CSC 474 Network Security

Syllabus

A. Instructor

Dr. Peng Ning
Associate Professor
Department of Computer Science
North Carolina State University
Raleigh, NC 27695-8206
Office: 3258 Engineering Building II
Voice: (919) 513-4457; Fax: (919) 515-7896
Email: pning AT ncsu.edu
URL: http://www.csc.ncsu.edu/faculty/ning

B. Course Pre-requisites or Restrictive Statements

Programming experience in C/C++ or JAVA

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:
- Explain concepts related to applied cryptography, including plaintext, ciphertext, symmetric cryptography, asymmetric cryptography, and digital signatures.
- Explain the theory behind the security of different cryptographic algorithms.
- Explain common network vulnerabilities and attacks, defense mechanisms against network attacks, and cryptographic protection mechanisms.
- Outline the requirements and mechanisms for identification and authentication. Identify the possible threats to each mechanism and ways to protect against these threats.
- Explain the requirements of real-time communication security and issues related to the security of web services.
- Explain the requirements of non-realtime security (email security) and ways to provide privacy, source authentication, message integrity, non-repudiation, proof of submission, proof of delivery, message flow confidentiality, and anonymity.
E.  Textbook


F.  Course Organization and Scope

(Assume each lecture takes 75 minutes. The following topics need 28 lectures. These will be adjusted based on the actual progress in a semester.)

T1. Introduction (1 lecture)
  o Motivating examples
  o Basic concepts: confidentiality, integrity, availability, security policies, security mechanisms, assurance

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

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

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

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

Midterm (1 lecture)

T6. Authentication (5 lectures)
  o Security Handshake pitfalls
  o Online vs. offline password guessing
  o Reflection attacks
  o Per-session keys and authentication tickets
  o Key distribution centers and certificate authorities

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

T8. Real-time Communication Security (4 lectures)
  o Introduction to TCP/IP protocol stack
Implementation layers for security protocols and implications

- IPsec: AH and ESP
- IPsec: IKE
- SSL/TLS

T9. Electronic Mail Security (2 lectures)
- Distribution lists
- Establishing keys
- Privacy, source authentication, message integrity, non-repudiation, proof of submission, proof of delivery, message flow confidentiality, anonymity
- Pretty Good Privacy (PGP)

T10. Firewalls and Web Security (2 lectures)
- Packet filters
- Application level gateways
- Encrypted tunnels
- Cookies
- Web security problems

Final review (1 lecture)

G. Schedule of Reading Assignments

- Topic T1: Chapter 1.
- Topic T2: Chapter 2.
- Topic T3: Chapters 3, 4.
- Topic T4: Chapter 5.
- Topic T5: Chapters 6 and 7.
- Topic T6: Chapters 9, 10, 11, 12.
- Topic T7: Chapters 15, 13.
- Topic T8: Chapters 16, 17, 18, 19.
- Topic T9: Chapters 20 and 22.
- Topic T10: Chapters 23 and 25.

H. Projected Schedule of Homework Due dates, Quizzes and Exams:

(The following is a tentative plan for homework assignments, labs, and exams. Please refer to the course website for the actual schedule.)

There are 5 homework assignments, 1 midterm exam, 3 labs, and 1 final exam. 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 4
- Homework 2: topics T3 and T4, due by week 6
- Homework 3: topics T5 and T6, due by week 9
- Homework 4: topics T7, T8, and T9 due by week 12
- Homework 5: topic T10 and T11, due by week 14
- Mid-term exam: week 8
• Final exam: decided by the university.

I. Grading

•Homework assignments 20%, midterms 30%, lab 20%, and final exam 30%.
•The final grades are computed according to the following rules:
  o A+: >= 95%
  o A: >= 90% and < 95%
  o A-: >= 85% and < 90%
  o B+: >= 80% and < 85%
  o B: >= 75% and < 80%
  o B-: >= 70% and < 75%
  o C+: >= 66% and < 70%
  o C: >= 63% and < 66%
  o C-: >= 60% and < 63%
  o D+: >= 56% and < 60%
  o D: >= 53% and < 56%
  o D-: >= 50% and < 53%
  o F: < 50%.

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.

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.

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

N. Laboratory Safety or Risk Assumption

N/A

O. “Pass-through” Charges

N/A

P. Statement on Transportation

Students have to provide their transportation for all class related trips.