CPEN 442 – Introduction to Cybersecurity

Module 0

Course Information

Course Information

- Simon Oya (he/him)
- email: `simon.oya@ece.ubc.ca`
- office hours:
  KAISER 4110
  Thu, 3:00pm – 4:00pm

- Lectures:
  - Tue, 12:30pm – 2:00pm, MacLeod 2002
  - Thu, 12:30pm – 2:00pm, MacLeod 3018
    → might change to MacLeod 2002!
  - (Attendance will not be mandatory)
- Lab sessions:
  - Fri, 2:00pm – 4:00pm, Orchard Commons 1001
  - (Not mandatory, mostly for assignment/group project feedback & work)
- Tas (to be confirmed):
  - Atrin Arya
  - Ali Balapour
  - Mohammed Elnawawy

- 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 (7 modules), three attempts, open for a week, on Canvas
  - Usually open when we finish module, but quiz 1 will open next week
- Assignments (45%)
  - Three assignments, each 15%
  - Work in groups, details coming soon
- Midterm exam (5%)
  - Open book
  - Tentative date: Oct 10th, during the lecture, on Canvas
- Final exam (15%)
  - Open book
  - Will cover content from all the modules
- Group project (30%)

Group Project

- The lectures provide a broad overview of cybersecurity
  - We will "go wide", but we cannot "go deep"
- The course project is where you'll have to go deep.
- Choose a problem/area that you like and/or you're familiar with.
  - Identify a security issue within this area (privacy issues are also OK).
- Groups will be formed based on topic preferences
- Halfway through the course:
  - Submit a 1-page summary of the project (5%)
- At the end:
  - Submit a 10-page paper explaining your project (20-ish%)
  - Give a 15-minute presentation of your project (5-ish%)
  - (Submit a short video where each participant explains their contribution to the project)
  - Provide feedback on other presentations (?%)

Exact and
final details
and deadlines
coming soon
to Canvas

Tomorrow there is no lab session, but…

- By the end of next Wednesday 13th: you'll have to submit a **project idea**
  - a project title
  - a one-paragraph description
- Instructions on how to submit this will be provided on Piazza, but you will be reminded during the next lecture (Tue 12th)
- I will select a subset of these project ideas and publish them in time for Fri 15th lab session. In this session I will give you time to read them and vote for your preferences
- The groups will be made shortly after

How to choose the project idea?

- Choose a topic that you like and have previous experience in, and think of security and/or privacy issues in that topic
- A good sign of "relevance" is the existence of publications in that topic in top-tier security venues. The "big 4" are
  - IEEE Security and Privacy
  - ACM Conference on Computer and Communications Security (CCS)
  - USENIX Security Symposium
  - Network and Distributed System Security Symposium (NDSS)
- For more privacy-focused projects:
  - Privacy-Enhancing Technologies Symposium (PETS)
- Check previous term's projects for inspiration (https://blogs.ubc.ca/cpen442/term-projects/)
- It can be an analysis project, a design project, an implementation project (read more about these in the link above). SoK-like projects will also be accepted.

Academic Misconduct

- The course should be fairly easy to pass if you do the quizzes, and do your part in the assignments and group project. (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
- 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: Program Security
- Module 3: Operating Systems Security
- Module 4: Network Security
- Module 5: Cryptography (Internet Applications Security)
- Module 6: Real-world Cryptographic Protocols
- Module 7: Non-technical Aspects of Security
    - Usability
    - Economics
    - Ethics