CSC 474/574
Information Systems Security

Dr. Peng Ning
ning@csc.ncsu.edu
http://www.csc.ncsu.edu/faculty/ning
(919) 513-4457

About Instructor

- Dr. Peng Ning, assistant professor of computer science
  - http://www.csc.ncsu.edu/faculty/ning
  - ning@csc.ncsu.edu
  - (919)513-4457
  - Office: Room 250 (in Suite 243), Venture III, centennial campus
  - Office hours: Tuesdays and Thursdays, 3:00pm – 4:00pm
About TA

- Kun Sun
  - ksun3@unity.ncsu.edu
- Office hours:
  - Thursdays, 2pm -- 4pm
  - Room 252 (in Suite 243), Venture III

Course Objectives

- Understanding of basic issues, concepts, principles, and mechanisms in information systems security.
  - Basic security concepts.
  - Introduction to cryptography.
  - Access control
  - Database security
  - Network security
  - Security management
- Be able to determine appropriate mechanisms for protecting information systems.
Course Styles

- Descriptive: what is out there.
- Critical: what is wrong with ...
- Both knowledge and skill oriented
  - Homework, projects, papers.
- Interactive: discussion and questions encouraged.

Course Outline

- Basic Security Concepts
  - Confidentiality, integrity, availability
  - Security policies, security mechanisms, assurance
- Cryptography and Its Applications
  - Basic number theory
  - Secret key cryptosystems
  - Public key cryptosystems
  - Hash function
  - Key management
- Identification and Authentication
  - Basic concepts of identification and authentication
  - Password authentication
Course Outline (Cont’d)

• Access Control
  – Basic concepts of access control
  – Discretionary access control and mandatory access control
  – Lattice-based Models
  – Covert Channels
  – Noninterference Models
  – Chinese Wall Security Policy
  – Role based Access Control

Course Outline (Cont’d)

• Assurance
  – Evaluation of Secure Information Systems
  – TCSEC, TNI, Common Criteria

• Database Security
  – Introduction to database security
  – Related course: CSC 591D Database Security
Course Outline (Cont’d)

- Network and Distributed Systems
  - Issues in Network and Distributed Systems Security
  - Firewall, Virtual Private Network, Secure Email, etc.
  - Introduction to IPSEC, SSL, ISAKMP/Oakley, etc.
  - Related course: CSC 774 Network Security
- Program Security
  - Virus, Trojan horse, and other malicious software

Course Outline (Cont’d)

- Auditing and Intrusion Detection
- Administrating Security
  - Risk Analysis.
  - Security Planning.
  - Organizational Security Policies
- Physical Security and Beyond
  - Physical security
  - TEMPEST
  - Legal and ethical issues in security, environmental issues, etc.
Prerequisites

- CSC 401 (Data and Computer Communications Networks)
- CSC 440 (Database Management Systems)
  - Further requires
    - CSC 216 (Programming Concepts – Java)
    - CSC 226 (Discrete Mathematics)

Textbook and Handouts

- Required texts
  - Research papers listed on the course website.
On-line Resources

- WWW page: [http://courses.ncsu.edu/csc574/lec/001](http://courses.ncsu.edu/csc574/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/csc574](http://courses.ncsu.edu/csc574)
  - For discussions, Q&As.

Grading

- CSC 474: Assignments 20%, midterm 40%, final 40%.
- CSC 574: Assignments 15%, project 15%, midterm 35%, final 35%.
- 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
Course Project

• Can be (a combination of):
  – Design of new algorithms and protocols.
    • Or new attacks!
  – Analysis/evaluation of existing algorithms, protocols, and systems.
    • Vulnerabilities, efficiency, etc.
  – Implementation and experimentation.

• Small team - one to three persons.

• Proposal, work, and final demo/write-up.

• Suggested topics (see course website), but you can define your own.

Check the website for details!
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)

- Lack of security in TCP/IP protocol suite
  - Most TCP/IP protocols not built with security in mind
  - Work is actively progressing within the Internet Engineering Task Force (IETF)
- Complexity of security management and administration
- Exploitation of software (e.g., protocol implementation) bugs
  - Example: Sendmail bugs
- Cracker skills keep improving

Security Objectives

- Secrecy (Confidentiality)
- Integrity
- Availability (Denial of Service)
Security Objectives

- Secrecy — Prevent/detect/deter improper disclosure of information
- Integrity — Prevent/detect/deter improper modification of information
- Availability — Prevent/detect/deter improper denial of access to services provided by the system

- Note the use of improper rather than unauthorized
- Authorized users are accountable for their actions

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

A Fourth Objective

- Securing computing resources — Prevent/detect/deter improper use of computing resources including
  - Hardware Resources
  - Software resources
  - Data resources
  - Network resources
Achieving Security

- Security policy — What?
- Security mechanism — How?
- Security assurance — How well?

Security Policy

- Organizational Policy
- Automated Information System Policy
Compusec + Comsec = Infosec

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

Security Services

- Confidentiality: protection of any information from being exposed to unintended entities.
  - Information content.
  - Parties involved.
  - Where they are, how they communicate, how often, etc.
- Authentication: assurance that an entity of concern or the origin of a communication is authentic - it’s what it claims to be or from
- Integrity: assurance that the information has not been tampered with
Security Services - Cont’d

• Non-repudiation: offer of evidence that a party is indeed the sender or a receiver of certain information
• Access control: facilities to determine and enforce who is allowed access to what resources, hosts, software, network connections
• Monitor & response: facilities for monitoring security attacks, generating indications, surviving (tolerating) and recovering from attacks

Security Services - Cont’d

• Security management: facilities for coordinating users’ service requirements and mechanism implementations throughout the enterprise network and across the internet
  – Trust model
  – Trust communication protocol
  – Trust management infrastructure
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.

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
Security by Legislation

- Security by legislation says that if we instruct our users on how to behave we can secure our systems
- It is a bad idea
- For example
  - Users should not share passwords
  - Users should not write down passwords
  - Users should not type in their password when someone is looking over their shoulder
- User awareness and cooperation is important, but cannot be the principal focus for achieving security

Security Tradeoffs

<table>
<thead>
<tr>
<th>Security</th>
<th>Functionality</th>
<th>Ease of Use</th>
<th>COST</th>
</tr>
</thead>
</table>

CSC 474/574  By Dr. Peng Ning
Threat-Vulnerability-Risk

- Threats — Possible attacks on the system
- Vulnerabilities — Weaknesses that may be exploited to cause loss or harm
- Risk — A measure of the possibility of security breaches and severity of the ensuing damage

- Requires assessment of threats and vulnerabilities

Risk Management

- Risk analysis
  - Mathematical formulae and computer models can be developed, but the underlying parameters are difficult to estimate.
- Risk reduction
- Risk acceptance
  - Certification
    - Technical evaluation of a system's security features with respect to how well they meet a set of specified security requirements
  - Accreditation
    - The management action of approving an automated system, perhaps with prescribed administrative safeguards, for use in a particular environment