CSC 774 Advanced Network Security

Dr. Peng Ning
pning@ncsu.edu
http://www.csc.ncsu.edu/faculty/ning

About Instructor

• Dr. Peng Ning, associate professor of computer science
  – http://www.csc.ncsu.edu/faculty/ning
  – pning(at)ncsu.edu
  – (919) 513-4457
  – Office: 3258 EB II, centennial campus
  – Office hours:
    • Tuesdays and Thursdays, 10:00am – 11:00am
About TA

• Juan Du
  – jdu@ncsu.edu
• Office hours:
  – TBD

Course Objectives

• Understanding of fundamental issues, concepts, principles, and mechanisms in network security (beyond CSC 574).
  – Network security primitives
  – Electronic payment systems
  – Broadcast authentication
  – Group key management
  – MANET and sensor network security
• Prepare for graduate research in network security
  – Advanced topics: ad-hoc security, Internet security, etc.
  – Will give a list of recently published papers
Prerequisites

- You must have taken
  - CSC 570
  - CSC 574
- Or convince the instructor that you have enough background knowledge

Text

- No required textbook
- Research papers listed on the course website
Course Mechanics

- Slides will be provided
- But be prepared to
  - Take notes, and
  - Work in class
- WWW page:
  - For course materials, e.g., slides, homework files, papers, tools, etc.
  - Will be updated frequently
- Message board at
  - http://courses.ncsu.edu/csc774/
  - For discussions, Q&As
  - TA will answer questions there regularly

Grading

- Assignments: 10%
- Midterm #1: 25%
- Midterm #2: 25%
- Research/survey paper: 30%
- In-class presentation: 10%
  - Duration TBD
  - On a technical paper assigned by the instructor.
Grading (Cont’d)

• 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%

• Audit students:
  – No in-class presentation;
  – No research paper;
  – Grade will be adjusted by grade = grade/0.6;
  – Need grade >=63% to pass.

Course Outline

• Topic 1: Course Introduction
  – Overview of the course contents
  – Review basic security concepts
Course Outline (Cont’d)

• Topic 2: Network security basics
  – Absolute basics
  – Hash-based primitives
  – Secret sharing
  – ID-based cryptography
  – Secret handshake
  – Rabin’s fingerprinting and information dispersal algorithms

Course Outline (Cont’d)

• Topic 3: Electronic Payment Systems
  – Electronic billing systems
    • NetBill
  – Micropayments
    • PayWords and MicroMints
  – Fair Exchange Protocols
    • Optimistic fair exchange protocol
Course Outline (Cont’d)

• Topic 4: Broadcast Authentication
  – EMSS
    • Based on signature amortization
  – TESLA
    • Based on hash chain and delayed disclosure of symmetric keys
  – BiBa
    • Based on collision of hash functions

Course Outline (Cont’d)

• Topic 5: Group Key Management
  – Group key agreement
    • Group Diffie-Hellman (GDH) protocols
    • Tree-based GDH
  – Group key distribution
    • Iolus
    • Logical Key Hierarchy (LKH)
      – Or key graph
Course Outline (Cont’d)

• Topic 6: Security in Ad-Hoc Networks
  – Security mechanisms for routing protocols
  – Random key pre-distribution
  – Secure and resilient data aggregation
  – Secure and resilient location discovery
  – Secure and resilient time synchronization

Course Outline (Cont’d)

• Advanced Topics:
  – Ad-hoc network security
  – Internet security
• Every student is responsible for presenting one technical paper in class, and managing a discussion forum in the message board
  – Will be graded. Instructions and grading policy is posted on the course website
  – Students are encouraged to write research papers related to these topics
What’s behind these Topics

• Efficient use of cryptography
  – Public key cryptography
  – Symmetric cryptography
    • One-way hash chains
    • Merkle hash trees
    • Cryptographic puzzles

• Non-crypto techniques

In-class Presentation

• Duration TBD
• Will be graded
  – See the grading sheet on course website
Research/Survey Paper

- Small team -- at most two students per group
- Proposal, work, and final write-up
- Both the proposal and the final submission will be graded
  - Proposal due: 3/13/07
  - Final submission due: midnight EST, 05/01/07
- Grading policy is posted on the course website
- The instructor will be available to discuss your topic during the office hours
- You should start thinking about your team and topic now

Check the website for details!
Review of Basic Security Concepts

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

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 Tradeoffs

![Security Tradeoff Diagram]

- Security
- Functionality
- Ease of Use
- Cost
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