University of Waterloo

Term and Year of Offering: Winter 2021

Course Number and Title: CS458, Computer Security and Privacy

Section	Lecture Time	Room	Instructor
0412	12:00-2:00 PM Thursday	Zoom	Navid Nasr Esfahani

Instructor's Name	Office Location	Contact	Office Hours

TA's Name	Office Location	Contact	Office Hours
Sina Faraji		sina.faraji@uwaterloo.ca	
Thomas Humphries		t3humphr@uwaterloo.ca	
Kassis Andre		akassis@uwaterloo.ca	
Nils Lukas		nlukas@uwaterloo.ca	
Miti Mazmudar		m2mazmud@uwaterloo.ca	
Matthew Rafuse		mrafuse@uwaterloo.ca	
Sajin Sasy		ssasy@uwaterloo.ca	
Justin Tracey		j3tracey@uwaterloo.ca	
Lindsey Tulloch		ltulloch@uwaterloo.ca	
Shannon Veitch		njunger@uwaterloo.ca	

Course Description:

This course introduces students to security and privacy issues that affect various aspects of computing, including programs, operating systems, networks, databases, and Internet applications. The course examines the causes of security and privacy breaches and provides methods to help prevent them.

Course Objectives:

At the end of the course, students should be able to

- Create programs that can defend against active attacks, not just against random bugs
- Analyze programs and computing systems to point out security and privacy vulnerabilities
- Identify and explain security and privacy related threats and issues across a range of computing systems
- Identify and explain common approaches to protecting security and privacy in computing systems and evaluate the effectiveness of their deployments
- Enumerate and differentiate key components of security and privacy policies, and evaluate proposed content for them
- Demonstrate knowledge of legal and ethical issues in computing, particularly as applied to security and privacy

Course Overview:

Introduction to computer security and privacy (1.5 hours)

- Meaning of computer security, comparing security with privacy, types of threats and attacks, methods of defense

Program security (6 hours)

- Secure programs, nonmalicious program errors, malicious code, controls against program threats

Operating system security (6 hours)

- Methods of protection, access control, user authentication

Network security (4.5 hours)

- Network threats, firewalls, intrusion detection systems

Internet application security and privacy (9 hours)

- Basics of cryptography, security and privacy for Internet applications (email, instant messaging, web browsing), privacy-enhancing technologies

Database security and privacy (4.5 hours)

- Security and privacy requirements, reliability, integrity, and privacy, inference, data mining, k-anonymity

Non-technical aspects (4.5 hours)

- Administration of security systems, policies, physical security, economics of security, legal and ethical issues

Required text:

Evaluation:

assignment 1: (25%) assignment 2: (25%) assignment 3: (25%) final assignment: (20%) self-tests (5%)

Late and Missed Assignments Policy:

Due dates are posted on the Piazza course site. Late submissions for final Assignments 1, 2 or 3, will be accepted only up to 48 hours after the original due date. There is no penalty for accepted late submissions. Assignments can be submitted multiple times -- the last one will be used for marking. There is no late submission for any milestones of Assignments 1, 2 or 3 and the final submission of Assignment 4. Course personnel will not normally give assistance for assignments after their original due dates. You must notify your instructor(s) well before the due date of any severe, long-lasting problems that prevent you from completing an assignment on time. The 48 hours grace period does not apply to the due dates for the CS 658 proposal and research survey paper; no lates will be accepted for them.

Rules for Group Work:

Assignment Submission and Pickup:

The assignments are sent via "submit", and the feedback is provided through info-dist.

Mental Health Resources

Mental Health: If you or anyone you know experiences any academic stress, difficult life events, or feelings like anxiety or depression, we strongly encourage you to seek support.

On-campus Resources

- Campus Wellness https://uwaterloo.ca/campus-wellness/
- Counselling Services: counselling.services@uwaterloo.ca / 519-888-4567 ext 32655 / Needles Hall North 2nd floor, (NH 2401)
- MATES: one-to-one peer support program offered by Federation of Students (FEDS) and Counselling Services: mates@uwaterloo.ca
- Health Services service: located across the creek from Student Life Centre, 519-888-4096.

Off-campus Resources

- Good2Talk (24/7): Free confidential help line for post-secondary students. Phone: 1-866-925-5454
- Here 24/7: Mental Health and Crisis Service Team. Phone: 1-844-437-3247
- OK2BME: set of support services for lesbian, gay, bisexual, transgender or questioning teens in Waterloo. Phone: 519-884-0000 extension 213

Diversity: It is our intent that students from all diverse backgrounds and perspectives be well served by this course, and that students' learning needs be addressed both in and out of class. We recognize the immense value of the diversity in identities, perspectives, and contributions that students bring, and the benefit it has on our educational environment. Your suggestions are encouraged and appreciated. Please let us know ways to improve the effectiveness of the course for you personally or for other students or student groups. In particular:

- We will gladly honour your request to address you by an alternate/preferred name or gender pronoun. Please advise us of this preference early in the semester so we may make appropriate changes to our records.
- We will honour your religious holidays and celebrations. Please inform of us these at the start of the course.
- We will follow AccessAbility Services guidelines and protocols on how to best support students with different learning needs.

Academic Integrity

Academic Integrity: In order to maintain a culture of academic integrity, members of the University of Waterloo community are expected to promote honesty, trust, fairness, respect and responsibility. [Check https://uwaterloo.ca/academic-integrity/ for more information.]

Grievance: A student who believes that a decision affecting some aspect of his/her university life has been unfair or unreasonable may have grounds for initiating a grievance. Read Policy 70, Student Petitions and

Grievances, Section 4. When in doubt please be certain to contact the department's administrative assistant who will provide further assistance.

Discipline: A student is expected to know what constitutes academic integrity [check https://uwaterloo.ca/academic-integrity/] to avoid committing an academic offence, and to take responsibility for his/her actions. A student who is unsure whether an action constitutes an offence, or who needs help in learning how to avoid offences (e.g., plagiarism, cheating) or about 'rules' for group work/collaboration should seek guidance from the course instructor, academic advisor, or the undergraduate Associate Dean. For information on categories of offences and types of penalties, students should refer to Policy 71, Student Discipline. For typical penalties check Guidelines for the Assessment of Penalties.

Appeals: A decision made or penalty imposed under Policy 70 (Student Petitions and Grievances) (other than a petition) or Policy 71 (Student Discipline) may be appealed if there is a ground. A student who believes he/she has a ground for an appeal should refer to Policy 72, Student Appeals.

MOSS (Measure of Software Similarities) is used in this course as a means of comparing students' assignments to ensure academic integrity. We will report suspicious activity, and penalties for plagiarism/cheating are severe. Please read the available information about academic integrity very carefully.

Discipline cases involving any automated marking system such as Marmoset or MarkUs include, but are not limited to, printing or returning values in order to match expected test results rather than making an actual reasonable attempt to solve the problem as required in the assignment question specification.

Note for Students with Disabilities: AccessAbility Services, located in Needles Hall, Room 1401, collaborates with all academic departments to arrange appropriate accommodations for students with disabilities without compromising the academic integrity of the curriculum. If you require academic accommodations to lessen the impact of your disability, please register with AccessAbility Services at the beginning of each academic term.

Intellectual Property: Students should be aware that this course contains the intellectual property of their instructor, TA, and/or the University of Waterloo. Intellectual property includes items such as:

- Lecture content, spoken and written (and any audio/video recording thereof);
- Lecture handouts, presentations, and other materials prepared for the course (e.g., PowerPoint slides);
- Questions or solution sets from various types of assessments (e.g., assignments, quizzes, tests, final exams); and
- Work protected by copyright (e.g., any work authored by the instructor or TA or used by the instructor or TA with permission of the copyright owner).

Course materials and the intellectual property contained therein, are used to enhance a student's educational experience. However, sharing this intellectual property without the intellectual property owner's permission is a violation of intellectual property rights. For this reason, it is necessary to ask the instructor, TA and/or the University of Waterloo for permission before uploading and sharing the intellectual property of others online (e.g., to an online repository).

Permission from an instructor, TA or the University is also necessary before sharing the intellectual property of others from completed courses with students taking the same/similar courses in subsequent terms/years. In many cases, instructors might be happy to allow distribution of certain materials. However, doing so without expressed permission is considered a violation of intellectual property rights.

Please alert the instructor if you become aware of intellectual property belonging to others (past or present) circulating, either through the student body or online. The intellectual property rights owner deserves to know (and may have already given their consent).