Concordia University
Concordia Institute for Information Systems Engineering

INSE6610: Cybercrime Investigation
TENTATIVE PROJECT DESCRIPTION
(Revision 1.0)

INSE6610		**Summer 2022**
Instructor:	Ivan Pustogarov	ivan.pustogarov@concordia.ca
TA:	Amir Naseri	am_naser@encs.concordia.ca
Team & Topic Due:		July 7, 2020, 23:59
Project Plan Due:		July 14, 2020, 23:59
Project Report Due:		August 8, 2020, 23:59

Contents

1 Introduction **2**

1.1 Project plan/summary 2

1.2 Possible Publication 2

1.3 Templates 2

1.4 Questions 2

2 Grading **2**

3 Project Topics **3**

1 Introduction

This project is a group work. Each group is encouraged to create a GitHub account/repository for the project files and share this repository with me, my github id for this course is `cu-pustogarov`. If you are unable to create/use GitHub, please contact me via email or via Moodle. The repository name should be "INSE6610-2022-Project-GroupN", where N is the group number.

Each team should use their GitHub repository to coordinate their group activities and manage the project's content, share documents and resources alike related to the group's project. *All students must produce substantial commits in repository history.* All of that will become a part of a single final report, and, depending on the project, combined with datasets or software artifacts in the end.

In addition, you must submit the final project report (PDF) electronically using Google Drive and provide a link to the report.

1.1 Project plan/summary

Each team should submit a short project description of the chosen project. Please us Google Doc and provide a link.

1.2 Possible Publication

The best team(s) will be invited to extend their final report with the course instructor's collaboration into real article(s) in different venues for formal publication.

1.3 Templates

The IEEE template is to be used for the reports: `https://www.ieee.org/conferences/publishing/templates.html`. Both Word and LaTeX templates are available; the latter is encouraged, but not required. (In the case of disputes on the amount of contribution, etc. within a team, you will also be required to submit a peer-evaluation form.)

1.4 Questions

If you are having difficulties understanding sections of this project, feel free to email the instructor to setup an appointment or resolve it by email.

2 Grading

General approach: a better quality work should get a better grade. The overall project grading depends on the completeness, originality, and quality of your work. Specific sections are evaluated between $[F \dots A+]$ as a percentage at the instructor's discretion and then certain sections are attributed weights

(detailed below). The letter grades are translated per regular GPA rules and then re-scaled to the assigned percentages.

A+	A	A-	B+	B	B-	C+	C	C-	D+	D	D-	F
4.3	4.0	3.7	3.3	3.0	2.7	2.3	2.0	1.7	1.3	1.0	0.7	0.0

Grading categories below are graded based on the letter grades above and then translated to numerical weights and rescaled as:

- /35: Methodology
- /20: Style / Quality
- /35: Synthesis / Source
- /10: References
- /X: Misc / Bonus – this category is to reward something very outstanding with bonus marks or subtract something very poor not covered by categories above.

3 Project Topics

Each team should select a project topic they would like to work on from the list below. If there are several teams that would like to work on the same project, please email me.

Students who do not select a project by the deadline will be assigned one to them by the instructor. Students without teams will be grouped/added into teams.

Project 1, SRVEY1 Survey and compare the use of software and hardware tools in cybercrime investigations.

Project 2, STDY1 Provide a detailed review and detailed case study from public reports, court proceedings, other sources (all must be properly cited), such as Sony hacks, Ashley Madison, Target, or others.

Project 3, CRYPTO1 Bitcoin Blockchain mixers (different types of mixers and recent attacks, implement minimum one attack using Bitcoin Testnet).

Project 4, CRYPTO2 Attacks on Monero anonymity? Implement attacks.

Project 5, CRYPTO3 Attacks on ZeroCoin anonymity? Implement attacks.

Project 6, STDY2 Study of Underground Hacker Forums. As an example (but not limited to) list of forums, what they are doing (e.g. selling credit cards, selling user data, malware etc.). How many of them are per country/language, what internet service providers do they use? How to get an account at those forums. Find as much information as possible.

Project 7, SRVEY2 Tor/Onion Hidden Service deanonymization techniques, Survey. Implement an attack against your own Onion service.

Project 8, SRVEY3 Log analysis for intrusion detection/investigation. Techniques using machine learning (review and comparison).

Project 9, CRYPTO4.1 Bitcoin Blockchain graph visualization (can use existing libraries). Collect and map known bitcoin addresses (e.g. exchanges, gambling, etc.) to graph nodes. Bonus points: being able to search bitcoin addresses and money flows on the graph.

Project 9, CRYPTO4.2 Ethereum Blockchain graph visualization (can use existing libraries). Collect and map known ethereum addresses (e.g. exchanges, gambling, etc.) to graph nodes. Bonus points: being able to search addresses and money flows on the graph.

Project 10, CRYPTO5 Tracking bitcoin addresses (https://www.bitcoinabuse.com/reports). Categorize reports. Groups addresses. Find connected addresses. Investigate some of the addresses or summarize/reproduce existing investigations.

OWN Suggest your own project.