

CIS 739 COMPUTER SECURITY

Fall 2006

Monday 8:10pm-10:15pm

232NE

Instructor: Ahmet M. Eskicioglu
Telephone: 718-951-5000/2049
Email: eskicioglu@sci.brooklyn.cuny.edu
Home page: <http://www.sci.brooklyn.cuny.edu/~eskicioglu>

COURSE DESCRIPTION

With the growing importance of national security, some organizations and universities have been offering courses on computer security to increase the awareness of critical computer systems operated across the nation. Until the mid-80's, mainframe and mini computers dominated the market, and the security problem was confined to the protection of files or processes on a single computer system. Recent advances in networking, and the immense popularity of the Internet has changed the definition of computer security. Because the Internet connects millions of computers located anywhere in the world, the type and the number of threats in computer networks have drastically increased. Assuming an authorized user's identity, the Trojan horses, computer viruses and worms are very effective in attacking computer systems, making the traditional access controls useless.

This course provides a comprehensive introduction to computer security. It covers both the theoretical foundations and practical aspects of secure systems. There is a wide range of topics needed for the development of secure computer systems. These include principles for designing secure systems, potential threats, criteria for evaluating secure systems, analysis of vulnerabilities, and auditing secure systems.

It should be understood that computer security is not just a science but also an art. It is an art because a system cannot be considered secure without an examination of the environment it will be used in. The design principles should take into account who will interact with the system and what potential threats are anticipated. Computer security is also a science because its theory is based on mathematical constructions, analyses, and proofs.

COURSE CONTENTS

Chapter 1	An Overview of Computer Security
Chapter 2	Access Control Matrix
Chapter 3	Foundational Results
Chapter 4	Security Policies
Chapter 5	Confidentiality Policies
Chapter 6	Integrity Policies
Chapter 7	Hybrid Policies
Chapter 8	Basic Cryptography
Chapter 9	Key Management
Chapter 10	Cipher Techniques
Chapter 11	Authentication
Chapter 12	Design Principles
Chapter 13	Representing Identity
Chapter 14	Access Control Mechanisms
Chapter 15	Information Flow
Chapter 16	Confinement Problem
Chapter 19	Malicious Logic
Chapter 21	Auditing
Chapter 22	Intrusion Detection

REQUIRED TEXTBOOK

Introduction to Computer Security
Matt Bishop
Addison Wesley Professional
ISBN: 0-321-24744-2
2005

RECOMMENDED TEXTBOOKS

Computer Security: Art and Science
Matt Bishop
Addison Wesley Professional
ISBN: 0-201-44099-7
2003

Security in Computing, 3/e
Charles P. Pfleeger, Shari Lawrence Pfleeger
Prentice Hall PTR
ISBN: 0-13-035548-8
2003

Computer Security Handbook
Eds. Seymour Bosworth and M. E. Kabay
John Wiley and Sons
ISBN: 0-471-41258-9
2002

Trust in Cyberspace
Committee on Information Systems Trustworthiness, National Research Council
National Academy Press
1999

RECOMMENDED PAPERS

Apu Kapadia, Geetanjali Sampemane, Roy H. Campbell, “Access control: KNOW Why your access was denied: regulating feedback for usable security,” Proceedings of the 11th ACM Conference on Computer and Communications Security, October 2004.

Mike Andrews, James A. Whittaker, “Computer Security,” IEEE Security and Privacy, September 2004.

Srivaths Ravi, Anand Raghunathan, Paul Kocher, Sunil Hattangady, “Security in embedded systems: Design challenges,” ACM Transactions on Embedded Computing Systems (TECS), Volume 3, Issue 3, August 2004.

George Whitson, “Computer security: theory, process and management,” Journal of Computing Sciences in Colleges, Volume 18, Issue 6, June 2003.

Rebecca T. Mercuri, “Security watch: Analyzing security costs,” Communications of the ACM, Volume 46 Issue 6, June 2003.

Joerg Abendroth, Christian D. Jensen, “Computer security: A unified security framework for networked applications,” Proceedings of the 2003 ACM Symposium on Applied Computing, March 2003.

WEB SITES

The National Colloquium for Information Systems Security Education (NCISSE) [<http://www.ncisse.org/index.htm>] is one of the leading proponents for implementing courses of instruction in information security into American higher education.

The National Information Assurance Training and Education Center (NIATEC) [<http://niatec.info/index.htm>] is a consortium of academic, industry, and government organizations to improve the literacy, awareness, training, and education standards in Information Assurance.

The Center for Information Security (CIS) at the University of Tulsa [<http://www.cis.utulsa.edu>] offers courses in cyber security education, and is engaged in research in a number of areas including Telecommunications Security and Digital Forensics.

The Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University [<http://www.cerias.purdue.edu>] is one of the centers for research and education in areas of information security that are crucial to the protection of critical computing and communication infrastructure.

The Computer Security Division (CSD) - (893) is one of eight divisions within NIST's Information Technology Laboratory [<http://csrc.nist.gov>]. The mission of the Computer Security Division is to improve information systems security by raising awareness of IT risks, vulnerabilities and protection requirements, particularly for new and emerging technologies; researching, studying, and advising agencies of IT vulnerabilities and devising techniques for the cost-effective security and privacy of sensitive Federal systems; developing standards, metrics, tests and validation programs; and developing guidance to increase secure IT planning, implementation, management and operation.

GRADING

Midterm Exam (Take-Home)	30%
Final Exam	40%
Paper Presentation (Optional)	15%
Attendance	15%

Each student's final grade will be computed using the above weights and a 100-point scale. The corresponding letter grade, however, will be based on a curve.

EXAMS

The exams will test the students' level of understanding of the terminology, concepts and other technical details discussed throughout the semester. The final exam is closed book/notes exams, and will be taken during regular class time. The students are expected to carefully read all the assigned papers and additional background material. If a student misses an exam without a medical report from a doctor, he/she will receive a zero for that exam. No excuses other than a doctor's report will be accepted.

ATTENDANCE

Attendance is very important for this class. If a student misses a class, he/she will lose 0.714 points. It is expected that the students will actively participate in the classroom by taking notes, asking questions, and expressing opinion. If a student anticipates that he/she will have a poor performance in the course, the instructor should be contacted as soon as possible to discuss possible remedies for improvement. The office hours are allocated to extend the time spent with the students for a discussion of all course-related academic problems. The best communication with the instructor can be established during the lectures and office hours.