

## COMP 7860 - Winter 2024

### Course Outline

**Course Title:** Computer Security

**Course Description:**

COMP 7860 is a graduate level course, and will investigate security challenges and techniques in computer systems. Students will be introduced to a variety of topics in operating system and network security, including auditing, logging and vulnerability/defences. Students will work in teams to learn about security mechanisms through class lectures, discussions/presentations, offline summaries and comments, and the course project. Analytical evaluation of the existing security mechanisms will be an ongoing aspect of the course.

**Instructor:**

Course Instructor	Office	Email
Dr. Azadeh Tabiban (Computer Science Department)	E2-480 EITC	<a href="mailto:Azadeh.Tabiban@umanitoba.ca">Azadeh.Tabiban@umanitoba.ca</a>

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:** Comp 4430, Comp 1020 and Comp 4140 (or equivalents) are strongly recommended.

**Textbook and Additional Course Materials:**

- Suggested textbook:
  - Computer Security. Art and Science, M.Bishop, Publisher: Addison-Wesley.
- Other recommended readings will be provided.

**Topics & Learning Objectives:**

At the end of this course, students will have gained knowledge and experience in computer security topics including (subject to minor changes):

Design principles and Unix security, auditing and logging, vulnerability and defenses, data provenance, provenance analysis in operating systems (application to root cause analysis, alert triage, threat detection, forensic report generation, log reduction, summarization, etc.), provenance analysis for virtualized environments (challenges of root cause analysis in virtualized environments, cloud management-level provenance, multi-level provenance in Network Functions Virtualization (NFV), provenance compression in clusters, complete provenance tracking for containers and serverless functions, etc.).

**Class Format:** The class format will consist of group discussions of relevant research papers as well as lecture material. Students will be expected to read 2-3 papers for each class, submit a short summary (1-2 pages) and one question and comment about each paper by 1:00pm the day before class, and actively participate in class discussions. For those classes that are dedicated to group discussions, 2-3 students will give a formal presentation on the read papers. The full schedule will be posted on the course website.

**Grade Breakdown:**

- Paper discussions:
  - Presentation: 20% (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: 10%
  - Submitted summaries, questions, and comments on papers: 5%
- Course project:
  - Proposal: 5%
  - Final project outcome: 10%
  - Presentation: 15%
  - Report: 20%
- Final exam: 15%

**Class Participation:** Students are expected to attend classes and participate in discussions.

**Course Project:** Students are expected to conduct an in-depth study of an existing provenance-based security solution. Specifically, students will research a proposed provenance-based security solution and attempt to implement it. Students are required to provide a final written report, completed code, and give a class presentation on their projects. The project scope must be approved by the instructor. Projects are marked based on the completeness of the implementation as well as analysis, clarity and organization of the project presentations and reports.

**Determination of Letter Grades:** The minimum percentage grade required for C+, B, B+, A, and A+ will be 65, 70, 75, 80, and 90%, respectively. These cutoffs might be adjusted plus or minus 5% at the end of term, at the discretion of the course instructor.

**Academic Honesty:** Academic dishonesty is a very serious offence and will be dealt with in accordance with the University's discipline bylaw. Examples of academic dishonesty include submitting assignments which are not entirely your own work or providing your work to another student or students, and plagiarizing the writing of other researchers. You can read more about academic integrity expectations in the CS department on [this page](#).

**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 U of M General Calendar for information on holidays, exams, and voluntary withdrawal dates.