
Information Assurance/Computer Security Introduction

CS461/ECE422

Fall 2007

Susan Hinrichs

Outline

- Administrative Issues
- Class Overview
- Information Assurance Overview
 - Components of computer security
 - Threats, Vulnerabilities, Attacks, and Controls
 - Human Issues

Administrivia

- Staff
 - Susan Hinrichs, lecturer
 - Ravinder Shankesi, TA
 - Lars Olson, grader
- Communications
 - Class web page <http://www.cs.uiuc.edu/class/fa07/cs461>
 - Newsgroup cs461
- Office Hours
 - Susan: 3-4pm Monday and after class
 - Ravinder: 7-8pm Tuesday and 3-4pm Thurs

More Administrivia

- Grades
 - 2 midterms worth 25% each. Sept 26 and October 31
 - Final worth 25%
 - Roughly weekly homework worth 25%. Can drop low homework
 - Extra project worth 20% for grad students taking for 4 credits
 - Submitting homeworks via compass
- Class Sections
 - १. Online students: geographically distributed
 - २. ECE and CS 3 and 4 credit sections
 - ३. CS ADD section
- 2. and 3. take exam during normal class time. Extra room assigned
- 3. can attend class in person assuming there is space

Security Classes at UIUC

- Three introductory courses
 - Information Assurance (CS461/ECE422)
 - Covers NSA 4011 security professional requirements
 - Taught every semester
 - Computer Security (CS463/ECE424)
 - Continues in greater depth on more advanced security topics
 - Taught every semester
 - Applied Computer Security Lab
 - Taught last spring as CS498sh Will be CS460
 - With CS461 covers NSA 4013 system administrator requirements
- Two of the three courses will satisfy the Security Specialization in the CS track for Computer Science majors.

More Security Classes at UIUC

- Theoretical Foundations of Cryptography
 - Taught once a year, this semester as CS498pr
- Security Reading Group CS591RHC
- Advance Computer Security
 - Taught once a year, this semester as CS598cag
 - <http://www.cs.uiuc.edu/class/fa07/cs598cag/>
- Math 595/ECE 559 – Cryptography
 - <http://www.math.uiuc.edu/%7Eduursma/Math595/>
 - Taught every couple years

Other Sources for Security News

- Bruce Schneier's blog
<http://www.schneier.com/blog/>
- Internet Storm Center <http://isc.sans.org/>
- Local talks
 - <http://www.iti.uiuc.edu/seminars.html>

Security Communities

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

Security in the News

- InfoWar
 - Estonia <http://blog.wired.com/27bstroke6/2007/08/cyber-war-and-e.html>
- 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
 - Monster.com 1.6 million affected
 - http://blog.washingtonpost.com/securityfix/2007/08/would_you_like_a_jol
 - ChoicePoint, Bank of America, disgruntled waiter
 - Often not purely a technology issue
- Spam
 - Washington post June 2004 claims spam costs large companies \$2,000 per employee
- Worms
 - Slammer worm crashed nuke power plant network

Security is not a Point Product



Class Topics

- Mix of motivation and mechanisms
- See lecture page
 - <http://www.cs.uiuc.edu/class/fa07/cs461/lectures>.
- A few open lecture spots if there are topics of particular interest

Security Components

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

Example

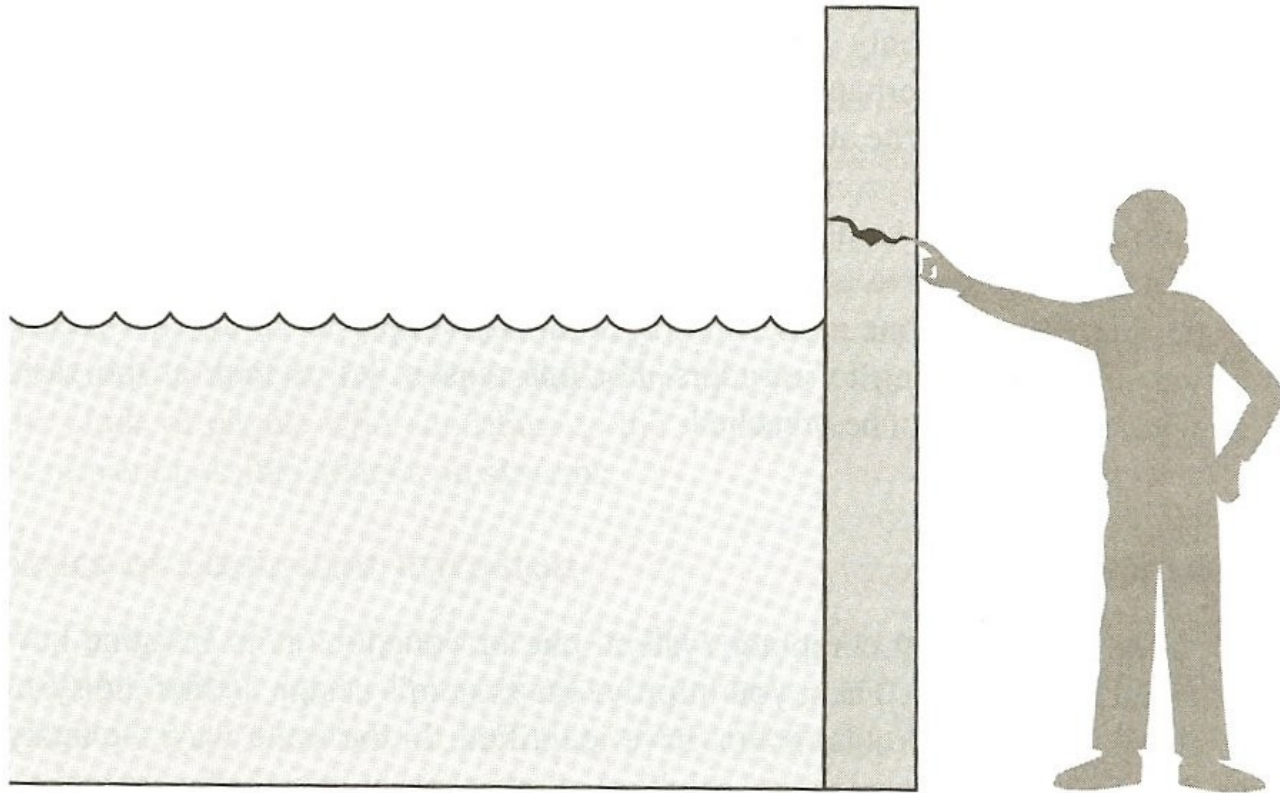


FIGURE 1-1 Threats, Controls, and Vulnerabilities.

Identifying Terms

- Vulnerability – Weakness in the system that could be exploited to cause loss or harm
- Threat – Set of circumstances that has the potential to cause loss or harm
- Attack – When an entity exploits a vulnerability on system
- Control – A means to prevent a vulnerability from being exploited

Types of threats

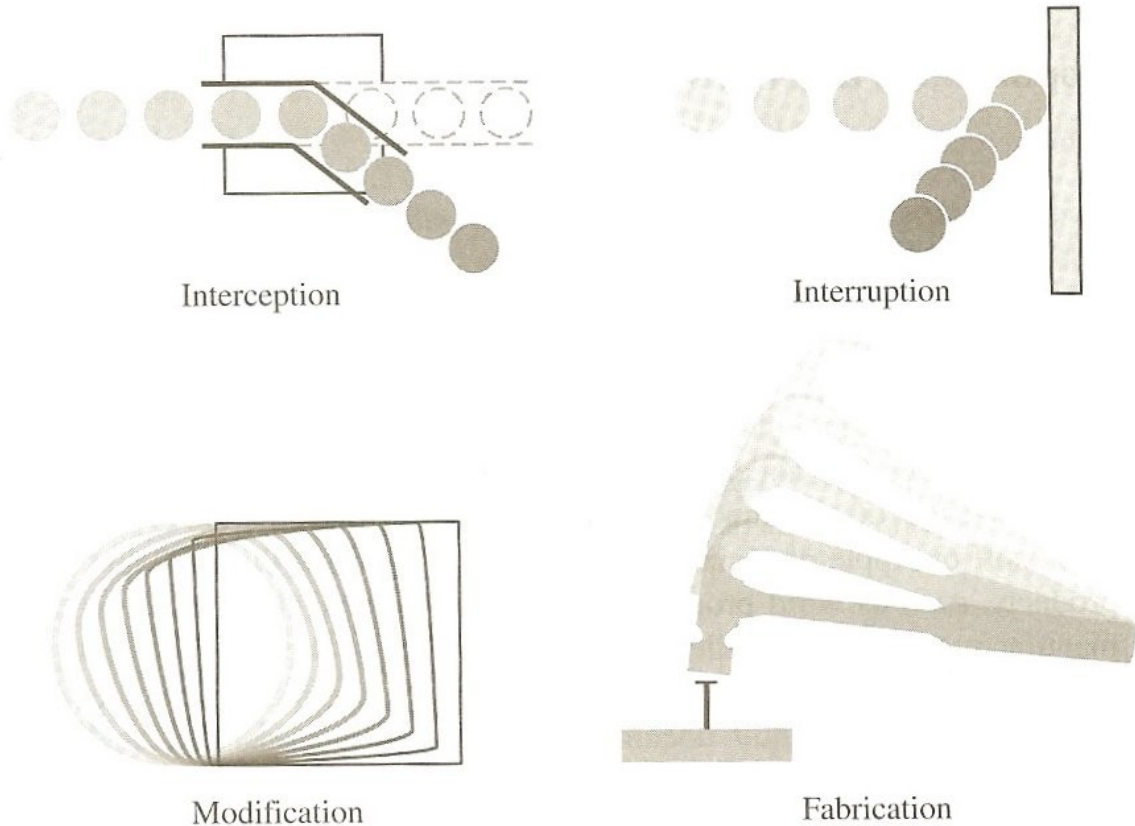


FIGURE 1-2 System Security Threats.

Types of threats

- Interception – an unauthorized party gains access
- Interruption – Prevent access to the asset
- Modification – Change the asset
- Fabrication – Create a counterfeit asset

Hardware Threats

Software Threats

Data Threats

Understanding the attacker

- Method – ability, resources, etc. to pull off attack
- Opportunity – time and access
- Motive – reason to perform attack

Example: Bored Teenager

- Method
- Opportunity
- Motive

Example: Nation State

- Method:
- Opportunity
- Motive

Example: Internal Engineer

- Method
- Opportunity
- Motive

Key Points

- Must look at the big picture when securing a system
- Main components of security
 - Confidentiality
 - Integrity
 - Availability
- Differentiating Threats, Vulnerabilities, Attacks and Controls
- The human factor – understand the attacker