UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

MSc Defence

Wednesday April 19, 2023 at 2pm via Zoom [Remote]

Jonah Stegman

Misleading Metrics: Quantifying Security of Behavioural Biometrics Against Adversarial Attacks

Chair: Dr. Fangju Wang
Advisor: Dr. Hassan Khan
Advisory: Dr. Rozita Dara
Non-Advisory: Dr. Charlie Obimbo

Abstract:

Behavioural biometrics is gaining popularity as the interaction with smartphones and other smart technologies increases. Behaviour biometrics, such as voice or how a person types, are used to authenticate users through binary classification using machine learning classifiers. Our research investigates the limitations of widely used metrics to evaluate these biometric authentication systems. We show that the contemporary metrics provide misleading results for five diverse biometric authentication systems including gait, mouse, keystroke, swipe, and voice biometrics. For instance, when we evaluate the voice biometric on a dataset of 22 users using mean Accuracy and Equal Error Rate metrics, the results are promising with the mean Accuracy score of 95% and mean Equal Error Rate of 0.04. However, a deeper analysis reveals that only four samples are required to bypass the whole population of 22 users using a simple brute-force attack. Our deeper analysis of ten metrics across five behavioural biometrics show that these metrics provide misleading results.

To better quantify the security of these biometrics, we propose four new metrics. These metrics include Bypass Rate of a Sample, Minimum Samples to Bypass N-Population, Coverage of Most Potent Sample, and Successful Victims Bypassed by an attacker. We revisit the security provided by behavioural biometrics using the proposed metrics and show that the proposed metrics provide much needed clarity in terms of the performance of these metrics against adversarial attacks. We perform experiments to show that these metrics perform well for different dataset sizes. Future evaluations of behavioural biometrics should consider reporting these new metrics to provide insights into the security of the biometrics.