Total points: 100

CMPT473/982 (2026 Summer)

Assignment 1

Due: 11:59 PM, 15th June 2026 (Mon)

In this assignment, you will write a critique for an academic paper.

Choosing a paper

The paper you choose needs to satisfy the following criteria:

- It is in the field of security & privacy.
- It uses machine learning to solve the problem.
- It is published in an academic conference or journal.
- It is not on the list of papers we will discuss in class.

Please ask me if you are uncertain if a paper satisfies these criteria.

It is helpful to choose a paper that has published/shared its data and code.

Note that a review paper (including a Systematization of Knowledge paper) does not satisfy these criteria as it does not use machine learning on its own.

For a list of good security conferences, you may refer to online resources, such as Guofei Gu's rankings: `https://people.engr.tamu.edu/guofei/sec_conf_stat.htm`

You are not required to choose the best papers. Your critique will be graded with consideration for the quality of the paper.

Reading the paper

You can consider the following questions while reading the paper to help you understand the paper:

- What is the problem being solved? What are the other potential avenues for solving this problem? Why are they insufficient? Who is affected by this problem and how?
- What is the technical context of this problem? (For example, is it using cryptography? Is it using certain network protocols?) What are the capacities and limitations given by the technical context?
- What is the methodology? How do they solve the problem, and why is the approach meaningful? What do they do that is different from other works?
- What experiments did the authors conduct to support their claims?

- What are the conclusions/main contributions of this work, and how are they supported by the methodology and experiments?

And consider the following questions while reading the paper to help you identify issues for critique:

- Is the problem being solved important? What is the expected impact of this work? Are the paper's claims scientific, i.e. falsifiable?
- What are the assumptions made by the paper's threat model, experimental setup, and methodology? Are these assumptions reasonable? Are they shared by other works in the area?
- Is the methodology well suited to solving the given problem? Is the machine learning technique appropriate for the problem? How does the methodology compare to other works?
- Does the experimental setup match the paper's methodology? Is it representative of realistic settings? Does it create any experimental error? Is it replicable?
- Do the presented results support the paper's conclusions? Are they presented well? Are there any other results that could've either supported or undermined the paper?
- How is the structure, organization, and quality of writing?

Do not answer these questions directly in your critique; they are meant to help you find the issues. It is also very helpful to read related papers as a comparison.

Writing your critique

In the introduction of your critique, introduce the paper, briefly explain its claims, and introduce your main critiques. Organize the rest of the paper so that each section covers one (category of) critique. Justify your critiques.

Whenever possible, provide evidence for your critiques. This may involve writing code and downloading the data used for the paper.

Write your critique using the USENIX Template:

`https://www.usenix.org/conferences/author-resources/paper-templates`

There is no limit on page count. Do not include an abstract.

Submit a ZIP file that contains:

- A PDF of the paper you are critiquing.
- A PDF of your critique.
- Any code or supplementary material to support your critique.