TASMAN

Using Targeted Symbolic Execution for Reducing False-Positives in Dataflow Analysis

Steven Arzt, Siegfried Rasthofer, Robert Hahn, Eric Bodden

TECHNISCHE UNIVERSITÄT DARMSTADT

Overview

TECHNISCHE UNIVERSITÄT DARMSTADT

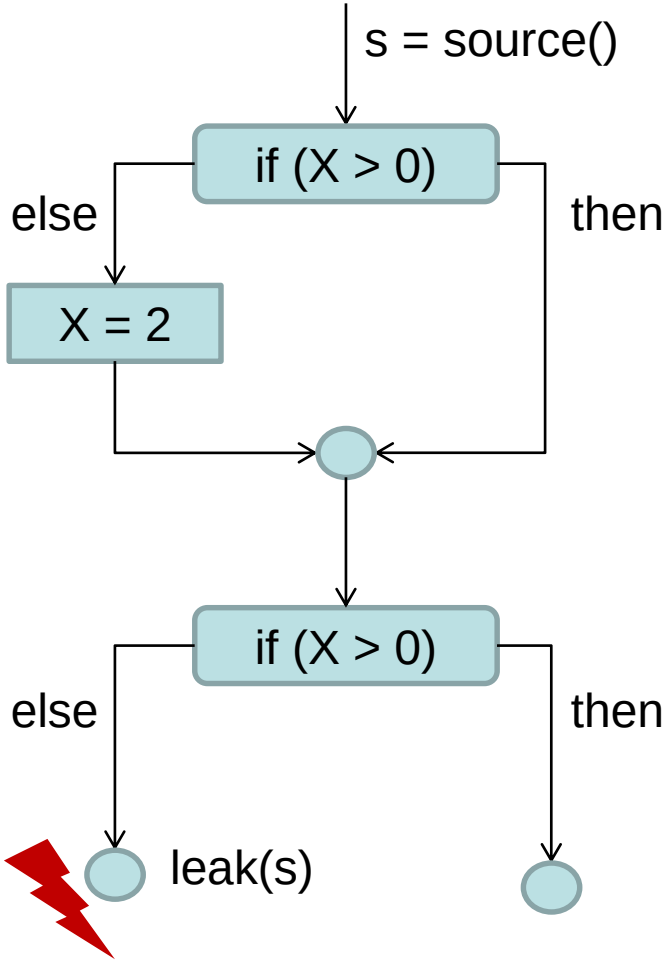
- Motivation: Imprecision in Static Taint Tracking
- Basic Constraint Generation
- Loops, Recursions, Exceptions
- Experiments
  - Micro Benchmarks
  - Real-World Applications
  - Performance

EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN

Taint Tracking vs. Symbolic Execution

TECHNISCHE UNIVERSITÄT DARMSTADT

- Taint Tracking: Meet Over All Paths
  - Conditions independent of each other
  - Stateless tracking
  - Lightweight contexts for control flow feasibility
- Good Performance
  - Summaries, re-use of partial results
  - Small state space

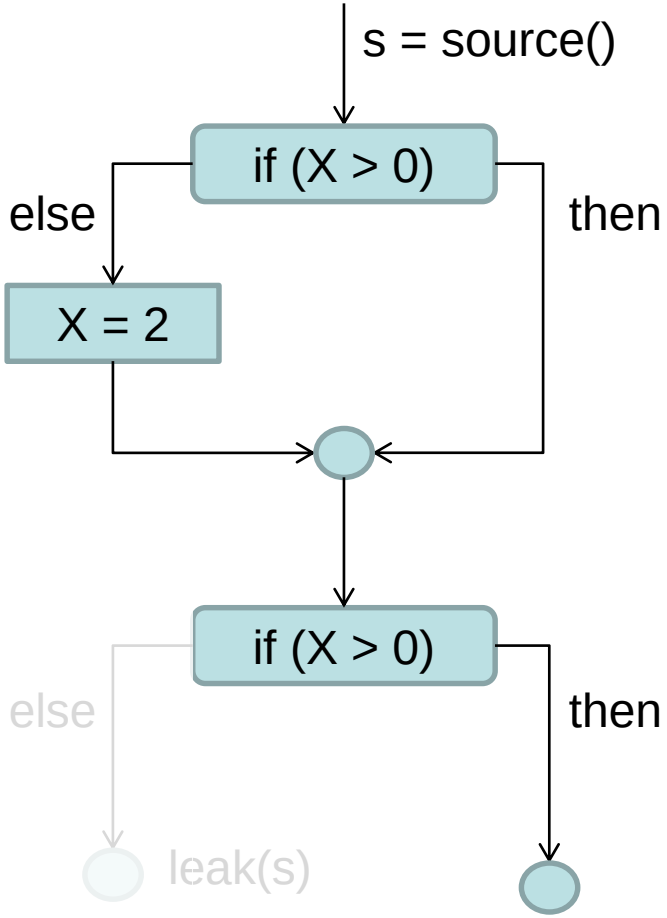


EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN

Taint Tracking vs. Symbolic Execution

TECHNISCHE UNIVERSITÄT DARMSTADT

- Symbolic Execution: Path Constraints
  - Track condition along paths
  - Stateful tracking
- Performance Challenging
  - Re-use only over equal full paths
  - Potential state space explosion



EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN

Finding False Positives in FlowDroid Results

ARCHITECTURE

Taint Tracking: False Positives

TECHNISCHE UNIVERSITÄT DARMSTADT

- Callback is always null
- bool1 is always false
- Leak can never happen
- FlowDroid reports a leak
- Symbolic execution on complete app does not scale

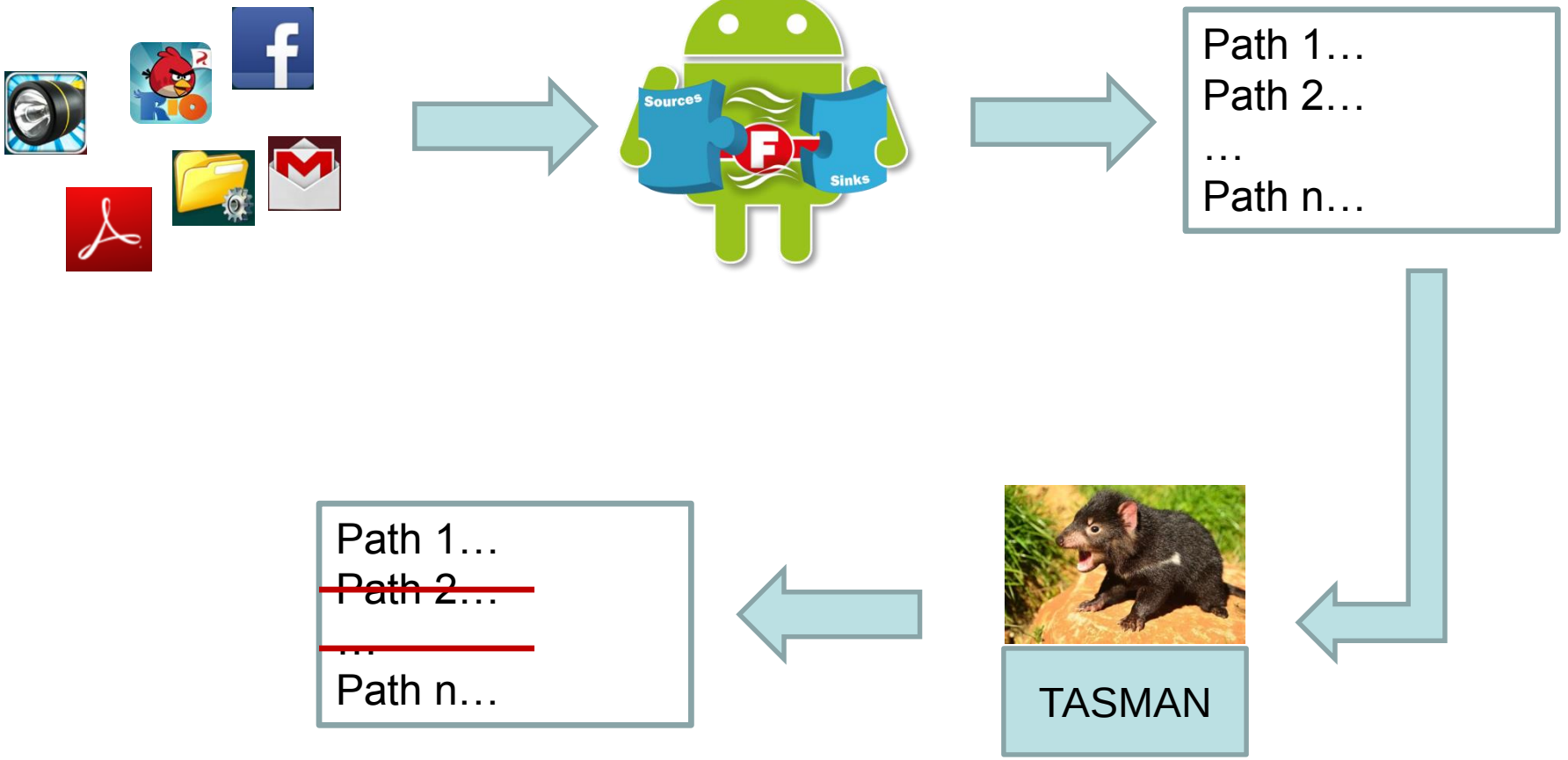
```
void onCreate () {
    show ( null );
}

void show ( AdDisplayListener listener )
{
    this.callback = listener;

    boolean bool1;
    if ( this.callback != null )
        bool1 = this.ad.show ();
    else
        bool1 = false;

    String secret = getSecret ();
    if ( bool1 )
        leak ( secret );
}
```

TASMAN: Targeted Symbolic Execution



Basic Constraint Generation

```
1: void onCreate () {
2:   show ( null );
3: }

5: void show(AdDisplayListener listener) {
6:    this.callback = listener;

7:  boolean bool1;
8:  if ( this.callback != null )
9:      bool1 = this.ad.show ();
10: else
11:     bool1 = false;

13: String secret = getSecret ();
14: if ( bool1 )
15:    leak ( secret );
16: }
```

Basic Constraint Generation

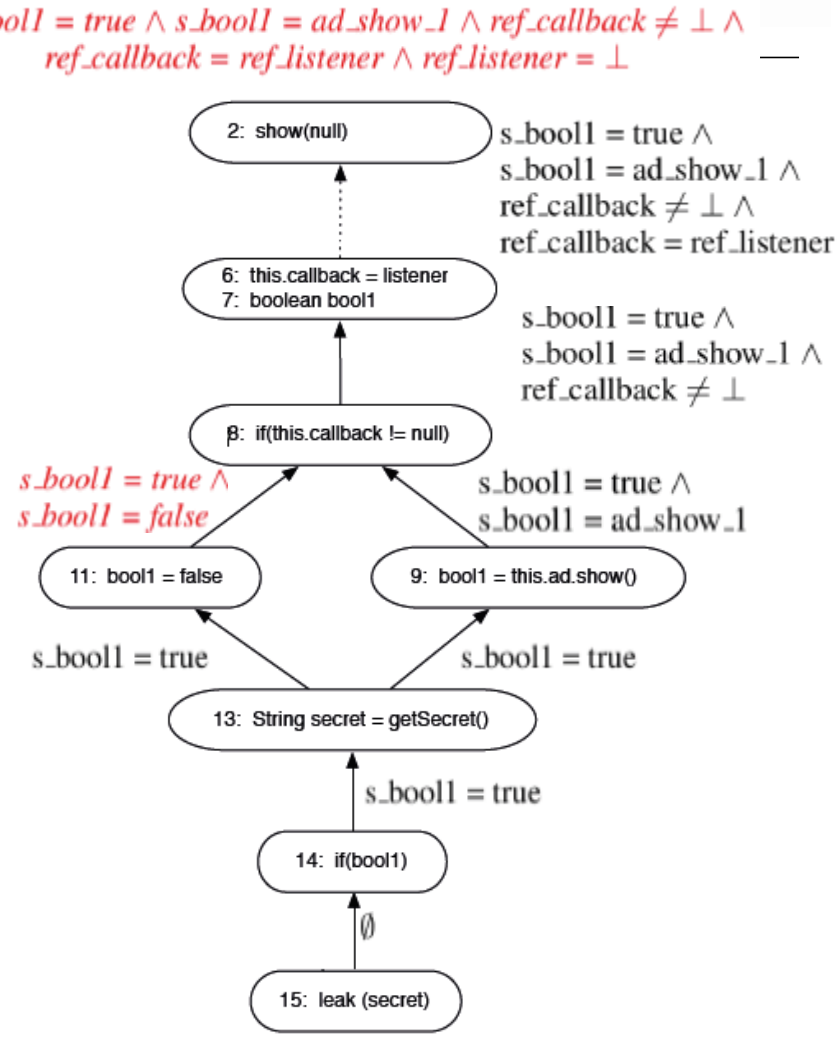
```
1: void onCreate () {
2:    show ( null );
3: }

5: void show(AdDisplayListener listener) {
6:    this.callback = listener;

7:    boolean bool1;
8:    if ( this.callback != null )
9:        bool1 = this.ad.show ();
10:   else
11:       bool1 = false;

13:   String secret = ge          ();
14:   if ( bool1 )
15:       leak ( secret );
16: }
```

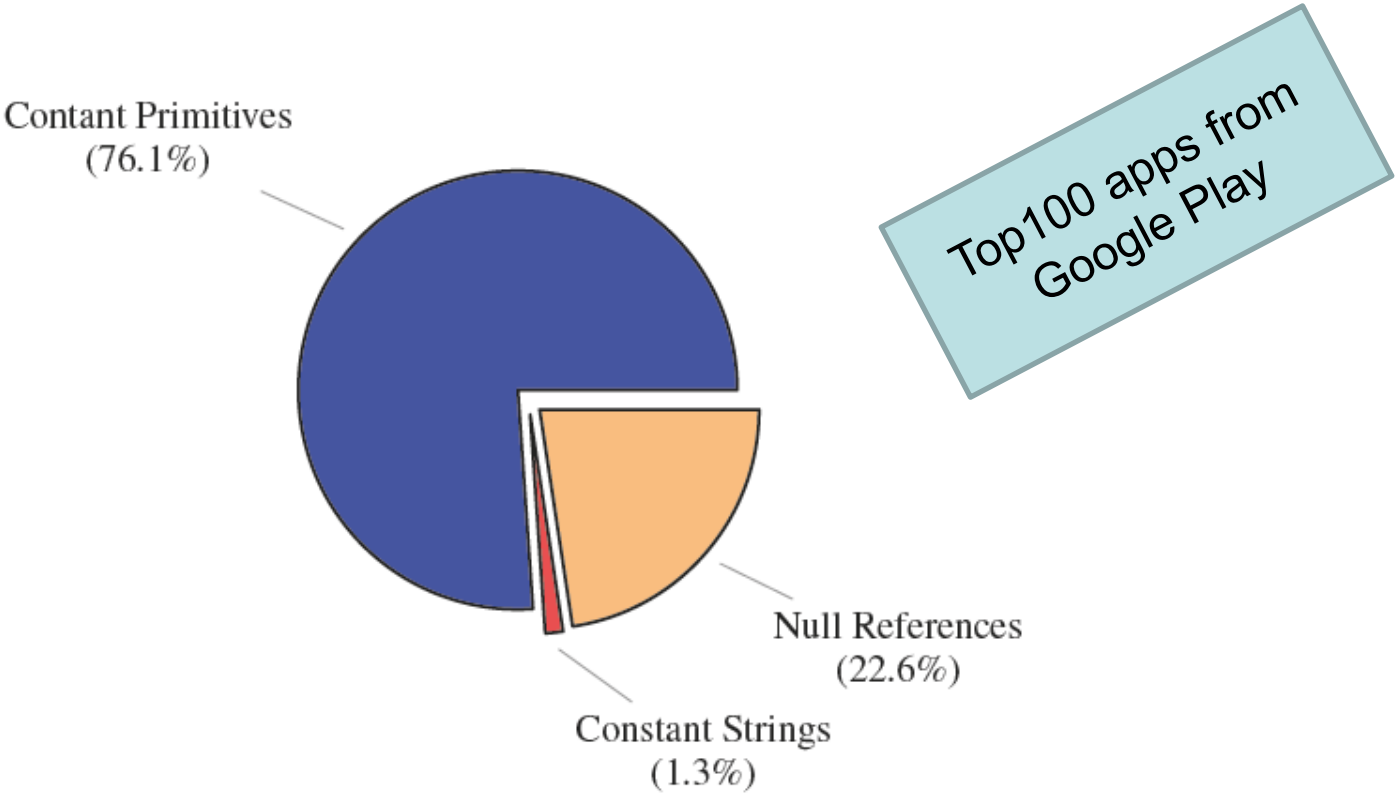
Propagation Path Disproved



Special Data Types

TECHNISCHE UNIVERSITÄT DARMSTADT

Which Data Types are Used in Conditions on the Path?



EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN

Loops, Recursion, Exceptions

TECHNISCHE UNIVERSITÄT DARMSTADT

- Method Call Inlining Up To Predefined Depth
  - Also deals with recursion
- Loop Unrolling Up To Predefined Depth
- Exceptional Control Flow In Taint Path
  - Just one more possible control flow
  - Implicit conditions for non-null exception objects, etc.

Performance, Precision, Recall

EVALUATION

Evaluation – Micro Benchmarks

TECHNISCHE UNIVERSITÄT DARMSTADT

Test-case group	False Positives	True Positives
Arrays	2/3	3/3
Casts	3/3	3/3
Collections	1/1	1/1
Exceptions	2/2	-
Fields and Objects	15/16	16/16
General Java	2/2	2/2
Interprocedural Data Flow	2/3	3/3
Library Handling	1/2	2/2
Loops and Recursion	4/4	4/4
Operators	2/3	3/3
Strings	1/4	
Sum	35/43 (81%)	

TASMAN is 100% safe

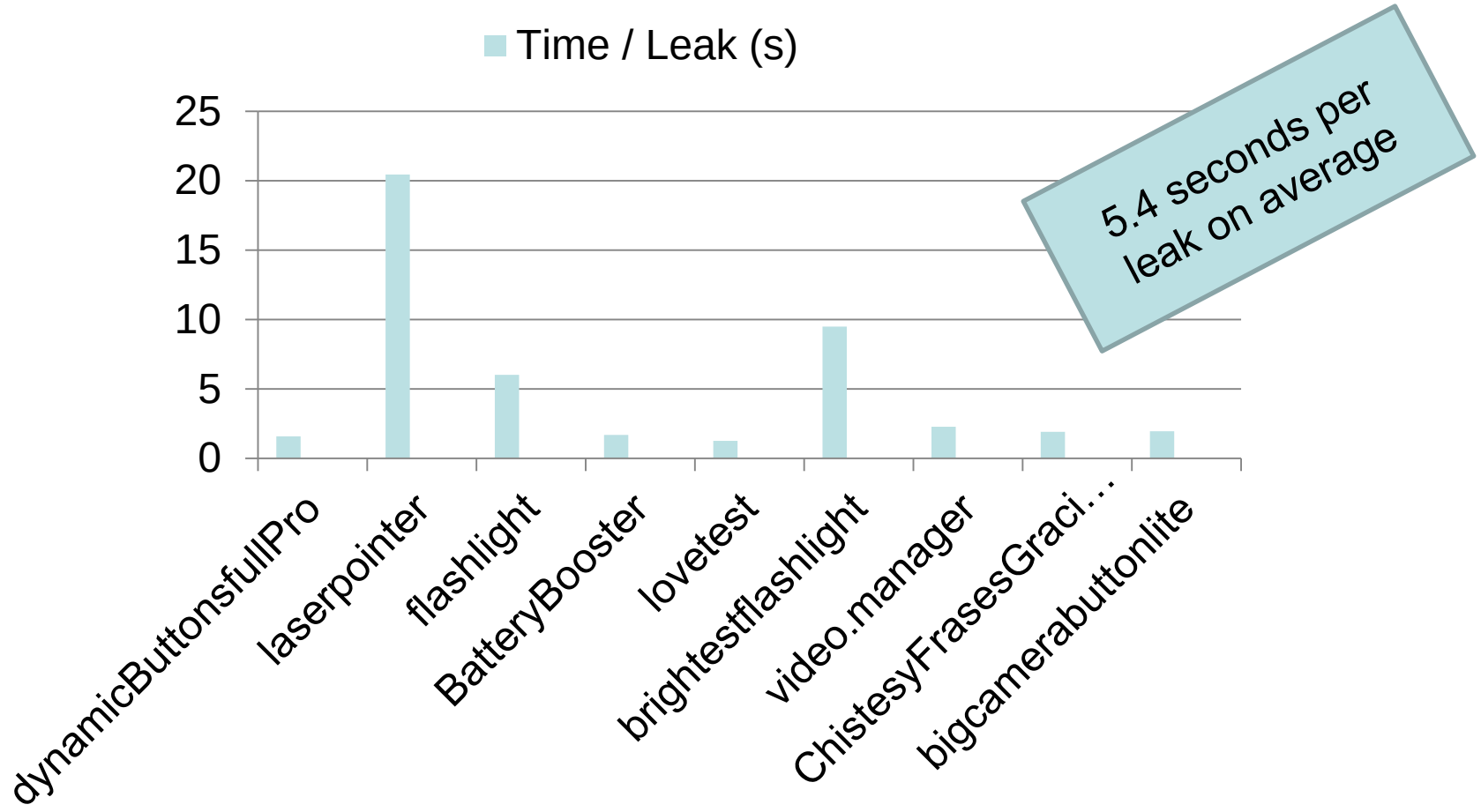
EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN

Evaluation – Real-World Applications

TECHNISCHE UNIVERSITÄT DARMSTADT

Test-case group	Leaks	FPs
com.buttons.dynamicButtonsfullPro	51	1
laser.pointer.laserpointer	120	7
com.devuni.flashlight	63	1
com.CrazyRobot.BatteryBooster	106	1
com.mobilplug.lovetest	57	1
goldenshorestechnologies.brightestflashlight.free	33	1
com.mattia.videos.manager	102	1
com.surpax.ledflashlight.panel	135	1
com.reviloapps.ChistesyFrasesGraciosas	21	1
love.bigcamerabuttonlite	50	2
Sum (Leaks)	739	17

Evaluation - Performance



Limitations

TECHNISCHE UNIVERSITÄT DARMSTADT

- Only One Path Per Leak
  - FlowDroid generates witness
  - Disproving a witness does not disprove leak
  - Theoretically: Disprove *all* possible paths

- No Environment Model
  - Files on the SD card
  - Servers on the network

TECHNISCHE UNIVERSITÄT DARMSTADT

S. Arzt, S. Rasthofer, R. Hahn, and Eric Bodden
Secure Software Engineering Group (EC-SPRIDE)
Email: steven.arzt@ec-spride.de
siegfried.rasthofer@ec-spride.de
eric.bodden@ec-spride.de
Blog: http://sse-blog.ec-spride.de
Website: http://sse.ec-spride.de

EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN