

# Computer Security

## CS 470 Spring 2009

### Course Objectives

- To develop an understanding of basic computer security terminologies and concepts.
- To understand the practical realities of computer security through hands-on case studies.
- To understand the concepts of security design principles.
- To familiarize and understand current federal regulations and compliance issues pertaining to computer security and privacy.
- To understand the concepts of basic cryptography and access control.

### Course Description

Study of network security architectures and models, cryptography, authentication and authorization protocols, secure application and systems development, and federal regulations and compliance. Emphasis is on security professional certification. *Prerequisite: CS350.*

### Software Used to Support the Course

NMap, Nessus, NetStumbler, WinHex, Wireshark, NetBeans 6 and Java.

### Course Materials

*Introduction to Computer Security*, by Matt Bishop. ISBN 0-321-24744-2. Pearson Education/Addison Wesley, 2005. (Required)

*Information Security* by Mark Stamp. ISBN 13 978-0-471-73848-0. John Wiley and Sons, 2006. (Optional)

Lecture notes, project descriptions, homework problems, and frequently asked questions (FAQ) about the course materials are freely accessible through JSU's Blackboard system.

### Brief Course Outline

Weeks 1-5: Overview of Computer Security. Access Control Matrix. Security/Confidentiality/Integrity/Hybrid Policies. Basic Cryptography. Key Management. Authentication. Design Principles. **Test 1.**

Weeks 6-10: Access Control, Auditing, Penetration Testing and Vulnerability Analysis, Intrusion Detection. Network Security. System Security. **Test 2.**

Weeks 11-14: Secure Application and System Development, Web Security, Security Certification. **Final Exam.**

### Grading Policy

Test 1	25.0%
Test 2	25.0%
Research Paper	10.0%
Case Studies/HW/Projects	15.0%
Final Exam	25.0%

Letter Grade	Points Earned (%)
A	90 - above
B	80 - 89
C	70 - 79
D	60 - 69
F	below 60

### Course Policy

To take a make-up exam, a student must have a legitimate reason for having missed the exam. No student,

regardless of the reason, may take more than two make-up exams. It is the responsibility of the student to request a make-up exam. No make-up will be given on any missed pop test. Be prepared to take the makeup exam as soon as you return to class.

All homework assignments are to be turned in at midnight on the due date. Late homework will be charged 10% deduction per day.

Any individual who qualifies for reasonable accommodations under the Americans With Disabilities Act or Section 504 of the Rehabilitation Act of 1973 should contact the Instructor immediately.

## Final Examination Schedule

April 21, 2009 Tuesday

## Instructor

**Dr. Guillermo A. Francia, III**

email : [gfrancia@jsu.edu](mailto:gfrancia@jsu.edu)

Phone: (256) 782-5723

Office: 228 Ayers Hall

Office Hours: 1200-1500 MW,  
1300-1500 TTh or by appointment

## Detailed Course Outline

- I. Overview of Computer Security
  - a. Confidentiality
  - b. Integrity
  - c. Availability
  - d. Threats
  - e. Assurance
  - f. Risk Analysis and Benefits
- II. Access Control Matrix
  - a. Protection States
- III. Security Policies
  - a. Trust
  - b. Types of Security Policies

- IV. Confidentiality Policies
  - a. Bell-LaPadula model
  - b. Examples
- V. Integrity Policies
  - a. Biba model
  - b. Clark-Wilson model
  - c. Examples
- VI. Hybrid Policies
  - a. Chinese Wall model
  - b. Clinical information systems security
  - c. ORCON
  - d. RBAC
- VII. Basic Cryptography
  - a. Classical systems
  - b. Public Key cryptography
  - c. Cryptographic checksums
  - d. Comparison of techniques: RSA, DES, MD5, SHA, 3DES, RC4, and AES features and strengths
- VIII. Key Management
  - a. Session and Interchange keys
  - b. Key exchange
  - c. Storing and revocation
  - d. Digital signatures
- IX. Authentication
  - a. Passwords
  - b. Challenge Response
  - c. Biometrics
  - d. Location
- X. Design Principles
  - a. Least privilege
  - b. Fail-safe defaults
  - c. Economy of mechanisms
  - d. Complete mediation
  - e. Open design
  - f. Separation of privilege
  - g. Least common mechanism
  - h. Psychological acceptability
- XI. Access Control
  - a. Creation and Maintenance
  - b. Capabilities
  - c. Locks and keys

- d. Ring-base access control
  - e. Propagated access control
- XII. Auditing
  - a. Logging, analyzing, notifying
  - b. Auditing mechanisms
  - c. Auditing file systems
- XIII. Intrusion Detection, Penetration Testing, and Vulnerability Analysis
  - a. Models: anomaly, misuses, specification
  - b. Intrusion response
  - c. Intrusion handling
  - d. Flaw hypothesis, generalization, and testing
  - e. Information gathering
  - f. Vulnerability classification
  - g. Frameworks
- XIV. Network and Physical Security
  - a. Organization
  - b. Policy development
  - c. Firewalls and proxies
  - d. Layered security
  - e. Physical Security
- XV. System Security
  - a. Networks
  - b. Users
  - c. Authentication
  - d. Processes
  - e. Files
  - f. Devices: USB drives, Fax, Videocams
  - g. Zone of control
  - h. Databases, Datawarehouses, Data mining
- XVI. Secure Application and System Development
  - a. Requirements and Policy
  - b. Design
  - c. Refinement and Implementation
  - d. Common security-related application development problems
  - e. Testing, validation, verification, maintenance, and operation
- XVII. Web Security
  - a. SQL Injection
  - b. Buffer Overflow
  - c. Cross site scripting
  - d. Web services security
- XVIII. Evaluating Systems
  - a. Formal evaluation
  - b. TCSEC/ITSEC
  - c. FIPS140
  - d. Common Criteria
  - e. SSE-CCM
- XIX. Security Certification.
  - a. CISSP certification
  - b. Sample test questions