Lecture 1
September 25, 2024

Administrative Stuff: Instructors

- Instructor: Matt Bishop, mabishop@ucdavis.edu
  - Office Hours: MWF2:10–3:00pm in 2203 Watershed Sciences
  - When you send email, please put “ECS 235A” in the subject so I will know it is class related
- TA: Lecen Li, lcnli@ucdavis.edu
  - Office Hours: *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-2024-04 (a backup web site)
- Grading
  - 50% Homework
  - 50% Project

Student Resources and No-Nos

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

Projects

- You choose the project
  - Teams: up to 3 people; ask if you want more to join
- Due:
  - Wed Oct 9: topic and team composition
  - Fri Nov 1: progress report
  - Wed Nov 27: presentations (may require slides only)
  - Fri Dec 13: completed projects

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

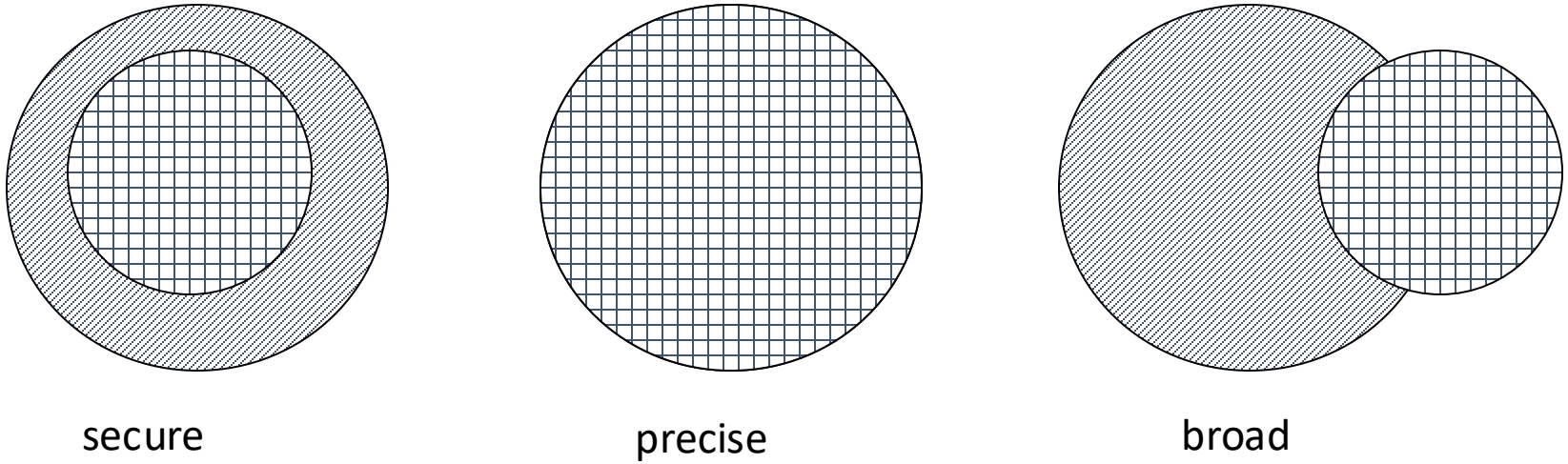
Goals of Security

- 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



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

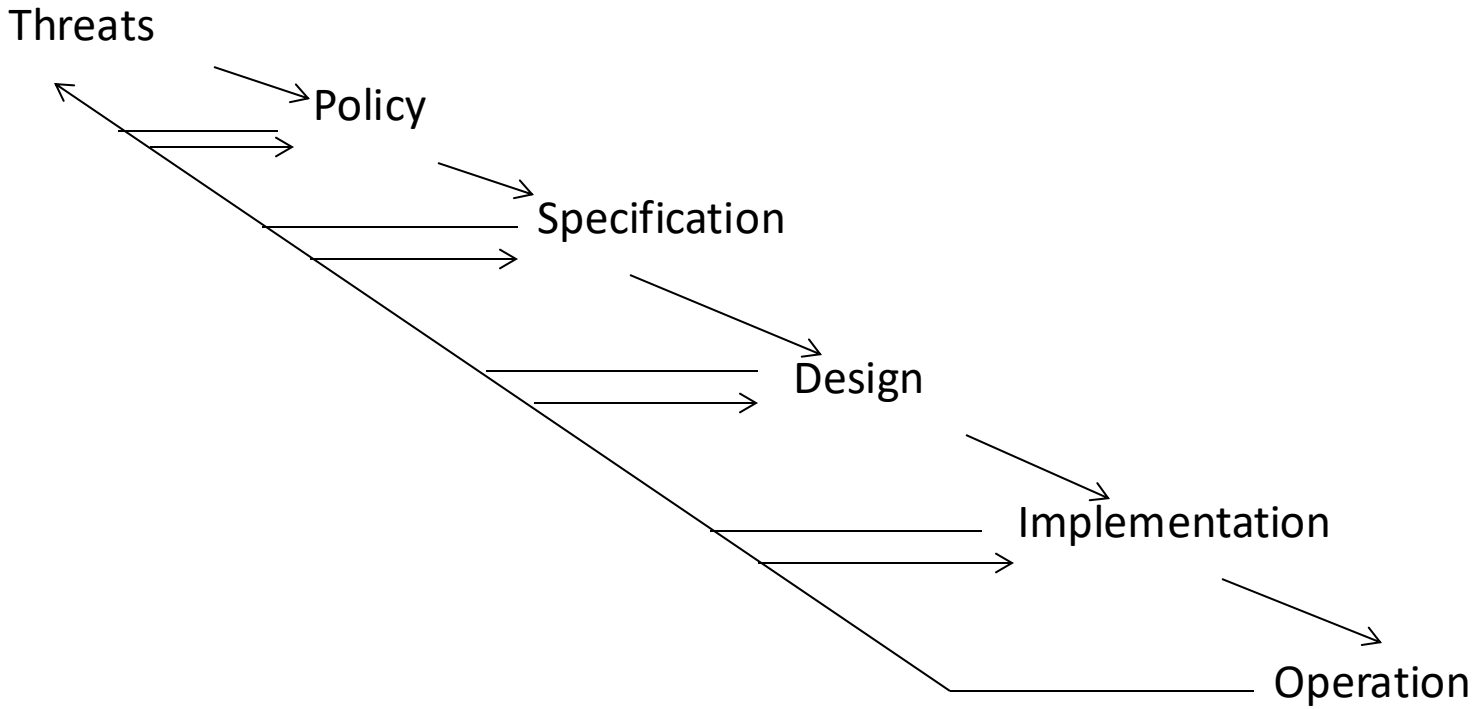
Operational Issues

- 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?

Human Issues

- Organizational problems
  - Power and responsibility
  - Financial benefits
- People problems
  - Outsiders and insiders
  - Social engineering

Tying Together



Key Points

- Policy defines security, and mechanisms enforce security
  - Confidentiality
  - Integrity
  - Availability
- Trust and knowing assumptions
- Importance of assurance
- The human factor