CIS*6560

Malicious Software Programming and Secure Coding

Fall Semester

UNIVERSITY of GUELPH

---

1 INSTRUCTOR

Instructor: Ali Dehghantanha and Hassan Khan

Office: REY 3326

Phone extension: 52999

E-mail: adehghan@uoguelph.ca; hkhan15@uoguelph.ca

2 AIMS & OBJECTIVES

2.1 Calendar Description

Through collaboration with industry partners, this course provides a comprehensive review of malicious program development, detection of software vulnerabilities, patching and avoiding those vulnerabilities, and building secure software. Students will develop understanding of malicious programs and ethical and legal boundaries in malicious software development.

2.2 Course Description

This course collaborates with industry partners to develop a comprehensive review of malicious program development, detection of software vulnerabilities and how to patch and avoid those vulnerabilities and build a secure software. The course develops students understanding of malicious programs and ethical and legal boundaries in malicious software development.

2.3 Learning Outcomes

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

1. Detect and avoid vulnerabilities associated with malicious software by documenting processes and developing coding that demonstrates an ability to:

a. Exploit weaknesses and loopholes of current systems by means of malicious software and exploits; and
b. Critically analyze various malicious software and malware species and develop relevant countermeasures;

2. Design a strategy that patches vulnerabilities and diffuses malicious software;
3. Analyse and integrate ethics, regulations, and best practices in development of malicious programs and best practices in secure software coding; and
4. 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 course is delivered in a flipped classroom format so most instructional content is delivered online while classroom time is used to deepen students' understanding through discussions and problem-solving activities facilitated by the instructor. The instructor delivers hands-on guided labs and practical lectures to practice key concepts of malicious software programming and secure coding along with in-depth analysis of real-world case studies.

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 malicious software and legal and ethical issues in malicious software development
Weeks 2-3	Fundamentals of malicious software and shellcode programming
Weeks 4-5	Vulnerability detection and exploit development in x86 platforms
Weeks 6-7	Exploit Development on Windows Platform
Weeks 8-10	Reversing Malicious Programs and software vulnerability assessment
Weeks 11-12	Countermeasures and secure coding principles

4 LEARNING RESOURCES

4.1 Course Website

Course material, news, announcements, and grades will be regularly posted to the CIS*6560 Courselink site. Students are responsible for checking the site regularly.

4.2 Required Resources

- Michael Sikorski, Andrew Honig “Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software," 2012.
- Chris Eagle, “The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler Paperback,” 2011.
- Eldad Eilam, “Reversing: Secrets of Reverse Engineering Paperback,” 2005.
- Jon Erickson, “Hacking: The Art of Exploitation,” 2008.
- Chris Anley, John Heasman, Felix Lindner, Gerardo Richarte, “The Shellcoder’s Handbook: Discovering and Exploiting Security Holes,” 2007.

5 ASSESSMENT

5.1 Dates and Distribution

Assessment	Due Date	Weighting	Learning Outcome(s) Assessed
Assignment	TBD (before the 40th class day)	50%	LO2, LO3, LO4
Practical Exam	TBD	50%	LO1, LO2, LO3

5.2 Assessment Descriptions

Research Assignment

Students will be required to find a software or application vulnerability, follow all legal and ethical requirements in responsibly reporting and disclosing the vulnerability as defined in the course, analyse the root cause of the weakness, develop an exploit as a proof of concept for the attack, and suggest patches or mitigation mechanisms for the detected vulnerability. Students will document their results and compile a professionally written, high-quality academic report. This is a group-based assignment (max 3-person in each group) that should be submitted electronically as advised by the instructor prior to the submission deadline.

Practical Exam

The practical exam will be conducted in the cybersecurity lab. The exam evaluates students’ skills in finding software vulnerabilities in a legal and ethical manner, writing programs that exploit the vulnerability, and writing software patch or developing a solution to mitigate risk of exploitation.

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