



CSC 774 Network Security

Dr. Peng Ning

pning@ncsu.edu

<http://www.csc.ncsu.edu/faculty/ning>

1

About Instructor

- Dr. Peng Ning, assistant professor of computer science
 - <http://www.csc.ncsu.edu/faculty/ning>
 - pning@ncsu.edu
 - (919)513-4457
 - Office: 250 Venture III, centennial campus
 - Office hours: Mondays and Thursdays, 3:00 pm – 4:00 pm

About TA

- Kun Sun
 - ksun3@ncsu.edu
- Office hours:
 - TBD

Course Objectives

- Understanding of fundamental issues, concepts, principles, and mechanisms in network security (beyond CSC 574).
 - Internet key management; Electronic payment systems
 - Broadcast authentication; Intrusion alert correlation
 - Group key management;
 - MANET and sensor network security
- Prepare for graduate research in network security
 - Advanced topics: Intrusion detection, MANET security, sensor network security.

Prerequisites

- You should 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

- WWW page: <http://courses.ncsu.edu/csc774/lec/002/>
 - For course materials, e.g., lecture slides, homework files, papers, tools, etc.
 - Will be updated frequently. So check frequently, too.
- Message board at <http://courses.ncsu.edu:8020/csc774/>
 - For discussions, Q&As.

Grading

- Assignments: 10%;
- midterm #1: 15%;
- midterm #2: 15%;
- final: 30%;
- Research/survey paper: 20%;
- in-class presentation: 10%
 - 20 -- 25 minutes
 - On a technical paper assigned by the instructor.

Grading (Cont'd)

- The final grades are computed according to the following rules:
 - A+: $\geq 95\%$; A: $\geq 90\%$ and $< 95\%$; A-: $\geq 85\%$ and $< 90\%$;
 - B+: $\geq 80\%$ and $< 85\%$; B: $\geq 75\%$ and $< 80\%$; B-: $\geq 70\%$ and $< 75\%$;
 - C+: $\geq 66\%$ and $< 70\%$; C: $\geq 63\%$ and $< 66\%$; C-: $\geq 60\%$ and $< 63\%$;
 - D+: $\geq 56\%$ and $< 60\%$; D: $\geq 53\%$ and $< 56\%$; D-: $\geq 50\%$ and $< 53\%$;
 - F: $< 50\%$
- Audit students:
 - no in-class presentation;
 - grade will be adjusted by $\text{grade} = \text{grade}/0.9$;
 - need grade $\geq 63\%$ to pass.

Lab

- Will be given as part of homework assignments
- Will be coordinated with the networking lab.
- Team
 - Two to three students each team.
- Possible topics:
 - Vulnerability scan
 - Setup VPN

Course Outline

- Topic 1: Course Introduction
 - Review basic security concepts

Course Outline (Cont'd)

- Topic 2: Review of cryptography and traditional network security techniques
 - Secret key and public key cryptosystems
 - One-way hash function
 - Authentication
 - Key distribution
 - Traditional network security techniques
 - Firewalls
 - IPsec
 - SSL

Course Outline (Cont'd)

- Topic 3: Internet Key Management
 - Basic concepts of key management
 - Session key security principles
 - Perfect forward secrecy
 - ...
 - Manual Key Management
 - Automatic Key Management
 - SKIP
 - Oakley
 - ISAKMP
 - IKE

Course Outline (Cont'd)

- Topic 4: Electronic Payment Systems
 - Electronic billing systems
 - NetBill (CMU)
 - Micropayments
 - PayWords and MicroMints
 - Fair Exchange Protocols
 - Optimistic fair exchange protocol

Course Outline (Cont'd)

- **Topic 5: Network Intrusion Detection**
 - **Intrusion Alert Correlation**
 - Similarity based approaches
 - Approaches based on known attack scenarios
 - Approaches based on prerequisites and consequences of attacks
 - Approaches that integrate multiple information sources

Course Outline (Cont'd)

- **Topic 6: Broadcast Authentication**
 - **TESLA**
 - Based on hash chain and delayed disclosure of symmetric keys
 - **EMSS**
 - Based on signature amortization
 - **Biba**
 - Based on collision of hash functions

Course Outline (Cont'd)

- Topic 7: Group Key Management
 - Group key agreement
 - Group Diffie-Hellman (GDH) protocols
 - Tree-based GDH
 - Group key distribution
 - LKH
 - SDR
 - Secret-sharing based approach

Course Outline (Cont'd)

- Topic 8: Security in Mobile Ad-Hoc Networks (MANET)
 - Secure MANET routing protocols
 - ARIADNE
 - Detect malicious/selfish nodes
 - WatchDog and PathRater

Course Outline (Cont'd)

- Topic 9: Security in Sensor Networks
 - Broadcast authentication
 - μ TESLA
 - Key pre-distribution
 - Random key pre-distribution scheme
 - q-composite scheme
 - Random pairwise keys scheme
 - Polynomial pool-based schemes
 - Secure location verification

Course Outline (Cont'd)

- Advanced Topics:
 - Intrusion Alert Correlation
 - MANET security
 - Sensor network 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.
 - *Content will be included in the final exam.*
 - Students are encouraged to write research papers related to these topics, but not required.

Research/Survey Paper

- Small team -- one to three persons.
- Proposal, work, and final write-up.
- Both proposal and the final submission will be graded.
- Grading policy is posted on the course website.
- The instructor will be available to discuss your topic during the office hours.

Check the website for details!