School of Computing and Information Sciences

Course Title: Network Security and Cryptography **Date:** 8/23/13

Course Number: CNT-4406

Number of Credits: 3

Subject Area:	**Subject Area Coordinator:** **email:**
Catalog Description: Topics include the concepts and principles of network security, including existing attacks and defenses	
Textbook: None.	
References: "Security in Computing (4th Edition)" by Charles Pfleeger and Shari L. Pfleeger. Prentice Hall PTR (ISBN: 0132390779) and "Applied Cryptography: Protocols, Algorithms, and Source Code in C (2nd Edition)" by Bruce Schneier (ISBN: 0471117099)	
Prerequisites Courses: COP-4338 OR CNT-4713	
Corequisites Courses: None	

Type: CS Elective

Prerequisites Topics:

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

School of Computing and Information Sciences
CNT-4406
Network Security and Cryptography

Course Outcomes:

1. Explain the importance and application of each of confidentiality, integrity, and availability
2. Describe efficient basic number-theoretic algorithms, including greatest common divisor, multiplicative inverse mod n, and raising to powers mod n.
3. Describe at least one public-key cryptosystem, including a necessary complexity-theoretic assumption for its security.
4. Master the concepts and principles of authentication and key exchange
5. Master the concepts and principles of password generation and management
6. Understand Intrusions and intrusion detection
7. Understand network vulnerabilities and attacks, including malware, networked attacks, spam and phishing.

8. Master the concepts and principles of network defenses, including firewalls, IPSec and SSL
9. Understand basic privacy concepts

School of Computing and Information Sciences
CNT-4406
Network Security and Cryptography

Outline

Topic	Lecture Hours	Outcome
• Introduction • Background and history of security	3	1

• Basic Cryptography
  • History of cryptography
  • Public/symmetric key crypto, hashes, signatures
  • Key exchange
  • Authentication
	18	2, 3, 4

• Network Vulnerabilities and Attacks
  • Vulnerabilities
  • Malware
  • Networked attacks
	12	6, 7, 9

• Network defenses
  • Access control
  • IPSec, SSL
  • Firewalls, intrusion detection
	12	5, 6, 8

Laboratory Projects/Assignments

Title	Outcomes	Expected Time
Crypto Implementation	1, 2, 3, 4	5 hours
Network Attacks	7	5 hours
Exploring Anonymity	9	2 hours
Password Breaking	5	3 hours
Network Protection (part I)	6	3 hours
Network Protection (part II)	8	3 hours

Oral and Written Communication: No significant coverage

Social and Ethical Implications of Networking: Covered throughout the Network Vulnerabilities and Attacks section of the class

School of Computing and Information Sciences
CNT-4406
Network Security and Cryptography

The Coverage of Knowledge Units within Computer Science Body of Knowledge[1]

Knowledge Unit	Topic	Lecture Hours
PF	Foundations of Information Security	9
AL	Cryptographic Algorithms	9
NC	Network Security	24

[1]See *Computing Curricula 2001 Computer Science*, by the Joint Task Force on Computing Curricula IEEE Computer Society Association for Computing Machinery; cf. Computer Science Body of Knowledge, page 17. Available at: http://www.computer.org/portal/c/document_library/get_file?p_l_id=2814020&folderId=3111026&name=DLFE-57603.pdf