Usable Security and Privacy (ECE 750 T38) Spring 2024

ECE 750

Published Apr 03, 2024

Class Schedule

Section	Location	Time	Instructor(s)
ECE 750 002 *[LEC]*	[redacted]	Tuesdays & Thursdays 2:30 p.m. 3:50 p.m.	Kami Vaniea kami.vaniea@uwaterloo.ca
			This table is generated automatically

Instructor & TA (Teaching Assistant) Information

Instructor:
Dr Kami Vaniea
kami.vaniea@uwaterloo.ca
Davis Center 2532

Course Description

> *Calendar Description for ECE 750*

Real world security and privacy failures can often be traced back to human factors issues where the system might have been theoretically sound but did not take into account how people would interact with it. People are a key part of how systems are built (developers), deployed (administrators), and used (end users). To be secure and privacy enabling, technology needs to consider the various people who will use it, their needs, workflows, expectations, and likely interaction patterns.

This course explores how to design for security and privacy using a human centric perspective by combining lessons from computer security, privacy, public policy, and human-computer interaction.

Students should have a strong general background in computers. The course has no programming requirement. But concepts like logic, network protocols, and Linux should be familiar to students.

Learning Outcomes

By the end of this course students should be able to:

Describe real-world instances of security and privacy failures in common technologies and how those technologies could be adjusted to better account for people.

Critique a usable privacy and security study design.
Conduct usable privacy and security studies.
Read usable security and privacy research papers and understand the implications as well as limitations of the results and recommendations.
Reason about how various stakeholders may respond to a technology.
Construct scientifically grounded advice about how to handle common problems organizations face, such as phishing.

Tentative Course Schedule

Each topic below is a combination of a security/privacy topic and a human computer interaction topic which often co occur. Progressing through these topics will teach a student about the current research in the field of Usable Security and Privacy as well as how to think critically about the science behind advice commonly given in the field, such as how often passwords should be changed.

- Staying safe online eliciting views and preferences from people
  - Self-reflection on how the students themselves think about privacy and security and how they encounter it in their daily lives
  - Key internet security concepts
  - Lite introduction to law and public policy
  - Threat modeling basics
- Encryption researcher assessment of usability and think aloud
  - Encryption from an end-user point of view, focus on assumptions and guarantees it can and cannot provide
  - Famous studies on email encryption - Why Johnny Can't Encrypt
  - Basics of paper reading and study replication
- Authentication - measuring security costs
  - Basics of authentication
  - Measuring everyday activities accurately
  - Stakeholders
- Privacy - survey design
  - What is privacy?
  - Privacy by design
  - Privacy surveys and how definition of "privacy" can impact results
  - Developers and privacy
  - Quantitative analysis basics
- Phishing advice, interventions, and support
  - Phishing, fraud and the effectiveness of social engineering
  - First look at interventions and advice giving
  - Giving users advice
- Warnings and advice measuring impact of interventions
  - Models of warning perception
  - Giving actionable and understandable advice
  - Qualitative analysis basics
- Developers and administrators working with expert users
  - Special examples of expert users who still need usability support
  - Working with security professionals
  - Balancing stakeholder needs

Texts / Materials

Title / Name	Notes / Comments	Required
Garfinkel S, Lipford HR. Usable Security: History, Themes, and Challenges. Morgan & Claypool Publishers; 2014.	Library copy: https://ocul wtl.primo.exlibrisgroup.com/permalink/01OCUL_WTL/vk29fk/alma9950695083505162	No

Reading materials will be provided throughout the course. The linked textbook is the most recent one on the subject, but it is rather old. So assigned reading will be research papers, policy documents, and some news articles.

Student Assessment

Component	Value
Assignments	30%
Midterm	30%
Final	40%

Assignment Screening

No assignment screening will be used in this course.

Notice of Recording

Short Version

Lecture recordings may be used in the course so that students who cannot attend or who want to revise lecture content can do so. Recordings will happen at the discretion of the Instructor and not all lectures or content are guaranteed to be recorded. Recordings will focus on the Instructor and not the students, however, students asking questions may have their voice recorded. If at any time you would like the recording paused, you may ask the instructor to do so. You may also notify the instructor after class or via email that you would like a question you asked removed from the recording. Such requests will be honored if possible. Recordings that include audio from students will only be accessible to the members of the course. Recordings with student audio removed may be made more widely available.

Official Policy

Activities for this course involve recording, in partial fulfillment of the course learning outcomes. You will receive notification of recording via at least one of the following mechanisms: within the Learning Management System (LEARN), a message from your course instructor, course syllabus/website, or other means. Some technologies may also provide a recording indicator. Images, and audio that have been recorded may be used and/or made available by the University to course students for the purpose of lecture review. Recordings will be managed according to the University records classification scheme, WatClass (https://uwaterloo.ca/records_management/records_classification_and_retention-schedules) , and will be securely destroyed when no longer needed by the University. Your personal information is protected in accordance with the Freedom of Information and Protection of Privacy Act (https://www.ontario.ca/laws/statute/90f31) , as well as University policies and guidelines (https://uwaterloo.ca/privacy/) and may be subject to disclosure where required by law.

The University will use reasonable means to protect the security and confidentiality of the recorded information, but cannot provide a guarantee of such due to factors beyond the University's control, such as recordings being forwarded, copied, intercepted, circulated, disclosed, or stored without the University's knowledge or permission or the introduction of malware into computer system which could potentially damage or disrupt the computer, networks, and security settings. The University is not responsible for connectivity/technical difficulties or loss of data associated with your hardware, software or Internet connection.

By engaging in course activities that involve recording, you are consenting to the use of your appearance, image, text/chat messaging, and voice and/or likeness in the manner and under the conditions specified herein. (In the case of a live stream event, if you choose not to have your image or audio recorded, you may disable the audio and video functionality (https://uwaterloo.ca/student-it-services/) . Instructions to participate using a pseudonym instead of your real name are included where the feature exists; however, you must disclose the pseudonym to your instructor in advance in order to facilitate class participation.) If you choose not to be recorded, this notice serves as confirmation of your understanding that the instructor will attempt to remove recording elements involving your likeness or voice, however, doing so for hard-to-hear background sounds may be impossible.

You are not permitted to disclose the link to/URL of an event or an event session recording or copies of recording to anyone, for any reason. Recordings are available only to authorized individuals who have been directly provided the above instructions/link for their use. Recordings for personal use, required to facilitate your learning and preparation of personal course/lecture notes, should not be shared with others without the permission of the instructor or event coordinator. Review the University's guidelines for faculty, staff and students entering relationships with external organizations offering access to course materials (https://uwaterloo.ca/secretariat/faculty-staff-and-students-entering-relationships_external) for more information on your obligations with respect to keeping copies of course materials. For more information about accessibility, connect with AccessAbility Services (https://uwaterloo.ca/accessability-services/) .

Administrative Policy

Generative AI

Generative artificial intelligence (GenAI) trained using large language models (LLM) or other methods to produce text, images, music, or code, like Chat GPT, DALL-E, or GitHub CoPilot, may be used in this course with proper documentation, citation, and acknowledgement. Permitted uses of and expectations for using GenAI will discussed in class and outlined on assignment instructions.

Recommendations for how to cite generative AI in student work at the University of Waterloo may be found through the Library: https://subjectguides.uwaterloo.ca/chatgpt_generative_ai (https://subjectguides.uwaterloo.ca/chatgpt_generative_ai) . Please be aware that generative AI is known to falsify references to other work and may fabricate facts and inaccurately express ideas. GenAI generates content based on the input of other human authors and may therefore contain inaccuracies or reflect biases.

In addition, you should be aware that the legal/copyright status of generative AI inputs and outputs is unclear. Exercise caution when using large portions of content from AI sources, especially images. More information is available from the Copyright Advisory Committee: https://uwaterloo.ca/copyright-at-waterloo/teaching/generative-artificial-intelligence (https://uwaterloo.ca/copyright at waterloo/teaching/generative artificial intelligence)

You are accountable for the content and accuracy of all work you submit in this class, including any supported by generative AI.

Faculty of Engineering Guiding Practices

Territorial Acknowledgement: The University of Waterloo acknowledges that much of our work takes place on the traditional territory of the Neutral, Anishinaabeg and Haudenosaunee peoples. Our main campus is situated on the Haldimand Tract, the land granted to the Six Nations that includes six miles on each side of the Grand River. Our active work toward reconciliation takes place across our campuses through research, learning, teaching, and community building, and is centralized within the Office of Indigenous Relations (https://uwaterloo.ca/indigenous) .

Inclusive Teaching Learning Spaces: The University of Waterloo values the diverse and intersectional identities of its students, faculty, and staff. The University regards equity and diversity as an integral part of academic excellence and is committed to accessibility for all. We consider our classrooms, online learning, and community spaces to be places where we all will be treated with respect, dignity, and consideration. We welcome individuals of all ages, backgrounds, beliefs, ethnicities, genders, gender identities, gender expressions, national origins, religious affiliations, sexual orientations, ability – and other visible and nonvisible differences. We are all expected to contribute to a respectful, welcoming, and inclusive teaching learning environment. Any member of the campus community who has experienced discrimination at the University is encouraged to seek guidance from the Office of Equity, Diversity, Inclusion & Anti racism (EDI R) (https://uwaterloo.ca/equity diversity inclusion anti racism/) via email at equity@uwaterloo.ca (mailto:equity@uwaterloo.ca) . Sexual Violence Prevention & Response Office (SVPRO) (https://uwaterloo.ca/sexual violence prevention response office) , supports students at UWaterloo who have experienced, or have been impacted by, sexual violence and gender-based violence. This includes those who experienced harm, those who are supporting others who experienced harm. SVPRO can be contacted at svpro@uwaterloo.ca (mailto:svpro@uwaterloo.ca)

Religious & Spiritual Observances: The University of Waterloo has a duty to accommodate religious and spiritual observances under the Ontario Human Rights Code. Please inform the instructor at the beginning of term if special accommodation needs to be made for religious observances that are not otherwise accounted for in the scheduling of classes and assignments. Consult with your instructor(s) within two weeks of the announcement of the due date for which accommodation is being sought.

Respectful Communication and Pronouns: Communications with Instructor(s) and teaching assistants (TAs) should be through recommended channels for the course (e.g., email, LEARN, Piazza, Teams, etc.) Please use your UWaterloo email address. Include an academic signature with your full name, program, student ID. We encourage you to include your pronouns to facilitate respectful communication (e.g., he/him; she/her; they/them). You can update your chosen/preferred name at WatIAM. (https://idm.uwaterloo.ca/watiam/) You can update your pronouns in Quest (https://uwaterloo.ca/quest/help/students/how-do-i/view-or-update-my-personal-information) .

Mental Health and Wellbeing Resources: If you are facing challenges impacting one or more courses, contact your academic advisor, Associate Chair Undergraduate, or the Director of your academic program. Mental health is a serious issue for everyone and can affect your ability to do your best work. We encourage you to seek out mental health and wellbeing support when needed. The Faculty of Engineering Wellness (https://uwaterloo.ca/engineering wellness program/) Program (https://uwaterloo.ca/engineering-wellness-program/) has programming and resources for undergraduate students. For counselling (individual or group) reach out to Campus Wellness and Counselling Services. (https://uwaterloo.ca/campus-wellness/counselling-services) Counselling Services is an inclusive, non-judgmental, and confidential space for anyone to seek support. They offer confidential counselling for a variety of areas including anxiety, stress management, depression, grief, substance use, sexuality, relationship issues, and much more.

Intellectual Property: 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 and academic integrity.

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.

Continuity Plan - Fair Contingencies for Unforeseen Circumstances (e.g., resurgence of COVID-19): In the event of emergencies or highly unusual circumstances, the instructor will collaborate with the Department/Faculty to find reasonable and fair solutions that respect rights and workloads of students, staff, and faculty. This may include modifying content delivery, course topics and/or assessments and/or weight and/or deadlines with due and fair notice to students. Substantial changes after the first week of classes require the approval of the Associate Dean, Undergraduate Studies.

Declaring absences: [*undergraduate students and/or courses only*] Regardless of the process used to declare an absence, students are responsible for reaching out to their instructors as soon as possible. The course instructor will determine how missed course components are accommodated. Self-declared absences (for COVID-19 and short-term absences up to 2 days) must be submitted through Quest (https://uwaterloo.ca/quest/help/students/how_do_i/self_declare-absence-undergraduate-students) . Absences requiring documentation (e.g., Verification of Illness Form, bereavement, etc.) are to be uploaded by completing the form on the VIF System (https://vif.uwaterloo.ca/) . The UWaterloo Verification of Illness form (https://uwaterloo.ca/campus-wellness/health-services/student-medical-clinic/verification_illness_services) , completed by a health professional, is the only acceptable documentation for an absence due to illness. Do not send documentation to your advisor, course instructor, teaching assistant, or lab coordinator. Submission through the VIF System, once approved, will notify your instructors of your absence.

Rescheduling Co-op Interviews: Follow the co-op process for rescheduling co-op interviews (https://uwaterloo.ca/co-operative_education/find_your_co_op_job/find_job_waterlooworks/interview/interview_conflicts) for conflicts to graded assignments (e.g., midterms, tests, and final exams). Attendance at co-operative work-term employment interviews is not considered to be a valid reason to miss a test.

University Policy

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 the Office of Academic Integrity (https://uwaterloo.ca/academic_integrity/) for more information.]

Grievance: A student who believes that a decision affecting some aspect of their university life has been unfair or unreasonable may have grounds for initiating a grievance. Read Policy 70, Student Petitions and Grievances, Section 4 (https://uwaterloo.ca/secretariat/policies-procedures-guidelines/policy-70) . 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 to avoid committing an academic offence, and to take responsibility for their actions. [Check the Office of Academic Integrity (https://uwaterloo.ca/academic-integrity/) for more information.] 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 (https://uwaterloo.ca/secretariat/policies-procedures-guidelines/policy-71) . For typical penalties, check Guidelines for the Assessment of Penalties (https://uwaterloo.ca/secretariat/guidelines/guidelines_assessment_penalties) .

Appeals: A decision made or penalty imposed under Policy 70, Student Petitions and Grievances (https://uwaterloo.ca/secretariat/policies_procedures_guidelines/policy_70) (other than a petition) or Policy 71, Student Discipline (https://uwaterloo.ca/secretariat/policies-procedures-guidelines/policy-71) may be appealed if there is a ground. A student who believes they have a ground for an appeal should refer to Policy 72, Student Appeals (https://uwaterloo.ca/secretariat/policies-procedures-guidelines/policy-72) .

Note for students with disabilities: AccessAbility Services (https://uwaterloo.ca/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.

Turnitin.com: Text matching software (Turnitin®) may be used to screen assignments in this course. Turnitin® is used to verify that all materials and sources in assignments are documented. Students' submissions are stored on a U.S. server, therefore students must be given an alternative (e.g., scaffolded assignment or annotated bibliography), if they are concerned about their privacy and/or security. Students will be given due notice, in the first week of the term and/or at the time assignment details are provided, about arrangements and alternatives for the use of Turnitin in this course.

It is the responsibility of the student to notify the instructor if they, in the first week of term or at the time assignment details are provided, wish to submit alternate assignment.