CS 458/658 (W23)

Syllabus

TABLE OF CONTENTS

This syllabus is a guideline for the course and not a contract. As such, its terms may be altered when doing so is, in the opinion of the instructor(s), in the best interests of the class.

Overview

This course provides an introduction to security and privacy issues in various aspects of computing, including programs, operating systems, networks, databases, and Internet applications. It examines causes of security and privacy breaches, and presents methods to help either find and prevent them or reducing the damages.

Students completing this course should be better able to produce programs that can defend against active attacks, and not just against random bugs.

Intended audience

Third or fourth year CS students (CS 458), or first year CS graduate students (CS 658)

Prerequisites

CS 350 (Operating Systems). Familiarity with C.

Course outline

1. Introduction to Computer Security and Privacy *[Instructor: Yousra Aafer]*
    - The meaning of computer security; comparing security with privacy; types of threats and attacks; methods of defense
2. Program Security *[Instructor: Yousra Aafer]*
    - Secure programs; non-malicious program errors; malicious code; controls against program threats
3. Operating System Security *[Instructor: Yousra Aafer]*
    - Methods of protection; access control; user authentication
4. Network Security *[Instructor: Yousra Aafer]*
    - Network threats; firewalls, intrusion detection systems
5. Internet Application Security and Privacy *[Instructor: Meng Xu]*
    - Basics of cryptography; security and privacy for Internet applications (email, instant messaging, web browsing); privacy-enhancing technologies, blockchain security
6. Data Security and Privacy *[Instructor: Meng Xu]*
    - Security and privacy requirements; reliability, integrity, and privacy; inference; data mining; k-anonymity, attacks on ML models or data poisoning
7. Non-technical Aspects *[Instructor: Meng Xu]*
    - Administration of security systems; policies; physical security; economics of security; legal and ethical issues

Grading policies

Score composition

Grades will be calculated as follows for undergraduate students (i.e., students taking CS 458):

- self-tests (8%)
- assignment 1: (23%)
- assignment 2: (23%)
- assignment 3: (23%)
- final assessment: (23%)

For graduate students taking CS 658, 80% of your grade will be computed through the above distribution. The research survey paper will account for the remaining 20% of your overall mark, as discussed below.

Please consult the course weekly schedule or LEARN for the assessment deadlines.

Assignment details

Course assignments: The three assignments contain both written and programming exercises and cover the new material in the course since the previous assignment.

Please start working on the assignments in advance of the deadlines. To motivate you to do so, we may require you to submit milestones for some or all of them.

Late submissions for 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, and the last one will be used for marking. Course personnel will not normally give assistance for assignments after their original due dates.

NOTE: **The 48 hours grace period does not apply** to the due dates for the self-tests, the final assessment, or the CS 658 proposal and research survey paper; no lates will be accepted for them.

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.

Assignments 1, 2, and 3 and their respective milestones are due at **3:00 pm Eastern Time** on their respective due dates. These assignments are to be submitted electronically with the "submit" command. Assignments submitted by other means will not be accepted.

Marks and comments for Assignment 1, 2 and 3 will be returned using infodist. See the course mechanics section below on how to access infodist.

Final assessment: The final assessment will be administered **on campus** in accordance with University policies. The exact date and time of the final exam is yet to be scheduled by the

Registrar office, we will update the syllabus once we receive more details.

The final assessment is written-only and covers material from the whole term. You have **2 hours and 30 minutes** to complete the set of questions. We will post more details about the logistics of the final assessment as we approach the end of the term. Note that if your score in the final assessment is below 50%, you cannot pass the course.

If you anticipate a problem with taking the final assessment, contact the course instructors **as early as possible**. In order to receive accommodation for the final assessment, you must obtain a Verification of Illness Form that has been filled out by a physician. If the final assessment is already written, no special action will be taken if you decide afterward that you did not do a good job due to illness.

If you are unable to write the final assessment due to illness, you should seek medical treatment and provide confirmation of the illness to the instructors **within 48 hours** by submitting a completed Verification of Illness Form to support your request. The Verification of Illness Form is normally the only acceptable medical documentation and is available online. You will receive an `INC` (incomplete) grade and you need to write the final assessment in a subsequent term in order to complete the course.

Self-tests: Self-tests are meant to help you keep up with the material, that is, to assess and improve your understanding of basic concepts. You can attempt each self-test as often as you like during its availability period; your last grade on each self-test will be the one recorded (although course personnel can see every attempt).

Each self-test corresponds to a module covered in the course outline. The availability and deadline information are posted in the course weekly schedule as well as will be available on LEARN. Late self-tests cannot be made up for **any** reason, including students signing up for the class late. (Students who join the class on or after the due date of the first self-test will instead be excused from that particular self-test.) Again, **the 48 hours grace period does not apply** to the due dates for the self-tests.

Research survey paper (CS 658): Students registered in CS 658 must write a research survey paper on a topic related to computer security or privacy. You should read Keshav's How to Read a Paper to *efficiently* read a paper and conduct a literature survey. In writing your paper, you must become familiar with the research literature relevant to your topic. Your focus should be on academic venues, such as the USENIX Security Symposium, ACM CCS, IEEE Symposium on Security and Privacy, Privacy Enhancing Technologies Symposium (PETS), and NDSS Symposium. Visit LEARN for a sample paper and deadlines for the proposal and paper. You should email your topic, proposal and paper to the instructors before the start of the reading week.

- **Topic approval:** Your topic must be approved in advance by the instructors before you submit your proposal.
- **Proposal:** Your proposal should be one page in length and include at least 10 references, preferably including (but not limited to) papers from the aforementioned venues. It is recommended but not required that you discuss the proposal with the instructors first.
- **Paper:** Your paper should be a summary of past and current work on your topic, as well as an overview of known open problems and potential future directions in the area. You should provide a concise summary of work, emphasizing major accomplishments, rather than a detailed accounting of individual pieces of research activity.
- **Format:** Your proposal and paper should be formatted in the two-column ACM proceedings format, using one of the ACM SIG Proceedings Templates. Your paper should not be longer than six pages. The ACM templates include headings for "Categories and Subject Descriptors," "General Terms," and "Keywords", which you do not need to use.

Late submissions

- Late submissions for Assignments 1, 2, or 3 (including their respective milestones), will be accepted **only up to 48 hours after the original due date**. There is no penalty for accepted late submissions.
- The 48 hours grace period **does not apply** to any other assessments, including the self-tests, the final assessment, and the CS 658 proposal and research survey paper no late submissions will be accepted for them.
- Course personnel will not normally give assistance for assignments after their original due dates.
- There will be no assistance from course staff for the final assessment.
- 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.
- Assignments 1, 2, and 3 can be submitted multiple times – the last submission will be used for marking.

Reappraisal policy

If you have an assignment that you would like to have reappraised, please follow the instructions given on Piazza to submit your request. Include a clear justification for your claims. The appeals deadline is **one week** after the respective graded item is first made available. If your appeal is concerned with a simple calculation error, please see the TA(s) during their office hours.

For students auditing this course

Students who are auditing this course are encouraged to complete all assignments similar to grade-seeking students. To pass this course in auditing, the minimal requirements are

- completing all self-tests (one for each module) **AND**
- scoring at least 80% in *each* self-test.

Textbook and other resources

The textbooks for this course include:

- **Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin** (2nd Edition) by *Paul C. van Oorschot*. Springer, 2021. ISBN: 978-3-030-83410-4 (hardcopy), 978-3-030-83411-1 (eBook). This text book is freely available for download from the author's web page.

- **Security in Computing** (5th Edition) by *Charles P. Pfleeger, Shari Lawrence Pfleeger, and Jonathan Margulies*. Prentice-Hall, 2015. ISBN: 0-13-408504-3. Link to book information.

Additional readings will be assigned, and will appear on the course website; readings marked as mandatory contain required material for the course. You must read these mandatory readings; those marked **before class** must be read before the date of the corresponding lecture.

Other resources for this course include:

- Schneier on Security: A blog covering current computer security and privacy issues.
- The RISKS Digest: A forum on risks to the public in computers and related systems.
- BugTraq: A full disclosure moderated mailing list for the detailed discussion and announcement of computer security vulnerabilities.
- Freedom To Tinker: A blog which often discusses security and privacy issues, frequently related to copyright and to electronic voting.
- Threat Level: A forum dedicated to privacy, crime and security online.

Course mechanics

- **Working remotely**: The CSCF offers a help page regarding CS and campus VPNs.
- **Linux account**: If you do not have a `linux.student.cs` account for some reason, ask CSCF helpdesk for help. If you need to reset your password see CSCF account help.
- **submit command**: We will be using the `submit` command to submit assignments 1, 2 and 3. You may consult this CSCF submit page. You should make sure early on that the `submit` command works for them. You should check whether their submitted files correspond to the ones that they intend to submit using the `-print` option of the `submit` command. We may run submissions through MOSS to detect code similarity.

Communication

It is your responsibility to keep up with all course-related information posted to LEARN, Piazza, and the course website.

- **Piazza**: Please direct all communication to the discussion forums to Piazza. This includes questions on materials in lectures, assignments, and general logistics. Bear in mind with the following etiquette when communicating on Piazza:
  - Please go through your peers' and the instructors/TAs' notes or comments, before posting a question.
  - If question doesn't exist and it involves private content (query about grades, partial progress towards solution), create a private question that is only visible to the instructors and TAs. (The instructor(s) or TAs may make a private question public, possibly after editing it, if they decide that it is of general interest.) Otherwise, in general, create a public post so that your peers can benefit from the answers/comments too.
  - Tag your question with the appropriate folder for the assignment etc.
- **Email**: Important course information will generally be posted to LEARN, but may also be sent to your `uwaterloo.ca` email address. For personal matters, such as an illness, please email the instructors directly. We will only reply back to email from your `uwaterloo.ca` email address, for privacy rules.

Teaching with COVID-19 considerations

Because we cannot predict what COVID will do and how the university will react, we are making the course lectures available remotely the whole term; You will not be required to be in any particular place to attend the lectures or the office hours.

Lecture content will be both livestreamed and recorded so as to not encourage anyone to come to class while potentially sick. If you are participating online, **we encourage you to participate synchronously** (joining the Bongo room live, as opposed to watching the recordings later).

The only exception is the final exam: the final will be in-person, as per the Math faculty guidelines.

We hope this added flexibility will avoid us having to make major changes in how the course is offered in the middle of the term, and will help keep everyone safe as COVID variants emerge.

Highlighted university policies

Security information

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. In particular, you will comply with all applicable laws and UW policies, including, but not limited to, the following:

- UW Policy 33, Ethical Behaviour
- Guidelines on Use of UW Computing and Network Resources
- Examples Reflecting the Application of the above Guidelines
- MFCF Account Usage Policy
- CSCF-Specific Policies

Violations will be treated severely, and with zero tolerance.

Academic integrity

Students are encouraged to talk to one another, to the TAs, to the instructor(s), or to anyone else about any of the assignments. Any assistance, though, must be limited to discussion of the problem and sketching general approaches to a solution. Each student must write his or her own solutions, including code and documentation if appropriate, for the assignments. Consulting another student's solution is prohibited, and submitted solutions may not be copied from any source. In particular, submitting assignments copied in whole or in part from assignment submissions to a previous offering of this course, or from any offering of any other course, is forbidden, *even if a student is resubmitting his or her own work*. These and any other forms of collaboration on assignments constitute cheating. If you have any questions about whether some activity constitutes cheating, please ask the instructor(s).

The general Faculty and 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's website 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, to avoid committing academic offenses, and to take responsibility for his/her actions. A student who is unsure whether an action constitutes an offense, or who needs help in learning how to avoid offenses (e.g., plagiarism, cheating) or about "rules" for group work/collaboration

should seek guidance from the course professor, academic advisor, or the Undergraduate Associate Dean. For information on categories of offenses and types of penalties, students should refer to Policy 71 — Student Discipline. For typical penalties, check Guidelines for the Assessment of Penalties.

- **Avoiding academic offenses**: Most students are unaware of the line between acceptable and unacceptable academic behaviour, especially when discussing assignments with classmates and using the work of other students. For information on commonly misunderstood academic offenses and how to avoid them, students should refer to the Faculty of Mathematics Cheating and Student Academic Discipline Policy.
- **Appeals**: A decision made or a 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.

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.

Note for Students with Disabilities: AccessAbility Services, located in Needles Hall North, 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 at the beginning of each academic term.

Mental health support

The Faculty of Math encourages students to seek out mental health support if needed.

On-campus Resources:

- Campus Wellness
- Counselling Services: email or 519-888-4567 ext 32655
- MATES: one-to-one peer support program offered by Federation of Students (FEDS) and Counselling Services: email
- Health Services: located across the creek from the Student Life Centre, 519-888-4096

Off-campus Resources:

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

Territorial acknowledgement

We acknowledge that we live and work on the traditional territory of the Attawandaron (Neutral), Anishinaabeg, and Haudenosaunee peoples. The University of Waterloo is situated on the Haldimand Tract, the land promised to the Six Nations that includes ten kilometres on each side of the Grand River.