

L1: Computer Security Overview



Hui Chen, Ph.D.
Dept. of Engineering & Computer Science
Virginia State University
Petersburg, VA 23806

Acknowledgement

- ❑ Many slides are or are revised from the slides of the author of the textbook
 - Matt Bishop, Introduction to Computer Security, Addison-Wesley Professional, October, 2004, ISBN-13: 978-0-321-24774-5. [Introduction to Computer Security @ VSU's Safari Book Online subscription](#)
 - <http://nob.cs.ucdavis.edu/book/book-intro/slides/>
- ❑ Many labs used in this classes are from the SEED Labs
 - <http://www.cis.syr.edu/~wedu/seed/labs.html>

Outline

- ❑ Experimental environment preparation
 - Creating virtual machines (Lab 1)
- ❑ Basic concepts

Course Overview

- Matt Bishop, Introduction to Computer Security, Addison-Wesley Professional, October, 2004, ISBN-13: 978-0-321-24774-5. [Introduction to Computer Security @ VSU's Safari Book Online subscription](#)

Course Overview

- ❑ Introduction: Chapter 1
- ❑ Access Control Matrix: Sections 2.1 – 2.3
- ❑ Security Policies
 - Sections 4.1 – 4.4
 - Selected sections from Chapter 5, 6, 7
- ❑ Cryptography:
 - Basics: Chapter 8
 - Key distributions: Sections 9.1– 9.2
 - Public Key Infrastructure: Section 9.3
 - Common Errors: Section 10.1
 - Cryptography in networks: Sections 10.3 – 10.4
- ❑ Noncryptographic mechanism
 - Identify: Sections 13.1 – 13.4
 - Identity and anonymity : 13.6
 - Controlling access to files: 14.1 – 14.2
 - Ring-based mechanism: 14.4
- ❑ Assurance
 - Chapter 18
- ❑ Design Principles
 - Chapter 12

Learning Environment

□ Virtual machines

- Use one computer system to emulate another
- Host (host system, host OS, host ...)
- Guest (guest system, guest OS, guest ...)

□ Advantage

- Portability
 - You can take the virtual machine with you
- Isolation
 - Easier to prevent from interfering other systems

Common Virtualization Software

□ VMware

- VMware player is free for non-commercial use
 - Available for Linux and Windows
- Feature-richer versions are available from the department's VMWare/MSDNAA web store
 - Available for Linux, Windows, and Mac OS X

□ Oracle VirtualBox

- Free and available for Linux, Windows, and Mac OS X
- Installed in classroom computers in HM 14S, 201S, and 210S

□

Operating System

- Mostly we use Linux
 - Open-source
 - No need to get license when install on virtual machines

Basic Concepts

- **C**onfidentiality
- **I**ntegrity
- **A**vailability

Confidentiality

- ❑ Concealment of information or resources
- ❑ Access control *mechanism* supports confidentiality
 - Cryptography (cryptographic keys)
 - System-dependent mechanism
- ❑ Information or resources concealed
 - Data
 - Existence of data
 - Resource hiding

Integrity

- ❑ Trustworthiness of data or resources
- ❑ Prevent improper or unauthorized change
- ❑ Types of integrity
 - Data integrity (the content of the information)
 - Origin integrity (the source of data, or authentication)
- ❑ Prevention mechanisms
 - Unauthorized attempts and change in unauthorized ways
- ❑ detection mechanisms
 - Report integrity violations

Availability

- ❑ Ability to use the information or resource desired
- ❑ Denial of service attacks

Threats

- ❑ Threat: *potential* violation of *security*
- ❑ Attacks: actions that may cause violations

Classes of Threats

- ❑ Disclosure: unauthorized access to information
 - Example: snooping
- ❑ Deception: acceptance of false data
 - Modification, masquerading (spoofing), repudiation of origin, denial of receipt
- ❑ Disruption: interruption or prevention of correct operation
 - Modification
- ❑ Usurpation: unauthorized control of a system
 - Modification, masquerading (spoofing), delay, denial of service

Policies and Mechanisms

- Security policy: statement of *what is, and is not, allowed*
 - It defines “security” for a system, a network, or a site
- Security mechanisms: method, tool, or procedure for enforcing a security policy
 - Mechanism can be nontechnical
 - Procedural mechanisms often complement technical mechanisms

Composition of Policies

- ❑ Mathematically, as a list of allowed (secure) and disallowed states
- ❑ In practice, policies often described in natural languages
- ❑ Example: two different systems communicate or cooperate
 - The policy of the network consists of the two are based on the security policies of the two systems
- ❑ If policies conflict, discrepancies may create security vulnerabilities

Goals of Security

- Given a security policy (specifying “secure” and “nonsecure” actions), prevent and detection attacks or recover from attacks via security mechanisms
 - Prevention
 - Detection
 - Recovery

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

Assurance

- Determine “how much” to trust a system
- Specification
 - Requirements analysis
 - Statement of desired functionality
- Design
 - How system will meet specification
- Implementation
 - Programs/systems that carry out design

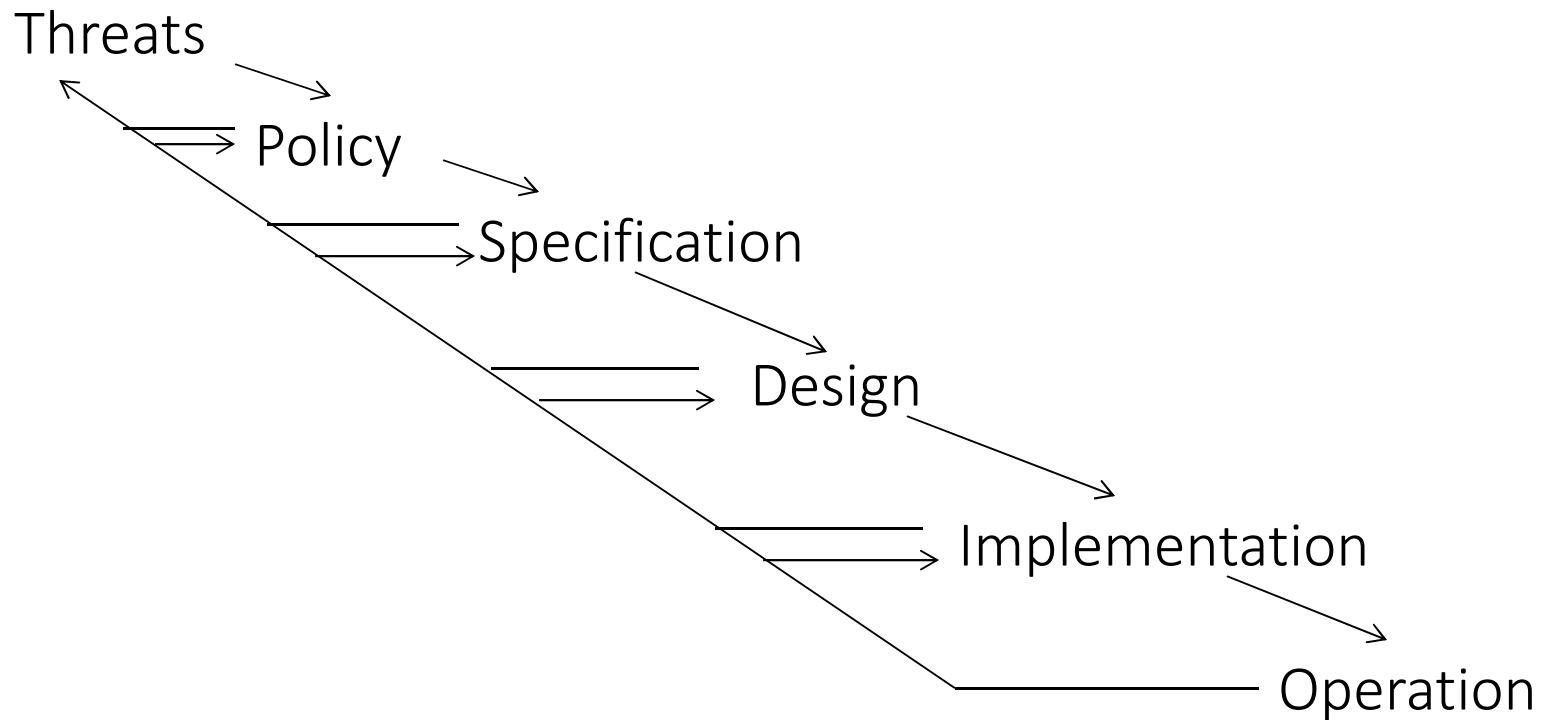
Operational Issues

- ❑ Cost-Benefit Analysis
 - Is it cheaper *to prevent* or *to 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



Lab 1

- ❑ Preparing Virtual-Machine based learning environment
- ❑ Demonstrate that you can run and log in your virtual machine in the class of Monday, August 22, 2016
 - No points for late work

Reading Assignment

- Paper reading and presentation
 - Three-student team makes an oral presentation using PowerPoint (or the similar) in the class on the designated date in the class website
 - **In the slides, state each team member's contribution**
 - The rest of class must prepare and ask questions
 - **The instructor grades students' presentation and class participation**
- Who is the first tem?

Summary

- ❑ Virtual machine based learning environment
- ❑ Policy defines security, and mechanisms enforce security
 - Confidentiality
 - Integrity
 - Availability
- ❑ Trust and knowing assumptions
- ❑ Importance of assurance
- ❑ The human factor