CSC 574 Information Systems and Network Security  
Syllabus

A. Instructors:

Dr. Peng Ning,  
Office: 3258 Engineering Building II  
Phone: (919) 513-4457  
Email: pning@ncsu.edu  
URL: http://www.csc.ncsu.edu/faculty/ning

B. Course prerequisites or restrictive statements:

• CSC 316 Data Structure for Computer Scientists  
• CSC 401 Data and Computer Communications Networks or CSC/ECE 570 Computer Networks  
• Ability to program in Java or C/C++

C. Designation of course as a General Education Requirement (GER)

N/A

D. Student learning outcomes:

By the end of this course, students will be able to:

- State the basic concepts in information security, including security policies, security models, and various security mechanisms.
- Explain concepts related to applied cryptography, including plaintext, ciphertext, symmetric cryptography, asymmetric cryptography, and digital signatures.
- Explain the basic number theory required for cryptographic applications as well as various cryptographic systems.
- Manually compute using Fermat's theorem, Euler's theorem, Euclid's algorithm, extended Euclid's algorithm; manually encrypt/decrypt and sign/verify signatures for small messages using RSA, Diffie-Hellman, and DSA algorithms.
- State the requirements and mechanisms for identification and authentication; explain and identify typical security pitfalls in authentication protocols.
- List network and distributed systems security issues and solutions, including authentication, key distribution, and network security protocols.
- Explain the network access control mechanisms, including the basic concepts of firewalls, packet filters, application gateways, and typical firewall configurations.
- Outline the protocols, i.e., AH and ESP protocols, for IP Security and the two modes for both protocols.
- Explain in their own words the goals of IP Security protocols (AH and ESP), the
- Use combinations of IP security protocols to achieve a given security goal (e.g., source authentication, content authentication, traffic confidentiality, etc.)
- Explain SSL/TLS protocols.
- State program security issues, including virus, worm, and logical bombs.
- State the basic concepts and general techniques in security auditing and intrusion detection.
- Explain and compare the various access control policies and models as well as the assurance of these models.
- State the characteristics of typical security architectures, including multi-level security systems.
- State the criteria of evaluating secure information systems, including evaluation of secure operating systems and secure network systems.

**E. Textbooks:**
- Handouts

**F. Course Organization and Scope:**
(Assume each lecture takes 75 minutes. These will be adjusted based on the actual progress in a semester.)

T1. Basic Security Concepts (1 lecture)
   - Confidentiality, integrity, availability
   - Security policies, security mechanisms, assurance

T2. Basic Cryptography (1 lecture)
   - Historical background
   - Transposition/Substitution, Caesar Cipher
   - Introduction to Symmetric crypto primitives, Asymmetric crypto primitives, and Hash functions

T3. Secret Key Cryptography (3 lectures)
   - Data Encryption Standard (DES)
   - Advanced Encryption Standard (AES)
   - Encrypting large messages (ECB, CBC, OFB, CFB, CTR)
   - Multiple Encryption DES (EDE)

T4. Message Digests (2 lectures)
   - Applications
   - Strong and weak collision resistance
   - The Birthday Paradox
   - MD5, SHA-1

T5. Public Key Cryptography (4 lectures)
   - Number theory: Euclidean algorithm, Euler Theorem, Fermat Theorem, Totent functions, multiplicative and additive inverse
   - RSA, Selection of public and private keys

T6. Authentication (4 lectures)
   - Basic concepts of identification and authentication
   - Password authentication
   - Authentication protocols

T7. Trusted Intermediaries (2 lecture)
o Public Key infrastructures
o Certification authorities and key distribution centers
o Kerberos

T8. Real-time Communication Security (5 lectures)
o IPsec: AH and ESP
o IPsec: IKE
o SSL/TLS
o Firewall
o Auditing and intrusion detection

T9. Access Control (2 lectures)
o Basic concepts of access control
o Discretionary access control and mandatory access control
o Lattice-based Models
o Covert Channels
o Role based Access Control

T10. Miscellaneous topics (1 lecture)
o Assurance and Evaluation of Secure Information Systems
o Database Security (Security requirements in databases, Access control and authorization in databases, Inference control)
o Malicious software
o Administering Security (Risk Analysis, Security Planning, Organizational Security Policies)

G. Schedule of reading assignments:

• Topic T1: Chapter 1.
• Topic T2: Chapters 2 – 7.
• Topic T3: Chapters 9 – 12.
• Topic T4: Chapters 13 – 19, 23; Handout H3.
• Topic T5: Handouts H1 – H2.
• Topic T6: TBD.

H. Projected schedule of homework due dates, quizzes and exams:
There are 5 homework assignments and 2 exams. Quizzes are given in the form of pop quizzes. Pop quizzes are adopted to encourage the students to study during the non-exam weeks. The results of pop quizzes are not counted in the final grade.
• Homework 1: topics T1 and T2, due by week 3
• Homework 2: topics T2 and T3, due by week 6
• Homework 3: topic T4, due by week 9
• Homework 4: topic T5, due by week 11
• Homework 5: topics T5 and T6, due by week 13
• Mid-term exam: week 8
• Research project report: due by week 15
• Final exam: decided by the university.

I. Grading:
• Assignments 15%, projects 10%, class participation 5%, midterm 35%, final 35%.
• The final grades are computed according to the following rules:
  o A+: >= 95%
  o A: >= 90% and < 95%
J. Policies on incomplete grade and late assignments:
Homework and project deadlines will be hard. Late homework will be accepted with a 10% reduction in grade for each class period they are late by. However, once a homework assignment is discussed in class or the solution is posted, submissions will no longer be accepted. All assignments must be turned in before the start of class on the due date.

K. Policies on absences (excused and unexcused) and scheduling makeup work:
The university policy on absences will be enforced. See the university policy at the following URL.
http://www.ncsu.edu/provost/academic_regulations/attend/reg.htm
- The students are responsible for discussing makeup exams if they miss exams due to excused absence. The instructor will choose a mutually agreed date and time for the makeup exam.
- Late submission of homework assignments due to excused absences is not subject to the policies on late assignments.

L. Academic integrity:
The university, college, and department policies against academic dishonesty will be strictly enforced. You may obtain copies of the NCSU Code of Student Conduct from the Office of Student Conduct, or from the following URL.
http://www.ncsu.edu/policies/student_services/student_discipline/POL11.35.1.php
The instructor expects honesty in the completion of test and assignments. It is the understanding and expectation of instructor that the student's signature on any test or assignment means that the student neither gave nor received unauthorized aid.

M. NC State policy on working with students with disabilities:
“Reasonable accommodations will be made for students with verifiable disabilities. In order to take advantage of available accommodations, students must register with Disability Service for Students at 1900 Student Health Center, Campus Box 7509, 515-7653.
http://www.ncsu.edu/provost/offices/affirm_action/dss/
For more information on NC State’s policy on working with students with disabilities, please see http://www.ncsu.edu/provost/hat/current/appendix/appen_k.html.
N. Laboratory Safety or Risk Assumption: Not Applicable.

O. “Pass-through” Charges: Not applicable.

P. Statement on transportation: Students have to provide their transportation for all class related trips.