CSE 708 Fall 2021
Course Project

Your course projects will be due soon, and at this point it is assumed that you are in the final stages of your project. If your project includes implementation, make sure that you test all components for correctness (you will be asked to report about it in your submission).

Project Report

Your project, including the source code, if applicable, and project report, is due at 11:59pm on Monday, December 6. Please submit all requested information to the instructor via email.

For non-survey projects, the project report needs to contain the following components:

1. An overview of the project describing:
   (a) the target functionality;
   (b) security model and objectives (this includes description of from whom information is to be protected and what the adversary is capable of, any trust assumptions on the participating parties, what security objectives are desired, etc.)
   (c) description of the complete cryptographic design with the steps listed in chronological order (as they might appear during execution). For not widely used constructions, this needs to include cryptographic formulas or functions computed in the implementation. For standard techniques, this needs to include pointers to a source containing a description of such techniques. The description also needs to include the format of all messages exchanged in the design/implementation. The rationale is that the description needs to be complete and self-contained enough to evaluate the design with respect to meeting the security objectives.
   (d) a list of security objectives that your design achieves if different from the full list in part (b) (otherwise, you can say that all security objectives of part (b) are met).
2. The outcome of the project including:
   (a) the project setup (the programming language, platform used, etc.);
   (b) the results of the implementation (e.g., performance analysis, security analysis, scalability issues, etc.);
   (c) description of what was achieved with respect to the project goals (e.g., if the goals were not met, a justification for adjusting the goals);
   (d) any difficulties encountered;
   (e) how testing of the cryptographic elements and other components was performed (correctness testing in particular).
3. The source code. Please clearly mark the code written for the purpose of this project and any other code you submit (e.g., code written by you at an earlier time or for a different course, etc.).
4. Description of the data on which the project was run.

For survey projects, please include the following in your project report:

1. A brief description of the problem and why it was chosen for the project.
2. The classification strategy used to organize the publications in the survey.
3. Lessons learned about the solutions used to solve the chosen problem.
4. Difficulties encountered during working on the survey.

The survey itself is expected to follow a regular publication format with a clearly marked introduction/motivation, review of the literature (including classification, analysis), and relevant publications. The survey is due at the time of project report submission.

Project Presentations

Our project presentations will be held during class on December 3 and 10. Each project has been assigned one of the two dates and if you are not sure on what day you are presenting, contact the instructor. As discussed in class, each project's presentation should be not shorter than 15 minutes and together with questions can be up to 20 minutes.

Project presentations contribute 10% of your project grade and thus their quality will be graded. In your presentation, you are expected to motivate and describe the problem, explain what the security goals are, and briefly say what techniques were used to achieve the goals. Clarity of the presentation is important.

Project Demos

If your project includes implementation, you will have a meeting scheduled with the instructor to discuss the outcome of your project and show a demo. These meetings will tentatively take place on Wednesday, December 8 and will be scheduled separately. For this meeting, you can either bring a laptop and demonstrate your project on your own machine or make sure that your program runs on CSE computers in Davis Hall.