Android Security

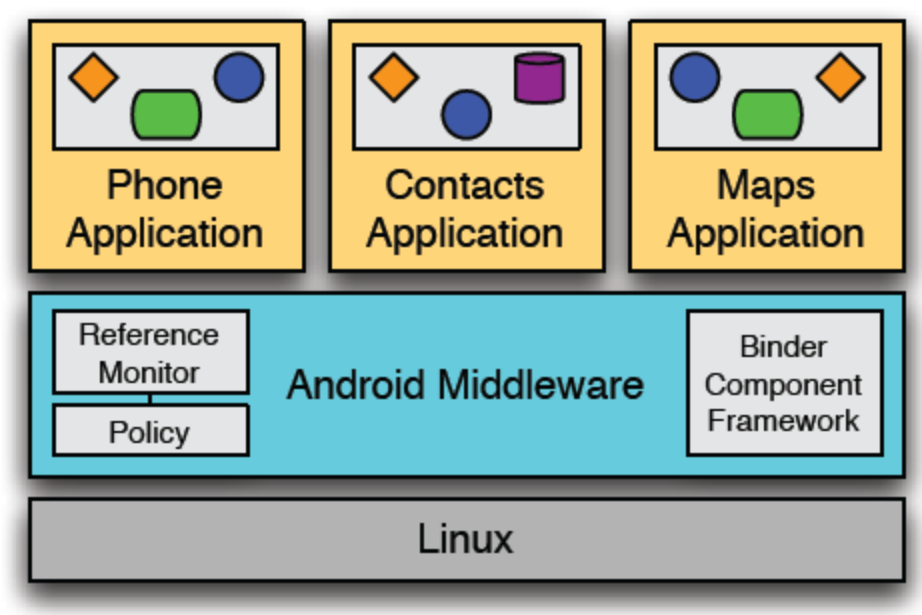
Brett Parker
Tyler Maclean
Ted Stein

Outline

- Android Overview
- Android Permissions
- Kirin
- Our work

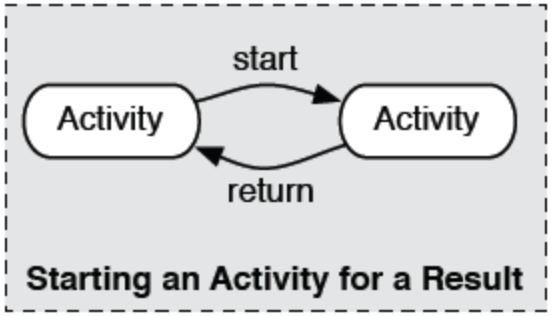
Android Overview

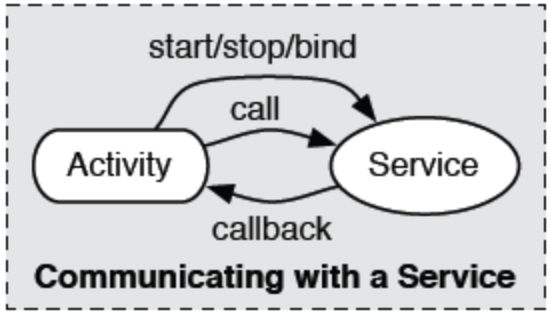
- Android platform is “middleware” between Linux kernel and applications

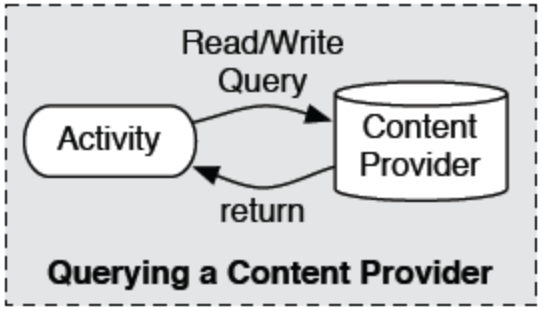


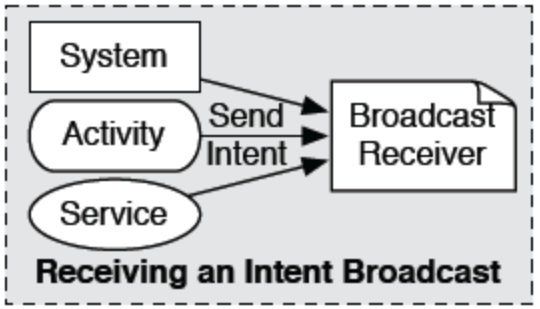
Android Overview

- Interactions based on 4 “component types”
  - Activity
  - Service
  - Content Provider
  - Broadcast Receiver





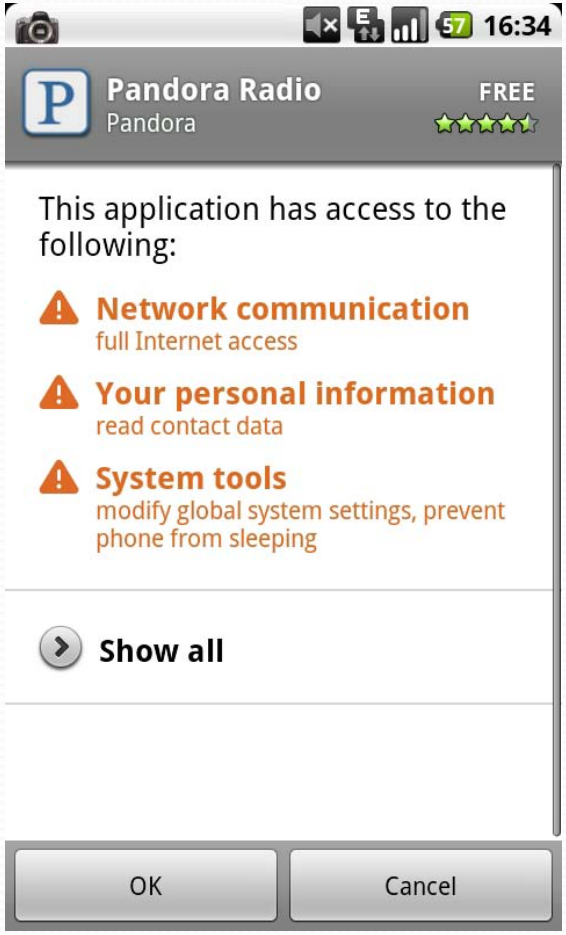




Android Permissions

- Fine-grained permissions for over 100 different sensitive functionalities
- Android apps can define custom permissions
- Android apps must declare each permission it wants to use at install time (list presented to user)
- File that declares these permissions is immutable after install
- Apps are completely trusted with the permissions they have been given

Android Permissions



Kirin

- Hooks into Package installer
- Maintains database of “dangerous combinations of permissions”
  - Ex: PHONE_STATE + RECORD_AUDIO + INTERNET
- At install time, if an app requests a “dangerous combination” of permissions, it denies installation

Kirin

- Limitations
  - Only checks permissions at install time
  - Cannot stop any other use of malicious permissions at run time
  - Does not do any logging or profiling

Our work

- Phase 1
  - Monitor all privileged access
- Phase 2
  - Inform the user of such access
- Phase 3
  - Provide facilities for blocking dangerous access

Our work

- Phase 1
  - Exploring Android permissions architecture to determine central points in the code
  - Find a place to “hook in” to monitor permissions

Our Work

- Phase 2
  - Inform the user of attempts at privileged access using pop-up notifications or “Toast” widgets

Our Work

Pop-up notification

Toast widget

Our Work

- Phase 3
  - User confirmation of actions – ability to block dangerous activities
  - Give user ability to create rules that automatically block such activities