NATIONAL UNIVERSITY OF SINGAPORE

School of Computing

PH.D DEFENCE - PUBLIC SEMINAR

Title:	**Characterization, Detection and Exploitation of Data-Injection Vulnerabilities in Android**
Speaker:	Ms Behnaz Hassanshahi
Date/Time:	29 August 2016, Monday, 06:30 PM to 08:00 PM
Venue:	MR1, COM1-03-19
Supervisor :	Dr Yap Hock Chuan, Roland, Associate Professor, School of Computing

Abstract:

Android is a popular mobile platform for which a huge number of apps (applications) has been developed during the past few years. However, the complexity in Android programming increases the possibility for developers to introduce vulnerabilities. We present a novel analysis framework to detect and confirm data-injection vulnerabilities in benign Android apps. We study two important classes of such vulnerabilities and use our analysis framework to show that many existing apps are vulnerable. As we are able to find many such vulnerabilities, we believe that a significant number of Android apps can be exploited by such attacks.

First, we develop an automated vulnerability detection system for Android apps which not only finds data-injection vulnerabilities but also confirms them with a proof-of-concept zero-day exploit. Our tool employs a novel combination of static data-flow analysis and symbolic execution with dynamic testing. We also use several optimizations to tame the path explosion problem in symbolic execution. We show through experiments that this design significantly enhances the detection accuracy compared with an existing state-of-the-art analysis.

Next, we present a detailed study of a new class of application vulnerabilities in Android that allows a malicious web attacker to exploit app vulnerabilities. It can be a significant threat as no malicious apps are needed on the device and the remote attacker has full control on the web-to-app communication channel. Analyzing real apps from the official Google Play store ? we found many confirmed vulnerabilities which suggest that these attacks are easy to mount and developers do not adequately protect apps against them.

Finally, we conduct a systematic study of the attacks targeting databases in benign Android apps. We present a comprehensive classification of database attacks. These attacks can be triggered either from content providers or intents received throughout the app. In order to

detect and exploit zero-day database vulnerabilities, we utilize our analysis framework and extend it with models for symbolically executing operations on the URI-based objects that are involved in database management. We evaluate our analysis framework by analyzing real-world Android applications and generating the corresponding proof-of-concept exploits. We also compare our results with a related work. We find both public and private database vulnerabilities. We also show new ways to exploit the previously reported and fixed vulnerabilities.