CS 489 / 698: Software and Systems Security

Module 1: Introduction
course logistics

Meng Xu *(University of Waterloo)*

Spring 2023

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)

About this (pilot) course

First thing first: this is a pilot course.

About this (pilot) course

First thing first: this is a pilot course.

- We hope to seek your feedback on course content and delivery.
- We hope the security topics covered in this course align with your future study / work / research plans.
- We are open to new topic suggestions.

About this (pilot) course

First thing first: this is a pilot course.

- We hope to seek your feedback on course content and delivery.
- We hope the security topics covered in this course align with your future study / work / research plans.
- We are open to new topic suggestions.

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

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, network, hardware, mobile, and cloud.

Logistics

Time: 11:30pm - 1pm every Tuesday and Thursday

Location: in-person at MC 4058

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

Logistics

Lectures will still be recorded and can be made available individually upon request with a valid VIF Form or Absense Declaration.
$\Longrightarrow$ there is no need to come to class if you are feeling unwell.

Logistics

Lectures will still be recorded and can be made available individually upon request with a valid VIF Form or Absense Declaration.
$\Longrightarrow$ there is no need to come to class if you are feeling unwell.

None of the graded components in this course requires in-person submission or completion.

Topics to cover

Refer to Course Outline.

Assessment

Component	**Weight** (CS 489)	**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 489)	**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 489, 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: Monday 3-4pm

- Online via BBB, access code: 085376
- 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

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