Smartphones have become an emerging platform for both personal and business applications. As the most popular mobile operating system for smartphones, Android offers great flexibility not only for users but also for application developers. However, this flexibility exposes users to additional security threats. This poster describes our ongoing research effort towards Android security issues. We first instantiate two types of possible attacks that can be launched on current Android applications available on the market. To further explore the vulnerabilities, particularly in the finance and health sector, we are developing a tool that leverages data mining techniques to automatically extract and analyze the security information of these applications, in order to detect and report the potential security threats. Moreover, we have analyzed and categorized more than a dozen security solutions proposed by different research groups. This poster provides a concise overview of this survey result. Most tools prevent potentially malicious attacks by educating developers to write more secure Android applications. The second proposed research direction is developing an Eclipse plug-in to provide Security on several levels. We first instantiate two types of possible attacks that can be launched on current Android applications available on the market. 

Multilevel Android Exploit Protection

Boston University – Metropolitan College (MET)

Felix Rohrer, Nebiyu Feleke, Kenneth Nimley
Supervised by: Yuting Zhang, Lou Chitkushev, Tanya Zlateva

Android Overview
Operating System for Mobile Devices
Based on Linux

Android Market reached 10 Billion App downloads by December 2011
Growth rate of 1 Billion App downloads per month
450'000 Apps

Market Share of Smartphones by Platform
Juniper Networks – 2011 Mobile Thread Report

Android Security
Each App runs in its own Virtual Machine (Dalvik), therefore isolated from other Apps.

Inter-application communication provided by Android Framework (very flexible but introduces vulnerabilities)

Resources are labelled with permissions (i.e. INTERNET, RECEIVE_SMS)

Malware analysis
Source: Juniper Networks – 2011 Mobile Thread Report

Types of Malware (2011)
- SMS Flooder
- SMS Trojan
- Worm
- Spyware

SMS Trojans and how they operate
- Send to premium number
- Send to third-party
- Matches user expectation

Cumulative Android Malware Increase
June - December 2011

Our current research (focus: Finance and Medical sector)

Educate developers to write secure Code

Proposed work

- Provide Security on several levels
- Create an access control based on roles in order to simplify dealing with permissions
- Minimize energy consumption of solution by introducing probabilistic security checks