ADVANCED COMPUTER SECURITY

CMPS 223
OVERVIEW

WHO ARE YOU?

▸ Owen Arden (hi!)
  ◦ Email: owen@soe.ucsc.edu
  ◦ Office: E2-349A
  ◦ Office hours: Wednesdays and Fridays after class (and by appointment)
  ◦ Research areas:
    ◦ security, PL, and distributed systems.
OVERVIEW

GOALS

- Read, present, and discuss classic and current papers on a variety of security-related topics
- Page: https://users.soe.ucsc.edu/~owen/courses/cmpts223/fa17/
- Particular emphasis on:
  - Distributed/decentralized security
  - Language-based security techniques
  - Formal guarantees
OVERVIEW

TOPIC AREAS

- Defining security formally
- Reasoning about authority
- Information flow control
- Trusted hardware mechanisms
- Cryptocurrencies and smart contracts
BACKGROUND

- **Security**: Familiarity with systems security, cryptography, and access control.

- **PL**: Operational semantics, type systems, functional programming, etc.

- **Formal methods**: Logical reasoning, ability to understand proofs.

- Please see me if you have any questions or concerns.
COURSEWORK

- Read papers
- Write and post short responses to Canvas
- Prepare and present a paper for discussion
- Classroom discussion
- Design and complete small final project
OVERVIEW

PAPER RESPONSES

- General contents:
  - Summary, research contributions, and impact
  - What you liked
  - What you disliked
  - What you didn’t understand
- Submit to Canvas site (ideally by ~3pm the day before)
- Read other student responses too!
PRESENTATIONS

- Presentation should be about 40 minutes
- Lead discussion of the paper for remaining time
- Start early. **It’s a good idea to come meet with me** to talk about the paper and your presentation beforehand.
- Sign up soon!
OVERVIEW

FINAL PROJECT

- Design and complete a small project
  - Not too big: aim for 30-40 expected hours of work
  - Bigger goals? Find an intermediate result to present
- Individual or small groups (2-4)
- Project proposal (*due early November*)
- Project write-up and short presentation
SURVEY PROJECT (1 PERSON)

- Pick an area of interest. For example:
  - Blockchain security mechanisms
  - Smart contract applications
  - Differential privacy for machine learning
  - IoT security mechanisms

**Key:** choose papers carefully and keep focus narrow, otherwise you won’t have anything interesting to say
OVERVIEW

SURVEY PROJECT (1 PERSON)

- Thoroughly read 2-5 published papers
- Superficially read 2-5 more
- Write a report:
  - What are the basic problems in the area?
  - What are the basic approaches to solving them?
  - What are the main results to date?
  - What are some currently unsolved challenges?
IMPLEMENTATION PROJECT (1–4 PEOPLE)

- Implement a non-trivial security mechanism, or build an application that is enabled in by a new security mechanism
  - A small programming language with security features
  - A tool for analyzing the security of smart contracts
  - A decentralized authorization service
  - A distributed application secured with trusted hardware
- Write a report on project’s design and implementation
OVERVIEW

RESEARCH PROJECT

- Hard, given time constraints, unless you already have a clear idea.

- A survey project could turn into a research project if you discover a potential research question during studies.

- Make sure you limit scope to ensure you have some results by the end of the quarter.
OVERVIEW

GRADING

- Responses: 30%
- Presentation: 30%
- Project: 30%
- Participation: 10%

- Discussing the papers (online and in class) is a big part of this course, so please come to class!
ACADEMIC INTEGRITY

- All work you turn in must be your own. If you are unsure about whether something is ok, please ask!
  - All paper responses are expected to be your own work
  - Projects should be new and original
  - Group members are expected to share the work of the project equally
OVERVIEW

QUESTIONS?