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

Stephen McCamant (he/him/his)

University of Minnesota, Computer Science & Engineering

Outline

Big-Picture Introduction

Breakout-group Introductions

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

Big-Picture Introduction

Breakout-group Introductions

Course Logistics

Say hello to your random group

- Rename for how you'd like others to refer to you
- Video appreciated if possible
- Ice-breaker question: where are you looking forward to traveling, once it's safe to travel again?
- Bowen and I will circulate separately

Outline

Big-Picture Introduction

Breakout-group Introductions

Course Logistics

Instructor information

- Stephen McCamant
- Office: 4-225E Keller (but I'm not there)
- Office hours: Mondays 1-2pm, via Zoom
- Email: `mccamant@cs.umn.edu`

Teaching assistant

- Bowen Wang
- Office hours: TBA, via Zoom

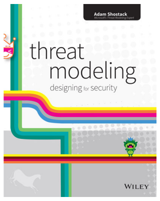
Prerequisites

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

Reading materials

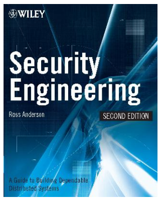
- Posted on the course web site
- Download, perhaps with library proxy
- Chosen to complement lecture discussions
- Comprehension questions on Canvas

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
5%	Lecture/discussion attendance
5%	Online lecture/reading Qs (best scores)
20%	Problem sets
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

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

Exams?

- No exams this semester
  - Hard to do well remotely
- Also no assignments during final exam period

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 lecture section
- 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

- Zoom links (how you got here, I hope)
- Recorded lectures
- Online lecture/reading questions
- Assignment submissions
- Viewing grades

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

Asynchronous online lectures

- Motivation: some topics benefit from discussion, others from being able to rewind
- Pre-recording of me talking with slides, sometimes demos
- Like readings, more in-depth but non-interactive
- Watch and answer online questions within one week
- On Canvas/Kaltura with hand-checked subtitles, downloadable

Synchronous lecture/discussions

- Always online via Zoom, TuTh 9:45-11am
- Mixture of lecture and discussions
  - Come prepared to participate
- Lecture slides posted, recordings on Canvas

Synchronous lab sections

- Hands-on and collaborative practice with code and tools
- Online, may later be available in person
- 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

Online labs

- At least first 2 weeks are all online, starting next Monday
- Hosted by Bowen, I may also sometimes attend
- Online labs will always be available

Socially-distanced in-person labs

- 1-262 Keller Hall reserved with a reduced capacity layout
- Starting no earlier than 2/8
  - Depending on demand and local COVID status
- Will be offered only at the 003 section time

In-person lab safety

- Mask wearing and 6-foot distancing required
- No professional cleaning between sections, do-it-yourself wipes
- No plexiglass, screen sharing still needs to be electronic
- I'll offer it when I think the risk to me is acceptable; you need to make your own decision

First lab

- No security content, just practice with online collaboration
  - In random small groups
- Vole and SSH access to CSE Labs (review)
- Read-only screen sharing via Zoom
- Interactive terminal sharing via `tmate`
- Off-campus access to library materials

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