
Information Assurance

Slide Set 1

CS498SH

Fall 2006

Susan Hinrichs

Outline

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

Reading

- For this lecture:
 - First Chapter of Computer Security: Art and Science
- For next lecture:
 - Read Chapter 2 of Computer Security: Art and Science

Administrivia

- Staff
 - Susan Hinrichs, lecturer
 - Jody Boyer, teaching assistant
- Communications
 - Class web page <http://www.cs.uiuc.edu/class/fa05/cs498sh>
 - Newsgroup cs498sh
- Office Hours:
 - Susan: Mondays 11am-1pm
 - Jody: TBA
- Grades
 - 2 midterms worth 25% each. Aiming for Sept 20 and October 27
 - Final worth 25%
 - Roughly weekly homework worth 25%. Can drop low homework
 - Extra project worth 20% for grad students taking for 4 credits

Security Classes at UIUC

- Security course roadmap
 - <http://iti.uiuc.edu/roadmaps/security-roadmap.html>
- Two course security introduction sequence
 - Cover “Computer Security: Art and Science” by Matt Bishop
 - Information Assurance (CS461)
 - Covers NSA 4011 security professional requirements
 - A broad overview of security.
 - Computer Security (CS463)
 - Covers more advanced topics
 - Covers introductory topics in greater depth

Security Classes at UIUC

- Applied Computer Security Lab - CS460
 - Taught in spring
 - With CS461 covers NSA 4013 system administrator requirements
 - Project oriented course. Hands on experience to reinforce how basic security concepts are implemented today.
- Advanced Computer Security - CS598cag
 - Prepares students for research in computer security
 - Seminar style course
- Cryptography
 - Computer science Manoj Prabhakaran teaching CS498PR Theoretical Foundations of Cryptography this semester
 - Similar course taught every other year by Math and ECE departments
- Reading Group
 - Listed as CS591rhc
 - Student lead group. Reads and discusses current security research papers.

Security in the News

- Worms
 - Microsoft Server Service buffer overflow exploit active this summer. Enables remote execution of arbitrary code.
 - Slammer worm crashed nuke power plant network
- Extortion
 - Threaten DDoS attack unless company pays up
 - DDoS protection from carriers can cost \$12K per month
 - <http://www.networkworld.com/news/2005/051605-ddos-extortion.html>
- Identity theft
 - ChoicePoint, Bank of America, disgruntled waiter, lost laptops, phishing
 - Not purely a technology issue
 - Can use technology to detect use after theft
- Spam
 - Washington post June 2004 claims spam costs large companies \$2,000 per employee
 - Claims of \$10-\$50 billion dollars in lost productivity

Security Communities

- Security lore rises from several communities with different motivations
 - Government – Information warfare, protection of critical infrastructures
 - Black hat – Glory, money
 - Industry – Return on investment, customer trust
 - Academia – Scientific method
- Class will draw from all communities

Why Information Assurance?

- Why not just call the course Computer Security?
 - Term focuses on the ultimate protection target
 - Historical government term

Class Topics

- Introduction and motivation
- Security Policies: Access Control Matrix, Confidentiality and integrity policies
- Trusted Operating Systems
- Risk Analysis
- Legislation and security
 - Exam 1 – September 20
- Applied Cryptography: basic crypto, key management, cipher techniques, authentication
- Network security mechanisms
- Legal and ethical issues in security
 - Exam 2 – October 28
- Security design principles, assurance techniques, Auditing
- System evaluation
- Code vulnerabilities and malicious programs
- Physical security
- EMSEC
- Hardware-enforced security

Basic Components

- Confidentiality
 - Keeping data and resources hidden
- Integrity
 - Data integrity (integrity)
 - Origin integrity (authentication)
- Availability
 - Enabling 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

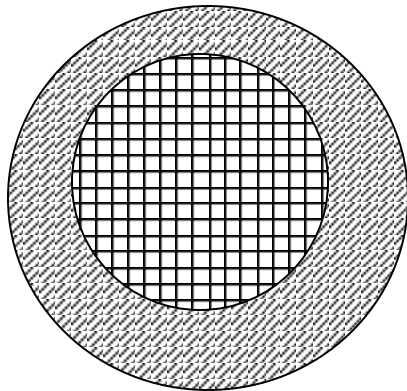
Goals of Security

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

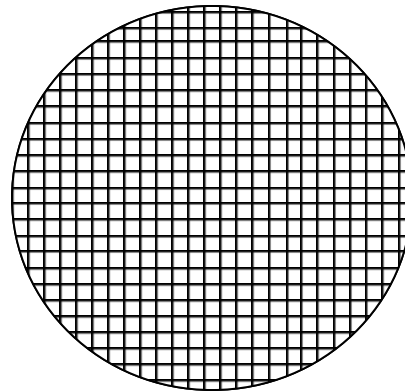
Trust and Assumptions

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

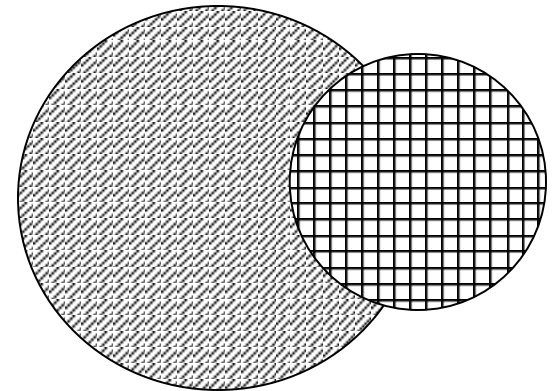
Types of Mechanisms



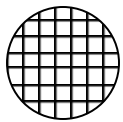
secure



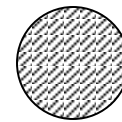
precise



broad



set of reachable states



set of secure states

Assurance

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

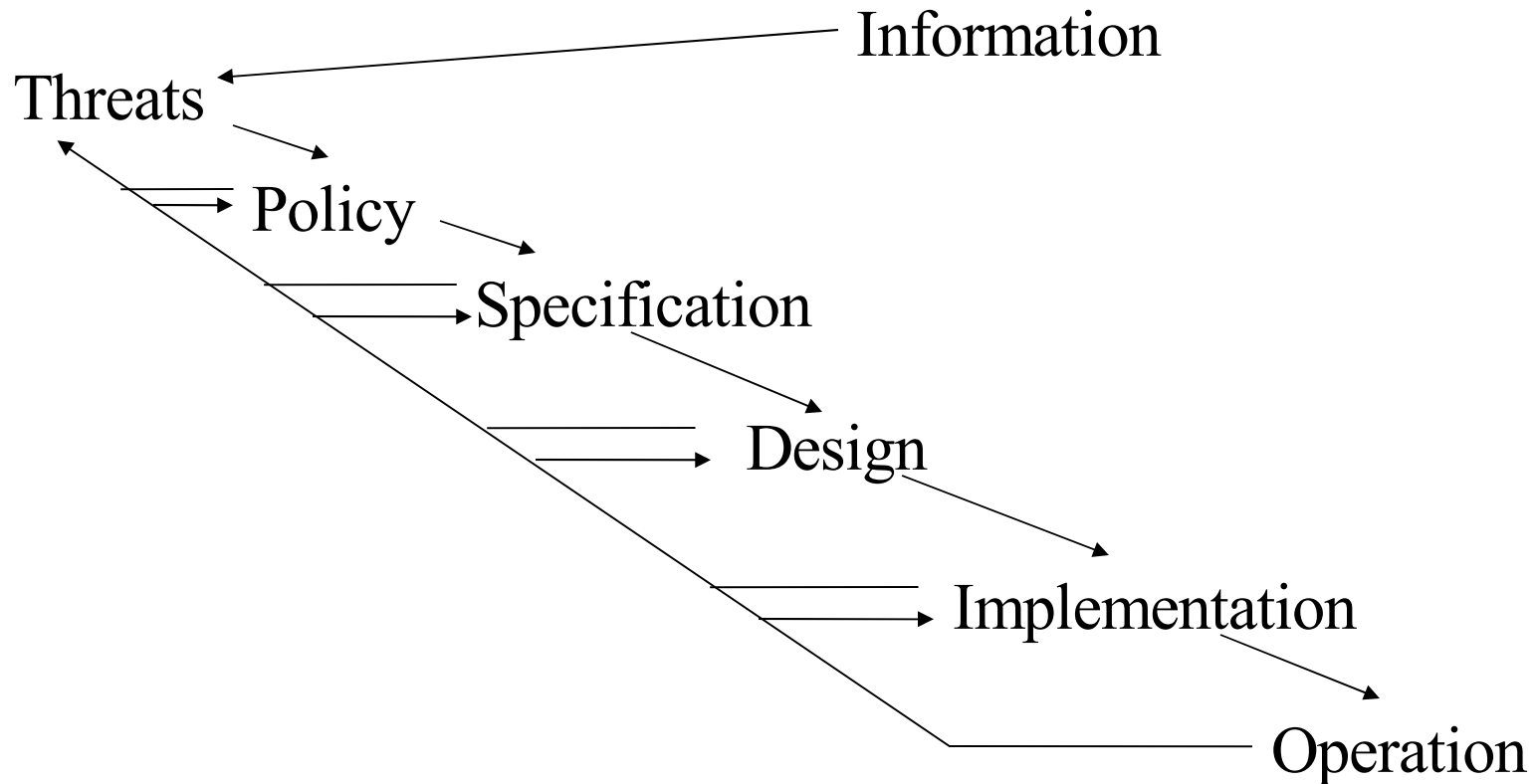
Operational Issues

- 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