EvoSec 2025W: Course Outline

Contents

Course Information

- **Course Number:** COMP 5900H/4900H
- **Term:** Winter 2025

- **Title:** Evolutionary Security
- **Institution:** Carleton University, School of Computer Science
- **Course Website**: https://homeostasis.scs.carleton.ca/wiki/index.php/Evolutionary_Security:_Winter_2025
- **Instructor:** Anil Somayaji (https://people.scs.carleton.ca/~soma) (he/him)
  - Student hours by appointment
  - Contact via Teams, Email (anil.somayaji at carleton.ca), and Discord (asomayaji#1800)
- **Lectures:** Tues. and Thurs. 11:35-12:55 via Zoom (see Brightspace (https://brightspace.carleton.ca) for the link), January 7-April 8, 2025.

University of Ottawa Students, please see here (https://gradstudents.carleton.ca/faculty-of-graduate-and-postdoctoral-affairs-access-to-brightspace/) to gain access to Brightspace; contact the instructor for lecture Zoom link.

Important dates and deadlines can be found here: https://carleton.ca/registrar/registration/dates/academic-dates/, including class suspension for winter break, and statutory holidays.

Course Calendar Description

A course on computer security from an evolutionary perspective, with the goal of understanding the computer security arms race. Covers models of cooperation and conflict from biology, economics, game theory, evolutionary computation, artificial life, and others. Focus is on an evolutionary analysis of existing defenses at the operating system, application, network, and user levels.

Prerequisite for COMP 4900H: COMP4108 with a minimum grade of A-, or permission of the instructor.

Learning Materials and Other Course-Related Resources

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

Assigned readings will be posted to the course page throughout the term.

Topics Covered and Learning Outcomes

TBA

Grading

The marking scheme for this course are:

- 70% for the course project, which should be either a research proposal or a research

paper.

  - 2% areas of interest
  - 3% elevator pitch
  - 20% literature review
  - 10% tests/preliminary work
  - 5% presentation
  - 30% research proposal/paper (Exam period)
- 20% for reading responses and journaling
- 10% for class participation

Due dates are subject to change. The various parts are explained below.

Course Project

In this course you'll be doing a term project that will produce a research paper or a research proposal. This project has multiple milestones.

You will first submit an areas of interest document that outlines the kinds of projects and the types of software systems you wish to work with. Then, you'll submit an "elevator pitch" which will be a few paragraph summary of your idea, concisely communicating the basic idea for your project. You'll then submit a literature review related to your idea and a report on preliminary findings/ tests before finally presenting your work to the class and, finally, submitting your completed paper or proposal. Through this process you should produce work that will either be publishable or is on the path to creating something publishable in the security literature.

Reading Responses & Journaling

For this class you'll maintain an electronic research journal which will detail your ongoing thoughts related to this class. You should record your responses to assigned readings, ideas that arise from class, brainstorming for your class project, and any other relevant thoughts. The instructor will review your journal before each class so he may address any questions or concerns that arise in your writings.

You may use any application to maintain your journal so long as it is easily shared with the course instructor. Journals will be graded as a participation grade, with marks assigned out of 4 for each class.

Class Participation

You are expected to attend most class meetings and participate in asynchronous class discussions. Students making a genuine effort to participate will earn most of these marks (with a bit reserved for truly exceptional participation).

Late and Missed Work Policies

Because reading responses directly relate to in-class work, reading responses will not be accepted late without extenuating circumstances.

Unless there are extenuating circumstances, all other work will suffer a 10% late penalty if submitted after Brightspace submissions close for that particular submission. There is no penalty for submitting after the due date so long as submissions are still open.

Communication and Lectures

This course is a virtual course using a mix of synchronous and asynchronous communication. We will use videoconferencing for scheduled class time and an online discussion forum for communication outside of class. The course webpage listed above is the canonical source of information for everything regarding this course *except* for private information (such as video call links, invites to discussion forums) which is available through the course's Brightspace page.

Collaboration

Participation and reading responses/journaling are graded individually. The course project should also be done on your own unless the instructor allows you to work in pairs. Having said this, you will be collaborating with other students in this class. When you have worked with others, outside contributions should be clearly acknowledged as they should be in any academic endeavor. All participants in the class are expected to act with the highest intellectual integrity, and violations of that integrity may be reported to the academic dean for disciplinary action.

Use of AI/LLMs

In this course, students may use AI systems such as ChatGPT that include large language models (LLMs) as part of their research process. Students may use AI systems to spell check and do light grammar checking on their submissions. Students may also use coding assistants such as CoPilot to assist with software development, with the understanding that any code produced by such systems is of questionable provenance which may impact the ability to legitimately license and distributed applications that include generated code.

Any written work, however, **should not** include the output of any AI system including any LLMs. I much prefer smaller amounts of student-authored text to large amounts of AI "slop". *Any inclusion of AI-generated text in submitted work will be considered a violation of academic integrity and will be reported to the Dean for disciplinary action.*

Course Notes

Notes from class will be posted to the class page. As part of class participation, students may (optionally) contribute to these notes.

Course Software

There is no required course software. However, depending on your project you may be creating applications. While support will be provided in class where feasible, ultimately students will be responsible for their own software development environments.

University Policies & Resources

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

The Carleton Wellness Website (https://wellness.carleton.ca/) is a wonderful resource link to include in the course outline for students.

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 are outlined on the Academic Accommodations website (https://students.carleton.ca/course-outline/).

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.

Misconduct in scholarly activity will not be tolerated and will result in consequences as outlined in Carleton University's Academic Integrity Policy (https://carleton.ca/secretariat/wp-content/uploads/Academic-Integrity-Policy-2021.pdf). A list of standard sanctions in the Faculty of Science can be found here (https://science.carleton.ca/academic-integrity/).

Additional details about this process can be found on the Faculty of Science Academic Integrity website (https://science.carleton.ca/academic-integrity/).

Students are expected to familiarize themselves with and abide by Carleton University's Academic Integrity Policy (https://carleton.ca/secretariat/wp-content/uploads/Academic-Integrity-Policy-2021.pdf).

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 (https://carleton.ca/studentaffairs/student-rights-and-responsibilities/#sect1.1) 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 visit during my student hours, 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 (https://carleton.ca/ombuds/).

Retrieved from "https://homeostasis.scs.carleton.ca/wiki/index.php?title=EvoSec_2025W:_Course_Outline&oldid=24925"

This page was last edited on 1 January 2025, at 16:19.

Content is available under GNU Free Documentation License 1.2 unless otherwise noted.