UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

PhD Seminar 1

Tuesday July 12, 2022 at 2pm via Zoom

Mohammad Maghsoudimehrabani

A Framework for Quantitative Privacy Risk Assessment of Masked Language Models

Advisor: Dr. Ali Dehghantanha
Advisory: Dr. Xiaodong Lin
Advisory: Dr. Lei Lei [SoE]
Advisory: Dr. Gautam Srivastava [Brandon University]

Abstract:

Increasingly pre-trained Masked Language Models (MLMs) are used to support privacy-sensitive tasks in diverse applications in different domains ranging from legal to healthcare. This makes privacy an essential and influential element in developing MLM-based applications. However, there are a few works on measuring leakage and robustness of MLMs to privacy attacks. In this work, we present a framework for quantitative privacy risk assessment of MLMs.

Our framework quantifies the impact of privacy attacks and assesses the privacy risk in MLM-based models. It includes models to perform different privacy attacks and quantify the impact of those attacks; models to estimate the success or failure rate of different privacy attacks; and models to predict the value at risk for privacy attacks in MLM.