CIS*6530

Cyber Threat Intelligence and Adversarial Risk Analysis

Winter Semester

UNIVERSITY of GUELPH

1 INSTRUCTOR

Instructor: Ali Dehghantanha

Office: REY 3326

Phone extension: 52999

E-mail: adehghan@uoguelph.ca

2 AIMS & OBJECTIVES

2.1 Calendar Description

This module provides an in-depth understanding of techniques for detecting, responding to, and defeating Advanced Persistent Threats (APT) and malware campaigns using artificial intelligence and data mining techniques. Students will identify, extract, and leverage intelligence from different types of cyber threat actors.

2.2 Course Description

This module provides an in-depth understanding of techniques for detecting, responding to, and defeating Advanced Persistent Threats (APT) and malware campaigns using artificial intelligence and data mining techniques. It enables students to identify, extract, and leverage intelligence from different types of cyber threat actors in a lawful and ethical manner.

2.3 Learning Outcomes

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

1. Recognize and utilize concepts of cyber threat intelligence to detect and defeat Advanced Persistent Threat (APT) actors and adversarial machine learning techniques;

2. Analyze both successful and unsuccessful advanced cyber intrusion attacks and malware campaigns using artificial intelligence and data mining techniques;
3. Leverage intelligence to build profiles of different adversarial groups and analyse risks associated with different threat actors;
4. Develop a threat intelligence report that justifies threat attribution based on analysis of intrusion artefacts;
5. Analyse and integrate ethics, regulations, and best practices regarding collection, analysis, and sharing of intelligence data and intelligence activities; 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 course is delivered in a flipped classroom format so most instructional content is delivered online while classroom time is being 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 cyber threat intelligence and adversarial risk analysis and provides feedback on students' activities.

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 cyber threat intelligence and understanding ethics, regulations, and best practices for cyber threat intelligence
Weeks 2, 3, 4	Foundation of cyber threat intelligence and applied machine learning
Weeks 5, 6	Adversarial machine learning and advanced malware analysis
Weeks 7, 8	Analysis of web-based and document-based malware
Weeks 9, 10	Cyber threat modelling and adversarial risk analysis
Weeks 11, 12	Tactical and operational threat intelligence

4 LEARNING RESOURCES

4.1 Required Resources

- Ali Dehghantanha, Mauro Conti, Tooska Dargahi (2017), Cyber Threat Intelligence (available electronically via library)
- Ian H. Witten, Eibe Frank, Mark A. Hall, Christopher J. Pal (2016), Data Mining: Practical Machine Learning Tools and Techniques, Fourth Edition
- Michael Bazzell (2015), "Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information", CreateSpace Independent Publishing Platform.
- Michael Sikorski, Andrew Honig (2012) Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, William Pollock
- Chris Eagle, "The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler", 2011

5 ASSESSMENT

5.1 Dates and Distribution

Assignment	Due Date	Weighting	Learning Outcome(s) Assessed
Research Assignment	TBD (before the 40th class day)	50%	LO3, LO4, LO5, LO6
Practical Exam	TBD	50%	LO1, LO2, LO3, LO4

5.2 Assessment Descriptions

Research Assignment: Students will analyse a recent campaign and leverage their data to build a profile of involved adversaries characteristics, tools, techniques, and procedures. Students will develop intelligent solutions to mitigate adversaries' risk in the future and submit a professionally written, high-quality report. This is a group-based assignment (max 3 people in each group), which 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 will assess student understanding of cyber threat intelligence and adversarial risk analysis concepts as well as students' abilities to analyse attack campaigns and leverage intelligence from different adversary groups in a lawful and ethical manner. The exam will evaluate students' capabilities to conduct in-depth investigation of different attack campaigns, extract indications of compromise, and build threat intelligence models to detect, deny, disrupt, degrade, deceive, and destroy future attacks.

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