CS 6431 – Security and Privacy Technologies

Project Proposal and Final Report

Instructor: Tom Ristenpart *Fall 2024*

A key learning objective for 6431 is the ability to perform high-quality academic research in computer security. The semester project represents the learning-by-doing that is key to this learning objective:

- A project should consist of publishable work. Of course you don't have to actually publish it, but it should aim for content that would find a home at a computer security or related publication venue. If you do want to publish it, that's great! Ask me about this if you need advice, but by default I won't be involved beyond our interactions during the semester (nor do I expect any acknowledgement or authorship for class project work).
- It's better to pick a narrower project and do it well, then to take on too big of a project. Can you extend an algorithm from a paper? (Dis)prove an open conjecture? Perform an ethics review of a line of work? Provide additional experiments that were lacking in some existing paper? Just because we want publishable work doesn't mean I'm asking for a full, 12-page paper's worth of results. It'd be better to do a narrower contribution that could be a section or two of a larger paper, or a short paper.
- It is fine to use ongoing research or work in collaboration with others as a project. Collaboration is one of the best parts of research! But, I will want to know what *your* specific contribution was, and expect you to do the bulk of the writing for the class project final report.
- It is ok to work on the project in pairs or larger groups of students from the class. The project's scope should be proportional to the group size.

The project will use a peer-review process. I am in the process of setting up a HotCRP instance for submitting both proposals and, later, final papers. You will all be involved in reviewing other proposals and papers. Reviews will also be graded for their utility.

Project proposal (due October 7, 2024). The project proposal is meant to force you to start thinking about projects ASAP and get some early feedback on your ideas. I will look at proposals, but we'll also use peer feedback to help refine ideas. The proposal should scope out your project. It should be at most about a one page PDF (latex preferred) consisting of the following:

- A short abstract, in the style of one for an academic research paper. We have seen many examples in the research papers we've been reading. The abstract should be written as if you have already done the project; i.e., what will the abstract say about your project once you've completed the work. This is a good exercise, to see if a project seems interesting, before you begin in earnest. You can also reuse the abstract (presumably with small updates) for the final paper.
- A concise outline consisting of:
  1. Short description of any relevant related work you've already uncovered, with citations. This won't be a full related work discussion, just a pointer to the papers and topics.
  2. Discussion of the methods you will employ for the project, and what data sets, implementations, or other resources you will need.

3. Fallback plan in case something doesn't work out with your original plan. For example, if you can't get a proof to work, what will you do instead? Note that doing a writeup of negative results is totally acceptable as long as we learn something from it — which means particularly that we need compelling discussion and evidence of why your approach failed. This can often be harder than a positive result.

You can add more beyond that, but please be concise and to the point — your classmates and myself will be reading this and likely to be less excited about having to read a novel.

You will turn these into a HotCRP instance that I am setting up.

Project proposal reviews (due Oct 16, 2024). Each person in the class will be responsible for providing three reviews of other proposals. The HotCRP instance will help us manage reviewing. For peer review of proposals, we'll proceed as follows:

- Bidding phase: You'll have until October 9 to bid on projects to review. You will get to see all project proposals. (We won't abide by typical conflict of interest rules for simplicity.)
- Review period: You'll have one week to review the two proposals, including providing a written assessment of:
    - Novelty: If successful, will this project represent potentially publishable work?
    - Feasibility: Does this seem feasible in a semester time frame?
    - Editorial quality: How is the abstract's writing? Do you have suggestions for making it stronger?

  Include any other feedback, either editorial such as listing typos, grammar errors, or comments on ambiguous writing, as well as technical — ideas for improving the direction of the project, suggestions for approaches or related work to look up. A good review will be about a page of text, and may require looking up some of the related work mentioned in the proposal.

  Good reviews are *constructive*: your job is to help the author(s) towards a great semester project. Be polite and respectful. I will be reading the reviews and part of your grade will rest on quality of reviews.

The HotCRP instance can be used to engage in discussions between authors and the reviewers, and I will encourage you to do so to answer questions about any ambiguities.

Draft final paper (due December 2, 2024). You should submit a paper of at most 6 pages, excluding references and appendices. It should include abstract, introduction, related work / background, and then results sections. It can have a conclusion or not. You should use latex and the USENIX Security class file that I'll distribute. Any other artifacts (code, experimental data) should be put online somewhere (e.g., a public Github repository) and linked from the paper.

Paper reviews (due December 9, 2021). You will provide reviews for the final version of the proposal you previously reviewed.

The review you write should expand on your earlier review, now evaluating the paper based on typical acceptance criteria at an academic venue. We'll release more info about the reviewing guide later in the semester.

Final paper (due December 16, 2021). You can revise your paper based on reviewer comments, and resubmit it.

Grading. You will be graded based on quality of your proposal, your reviews (how constructive and helpful were they), and the overall quality of the final paper after taking into account any feedback.

Deadlines will be firm. If you see big problems with the deadlines (e.g., conflicting with some other deadline for many students in the class), let me know. That said we will try to fix them as soon as possible, and once set, like real paper deadlines, we can't comfortably support late submissions. If you submit late, you are cramping the schedule and, particularly, making life hard for your reviewers. You can always submit earlier, if the deadlines fall on awkward or busy days for you. If you do end up submitting your proposal or final paper late, you will not get reviews, and your grade will end up being docked accordingly. More importantly, you won't benefit from constructive feedback. Late reviews are also not acceptable, and will be worth zero points.

Of course if you have a serious life event (illness or other issue) you can come talk to me. But please let me know ASAP, day-of excuses will be met skeptically (since you could have submitted the day before).