

CSci 4271W
Development of Secure Software Systems
Day 1: Introduction and logistics

Stephen McCamant (he/him/his)
University of Minnesota, Computer Science & Engineering

Outline

- COVID-19-related Logistics
- Big-Picture Introduction
- Discussion Group Greetings
- Course Logistics

Masks required

- You should be wearing a mask, cloth face covering, etc., covering your nose and mouth
 - So, don't plan on eating breakfast in class

Vaccination

- Getting a vaccine is the single most important thing you can do to reduce your risk of serious illness from COVID-19
 - And reduces risk of spreading to others, too
- I request that you cooperate promptly with the U's COVID-19 vaccine requirement
 - Though I am not otherwise involved

Other things you can do

- Be more careful than usual to stay home if you're sick
- Sit in a consistent place in the classroom
- Exchange contact info with the students near you, or install a contact-tracing app on your phone

Exams are still in person

- There will be two midterm exams planned in-person, in this room
- The idea is that this will be after the spike

Planning for medical absences

- Especially during this spike, aware more students will have reason not to come in person
 - If you have been exposed to or infected with COVID
 - If you have fever, cold, or flu-like symptoms anyway
 - If you don't feel safe coming to class amid all-time-high infection rates

Medical absences, cont'd

- Taking steps to accommodate non-in-person students
 - Don't want to disadvantage you in terms of grades and assignments
 - But the experience may not be as good, e.g. missing discussion opportunities
- E.g., attempting to record audio of today's lecture

Be prepared for change

- I'm optimistic the pandemic will improve before the end of the semester
- If it gets too much worse, we may shift to all-online
 - Likely based on campus-wide decisions, or temporarily if I get sick
 - If we switch to Zoom, links will on the course Canvas page

Outline

- COVID-19-related Logistics
- Big-Picture Introduction
- Discussion Group Greetings
- Course Logistics

What is computer security?

- Keep "bad things" from happening
- Distinguished by presence of an **adversary**

Two sides of security

- Defenders / white-hats / good guys[sic]
- Attackers / black-hats / bad guys[sic]
- Each side's strategy depends on the other
- In some ways like a game

Common security threats

- Spoofing
- Tampering
- Repudiation
- Information disclosure
- Denial of service
- Elevation of privilege

Threat modeling

- What are the relevant parts of your system?
- What threats are possible?
- How can you stop the threats?

Course areas

- Low-level software security
- OS interaction security
- Web software security
- Using cryptography
- User identities and usability

Outline

- COVID-19-related Logistics
- Big-Picture Introduction
- Discussion Group Greetings
- Course Logistics

Say hello to your neighbors

- From time to time I'll ask you to discussions or exercises in groups with people sitting near you
- For today, just introduce yourself to the folks sitting nearby

Outline

- COVID-19-related Logistics
- Big-Picture Introduction
- Discussion Group Greetings
- Course Logistics

Instructor information

- Stephen McCamant
- Office: 4-225E Keller (at least some days)
- Office hours: TBA
- Email: mccamant@cs.umn.edu

Teaching assistants

- Aditya Pakki, Alex Backman
- Office hours: TBA

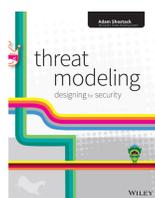
Prerequisites

- Software design and development (3081)
- C, machine code, and compilation
 - E.g. 2021, transitive for 3081

Reading materials

- Posted on the course web site
- Download, perhaps with library proxy
- Chosen to complement lecture discussions
- Comprehension questions on Canvas

Optional book 1



Provides more detail on threat modeling, but no assigned readings

Optional book 2



Source for several readings, but chapters are free online

Evaluation components

- 10% Lab participation
- 6% Online lecture/reading Qs (best scores)
- 10% Problem sets
- 14% Two in-class midterms
- 60% Projects

Online lecture/reading questions

- Auto-graded questions to check your understanding
- Due within a week from the material posting
- Can repeat to improve your score

Problem sets

- 2-3 sets, roughly by topic areas
- Done individually
- Mostly thinking and writing, not much programming
- Submit in PDF online
- 75% technical correctness, 25% writing

Midterm exams

- Two in-class exams, in February and April
- Open-book, open-notes, but no electronics
- No final exam

Projects

- Single most important and time-consuming part of course
- Each may cover:
 - Modeling possible threats against a system
 - Finding bugs and testing attacks
 - 4-5 page writeup of your results, with revision
 - Fixing the bugs
- Mostly individual, 50% of grade is writing

Three projects

- Proj 1: memory safety vulnerabilities
- Proj 2: OS interaction vulnerabilities
- Proj 3: design project, no implementation

Writing intensive

- A major focus is effectively communicating about security
- Writing techniques will be a periodic topic in lectures
- Lots of feedback (and grading) about writing assignments
 - Projects 1 and 3 include revision in response to feedback

Late assignments

- Problem sets: half credit for up to 48 hours late
- Projects: may request an extension (from Friday night to Monday night) for one project submission

Collaboration

- Be careful about bugs: "no spoilers"
- OK to discuss general concepts
- OK to help with side tech issues
- Sharing code or written answers is never OK

External sources

- Many assignments will allow or recommend outside (library, Internet) sources
- But you must appropriately acknowledge any outside sources you use
- Failure to do so is **plagiarism**

Security ethics

- Don't use techniques discussed in class to attack the security of other people's computers!
- If we find you do, **you will fail**, along with other applicable penalties

Academic misconduct generally

- Don't cheat, plagiarize, help others cheat, etc.
- Minimum penalty: 0 on assignment, report to OCS
- More serious: F in course, other OCS penalties

Course web site

- Department web site will be under `csci4271`
- Also linked from my home page `~mccamant`

On Canvas

- Recorded lectures
- Online lecture/reading questions
- Assignment submissions (or Gradescope?)
- Viewing grades
- Zoom links (if needed)

Mostly Piazza

- Online Q&A
 - Can be anonymous and/or private
 - Both students and staff can answer
- Course announcements
 - Can control delivery preferences, defaults to email
- Reserve email for personal, administrative issues

In-person lecture/discussions

- TuTh 9:45-11am in 43 Rapson
- Mixture of lecture and discussions
 - Come prepared to participate
- Lecture slides posted, attempting recordings

Synchronous lab sections

- Hands-on and collaborative practice with code and tools
- Graded on participation, meaning:
 - Be present and working on 4271 material
 - If you have a question, that interaction counts
 - No questions? Show off your progress

In-person vs. online labs

- 1-262 Keller Hall reserved for Monday labs
- Interested in your thoughts now: pros and cons of labs in-person versus over Zoom?

4271 vs. 5271

- Designed so you can take either or both
 - 5271 easier but still worthwhile after 4271
- 4271 has more of: threat modeling, software engineering, writing support
- 5271 has more of: research perspectives, novel/difficult attacks