

All Your Code Belongs To Us

Dismantling Android Secrets With CodeInspect

Steven Arzt





**Click 'engage'
to rate sessions
and ask questions**



All Your Code Belongs To Us

Dismantling Android Secrets With CodeInspect



TECHNISCHE
UNIVERSITÄT
DARMSTADT



#whoami

- 3rd year PhD student at TU Darmstadt
- Researcher in the Secure Software Engineering Group
 - Group lead: Eric Bodden
- Main interests:
 - Static code analysis
 - Smartphone security
- Maintainer of Soot and FlowDroid
- sseblog.ec-spride.de





Android Distribution Process



- Source code
- Create, modify
- Debug, inspect, understand

- Binary code
- Run the app



Is this really true?

HOW EASY IS IT TO DISMANTLE YOUR APP?



How to secure my app against piracy

I am developing an android app and I am planning to publish it (paid app). **I have heard that it is very easy to pirate Android apps** (much easier than iphone). I was wondering from your experience or what you know, **how can increase the security of my app?** I know that I can never get it 100% secured but I want to **make it harder for people to pirate it** or distribute it illegally Any ideas, experiences, comments you can share? That will be greatly appreciated

Source: stackoverflow.com

Android Still Has A Massive Piracy Problem

Ustwo Games, the developer behind the wildly popular mobile game “Monument Valley,” revealed in a series of tweets that **only 5% of all Android installs of its game were paid for.**

In 2012, Gamasutra reported that piracy for a game called Shadowgun reached 90% on Android; a year later, developer Butterscotch Shenanigans reported **that 95% of the 34,091 Android installs of its first game were “unofficial.”**

Source: uk.businessinsider.com

Piracy On Android: How Bad Is It Really?

In other words, Android users want things for free and are clever enough to know how to get those things for free.

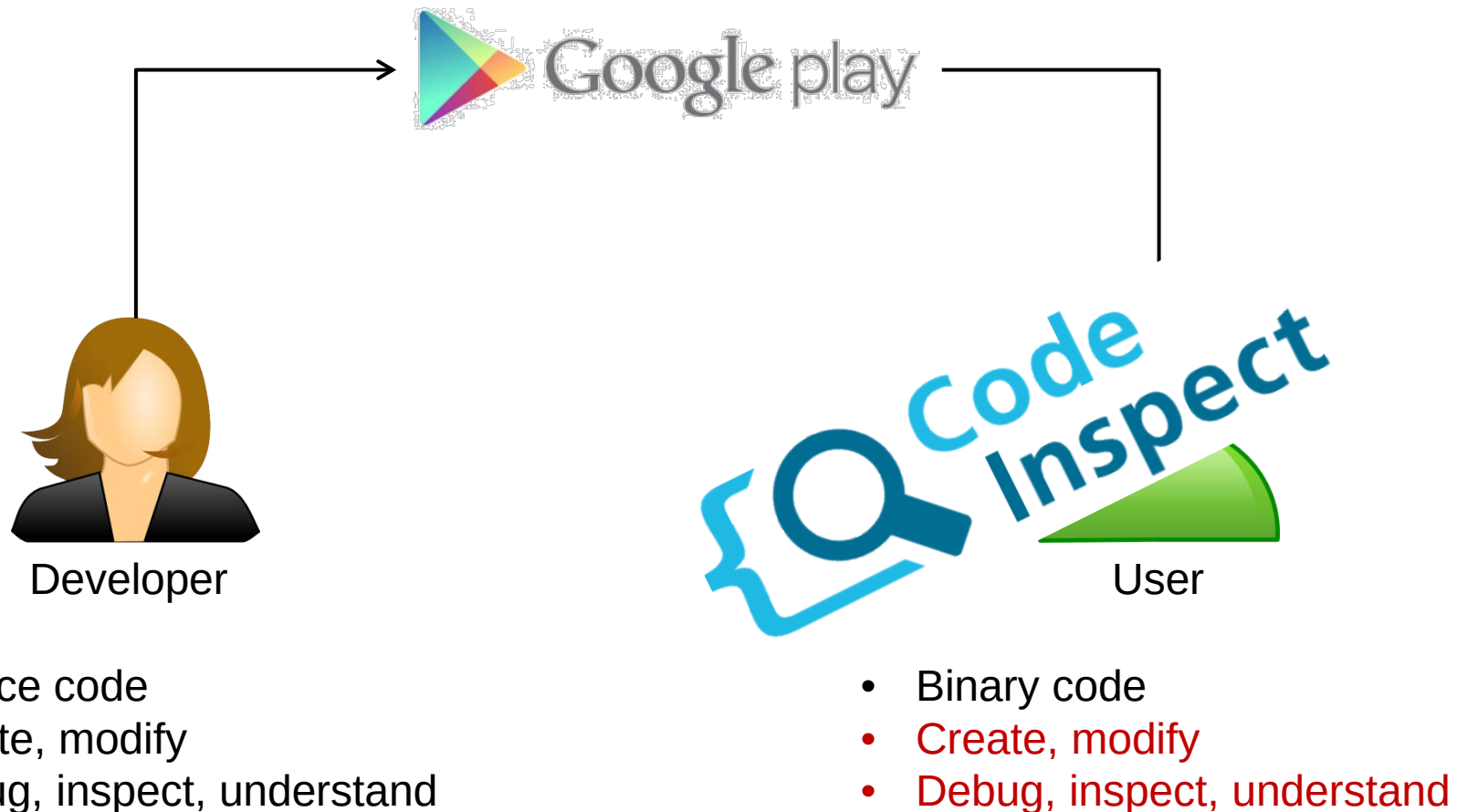
While there are a few steps that can be taken to make the cracking process less convenient, **a determined pirate will be able to break through any kind of app protection if given enough time.**

Source: makeuseof.com



A new Binary Analysis Framework
for Android and Java Bytecode

Android Distribution Process



Why?



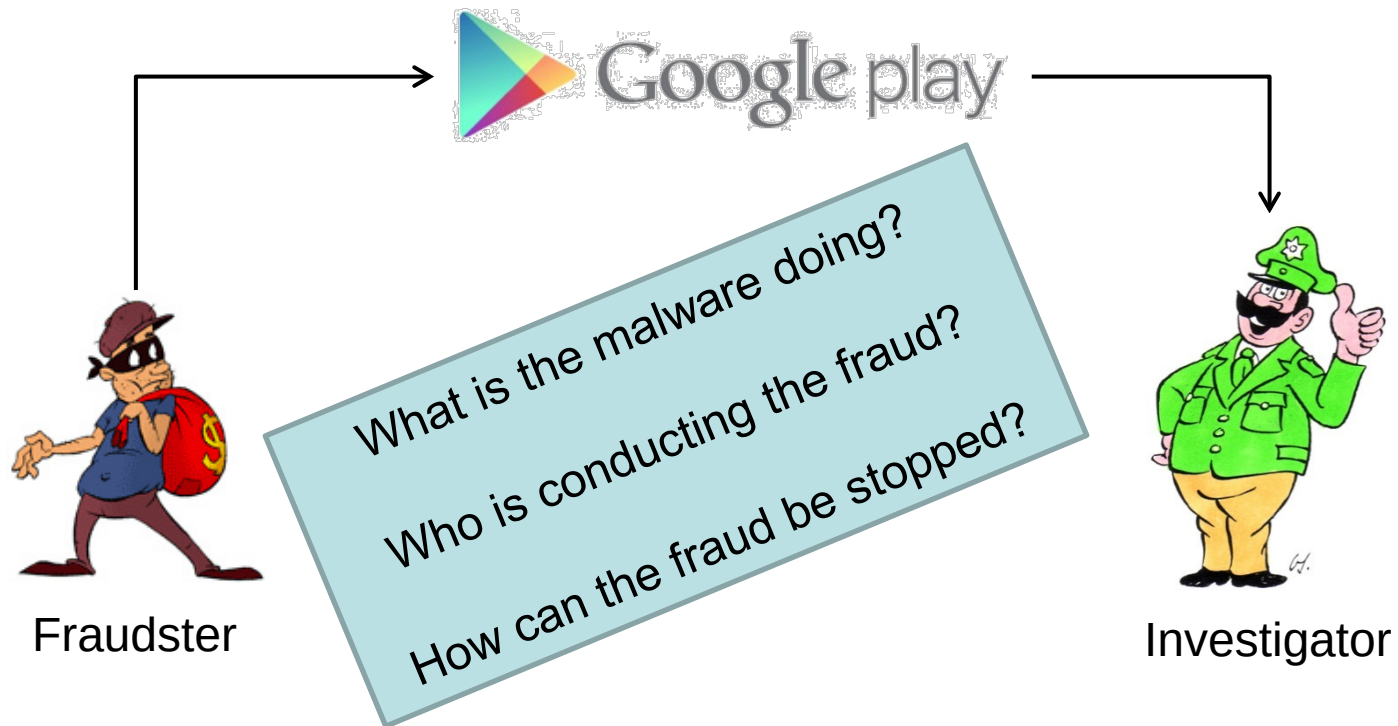
TECHNISCHE
UNIVERSITÄT
DARMSTADT



VS.



Android Distribution Process

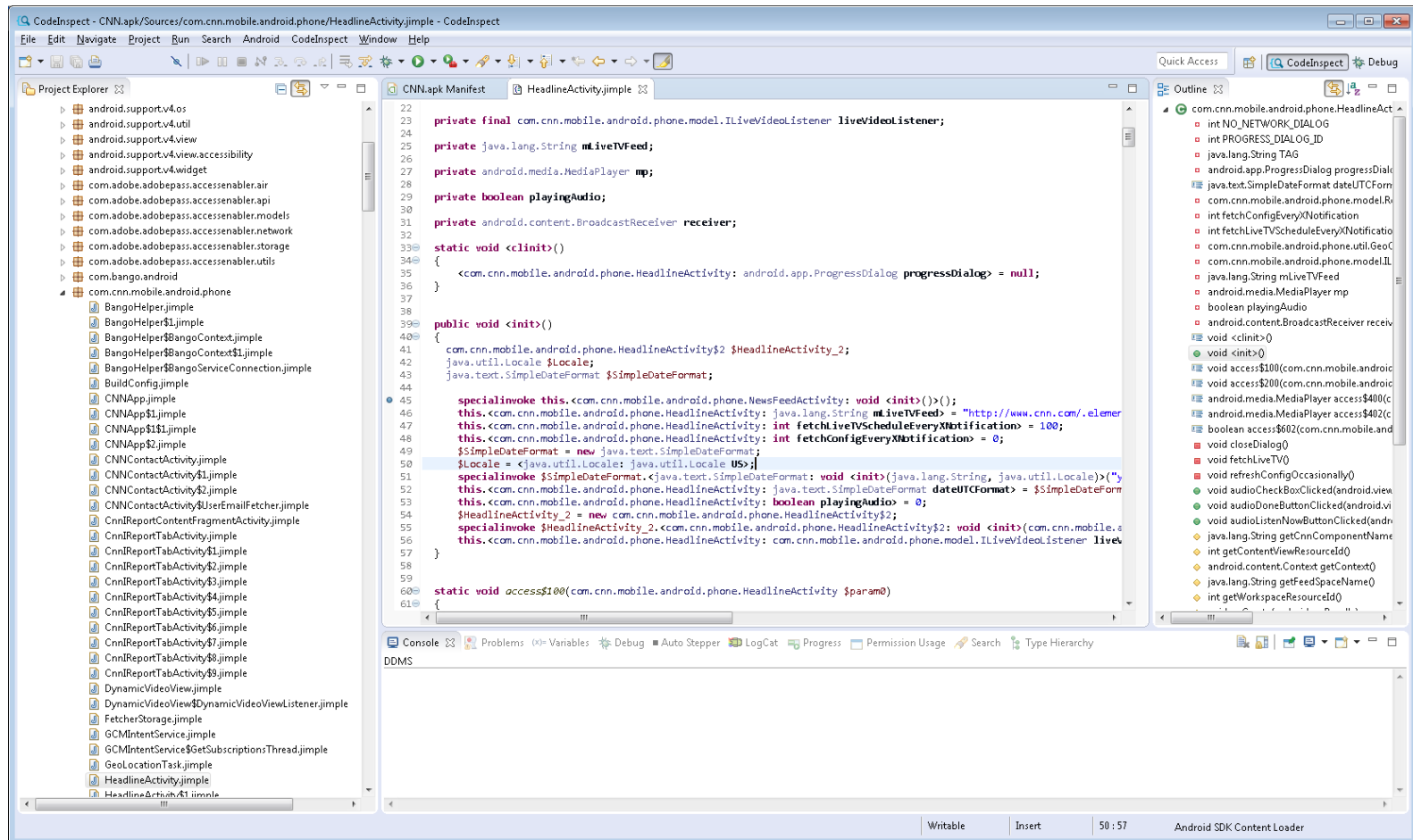




A new Binary Analysis Framework
for Android and Java Bytecode

Debug. Understand. Manipulate.
without the source code

CodeInspect





Project Explorer

android.support.v4.os
 android.support.v4.util
 android.support.v4.view
 Packages and
 Classes
 com.adobe.adobepass.accessenabler.storage
 com.adobe.adobepass.accessenabler.utils
 com.bango.android
 Manifest File
 Assets
 BuildConfig.jimple
 CNNApp.jimple
 CNNApp\$1.jimple
 CNNApp\$1\$1.jimple
 CNNApp\$2.jimple
 CNNContactActivity.jimple
 CNNContactActivity\$UserEmailFetcher.jimple
 CnnIReportContentFragmentActivity.jimple
 CnnIReportTabActivity.jimple
 CnnIReportTabActivity\$1.jimple

CNN.apk Manifest

HeadlineActivity.jimple

```

22
23 private final com.cnn.mobile.android.phone.model.ILiveVideoList
24
25 private java.lang.String mLiveTVFeed;
26
27 private android.media.MediaPlayer mp;
28
29 private boolean playingAudio;
30
31 private android.content.BroadcastReceiver receiver;
32
33 static void <clinit>()
34 {
35     <com.cnn.mobile.android.phone.HeadlineActivity: android.ap
36 }
37
38
39 public void <init>()
40 {
41     com.cnn.mobile.android.phone.HeadlineActivity$2 $HeadlineAct
42     java.util.Locale $Locale;
43     java.text.SimpleDateFormat $SimpleDateFormat;
44
45     specialinvoke this.<com.cnn.mobile.android.phone.NewsFeedA
46     this.<com.cnn.mobile.android.phone.HeadlineActivity: java.
47     this.<com.cnn.mobile.android.phone.HeadlineActivity: int f
48     this.<com.cnn.mobile.android.phone.HeadlineActivity: int f
49     $SimpleDateFormat = new java.text.SimpleDateFormat;
50     $Locale = <java.util.Locale: java.util.Locale us>;|
51     specialinvoke $SimpleDateFormat.<java.text.SimpleDateFormat
52     this.<com.cnn.mobile.android.phone.HeadlineActivity: java.
53     this.<com.cnn.mobile.android.phone.HeadlineActivity: boole
54     $HeadlineActivity_2 = new com.cnn.mobile.android.phone.Hea
55     specialinvoke $HeadlineActivity_2.<com.cnn.mobile.android.
56     this.<com.cnn.mobile.android.phone.HeadlineActivity: com.c
57
  
```

Jimple Code

```

ivate final com.cnn.mobile.android.phone.model.ILiveVideoListener liveVideoListener;

ivate java.lang.String mLiveTVFeed;

ivate android.media.MediaPlayer mp;

ivate boolean playingAudio;

ivate android.content.BroadcastReceiver receiver;

atic void <clinit>()

    <com.cnn.mobile.android.phone.HeadlineActivity: android.app.ProgressDialog progressDialog> = null;

olic void <init>()

com.cnn.mobile.android.phone.HeadlineActivity$2 $HeadlineActivity_2;
java.util.Locale $Locale;
java.text.SimpleDateFormat $SimpleDateFormat;

specialinvoke this.<com.cnn.mobile.android.phone.HeadlineActivity: void <init>()>();
this.<com.cnn.mobile.android.phone.HeadlineActivity: java.lang.String mLiveTVFeed> = "http://www.cnn.com/.elementalLiveTVScheduleEveryXNotification" = 100;
this.<com.cnn.mobile.android.phone.HeadlineActivity: int fetchConfigEveryXNotification> = 0;
$SimpleDateFormat = new java.text.SimpleDateFormat("MM/dd/yyyy");
$Locale = <java.util.Locale: java.util.Locale US>;]
specialinvoke $SimpleDateFormat.<java.text.SimpleDateFormat: void <init>(java.lang.String, java.util.Locale)>("y
this.<com.cnn.mobile.android.phone.HeadlineActivity: java.text.SimpleDateFormat dateUTCFormat> = $SimpleDateFormat;
this.<com.cnn.mobile.android.phone.HeadlineActivity: boolean playingAudio> = 0;
$HeadlineActivity_2 = new com.cnn.mobile.android.phone.HeadlineActivity$2;
specialinvoke $HeadlineActivity_2.<com.cnn.mobile.android.phone.HeadlineActivity$2: void <init>(com.cnn.mobile.android.phone.HeadlineActivity)>();
this.<com.cnn.mobile.android.phone.HeadlineActivity: com.cnn.mobile.android.phone.model.ILiveVideoListener liveVideoListener> = $HeadlineActivity_2.liveVideoListener;

atic void access$100(com.cnn.mobile.android.phone.HeadlineActivity $param0)

```

Jimple Code

- com.cnn.mobile.android.phone.HeadlineActivity
 - int NO_NETWORK_DIALOG
 - int PROGRESS_DIALOG_ID
 - java.lang.String TAG
 - android.app.ProgressDialog progressDialog
 - java.text.SimpleDateFormat dateUTCFormat
 - com.cnn.mobile.android.phone.model.ILiveVideoListener liveVideoListener
 - int fetchConfigEveryXNotification

Code Outline

- android.content.BroadcastReceiver receiver
- void <clinit>()
- void <init>()
- void access\$100(com.cnn.mobile.android.phone.HeadlineActivity \$param0)
- void access\$200(com.cnn.mobile.android.phone.HeadlineActivity \$param0)
- android.media.MediaPlayer access\$400(com.cnn.mobile.android.phone.HeadlineActivity \$param0)
- android.media.MediaPlayer access\$402(com.cnn.mobile.android.phone.HeadlineActivity \$param0)
- boolean access\$602(com.cnn.mobile.android.phone.HeadlineActivity \$param0)
- void closeDialog()
- void fetchLiveTV()
- void refreshConfigOccasionally()
- void audioCheckBoxClicked(android.view.View \$view)
- void audioDoneButtonClicked(android.view.View \$view)
- void audioListenNowButtonClicked(android.view.View \$view)
- java.lang.String getCnnComponentName()
- int getContentViewResourceId()
- android.content.Context getContext()
- java.lang.String getFeedSpaceName()
- int getWorkspaceResourceId()

Debug - org.wikipedia_25.apk/Sources/org.wikipedia/WikipediaApp.jimple - CodeInspector

File Edit Navigate Project Run Search Android CodeInspector Window Help

Debug

Android - org.wikipedia_25.apk [Android App]

Android

Thread [main] (Suspended (breakpoint at line 87 in WikipediaApp))

WikipediaApp.onCreate() line: 87

Instrumentation.callApplicationOnCr...

ActivityThread.handleBindApplication

ActivityThread.access\$1500(ActivityT...

ActivityThread\$H.handleMessage(Me...

ActivityThread\$H\$Handler.dispatchH...

Looper.loop() line: 135

ActivityThread.main(String[]) line: 52

Method.invoke(Object, Object[]), boo...

Method.invoke(Object, Object...) line...

ZygoteInit\$MethodAndArgsCaller.ru...

ZygoteInit.main(String[]) line: 698

Thread [Binder_1] (Running)

Thread [Binder_2] (Running)

Variables

Breakpoints

Name

Value

this

WikipediaApp (id=26)

\$SharedPreferences

null

\$String

\$SharedPreferences.Editor

\$PackageManager

\$int

\$PackageInfo

\$PackageManager_NameNotFoundException

\$int_1

Stack Trace

CodeInspector

WikipediaApp.jimple

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

public void onCreate()
{
 android.content.SharedPreferences\$Editor \$SharedPreferences_Editor;
 android.content.SharedPreferences \$SharedPreferences;
 android.content.pm.PackageManager \$PackageManager;
 android.content.pm.PackageManager\$NameNotFoundException \$Pa
 int \$int, \$int_1;
 java.lang.String \$String;
 android.content.pm.PackageInfo \$PackageInfo;

 specialinvoke this.<android.app.Application: void onCreate
 \$SharedPreferences = virtualinvoke this.<org.wikipedia.Wi
 \$int = interfaceinvoke \$SharedPreferences.<android.content
 \$PackageInfo = null;

 Label3:
 \$PackageManager = virtualinvoke this.<org.wikipedia.Wiki
 \$String = virtualinvoke this.<org.wikipedia.WikipediaApp:
 \$PackageInfo = virtualinvoke \$PackageManager.<android.content.pm.PackageManager: android.content.pm.PackageInfo getPackageInfo(java.lang.String, int)>(\$String, 0);

 Label2:
 if \$int == 0 goto Label0;
 \$int_1 = \$PackageInfo.<android.content.pm.PackageInfo: int versionCode>;
 if \$int_1 <= \$int goto Label1;
}

Jimple Code

Outline

org.wikipedia.WikipediaApp

java.lang.String PREFS_NAME

void <init>()

migrateDatabaseFromv1()

void onCreate()

Code Outline

LogCat

Saved Filters +

All messages (no filters)

Search for messages. Accepts Java regexes. Prefix with pid; app; tag; or text to limit scope.

verbose

Time

PID

TID

Application

Tag

Text

QLiteData... at android.os.HandlerThread.run(Hand

WifiService acquireWifiLockLocked: WifiLock[NlpW

s.BinderProxy@19d990c1]

WifiStateM... WifiStateMachine CMD_START_SCAN sour

uccessRate=0.00 targetRoamBSSID=1c:1

cing

Query from com.google.android.google

ayLogger... Service was disconnected. Will try

Console

Android - org.wikipedia_25.apk - debug

org.wikipedia: application org.wikipedia is waiting for

org.wikipedia: Sending WAIT chunk

org.wikipedia: Debugger is active

org.wikipedia: Debugger has connected

org.wikipedia: waiting for debugger to settle...

org.wikipedia: waiting for debugger to settle...

org.wikipedia: waiting for debugger to settle...

org.wikipedia: waiting for debugger to settle...

org.wikipedia: waiting for debugger to settle...

org.wikipedia: waiting for debugger to settle...

org.wikipedia: waiting for debugger to settle...

org.wikipedia: waiting for debugger to settle...

org.wikipedia: debugger has settled (1419)

Console

- Based on Eclipse RCP
- Work as you would on source code in Eclipse
 - Navigate through the code
 - Add, change, and remove code
 - Inject arbitrary Java code
 - Start and debug your app
 - Inspect and change runtime values



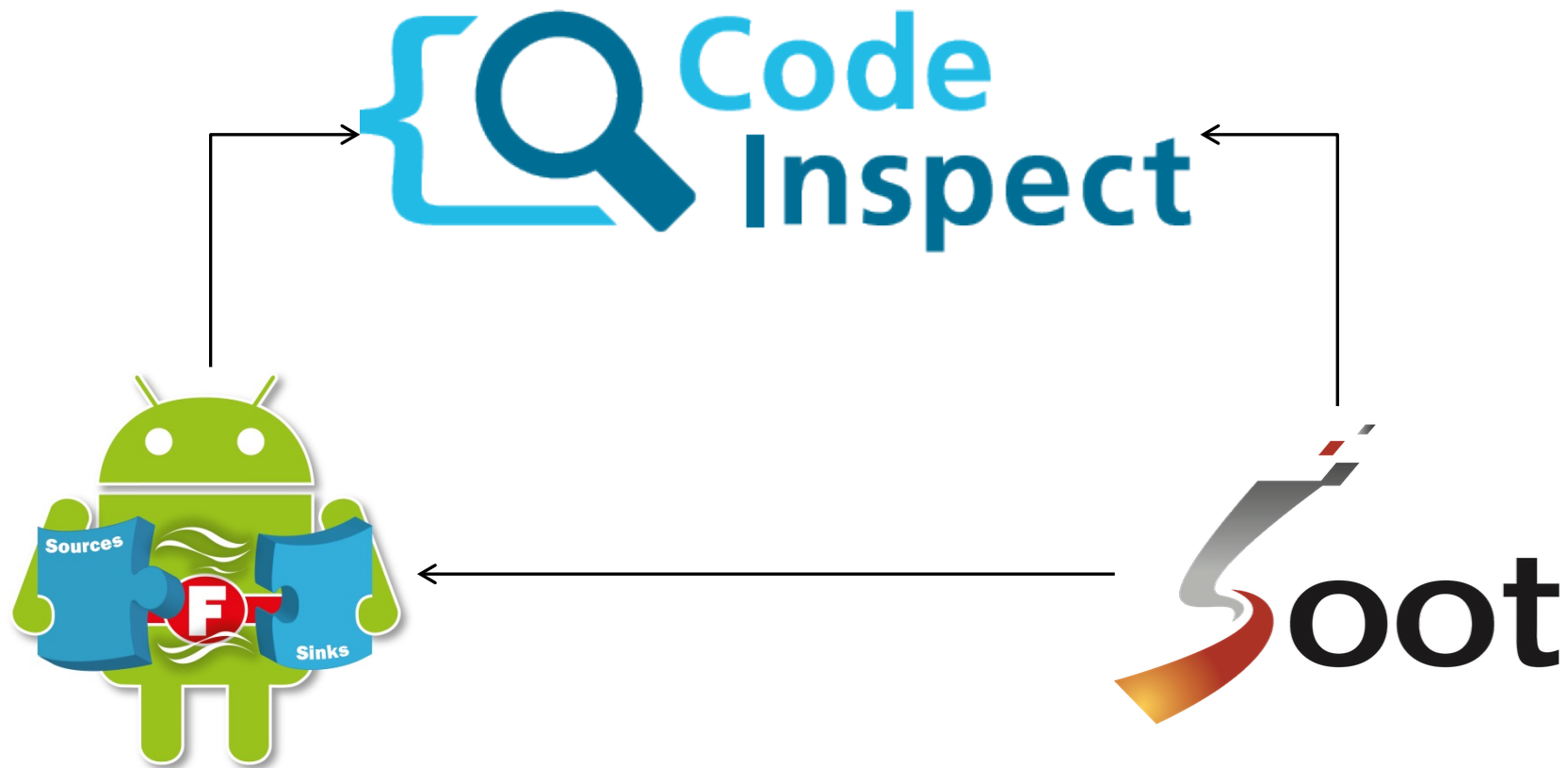


How does it work?

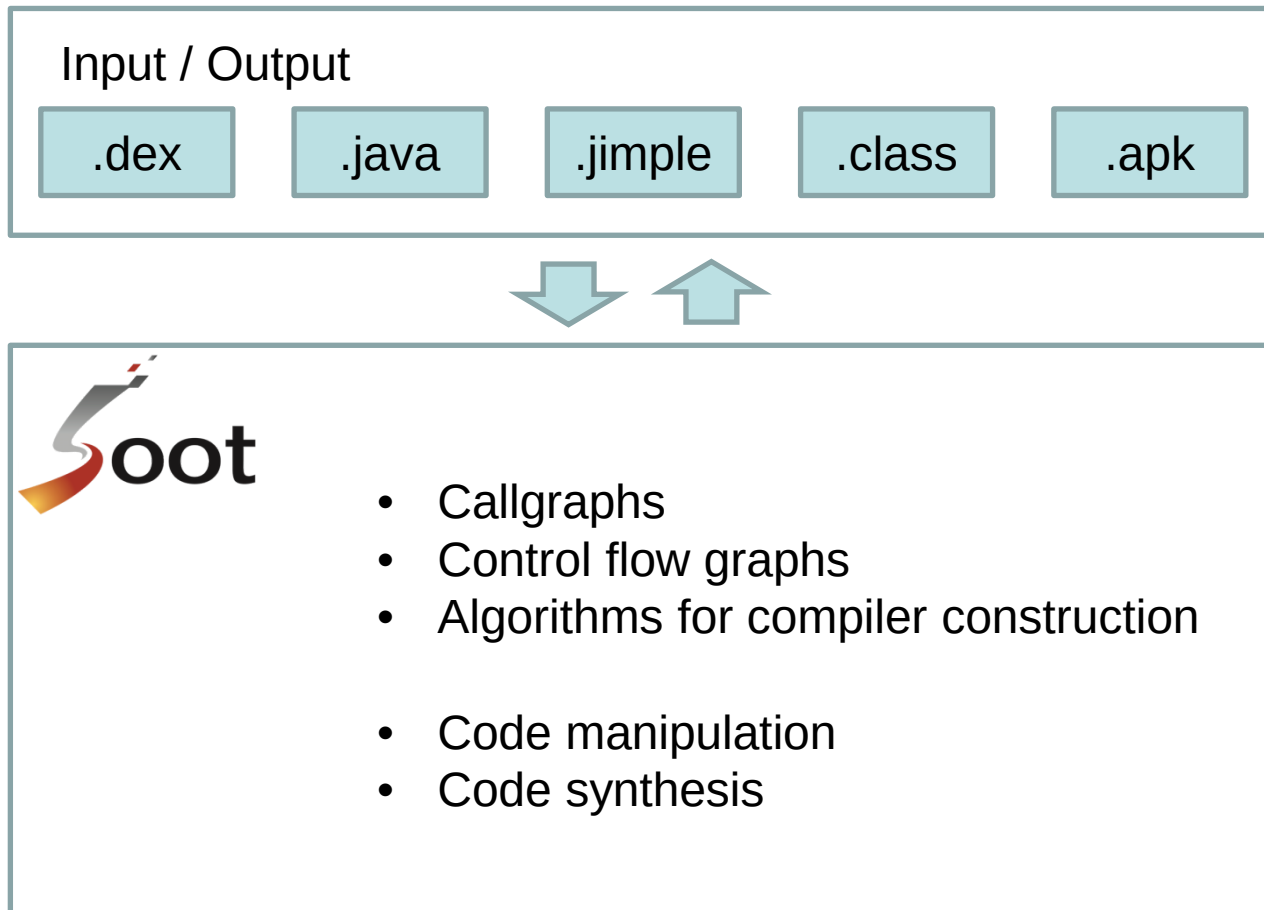
ARCHITECTURE



CodeInspect Architecture

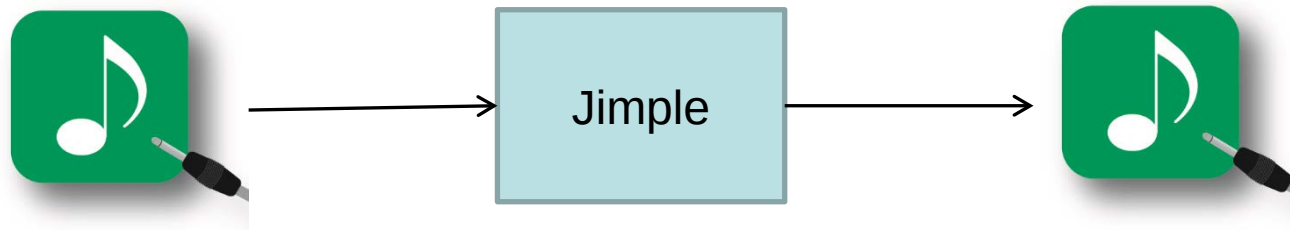


CodeInspect Architecture



The Jimple IR

- Between Dalvik / Java bytecode and Java source code
- Jimple: Java, but simple
- Originally optimized for static analyses



The Jimple IR



TECHNISCHE
UNIVERSITÄT
DARMSTADT

Method Declaration

```
public void foo() {
```

```
    byte[] $arrbyte;  
    java.io.FileOutputStream $FileOutputStream;  
    ...
```

Variable Declarations

```
    specialinvoke this.<android.app.Service: void onCreate()>();  
  
    $File = new java.io.File;  
    specialinvoke $File.<java.io.File: void <init>(java.lang.String)>("/sdcard/test.apk");  
    specialinvoke $FileOutputStream.<java.io.FileOutputStream: void <init>(java.io.File)>($File);  
  
    $arrbyte = newarray (byte)[1024];  
    $int = virtualinvoke $InputStream.<java.io.InputStream: int read(byte[])>($arrbyte);  
    ...
```

Implementation



Class:

```
public class my.package.name.ClassName extends java.lang.Object
{
...
}
```

Package-Name Class-Name Inheritance

```
public class my.package.name.ClassName extends java.lang.Object implements
java.lang.Runnable
{
...
}
```

Interface

Field:

Declaration: private final java.lang.String fieldName;

Modifier Type Name

Access: <my.package.name.ClassName: java.lang.String fieldName>

Package Class Type Name

Method-Declaration:

Modifier	Return-Type	Method-Name	Argument 1 - Type	Argument 1 - Name
<u>public</u>	<u>void</u>	<u>onCreate</u>	<u>(android.os.Bundle</u>	<u>\$param0)</u>
{				
<u>boolean</u> <u>\$z0</u> ;				
<u>java.lang.Object</u> <u>\$Object</u> ;				
<u>java.lang.String</u> <u>\$String</u> ;				
<u>com.util.SPUtil</u> <u>\$SPUtil</u>				
}				
... <u>\$SPUtil</u> = <u>new</u> <u>com.util.SPUtil</u> ;				
... }				

Variable-Declarations

Code

Code:

Assignment:

```
$SPUtil = new com.util.SPUtil;
```

Method-Call:

Static Method Invoke:

```
staticinvoke <com.util.Manager: boolean isWindowShowing()>();
```

Fully-qualified Class Name	Return Type	Method Name
----------------------------	-------------	-------------

Virtual Method Invoke:

```
virtualinvoke $SPUtil.<com.util.Util: void setValue(java.lang.String, java.lang.String)>("username", "Max");
```

"This"-Instance	Argument1-Type	Argument2-Type	Argument1-Value	Argument2-Value
-----------------	----------------	----------------	-----------------	-----------------

Special Method Invoke:

```
specialinvoke $StringBuilder.<java.lang.StringBuilder: void <init>(java.lang.String)>($String);
```

Interface Method Invoke:

```
interfaceinvoke $List.<java.util.List: int size()>();
```

Condition:

```
      Condition      Goto-Statement
    {
if $int < $int_1 goto label0;
//Else Branch
label0:
//This Branch
    }
```

Loop:

```
label0:
if $int < $int_1 goto label1;
    $int = $int + 1;
    goto label0;
label1:
//Quit Loop
```

Exception:

NO explicit goto label6 instruction;
gets called during runtime when an exception gets thrown

```
    {
label6:
    $Throwable := @caughtexception;
    exitmonitor this;
    throw $Throwable;
    }
```



CodeInspect in Action

CASE STUDIES



- Malware analysis
 - Debug malware
 - Find backend credentials
 - Remove anti-analysis checks

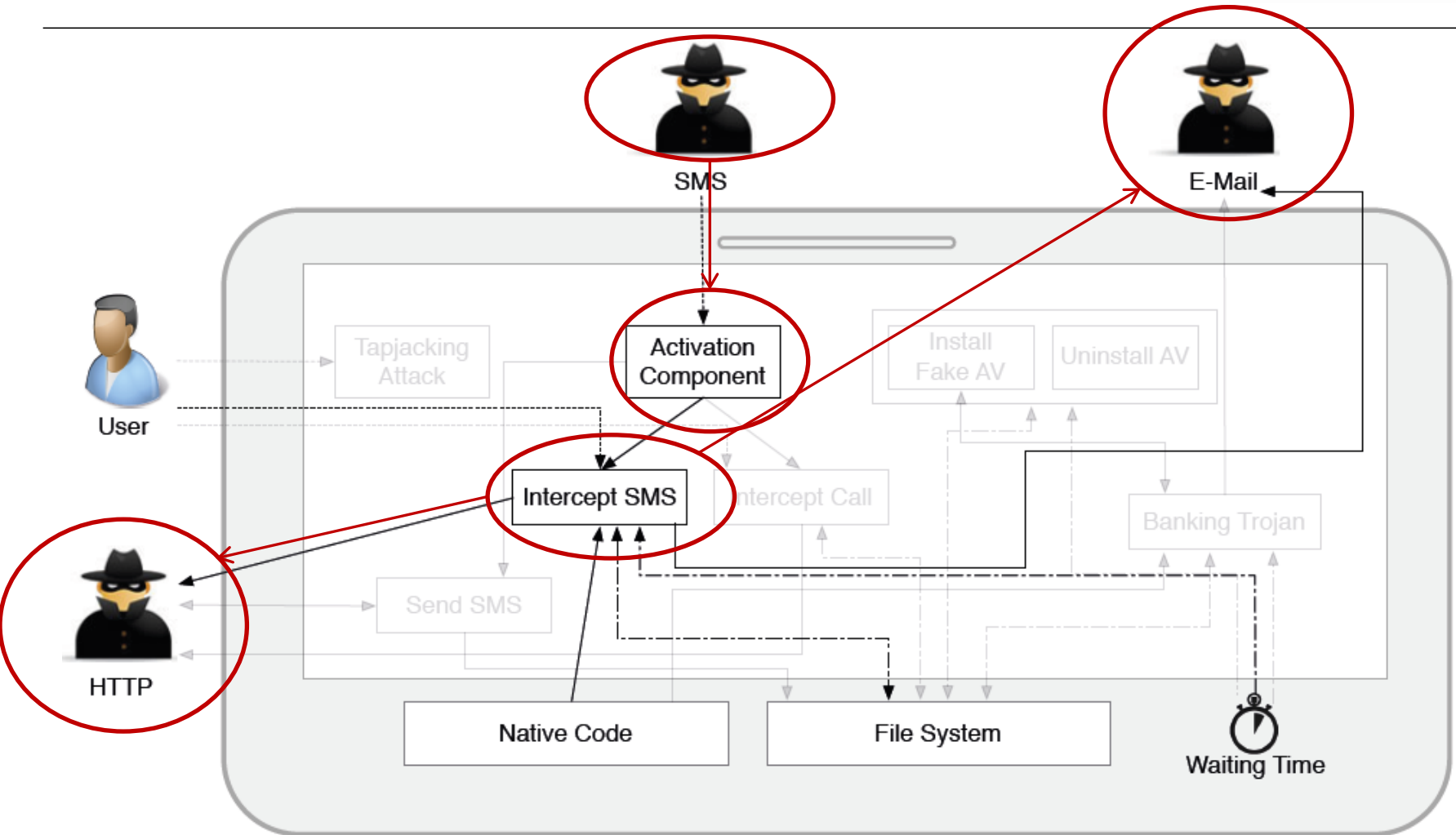
> 20.000 infected phones



The BadAccents Malware



TECHNISCHE
UNIVERSITÄT
DARMSTADT





CodeInspect in Action

LIVE DEMO



- Software development
 - Inspect libraries
 - Look for security vulnerabilities
 - Understand exceptions and problems
 - See what happens under the hood



- Don't be evil
 - Remove license checks
 - Reverse-engineer competitor apps
 - Steal intellectual property
- Copyright laws apply!





What does this all mean?

CONSEQUENCES FOR DEVELOPERS



Consequences for Developers

- All apps are “open-source”
- Never hide secrets inside the app code
 - Backend credentials
 - Encryption keys
- Piggybacking malware is simple
- Cracking apps is simple



Consequences for Developers

- Backend-as-a-Service study
- Will be presented at Blackhat Europe in Amsterdam

18,670,00 records

56,000,000 data items

- E-Mail addresses
- Health records
- Employee databases
- Customer databases
- Server backups
- Voice records

Countermeasures

- String encryption
 - Use the debugger, get de-obfuscated result
- Code encryption
 - Use debugger to get the code as it is about to be loaded
- Hide calls in reflection
 - Use debugger to step into right target method
- Debugger detection
 - Patch the code to remove the check





Extending CodeInspect

THE PLUG-IN SYSTEM



Data Flow Analysis Plugin

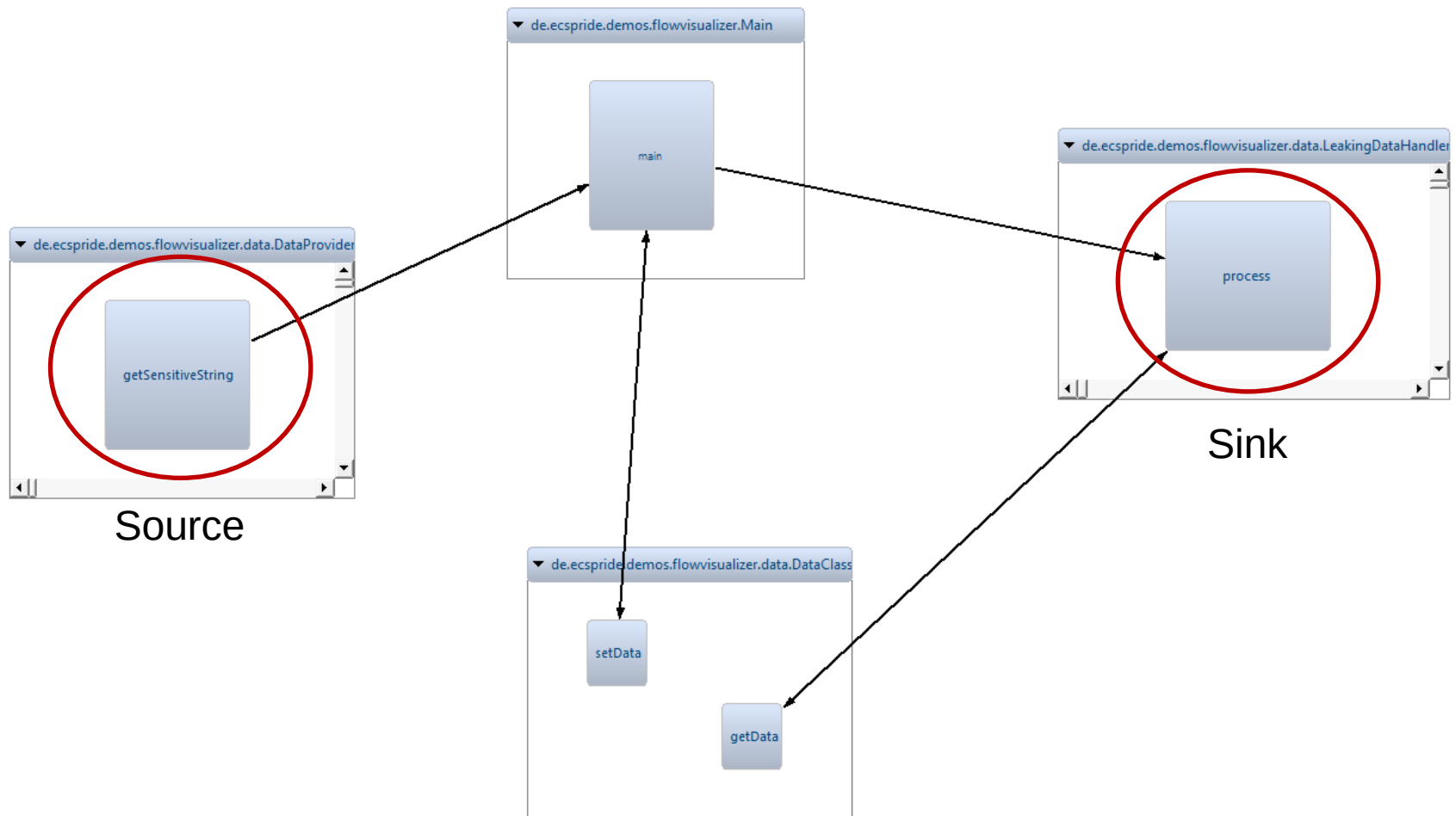
- Which data is read?
- What happens with the data?
- Where is the data sent to?



**Angry Birds and other Mobile Gaming apps
leaking your private information to NSA**

by Swati Khandelwal on Monday, January 27, 2014

Data Flow Analysis Plugin



Data Flow Analysis Plugin



TECHNISCHE
UNIVERSITÄT
DARMSTADT

FlowDroid Information Flow - FlowVisualizerDemo/src/de/ecspride/demos/flowvisualizer/data/DataProvider.java - CodeInspect

File Edit Source Refactor Navigate Project Run Search Android CodeInspect Window Help

Quick Access CodeInspect Debug FlowDroid Information Flow

WikipediaAp... DataClass.java LeakingDataH... Main.java DataProvide... » 1

Calltrace View

Line Instruction

13 \$r2 = staticinvoke <de.ecspride.demos.flowvisualizer.android.TelephonyManager: java.lang.String getDeviceId()> ()

13 \$r3 = virtualinvoke \$r1.<java.lang.StringBuilder: java.lang.StringBuilder append(java.lang.String)> (\$r2)

13 \$r4 = virtualinvoke \$r3.<java.lang.StringBuilder: java.lang.String toString()> ()

13 return \$r4

17 virtualinvoke r1.<de.ecspride.demos.flowvisualizer.data.DataClass: void setData(java.lang.String)> (\$r6)

21 r0.<de.ecspride.demos.flowvisualizer.data.DataClass: java.lang.String stringData> = r1

22 return

19 virtualinvoke r3.<de.ecspride.demos.flowvisualizer.data.LeakingDataHandler: void process(de.ecspride.demos.flowvisualizer.data.Da

16 \$r5 = virtualinvoke r1.<de.ecspride.demos.flowvisualizer.data.DataClass: java.lang.String stringData> ()

25 \$r1 = r0.<de.ecspride.demos.flowvisualizer.data.D

25 return \$r1

16 virtualinvoke r2.<de.ecspride.demos.flowvisualizer

Jimple Code

Propagation Path

Data Flows

Global Findings Graph View

Source

de.ecspride.demos.flowvisualizer.data.DataProvider.getSensitiveString

Sink

de.ecspride.demos.flowvisualizer.data.Leak

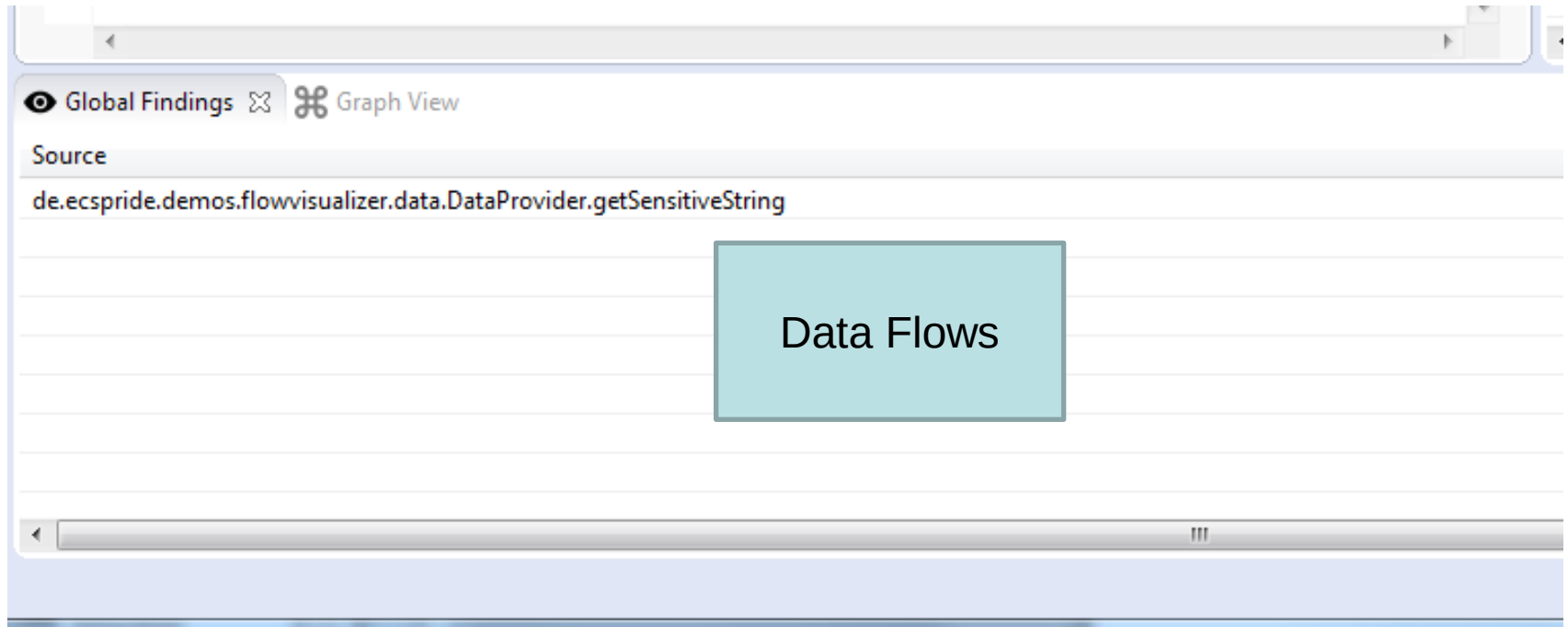
Writable Smart Insert 13 : 68



Data Flow Analysis Plugin



TECHNISCHE
UNIVERSITÄT
DARMSTADT



Data Flow Analysis Plugin

Quick Access | CodeInspect | Debug | FlowDroid Information Flow

Calltrace View

Line	Instruction
13	\$r2 = staticinvoke <de.ecspride.demos.flowvisualizer.android.TelephonyManager: java.lang.String getId()> ()
13	\$r3 = virtualinvoke \$r1.<java.lang.StringBuilder: java.lang.StringBuilder append(java.lang.String)> (\$r2)
13	\$r4 = virtualinvoke \$r3.<java.lang.StringBuilder: java.lang.String toString()> ()
13	return \$r4
17	virtualinvoke r1.<de.ecspride.demos.flowvisualizer.data.DataClass: void setData(java.lang.String)> (\$r6)
21	r0.<de.ecspride.demos.flowvisualizer.data.DataClass: java.lang.String stringData> = r1
22	return
19	virtualinvoke r3.<de.ecspride.demos.flowvisualizer.data.LeakingDataHandler: void process(de.ecspride.demos.flowvisualizer.data.Da
16	\$r5 = virtualinvoke r1.<de.ecspride.demos.flowvisualizer.data.DataClass: java.lang.String getData()> ()
25	\$r1 = r0.<de.ecspride.demos.flowvisualizer.data.DataClass: java.lang.String string
25	return \$r1
16	virtualinvoke r2.<de.ecspride.demos.flowvisualizer.android.ConnectionManager:

Propagation Path

Data Flow Analysis Plugin



TECHNISCHE
UNIVERSITÄT
DARMSTADT

```
1 package de.ecspride.demos.flowvisualizer.data;
2
3 import de.ecspride.demos.flowvisualizer.android.TelephonyManager;
4
5 /**
6  * Class that is used to obtain data
7  *
8  * @author Steven Arzt
9  */
10 public class DataProvider {
11
12     public String getSensitiveString() {
13         return "Sensitive data: " + TelephonyManager.getDeviceId();
14     }
15
16 }
17
18
```

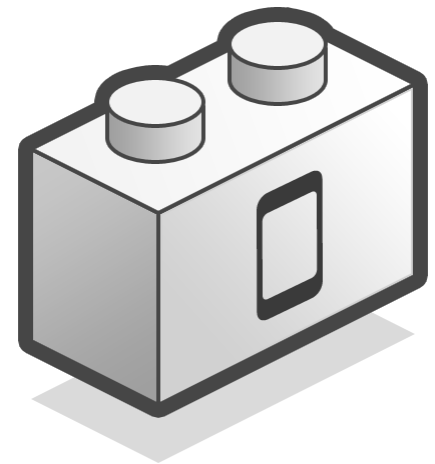
Line	Inst
13	\$r2:
13	\$r3:
13	\$r4:
13	retu
17	virtu
21	r0.<
22	retu
19	virtu
16	\$r5:
25	\$r1:
25	retu
16	virtu

Jimple Code



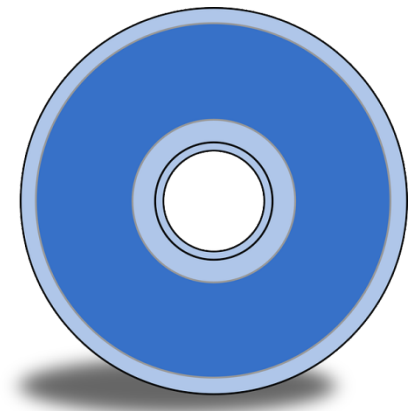
Other Planned Plugins

- Runtime value reconstruction
- Interactive callgraph and control flow visualization
- Malware analysis assistance
- (Semi-)Automatic deobfuscation
- Plugins directly from research



Obtaining CodeInspect

- Will be a commercial product
- Free 60 day demo license available
 - All features available
 - No restrictions on target APKs
 - E-Mail me





www.codeinspect.de

Steven Arzt

Secure Software Engineering Group (EC-SPRIDE)

Email: steven.arzt@ec-spride.de

Blog: <http://sse-blog.ec-spride.de>

Website: <http://sse.ec-spride.de>



Please

**Remember to
rate this session**

Thank you!

