2013/2014

Seminar Series

www.cs.unb.ca/
seminarseries

UNB Faculty of COMPUTER SCIENCE

Fredericton · New Brunswick · Canada

Memory Retrieval and Graphical Passwords

By: Elizabeth Stobert, PhD Student, Carleton University

Baton: Key Agility for Android Without a Centralized Certificate Infrastructure

By: David Barrera, PhD Student, Carleton University

Memory Retrieval and Graphical Passwords

Graphical passwords are an alternative form of authentication that use images for login, and leverage the picture superiority effect for good usability and memorability. Categories of graphical passwords have been distinguished on the basis of different kinds of memory retrieval (recall, cued-recall, and recognition). Psychological research suggests that leveraging recognition memory should be best, but this remains an open question in the password literature. This paper examines how different kinds of memory retrieval affect the memorability and usability of random assigned graphical passwords. A series of five studies of graphical and text passwords showed that participants were able to better remember recognition-based graphical passwords, but their usability was limited by slow login times. A graphical password scheme that leveraged recognition and recall memory was most successful at combining memorability and usability.

Baton: Key Agility for Android without a Centralized Certificate Infrastructure

Android's trust-on-first-use application signing model associates developers with a fixed signing key, but lacks a mechanism to transparently update the key or renew their signing certificate. As an advantage, this feature allows application updates to be recognized as authorized by a party with access to the original signing key. Changing keys or certificates requires that end-users manually uninstall/reinstall apps, losing all non-backed up user data. In this paper, we show that with appropriate OS support, developers can securely and without user intervention transfer signing authority to a new signing key. Our proposal, Baton, modifies Android's app installation framework enabling key agility while preserving backwards compatibility with current apps and current Android releases. Baton is designed to work consistently with current UID sharing and signature permission requirements. We discuss the technical changes made to Android, and remaining open issues such as key loss and signing authority revocation on Android.

Tuesday, August 6th @ 1:30pm
Gillin Hall (540 Windsor St.) , GC127