CSCE 5550.002 Introduction to Computer Security  
Spring 2024

1. Course Information

CSCE 5550.002: Tuesday, 6:00 pm - 8:40 pm, NTDP B140

Instructor:
Tao Hou  
Email: tao.hou@unt.edu  
Office Location: NTDP F278  
Office Hours: Tuesday, 2:00 pm – 4:00 pm

TA:
Lang Zhou  
Email: langzhou@my.unt.edu  
Office Location: NTDP F258  
Office Hours: Thursday, 3:00 pm – 5:00 pm

2. Course Description and Goals

The course will provide a solid theoretical foundation for computer security, and hands-on experience in applying the theory to practice. Students will get a comprehensive understanding of computer security, including basic security concepts, common attack and defense techniques, and emerging security topics.

Main goals:
- Understand the basic security problems in computer systems.
- Understand both security theories and security practices.
- Understand design and implementation of secure computer systems.

3. Course Contents (tentative)

- Introduction of security: concept of security and insecurity, technical, operational, and human threats, etc.
- Access control and cryptography: principle of enforcing security policies, identity: subject, object and role, mechanisms and practice, firewall, encryption and decryption, key management, etc.
• Software security: buffer overflow, typical attacks and defenses, isolation, sandboxing, security analysis, etc.
• Web security: same origin policy, typical attacks and defenses, DNS security, https, etc.
• Network security: user privacy; typical attacks and defenses, IoT security, etc.
• Emerging topics: Intel SGX, Spectre/Meltdown attacks, mobile security, etc.

4. Textbook Information

Please check the course website (Canvas) regularly for announcements, lecture slides, and an up-to-date schedule.

5. Evaluation Items and Grading Policy

<table>
<thead>
<tr>
<th>Item</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignments</td>
<td>40%</td>
</tr>
<tr>
<td>Team project</td>
<td>30%</td>
</tr>
<tr>
<td>Exam</td>
<td>25%</td>
</tr>
<tr>
<td>Class participation</td>
<td>5%</td>
</tr>
</tbody>
</table>

The weights are subject to minor variation.

6. Assignments

There will be written homework assignments and programming assignments.

Discussions with friends to enhance understanding of the course materials are encouraged. However, please be aware of the following strict prohibitions to assignment problems: (1) discussing specific solutions, and (2) using ChatGPT or similar tools. It is imperative that the assignment reflects your own work.

7. Team Project

This course will have a team project. Students can work on the project in a small group of 2 students. The project involves performing and presenting cooperative research in the broad area of cybersecurity. The students will select the topic by themselves, but the topic should be advanced techniques related to cybersecurity and the fundamental topics covered in classes are not suggested. The research could be: (1) Write a survey paper of a security topic (e.g., Advanced DDoS, ML in security) which covers at least 50 recently published papers, or (2) Develop a new attack or defense system. Specifically,
1) Each group will have to submit a preliminary project proposal (1-2 pages) describing the members in your team, the problem you plan to work on, existing approaches to the problem, and techniques or plans to address the problem. We may also schedule some class time for you to present your research plan.

2) At the end of the semester, each group need to prepare a formal in-class presentation to show your research findings. The presentation slides must be made by yourself and it’s not allowed to use others’ shared slides.

3) Write a final research/survey paper. Your paper should present small-scale research or comprehensive survey in the broad area of cybersecurity. This paper will be graded on readability, correctness, thoroughness, novelty, and significance. Your paper will be at least 12 pages in length for main content, plus well-formatted references. It’s required that to use Latex and IEEE conference template to write the paper. The template can be downloaded from this link. In the paper, please include at least the following:

   For research papers:
   - An **abstract** that summarizes your work.
   - An **introduction** that motivates the research problem you are trying to solve.
   - A **related work** section that differentiates your contributions.
   - Section(s) describing your **architecture** or **methodology**.
   - **Results** and/or **evaluation** section(s), with data or figures to support your claims as appropriate.
   - A brief **future work** section explaining what is left to do.
   - Appropriate **citations** and **references** from the literature.

   For survey papers:
   - An **abstract** that summarizes your work.
   - An **introduction** that motivates the survey you are trying to conduct.
   - A **related work** section that differentiates your contributions.
   - Section(s) describing your **survey results**, with tables or figures to support your claims as appropriate.
   - A **future research opportunity** section discussing the potential research directions in the area.
   - Appropriate **citations** and **references** from the literature.
8. Class Participation

Attendance is highly RECOMMENDED. The lectures cover the knowledge and skills directly for all assignments and exams.

Class participation will be graded based on the contributions to class conversation and popup quizzes.

9. Grading System

The scale for final letter grades is as follows, using standard notation for ranges:

A = (∞,90]  
B = (90,80]  
C = (80,70]  
D = (70,60]  
F = (60,-∞)

10. Course Policy

Drop: YOU MUST OFFICIALLY WITHDRAW FROM THIS CLASS BEFORE THE LAST DROP DAY. Then, you will get “W”. Otherwise, you will get “U” (uneearned failure).

Incomplete: The "I" grade may be assigned when, due to unusual circumstances beyond the student’s control, a significant portion of a course, such as a term paper or final examination, has not been completed. If you cannot complete a class for any reason and need to retake the class in a future semester, I cannot give you “I”.

Makeup: NO MAKEUP EXAM OR MAKEUP HOMEWORK OR MAKEUP PROJECT OR MAKEUP QUIZ.

Submissions: NO EMAIL submission. All assignments shall be submitted in Canvas.

Late Policy: Starting right after the required submission date of every assignment, 10% of the grade will be deducted per day up to five days. NO points will be given to submissions more than five days late.

Copyright: The materials provided on the Canvas course site including recorded lectures, lecture slides, assignments, handout code, and exams are protected by Copyright and for the exclusive use of students enrolled in this course. Allowing others
to access this material by placing it on publicly available git repositories or submitting to note sharing sites (which encourage you to break the law and post copyrighted content you don’t own) is expressly forbidden.

**Academic Honesty:** All assignments are automatically checked for plagiarism in Canvas. Any attempts at obtaining homework, project, or exam solutions from note sharing sites or from other sources are considered cheating and carry the same penalty. The department regularly monitors websites for posted solutions. NO copying or sharing any code and writing in any assignment, project or exam with anyone or from any source.

**Academic Integrity Standards and Consequences:** According to UNT Policy 06.003, Student Academic Integrity, academic dishonesty occurs when students engage in behaviors including, but not limited to cheating, fabrication, facilitating academic dishonesty, forgery, plagiarism, and sabotage. A finding of academic dishonesty may result in a range of academic penalties or sanctions ranging from admonition to expulsion from the University. Based on the Student Academic Integrity Policy (UNT Policy 6.003), any form of "unauthorized assistance" constitutes cheating. If the use of artificial intelligence (e.g., ChatGPT) is not authorized for the assignment in question, the violation is "cheating". All the students are expected to read: https://policy.unt.edu/policy/06-003

**University Policies:** This course complies with all academic policies of University of North Texas. Do check these policies through university websites and student handbooks.

*Every part of this syllabus is subject to adjustment as the semester progresses. Please contact me as soon as possible if you’re dissatisfied with the course policies, discussions, readings, grading, etc.; I’ll be happy to accommodate reasonable requests for modifications.*