Comp 790-184:
Research Topics in Computer Security

August 17, 2026

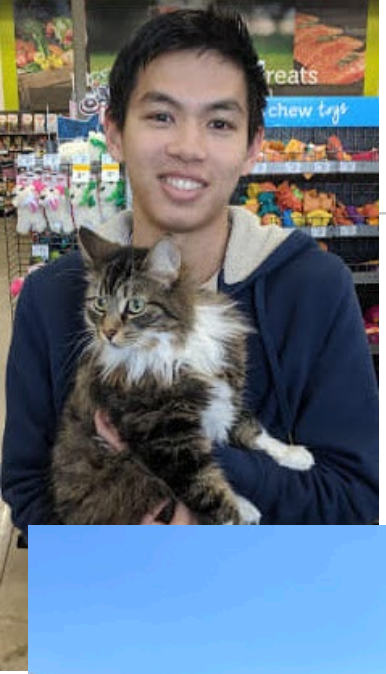
Andrew Kwong

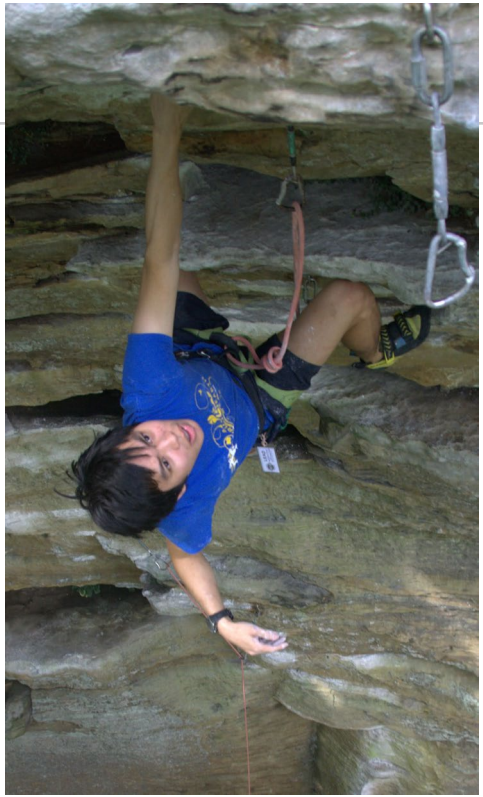
Department of Computer Science

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Today's Class

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

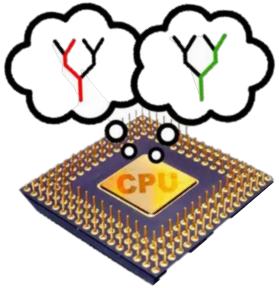




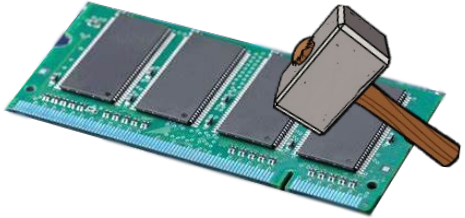
Who am I?

- Andrew Kwong
  - Assistant Professor

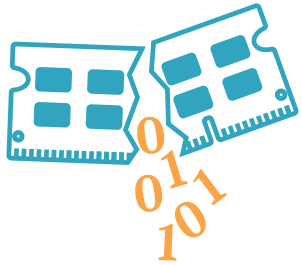
- Site: https://andrewkwong.org
- Email: andrew@cs.unc.edu
- Office: FB 340



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

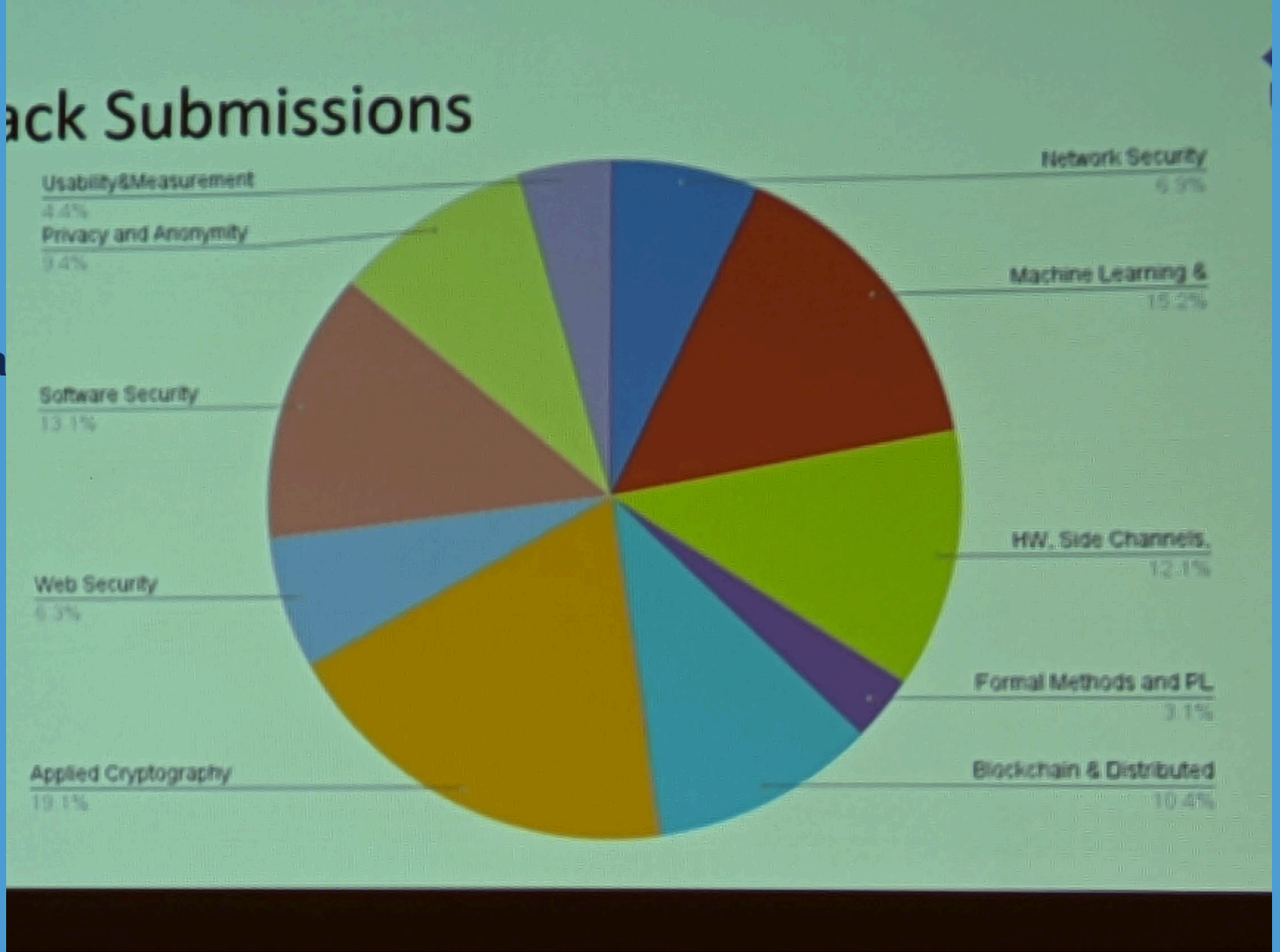
Who are you?

- 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

Presenta

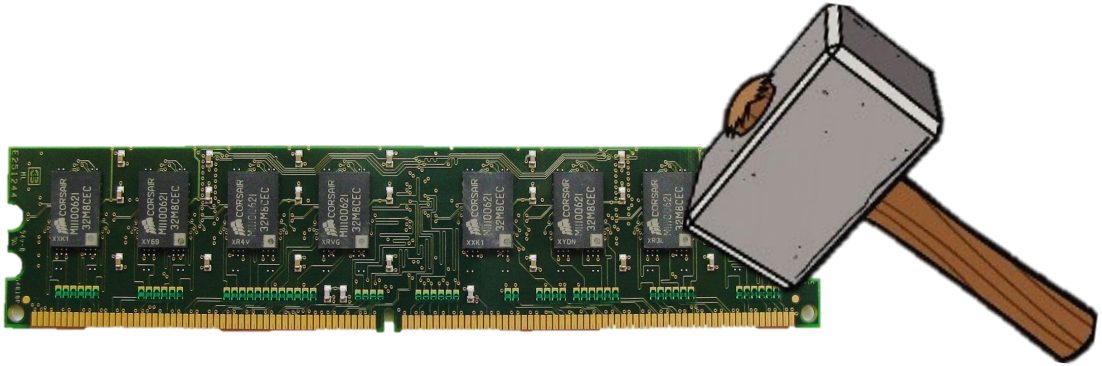

ack Submissions
Usability&Measurement
4.4%
Privacy and Anonymity
9.4%
Software Security
13.1%
Web Security
6.3%
Applied Cryptography
19.1%
Network Security
6.9%
Machine Learning &
15.2%
HW, Side Channels,
12.1%
Formal Methods and PL
3.1%
Blockchain & Distributed
10.4%

ack Acceptance Rates

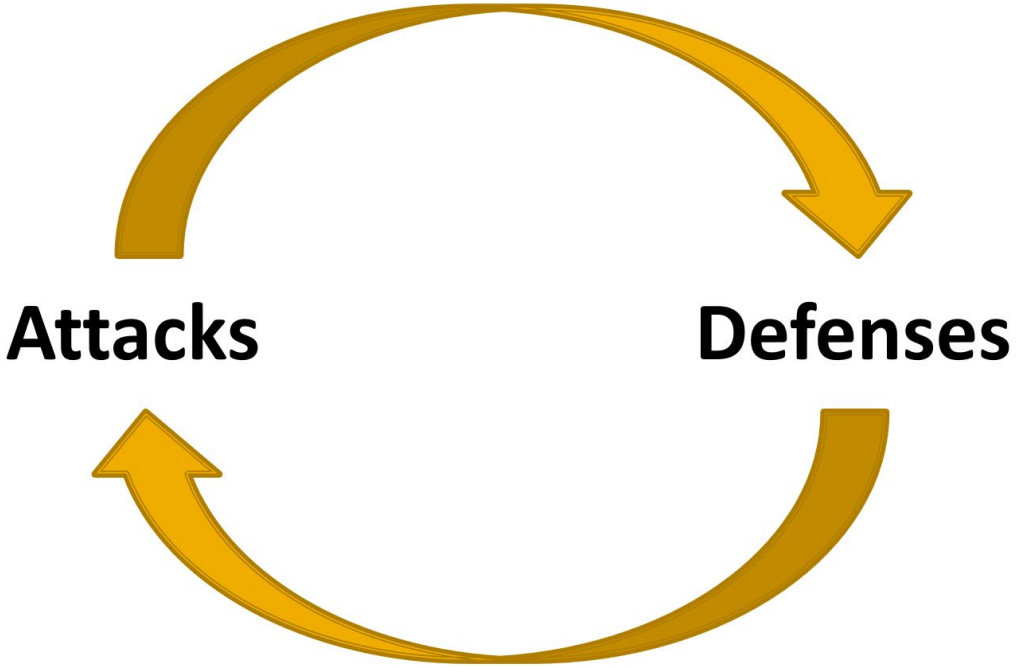
What is Security Research?

- 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

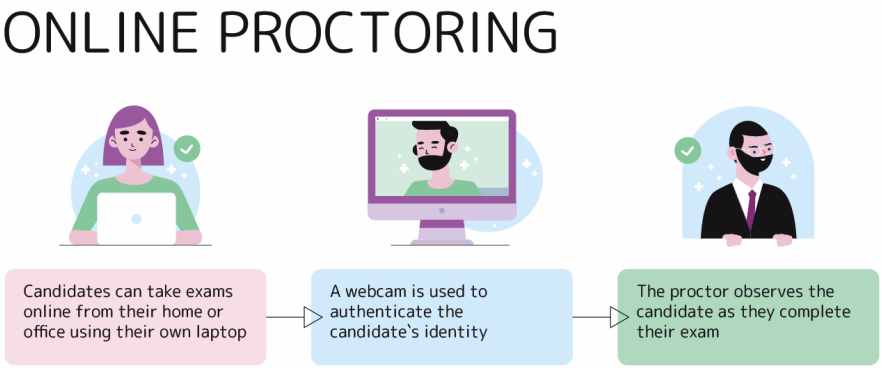
Thinking Like an Attacker

- 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
- In-class debates
  - Students will be assigned into debate teams
    - Pretend that they are reviewers on a PC arguing for or against acceptance of the paper
- 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
- Late Policy
  - no credit if turned in after class has started and we've discussed the paper
  - Ask me if you need an extension

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
  - Include discussion questions for the class
    - Controversial opinions are welcomed!
  - Also include a discussion of how the state-of-the-art has advanced since publication of the paper
- Paper list found at https://andrewkwong.org/comp790-184.html
- Send me preferences (at least 5) by Wednesday

Course Project (40%)

- Conduct original research on a topic related to computer security over the course of the semester.
  - Likely can connect your current research to a security topic
  - I can brainstorm topic with you
- In class proposal/presentation End of September/end of course
- 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
- Email me at andrew@cs.unc.edu with the title: “COMP 790-184 Paper Preferences”:
  - Rate preferences for paper presentations (Give me your top 5 at the very least)
- Start thinking about your course project
  - Proposals due end of of September

How to Give a Talk

Slides Adapted from David Bindel

Why put in the effort?

- “A good conference talk is more valuable than a good paper.”
  - Wise words from Manos Kapritsos at Umich
- First impressions count
  - People remember your first talk!
- You need to give a talk to get an academic job
  - Or any job really

What is a successful talk?

While going to meetings I had already been studying why some papers are remembered and most are not. The technical person wants to give a highly limited technical talk. Most of the time **the audience wants a broad general talk** *and wants much more survey and background than the speaker is willing to give. As a result, many talks are ineffective. The speaker names a topic and suddenly plunges into the details he's solved. Few people in the audience may follow.* **You should paint a general picture to say why it's important, and then slowly give a sketch of what was done.**

– Richard Hamming, "You and Your Research"

What is a successful talk?

- A successful talk has...
  - Interesting big ideas
  - A compelling story
  - *Carefully selected* details
- Talk is an advertisement for your paper
  - Not paper condensed into 15 minutes
- You want to sell your ideas *and yourself*.

Format

- Grab them in the first thirty seconds
- Very first slide after intro should be motivation for the problem
  - Convince audience, in a comprehensible manner, that you are working on an interesting problem
- Describe the status quo, SOTA limitations
- Describe how you advance over SOTA
  - Give some high level, flashy results
- Now the intro is over, all before diving into technical details
  - Most important part of the talk

Body

- Present select technical details
  - Convey the high level approach and contributions of your paper
- Lots of examples throughout
- Slowly become more technical, and then less technical

Conclusion

- Remind audience of the take home message
- List of contributions in final slide
- Picture of yourself!

Slides

- Learn your timing (one to two minutes per slide is typical)
- Show, don’t tell
  - Not too much text!
- Can’t have too many pictures/animations

Higham's ten commandments

1. Design the talk for the audience.
2. Prepare thoroughly and rehearse the talk.
3. Produce clear, legible slides.
4. Arrive early and check the lecture room.
5. Speak slowly and loudly.
6. Be enthusiastic about what you say.
7. Look at the audience as you speak.
8. Don't fidget with the slides or the pointer.
9. Finish on time (or early).
10. Answer questions courteously and concisely, and admit if you don't know the answer.

Offline reading

- N. Higham, *Handbook of Writing for the Mathematical Sciences* (chapters 10–11)
- R. Hamming, “You and Your Research” http://www.cs.virginia.edu/~robins/YouAndYourResearch.html
- Ken Birman, “Thoughts on Giving Professional Talks” http://www.cs.cornell.edu/~stevenan/givingatalk.pdf
- Charlie Van Loan, “The Short Talk” http://www.cs.cornell.edu/cv/ShortTalk.htm
- Matt Blaze, “No, You Can’t Have My Slides” http://www.crypto.com/blog/slideware

A final thought

Beware of advice, even this.

— Carl Sandberg

THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL