CSC 547 – CYBER SECURITY CONCEPTS AND PRACTICES

CREDIT HOURS: 3
PREREQUISITES: CSC 241 and CSC 331.
GRADE REMINDER: Must have a grade of C or better in each prerequisite course.
CROSS LISTING: CSC 447

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.

NOTE: Students taking CSC 547 will be expected to complete additional requirements, including but not limited to special projects, class presentations, relevant research including literature review and current research topics from professional journals, and supplemental evaluation (i.e., additional questions, quizzes, tests). Students taking CSC 547 are expected to perform at a higher level than undergraduates taking CSC 447. Students should contact the course instructor early in the semester (i.e., before the end of the add/drop period) to determine the specific additional requirements.

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.

CONTENT

<table>
<thead>
<tr>
<th>Security Overview</th>
<th>HOURS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course introduction</td>
<td>3</td>
</tr>
<tr>
<td>Security overview</td>
<td></td>
</tr>
<tr>
<td>Threats/Attacks</td>
<td></td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td></td>
</tr>
</tbody>
</table>
Authentication

Authentication
Access Control
Cryptography

Malicious Software

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

Client Side Web Security

Browser Attacks
User Targeted Web Attacks
Obtaining User Data
Phishing attacks
Social Engineering

Operating Systems

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

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

Privacy

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

Exams (plus a comprehensive final)

TOTAL 45
REFERENCES


Readings in Current Trends