CS 458 / 658: Computer Security and Privacy

* - Final Exam

- - -

Meng Xu *(University of Waterloo)*

Winter 2023

Outline

Exam date, time, and location

- Date: **April 17th**
- Time: **12:30pm - 3:00pm** (2.5 hours)
- Location: **MC 4059** — for students enrolled in Section 1
- Location: **MC 4061** — for students enrolled in Section 2

Exam date, time, and location

- Date: **April 17th**
- Time: **12:30pm - 3:00pm** (2.5 hours)
- Location: **MC 4059** — for students enrolled in Section 1
- Location: **MC 4061** — for students enrolled in Section 2

Common Q & A:

Q : What if I am registered with Alternative Testing Arrangement?

A : You will have the accomodations based on the policies

Exam date, time, and location

- Date: **April 17th**
- Time: **12:30pm - 3:00pm** (2.5 hours)
- Location: **MC 4059** — for students enrolled in Section 1
- Location: **MC 4061** — for students enrolled in Section 2

Common Q & A:

Q : What if I am registered with Alternative Testing Arrangement?

A : You will have the accomodations based on the policies

Q : What if I feel unwell on the exam day?

A : Seek medical care first, submit a Verification of Illness Form that is filled out by a physician within 48 hours, and write the exam in a subsequent term.

Exam format

The exam will be a **paper exam**

- Questions include true/false, multiple-choice, and short answers
- Close book and close notes
- University-approved calculators can be used
- No other electronic devices are permitted
- Covers the entire course (i.e., all modules)
- The review slides will guide you on where you should pay attention

Outline

Module 1

- Understand basic terminology: Security, Privacy, Adversaries.
- Be able to identify assets, vulnerabilities, threats, attacks, and defences.
- Distinguish different types of defence mechanisms and be able to apply a defence scenario.

Module 2

General note: we will not ask you to write PoC code since this was extensively covered in A1.

- Understand basic terminology and concepts: flaws, fault, failures, control against security flaws in programs.
- Identify unintentional security flaws in a program and their root cause, and be able to suggest and/or evaluate a defence mechanism.
- Understand malware taxonomy and malware-pertaining concepts, e.g., spreading, payload, infection.
  - *No questions will be asked on specific details of the malware instances discussed in class*
- Distinguish / evaluate different malware detection mechanisms.
- We will not ask questions on non-malicious flaws

Module 3

- Understand and apply access control concepts (we will not ask questions on RBAC).
- Understand and evaluate key principles of user authentication, understand and distinguish authentication vs identification
  - Focus less on Password Hygiene / Strength, Password Advice for Developers
- We will not ask questions on the following Security Policies and Models as it was extensively covered in A2: Bell-La-Padula, Biba and Low Watermark.
- Understand and evaluate the design of a Trusted OS
  - The following is not going to be covered: accountability and audit, and assurance, evaluation, common criteria

Module 4

- Understand basic network terminology and concepts
- Be familiar with different threats in networks
  - we will not ask questions on integrity attacks.
- Understand, and apply Network Security controls and firewalls.

Module 5

- Understand the definition of confidentiality, integrity, and authenticity in the context of cryptography.
- Be familiar with the Diffie-Hellman key exchange protocol
  - we will not ask questions on calculation here
- Understand cryptography use cases, focus on IPSec and off-the-record (OTR) conversation
- Understand the concept of private information retrieval (PIR)

Module 6

- Understand how to use SQL views to implement access controls in a database
  - Focus on DAC, we will not ask questions on RBAC
- Understand how to ensure element integrity, referential integrity, and atomicity in database
- Know the definitions of k-anonymity, l-diversity, and t-closeness and understand why these syntatic notions are not enough
  - We will not ask questions on calculation here
- Understand how to calculate l_1 diversity in the context of differential privacy, for both bounded and unbounded DP.

Module 7

- Know the differences between law and ethics
- Be aware of the ethical practices commonly seen in security/privacy domain
- Understand different types of intellectural properties
- Be familiar with security planning
- Know the calculation of risk exposure as well as savings due to employing a control mechanism.

Outline

Student Course Perception Survey

Complete by **April 10th, 11:59pm**

Available at https://perceptions.uwaterloo.ca/