Simplifying

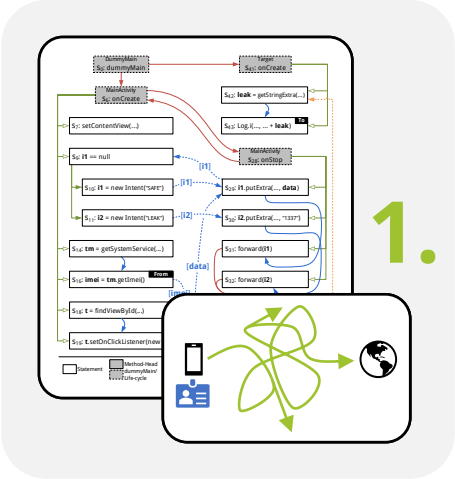
(Slicing)

Cooperative Android App Analysis

Tasks

www.Felix Pauck.de, Heike Wehrheim

9/13/2021

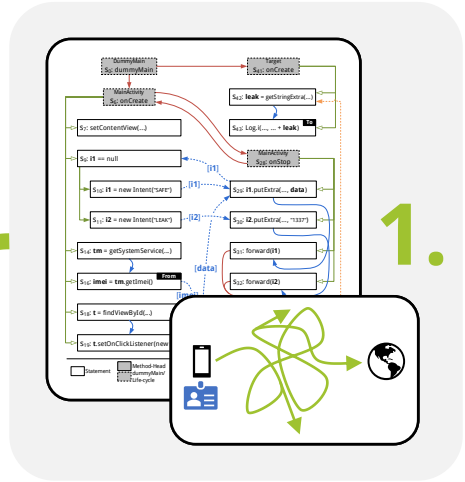


1.

Simplifying
(Slicing)

Cooperative Android App Analysis

Tasks



1.

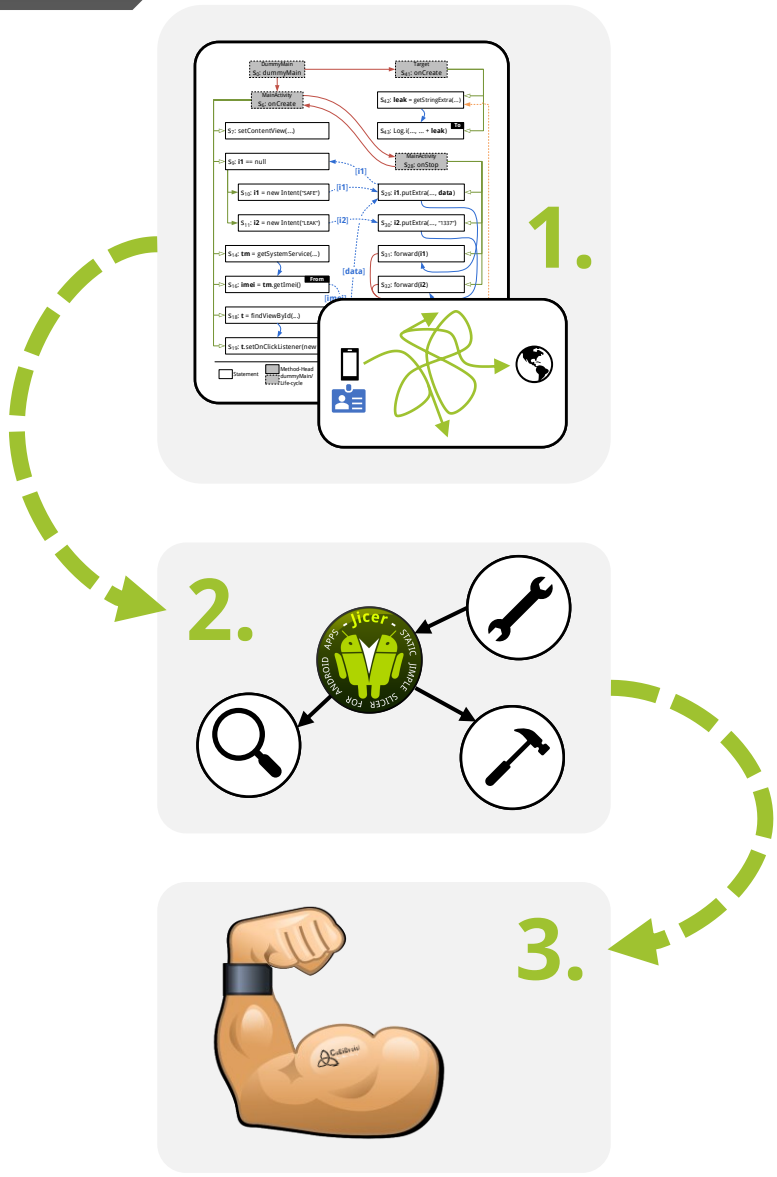
2.

Simplifying

(Slicing)

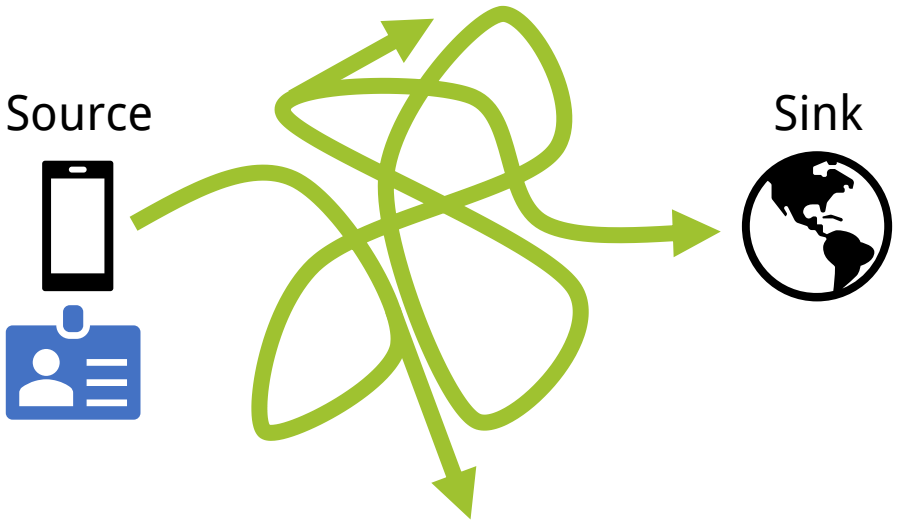
Cooperative Android App Analysis

Tasks

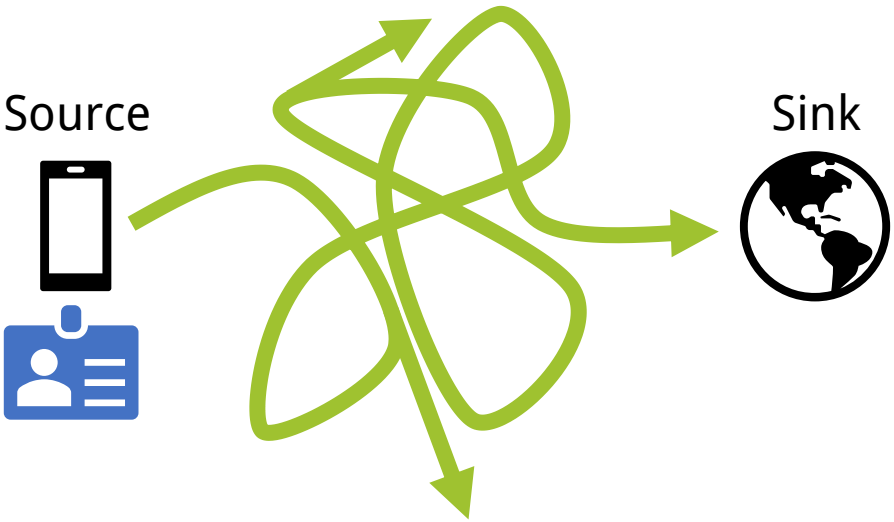


Simplifying
(Slicing)
Cooperative Android App Analysis
Tasks

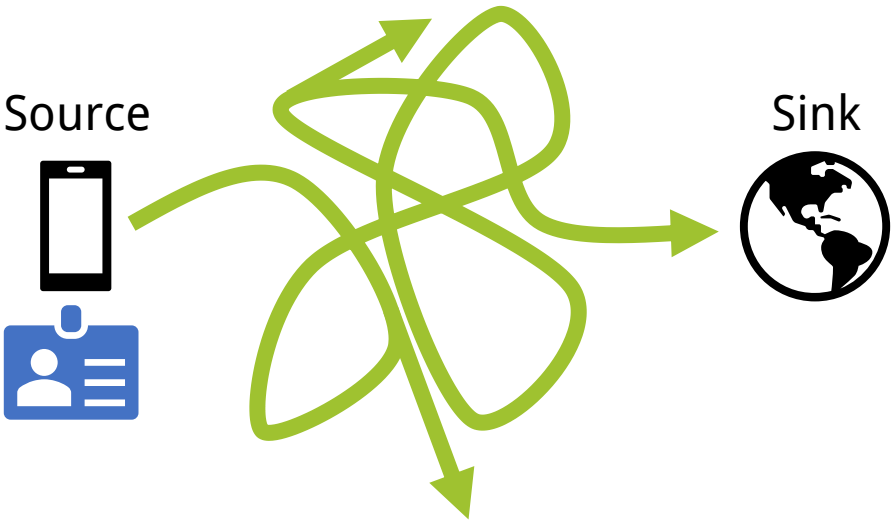
Cooperative Taint Analysis



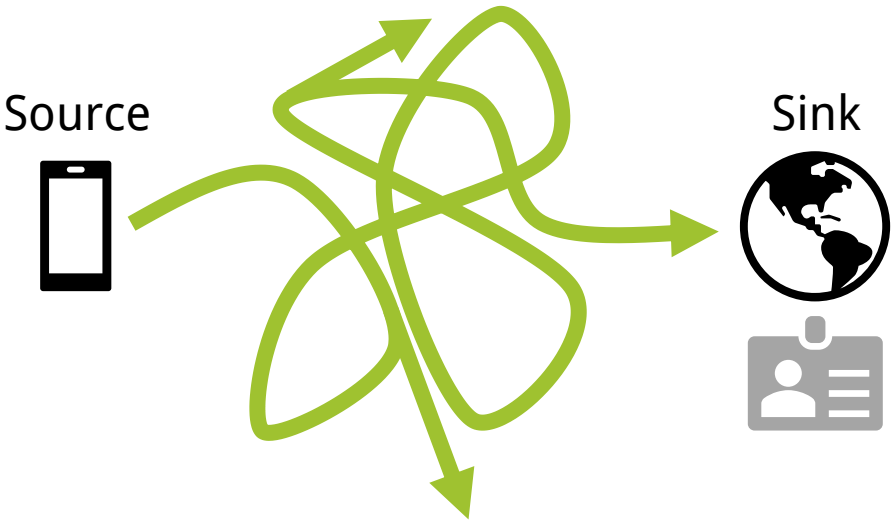
Cooperative Taint Analysis



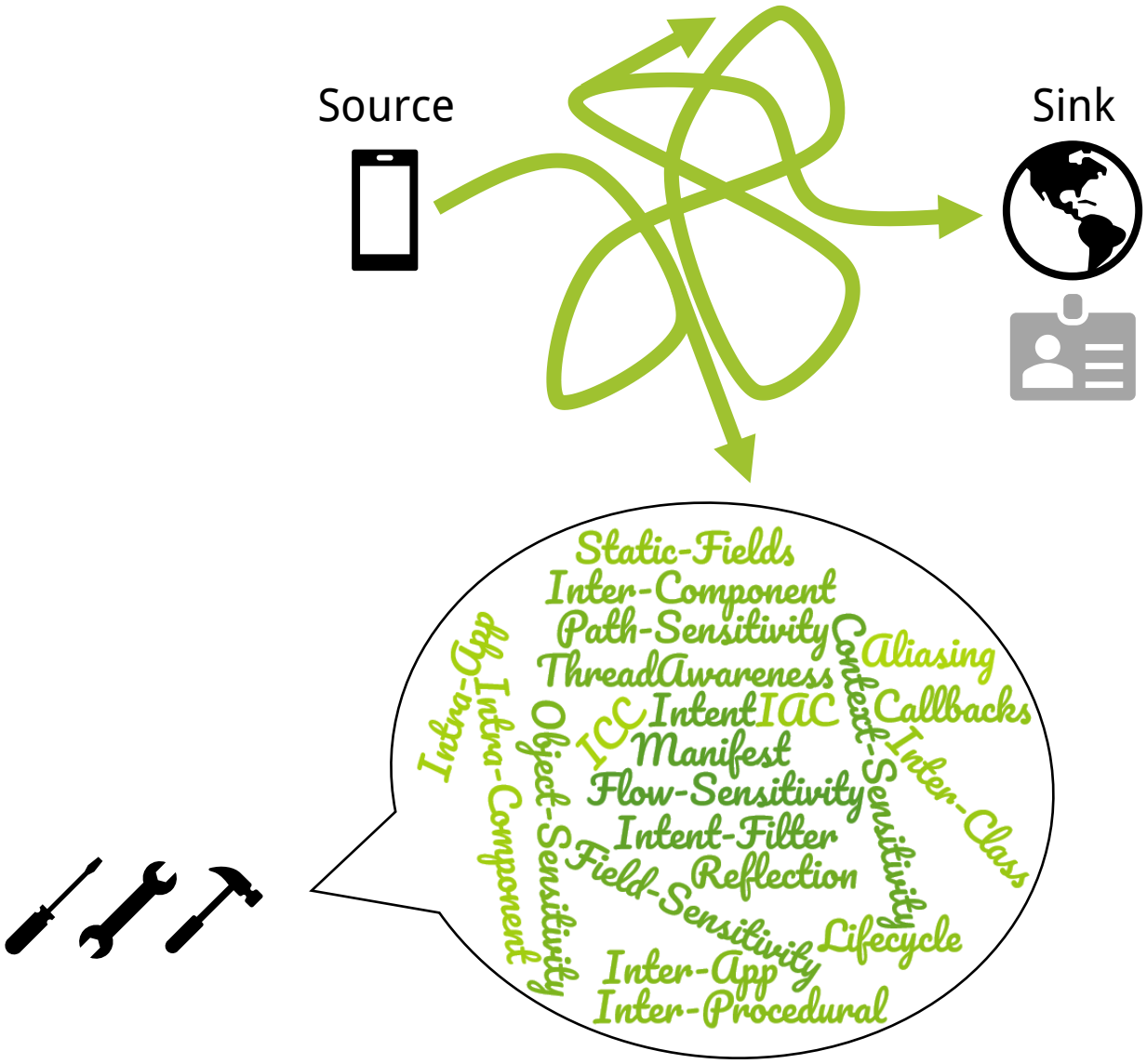
Cooperative Taint Analysis



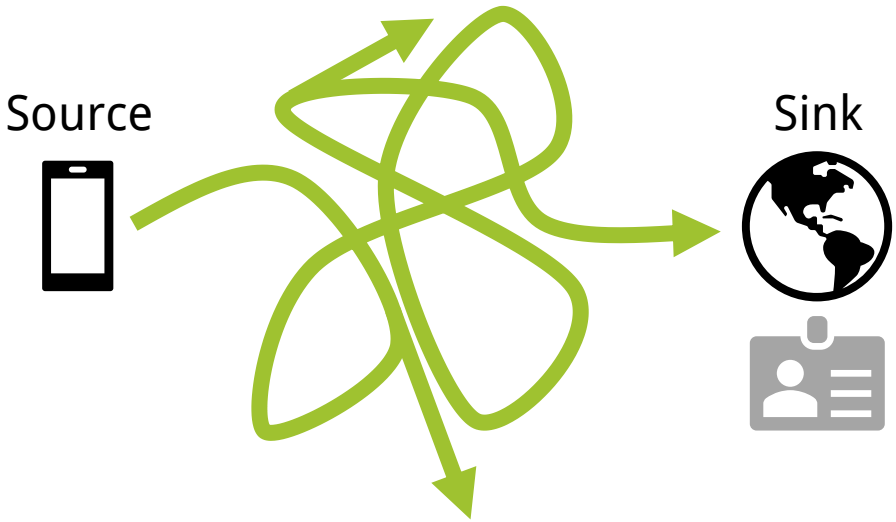
Cooperative Taint Analysis

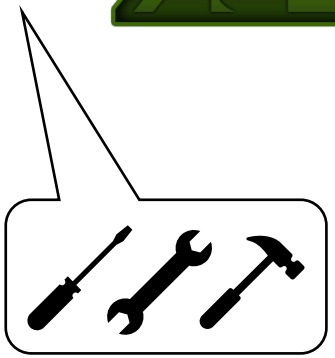


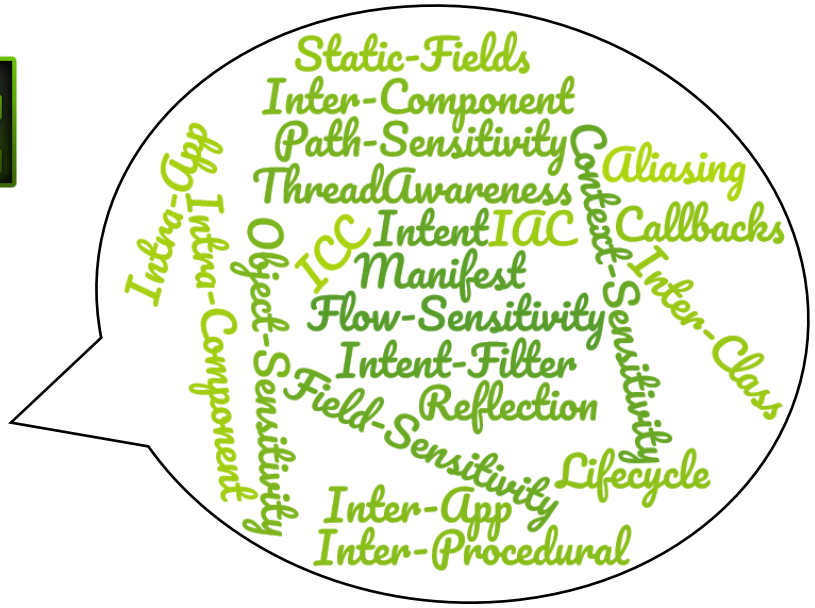
Cooperative Taint Analysis



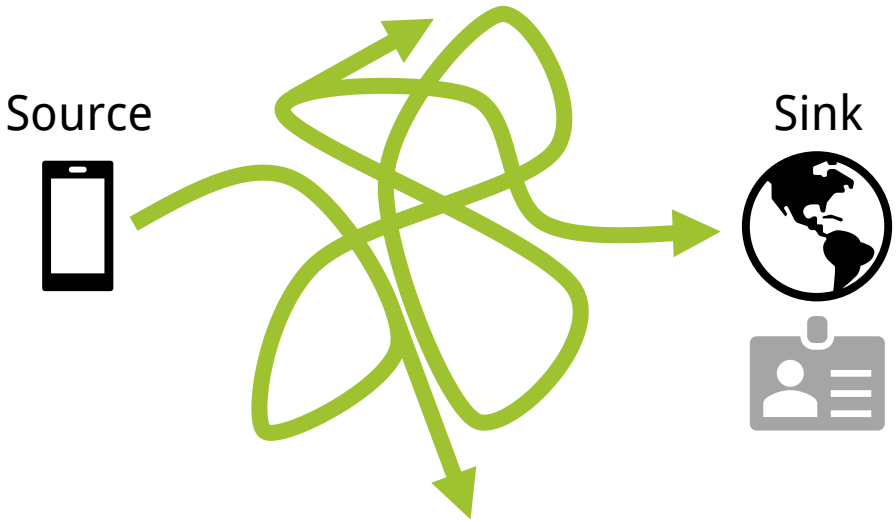
Cooperative Taint Analysis



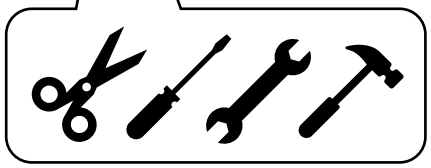


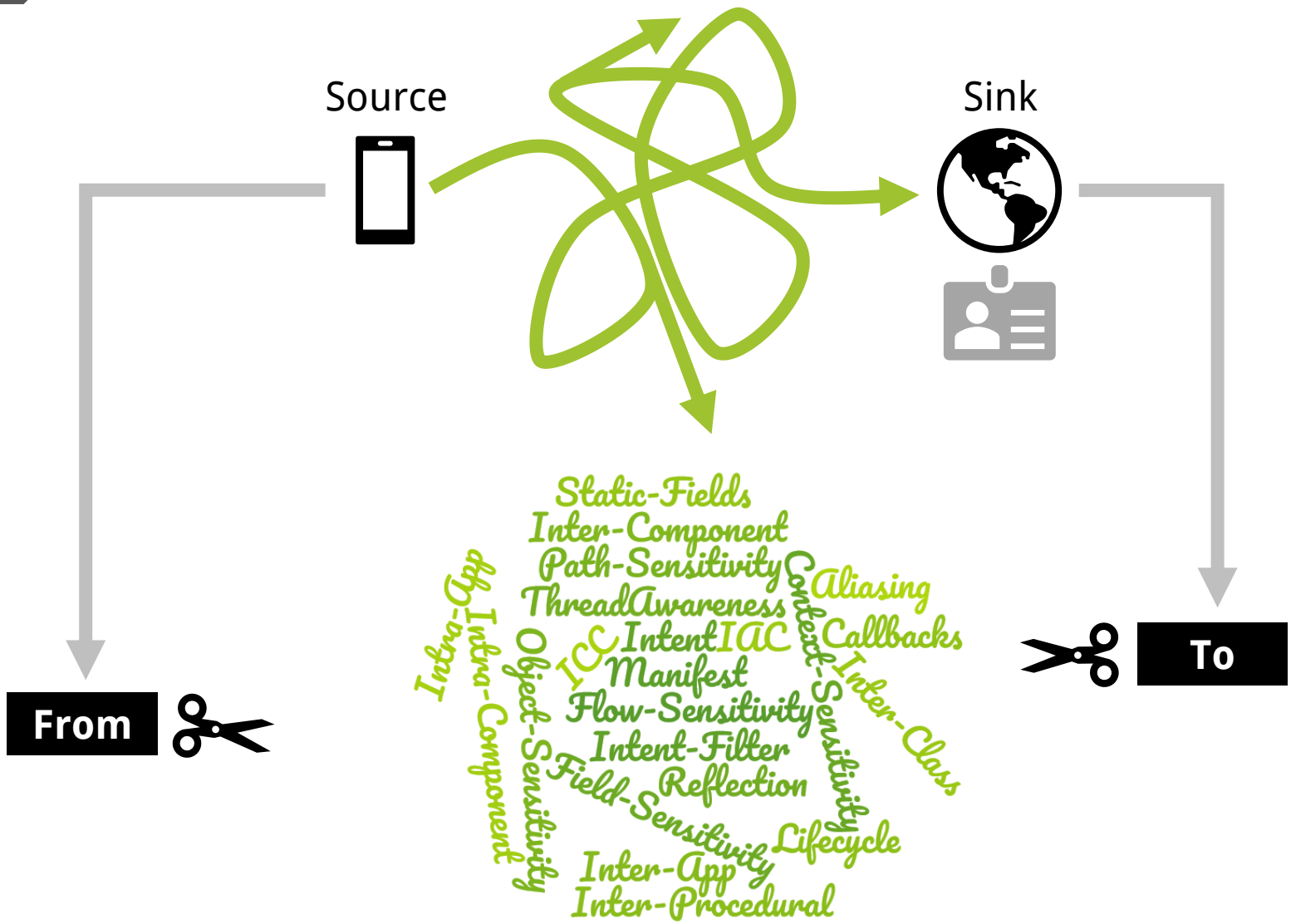


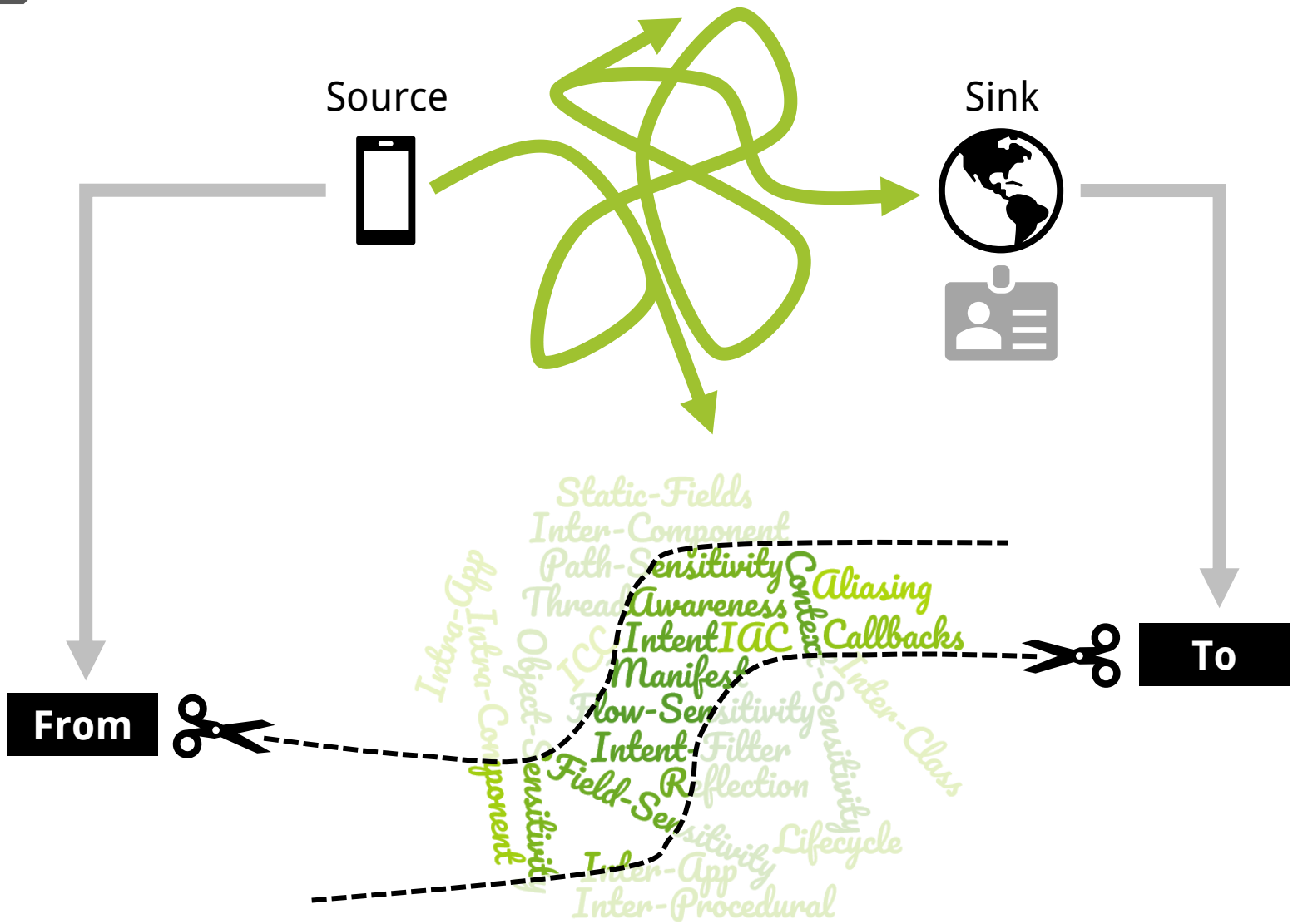
Cooperative Taint Analysis

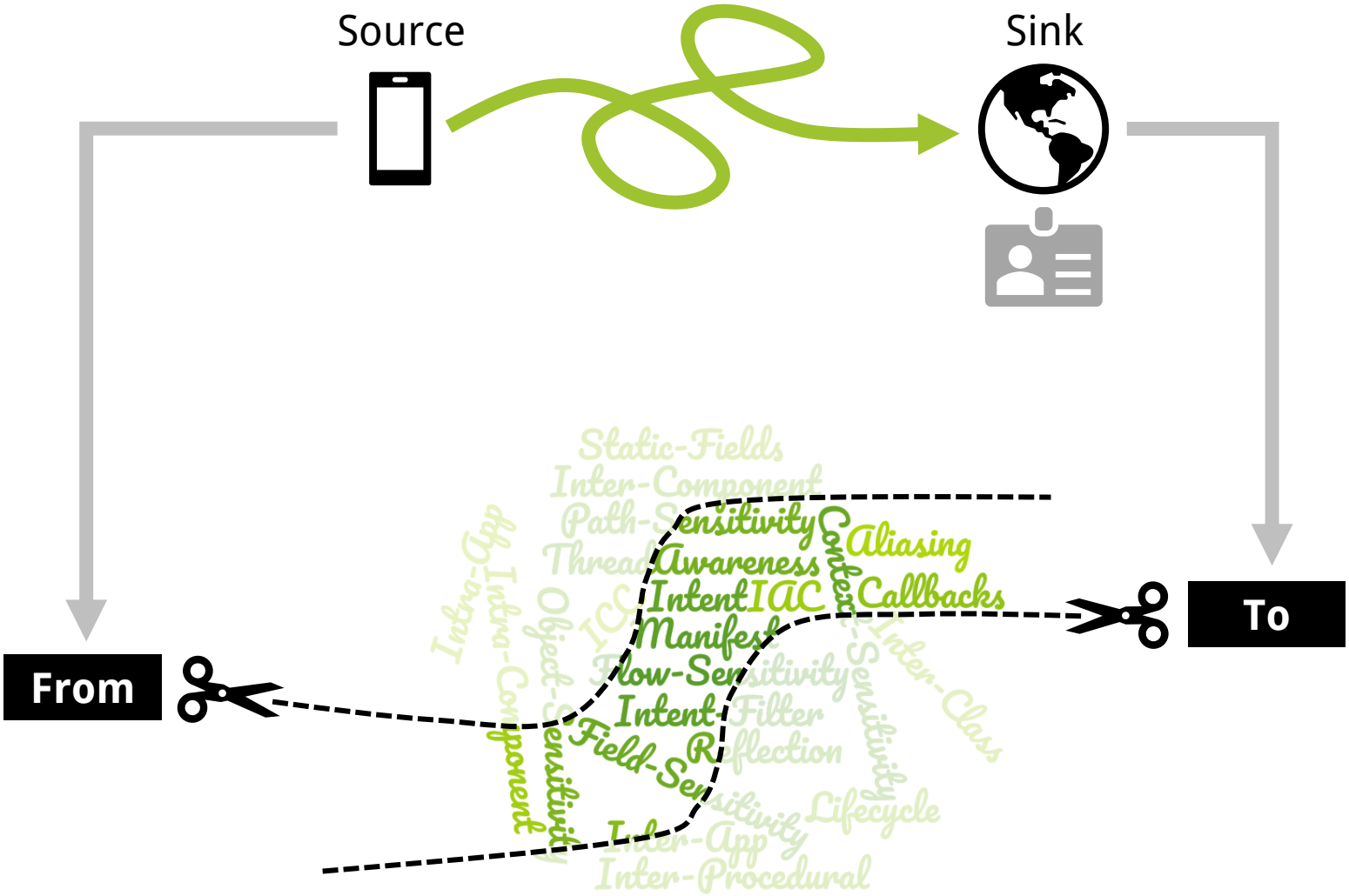


CoDiDroid
together strong!

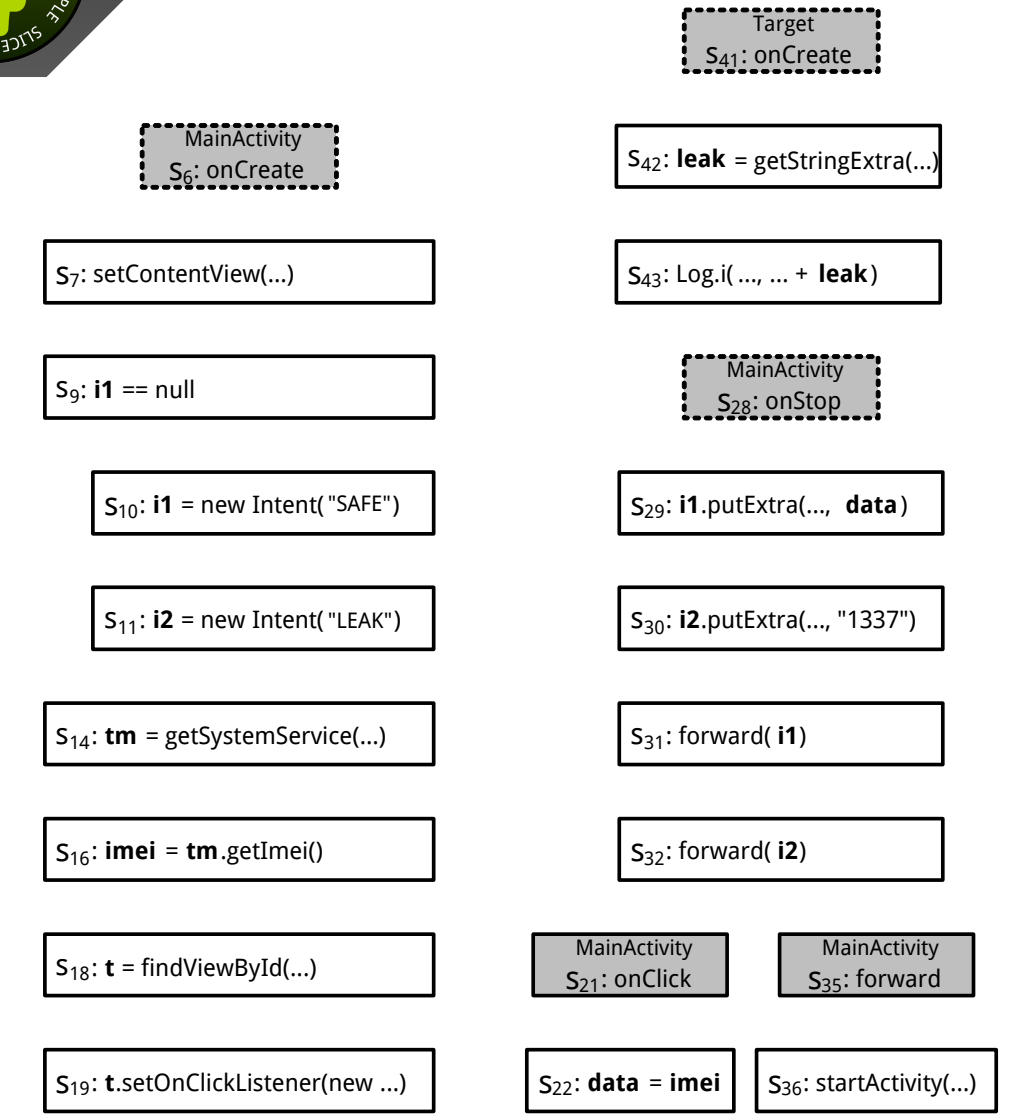



Source
Sink
From
To
Static-Fields
Inter-Component
Path-Sensitivity
Aliasing
ThreadAwareness
Context-Sensitivity
Callbacks
Intra-App
IAC
Intent
ICC
Inter-Class
Manifest
Flow-Sensitivity
Intra-Component
Object-Sensitivity
Intent-Filter
Field-Sensitivity
Reflection
Lifecycle
Inter-App
Inter-Procedural

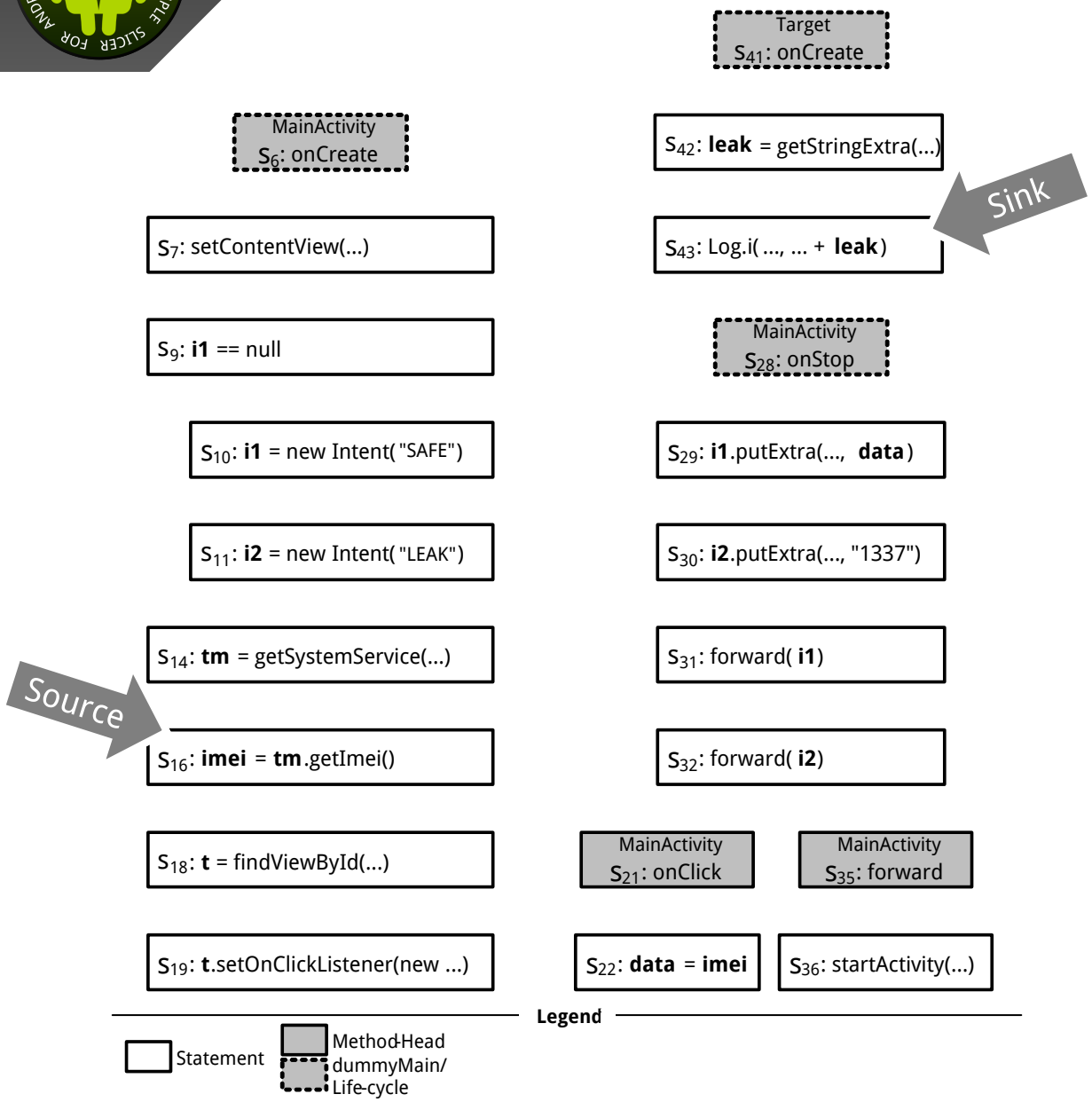

Source
Sink
From
To
Static-Fields
Inter-Component
Path-Sensitivity
Thread
Intra-App
Intra-Component
Object-
ICC
Sensitivity
Awareness
Context
Aliasing
Intent
IAC
Callbacks
Manifest
Flow-Sen
Intent
Field-Sen
Filter
Reflection
Lifecycle
Inter-App
Inter-Procedural
Inter-Class


Source
Sink
From
To
Static-Fields
Inter-Component
Path-Sensitivity
Context-Sensitivity
Aliasing
Awareness
Intent
IAC
Callbacks
Manifest
Flow-Sensitivity
Intent
Field-Sensitivity
Filter
Reflection
Lifecycle
Inter-App
Inter-Procedural
Intra-App
Object-Sensitivity
Inter-Class

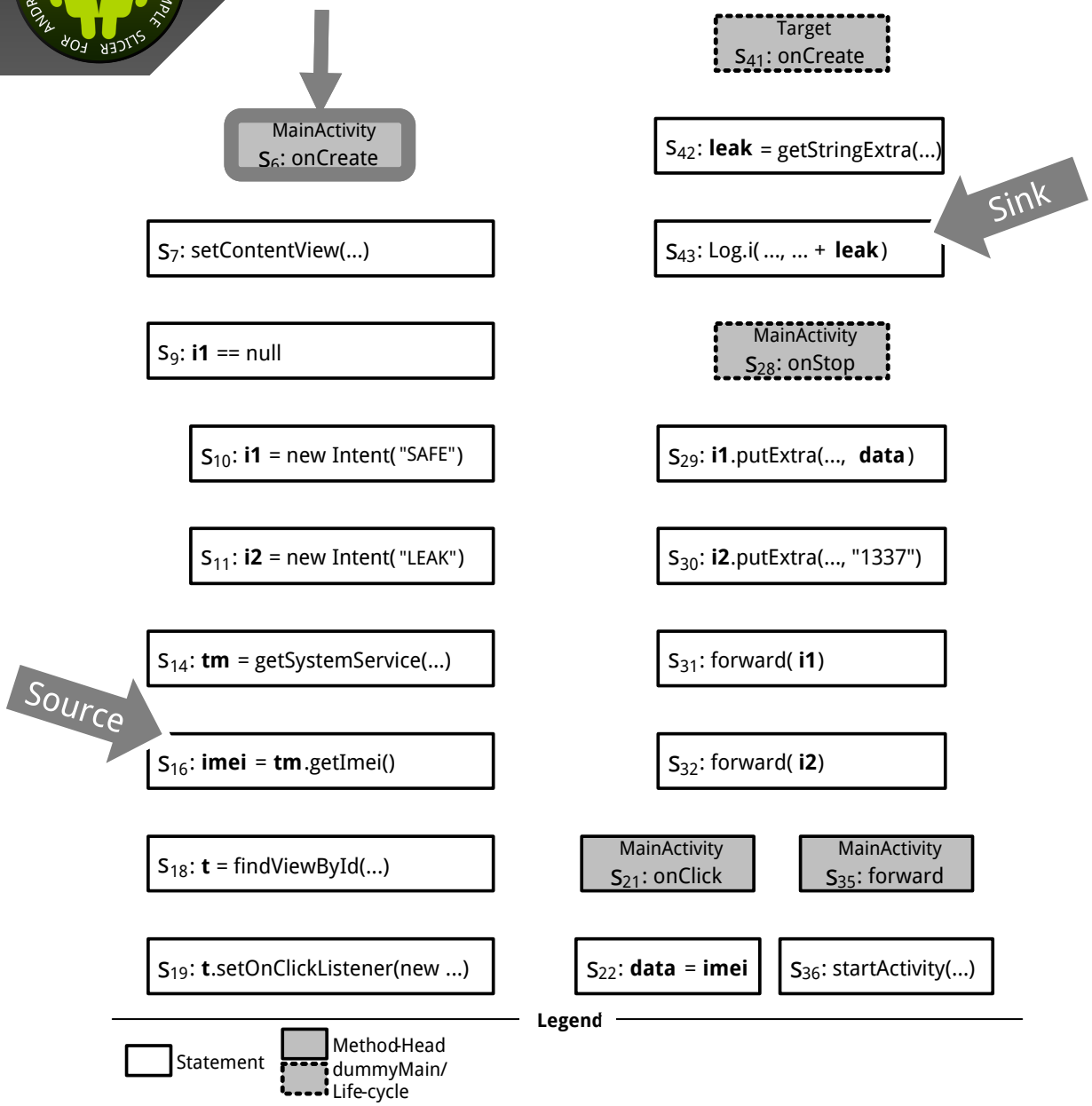
Example: Cooperative Taint Analysis



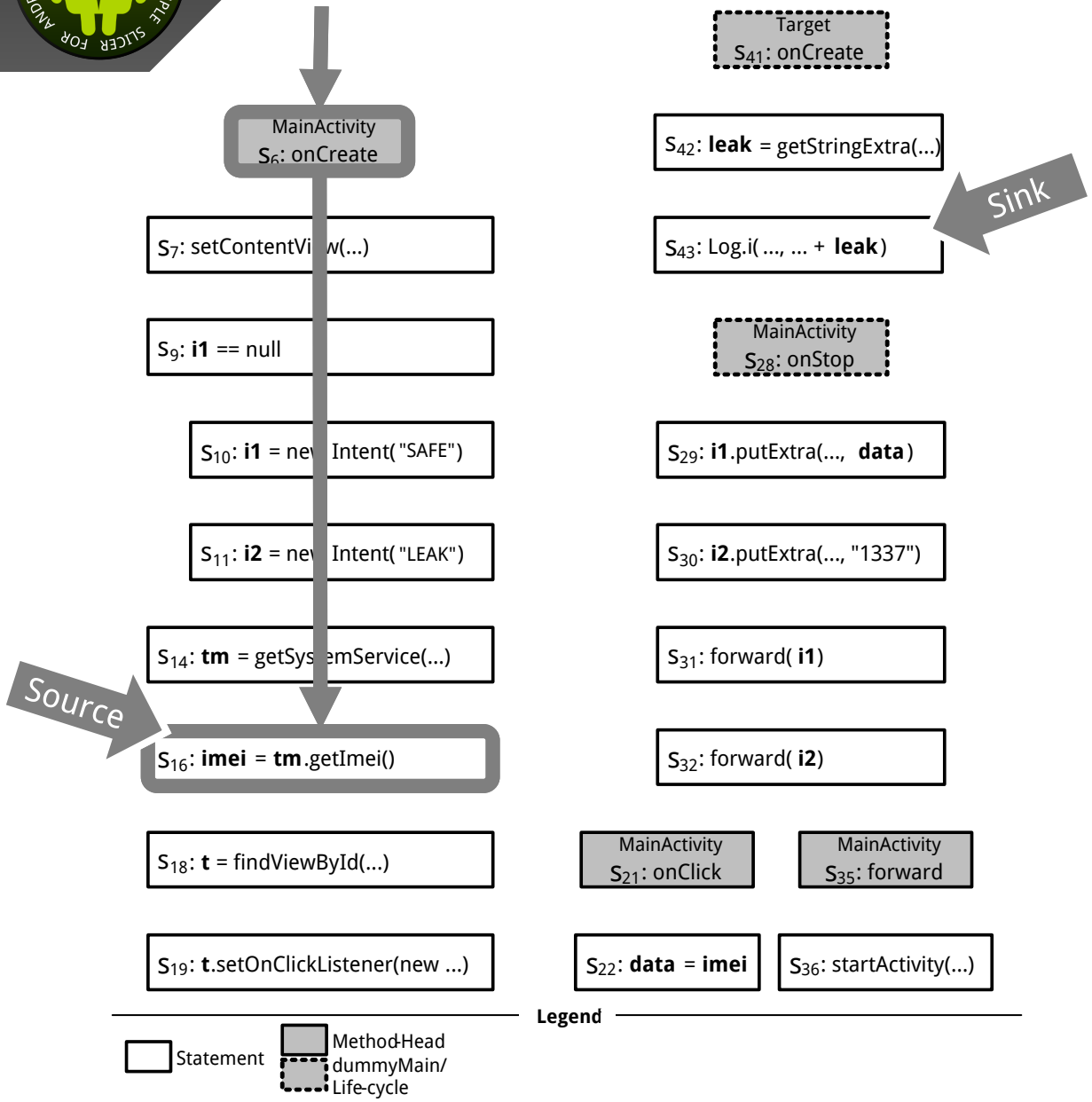
Example: Cooperative Taint Analysis



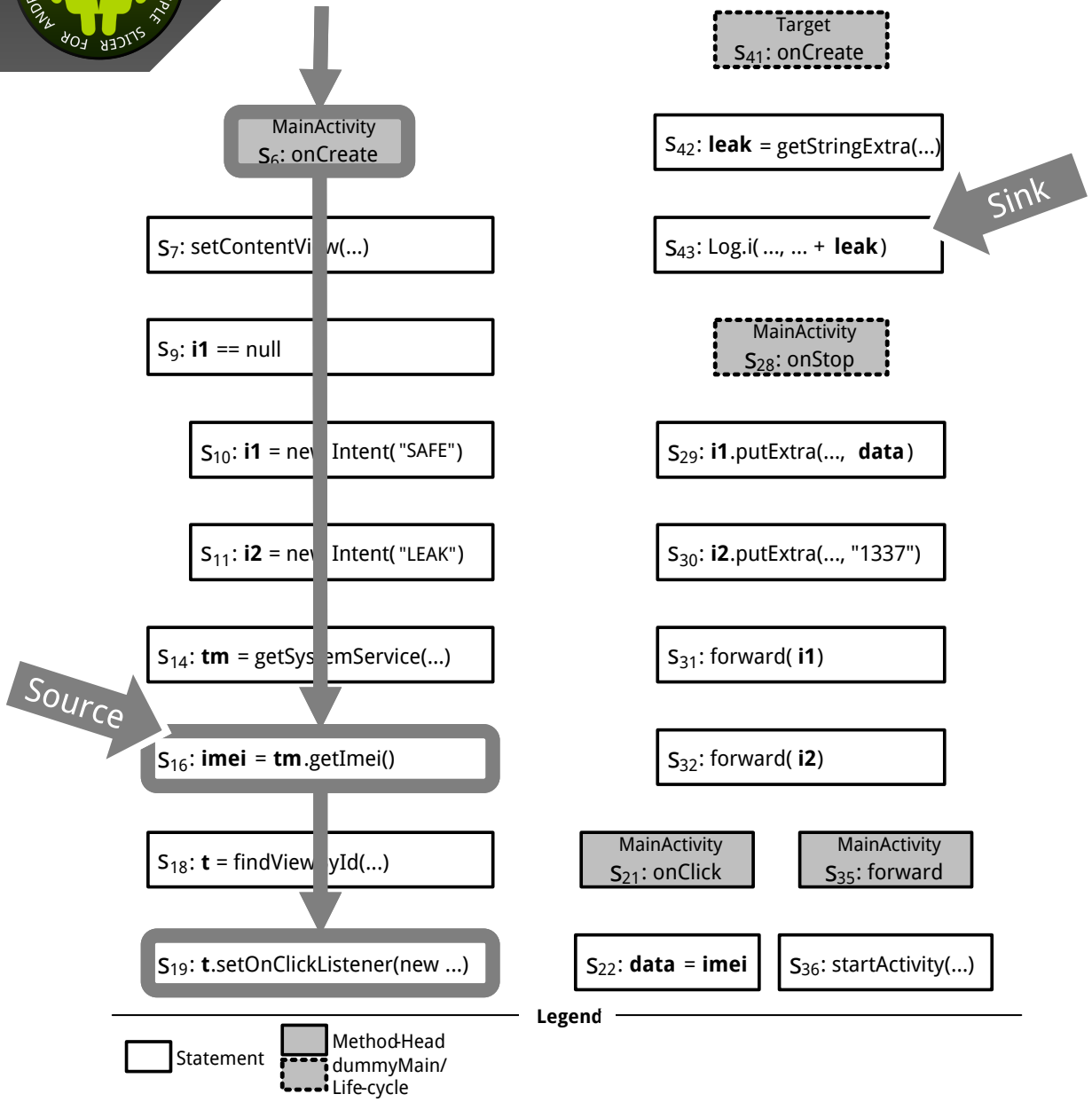
Example: Cooperative Taint Analysis



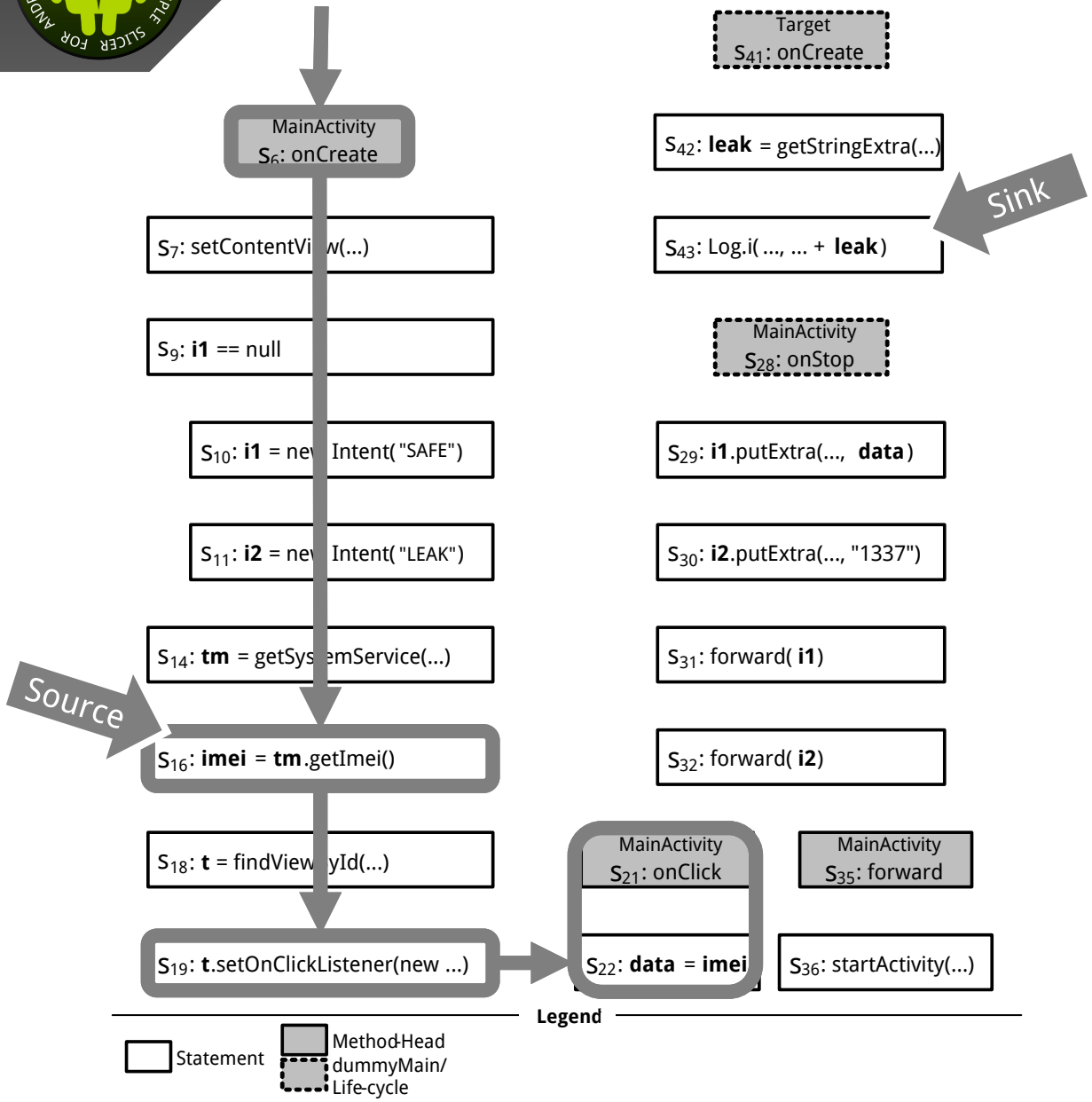
Example: Cooperative Taint Analysis



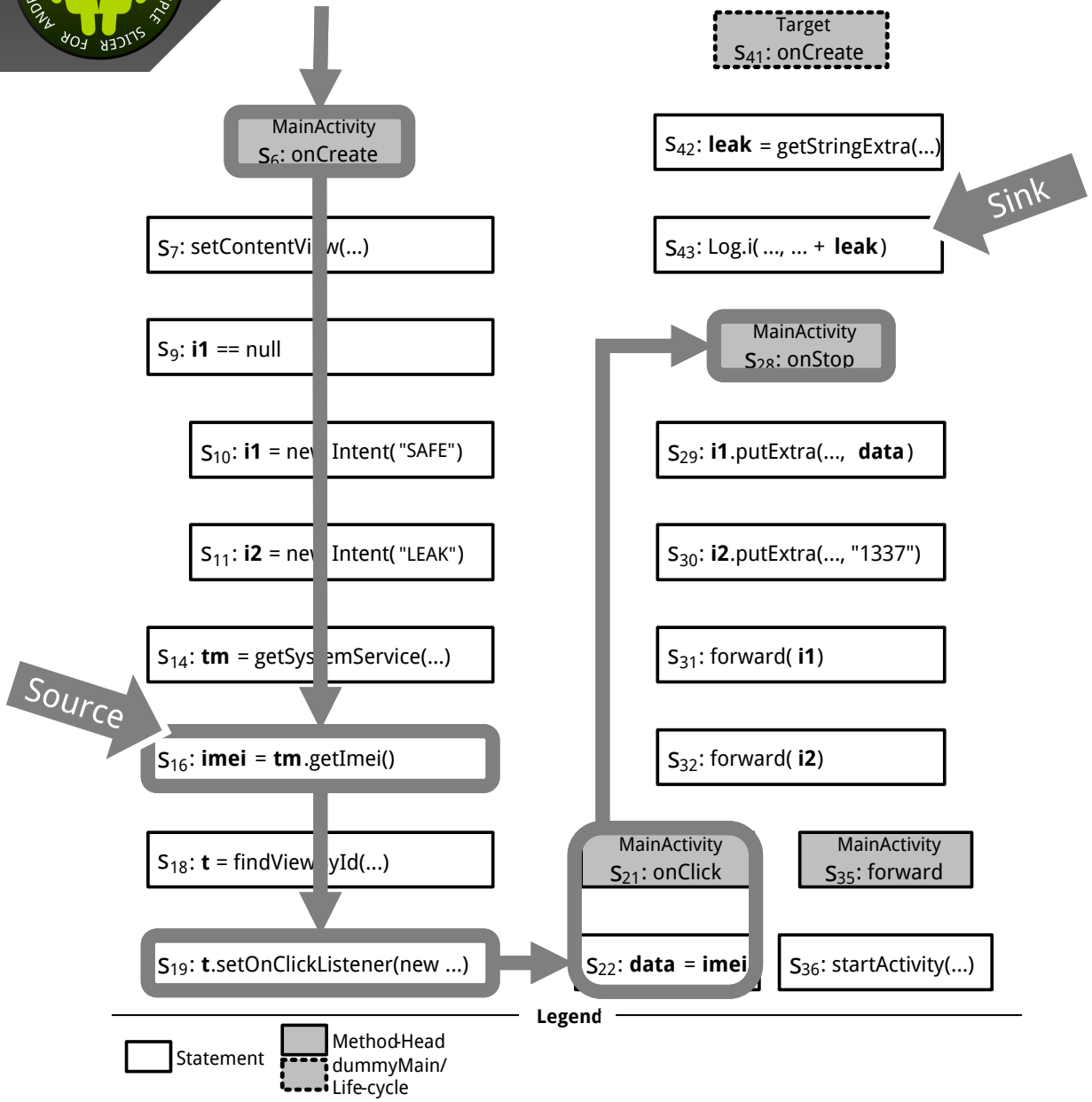
Example: Cooperative Taint Analysis



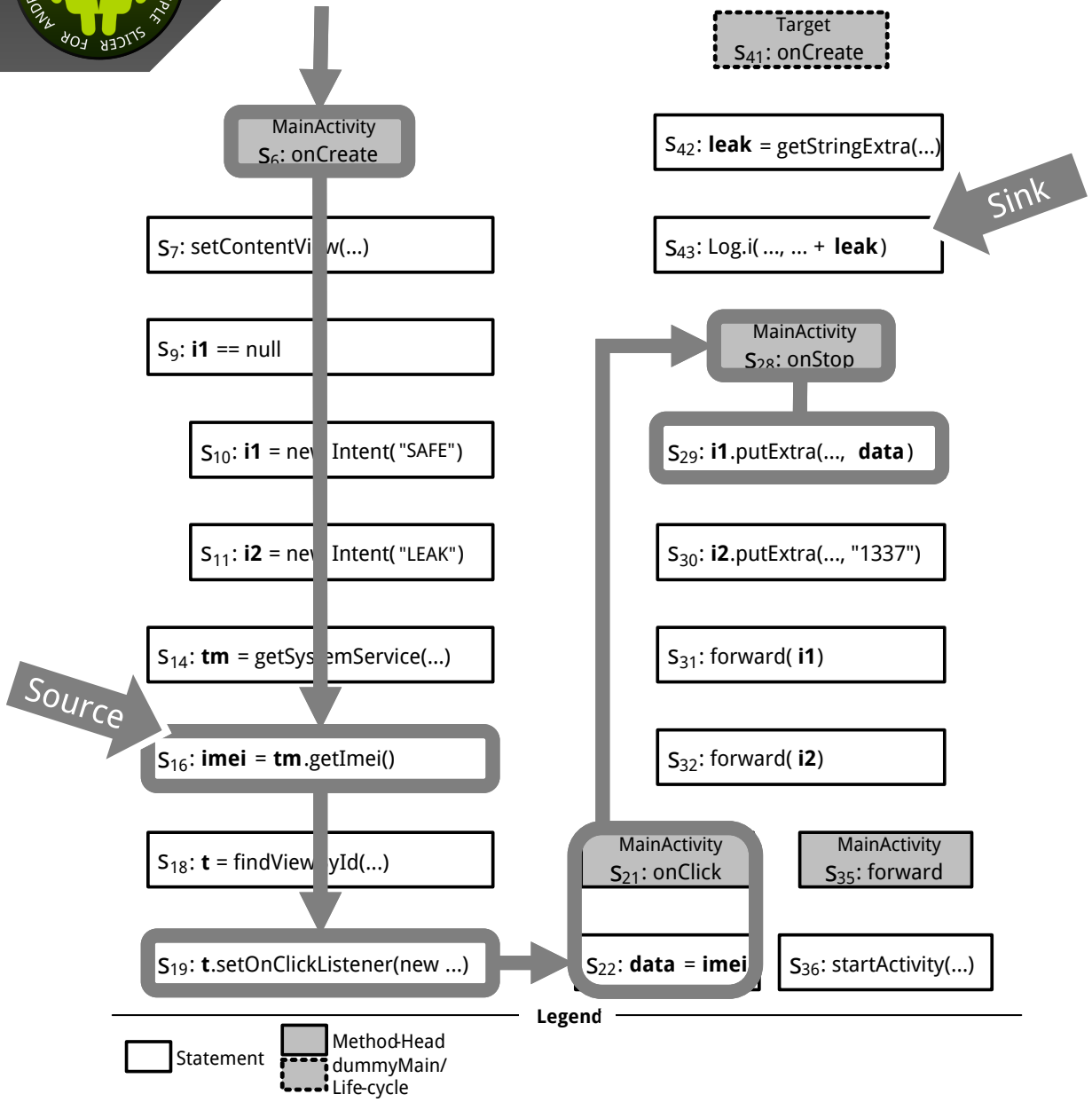
Example: Cooperative Taint Analysis



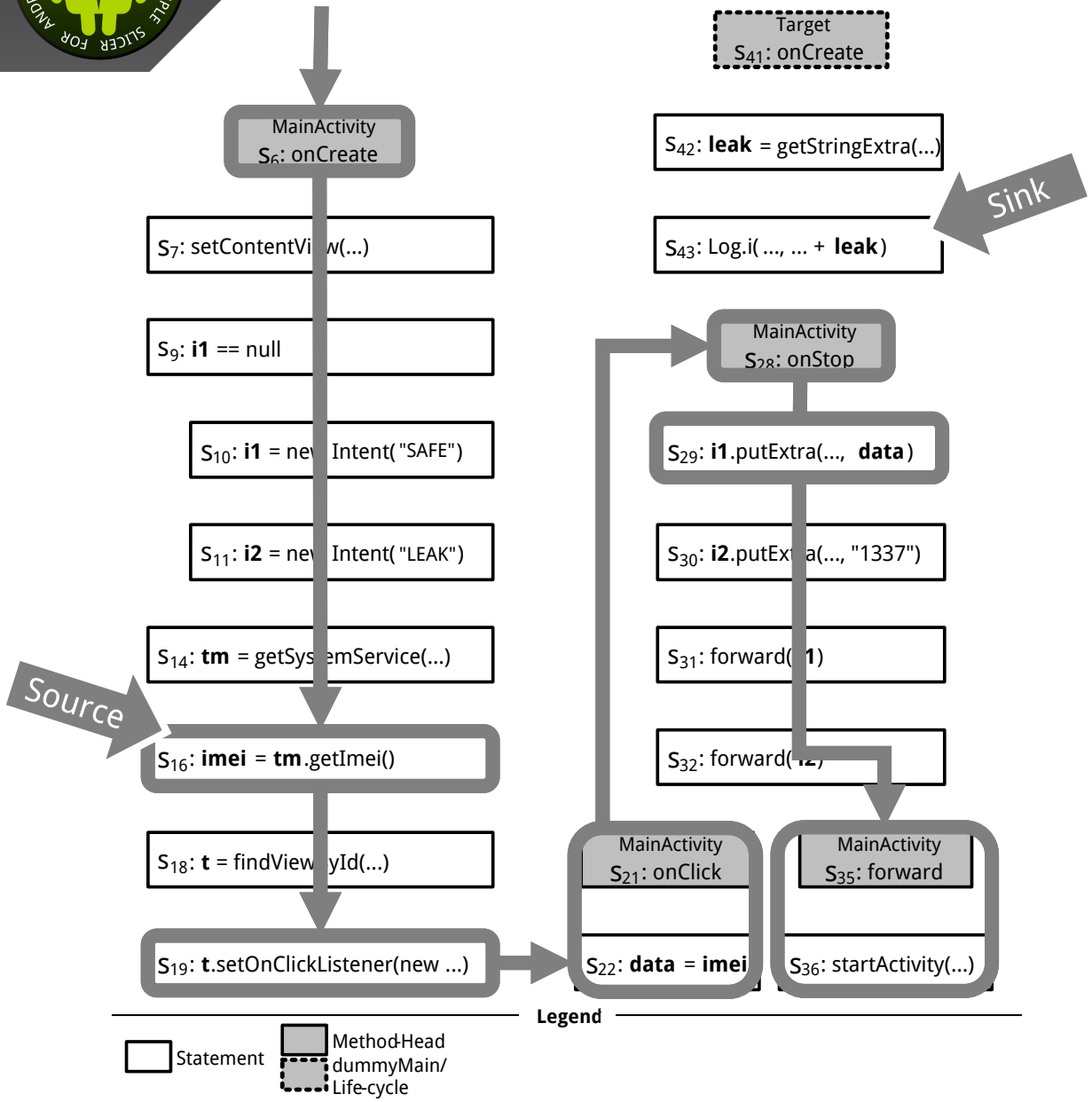
Example: Cooperative Taint Analysis



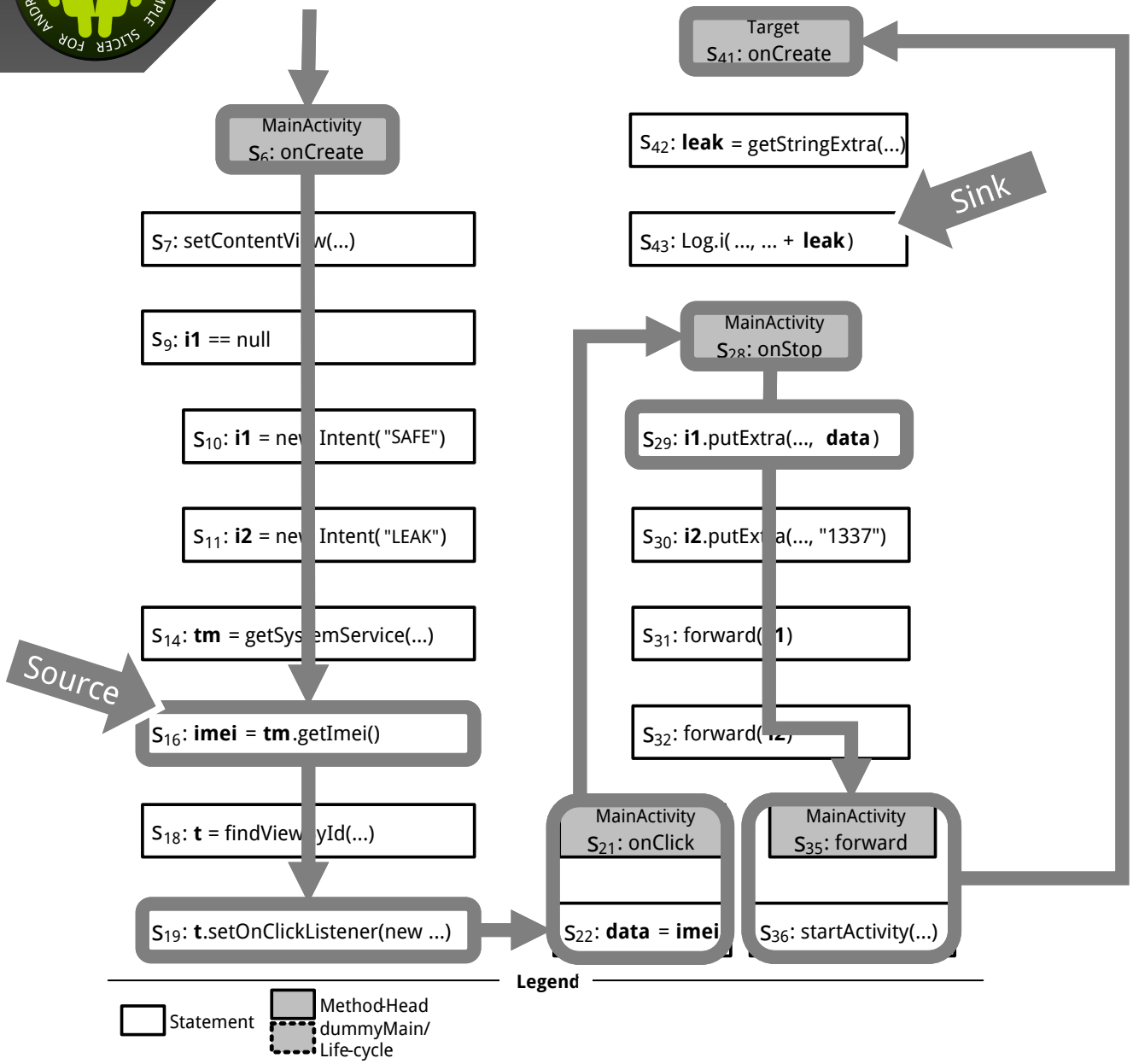
Example: Cooperative Taint Analysis



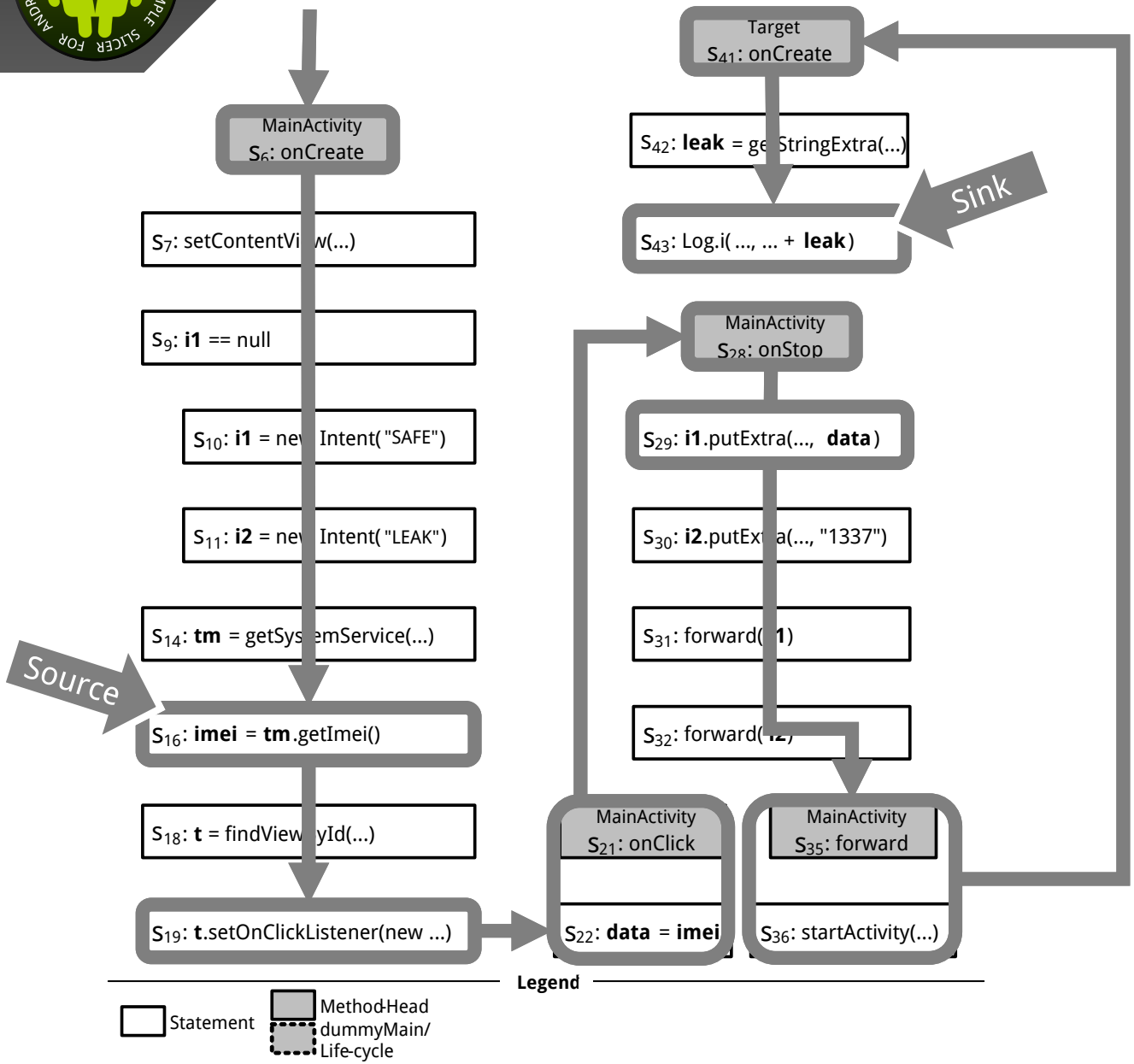
Example: Cooperative Taint Analysis



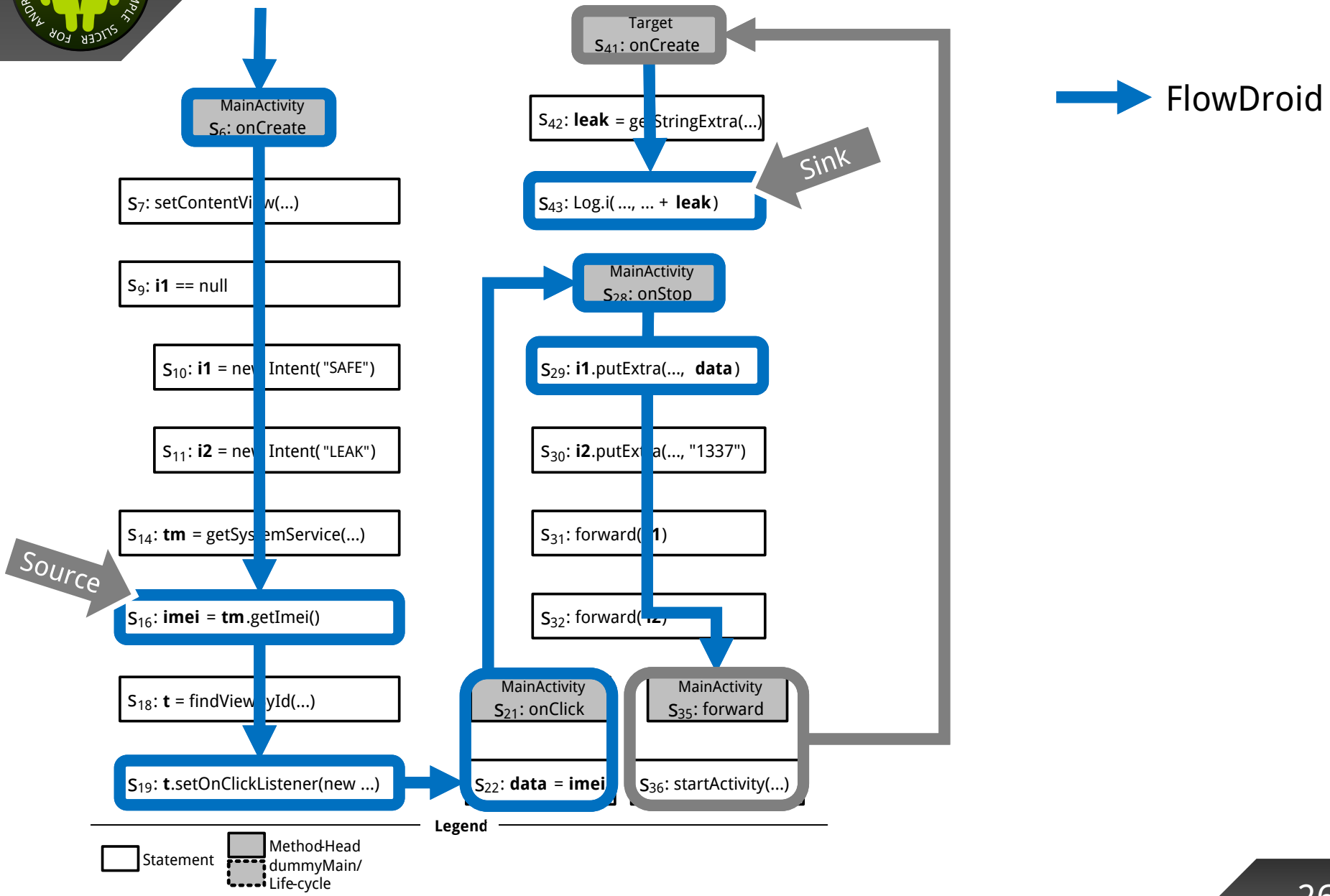
Example: Cooperative Taint Analysis



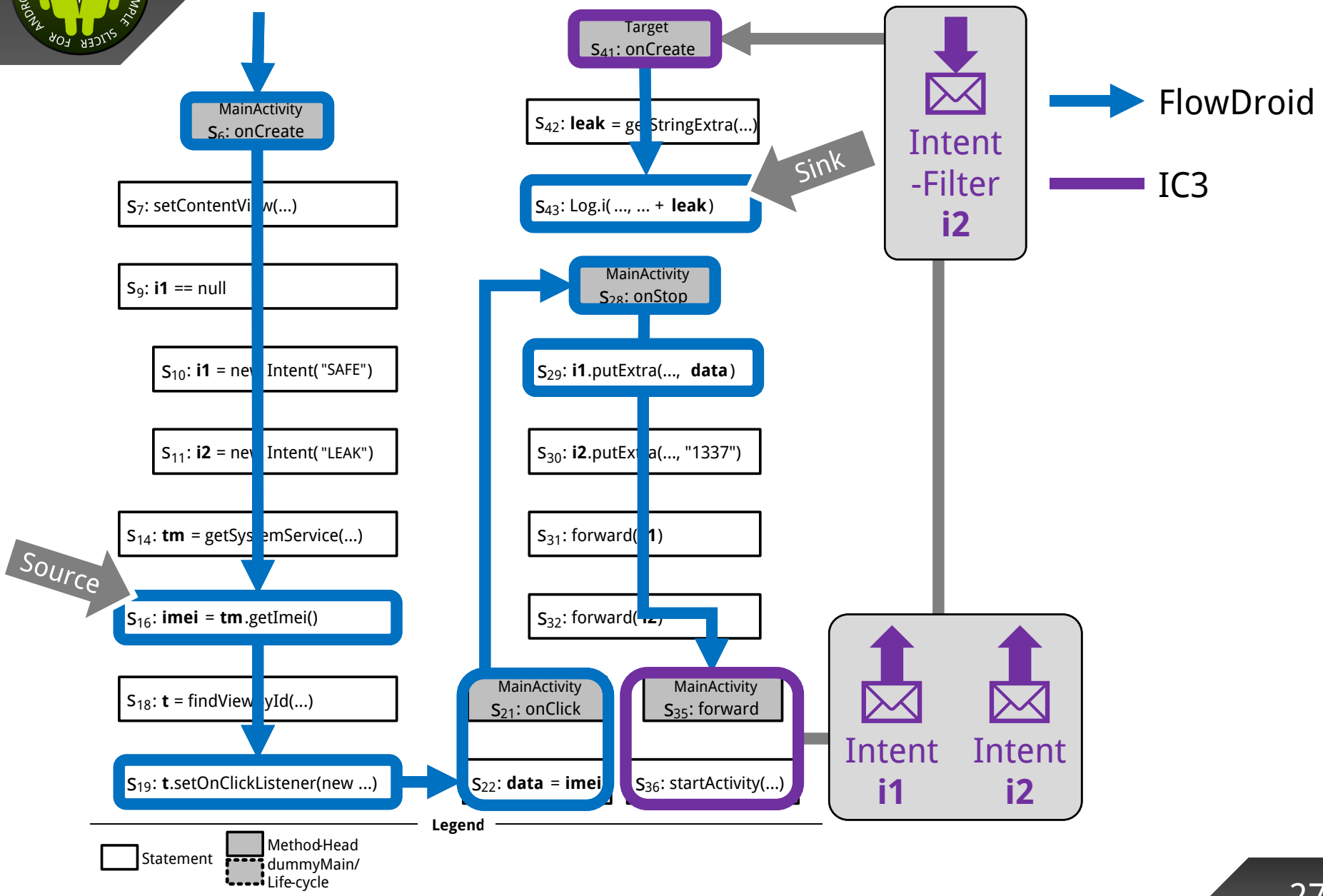
Example: Cooperative Taint Analysis



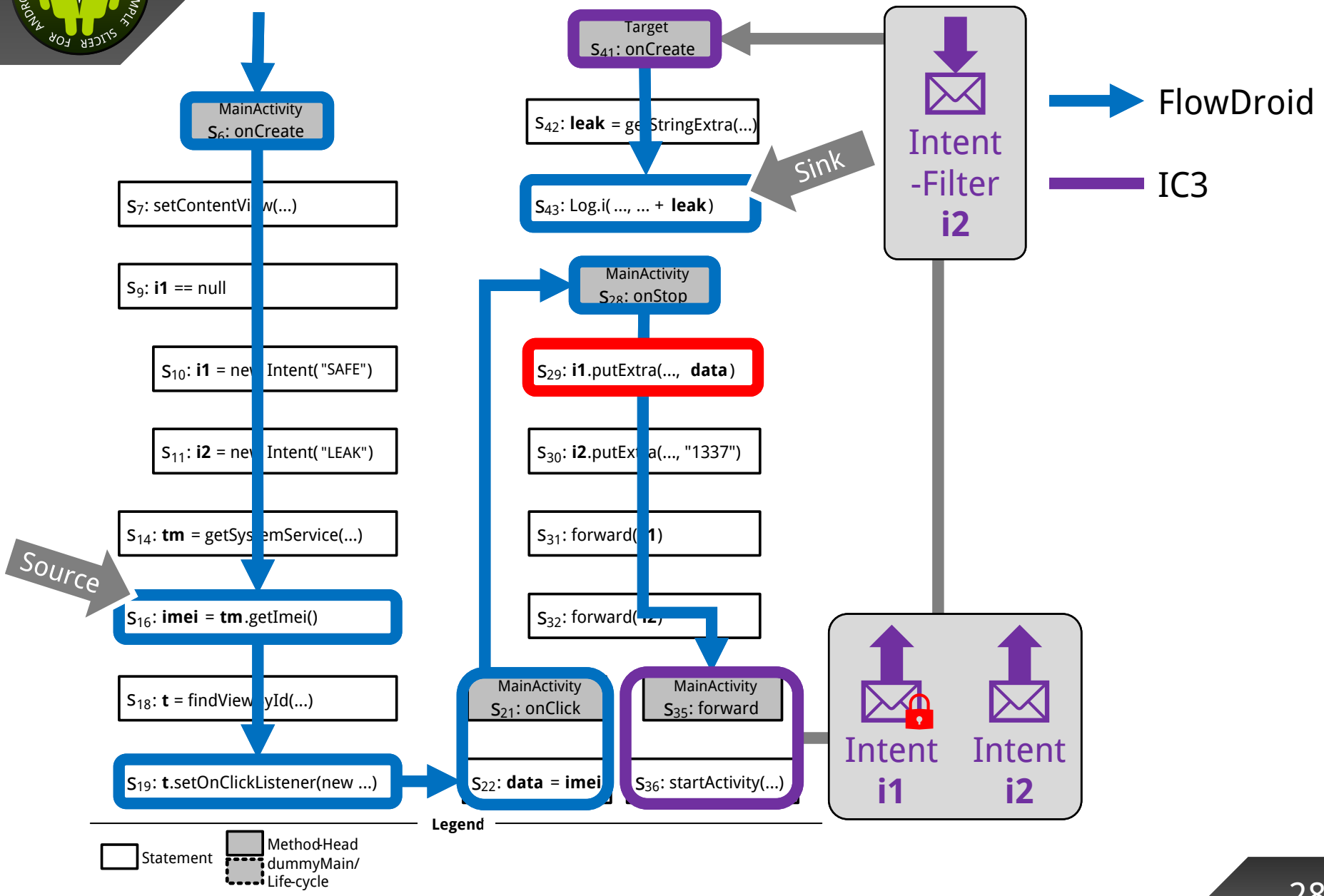
Example: Cooperative Taint Analysis



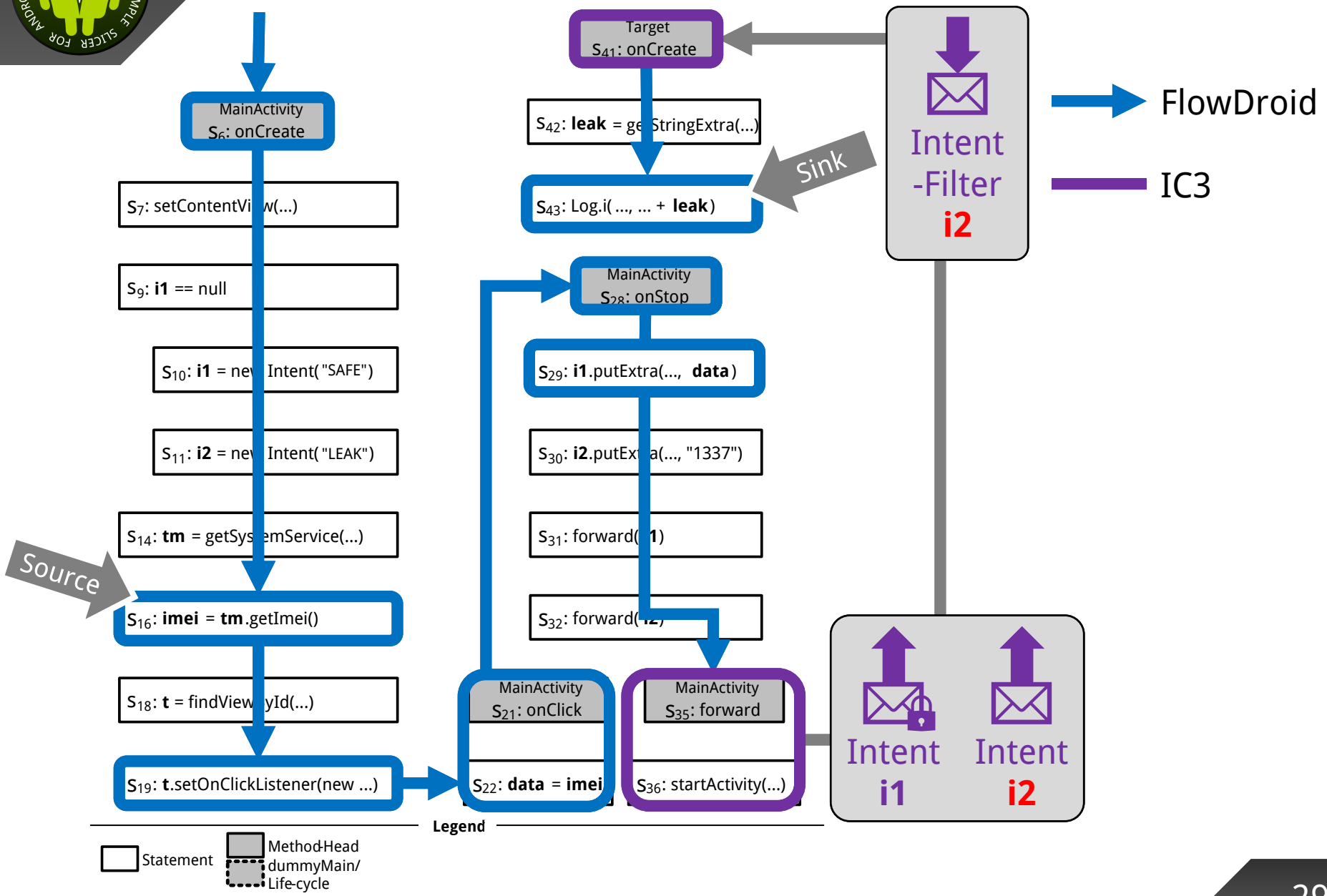
Example: Cooperative Taint Analysis



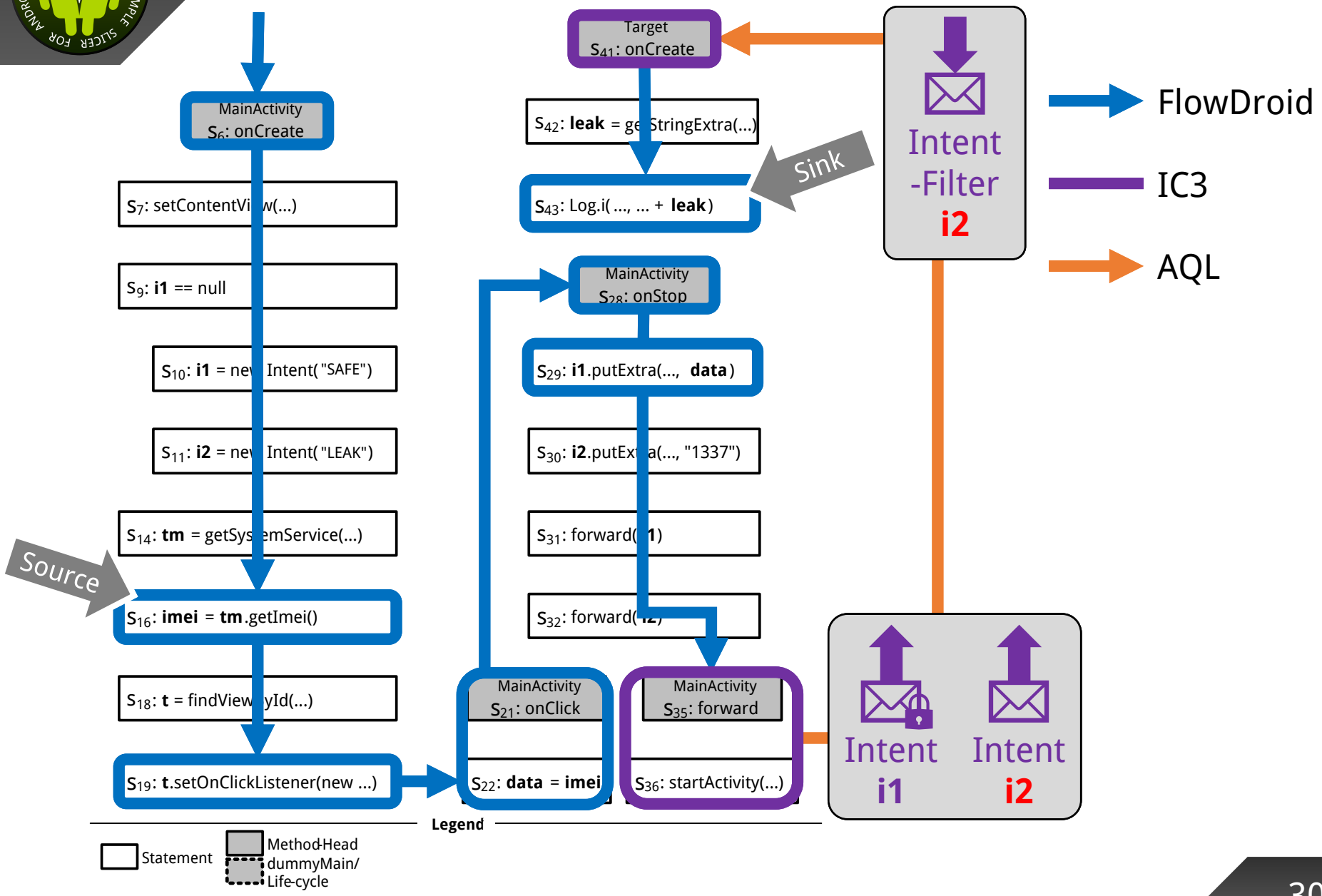
Example: Cooperative Taint Analysis



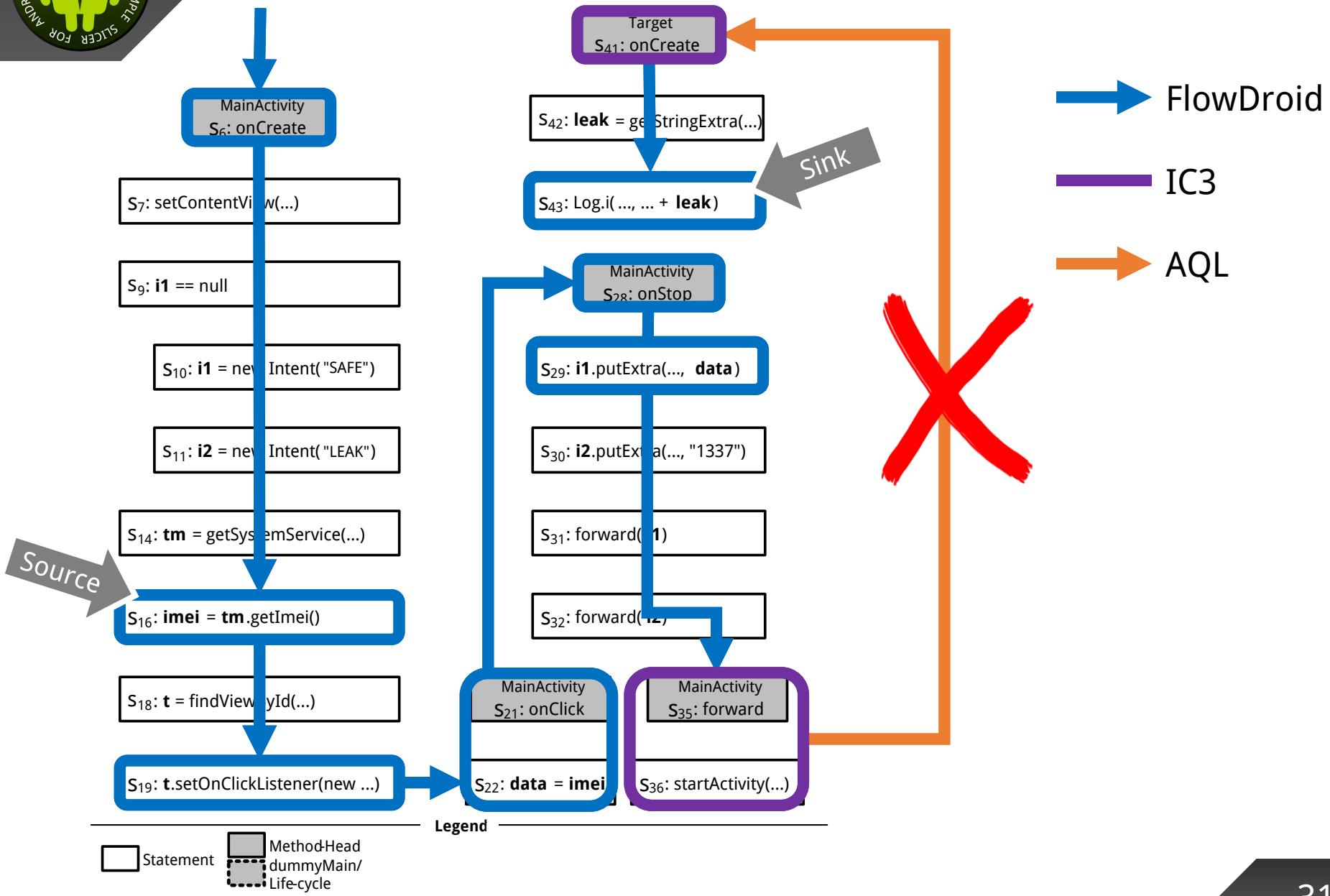
Example: Cooperative Taint Analysis



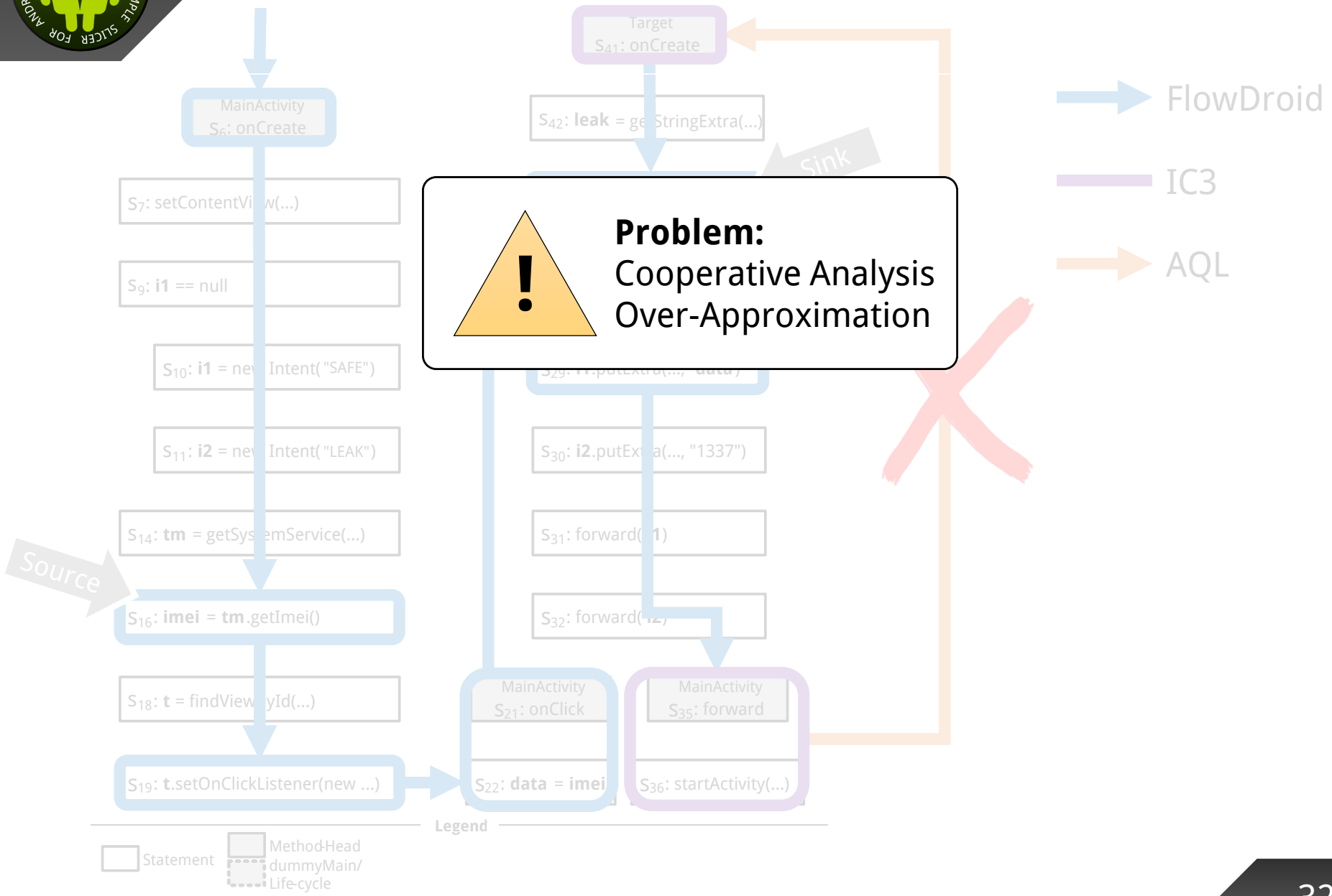
Example: Cooperative Taint Analysis



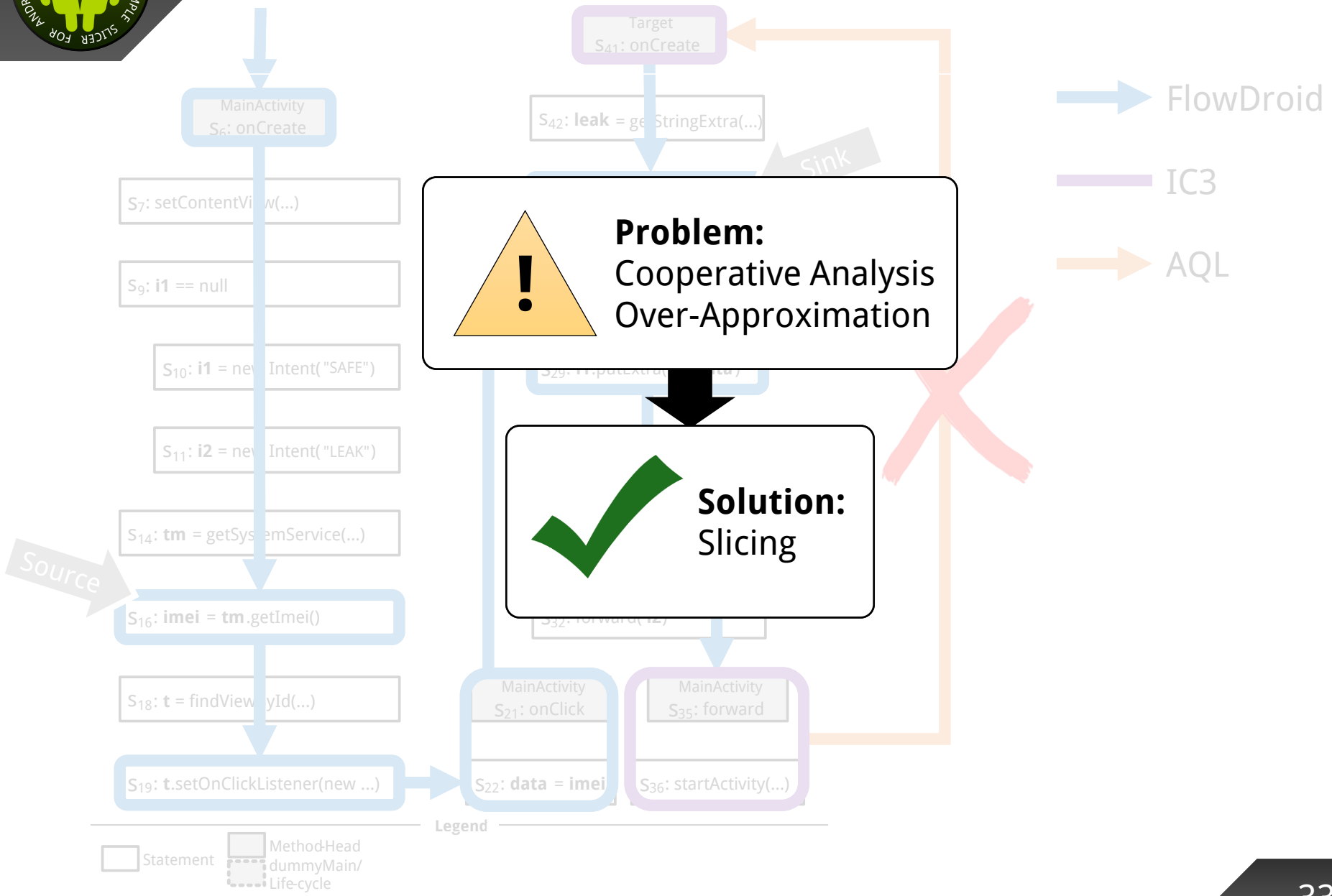
Example: Cooperative Taint Analysis



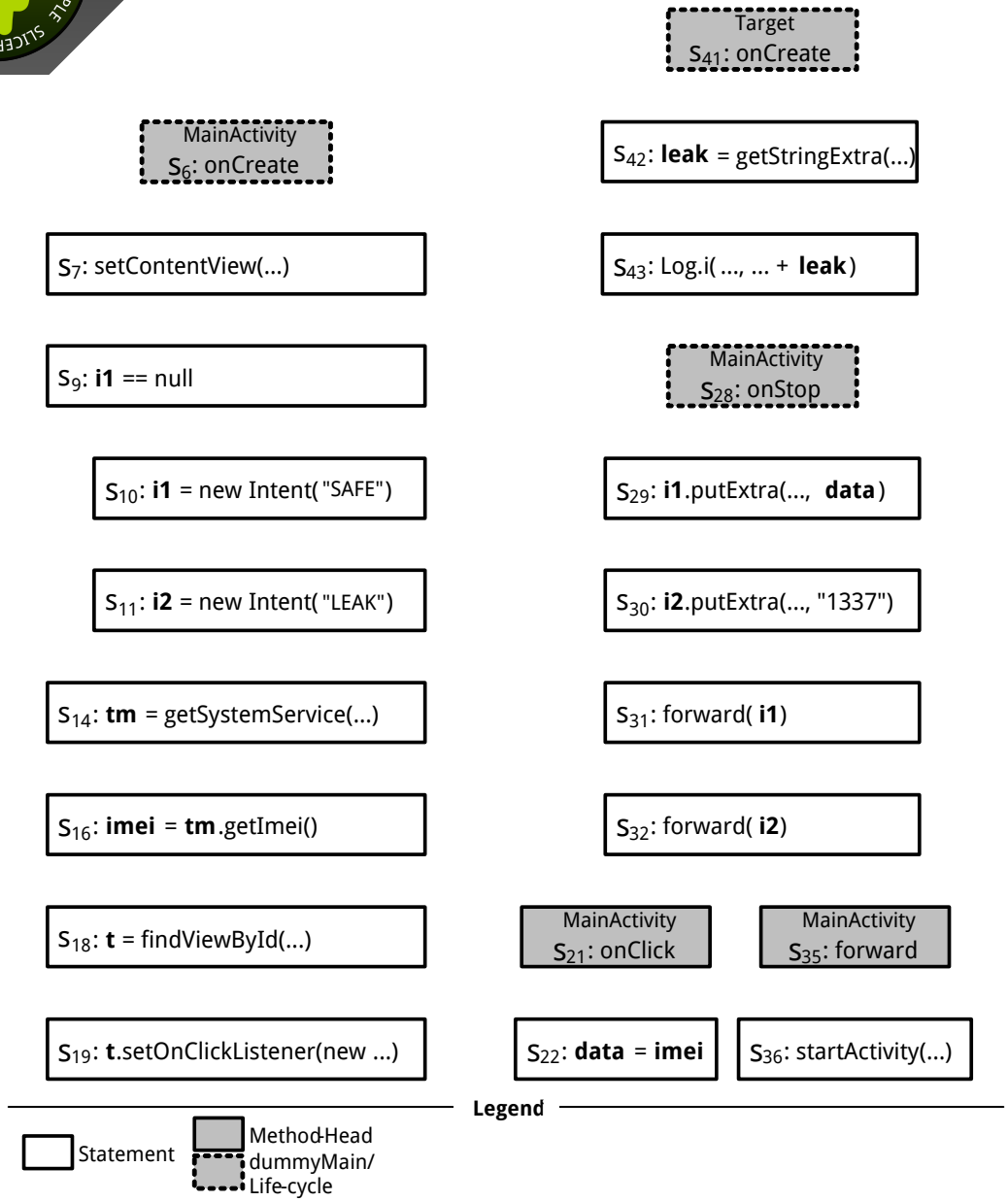
Example: Cooperative Taint Analysis



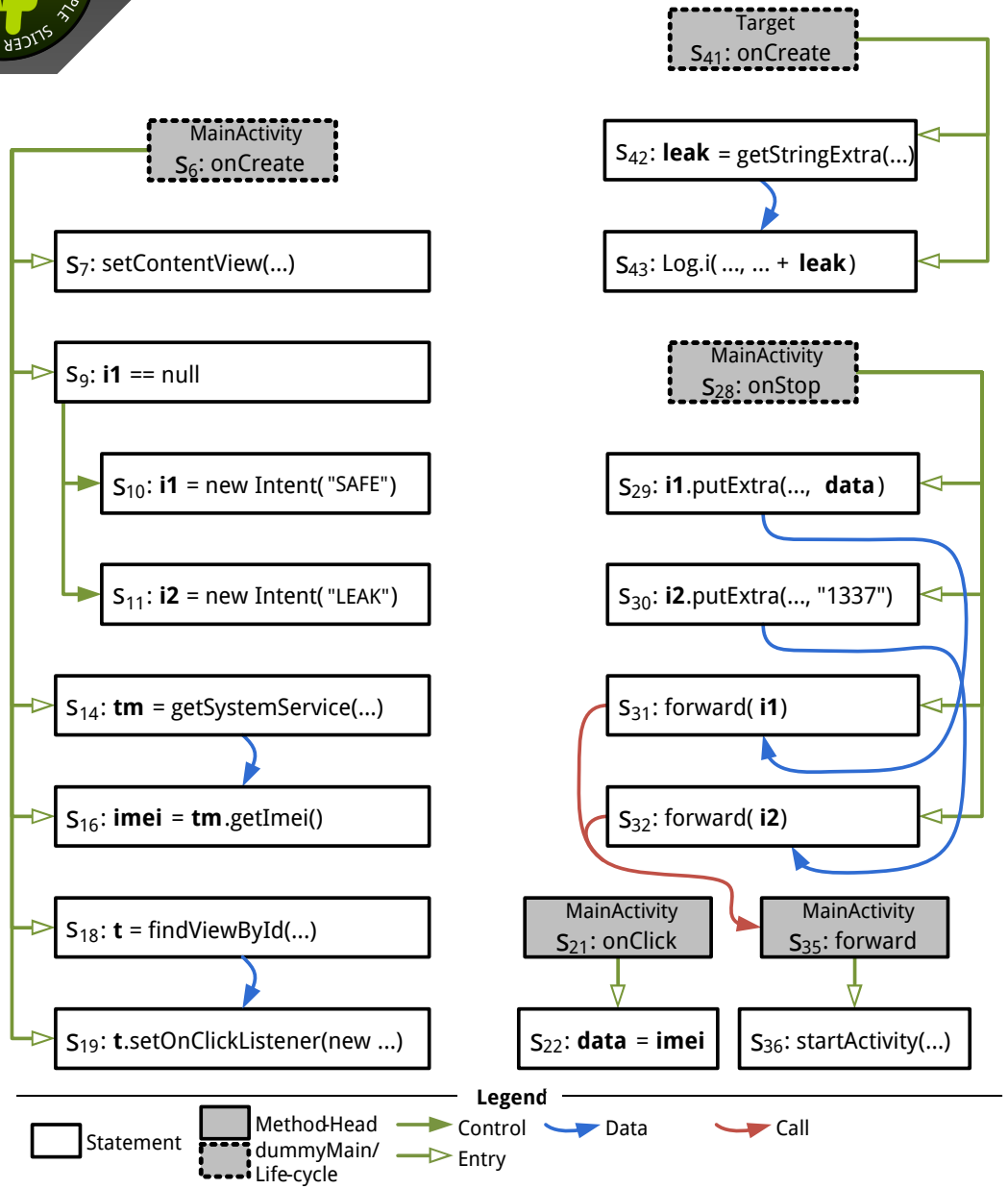
Example: Cooperative Taint Analysis



Example: Slicing

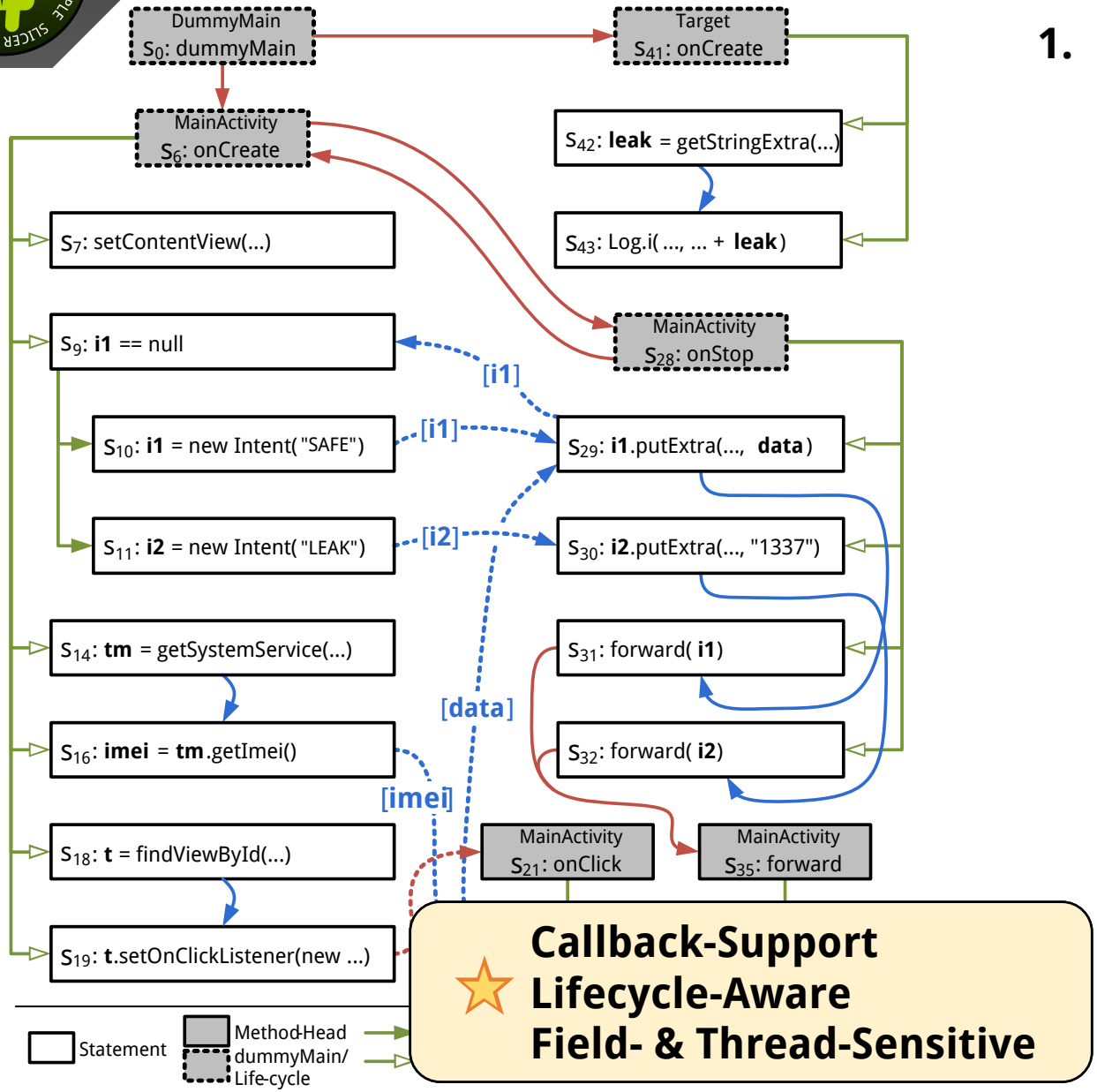


Example: Slicing



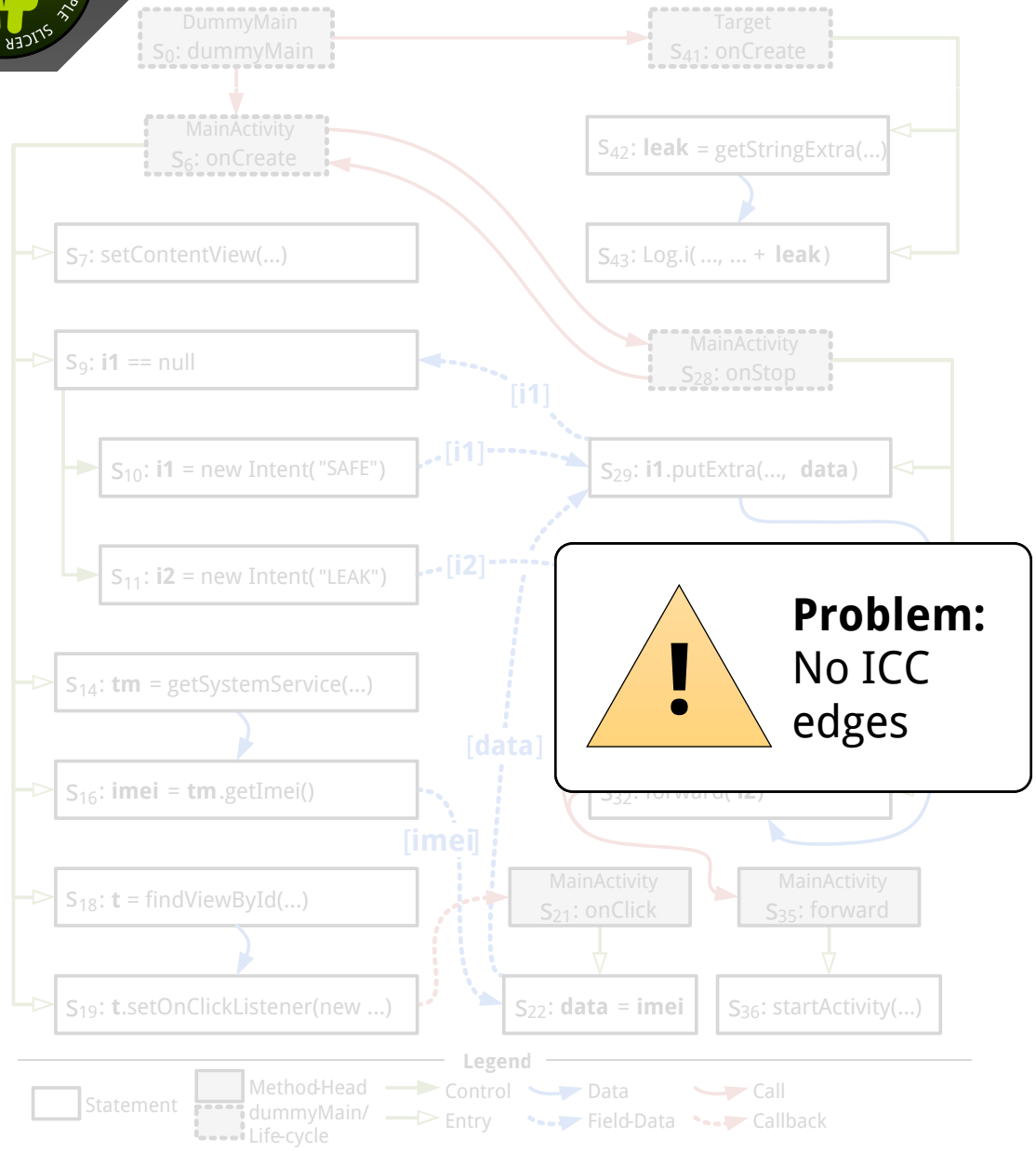
1. **Graph Generation**
   - Build **PDG**
   - Merge to **SDG**

Example: Slicing



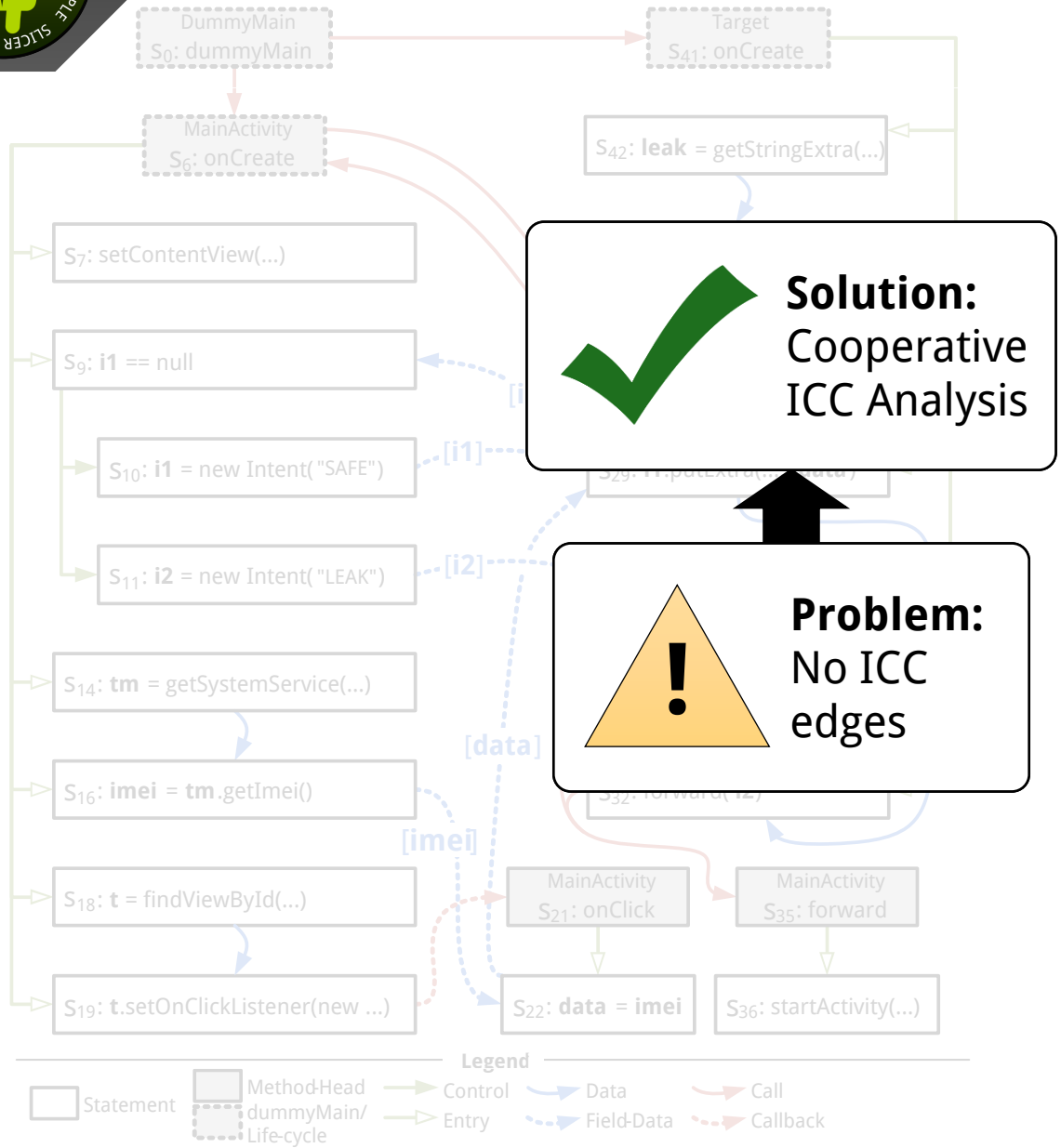
1. **Graph Generation**
   - Build **PDG**
   - Merge to **SDG**
   - Enhance to **ADG**

Example: Slicing



1. **Graph Generation**
   - Build **PDG**
   - Merge to **SDG**
   - Enhance to **ADG**

Example: Slicing

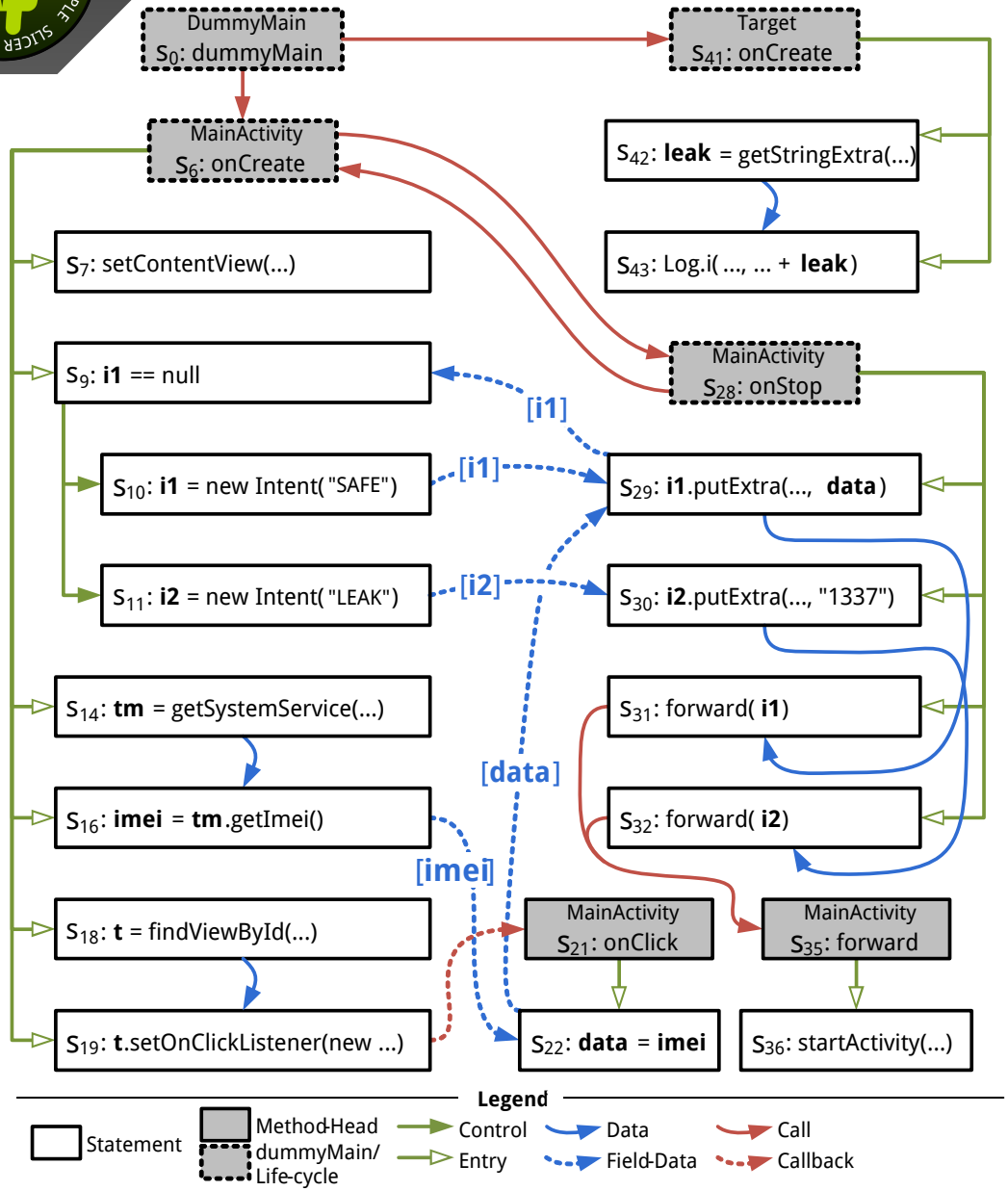


Solution:
Cooperative
ICC Analysis

Problem:
No ICC
edges

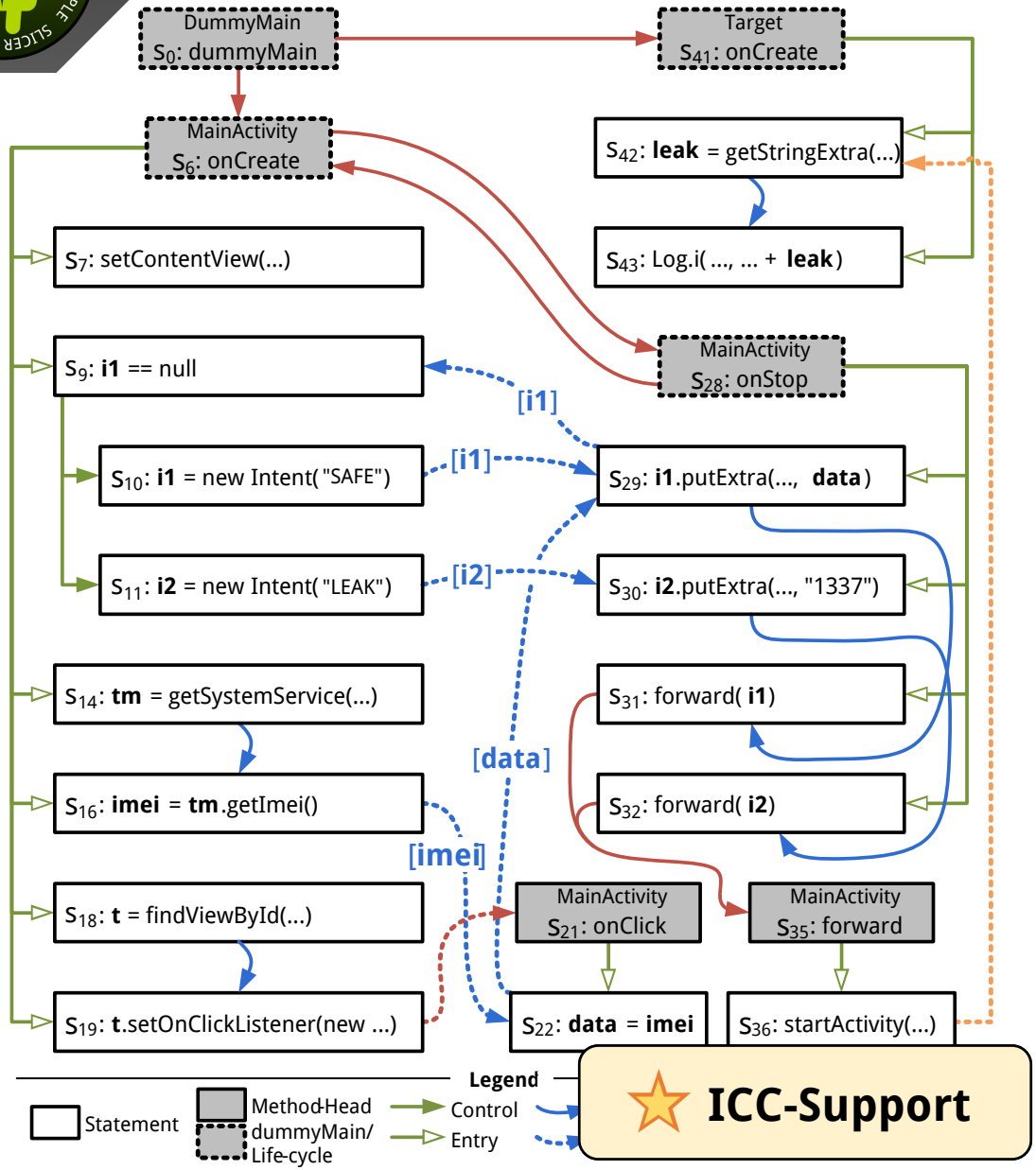
1. **Graph Generation**
   - Build **PDG**
   - Merge to **SDG**
   - Enhance to **ADG**

Example: Slicing



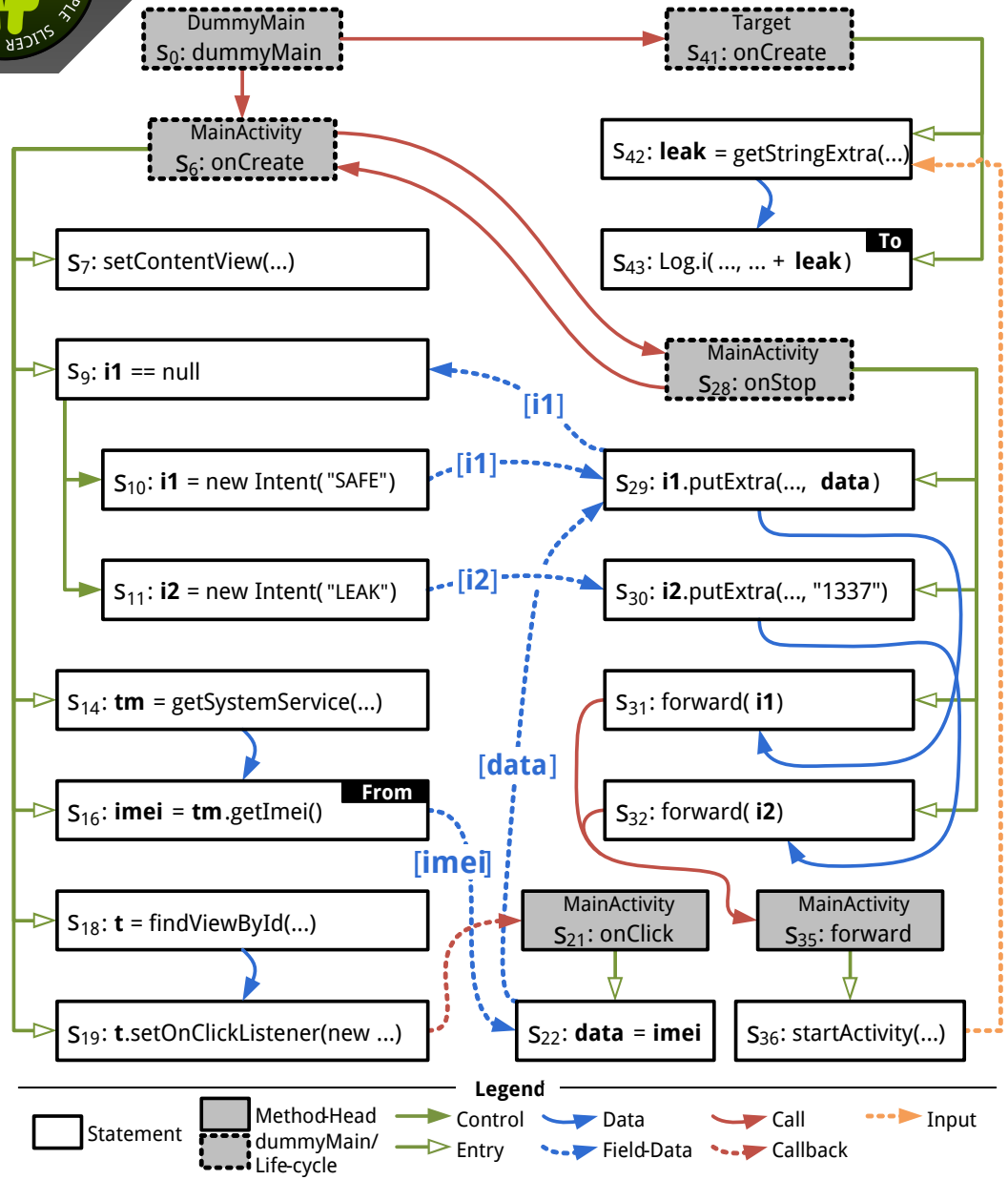
1. **Graph Generation**
   - Build **PDG**
   - Merge to **SDG**
   - Enhance to **ADG**

Example: Slicing



1. **Graph Generation**
   - Build **PDG**
   - Merge to **SDG**
   - Enhance to **ADG**

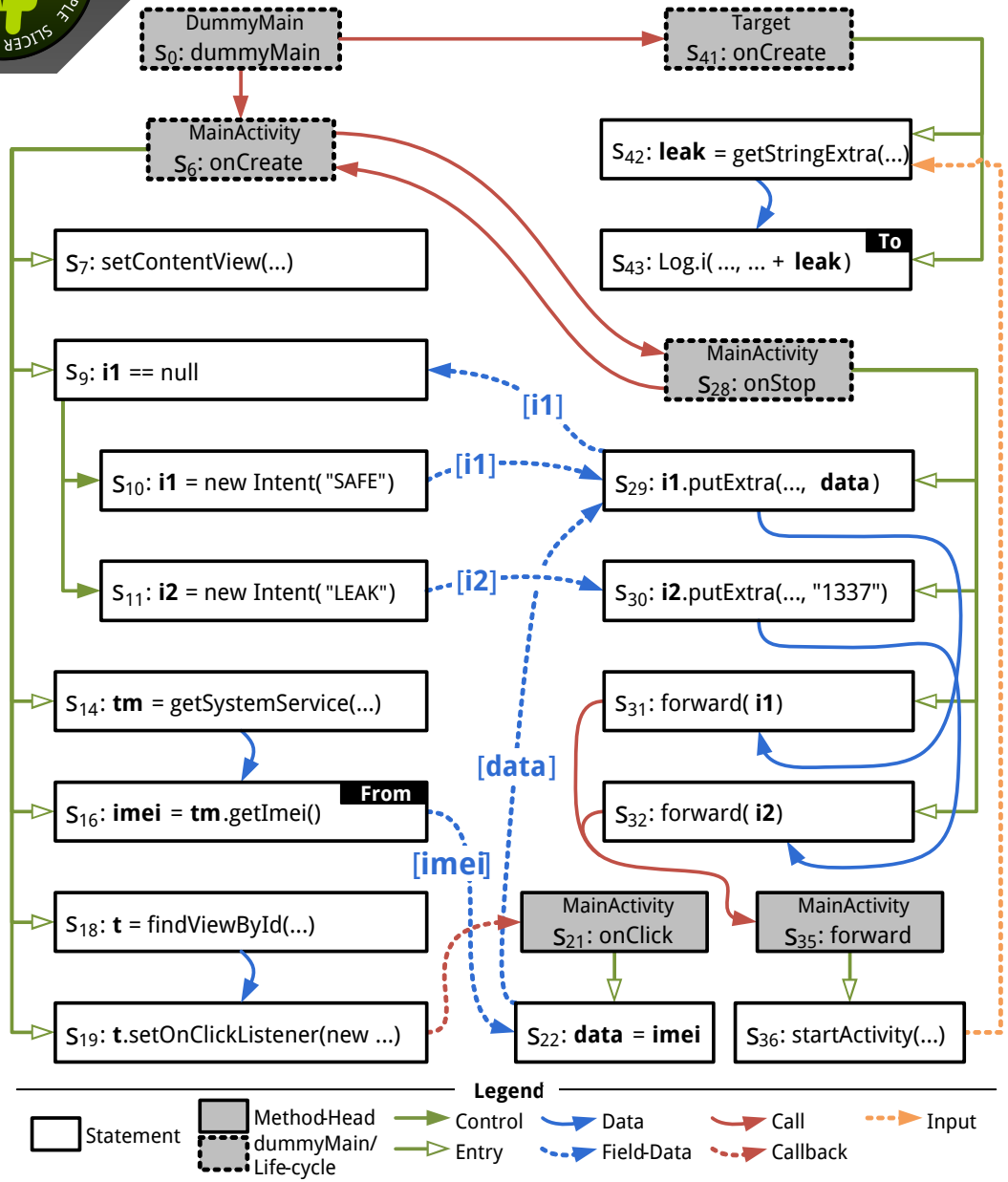
Example: Slicing



1. **Graph Generation**
   - Build **PDG**
   - Merge to **SDG**
   - Enhance to **ADG**

2. **Slicing**
   - Identify Criteria

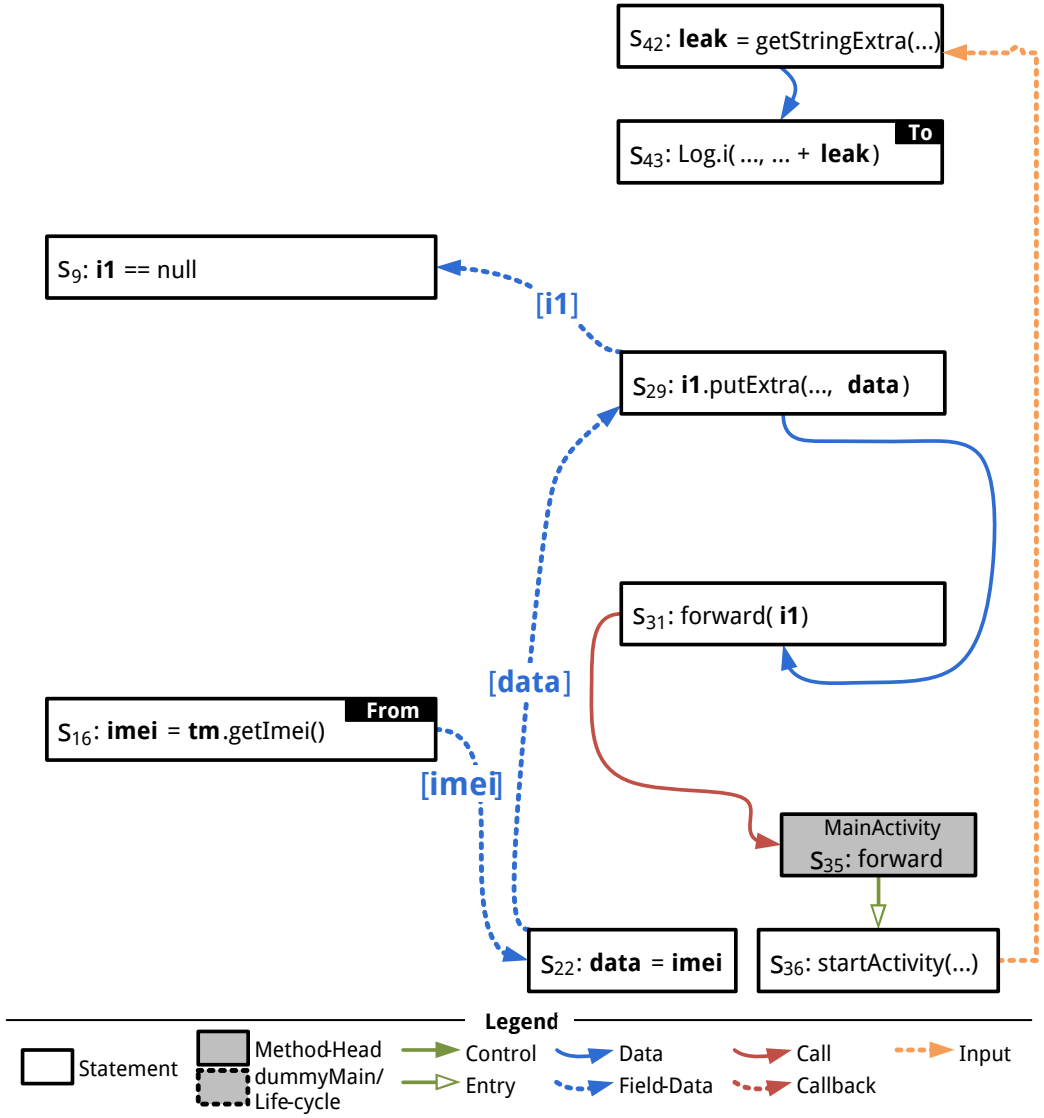
Example: Slicing



1. **Graph Generation**
   - Build **PDG**
   - Merge to **SDG**
   - Enhance to **ADG**

2. **Slicing**
   - Identify Criteria
   - Slice Forward
     - **FFF:** Forward Field Filtering

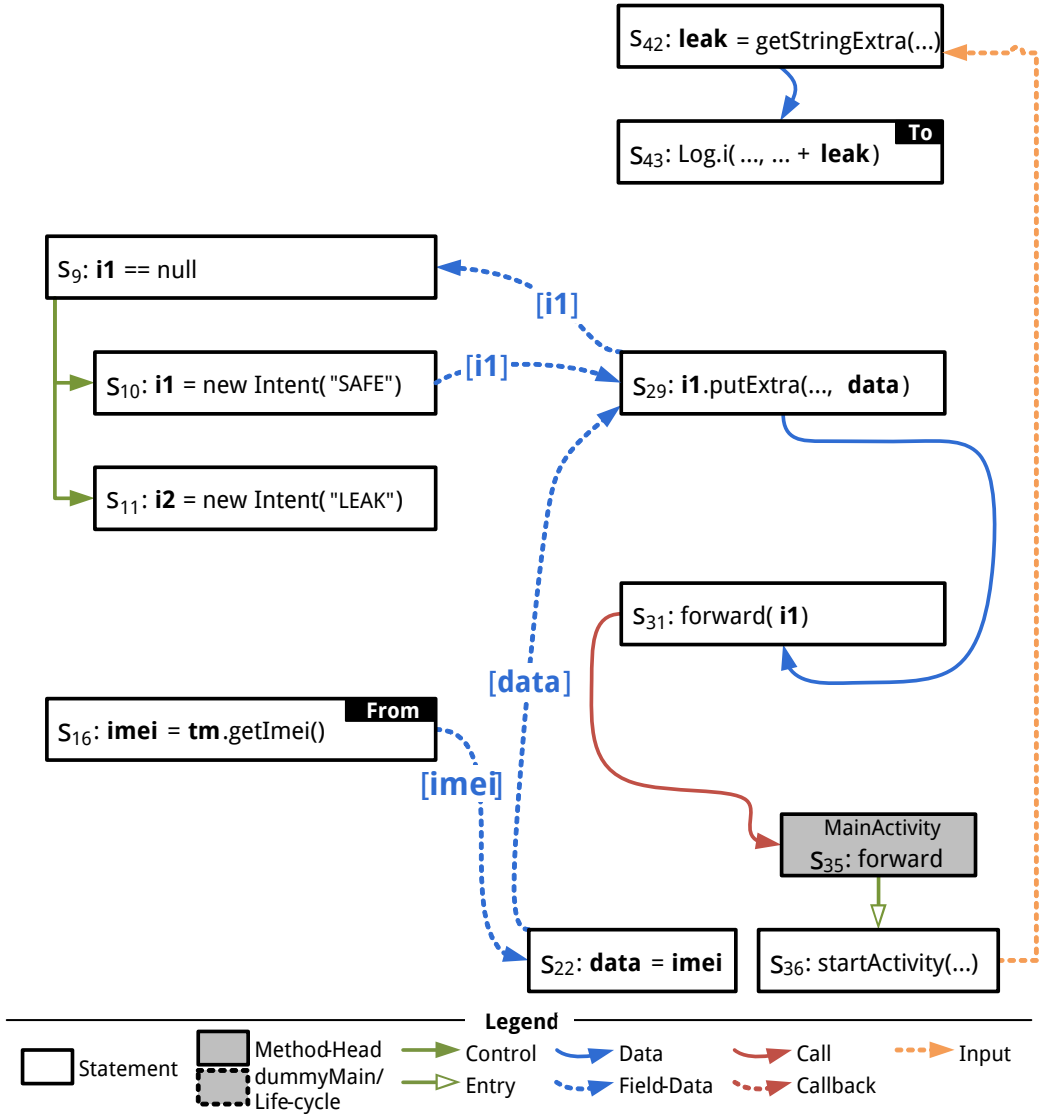
Example: Slicing



1. **Graph Generation**
   - Build **PDG**
   - Merge to **SDG**
   - Enhance to **ADG**

2. **Slicing**
   - Identify Criteria
   - Slice Forward
     - **FFF:** Forward Field Filtering

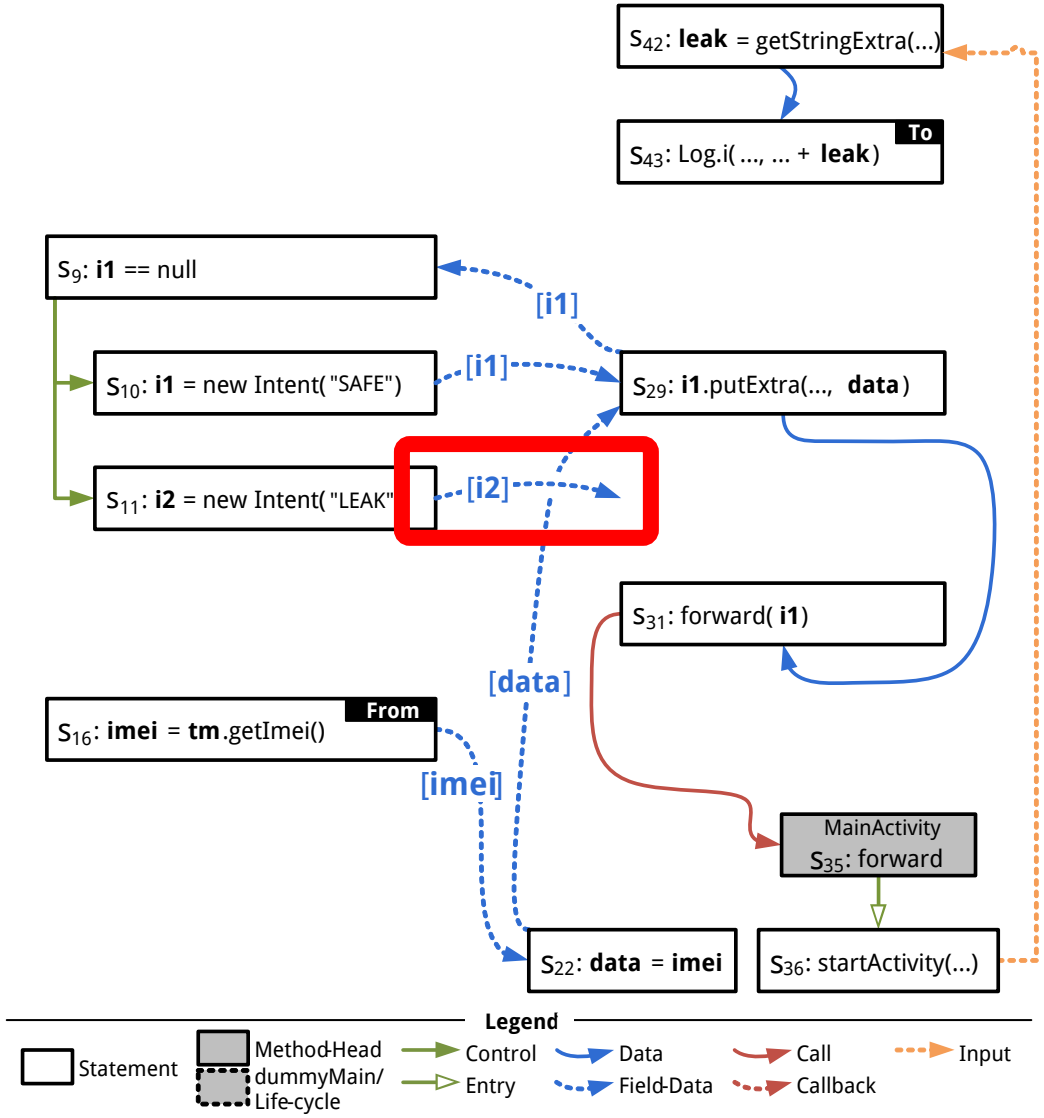
Example: Slicing



1. **Graph Generation**
   - Build **PDG**
   - Merge to **SDG**
   - Enhance to **ADG**

2. **Slicing**
   - Identify Criteria
   - Slice Forward
     - **FFF:** Forward Field Filtering

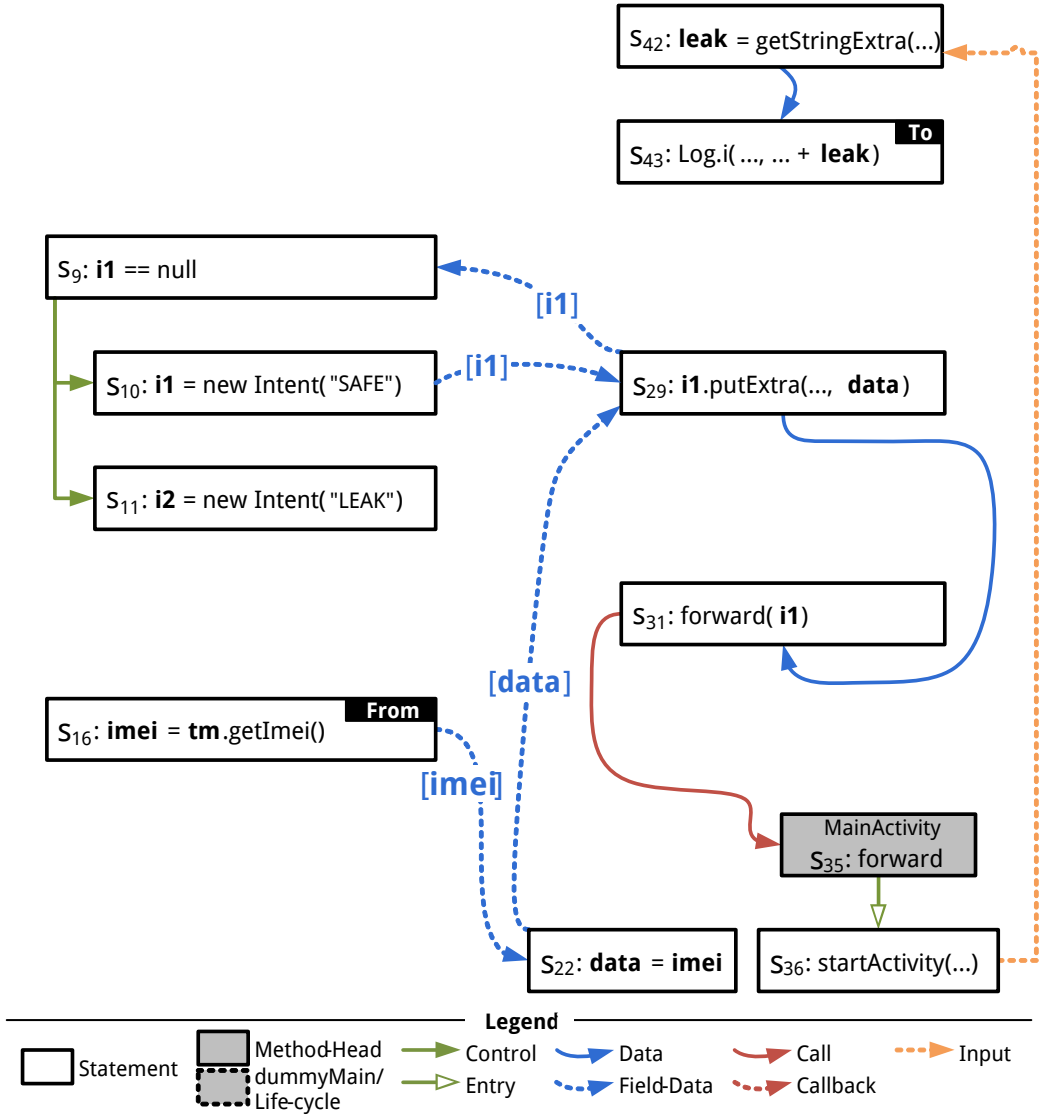
Example: Slicing



1. **Graph Generation**
   - Build **PDG**
   - Merge to **SDG**
   - Enhance to **ADG**

---

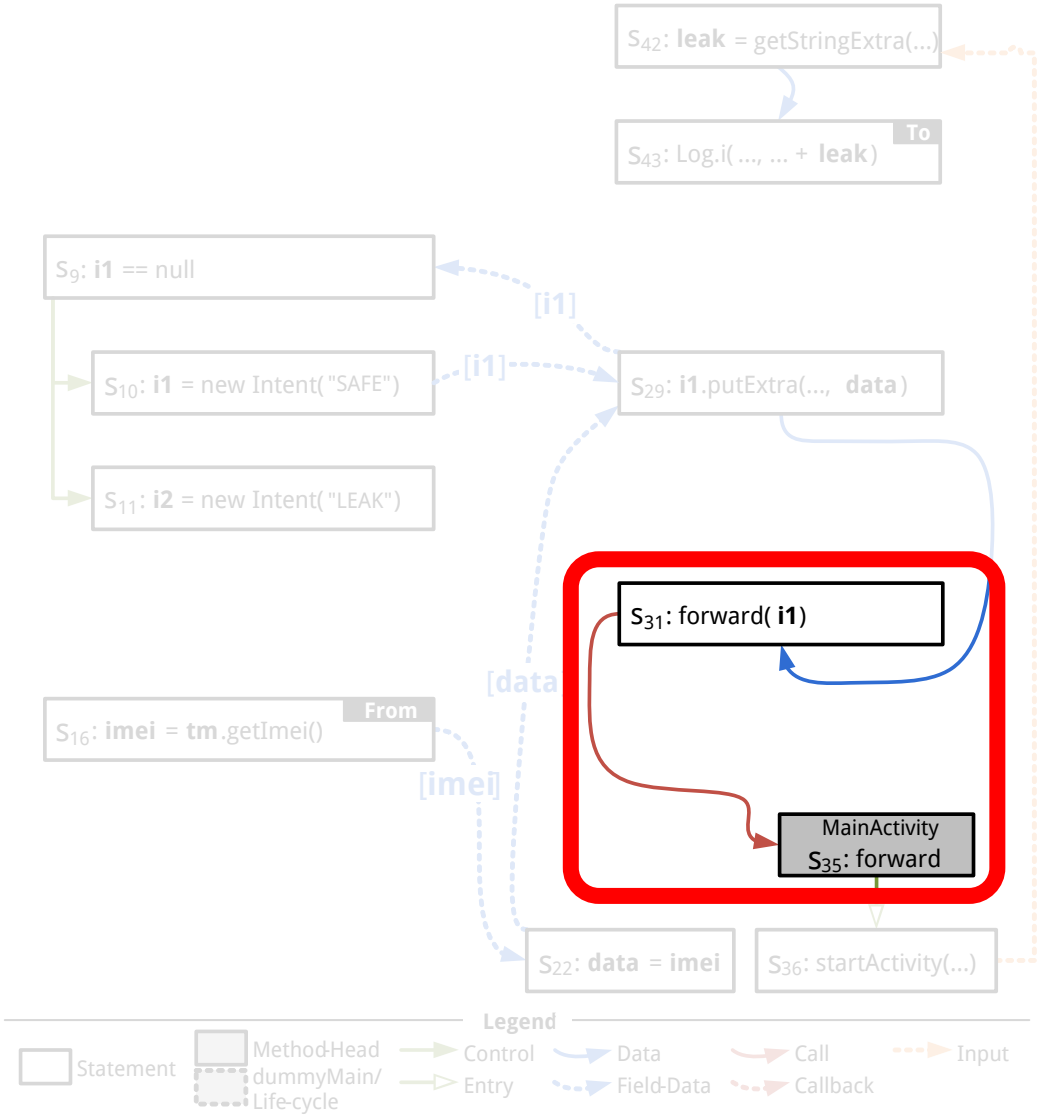
2. **Slicing**
   - Identify Criteria
   - Slice Forward
     - **FFF:** Forward Field Filtering



1. **Graph Generation**
   - Build **PDG**
   - Merge to **SDG**
   - Enhance to **ADG**

2. **Slicing**
   - Identify Criteria
   - Slice Forward
     - **FFF:** Forward Field Filtering

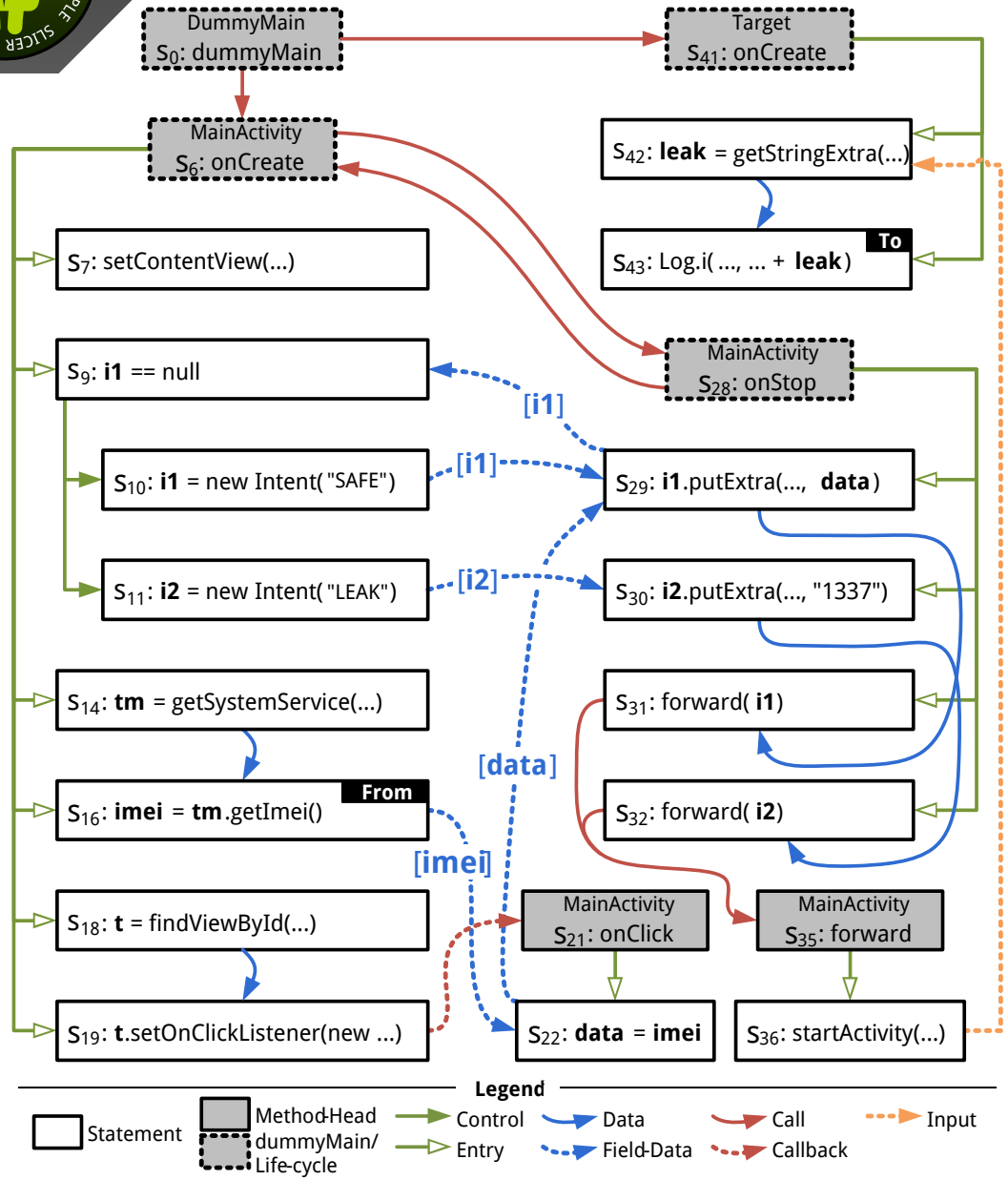
Example: Slicing



1. **Graph Generation**
   - Build **PDG**
   - Merge to **SDG**
   - Enhance to **ADG**

2. **Slicing**
   - Identify Criteria
   - Slice Forward
     - **FFF:** Forward Field Filtering

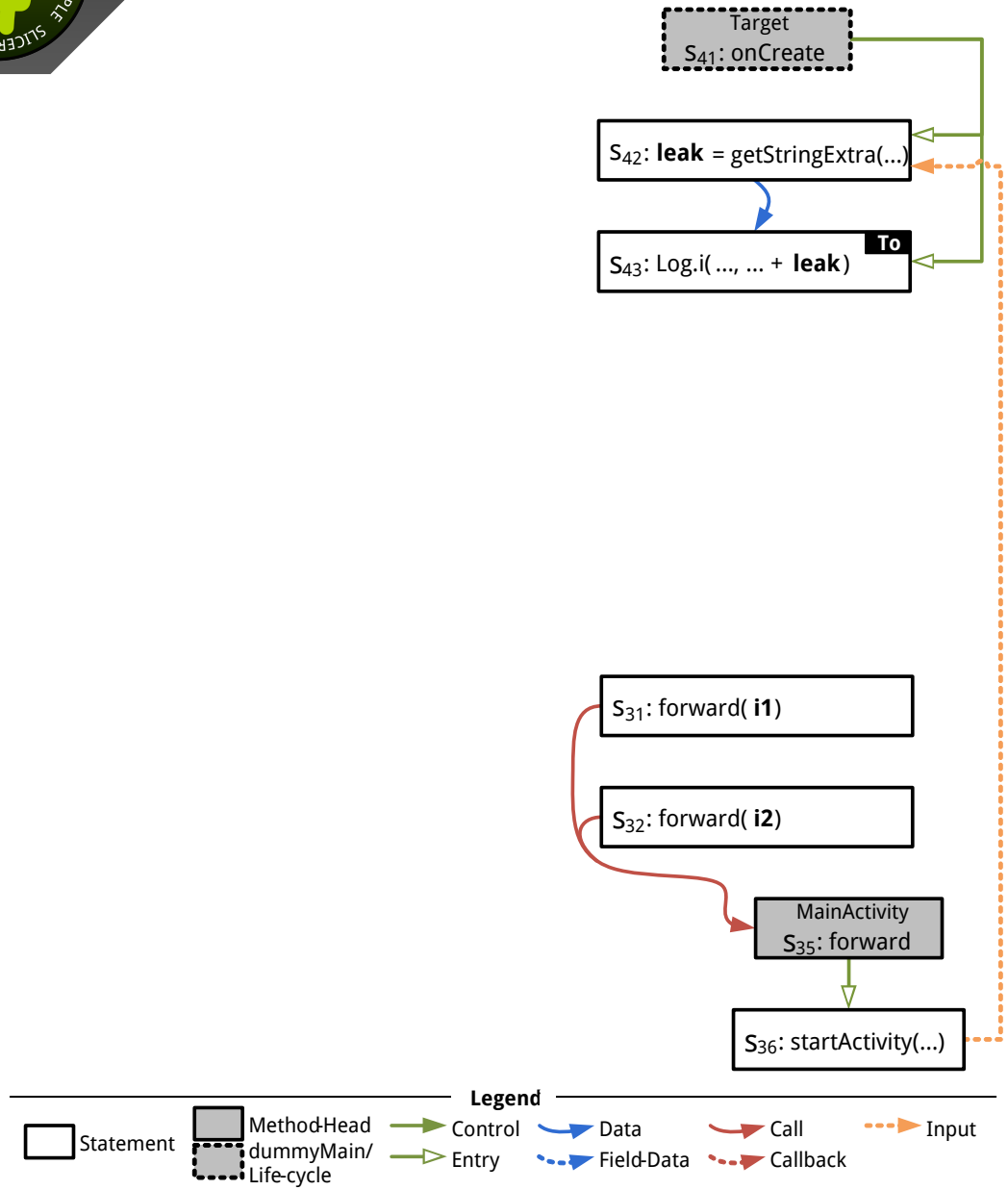
Example: Slicing



1. **Graph Generation**
   - Build **PDG**
   - Merge to **SDG**
   - Enhance to **ADG**

2. **Slicing**
   - Identify Criteria
   - Slice Forward
     - **FFF:** Forward Field Filtering
   - Slice Backward
     - **CSR:** Context-Sensitive Refinement

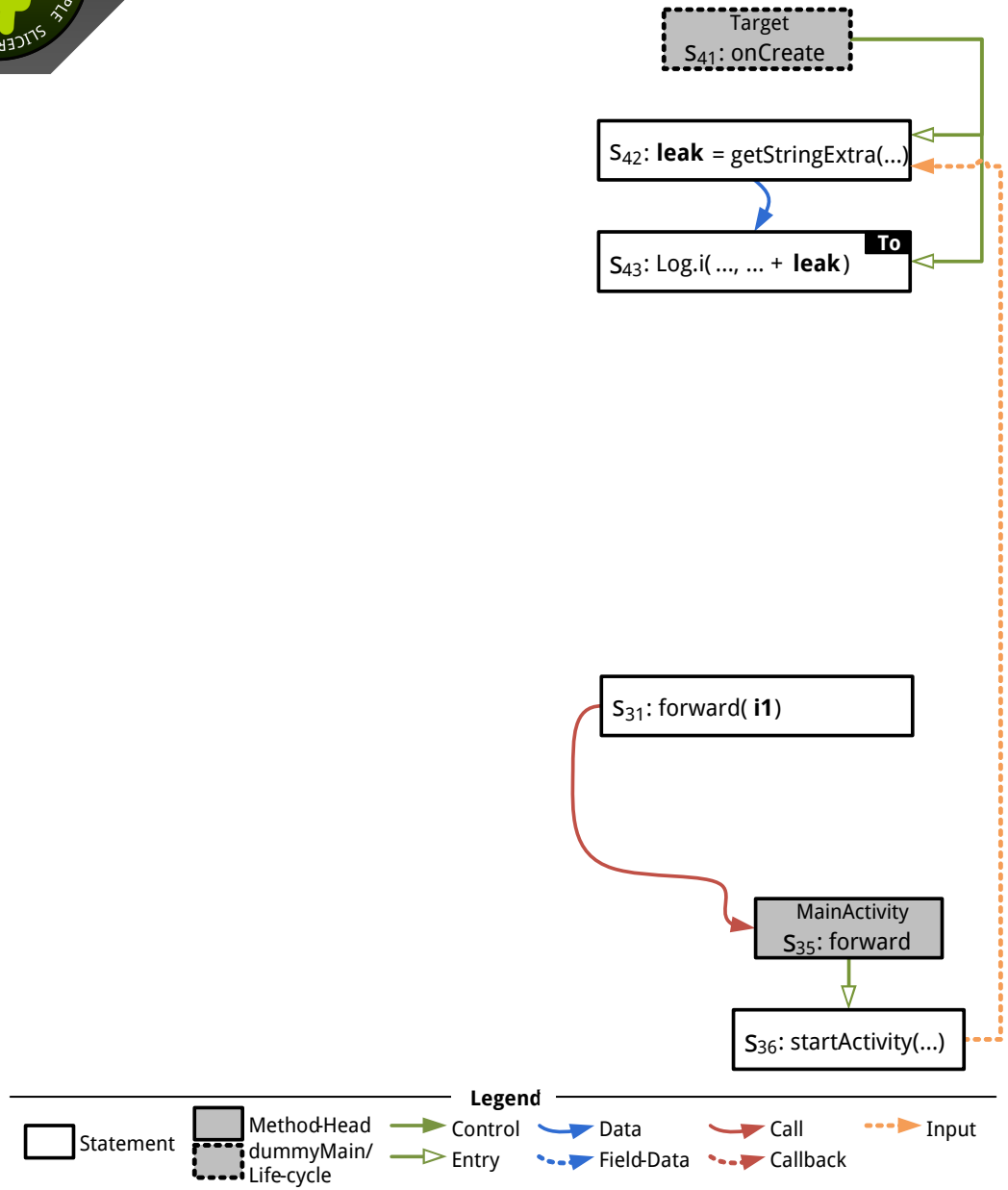
Example: Slicing



1. **Graph Generation**
   - Build **PDG**
   - Merge to **SDG**
   - Enhance to **ADG**

2. **Slicing**
   - Identify Criteria
   - Slice Forward
     - **FFF:** Forward Field Filtering
   - Slice Backward
     - **CSR:** Context-Sensitive Refinement

Example: Slicing

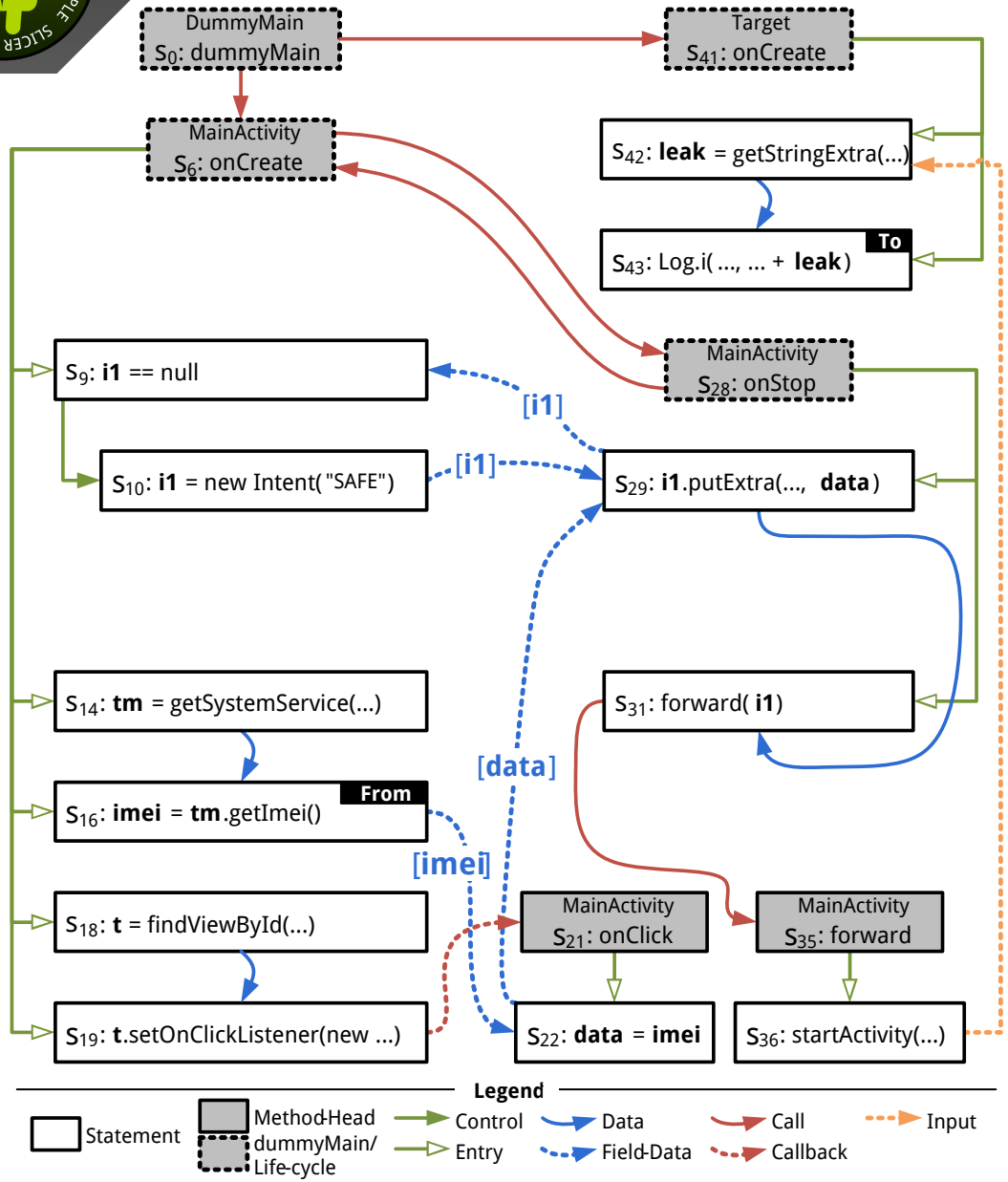


1. **Graph Generation**
   - Build **PDG**
   - Merge to **SDG**
   - Enhance to **ADG**

---

2. **Slicing**
   - Identify Criteria
   - Slice Forward
     - **FFF:** Forward Field Filtering
   - Slice Backward
     - **CSR:** Context-Sensitive Refinement

Example: Slicing

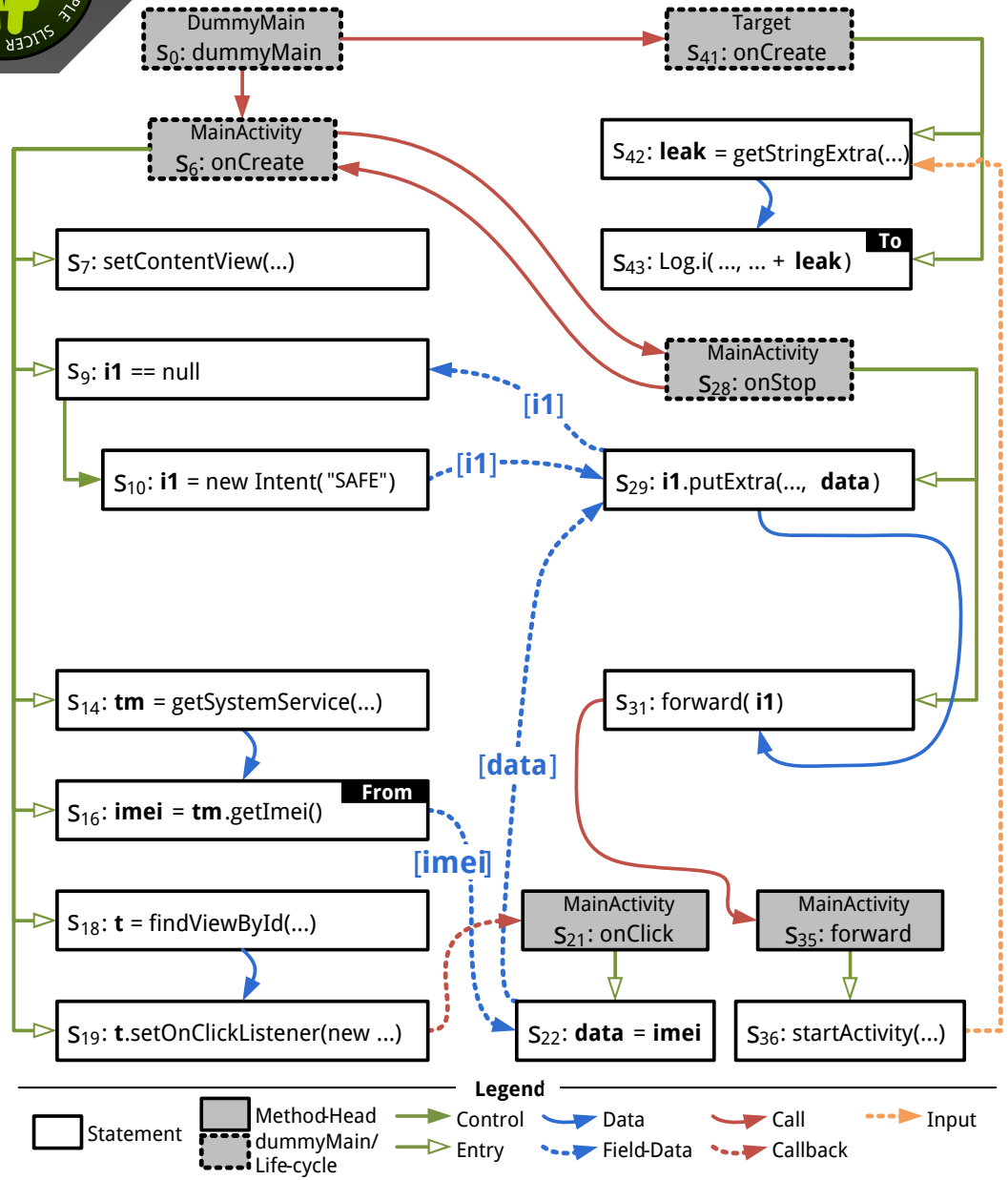


1. **Graph Generation**
   - Build **PDG**
   - Merge to **SDG**
   - Enhance to **ADG**

---

2. **Slicing**
   - Identify Criteria
   - Slice Forward
     - **FFF:** Forward Field Filtering
   - Slice Backward
     - **CSR:** Context-Sensitive Refinement

Example: Slicing

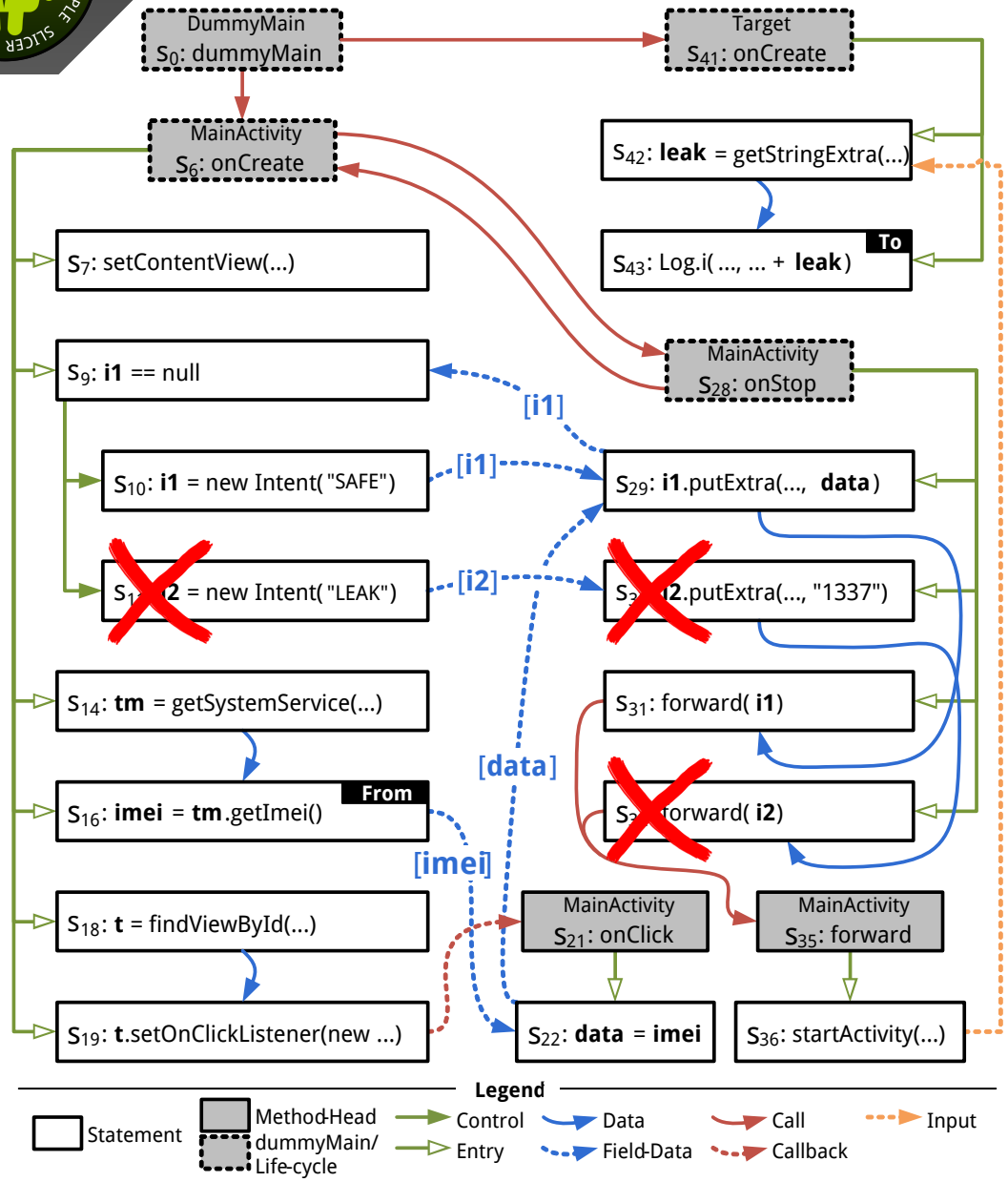


1. **Graph Generation**
   - Build **PDG**
   - Merge to **SDG**
   - Enhance to **ADG**

---

2. **Slicing**
   - Identify Criteria
   - Slice Forward
     - **FFF:** Forward Field Filtering
   - Slice Backward
     - **CSR:** Context-Sensitive Refinement

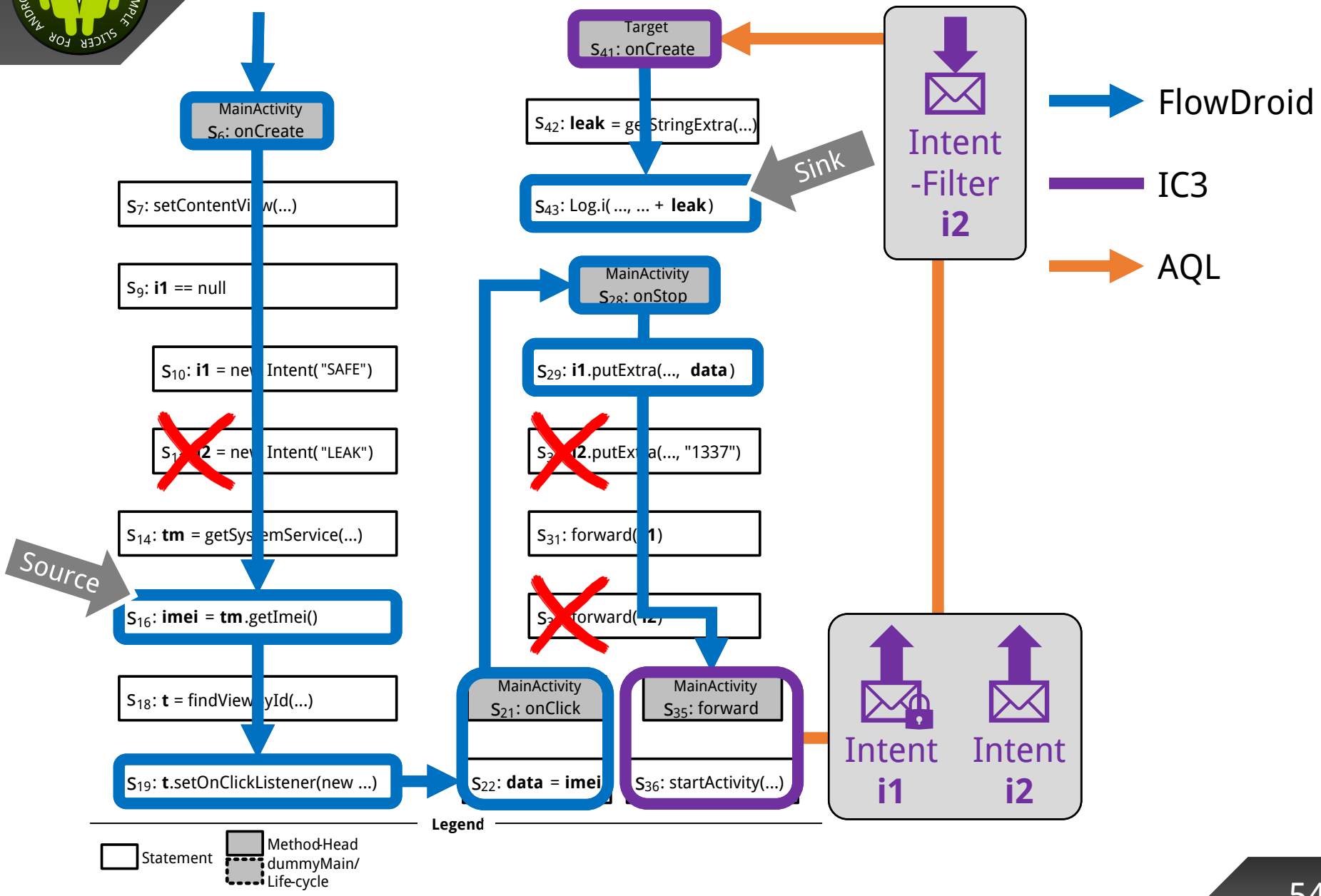
Example: Slicing



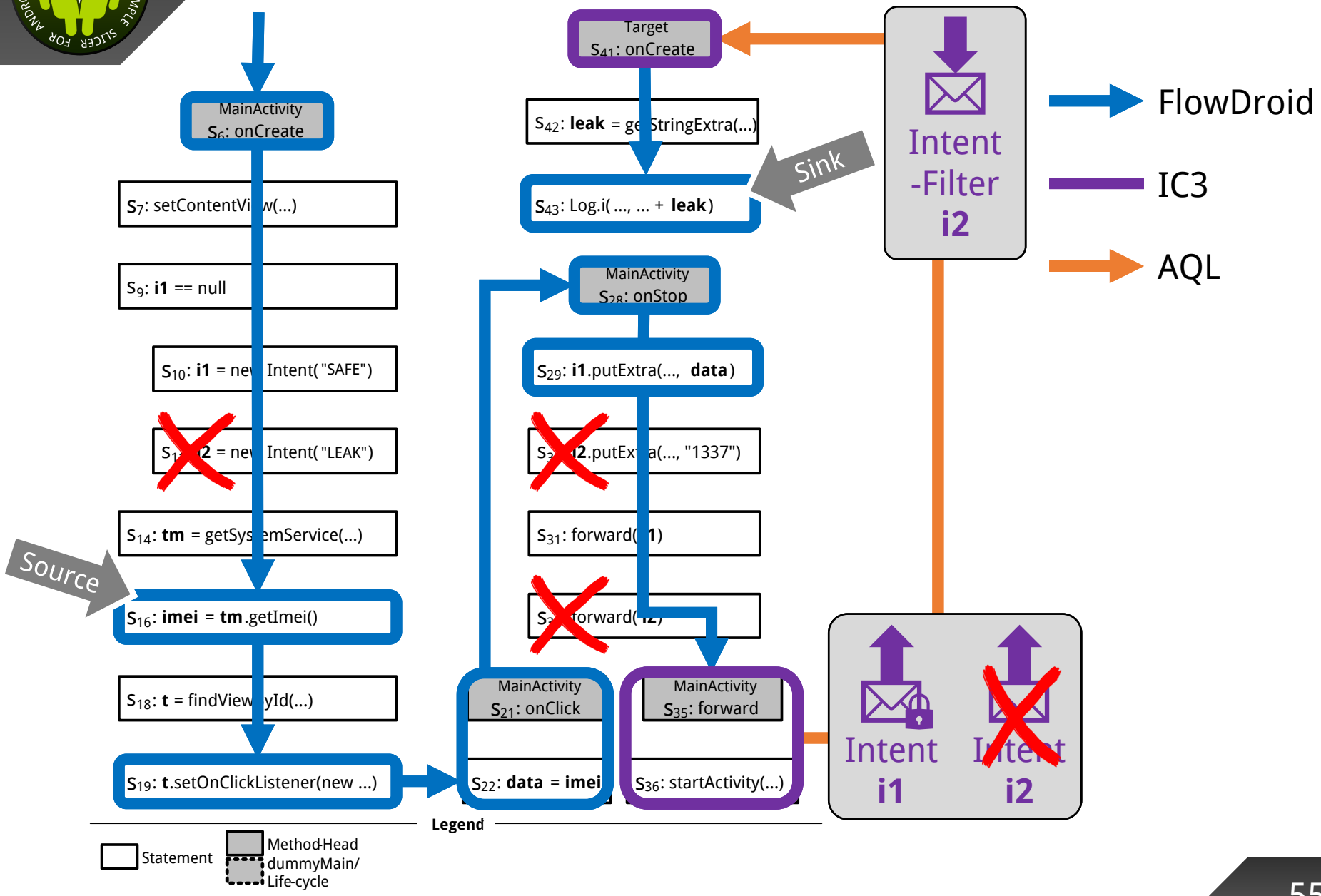
1. **Graph Generation**
   - Build **PDG**
   - Merge to **SDG**
   - Enhance to **ADG**

2. **Slicing**
   - Identify Criteria
   - Slice Forward
     - **FFF:** Forward Field Filtering
   - Slice Backward
     - **CSR:** Context-Sensitive Refinement

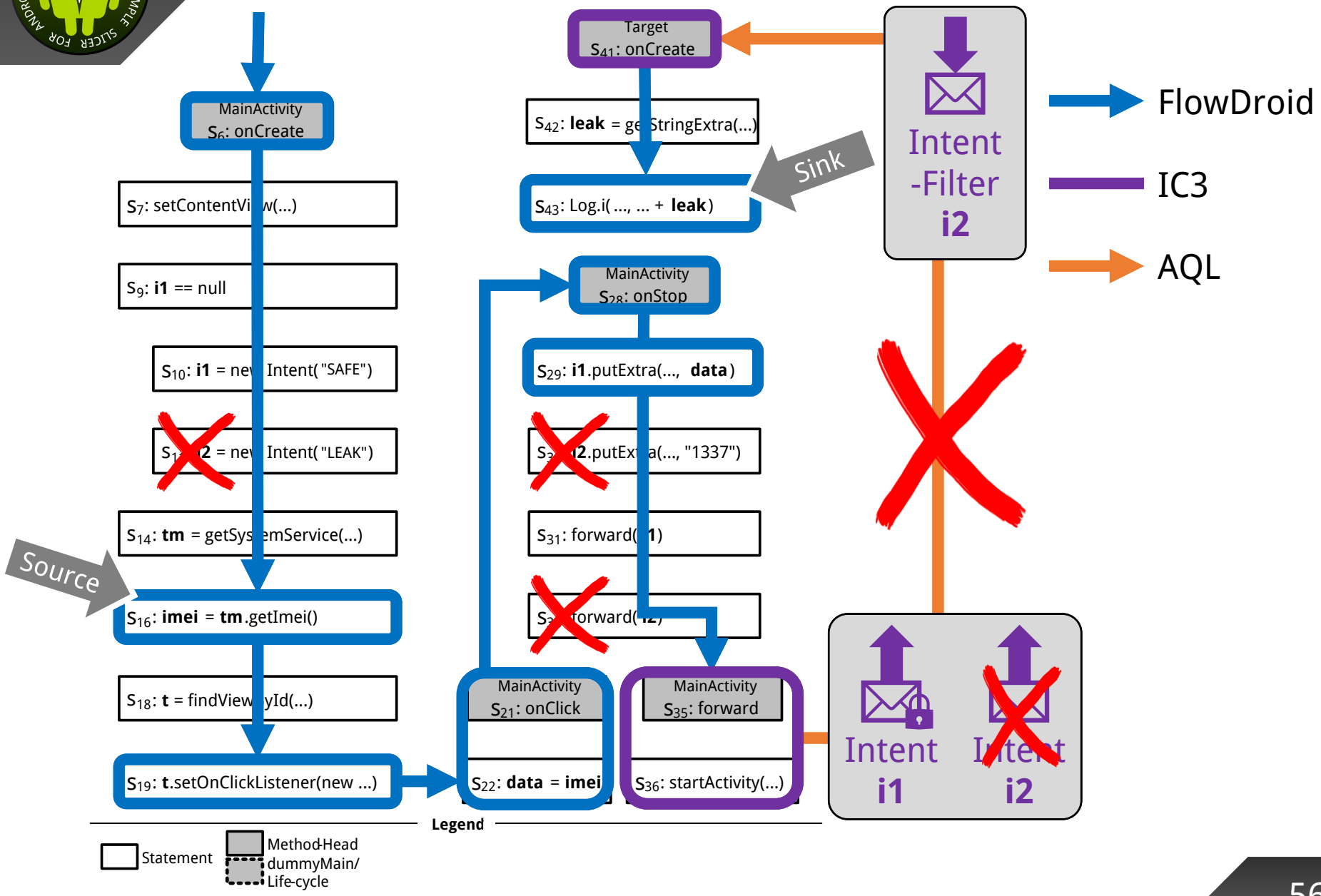
Example: Cooperative Taint Analysis + Slicing



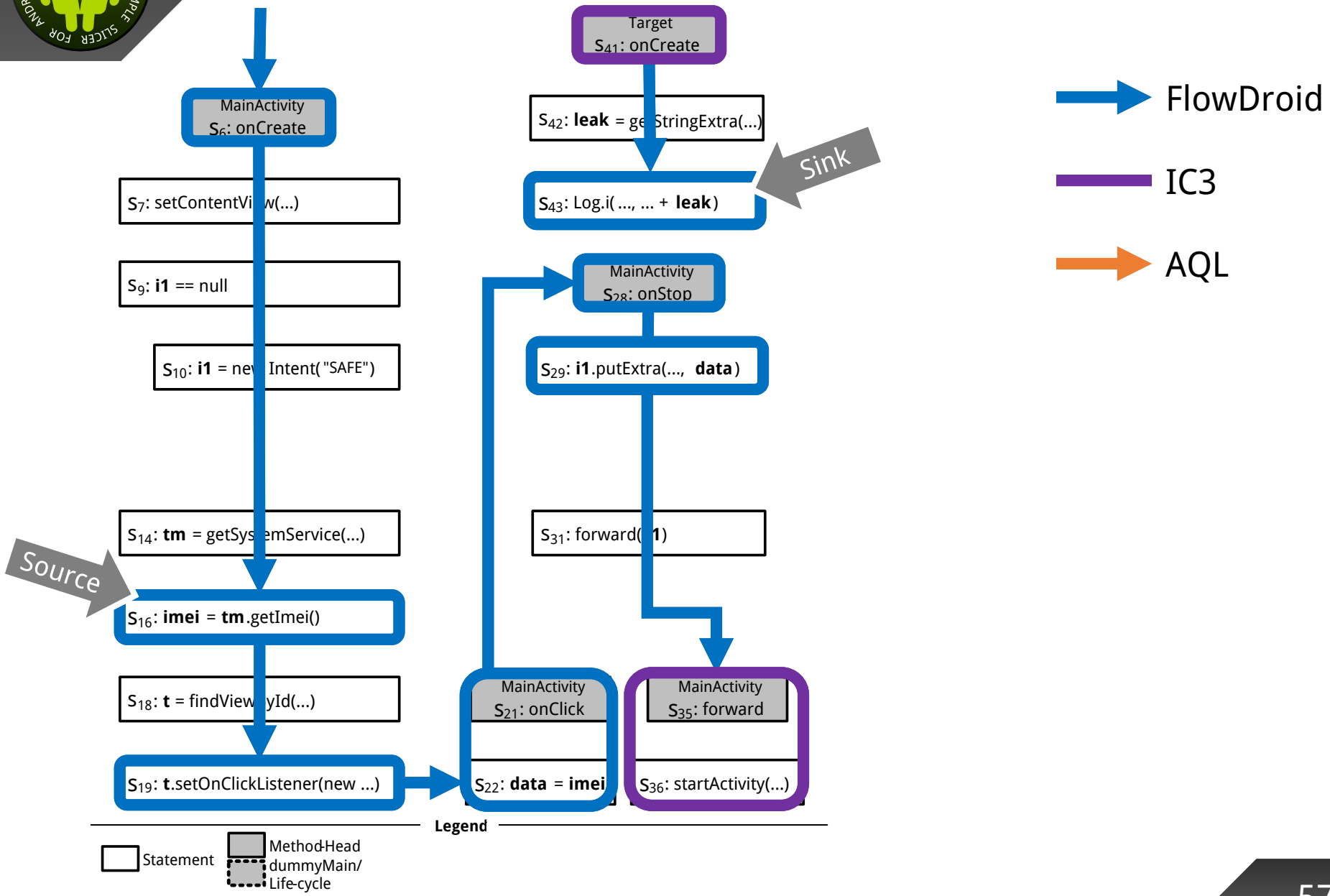
Example: Cooperative Taint Analysis + Slicing



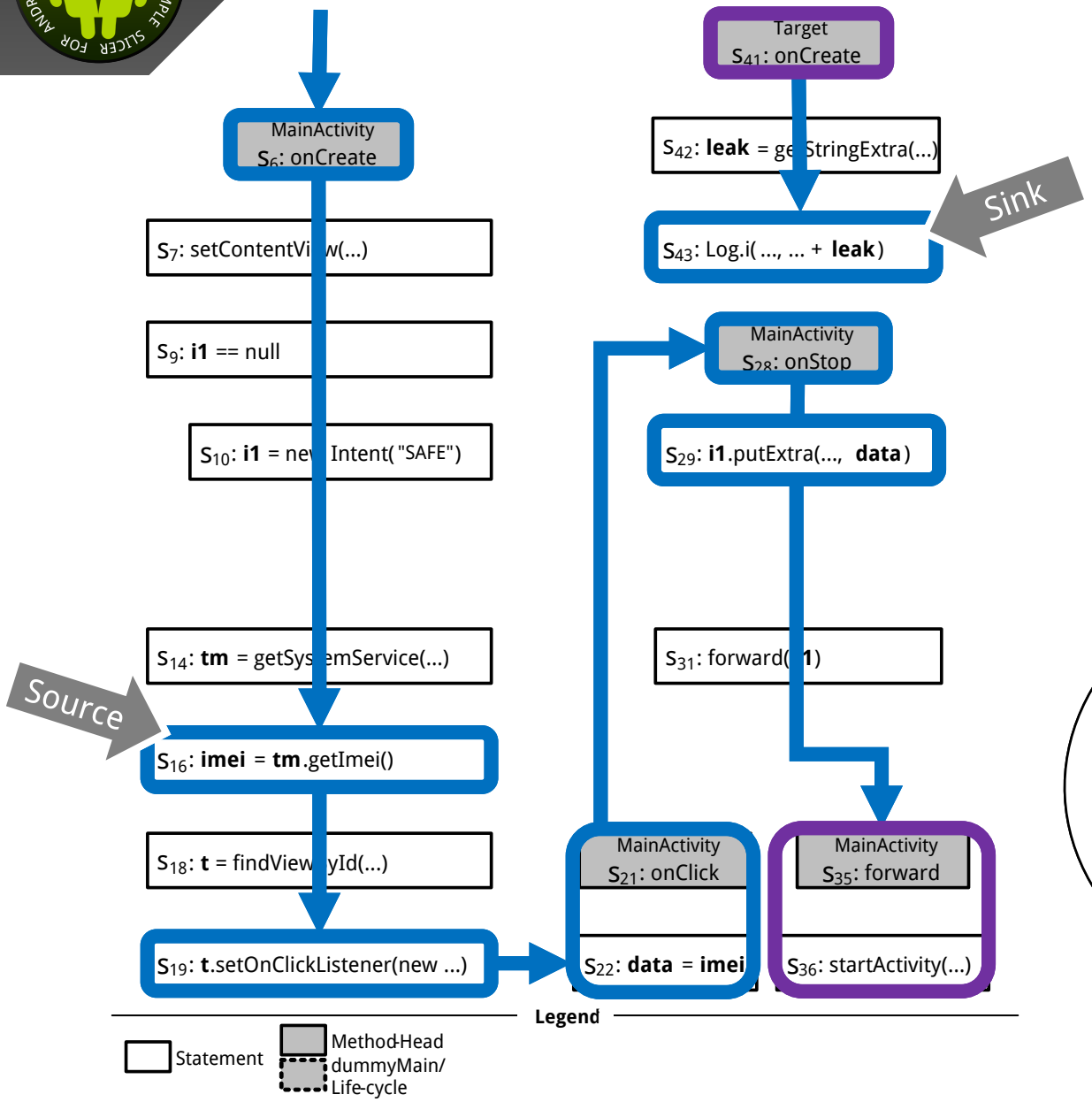
Example: Cooperative Taint Analysis + Slicing



Example: Cooperative Taint Analysis + Slicing



Example: Cooperative Taint Analysis + Slicing



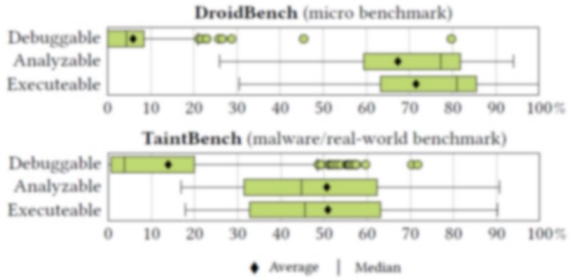
FlowDroid

IC3

AQL

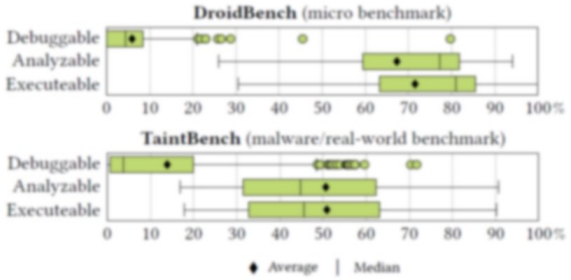
False Positive Eliminated

- **Slice Size**
  - Analyzable/Executeable **>** Debuggable
  - Debuggable slices are still small (< 4%)



- **Slice Size**
  - Analyzable/Executeable **>** Debuggable
  - Debuggable slices are still small (< 4%)

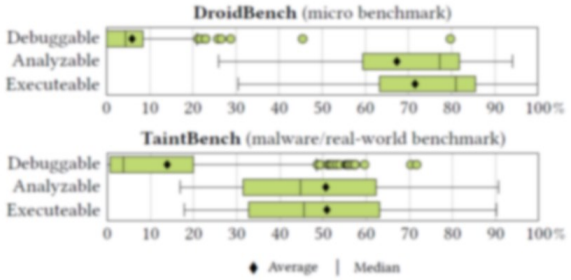
- **Comparison**
  - Dynamic slicers are more precise
  - No need for execution traces/test cases



Slicing Tool	Type	Requirements				USRs				
		1	2	3	4	1	2	3	4	5
AndroidSlicer [5]	dynamic	✔*	✔	✔	✔	✘	✘	✔	✘***	✘
Mandoline [1]	dynamic	✔	✔	✔	?	✔	✘	✔	✘***	✘
Jicer	static	✔**	✔	✔	✔	✔	✔	✔	✔	✔

✔: fulfilled, ✘: not fulfilled, ?: unknown, *: except 1.3, **: except 1.6,
***: 4.1 not fulfilled and 4.2 only fulfilled w.r.t. dynamic analysis tools

- **Slice Size**
  - Analyzable/Executeable **>** Debuggable
  - Debuggable slices are still small (< 4%)

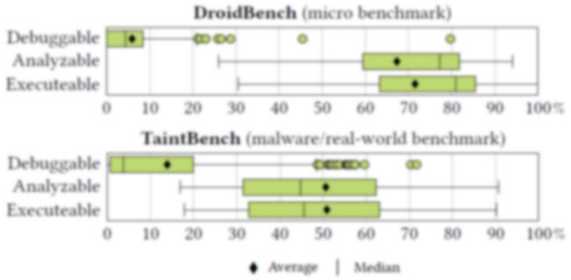


- **Comparison**
  - Dynamic slicers are more precise
  - No need for execution traces/test cases
  - Usable in **Cooperative Analysis!!!**

Slicing Tool	Type	Requirements 1	2	3	4	USRs 1	2	3	4	5
AndroidSlicer [5]	dynamic	✔*	✔	✔	✔	✘	✘	✔	✘***	✘
Mandoline [1]	dynamic	✔	✔	✔	?	✔	✘	✔	✘***	✘
Jicer	static	✔**	✔	✔	✔	✔	✔	✔	✔	✔

✔: fulfilled, ✘: not fulfilled, ?: unknown, *: except 1.3, **: except 1.6,
***: 4.1 not fulfilled and 4.2 only fulfilled w.r.t. dynamic analysis tools

- **Slice Size**
  - Analyzable/Executeable > Debuggable
  - Debuggable slices are still small (< 4%)



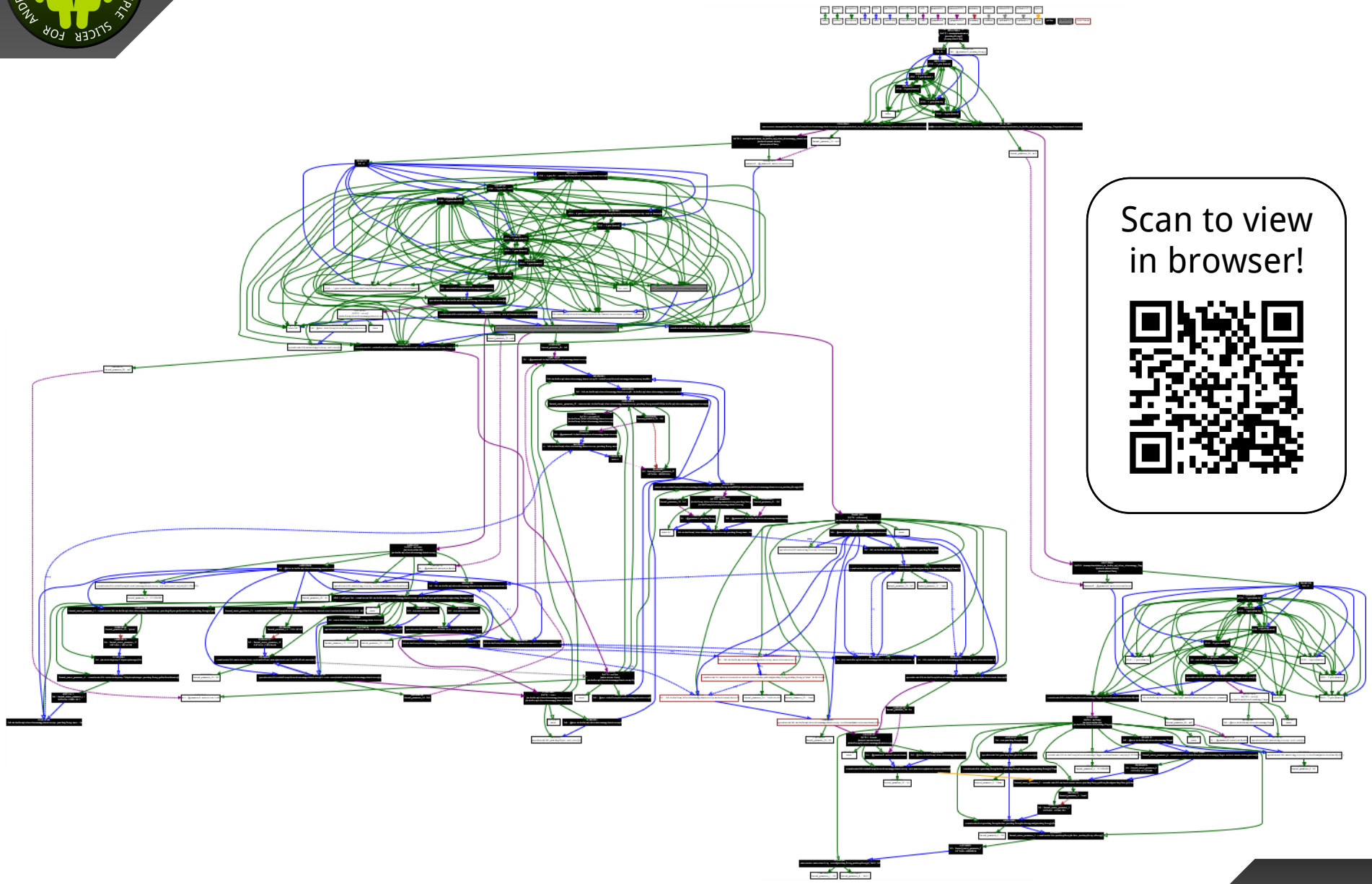
- **Comparison**
  - Dynamic slicers are more precise
  - No need for execution traces/test cases
  - Usable in **Cooperative Analysis!!!**

Slicing Tool	Type	Requirements 1	2	3	4	USRs 1	2	3	4	5
AndroidSlicer [5]	dynamic	✔*	✔	✔	✔	✘	✘	✔	✘***	✘
Mandoline [1]	dynamic	✔	✔	✔	?	✔	✘	✔	✘***	✘
Jicer	static	✔**	✔	✔	✔	✔	✔	✔	✔	✔

✔: fulfilled, ✘: not fulfilled, ?: unknown, *: except 1.3, **: except 1.6, ***: 4.1 not fulfilled and 4.2 only fulfilled w.r.t. dynamic analysis tools

- **Analysis Performance**
  - Analysis time reduced
  - False positives eliminated (> 80%)

Example: Real ADG



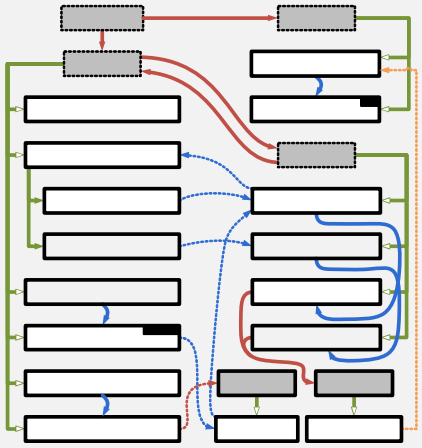
Scan to view in browser!

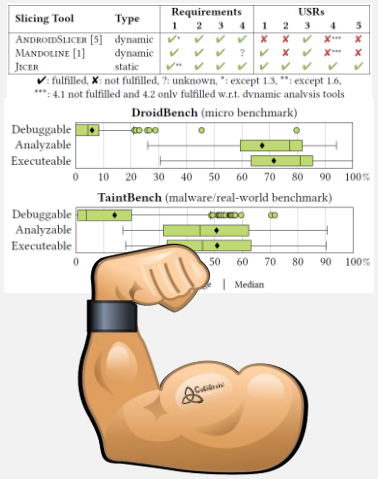
Summary

Jicer is available: https://FoelliX.github.io/Jicer

Jicer is awesome:

- APK/class input
- APK/Jimple output
- ADG Generation
  - flow-, context-, field-, object- and thread-sensitive
  - Callback- & Lifecycle-aware
- Scalable w.r.t. libraries (through StubDroid summaries)
- ICC & IAC support via cooperative analysis (input edges)
- *Debugable*, *Analyzable* or *Executable* output
- Valid code slicing through extra-slicing
- Forward Field Filtering
- Context-Sensitive Refinement
- Prefer Local Data
- Call Graph Enhancing
- GUI … and much more





Related Projects

Android App Analysis Query Language

CoDiDroid

More information on:

- https://FelixPauck.de
- https://FoelliX.github.io