ECE 458 - Computer Security, Spring 2022

Instructor: Professor G. Gong
Office: E7 5436, x45650, ggong@uwaterloo.ca
https://uwaterloo.ca/scholar/ggong
Office hours: TBD

Webpage: UW-LEARN

Course Description This is an introductory course for computer security. The course will consist of five modules and cover the topics of models of security, attacks on program and operation system, practical cryptography, threats to networks and wireless system, web security, secure design principles, evaluation, privacy, and applications.

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 254 or SE 350; Level at least 4A Computer Engineering or Electrical Engineering or Software Engineering.

Antirequisites CS 458.

Resources

Lectures:	10:00-11:25MF	E7 4043
Tutorials:	07:00(pm)-07:50(pm)W	E7 4043

Textbooks and References

- There is **NO** required text book. 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.
- Lecture Notes: Available on UW-LEARN.
- Some revised contents for the book, *Communication System Security*, CRC, 2012, by L.D. Chen and G. Gong, will be provided.
- Some additional links for reading will be provided.

Course Outline

1. Basics of Security
   - Confidentiality, integrity and availability
   - Trust and threat model
   - Program security
   - Malicious code - Malware
   - Trusted platform
   - Memory security
2. Practical Cryptography
   - Pseudorandom generation
   - Symmetric-key cryptography
   - Public-key cryptography and digital signature
   - Hash chain based authentication and applications (blockchain)
3. Network and Wireless Security
   - Basics of network security
   - Security protocols (TLS/SSL) and attacks on TLS
   - Firewalls and VPN
   - Security of IEEE 802.11 and 4G-LTE/5G
   - Attacks on wireless link (jamming and location services)
4. Web Security
   - HTTPS, sessions and cookies
   - Privacy attacks
   - Attacks on clients and servers
   - Email security
   - Password based authentication
   - Multi-factor authentication and passwordless authentication
   - Kerberos and open-authorization
5. Applications
   - Securing IoT
   - Security and privacy of RFIDs
   - Privacy preserving machine learning

Tutorial Description The tutorials will be conducted by TAs, which are aimed for questions and answers on material covered in lectures and homework assignments, and problem solving skills.

Teaching Assistants

- Radi Abubaker, rabubaker@uwaterloo.ca
- Guiwen Luo, g27luo@uwaterloo.ca
- Yiqin Huang, yiqin.huang@uwaterloo.ca

Course Grading

- Five homework assignments (35% total).
- One course project (20%). Done individually or in groups of 2.
- A final exam (close book) (45%).

The due dates (all will be 11:59am ET) and the distribution of the marks are given below.

Tasks	Due Dates	Marks
Assignment 1	May 18	8
Assignment 2	June 1	8
Project	June 18	20
Assignment 3	June 29	7
Assignment 4	July 13	8
Assignment 5	July 27	4
Final Examination	TBD	45

Other Resources

- 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.html`. The lab contains many hand-on experiments and some crafted attacks can be launched under their specific environment for better understanding them.
- BugTraq, `http://www.securityfocus.com/archive/1`. A full disclosure moderated mailing list for the detailed discussion and announcement of computer security vulnerabilities.

In-person classroom safety If you are uncomfortable attending in-person lectures and tutorials in any way, please do not attend in-person lectures and tutorials. We will follow all university guidelines. In addition, if I feel there is a safety issue, I reserve the right to cancel the lecture immediately, and ask everyone to leave. If a lecture is cancelled because someone makes the lecture room unsafe, the issue may be raised with the associate dean of undergraduate studies under Policy 71.

A safety presentation is available on the Learn website. Please review the presentation.

- Students shall not attend class if they are experiencing influenza-like illness, have been in close contact with someone who is ill, or have travelled outside of Canada within the past 14 days.
- Wearing of face-covering/mask is a requirement in all common areas on campus, including all indoor instructional spaces.
- As such, no food is allowed to be consumed in instructional space. Beverages are allowed if a straw is used or if the mask is lowered only for a brief period.
- When a student asks or answers a question it may be difficult to be heard while wearing a mask. A student may briefly lower their mask to ask/answer the question and then the mask must be replaced.
- Students are expected to practice frequent hand hygiene (handwashing with soap and water or use of hand sanitizer), including immediately before coming into an instructional space
- Students are permitted to sit where they wish. You are encouraged to sit with one seat left empty between you and other students when possible. Also, please be considerate – the person next to you may want some distance as well.
- If you becomes ill in class: i) please proceed directly home to self-isolate and to contact Health Services' Testing and Assessment Centre to book an appointment for testing, ii) you will be directed on self-isolate and are asked to report a positive test to Health Services via the COVID-19 Support and Advice form:

  `https://uwaterloo.ca/campus-wellness/covid-19-testing-assessment-centre/`covid-19-support-and-advice
- If you have tested positive for COVID-19: i) report the positive result to Health Services via the COVID-19 Support and Advice form below, ii) staff managing the form submissions will guide you through next steps and co-ordinate tracking the case and initiating Public Health contact tracing.
- COVID-19 Return to Campus safety information and protocols: `https://uwaterloo.ca/coronavirus/return`

Academic Integrity, Discipline, Grievances, and Appeals

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 `www.uwaterloo.ca/academicintegrity/` 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, `www.adm.uwaterloo.ca/infosec/Policies/policy70.htm`. When in doubt please be certain to contact the departments administrative assistant who will provide further assistance.

Discipline: A student is expected to know what constitutes academic integrity [check `www.uwaterloo.ca/academicintegrity/`] 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, `www.adm.uwaterloo.ca/infosec/Policies/policy71.htm`. For typical penalties check Guidelines for the Assessment of Penalties, `www.adm.uwaterloo.ca/infosec/guidelines/penaltyguidelines.htm`.

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) `www.adm.uwaterloo.ca/infosec/Policies/policy72.htm`.

Note for Students with Disabilities: The Office for Persons with Disabilities (OPD), located in Needles Hall, Room 1132, 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 the OPD at the beginning of each academic term [check `http://www.studentservices.uwaterloo.ca/disabilities/`].