

CPEN 442 – Introduction to Cybersecurity

Module 0



Course Information

Course Information



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

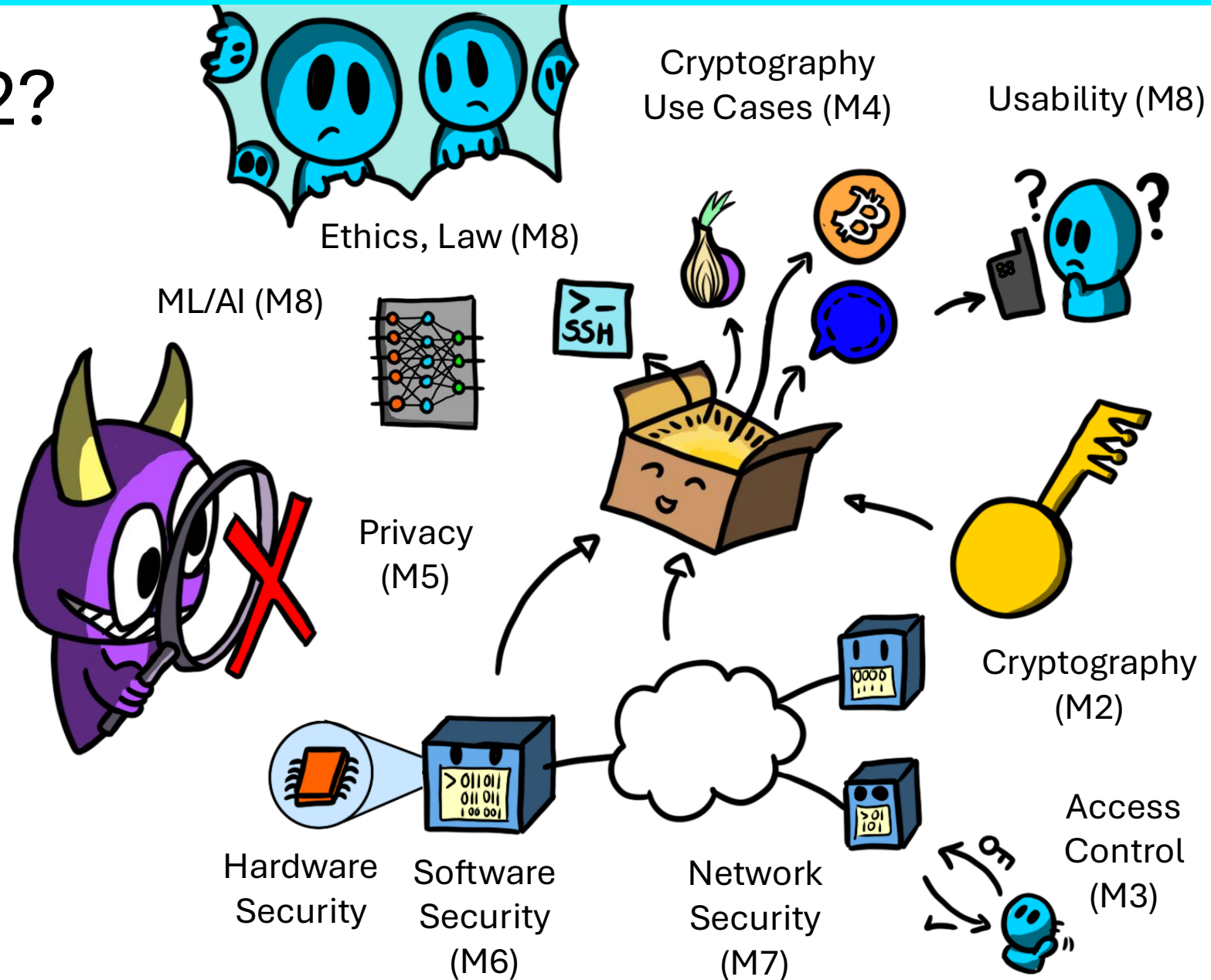
- Lectures:
 - Tue, 9:30 – 11:00am, CHBE 102
 - Thu, 9:30 – 11:00am, CHBE 102
 - Attendance will not be mandatory
 - *Might* be recorded
- Labs:
 - Fri, 2-4pm, in the ether
- TAs:
 - Mohammed Elnawawy
 - Evan Rossiter
 - Ali Bazshoushtari



- Syllabus available in Canvas
- Communication through Piazza (self-enroll)
- Quizzes in PrairieLearn (self-enroll)

What is CPEN 442?

- A broad introduction to cybersecurity.
- Cybersecurity is very broad.
- We can only go (slightly) **deep** in a few topics.
- Course contents:
 - Module 1: Introduction
 - **Module 2: Cryptography**
 - Module 3: Access Control
 - **Module 4: Cryptography Use Cases**
 - **Module 5: Privacy**
 - Module 6: Software Security
 - Module 7: Network Security
 - Module 8: Selected topics (ML/AI privacy and security, usability, law, ethics)



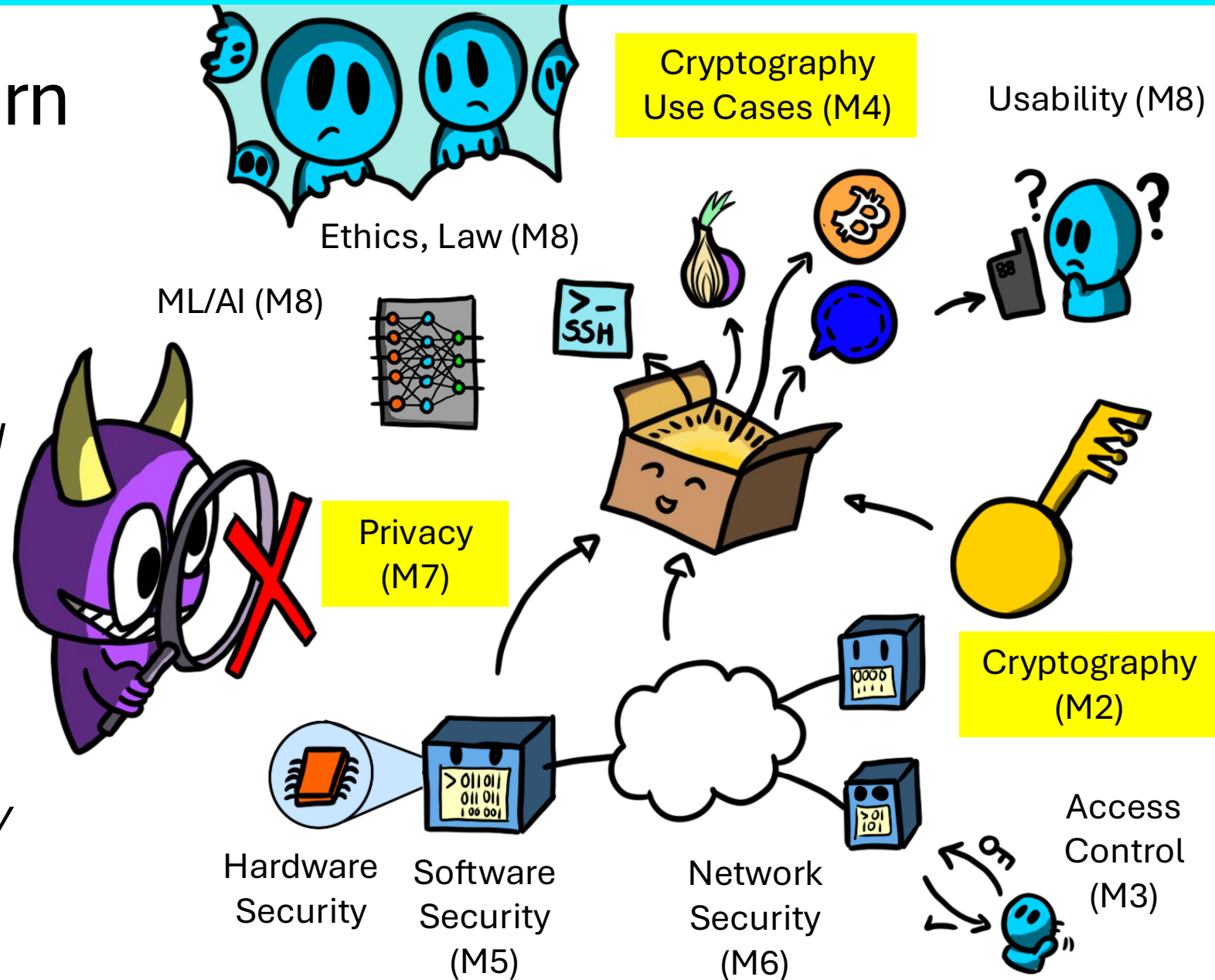
Course Goals

This is a *foundational* course on cybersecurity, covering the basics of cryptography, access control, privacy, and key protocols that rely on cryptography.

- The primary goal is to develop a **security mindset** and be able to **identify security issues** in various aspects of computing.
- The secondary goal is to use this ability to **design systems that are more protective of security** (and privacy).

Things you will learn

- *How do we hide data with cryptography? Can anyone break cryptography?*
- *How do digital signatures work? What about password authentication? Passkeys?*
- *What real-world protocols use cryptography, how, and why? (TLS, SSH, Tor, Bitcoin,...)*
- *What is privacy? How do we measure and provide privacy today?*
- *Are ML models “secure”?*

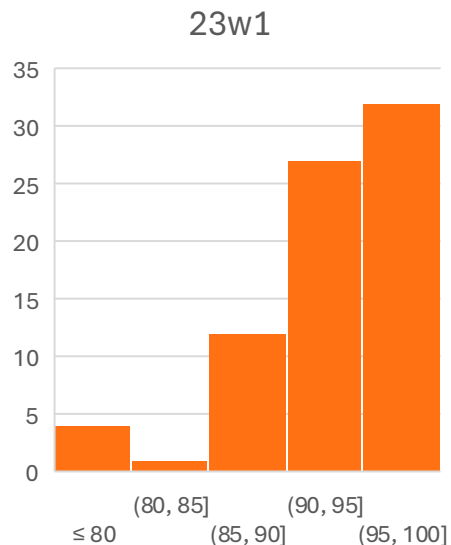


(Sadly,) this is not a CTF course.

For the most part, we will not be doing any “hacking”.

This course over the years: 2023

Evaluation Method	23W1 (CPEN 442)
Module quizzes	5%
Assignments	45%
Midterm exam	5%
Final exam	15%
Group projects	30%

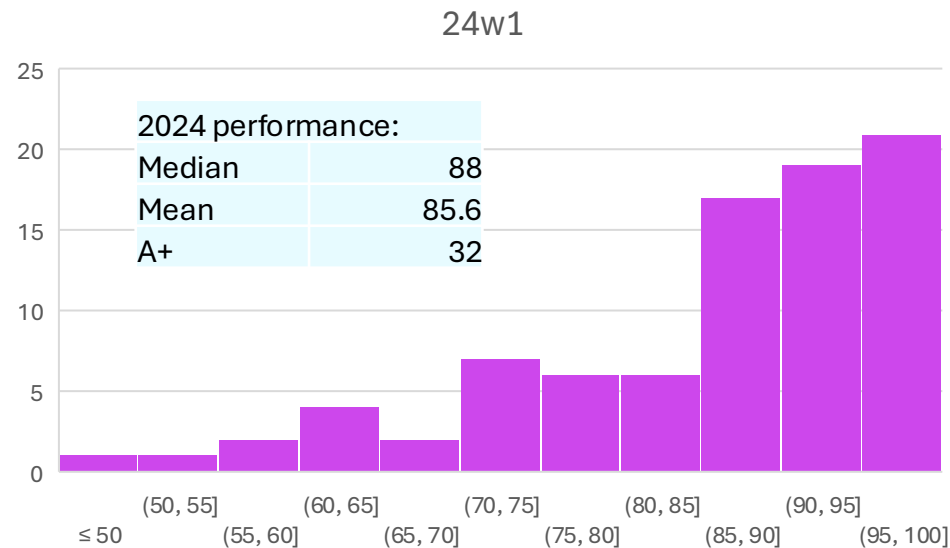
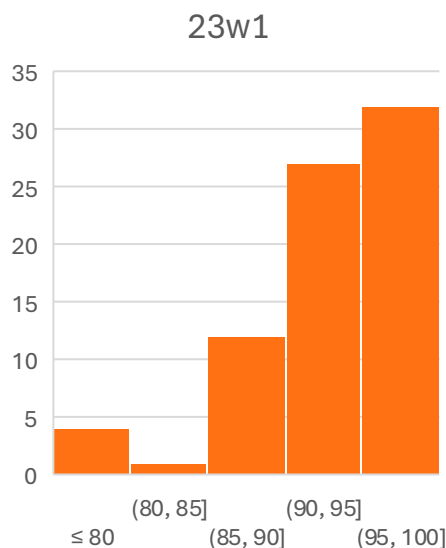


Feedback:

- Group projects are not “fair”; lots of free riders.
- Not enough work (?).
- Some people didn’t do anything in the assignments (they were groups of four).

This course over the years: 2024

Evaluation Method	23W1 (CPEN 442)	24W1 (CPEN 442)
Module quizzes	5%	5%
Assignments	45%	65%
Midterm exam	5%	5%
Final exam	15%	25%
Group projects	30%	–



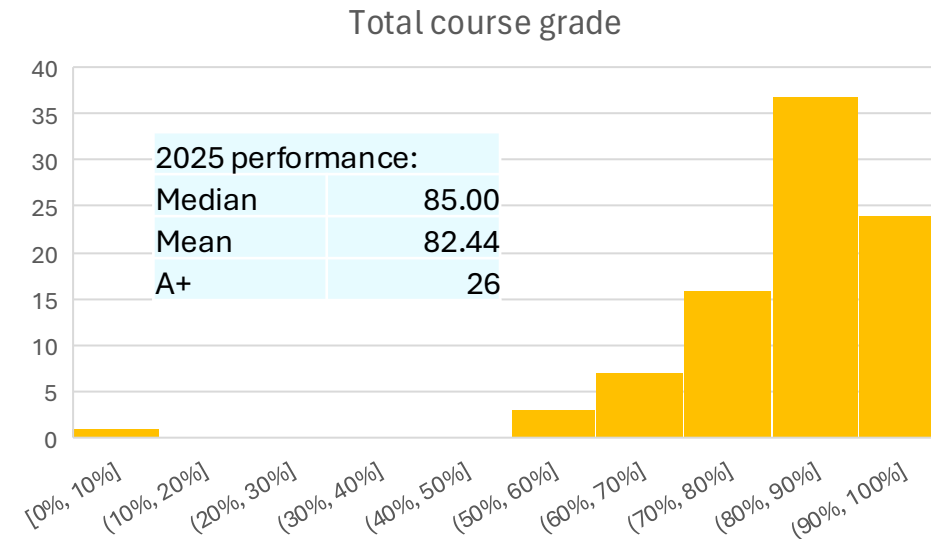
Problem:

- Starting 2025, AI became too good and solved most of these assignments.
- An open-Internet exam would allow students to get really good grades without learning much.

This course over the years: 2025

Evaluation Method	23W1 (CPEN 442)	24W1 (CPEN 442)	24W2 (CPEN 542)	25W1 (CPEN 442)	25W2 (CPEN 542)
Module quizzes	5%	5%	5%	5%	5%
Assignments	45%	65%	60%	55%	55%
Midterm exam	5%	5%	10%	15%	15%
Final exam	15%	25%	25%	25%	25%
Group projects	30%	–	–	–	–

- Big change: exams went from “open Internet” to “pen and paper”.
 - There were lots of practice exercises, and I told students what the questions would be.
 - They could bring one sheet with notes to the exam.
 - The exam had assignment-specific questions to make sure students understood what they did in the assignments.
- Slightly more weight on exams (5% more)



This year: 2026

Evaluation Method	23W1 (CPEN 442)	24W1 (CPEN 442)	24W2 (CPEN 542)	25W1 (CPEN 442)	25W2 (CPEN 542)	26W1 (CPEN 442)
Module quizzes	5%	5%	5%	5%	5%	10%
Assignments	45%	65%	60%	55%	55%	45%
Midterm exam	5%	5%	10%	15%	15%	20%
Final exam	15%	25%	25%	25%	25%	25%
Group projects	30%	–	–	–	–	–

Some issues

- AI keeps getting better, assignments are less reliable indicators of learning.
- Quizzes were not very useful for learning.
- We do not have enough TA hours to do fancy activities (e.g., projects).

Changes this term

- Quizzes will be more demanding. Still unlimited tries, keep best grade. Weight increased 5% → 10%.
- Assignment grade decreased (55% → 45%).
- Midterm exam(s): two midterms, at the ORCA testing facility. Almost repetition of quizzes, there's lots of practice. Easier than past terms (?), and more weight (15% → 20%).
- Final exam: similar to past terms. Probably in PrairieLearn, closed-book, one-page sheet allowed. Same weight as last years. There'll be lots of practice questions to get ready.

Grading Scheme

- Module quizzes (10%)
 - Roughly one quiz per module, on **PrairieLearn**.
 - Usually open when we finish the module, sometimes earlier.
 - Goal: to check that you have somewhat followed the content so far, and that you can solve exercises in exams.
 - Unlimited attempts: everyone should get this 10%.
- Assignments (45%)
 - Around 6 or 7 assignments total.
 - Typically, heavier workload at the beginning, lighter towards the end.
 - To be done individually.
 - Require some Python programming.
- Midterm exams (10% + 10%) and final exam (25%).
 - **(NEW)** Two midterms done at the ORCA testing facility in PrairieLearn.
 - Lots of practice (current version of Midterm 1 is almost the same as Quiz 2).
 - That might not be necessarily true for Midterm 2 (we'll see how it goes).
 - There is one week to book them; you choose your own slot.
 - Exam very likely also in PrairieLearn, but not in ORCA. We will allow a one-page sheet.
 - Cover contents of assignments and possibly other exercises; I will make lots practice exercises available.
 - No “memorization” questions.

Course Mechanics

Sessions

- **Lectures:** not mandatory. Maybe recorded. We cover all the course content, sometimes do practice exercises, etc.
- **Labs:** not mandatory. Help for assignments and problem-solving activities. By default, there is no lab unless there is an announcement that there will be a lab.
 - Also, we don't have a room?

Platforms

- **Canvas:** course website, syllabus, slides, public materials, ...
- **Piazza:** Q&A, general discussions
 - Please keep up with the information on Piazza. Enable notifications!
 - Use a private question if needed. Do not leak solutions!
- Please use **email** as a last resort (and should be from a UBC email address).
- **PrairieLearn:** for module quizzes and midterms.

Academic Misconduct

- The course should be very easy to pass if you do the quizzes and the assignments. (Coming to the lectures will help a lot!).
- The easiest way to fail the course is by cheating
 - This should be obvious for graduate 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

Is Generative AI Allowed?

Yes^{*}

^{*} But you must explain how and where you used it. And the exams are just you, to make sure that you understood the assignments.

Course Source Material and Textbooks

- The 2023 version of this course 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
 - This course has changed quite a bit since then
- 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!