A Closer Look at Mobile App Usage as a Persistent Biometric: A Small Case Study

Md A. Noor, G. Kaptan, V. Cherukupally, P. Gera*, T. Neal, University of South Florida

Mobile devices store, transmit, and manipulate sensitive data, resulting in novel user authentication approaches leveraging the user's behavior, such as patterns found in mobile app usage, to passively protect users from unauthorized device access. Because prior work assumes that human behavior is highly variable, many of these approaches use sliding window approaches to continuously discard outdated data. In contrast, we explore the possibility that persistent patterns of behavior actually *do* exist, as this could minimize authentication latency and help improve authentication accuracy. To evaluate our hypothesis, we extracted 2-dimensional matrices of hand-engineered features from the app use of 15 smartphone users (297 matrices per user on average, SD=70). These matrices were treated as images, where the pixels (i.e., elements of a matrix) represent the frequency of each unique app used (columns) at certain times of the day (rows), to train a convolutional neural network (CNN) via 5-fold cross-validation with shuffling. Thus, the order in which the images were processed by the CNN was random to minimize the network's ability to learn sequential patterns in user behavior. Our results yielded a 96.8% F-score without any sequential updates to the training data, suggesting that user behaviors may not be as sporadic as previously believed. To our knowledge, this is the first demonstration of persistent, mobile biometric behaviors.

Keywords: Biometrics, behavior, deep learning, mobile applications, mobile devices