School of Computing and Information Sciences

Course Title: Computing and Network Security **Date:** 01/26/10

Course Number: CNT 4403

Number of Credits: 3

Subject Area: Security	**Subject Area Coordinator:** Nagarajan Prabakar **email:** prabakar@cs.fiu.edu
Catalog Description: Fundamental concepts and principles of computing and network security, symmetric and asymmetric cryptography, hash functions, authentication, firewalls and intrusion detection, and operational issues. Not acceptable for credit for Computer Science majors.	
Textbook: "Principles of Computer Security: Security+ and Beyond" by Wm. Arthur Conklin, et al. McGraw Hill Higher Education (ISBN: 0072255099)	
References: "Introduction to Computer Security" by Matt Bishop Addison Wesley (ISBN: 0321247442)	
Prerequisites Courses: CGS 4285 and COP 3804	
Corequisites Courses: None	

Type: Required

Prerequisites Topics:

- Java programming
- Fundamental concepts of operating systems
- Shell scripting
- Basic network concepts, including TCP/IP

Course Outcomes:

1. Be familiar with basic concepts in information security
2. Master the concepts related to applied cryptography, including symmetric cryptography and asymmetric cryptography
3. Be familiar with public key infrastructure
4. Master the theory and common types of access control
5. Master the key factors involved in authentication
6. Be familiar with runtime communication techniques such as intrusion detection systems
7. Be familiar with policy and operational issues in security

8. Be exposed to vulnerabilities, attacks, auditing, and forensics

School of Computing and Information Sciences
CNT 4403
Computing and Network Security

Outline

Topic	Number of Lecture Hours	Outcome
• Basic security concepts o Security services: confidentiality, integrity, availability, etc – IAS9:0.5 o Design principles – IAS1:1 o System/security life-cycle – IAS1:0.5 o Security implementation mechanisms – IAS1:0.5 o Information assurance analysis model – IAS1:0.5	3	1
• Cryptography o Symmetric cryptosystems – IAS2:2 o Asymmetric cryptosystems – IAS2:2 o Hash functions – IAS2:2 o Digital signatures – IAS2:2	8	2
• Access control o Access control matrix model o Discretionary access control (DAC) o Mandatory access control (MAC) o Role-based access control (RBAC)	4	4
• Authentication – IAS2:4 o Password o Challenge-response o Biometric o Two-factor authentication	4	5
• Trusted intermediaries o Public key infrastructure (PKI) o Certification authorities	3	3
• Runtime communication security o Firewall o Auditing – IAS3:1 o Intrusion detection – IAS2:2	4	6
• Operational issues o Disaster recovery – IAS3:2 o Legal issues – IAS3:1	3	7
• Policy – IAS4:3 o Creation and maintenance of policies o Prevention o Avoidance	3	7
• Attacks – IAS5:3 o Social engineering	3	8

○ Denial of service ○ Protocol attacks ○ Active and passive attacks ○ Malware		
• Miscellaneous topics ○ Forensics – IAS7:2 ○ Web security and vulnerabilities – IAS6:2	4	8

School of Computing and Information Sciences
CNT 4403
Computing and Network Security

Course Outcomes Emphasized in Laboratory Projects / Assignments

	Outcome	Number of Weeks
1	Cryptography and PKI Outcomes: 2, 3	3
2	Authentication Outcomes: 1, 5	2
3	Access control Outcomes: 4, 7	2
4	Runtime communication security Outcomes: 6	3
5	Attacks and vulnerability analysis Outcomes: 8	1

Oral and Written Communication: No significant coverage

Number of written reports:

Approximate number of pages for each report:

Number of required oral presentations:

Approximate time for each presentation:

Social and Ethical Implications of Computing Topics

No significant coverage

Topic	Class time	Student performance measures

School of Computing and Information Sciences
CNT 4403
Computing and Network Security

Theoretical Contents

Topic	Class time
Cryptography	0.6
Access control model	0.1

Problem Analysis Experiences

1.

Solution Design Experiences

1. Design of access control policy for a given system