COURSE NUMBER/TITLE: CS-480 INTRODUCTION TO COMPUTER SECURITY

CREDITS: 3

COURSE DESCRIPTION: Computer security problems and challenges, relationship between policy and security, cryptography, implementation of requirements imposed by policies, use of standards to ensure that the system will meet its goal, system vulnerabilities analysis and detection, intrusion detection, application of desired policy and procedures to support the policy. Prerequisite: CS-245 Introduction to Computer Organization

TEXTBOOK: *Introduction to Cryptography w/Coding Theory*, 2nd Ed., by Trappe (adopted Fall 2014)
*Elementary Information Security*, 2nd Ed., by Smith (adopted Fall 2016)

Previous:
*Elementary Information Security*, 1st Ed., by Smith (adopted F14)
*Computer Security Principles and Practice*, 2nd Ed., by Stallings (adopted F12)
*Computer Security Principles and Practice*, 1st Ed., by Stallings (adopted S10)

COURSE OBJECTIVES:
1. Understand computer and system security and value its importance.
2. Recognize good computing security practice.
3. Identify and detect security violations.
4. Understand and apply intrusion detection techniques.
5. Know information flow policies.
6. Recognize computer and network security policies that identify the threats and define the requirements for ensuring a secure system.
7. Understand the security mechanisms of how to detect and prevent attacks and how to recover from those that succeed.
8. Analyze the security of a system and the mechanisms that enforce the security policy.
9. Identify the related assumptions and trust that leads to the threats and the degree to which they may be realized.
10. Discover the role of risk analysis and acquire the knowledge to design better mechanisms and policies to neutralize these threats.
11. Recognize that policies and procedures must take people into account and know that the weakest link in the security mechanisms of any system is the human beings.
12. Identify the differences between cryptography, computer security, and information assurance.

COURSE OUTLINE:
1. Overview of computer security, confidentiality, integrity, and availability (Objectives 1, 2, 3, 12)
2. Operational issues, cost-benefit and risk analyses, legal and human factors (Objectives 9, 10, 11)
3. Planning and implementing effective access control (Objectives 6, 7, 8)
4. Defining security, confidentiality, and integrity policies (Objectives 5, 6, 7, 8)
5. Using cryptography and public-key systems, and recognizing their limits (Objectives 1, 12)
6. Understanding and using authentication: from passwords to biometrics (Objectives 1, 7, 8, 11)
7. Security design principles: least-privilege, fail-safe defaults, open design, economy of mechanism, and more (Objectives 7, 8, 9, 10)
8. Recognizing the control of information flow through systems (Objectives 5, 6, 7)
9. Assuring security throughout the system lifecycle (Objectives 1 TO 12)
10. Malicious logic: Trojan horses, viruses, boot sector and executable infectors, rabbits, bacteria, logic bombs--and defenses against them (Objectives 2, 3, 4, 7)
11. Vulnerability analysis, penetration studies, auditing, and intrusion detection and prevention (Objectives 2, 3, 4, 7, 11)
12. Applying security principles to networks, systems, users, and programs (Objectives 1 to 12)