CSCE 3550 Foundations of Cybersecurity
Department of Computer Science and Computer Engineering
University of North Texas

Instructor: Dr Lotfi ben Othmane <lotfi.benothmane@unt.edu>

Classe meetings: Tuesday/Thursdays 10:00 AM - 11:50 AM in FRLD 380

Instructor Office Hours: Thursdays: 12:00 to 1:00 pm - Take appointment using https://calendly.com/lotfi-benothmane/office-hours

Recitations

CSCE 3550-551
Tu 12:30PM - 1:50PM
Fahmid Shahriar Iqbal <FahmidShahriarIqbal@my.unt.edu>
FOLD 480

Send your emails to me <lotfi.benothmane@unt.edu> and the TA < FahmidShahriarIqbal@my.unt.edu > and will answer your emails within 1 business days. **Begin the subject of your message with"CSCE3550"** for your message to get priority.

The information in this syllabus is subject to change in extenuating circumstances. Changes to the course syllabus, if needed, will be announced via course-wide announcements.

Course Goals and Learning Objectives

The goal of this course is to provide students with foundational knowledge and hands-on experience necessary to manage the security of information systems. Students will become familiar with security threats and vulnerabilities, cryptography, operating system security, network security, and security program management.

Course outcomes are measurable achievements to be accomplished by the end of the course. These outcomes are evaluated as part of our ABET accreditation process:

1. Describe basic security terminology and concepts as well as analyze security threats, vulnerabilities, and attacks.
2. Describe the role of computers and networks in a security context.
3. Develop basic organizational security policies.
4. Demonstrate basic principles and concepts of cryptography and general cryptanalysis.
5. Demonstrate various types of penetration testing to measure the security posture.
6. Discuss the legal and ethical issues involved with securing computer systems, networks, and information.
7. Apply security design principles using a modern programming language to solve various cybersecurity problems.

At the end of the course, students will be able to:

- Assess the security of an information system
- Apply access control and authentication mechanisms to secure systems
- Use encryption mechanisms to ensure the confidentiality of files and volumes
- Monitor and enforce the security of computer networks
- Understand the foundational principles of Internet security

Prerequisites and Corequisites

Corequisite(s): CSCE 2110

Course Format

The course will be delivered onsite. Students can join the lecture sessions on Teams using the link above as observer.

We will have practice exercises during class. The instructor will review submissions from onsite students only and provide feedback on a randomly selected portion of these.

Course Materials

The main Textbook is "Elementary Information Security," authored by Richard Smith, Third/Fourth Edition. The book is accompanied with online lab exercises. You may purchase the eBook and Cloud Lab bundle from the provider at
https://www.jblearning.com/catalog/productdetails/9781284305937

Required Book Title: EBC: Elementary Information Security 4E eBook
ISBN: 9781284282801
Use Course ID **853DCD** to enroll in course labs on the www.jblearning.com.

Learning Activities and Assessments

Learning Activities

To successfully complete this course, students will do the following:

- Attend the lectures or watch the recorded lectures.
- Participate in discussion topics
- Complete the quizzes
- Complete the labs
- Complete the HomeWorks
- Complete the project

Assessments

Security News- Each team (composed of up to 3 students) will select a recent news story about cybersecurity attacks, prepare a presentation of up to 10 minutes, and present it to their peers. The presentation counts for 10% of the final grade.

Labs - There will be 6 lab exercises, each carrying equal weight. The labs account for 25% of the final grade. This is individual work.

Homework - There will be a set of homework assignments, each carrying equal weight. The assignments account for 15% of the final grade. This is individual work.

Project - Each team (composed of up to 4 students) will apply their knowledge in a project and submit a report at the end of the semester. The project counts for 15% of the final grade.

Quizzes - There will be a set of quizzes, each carrying equal weight, with almost one quiz per module. The dates of the quizzes will be announced as the semester progresses. The quizzes account for 25% of the final grade. Each student will have the opportunity to exclude their lowest quiz score or the score from a quiz they missed.

In-Class Exercises - There will be frequent in-class practice exercises and online participation activities. Students will submit their individual attempts to earn grades, and the answers will be discussed in class. These activities account for 10% of the final grade. Grades are based on participation and attempts, not on the correctness of answers.

On certain occasions, students will be invited to solve problems on the board and will be rewarded with quiz bonus points.

Final Grade Calculation

Canvas assumes that the scores for activities within each assessment group are cumulative when computing final grades. Since we use equal-weight assessment activities, the Canvas grade will be an approximation of the final grade. The rules outlined above will be applied when calculating the final grades at the end of the semester.

Grading Policies

The grading scheme is:

Current grading scheme for this assignment

Name:		**Range:**
A	100 %	to 90.0%
B	< 90.0 %	to 80.0%
C	< 80.0 %	to 70.0%
D	< 70.0 %	to 60.0%
F	< 60.0 %	to 0.0%

Grade Appeal Process

If you become concerned about the class management, please communicate your concerns with your instructor. Concerns sometimes relate to grading methods, paper turnaround time, and course policies, as examples.

Students have 7 days after returning the grades to contest their scores. Requests that come after 7 days will be ignored.

Course Policies

Feedback

All graded assessments will be returned with feedback within 10 days of the due date, when possible. Personalized feedback will be provided for each assignment and reflection. In addition, responses to common questions and unclear content will be posted at the conclusion of each module. Comments will be posted at the conclusion of each discussion.

Unclaimed student quiz sheets will be discarded one week after they are returned in class.

Missed and late coursework

It is important to keep up with the pace of this course; therefore late submissions will be reduced by a penalty of 5% for each late day up to 5 days.

Make sure to keep careful track of submission deadlines for all your work in this class.

Integrity and Student Conduct

All department policies on Academic Integrity and Student Conduct apply for this course – these are available at the following link: http://cse.unt.edu/resources/cse_integrity_policy.html Any exceptions to this policy are noted explicitly in the syllabus

While students are encouraged to use generative AI, submitting solutions or/and answers to the assessment activities generated using of these technologies is considered violation of academic integrity.

Attendance

Course attendance is optional, but **recitation attendance is mandatory.**

Expectations

- Each student should have laptop that they could use for the in-class activities.
- Students are expected to focus on the lecture during the course sessions.

Course Topics

The modules are:

1. Overview of cybersecurity
2. Access control
3. Authentication
4. Encryption
5. Network security
6. Internet security
7. Software Security