Continuous Authentication on Mobile Devices

Dr. Terence SIM

Associate Professor

School of Computing, National University of Singapore

ABSTRACT

Today's mobile devices (aka smartphones) are typically protected by one-time authentication mechanisms, such as pins, passwords, or biometrics. This is inadequate, considering that smartphones are increasingly used to store sensitive personal data, as well as to conduct financial, medical, and government-related transactions. We propose a Continuous Authentication system for mobile devices that will increase both its security and user-convenience. The key idea is to utilize the many sensors on the smartphone to continuously and passively verify the presence of the authorized user. If the legitimate user is operating the smartphone, he/she will automatically be permitted to access sensitive data, and perform high-value transactions. If someone else is using the smartphone, he/she will be denied access to certain apps and data, while allowing the guest user to continue using low-value apps, such as playing games or watching videos. If a thief steals the phone, the phone will collect biometrics evidence to be used against the thief.

To implement a Continuous Authentication system, several challenges need to be solved: (1) how to combine multiple sensors to reliably determine the presence of the user; (2) how to authenticate while conserving battery power; (3) how the CA may be used to provide Authentication-as-a-Service to other apps; (4) how to encourage the widespread user-adoption of such a CA system.

Ten years ago, we have solved (1). Our current research focuses on the three other challenges. We invite partners from the industry join us in this research. In particular, we would like to implement a live CA system and trial it on hundreds of real users using real apps. Such a trial will help us improve both the technical and usability aspects of our CA system, and spread the benefits of CA to many people and apps.