On Lightweight Mobile Phone Application Certification

William Enck, Machigar Ongtang, and Patrick McDaniel

Mobile Phone Threats

- Cabir
  - Used on Symbian platform
  - Did not exploit code
  - Repeatedly request file transfer via Bluetooth
- Other viruses more malicous

Threat Down

- Proof of Concept
  - No damage done
  - Proves that attack vector exists
- Destructive
  - Delete data
  - Mostly harmless
- Spyware
  - Bugging the phone via software

Threat Down II

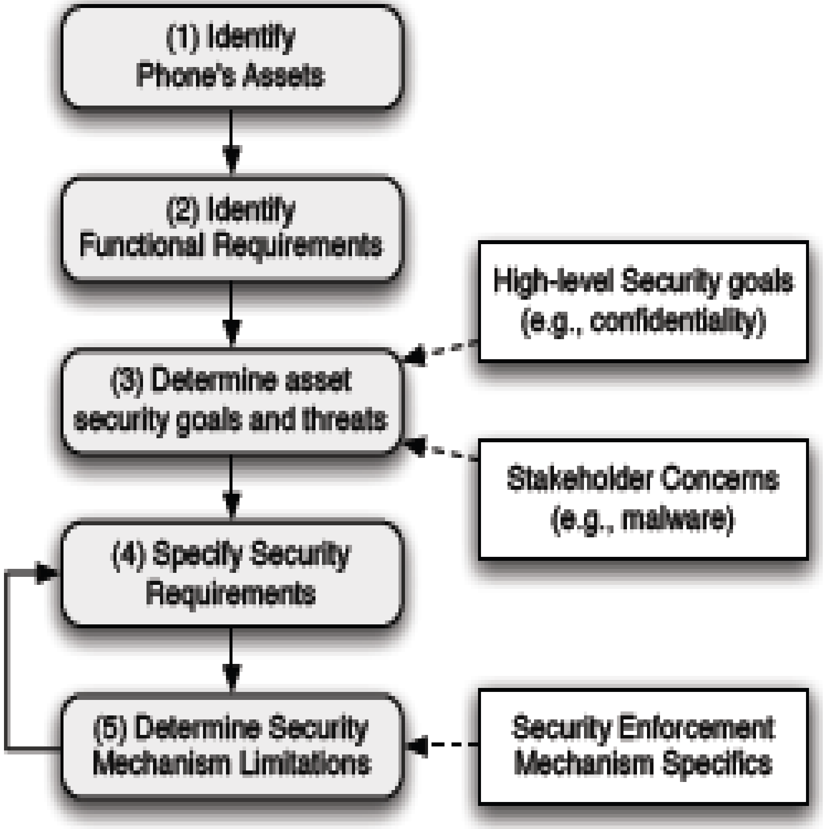
- Direct payoff
  - Calling premium services
  - Directly generate revenue for attacker
- Information Scavengers
  - Steal user data like contacts
- Ad-ware
- Botnet
  - Voice spam

Why Kirin?

- Android defines sets of permissions
- Permissions are static
- Certain combinations can be used maliciously

Security requirements engineering

- Three basic concepts
  - Assets
  - Functional Requireme
  - Security Requirement


(1) Identify Phone's Assets
(2) Identify Functional Requirements
(3) Determine asset security goals and threats
(4) Specify Security Requirements
(5) Determine Security Mechanism Limitations
High-level Security goals (e.g., confidentiality)
Stakeholder Concerns (e.g., malware)
Security Enforcement Mechanism Specifics

Assets

- Extracted from Android platform
  - Permissions
  - Intents
  - Components
- Example: Microphone Input, call activity

Functional Requirements

- Descriptions of how Assets interact with rest of the system
- Example:
  - Redirecting international calls to calling card number
  - Recording audio using MediaRecorder API

Determine Assets Security Goals and Threats

- Consider things such as confidentiality, integrity, and availability.
- How can functional requirements be abused
  - Threat descriptions

Develop Asset’s Security Requirements

- Define what combination of permissions might be harmful
- Example:
  - Receive phone state
  - Record audio
  - Access the Internet

Determine Security Mechanisms

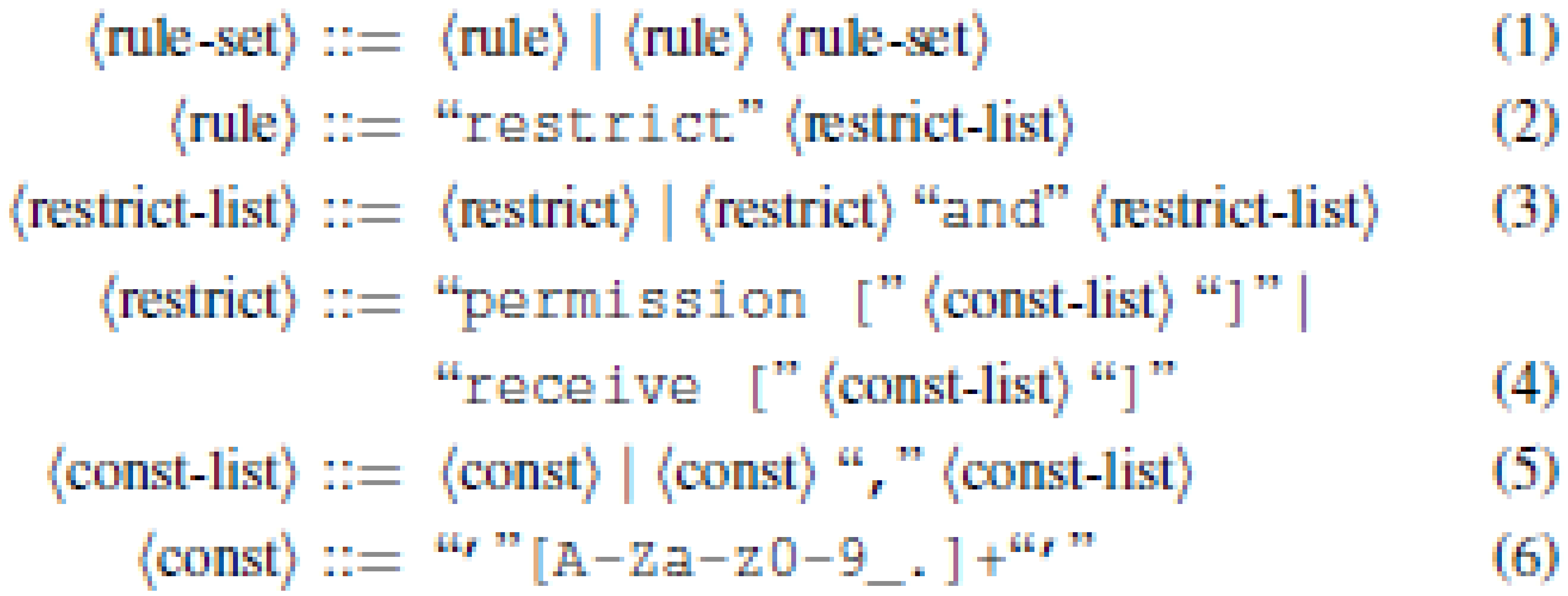
- Limited by PackageInstaller
- Permissions only set at install time
- Can’t set policies not defined in by Android
  - Monitoring how many SMS messages sent during a set time period

Kirin Rules

- Dangerous combination of permissions
  - GPS + Internet + Start On Boot
  - Install Shortcut + Uninstall Shortcut
  - Debug

Kirin Rule Syntax

- KSL – Kirin Security Language



⟨rule-set⟩ ::= ⟨rule⟩ | ⟨rule⟩ ⟨rule-set⟩ (1)

⟨rule⟩ ::= “restrict” ⟨restrict-list⟩ (2)

⟨restrict-list⟩ ::= ⟨restrict⟩ | ⟨restrict⟩ “and” ⟨restrict-list⟩ (3)

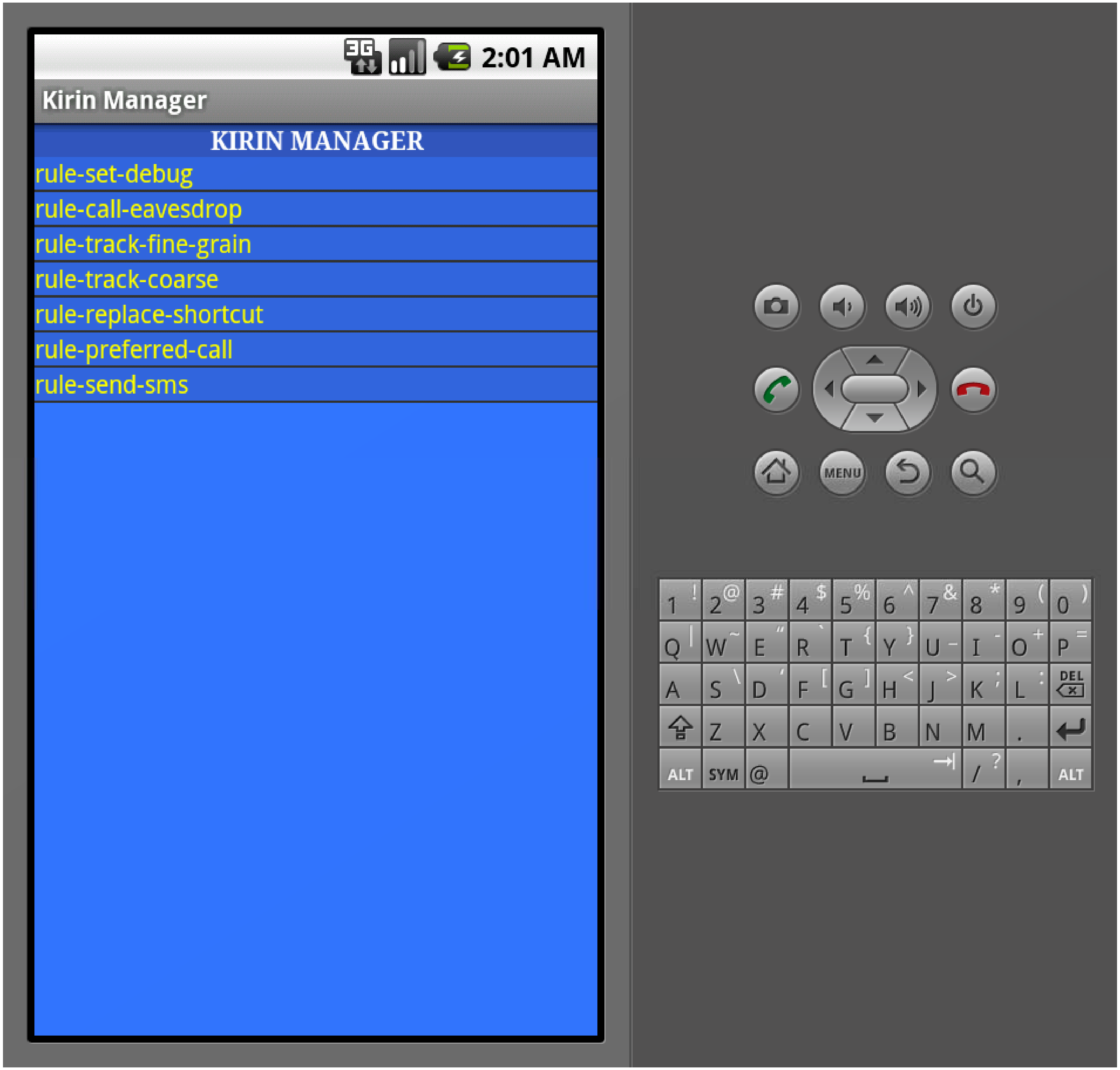
⟨restrict⟩ ::= “permission [” ⟨const-list⟩ “]” |
“receive [” ⟨const-list⟩ “]” (4)

⟨const-list⟩ ::= ⟨const⟩ | ⟨const⟩ “,” ⟨const-list⟩ (5)

⟨const⟩ ::= “'”[A-Za-z0-9_.]+“'” (6)

Kirin Security Service

- Three components
  - Service and ContentProvider that is a database of rules
  - Patches to the PackageInstaller application
  - Activity to manage the rules



Kirin Manager

KIRIN MANAGER

rule-set-debug

rule-call-eavesdrop

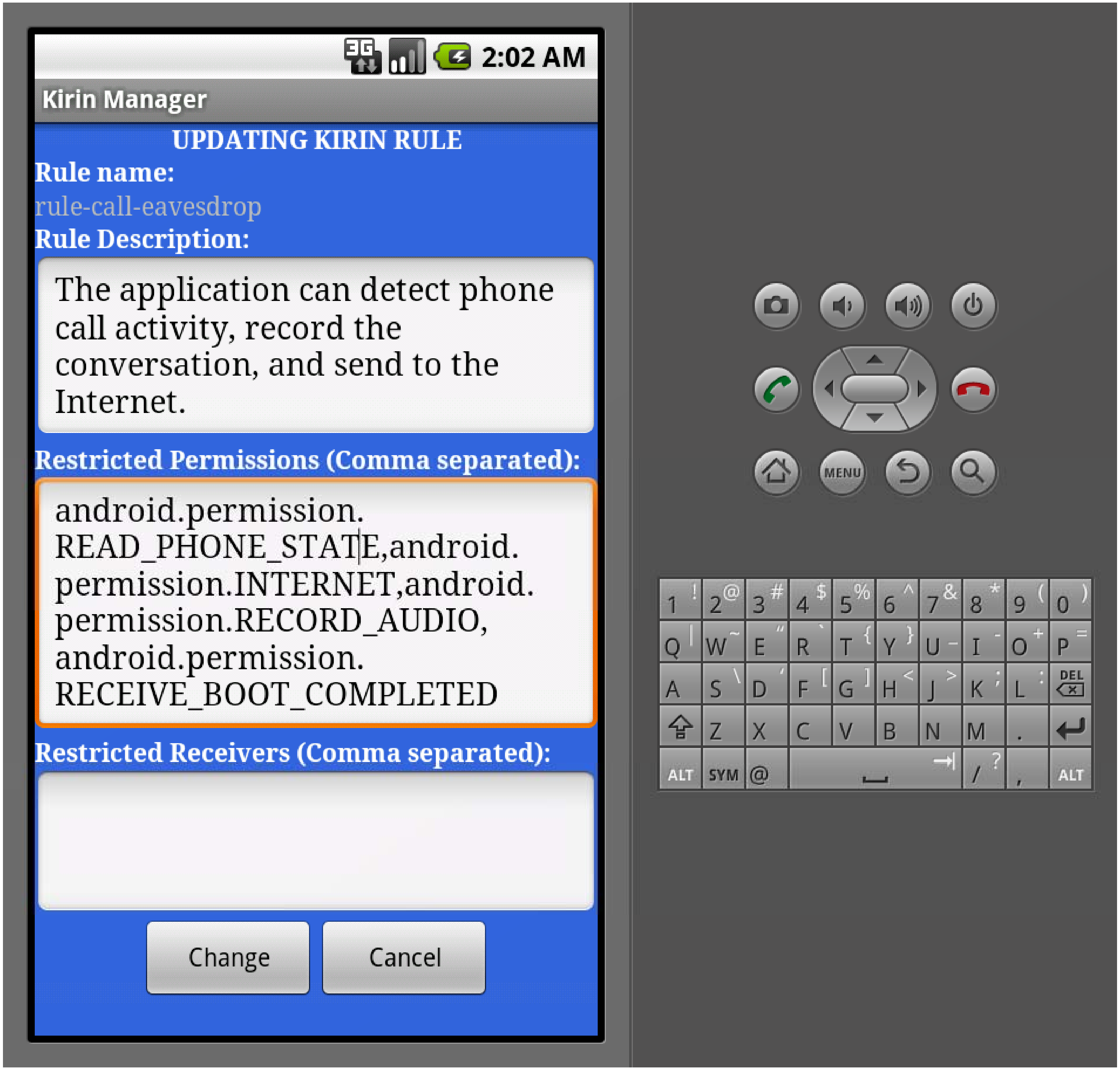
rule-track-fine-grain

rule-track-coarse

rule-replace-shortcut

rule-preferred-call

rule-send-sms



UPDATING KIRIN RULE

Rule name:

rule-call-eavesdrop

Rule Description:

The application can detect phone call activity, record the conversation, and send to the Internet.

Restricted Permissions (Comma separated):

android.permission.READ_PHONE_STATE,android.permission.INTERNET,android.permission.RECORD_AUDIO,android.permission.RECEIVE_BOOT_COMPLETED

Restricted Receivers (Comma separated):

Evaluation

- Assumed apps in market do not contain malware
- Investigate further apps not passing security rules
- Downloaded top 20 apps from each of the 16 categories, 311 total

Empirical Results

- 12 failed to pass
- 3 failed Rule 2
  - Phone State + Record Audio + Internet
- 9 failed Rules 4 and 5
  - Access {fine, coarse} location + Internet + Receive Boot Complete

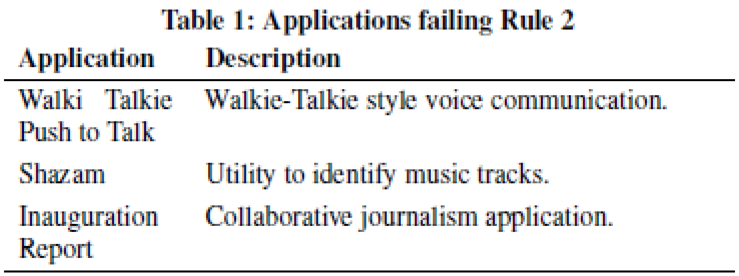


Table 1: Applications failing Rule 2

Application	Description
Walki Talkie Push to Talk	Walkie-Talkie style voice communication.
Shazam	Utility to identify music tracks.
Inauguration Report	Collaborative journalism application.

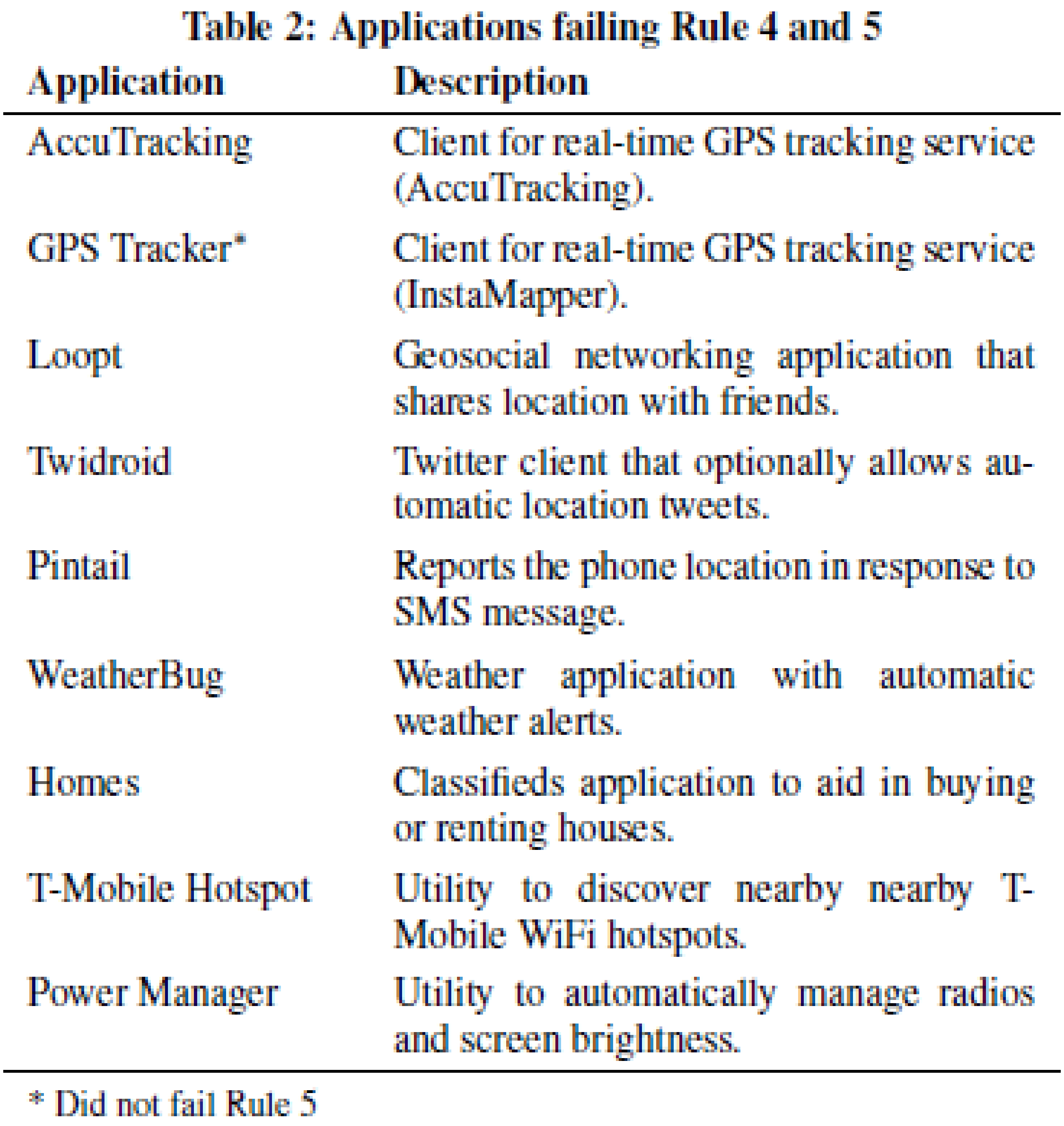


Table 2: Applications failing Rule 4 and 5

Application	Description
AccuTracking	Client for real-time GPS tracking service (AccuTracking).
GPS Tracker*	Client for real-time GPS tracking service (InstaMapper).
Loopt	Geosocial networking application that shares location with friends.
Twidroid	Twitter client that optionally allows automatic location tweets.
Pintail	Reports the phone location in response to SMS message.
WeatherBug	Weather application with automatic weather alerts.
Homes	Classifieds application to aid in buying or renting houses.
T-Mobile Hotspot	Utility to discover nearby nearby T-Mobile WiFi hotspots.
Power Manager	Utility to automatically manage radios and screen brightness.

* Did not fail Rule 5

Mitigating Malware

- Only protects against complex attacks
- Useful in stopping some attacks like SMS spam or information gathering
- No runtime logic
  - Limitation of Android, not Kirin