Syllabus and Course Overview

University of Illinois

ECE 422/CS 461

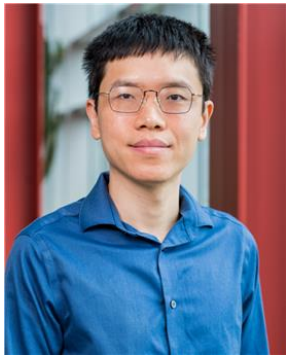
Computer Security I

Agenda for Today

- Course information: instructional team, logistics, syllabus, grading, policy, resources
- Academic integrity
- Ethics and laws

Instructional Team

- Instructor: Ling Ren and Adam Bates



- Teaching assistants: Tzu-Bin Yan, Ryan Ziegler, Tianyang Zhou, Jacob Stolker
- Course assistants: TBA

Fully in-person this semester

- After carefully weighing the pros and cons, lectures and discussions are in-person only
  - Slides will be uploaded shortly after each lecture
  - Recordings only provided before exams (if at all)

- Prof. Bates is piloting a fully online version of CS 461 / ECE 422 for *graduate* students. Contact batesa@illinois.edu to sign up.

Course Description

This course teaches fundamental principles of computer and communication security: notions of threats, vulnerabilities, risks, confidentiality, integrity, and availability; software security, web security, database security, OS security, network security; security mechanisms such as access control, authentication, auditing, cryptography, and security protocols.

Course Description

- Common attacks and defenses in software, systems, networks, web, databases, …
- Advanced security topics: cryptography, auditing, malware, anonymity, …
- Become security-aware and capable of evaluating risks and developing security solutions across CS domains

Prerequisites

- Systems programming: CS 341, ECE 391, or a comparable course from another university
  - Proficiency in assembly programming is required
  - Basic knowledge in web, database, and network helps, but not required
- Willingness to conduct independent inquiry to solve hard challenges!
- Ability to pick up new programming languages quickly

Class Components

- Lectures: cover security concepts, common attacks and defenses in various systems (breadth)
- MPs: programming projects that delve into a small number of systems (depth)
- Discussion sections: provide necessary background and guidance on MPs
- Weekly quizzes: short and easy
- Midterm and final: test your mastery of lecture, discussion, and MP contents

Lectures and Discussions

- Lectures: Tuesday / Thursday 12:30pm – 1:45pm, 1404 Siebel Center for Comp Sci
- Discussion sections: Wednesday 1pm, 2pm, 3pm, 4pm, 2406 Siebel Center for Comp Sci
  - Not every week, first discussion next week

- Lectures and discussions are in-person only
- Attendance is **strongly** encouraged

Grading

- 40% Machine Problems (MPs)
- 10% Weekly Quizzes
- 20% Midterm Exam (in class, Mar. 13)
- 30% Final Exam (during Finals Week)

Quizzes and Exams

- Quizzes
  - 4~5 easy questions on Canvas
  - Weekly, out every Thursday, due next Friday
    - 1st deadline: Jan. 31 (for week 1 contents)
- Midterm and Final Exams
  - In-person, open book, no digital device

Machine Problems

- Test your technical ability to investigate and solve real-world security problems

- You can use your own laptop or a remote machine we provide
  - If your have Apple silicon, you will have to use our provided remote machine

Machine Problems

- MP1: Application (Software) Security
  - Students perform buffer overflow and control flow hijacking attacks. Require familiarity with assembly, basic x86_32 architecture, and debugging in gdb.

- MP2: Web Security
  - Students perform SQL injection, XSS, CSRF attacks, and will develop a rudimentary knowledge in HTML, Javascript, and one variant of SQL.

Machine Problems

- MP3: Cryptography
  - Students will gain a basic understanding of public-key cryptography, symmetric cryptography, and cryptographic hash functions using Python.
- MP4: Network Security
  - Students will gain familiarity with basic network protocols (IP, TCP, UDP, ICMP, ARP), network utilities (ping, traceroute, wireshark) as well as socket programming in C and C++.

Machine Problems

- Each MP is divided into 2 checkpoints
  - cp1 is easy and due in 1 week
  - cp2 is **challenging** and due in 1.5 weeks
  - Start cp2 early!

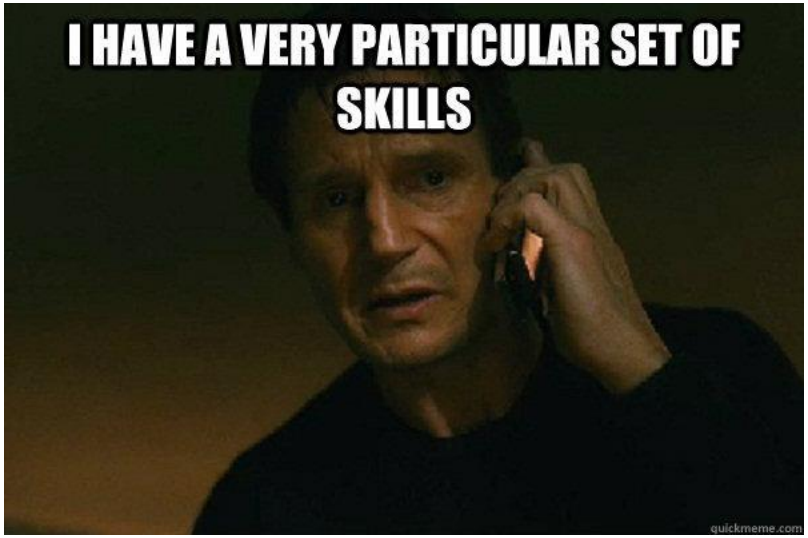
- 24-hour automatic extension for CP2
- No penalty and no help during this 24 hours
- No more extension will be granted

Workload

- You may have noticed that this will be a challenging class
  - Each MP requires 20+ hours of work (somewhat easier than ECE 391, comparable to CS 241).
  - Exams will expect mastery of course content, may require many hours of studying.
  - Getting an A would not be easy

What's in it for you?

- Understand root causes of computer (in)security
- Learn how to apply security concepts, mindset, and methodologies to various computer systems
- Acquire a very particular (and lucrative) set of skills
- Have fun!



What to do if you need help

- Confused about a lecture topic?
  - Visit professor office hours (10-11 Thursday, Siebel 4312)
  - Post a question on Piazza
- Stuck on an MP?
  - Attend discussion sections
  - Visit TA office hours (9:30-11:30 Mon, 3-5 Tue, 4-6 Wed, Siebel 0th floor, starting next week)
  - Post a question on Piazza
- Struggling for any other reason?
  - Reach out to anyone on the instructional team and we will connect you with the right person to help

Statement on Mental Health

Diminished mental health, including significant stress, mood changes, excessive worry, substance/alcohol abuse, or problems with eating and/or sleeping can interfere with optimal academic performance, social development, and emotional wellbeing. The University of Illinois offers a variety of confidential services including individual and group counseling, crisis intervention, psychiatric services, and specialized screenings at no additional cost. If you or someone you know experiences any of the above mental health concerns above, it is strongly encouraged to contact or visit any of the University's resources provided below. **Getting help is a smart and courageous thing to do** -- for yourself and for those who care about you.

- Counseling Center: 217-333-3704, 610 E John Street Champaign, IL 61820
- McKinley Health Center:217-333-2700, 1109 South Lincoln Avenue, Urbana, Illinois 61801

Disability-Related Accommodations

To obtain disability-related academic adjustments and/or auxiliary aids, students with disabilities must contact the course instructor and the as soon as possible. To insure that disability-related concerns are properly addressed from the beginning, students with disabilities who require assistance to participate in this class should contact Disability Resources and Educational Services (DRES) and see the instructor as soon as possible. If you need accommodations for any sort of disability, please speak to me after class, or make an appointment to see me, or see me during my office hours. DRES provides students with academic accommodations, access, and support services. To contact DRES you may visit 1207 S. Oak St., Champaign, call 333-4603 (V/TDD), or e-mail a message to disability@uiuc.edu. http://www.disability.illinois.edu/.

Statement on Code of Conduct

All members of the Illinois Computer Science department -- faculty, staff, and students -- are expected to adhere to the CS Values and Code of Conduct

https://cs.illinois.edu/about/values

The CS CARES Committee is available to serve as a resource to help people who are concerned about or experience a potential violation of the Code. If you experience such issues, please contact the CS CARES Committee. The instructors of this course are also available for issues related to this class.

https://cs.illinois.edu/about/cs-cares/contact

Academic Integrity Policy

The University of Illinois at Urbana-Champaign Student Code should also be considered as a part of this syllabus. Students should pay particular attention to Article 1, Part 4: Academic Integrity. Read the Code at the following URL:

http://studentcode.illinois.edu/

Ignorance is not an excuse for any academic dishonesty. It is your responsibility to read this policy to avoid any misunderstanding. Do not hesitate to ask the instructor(s) if you are ever in doubt about what constitutes plagiarism, cheating, or any other breach of academic integrity.

Academic Integrity Policy

What violates academic integrity?

- **Cheating** – using or attempting to use unauthorized materials
- **Plagiarism** – representing the words, work, or ideas of another as your own
- **Facilitating Infractions of Academic Integrity** – helping or attempting to help another commit an infraction
- **Bribes, Favors, and Threats** – actions intended to affect a grade or evaluation
- **Academic Interference** – tampering, altering or destroying educational material or depriving someone else of access to that material

https://provost.illinois.edu/policies/policies/academic-integrity/students-quick-reference-guide-to-academic-integrity/

Academic Integrity Policy

- Discussion of general method is encouraged, but you **MUST write your own solution**
- We **will** scrutinize all exams, quizzes, and MP submissions for evidence of violations.

- We have **highly effective automated tools** to detect **plagiarism**.
  - Copying from current or past students **will** be caught,
  - … even if you make "cosmetic" changes to coding styles and variable names
  - Use of Large Language Model (LLM, e.g., ChatGPT) will likely be detected as plagiarism

Academic Integrity Policy

- The standard sanction is a **“zero”** on the assignment and a **full letter down** in the final grade.

- Cheating is the **most reliable way to fail** the class
  - 21 students caught cheating in the last two offerings
  - 11 of them failed (after sanctions)
  - 3 students failed without cheating

- All cases of academic integrity violations will be **reported** to the Provost’s office.

Ethics Statement

This course will include topics related computer security and privacy. As part of this investigation, we will cover **technologies whose abuse could infringe on the rights of others**. As computer scientists, we rely on the ethical use of these technologies. Unethical use includes circumvention of existing security or privacy mechanisms for any purpose, or the dissemination, promotion, or exploitation of vulnerabilities of these services. Any activity outside the letter or spirit of these guidelines **will be reported to the proper authorities** and may result in dismissal from the class and **possibly more severe academic and legal sanctions.**

When in doubt, contact the instructors for advice. **Do NOT** undertake any action which could be perceived as technology misuse anywhere and/or under any circumstances.

Unique to this Course …

- We will cover technologies whose abuse could infringe on the right of others:
  - Common flaws and vulnerabilities in computer systems
  - Common attacks and exploits

- In this class, you will NOT be asked to do anything illegal or unethical, or to attack any real systems
  - The MPs ask you to attack dummy systems created by the course staff

But Oh, the temptations!

- To try what you learned
- To show off your hacking skills
- Genuinely want to help expose problems

Don’t be this girl/guy

- A Pennsylvania high school student launched a Distributed Denial of Service (DDoS) attack on her school district’s computers
- “It was to play a **prank** on her school”
- She **pleaded guilty to two felony counts** of unlawful use of computers and would server **two years of probation**

https://triblive.com/local/westmoreland/former-franklin-regional-student-to-serve-probation-for-cyber-attack-that-crippled-school-county-computers/

Don’t be this girl/guy

- An Arizona teenager exploited a bug in iOS that made a user’s iPhone, upon opening a link he created, dial 911 repeatedly
- The attack nearly crashed a 911 call center
- He told police he was **bug hunting** and **pranking** his friends
- He was charged with **four felony accounts** and was sentenced to **three years of probation**

https://www.bleepingcomputer.com/news/security/teen-sentenced-for-prank-that-almost-brought-down-a-countys-911-service/

Don’t be this girl/guy

- A University of Iowa student used a keylogger to steal professors’ passwords, with which he stole exams and changed his grades >90 times

- He was sentenced to **four months in federal prison** and **$67,900 restitution**

https://www.thegazette.com/education/former-ui-student-sentenced-to-4-months-in-federal-prison-for-changing-grades-copying-exams/

Relevant Technology Laws

I am not a lawyer

- Computer Fraud and Abuse Act (CFAA)
  - 18 U.S.C. § 1030
- Electronic Communications Privacy Act (ECPA)

- Under these laws, hacking into a protected computer is a federal crime
  - Basically, any computer is a protected computer

Offense	Penalties (Prison Sentence)
Obtaining National Security Information	First conviction: Up to 10 years Second conviction: Up to 20 years
Accessing a Computer to Defraud and Obtain Value	First conviction: Up to five years Second conviction: Up to 10 years
Accessing a Computer and Obtaining Information	First conviction: Up to one year Second conviction: Up to 10 years
Intentionally Damaging by Knowing Transmission	First conviction: Up to 10 years Second conviction: Up to 20 years
Extortion Involving Computers	First conviction: Up to five years Second conviction: Up to 10 years
Trafficking in Passwords	First conviction: Up to one year Second conviction: Up to 10 years

https://www.findlaw.com/criminal/criminal-charges/hacking-laws-and-punishments.html

Relevant Technology Laws

I am not a lawyer

- State and Local Laws
  - Illinois 720 ILCS § 5/17-50 to -55 (e.g., computer fraud, computer tampering)

- Computers and networks may carry data for hospitals, universities, and K-12 organization
  - Family Educational Right to Privacy Act (FERPA)
  - Federal Standards for Privacy of Individually Identifiable Health Information

Contracts and Policies

I am not a lawyer

- End User License Agreements (EULA)
  - Do not criticize this product publicly
  - Do not reverse-engineer this product

  ❑ I accept the terms in the license agreement

- Organization policies
  - E.g., Policy on Appropriate Use of Computers and Network Systems at the University of Illinois

Ethics Standards

- IEEE Code of Ethics
  - commits members “to the highest ethical and professional conduct”: avoid conflicts of interest, be honest, make responsible decisions, etc..
- ACM Code of Ethics and Professional conduct
  - “contribute to society and human well-being”, “avoid harm to others”, “respect privacy”, etc..

As Computer Security Practitioners

- All systems have bugs:
  - A bug is an error or flaw in a computer program or system that causes it to produce an incorrect or unexpected result, or to behave in unintended ways
  - Some bugs lead to security problems (vulnerability)

- What should you do when you find a bug / vulnerability?

Responsible Disclosure

- **Latent Flaw**. A flaw is introduced into a product during its design, specification, development, installation, or default configuration.
- **Discovery**. One or more individuals or organizations discover the flaw through casual evaluation, by accident, or as a result of focused analysis and testing.
- **Notification**. A reporter or coordinator notifies the vendor of the vulnerability ("Initial Notification"). In turn, the vendor provides the reporter or coordinator with assurances that the notification was received ("Vendor Receipt").
- **Validation**. The vendor or other parties verify and validate the reporter's claims ("Reproduction").
- **Resolution**. The vendor and other parties also try to identify where the flaw resides ("Diagnosis"). The vendor develops a patch or workaround that eliminates or reduces the risk of the vulnerability ("Fix Development"). The patch is then tested by other parties (such as reporter or coordinator) to ensure that the flaw has been corrected ("Patch Testing").
- **Release**. The vendor, coordinator, and/or reporter release the information about the vulnerability, along with its resolution.
- **Follow-up**. The vendor, customer, coordinator, reporter, or security community may conduct additional analysis of the vulnerability or the quality of its resolution.

As Computer Security Practitioners

- What should you do when you find a bug?
  - Responsible Disclosure
  - If it is for University of Illinois systems and networks, report to the cybersecurity team security@illinois.edu
- What if a company refuses to fix the problem?
  - If repeated attempts at responsible disclosure have failed, one can consider *full public disclosure*.
  - There may be moral and legal consequences; don't hesitate to talk to the instructor(s)

Summary

- This is challenging and fun class
  - Teaches common security flaws and mechanisms, security principles and mindset
  - In-person only, attendance strongly recommended
  - Start MPs (cp2) early

- Do NOT cheat
- Do NOT break any law
- Ethical behaviors and responsible disclosure

Class Resources

- Course website:
  - https://courses.engr.illinois.edu/cs461/sp2025/
- Piazza for Q/A:
  - https://piazza.com/illinois/spring2025/cs461ece422/
- Canvas for quizzes, slides, and handouts
  - https://canvas.illinois.edu/courses/53548/
- Contact:
  - ece422-staff@illinois.edu

Suggested Reading

There are a lot of great textbooks that will supplement what we cover in lectures.

- *Security Engineering* by Ross Anderson
  (it's free! https://www.cl.cam.ac.uk/~rja14/book.html)
- *Cryptography Engineering* by Ferguson, Schneier, and Kohno
- *Introduction to Computer Security* by Matt Bishop
- *Computer Security: Principles and Practice* by William Stallings
- *Computer Security: Art and Science* by Matt Bishop
- *Security in Computing* by Charles P. Pfleeger
- *Introduction to Computer Security* by Michael Goodrich and Roberto Tamassia