Comp 790-185: Research Topics in Computer Security

Introduction

August 19, 2024
Andrew Kwong

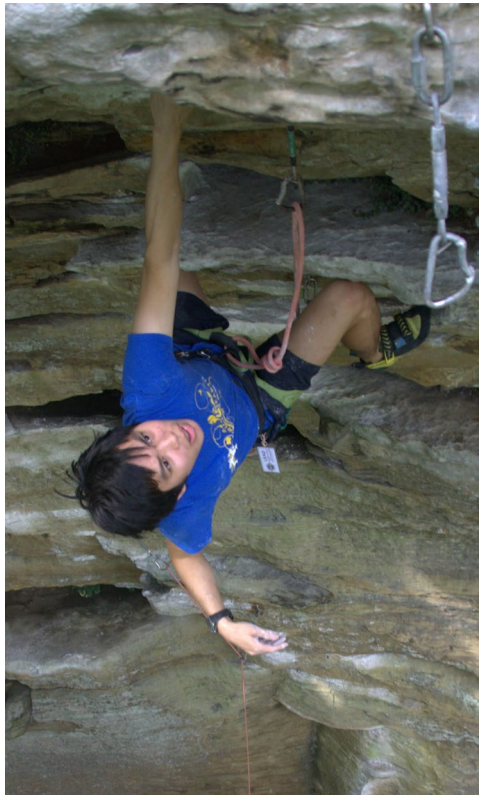
Slides adapted from Alex Halderman's EECS 588

Department of Computer Science

THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL

Today's Class

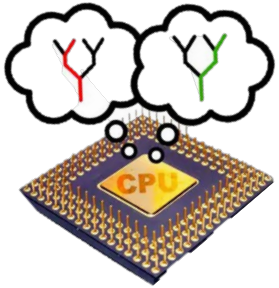
- Introductions
- Course Goals
- What is Security Research?
- Security Mindset
- Course Structure



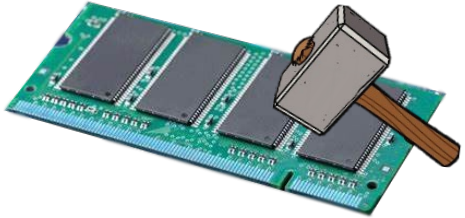
Who am I?

- Andrew Kwong
  - Assistant Professor

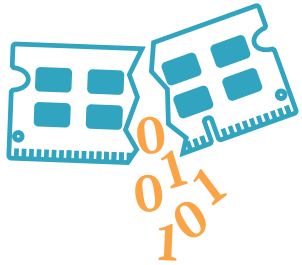
- Site: https://andrewkwong.org
- Email: andrew@cs.unc.edu
- Office: FB 340



CacheOut



Rowhammer



RAMBleed

My Research

- Hardware Security:
  - Memory
  - CPU
  - Applied-crypto
- Will talk more next class!

Course Goals

- Learn how to conduct security research
  - Broad overview of topics in computer security
    - Foundational works (e.g. Test of Time Award winning papers)
    - Recently Influential papers (Best paper awards)
  - Exposure to useful techniques

- Improve research, reading, writing, presentation skills
  - All are important!
- Develop a security mindset

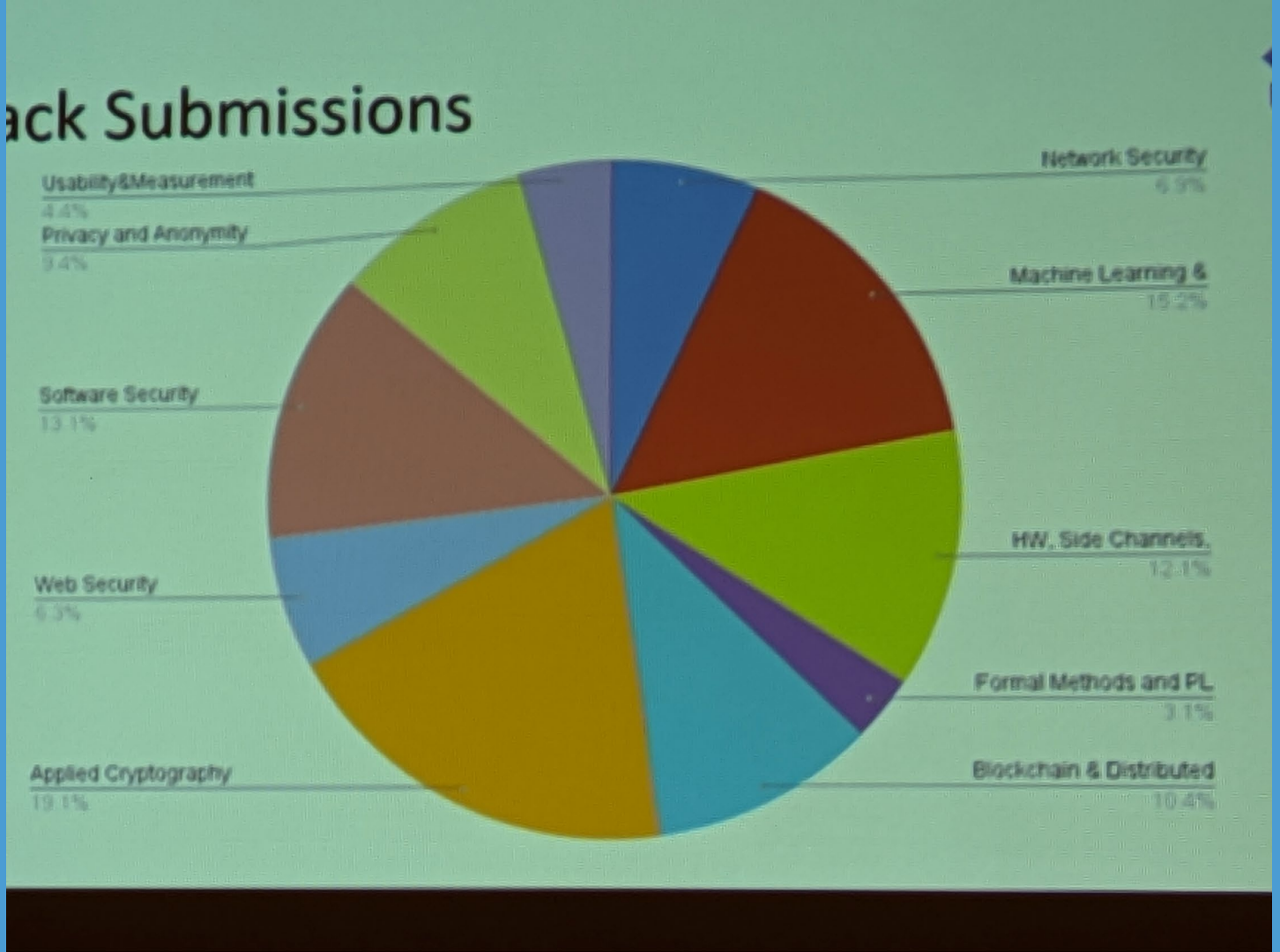
Who are you?

- Research Field
- Hobby/interesting fact
- Something you want to learn from this course.

What is Security Research?

- Pwning?
  - Scientific term for writing a binary exploit that gives the attacker root

ack Submissions

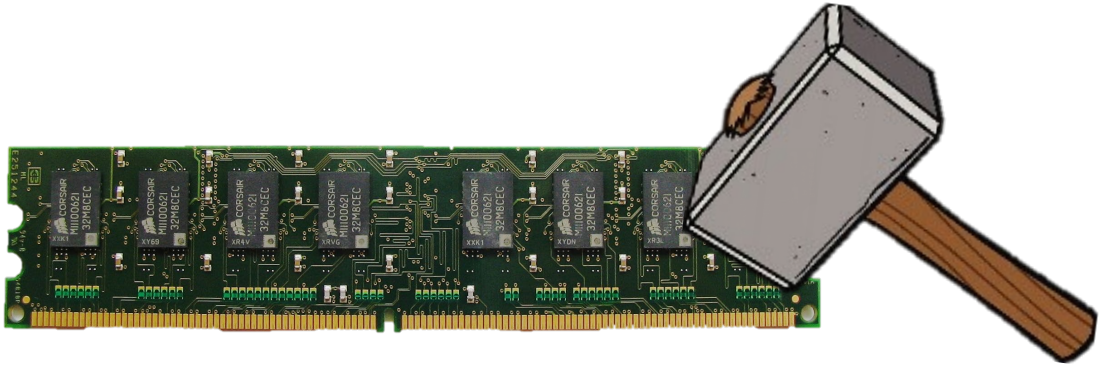


ack Acceptance Rates

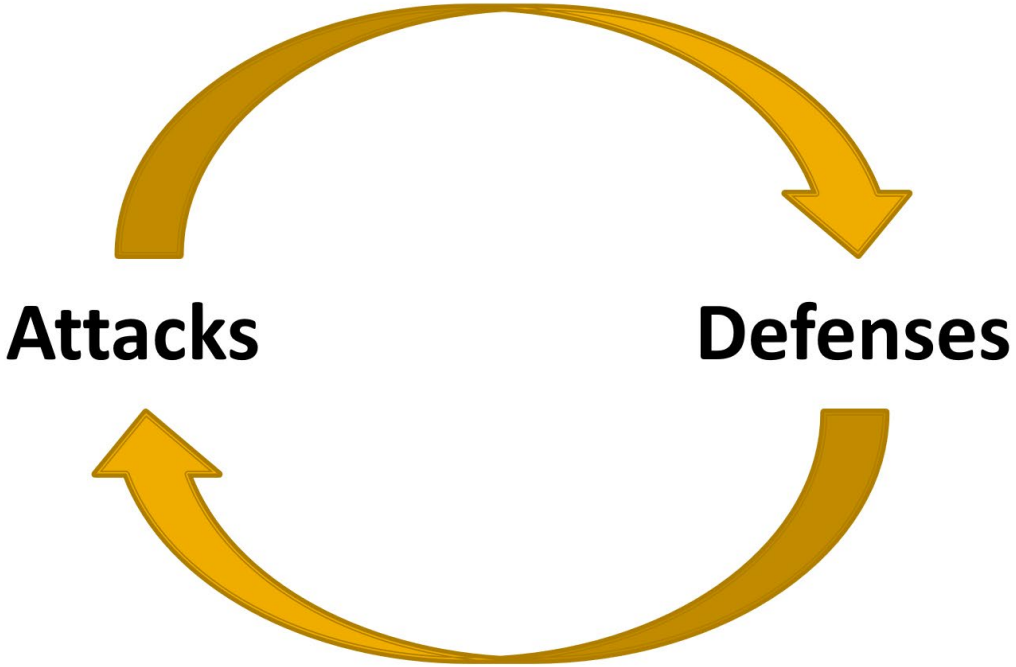
What is Security Research?

- Pwning?
  - Scientific term for writing a binary exploit that gives the attacker root
- “Computer security studies how systems behave in the presence of an adversary.”
- Adversary:
  - An intelligence that actively tries to cause the system to misbehave.

Adversarial Example



High Level Approach



Attack Research

- Identify vulnerabilities so they can be fixed.
- Create incentives for vendors to be careful.
- Learn about new classes of threats.
  - Determine what we need to defend against.
  - Help designers build stronger systems.
  - Help users more accurately evaluate risk.

More than just finding vulnerabiltiies!

- Generalizable lesson is learned
  - Used to build more effective defenses

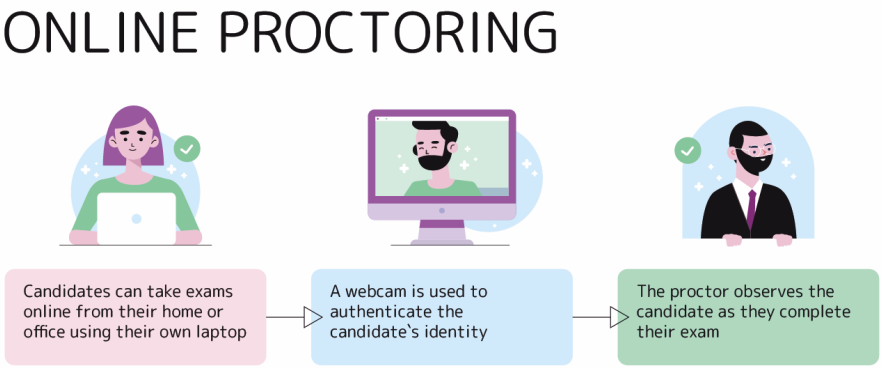
Thinking Like an Attacker

- Look for the weakest links – easiest to attack.
- Identify assumptions that security depends on. Are they false?
- Think outside the box: Not constrained by system designer's worldview.

Practice a Security Mindset:
For every system you interact with, think about what it means for it to be secure, and imagine how it could be exploited.

Exercises

- How to cheat in class?
- How to cheat out of class? (remote proctoring software)



Exercises

- How to steal my password?

Exercises

- How to steal library books?

Exercises

- What are some security systems that you interact with in everyday life?

Thinking Like a Defender

- Security policy
  - What are we trying to protect?
  - What properties are we trying to enforce?
- Threat model
  - Who are the attackers? Capabilities? Motivations?
  - What kind of attack are we trying to prevent?
- Risk assessment
  - What are the weaknesses of the system?
  - What will successful attacks cost us?
  - How likely?
- Countermeasures
  - Costs vs. benefits?
  - Technical vs. nontechnical

Election Security

What Not to do

- Common mistake:
  - Looking for evidence that your system is secure
- Security through obscurity
  - Fails historically!
- Kerckhoff's principle
  - Design of a system should not require secrecy

Course Structure

Grading

- Class Participation – 20%
- Paper Reviews – 20%
- Paper Presentations – 20%
- Course Project – 40%

Class Participation (20%)

- 2 paper readings each class
- Come prepared to contribute/ask questions
- Full points for speaking up and contributing substantial ideas

Paper Reviews(20%)

- 2 paper readings each class
- For each paper:
  - 2 strengths
  - 2 weaknesses
  - 1 question for discussion
- Submit on canvas

Paper Presentations (20%)

- Give conference style talk on assigned papers
- Can make or reuse/augment slides
- Roughly 20 minute presentation
  - High level advertisement for the paper
- Paper list found at https://andrewkwong.org/comp790-185.html
- Send me preferences (at least 5) by Thursday

Course Project (40%)

- Conduct original research on a topic related to computer security over the course of the semester.
- In class proposal/presentation 2nd week of October
- submit a final report (6-12 pages) at end of the course
- Give a conference style talk on results during the final week of class
- Working in groups is allowed, but a more substantial product is expected when working with more people

Your Assignments

- First paper discussion next Monday
- Rate preferences for paper presentations (Give me your top 5 at the very least)
- Start thinking about your course project
  - Proposals due second week of October

THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL

Content Slide Title 1

Content Slide Subtitle