Concordia University
Concordia Institute for Information Systems Engineering

INSE 6210: Cryptographic Protocols and Network Security
PROJECT DESCRIPTION
(Revision 1.0)

INSE 6210		**Winter 2023**
Instructor:	Ivan Pustogarov	ivan.pustogarov@concordia.ca
Project Report Due:		April 3 23:59
Project presentation dates (tentative):		April 04, April 11, during lecture time

Contents

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 "INSE6210-2023-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 $[F \ldots A+]$ 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 will be assigned one by the instructor. Students without teams will be grouped/added into teams.

Project 1 Attacks on DNS, DNS over TLS/HTTPS, and DNSSEC. Systematization of Knowledge (SoK).

In this project, you will need to:

- Review papers published in the last two years (at least) at major security conferences: IEEE S&P, ACM CCS, NDSS, etc.
- Implement at least one attack (can be done in a network simulator, e.g. `mininet`)

Project 2 . Crypto Attacks on TLS. Systematization of Knowledge (SoK). In this project, you will need to:

- Describe past attacks on SSL/TLS protocol (e.g. Padding Oracle, Poodle, etc).
- Review papers published in the last two years (at least) at major security conferences: IEEE S&P, ACM CCS, NDSS, etc.
- Implement at least one attack.

Project 3 . Tor and Tor Onion Services. Systematization of Knowledge (SoK). In this project, you will need to:

- Describe past attacks on Tor/Onion Services.
- Review papers published in the last two years (at least) at major security conferences: IEEE S&P, ACM CCS, NDSS, etc.
- Implement at least one attack.

Project 4 . Blockchain and its applications. In this project, you will need to:

- Analyze academic publications and software projects that use/claim to use Bitcoin as the underlying technology (e.g. voting protocols).
- Understand and explain why they use Blockchain and how it makes their approach/software better.

Project 5 . Bitcoin mixers (centralized and decentralized). Multicoin mixers. In this project, you will need to:

- Analyze academic publications and software projects that describe/implement Bitcoin mixers.
- Review papers published in the last two years (at least) at major security conferences: IEEE S&P, ACM CCS, NDSS, etc.
- For each type of mixers provide its level of anonymity.
- Analyze attacks on Bitcoin mixers.

Project 6 . Ethereum smart contracts. Analysis tools. In this project, you will need to:

- Describe common types of vulnerabilities in Ethereum smart contracts.
- Review smart contracts analysis tools (e.g. Manticore symbolic execution).
- Use one or more of these tools to rediscover known vulnerabilities and create an exploit.

Project 7 . Monero and ZCash. In this project, you will need to:

- Describe in detail how these protocols work. Differences and similarities.
- Recent attacks: review papers published in the last two years (at least) at major security conferences: IEEE S&P, ACM CCS, NDSS, etc.

Project 8 . Attacking SSL/TLS implementations. In this project, you will need to:

- Survey existing libraries that implement SSL/TLS protocol (e.g. in browsers, in IoT devices, etc.)
- Review past vulnerabilities in these libraries (both protocol-based, e.g. Padding Oracle, and software-based, e.g. memory corruption).

Project 8 . Wifi Security. In this project, you will need to:

- Review (in detail) existing attacks on WiFi WEP/WPA/WPA2.
- Reimplement crypto attacks on WEP: PTW and FMS/Korek.

Project 9 . Smart card reverse engineering/Analysis (NFC reader will be provided). In this project, you will need to choose a smart card (e.g. OPUS card) and reverse engineer its protocol. Your task is to understand how this system works, what information is stored, etc, and find vulnerabilities.

Project 10 . Suggest your own project.