CIS*6510

Cybersecurity and Defense in Depth

Fall Semester

UNIVERSITY *of* GUELPH

---

1   INSTRUCTOR

Instructor: Hassan Khan
Office: REY 3319
Phone extension: 53138
E-mail: hkhan15@uoguelph.ca

2   AIMS & OBJECTIVES

2.1   Calendar Description

This course provides an overview of concepts and technical measures that are employed to enforce security policies and protect networks and systems from malicious activities. Students will learn how to engineer a secure system and how to secure networks in an ethical manner.

2.2   Course Description

This course provides an overview of concepts and technical measures that are employed to enforce security policies and protect networks and systems from malicious activities. The course will investigate data layer, system layer, network layer, and perimeter layer defence mechanisms and how all those techniques can be orchestrated into a defence in-depth strategy. It also provides additional knowledge to students on how to engineer a secure system in an ethical manner and how to secure networks using Firewalls, IDS, IPS, proxies, etc.

2.3   Learning Outcomes

Upon successful completion of this course, students will have demonstrated the ability to:

1. Design and implement fully-secure and layered defence systems;

2. Identify common security vulnerabilities and pitfalls in system design and suggest measures to avoid those;

3. Apply appropriate cybersecurity concepts and controls to analyse threats and protect data and systems;

4. Evaluate and interpret relevant facts, concepts, principles, and theories relating to designing and developing secure systems and use them to evaluate and improve the security of real-world systems;

5. Integrate ethics, regulations, and best practices in cybersecurity; and

6. Work collaboratively in teams to conduct research and communicate rational and reasoned arguments using appropriate methods.

2.4 Instructor's Role and Responsibility to Students

The role of the instructor is to deliver lectures, facilitate discussion, provide guidance for the course project, and provide feedback to students.

3 TEACHING AND LEARNING ACTIVITIES

3.1 Timetable

Lectures: 3 hours per week

3.2 Course Topics and Schedule

Week	Topic
Week 1	Introduction to ethics, regulations and best practices in cyber security
Week 2	Program Security
Week 3	Operating Systems Security
Week 4	Network Security
Week 5	Network Security
Week 6	Fundamentals of Cryptography
Week 7	Web Applications Security
Week 8	Web and Email Applications Security
Week 9	Usable Security, User Authentication
Week 10	Copyrights and DRM, Privacy Enhancing Technologies
Week 11	Managing Development of Secure Systems
Week 12	Security Economics, Legal, and Ethical Issues

4 LEARNING RESOURCES

4.1 Course Website

Course material, news, announcements, and grades will be regularly posted to the CIS*6510 Courselink site. Students are responsible for checking the site regularly.

4.2 Required Resources

Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Edition by Ross Anderson, Wiley. Available online for free.

5 ASSESSMENT

5.1 Dates and Distribution

Assessment	Due Date	Weighting	Learning Outcome(s) Assessed
Assignment 1	TBA	20%	LO1, LO2, LO5
Assignment 2	TBA	20%	LO3, LO4, LO5
Final Project	TBA	60%	LO1, LO2, LO3, LO4, LO5, LO6

5.2 Assessment Descriptions

Assignments

All assignments are to be submitted individually and electronically. Submission deadline is at 23:59 on the due date. Detailed instruction on the content of each assignment will be distributed during the term.

Assignment 1: Students are presented with a real-world scenario and are required to apply their knowledge and skills to analyse security and privacy issues. They communicate their findings in a written report. Students will evaluate following a standard approach to identify vulnerabilities in a system.

Assignment 2: Students are presented with security and privacy issues and are asked to develop solutions to mitigate those issues. They communicate their findings through a written report and software artifacts.

Final Project

Students should undertake novel research in the areas of security and privacy. They will identify security and privacy issues with real-world systems and apply their knowledge to develop solutions. They will communicate their findings in the form of a written report.

Projects should be done in a group of two. If students have strong reasons to do the project individually or in a larger group, they need permission from the instructor.

A one-page project proposal (5% of the final grade) will be due by the end of the third week of the course. A one-page progress report (5% of the final grade) will be due at the end of the seventh week of the course. Project artifacts (e.g., source code, applications, or sploits) and a project report will be due at the end of the classes and will comprise 30% of the final grade.

5.3 Course Grading Policies

Accommodation of Religious Obligations: If you are unable to meet an in-course requirement due to religious obligations, please email the course instructor within two weeks of the start of the semester to make alternate arrangements. See the graduate calendar for information on regulations and procedures for Academic Accommodation of Religious Obligations: https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/sec_d0e2228.shtml

Passing grade: In order to pass the course, students must obtain a grade of 65% or higher on the total mark of all assessments.

6 UNIVERSITY STATEMENTS

6.1 Email Communication

As per university regulations, all students are required to check their e-mail account regularly; e-mail is the official route of communication between the University and its students.

6.2 When You Cannot Meet a Course Requirement

When you find yourself unable to meet an in-course requirement because of illness or compassionate reasons please advise the course instructor (or designated person, such as a teaching assistant) in writing, with your name, id#, and e-mail contact. The grounds for Academic Consideration are detailed in the Graduate Calendar: https://www.uoguelph.ca/registrar/calendars/graduate/current/index.shtml

6.3 Drop Date

Courses that are one semester long must be dropped by the end of the fortieth class day; two-semester courses must be dropped by the last day of the add period in the second semester. The regulations and procedures for changing graduate course registration are available in the Graduate Calendar: https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/genreg-reg-regchg.shtml

6.4 Copies of Out-of-class Assignments

Keep paper and/or other reliable back-up copies of all out-of-class assignments; you may be asked to resubmit work at any time.

6.5   Accessibility

The University promotes the full participation of students who experience disabilities in their academic programs. To that end, the provision of academic accommodation is a shared responsibility between the University and the student.

When accommodations are needed, the student is required to first register with Student Accessibility Services (SAS). Documentation to substantiate the existence of a disability is required; however, interim accommodations may be possible while that process is underway.

Accommodations are available for both permanent and temporary disabilities. It should be noted that common illnesses such as a cold or the flu do not constitute a disability.

Use of the SAS Exam Centre requires students to book their exams at least seven days in advance and not later than the fortieth class day.

More information can be found on the SAS website: https://www.uoguelph.ca/sas

6.6   Academic Misconduct

The University of Guelph is committed to upholding the highest standards of academic integrity, and it is the responsibility of all members of the University community—faculty, staff, and students—to be aware of what constitutes academic misconduct and to do as much as possible to prevent academic offences from occurring. University of Guelph students have the responsibility of abiding by the University's policy on academic misconduct regardless of their location of study; faculty, staff, and students have the responsibility of supporting an environment that discourages misconduct. Students need to remain aware that instructors have access to and the right to use electronic and other means of detection.

Please note: Whether or not a student intended to commit academic misconduct is not relevant for a finding of guilt. Hurried or careless submission of assignments does not excuse students from responsibility for verifying the academic integrity of their work before submitting it. Students who are in any doubt as to whether an action on their part could be construed as an academic offence should consult with a faculty member or faculty advisor.

The Academic Misconduct Policy is detailed in the Graduate Calendar: https://www.uoguelph.ca/registrar/calendars/graduate/current/genreg/sec_d0e2642.shtml

6.7   Recording of Materials

Presentations that are made in relation to course work—including lectures—cannot be recorded or copied without the permission of the presenter, whether the instructor, a student, or guest lecturer. Material recorded with permission is restricted to use for that course unless further permission is granted.

6.8   Resources

The Academic Calendars are the source of information about the University of Guelph's procedures, policies, and regulations that apply to undergraduate, graduate, and diploma programs: https://www.uoguelph.ca/academics/calendars