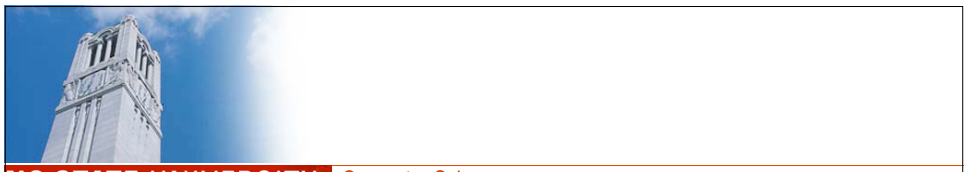


NC STATE UNIVERSITY Computer Science

CSC 774 Advanced Network Security

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

About Instructor

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

About TA

- Mithun Acharya
  - mpachary(at)ncsu.edu
- Office hours:
  - Tuesdays 9:30 am - 11:30 am
  - Ventures I, Suite 110, Room 102
    - please ring the bell

Course Objectives

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

- WWW page:
  - For course materials, e.g., lecture 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%;
- Final: 30%;
- Research/survey paper: 20%;
- In-class presentation: 10%
  - 15 minutes
  - 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;
  - Grade will be adjusted by grade = grade/0.9;
  - 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: Review of cryptography and traditional network security techniques
  - Secret key cryptosystems
  - Public key cryptosystems
  - One-way hash function
  - Merkle hash tree
  - Pseudo random generator and function
  - Key distribution and management

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 Mobile Ad-Hoc Networks (MANET)
  - Secure MANET routing protocols
    - ARIADNE
    - Security mechanisms for routing protocols
  - Detect malicious/selfish nodes
    - WatchDog and PathRater

Course Outline (Cont'd)

- Topic 7: Security in Wireless Sensor Networks
  - Key pre-distribution
    - Random key pre-distribution scheme
    - q-composite scheme
    - Random pairwise keys scheme
    - Polynomial pool-based schemes
  - Secure and resilient data aggregation
    - SIA
  - Secure and resilient location discovery
    - Tolerate malicious data
    - Detect malicious nodes

Course Outline (Cont'd)

- Topic 8. Misc Topics
  - Client puzzle
    - Mitigate DoS attacks
  - Security for, and by, mobile devices

Course Outline (Cont'd)

- Advanced Topics:
  - 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

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

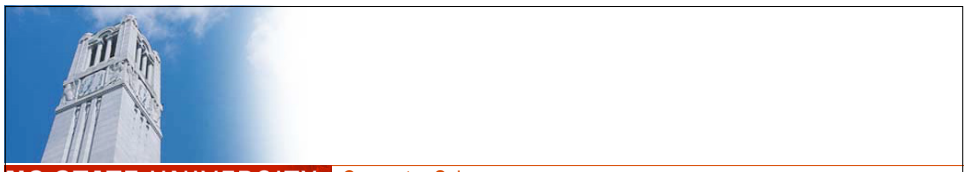
In-class Presentation

- 15 minutes
- Will be graded
  - See the grading sheet on course website

Research/Survey Paper

- Small team -- one to three students
- Proposal, work, and final write-up
- Both the proposal and the final submission will be graded
  - Proposal due: 10/05/05
  - Final submission due: 12/02/05
- 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

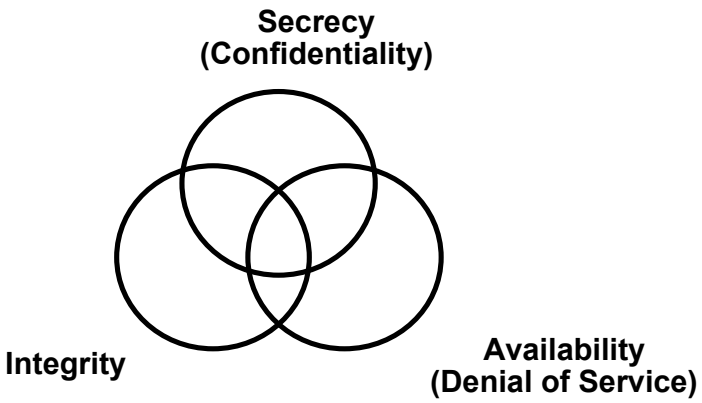
Check the website for details!



NC STATE UNIVERSITY Computer Science

Review of Basic Security Concepts

Security Objectives



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

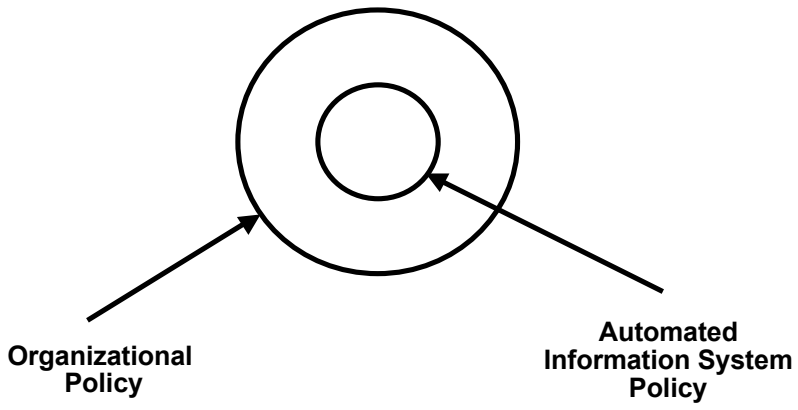
A Fourth Objective

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

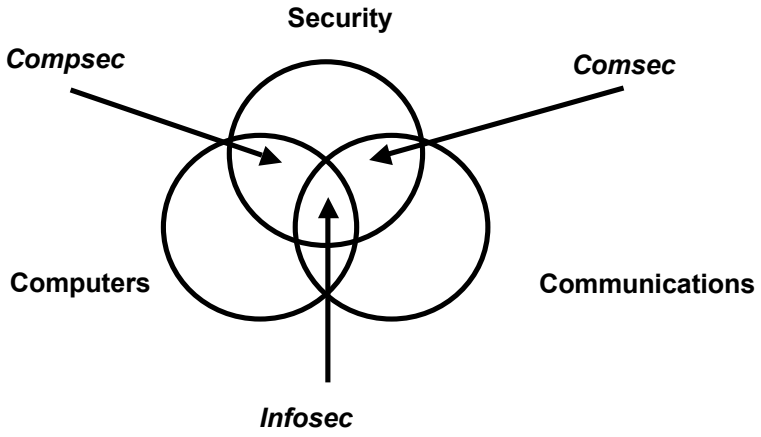
Achieving Security

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

Security Policy



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

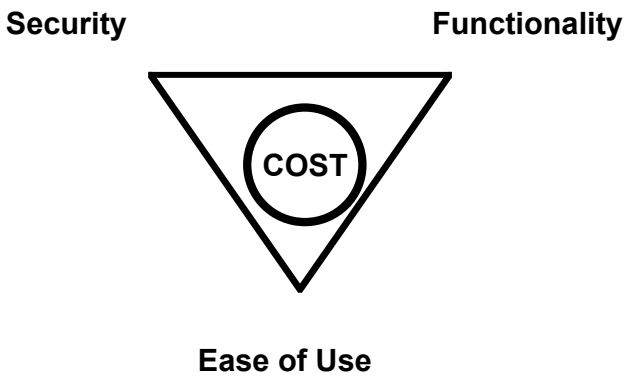
Security Services - Cont'd

- 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



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