Advanced Computer Security

CS563 / ECE524

Nikita Borisov, Spring 2026

Today

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

Introduction Questions

- Preferred name, pronouns
  - *Nikita, he/him*
- Program, advisor
  - *Prof ECE, associate head of undergrad programs, affiliate of CS*
- Research interests
  - *Network security, privacy, applied cryptography*
- Interesting non-work fact about yourself
  - *Like ultra-marathons, baking, chess*

Course Goals

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

Course Non-Goals

- Explicit qual prep
  - Qual requires you to read, present, and discuss certain papers
  - This course requires you to read, present, and discuss other papers
- Practical security knowledge
  - Focus on security **research** not **practice**, though aim for papers likely to have impact
- Comprehensive coverage
  - 1200+ papers published in top computer security conferences in 2025!

Class Format

- 5-6 modules
- Each module will have:
  - One introductory lecture (by me) to review background work
  - 5-10 papers, 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

- Detailed review: 500-word review with a detailed perspective. Graded on a check/check+/check- scale
  - 1-2 hours
  - **A** standard: 15 x check
  - Due at start of class
- Quick summary: bullet points for discussion, 15 minutes worth. Graded on a P/NP scale
  - Expect this to take 15 minutes
  - **A** standard: 80% * P
  - Due 24 hours before class
  - Half credit if submitted before class but < 24 hours ahead

Paper presentations

- Each student will present one paper
  - Summarize paper (briefly)
  - Moderate discussion
  - 30-45 minutes per 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 7)
- Conference-style report (due May 15)
- Milestones (more details soon)
  - Pre-proposal
  - Proposal
  - Literature review
  - Experiment plan
  - Update

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

Grading

- Paper reading / reviews: 50%
  - Reviews, full: 15%
  - Reviews, short: 5%
  - Presentation: 10%
  - Participation: 10%
  - Blog post: 10%
- Project: 50%
  - Proposal: 10%
  - Literature review: 5%
  - Technical approach: 5%
  - Presentation: 5%
  - Final report: 25%

Logistics

- Fill out interests form
- Join SPRI slack, #adv-sec-sp26 channel
  - https://sprai.slack.com/
- Introduce yourself
- Next lecture: overview of authentication, credentials, and abuse