

Brooklyn College
Department of Computer & Information Sciences

CISC 7320 [*739X] Computer Security

37½ hours plus conference and independent work; 3 credits

Basic concepts of computer security: Security related services: confidentiality, integrity, availability. Threats, security policies and security mechanisms. Cryptographic concepts and terminology. Secure design principles. Information flow and the confinement problem. Life cycle of a secure and trusted system. System evaluation criteria. Trojan horses, worms and viruses. Vulnerability analysis. System auditing. Intrusion detection.

Syllabus:

1. Overview of Computer Security
2. Access Control Mechanisms
 - a. Protection state
 - b. Access control matrix
 - c. Protection state transitions
3. Security Policies
 - a. Types of security policies
 - b. The role of trust
 - c. Types of access control
 - d. Policy languages
4. Information Security Objectives
 - a. Confidentiality
 - b. Data integrity
 - c. Authentication: entity authentication, message authentication
 - d. Non-repudiation
5. Symmetric Key Cryptography
 - a. Block ciphers
 - b. Stream ciphers
6. Public Key Cryptography
 - a. Public/private key pairs
 - b. Public key encryption
 - c. Digital signatures
7. Key Management
 - a. Key generation
 - b. Key establishment
 - c. Key storage
 - d. Key revocation
8. Identity and Authentication
 - a. Passwords

- b. Challenge-response protocols
 - c. Biometrics
- 9. Secure Design Principles
 - a. Eight design principles
- 10. Information Flow
 - a. Nonlattice information flow policies
 - b. Compiler-based information flow mechanisms
 - c. Execution-based information flow mechanisms
- 11. The Confinement Problem
- 12. Development of Secure and Trusted Computer Systems
 - a. Security requirements
 - b. Design
 - c. Implementation
- 13. System Evaluation
 - a. Formal techniques
 - b. US Government: The Trusted System Evaluation Criteria (TCSEC)
 - c. International efforts
- 14. Malicious Logic
 - a. Trojan horses
 - b. Computer viruses
 - c. Computer worms
 - d. Other forms of malicious logic
- 15. Vulnerability Analysis
 - a. Penetration studies
 - b. Vulnerability classification
 - c. Frameworks
- 16. Auditing Computer Systems
 - a. 3 components: logger, analyzer, notifier
 - b. Auditing system design
 - c. Auditing mechanisms
 - d. Audit browsing
- 17. Intrusion Detection
 - a. Representative models
 - b. Architecture: agent, director, notifier
 - c. Organization of intrusion detection systems
 - d. Intrusion response

Bibliography:

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

Bishop M.: Introduction to Computer Security, 1/e

Addison Wesley Professional
ISBN: 0-321-24744-2
2005

Pfleeger, C. and S. Pfleeger: Security in Computing, 3/e
Prentice Hall PTR
ISBN: 0-13-035548-8
2003

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

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

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.

