

Project

INSE 6150: Security Evaluation Methodologies

Due: **Wednesday December 8.**

Upload on EAS by 15:00 (3:00 PM).

*Projects should be in PDF format and uploaded to the EAS system under "Project."
Please ensure you are registered for it well in advance of the deadline.*

EAS: <https://fis.encs.concordia.ca/eas/>

The project will consist of a written report. The subject of the report may be either a novel research topic or a systemization of knowledge. Research papers should contain an element of *security evaluation*, and not merely demonstrate an attack, vulnerability or tool for improving security.

Requirements:

- 1) You may work individually or in pairs.
- 2) The report should be no more than 8 pages. This is a maximum and shorter papers are acceptable.
- 3) You can use any template with normal margins and font sizes.
- 4) Review and understand how to avoid plagiarism:
<https://www.concordia.ca/encs/students/sas/expectation-originality.html>

Tips:

- 1) You can write a paper based on the research of others but do not write a "survey." A survey starts with a set of papers and reviews them. Instead, write a "systemization of knowledge (SoK)." An SoK starts with a topic and uses what others have written about the topic (while citing them) to present an interesting perspective on the topic.
- 2) To help understand the difference between a survey and SoK, pretend that the reader of your paper has actually read all of the references you cite in their entirety. For this reader, it is pointless to summarize the references because they already know them. Instead, you should focus on things they might have read but not really thought about: weaknesses in the papers, how the papers relate to each other, what the papers have in common, etc.

- 3) There is no requirements on how many other papers you draw from or if the type of papers they are, however you are responsible for checking to see if there are relevant academic papers on your chosen topic.
- 4) If you are describing the work of others, you should do it critically: having looked at a broad set of knowledge on the subject, compare and contrast individual contributions. You can be skeptical of what others have written—authors may miss or leave out important criteria in evaluating their own results.
- 5) If you are having difficulty selecting a topic, thumb through the proceedings of a security conference to see the types of things being explored in the research literature: *IEEE Symposium on Security & Privacy*, *USENIX Security*, *ACM CCS*, and *NDSS* are good places to start. Once you find a subject that is interesting, you can use Google Scholar to find papers (number of citations can be useful in seeing the impact of the paper) and once you have a few papers, pay attention to the “Related Work” section included in most papers to find other papers you might have missed (as well as seeing a summary of the research in the area).
- 6) I am here to help. You are not required to submit anything to me other than the final report. But I am happy to discuss your topic during office hours. I cannot review drafts of reports as there are too many students and it takes too much time.
- 7) It is not necessary but an approach that has worked very well for projects in the past is to phrase the topic of the report as a question. And then look for the answer by research and reading, and use the report to write a detailed answer to the question. If a particular paper you read doesn't help you answer the question, don't include it.
- 8) References can be in any format.
- 9) Security is a broad field. Be creative.

Grading:

Grading Scheme	
20	Scope and execution
10	Interpretation
10	Technicality
10	Presentation
50	Total

Scope and execution

A good project will have a clearly defined scope: what is on-topic for the project and what is off-topic. I recommend phrasing your project topic as a question and the project itself answers the question. The topic should be important and timely. With a well-defined topic, the paper should be organized with a logical flow through that links its material together. There should be a reason that each portion of the paper exists. The paper should be complete and comprehensive. The material will be appropriate to evaluation methodologies.

Interpretation

It is easy to read other research or technical documents and repeat what they say without truly understanding it. A good project will explain existing research in way that makes it clear that the writer really understands it. It will be selective in how much detail is included to ensure the main point of the paper is made.

Technicality

A good project will include technical details that appropriate for a graduate-level course in security. It will be correct in what it says.

Presentation

The deliverable should be high quality. It should be well written. Sections and subsections should provide a useful organization of the paper. Figures and tables should be used appropriately. Citations should be used appropriately. A good project will demonstrate an adequate level of work went into it (it is a project that is meant to be worked on for the whole course).