[preliminary version, subject to change]

COMP 5808F/4900K (Fall, 2026)

Trusted Computing and Emerging Attacks

Instructor: Lianying Zhao

Email: firstname.lastname@carleton.ca

Best Ways to be in Touch: in class, via email, or by appointment

Teaching Assistant: A list of teaching assistants and their contact/office hours information will be posted once the course starts.

Class Location: Please check Carleton Central for the room location

Class Time: 14:35 - 17:25, Mondays (Sep. 14 to Dec. 11, 2026)

Course Website: Please use Brightspace (link) as the primary source of information, where important instructions can be found that must be followed.

COMP5808F students only:

- Brightspace access for University of Ottawa Students; please see information here: https://gradstudents.carleton.ca/faculty-of-graduate-and-postdoctoral-affairs-access-to-brightspace/
- University of Ottawa Students who need access to SCS IT resources such, as OpenStack and Nextcloud, must submit a request to SCS Tech Support SCS.Tech.Support@cunet.carleton.ca. The request must be sent from their @cmail.carleton.ca email address and the email should say which resource is required and for which course (including section).

Important dates and deadlines can be found here: Dates, Deadlines, and Regulations—Registrar's Office, including class suspension for fall, winter breaks, and statutory holidays.

Course Calendar Description

A systematic discussion of current threats to code execution and the paradigm of employing hardware to achieve secure code execution. Topics include state-of-the-art security hardware support including trusted execution environments on various platforms/architectures, and applications of such hardware support to address various attack vectors.

Prerequisite(s) for COMP4900: COMP 3000 with a minimum grade of C-. SYSC 4001 may only be used as a prerequisite if taken prior to Fall 2025.

Prerequisite(s) for COMP5808: permission of the School of Computer Science

Prerequisite knowledge: 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.

[preliminary version, subject to change]

Topics Covered and Learning Outcomes

Students are not required to purchase textbooks or other learning materials for this course.

Detailed list of topics to be covered:

Week	Topic	Comment
1	Introduction to trusted computing (TC)	
2	Trust	
3	Application of TC technologies	
4	Making TC technologies more adoptable/usable	
5	Side-channel attacks	
6		Midterm test
7		Fall break
8	Internal misbehavior: memory attacks	
9	Human factors	
10	State continuity	
11	Secure input/output	
12	Proposed hardware improvements	
13	Proposals based on existing (non-security) hardware support	

Learning Outcomes: *By the end of this course, students will 1) have a systematic understanding of how a computer program in execution can be attacked/compromised (excluding network security factors) and the roles of hardware and software in terms of both defenses and attacks; 2) for COMP5808 students, gain a research mindset with improved academic writing and reading; and 3) for COMP4900 students, acquire hands-on skills for systems security which is also useful in non-security technical tasks.*
Note that, to be able to achieve these outcomes, students must come into this course with the aforementioned prerequisite knowledge/skills.

Calendar prerequisites are strictly enforced; this includes students writing deferred final exams. For details, see the SCS Prerequisite Policy: Prerequisites.

Assessment Scheme

Grade Breakdown for COMP 5808F students

COMPONENT	GRADE VALUE	DATE & NOTES
Midterm test	15 %	**October 19th** (during class time, in person, closed-book) based on posted **lecture slides** and **class discussion**
Assignment	15 %	paper survey, due **November 8th**

Paper discussion lead	25 %	sign up for two papers **ending with an (*)** by **September 27th**: reading list 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. The same level of discussion depth is expected regardless of paper length (not the shorter the easier).
Course project	30 %	report due **December 11th**, individual work grading based on: **written report + oral presentation**
Participation	15 %	class discussions, forum posts, emails, etc. must be about course topics, not logistics

Grade Breakdown for 4900K students

COMPONENT	**GRADE VALUE**	**DATE**
Midterm test	25 %	**October 19th** (during class time, in person, closed-book) based on posted **lecture slides** and **class discussion**
Assignment	30 %	due **November 8th** (2/3 hands-on tasks, 15%/10% each)
Course project	30 %	report due **December 11th**, group work of 2 or 3 grading based on: **written report + oral presentation**
Participation	15 %	class discussions, forum posts, emails, etc. must be about course topics, not logistics

Notes: Collaboration is only allowed for the designated group work and **prohibited** for all other assessment components including the midterm test and assignment. Similarity between submissions that has not been appropriately documented will be treated as plagiarism - the same as copying on an exam - and will be submitted to the Dean for disciplinary action. If you are unsure of the expectations regarding academic integrity (e.g., how to use and cite outside materials), then you must ASK the instructor.

Sharing assignment or exam specifications or posting them online (to sites like Chegg, CourseHero, OneClass, etc.) is ALWAYS considered academic misconduct. You are never permitted to post, share, or upload course materials without explicit permission from the instructor. Academic integrity offences are reported to the office of the Dean of Science.

You are only permitted to use AI tools like ChatGPT/Gemini for 1) grammar/spell checking your write-up, and 2) preparing for any non-written work, e.g., to help you summarize materials and generate ideas. It is prohibited to use such tools for producing any submitted **written work** and you will bear the consequences including but not limited to mark loss due to **irrelevance**, e.g., there is always some marks dedicated to our class discussion context, and if the submitted written work does not have such context reflected (nothing to do with class discussions, just blindly generated) it will receive lower marks.

Late and Missed Work Policies

Late Work

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. Certain extenuating circumstances will be handled on a case-by-case basis, potentially treated as missed work (see below).

Technical problems do not exempt you, so if you wait until the last minute and then have issues with your connection, you will still receive a mark of zero. Consequently, you are advised to submit your work several hours in advance of the due time. You can also submit a work-in-progress version and override it with the completed version before the deadline. Contact the TAs/instructor in case of any problems.

NO submission by email will be accepted without any exception (so please do not email your work to a TA or the instructor). If you are granted a submission, the submission entry will reappear in Brightspace.

Missed Work

Short-term (5 days or less): In the case of health issues or other personal/family emergencies a self-declaration form can be used request accommodation (link to the academic considerations form). You are only allowed to use this form up to twice in the entire term.

Long-term (> 5 days): Accommodation must be requested formally which is not directly handled by the instructor (longer-term accommodation).

All accommodation requests must be received by the instructor within 24 hours following the due time and accommodations for short-term missed work may include (but are not limited to) weight adjustments, extension with/without mark reduction, or substitute work.

School of Computer Science Laptop Requirement

Every student that has been enrolled in a 1000-level (i.e., first year) course offered is required to have a laptop. This includes COMP1001, COMP1005, and COMP1006. For more information, please visit https://carleton.ca/scs/scs-laptop-requirement/ and then review the requirements at https://carleton.ca/scs/scs-laptop-requirement/laptop-specs/.

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/.

Mental Health and Wellness

Always first visit the Carleton Wellness Website whenever you feel there is a need.

Academic Accommodations and Regulations

Academic Accommodation

Carleton is committed to providing academic accessibility for all individuals. You may need special arrangements to meet your academic obligations during the term. The accommodation request processes, including information about the Academic Consideration Policy for Students in Medical and Other Extenuating Circumstances, are outlined on the Academic Accommodations website (https://students.carleton.ca/course-outline/).

Chat GPT/Generative AI Usage

As our understanding of the uses of GenAI and its relationship to student work and academic Integrity continue to evolve, students are required to discuss their use of GenAI in any circumstance not described here with the course instructor to ensure it supports the learning goals for the course.

Academic Integrity

Students are expected to uphold the values of academic Integrity, which include fairness, honesty, trust, and responsibility. Examples of actions that compromise these values include but are not limited to plagiarism, accessing unauthorized sites for assignments or tests, unauthorized collaboration on assignments or exams, and using artificial intelligence tools such as ChatGPT when your assessment instructions say it is not permitted.

Everything you submit for evaluation must be the result of your own work and only your own work. If you copy more than ten consecutive words or any non-trivial snippet of code from a single source without providing a valid reference, then that is considered plagiarism and an example of academic misconduct.

Misconduct in scholarly activity will not be tolerated and will result in consequences as outlined in Carleton University's Academic Integrity Policy. A list of standard sanctions in the Faculty of Science can be found here.

Additional details about this process can be found on the Faculty of Science Academic Integrity website.

Students are expected to familiarize themselves with and abide by Carleton University's Academic Integrity Policy.

Student Rights & Responsibilities

Students are expected to act responsibly and engage respectfully with other students and members of the Carleton and the broader community. See the 7 Rights and Responsibilities Policy for details regarding the expectations of non-academic behaviour of students. Those who participate with another student in the commission of an infraction of this Policy will also be held liable for their actions.

Student Concerns

If you have any concerns regarding this course, your first point of contact is me. Please email me or message me on MS Teams, and I will do my best to address your concerns. If I cannot resolve the issue, the next point of contact is the School of Computer Science at studentconcerns@scs.carleton.ca. If the concern remains unresolved, the final point of contact is the Office of the Dean of Science at ODScience@carleton.ca. Please follow this order of contact.

Note: You can also bring your concerns to Ombuds services.