

COMP 7570 Security and Privacy

1. General Information

- Instructor: Noman Mohammed
- Email:
- Office location:
- Lecture time and location:
- Office hours:
- Course website:
- Prerequisites: COMP 4580 (Computer Security) is recommended.

2. Course Description

Summary: The objective of this course is to train students in secure data collection, protection, and dissemination of information for data analysis. This course will cover legal, ethical, and technical aspects of information privacy. The main topics include conceptions and legal foundations of information privacy, security primitives, different privacy models, and various anonymization algorithms for diverse data sharing scenarios. Students will explore cutting-edge privacy solutions and learn how to apply privacy technologies to real-life applications.

3. Grading

- Paper presentation: 15%
- Participation: 15%
- Assignments (mostly review of papers): 20%
- Project:
 - Proposal: 5%
 - Progress report: 10%
 - Final report: 25%
 - Project presentation: 10%

The course will consist of a combination of lectures by the instructor, student-led discussions of research papers, and occasional visiting lecturers. This course will primarily consist of reading, reviewing, and presenting research papers (the exact number per student will depend on the total enrollment). There will be two papers assigned to each class period, selected from the reading list. All students are to have read both of the papers before the class, and to have submitted a review (comments, discussion questions, etc.) for one of them (of the student's choice) on the evening before the class.

Project: The course includes a substantial course project. Different project ideas and options will be discussed and posted. Project deliverables include project proposal, progress report, in-class project presentation, final report, source code and executable package if applicable. Projects should ideally be done in groups of two.

4. Course Topics (*subject to change*)

- Introduction to data privacy and security
- Legal foundations of information privacy
- k -anonymity and its application
- Beyond k -anonymity: l -diversity, confidence bounding & t -closeness
- Introduction to differential privacy
- Methodology for managing re-identification risk
- Social network privacy
- Privacy in DNA, set-valued data & trajectory data
- Privacy in data outsourcing & cloud computing applications
- Secure multiparty computation
- Smartphone privacy and security

5. Textbook and Other Readings

- **Textbook:** There will be no required textbook. Reading material for the course will consist mainly of research articles, in conjunction with sections from a selection of different books.

6. Student's Responsibilities

Students are expected to attend every class. Some material may only be covered in class and not made available on the course note/website. Students are expected to read the assigned materials and to actively participate in class discussions.

7. Student Resources

A list of University governing documents pertaining to students can be found [here](#).

Academic Recourses

Various academic resources are available to students including the [Science and Technology Library](#) and various departmental help centers.

Health & Mental Health Resources

Students with Health and/or Mental Health issues may seek advice and/or help from [Student Counselling Center](#), [Student Accessibility Services](#), and [University Health Services](#).

Copyright and Intellectual Property Resources

Copyrights and intellectual property must be respected by all students. For more information, please refer to the [copyright office](#).

Academic Integrity Resources

The Faculty of Science takes academic integrity very seriously. Any evidence of academic dishonesty on assignments, labs and/or tests will be forwarded to the appropriate authorities for potential disciplinary actions.

The University Student Discipline By-Law may be accessed at:

http://umanitoba.ca/admin/governance/governing_documents/students/student_discipline.html
. Information from the Faculty of Science regarding Cheating and Plagiarism can be found at <http://umanitoba.ca/faculties/science/undergrad/resources/webdisciplinedocuments.html>.

Respectful Behavior Resources

Students are expected to act in a respectful manner. Policies regarding respectful work and learning environment and sexual assault can be found [here](#).

Final Examinations, Grades and Grade Appeals Resources

Final examination and grades policies can be found [here](#). For more resources about examinations, see [here](#).

Students wishing to appeal their term work grade can do so through the Registrar's office. A fee is charged for each appeal. More information can be found [here](#).

To view your final examination, please check with the department offering the course for policies. More information can be found [here](#).

To appeal your final grade, you can initiate the process at the Registrar's office. A fee will be charged for each appeal. See the [Registrar's office](#) for more information.

Limited Access and VW Resources

Students who fail or VW from a course will be subject to limited access to that course in future terms. That is, students will not be able to register for a course (for which they have VWed or failed) during the limited access registration period. For more information, please see the [policy document](#) for repeated courses.