

**A Novel System for Assessing the Security of Android Apps (PI: Dr. Chang Kow Chuen Rocky; 2012/13)**

Smartphone is becoming an indispensable device to lots of people for managing their daily activities. At the same time, it is reported that attacks targeting on smartphones---especially those using the Android platform whose market share is more than 50%---have been increased drastically. Since the first Android malware discovered on 9 August 2010, Juniper Networks recently reported a 3,325 percent increase in malware aiming at the Android platform in the second half of 2011. Although the industry and academia have developed several products and prototypes for detecting Android malwares, their detections rely on identified patterns for discovering malwares. Therefore, an attacker can easily evade these systems by changing the patterns through either source code or call sequences. Moreover, they cannot detect brand-new attacks. In this project, we take a different approach to increasing the security of Android Apps. Instead of detecting malwares based on known patterns, our approach proactively identify possible system vulnerabilities in Android Apps which could be exploited by existing or new malwares for various types of attacks. Therefore, patching these vulnerabilities is a much more effective approach than detecting individual malware. The main deliverable of this project is a novel system for assessing the security of Android Apps. This system will automatically collect Apps from major Android markets and perform vulnerability analysis. It adopts two key methodologies to build a vulnerability library, including whole-system analysis and instance-based learning. The former determines vulnerabilities by modeling the relationships among elements in Apps and those between Apps and the Android platform, whereas the latter generalizes existing attacks to

recognize vulnerabilities in Apps. Based on the vulnerability library, the system applies static and dynamic program analysis techniques to determine whether an Android App has one or more vulnerabilities. Our preliminary results are very encouraging: new vulnerabilities detected in more than one hundred of popular Apps, including anti-malware Android Apps used by millions of users.