Title: Mechanisms for Resource Protection on the Android Platform

Speaker: Mr Li Xiaolei

Date/Time: 4 February 2015, Wednesday, 04:00 PM to 05:30 PM

Venue: Executive Classroom, COM2-04-02

Supervisor: Dr Liang Zhenkai, Associate Professor, School of Computing

Abstract:

As Android devices become increasingly popular worldwide, security issues also become severe. Threats to the sensitive resources, such as user privacy violation and premium service abusing, have become a big concern. Even though the Android system applies a permission-based model to regulate the resource access by Android applications (apps), malicious apps still get the chance to abuse the available resources. To address the threats to sensitive resources, in this thesis we propose new frameworks on the Android platform to enhance resource protection with trade-offs between security and usability.

To mitigate the threats to sensitive system resources (e.g., user contacts, location data) by aggressive apps, we propose a virtualization-based framework that provides a sandbox environment for Android resources. It simulates a virtual but consistent view of all available resources. The resource access by an app is confined inside its corresponding virtual view. This framework guarantees a baseline of transparent data protection with a high compatibility with the existing Android architecture.

For more important user credentials, such as confidential documents, apps have to fully access them to work properly. To allow for tighter control over the usage of these sensitive data, we design another partition-based framework to provide a tightly-controlled and resource-constrained environment that supports only limited functionality for authorized apps to operate on the sensitive data.

Specially, we build our prototype on the ARM TrustZone architecture, which provides a trusted environment with a strong security guarantee by the hardware-level protection. It provides a standalone constrained runtime environment which is completely separate with the Android OS. For adapting Android apps into this architecture, developers only need to re-organize a small portion of security-critical code into this resource-constrained environment. We have demonstrated that our proposed architecture is adoptable by legacy Android apps with little re-development efforts.
Finally, we design a scalable static analysis mechanism that provides comprehensive understanding on how real-world apps utilize the sensitive data, specifically, the impact of a set of operations on the sensitive data. With this comprehensive knowledge regarding the resource usage, users can properly assess the potential threats of unknown apps to their sensitive resources and have more confidence over granting sensitive resource access. Existing taint-based techniques only detect the presence of exfiltration flow for the sensitive data, but cannot detect how much sensitive data are leaked. Users need more intuitive measures to inform them which apps are going to leak more of their private information. We represent such impact as a sequence of operations on the sensitive data and design an efficient static analysis to automatically extract these operations. According to their different usages, we rank the potential risks of large-scale Android apps.

With the proposed solutions, we are able to reinforce the resource protection on the existing Android platform with different levels of security guarantees.