SCHOOL OF STEM SYLLABUS

TERM:

INSTRUCTOR:

COURSE CODE: CSC-232

OFFICE HOURS:

COURSE TITLE: Cybersecurity

OFFICE LOCATION:

DAY(S) AND TIME(S):

EMAIL:

LOCATION:

PHONE:

COURSE PREREQUISITE: Complete CSC-115 OR CSC-117 OR CSC-118 Can be taken concurrently

CREDITS: 3

COURSE DESCRIPTION:
This course is designed as a core major requirement for students majoring in Computer Science - Cyber Security Option, or as an elective course for students majoring in Computer Science Option. In this course, students will learn and understand threats, risks and challenges facing the cyber world. Students will learn different techniques to make the computing environment and crucial data safer and more secure. Students will be able to realize the impact of security breaches caused by malware, counterfeit software, viruses and worms.

This course covers all security topics considered Core Computer Science Curriculum. Learned knowledge can be used to prep for CISSP Certification, and includes in-depth coverage of Computer Security, Technology and Principles, Software Security, Management Issues, Cryptographic Algorithms, Internet Security and more

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

1. **Demonstrate the understanding** of a variety of computer security techniques, security polices, computer network security principals, technical documents regarding information hiding techniques, challenges and risks in securing the computing environments.
2. **Apply** the use of filters to protect assets – Routers, Firewalls, Demilitarized Zones (DMZ), and perform security awareness.
3. **Interpret** the overall needs, risks threats and challenges to the cyber world and to digital data.
4. **Apply** different types of encryption techniques needed to secure digital data.
5. **Perform** watermarking of digital images using MATLAB.
6. **Perform** risk analysis and resources management required for securing crucial data.

7. **Demonstrate the understanding of Biometric techniques** – Fingerprinting, Vascular Patterns, Thermal Scans, Retinal Scans, etc.

TEXTBOOK AND SUPPLEMENTAL MATERIALS:
Computer Security – Principles AND Practice

4th Edition William Stallings and Lawrie Brown

Pearson

ISBN:978-0-13-479410-5

ISBN: 9-13-4794-10-9

GRADING POLICY:

Item	Weight
Test 1	**25%**
Test 2	**25%**
Labs	**30%**
Discussions & Assignments (writing 1 to two pages about current events or about a topic selected by the instructor)	**20%**

SAMPLE COURSE SCHEDULE:

Session/ week	Unit Learning Outcomes (ULOs)	Assessments and Rubrics	Activities: Learner Interaction and Engagement
1	**Overview** **Course contents** **Course mechanics**	**Homework** **Write one to two pages about Cybersecurity Current Events.** **You may use any Newspaper, News station, Magazine for your reference**	Get familiar with Infosec environment. Watch the Infosec registration video Get Access to Infosec and link your account to the instructor **Watch a video on how labs are done (provided by instructor)**

2 **Chapter 1**	**Upon completing this unit student will understand**: 1.1 Computer Security concepts. 1.2 Threats, Attacks, and Assets. 1.3 Security Functional Requirements 1.4 Fundamental Security Design Principles. 1.5 Attack Surfaces and Attack Trees. 1.6 Computer Security Strategy 1.7 Standards	**Discussion current events**	Lab: Implementing Security Policies on Windows and Linux
3 **Chapter 2** **Cryptographic Tools & User Authentication**	**Upon completing this unit student will understand** 2.1 Confidentiality with Symmetric Encryption 2.2 Message Authentication and Hash Functions 2.3 Public-Key Encryption 2.4 Digital Signatures and Key Management 2.5 Random and Pseudorandom Numbers 2.6 Practical Application: Encryption of Stored Data	**Homework** **Write one to two pages about Cybersecurity Current Events.** **You may use any Newspaper, News station, Magazine for your reference**	Lab: Using Public Key Encryption to Secure Messages
4 **Chapter 3**	**Upon completing this unit student will understand** 3.1 Digital User Authentication Principles 3.2 Password-Based Authentication 3.3 Token-Based Authentication 3.4 Biometric Authentication	Discuss previous assignment	Lab: Implementing NAT and Allowing Remote Access

5 **Chapter 3**	3.5 Remote User Authentication 3.6 Security Issues for User Authentication 3.7 Practical Application: An Iris Biometric System 3. Case Study: Security Problems for ATM Systems		
6 **Access Control** **Chapter 4** ========== **7** **Access Control** **Chapter 4**	**Upon completing this unit student will understand** 4.1 Access Control Principles 4.2 Subjects, Objects, and Access Rights 4.3 Discretionary Access Control 4.4 Example: UNIX File Access Control 4.5 Role-Based Access Control ========== 4.6 Attribute-Based Access Control 4.7 Identity, Credential, and Access Management 4.8 Trust Frameworks 4.9 Case Study: RBAC System for a Bank	**Homework** **Write one to two pages about Cybersecurity Current Events.** **You may use any Newspaper, News station, Magazine for your reference**	Lab: Implementing Common Protocols and Services
8	Midterm Exam		

9 **Malicious Software** **Chapter 6**	**Upon completing this unit student will understand:** 6.1 Types of Malicious Software 6.2 Advanced Persistent Threat 6.2 Propagation — Infected Content - Viruses 6.3 Propagation — Vulnerability Exploit - Worms 6.4 Propagation — Social Engineering — SPAM E-Mail, Trojans 6.5 Payload — System Corruption 6.6 Payload — Attack Agent — Zombie, Bots 6.7 Payload — Information Theft — Keyloggers, Phishing, Spyware 6.8 Payload — Stealthing — Backdoors, Rootkits 6.9 Countermeasures	**Homework** **Write one to two pages about Cybersecurity Current Events.** **You may use any Newspaper, News station, Magazine for your reference**	Lab: 1) Crafting and Deploying Malware Using a Remote Access Trojan (RAT) 2) Social Engineering Using SET
10 **Denial-of-Service Attacks** **Chapter 7**	**Upon completing this unit student will understand:** 7.1 Denial-of-Service Attacks 7.2 Flooding Attacks 7.3 Distributed Denial-of-Service Attacks 7.4 Application-Based Bandwidth Attacks 7.5 Reflector and Amplifier Attacks 7.6 Defenses Against Denial-of-Service Attacks 7.7 Responding to a Denial-of-Service Attack	**Homework** Discuss previous assignment	Lab: 1) Incident Response Procedures, Forensics, and Forensic Analysis 2) Remote and Local Exploitation

11 and 12 **Intrusion Detection & Firewalls and Intrusion Prevention Systems** **Chapter 8**	**Upon completing this unit student will understand:** 8.1 Intruders 8.2 Intrusion Detection 8.3 Analysis Approaches 8.4 Host-Based Intrusion Detection 8.5 Network-Based Intrusion Detection 8.6 Distributed or Hybrid Intrusion Detection 8.7 Intrusion Detection Exchange Format 8.8 Honeypots	**Homework** **Write one to two pages about Cybersecurity Current Events.** **You may use any Newspaper, News station, Magazine for your reference**	Lab: Deep Dive in Packet Analysis - Using Wireshark and Network Miner
13 **Intrusion Detection & Firewalls and Intrusion Prevention Systems** **Chapter 8**	**Upon completing this unit student will understand:** 8.1 Intruders 8.2 Intrusion Detection 8.3 Analysis Approaches 8.4 Host-Based Intrusion Detection 8.5 Network-Based Intrusion Detection 8.6 Distributed or Hybrid Intrusion Detection 8.7 Intrusion Detection Exchange Format 8.8 Honeypots		
14 **Chapter 9**	**Upon completing this unit student will understand:** 9.1 The Need for Firewalls 9.2 Firewall Characteristics and Access Policy 9.3 Types of Firewalls 9.4 Firewall Basing	**Homework** **Write one to two pages about Cybersecurity Current Events.** **You may use any Newspaper, News**	Lab: Deep Dive in Packet Analysis - Using Wireshark and Network Miner Lab: 1)Securing the pfSense Firewall

	9.5 Firewall Location and Configurations 9. Intrusion Prevention Systems 9.7 Example: Unified Threat Management Products	**station, Magazine for your reference**	2)Patching, Securing Systems, and Configuring Anti-Virus
15	Final EXAM		

HCCC POLICIES, STATEMENTS, AND SERVICES:
https://www.hccc.edu/administration/academic-affairs/syllabus-addendum.html