About Instructor

• Dr. Peng Ning, Professor of Computer Science
  – [http://www.csc.ncsu.edu/faculty/ning](http://www.csc.ncsu.edu/faculty/ning)
  – pning@ncsu.edu
  – (919) 513-4457
  – Office: 3258 EB II, centennial campus
  – Office hours:
    • Mondays and Wednesdays, 3:45pm – 4:45pm
    • Or by appointment

About TA

• Mr. Jung Ki So
  – jkso@ncsu.edu
  – Office hours
    • Tuesdays and Thursdays, 1pm – 2pm
    • 3240 EB II
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
  – Wireless network security
  – Security of virtual cloud computing (if time permits)
• 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: 15%;
• Midterm #2: 15%;
• Lab: 10%
  – WiSeNeT – A wireless sensor network testbed
  – VCL – virtual cloud computing (if time permits)
• Research/survey paper: 20%;
• Final: 30%

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
  – ID-based cryptography

Course Outline (Cont’d)

• Topic 3: Electronic Payment Systems
  – Electronic billing systems
    • NetBill
    • Micropayments
  – Fair Exchange Protocols
    • Optimistic fair exchange protocol
  – Illustration of efficient crypto in real applications
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
  – Broadcast authentication in sensor networks

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)
      – AKH key graph

Course Outline (Cont’d)

• Topic 6: Security of Ad-Hoc Networks
  – Random key pre-distribution in sensor networks
  – Secure and resilient localization
  – Secure and resilient time synchronization
Course Outline (Cont’d)

• Topic 7. Wireless Security
  – Anti-jamming wireless communications
  – New topic this semester

• Topic 8. Security in Virtual Cloud Computing
  – Security threats in virtual cloud computing
  – A few example defenses
  – New topic this semester

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
  – Crypto does solve all problems

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: 9/29/10
  – Final submission due: midnight EST, 12/06/10
• 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
A Brief 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

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

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