Introductory Computer Security

CS461/ECE422

Fall 2009

Susan Hinrichs

Outline

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

Administrivia

- Staff
  - Susan Hinrichs, lecturer
  - Fariba Khan, TA
  - Omid Fatemieh, TA
- Communications
  - Class web page http://www.cs.illinois.edu/class/fa09/cs461
  - Newsgroup cs461
  - Jabber Chat room cs461
- Office Hours
  - Susan: 12:30-1:30pm Wednesday and after class
  - Fariba and Omid: TBA

More Administrivia

- Grades
  - 2 midterms worth 25% each.
    - October 7 and November 18.
  - Final worth 25%.
    - December 18.
  - Roughly weekly homework worth 25%. Can drop low homework. 8 homeworks last year.
  - Extra project worth 20% for grad students taking for 4 credits
  - Submit homework via compass
- Class Sections
  1. Online students: geographically distributed
  2. ECE and CS 3 and 4 credit sections

A Few Words on Class Integrity

- Review department and university cheating and honor codes:
  - https://agora.cs.illinois.edu/display/underg
  - http://admin.illinois.edu/policy/code/articl
- This has been an issue in the past
- Expectations for exams, homeworks, and projects

Class Readings

- Text *Computer Security: Art and Science* by Matt Bishop
- Additional readings provided via compass or public links
- Books on reserve at the library

Class Format

- Meet three times a week
- Mostly lecture format
  - Will attempt to have a class exercise about once a week. Will be noted on class web site.
  - Will attempt to make this relevant for online students too.
- Lectures video taped for online students
  - All have access to tapes. Link on class web site.
- A few lectures will be video only. Noted on schedule
  - Will still play video in class
- Posted slides not sufficient to master material alone

Class communication

- Limited physical access
  - Lecturer part time on campus
- Use technology to help
  - Newsgroup for timely, persistent information
  - Jabber and Jabber chat room for questions and conversation
  - Email and phone

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 or so
  - 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 about once a year, last year as CS498pr
- Security Reading Group CS591RHC
- Advance Computer Security
  - Taught once a year, this semester as CS598cag
- Math 595/ECE 559 – Cryptography
  - http://www.math.uiuc.edu/%7Eduursma/Math595
  - Taught every couple years
- ITI Security Roadmap
  - http://www.iti.illinois.edu/content/security

Other Sources for Security News

- Bruce Schneier's blog
  http://www.schneier.com/blog/
- Local talks
  - http://www.iti.illinois.edu/content/seminars-ar

Security in the News

- DNS flaws
  - Dan Kamisky found flaw in widely used DNS protocol requiring upgrade of network infrastructure
  - http://blog.wired.com/27bstroke6/2008/07/details-of-dns.html
- 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
- Privacy/Identity theft
  - Albert Gonzalez and 130 million credit card numbers.
  - Cars.gov ?
  - ChoicePoint, Bank of America, disgruntled waiter
- Worms
  - Conflicker, twitter worms
  - Slammer worm crashed nuclear power plant network

Class Topics

- Mix of motivation, design, planning, and mechanisms
- See lecture page
  - http://www.cs.illinois.edu/class/fa09/cs461/lectur
- A few open lecture spots if there are topics of particular interest
- May have some industry guest lectures

Security Components

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

CIA Examples

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

Example

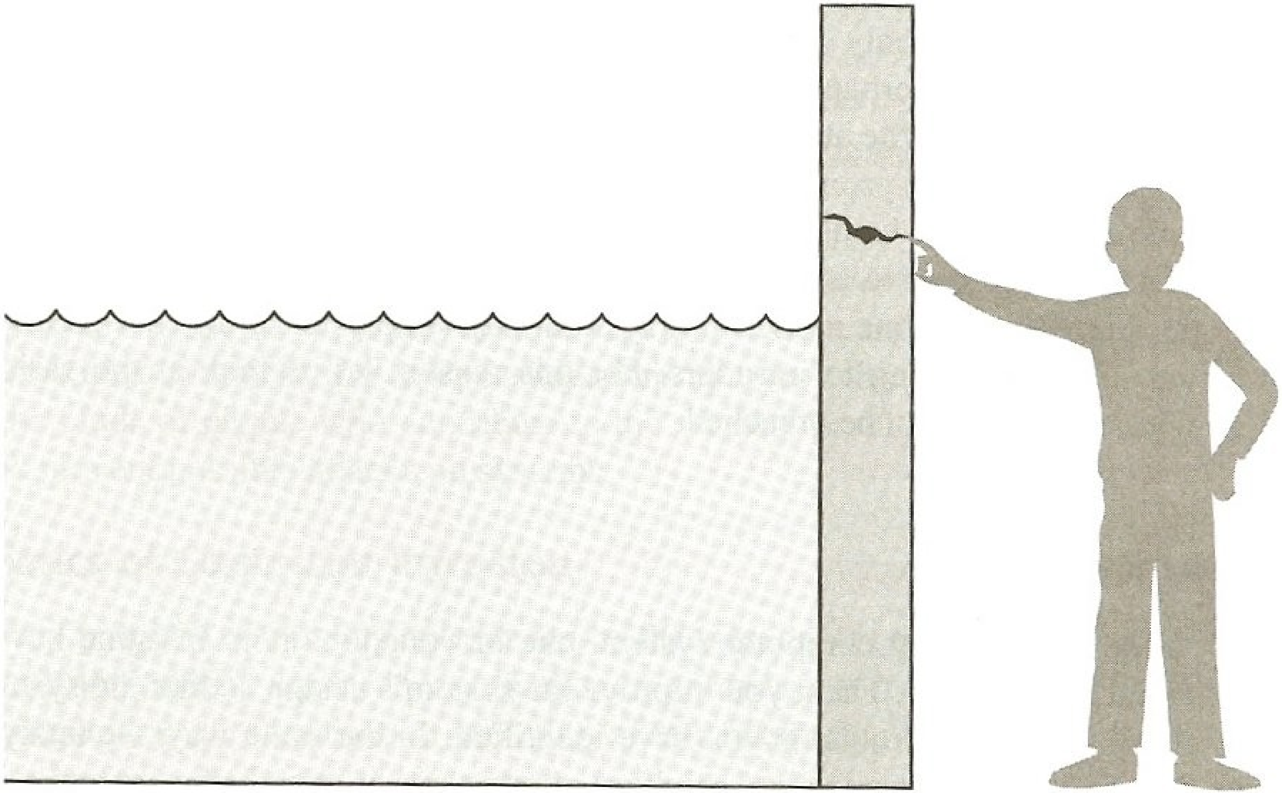

FIGURE 1-1 Threats, Controls, and Vulnerabilities.

Classes of Threats

- Disclosure – Unauthorized access to information
- Deception – Acceptance of false data
- Disruption – Interruption or prevention of correct operation
- Usurpation – Unauthorized control of some part of a system

Some common threats

- Snooping
  - Unauthorized interception of information
- Modification or alteration
  - Unauthorized change of information
- Masquerading or spoofing
  - An impersonation of one entity by another
- Repudiation of origin
  - A false denial that an entity sent or created something.
- Denial of receipt
  - A false denial that an entity received some information.

More Common Threats

- Delay
  - A temporary inhibition of service
- Denial of Service
  - A long-term inhibition of service

More definitions

- Policy
  - A statement of what is and what is not allowed
  - Divides the world into secure and non-secure states
  - A secure system starts in a secure state. All transitions keep it in a secure state.
- Mechanism
  - A method, tool, or procedure for enforcing a security policy

Is this situation secure?

- Web server accepts all connections
  - No authentication required
  - Self-registration
  - Connected to the Internet

Policy Example

- University computer lab has a policy that prohibits any student from copy another student's homework files.
  - The computers have file access controls to prevent other's access to your files.
- Bob does not read protect his files
- Alice copies his files
- Who cheated? Alice, Bob, both, neither?

More Example

- What if Bob posted his homework on his dorm room door?
- What if Bob did read protect his files, but Alice found a hack on the mechanism?

Trust and Assumptions

- Locks prevent unwanted physical access.
  - What are the assumptions this statement builds on?

Policy Assumptions

- Policy correctly divides world into secure and insecure states.
- Mechanisms prevent transition from secure to insecure states.

Another Policy Example

- Bank officers may move money between accounts.
  - Any flawed assumptions here?

Assurance

- Evidence of how much to trust a system
- Evidence can include
  - System specifications
  - Design
  - Implementation
- Mappings between the levels

Aspirin Assurance Example

- Why do you trust Aspirin from a major manufacturer?
  - FDA certifies the aspirin recipe
  - Factory follows manufacturing standards
  - Safety seals on bottles
- Analogy to software assurance

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
- Policy vs mechanism
- Assurance