Course Syllabus for CSCE 4565 – Secure Software Systems
Department of Computer Science and Computer Engineering
University of North Texas

This course covers: Fundamentals and techniques to design and implement software systems. Assessment of security vulnerabilities in software systems, exploitation of software vulnerabilities, and methods to secure vulnerable software. Secure coding practices, data analytics for security, microservices and cloud services security. Reverse engineering and security assessment of cyber-physical systems.

Term: Spring 2026 (January 12, 2026, to May 8, 2026)

Credit hours: 3

Pre-requisite: CSCE 3550 - Foundations of Cybersecurity

Meeting times: Section 1 - Fr 8:30AM - 11:20AM in NTDP K110

Recitation - We 10:30AM - 1:20PM in NTDP F210

Instructor & Contact Information

- **Instructor:** Dr. Lotfi ben Othmane
- **Email:** lotfi.benothmane@unt.edu
- **Office Hours:**
  - Tue: 1:00–2:00 PM
  - Wed: 10:00–11:00 AM
  - Thu: 2:00–3:00 PM
  Reserve 15 minutes timeslot via Calendly
- **Teaching Assistants:**
  - Feras Benchellal (FerasBenchellal@my.unt.edu)

Note: The information in this syllabus is subject to change in extenuating circumstances. Any changes will be announced via course-wide communications.

Course Goals and Learning Objectives: The goal of the course is to provide students with the knowledge and first-hand experience they need to develop secure software. The students will get familiar with exploiting software vulnerabilities and will experiment with the techniques to design secure software and to ensure the security of developed software. In addition, they will learn to use of empirical research methods to study software security challenges.

At the end of the course, the students will be able to:
- Assess the security in vulnerable software systems
- Exploit software vulnerabilities
- Apply best practices in secure software development
- Build effective cryptographic-based functionalities and assess their vulnerabilities
- Assess security implications for emerging software technologies

Course Materials

There is no textbook. A set of papers and chapters will be distributed.
Lotfi ben Othmane, Practice Exercises for Secure Software Engineering, HERE

Course Format

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

[Meeting Link on Teams](#)
Meeting ID: 270 479 709 594 08
Passcode: ML6uR69R

Note: Practice exercises will take place during class. The instructor will review submissions from onsite students and provide feedback for a randomly selected portion of these. Submissions from students attending online will not be reviewed. Students attending via Teams will not have visibility of the classroom board used for in-class activities.

<u>**Learning Activities and Assessments**</u>

Learning Activities

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

- Attend the lectures or watch the recorded lectures.
- Watch additional media.
- Participate in discussion topics.
- Participate in assigned group projects.
- Complete quizzes and exams.
- Complete the project.

Assessments

1. **Labs on Software Attacks**
   o There will be 3 lab exercises that have equal weights.
   o The labs work on Windows-based computer only.
   o The labs count 25% of the grade.
   o You can work on the labs in **pairs** or individually.
2. **Assignments**
   o Four assignments with equal weight, worth 20% of the grade.
   o Individual work only.
3. **Project**
   o Teams (up to 4 members) will assess the security of open-source software or research a related topic.
   o Worth 20% of the grade.
4. **Quizzes**
   o 7 One quiz per module (approximately). Dates announced during the semester.
   o Lowest quiz score or missed quiz excluded from the final grade.
   o Collectively worth 25% of the grade.
5. **In-Class Exercises**
   o Frequent in-class practice exercises and online participation activities.
   o The students will submit their individual attempts to get grades, and the answers will be discussed in-class.
   o The activity counts for 10% of the grade. (The grades are given based on attempts and not correct answers.)

      ○   On certain occasions, students will be invited to come up to the board, solve problems, and get consequently rewarded with quiz bonus points.

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

Differences in Requirements for Graduate and Undergraduate Students

- Undergraduate students will complete three designated labs, while graduate students will complete five labs. Undergraduate students may choose to complete the two other labs for bonus points.
- Undergraduate students are expected to attend recitation sessions to receive assistance from Instructional Assistants (IAs) on labs and assignments. Attendance of the recitation sessions will be counted in the participation score.
- Undergraduate students are encouraged to focus on projects that analyze the security of open-source software, rather than pursuing research projects.

Grading Policies
A: 90%-100%
B: 80%-89.99%
C: 70%-79.99%
D: 60%-69.99%
F: Below 60%

Grade Appeal Process:

- Students have seven days to contest grades after they are returned.

<u>**Course Policies**</u>

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.

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 of 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

Academic Integrity & Generative AI

- Generative AI tools (e.g., ChatGPT, Copilot) may be used only for clarification, writing improvement, or additional study support.
- **Prohibited:** Submitting AI-generated solutions to labs, assignments, quizzes, or projects.
- **Examples:**
    - ✅ Acceptable: Using AI to check grammar in reports.
    - ❌ Unacceptable: Using AI to solve an assignment or generate code for labs.

Attendance

Attendance is not required.

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.

Communication Channels

You can contact your instructor via the following channels:

- **Send your emails through Canvas.** A TA is assigned to answer your emails within 1 business days. You may also email ma at lotfi.benothmane@unt.edu) on time and I will try to answer you within 2 business days. Begin the title of your message with "CSCE4565" or "CSCE5565" if you email me directly. Send me a reminder if I do not answer on time.
- General announcements will be in the Announcements section of this Canvas course | sent via email | sent using the Canvas Inbox.

Netiquette

- All communication within the course should adhere to university standards. Specifically, communication should be scholarly, respectful, professional, and polite.
- You are encouraged to disagree with other students, but such disagreements need to be based upon facts and documentation. It is my goal to promote an atmosphere of mutual respect in our interactions. Please contact me if you have suggestions for improving the interactions in this course.
- Professional and respectful tone and civility are used in communicating with fellow learners and the instructor, whether the communication is by electronic means or by phone or face-to-face.
- Video interactions reflect a respectful tone in verbal communications and body language.
- Use correct spelling and grammar

Group Communication

In this course, you will work with peers in small groups. You may need to schedule synchronous calls, participate in group discussions or other learning activities. The same group communication guidelines apply:

- Engage, follow-through, contribute and ask questions.
- Be on time and make sure that tall of your technology works before you start.
- Before you contact the instructor with any group-related issues, talk through them first with your group members. If you are getting no positive reaction, make arrangements to discuss the issues with your instructor.

Technology Requirements

For optimized learning experience in this course, please ensure you have access to the following technology:

- Student-provided personal computer.
- Reliable Internet access. A wired Ethernet connection to the internet is very strongly suggested. Wireless and cellphone data connections may experience connection problems. Android and iOS operating systems are not fully supported at this time.
- While tablets, smartphones and other mobile devices may allow for some completion of coursework, they are not guaranteed to work in all areas. It is recommended that you have access to a Windows or Mac-based computer to complete coursework in the event your selected mobile device does not meet the needs of the course.

Students who need assistive technologies might have different computer and technology requirements. Please check with Student Accessibility Services to determine the requirements for the specific technologies needed to support you in your online classes.

Course Technologies

This course will use several technologies. Check out the technology descriptions, accessibility and privacy security statements and technology-specific guides in the links provided below.

1. This course uses Canvas as the learning management system.
2. This course will use Teams for synchronous online interactions.

Course Topics

1. Introduction to Software Security
2. Risk Analysis
3. Security Architecture
4. Implementing Security Features
5. Secure Coding
6. Reverse Engineering
7. Security Assessment
8. AI for Security