Taking Advantage of App Stores for Increased User Security and Privacy
Patrick Mutchler, John Mitchell, Alex Aiken, Jason Franklin, Saswat Anand, Manolis Papadakis, and Lazaro Clapp

The Problem:
The Android Permission system provides inadequate information and guarantees about the behavior of a program. It is impossible for a user to know how an app uses sensitive data. Users must expose themselves to data theft to use most apps.

An Observation:
Apps are delivered to users through a centralized and trusted app store instead of an untrusted site. We now have hours or days to analyze programs rather than moments. More powerful program analysis techniques can be used to audit apps and provide guarantees for users.

STAMP: An auditing platform for Android Apps.

Challenges:
- Implicit control flow
- `startActivityForResult()` -> `onResult()`
- Modeling the Android API
- `sendSmsMessage()`
- Giving auditors useful information (too much of a good thing)
- Handling parameter dependent behavior
- `query("contacts") vs query("messages")`

Observations and Results:
- ~500,000 lines of code analyzed using STAMP
- Many data flows can be found with simple techniques.
- Android apps are usually small, making scalability much easier
- Dynamic data can be very useful to an auditor. We are building a system for collecting real user traces for dynamic results