

CSC 405 Introduction to Computer Security

Syllabus

A. Instructors:

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

B. Course prerequisites or restrictive statements:

CSC 246 (Basic knowledge on operating systems; C programming skills).

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 security mechanisms.
- Explain concepts related to applied cryptography, including plain-text, cipher-text, the four techniques for crypto-analysis, symmetric cryptography, asymmetric cryptography, digital signature, message authentication code, hash functions, and modes of encryption operations.
- Explain the concepts of malicious code, including virus, Trojan horse, and worms.
- Explain common vulnerabilities in computer programs, including buffer overflow vulnerabilities, time-of-check to time-of-use flaws, incomplete mediation.
- Outline the requirements and mechanisms for identification and authentication.
- Explain issues about password authentication, including dictionary attacks (password guessing attacks), password management policies, and one-time password mechanisms.
- Explain and compare security mechanisms for conventional operating systems, including memory, time, file, object protection requirements and techniques and protection in contemporary operating systems.
- Explain the requirements for trusted operating systems, and describe the independent evaluation, including evaluation criteria and evaluation process.
- Describe security requirements for database security, and describe techniques for ensuring database reliability and integrity, secrecy, inference control, and multi-level databases.
- Describe threats to networks, and explain techniques for ensuring network security, including encryption, authentication, firewalls, and intrusion detection.
- Explain the requirements and techniques for security management, including security policies, risk analysis, and physical threats and controls.

E. Textbook:

- Charles P. Pfleeger and Shari L. Pfleeger. Security in Computing (3rd edition). Prentice-Hall. 2003. ISBN: 0-13-035548-8.

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)

- Basic concepts: threats, vulnerabilities, controls; risk; confidentiality, integrity, availability; security policies, security mechanisms; assurance; prevention, detection, deterrence

T2. Basic cryptography (3 lectures)

- Basic cryptographic terms
- Historical background
- Symmetric crypto primitives
- Modes of operation
- Cryptographic hash functions
- Asymmetric crypto primitives

T3. Program security (4 lectures)

- Flaws
 - Malicious code: viruses, Trojan horses, worms
 - Program flaws: buffer overflows, time-of-check to time-of-use flaws, incomplete mediation
- Defenses
 - Software development controls
 - Testing techniques

T4. Security in conventional operating systems (5 lectures)

- Memory, time, file, object protection requirements and techniques
- Protection in contemporary operating systems
- Identification and authentication
 - Identification goals
 - Authentication requirements
 - Human authentication
 - Machine authentication

Mid-term Review: topics 1 – 4 (1 lecture)

T5. Trusted operating systems (3 lectures)

- Assurance; trust
- Design principles
- Evaluation criteria
- Evaluation process

T6. Database management systems security (4 lectures)

- Database integrity
- Database secrecy
- Inference control
- Multilevel databases

T7. Network security (3 lectures)

- Network threats: eavesdropping, spoofing, modification, denial of service attacks
- Introduction to network security techniques: firewalls, virtual private networks, intrusion detection,

- T8. Management of security (2 lectures)
 - Security policies
 - Risk analysis
 - Physical threats and controls
- T9. Miscellaneous (1 lecture)
 - Legal aspects of security
 - Privacy and ethics

Final review: topics 1 – 9 (1 lecture)

G. Schedule of reading assignments:

- Topic T1: Chapter 1.
- Topic T2: Chapter 2.
- Topic T3: Chapter 3.
- Topic T4: Chapter 4
- Topic T5: Chapter 5.
- Topic T6: Chapter 6.
- Topic T7: Chapter 7.
- Topic T8: Chapter 8.
- Topic T9: Chapter 9.

H. Projected schedule of homework due dates, quizzes and exams:

There will be one homework assignment for each topic except for topic 1, and there will be a mid-term and a final exam. The mid-term exam will be given after topic 5. The final exam is scheduled by the university.

I. Grading:

- Assignments 10%, midterm 30%, final 30%, project 30%.
- 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: $< 50\%$.

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.