UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

PhD Seminar 1

Friday August 13, 2021 at 10AM via Zoom

Statistical Adversarial Machine Learning Against Authentication Systems

Sohail Yamin Habib

Advisor: Dr. Hassan Khan
Co-Advisor: Dr. Mihai Nica [Math & Stats]
Advisory Member: Dr. Andrew Hamilton-Wright

ABSTRACT:

Researchers have proposed machine learning based authentication systems that authenticate users based on their unique behaviour (e.g., keystroke or gait patterns). The uniqueness of behaviour biometrics has been challenged by recent works, where researchers have proposed statistical attacks that infer general population statistics to defeat these systems. However, we show that these attacks do not perform robustly against different types of biometrics due to the different nature of behavioural overlap in these metrics. Furthermore, no defense has been proposed to date that effectively defends against statistical attacks.

In this work, we propose a new statistical attack and show that unlike existing methods it: 1) is successful against a variety of behaviour biometrics; 2) is successful against more users; and 3) requires fewest attempts to successfully break a user. We also propose and evaluate a mechanism that is able to detect statistical attacks. False rejects in such systems are not uncommon and by distinguishing statistical attacks from false rejects, our mechanism helps to improve usability and security.

Our detection method needs only two unsuccessful statistical attack attempts to accurately detect 90% of statistical attacks attempts while incorrectly labelling only 5% of false rejects of a user as a statistical attack. The accuracy of our system scales when the number of rejected samples seen by the detection mechanism are increased thereby demonstrating its potential as an effective defense against such attacks.