic limits;
- Learn the basic policy models underlying security;
- Know about common vulnerabilities, the basics of software security and formal verification;
- Learn the basic techniques of cryptography;
- Learn about host-based security, network security, and intrusion detection; and
- Explore other topics of interest.

# Class Information

- Textbook: M. Bishop, *Computer Security: Art and Science*, Second Edition, Addison-Wesley, Boston, MA (2019). ISBN 978-0-321-71233-2
- Web Sites
  - Canvas (this is the regular class web site)
  - http://nob.cs.ucdavis.edu/classes/ecs235a-2025-04 (a backup web site)
- Grading
  - 50% Homework
  - 50% Project

# Getting a PTA

## How Not to Get a PTA

Please do not ask me to give you a PTA. Only the department can do so.

## How to Get a PTA

1 Go to the graduate program policies web site:
https://cs.ucdavis.edu/graduate/policies.
2 Click on, and review, the “PTA Policy & Expectations” section.
3 Submit your PTA request using the linked form in the policy section.

# Student Resources and No-Nos

- Resources: Frequently Asked Questions — UC Davis Student Resources

  https://ebeler.faculty.ucdavis.edu/resources/faq-student-resources
- Academic Integrity: Code of Academic Conduct https://sja.ucdavis.edu/files/cac.pdf

# Projects

- You choose the project
  - Teams: up to 3 people; ask if you want more to join
- What is due, and when:
  - Question, 10% of project grade; due Friday, October 10
  - Progress Report, 20% of project grade; due Friday, November 7
  - Completed Project, 70% of project grade; due Tuesday, December 9
- Note each submission also requires a brief video!

# Question

## What do you think of this statement?

Online business risks are ever-increasing as we move further into the digital age. Cyber threats are becoming increasingly common, so taking proactive steps to reduce attacks is important. One way to do this is by **implementing a robust organizational security policy that covers all possible vulnerabilities.**

Data security is essential for businesses that deal with sensitive information regularly. Even though businesses are encouraged to promote a culture of security within their offices and to educate employees about the threats and what they can do to avoid them, some employees might still make mistakes.

From https://www.rocket.chat/blog/organizational-security

# Outline

- Components of computer security
- Threats
- Policies and mechanisms
- The role of trust
- Assurance
- Operational Issues
- Human Issues

# Basic Components

- Confidentiality
  - Keeping data and resources hidden
- Integrity
  - Data integrity (integrity)
  - Origin integrity (authentication)
- Availability
  - Allowing access to data and resources

# Classes of Threats

- Disclosure
  - Snooping
- Deception
  - Modification, spoofing, repudiation of origin, denial of receipt
- Disruption
  - Modification
- Usurpation
  - Modification, spoofing, delay, denial of service

# Policies and Mechanisms

- Policy says what is, and is not, allowed
  - This defines “security” for the site/system/*etc*.
- Mechanisms enforce policies
- Composition of policies
  - If policies conflict, discrepancies may create security vulnerabilities

# Goals of Security

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

# Assumptions and Trust

- Underlie *all* aspects of security
- Policies
  - Unambiguously partition system states
  - Correctly capture security requirements
- Mechanisms
  - Assumed to enforce policy
  - Support mechanisms work correctly

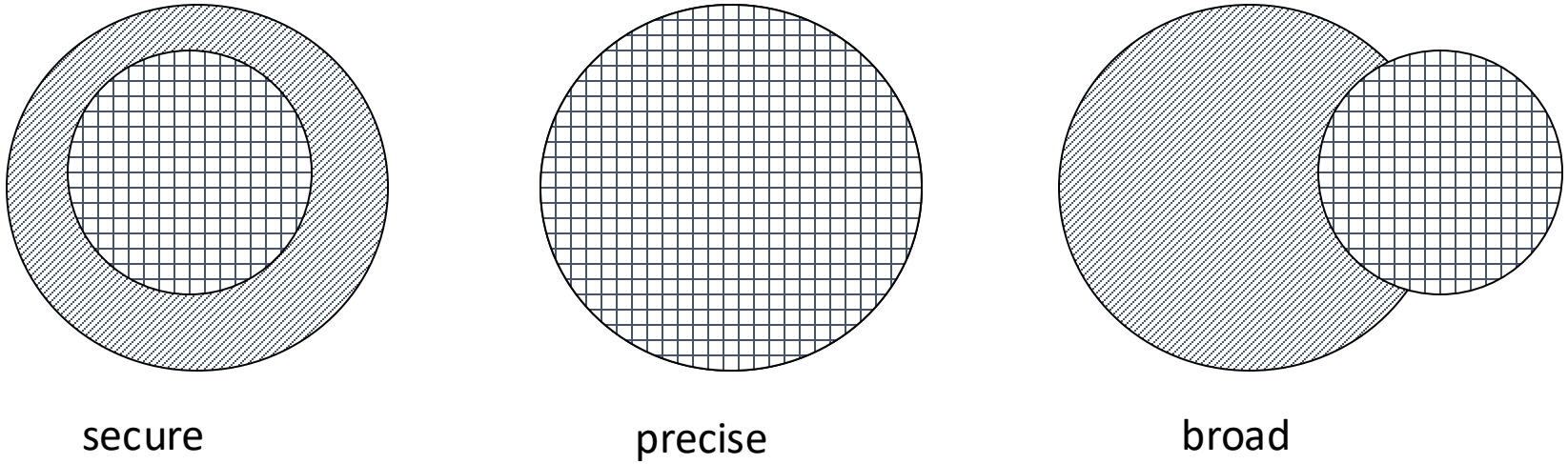
# Types of Mechanisms

- Let $P$ be the set of all possible states of a system
- Let $Q$ be the set of secure states as defined by the security policy
- Let $R$ be the set of states that can be reached under the security policy

**Definition**: A security mechanism is:

- *secure* if $R \subseteq Q$;
- *precise* if $R = Q$; and
- *broad* if there are states r such that $r \in R$ and $r \notin Q$.

# Types of Mechanisms



# Assurance

- Specification
  - Requirements analysis
  - Statement of desired functionality
- Design
  - How system will meet specification
- Implementation
  - Programs or systems that carry out design

# Example: SolarWinds

- SolarWinds provides widely used system management tools for network and infrastructure monitoring
  - Among the components is Orion, a performance monitoring system
  - Orion is used by over 30,000 public, private organizations, including government
- Attackers compromised system with Orion source code
- They then altered the source to create a back door
- At next upgrade of Orion, the rigged program was distributed
  - This gave the attackers access to organizations' infrastructure
- FireEye spotted infected customers' systems, then found they had been infected

# Operational Issues

- Cost-benefit analysis
  - Is it cheaper to prevent or recover?
- Risk analysis
  - Should we protect something?
  - How much should we protect this thing?
- Laws and customs
  - Are desired security measures illegal?
  - Will people do them?