Advanced Computer Security

CS563 / ECE422

Nikita Borisov, Spring 2025

Today

- Course overview
  - Course format
  - Student expectations
  - Project
  - Grading

Course Goals

- Prepare for independent research in computer security
- Read, review, and discuss current research papers
- Carry out a research project

Class Format

- 6 modules
- Each module will have:
  - One introductory lecture (by me) to review background work
  - 3-4 lectures w/ 2 papers / lecture, presented by students
- + a few auxiliary lectures on logistics, projects, guest lectures

Reading papers

- This is a reading heavy course
  - Up to 4 papers / week
  - Plus background papers
- Reading papers quickly and proficiently is a key research skill!

Paper Reviews

- Two styles of review
  - *Short*: bullet points summarizing contributions, highlighting high and low points of a paper. Expect this to take 15 minutes (in addition to reading paper)
  - *Full*: a ~500-word review with a detailed perspective on the paper. Expect this to take ~2 hours
- You will be required to write one long review per week, and short reviews for all other papers
- Reviews due 24hrs before class

Paper presentations

- Each student will present one paper
  - Summarize paper (briefly)
  - Moderate discussion
  - Roughly 30 minutes / paper
- Non-presenters: come prepared to talk!

Scribe / Blog post

- Each student will be assigned one paper for a blog post
- Blog post should:
  - Summarize key ideas in the paper
  - Discuss strengths and weaknesses
  - Summarize in-class discussion
- Post should be narrative format, ~1000 words in length
- Due 2 weeks after lecture

Research Project

- Semester-long research project
- Three types:
  - Novel research on a topic of choosing
  - Systematization of knowledge: a survey that includes a high-level perspective
  - Reproduction study: reproduces an existing paper with a critical perspective on results and methodology

Project Deliverables

- Presentation (reading day, May 8)
- Conference-style report (due May 16)
- Other milestones (more details next week)
  - Project proposal
  - Literature review
  - Progress checkin

Project Groups

- Groups of up to 3 students are encouraged
- A multi-student group should have:
  - A collaboration plan submitted around proposal time
  - A collaboration report submitted at project
- Larger groups come with better expectations
  - 1-person group: workshop-quality paper
  - 2-person group: 2nd tier conference paper
  - 3-person group: top conference paper

Special Circumstances

- Discuss with me before planning a project that:
  - Is used for credit in multiple courses (including 597)
  - Involves collaborators outside of the course (including advisor!)
  - Extends your own research
- The above are fine, but we need to set appropriate expectations

Timeliness

- This is a high workload / high reward course
- Need to read and review papers before class!
  - 24hr before lecture: full credit
  - 23:59-00:00: half credit
  - Late: no credit
  - 80% full credit = A
- Be prepared to discuss read papers
  - Lecture participation: 10% of grade

Timeliness, or lack thereof

- Other HARD deadlines
  - Paper presentation
  - Project presentation
- Other deadlines are SOFT
  - I'd rather have you submit great work late than mediocre work on time
  - Happy to give grad students incomplete but need to make plan for resolving it

Grading

- Paper reading / reviews: 40%
  - Reviews: 10%
  - Presentation: 10%
  - Participation: 10%
  - Blog post: 10%
- Project: 60%
  - Proposal: 10%
  - Literature review: 10%
  - Presentation: 15%
  - Final report: 25%

Next lectures

- Thursday, Jan 23
  - Introductions
  - Privacy on the Web lecture (by me)
- Tuesday, Jan 28
  - How to read / review a paper
  - Project milestones
- Web page: https://adv-sec-sp25.nikita.phd/