CPEN 442 – Introduction to Cybersecurity

Module 0

Course Information

Course Information

- Simon Oya (he/him)
- email: simon.oya@ubc.ca
- office hours:
  KAIS 4110
  Fridays, 12:30pm – 1:30pm

- Lectures:
  - Tue, 12:30pm – 1:50pm, IRC-4
  - Thu, 12:30pm – 1:50pm, IRC-4
    → might change to MacLeod 2002!
  - Attendance will not be mandatory
- Lab sessions:
  - Fri, 2:00pm – 4:00pm, IRC-5
  - Starting next week! (there's no lab session tomorrow)
- TAs:
  - Mohammed Elnawawy
  - Joshua Chiu
  - TBD

- Syllabus/Canvas coming later this week!

Course Mechanics

- **Canvas**: course website, syllabus, slides, public materials, …
- **Piazza**: Q&A, general discussions
  - Please keep up with the information on Piazza.
  - Use a private question if needed.
- Please use **email** as a last resort (and should be from a UBC email address)

Grading Scheme

- Module quizzes (5%)
  - One quiz per module (9 modules), three attempts, open for a week, on Canvas
  - Usually open when we finish module, but quiz 1 will open next week
- Assignments (65%)
  - Most assignments have a deliverable part to do in the lab, and another part to do at home.
  - Assignments can be done in pairs. If so, both students are expected to understand every part of the assignment.
  - Tentative: 7 assignments, more details coming soon.
  - The first one starts next week, on the lab session of Friday, Sep 13th
- Midterm exam (5%)
  - Open book
  - Tentative date: Oct 22nd, during the lecture, on Canvas
- Final exam (25%)
  - Open book
  - Will cover content from all the modules
  - Some minimum grade will be required for an A+

Lab sessions

- Tomorrow there is no lab session.
- The first lab session is next week, on Sep 13th.
- Lab sessions (and assignments in general) will require you to be comfortable with Python.
- Attendance is required to submit the deliverable part to be done in the lab.

Academic Misconduct

- The course should be fairly easy to pass if you do the quizzes, and do your part in the assignments. (Coming to the lectures will help!)
- The easiest way to fail the course is by cheating
  - This should be obvious for 4th year students!
- It is not worth it!
- You are encouraged to discuss the course contents with other students; but there's a clear difference between this and plagiarism
  - Check the UBC website on academic misconduct
  - Check the UBC website on generative AI tools

    "Students may use GenAI in work submitted for courses or other academic requirements only if expressly permitted within their courses or programs"
- Careful with Piazza; post private questions if you're not sure if they should be public

Course Source Material and Textbooks

- Most of the content of this offering of CPEN 442 has been taken/inspired by the CS458 – Computer Security and Privacy course from the University of Waterloo
  - Initially mostly designed by Prof. Ian Goldberg and Prof. Urs Hengartner from the CrySP research group.
  - Many CrySP faculty (and some students) have contributed to the material as well
- Some material has also been adapted from CS 489/689 – Privacy, Cryptography, Network and Data Security also from the University of Waterloo (taught by Prof. Bailey Kacsmar and Thomas Humphries).

- Recommended textbooks for this offering of CPEN 442:
  - *van Oorschot* "Tools and Jewels". Publicly available at the author's website.
  - *Stamp* "Information Security: Principles And Practice". Available at the Campus Library

A Note on Security

- Spiderman principle:

  "with great power comes great responsibility"

- In this course, we will see security vulnerabilities, attacks, etc.
- You are not to use this to attack any system or network (without consent of the owner)
- Be especially careful with complying with university policies!

Course Structure

- Module 1: Introduction
- Module 2: Cryptography
- Module 3: Access Control
- Module 4: Cryptography Use Cases
- Module 5: Program Security
- Module 6: Network Security
- Module 7: Data Privacy
- Module 8: Usable Security
- Module 9: Non-technical Aspects of Security