COMP3632 Project (2020 Spring)

For 10% of your grade, you will be required to do an open project on some topic in cybersecurity and/or privacy. There are broadly two types of projects you can do:

1. Programming project. You will write a program to achieve something related to cybersecurity/privacy.

2. Written project. You will investigate some issue or topic related to cybersecurity/privacy and write a report based on your findings.

You must choose a topic before 24th April (Friday) midnight by e-mailing me with the title "COMP3632 Project". Write your topic in the body of the e-mail, describe in one or a few sentences what you want to do, as well as which type of project you chose. For programming projects you must also choose which type of presentation you want. There are several example topics for each project in the following pages. You are allowed to and in fact encouraged to choose your own topic.

The project submission is due on the 22nd of May (Friday). There is a 2-day late submission grace period, same as the assignments.

The grading criteria for each project will follow. Especially high-quality projects may receive up to a 5% bonus beyond the 10% grade.

Programming Project

If you choose this option, you will be asked to submit code as your deliverable. You have two choices in how you want to present this project:

1. Submit a PDF report named **report.pdf** explaining your code, how to run it, and what you have achieved, OR:
2. Schedule a 5-minute Zoom presentation with me, where you will share your screen to show your code.

In the former case I will run your code following your instructions for grading.

Grading

Your project will be graded on:

- Work; the amount of effort spent on this project. A rough ballpark of how much work I expect is around 200–400 lines of code.
- Quality; the project should use good software engineering techniques and show off your understanding of the topics of this course.
- Presentation; how easy it is to understand your work. The report or Zoom presentation should be clear, the code should run consistently, and give meaningful output.
- Quality of code; the code itself should be clear and well documented.

If your project is excellent by the above standards, a bonus grade may be given based on innovativeness, i.e. whether you have achieved something surprising, and whether or not you actively pursued further learning through the project.

Example topics

- Software Vulnerabilities. Write a piece of code with at least three types of vulnerabilities, such as a buffer overflow, a format string vulnerability, and an integer overflow vulnerability, then demonstrate how each could be exploited.
- Implementation of Elliptic Curve Cryptography. Study it and write your own code to implement it.
- Automated Two-time Pad Breaker. Given two or more plaintexts encrypted with the same OTP, automatically break them, possibly based on a dictionary or manual instructions.
- Optimal k-anonymity Finder. Write a program that will automatically find a way to k-anonymize a data set with minimal disruption to the data (use your own definition for disruption).

Written Project

If you choose this option, you will be asked to submit a report as your deliverable. Using a single-column, single spacing, 12pt font on A4 paper, your report should be between 6 to 12 pages, and should be titled **r**eport.pdf.

Grading

Your project will be graded on:

- Work; the report should reflect a significant degree of reading and learning. A rough ballpark of how much I expect is around 30 pages of reading.
- Quality; the report should explain a topic clearly, it should be typeset, structured and written correctly, and it should use figures and other techniques to supplement its content.
- Depth; the report should show a clear understanding of some topic, and present the subject matter without ambiguity.

If your project is excellent by the above standards, a bonus grade may be given based on innovative independent work, e.g. your report contains your own findings and experimental results.

Example topics

You should choose a topic that was not already covered in-depth in class.

- Software vulnerabilities in a well-known program. Use my explanation of Zoom vulnerabilities as an example.
- History of SSL/TLS. Describe all of its versions; expound on the weaknesses in each version that led to the development of newer versions.
- Security/insecurity of a cryptographic protocol (including hashes). Focus on the mathematics and explain the attacks and fixes.
- Major network attacks targeting a web service company (e.g. Cloudflare) and their defensive response.
- The use of differential privacy in commercial products.

Plagiarism warning

Plagiarism is strictly forbidden as usual. To clarify what constitutes plagiarism:

- Using someone's code library is okay, but you must attribute them. Do not copy-paste any code in your work.
- When writing any text, do not copy from a source. If you want to use someone else's explanation, read it, close the window/book, then write it out yourself.
- Do not copy anyone else's graphics, including figures and graphs. (Do not do so even with attribution.)