CS 453/698: Software and Systems Security

Module: Introduction

Lecture: course logistics

Meng Xu *(University of Waterloo)*

Winter 2025

Outline

1. Formalities

About me

- Name: Meng Xu
- Assistant Professor at Cheriton School of Computer Science
  - Joined on September 2021.
- Member of CrySP and CPI.

About me

- Name: Meng Xu
- Assistant Professor at Cheriton School of Computer Science
  - Joined on September 2021.
- Member of CrySP and CPI.

- Completed PhD at Georgia Tech (August 2020)
- One gap-year at Facebook / Meta on Diem blockchain
- Worked on several streams of software security research:
  - Moving-target defense (i.e., software diversity)
  - Static program analysis (e.g., symbolic execution)
  - Dynamic program analysis (e.g., fuzz testing)
  - Formal verification (e.g., Move Prover)

Learning outcomes

On course website

> *Students completing this course should be able to identify common attack vectors against modern computing environments and deploy state-of-the-practice detection and defense practices.*

Learning outcomes

On course website

> *Students completing this course should be able to identify common attack vectors against modern computing environments and deploy state-of-the-practice detection and defense practices.*

Learning outcomes

On course website

> *Students completing this course should be able to identify common attack vectors against modern computing environments and deploy state-of-the-practice detection and defense practices.*

Modern computing environments include software, operating system, mobile, hardware, and emerging systems.

About this course

Expectation: treat this course as a guided tour on the software and systems security landscape.

About this course

Expectation: treat this course as a guided tour on the software and systems security landscape.

- We cannot possibly cover every single topic in this area.
- We hope the security topics covered in this course align with your future study / work / research plans.
- We are open to new topic suggestions as well as feedback on course content and delivery.

Logistics

Two sections which are supposed to cover identical content:

- For students enrolled in CS453-001 and CS698-003
  - **Time**: 4pm - 5:20pm on Tuesdays and Thursdays
  - **Location**: MC 2034
- For students enrolled in CS453-002 and CS698-005
  - **Time**: 1pm - 2:20pm on Tuesdays and Thursdays
  - **Location**: MC 2054

Materials available online include lecture slides plus any supplement materials to facilitate the understanding of the topic

Communication channels:

- Public information will be posted on course website
- Questions and discussions should go on Piazza
- Personal matters can be discussed through your `uwaterloo` email

Topics to cover

Refer to Course Outline.

Assessment

Component	**Weight** (CS 453)	**Weight** (CS 698)
Assignment 1	25%	20%
Assignment 2	25%	20%
Assignment 3	25%	20%
Assignment 4	25%	20%
Research write-up	(optional)	20%

Assessment

Component	Weight (CS 453)	Weight (CS 698)
Assignment 1	25%	20%
Assignment 2	25%	20%
Assignment 3	25%	20%
Assignment 4	25%	20%
Research write-up	(optional)	20%

- A research project is optional for students in CS 453, but if you choose to do it, you can use the grade to replace the worst grade of your assignments.
- Late submissions are generally not accepted, unless
  - with valid VIF Form or Absense Declaration
  - with early notification to the instructor well before the due date (at least a week) for any long-lasting problems.
- Re-appraisal can be requested with a clear justification of claims
  - send the request to the TA(s) within one week of grade release.

Office hours

Instructor office hours: Tuesdays 2:30pm to 3:30pm

- Online via BBB, access code: `1xszia`
- In-person by appointment only

Instructors are available to answer questions about module content, course policies, syllabus matters, and special situations.

TA office hours will be given to you in assignment details.

University policies

In this course, you will be exposed to information about security problems and vulnerabilities with computing systems and networks. To be clear, you are NOT to use this or any other similar information to test the security of, break into, compromise, or otherwise attack, any system or network without the express consent of the owner.

Refer to the list of relevant university policies when in doubt.

Academic integrity

Don't copy-paste!

Academic integrity

Don't copy-paste!

- Read this excellent explanation of plagiarism online
- Ignorance is no excuse!
- Plagiarism applies to both text and code. You are free (and encouraged) to exchange ideas, but sharing code or text is a violation of academic integrity policies.

Academic integrity

Don't copy-paste!

- Read this excellent explanation of plagiarism online
- Ignorance is no excuse!
- Plagiarism applies to both text and code. You are free (and encouraged) to exchange ideas, but sharing code or text is a violation of academic integrity policies.

Possible penalties:

- First offense: 0% for that assignment, -5% on final grade
- Second offense, more severe penalties, including suspension

Use of Generative AI (GenAI) tools

Permitted, but you need to properly cite it and follow other university guidelines.

Use of Generative AI (GenAI) tools

Permitted, but you need to properly cite it and follow other university guidelines.

If you used any LLM-based tools to solve whole or part of the assignment, I am personally very interested in how you prompt it to give you the solution.

$\langle$ **End** $\rangle$