EECS 588 - Winter 2024 - Computer & Network Security

Instructor: Ang Chen (chenang@umich.edu)
GSI: Elisa Tsai (eltsai@umich.edu)

Format: This is a seminar-based course, with an extensive reading list in various topics in computer and network security, broadly organized in three sections as in the spreadsheet. Expected learning outcomes are a) deep familiarity with latest security research, b) ability to write critical reviews and judge the quality of security research, c) end-to-end formulation and execution of a security research project, resulting in a short paper of submittable quality at the end of the semester. Further, the lectures are driven by paper presentations from every student in the class, and everyone will present a research paper at least once in the semester. There will also be a group project, with a team size of three, with two presentations in-class.

- Time: Mondays + Wednesdays 1:30-3:30pm, divided as follows:
- Main lecture: 1:30-3pm:
  - 1:30-2:30pm: One student presentation, on a research paper of their choice.
  - 2:30pm-3pm: Review and ShortReview paper discussion.
- Discussion time: 3-3:30pm
  - For most classes, this is a Discussion period **optional** for students. The instructor will be available throughout this time to discuss any part of the course, such as the research project, presentations, and review papers. Students are dismissed if they don't have questions to discuss.
  - Depending on the number of registered students, we may repurpose some of this time to accommodate more student presentations to make sure everyone gets to present. In this case, we will likely schedule a second in-class presentation from 2:30-3:30pm, while skipping the review/SR paper discussion. In this case, the second talk is a **required** part of the class.
- Office Hours:
  - Ang Chen: By appintment, Location: 4753 BBB or Zoom link on Piazza
  - Elisa Tsai: Tuesday 9-10 AM, Location: Zoom (https://umich.zoom.us/j/6543751542) or BBB Learning Center (table #1).
- Attendance: In-person attendance is highly encouraged, but nonetheless not required. Note however, class participation contributes to your scores as detailed below.
- Canvas: Please submit all reviews, project reports, at Canvas.
- Piazza: Will be used for discussion and announcements. Sign up at: https://piazza.com/umich/winter2024/eecs588

Key tasks:

- Write a Full Review on every Review paper, and a Short Review on every SR paper. Reviews are due 11pm eastern time one day before the class. In the class, we are going to spend about 30 minutes discussing the review paper and the reviews you have submitted. Full Reviews account for **30%** of your overall score, and will be graded. Short Review submissions, while not required or graded, are highly encouraged and contribute to your class participation. The in-class discussions, whether on the Review or SR papers, contribute to your class participation as well.

- Every student gives one or more presentations during the semester, and the dates can be selected by changing “Available” slots to your name and paper name. The paper must be approved by the instructor, please email me and GSI with 2-3 papers from the top-four conferences held in 2022, 2023, and 2024: IEEE SP/USENIX Security/NDSS/CCS by **January 15 at noon** eastern time 2024, with email title **[EECS 588: Paper selection: Student Bio].** Please include a short bio and a recent photo of yours – we would love to get to know you better! – as well as 2-3 papers you are interested in presenting; we will select one from your list and email it to you. Please sign up at the spreadsheet for a slot to present by January 15 noon as well. Note that slots fill up fast so please secure your slot **NOW**!
    - Every presentation lasts for one hour. One presentation per class unless otherwise arranged.
    - 35 min on the main paper, 10 min on your own criticism + praise of the paper. 15 min for QA from the entire class and myself.
    - Short (e.g., 3 min) break then the review paper discussion.
    - (Tentative: We may use a Piazza poll for everyone in the audience to give a rating of your talk, and take the class rating into account when grading your presentation.)
    - Presentation accounts for **15% of your overall score**.
- Research project lasts for 7-8 weeks, and it must be a substantial undertaking and the topic needs discussion with and approval from the instructor. We grade not only the final outcome but also your planning and progress throughout the semester. Each project team has three members. The project accounts for **40% of your overall scores**. Please see due dates in the spreadsheet in the class schedule. Note that the format+length below is only a suggestion, reports only need to roughly follow the suggested format/length. Every team only needs to submit one copy via Canvas, and the submission must contain all members’ names; all members in the same team receive the same score for all components of this research project.
    - Project proposal: 1pg limit. Must cover the following items, one paragraph each
        - What is the problem?
        - How is it done today?
        - Why is it insufficient?
        - What is your proposal and unique insight?
        - A bullet list of timeline for the project, with weekly progress plans so we’ll have about 7-8 data points for your timeline. (Including the break, there are in total 8 weeks between the proposal and final presentation.)
        - The proposal will be graded and contributes to **5%** of your scores.
        - The proposal presentation contributes to **5%** of your scores, and will be conducted in class. We will announce logistic details (such as presentation order and length) depending on the number of teams.
    - Project progress/midterm report: 3 pg limit
        - The first page is your proposal: No longer graded at this milestone.

        - Pages 2-3: What you have achieved so far. Describe in detail the system components, the codebases you may be building upon, the findings you had, potential setbacks you have experienced. Document your discussions with the instructor on your project over the past month, the feedback you've been given, and how you've taken actions to address the feedback.
        - The midterm report will be graded and contributes to **10%** of your scores.
    - Final report + source code + evaluation data: 6pg limit
        - Pages 1-3 are the same as your previous report, no longer graded.
        - Page 4: Describe three key challenges in the design of the system.
        - Page 5: Describe three solutions you've designed to address the challenges
        - Page 6: Measurement/benchmark results, figures, pointer to your codebase, reflection on future work.
        - Please include all your source code and evaluation data. If you have large data files, please email instructor and GSI to set up another way of submission.
        - The final report will be graded and contributes to **15%** of your overall scores. Treat this as a "short paper" of submittable quality to an academic workshop / conference.
        - The final project presentation contributes to **5%** of your scores, and will be conducted in class. We will announce logistic details (such as presentation order and length) depending on the number of teams.
- Class participation **15%**: This includes participation in the discussions during the class, submission of Short Reviews, as well as engagements with the instructor and GSI offline – such as discussions, Piazza, office hours, etc.
- Late policies: For late submissions, 10% deduction for each late day.

- **Sample project ideas:** We will provide a list of sample project ideas as examples.
    - A: Explore the use of LLMs as a medium to distribute censored content. Normally, the information carrier is the Web, and websites get censored by blocking. LLMs, however, are in a different class as they do not exhibit explicit features that enable precise blocking.
    - B: IoT devices form an important class of distributed systems. Design a tool and conduct studies that fingerprint and reliably detect IoT devices in the wild.
    - C: Investigate the use of eBPF for security.
    - D: Reproduce research paper X and its key results.
    - E: Measurement of the (mal)practice of anti-scam apps (see slides).
    - F: Reproduction/Defense against text-to-image generative models jailbreaking attacks (see slides).

- Review submission: We have curated a Review template (SRs follow the same, without the “Detailed review” section in the template) from a typical academic conference review system: https://drive.google.com/file/d/1g9eye9PsJegmMornp6SgqHuHGwPcgu9y/view?usp=sharing