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 version 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
  - Data: encryption (cryptography)
  - Existence of data: steganography
  - Resource hiding
  - Identity (anonymity)

Integrity

- Trustworthiness of data or resources
  - Data integrity
  - Program integrity
  - System integrity
  - Identity integrity (non-repudiation)
  - Origin (location) integrity

Availability

- Ability to use the information or resource desired
- Threat
  - Denial of service
- Tradeoff
  - Confidentiality
  - Integrity
  - Availability

Threats

- Threat: *potential* violation of security

- What may be the threats?
  - When using computer systems?
  - When setting up computer systems and networks?
  - When developing computer programs and systems?

Classes of Threats

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

Policies and Mechanisms

- Policy says *what is, and is not, allowed*
  - It defines "security" for a system, a network, or a site
- Mechanisms enforce policies
- Composition of policies
  - 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

- Prevention: prevent attackers from violating security policy
  - Make it impossible (prevention)
  - Make it harder (deterrence)
  - Make other targets more attractive (deflection)
- Detection: detect attackers' violation of security policy
  - Monitoring
  - Intrusion detection
- Recovery
  - Identify damage
  - Recover data
  - Find the cause (individuals, bugs, misconfiguration …)
  - Continue to function 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

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 *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*

THE FBI FEDERAL BUREAU OF INVESTIGATION

CONTACT US | ABOUT US | MOST WANTED | NEWS | STATS

San Diego Division

Home • San Diego • Press Releases • 2013 • FBI Warns Public That Cyber Criminals Continue to Use Spear-Phishing Att

Twitter (16) Facebook Share

FBI Warns Public That Cyber Criminals Continue to Use Spear-Phishing Attacks to Compromise Computer Networks

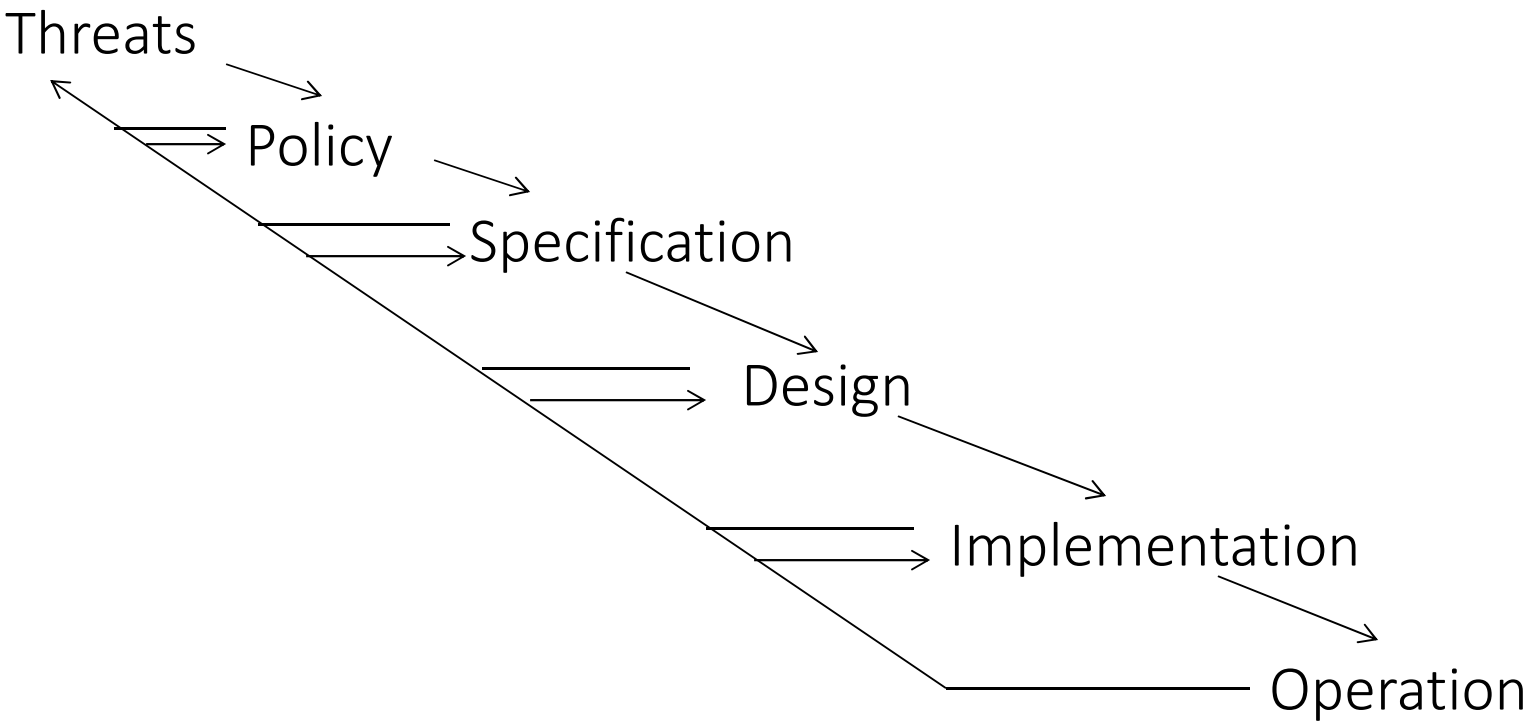
FBI San Diego
July 12, 2013

Darrell Foxworth
(858) 320-8302

The FBI has seen an increase in criminals who use spear-phishing attacks to target multiple industry sectors. These attacks allow criminals to access private computer networks. They exploit that access to create fake identities, steal intellectual property, and compromise financial credentials to steal money from

Excerpt from https://www.fbi.gov

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

- In Class Website
  - http://sest.vsu.edu/~hchen/course/CSCI451/
- Paper reading and presentation
  - Two student team makes an oral presentation using PowerPoint (or the similar) in the class of Monday, August 24, 2015
  - The rest of class must prepare and ask questions
  - The instructor grades students' presentation and participation

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