CSC/ECE 774 Advanced Network Security

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

About Instructor

• Dr. Peng Ning, Professor of Computer Science
  – http://www.csc.ncsu.edu/faculty/ning
  – pnning(at)ncsu.edu
  – (919) 513-4457
  – Office: 3258 EB II, centennial campus
  – Office hours:
    • Mondays, 2:30pm – 3:30pm
    • Or by appointment

Course Objectives

• Understanding of fundamental issues, concepts, principles, and mechanisms in network security (beyond CSC 574).
  – Network security primitives
  – Broadcast authentication
  – Group key management
  – Wireless sensor network security
  – Wireless physical layer security
• Prepare for graduate research in network security
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%

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 research paper;
  - Grade will be adjusted by grade = grade/0.8;
  - 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
  – Rabin’s information dispersal algorithms
  – Secret handshake

Course Outline (Cont’d)

• Topic 3: 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
  – HORS
    • “Better-than-BiBa”

Course Outline (Cont’d)

• Topic 4: Group Key Management
  – Group key agreement
    • Group Diffie-Hellman (GDH) protocols
    • Tree-based GDH
  – Group key distribution
    • Iolus
    • Logical Key Hierarchy (LKH)
      – AKA key graph
### Course Outline (Cont’d)

<table>
<thead>
<tr>
<th>Topic 5: Security of Wireless Sensor Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Random key pre-distribution in sensor networks</td>
</tr>
<tr>
<td>- Secure and resilient localization</td>
</tr>
<tr>
<td>- Secure and resilient time synchronization</td>
</tr>
<tr>
<td>- Message specific puzzles</td>
</tr>
<tr>
<td>- Defense against Denial-of-Service (DoS) attacks against broadcast authentication</td>
</tr>
<tr>
<td>- Secure remote programming</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Topic 6: Wireless Physical Layer Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Recent advances in anti-jamming wireless communications</td>
</tr>
<tr>
<td>- Wireless link signature</td>
</tr>
</tbody>
</table>

### What’s behind these Topics

<table>
<thead>
<tr>
<th>Efficient use of cryptography</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Public key cryptography</td>
</tr>
<tr>
<td>- Symmetric cryptography</td>
</tr>
<tr>
<td>- One-way hash chains</td>
</tr>
<tr>
<td>- Merkle hash trees</td>
</tr>
<tr>
<td>- Cryptographic puzzles</td>
</tr>
<tr>
<td>Non-crypto techniques</td>
</tr>
<tr>
<td>- Crypto does solve all problems</td>
</tr>
</tbody>
</table>
Research/Survey Paper

- Small team -- at most three students per group
- Proposal, work, and final write-up
- Both the proposal and the final submission will be graded
  - Proposal due: 10/03/11
  - Final submission due: midnight EST, 12/05/11
- 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!
A Brief Review of Basic Security Concepts

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
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 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