Computer Science 161: Computer Security

Website: https://cs161.org

Peyrin Kao

Ryan Lehmkuhl
If you are here: you’ve finished your first 161 assignment!

- Log into Gradescope (https://www.gradescope.com/)
- Open the **Homework 1** assignment
- Find **Q2.3**
- Enter the password: **botnet**
- Do not share the password with your friends!
Who Am I:
Ryan Lehmkuhl (he/him)

- From San Diego!!
- EECS Senior
- Taught CS 161 twice
- Research interests: Cryptography/Complexity Theory (systems + zero-knowledge proofs)
- Slightly unhealthy relationship with coffee
- In a weird singing group
Who Am I: 
Peyrin Kao (he/him)

- From: Diamond Bar (LA area)
- CS Senior
- Taught CS 161 twice
- I sometimes research: human-AI interactions
- A funny thing that happened to me recently: was arrested for breaking curfew
- I speak: Chinese (fluent), Japanese (very poor)
And a team of talented TAs...

Albert Tang
he/him

Ben Hoberman
he/him

Nicholas Ngai
he/him

Shivam Shorewala
he/him

Shormil Jain
he/him

Vron Vance
they/them
And a team of talented TAs...
Nicholas Ngai (he/him)

- From San Jose (well, close enough)
- EECS sophomore
- Took CS 161 in Spring 2020 (and definitely over-engineered Project 2)
- Far too interested in cryptography
- Far too paranoid about privacy
And a team of talented TAs...
Vron Vance (they/them)

- from san carlos and san diego
- comp sci senior
- academic interests: accessibility, safety, security in computer science
- personal interests: cats, turtles, succulents
...and readers...

Caroline Liu  
she/her

Evan Sun  
he/him

Arvind Sridhar  
he/him

Sid Bansal  
he/him
...and professors

David Wagner

- Worked on software security, mobile security, cryptography, security of electronic voting, usable security, system security
- Currently excited about security for machine learning
...and professors
Raluca Ada Popa

- Lead the system security research group, and co-run RISELab at UC Berkeley
- Research topics: **broadly** systems security and applied cryptography, and **more specifically**: secure analytics, databases, IoT and ML; decentralized security via blockchains/ledgers
- CTO & co-founder of a cybersecurity company, PreVeil
- Taught this class 3 times
What Will You Learn In This Class?

• How to think adversarially about computer systems
• How to assess threats for their significance
• How to build programs & systems with robust security properties
• How to gauge the protections and limitations provided by today’s technology
• How attacks work in practice
Prerequisites

- CS 61B (Data Structures)
- For experience working with large codebases (500-1000 lines of code) and basic data structures
- Relevant for Project 2 (weeks 4-6)
Prerequisites

- CS 61C (Machine Structures)
- For understanding of C memory layout and hex/binary number representation
- Relevant for the memory safety unit (Project 1, weeks 1-2)
- See optional review lecture if you want a refresher
Prerequisites

- CS 70 (Discrete Math and Probability Theory)
- For basic understanding of modular arithmetic/set notation and some mathematical intuition
- Relevant in the cryptography unit (weeks 2-3)
- We’ll do our best to review any CS 70 prerequisite material during lecture
Prerequisites

- Q: Do I need to already know a coding language?
- A: Basic understanding of C and Python is recommended
- Project 2 (500-1000 lines of code) is in Go
- You don’t need to know Go as a prerequisite, but you should be able to learn a new language on your own (we won’t have lectures on Go syntax)
Engage!

- In office hours, section, etc.
- Feedback is highly valuable: https://cs161.org/feedback
- Participate in Piazza (use same name as Gradescope)
- For private matters, contact instructors using private Piazza posts
Course structure

- Intro to Security
- Memory Safety
- Cryptography
- Network Security
- Web Security
- Miscellaneous Topics
Course structure

- Lectures
- Discussions
- Office hours
- Exams
Lecture

- Lectures will be pre-recorded and split into small chunks with short questions to check your understanding
- Will reuse many lectures from Spring 2020 (Raluca Popa and David Wagner)
- A few lectures will be live (will be recorded as well)
Live lecture time

- Lecture time is 5pm-6pm PT
- Any interactive live lectures will be at this time
- When there’s no live lecture, Ryan and/or Peyrin will be around to answer any questions
- May also be used as extra office hours during project weeks
Discussion

- Discussions will start Wednesday, June 24:
- Synchronous sections over Zoom (everyone attends a meeting at the scheduled time)
- LOST section (2 hours long)
- Discussion worksheet recording
Discussion schedule

- See the course website: https://cs161.org/calendar
- We tried to accommodate everyone’s time preferences: According to the form you filled out, everyone should have at least one discussion they can attend
- Possible minor change: the 7am section may be moved to 8am starting next week
Office hours

- Online queue at https://cs161.org/oh
- When it’s your turn, you will join a Zoom meeting with a TA
- We tried to accommodate everyone’s time preferences: According to the form you filled out, everyone should have at least one OH they can attend
- Extra office hours might be added during project weeks
If you are here: you’ve finished your first 161 assignment!

- Log into Gradescope (https://www.gradescope.com/)
- Open the **Homework 1** assignment
- Find **Q2.3**
- Enter the password: **botnet**
- Do not share the password with your friends!
Grading structure

- 3 projects (30%)
- 7 homeworks (20%)
- One midterm (20%)
- A comprehensive final exam (30%)
Class Policies

- Late homeworks are not accepted - You get one drop
- You have 3 project slip days
- Late project without slip days:
  - <24 hours: -10%, <48 hours: -20%,
  - <72 hours: -40%, >72 hours: no credit
- We will release a form for extenuating circumstances:
  https://cs161.org/accommodations
Midterms and Final Policy

- Midterm and Final are *synchronous* (everyone takes them at the same time)
- Midterm: July 13th (4pm-6pm PT)
- Final: August 13th (4pm-7pm PT)
- If you need DSP accommodations (extra time on exams, etc) process them ASAP
Midterms and Final Policy

Q: I can’t take the exam at the scheduled time.
A: If you absolutely can’t take the scheduled exam, we have one alternate time:

- Midterm: July 13th (8pm-10pm PT)
- Final: August 13th (7pm-10pm PT)

If you absolutely can’t make these times either, please message us on Piazza to discuss alternate exam times.

We might ask you to take a short verbal exam if you choose an alternate exam time.
Exam Proctoring

- Both exams will have video proctoring: as you take the exam, we should be able to see your computer screen and your paper answer sheet.
- Midterm: record a video that you upload after the exam
- Final: join a Zoom meeting during the exam
- If you don’t feel comfortable with video proctoring, please reach out to us and we will discuss alternatives (most likely an additional verbal exam).
Q: Is Zoom secure for exam proctoring?
A: More secure alternatives exist, but Zoom is what administration has authorized us to use (and paid for).
Online Resources & Accounts...

- Course website: [https://cs161.org](https://cs161.org)
- We will use **Gradescope** for HWs, projects, and exams
- Gradescope entry code: MZ6KZX
- We will use **Piazza** for class announcements
- We will use **Zoom** for sections, office hours, and exams
Intellectual Honesty Policy: Detection and Retribution

Nicholas Weaver
Intellectual Honesty Policy: Detection and *Retribution*

- We view those who would cheat as “attackers”
  - This includes sharing code on homework or projects, midterms, finals, etc…
- But through this class we (mostly) assume rational attackers
  - Benefit of attack > *Expected* cost of the attack
    - Cost of launching attack + cost of getting caught * probability of getting caught
- We take a detection and response approach
  - We use many tools to detect violations
    - "Obscurity is not security", but obscurity *can help.* Just let it be known that "We Have Ways"
  - We will go to DEFCON 1 (aka "launch the nukes") *immediately*
    - You will, *at minimum*, receive negative points
    - “Nick doesn’t make threats. *He keeps promises*”
Ethics Guide for Defense Against the Dark Arts

- Of necessity, this class has a fair amount of "dark arts" content
- As defenders you must understand the offense: You can't learn defense against the dark arts without including the dark arts
- But a lot of "don't try this at home" stuff

Big key is **consent**

- It's usually OK to break into your own stuff
  - It's a great way to evaluate systems
- It's usually OK to break into someone else's stuff with explicit permission to do so
- It is both grossly unethical and often exceedingly criminal to access systems without authorization
Stress Management & Mental Health...

- We'll try to not over-stress you too much
- But there really is a lot to cover
- If you feel overwhelmed, please use the resources available
  - Academically: Ask on Piazza, Office hours
  - Non-Academic: Take advantage of University Health Services if you need to

These are hard times. We as staff recognize that and want to do our best to accommodate all of you.