CSCI 4391 Cyber Attacks and Defense
(Fall 2018)

Class Room: Delta 201 **Time:** Tue/Thu 10:00am – 11:20am

Instructor: Wei Wei
Office: Delta 175 *Phone*: (281) 283-3732
Office Hours: Thursday 3:00-5:00pm *Email*: wei@uhcl.edu

Course Objectives and Learning Outcomes:

This course serves as the first cybersecurity class for Computer Science undergraduate students. It introduces the basics of cyber attacks and cyber defense mechanisms, with an emphasis on cyber operations. This course introduces what cybersecurity entails in organizational and enterprise settings, plus other non-technical factors in securing the cyberspace. The overall objective is to help our future computing professionals develop essential understanding of the fundamental concepts underlying cybersecurity. In addition, the understanding will be augmented through multiple hands-on/programming activities, which enhance the understanding by allowing students to see security-in-action. The course is designed in modular fashion so that elements of the courseware could be plugged in other instructional efforts.

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

- Clearly define basic cybersecurity related concepts.
- Illustrate and apply fundamental security principles and practices to typical IT infrastructure components.
- Accurately describe various types of cyber threats and attacks.
- Describe security countermeasures.
- Exercise the secure software development principles in coding.
- Demonstrate skills with tools to enhance systems security.
- Demonstrate understanding of human, organizational, and societal factors in cybersecurity.
- Articulate the emerging security issues with modern enterprise computing.
- Develop understanding of what cyber security entails as a profession.

This course is designed taking into consideration of several industry and academic standards and guidelines as follows:

- *The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF)*;
- *Cybersecurity Curricula 2017-Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity* by Joint Task Force of (1) Association for Computing Machinery (ACM), (2) IEEE Computer Society (IEEE-CS), (3) Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC), and (4) International Federation for Information Processing Technical committee on Information Security Education (IFIP).

- *ABET Cybersecurity Accreditation Initiative*

Course Prerequisites:

CSCI 2315 Data Structures or instructor approval.

Recommended Textbooks and Material:

1. There are two textbooks recommended for this course as follows:
   - Michael Goodrich, Roberto Tamassia, "Introduction to Computer Security", 1st Edition. Pearson. ISBN-13: 978-0321512949, ISBN-10: 9780321512949
   - Wenliang Du, "Computer Security: A Hands-on Approach", 1st Edition. CreateSpace Independent Publishing Platform. ISBN-13: 978-1548367947, ISBN-10: 154836794X.
2. Various readings, lecture notes, and tutorials will be distributed throughout the semester through BlackBoard.

Grading Policy:

Midterm	25%
Final Exam	25%
Individual Assignments (Labs included)	30%
Quizzes	20%

Letter grades will be assigned approximately as follows.

A	93-100	C	74-76.9
A-	90-92.9	C-	70-73.9
B+	87-89.9	D+	67-69.9
B	84-86.9	D	64-66.9
B-	80-83.9	D-	60-63.9
C+	77-79.9	F	<60

Course Website:

We will be using Blackboard for our course management purposes. All materials for the course are available on the web via: https://blackboard.uhcl.edu/webapps/login/. Students who are officially registered to the course have already been added to the course and you have full access to the course contents. By default, your login to the Blackboard system is your university computer account.
It is your responsibility to access blackboard regularly for any updates. You are also encouraged to initiate, participate course-related discussion using the communication tools provided by Blackboard.

General Course Policy:

1. **Academic Honesty Policy:** Please note the guidelines for academic integrity and penalties imposed for violation of these rules. **If you are caught cheating on any of your assignments/exams, you will receive a failing grade for the class**.

University of Houston-Clear Lake Honesty Code:

(For more details, see:

http://prtl.uhcl.edu/portal/page/portal/DOS/Documents_and_Forms/Academic_Honesty_Policy.pdf)

Students assume full responsibility for the content and integrity of the academic work they submit. The guiding principle of academic integrity shall be that a student's submitted work, examinations, reports, or projects must be that student's own work, unless clearly following the rules for allowable group work. Students shall be guilty of violating the Code and be subject to proceedings under it if they cheat, fabricate, plagiarize, and represent others work as their own. You are responsible for reading and understanding the University's policy as described in the above Web Site.

If you violate the honesty code, you may subject yourself to loss of credit for the affected assignment or even a failing grade for the entire course.

2. **UHCL General Program Requirements:**
   http://b3308-adm.uhcl.edu/uhcl_online_catalog/2012-2013UndergradCatalog/general-program-requirements.htm

3. **Class Attendance Policy:** Class activities are intended to give an overview of the material, provide examples and conduct discussions to help you think critically about information systems. You are encouraged to ask questions during the class. Lectures focus on concepts and their applications. Lectures may contain material that is not in the textbook, but you will still be responsible for them on the tests. You are responsible for all lecture material regardless of whether you attend each class, and you must get your own notes from your classmates if you miss a class. **Please note that office hours are not to be used as a substitute for class attendance.**
   The instructor will sample attendance from time to time throughout the semester. ***Attendance is mandatory.***

4. **Classroom Conduct:** Do **NOT** use cell phones in classes. **NO** talking or texting on cell phones. All ringers must be turned off. All earphones, headphones, headset or any other accessories of similar nature must be out of sight during class. Do **NOT** use any electronic devices such as mp3 player and tablet during class. Laptop usage is restricted to class related tasks only.

5. **Special Accommodations:** If you require special academic accommodations under the Americans with Disabilities Act, Section 504, or other state or federal laws, please contact the instructor and the Office of Disability Services (281-283-2626) immediately.

6. **Incompletes:** A grade of "I" (incomplete) will not be administered for this course. UHCL policy allows for the awarding of grades of "I" at the discretion of the instructor, in

extreme cases which prevent a student from completing the course requirements. I will work with any student encountering such a situation to make alternative arrangements for completion of the course requirements by semester's end.

7. **Drop Date:** The last day to drop this course without receiving a grade is **Sep 12th, 2018**. The last day to withdraw the class is **Nov 12th, 2018**. It is the students' responsibility to sign and submit a course withdrawal form in the office of enrollment services in order to be formally withdrawn from the course.

Tentative Course Schedule

Date	Module	Topics
Aug 28	**Security Fundamentals**	Security Concepts and Principles
Aug 30		
Sep 4		Security Management
Sep 6		
Sep 11		The Cybersecurity Industry and Careers
Sep 13		
Sep 18	**Security Threats and Countermeasures**	Security Threat & Cyber Crimes
Sep 20		Safeguard & Countermeasures
Sep 25		Safeguard the IT Infrastructure
Sep 27		
Oct 2		Introduction to Cryptography
Oct 4		
Oct 9	**Network Security**	Network Basics
Oct 11		Network Protocols
Oct 16		Network Administration Basics
Oct 18		
Oct 23		Network Security Basics
Oct 25		
Oct 30	**Midterm**	
Nov 1	**Software Security**	Software Vulnerabilities and Security
Nov 6		Low-level Attacks and Defense
Nov 8		
Nov 13		Secure Programming
Nov 15		
Nov 20		
Nov 27		Web-based System Attacks and Defense
Nov 29		
Dec 4	**Cloud Security**	Cloud Computing Fundamentals
Dec 6		Cloud Security
Dec 13	**Final Exam 10:00am – 12:50pm**	