UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

MSc Defence

Wednesday August 11, 2021 at 2PM via Zoom

Skimming Smartphone PINs Using Machine Learning Techniques

Rawan Abulibdeh

Chair: Dr. Fangju Wang
Advisor: Dr. Hassan Khan
Advisory Member: Dr. Charlie Obimbo
Non-Advisory Member: Dr. Stacey Scott

ABSTRACT:

Personal Identification Number (PIN) authentication is not only used to authenticate mobile devices but also used in bank security (e.g., ATM cards), and security of physical assets (e.g., homes). Attacks on PINs have become more widespread. Mobile phones store nearly every aspect of personal data on them. Therefore, securing the PIN entry is an important consideration in this technological era. The use of a mobile device in any public area opens up the possibility of an attack.

In our work, we introduce a new video-based attack on a mobile device to decipher the PINs used for authentication on smartphones. Our approach varies from the previous works as it does not require any visibility of the device's screen or the hand of the person entering the PIN. By using just the tilt of the corners of the screen when a person enters their PIN, we identify the areas where the victim's hand touched the screen and as a result, predict the PIN entered. This strategy enables us to reduce the search space compared to an exhaustive search method by obtaining an average of 2-4 candidate keys for each key-press in a PIN. Our method resulted in a 75% accuracy rate of predicting which cluster group out of X cluster groups each key in the PIN belongs. Therefore, we are able to highlight the threat users face when entering their PIN in a public setting and show that hiding the screen during authentication provides no safety to the user.