TROY UNIVERSITY

CS 451

Computer Security

COURSE SYLLABUS

Spring 2026

PRE-REQUISITES:

CS 3323 or CS3330

INSTRUCTOR INFORMATION:

Anh Tu Tran

Secure AI Lab: https://secureai-lab.com/

Email: tu.trananh@hust.edu.vn

Phone: +84 367139457

INSTRUCTOR EDUCATION:

CATALOG DESCRIPTION:

This course provides a comprehensive introduction to Information Security, covering both foundational principles and modern security technologies. Students will explore core concepts such as confidentiality, integrity, availability (CIA), risk management, and defense-in-depth, alongside key technical domains including network security, endpoint protection, identity and access management, cloud and mobile security, digital forensics, and security operations.

Through real-world case studies, threat analysis, and a hands-on final project, the course develops the ability to evaluate security risks, understand common attack techniques, and apply structured security frameworks in organizational and technical environments. By the end of the course, students will be equipped with both conceptual understanding and practical insight into protecting digital systems, data, and critical infrastructure in today's evolving threat landscape.

STUDENT OUTCOMES:

By the end of this course, students will be able to:

- Understand core security principles (CIA, risk, defense-in-depth).
- Identify common threats across network, endpoint, cloud, mobile, and AI contexts.
- Explain key security technologies (firewalls, encryption, IAM, monitoring tools).
- Analyze security incidents using structured frameworks.
- Apply basic incident response and risk assessment concepts.

COURSE REQUIREMENTS

To successfully complete this course, students are expected to:

- Attend and actively participate in lectures and discussions.
- Complete the midterm multiple-choice examination.
- Work collaboratively on the final group project.
- Submit required reports and presentations on time.
- Demonstrate academic integrity in all assessments.

No advanced technical background is required, but basic familiarity with digital systems and networking concepts is recommended.

GRADING

Participation: 10%

Discussion: 10%

Quizzes: 25%

Individual Projects: 25%

Team Final Project: 30%

GRADING SCALE:

Grades will be assigned according to the following scale:

A 90 - 100

B 80 - 89

C 70 – 79

D 60 – 69

F below 60

TEXTBOOK

Computer Security Fundamentals, 5th Edition By Easttom, William

ISBN-13: 978-0-13798478-7 ISBN-10: 0-13-798478-2

REFERENCE

METHODS OF INSTRUCTION: In-Classroom Lectures, Projects Handouts/Homework, Class Participation and Reading assignments.

TEAMS CODE:

HONESTY AND PLAGIARISM

*Plagiarism is defined as submitting anything for credit in one course that has already been submitted for credit in another course or copying any part of someone else's intellectual work – their ideas and/or words – published or unpublished, including that of other students, and portraying it as one's own. All students are required to read the material presented at: http://troy.troy.edu/writingcenter/research.html

All material submitted for grade must be the student's own work.

Anyone found cheating and/or copying will receive an automatic 0 for that assignment or exam or dismissal from the course. This goes for the person who copies as well as the person who allows their work to be copied. A serious penalty (e.g: one lower letter grade) will be given for cheating and plagiarism and students will be required to retake a course if they get D or worse for that course.

OTHER POLICY

There will be no make-up test. A missed test or exam will result in 0 points. Contact me in advance in case of emergency such as illness. An original letter address to me on a letterhead paper from a physician or hospital stating that you could not take the test or exam as scheduled is necessary for me to consider your case.

Students with more than 3 absences will not be allowed to take final exam.

PROJECTS

Students are required to submit their source code file(s) as email attachments prior to the project deadline. In the event you are unable to complete a project or make it work correctly, be sure to email your latest source code to receive partial credit. Students failing to submit projects within the allotted time will receive a project grade of zero and will not be allowed to make late submissions. Exceptions will be made ONLY under extenuating circumstances and ONLY with prior approval by the instructor. To receive full credit, projects must be submitted on or before the due date.

TENTATIVE SCHEDULE

1	Introduction to Computer Security	
2	Identity & Access Management	
3	Social Engineering & Human Factor	
4	Cryptography & Data Protection Basics	
5	Endpoint Security & Malware	
6	Network Security Fundamentals	
7	Midterm	
8	Application & Web Security	
9	Cloud Security Fundamentals	
10	Mobile Security & IoT Risks	
11	AI, Deepfake & Emerging Threats	
12	Incident Response Lifecycle	
13	Digital Forensics Fundamentals	
14	Security Management & Risk Governance	
15	Final Exam	