CSCI 4347 – CYBER SECURITY CONCEPTS AND PRACTICES

CREDIT HOURS: 3
PREREQUISITES: CSCI 3302
GRADE REMINDER: Must have a grade of C or better in each prerequisite course.

CATALOG DESCRIPTION:

Study of computer and Internet security concepts and practices. Introduction to cryptography and information security. Understanding the different types of malware and how to prevent them. Cloud computing and emerging technologies security risks and practices.

PURPOSE OF COURSE

Introduces students to concepts common in the computer security field. Students will learn about threats and attacks to computer systems and how these threats are mitigated. The students will be introduced to cryptography through the topics of privacy and authentication. Students will use information security concepts to study policy that drives current cloud based and networked systems. The students will be capable of discussing historical perspectives in security and how it is relevant to current technologies.

EDUCATIONAL OBJECTIVES

Upon successful completion of the course, students should be able to:

1. Describe, discuss, and apply security principles to solve problems.
2. Create security policies for different organizational scenarios.
3. Understand and apply cryptography to applications.
4. Detect malicious software and know how to remove it from an infected system.
5. Discuss and build policies for cloud based systems.
6. Apply privacy practices and policies.

COURSE CALENDAR

This course meets for a minimum of 37.5 lecture contact hours during the semester. Students have significant weekly reading assignments. Students are expected to complete 3-4 homework assignments, 4-5 laboratory or programming assignments, and 2-3 periodic exams in addition to the final exam. Students are expected to prepare for any class assignments or quizzes over the material covered in class or in the reading material. Successful completion of these activities requires at a minimum six additional hours of outside of classroom work each week.

CONTENT	HOURS
Security Overview	3
Course introduction Security overview Threats/Attacks Vulnerabilities	
Authentication	6
Authentication Access Control Cryptography	
Malicious Software	6
Unintentional oversights	

Buffer Overflows
Undocumented Access points
Malware-Viruses, Worms, Trojans
Countermeasures

Client Side Web Security 6
Browser Attacks
User Targeted Web Attacks
Obtaining User Data
Phishing attacks
Social Engineering

Operating Systems.......... 6
Overview of Security in Operating Systems
Protected Objects
Secure OS Design
File System Encryption
Correctness and Completeness
Trusted Systems
Rootkits-History and Examples

Cloud Computing 6
Cloud Computing Models
Risk Analysis and Assessment
Tools and Techniques
Authentication
Securing IaaS

Privacy.......... 9
Privacy Concepts
Principles and Polices
Practices
Authentication and Privacy
Data Mining
Web based Privacy
Email Security
Security Planning
Impact on Emerging Technologies

Exams (plus a comprehensive final).......... 3

TOTAL 45

REFERENCES

Bellovin, S.M., Thinking Security, Addison-Wesley, 2016

Pfleeger, C.P. and Pfleeger, S.L. and Margulies, J., Security in Computing, 5th Ed, Pearson, 2015

Stallings, W. and Brown, L., Computer Security Principles and Practice, 3rd Ed, Pearson, 2015

Readings in Current Trends