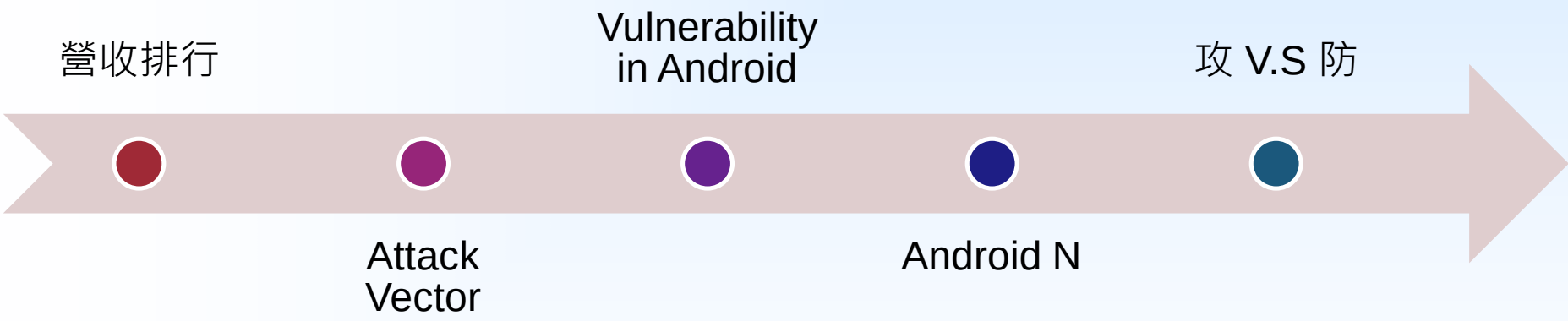
淺談Android APP之攻防思維

江啟賓　Ci-Bin Jiang

成功大學電腦與通信工程博士

Outline


營收排行
Attack Vector
Vulnerability in Android
Android N
攻 V.S 防

App 營收排行

Top Apps

iOS & Google Play Combined - Overall - Taiwan - May 2016

#	By Downloads		Company
1	LINE (ライン)	▲1	LINE (ライン)
2	SNOW	▲38	NAVER
3	Facebook	▲2	Facebook
4	Facebook Messenger	▲3	Facebook
5	Shopee (蝦皮拍賣)	▲4	Garena Online
6	Lucky KoKo (五元寶寶)	▲21	5 Dollars Trading
7	Ce Three Kingdoms (策三国)		Digital Sky Entertainment (成都数字天空科技)
8	LINE Manga (LINE マンガ)		LINE (ライン)
9	Elsword (艾尔战记)	New Release	Kunlun (昆仑万维)
10	Clean Master (猎豹清理大师)	▲3	Cheetah Mobile (猎豹移动)

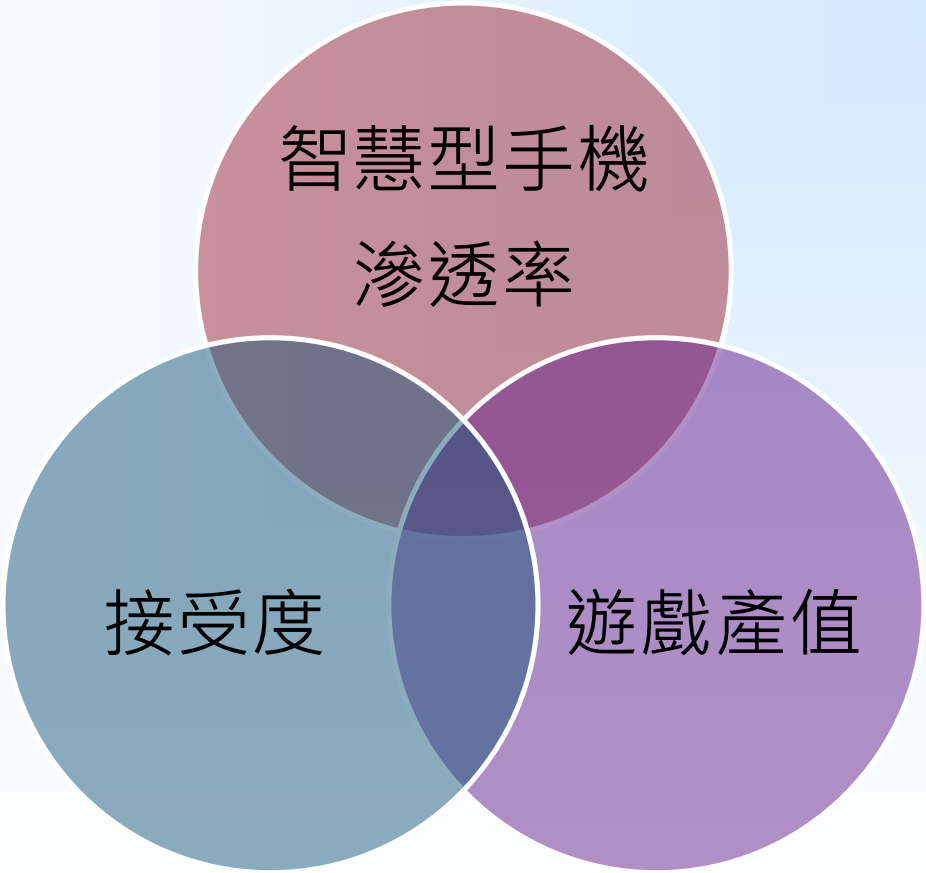
#	By Revenue		Company
1	LINE (ライン)	-	LINE (ライン)
2	Clash of Kings	-	Elex Technology (智明星通)
3	Loong Craft (六龙争霸)	-	37Wan EFUN (易幻) Tencent (腾讯)
4	Seven Knights (세븐나이츠)	-	Netmarble (넷마블)
5	MARVEL Future Fight	▲32	Netmarble (넷마블)
6	The King of Fighters' 98 Ultimate Match (拳皇98终极之战)	▲1	Tencent (腾讯) Smart Alec (阿達馬數位) OurPalm (掌趣)
7	Clash Royale	▼2	Supercell
8	Tower of Saviors (神魔之塔)	▲5	Mad Head
9	Everybody's Marble (모두의마블)	▲2	Netmarble (넷마블) LINE (ライン) Tencent (腾讯)
10	Clash of Clans	▼2	Supercell

Related Report:
App Annie Index Reports

Source: App Annie Intelligence

App Annie: http://cn.blog.appannie.com/taiwan-next-billion-dollar-market/
App Annie Rank: https://www.appannie.com/indexes/all-stores/rank/overall/?month=2016-05-01&country=TW

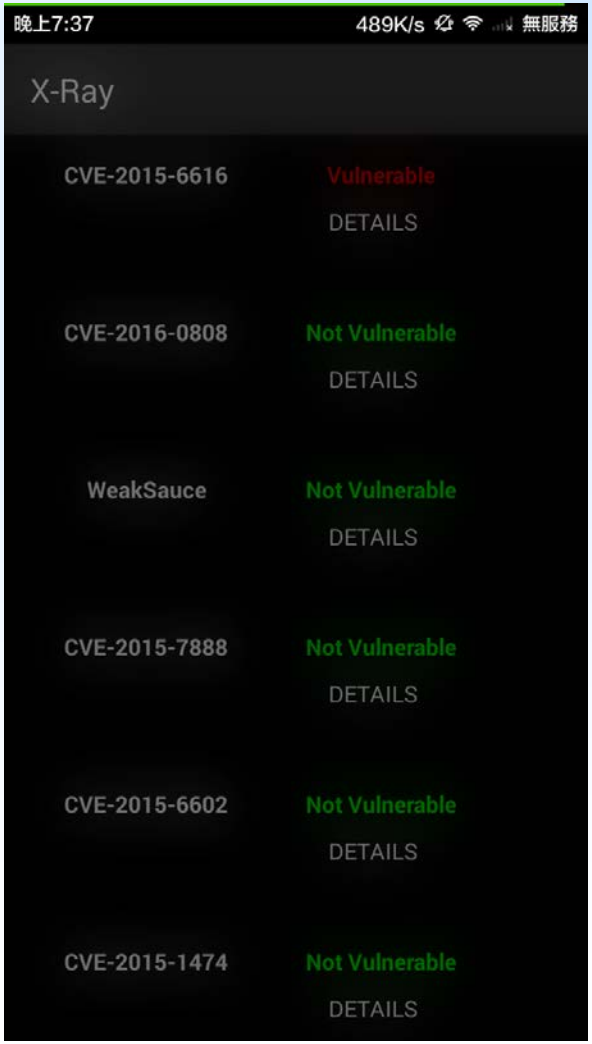
台灣為什麼特別？



APP Attack Vector

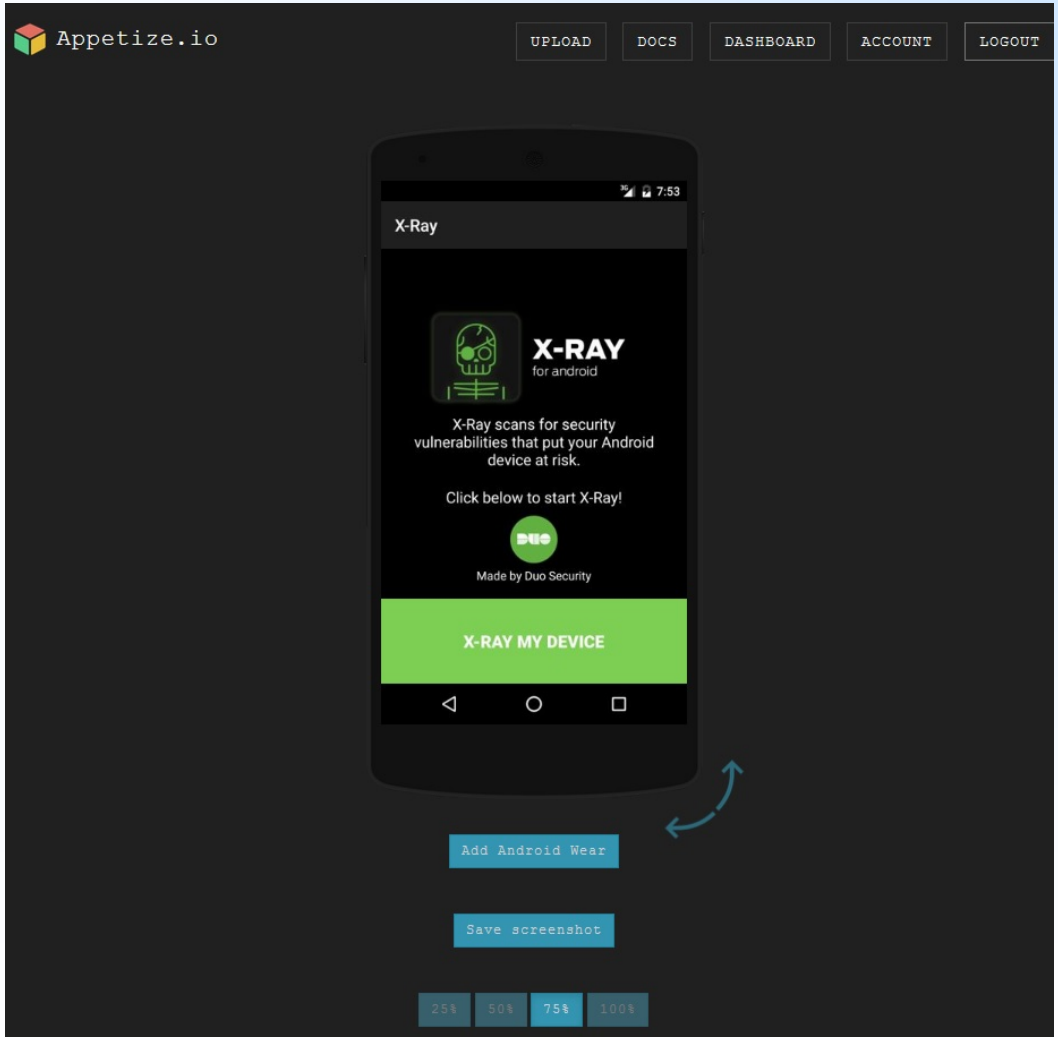
- Sensitive Data Storage
- No Encryption / Weak Encryption
- Improper SSL Validation
- Config Manipulation
- Dynamic Runtime Injection
- Unintended Permissions
- Escalated Privileges
- Access to Device / User Info

Android Vulnerability Scanner



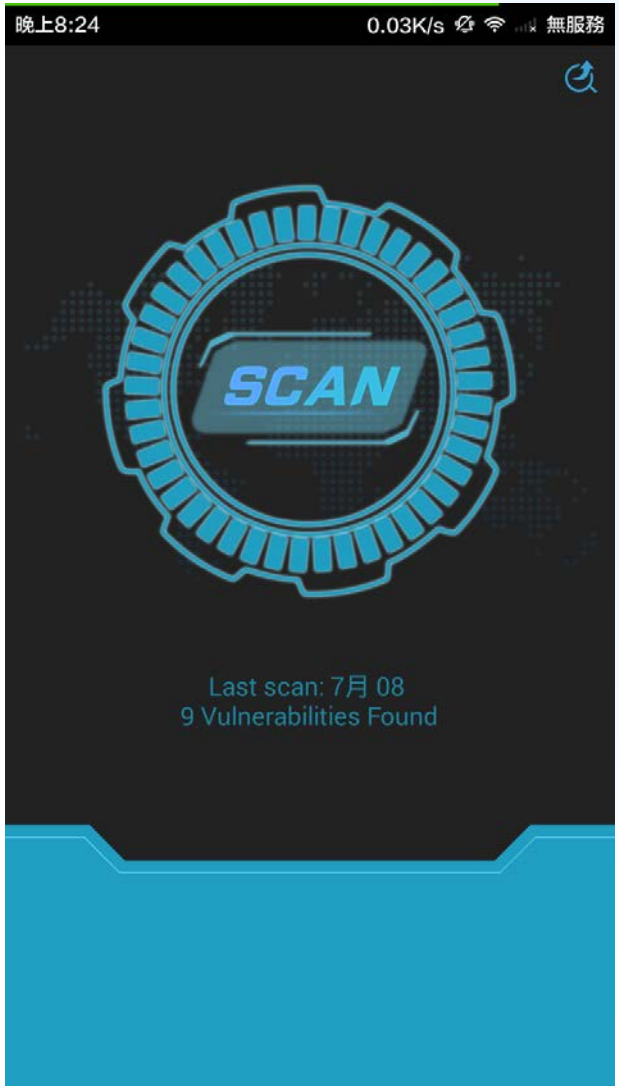
X-Ray 2.0: https://labs.duo.com/xray

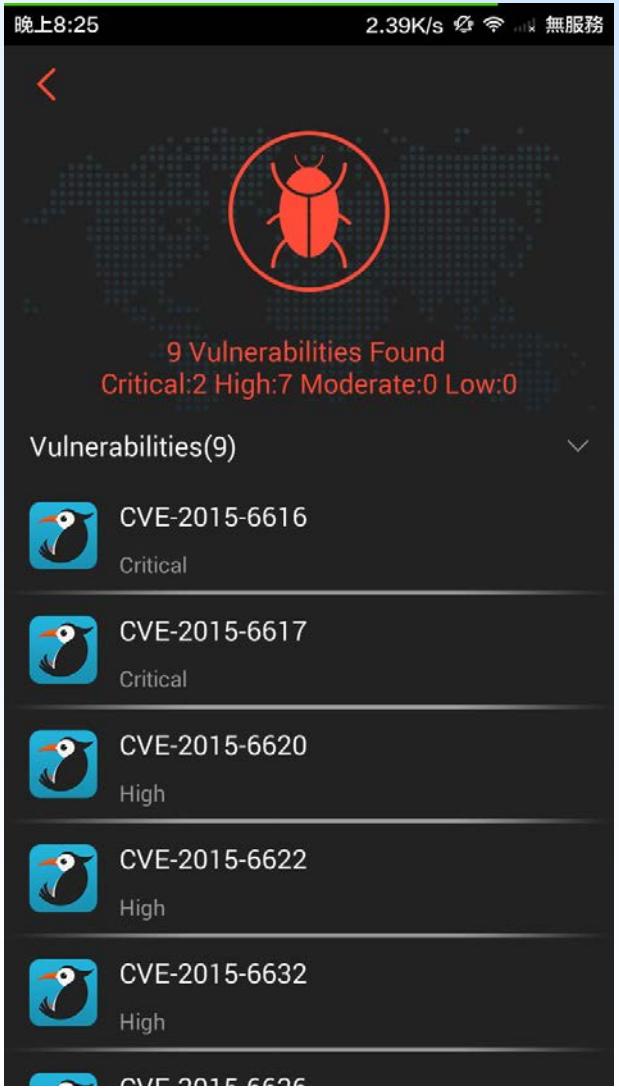
Apps in the Browser



Appetize: https://appetize.io

Woodpecker in Android





Android-CVE

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2016-4477	19		DoS +Priv	2016-05-09	2016-05-10	4.4	None	Local	Medium	Not required	Partial	Partial	Partial
wpa_supplicant 0.4.0 through 2.5 does not reject \n and \r characters in passphrase parameters, which allows local users to trigger arbitrary library loading and consequently gain privileges, or cause a denial of service (daemon outage), via a crafted (1) SET, (2) SET_CRED, or (3) SET_NETWORK command.														
2	CVE-2016-2500	200		+Info	2016-06-12	2016-06-15	4.3	None	Remote	Medium	Not required	Partial	None	None
Activity Manager in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-06-01 does not properly terminate process groups, which allows attackers to obtain sensitive information via a crafted application, aka internal bug 19285814.														
3	CVE-2016-2499	200		+Info	2016-06-12	2016-06-14	4.3	None	Remote	Medium	Not required	Partial	None	None
AudioSource.cpp in libstagefright in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-06-01 does not initialize certain data, which allows attackers to obtain sensitive information via a crafted application, aka internal bug 27855172.														
4	CVE-2016-2498	200		Bypass +Info	2016-06-12	2016-06-14	4.3	None	Remote	Medium	Not required	Partial	None	None
The Qualcomm Wi-Fi driver in Android before 2016-06-01 on Nexus 7 (2013) devices allows attackers to bypass intended data-access restrictions via a crafted application, aka internal bug 27777162.														
5	CVE-2016-2496	264			2016-06-12	2016-06-14	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
The Framework UI permission-dialog implementation in Android 6.x before 2016-06-01 allows attackers to conduct tapjacking attacks and access arbitrary private-storage files by creating a partially overlapping window, aka internal bug 26677796.														
6	CVE-2016-2495	20		DoS	2016-06-12	2016-06-14	7.1	None	Remote	Medium	Not required	None	None	Complete
SampleTable.cpp in libstagefright in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-06-01 allows remote attackers to cause a denial of service (device hang or reboot) via a crafted file, aka internal bug 28076789.														
7	CVE-2016-2494	264		+Priv	2016-06-12	2016-06-14	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
Off-by-one error in sdcard/sdcard.c in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-06-01 allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 28085658.														
8	CVE-2016-2493	264		+Priv	2016-06-12	2016-06-14	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
The Broadcom Wi-Fi driver in Android before 2016-06-01 on Nexus 5, Nexus 6, Nexus 6P, Nexus 7 (2013), Nexus Player, and Pixel C devices allows attackers to gain privileges via a crafted application, aka internal bug 26571522.														
9	CVE-2016-2492	264		+Priv	2016-06-12	2016-06-16	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
The MediaTek power-management driver in Android before 2016-06-01 on Android One devices allows attackers to gain privileges via a crafted application, aka internal bug 28085410.														
10	CVE-2016-2491	264		+Priv	2016-06-12	2016-06-14	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
The NVIDIA camera driver in Android before 2016-06-01 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 27556408.														
11	CVE-2016-2490	264		+Priv	2016-06-12	2016-06-14	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
The NVIDIA camera driver in Android before 2016-06-01 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 27533373.														
12	CVE-2016-2489	264		+Priv	2016-06-12	2016-06-14	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
The Qualcomm video driver in Android before 2016-06-01 on Nexus 5, 5X, 6, and 6P devices allows attackers to gain privileges via a crafted application, aka internal bug 27407629.														
13	CVE-2016-2488	264		+Priv	2016-06-12	2016-06-14	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
The Qualcomm camera driver in Android before 2016-06-01 on Nexus 5, 5X, 6, 6P, and 7 (2013) devices allows attackers to gain privileges via a crafted application, aka internal bug 27600832.														
14	CVE-2016-2487	20		+Priv	2016-06-12	2016-06-13	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
libstagefright in mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-06-01 allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOrSystem access, aka internal bug 27833616.														

Reference: http://www.cvedetails.com/vulnerability-list/vendor_id-1224/product_id-19997/Google-Android.html

Android N Security

網路安全設定

- 自訂信任錨點
- 僅偵錯覆寫
- 退出明碼流量
- 憑證關聯

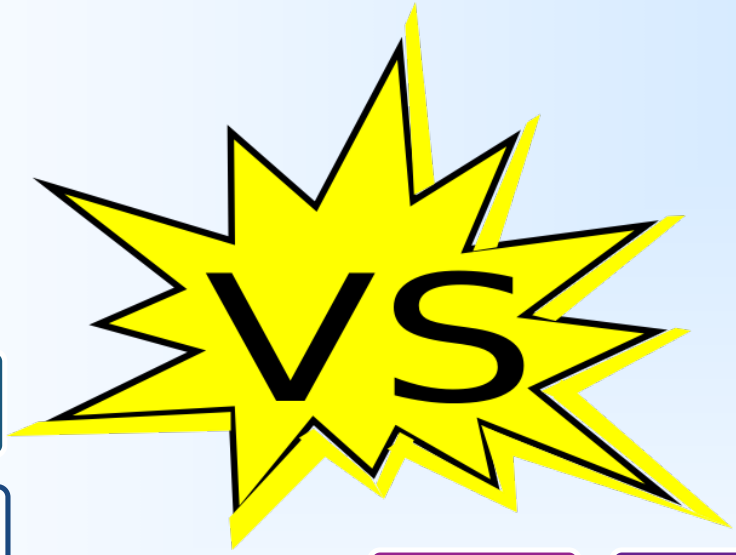
APK 簽章配置第 2 版

- 全檔案簽章配置，改善驗證速度並增強完整性

限定範圍目錄存取

- 存取特定外部儲存空間目錄

攻 V.S. 防



- 靜態分析
  - 反編譯 apk
  - Smali 檔
  - Dex檔結構
  - Jar檔
- App 破解
  - 動態分析
    - Debugger
    - 模擬器
  - 對抗反編譯
    - 反編譯工具
    - Dex2jar
  - 反動態分析
    - Trace檢查
- 靜態技術
  - 代碼混淆
  - NDK保護
  - 加殼保護
  - JNI佈密鑰
- 重新編譯
  - 檢查簽名
  - 完整性保護

Code Analysis

反編譯 apk 檔

- 主要的 Activity
- Application 類

Smali 檔 – baksmali產生

Dex 檔結構 – Dalvik字串碼

Jar檔 – dex2jar產生

Tools

- Androguard、IDA pro、dex2jar、jd-gui、apktool

反編譯apk檔

APP名稱

- META-INF
- res
- AndroidManifest.xml
- classes.dex
- resources.arsc
- smali

反編譯apk檔

Online apk檔：http://www.ludaima.cn/android.html

Android apk decompiler：http://www.decompileandroid.com

Smali檔格式

.field 權限 修飾關鍵字 字串名：字串類型

```
# instance fields
.field public final a:Landroid/content/Context;

.field public final b:Ljp/naver/line/android/util/b;
```

Smali檔格式

.method 訪問權限 修飾子 方法名稱

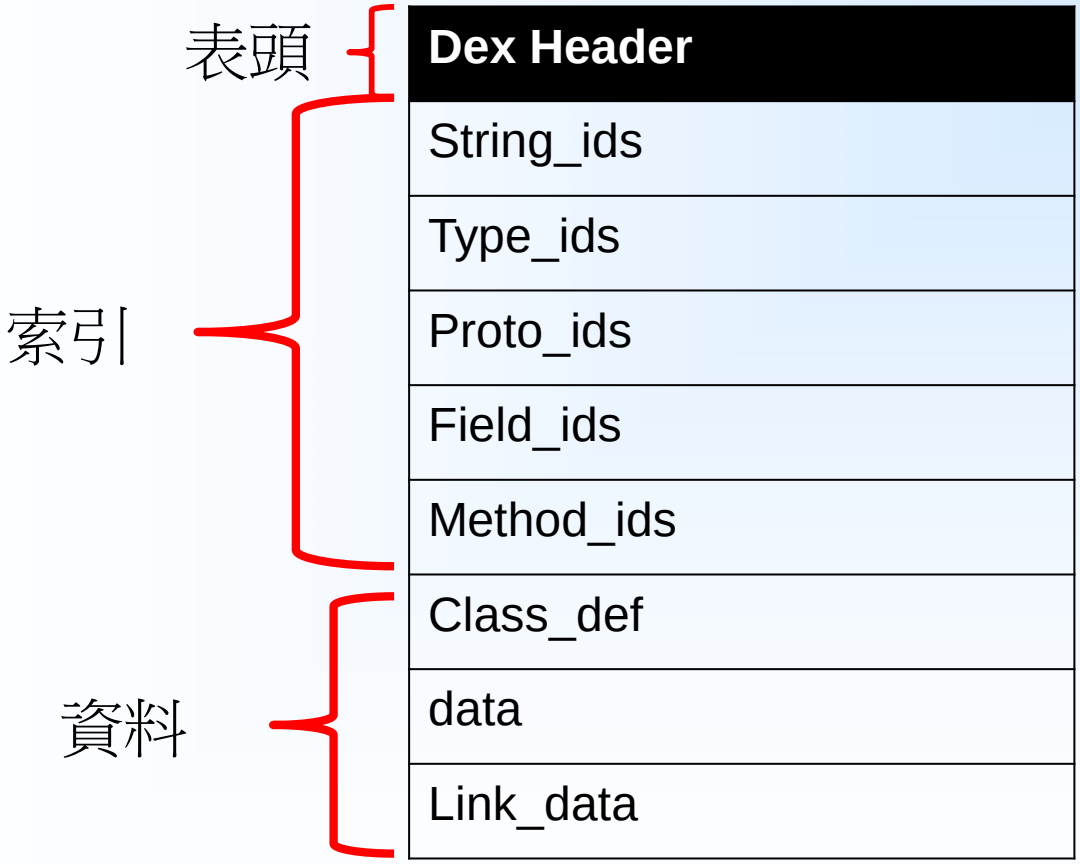
```
# direct methods
.method protected onDestroy()V
    .locals 1

    .prologue
    .line 86
    invoke-super {p0},
Ljp/naver/line/android/common/CommonBaseActivity;>onDestroy()V

    invoke-virtual {v0}, Ljp/naver/line/android/util/b;->a()V

    .line 89
    return-void
.end method
```

Dex檔結構


表頭
索引
資料
Dex Header
String_ids
Type_ids
Proto_ids
Field_ids
Method_ids
Class_def
data
Link_data

對抗反編譯

編譯失敗，使工具無法反編譯

- Ex: apktool、baksmali、dex2jar
- 查看來源碼，是否存在Bug？
- 壓力測試：測試大量的apk，尋找編譯器異常的錯誤訊息
- Anti dex2jar(0.0.7.8): https://github.com/jltxgcy/AntiCrack/tree/master/Antidex2jar

編譯成功，使得到的代碼並不是正確的

靜態技術

代碼混淆

- ProGuard (Android 2.3版起) [1]、DexGuard [2]、APKfuscator [3]、DashO [4]
- DexProtector [5] 、Shield4J [6] 、Stringer [7]、Allitori [8]

NDK保護

- 將邏輯寫在C / C++實現

加殼保護

- 代碼加密, Ex: upx or sstriping
- loader: /system/bin/linker
- System.LoadLibrary

JNI佈密鑰

靜態技術– 優缺點

優點

- 可讀性變差
- 全面掌控代碼的難度增加
- 壓縮代碼

缺點

- 無法真正保護代碼不被反編譯
- 動態debug時失效
- 驗證本地簽名容易bypass

對抗混淆

Dex-oracle

- https://github.com/CalebFenton/dex-oracle

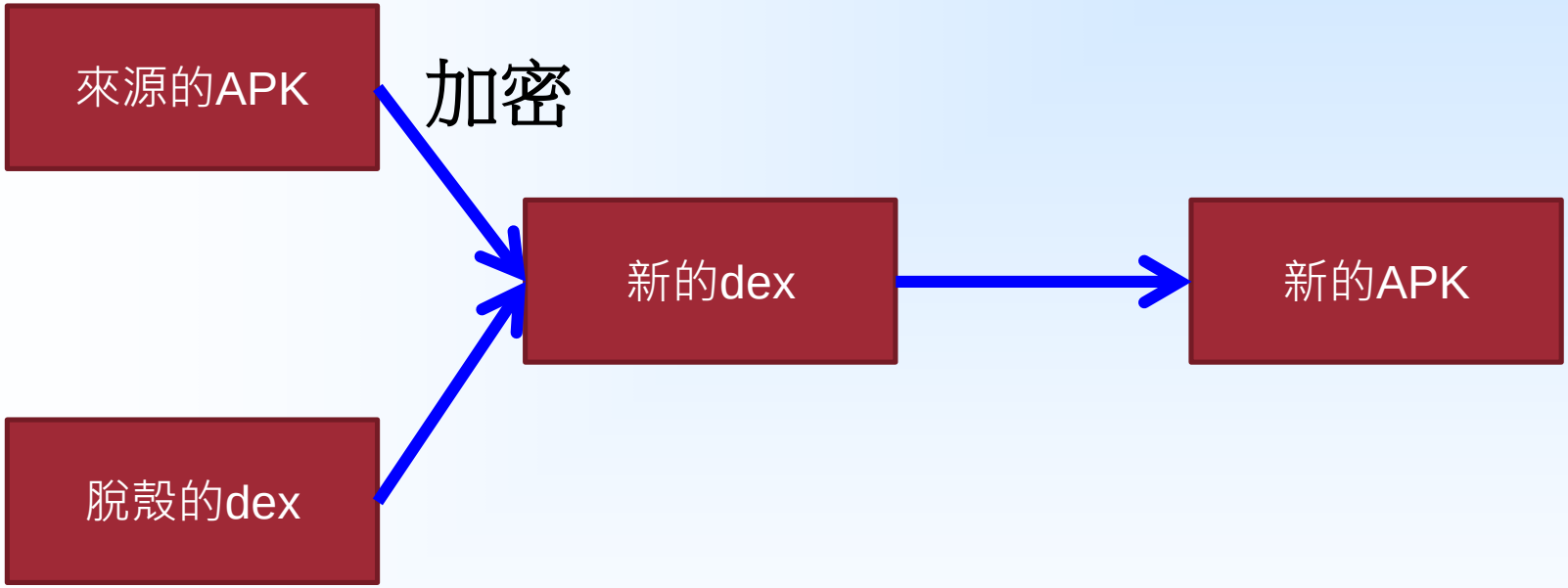
Simplify

- https://github.com/CalebFenton/simplify

Bytecode-viewer

- https://github.com/konloch/bytecode-viewer

Android加殼的原理



Android加殼步驟

Checksum

- 使用alder32 演算法再除去 magic 及 checksum

Signature

- 使用 SHA-1 演算法再除去 magic, checksum 和 signature

File_size

Android加殼步驟

重新編譯

檢查簽名

- 在 JAVA 端檢測簽名 [9]
- PackageManager的 getPackageInfo()
- 可比對 hashCode()

完整性檢驗

- 檢查 classes.dex 的 Hash [10]
- 檢查 META-INF 底下的 MANIFEST.MF

反動態分析

Debugger, Ex: GikDbg: http://gikir.com/product.php

- 限制debugger連接，若偵測到連接則停止執行
- 加入android:debuggable="false"
- android.os.debug.isdebuggerconnected()

Trace檢查

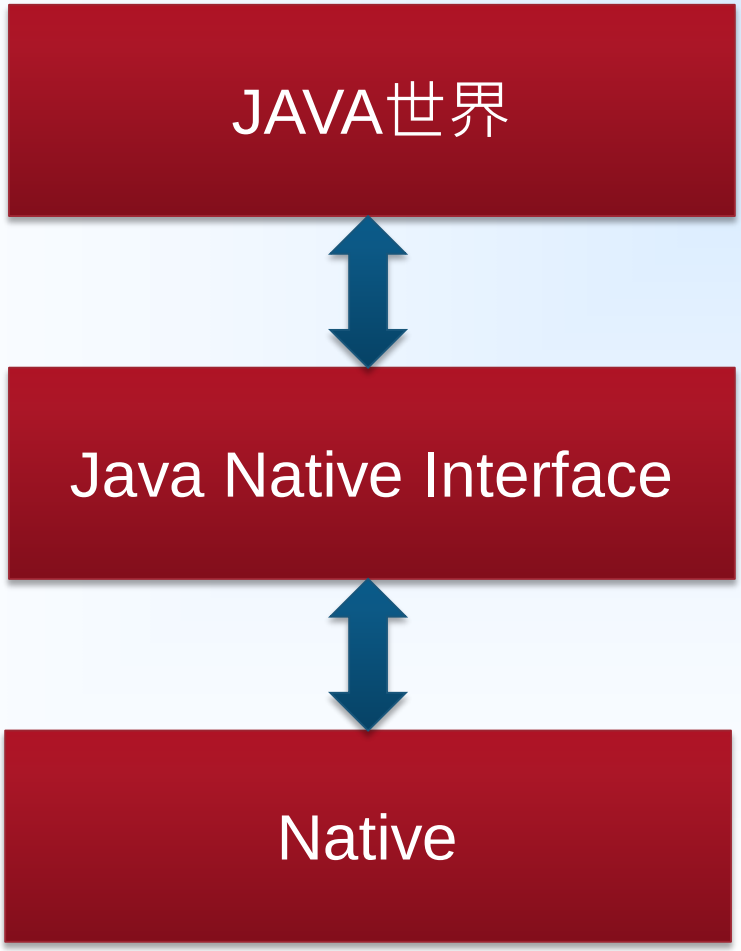
- 父行程、行程狀態檢查
- 比較 ptrace 返回值
- 設置 app 執行最大的時間
- 檢查 filedescriptor
- 防止 dump
- 對read做hook

```
# getprop
getprop
[ro.secure]: [0]
[ro.allow.mock.location]: [1]
[ro.debuggable]: [1]
[persist.service.adb.enable]: [1]
[ro.kernel.qemu]: [1]
[ro.kernel.console]: [ttyS0]
[ro.kernel.android.checkjni]: [1]
[ro.kernel.android.qemud]: [ttyS1]
[ro.kernel.ndns]: [2]
[ro.factorytest]: [0]
[ro.serialno]: []
[ro.bootmode]: [unknown]
```

模擬器

- adb shell getprop
- ro.product.model:sdk or google_sdk
- ro.build.tags:test-keys
- ro.kernel.qemu:1
- 判斷IMEI

JNI佈密鑰



JNI佈密鑰

Signature – JNI版

- JAVA版6行….

Checksum – JNI版

- 程式邏輯和流程已知
- 散在判斷式
- Memory Point

經濟學問題

密鑰重要

付出時間

軟體成本

駭客關注

Conclusion

- 設置障礙，阻礙通行
- 安全等級
- Server端存簽名和CRC碼
- SO檔加殼

附錄

[1] http://proguard.sourceforge.net/index.html#manual/examples.html
[2] https://www.guardsquare.com/dexguard
[3] https://github.com/strazzere/APKfuscator
[4] https://www.preemptive.com/products/dasho/overview
[5] https://dexprotector.com
[6] https://java.net/projects/shield4j
[7] https://jfxstore.com/stringer
[8] http://www.allatori.com
[9] https://github.com/jltxgcy/AntiCrack/tree/master/CheckSignature
[10] https://github.com/jltxgcy/AntiCrack/tree/master/CheckCRC

Q and A

Thanks for your attention