COMPUTER SECURITY
CS 470

Catalog Description

PREREQUISITE: *CS 350.* 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.

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 Materials

- Textbook
    - Title: Introduction to Computer Security
    - Author: Matt Bishop
    - Publisher: Pearson Education/Addison Wesley
    - Date: 2005
- Software
    - NMap
    - Nessus
    - NetStumbler
    - WinHex
    - Wireshark
    - NetBeans 6
    - Java Software Development Kit
- Supplementary Resources

- Information Security by Mark Stamp. John Wiley and Sons, 2006.
- Lecture notes, project descriptions, homework problems, and frequently asked questions (FAQ) about the course materials are freely accessible through **JSU's Blackboard system**.

Detailed Course Outline

Topic		Lecture Hours
I	**Overview of Computer Security**	**1.5**
a	Confidentiality	0.25
b	Integrity	0.25
c	Availability	0.25
d	Threats	0.25
e	Assurance	0.25
f	Risk Analysis and Benefits	0.25
II	**Access Control Matrix**	**0.5**
a	Protection States	0.5
III	**Security Policies**	**2**
a	Trust	0.5
b	Types of Security Policies	0.5
c	Access Controls	1
IV	**Confidentiality Policies**	**0.5**
a	Bell-LaPadula model	0.25
b	Examples	0.25
V	**Integrity Policies**	**1**
a	Biba model	0.5
b	Clark-Wilson model	0.25
c	Examples	0.25
VI	**Hybrid Policies**	**1**
a	Chinese Wall model	0.25
b	Clinical information systems security	0.25
c	ORCON	0.25
d	RBAC	0.25
VII	**Basic Cryptography**	**4**
a	Classical systems	1
b	Public Key cryptography	1
c	Cryptographic checksums	1
c	Comparison of techniques: RSA, DES, MD5, SHA, 3DES, RC4,	1

Topic		Lecture Hours
	and AES features and strengths	
VIII	**Key Management**	**1.5**
a	Session and Interchange keys	0.5
b	Key exchange	0.5
c	Storing and revocation	0.25
d	Digital signatures	0.25
IX	**Authentication**	**1.5**
a	Passwords	0.5
b	Challenge Response	0.5
c	Biometrics	0.25
d	Location	0.25
X	**Design Principles**	**2**
a	Least privilege	0.25
b	Fail-safe defaults	0.25
c	Economy of mechanisms	0.25
d	Complete mediation	0.25
e	Open design	0.25
f	Separation of privilege	0.25
g	Least common mechanism	0.25
h	Psychological acceptability	0.25
XI	**Access Control**	**2.5**
a	Creation and Maintenance	0.5
b	Capabilities	0.5
c	Locks and keys	0.5
d	Ring-base access control	0.5
e	Propagated access control	0.5
XII	**Auditing**	**1.5**
a	Logging, analyzing, notifying	0.5
b	Auditing mechanisms	0.5
c	Auditing file systems	0.5
XIII	**Intrusion Detection, Penetration Testing, and Vulnerability Analysis**	**3.5**
a	Models: anomaly, misuses, specification	0.5
b	Intrusion response	0.5
c	Intrusion handling	0.5
d	Flaw hypothesis, generalization, and testing	0.5
e	Information gathering	0.5

Topic		Lecture Hours
f	Vulnerability classification	0.5
g	Frameworks	0.5
XIV	**Network and Physical Security**	**2.5**
a	Organization	0.5
b	Policy development	0.5
c	Firewalls and proxies	0.5
d	Layered security	0.5
e	Physical Security	0.5
XV	**System Security**	**3**
a	Networks	0.5
b	Users	0.25
c	Authentication	0.25
d	Processes	0.25
e	Files	0.25
f	Devices: USB drives, Fax, Videocams	0.5
g	Zone of control	0.5
h	Databases, Datawarehouses, Data mining	0.5
XVI	**Secure Application and System Development**	**3**
a	Requirements and Policy	0.5
b	Design	0.5
c	Refinement and Implementation	0.5
d	Common security-related application development problems	0.5
e	Testing, validation, verification, maintenance, and operation	1
XVII	**Web Security**	**2**
a	SQL Injection	0.5
b	Buffer Overflow	0.5
c	Cross site scripting	0.5
d	Web services security	0.5
XVIII	**Evaluating Systems**	**3.5**
a	Formal evaluation	0.5
b	TCSEC/ITSEC	1
c	FIPS140	0.5
d	Common Criteria	1
e	SSE-CCM	0.5
XIX	**Security Certification**	**1**
a	CISSP certification	0.75

Topic		Lecture Hours
b	Sample test questions	0.25

Course Policy

Grading Policy

Test 1	25%
Test 2	25%
Research Paper	10%
Case Studies/HW/Projects	15%
Final Exam	25%

Grading scale (Percentage)	
A	90 - above
B	80 - 89
C	70 - 79
D	60 - 69
F	below 60

Make-up Exams

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.

Late Assignments

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

Other Course Policies

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.

Course Syllabus

The syllabus for this course can be downloaded **here** in PDF format.