COLLEGE OF ENGINEERING
COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

CSE Dissertation Defense

Kassem Fawaz

Location Privacy Protection in the Mobile Era and Beyond

ABSTRACT: As interconnected devices become embedded in every aspect of our lives, they accompany many privacy risks. Location privacy is one notable case, consistently recording an individual's location might lead to his/her tracking, fingerprinting and profiling. An individual's location privacy can be compromised when tracked by smartphone apps, in indoor spaces, and/or through Internet of Things (IoT) devices. Recent surveys have indicated that users genuinely value their location privacy and would like to exercise control over who collects and processes their location data. They, however, lack the effective and practical tools to protect their location privacy. An effective location privacy protection mechanism requires real understanding of the underlying threats, and a practical one requires as little changes to the existing ecosystems as possible while ensuring psychological acceptability to the users. This thesis addresses this problem by proposing a suite of effective and practical privacy preserving mechanisms that address different aspects of real-world location privacy threats.

First, we present LP-Guardian, a comprehensive framework for location privacy protection for Android smartphone users. LP-Guardian overcomes the shortcomings of existing approaches by addressing the tracking, profiling, and fingerprinting threats posed by different mobile apps while maintaining their functionality. Other than mobile platform changes, LP-Guardian requires no changes in apps or service provider. We then propose LP-Doctor, a light-weight user-level tool which allows Android users to effectively utilize the OS's location access controls while maintaining the required apps' functionality. LP-Doctor builds on a two-year data collection campaign in which we analyzed the location privacy threats posed by 1160 apps for 100 users. For the case of indoor location tracking, we present PR-LBS (Privacy vs. Reward for Location-Based Service), a system that balances the users' privacy concerns and the benefits of sharing location data in indoor location tracking environments. PR-LBS fits within the existing indoor localization ecosystem whether it is infrastructure-based or device-based. Finally, we target the privacy threats originating from the IoT devices that employ the emerging Bluetooth Low Energy (BLE) protocol through BLE-Guardian. BLE-Guardian is a device agnostic system that prevents user tracking and profiling while securing access to his/her BLE-powered devices. We evaluate BLE-Guardian in real-world scenarios and demonstrate its effectiveness in protecting the user along with its low overhead on the user's devices.

Chair: Prof. Kang G. Shin

Friday, April 21, 2017 9:00 – 11:00 am 3725 Beyster Building