Information Flow Security for Android Apps
David Orshan, Julian Sexton (Advised by Prof. Dave Naumann)

Introduction
• Android is an operating system designed for smartphones.
• Android is open source, and applications are written in the Java language.
• It is relatively new, and has only been around since 2008, so security flaws are not widely known among developers.
• This is part of a project to create a tool that will analyze the security of a given android application, funded by the National Science Foundation.
• This project's goal was to create apps as test-cases for analysis later.

Malicious Apps

Contact Stealer
- Accesses and broadcasts contact information without permission.

Usage App Breaker
- Tricks Usage App into counting extra messages.

Evil GPS App
- Appears to be an app that tells you how far away you are from a place.
- Actually works with another app to broadcast the phone's location.
- Neither app has permission to use both the GPS and text messages.

Friendly Apps

Anonymous Texting App
- Sends anonymous text messages.

Usage App
- Monitors in-call time as well as the number of text messages.
- Followed recommended practices for defending against attacks.
- Can still be tricked by a malicious app

Conclusion
- Current “best practices” can fall short of providing sufficient security
- The Android interface features more open communication between apps, which can be exploited in subtle ways.
- Something more fine-grained than a permission system is necessary.