CSE 4380: Information Security I

Spring 2025

Instructor Information

Instructor: Faysal Hossain Shezan

Office Number: ERB 556-C

Email Address: faysal.shezan@uta.edu

Faculty Profile: **fhshezan.github.io**

Office Hours: Wednesday, 2:30 PM - 3:30 PM

Course Information

Section Information: CSE 4380, Section 004

Time of Class Meetings: Wednesday, 4:00 PM -6:50 PM

Place of Class Meetings: NH 111

Lab Information

Lab Section Information: CSE 4380 Sections 005, CSE 4380 Sections 006 and CSE 4380 Sections 007.

Time of Class Meetings: MO 5:30- 8:20 PM, TU 5:30PM - 8:20PM and TH 5:30PM - 8:20PM

Place of Lab Meetings: ERB 106

GTA Information

GTA: Vasudevamurthy, Karan

GTA Email Address: kxv4439@mavs.uta.edu

Office Number: Online (Microsoft Teams)

Office Hours: Friday 01:00 PM to 03:00 PM

GTA: Shekofteh, Amirhossein

GTA Email Address: axs8187@mavs.uta.edu

Office Number: ERB 204

Office Hours: Friday 3:00 PM to 5:00 PM

Course Description

Description of Course Content:
This is the hands-on introduction to the basics of security for upper-level undergraduate students and graduate students. Includes system security, buffer overflows, a high-level overview of cryptography, firewalls and intrusion detection/prevention, malware, penetration testing, forensics, and system administration.

Student Learning Outcomes:

- Use cryptographic primitives directly in order to understand their respective uses and how they work together to provide security.
- Develop simple malware in order to understand hooking and how hooking can be subverted for malicious purposes.
- Set up and use defensive and security testing technologies in the network and operating system in order to see how they defend against attacks.
- Exploit software vulnerabilities in order to understand how they work and how defenses could stop them.
- Study a range of concepts to gain a broad understanding of the field of information security.
- Apply class knowledge in a capture-the-flag simulation exercise at the end of the semester.

Required Textbooks and Other Course Materials:

- *Computer Security: Principles and Practices by William Stallings and Lawrie Brown (3rd edition) ISBN-13: 978-0133773922, ISBN-10: 0133773922*
- In addition to the textbook, each week the instructor may provide some papers and articles.

Technology Requirements
Assignments and slides are posted on Canvas. You should submit your assignments on Canvas. The exams will be in-person. We try to record and share the course on Canvas.

Grading Information

Grading:

Exams (2 in-class):	30%
Lab Exercises (4 in-labs with 4 pre-lab exercises): Labs 1 & 3 worth 7%, Labs 2 & 4 are worth 10%	34%
CTF Lab:	11%
Presentation + Class Participation:	10%
Pop Quiz	5%
In-Class Quiz:	10%

Grades for the exam will be curved by the instructor and scaled to a standard A = 90-100, B = 80-89, C = 70-79 scale. Final grades will simply be the weighted average of the scores based on the above percentages. Small amounts of extra credit may be available, but only on a class-wide basis (no individual requests will be granted). No grade bumps will be offered; 89.99 is a B in this class.

All students are expected to take responsibility for their own work. Full or partial copying of another's work will be considered ***plagiarism***. The instructor reserves the right to make decisions in such cases. Students found engaging in these activities may face penalties ranging from receiving a score of zero to a negative score for the assignment. Both the original author of the content and the individual who copied it will be held equally responsible and face the same consequences. Based on the situation, the instructor reserves the right to decide the penalty.

Students are expected to keep track of their performance throughout the semester, which Canvas facilitates, and seek guidance from available sources (including the instructor) if their performance drops below satisfactory levels; see "Student Support Services" below.

Expectations for Out-of-Class Study: Beyond the time required to attend each class meeting, students enrolled in this course should expect to spend at least additional 9 hours per week.

Make-up Exams: Make-ups for graded activities may be arranged if your absence is caused by illness or a personal emergency. A written explanation (including supporting documentation) must be submitted to your instructor; an alternative to the graded activity will be arranged if the explanation is acceptable. Make-up arrangements must be arranged before the scheduled due date.

Grace periods: To accommodate for unavoidable circumstances, you will be given one **3-day** grace period for your assignments. Beyond the deadline (and grace period if applicable), you will be penalized 25% a day. For example, if you score 73% and are 5 minutes late, you will be penalized 25% for one day, resulting in a score of 73 – 25 = 48%). Use these freebies wisely — they are meant for circumstances such as falling ill or interviewing. I will not grant any additional extensions.

Attendance: At the University of Texas at Arlington, taking attendance is not required, but attendance is a critical indicator of student success. Each faculty member is free to develop their methods of evaluating students' academic performance, including establishing course-specific attendance policies. As the instructor of this section, I will be grading attendance based on your participation in each lecture**.** However, while UT Arlington does not require instructors to take attendance in their courses, the U.S. Department of Education requires that the University have a mechanism to verify Federal Student Aid recipients' course attendance. UT Arlington instructors should be prepared to report the last date of attendance as part of the final grading process. Specifically, when assigning a student a grade of F, faculty must report the last date a student attended their class based on evidence of academic engagement such as a test, participation in a class project or presentation, or an engagement online via Canvas. This data is reported to the Department of Education for federal financial aid recipients.
Lab Attendance and Completion: Attendance to your assigned virtual lab section during lab 1 is mandatory. Other lab exercises will take place at home.

Lab Attendance and Completion: Attendance to your assigned lab section during lab weeks is mandatory. You are expected to come to the lab having completed a pre-lab assignment that the GTA will check before you may begin the lab. No make-up lab except for illness or personal emergency. A written explanation must be submitted to your instructor at least one day before your assigned lab time.

Descriptions of major assignments and examinations:

- **Presentations:** Students will give a 10-minute brief presentation in class to discuss a couple of recent security vulnerabilities or defenses related to the class's topic that week. The presentation topic should have a dedicated CVE/CWE number. The instructor arranges the date for each student. Student + Instructor will grade the presenter's presentation.

- **Labs:** You will work in pairs to learn how attacks operate and how to defend against them.

  Lab 1: Cryptography: Week 4
  Lab 2: User, system, network security: Weeks 6 and 7
  Lab 3: Buffer overflows: Week 12
  Lab 4: Security testing software: Weeks 13 and 14
  CTF: Lab 15

- **Assignments**: There will be 4 assignments through the semester. Each lab exercise includes a pre-lab assignment due by Sunday midnight before the lab week.

  Pre-Lab 1. Cryptography: due by Feb 2
  Pre-Lab 2. User, System, Network Security: due by Feb16

Pre-Lab 3: Malware: due by Mar 30
Pre-Lab 4: Buffer Overflows: due by Apr 06
Pre-CTF: due by Apr 20

- **Exam 1**: in-class, Mar 26
  Covers everything discussed up to and including Week 8

- **Exam 2**: in-class, May 7
  Comprehensive; focus on Buffer Overflows and Web Security

- **In-Class Quiz:** Based on the previous class lecture there will be **10 marks "**surprised" in-class quiz

- **Pop Quiz:** Based on the current class lecture there will be **two "**surprised" in-class pop quiz. For this you need to pay attention to the class lecture and discussion.

- **Quiz:** (Information Assurance Education Certificate**, NOT** included in the grading)
  The quiz covers administrative issues in securing networks.

Institution Information

UTA students are encouraged to review the below institutional policies and informational sections and reach out to the specific office with any questions. To view this institutional information, please visit the Institutional Information page (https://resources.uta.edu/provost/course-related-info/institutional-policies.php), which includes the following policies, among others:

- Drop Policy
- Disability Accommodations
- Title IX Policy
- Academic Integrity
- Student Feedback Survey
- Final Exam Schedule

Recording of Classroom and Online Lectures

Faculty maintain the academic right to determine whether students are permitted to record classroom and online lectures. Recordings of classroom lectures, if permitted by the instructor or pursuant to an ADA accommodation, may only be used for academic purposes related to the specific course. They may not be used for commercial purposes or shared with non-course participants except in connection with a legal proceeding.

Generative AI Use in This Course

The use of Generative AI (GenAI) in course assignments and assessments must align with the guidelines established by the instructor. Unauthorized use of GenAI could result in breaches of academic integrity. Instructors bear the responsibility of clearly delineating the permissible uses of GenAI in their courses, underscoring the importance of responsible and ethical application of these tools. The UTA Office of Community Standards articulates the university's stance on academic integrity and scholastic dishonesty. These standards extend to the use of GenAI. Unauthorized or unapproved use of GenAI in academic work falls within the scope of these policies and will be subject to the same disciplinary procedures.

Course Schedule (Subject to Change)

Week	*Class Dates*	*Topic*	*Activity*	*Due Dates*
1	Jan 15	Class overview, motivation and overview of computer security		
2	Jan 22	Cryptography: Symmetric Encryption	Pre-Lab 1	Feb 2
3	Jan 29	Cryptography: Message Authentication and Hash Functions		
4	Feb 5	Cryptography: Public-Key Encryption and Homomorphic Encryption	Lab 1 and Pre-Lab 2	Feb 16
5	Feb 12	User Authentication		
6	Feb 19	Access Control	Lab 2.1	
7	Feb 26	Securing the Internet: intrusion detection systems	Lab 2.2	
8	Mar 5	Securing the Internet: firewalls, intrusion detection systems + Exam Review		
9	**Mar 19**	**EXAM 1**	Pre-lab 3	Mar 30
10	Mar 26	Internet vulnerability: malware, viruses, worms	Pre-lab 4	Apr 6
11	Apr 2	Internet vulnerability: Denial-of-Service Attacks Software security: Memory architecture + buffer overflow	Lab 3	
12	Apr 9	Defense for buffer overflow + common attacks	Lab 4.1 Pre-CTF	 Apr 20
13	Apr 16	Web Security: Injection Attacks	Lab 4.2	
14	Apr 23	Web Security: Injection Attacks + Exam Review	CTF	
15	Apr 30	Student Study Day (No class)		
17	**May 7**	**Exam 2 + Quiz (Information Assurance Education Certificate)**		

As the instructor for this course, I reserve the right to adjust this schedule in any way that serves the educational needs of the students enrolled in this course. — Faysal Hossain Shezan

Additional Information

Mandatory Face Covering Policy
Face coverings are not mandatory; all students and instructional staff are welcome to wear face coverings while they are on campus or in the classroom.

Emergency Exit Procedures:
Should we experience an emergency event that requires evacuation of the building, students should exit the room and move toward the nearest exit. When exiting the building during an emergency, do not take an elevator but use the stairwells instead. Faculty members and instructional staff will assist students in selecting the safest route for evacuation and will make arrangements to assist individuals with disabilities.

Academic Success Center:
The Academic Success Center (ASC) includes a variety of resources and services to help you maximize your learning and succeed as a student at the University of Texas at Arlington. ASC services include supplemental instruction, peer-led team learning, tutoring, mentoring and TRIO SSS. Academic Success Center services are provided at no additional cost to UTA students. For additional information visit: Academic Success Center (https://www.uta.edu/student-success/course-assistance). To request disability accommodations for tutoring, please complete this tutoring request form (https://www.uta.edu/student-success/course-assistance/tutoring/request).

The IDEAS Center (https://www.uta.edu/ideas/) (2nd Floor of Central Library) offers **FREE** tutoring and mentoring to all students with a focus on transfer students, sophomores, veterans and others undergoing a transition to UT Arlington. Students can drop in or check the schedule of available peer tutors at www.uta.edu/IDEAS, or call (817) 272-6593.

The English Writing Center (411LIBR):
The Writing Center offers **FREE** tutoring in 15-, 30-, 45-, and 60-minute face-to-face and online sessions to all UTA students on any phase of their UTA coursework. Register and make appointments online at the Writing Center (https://uta.mywconline.com). Classroom visits, workshops, and specialized services for graduate students and faculty are also available. Please see Writing Center: OWL (http://www.uta.edu/owl) for detailed information on all our programs and services.

Librarian to Contact:
Each academic unit has access to Librarians by Academic Subject (http://www.uta.edu/library/help/subject-librarians.php) that can assist students with research projects, tutorials on plagiarism and citation references as well as support with databases and course reserves.

Emergency Phone Numbers
In case of an on-campus emergency, call the UT Arlington Police Department at **817-272-3003** (non-campus phone), **2-3003** (campus phone). You may also dial 911. Non-emergency number 817-272-3381.