Cyber Threat Intelligence and Adversarial Risk Analysis

CIS*6530, Winter 24

1. INSTRUCTOR

Instructor: Fatemeh Khoda Parast

Office#: 120H

Email: khodapaf@uoguelph.ca

2. AIMS & OBJECTIVES

In this course, you will be introduced to Advanced Persistent Threat (APT) groups, tactics, and techniques to carry out attacks. We will explore how machine learning and data mining techniques are applied to identify Malware as APT groups' key method for conducting their malicious operations.

2.1. Course Description

Threat intelligence refers to information that helps organizations understand and proactively address potential threats to their security. It involves gathering, analyzing, and interpreting data about various cyber threats, including threat actors' tactics, techniques, and procedures. A group of threats we focus on are Advanced Persistent Threats or APT. As its name implies, APT refers to a group of attacks with advanced complicated methods, procedures, and tools. APTs are typically funded by the government and carried out by highly skilled threat actors. In the context of APTs, malware plays a crucial role as a delivery mechanism and a means of achieving the attackers' objectives. APTs commonly employ custom-built or advanced malware designed to evade detection, remain persistent, and facilitate unauthorized access or exfiltrate sensitive data.

2.2. Learning Outcomes

- Leveraging cyber threat intelligence for detecting and countering Advanced Persistent Threats (APTs).
- Utilizing artificial intelligence, machine learning and data mining techniques to analyze advanced cyber intrusion attacks and malware campaigns.
- Leveraging threat intelligence to determine the adversarial group and analyze the associated risks of different threat actors.
- Document and develop a report indicating the correlation between the threat elements and adversarial group indicators. Based on the threat actor profile, model

system threats, simulate an attack, and adapt defence.

3. INSTRUCTOR’S ROLE AND RESPONSIBILITIES

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

4. TEACHING AND LEARNING ACTIVITIES

Lectures: 3 hours per week

Timetable

Week	Date	Topic
Week 1	8-Jan	Introduction to threat intelligence, malware analysis, ethics, rules, and regulations.
Week 2	15-Jan	Static Malware Analysis
Week 3	22-Jan	Dynamic Malware Analysis
Week 4	29-Jan	Dynamic Malware Analysis
Week 5	5-Feb	Machine Learning for Malware Analysis
Week 6	12-Feb	Introduction to Advanced Persistent Threat (APT) groups, attack vectors and frameworks.
Week 7	19-Feb	READING WEEK - NO CLASS
Week 8	26-Feb	Introduction to Advanced Persistent Threat (APT) groups, attack vectors and frameworks.
Week 9	4-Mar	MIDTERM EXAM
Week 10	11-Mar	Study malware campaigns, profile APT group features, malware campaigns, profile APT groups features and analysis activities.
Week 11	18-Mar	Study malware campaigns, profile APT group features, malware campaigns, profile APT groups features and analysis activities.
Week 12	25- Mar	Reviewing current updates on cyber threat intelligence and adversarial risk analysis.
Week 13	1-Apr	FINAL EVALUATION

5. LEARNING RESOURCES

- Sikorski, Michael, and Andrew Honig. *Practical malware analysis: the hands-on guide to dissecting malicious software*. No Starch Press, 2012.
- Aggarwal, Charu C. *Data mining: the textbook*. Vol. 1. New York: Springer, 2015
- Ali Dehghantanha, Mauro Conti, Tooska Dargahi (2017), *Cyber Threat Intelligence* (available electronically via library)

6. COURSE POLICIES

- To complete the course, students must achieve at least 65% of the total marks.
- Missing up to two deliverables, such as assignments or quizzes, is permissible due to valid reasons, such as illness. Exceeding this limit will lead to course failure.
- All communication should be directed through the course TA. In cases where the TA cannot address a particular request, it will be forwarded to the instructor by the TA.

7. ASSESSMENTS

7.1. Assessments Date Details

Item	Date	Mark
Assignment	29-Jan, 12-Feb, 11-Mar, 25-Mar	20%
Quiz	22-Jan,5-Feb, 26-Feb, 18-Mar	20%
Midterm exam	4-Mar	25%
Final evaluation	1-Apr	35%

7.2. Assessments Description

Quiz: Students should expect questions from previous session topics in this module.
Assignment: This module evaluates the practical aspect of the course through projects.
Midterm: Evaluate all content of the course up to the midterm examination.
Final Exam: Evaluate all content of the course.

8. UNIVERSITY STATEMENTS

8.1. Email Communication

As per university regulations, all students must check their e-mail accounts regularly; e-mail is the official communication route between the University and its students.

8.2. 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 a 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.

8.3. Drop Date

One semester-long course 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.

8.4. Copies of Out-of-class Assignments

Keep paper and/or other reliable backup copies of all out-of-class assignments; you may be asked to resubmit work anytime.

8.5. Accessibility

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

8.6. 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. The 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 to 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 doubt 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.

8.7. Recording of Materials

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

8.8. 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.