Advanced Topics on Secure Hardware

Instructors: Dawn Song, Krste Asanoivc, and David Kohlbrenner
Volunteer TA: Dayeol Lee

Why build secure hardware?

Why build secure hardware?

Can’t we just write better software?

Topics List

- Enclaves
- Side-channel attacks on hardware
- Side-channel defenses for hardware
- Memory models
- TPMs and Trusted Boot
- Physical attacks on hardware (and defenses)
- Formal verification
- Physical constraints of building hardware

Readings will be posted >=2 weeks before hand.

Prerequisites

- Assume knowledge of modern architecture
  - Familiar with material like caches, speculative execution, etc
  - Some very basic cryptographic knowledge

- For undergraduate students, must fill out form on website!
  - We will send you an add code if we approve your application.
  - If you applied but haven’t heard from us, talk to me after class

Course Format

- Approximate Lecture format
  - Main lecture (50 mins)
  - In-depth discussion (30 mins)
- Weekly reading, discussion questions
- Projects

Weekly Readings

- Research papers on week’s topic
  - We may post additional optional reading
  - I encourage you to read cited papers if they seem helpful

Discussion Questions

- Each student proposes at least three discussion questions
  - General questions about the topic
  - Specific questions about the technical details in papers

- We will use these to guide the discussion

Discussion Question Schedule

- Questions due **Fri noon**
- We will post a piazza post with instructions on question submission

Projects

- 4 Types
  - Traditional Literature Review
  - Replication and refinement (attacks)
  - Implementation with enclaves
  - Conference quality research project
    - Especially on enclave applications
- Groups of 2-3 people
  - Talk to instructors if need to form group of 1 or 4 people
- Further seed ideas will be posted this week

Project Schedule

- **9/10**: Groups due
- **9/27**: Project proposals due
- **10/29**: Progress report due
- **11/26**: Final project presentations
- **11/30:** Project report due

Grading and variable units

- 20% Class Participation
- 20% Weekly Reading Assignment
  - 10% participation
  - 10% question submission
- 60% Project
- 1 unit for readings, 3 units for both

Next steps

- Join Piazza https://piazza.com/class/jlbppizryjy74k
- Join the mailing list (on website)
- Reading for next lecture
- Plan for course project

Website: https://berkeley-secure-hardware.github.io/cs294-156-f18/

Next up: Paul Kocher