

Syllabus

Instructor: Dr. Guan-Hua (Scott) Tu

Email: ghtu@msu.edu

Office: 1124B Engineering Building

Office hours: 2:15pm-3pm, Monday (<https://msu.zoom.us/j/98303816307>) (passcode: CSE425SS).

Teaching assistant: Yiwen Hu

Email: huyiwen3@msu.edu

Office hours: 10am-12pm, Wednesday (<https://msu.zoom.us/j/7282337364>).

Teaching assistant: Cameron White

Email: whitec60@msu.edu

Office hours: 3pm-4pm, Thursday (<https://msu.zoom.us/j/6165580662>).

Times and location

Times: 12:40pm-2pm, Monday and Wednesday

Location: STEM 1202 and Zoom (<https://msu.zoom.us/j/91358648744>, passcode: CSE425SS)

Website and Discussion Forum:

Course website: <https://d2l.msu.edu/d2l/home/1383919>

Discussion forum: <https://piazza.com/msu/spring2022/cse425> (class access code: CSE425)

Course Description

This course provides an introduction to a variety of topics in computer security for juniors and seniors majoring in computer science and engineering. It covers four parts: (1) computer security technology and principles (cryptography, authentication, access Control, database Security, DoS, malicious software, intrusion detection, firewall, etc.), (2) software security and trusted Systems (buffer overflow, software security, operating system security, etc.), (3) network security (internet security protocols, authentication app, etc.), and (4) state-of-the-art security research.

Prerequisites/Corequisites

CSE 422, Computer Networks

Textbook

Computer Security: Principles and Practice, Third Edition, by William Stallings and Lawrie Brown

Grading

- Attendance (5%)
- Homework (30%): Four assignments; only the highest three HW scores will be selected.
 - HW1: Release date: 1/31; Coverage: lectures given on 1/10, 1/12, 1/19, 1/24, 1/26, 1/31; and **Due:** 2/7.
 - HW2: Release date: 2/21; Coverage: lectures given on 2/2, 2/7, 2/9, 2/14, 2/16, 2/21; and **Due:** 2/27 (one day before exam; no late submission).

- HW3: Release date: 3/28; Coverage: lectures given on 3/2, 3/14, 3/16, 3/21, 3/23, 3/28; and **Due:** 4/4.
- HW4: Release date: 4/18; Coverage: lectures given on 3/30, 4/4, 4/6, 4/11, 4/13, 4/18; and **Due:** 4/24 (one day before exam; no late submission).
- Midterm exam on **2/28** by Zoom (30% using an error-correction-80 rule)
 - Covering lectures given from 1/10 to 2/21.
 - Corrected answers must be submitted to D2L by 11:59pm, 3/16.
- Final exam on **4/25** by Zoom (35% using an error-correction-80 rule)
 - Covering lectures given from 3/2 to 4/18.
 - Corrected answers must be submitted to D2L by 11:59pm, 5/6.
- Bonus (5%) You can choose to do a programming project or present a security paper by uploading a demo video or a 10-min paper presentation video to D2L (You can do it alone or team up with another student). **Due:** 4/29. Note that this is an optional bonus.
 - **Voice over Wi-Fi Security:** identify the W-Fi calling traffic of your phones and launch DoS attacks against your phones. References: [The Untold Secrets of Wi-Fi-Calling Services: Vulnerabilities, Attacks, and Countermeasures](#)
 - **Security Paper Presentation:** select a paper published in top four security conferences, namely IEEE S&P, ACM CCS, Usenix Security, and NDSS, from 2019 to 2021, read it, and make a 10-min paper presentation.

Late submissions of homework assignments will be penalized with a 50% point deduction. No work will be accepted later than 24 hours after the due date. Note that there are NO makeup exams unless you can show proof of a severe emergency (e.g., admission to an emergency room).

Grading Policy

4.0: 90%-100% of points available
3.5: 85%-89.99% of points available
3.0: 80%-84.99% of points available
2.5: 75%-79.99% of points available
2.0: 70%-74.99% of points available
1.5: 65%-69.99% of points available
1.0: 60%-64.99% of points available

Collaboration and Cheating

Any student caught cheating will receive a grade of 0.0 for this course.

Tentative Schedule (subject to change)

Class	Day	Topics
1	10. January	Overview
2	12. January	Overview
3	17. January	Holiday (no class)
4	19. January	Cryptographic tools
5	24. January	Cryptographic tools
6	26. January	User authentication
7	31. January	Access control
8	2. February	Denial-of-service attacks
9	7. February	Malicious software
10	9. February	Database and cloud security
11	14. February	Intrusion detection
12	16. February	Firewall and intrusion prevention systems
13	21. February	Buffer overflow
14	23. February	Pre-exam review
15	28. February	Midterm exam
16	2. March	Discuss answers and Software security
17	7. March	Spring break
18	9. March	Spring break
19	14. March	Operating system security
20	16. March	Internet Authentication Applications
21	21. March	Public-Key cryptography and message authentication
22	23. March	Symmetric encryption and message confidentiality
23	28. March	Wireless network security (WiFi)
24	30. March	Cellular network security (4G LTE and 5G NR)
25	4. April	Cellular network voice service security
26	6. April	Cellular network data and text service Security
27	11. April	Wireless IoT security (WiFi & Cellular)
28	13. April	Wireless IoT security (WiFi & Cellular)
29	18. April	Wireless IoT security (WiFi & Cellular)
30	20. April	Pre-exam review
31	25. April	Final exam
32	27. April	Discuss answers to the final exam