

# Android App Analysis





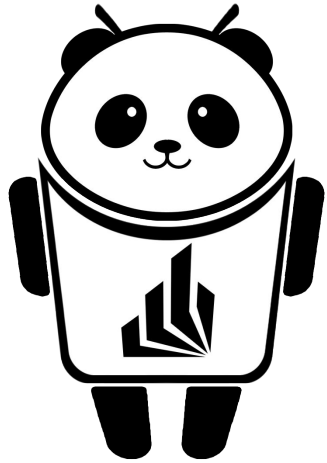
- **Short Recap**
- **Live Demo**
- **Evaluation**
  - Intra- & Inter-App Permission Usage Analysis
  - Intra-App Information Flow Analysis
- **Future work**
- **Conclusion**





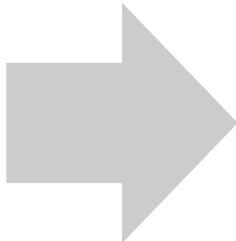
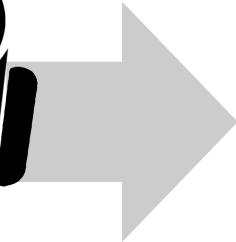
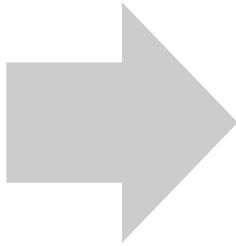
## **PAndA<sup>2</sup> - Paderborn Android App Analysis**

- Is Android App A trustworthy?
- Is it cooperating with another App B?



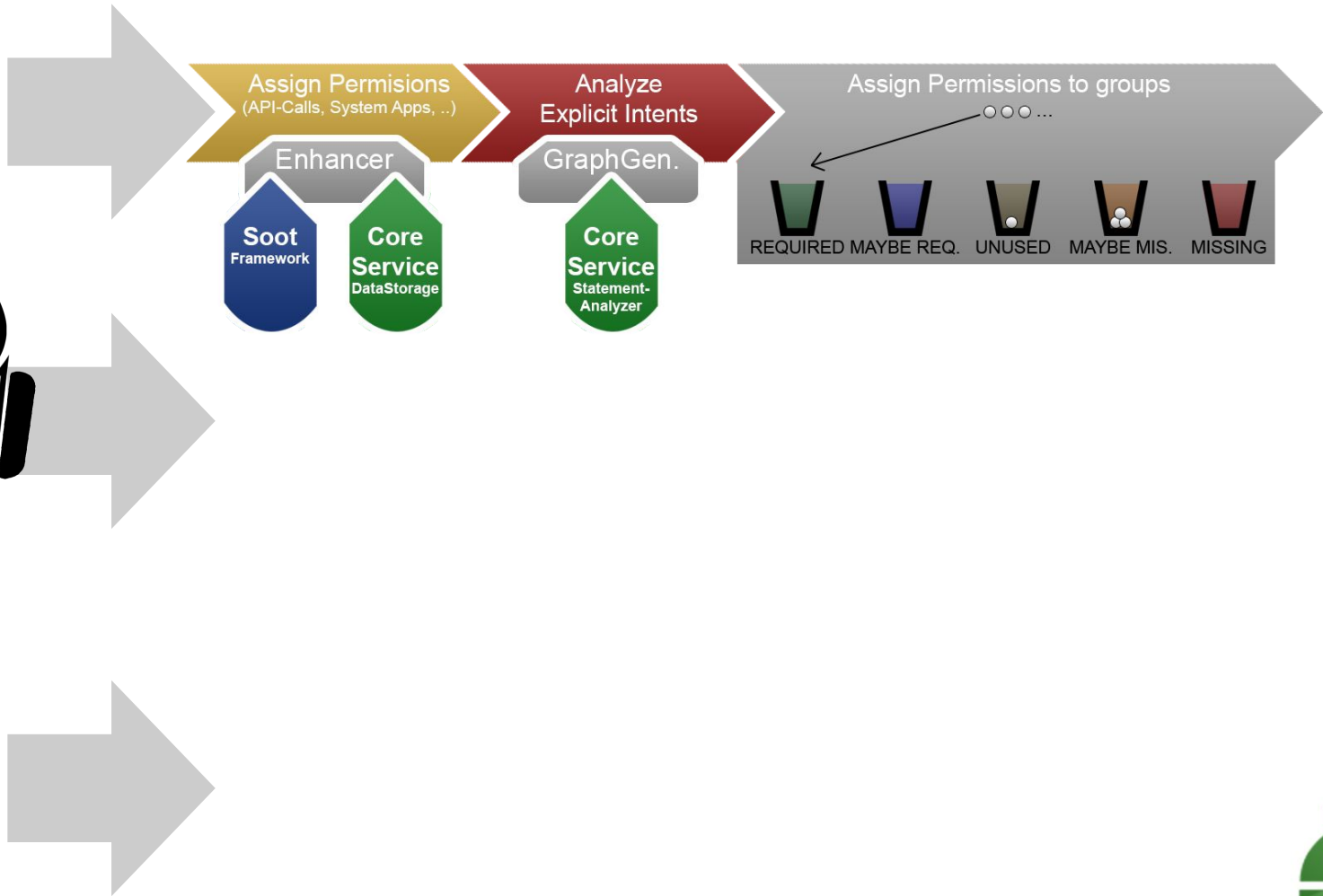


### 3 different analyses



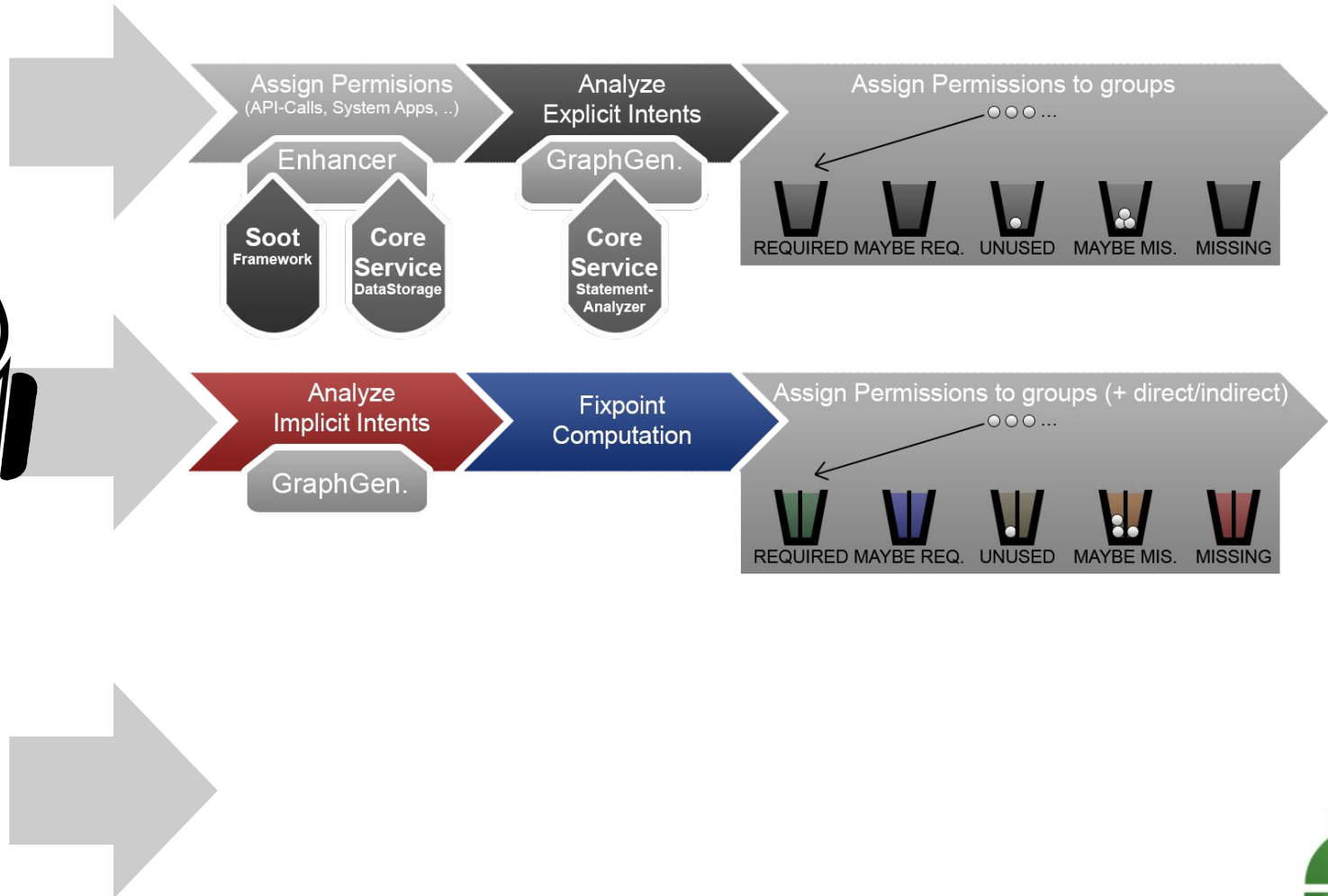
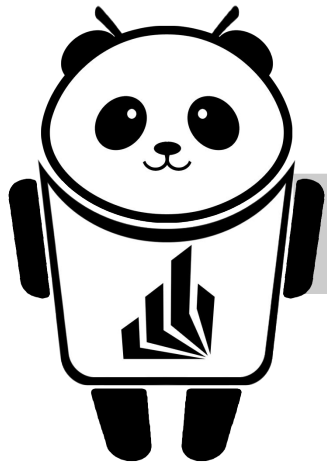


## 1. Intra-App Permission Usage Analysis



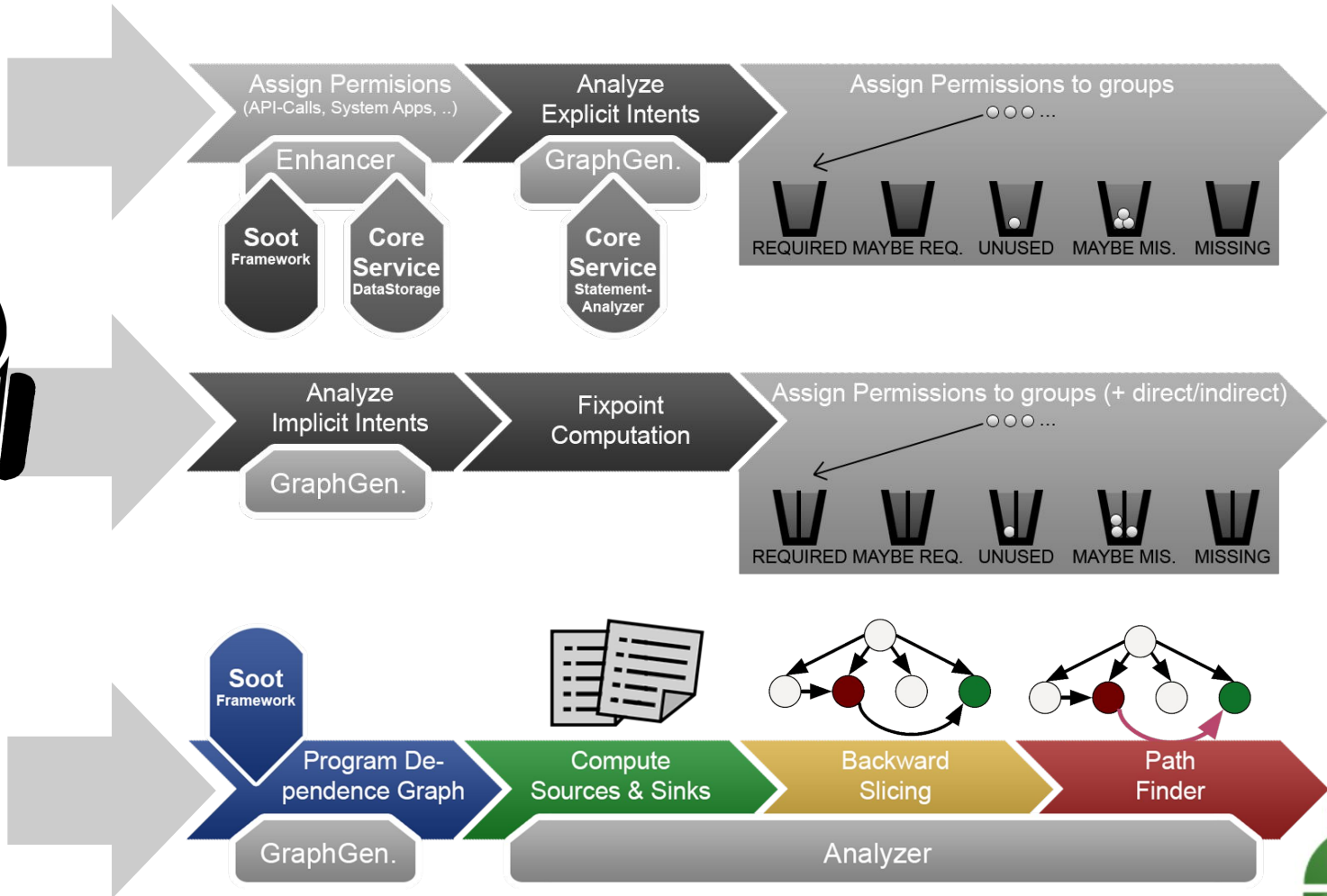
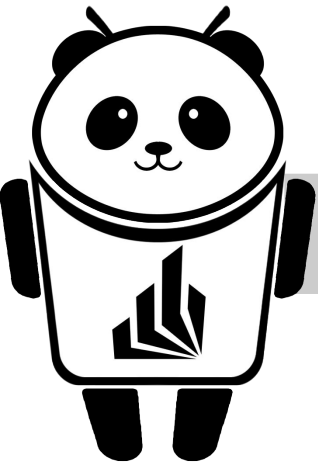


## 2. Inter-App Permission Usage Analysis





### 3. Intra-App Information Flow Analysis





# Live Demo







- What about a **METHOD** detail level?

RES TO RES - COMPONENT - **METHOD** - STATEMENT



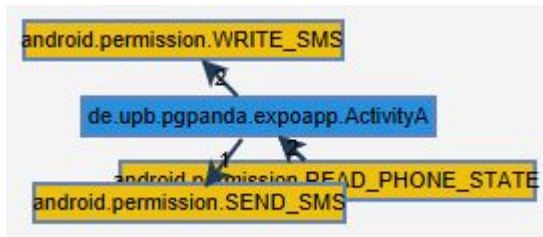
better  
overview

more  
detailed

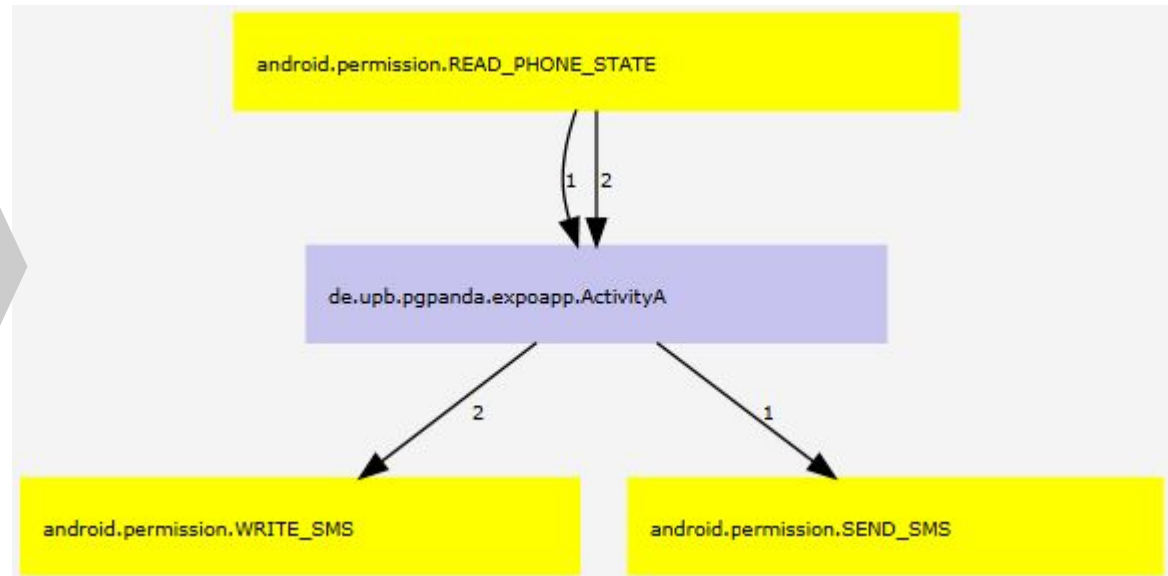




- Will the graphical result be improved?



JGraphX



GraphViz



## 1. **Custom Apps**

Developed by ourselves.





## 1. Custom Apps

Developed by ourselves.

## 2. DroidBench

.. “Android applications to be used as a testing ground for static and dynamic security tools.” \*

\* <https://blogs.uni-paderborn.de/sse/tools/droidbench/>





### 1. Custom Apps

Developed by ourselves.

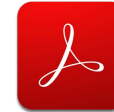
### 2. DroidBench

.. “Android applications to be used as a testing ground for static and dynamic security tools.” \*

### 3. Real World Apps



ADAC  
Pannenhilfe



Adobe Acrobat  
Reader



Barcode  
Scanner



ES File Explorer



Google Photos



Instagram



Tiny Flashlight



WhatsApp  
Messenger

\* <https://blogs.uni-paderborn.de/sse/tools/droidbench/>





### 1. Custom Apps

Developed by ourselves.

### 2. DroidBench

.. “Android applications to be used as a testing ground for static and dynamic security tools.” \*

### 3. Real World Apps



- **Tools for comparison:**

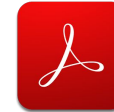
FlowDroid, Amandroid

\* <https://blogs.uni-paderborn.de/sse/tools/droidbench/>



ADAC

Pannenhilfe



Adobe Acrobat  
Reader



Barcode  
Scanner



ES File Explorer



Google Photos



Instagram



Tiny Flashlight



WhatsApp  
Messenger





**REQUIRED** (direct)  
**REQUIRED** (indirect)  
**REQUIRED** (direct & indirect)  

---

**MAYBE\_REQUIRED**  

---

**UNUSED**  

---

**MISSING** (direct)  
**MISSING** (indirect)  
**MISSING** (direct & indirect)  

---

**MAYBE\_MISSING**





4 Apps → 9 Setups → 9 Expected results → 9 Matches

REQUIRED (direct)  
REQUIRED (indirect)  
REQUIRED (direct & indirect)  

---

MAYBE\_REQUIRED  

---

UNUSED  

---

MISSING (direct)  
MISSING (indirect)  
MISSING (direct & indirect)  

---

MAYBE\_MISSING







4 Apps → 9 Setups → 9 Expected results → 9 Matches

REQUIRED (direct)  
REQUIRED (indirect)  
REQUIRED (direct & indirect)  

---

MAYBE\_REQUIRED  

---

UNUSED  

---

MISSING (direct)  
MISSING (indirect)  
MISSING (direct & indirect)  

---

MAYBE\_MISSING



Permission Usage Analyses are working as expected





App	REQUI- RED	MAYBE_ REQUIRED	UN- USED	MAYBE_ MISSING	MIS- SING	MISSING edited	R1	R2	R3
ADAC Pannenhilfe	3	5	0	165	2				
Adobe Acrobat Reader	2	2	0	170	1				
Barcode Scanner	6	3	0	162	4				
ES File Explorer	10	9	0	151	5				
Google Photos	15	5	0	143	12				
Instagram	9	3	0	155	8				
Tiny Flashlight	4	3	0	162	6				
WhatsApp Messenger	25	7	0	140	3				





App	REQUI- RED	MAYBE_ REQUIRED	UN- USED	MAYBE_ MISSING	MIS- SING	MISSING edited	R1	R2	R3
ADAC Pannenhilfe	3	5	0	165	2				
Adobe Acrobat Reader	2	2	0	170	1				
Barcode Scanner	6	3	0	162	4				
ES File Explorer	10	9	0	151	5				
Google Photos	15	5	0	143	12				
Instagram	9	3	0	155	8				
Tiny Flashlight	4	3	0	162	6				
WhatsApp Messenger	25	7	0	140	3				

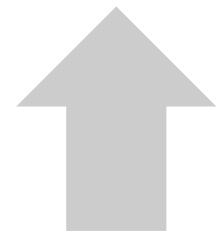




App	REQUI- RED	MAYBE_ REQUIRED	UN- USED	MAYBE_ MISSING	MIS- SING	MISSING edited	R1	R2	R3
ADAC Pannenhilfe	3	5	0	165	2		0,05		
Adobe Acrobat Reader	2	2	0	170	1		0,02		
Barcode Scanner	6	3	0	162	4		0,05		
ES File Explorer	10	9	0	151	5		0,11		
Google Photos	15	5	0	143	12		0,11		
Instagram	9	3	0	155	8		0,07		
Tiny Flashlight	4	3	0	162	6		0,04		
WhatsApp Messenger	25	7	0	140	3		0,18		



$$ALL = \text{REQUIRED} + \dots + \text{MISSING}$$



$$R1 = 1 - \frac{\text{MISSING} + \text{MAYBE\_MISSING}}{ALL}$$



App	REQUI- RED	MAYBE_ REQUIRED	UN- USED	MAYBE_ MISSING	MIS- SING	MISSING edited	R1	R2	R3
ADAC Pannenhilfe	3		0		2		0,05	0,60	
Adobe Acrobat Reader	2		0		1		0,02	0,67	
Barcode Scanner	6		0		4		0,05	0,60	
ES File Explorer	10		0		5		0,11	0,67	
Google Photos	15		0		12		0,11	0,56	
Instagram	9		0		8		0,07	0,53	
Tiny Flashlight	4		0		6		0,04	0,40	
WhatsApp Messenger	25		0		3		0,18	0,89	



$$ALL = \text{REQUIRED} + \dots + \text{MISSING}$$



$$R2 = 1 - \frac{\text{MISSING}}{\text{ALL}}$$





App	REQUI- RED	MAYBE_ REQUIRED	UN- USED	MAYBE_ MISSING	MIS- SING	MISSING edited	R1	R2	R3
ADAC Pannenhilfe	3		0		2	0	0,05	0,60	
Adobe Acrobat Reader	2		0		1	0	0,02	0,67	
Barcode Scanner	6		0		4	2	0,05	0,60	
ES File Explorer	10		0		5	3	0,11	0,67	
Google Photos	15		0		12	6	0,11	0,56	
Instagram	9		0		8	3	0,07	0,53	
Tiny Flashlight	4		0		6	5	0,04	0,40	
WhatsApp Messenger	25		0		3	1	0,18	0,89	

**MISSING** edited = **MISSING**  $\cap$  dangerous



- **Protectionlevel: dangerous**  
Permission has to be defined in the manifest
- **Protectionlevel: normal**  
Does not have to be assigned in the manifest.  
(Nice to know information)





App	REQUI- RED	MAYBE_ REQUIRED	UN- USED	MAYBE_ MISSING	MIS- SING	MISSING edited	R1	R2	R3
ADAC Pannenhilfe	3		0			0	0,05	0,60	1,00
Adobe Acrobat Reader	2		0			0	0,02	0,67	1,00
Barcode Scanner	6		0			2	0,05	0,60	0,75
ES File Explorer	10		0			3	0,11	0,67	0,77
Google Photos	15		0			6	0,11	0,56	0,71
Instagram	9		0			3	0,07	0,53	0,75
Tiny Flashlight	4		0			5	0,04	0,40	0,44
WhatsApp Messenger	25		0			1	0,18	0,89	0,96



ALL = REQUIRED + ... + MISSING edited



$$R3 = 1 - \frac{\text{MISSING edited}}{\text{ALL}}$$





App	REQUI- RED	MAYBE_ REQUIRED	UN- USED	MAYBE_ MISSING	MIS- SING	MISSING edited	R1	R2	R3
ADAC Pannenhilfe	3		0			0	0,05	0,60	1,00
Adobe Acrobat Reader	2		0			0	0,02	0,67	1,00
Barcode Scanner	6		0			2	0,05	0,60	0,75
ES File Explorer	10		0			3	0,11	0,67	0,77
Google Photos	15		0			6	0,11	0,56	0,71
Instagram	9		0			3	0,07	0,53	0,75
Tiny Flashlight	4		0			5	0,04	0,40	0,44
WhatsApp Messenger	25		0			1	0,18	0,89	0,96







## Analysis: **WhatsApp** (All other RWA as environment)

- Higher precision:
  - Direct / Indirect (Through another App)
  - Known environment  
(**...permission.SEND** associated with Intent but Intent has no target.)



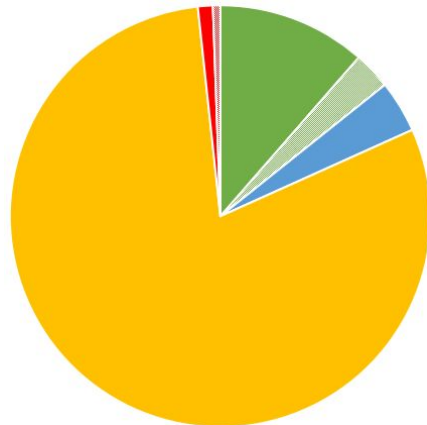


Analysis: **WhatsApp** (All other RWA as environment)

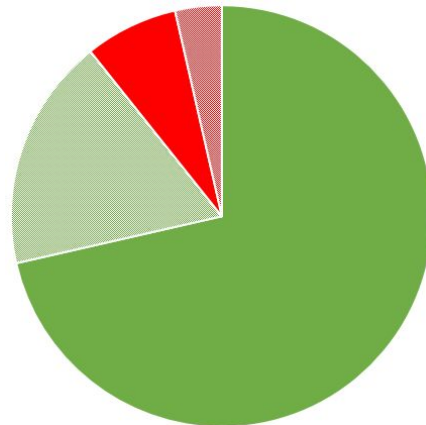
- Higher precision:
  - Direct / Indirect (Through another App)
  - Known environment  
(...**permission.SEND** associated with Intent but Intent has no target.)



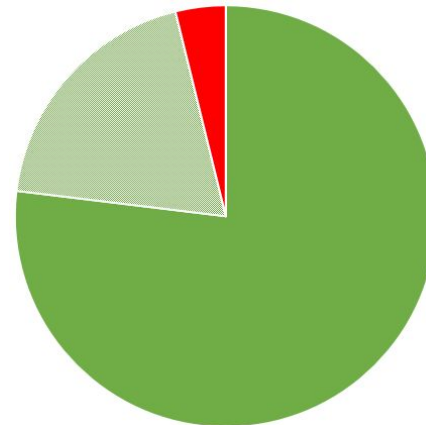
R1 = 0,18



R2 = 0,89



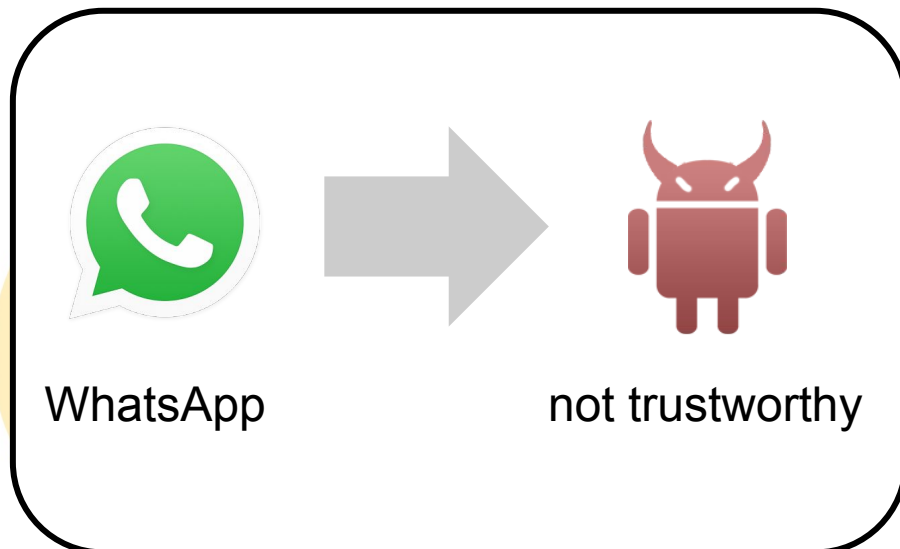
R3 = 0,96



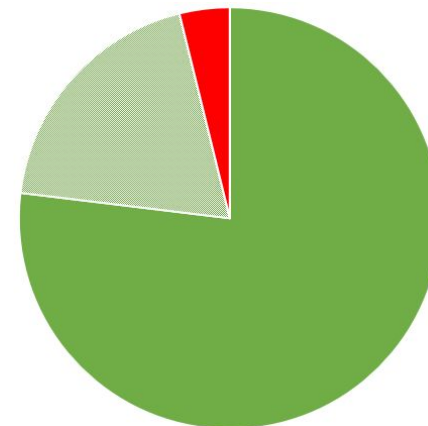


Analysis: **WhatsApp** (All other RWA as environment)

- Higher precision:
  - Direct / Indirect (Through another App)
  - Known environment  
(...**permission.SEND** associated with Intent but Intent has no target.)



$R3 = 0,96$





### Runtime Evaluation (in seconds)

App	FlowDroid	AmanDroid	PAndA <sup>2</sup>
ADAC Pannenhilfe	7	112	13
Adobe Acrobat Reader		197	31
Barcode Scanner	14	23	17
Google Photos		1062	138
Instagram		4246	83
Tiny Flashlight		1328	28
WhatsApp Messenger			12330

 PAndA<sup>2</sup> is working on **all** Apps

 PAndA<sup>2</sup> is **~22 times** faster than AmanDroid

 All tools share one bottleneck: **Memory**





- **Comparison of 3 tools:**  
Aandroid, FlowDroid, PAndA<sup>2</sup>
- **Compared Properties**
  - (Information Flow) Paths
  - Sources
  - Sinks
- **Hard to compare**
  - Different Source & Sink definitions
    - Adapted our tool
    - Unified the results



**Aandroid**  
Unknown

**FlowDroid**  
SuSi

**PAndA<sup>2</sup>**  
SuSi  $\cap$  Permission





- **Precision p**

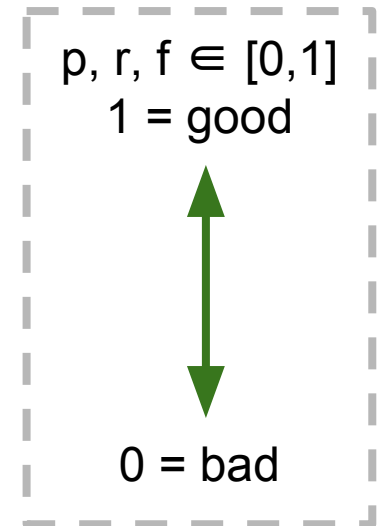
- $$p = \frac{|\text{Real property} \cap \text{Found property}|}{|\text{Found property}|}$$

- **Recall r**

- $$r = \frac{|\text{Real property} \cap \text{Found property}|}{|\text{Real property}|}$$

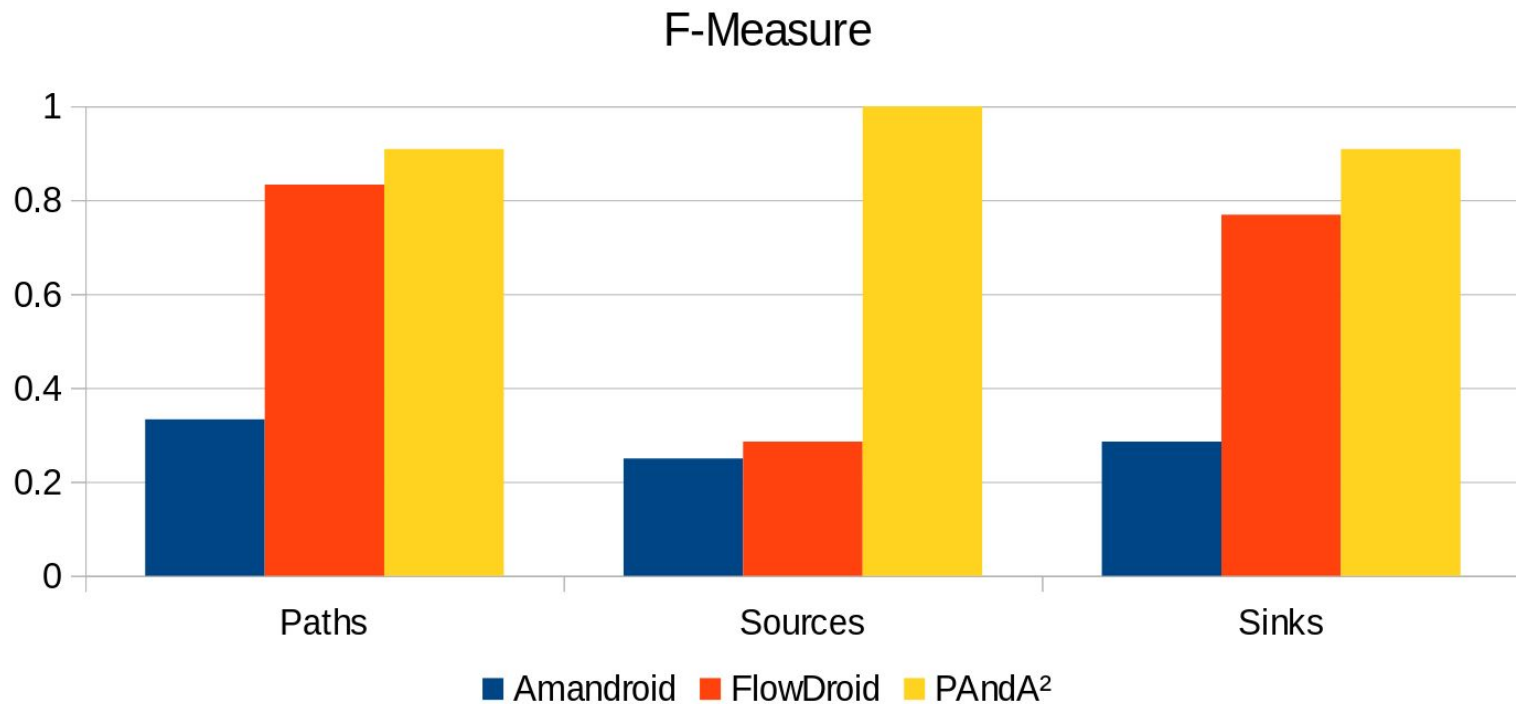
- **F-Measure f**

- f = Harmonic mean of precision and recall





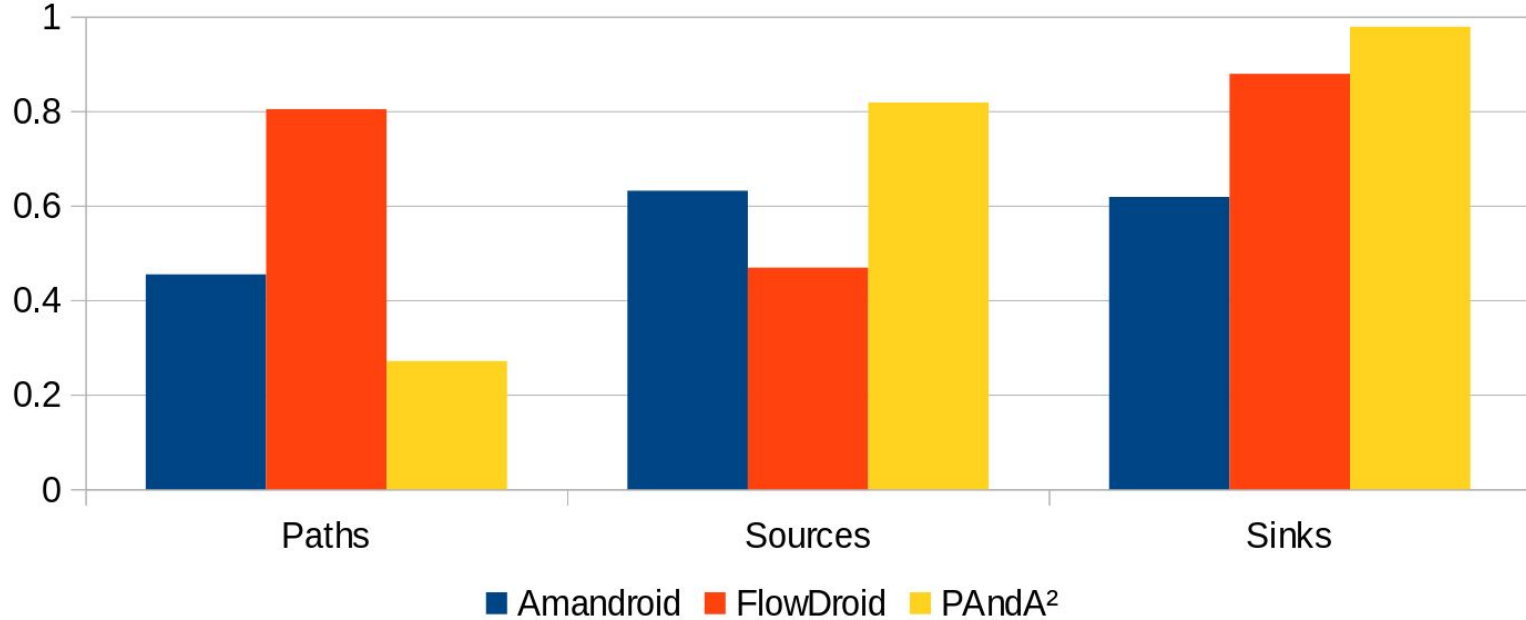
- **Created 4 Apps for Testing**
  - Intra-Component Flow
  - Inter-Component Flow





- **Took 50 Apps from 5 categories**
  - Selected categories due to predefined limitations (e.g. no Inter-App)


F-Measure







App	PAndA <sup>2</sup>			FlowDroid			AmanDroid		
	Sources	Sinks	Paths	Sources	Sinks	Paths	Sources	Sinks	Paths
ADAC	1	0	0	84	29	10	0	2	0
Adobe	1	1	0	-	-	-	-	-	-
Barcode	2	2	0	0	0	0	0	0	0
ES File Explorer	-	-	-	-	-	-	-	-	-
Google Photos	8	7	0	-	-	-	-	-	-
Instagram	8	2	0	-	-	-	1	156	0
Flashlight	4	1	0	-	-	-	6	3	0
Whatsapp	-	-	-	-	-	-	-	-	-

 PAndA<sup>2</sup> is working on **most** of the Apps

 No Information flow analysis was working on WhatsApp Messenger

 All tools share one bottleneck: **Memory**





### Runtime Evaluation (in seconds)

App	FlowDroid	Amandroid	PAndA <sup>2</sup>
ADAC Pannenhilfe	7	112	18
Adobe Acrobat Reader		197	68
Barcode Scanner	14	23	26
Google Photos		1062	1238
Instagram		4246	537
Tiny Flashlight		1328	76

**+** PAndA<sup>2</sup> is **~3 times** faster than AmanDroid

- Slower than FlowDroid, but...
- FlowDroid only works for 2 Real World Apps.
  - only partial paths are computed.





## Usability **VS** Performance

- +** Result representation
  - More than plain text
  - Filterable
  
- +** GUI
  
- +** Reusability of results
  - View a result again
  - Comparing result to another analysis
  - Perform aggregation analysis
  
- Coverage of special cases





*A lot of special cases can be constructed with Java/Android.*





*A lot of special cases can be constructed with Java/Android.*

- **Permission Usage Analyses**



Cover more special cases

- Improve PermissionMapper
- Improve CoreServices: DataStorage, StatementAnalyzer





*A lot of special cases can be constructed with Java/Android.*

- **Permission Usage Analyses**



Cover more special cases

- Improve PermissionMapper
- Improve CoreServices: DataStorage, StatementAnalyzer

- **Information Flow Analysis**



Remove limitations (e.g. no global variables)



Cover more special cases

- Add object sensitivity
- Add thread sensitivity
- ...





*Quality Assurance can always be improved.*

- Written **265** unit test cases for covering more than **80%** of code (method-wise)
- Removed critical code violations for achieving quality “code base”





*Quality Assurance can always be improved.*

- Written **265** unit test cases for covering more than **80%** of code (method-wise)
- Removed critical code violations for achieving quality “code base”

**➔ Improvement:**

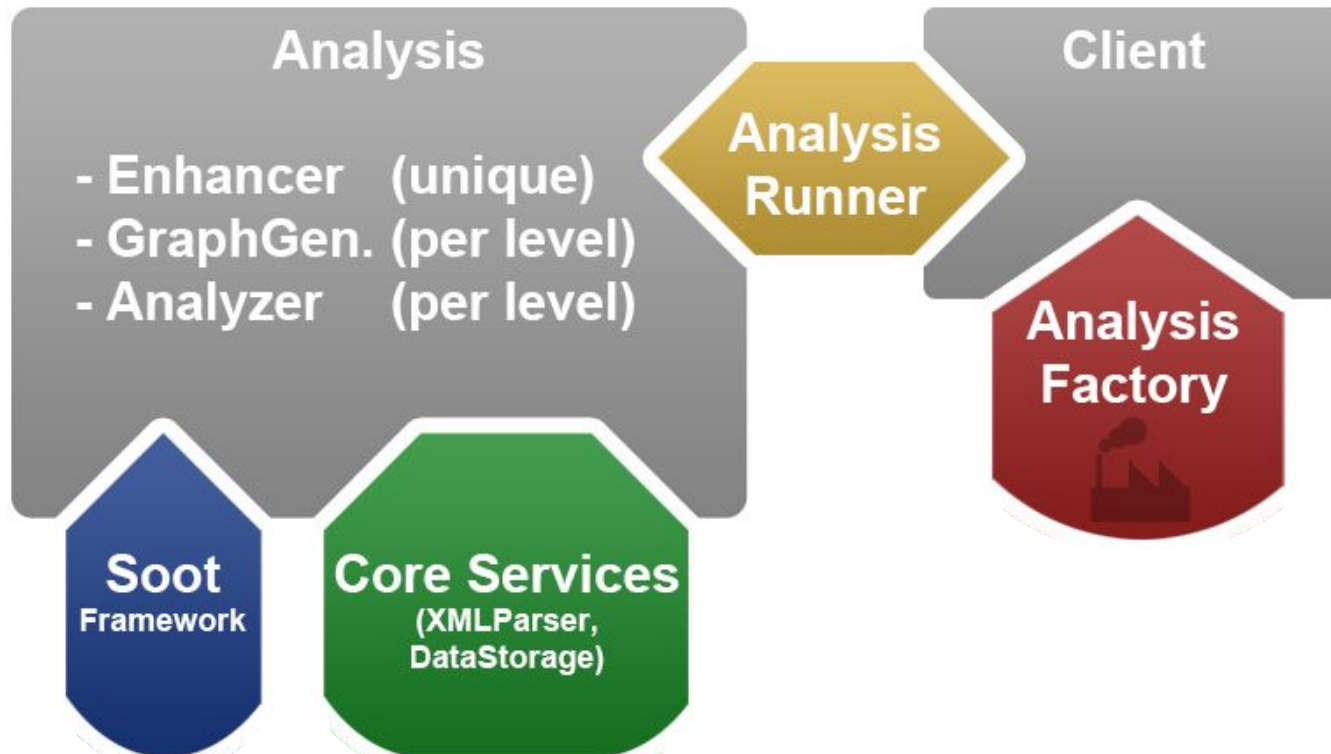
- More test cases for branch-wise code coverage
- Extend test-driven development







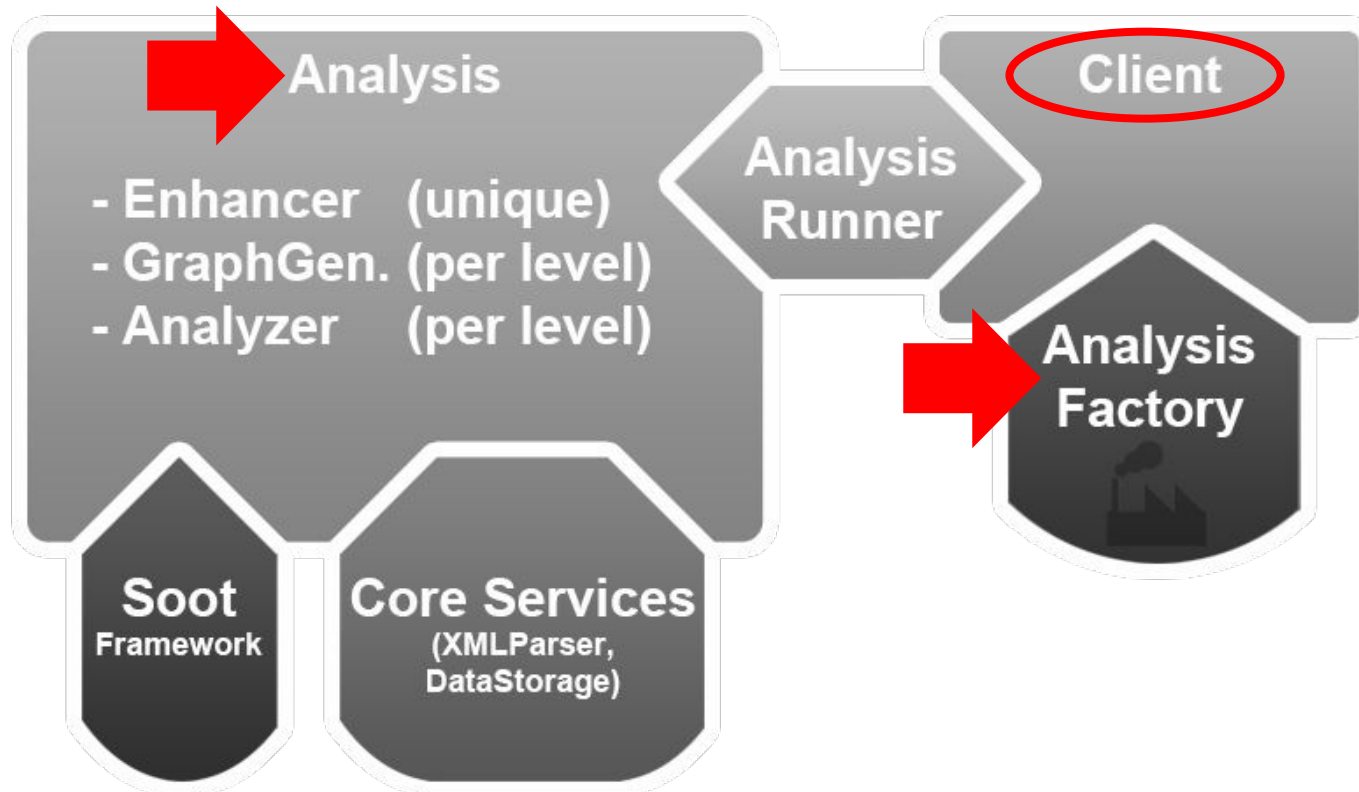
- **Inter-App** Information Flow Analysis
  - Easy to add because of the framework's structure and the availability of the CoreServices.





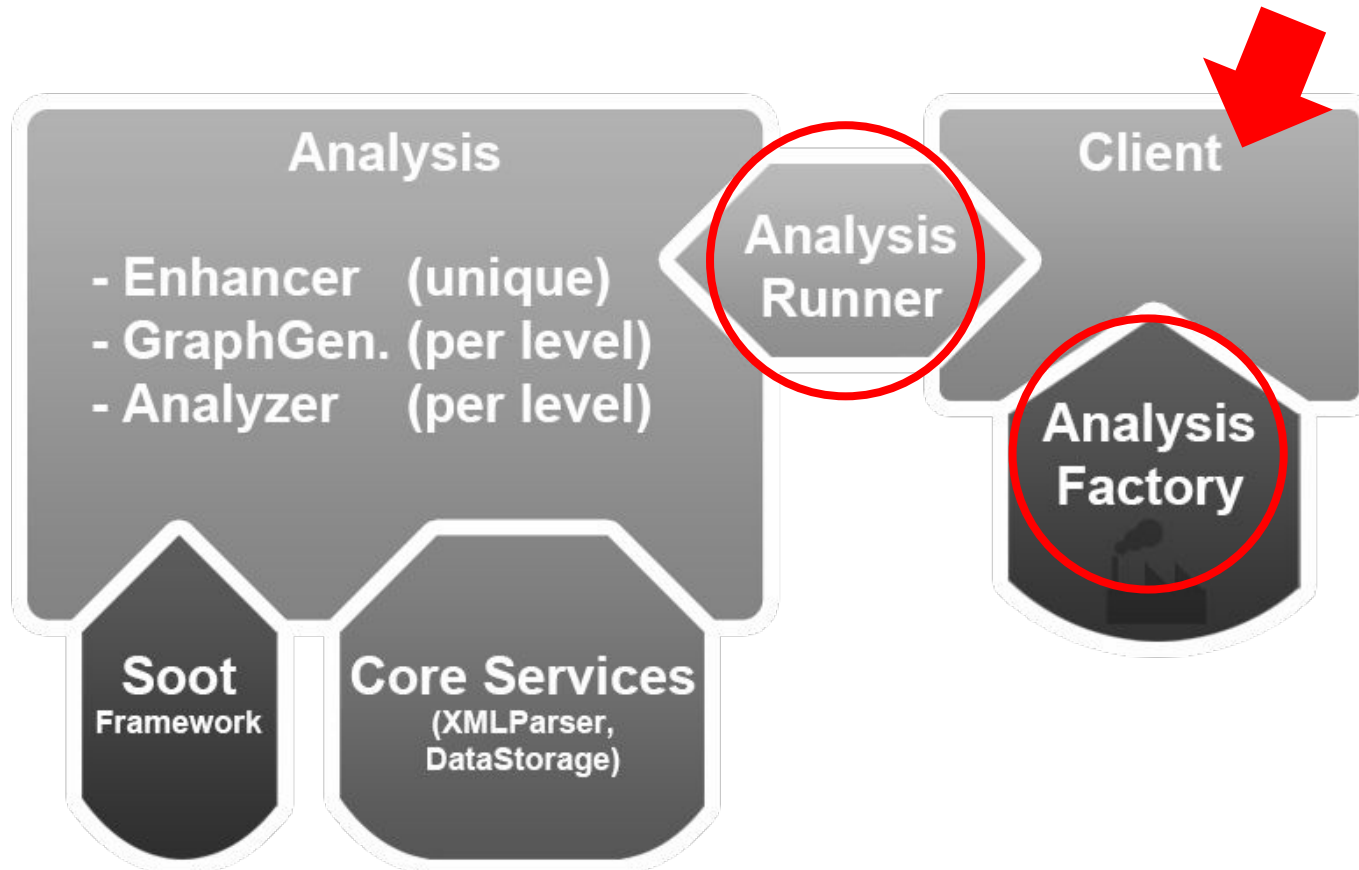
- **Add a new analysis**

- Add analysis
- Add factory
- Tell the Client





- **Add a new Client / User Interface**
  - Add client
    - Loosely coupled to AnalysisRunner and AnalysisFactory





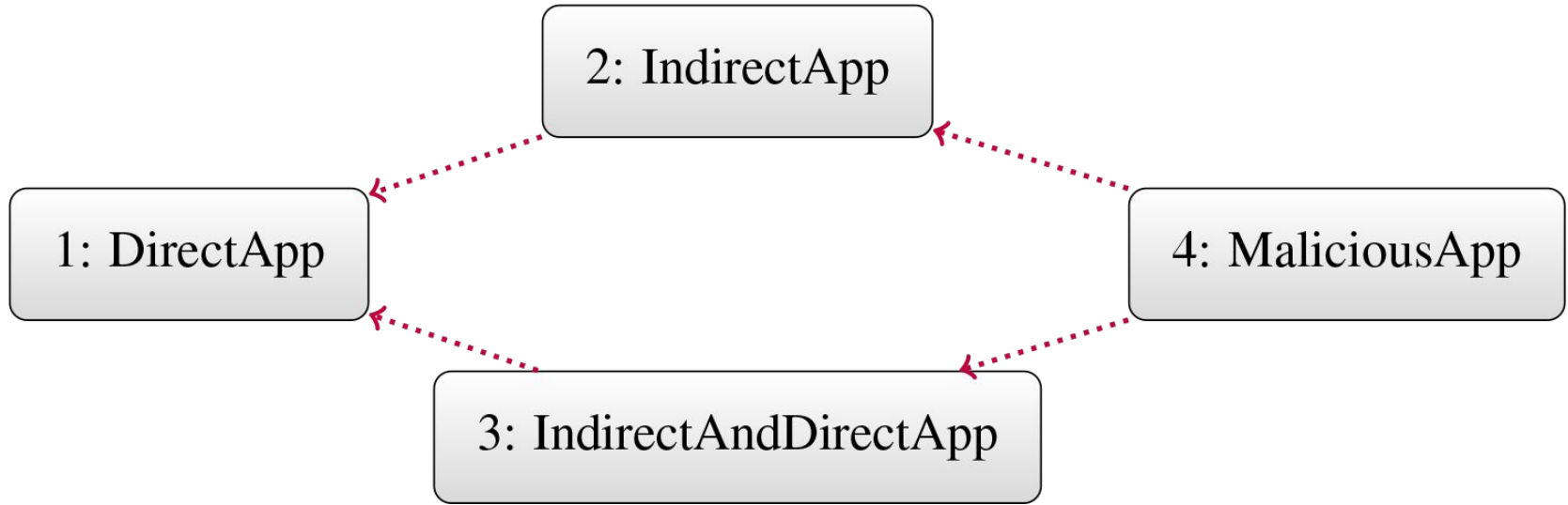
- PAndA<sup>2</sup>
  - Checks App's trustworthiness with 3 analyses
  - User friendly
  - Complete Framework
    - Easily extendable
- Evaluation
  - The Permission Usage Analyses represent useful alternatives
    - Faster than other analyses
    - Less precise than other analyses
    - ➔ Often sufficient results
  - Information Flow Analysis is a solid basis
    - Inter-Component flows can be detected (non-partial)
    - Needs refinement for special cases





[www.pg-a3.foellix.de](http://www.pg-a3.foellix.de)





App	Actual Permission Uses	Permissions in Android Manifest	Implicit Intent Targets
1: DirectApp	CAMERA, INTERNET	CAMERA, VIBRATE	
2: IndirectApp		CAMERA	1: DirectApp
3: DirectAndIndirectApp	CAMERA, INTERNET	CAMERA	1: DirectApp
4: MaliciousApp	VIBRATE	VIBRATE	2: IndirectApp 3: DirectAndIndirectApp





### Sources

Tool	TP	FP	FN	Precision	Recall	F-Measure
<b>PAndA<sup>2</sup></b>	36	0	16	1	0,69	0,82
<b>Amandroid</b>	24	0	28	1	0,46	0,63
<b>FlowDroid</b>	49	108	3	0,31	0,94	0,47

### Sinks

Tool	TP	FP	FN	Precision	Recall	F-Measure
<b>PAndA<sup>2</sup></b>	69	0	3	1	0,96	0,98
<b>Amandroid</b>	47	33	25	0,59	0,65	0,62
<b>FlowDroid</b>	69	16	3	0,81	0,96	0,88

### Paths

Tool	TP	FP	FN	Precision	Recall	F-Measure
<b>PAndA<sup>2</sup></b>	8	2	41	0,8	0,16	0,27
<b>Amandroid</b>	15	2	34	0,88	0,31	0,45
<b>FlowDroid</b>	39	9	10	0,81	0,8	0,8

