Android reverse-engineering

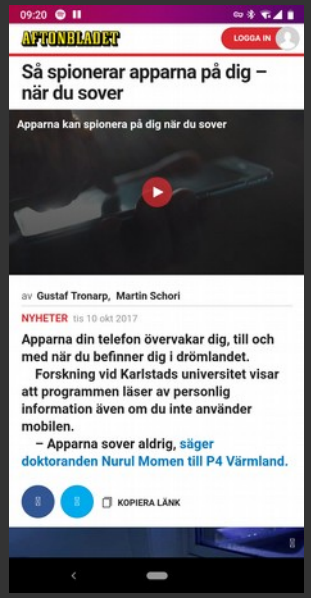
review and modify closed source apps

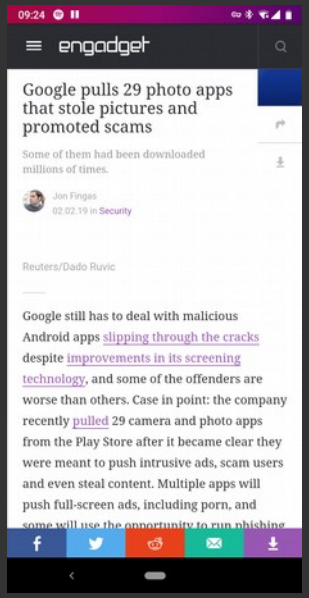
Magnus, Tech-Evangelist @ 0xFF

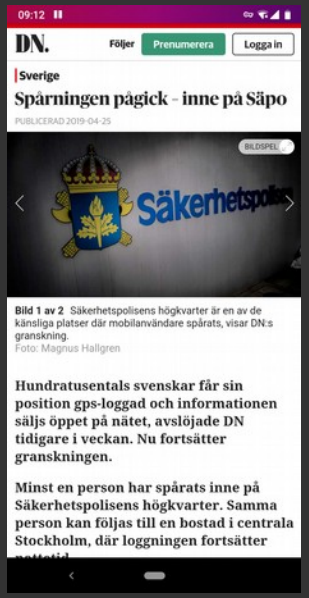
Why?

review/audit
patch/modify
exploit


DAGENS NYHETER.
Nyheter
Ekonomi
Kultur
Sverige
Världen
Politik
Fakta i frågan
Sverige
Erbjudandet: Spåra en halv miljon mobiler i realtid
UPPDATERAD 2019-04-24 PUBLICERAD 2019-04-23
Hundratusentals svenskar blir spårade via appar i mobilen.
02:02. DN avslöjar: Hundratusentals vanliga svenskar gps-spåras dygnet runt genom sina mobiler – av appar som sedan säljer informationen. Björn Sjögren är en av de som övervakats utan att veta om det.
DN:s reportrar erbjöds att spåra hundratusentals svenskars rörelsemönster via mobilerna. I ett samtal lockar en säljare med att de kan följas med bara några sekunder


AFTONBLADET
LOGGA IN
Så spionerar apparna på dig – när du sover
Apparna kan spionera på dig när du sover
av Gustaf Tronarp, Martin Schori
NYHETER tis 10 okt 2017
Apparna din telefon övervakar dig, till och med när du befinner dig i drömlandet.
Forskning vid Karlstads universitet visar att programmen läser av personlig information även om du inte använder mobilen.
– Apparna sover aldrig, säger doktoranden Nurul Momen till P4 Värmland.
KOPIERA LÄNK


engadget
Google pulls 29 photo apps that stole pictures and promoted scams
Some of them had been downloaded millions of times.
Jon Fingas
02.02.19 in Security
Reuters/Dado Ruvic
Google still has to deal with malicious Android apps slipping through the cracks despite improvements in its screening technology, and some of the offenders are worse than others. Case in point: the company recently pulled 29 camera and photo apps from the Play Store after it became clear they were meant to push intrusive ads, scam users and even steal content. Multiple apps will push full-screen ads, including porn, and


DN.
Följer
Prenumerera
Logga in
Sverige
Spårningen pågick – inne på Säpo
PUBLICERAD 2019-04-25
BILDSPEL
Säkerhetspolis
Bild 1 av 2 Säkerhetspolisens högkvarter är en av de känsliga platser där mobilanvändare spårats, visar DN:s granskning.
Foto: Magnus Hallgren
Hundratusentals svenskar får sin position gps-loggad och informationen säljs öppet på nätet, avslöjade DN tidigare i veckan. Nu fortsätter granskningen.
Minst en person har spårats inne på Säkerhetspolisens högkvarter. Samma person kan följas till en bostad i centrala Stockholm, där loggningen fortsätter

Disclaimer

APK

Manifest

Resources

Code

Manifest
Resources
Code

Manifest
Resources
Code

Activities
Services
Content providers
Intents

demo

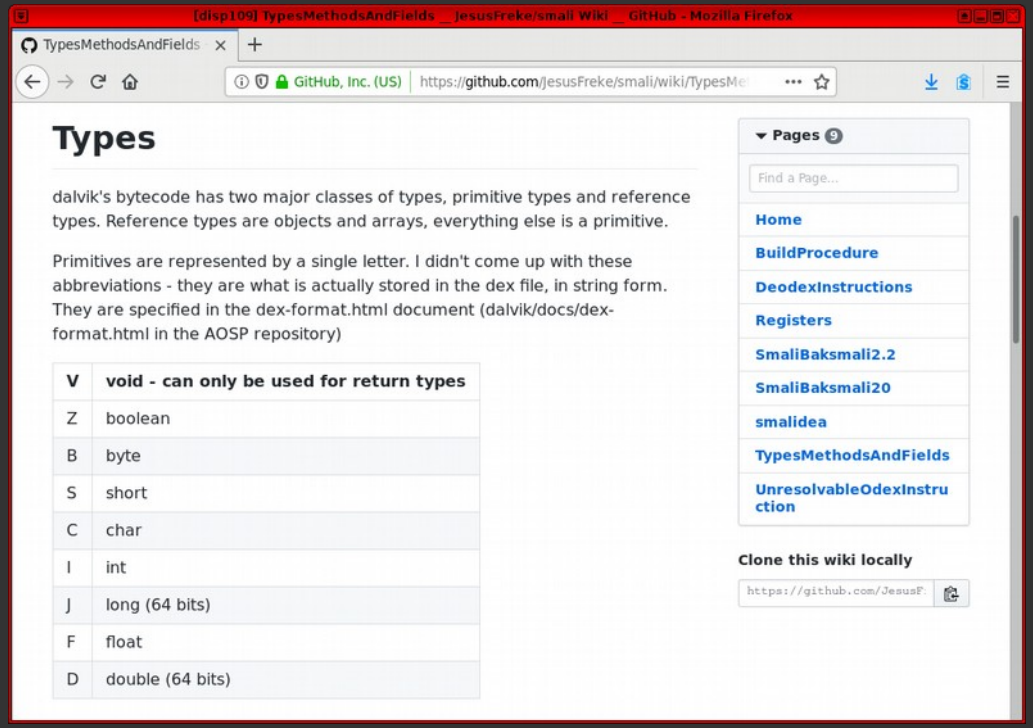
Java/Kotlin > DEX > ~~JIT/Dalvik~~ > ARM/x86/etc

Java/Kotlin > DEX > OAT > ART > ARM/x86/etc

DEX > Smali

```
.class public LHelloWorld;

.super Ljava/lang/Object;

.method public static main([Ljava/lang/String;)V
    .registers 2

    sget-object v0, Ljava/lang/System;->out:Ljava/io/PrintStream;

    const-string v1, "Hello World!"

    invoke-virtual {v0, v1}, Ljava/io/PrintStream;->println(Ljava/
lang/String;)V

    return-void
.end method
```

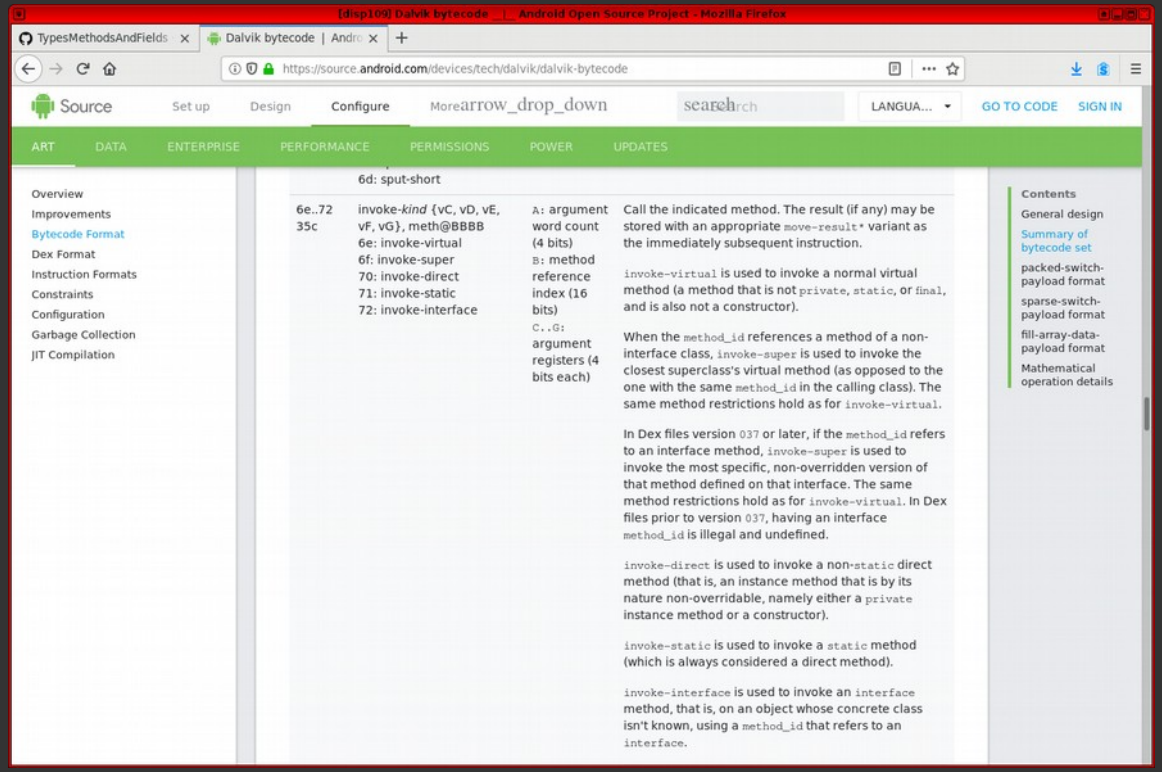
Data-types



https://github.com/JesusFreke/smali/wiki/TypesMethodsAndFields

0xFF

Instructions



https://source.android.com/devices/tech/dalvik/dalvik-bytecode

0xFF

Smali registers

v0, v1, v2... - local registers
p0, p1, p2... - method argument alias

(all 32-bit, so how to pass a 64-bit Long?)

```
.class public LHelloWorld;

.super Ljava/lang/Object;

.method public static main([Ljava/lang/String;)V
    .registers 2

    sget-object v0, Ljava/lang/System;->out:Ljava/io/PrintStream;

    const-string v1, "Hello World!"

    invoke-virtual {v0, v1}, Ljava/io/PrintStream;->println(Ljava/
lang/String;)V

    return-void
.end method
```

Obfuscation

```
Ball.getColor() == a.a()
```

demo

debugging smali

grep is your friend

grep is your friend

```
grep -inr facebook.com --include=*.smali
```

```
-i ignores character case
-n display line numbers
-r recursive, search sub folders
--include=*.smali only search files matching
--color=always add coloring
```

grep is your friend – Trackers

facebook *google.com* *firebase*

urbanairship *crashlytics* *bugfender*

*track** *analytic** *ads*

grep is your friend – Privacy intrusive API calls

QueryIntentActivities *getRunningAppProcesses*

ActivityManager *PackageManager* *WifiManager*

SensorManager *BluetoothAdapter*

Address *LocationManager*

TelephonyManager *AdvertisingIdClient*

grep is your friend – File I/O

file *read* *write*

directory *sdcard*

document

grep is your friend – Net I/O

http *http:*

connect *socket* *uri* *address*

post *.com/.net* *loadUrl*

grep is your friend – Scary stuff

loadLibrary *native*

install

addJavaScriptInterface

demo

OWASP Mobile Top 10

Exploiting GoatDroid

Tools used in this talk

(free and open source)

ADB

ApkTool

uber-apk-signer

ApkStudio

Idea

Ideasmali

Profiling tools
(root required)

Frida
Introspy
Xposed

Automated tools

Mobile Security Framework (MobSF)

Quick Android Review Kit (QARK)

Drozer

Resources

Smali/Smalidea
https://github.com/JesusFreke/smali/

Dalvik instructions
https://source.android.com/devices/tech/dalvik/dalvik-bytecode

ADB
https://developer.android.com/studio/releases/platform-tools

ApkStudio
https://github.com/vaibhavpandeyvpz/apkstudio

OWASP Mobile Top 10
https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

Thank you!

magnus@0xFF.se
@0xFFse https://0xff.se/