Carleton University
School of Computer Science

Last updated: August 27, 2024 (preliminary version, subject to change)

COMP 5900H/4900K (FALL 2024, CSI 5140 IH00) TRUSTED COMPUTING AND EMERGING ATTACKS

GENERAL INFORMATION

Class time: 08:35-11:25, Wednesdays (Sep. 4 to Dec. 6, 2024)

Instructor: Lianying Zhao (firstname.lastname@scs.carleton.ca)

Location: Refer to the public class schedule (in-person)

Office hours: By appointment - via Brightspace (flexible), or HP5129 (Wed. only)

Course Website: Please use Brightspace as the primary source of information, where important instructions can be found that must be followed. Brightspace access for University of Ottawa Students: please see information here.

Prerequisites: Familiarity with computer architecture and operating system. Computer security, especially basic understanding of cryptography, is a plus but not mandatory. Otherwise, instructor permission is required.

For COMP4900K: COMP3000 with a minimum grade of C-

Teaching assistants: TA info will be posted once the course starts

COURSE DESCRIPTION

The course introduces the paradigm of trusted computing and its evolution over the past decade. Common trusted computing technologies are characterized and categorized. Their application in several academic proposals and industrial solutions is also explained. Alongside the discussion, the positioning of trusted computing is shown in a bigger picture and compared with other types of defenses/attacks. Recent (new) attack vectors concerning trustworthy program execution are also reviewed.

GRADING SCHEME

COMP5900H students:

15%: midterm test, **October 16th** (online, during class time, open-book)
based on posted lecture slides and class discussion

15%: assignment (paper survey), due **November 3rd**

25%: paper discussion lead (sign up for two papers by **September 22nd**: reading list)

In addition to "first come, first served", your chance to get a paper is also affected by topic popularity, so try to decide earlier. You can also propose papers to discuss with the instructor's approval.

Note: 10% is dedicated to the student's own original opinions about the discussed papers, including but not limited to criticisms, suggested improvements, limitations, and strengths. Regardless of the paper length, the same level of discussion depth is expected, so it is not the shorter the better.

30%: course project (individual work), report due **December 5th**

15%: participation (in-class, forum posts, emails, etc.)

COMP4900K students:

25%: midterm test, **October 16th** (online, during class time, open-book)

based on posted lecture slides and class discussion

30%: assignment (2/3 hands-on tasks, 15%/10% each), due **November 3rd**

30%: course project (group work, 2 - 3 students), report due **December 5th**

15%: participation (in-class, forum posts, emails, etc.)

Note: with instructor approval, COMP4900K students might be able to opt for the COMP5900H grading scheme until spots are filled.

Assignments and project reports submissions are handled electronically and there is no "grace period" with respect to a deadline - an assignment submitted even one minute after the deadline is late and subject to mark deductions.

Direct copy-paste of any content will be treated as plagiarism, regardless of whether the source of the content has been cited. The only exception is slides you use for presentations which you will not submit for credits (but reuse of public/existing material will lower your marks).

Everything you submit for evaluation (i.e., assignments, quizzes, tutorials, examinations, etc.) must be the result of your own work and only your own work. Unless it is explicitly stated otherwise, the use of any tools to generate material will be considered academic misconduct. This includes, but is not limited to, chatbots (e.g., ChatGPT, Google Bard, Bing Chart), research assistants (e.g., Elicit), and image generators (e.g., Stable Diffusion, Dall-E), etc. An exception to this rule is made for automated grammar and punctuation checking tools (such as Grammarly).

In case of any academic accommodation, email the instructor with the self-declaration form: https://carleton.ca/registrar/wp-content/uploads/self-declaration.pdf

TOPICS COVERED (TENTATIVE)

Important dates and deadlines can be found here, including class suspension for the fall break.

Papers corresponding to the topics are listed here and might be discussed (if at all) in a different order based on class progress. There will be lectures in the first few weeks in preparation for the midterm test.

- Introduction to trusted computing (TC)
- Trust
- Application of TC technologies
- Making TC technologies more adoptable/usable
- Side-channel attacks
- Internal misbehavior: memory attacks
- Human authenticating machine
- State continuity
- Secure input/output
- Proposed hardware improvements
- Proposals based on existing (non-security) hardware support

ADDITIONAL INFORMATION

For information about Carleton's academic year, including registration and withdrawal dates, see Carleton's Academic Calendar.

Undergraduate Academic Advisors. The Undergraduate Advisors for the School of Computer Science are available in Room 5302HP; or by email at scs.ug.advisor@cunet.carleton.ca. The undergraduate advisors can assist with information about prerequisites and preclusions, course substitutions/equivalencies, understanding your academic audit and the remaining requirements for graduation. The undergraduate advisors will also refer students to appropriate resources such as the Science Student Success Centre, Learning Support Services and Writing Tutorial Services.

Graduate Academic Advisors. The Graduate Advisors for the School of Computer Science are available in Room 5302 HP; or by email at grad.scs@carleton.ca. The graduate advisors can assist with understanding your academic audit and the remaining courses required to meet graduation requirements.

SCS Computer Laboratory. Students taking a COMP course can access the SCS computer labs. The lab schedule and location can be found at: https://carleton.ca/scs/tech-support/computer-laboratories/. All SCS computer lab and technical support information can be found at: https://carleton.ca/scs/tech-support/. Technical support staff may be contacted in-person or virtually, see this page for details: https://carleton.ca/scs/tech-support/contact-it-support/.

UNIVERSITY POLICIES

Academic Accommodations. Carleton is committed to providing academic accessibility for all individuals. Please review the academic accommodation available to students here: https://students.carleton.ca/course-outline/.

Student Academic Integrity Policy. Every student should be familiar with the Carleton University Student Academic Integrity policy. A student found in violation of academic integrity standards may be sanctioned with penalties which range from a reprimand to receiving a grade of F in the course, or even being suspended or expelled from the University. Examples of punishable offences include plagiarism and unauthorized collaboration. Any such reported offences will be reviewed by the office of the Dean of Science. More information on this policy may be found on the ODS Academic Integrity page: Academic Integrity | Faculty of Science (carleton.ca).

Plagiarism. As defined by Senate, "plagiarism is presenting, whether intentional or not, the ideas, expression of ideas or work of others as one's own". Such reported offences will be reviewed by the office of the Dean of Science. More information and standard sanction guidelines can be found here: https://science.carleton.ca/students/academic-integrity/. Please note that content generated by an unauthorized A.I.-based tool *is* considered plagiarized material.

Unauthorized Collaboration. Senate policy states that "to ensure fairness and equity in assessment of term work, students shall not co-operate or collaborate in the completion of an academic assignment, in whole or in part, when the instructor has indicated that the assignment is to be completed on an individual basis". Please refer to the instructions of a specific assignment and/or the instructor concerning this issue.