UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

PhD Qualifying Exam

Tuesday May 31, 2022 at 9am via Zoom

Sohail Habib

Revisiting the Security of Biometric Authentication Systems

Chair: Dr. Joe Sawada
Advisor: Dr. Hassan Khan
Advisory: Dr. Andrew Hamilton-Wright
Non-Advisory: Dr. Charlie Obimbo
Non-Advisory: Dr. Radu Muresan [SoE]

Abstract:

Usage of behavioural biometrics as continuous secondary authentication is getting good traction. Diverse set of behavioural biometrics (e.g., voice, keystroke patterns, gait, gaze, etc.) have been proposed, with promising results. Like other security systems, their perceived security has been challenged by recent works. Works related to attacks tend to focus on specific biometrics, although this provides valuable insights into performance against the attack, but in the real-world applications an attacker might attack multiple behavioural biometric modalities and can use publicly available datasets for malicious purposes. The work on potential defences is also scarce. Another factor requiring attention is that the use synthetic data augmentation introduce vulnerability that can be exploited by the attackers.

With the rising adoption of behavioural biometrics and the lack of available research introduces wide gaps in the aforementioned areas. We address these gaps by researching new state of the art attacks and defences. We will develop two state of the art attacks with different assumptions to the data availability, and perform a vulnerability analysis of synthetic data augmentation techniques. Our first attack will assume that the attacker does not have access to victim's data. This attack will identify overlaps in general population's behavioural biometrics using either opensource datasets or through crowd sourcing. Identified overlaps will be used to mount a state-of-the-art statistical attack. We will compare our work with current state-of-the-art statistical attacks. This phase will also include work on first ever defence against statistical attacks.

The second attack will evaluate an insider threat. The insider can observe the victim, to identify key behaviours. Then the attacker would query opensource databases to find a close adversarial sample. For this work we will experiment with human participants by collecting behavioural biometric data, implement an authentication system and attacking it using human subjects. Imbalance in data for behavioural biometric-based security application is common, and often data augmentation techniques are used to balance the training data. It is well established that behavioural overlaps can open the possibility of a statistical attack. Yet, the impact of synthetic data augmentation on security is not well studied. We will evaluate the effect of data augmentation on security and identify best practices to avoid creation of any backdoor that can be used by the statistical attacks.