ScanDroid: Static Analysis Tool to Promote Secure Android Development

Work-In-Progress
Edward Hill, Keheira Henderson, Xiaohong Yuan
North Carolina A&T State University
Introduction

- Mobile devices are now storing a lot of sensitive data
- Security vulnerabilities in the mobile apps will lead to leakage of user’s sensitive data
- Improper designs lead to security vulnerabilities in mobile apps
- We are developing a tool help Android application developers to develop secure Android apps.
Background

- The CERT Oracle Secure Coding Rules for Android
- CERT published 23 rules for secure coding
- Example rules are:
  - Secure externally stored data
  - Do not send sensitive data implicitly
  - Do not log sensitive data
  - Restrict access to applications
  - Secure applications from being debugged
  - Secure webview activities
Background

- **Static Analysis**
  - **Copes**
    - Detects permission gaps where applications are given more permission than they need to function
  - **Brox**
    - Detect if application requested location, deviceID, contact information and send it via network or SMS
  - **LeakMiner**
    - Detect if applications requested that the location, deviceID, contact information, calendar or sms is sent to log files
  - **FlowDroid**
    - Has a large library of sources and sinks to determine any data leakage.
  - **TaintDroid**
    - Detect when sensitive data is leaving the system with the assistance of third party applications
Methodology

![Diagram showing the methodology process]

1. **APK** → **FlowDroid** → **Parse For Information Leakage**
2. **Parsing Based on CERT Rules** → **Integrated Report**
ScanDroid parses the output of FlowDroid.

It looks for any leakage of the GPS or DeviceID to either a log file or via implicit intents.

This can capture data leakage even if the GPS or DeviceID data is stored in a different class.
Future Work

- Finish implementing all the algorithms and add more algorithms as CERT rules are finished
- Test the tool regarding false positive and false negative
- Compare the tool with other static analysis tools for android programs