Dalvik Executable (DEX) Trick: Hidex

Axelle Apvrille

Insomni'Hack, March 2014

FORTINET

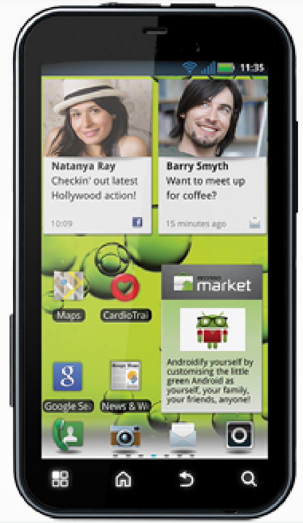
Who am i?

whoami

```perl
#!/usr/bin/perl -w # recently converting to Python!
my $self = {
    realname => ’Axelle Apvrille’,
    nickname => ’Crypto Girl’,
    twitter => ’@cryptax’,
    job => ’Malware Analyst and Researcher’,
    focus => ’Misc malware = mobile, Internet of Things...’,
    title => ’Senior’, # white hair
    company => ’Fortinet, FortiGuard Labs’,
    before => ’Security software eng.: protocols, crypto...’,
    languages => ’French, English, Hexadecimal :)’
};
```

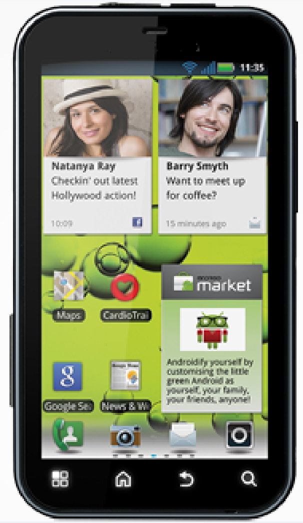
Quick Android background

Android mobile phone

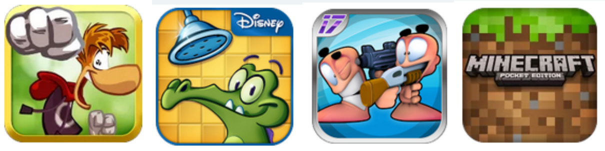


Quick Android background

Android mobile phone

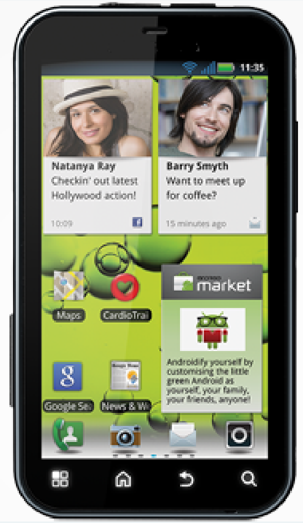

11:35
Natanya Ray
Checkin' out latest Hollywood action!
10:09
Barry Smyth
Want to meet up for coffee?
15 minutes ago
market
Androidify yourself by customising the little green Android as yourself, your family, your friends, anyone!
Maps
CardioTrai
Google Se
News & W

Applications: APK

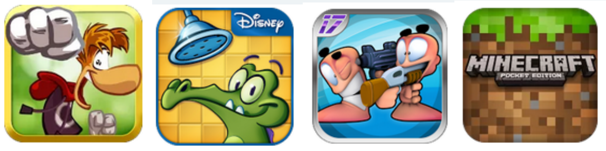


Quick Android background

Android mobile phone


11:35
Natanya Ray
Checkin' out latest Hollywood action!
10:09
Barry Smyth
Want to meet up for coffee?
15 minutes ago
market
Maps
CardioTrai
Androidify yourself by customising the little green Android as yourself, your family, your friends, anyone!
Google Se
News & W

Applications: APK



Inside the APK: DEX

Dalvik Executable with Dalvik bytecode

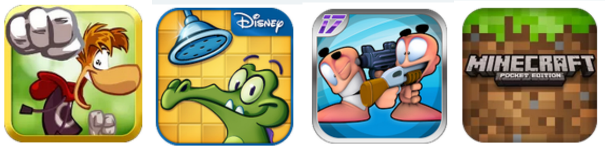
```
dex.035.V..d..$g
```

Quick Android background

Android mobile phone

11:35
Natanya Ray
Checkin' out latest Hollywood action!
10:09
Barry Smyth
Want to meet up for coffee?
15 minutes ago
market
Maps
CardioTrai
Androidify yourself by customising the little green Android as yourself, your family, your friends, anyone!
Google Se
News & W

Applications: APK



Inside the APK: DEX

Dalvik Executable with Dalvik bytecode

`dex.035.V..d..$g`

Inside the DEX

Classes, methods, fields, strings

`'bytes', '** I am Mr Hyde **', '<init>'...`

Part 1: Hiding a method

Hiding a method

Part 1: goal and demo

Goal

1. Write an app
2. Hide a given *method* of the app to disassemblers

Part 1: goal and demo

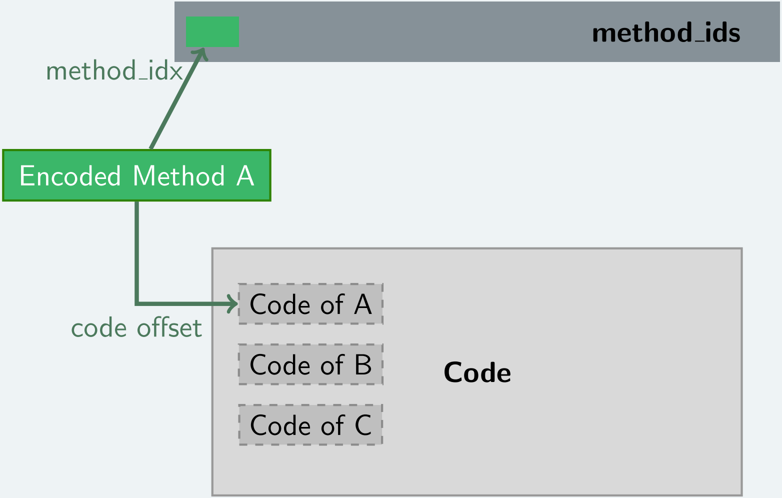
Goal

1. Write an app
2. Hide a given *method* of the app to disassemblers

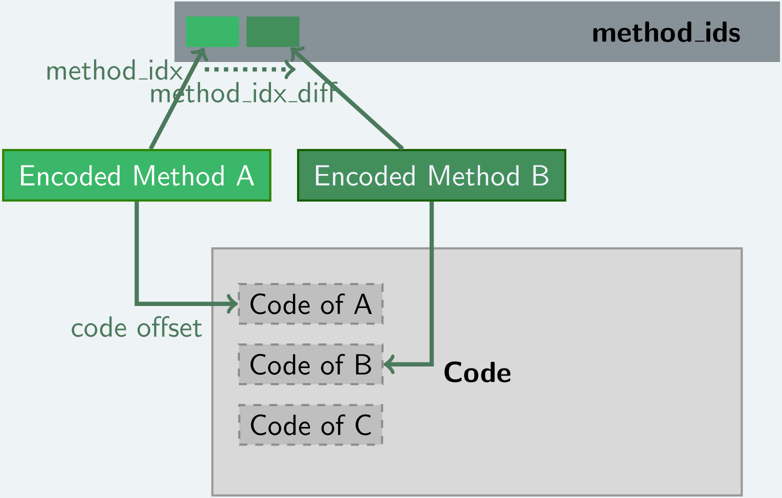
Demo - source code: `https://github.com/cryptax/dextools`

1. Example method **thisishidden()**:
   - Logs `"In thisishidden(): set mrhyde="` etc
   - Accesses file "identity" in app dir
   - Exact prototype: `public void thisishidden(boolean ismrhyde)`
2. Hide **thisishidden()**: Baksmali, dex2jar, Androguard, JEB, IDA Pro do not see it!
3. Back: reveal **thisishidden()**

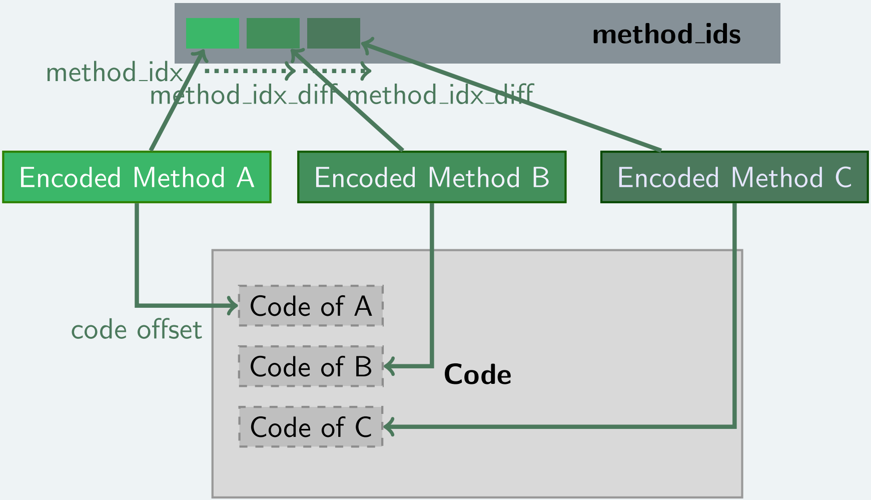
How it works / inside class_data items



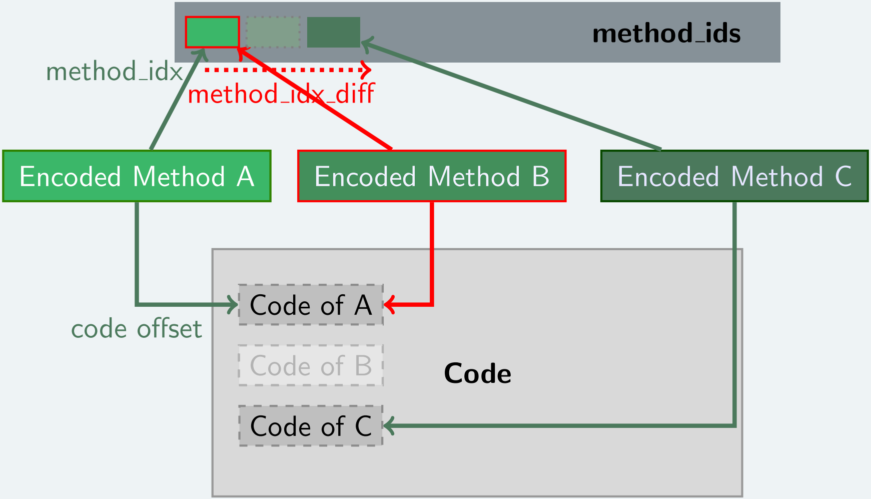
How it works / inside class_data items



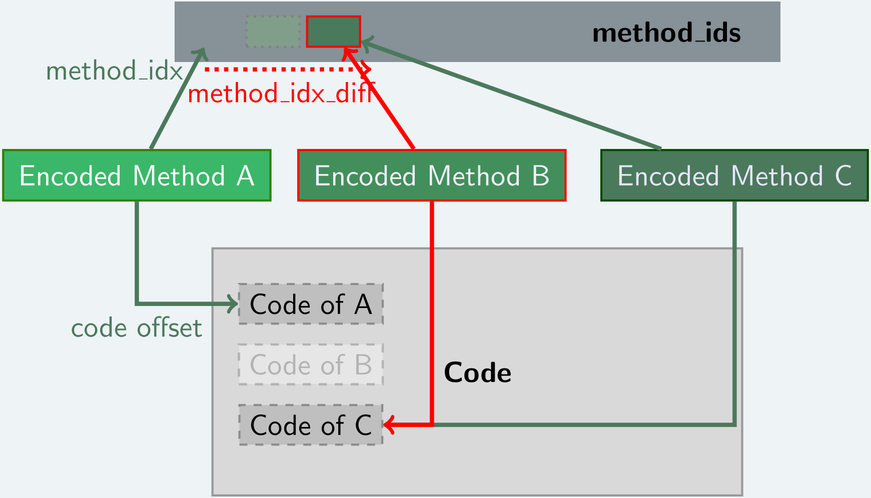
How it works / inside class_data items



How it works / inside class_data items



How it works / inside class_data items



Hiding - Advanced

Access flags

You *may* modify it

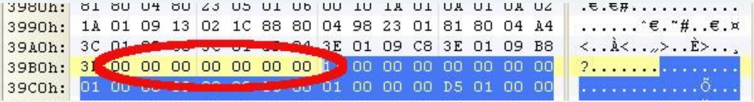
but must remain with the same category of methods:

- direct methods: static, private, constructors
- virtual methods: others ;)

Single method to hide?

In class_data_item, set *direct_methods_size* (or *virtual_methods_size*)

+ nullify encoded_method



```
3980h: 81 80 04 80 23 05 01 06 00 10 1A 01 0A 01 0A 02   .€.€#...........
3990h: 1A 01 09 13 02 1C 88 80 04 98 23 01 81 80 04 A4   ......ˆ€.˜#..€.¤
39A0h: 3C 01 09 C0 3C 01 09 84 3E 01 09 C8 3E 01 09 B8   <..À<..„>..È>..¸
39B0h: 3F 00 00 00 00 00 00 00 1[illegible] 00 00 00 00 00 00 00   ?...............
39C0h: 01 00 00 [illegible] 00 00 [illegible] 00 01 00 00 00 D5 01 00 00   .............Õ...
```

Re-build the APK

Build a valid DEX

- Compute the SHA-1 of the new DEX → Write to header
- Compute the checksum of the new DEX → Write to header
- hidex or dexrehash in https://github.com/cryptax/dextools

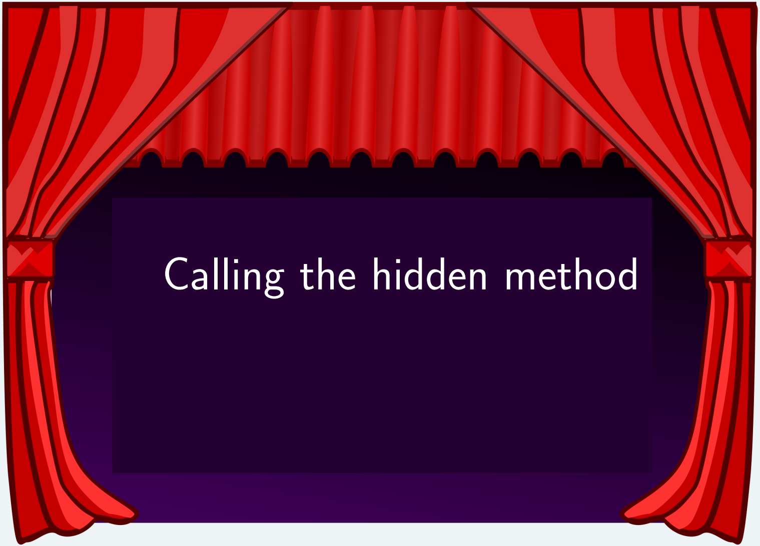
Re-package: easy

- In original APK, replace DEX with new one
- Zip, sign package (jarsigner)

Did you know?

You can write a .dex 'manually' using Yasm - thanks @angealbertini
Hello World: 695 bytes

Part 2: calling the hidden method - PoC

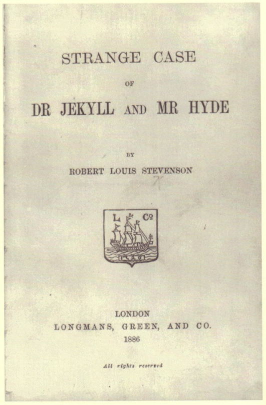


Calling the hidden method

Part 2: PoC

calling `thisishidden()`

- The method is hidden to disassemblers
- ... but it can be run!



STRANGE CASE

OF

DR JEKYLL AND MR HYDE

BY

ROBERT LOUIS STEVENSON

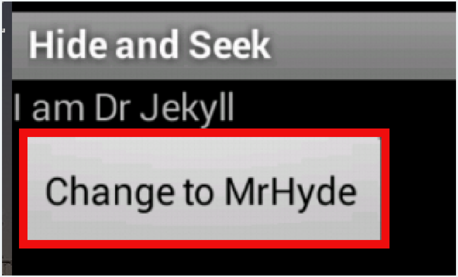
LONDON
LONGMANS, GREEN, AND CO.
1886

All rights reserved

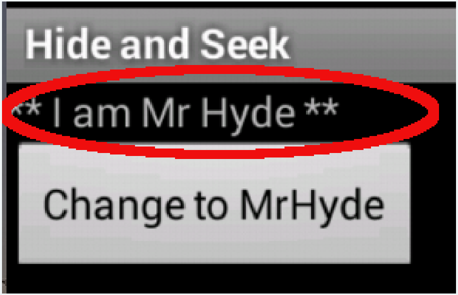
The strange case of Dr Jekyll and Mr Hyde – R. Stevenson

- Split personalities: Dr Jekyll or Mr Hyde
- Only one way to change into MrHyde: call `thisishidden()`
- Current personality displayed in main activity

Part 2: Demo



I am Dr Jekyll

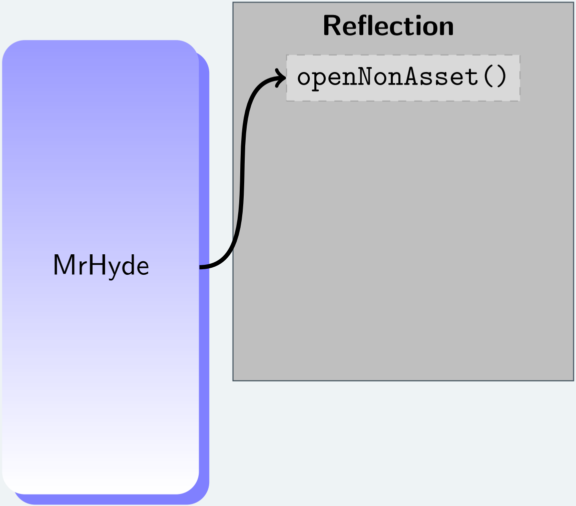


** I am Mr Hyde **

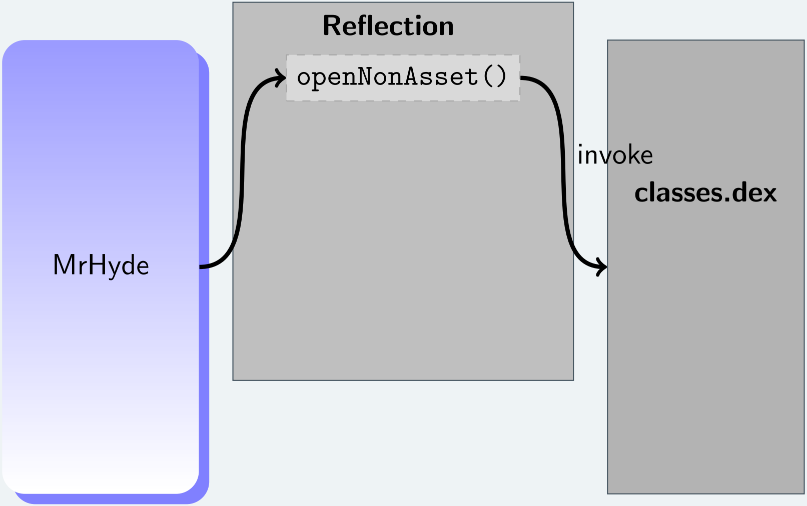
```
I/HideAndSeek(  851): invoking thisishidden() with arg=true
I/HideAndSeek(  851): In thisishidden(): set mrhyde=true
I/HideAndSeek(  851): thisishidden(): context=android.app.Applic
I/HideAndSeek(  851): thisishidden(): dir=/data/data/com.fortigu
I/HideAndSeek(  851): thisishidden(): file: /data/data/com.forti
I/HideAndSeek(  851): thisishidden(): done
```

Implementation... technical but illustrated ;)

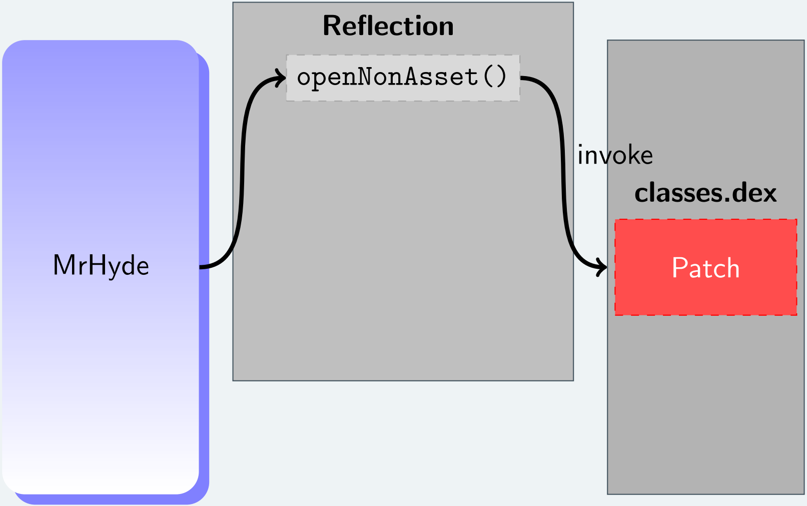
Implementation... technical but illustrated ;)



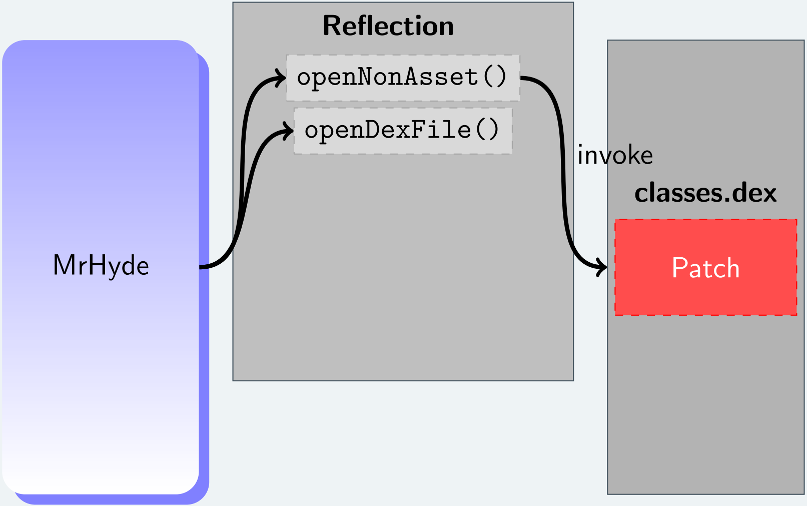
Implementation... technical but illustrated ;)



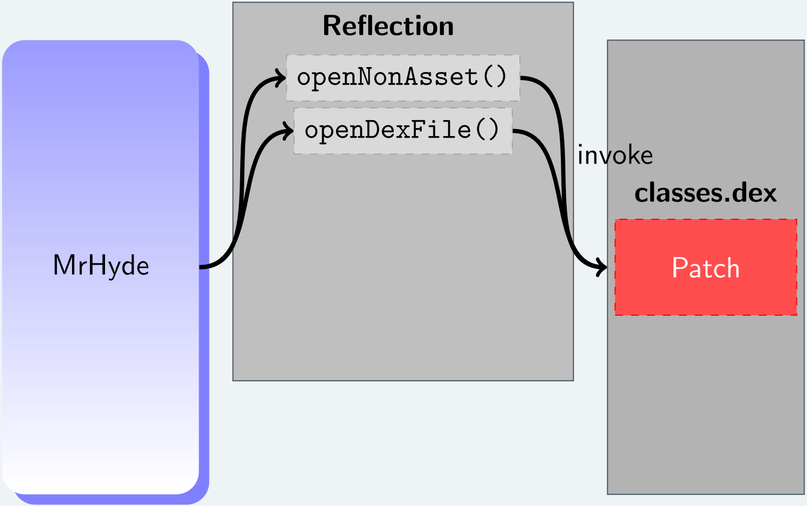
Implementation... technical but illustrated ;)



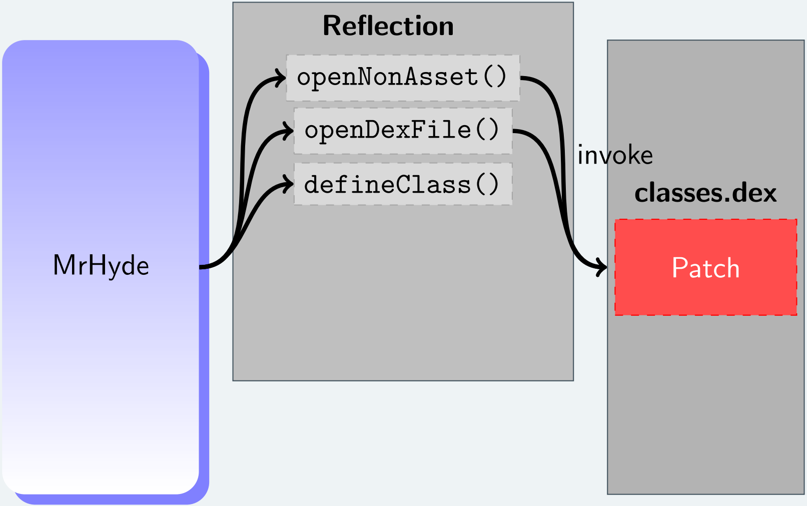
Implementation... technical but illustrated ;)



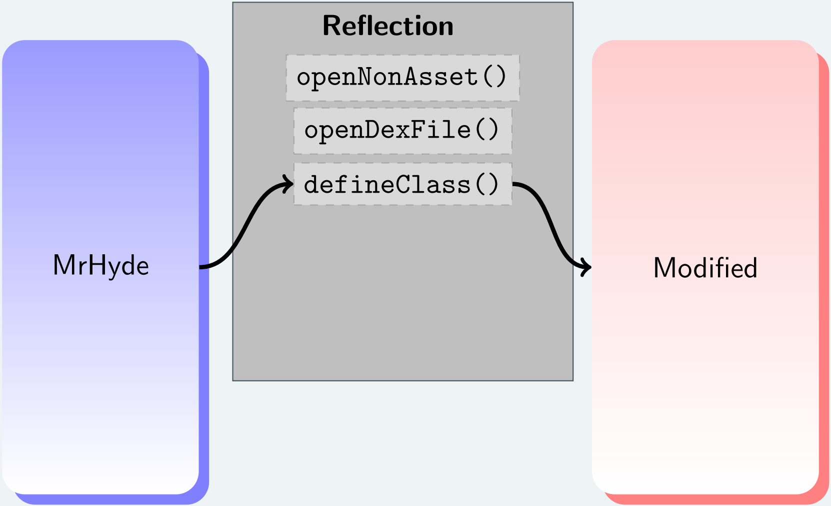
Implementation... technical but illustrated ;)



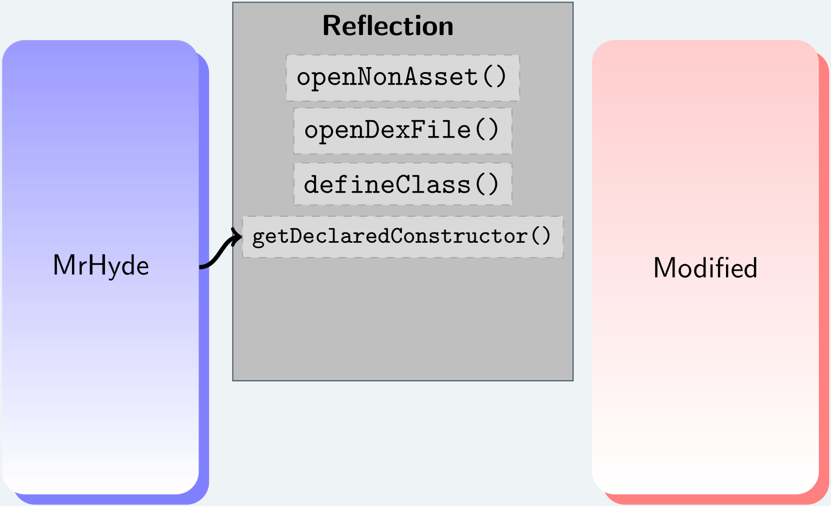
Implementation... technical but illustrated ;)



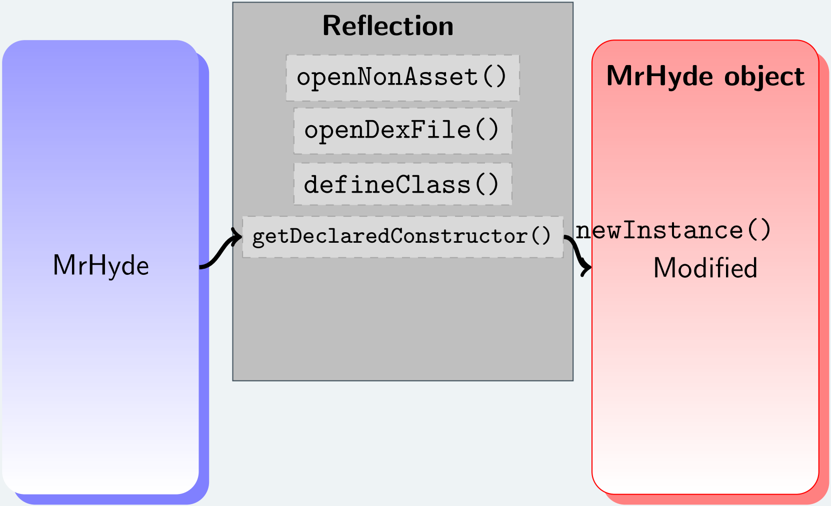
Implementation... technical but illustrated ;)



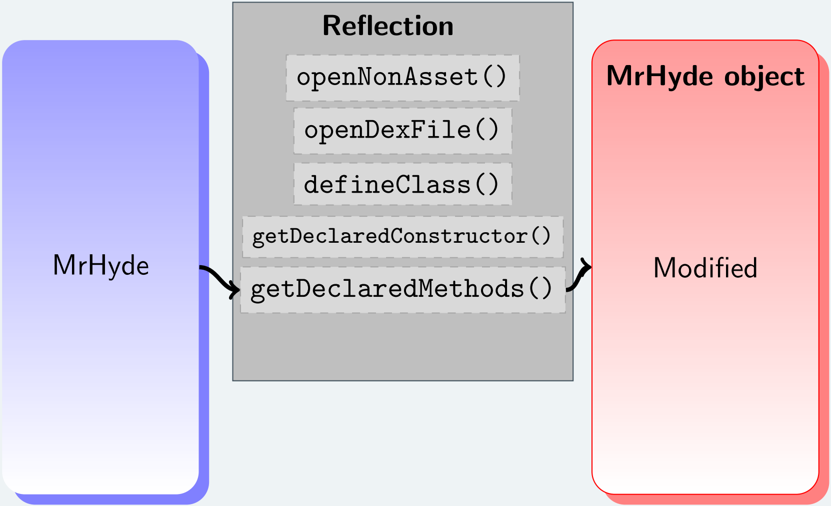
Implementation... technical but illustrated ;)



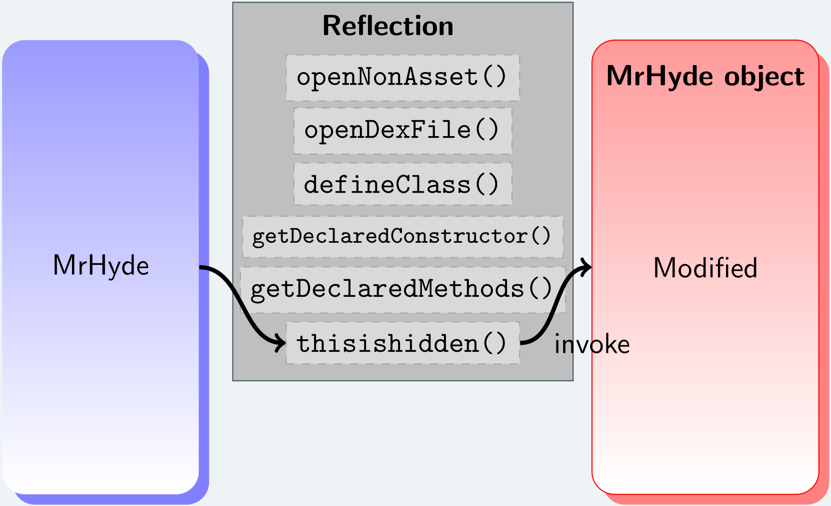
Implementation... technical but illustrated ;)



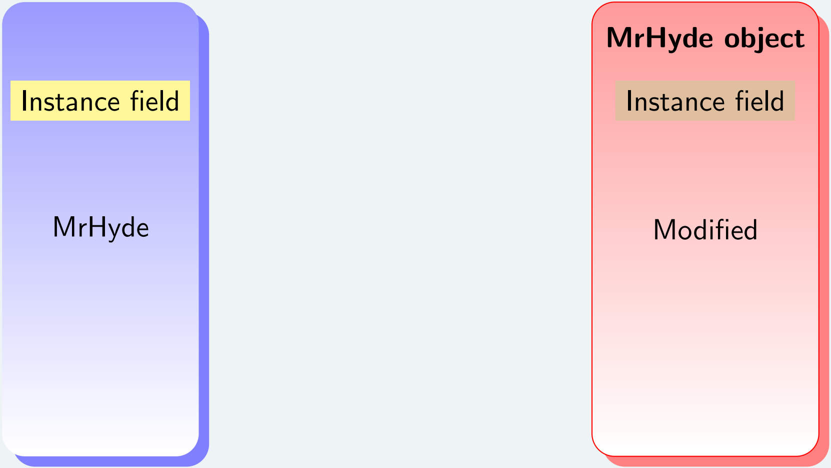
Implementation... technical but illustrated ;)



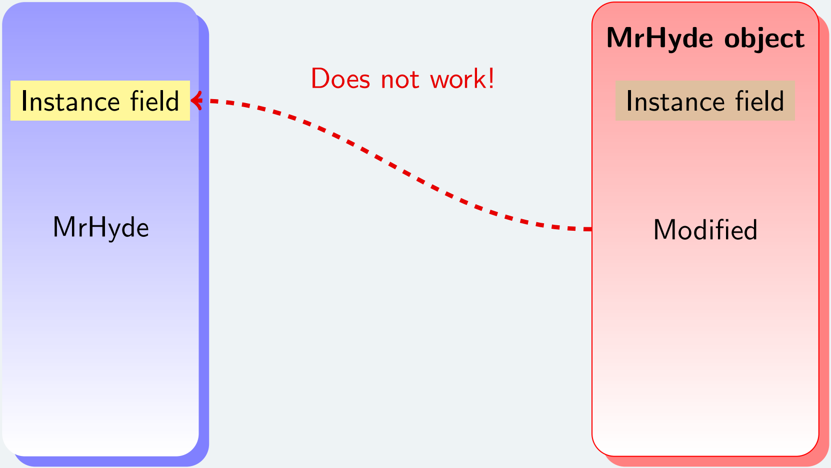
Implementation... technical but illustrated ;)



Implementation... technical but illustrated ;)



Implementation... technical but illustrated ;)



Instance field

MrHyde

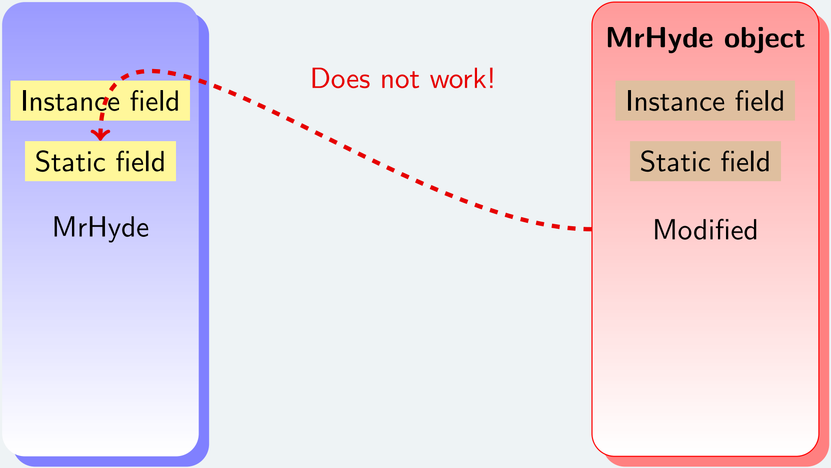
Does not work!

MrHyde object

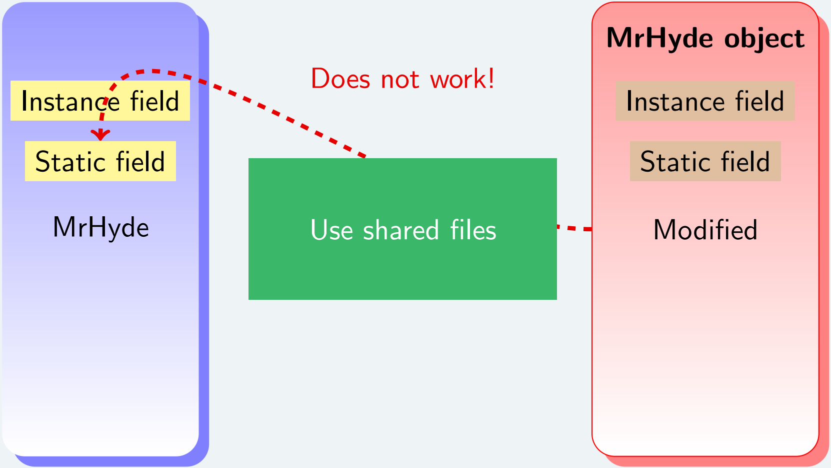
Instance field

Modified

Implementation... technical but illustrated ;)



Implementation... technical but illustrated ;)



Status

It works :)

- Dex manipulation: working on all versions
- Calling hidden method: $< 4.4.2$.
  Prototypes for `openDexFile` and `defineClass` changed
  - minor modif for defineClass
  - openDexFile no longer works on byte[]

  Work in progress: looks feasible.
- Android Security Team notified in June 2013

Detecting hidden methods

How? Use '--detect' option in hidex.pl

```
$ ./hidex.pl --input classes.dex | grep -B 1 "WARNING"
$ ./nonreferenced-methods.sh classes.dex
```

- null code offset: just a hint
- null or negative method_idx_diff
- code offset or method_id already referenced
- method_id never referenced: beware, there are valid methods not implemented in the DEX.

Something is wrong with openNonAsset()

```
Class: Lcom../MrHyde; Method: openNonAsset Position: 0x2C99
WARNING: Code offset 0x13D8 ALREADY REFERENCED
Class: Lcom../MrHyde; Method: openNonAsset Position: 0x2C99
WARNING: method_idx_diff <= 0 detected
Class: Lcom../MrHyde; Method: openNonAsset Position: 0x2C99
WARNING: METHOD_IDX 22 ALREADY REFERENCED
```

Non Referenced Methods Detection results

```
Method Landroid/annotation/SuppressLint;->value is never used
Method Landroid/annotation/TargetApi;->value is never used
```

→ abstract methods indeed never used.

```
Method Lcom/fortiguard/hideandseek/MrHyde;->thisishidden is never used
```

→ hidden method!

```
Method Ljava/io/File;->delete is never used
Method Ljava/io/File;->exists is never used
Method Ljava/io/FileOutputStream;-><init> is never used
Method Ljava/io/FileOutputStream;->close is never used
Method Ljava/io/FileOutputStream;->write is never used
Method Ljava/lang/Object;->toString is never used
```

→ methods used only by the hidden method!

Reversing the hidden method

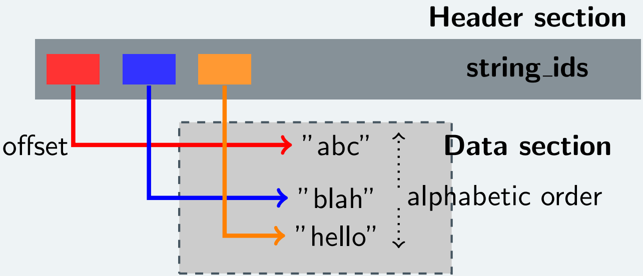
Fixing

- Implement method_idx_diff check?
- Implement code or method_id duplicate references check?

Working around

- Unpatch the DEX: `hidex.pl`
- Disassemble bytecode at a given location: `androdis.py`

How about hiding strings?



- **No idx_diff**. No chaining.
- **String as byte []** → not in strings list but visible in hex (e.g strings Unix command)
- **Encode, encrypt, obfuscate string** → possible - nothing new.

Thank You !

Where's the source code?

`https://github.com/cryptax/dextools`

FortiGuard Labs

Follow us on twitter: **@FortiGuardLabs**
or on our blog http://blog.fortinet.com
Me: **@cryptax** or `aapvrille` at `fortinet` dot `com`

Useless/shameless/stupid speaker challenge

I told @angealbertini I could keep it under 20 slides ;)

Are those PowerPoint slides? No way! It's LaTeX+ TikZ + Beamer + Lobster