Attacking Android

one application at a time

sourcetoad

Our plan today

- Learn about APKs
- Reverse Engineering Techniques
- Application examples
- Android Security Enhancements
- Tips to prevent

sourcetoad
DEVELOPMENT STUDIO

Connor Tumbleson

Senior Software Engineer

Apktool Maintainer

@iBotPeaches

connortumbleson.com

Goals

- Understand Format
- Learn some tools
- Extract
  - Assets
  - Logic
- Rebuild

sourcetoad
DEVELOPMENT STUDIO

Unzipping an APK

```
total 12M
drwxrwxr-x  7 ibotpeaches 4.0K Aug  4 08:49 .
drwxrwxr-x  4 ibotpeaches 4.0K Aug  4 08:49 ..
-rw-rw-r--  1 ibotpeaches  21K Sep 29  2065 AndroidManifest.xml
drwxrwxr-x 19 ibotpeaches 4.0K Aug  4 08:49 assets
-rw-rw-r--  1 ibotpeaches 9.6M Sep 29  2065 classes.dex
drwxrwxr-x  4 ibotpeaches 4.0K Aug  4 08:49 com
drwxrwxr-x  4 ibotpeaches 4.0K Aug  4 08:49 lib
drwxrwxr-x  3 ibotpeaches 4.0K Aug  4 08:49 META-INF
-rw-rw-r--  1 ibotpeaches 2.3K Sep 29  2065 NDK_LICENSES
drwxrwxr-x 24 ibotpeaches 4.0K Aug  4 08:49 res
-rw-rw-r--  1 ibotpeaches 2.1M Sep 29  2065 resources.arsc
➜  unzip git:(master) ✗
```

sourcetoad
DEVELOPMENT STUDIO

Unzipping an APK

```
total 12M
drwxrwxr-x  7 lbotpeaches 4.0K Aug  4 08:49 .
drwxrwxr-x  4 lbotpeaches 4.0K Aug  4 08:49 ..
-rw-rw-r--  1 lbotpeaches  21K Sep 29  2065 AndroidManifest.xml
drwxrwxr-x 19 lbotpeaches 4.0K Aug  4 08:49 assets
-rw-rw-r--  1 lbotpeaches 9.6M Sep 29  2065 classes.dex
drwxrwxr-x  4 lbotpeaches 4.0K Aug  4 08:49 com
drwxrwxr-x  4 lbotpeaches 4.0K Aug  4 08:49 lib
drwxrwxr-x  3 lbotpeaches 4.0K Aug  4 08:49 META-INF
-rw-rw-r--  1 lbotpeaches 2.3K Sep 29  2065 NDK_LICENSES
drwxrwxr-x 24 lbotpeaches 4.0K Aug  4 08:49 res
-rw-rw-r--  1 lbotpeaches 2.1M Sep 29  2065 resources.arsc
➜  unzip git:(master) ✗
```

sourcetoad
DEVELOPMENT STUDIO

Whats in an APK?

- **arsc/xml** files
  - strings, layouts, images, assets
- **dex** files
  - java/kotlin code
- **so** files
  - libraries, game engines, native code

sourcetoad
DEVELOPMENT STUDIO

Android XML (AXML)

```
1   u?4?\"<Vt????$0Rl??????
•   .BZh??????*Th?????X\n???
•   ,4BVz??6r??J??.l?? n ? ? D
2   ~
3   ?
4   D`??P??6t?6??J?T??b???X
•   l???J?bv??\v?,8L?N????,P\
•   dx???????v?F????d?l?????
•   d ?
•   b!?!""6"?"?"?"t#?#?#?$?$%|%?%.&??&??&&'^'?'2(?(?(d)?)?)$*
•   V*f*?*J+?+0,?,?,6-~-?-(.?./j/?/0N0?0installLocationv
•   ersionCodeversionNameminSdkVersiontargetSdkVersion
```

toad
DEVELOPMENT STUDIO

If only we had a tool...

AXML - Disassembled

```
1  <?xml version="1.0" encoding="utf-8" standalone="no"?><manifest
•  xmlns:android="http://schemas.android.com/apk/res/android" android:installLocation="auto"
•  package="com.snapchat.android" platformBuildVersionCode="26" platformBuildVersionName="8.0.0">
2      <supports-screens android:anyDensity="true" android:largeScreens="true" android:normalScreens="true"
•      android:smallScreens="true" android:xlargeScreens="true"/>
3      <uses-permission android:name="com.google.android.c2dm.permission.RECEIVE"/>
4      <uses-permission android:name="android.permission.GET_ACCOUNTS"/>
5      <uses-permission android:name="android.permission.WAKE_LOCK"/>
6      <uses-permission android:name="android.permission.INTERNET"/>
7      <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
8      <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
```

sourcetoad
DEVELOPMENT STUDIO

Tool: Apktool

- Disassemble resources/source
- Rebuild application
- Open source
  - 6~ million downloads
  - Amazing contributors

sourcetoad
DEVELOPMENT STUDIO

Types of **Attacks**

- **Network** Attacks
  - MITM, Proxy
- **Source** Attacks
  - Application modification
- **Hook** Attacks
  - Xposed, Substrate

sourcetoad
DEVELOPMENT STUDIO

Network **Attack**

graph.facebook.com		06:20:58	12300 ms	5.51 KB	Complete
service.supercell.net		06:20:58	264 ms	4.13 KB	Complete
inbox.clashofclans.com		06:21:01	266 ms	4.25 KB	Complete
inbox.clashofclans.com		06:21:02	7772 ms	1.03 MB	Complete
b46f744d64acd2191eda-3720c0374d47e9a...	/a23444f47413a7430f15150e47254db166337f55/sc/news_tex.sc	06:21:03	320 ms	54.93 KB	Complete
b46f744d64acd2191eda-3720c0374d47e9a...	/a23444f47413a7430f15150e47254db166337f55/sc/news.sc	06:21:03	184 ms	15.91 KB	Complete
www.google-analytics.com		06:21:03	162 ms	281 bytes	Failed
b46f744d64acd2191eda-3720c0374d47e9a...	/a23444f47413a7430f15150e47254db166337f55/logic/townhall_levels.csv	06:21:03	117 ms	1.82 KB	Complete
b46f744d64acd2191eda-3720c0374d47e9a...	/a23444f47413a7430f15150e47254db166337f55/logic/locales.csv	06:21:03	150 ms	1.39 KB	Complete
b46f744d64acd2191eda-3720c0374d47e9a...	/a23444f47413a7430f15150e47254db166337f55/logic/leagues2.csv	06:21:03	248 ms	1,005 bytes	Complete
b46f744d64acd2191eda-3720c0374d47e9a...	/a23444f47413a7430f15150e47254db166337f55/logic/heroes.csv	06:21:04	173 ms	4.09 KB	Complete
b46f744d64acd2191eda-3720c0374d47e9a...	/a23444f47413a7430f15150e47254db166337f55/logic/gem_bundles.csv	06:21:04	234 ms	3.49 KB	Complete
b46f744d64acd2191eda-3720c0374d47e9a...	/a23444f47413a7430f15150e47254db166337f55/logic/characters.csv	06:21:04	35 ms	8.87 KB	Complete
b46f744d64acd2191eda-3720c0374d47e9a...	/a23444f47413a7430f15150e47254db166337f55/logic/buildings.csv	06:21:04	46 ms	12.99 KB	Complete
b46f744d64acd2191eda-3720c0374d47e9a...	/a23444f47413a7430f15150e47254db166337f55/csv/texts_patch.csv	06:21:04	75 ms	23.22 KB	Complete
b46f744d64acd2191eda-3720c0374d47e9a...	/a23444f47413a7430f15150e47254db166337f55/csv/news.csv	06:21:04	31 ms	2.50 KB	Complete
b46f744d64acd2191eda-3720c0374d47e9a...	/a23444f47413a7430f15150e47254db166337f55/csv/client_globals.csv	06:21:04	34 ms	5.25 KB	Complete
b46f744d64acd2191eda-3720c0374d47e9a	/a23444f47413a7430f15150e47254db166337f55/csv/billing_packages.csv	06:21:04	38 ms	1.64 KB	Complete

sourcetoad
DEVELOPMENT STUDIO

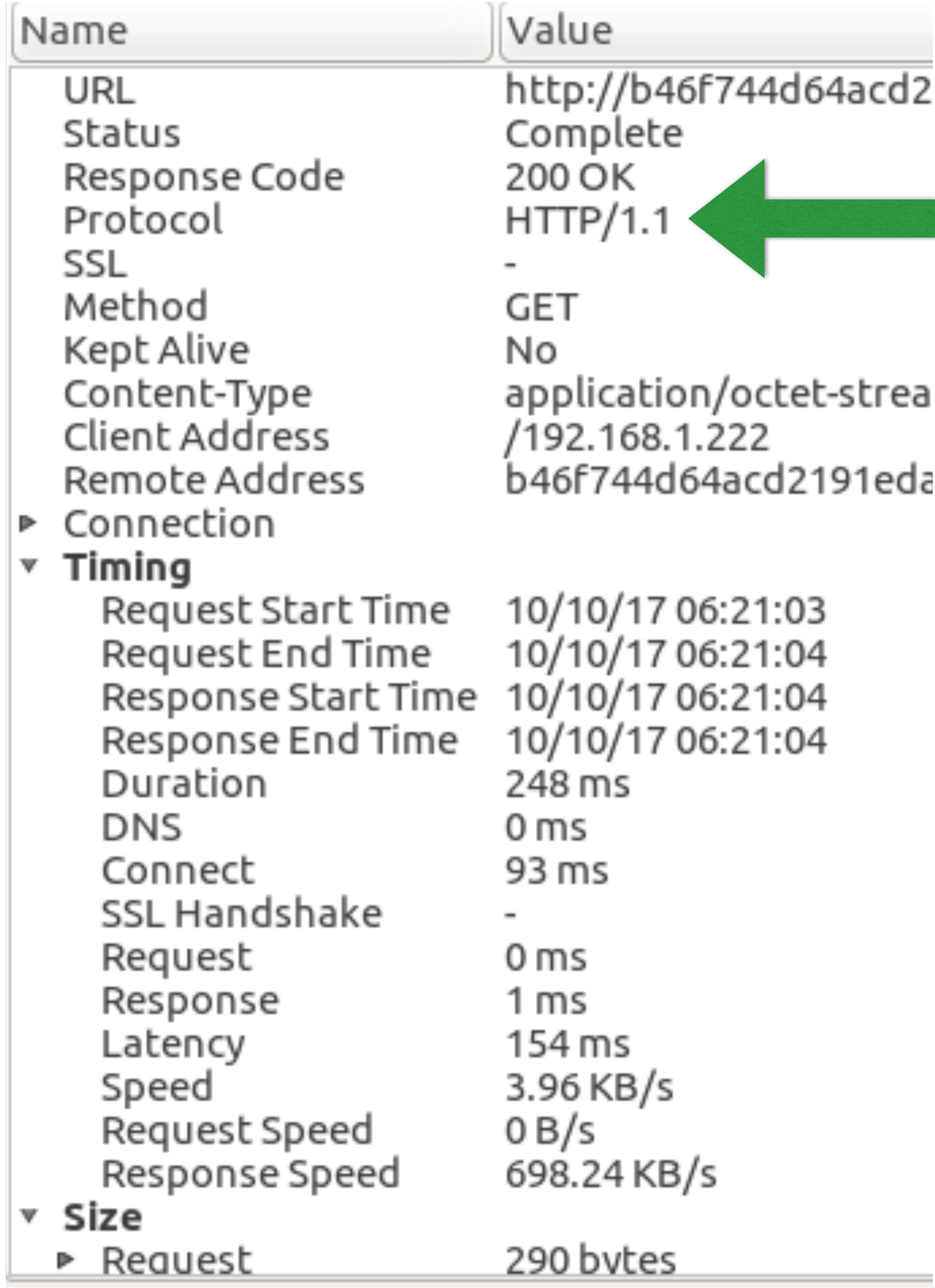
Tool: Charles Proxy

- Monitor Requests
- Proxy Requests
- View SSL/HTTPS Traffic
- $$
- Free Alternative - Fiddler

sourcetoad
DEVELOPMENT STUDIO

No **SSL**

- Contents plaintext
- Allows easy rewriting
- Simple proxy
- Downloads csv file



Uh **oh.**

```
1  ]?&?MF.??>(?o?????k?????????@?+?qgA??u(bb?????S5????k??>"?S?ᴍN??(
2  ???$?L?7???X?????r???z???U.K?]??i?L2?z? Nb0??F?}?/?ỹ?&???'E?>G?2-
3  f????l?Ś□??????,t?DJk?'??2`??a??;X?w?~???+p?5???.OM□Q?Jn?  ???U
•  ???iB.Ft*??i?Y?p?.?3?y?_Z??Y???<U??1WK?M?tz?_U?nRQ??:?n???K0???>
•  t?????]
```

sourcetoad
DEVELOPMENT STUDIO

Decoding **CSV** File

- Not encryption
- Probably compression
  - .bz2 / .gz
  - .lzma / .lzo
  - .z

sourcetoad
DEVELOPMENT STUDIO

Decoding **CSV** File

```
lzma

00339ed8  LZMAReader: Unable to read full header
00339f00  LZMAReader: lzham_decompress_init failed
00339f30  LZMAReader: not LZMA or LZHAM file probably
0035ab30  SC m_pLZMAReader != NULL
0047edab  LZMAReader: Unable open file
```

sourcetoad
DEVELOPMENT STUDIO

Tool: Binary Ninja

- Reverse Engineering platform
- Strings, Disassembly
- Scripting
- $
- Free Alternative - Radare2

sourcetoad
DEVELOPMENT STUDIO

Reading **csv** File

```
→ csv binwalk animations.csv

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------

→ csv binwalk animations.csv

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             LZMA compressed data, properties: 0x5D, d
ictionary size: 262144 bytes, uncompressed size: 116453 bytes
```

sourcetoad
DEVELOPMENT STUDIO

Tool: binwalk

- Identify executable code / custom files
- On GitHub (free)
- Custom magic database

```
root@kali:~# binwalk -B dd-wrt.v24-13064_VINT_mini.bin

DECIMAL     HEX         DESCRIPTION
--------------------------------------------------------------------------------
0           0x0         TRX firmware header, little endian, header size: 28 bytes, image size: 2945024 bytes, CRC32:
28          0x1C        gzip compressed data, from Unix, NULL date: Wed Dec 31 19:00:00 1969, max compression
2472        0x9A8       LZMA compressed data, properties: 0x6E, dictionary size: 2097152 bytes, uncompressed size: 20
622592      0x98000     Squashfs filesystem, little endian, DD-WRT signature, version 3.0, size: 2320835 bytes,  547
```

sourcetoad
DEVELOPMENT STUDIO

Tweaked **LZMA** header

- Header was modified
- Header required tweaks
- 4 additional bytes of padding
- Trial and error

sourcetoad
DEVELOPMENT STUDIO

Decoded CSV File

Name	AttackCost	ResourceStorageLootPercentage	DarkElixirStorageLootPercentage
String	int	int	int
1	10	20	6
2	50	20	6
3	75	20	6
4	110	20	6
5	170	20	6
6	250	20	6
7	380	18	6
8	580	16	6
9	750	14	5
10	900	12	4
11	1000	10	4

sourcetoad
DEVELOPMENT STUDIO

Snapchat Time

- Send photos, disappear after gone
- Encrypted photos so MITM useless
- Unless - You know the decryption

sourcetoad
DEVELOPMENT STUDIO

Snapchat in **2013**

```
# direct methods
.method static constructor <clinit>()V
    .locals 1

    .prologue
    .line 8
    const-string v0, "1234567891123456"

    sput-object v0, Lcom/snapchat/android/util/AESEncrypt;->ENCRYPT_KEY:Ljava/lang/String;

    .line 9
    const-string v0, "M02cnQ51Ji97vwT4"

    sput-object v0, Lcom/snapchat/android/util/AESEncrypt;->ENCRYPT_KEY_2:Ljava/lang/String;

    return-void
.end method
```

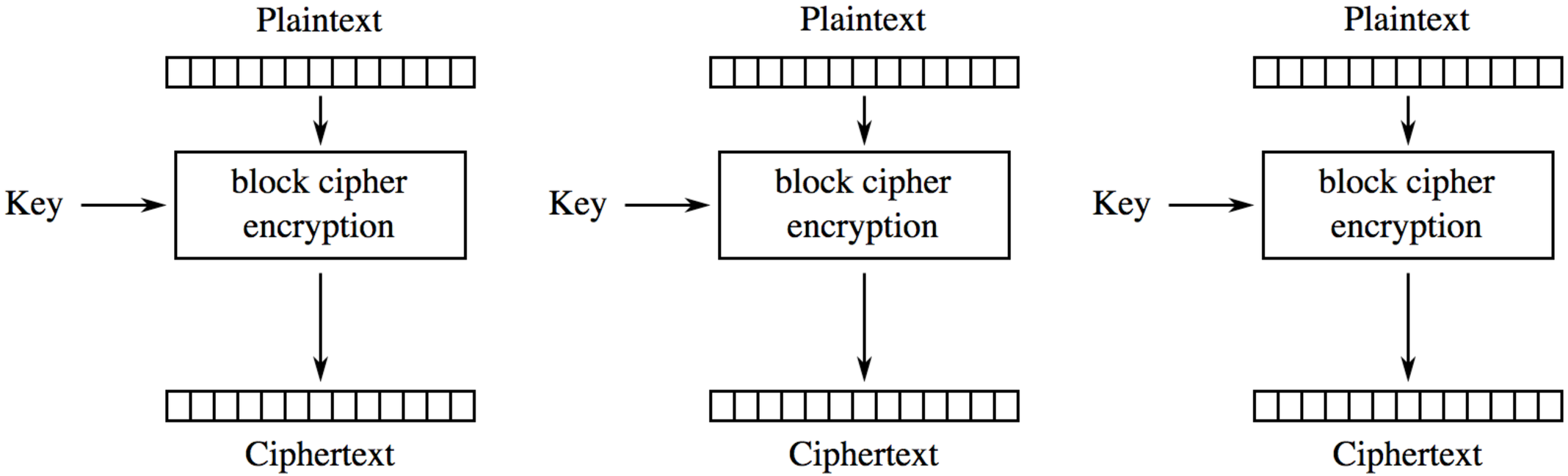
sourcedoa
DEVELOPMENT STUDIO

Snapchat Encryption **2013**

- 2013 - AES (ECB)
  - **E**lectronic **C**ode**b**ook
  - Hardcoded key
  - Other key (ENCRYPT_KEY) unused

sourcetoad
DEVELOPMENT STUDIO

Context: AES (ECB)



Electronic Codebook (ECB) mode encryption

sourcetoad
DEVELOPMENT STUDIO

Snapchat in **2014**

```
const-string v1, "android_id"
invoke-static {v0, v1}, Landroid/provider/Settings$Secure;->getString(Landroid/content/ContentResolver;Ljava/lang/String;)Ljava/lang/String;
sget-object v0, Landroid/os/Build;->FINGERPRINT:Ljava/lang/String;
const-string v1, "MD5"
invoke-static {v1}, Ljava/security/MessageDigest;->getInstance(Ljava/lang/String;)Ljava/security/MessageDigest;
move-result-object v1
invoke-virtual {v0}, Ljava/lang/String;->getBytes()[B
move-result-object v0
invoke-virtual {v1, v0}, Ljava/secu essageDigest;->update([B)V
const-string v0, "seems legit..."
invoke-virtual {v0}, Ljava/lang/String;->getBytes()[B
move-result-object v0
invoke-virtual {v1, v0}, Ljava/security/MessageDigest;->update([B)V
```

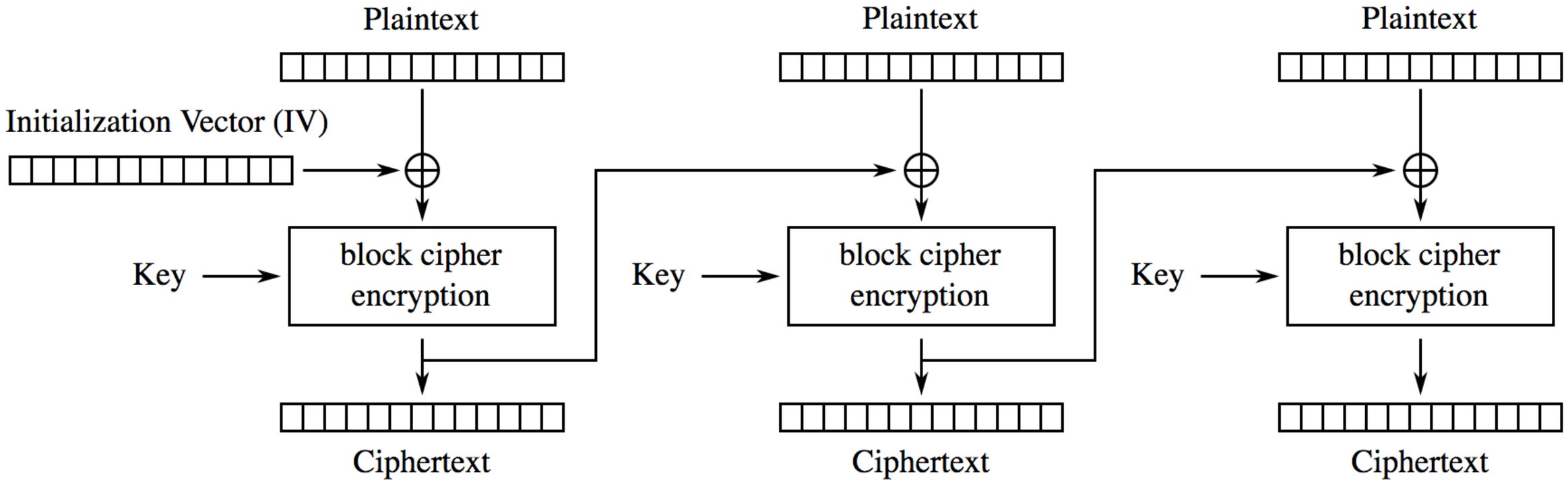
sourcetoad
DEVELOPMENT STUDIO

Snapchat Encryption **2014**

- 2014 - AES / CBC
  - **C**ipher **B**lock **C**haining
  - Random IV/Key per image
  - IV/Key saved to encrypted file
  - *md5*(android_id + “seems legit…”)
  - Decrypt cold file, obtain IV/Key

sourcetoad
DEVELOPMENT STUDIO

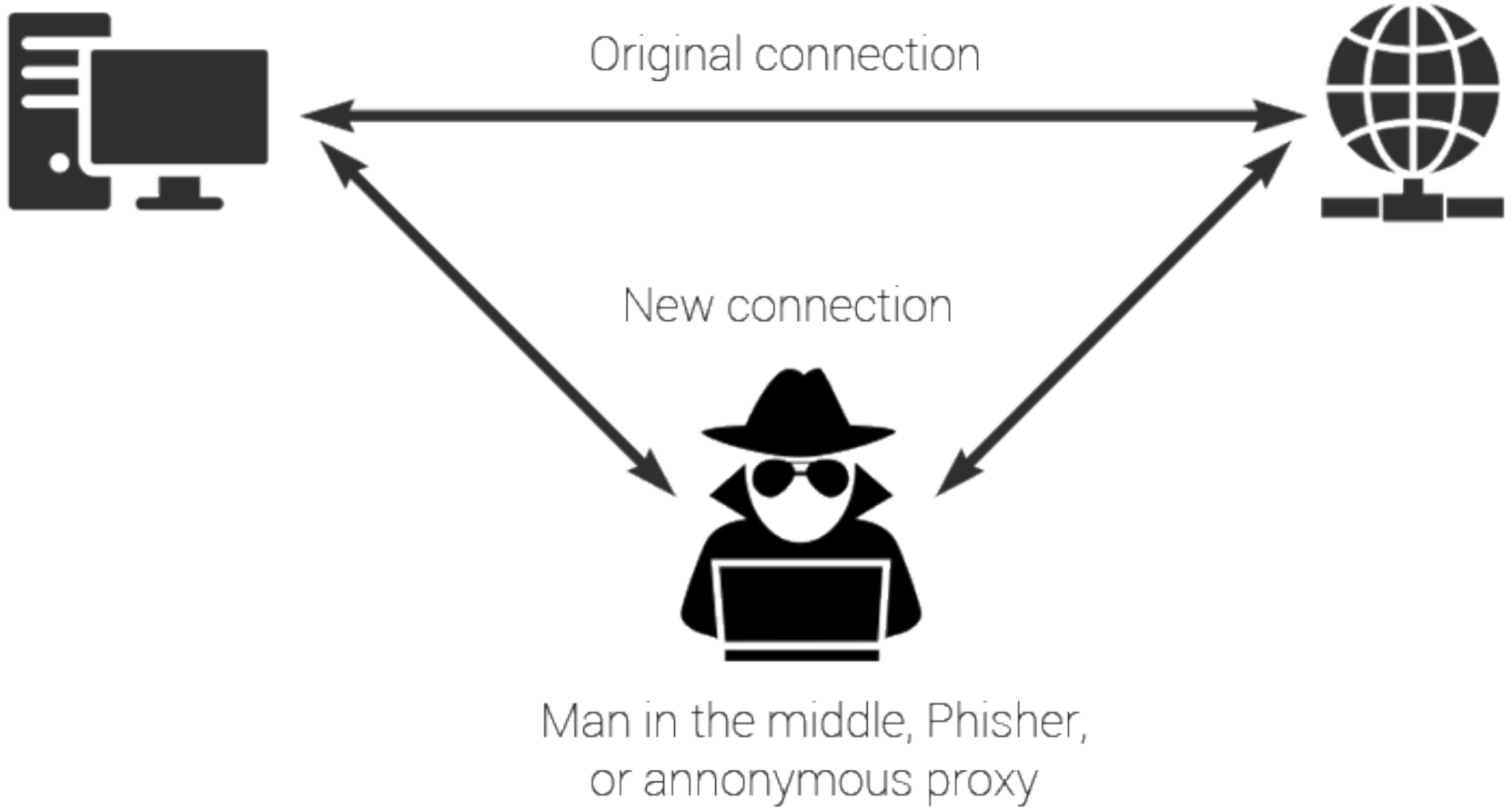
Context: AES (CBC)



Cipher Block Chaining (CBC) mode encryption

sourcetoad
DEVELOPMENT STUDIO

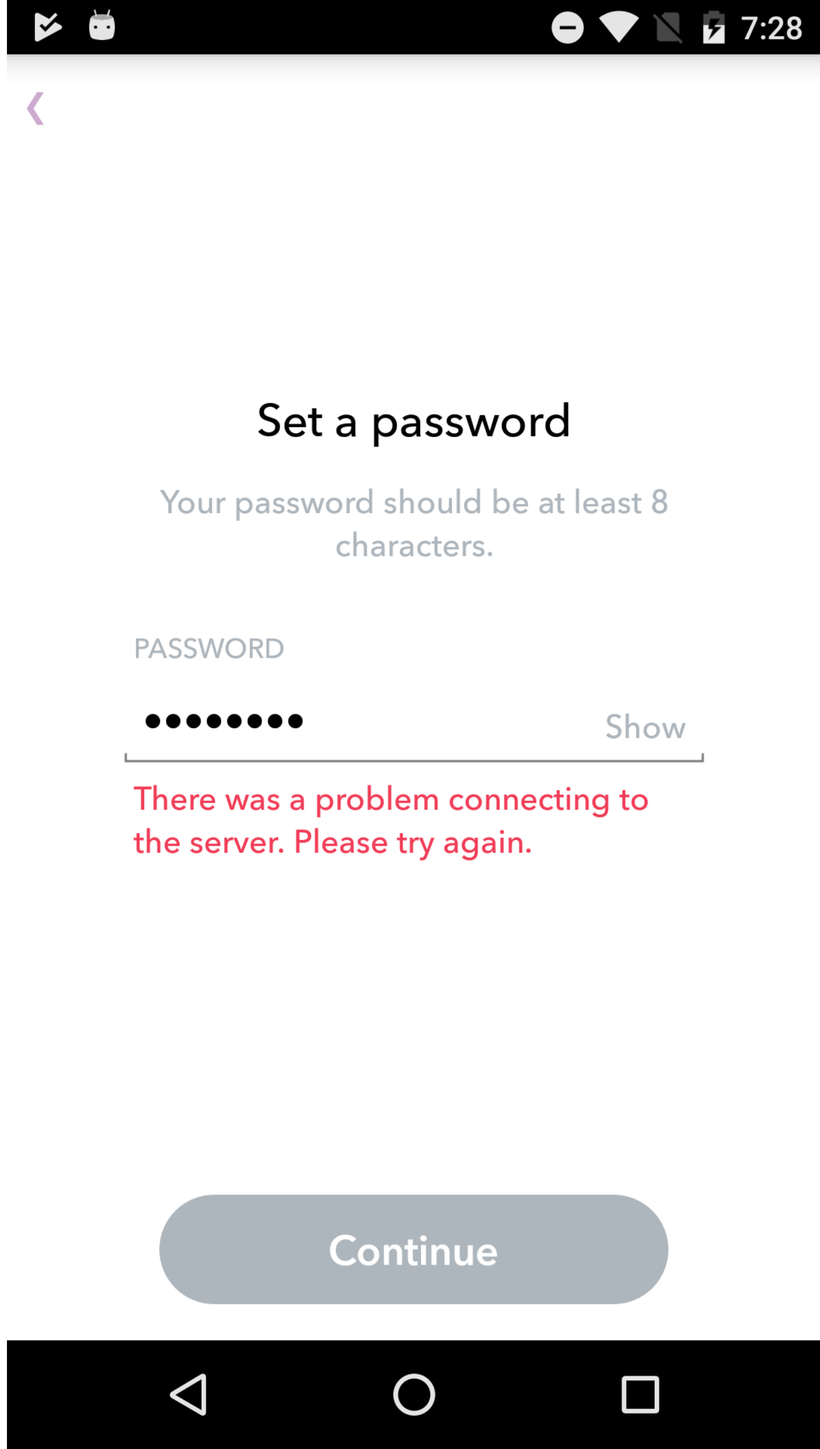
Man in the **Middle**



sourcetoad
DEVELOPMENT STUDIO

Snapchat MITM

- Hmmm
- MITM Failed
- Requests are denied
- Onward to door 2



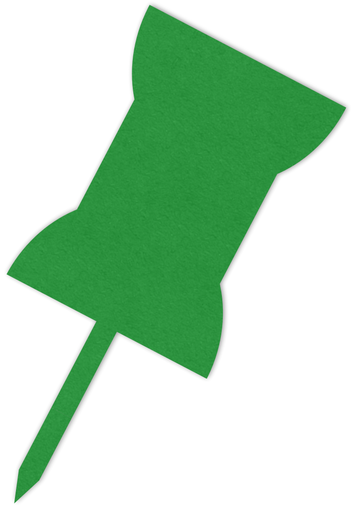
Snapchat MITM

```
 Receive action: android.intent.action.PACKAGE_ADDED
 mHandler: 3
dler: 9 phoneId: 0
Verification result: checking for a statement with source a <
  a: "https://snapchat.com"
>
, relation delegate_permission/common.handle_all_urls, and target b <
  a: "com.snapchat.android"
  b <
    a: "A4:0D:A8:0A:59:D1:70:CA:A9:50:CF:15:C1:8C:45:4D:47:A3:9B:26:98:9D:8B:64:0E:CD:74:5B:A7:1B:F5:DC"
  >
>
 --> false.
rification 4 complete. Success:false. Failed hosts:www.snapchat.com,snapchat.com.
```

sourcetoad
DEVELOPMENT STUDIO

SSL **Pinning**

- Enforce certificate used
- Prevents bogus cert, patches MITM
- Can backfire if not proper
- Leaf/Intermediate/Root Pinning



sourcetoad
DEVELOPMENT STUDIO

Snapchat **Search**

```
ibotpeaches@ivorytower:~/Desktop/NewDevFest/snapchat$ egrep -r 'checkClientTrusted|checkServerTrusted' *
Binary file build/apk/classes6.dex matches
Binary file build/apk/classes5.dex matches
Binary file build/apk/classes4.dex matches
smali_classes4/hvx.smali:.method public final checkClientTrusted([Ljava/security/cert/X509Certificate;Ljava/lang/String;)V
smali_classes4/hvx.smali:.method public final checkServerTrusted([Ljava/security/cert/X509Certificate;Ljava/lang/String;)V
smali_classes4/hvx.smali:    invoke-interface {v0, p1, p2}, Ljavax/net/ssl/X509TrustManager;->checkServerTrusted([Ljava/securit
y/cert/X509Certificate;Ljava/lang/String;)V
smali_classes6/ywm.smali:    const-string v2, "checkServerTrusted"
smali_classes6/yls$d.smali:.method public final checkClientTrusted([Ljava/security/cert/X509Certificate;Ljava/lang/String;)V
smali_classes6/yls$d.smali:    invoke-interface {v0, p1, p2}, Ljavax/net/ssl/X509TrustManager;->checkClientTrusted([Ljava/secur
ity/cert/X509Certificate;Ljava/lang/String;)V
smali_classes6/yls$d.smali:.method public final checkServerTrusted([Ljava/security/cert/X509Certificate;Ljava/lang/String;)V
smali_classes6/yls$d.smali:    invoke-interface {v0, p1, p2}, Ljavax/net/ssl/X509TrustManager;->checkServerTrusted([Ljava/secur
ity/cert/X509Certificate;Ljava/lang/String;)V
ibotpeaches@ivorytower:~/Desktop/NewDevFest/snapchat$
```

sourcetoad
DEVELOPMENT STUDIO

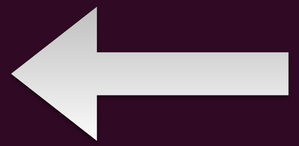
Snapchat smali

```
.method public final checkServerTrusted([Ljava/security/cert/X509Certificate;Ljava/lang/String;)V
    .locals 6

    .prologue
    const/4 v2, 0x1

    const/4 v3, 0x0

    .line 47
    iget-object v0, p0, Lhvx;->b:Ljavax/net/ssl/X509TrustManager;

    invoke-interface {v0, p1, p2}, Ljavax/net/ssl/X509TrustManager;->checkServerTrusted([Ljava/security/ce
rt/X509Certificate;Ljava/lang/String;)V

    .line 59
    aget-object v0, p1, v3
```

sourceload
DEVELOPMENT STUDIO

Snapchat **Patched**

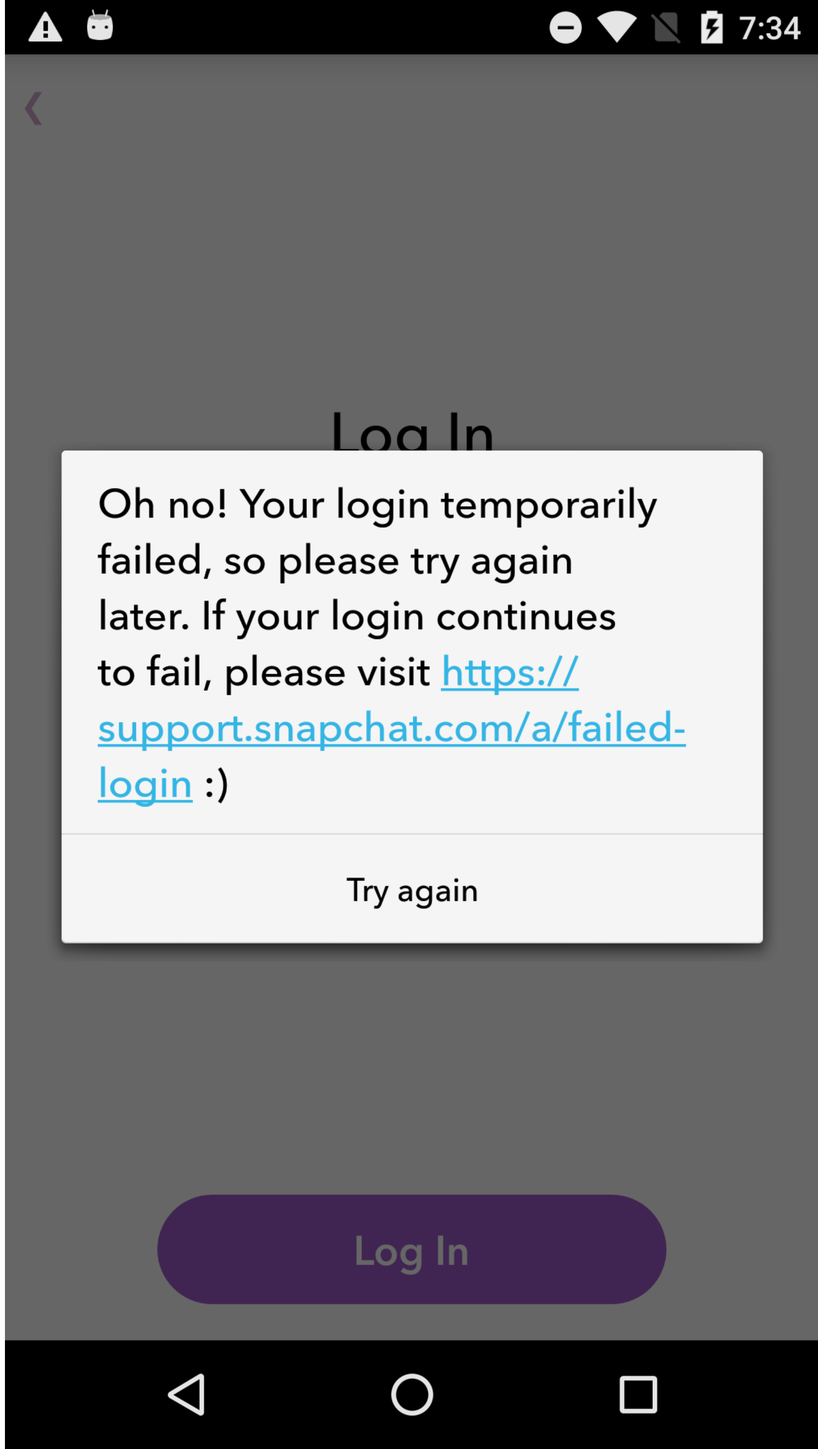
```
.method public final checkServerTrusted([Ljava/security/cert/X509Certificate;Ljava/lang/String;)V
    .locals 6

    .prologue
    return-void
    const/4 v2, 0x1

    const/4 v3, 0x0

    .line 47
    iget-object v0, p0, Lhvx;->b:Ljavax/net/ssl/X509TrustManager;

    invoke-interface {v0, p1, p2}, Ljavax/net/ssl/X509TrustManager;->checkServerTrusted([Ljava/security/ce
rt/X509Certificate;Ljava/lang/String;)V

    .line 59
    aget-object v0, p1, v3
```



sourcetoad
DEVELOPMENT STUDIO

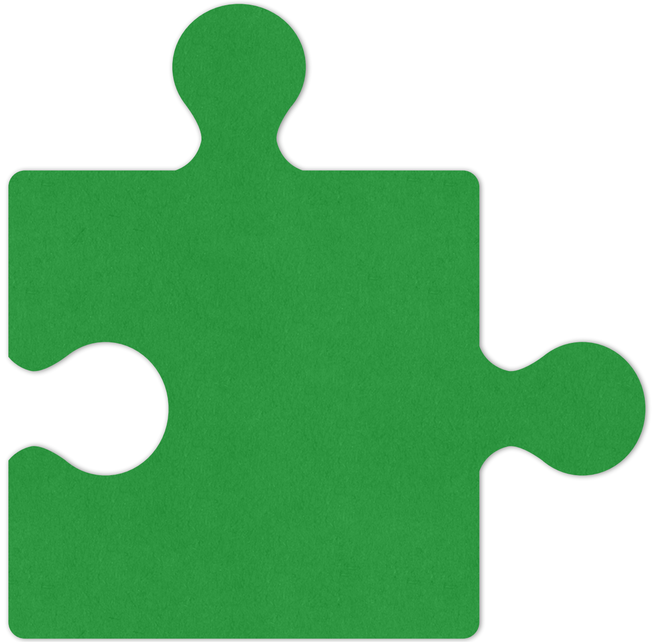
Snapchat Rebuilt

- Hmmm
- Rebuilt APK is rejected
- Some sort of detection
- Onward to door 3



Xposed Framework

- Hooks “code”, no modifying apps
- Install onto system
- Requires ROOT
- Nougat (7.0) - recent release
- Oreo (8.0) - nothing official



sourcetoad
DEVELOPMENT STUDIO

Snapchat **Hooked**

- Success
- Using an Xposed module
- Newer Android is no go

Android **7.0** - Nougat

- NSP Rules
- Debug overrides
- Standard CAs
- Ignore User certs
- API24+

```
<network-security-config>
      <base-config>
            <trust-anchors>
                  <!-- Trust preinstalled CAs -->
                  <certificates src="system" />
            </trust-anchors>
      </base-config>
 </network-security-config>
```

sourcetoad
DEVELOPMENT STUDIO

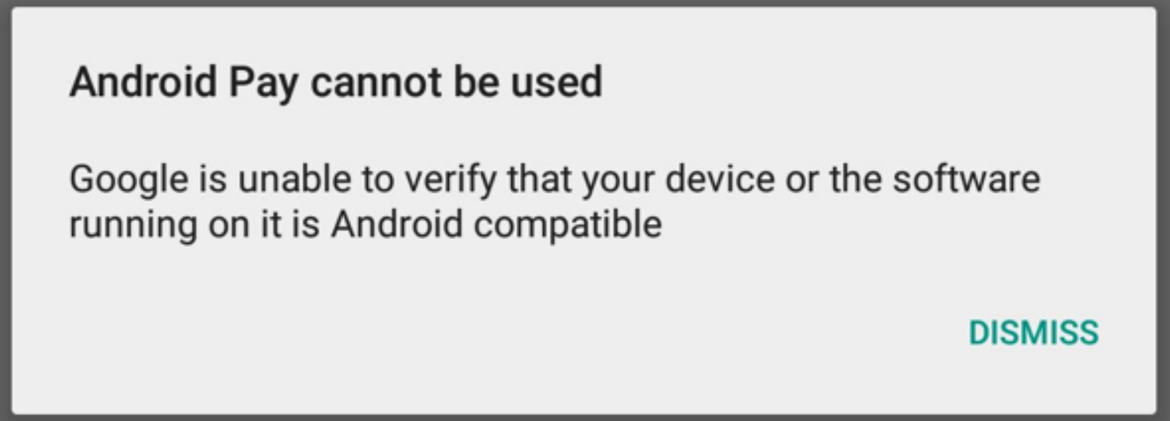
7.0 - Signature Scheme **v2**

- Full block signature
- Replaces v1 (jar signature)
- Modifying applications

sourcetoad
DEVELOPMENT STUDIO

Introducing **SafetyNet**

- Device passes CTS
- Emulator Detection
- Root Detection
- API Hooking Detection
- Other attacks



sourcetoad
DEVELOPMENT STUDIO

Magisk & Root **Switch**

- Systemless Root
- Reset props
- Tricks callers
- Pairs with Xposed

sourcetoad
DEVELOPMENT STUDIO

SafetyNet **v2**

- Basic Integrity
- DroidGuard
- Idle (12h checks)
- Safe Browsing, reCAPTCHA
- Zygote Inspection

sourcetoad
DEVELOPMENT STUDIO

Cat n **Mouse**

- suhide
- root switch
- Magisk (Magic Mask)
- Systemless Xposed

sourcetoad
DEVELOPMENT STUDIO

Android **8.0** - Oreo

- SSL downgrading fixes
- ANDROID_ID is tweaked
- Verified Boot System
- Broke Xposed (see the pattern?)

sourcetoad
DEVELOPMENT STUDIO

In **Closing**

- Never trust the client
- SSL is a requirement
- Crypto is tough. Don’t reinvent
- Iterate, sunset old versions

sourcetoad
DEVELOPMENT STUDIO

Q / A
#DevFestFL

sourcetoad

@iBotPeaches

connortumbleson.com