COMP 7860 - Fall 2024

Course Outline

Course Title: Cyber Threat Intelligence and Response

Course Description:

COMP 7860 is a graduate level course, which will introduce and explore a variety of topics and solutions in cyber threat intelligence including vulnerabilities, system auditing, threat detection and response, provenance analysis and Machine Learning (ML) in securing computing systems. Students will work in teams to learn about security mechanisms through class lectures, assignments, discussions/presentations, offline summaries/questions/comments, and the course project. Gaining hand-on, technical experience and analytical evaluation of security mechanisms and incidents will be ongoing aspects of the course.

Course Instructor	Office	Email
Dr. Azadeh Tabiban (Computer Science Department)	E2-480 EITC	Azadeh.Tabiban@umanitoba.ca

Instructor office hours will be posted on the course website in UM Learn.

Website: UM Learn is used in this course. Make sure that you can access COMP 7860 in UM Learn.

Prerequisites: Solid background in Operating Systems (COMP 3430 or equivalent), and programming (COMP 2160 or equivalent) is strongly recommended.

Topics & Learning Objectives: At the end of this course, students will have gained knowledge and technical experience on topics and solutions in cyber threat intelligence, which include (subject to minor changes): system auditing, vulnerability and defences, intrusion detection systems, ML-based threat detection, the combination of provenance analysis and ML application to forensic investigation, threat detection, threat hunting and report generation, mimicry attacks and evasion of security solutions, provenance analysis for cloud-scale environments and network security.

Class Format: The class format will consist of instructor's lectures and students' presentations and discussions. For paper presentation sessions, all students (including the presenter) will be expected to read papers, submit a short summary (300-450 words) and one question and comment about each paper by 24 hours prior to the class, and actively participate in class discussions. Students who present research papers must submit their slides to the class website. The full schedule, and detailed descriptions about deliverables will be posted on the course website.

Grade Breakdown:

- Paper presentations and summaries/comments: 17%
  - Presentation: 12% (based on the content (depth and breadth of the covered material), clarity/visualization, organization, leading the discussions around the presented material, etc.)
  - In-class discussion participation: 2%
  - Submitted summaries, questions, and comments on papers: 3%
- Course project: 40%
- Assignments: 25%
- Final exam: 18%

Absences, late submissions, missed presentations: Students are expected to attend classes and participate in discussions.

- Paper and assignment presentations: Only one self-declaration form per term will be accepted for an excused absence from a class that the student is scheduled to present a paper/assignment. If the student is sick (they are unable to attend classes that they are scheduled to present), they must submit the Self-declaration for Brief and Temporary Absences form, and inform the instructor at least 24-48 hours prior to the class. If a student needs to miss attending more than one of such sessions, they should get in touch with an advisor in your faculty/college/school of registration.
- Late assignments, project report/code and project presentation video: 2% deduction will be applied for each 24-hour period after the deadline. The deliverables will get no mark if submitted more than 72 hours after the deadline.
- Late paper summaries/comments/questions will not be marked (i.e., will receive a zero grade).

Course Project: Students are expected to study the implementation, run and experimentally evaluate a recent existing open-source provenance solution published in a top-tier security conference. The full description of the project and expectations will be posted on the course website.

Assignments: There will be four assignments: Two assignments involve studying and running a CVE proof of concept on a VM, deploying auditing mechanisms that detect the exploit, and presenting the findings in the class. The other two assignments involve providing a thorough comparison analysis on the specified papers presented in the class. The full description and expectations will be posted on UM Learn.

Recording Policy: Recording of lectures, discussions, office hours meeting, and any other course-related activities is not allowed.

Tech Requirements: Students must have access to a modern laptop or other workstations/servers that can be used to do the assignments and the project of the course. A tablet computer will not suffice.

Determination of Letter Grades: The minimum percentage grade required for F, D, C, C+, B, B+, A, and A+ will be 0, 50, 60, 65, 70, 75, 80, and 90%, respectively. These breakdowns will be used when assigning final grades, plus or minus 5%. Any adjustment will be made to ensure grades are assigned fairly. Please note: All final grades are subject to departmental review.

Textbook: None – Recommended and required readings will be provided.

Academic Honesty: Academic dishonesty is a very serious offence and will be dealt with in accordance with the University's discipline bylaw.

- Students are encouraged to discuss programs or setups/simulations in general to learn from each other. However, unless otherwise noted, having the simulations/setups/evaluations conducted by someone else, and using the code, code comments and reports written by someone else are examples of academic dishonesty.
- You can read more about academic integrity expectations in the CS department on this page.

Ethics Statement: As computer scientists, we rely on the ethical use of computing technologies covered in the class. Students must avoid the unethical use of technologies which includes circumvention of existing security or privacy mechanisms, or the unethical exploitation of vulnerabilities.

Equity, Diversity, and Inclusion: At the Faculty of Science, we believe in the principles of equity, diversity, and inclusion (EDI) and rely on them to create a supportive and inclusive community. Learn more about the importance of these key values and related resources that you can use on this page.

Important Dates: Please see the Important Dates section of the UofM General Calendar for information on holidays, exams, and voluntary withdrawal dates.