CIS*6530

Cyber Threat Intelligence and Adversarial Risk Analysis

Fall 2023

---

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, their tactics, and the techniques they use 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 types of 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 defense.

3. TEACHING AND LEARNING ACTIVITIES

3.1. Timetable

Lectures: 3 hours per week

3.2. Course Topics and Schedules

Week	**Topic**
Week 1	Introduction to threat intelligence, ethics, rules, and regulations.

Week 2, 3	Introduction to Advanced Persistent Threat (APT) groups, profile group features, and analysis activities.
Week 4, 5, 6	Social engineering and malware campaigns.
Week 7, 8, 9	Applying machine learning methods for cyber threat detection and malware analysis.
Week 10, 11, 12	Reviewing current updates on cyber threat intelligence and adversarial risk analysis.

4. LEARNING 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. ASSESSMENTS

5.1. Assessments Date Details

Item	**Date**	**Mark**
Quiz	Week 3, 5, 8, 9, 10	10 (2 per quiz)

Research Project	Topic should be determined by week 5. Delivery week 11 and 12. (more details will be posted on this module)	20
Midterm exam	Week 7	20
Hands-on and projects	Week 4, 6, 8, 10	28 (7 per item)
Final Project	TBD	22
Class Activity	-	10 EXTRA MARKS

5.2. Assessments Description

Quiz: In this module, you should answer questions from previous sessions' topics.

Research: Students, in group of two/three, should select either an APT group or a malware campaign, operate comprehensive research, and generate a report. The report should be submitted electronically before the 10th week in IEEE format, two-column, min 8 and max 15 pages. Weeks 11 and 12 are group presentation on the findings of the research.

Hands-on: This module includes structure to implement a toy project to learn a procedure or analysis. Based on the learning objective, students will be given a similar but more complicated task to submit afterward.

Final Project: This course has no final exam. Instead, students should work on a practical exam in the lab environment.

Class activity: Students actively participating in Q&A or volunteer presentations can secure ten extra marks. Each question has one mark, and the presentation has five marks.

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