SEC 150
SECURE COMMUNICATIONS

COURSE DESCRIPTION:

Prerequisites: None
Corequisites: None

This course provides an overview of current technologies used to provide secure transport of information across networks. Topics include data integrity through encryption, Virtual Private Networks, SSL, SSH, and IPSec. Upon completion, students should be able to implement secure data transmission technologies. Course Hours Per Week: Class, 2. Lab, 2. Semester Hours Credit, 3.

LEARNING OUTCOMES:

Upon completion of this course, students will be able to:

a. Discuss basic security concepts, including terminology and models
b. Describe elements of cryptography, including encryption and hashing algorithms
c. Apply symmetric and asymmetric encryption to appropriate activity
d. Implement management of Public Key Infrastructure and certificates
e. Identify and implement access control models
f. Identify and use multiple authentication types
g. Classify examples of network and computer attacks and malware
h. Harden systems to increase security
i. Implement security on wireless networks
j. Identify network security devices
k. Implement access control and account management security measures
l. Assess vulnerability to identify and manage risk and threats
m. Develop a business continuity and disaster recovery plan
n. Implement secure communication pathways

OUTLINE OF INSTRUCTION:

I. Introduction to Computer Security
   a. Historical review of the security problem
   b. Types and avenues of attack
   c. Types of defenses

II. Systems Threats and Risks
   a. Software attacks
   b. Hardware attacks
III. Protecting Systems
   a. Hardening the operating system
   b. Hardening the web browser
   c. Hardening web and network services
   d. Controlling network access

IV. Network Vulnerabilities and Attacks
   a. Media and network device vulnerabilities
   b. Categories of attack
   c. Methods of attack

V. Network defenses
   a. Secure network design
   b. Secure network technologies
   c. Network security devices
   d. Intrusion detection and prevention
   e. Protocol analyzers

VI. Wireless Network Security
   a. Weaknesses and hardening of wireless networks
   b. Wireless encryption systems

VII. Access Control
   a. Logical versus physical
   b. Mandatory, discretionary, and role-based access control

VIII. Authentication, Authorization, and Accounting
   a. Authentication and access control terminology
   b. Credentials and identity
   c. Privilege management

IX. Vulnerability Assessments
   a. Threat and risk assessment
   b. Risk management models and tools
   c. Identifying vulnerabilities

X. Security Audits
   a. Privilege auditing, management, and assignment
   b. Usage auditing
   c. Auditing tools

XI. Cryptography
   a. Encryption algorithms
   b. Hashing algorithms
   c. Symmetric encryption
   d. Asymmetric encryption
e. Network, drive, and file encryption  
f. Public Key Infrastructure basics and digital certificates  
g. Certificate and registration authorities

XII. Disaster Recovery and Business Continuity  
a. Disaster Recovery planning and execution  
b. Disaster recovery policies and procedures

XIII. Security Policies and User Training  
a. Organizational security policies  
b. Types of Security policies  
c. User education  
d. Social engineering

REQUIRED TEXTBOOK AND MATERIALS:

Text to be assigned by the instructor each semester

STATEMENT FOR STUDENTS WITH DISABILITIES:

Students who require academic accommodations due to any physical, psychological, or learning disability are encouraged to request assistance from a disability services counselor within the first two weeks of class. Likewise, students who potentially require emergency medical attention due to any chronic health condition are encouraged to disclose this information to a disability services counselor within the first two weeks of class. Counselors can be contacted by calling 919-536-7207, ext. 1413 or by visiting the Student Development Office in the Phail Wynn Jr. Student Services Center, room 1209.