Dismantling droids for breakfast - The current state of app reverse engineering

Siegfried Rasthofer

SECURE SOFTWARE ENGINEERING GROUP
TECHNISCHE UNIVERSITÄT DARMSTADT
Fraunhofer SIT
EC SPRIDE

#whoami

- 3rd year PhD-Student at Secure Software Engineering Group Darmstadt, Germany (Prof. Dr. Eric Bodden)
- Research interest:
  - Applied software security on Android
  - Static-/dynamic code analyses

- Android Security:
  - Found 2 AOSP exploits
  - Security Analysis of Backend-as-a-Service
  - Korea Threat investigation together with McAfee Research Lab

Google play

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 illegaly Any ideas, experiences, comments you can share? That will be greatly appreciated Best regards

Source: stackoverflow.com

Is it still easy to dismantle your app?

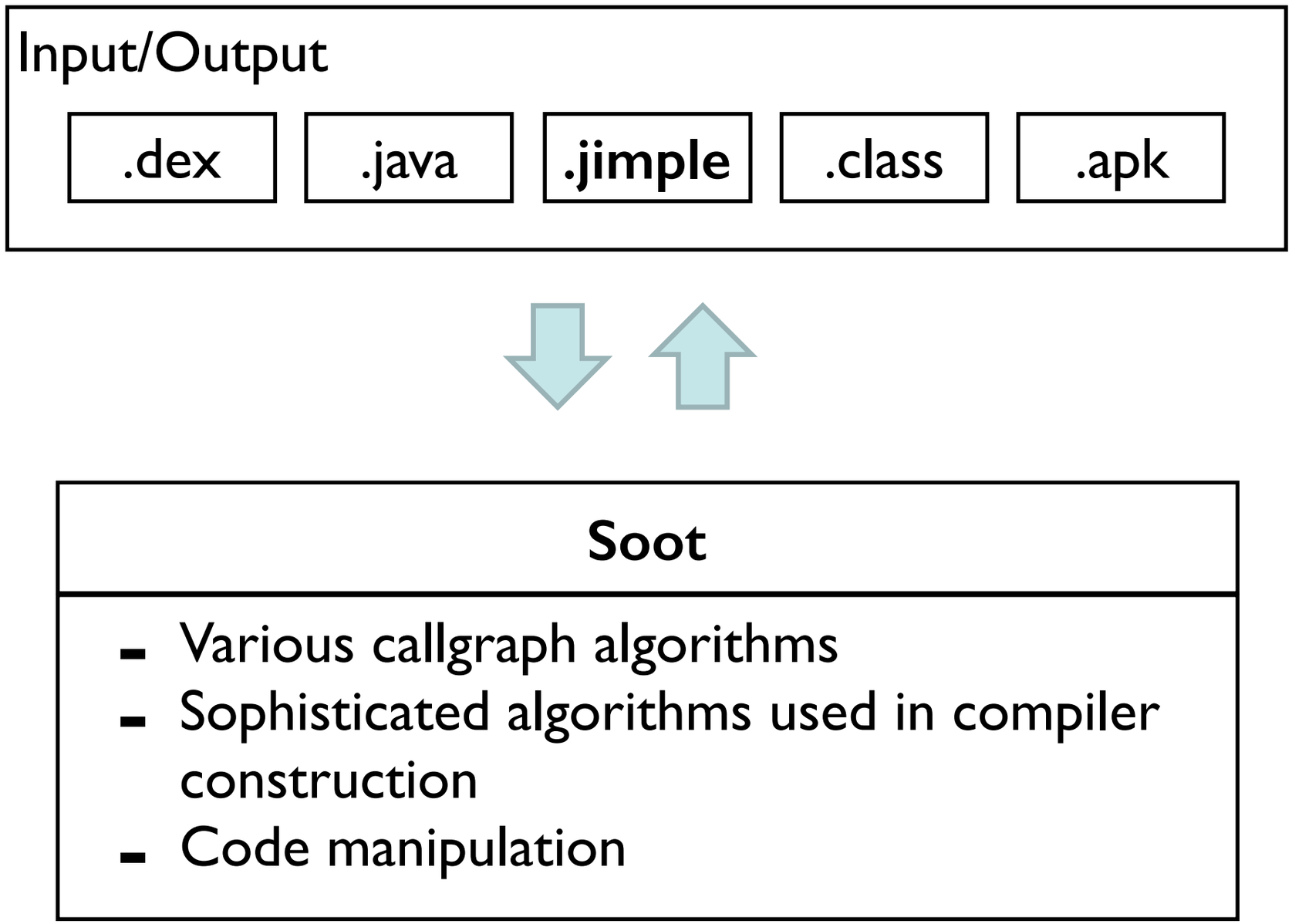
Code Inspect

A new Binary Analysis Framework for Android and Java Bytecode

VS

Soot

Soot



https://github.com/Sable/soot/wiki

Jimple

Soot

Jimple

Soot

```
public static boolean UsbAutoRunAttack(android.content.Context $param0)
{
  java.lang.String $String;
  $String = <smart.apps.droidcleaner.Tools: java.lang.String urlServer>;
  ...
  staticinvoke <smart.apps.droidcleaner.Tools: boolean
     DownloadFile(java.lang.String, java.lang.String, java.lang.String,
     java.lang.String, android.content.Context)>
     ($String, "autorun.inf", "ftpupper", "thisisshit007", $param0);
  return true;
}
```

Declarations

Code

Return-Statement

CodeInspect

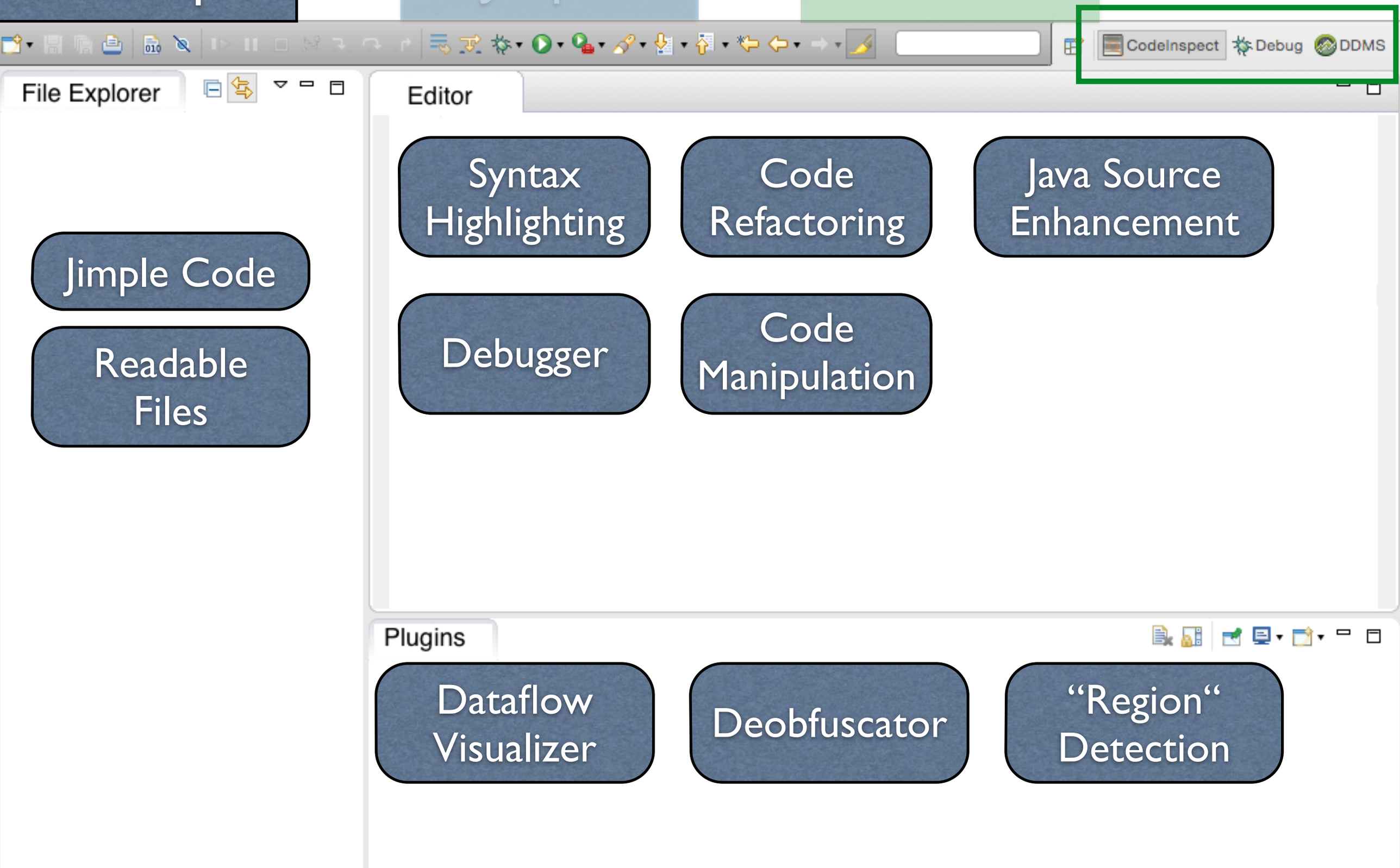
Jimple

Soot

CodeInspect

Jimple

Soot



Jimple Code

Readable Files

Syntax Highlighting

Code Refactoring

Java Source Enhancement

Debugger

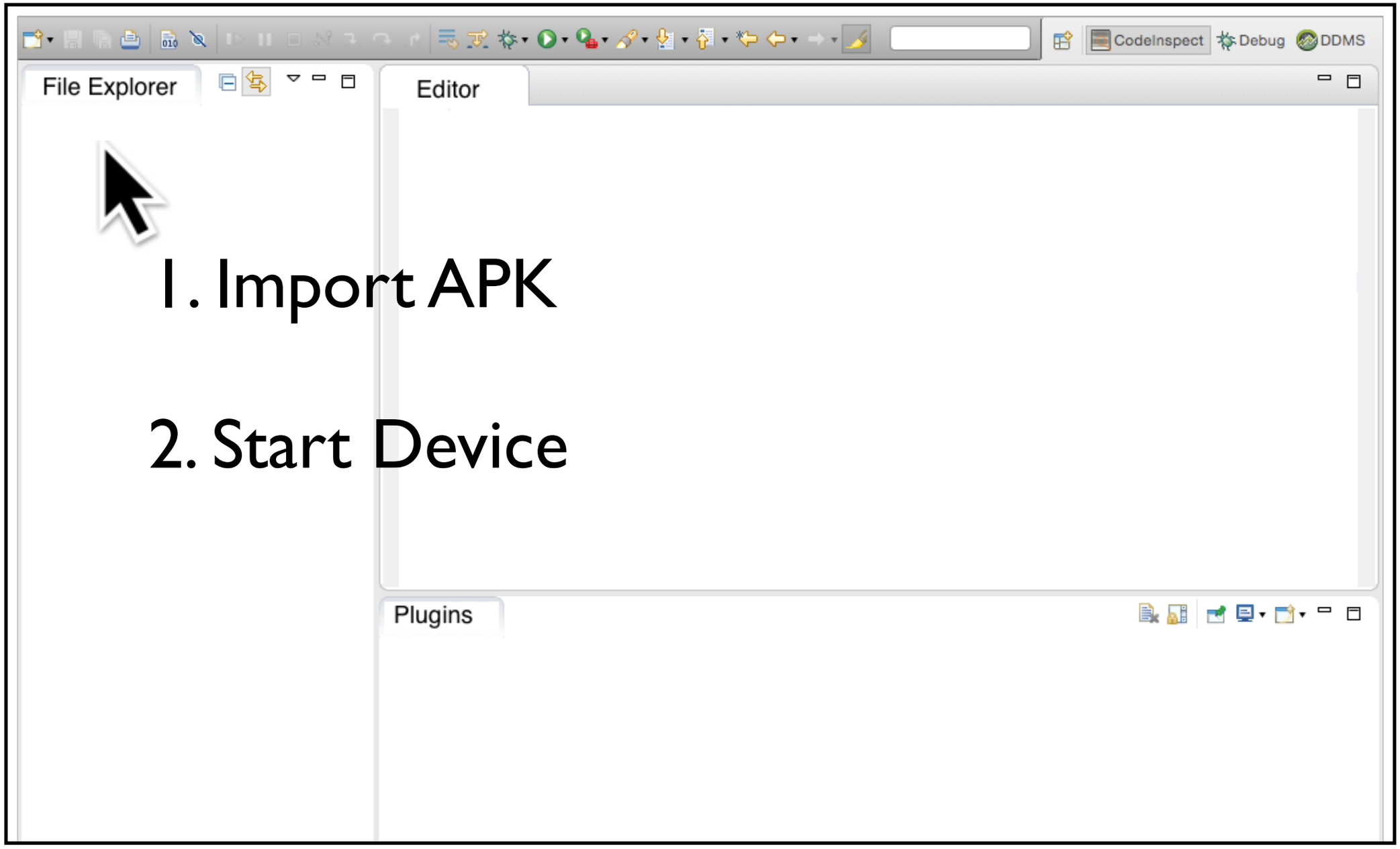
Code Manipulation

Dataflow Visualizer

Deobfuscator

"Region" Detection

Let's get started…

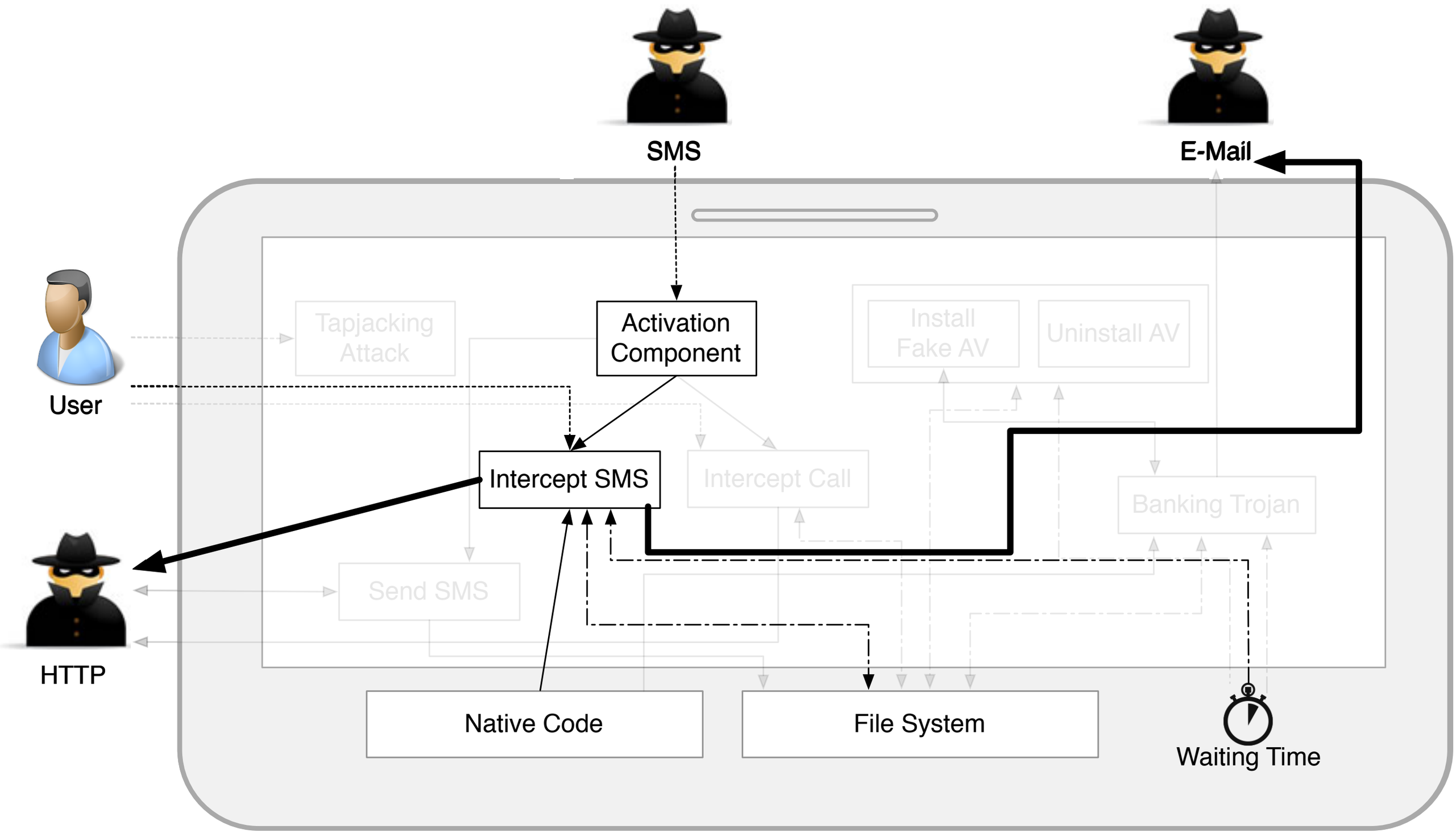


1. Import APK

2. Start Device

infected >20,000 user

Android/BadAccents



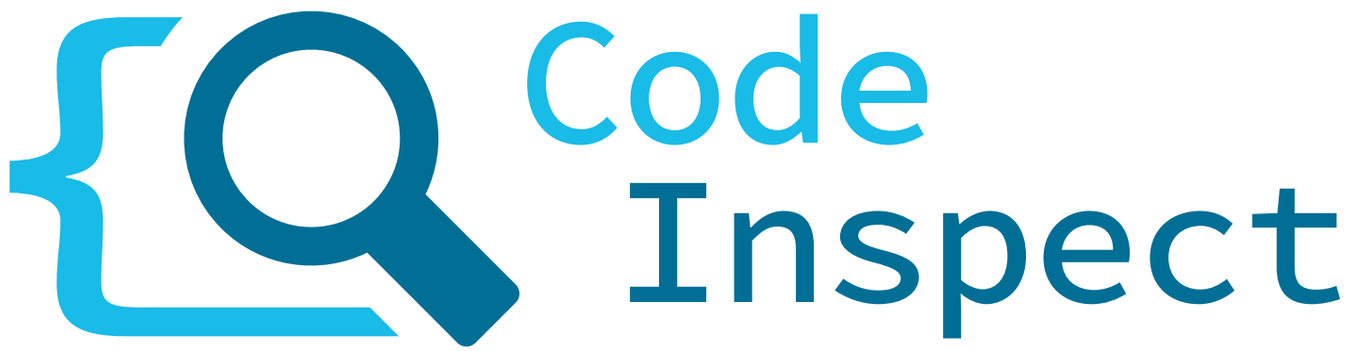
Live-Demo

Future Steps

Plugins

- New Plugins under development
- Easily add own analyses

How do I get this tool?



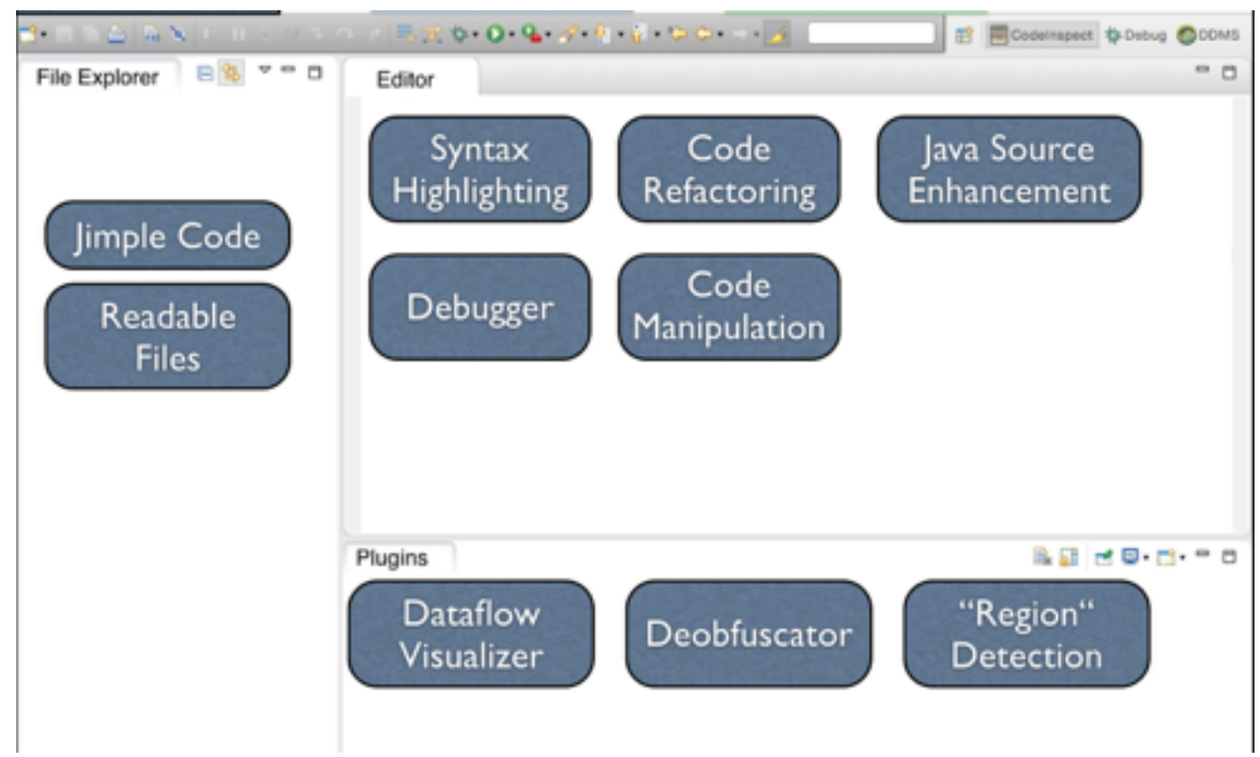
How to secure my app against piracy

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 illegaly Any ideas, experiences, comments you can share? That will be greatly appreciated Best regards

Source: stackoverflow.com

Code Inspect

A new Binary Analysis Framework for Android and Java Bytecode



Siegfried Rasthofer
Secure Software Engineering Group
Email: siegfried.rasthofer@cased.de
Blog: http://sse-blog.ec-spride.de
Website: http://sse.ec-spride.de
Twitter: @CodeInspect