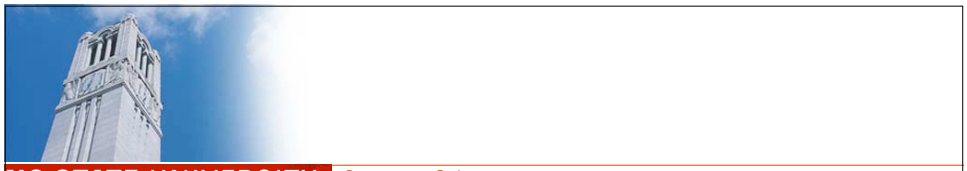


NC STATE UNIVERSITY Computer Science

CSC 405
Introduction to Computer Security

Course Introduction

About Instructor

- Dr. Peng Ning, associate professor of computer science
  - http://www.csc.ncsu.edu/faculty/ning
  - pning@ncsu.edu
  - (919)513-4457
  - Office: Room 3258, EB II
  - Office hours: Mondays and Wednesdays, 3:45pm – 4:45pm

About TA

- Yuzheng Zhou
  - yzhou3@ncsu.edu
- Office hours:
  - Tuesdays 1pm -- 3pm
  - EB II, Room 3234

Course Outline

- Basic Security Concepts
  - Threats, vulnerabilities, controls
  - Confidentiality, integrity, availability
  - Security policies, security mechanisms, assurance
- Basic Cryptography
  - Basic cryptography terms
  - Historical background
  - Secret key cryptosystems
  - Public key cryptosystems
  - Hash functions

Course Outline (Cont'd)

- Program Security
  - Malicious code
  - Program flaws
  - Defenses
- Security in Conventional Operating Systems
  - Memory, time, file, object protection
  - Identification
  - Authentication

Course Outline (Cont'd)

- Trusted Operating Systems
  - Assurance, trust
  - Design principles
  - Evaluation criteria
  - Evaluation process
- Database Management Systems Security
  - Database integrity
  - Database secrecy
  - Inference control
  - Multilevel databases

Course Outline (Cont'd)

- Network Security
  - Network threats: eavesdropping, spoofing, modification, denial of service attacks
  - Introduction to network security techniques
  - Take CSC 474 for more in-depth treatment of network security
- Management of Security
  - Security policies
  - Risk analysis
  - Physical threats and controls

Course Outline (Cont'd)

- Miscellaneous Topics
  - Legal aspects of security
  - Privacy and ethics

Course Projects

- Operating Systems Security Labs
  - Adopted from the SEED project at Syracuse
  - Use an instructional OS (Minix) on VMWare
  - One project requires Linux on VMWare
  - You are encouraged to use your own computer, but VCL access is available
  - Tentative list of projects
    - Warm up
    - Set UID lab
    - Set Random UID lab
    - Capability lab

Prerequisites

- CSC 246: Concepts and Facilities of Operating Systems for Computer Scientists
  - Basic knowledge of operating systems
  - C programming skills

Textbook and Handouts

- Required textbook
  - Charles P. Pfleeger and Shari L. Pfleeger. Security in Computing (3rd edition). Prentice-Hall. 2003. ISBN: 0-13-035548-8.

On-line Resources

- WWW page
  - http://courses.ncsu.edu/csc405/lec/001/
  - For course materials, e.g., lecture slides, homework files, papers, tools, etc.
  - Will be updated frequently. So check frequently.
- Message board
  - http://courses.ncsu.edu/csc405
  - For discussions, Q&As.

Grading

- Assignments 10%, midterm 30%, final 30%, project 30%
- The final grades are computed according to the following rules:
  - **A+: >= 95%; A: >= 90% and < 95%; A-: >= 85% and < 90%;**
  - **B+: >= 80% and < 85%; B: >= 75% and < 80%;**
  - **B-: >= 70% and < 75%; C+: >= 66% and < 70%;**
  - **C: >= 63% and < 66%; C-: >= 60% and < 63%;**
  - **D+: >= 56% and < 60%; D: >= 53% and < 56%;**
  - **D-: >= 50% and < 53%;**
  - **F: < 50%.**

Policies on incomplete grades and late assignments

- Homework and project deadlines will be hard.
- Late homework will be accepted with a 10% reduction in grade for each class period they are late by.
- Once a homework assignment is discussed in class, submissions will no longer be accepted.
- All assignments must be turned in before the start of class on the due date.

Policies on absences and scheduling makeup work

- You may be excused from an exam only with a university approved condition, with proof. For example, if you cannot take an exam because of a sickness, we will need a doctor's note.
- Events such as going on a business trip or attending a brother's wedding are not an acceptable excuse for not taking an exam at its scheduled time and place.
- You will have one chance to take a makeup exam if your absence is excused. There will be no makeup for homework assignments.

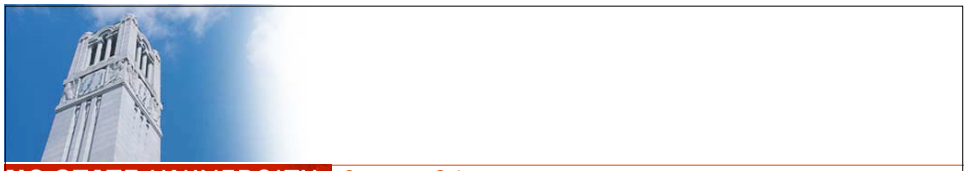
Academic integrity

- The university, college, and department policies against academic dishonesty will be strictly enforced.
- You may obtain copies of the NCSU Code of Student Conduct from the Office of Student Conduct, or from the following URL.
- http://www.fis.ncsu.edu/ncsulegal/41.03-codeof.htm

NC State policy on working with students with disabilities

- Reasonable accommodations will be made for students with verifiable disabilities.
  - Please schedule an appointment with the instructor.
- In order to take advantage of available accommodations, students must register with Disability Service for Students at 1900 Student Health Center, Campus Box 7509, 515-7653.
  - http://www.ncsu.edu/provost/offices/affirm_action/dss/
- For more information on NC State's policy on working with students with disabilities, please see
  - http://www.ncsu.edu/provost/hat/current/appendix/appen_k.html.

Check the website for details!



NC STATE UNIVERSITY Computer Science

CSC 405
Introduction to Computer Security

Topic #1. Introduction

Information Security Problems

- Public, private, and government networks have been penetrated by unauthorized users and rogue programs
- Increased volume of security breaches attributed Computer Emergency Response Team (CERT) reports a tremendous increase in cracking incidents
- Insider attacks

Information Security Concerns

- Distributed Denial of Service (DDOS) attacks
- Worm attacks (e.g., code red)
- Monitoring and capture of network traffic
  - User IDs, passwords, and other information are often stolen on Internet
- Exploitation of software bugs
- Unauthorized access to resources
  - Disclosure, modification, and destruction of resources
- Compromised system used as hostile attack facility
- Masquerade as authorized user or end system
- Data driven attacks
  - Importation of malicious or infected code
- E-Mail forgery

Contributing Factors

- Lack of awareness of threats and risks of information systems
  - Security measures are often not considered until an Enterprise has been penetrated by malicious users
- Wide-open network policies
  - Many Internet sites allow wide-open Internet access
- Vast majority of network traffic is unencrypted
  - Network traffic can be monitored and captured

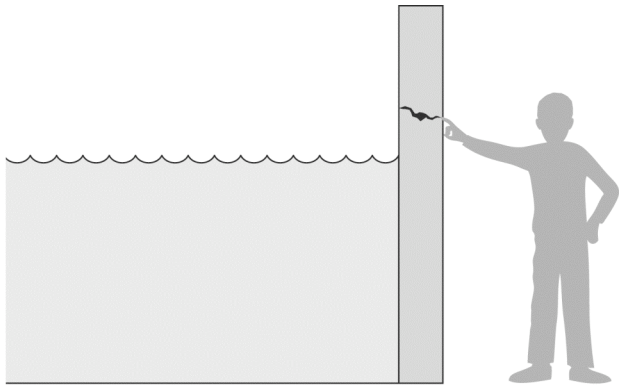
Contributing Factors (Cont'd)

- Complexity of security management and administration
- Exploitation of software (e.g., protocol implementation) bugs
  - Example: Sendmail bugs
- Cracker skills keep improving

Threats, Vulnerabilities, and Controls

- Vulnerability
  - Weakness in the security system that might be exploited to cause loss or harm
  - Example: no authentication for data access
- Threat
  - A set of circumstances that has the potential to cause loss or harm
  - Risk: the possibility for threat to cause harm
- Control
  - A protective measure
  - An action, procedure, or technique that removes or reduces a vulnerability

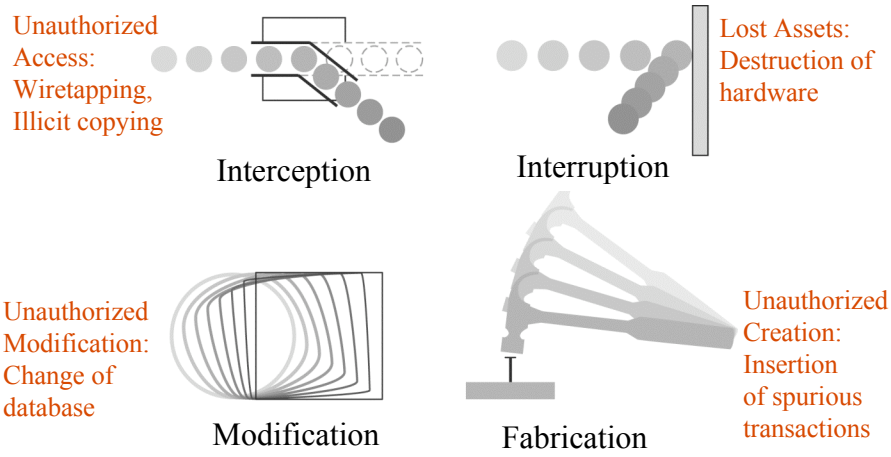
Threats, Vulnerabilities, and Controls (Cont'd)



Pfleeger/Pfleeger Fig. 01-01

- A *threat* is blocked by *control* of a *vulnerability*

System Security Threats

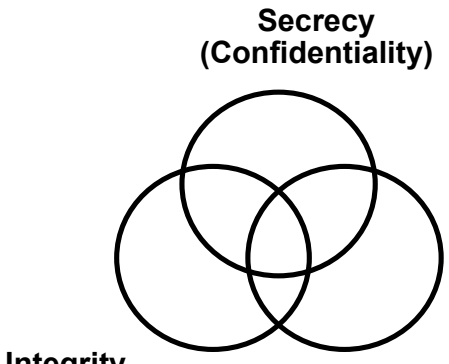


Pfleeger/Pfleeger Fig. 01-02

Security Goals

- Confidentiality (Secrecy)
  - Computer related assets can only be accessed by authorized parties
- Integrity
  - Computer related assets can be modified only by authorized parties
- Availability
  - Assets are accessible to authorized parties at appropriate times
  - Authorized parties cannot be denied access to the assets
- These could mean different things in different contexts

Relationship between Security Goals



The three goals can be independent, can overlap, and can even be mutually exclusive.

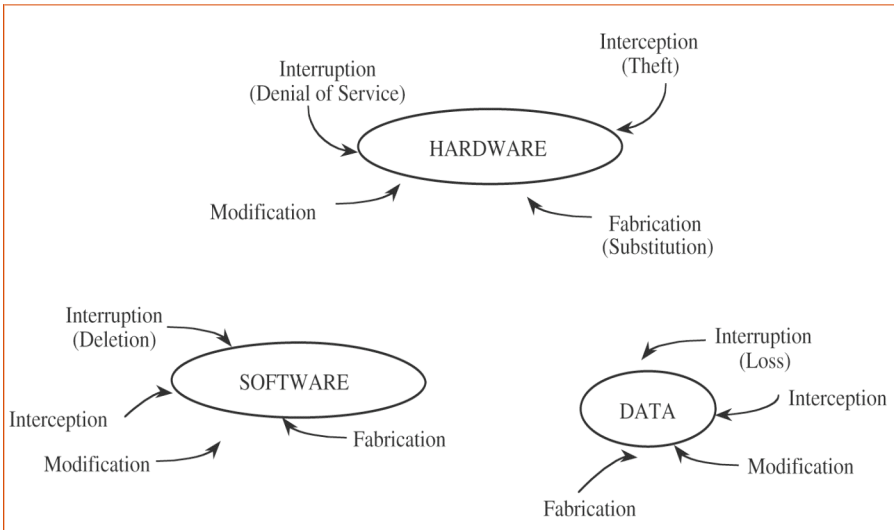
Commercial Example

- Secrecy — An employee should not come to know the salary of his manager
- Integrity — An employee should not be able to modify the employee's own salary
- Availability — Paychecks should be printed on time as stipulated by law

Military Example

- Secrecy — The target coordinates of a missile should not be improperly disclosed
- Integrity — The target coordinates of a missile should not be improperly modified
- Availability — When the proper command is issued the missile should fire

Vulnerabilities of Computer Systems



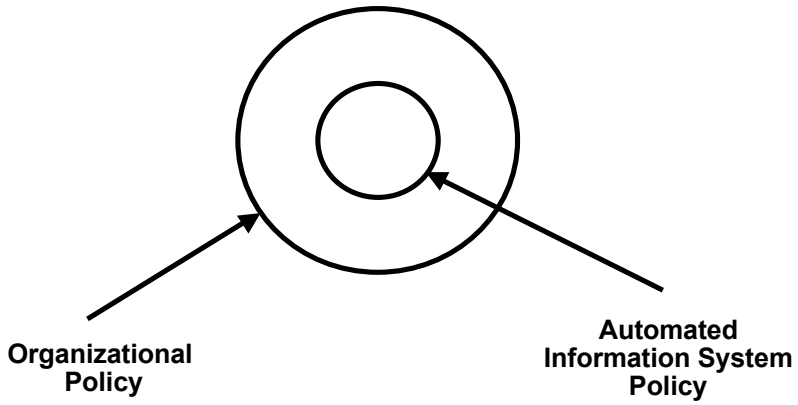
Computer Criminals

- Amateurs
  - Normal people who discover they have access to something valuable
  - Used to be the main source of computer crimes
- Crackers
  - People who break in for challenges, curiosity, self-satisfaction
- Career criminals
  - Computer professionals or groups engaging in computer crimes
  - Spam, phishing emails/websites, blackmail, credit card crimes, …
  - Now the main source of computer crimes

Achieving Security Goals

- Security policy — What?
- Security mechanism (control) — How?
- Security assurance — How well?

Security Policy



Security Mechanism

- Prevention — Access control
- Detection — Auditing and intrusion detection
- Tolerance — Practicality

Good prevention and detection both require good authentication as a foundation

Security Mechanism

- Security mechanisms implement functions that help *prevent*, *detect*, and *respond* to security attacks
- Prevention is more fundamental
  - Detection seeks to prevent by threat of punitive action
  - Detection requires that the audit trail be protected from alteration
- Sometime detection is the only option, e.g.,
  - Accountability in proper use of authorized privileges
  - Modification of messages in a network
- Security functions are typically made available to users as a set of *security services* through APIs or integrated interfaces
- Cryptography underlies (almost) all security mechanisms

Overview of Security Mechanisms (Controls)

- Encryption
- Software controls
  - E.g., OS controls
- Hardware controls
  - E.g., firewalls
- Policies and procedures
  - E.g., frequent changes of passwords
- Physical controls
  - E.g., locked doors, guards

Enhance the Effectiveness of Controls

- Awareness of problem
  - People using controls must be convinced of the need for security
- Likelihood of use
  - Controls must be efficient, easy to use, and appropriate
- Overlapping controls
  - Few controls are permanently effective
  - Judging the effectiveness of a control is an ongoing task
    - Periodic review
  - Combination of controls addressing a single vulnerability
    - Layered defense

Security Assurance

- How well your security mechanisms guarantee your security policy
- Everyone wants high assurance
- High assurance implies high cost
  - May not be possible
- Trade-off is needed

A Misconception: Security by Obscurity

- Security by obscurity says that if we hide the inner workings of a system it will be secure
- It is a bad idea
- Less and less applicable in the emerging world of vendor-independent open standards
- Less and less applicable in a world of widespread computer knowledge and expertise