# ECE 458 - Computer Security (Online)

Spring 2021

| | | | |
|---|---|---|---|
| **Instructor:** | Behkish Nassirzadeh | **Time:** | M & F 11:30 – 13:00 |
| **Email:** | bnassirz@uwaterloo.ca | **Place:** | Online (Hybrid Mode) |

**Webpage:** UW-LEARN ( learn.uwaterloo.ca )

**Course Description:** This is an introductory course for computer security. The course will cover the topics of models of security, elementary cryptography, software security, vulnerabilities, threats, defenses and secure-software development processes, threats to networks and defenses, Security issues at the application layer, Secure design principles, techniques and security evaluation. Privacy, ethics and legal issues.

**Objectives:** A primary objective of this course is that the student should gain wide-ranging knowledge of many aspects of computer security and think adversarially about computer systems.

**Prerequisites:** ECE 252 or SE 350; Level at least 4A Computer Engineering or Electrical Engineering or Software Engineering

**Antirequisites:** CS 458

**Course Outline:**

1. Introduction to Security and Cryptography
2. Symmetric Key Encryption
3. Public Key Encryption
4. Cryptographic Hash Functions
5. Hybrid Encryption and Digital Signatures
6. Blockchain
7. Side Channel Attacks
8. Physical Security - Fault Attacks
9. Web Security
10. Secure Design Principles
11. Buffer Overflow Attacks

**Teaching Assistants:**

- Mohammadtaghi Badakhshan, mbadakhshan@uwaterloo.ca
- Aliasghar Iman, aiman@uwaterloo.ca

**Main References:** In addition to the course slides (which will be posted on LEARN), there will be some assigned readings (online articles, news, blogs, etc.) as well as several academic papers.

There is **NO required textbook.** If you want additional reading:

- C. Pfleeger, S. Pfleeger, and J. Margulies, Security in Computing, 5th edition, Prentice Hall, 2015. ISBN: 0134085043.
- W. Stallings and L. Brown, Computer Security: Principles and Practice, 4th edition, Pearson, 2017. ISBN: 0134794109.
- S. Smith and J. Marchesini, The Craft of System Security, Pearson, Addison Wisely, 2007. ISBN: 9780321434838.
- S. Mcclure, J. Scambray, G. Kurtz Hacking Exposed, 7th edition, McGraw-Hill Osborne, 2012. ISBN: 0071780289.

**Course Logistic:**

- The lectures will be in asynchronous and synchronous (hybrid) mode. Each lecture is provided by a video a week in advance. The Monday sessions will be used for live Q/As and extra explanations for the lecture materials. Friday sessions will be used for info sessions for the assignments, demos and extra contents.
- In addition to the live sessions, you can also use Piazza for discussions on course-related questions and comments. Find our class page at: http://piazza.com/uwaterloo.ca/spring2021/ece458
- All the course materials and extra resources will be available on Learn.
- There are no office hours due to covid-19. However, we can set up an online meeting if needed. Please send me an email to arrange the online meeting.

**Grading Policy:**

- 3 Assignments (30% total). Done in groups of 2
- A midterm exam (20%)
- A comprehensive open book final exam (50%)

**Important Dates:**

Assignment #1 ..... June 2, 2021
Assignment #2 ..... July 7, 2021
Assignment #3 ..... July 28, 2021
Midterm ..... June 21, 2021 (Tentative)
Final Exam ..... Will be announced

**Other Resources:**

- Prof. Ganesh's slides, https://ece.uwaterloo.ca/ vganesh/TEACHING/S2014/ECE458/index.html
- Schneier on Security, http://www.schneier.com/blog/. A blog covering current computer security and privacy issues.

- Kevin Du, Seed Labs, University of Syracuse, https://seedsecuritylabs.org/lab_env.
- BugTraq, http://www.securityfocus.com/archive/1.

**Due dates and Deadline policies:** Assignments will be posted through LEARN; it is each student's responsibility to regularly check the course page on LEARN for posted assignments, new material, announcements, etc. Missing any announcements about posted assignments does NOT constitute justification for submitting late or missing an assignment.

If a student misses any deadline or exam, he or she would receive a grade of 0 for the missed evaluation item, except in cases of a medical emergency, some documented medical condition, or any other emergency case that justifies the incident. In all cases,any medical incident must be accompanied by the proper documentation, as per Department policy and protocols.

In those cases of justified situations, the following rules apply:

(1) If the missed item is the midterm, then the grade assigned for the midterm is the same grade obtained in the final.

(2) If the missed item is the final exam, then the student should contact me as soon as possible to arrange an alternative

(3) If the missed item is an assignment, either the other group member carries that assignment if he/she agrees or the grade assigned to that assignment would be the average of the grades of the remaining (submitted) assignments. In this case, the student and the other group member should contact me as soon as possible.

**Course Policy:** In the (hopefully unlikely) event of any student(s) discovered in an incident of academic dishonesty, every student involved will receive a grade of 0 (zero) for the corresponding evaluation item, and additionally will receive a deduction of 5 (five) marks from the final grade of the course as a standard penalty. Additionally, the student(s) will be reported to the Associate Dean of Undergraduate Studies, who may impose additional penalties (see information on Academic Integrity). In cases where the incident consists of submitting common work, every student involved will be subject to the above penalty. No student will be allowed to take full responsibility, regardless of who copied and who is the genuine author of the work submitted; and regardless of the actions by the students involved or related events that led to the incident. The rule is unconditional. All of the above applies to multiple instances—a student caught in several incidents of academic dishonesty will be subject to the above penalties for each of the incidents.

**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. [ For more information and details, please visit https://uwaterloo.ca/academic-integrity/ ]

**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. For related information, see https://uwaterloo.ca/secretariat-general-counsel/policies-procedures-guidelines/policy-70 (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.

**Turnitin.com and MOSS:** Text matching software (Turnitin and/or MOSS) may be used to screen assignments in this course.Turnitin is used to verify that all materials and sources in assignments are documented. In the case of Turnitin, student submissions are stored on a U.S. server. Therefore students must be given an alternative. You should contact me as soon as possible if you need an alternative, and we will arrange that.