Contextual Policy Enforcement in Android Applications with Permission Event Graphs

Kevin Chen, Noah Johnson, Vijay D'Silva, Shuaifu Dai, Kyle MacNamara, Tom Magrino, Edward Wu, Martin Rinard*, and Dawn Song

University of California, Berkeley
*Massachusetts Institute of Technology

Android

Figure: Google Play App Market Growth

Android Malware

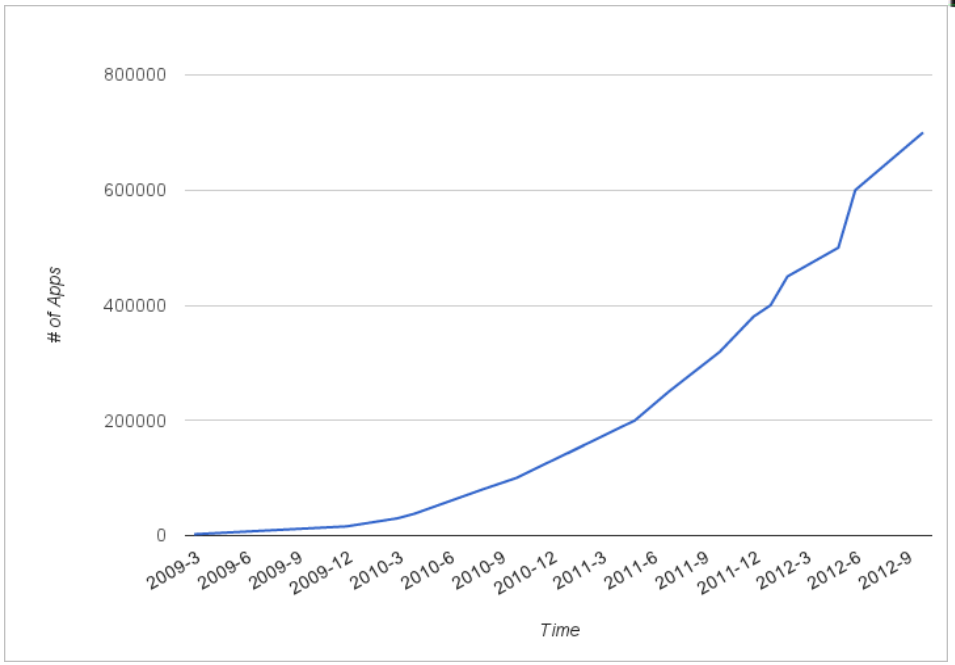


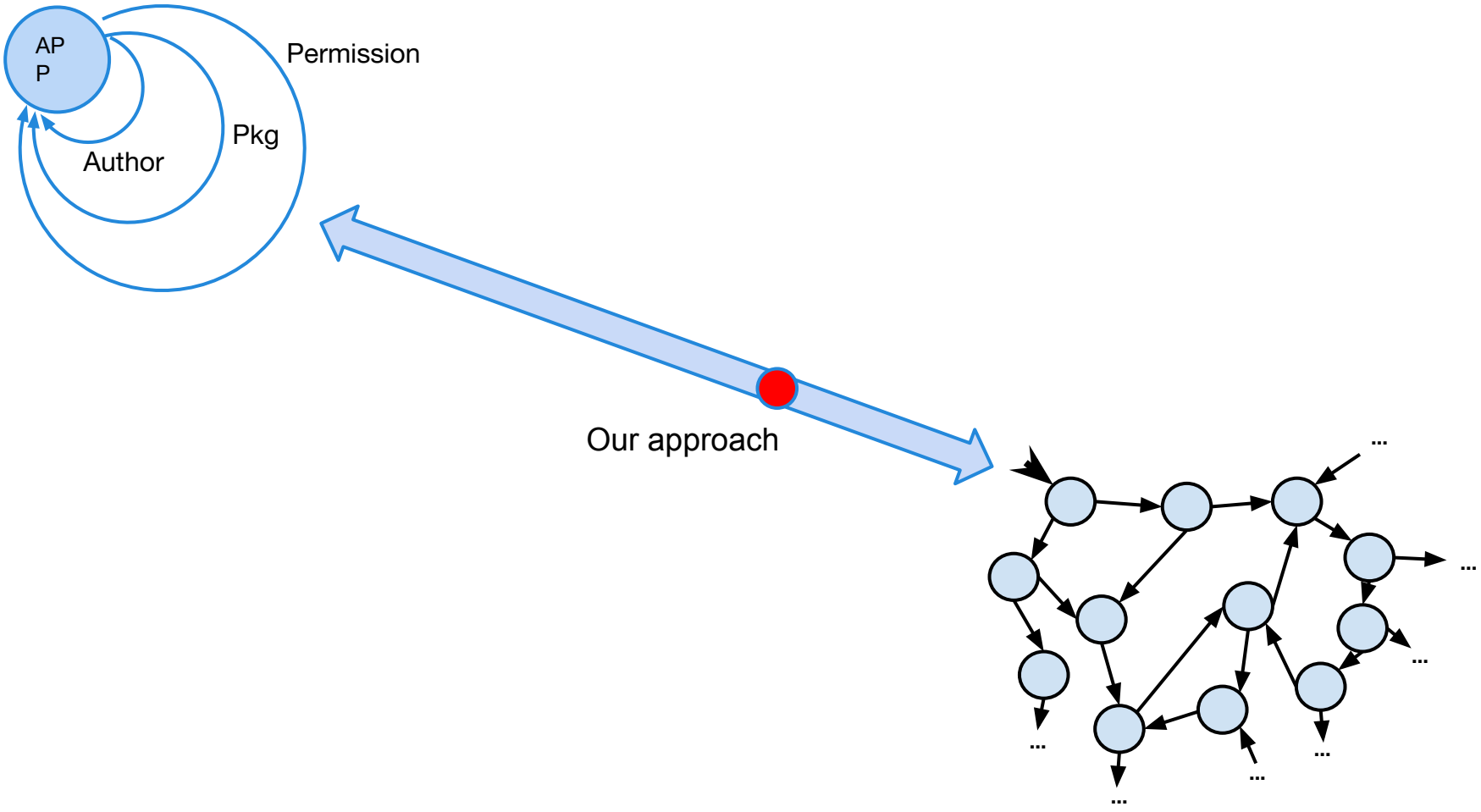
Figure: Google Play App Market Growth

"2577% growth over 2012" -Cisco Security Report 2013

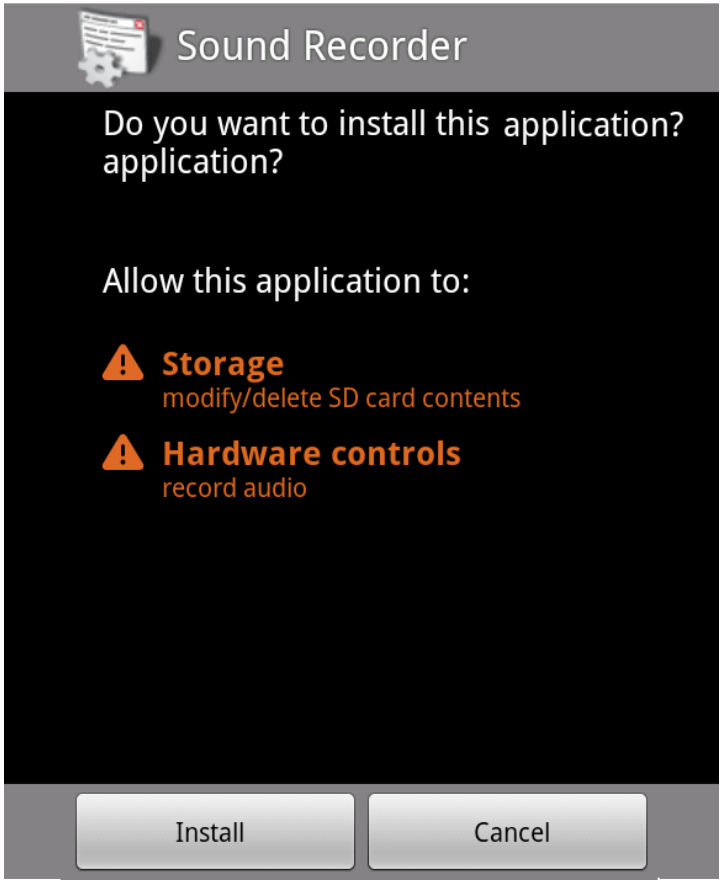
"Android malware cases to hit 1 million in 2013"

-Trend Micro Annual Threat Report

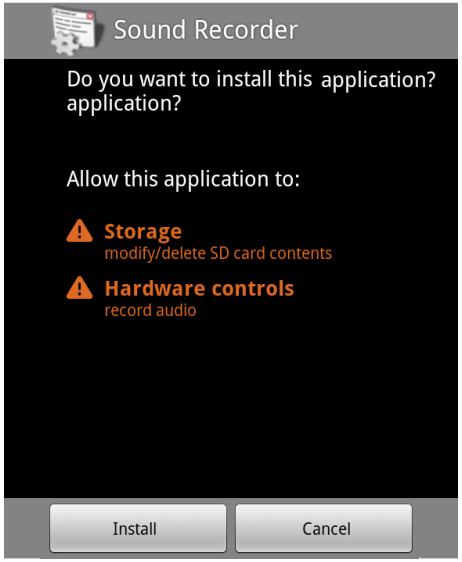
Android Malware Detection



Undetected Malware Example



User Intended Policy

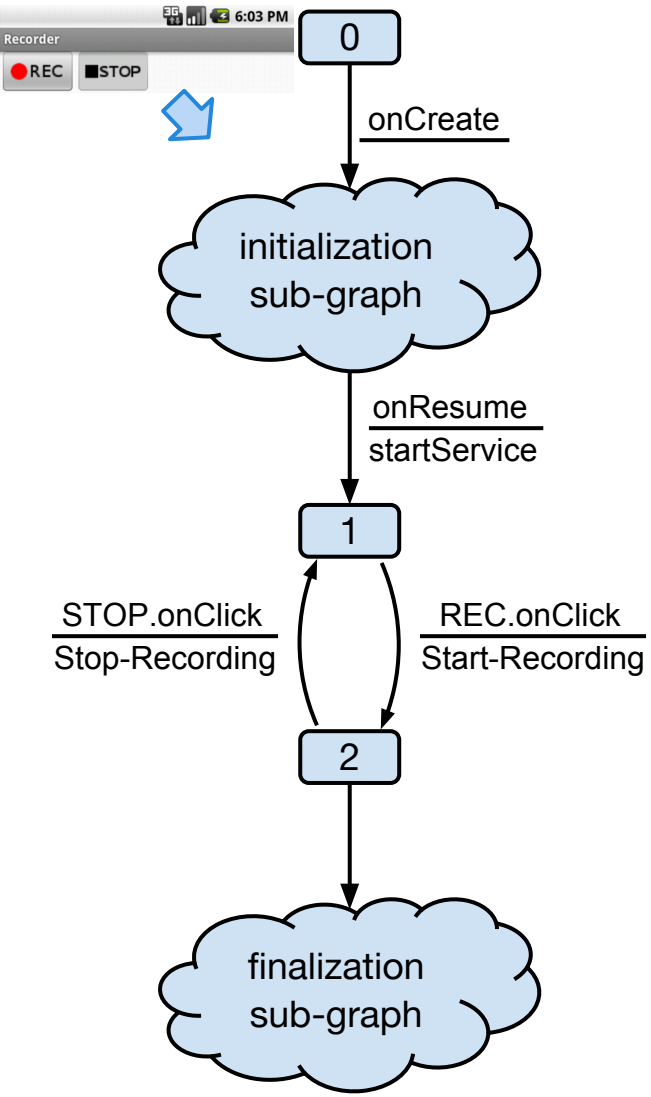


"The recording can only be started by clicking the REC button, and it will be stopped when the user clicks the STOP button."

Intuition

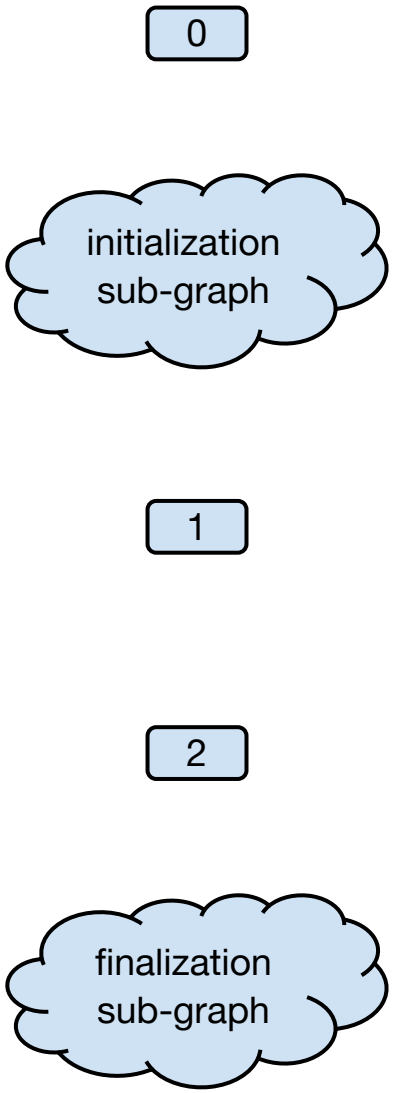
A **representation** that summarizes the **event dependencies** and their **API/permission** level behaviors (*The Permission Event Graph*), and a policy language based on that.

Permission Event Graph (PEG)

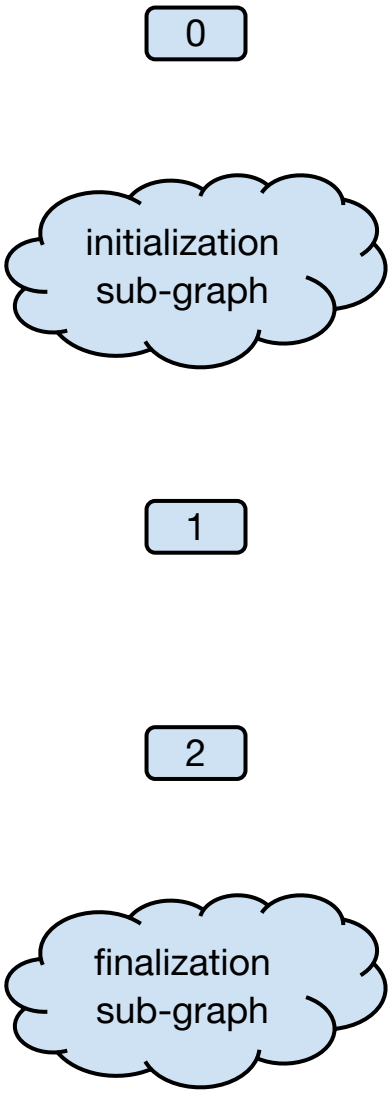


"The recording can only be started by clicking the REC button, and it will be stopped when the user clicks the STOP button."

PEG: States



PEG: States



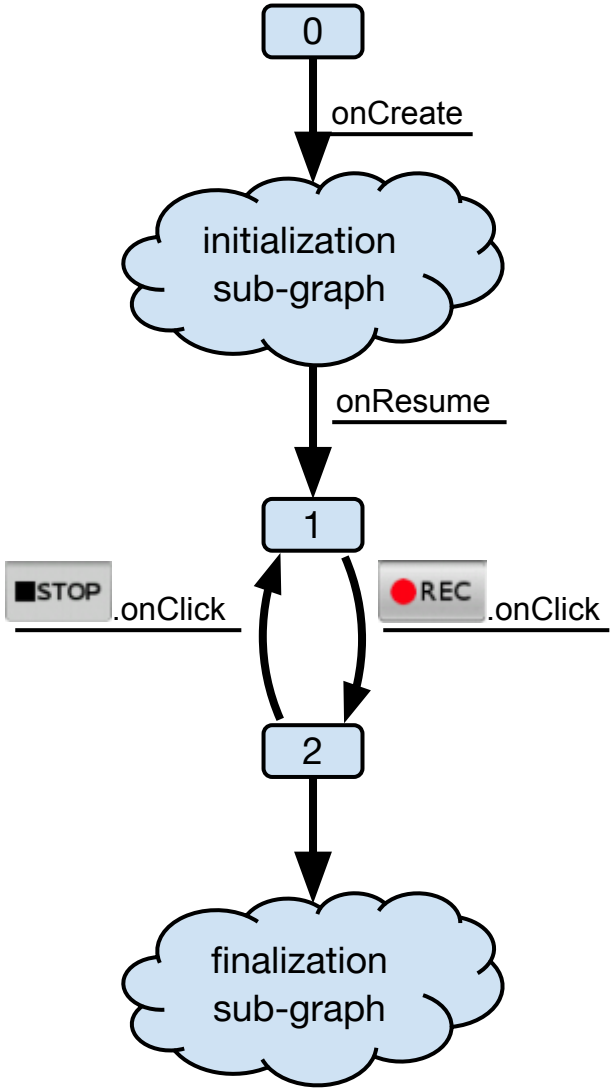
State *s*: {true, false} ^ ModeVar

Predicate abstraction of event states.

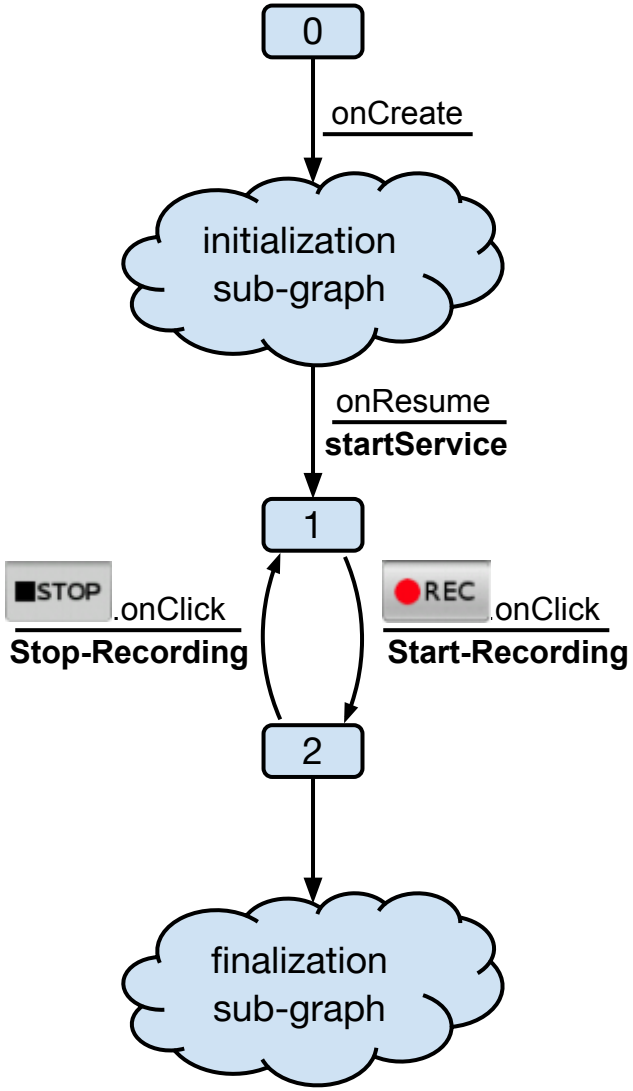
e.g.

- *Button.registered,*
- *Activity.foreground,*
- *API.called*

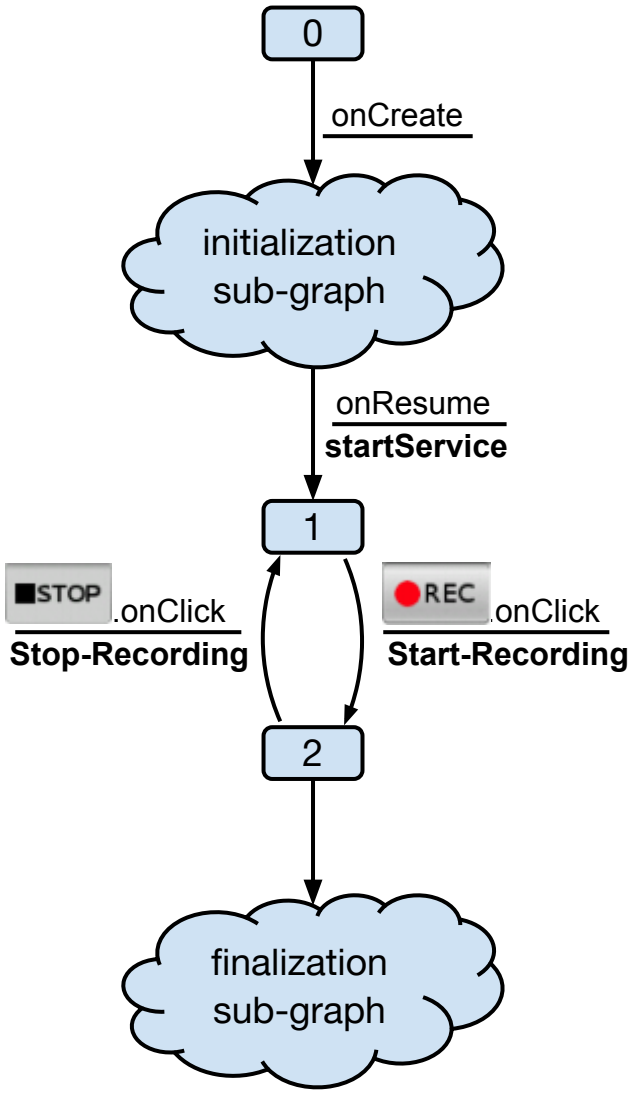
PEG: Transitions



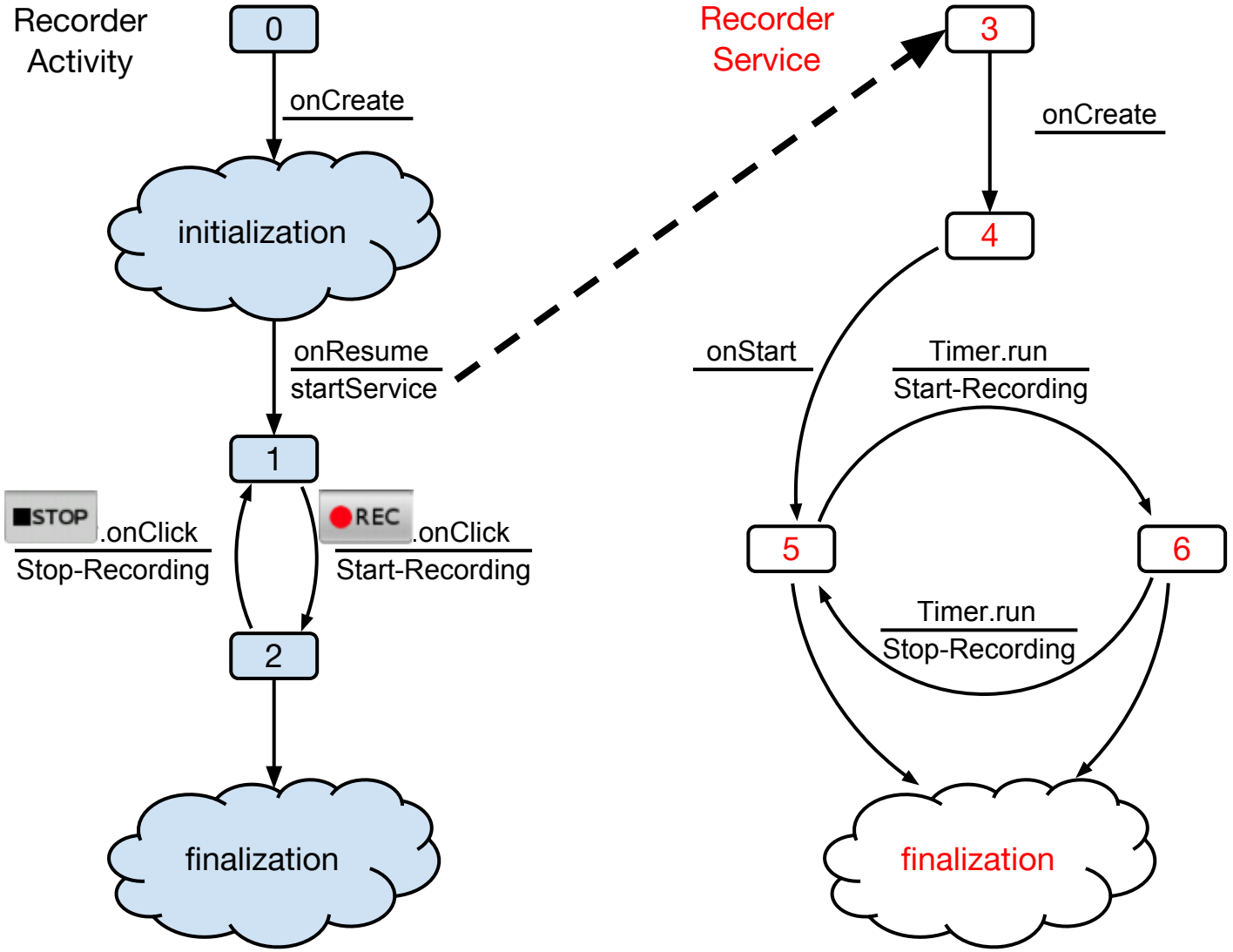
PEG: Labels


0
onCreate
initialization sub-graph
onResume
startService
1
STOP
.onClick
Stop-Recording
REC
.onClick
Start-Recording
2
finalization sub-graph

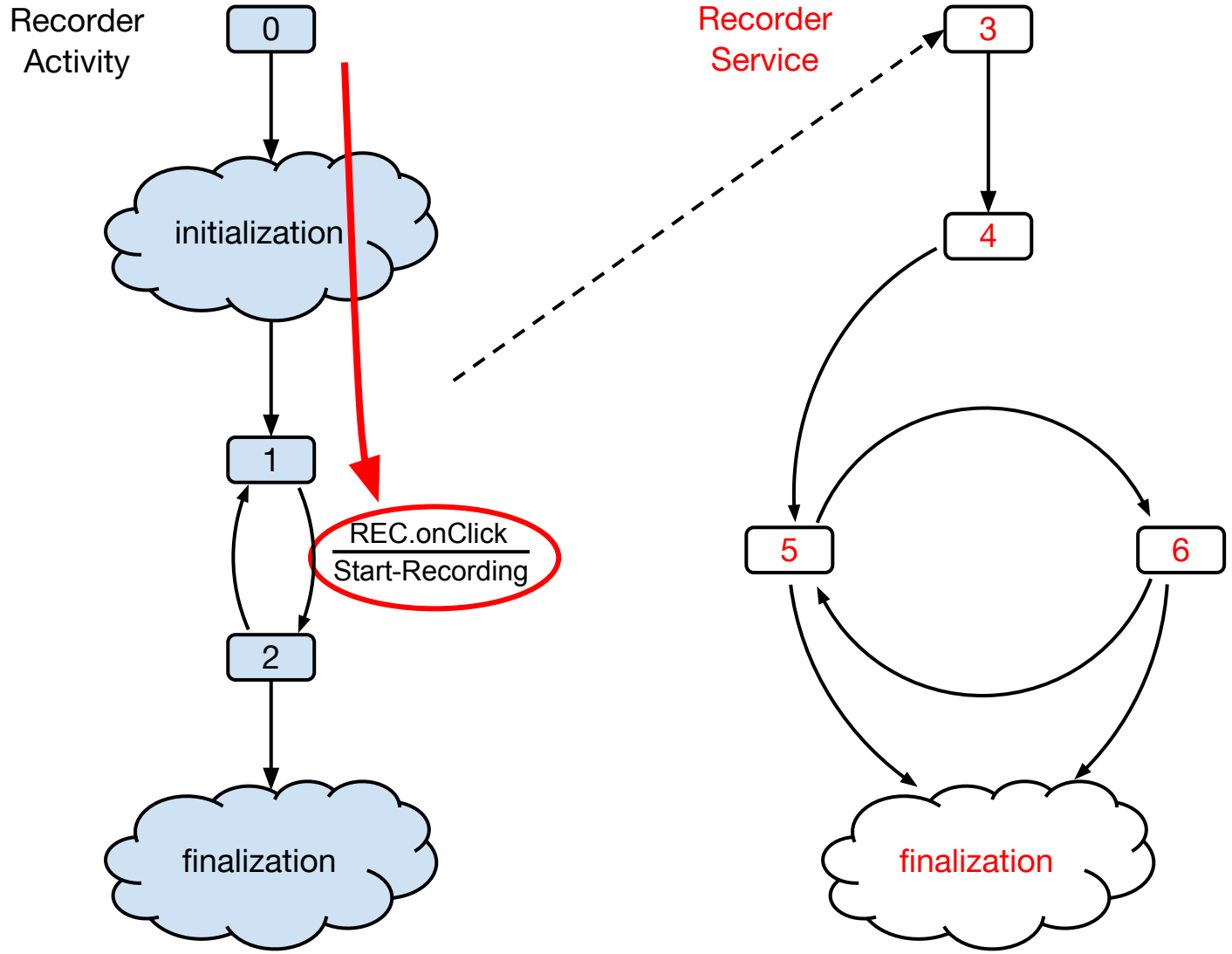
Sound Recorder: The Good Part



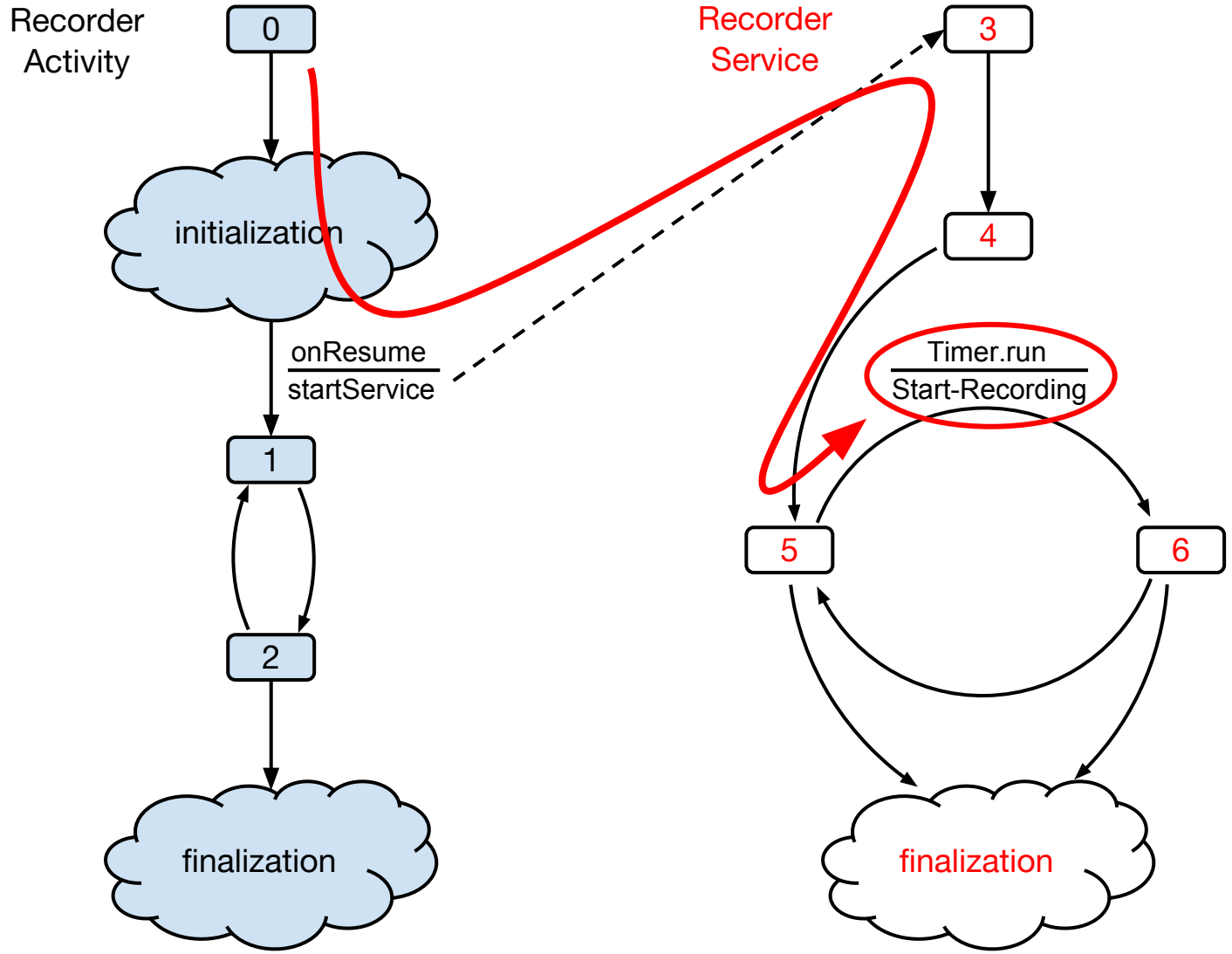
The Complete PEG



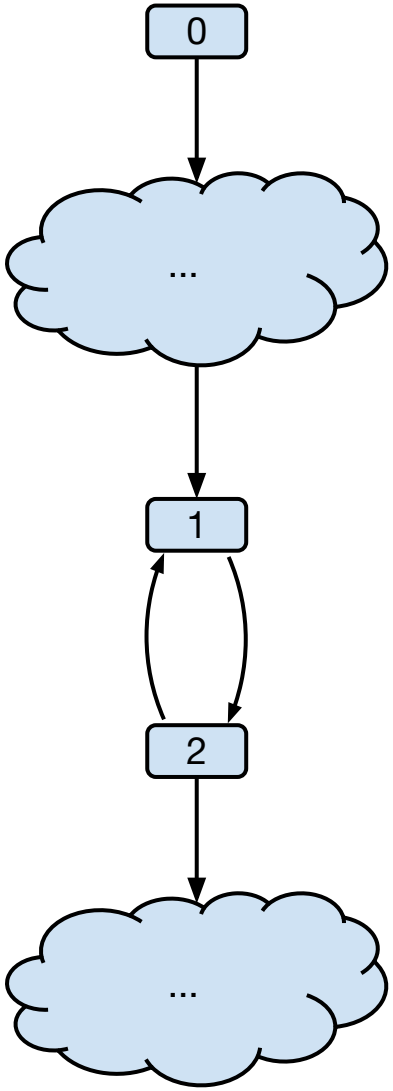
PEG: Context of the Benign Use



PEG: Context of the Malicious Use



Formal Specification



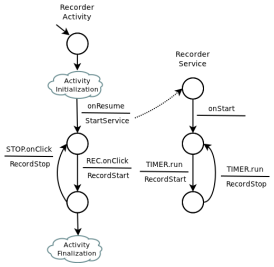
"The recording can only be started by clicking the REC button, and it will be stopped when the user clicks the STOP button."

$$(\neg\text{Start-Recording}\ \mathbf{U}\ \text{REC.onClick})$$
$$\wedge\ (\text{Stop-Recording} \iff \text{STOP.onClick})$$

Approach Overview

Apps

Abstraction Phase



Permission Event Graph

Verification Phase

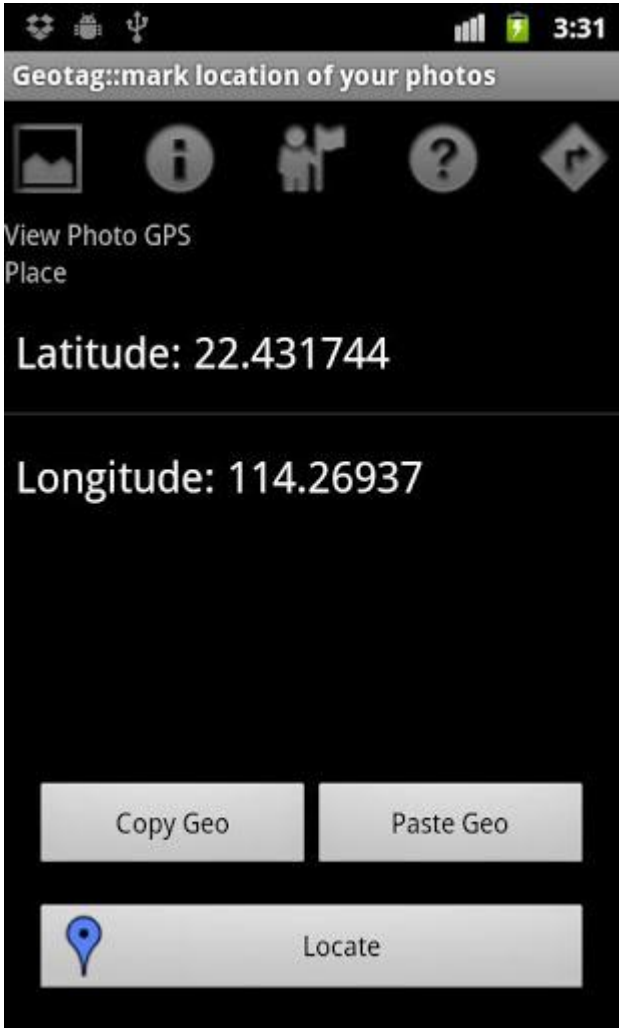
Conformance or **counter-examples**

$(\neg \text{Start-Recording } \mathbf{U} \text{ REC.onClick})$
$\wedge (\text{Stop-Recording} \iff \text{STOP.onClick})$

Policies

Case Study: Geotag

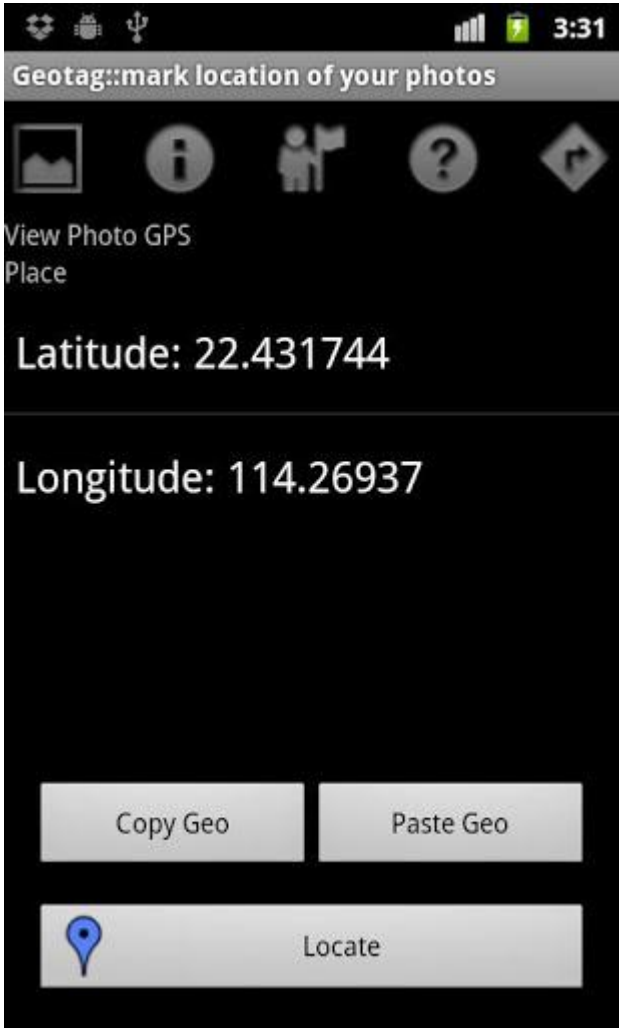
"Mark location of your photos"



Case Study: Geotag

"Mark location of your photos"

¬Access-GPS $\mathbf{U}$ Locate.onClick

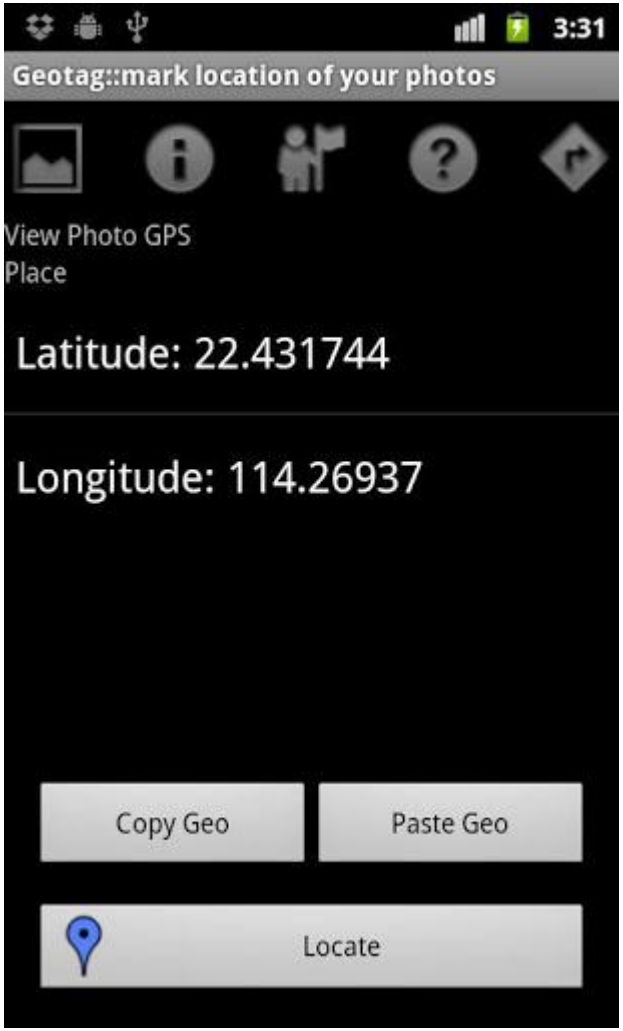


Case Study: Geotag

"Mark location of your photos"

$$\neg\text{Access-GPS}\ \mathbf{U}\ \text{Locate.onClick}$$

$$\neg\text{Access-GPS}\ \mathbf{U}\ \left(\begin{array}{l}\text{Locate.onClick}\\ \vee\quad \text{AdTask.onPreExecute}\end{array}\right)$$



Case Study: SMS Replicator Secret

A spyware that secretly forwards every SMS to another number.

Case Study: SMS Replicator Secret

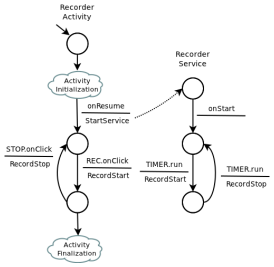
A spyware that secretly forwards every SMS to another number.

$$\neg \text{Send-SMS} \; \mathbf{U} \; \text{Button.onClick}$$

LIFE OF PEG

Apps

Abstraction Phase



Permission Event Graph

Verification Phase

Conformance or **counter-examples**

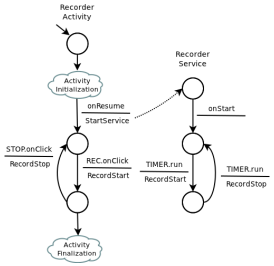
$$(\neg \text{Start-Recording } \mathbf{U} \text{ REC.onClick}) \wedge (\text{Stop-Recording} \iff \text{STOP.onClick})$$

Policies

Abstraction

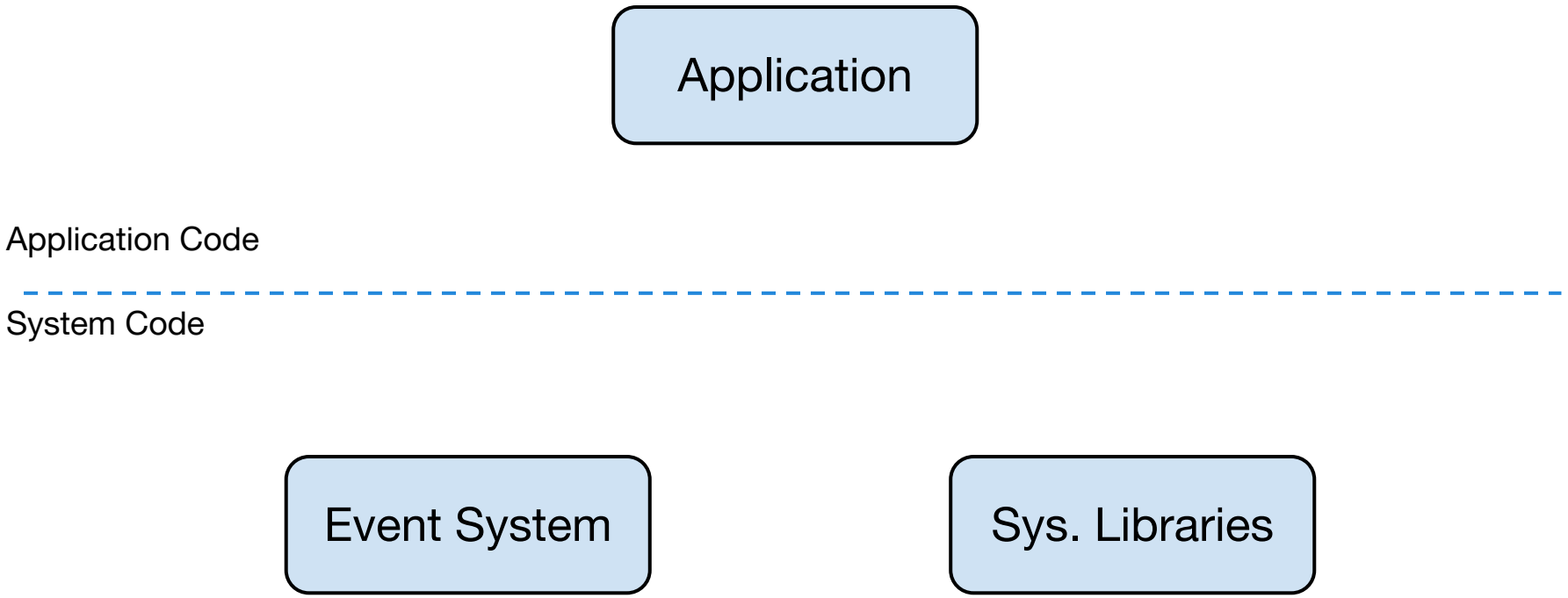
Apps

Abstraction Phase

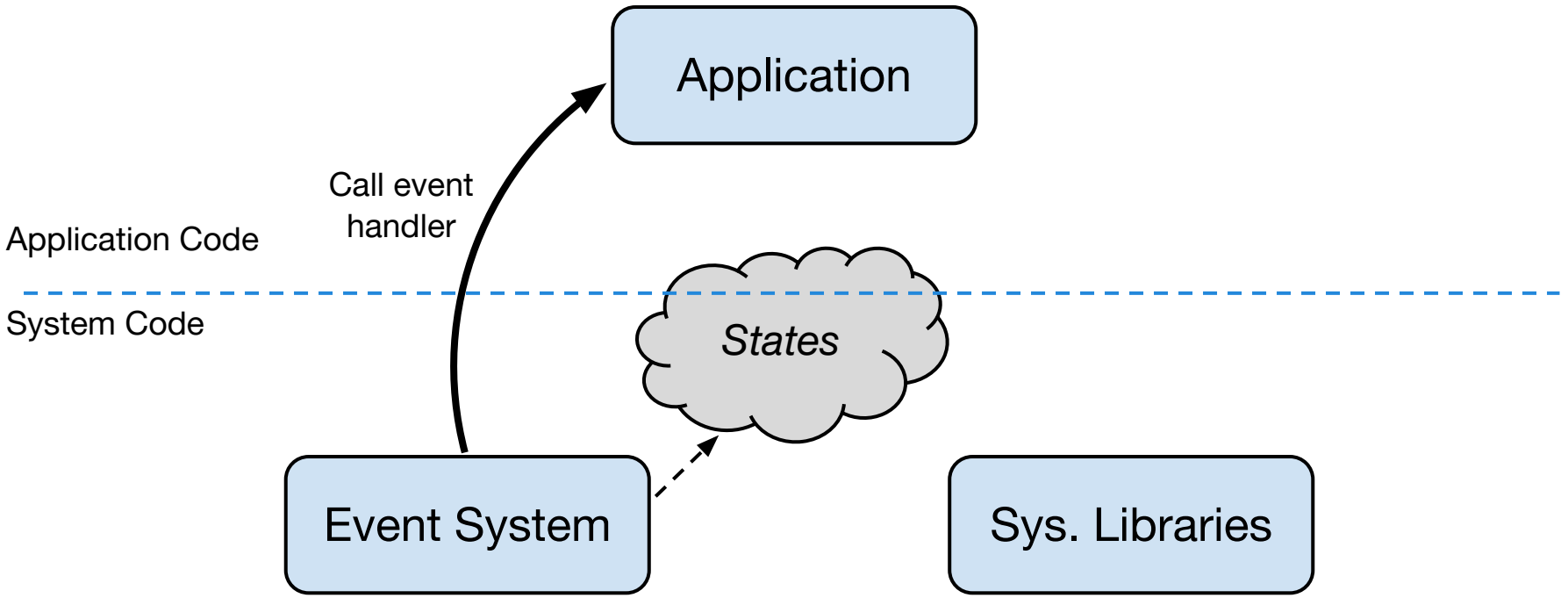


Permission Event Graph

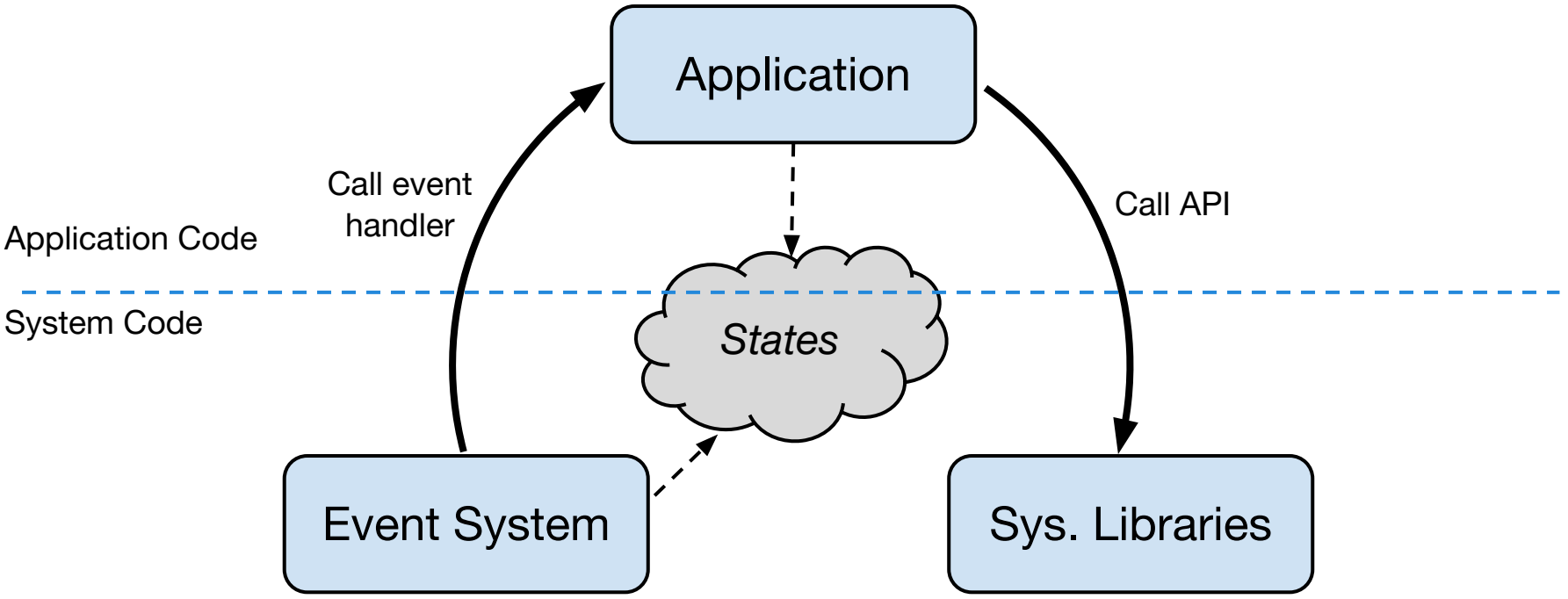
Abstraction: The Android Trinity



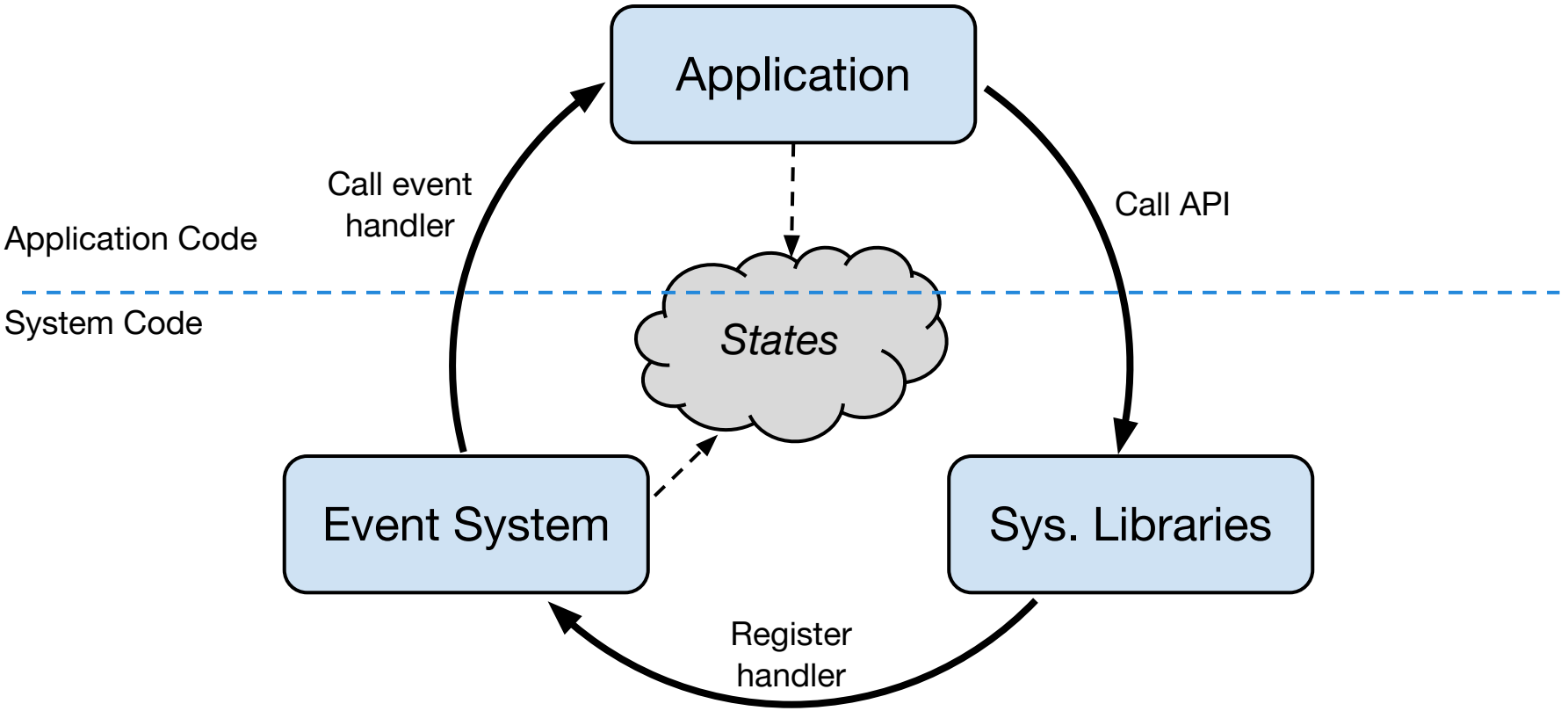
Abstraction: The Android Trinity



Abstraction: The Android Trinity

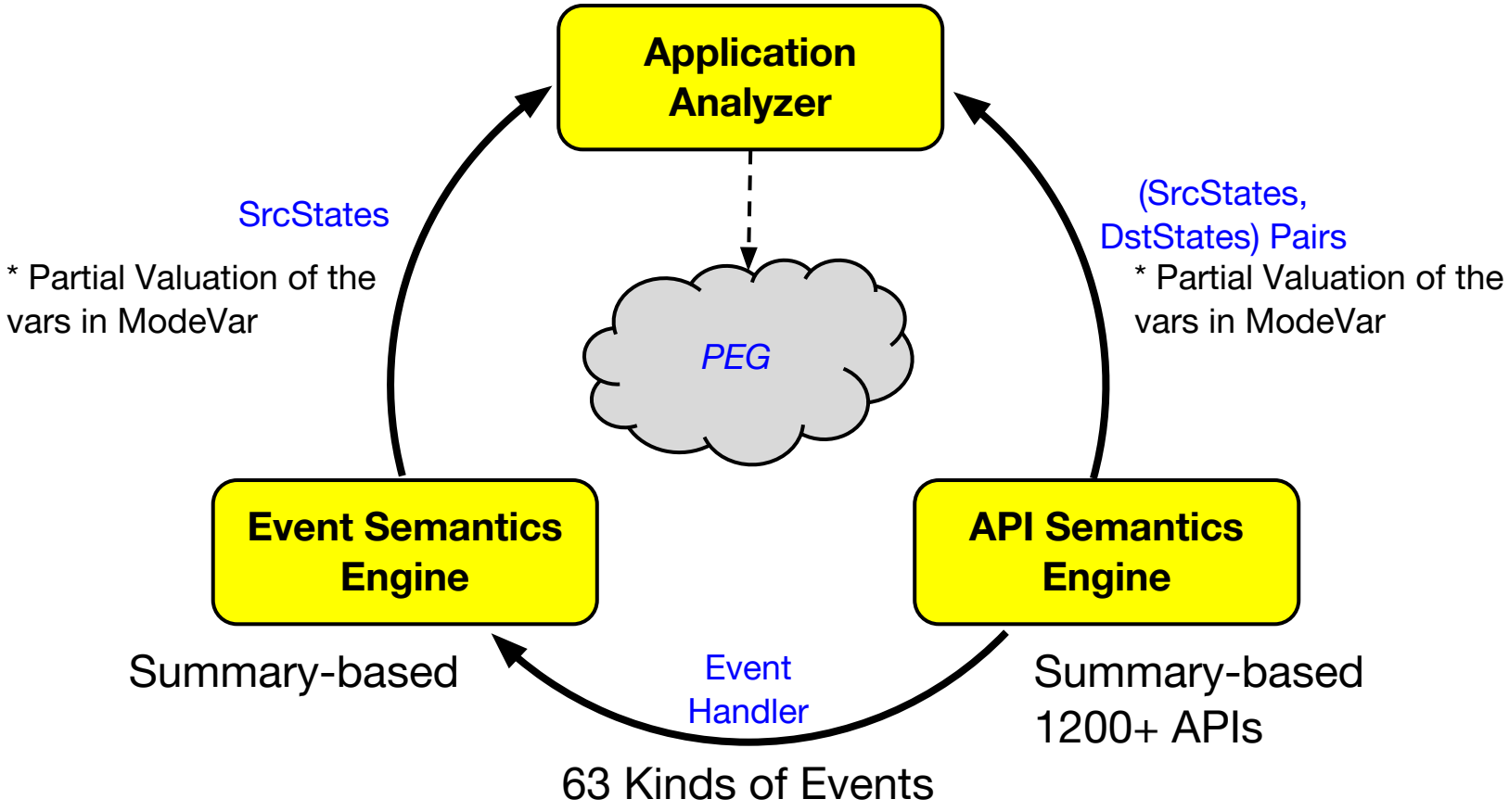


Abstraction: The Android Trinity

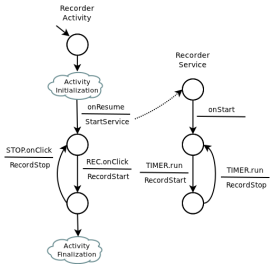


Abstraction: The Algorithm

Abstract Interpretation on (P(aState) x P(API) x P(aState)).
Interprocedural CFG with a partially context sensitive points-to analysis



Verification: BFS for Conformance



Permission Event Graph

Verification Phase

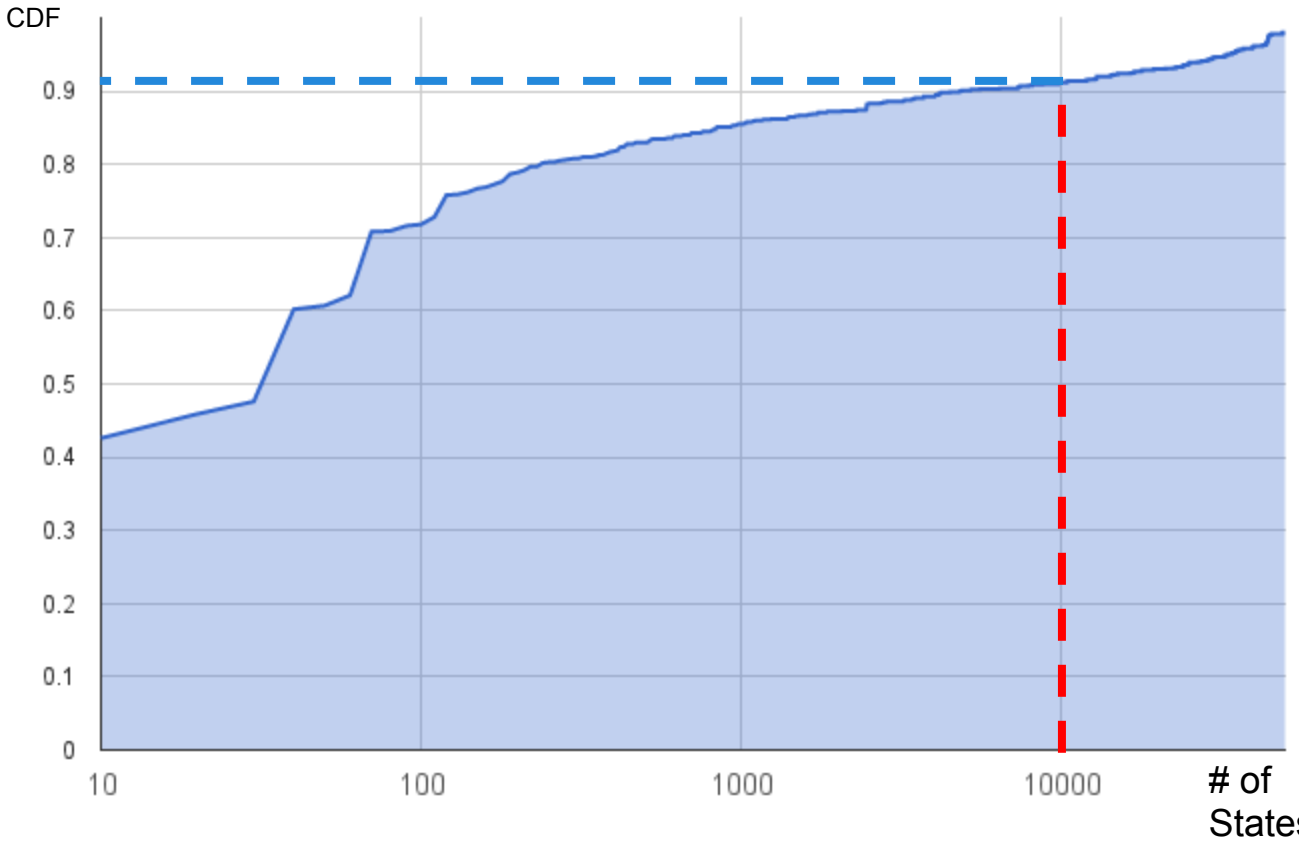
Conformance or **counter-examples**

$(\neg \text{Start-Recording } \mathbf{U} \text{ REC.onClick})$
$\wedge (\text{Stop-Recording} \iff \text{STOP.onClick})$

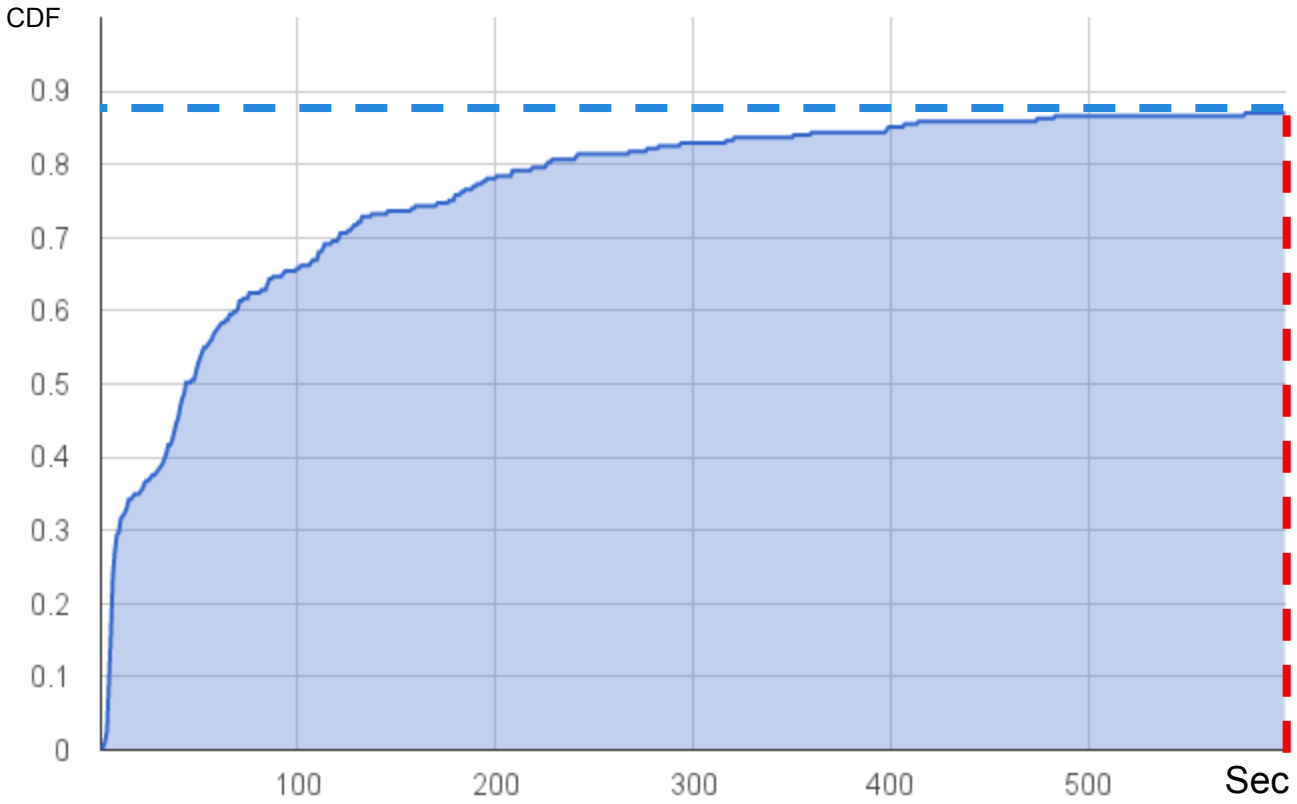
Policies

Evaluation: PEG size (# states, CDF)

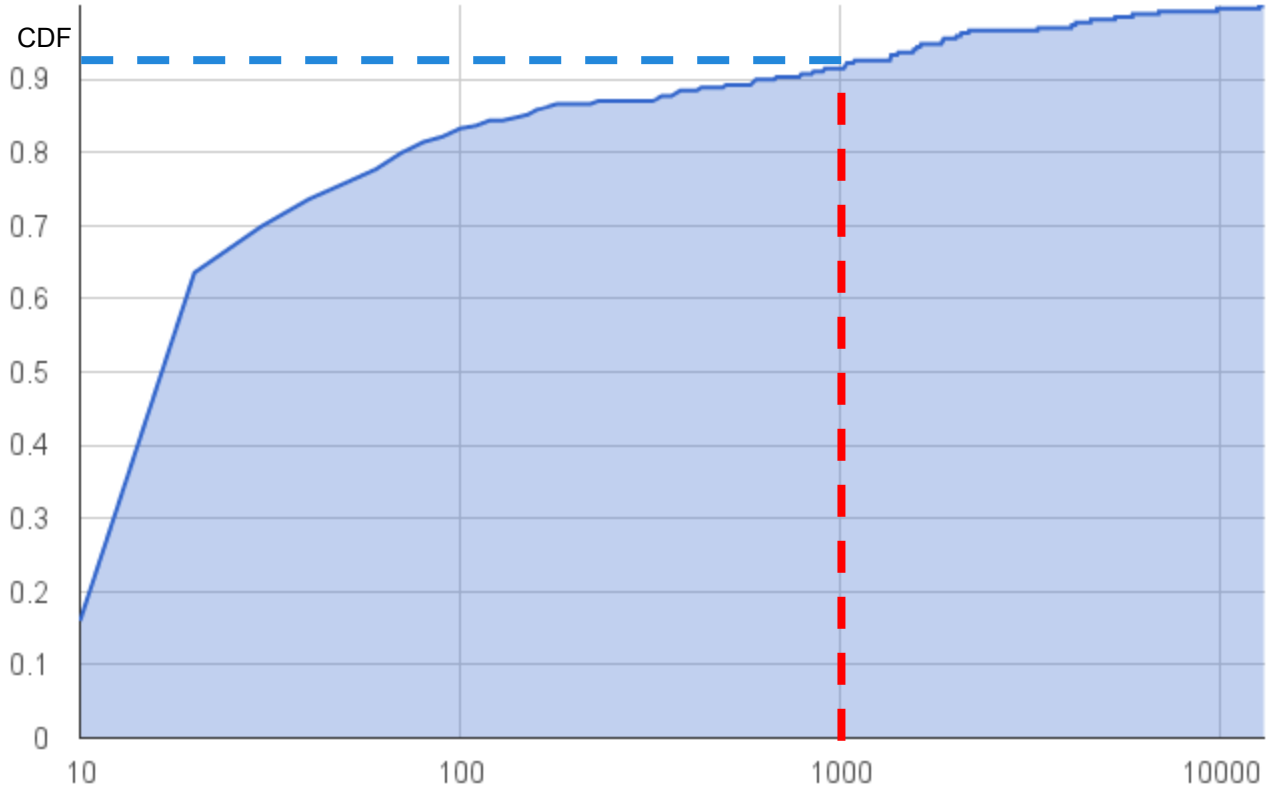
* 269 applications. Binary code sizes vary from 4KB to 6MB



Evaluation: Abstraction Time (CDF)



Evaluation: Verification Time (CDF)



* Always terminate within 3.6 hours

LOG scale

Conclusion

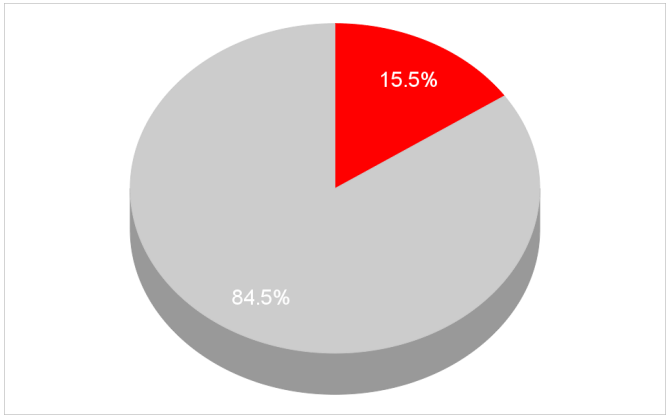
- Permission event graph: event-dependencies and their API/permission-level behaviors
- Contextual policies based on event sequences enable the detection and analysis of complex malicious behaviors (user-oriented security)
- Enriches the set of detection techniques used by security analysts

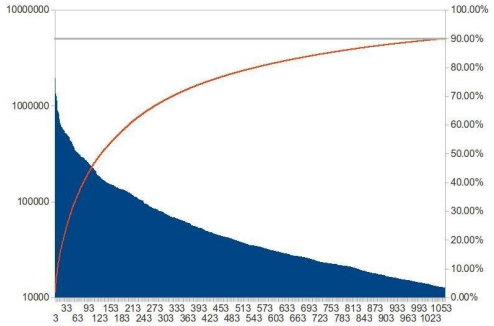
Questions ?

Kevin Chen <kevinchn@cs.berkeley.edu>

Backup Slides

Backup Slides





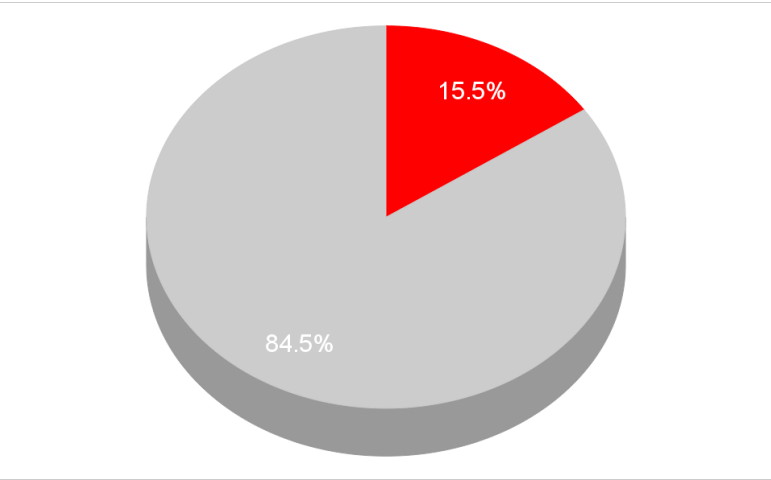
Native Code

- Known
  - The API Semantics Engine
- Unknown
  - Do NOT support

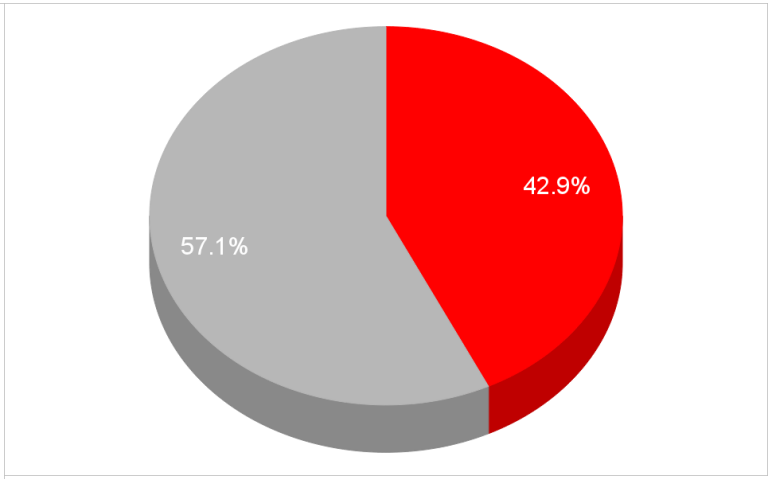
Rewriting

- Barriers for static analysis:

Unresolved Reflection

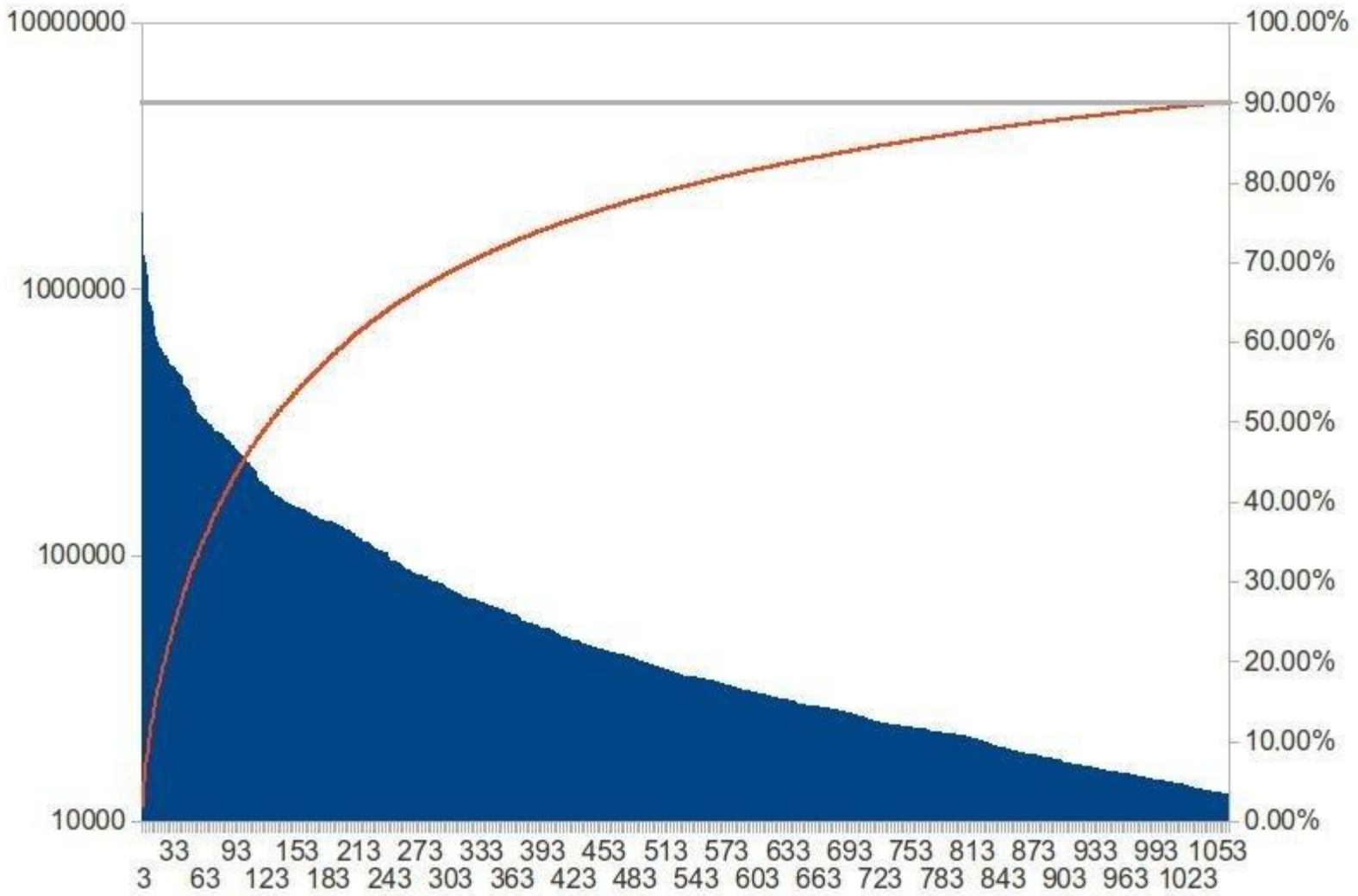


Unresolved Dynamic dispatching



- Solutions:
  - Insert runtime checks
  - More in the paper

API Frequency in 95,000 Apps



Specification Constructs

$$(\neg \text{Start-Recording}\ \mathbf{U}\ \text{REC.onClick}) \wedge (\text{Stop-Recording} \iff \text{STOP.onClick})$$

Information Type	Example
System status variables (Mode variables)	*STOPButton.registered*, *MyActivity.inBackground*
System APIs and their arguments	*android.location.Location: double getLatitude()*, "*content://com.android.contacts/contacts*"
Permissions	"*android.permission.INTERNET*"

Specification Checker Interface

Bounded BFS for conformance analysis

Write the specification FSM using the following interfaces:

```
public int getStateId();
public void restoreFromStateId(int id);
public ListenerResult stateListener(ModelState state);
public ListenerResult actionListener(EventModality action);
public ListenerResult methodListener(PathItemMethod method);
```

Evaluation

Sensitive Operation	Malicious		Benign	
	NoUI	Total	NoUI	Total
GPS	15	15	18	30
SD card	25	26	25	32
SMS	10	11	0	1

Applications

- Usage scenarios:
  - Extra semantics-based filter for malware screening
  - Diagnostic tool for security analysts
  - Fine-grained information about permission use for the user

FP/FN

- emphasis: a new representation to detect a specific category of malicious behaviors. ... in addition to the traditional Android malware detection techniques.
- 2/18 for the specific set of behaviors
- no longer binary,
  - should be a continues answer.
  - Geotag