COMP 590: Privacy Enhancing Technologies – Project Expectations

The most important part of this class is a course project. The project will require **significant** self-directed effort and learning outside of class. It is a big part of your grade and the main source of outside-of-classroom work other than reading responses. You may work on the project in groups of 3-5 students. Every member of the group will be expected to contribute.

The project requires the following deliverables:

1. **Project proposal**: In 1 page (in any format), list group members, describe what the project will be, what work you intend to complete by the project update, and roughly what each group member will do. I am happy to meet with groups ahead of time to discuss your ideas. Meeting ahead of time, while not required, can be extremely helpful in making sure the project idea aligns well with course expectations.

3. **Project update:** 2-3 page document (not counting references) typeset in Latex using IEEE document style. This update should consist of 1) an introduction motivating and describing your project goals, 2) a brief overview of how your solution/tool will work, and 3) a summary of what has been done so far and what each group member has done. The expectation is that there will be significant progress from the proposal to the update. Please include a link to a Github repository with your source code.

3. **Final presentation**: present your project in front of the class. Focus on motivating the problem you solve and explain your solution briefly. Project presentations will be 5 minutes long with 2-3 additional minutes for Q&A after.

4. **Final report**: 5-7 page document (not counting references) that has an introduction that motivates the problem, a brief description of existing related work, an overview of your solution, a more detailed discussion of the design, and a brief description of what could be completed in future work. Please also state what each group member has done since the update. You can use the introduction and overview from the update as a starting point for the final report, but the expectation is that there will be significant progress from the update to the final report. Please include a link to a Github repository with your source code.

NOTE: projects must be completed in groups of 3-5, with the exception of students who are involved in relevant outside research projects, who may do the project alone. This means you need to find others in the class to do the project with. Students who would like help finding partners can use the discussion features on Canvas or reach out to me for assistance forming groups. One goal of starting the project later in the semester is to make sure you have time to meet others in the class and brainstorm potential projects together based on the material in class.

Some Potential Project Ideas

- Build an end-to-end encrypted private messaging application (desktop, web-based, or mobile – your choice). In addition to having end-to-end encryption, the system should allow users to authenticate their sessions with each other out of band and make an effort to reduce the amount of user metadata it requires to deliver messages.

- Build a tool for end-to-end encrypted private file storage on top of a public cloud storage system, e.g., Google drive or dropbox. In addition to encrypting files, the tool should try to hide metadata like file names and which files you are accessing/modifying. If time permits, a cryptographic tool like ORAM may be a good thing to study and discuss.

- Build a tool for a group of users, each of which holds sensitive private data, to compute joint statistics on their data, without sharing it. This will require learning about and implementing cryptographic multiparty computation (MPC) techniques.

- Build a tool that allows users to stay logged in to a few selected sites, e..g, news websites, while browsing the web on private browsing mode, while maintaining the benefits of this mode for other sites. Use hardware enclaves to protect and hide information needed across multiple sessions. This will require building a browser extension that manipulates session cookies and connects the browser to the hardware enclave.

- Read 1-3 research papers in the field, implement the ideas in one or more of those papers, and report on the performance of the resulting implementation. You may not just run the code that the authors provide, although you can compare the performance of your implementation to the authors' version if it is available.

- Suggest a project of your own design. The project should be large enough to involve a month's worth of work. A good starting point for this is to think of some technology with which you regularly interact that would benefit from additional privacy features.

- Use your own pre-existing security or privacy-related research as the course project