

| | | | | | | | |
|----------|-------------------------|----------------------------|--------------------|----------|-------------------------|-------------------------|--------------------|
| 00001176 | 8d eb 68 46 bf e2 2b 0e | 13 f5 5e 93 85 9c 1f da | .kF+.+.+.+.+ | 00001150 | 30 00 41 28 00 00 00 61 | 65 61 62 69 00 01 1e 00 | 0.A(...seabi.... |
| 00001180 | 5d 5e 68 1f c3 c2 82 86 | 78 13 07 1e 4d f4 63 c7 | ...x...M.c. | 00001160 | 00 00 05 35 54 45 00 06 | 04 08 01 09 01 12 04 14 | ...5TE..... |
| 00001180 | 8d eb 90 06 9e 46 49 0d | 33 4f ad ad 0c 1b aa 0e 85 | a...FY.30.... | 00001170 | 01 15 01 17 03 18 01 19 | 01 1a 02 00 21 73 68 73 | ...ahs..... |
| 00001190 | 61 08 a1 9e 99 5e d9 19 | f0 81 ba 8e aa 76 2e 1c 8f | a...T...T... | 00001180 | 74 72 74 61 62 00 2e 69 | 6e 74 65 72 70 00 2e 68 | tntab..interp..h |
| 000011a0 | fb 2f 24 c2 b9 26 0d 02 | 22 9a 8e aa 5a 75 2e 1c 8f | ./8.&...v...v | 00001190 | 61 73 68 00 2e 64 79 6e | 73 79 6d 00 2e 64 79 6e | ash..dynsym..dyn |
| 000011b0 | b4 03 1d 7d 12 3f 0f 6e | 54 37 57 c6 4b 76 36 cf | ...?.nT7W.Kv6. | 000011a0 | 73 74 72 00 2e 72 65 6c | 2e 60 7c 64 70 2e 74 65 | str...rel.plt..tel |
| 000011c0 | 8d 45 94 9e 7f 4d be da | 55 c7 63 c0 99 ce 45 77 | .E...G...E..w | 000011b0 | 78 74 00 2e 72 6f 64 61 | 74 61 00 2e 70 72 65 69 | xt..rodada..prel |
| 000011d0 | 43 38 ff 2e 50 89 c0 92 | 1c f2 ae ae af 96 44 0f | C8.P...C...Do | 000011c0 | 6e 69 74 5f 61 72 72 61 | 79 00 2e 69 6e 69 74 5f | nit.array..init. |
| 000011e0 | 49 96 c2 61 66 c6 40 e8 | fe 6a 44 2c 54 88 e7 d8 | .a.f.e..jd.T... | 000011d0 | 61 72 72 61 79 00 2e 66 | 69 6e 69 5f 61 72 72 61 | array..fini.array |
| 000011f0 | 17 aa c1 92 7e 9b 4c f8 | 05 67 19 53 0c 06 0f | ...f..l.g'.S... | 000011e0 | 79 00 2e 63 74 6f 72 73 | 00 2e 64 79 6e 61 6d 69 | y.ctors..dynami |
| 00001200 | c1 b4 0d 33 46 e8 da 73 | 49 0e 05 ef 9d 9e fc 0f | ...F...eL...N | 000011f0 | 63 00 2e 67 74 70 2e | 62 73 73 00 2e 63 6f 6d | c..got..bss..com |
| 00001210 | a3 93 c5 b5 38 96 f0 | 22 43 7f 5c f8 da 12 b6 | ...8u...C...N | 00001200 | 6d 65 6e 74 00 2e 41 52 | 4d 2e 61 74 74 72 69 62 | ment..ARM.attrib |
| 00001220 | de 67 3b 6b 02 b3 70 4a | 90 18 04 86 03 20 01 1e | g.kj..p.j.... | 00001210 | 75 74 65 73 00 00 00 00 | 00 00 00 00 00 00 00 00 | utes..... |
| * | | | | 00001220 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | |
| 00001240 | 76 29 3c 26 e6 ee 85 32 | 02 11 e5 a4 a4 1f 3a 78 | v)<&...2...:x | * | | | |
| 00001250 | 36 42 d1 5a 24 86 1f 9e | 33 55 ff 82 b3 8d d5 2e | 66.Z\$.35..... | 00001240 | 06 00 00 00 01 00 00 00 | 02 00 00 00 d4 80 00 00 | |
| 00001260 | ea b6 f6 20 c4 c5 8e 8e | 16 90 5e 84 8e ff 5f | | 00001250 | 06 00 00 00 13 00 00 00 | 00 00 00 00 00 00 00 00 | |
| 00001270 | 16 89 82 ef c4 c5 8e 8e | 16 90 5e 84 8e ff 5f | | 00001260 | 06 00 00 00 13 00 00 00 | 00 00 00 00 00 00 00 00 | |
| 00001280 | d3 27 d1 a5 e5 8f | 16 90 5e 84 8e ff 5f | | 00001270 | 06 00 00 00 13 00 00 00 | 00 00 00 00 00 00 00 00 | |
| 00001290 | f4 57 3a 13 6d 1f b6 cf | 44 34 e2 ab 5c 35 bc 91 | .W..m...a...f | 00001280 | 03 00 00 00 00 00 00 00 | 04 00 00 00 04 00 00 00 | |
| 000012a0 | df 9e 38 84 04 9c fc 2c | 77 d2 73 bc aa c2 39 72 | ...w...s...9p | 00001290 | 19 00 00 00 0b 00 00 00 | 02 00 00 00 b4 81 00 00 | |
| 000012b0 | f5 0a 83 b4 3a b5 de 83 | 68 32 c4 c3 c6 9a de | ...h2MP..... | 000012a0 | b4 01 00 00 02 00 00 00 | 04 00 00 00 01 01 00 00 | |
| 000012c0 | c0 24 e7 68 23 75 83 83 | 1e 8a e2 ad c5 17 ac 56 | .s.hhu...V... | 000012b0 | 04 00 00 00 10 00 00 00 | 21 00 00 00 03 00 00 00 | |
| 000012d0 | 1a 17 83 0e b6 9c 17 0c | 84 ad 3c 2d 03 ff 1a 82 | ...<..... | 000012c0 | 02 00 00 00 b4 83 00 00 | b4 03 00 00 05 01 00 00 | |
| 000012e0 | f1 e7 9f 9c fb e6 2e 1a | 66 97 71 99 f4 6e c3 88 | ...f..q...n... | 000012d0 | 00 00 00 00 00 00 00 00 | 01 00 00 00 00 00 00 00 | |
| 000012f0 | 8b 3a b4 33 88 67 ea 84 | af ab f8 14 56 1d 40 82 | ...3.g...V...e | 000012e0 | 29 00 00 00 09 00 00 00 | 02 00 00 00 bc 84 00 00 | |
| 00001300 | ef 28 b7 3c 8d c1 a0 08 | b7 be 8b fd a2 8e 96 73 | ...e..... | 000012f0 | bc 04 00 00 98 00 00 00 | 03 00 00 00 06 00 00 00 | |
| 00001310 | d6 c3 a7 58 07 9a 9c 81 | 0f 98 85 84 8e ff 5f | | 00001300 | 04 00 00 00 08 00 00 00 | 02 00 00 00 01 00 00 00 | |
| 00001320 | 04 b7 46 ae af ab 9a 17 | 4e 10 5f 84 8e ff 5f | | 00001310 | 04 00 00 00 08 00 00 00 | 02 00 00 00 01 00 00 00 | |
| 00001330 | e2 74 73 f4 0a 33 ca c2 | 4e 10 5f 84 8e ff 5f | ...3..N.e...X | 00001320 | 00 00 00 00 00 00 00 00 | 04 00 00 00 04 00 00 00 | |
| 00001340 | 64 1b ec dd b8 ab 1e 12 | 50 a3 a4 65 17 86 1b 6b | d...e...e...b | 00001330 | 32 00 00 00 01 00 00 00 | 06 00 00 00 50 86 00 00 | 2.....P... |
| 00001350 | 8f 59 1b ec d8 ba c7 d8 | 69 b1 48 e2 e8 e3 69 6b | ...e...e...e...e | 00001340 | 00 00 00 00 08 02 00 00 | 00 00 00 00 00 00 00 00 | P..... |
| 00001360 | 85 a7 1c 32 59 24 de d1 | e2 84 cc bc b9 1e 7d 9c 1c | ...e...e...e...e | 00001350 | 00 00 00 00 00 00 00 00 | 38 00 00 00 01 01 00 00 | 2.....8..... |
| 00001370 | a5 55 9f 5e 0b 9a c8 3e | 89 64 21 61 62 f6 de d5 | ...q...>.dlab... | 00001360 | 32 00 00 00 38 89 00 00 | 38 09 00 00 e0 02 00 00 | 2.....8..... |
| 00001380 | df 6f c4 f1 5e 1d 9b c8 | 32 15 2b 09 42 25 53 91 | ...o.q...2+.B.S. | 00001370 | 00 00 00 00 00 00 00 00 | 04 00 00 00 01 00 00 00 | B..... |
| 00001390 | 01 09 2a c2 9e 1e 89 93 | 59 9f e8 cf 18 7d 20 29 | K...FT...I...E | 00001380 | 40 00 00 00 10 00 00 00 | 03 00 00 00 00 90 00 00 | B..... |
| 000013a0 | 4b 06 1c d8 bc f2 7f 66 | 54 aa c3 b4 91 45 f7 95 | K...FT...I...E | 00001390 | 00 10 00 00 08 00 00 00 | 00 00 00 00 00 00 00 00 | B..... |
| 000013b0 | 5e 1f 5a f6 fc bd 05 60 | fd d5 f6 4f 6e bc 1a fe | K...FT...I...E | 000013a0 | 01 00 00 00 00 00 00 00 | 4f 00 00 00 0e 00 00 00 | B..... |
| 000013c0 | 1a 17 83 0e b6 9c 17 0c | 84 ad 3c 2d 03 ff 1a 82 | K...FT...I...E | 000013b0 | 03 00 00 00 08 90 00 00 | 08 10 00 00 08 00 00 00 | B..... |
| 000013d0 | 93 e2 7f 3a 55 ed 0b ba | 6e 10 5f 84 8e ff 5f | ...w.U...n.q...w | 000013c0 | 00 00 00 00 00 00 00 00 | 01 00 00 00 00 00 00 00 | B..... |
| 000013e0 | e1 d0 66 6d 77 27 1e d5 | 22 4b 4c b5 66 59 79 b6 | ...kmu'...'KL.f.y. | 000013d0 | 5b 00 00 00 0f 00 00 00 | 03 00 00 00 10 90 00 00 | B..... |
| 000013f0 | 0e 3a 48 71 28 81 d6 11 | 74 48 5e a4 f3 e4 e9 27 | ...hld...th'... | 000013e0 | 10 10 00 00 08 00 00 00 | 00 00 00 00 00 00 00 00 | B..... |
| 00001400 | 6d 8e c4 52 e2 bb c4 42 | a5 ba 8d 3c 2d 03 ff 1a 82 | ...hld...th'... | 000013f0 | 04 00 00 00 00 00 00 00 | 07 00 00 00 01 00 00 00 | B..... |
| 00001410 | 1a 17 83 0e b6 9c 17 0c | 84 ad 3c 2d 03 ff 1a 82 | ...hld...th'... | 00001400 | 04 00 00 00 00 00 00 00 | 18 10 00 00 08 00 00 00 | B..... |
| 00001420 | ff c9 33 80 7f 3b 30 33 | 3c 2e bc 00 c0 99 ce 45 77 | ...hld...th'... | 00001410 | 04 00 00 00 00 00 00 00 | 01 00 00 00 00 00 00 00 | B..... |
| 00001430 | da 21 47 c5 af 03 de e0 | 8a ce 8c 91 70 d8 db da | ...hld...th'... | 00001420 | 06 00 00 00 06 00 00 00 | 03 00 00 00 20 90 00 00 | B..... |
| 00001440 | 48 f9 9e 18 d8 e8 26 b9 | f7 aa 0e 47 01 5e d2 43 | H...>...p...p | 00001430 | 10 00 00 00 c8 00 00 00 | 04 00 00 00 00 00 00 00 | B..... |
| 00001450 | fd 57 0f ca ee cc 3d df | 2d 59 95 13 31 55 d0 51 | H...>...p...p | 00001440 | 00 00 00 00 08 00 00 00 | 77 00 00 00 01 00 00 00 | B..... |
| 00001460 | 04 b7 46 ae af ab 9a 17 | 4d 79 ed 97 d5 95 1e c2 | H...>...p...p | 00001450 | 03 00 00 00 e8 90 00 00 | e8 10 00 00 58 00 00 00 | B..... |
| 00001470 | 4c 8d 79 fc 6c dd 36 f7 | 49 65 a5 ad 66 8b e1 8d | L.U.1.6..F..f.. | 00001460 | 00 00 00 00 00 00 00 00 | 04 00 00 00 04 00 00 00 | B..... |
| 00001480 | a5 7b 73 47 a3 b7 d4 98 | 09 a9 8b 0b b7 2b e6 b6 | ...f...f...f...f | 00001470 | 7a 00 00 00 00 00 00 00 | 02 00 00 00 00 00 00 00 | B..... |

Hide Android Applications in Images

Axelle Aprville - FortiGuard Labs, Fortinet
 Ange Albertini, Corkami

BlackHat Europe, Amsterdam, NH
 October 2014



What is this all about?



Read the title! ;)

What is this all about?



Read the title! ;)

Hiding

What is this all about?



Read the title! ;)

Hiding Android Applications

What is this all about?



Read the title! ;)
Hiding **Android Applications**
in ...

What is this all about?



Read the title! ;)
Hiding Android Applications
in ... images

Who are we?



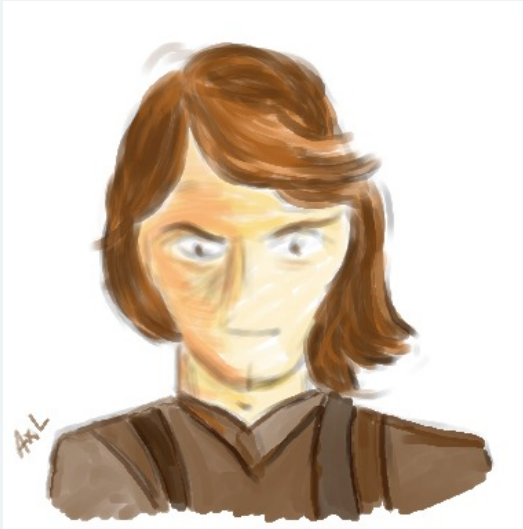
Axelle

```
axelle = {  
    'realname' : 'Axelle Apvrille',  
    'job' : 'Mobile/IoT Malware Analyst and Research',  
    'company' : 'Fortinet, FortiGuard Labs' }
```

Ange

```
ange = {  
    'realname' : 'Ange Albertini',  
    'hobby' : 'Corkami' }
```

What is this?



Nice? Thanks that's GIMP art from me ;)

It's an image!



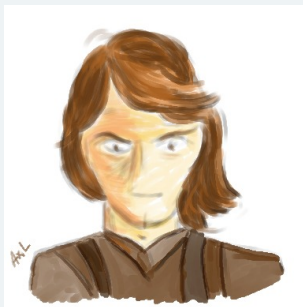
file says...

anakin.png: PNG image data, 636298042 x 1384184774, 19-bit

PNG file format

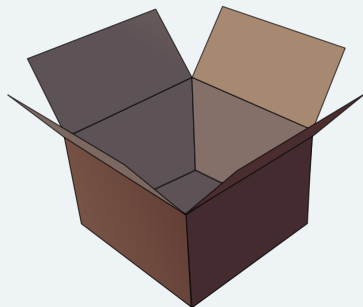
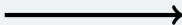
```
89 50 4e 47 0d 0a 1a 0a 00 01 b4 40 61 61 61 61 |.PNG.....0a
25 ed 23 3a 52 80 fb c6 13 cc 54 4d 74 f5 78 87 |%.# :R.....Tmt
ba 7d b5 f6 93 63 43 f0 e0 b9 99 9b 37 06 cc 8f |.}...cC.....7
32 59 5b 55 da 14 e2 87 68 f7 89 e5 88 14 fe 76 |2Y[U....h....
3e 0b cd 65 ec c4 7a 71 4d 95 c0 4e de 48 30 91 |>..e...zqM...N
...
```

It is more than that!



Valid PNG

AES Decrypt



Valid Android Package (APK)

Embed this “PNG” in an Android app?

Imagine...

...if that PNG/APK is malicious!

- ▶ (Nearly) invisible to reverse engineering!
- ▶ The Android app is **encrypted**

Arg! What will I see?

- ▶ A **fat** image
- ▶ The wrapping application
 - ▶ Code that decrypts an asset
 - ▶ Code that loads/installs an application

But that depends how well the wrapping app is written
It can be *obfuscated*...



Party time!
Demo!
Wake up!

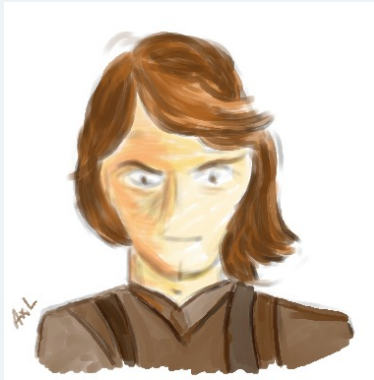
The APK looks genuine

Archive: PocActivity-debug.apk

| Length | Date | Time | Name |
|--------|------------|-------|----------------------------|
| 508720 | 2014-09-11 | 13:41 | assets/anakin.png |
| 1272 | 2014-09-11 | 14:03 | res/layout/main.xml |
| 1988 | 2014-09-11 | 14:03 | AndroidManifest.xml |
| 1444 | 2014-09-11 | 14:03 | resources.arsc |
| 7515 | 2014-09-11 | 14:03 | res/drawable-hdpi/logo.png |
| 2455 | 2014-09-11 | 14:03 | res/drawable-ldpi/logo.png |
| 4471 | 2014-09-11 | 14:03 | res/drawable-mdpi/logo.png |
| 8856 | 2014-09-11 | 14:03 | classes.dex |
| 634 | 2014-09-11 | 14:03 | META-INF/MANIFEST.MF |
| 687 | 2014-09-11 | 14:03 | META-INF/CERT.SF |
| 776 | 2014-09-11 | 14:03 | META-INF/CERT.RSA |
| 538818 | | | 11 files |

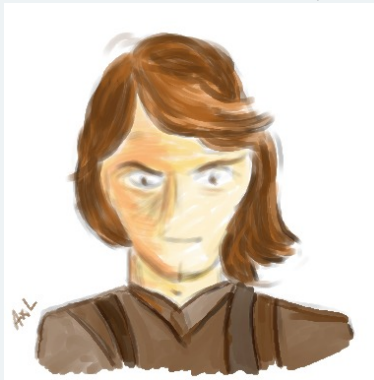
In case the demo crashes - lol

The image looks genuine: assets/anakin.png



In case the demo crashes - lol

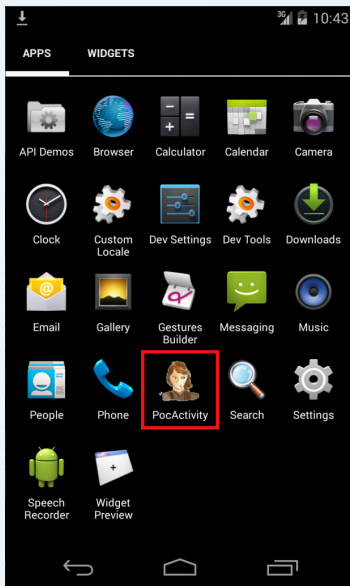
The image looks genuine: assets/anakin.png



Perhaps a bit 'fat'

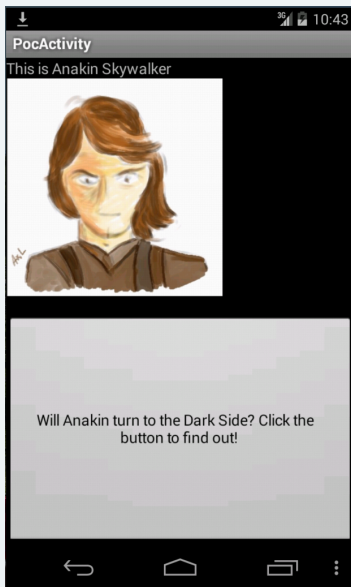
508720 bytes (\approx 500K) for 382x385 pixels

In case the demo crashes - lol

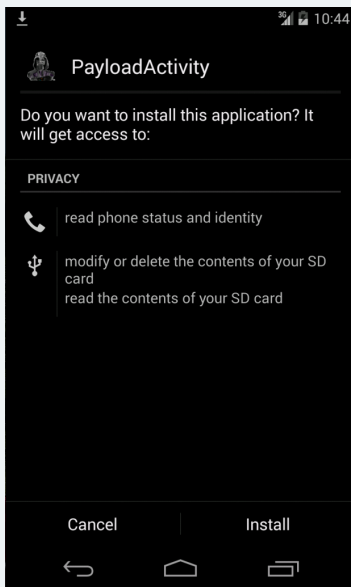


```
adb install  
WrappingApk.apk
```


In case the demo crashes - lol

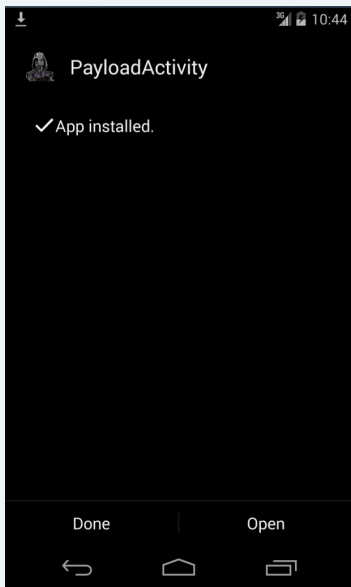


In case the demo crashes - lol



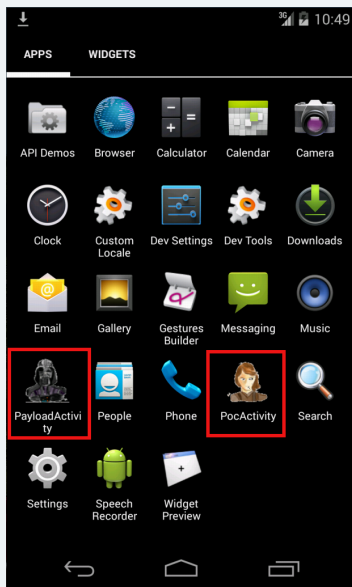
We could use
DexClassLoader to
hide this

In case the demo crashes - lol



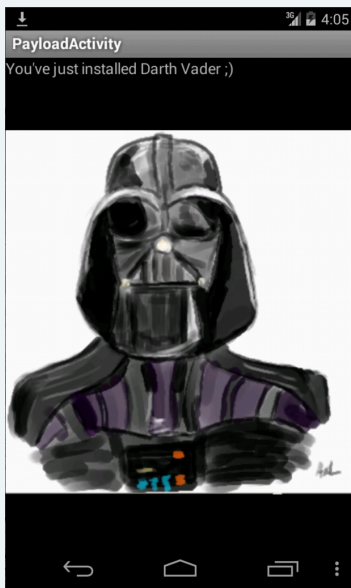
We could use
DexClassLoader to
hide this

In case the demo crashes - lol



We could use
DexClassLoader to
hide this

In case the demo crashes - lol



Payload gets
executed

How do we do that?



1. We write a payload APK

How do we do that?



1. We write a payload APK
2. We encrypt it using AngeCryption: it looks like a valid PNG

How do we do that?



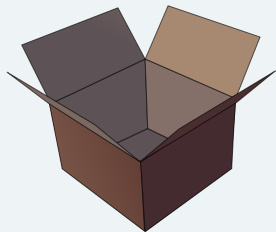
1. We write a payload APK
2. We encrypt it using AngeCrypton: it looks like a valid PNG
3. We hack it (a little)

How do we do that?

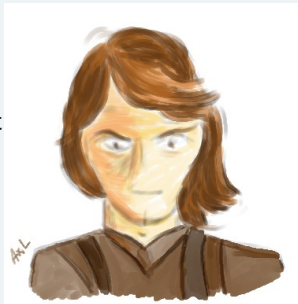


1. We write a payload APK
2. We encrypt it using AngeCryption: it looks like a valid PNG
3. We hack it (a little)
4. We implement another APK containing the PNG

Power: controlling encryption!



encrypt
.....→



Android Package (APK)
Plaintext

Genuine PNG
Ciphertext

Is this possible?

key: 'MySecretKey12345'

block: 'a block of text.'

7 ◀ nLi ☀ ← ∞ L f·iû▶
(BF 11 6E CA 69 DE 0F 1B EC C0 C6 F9 69 96 D0 10)

key: 'MySecretKey12346'

block: 'a block of text.'

gO†η ÑëΩcë ▼ LÇkllî
(67 4F C5 BB A5 89 EA 63 89 20 1F 4C 80 6B D0 8C)

key: 'MySecretKey12345'

block: 'a block of text!'

wεll—■y&↑ú@αùαφ♣O
(77 EE CA 16 DC 79 26 12 A3 40 E0 97 E0 ED 05 4F)

Can we control the output?



With a **tiny change** in the key in the key or the block, the output block is **completely different**

Can we control the output?



With a **tiny change** in the key in the key or the block, the output block is **completely different**

We can't control the output
The output block is (more or less) 'unpredictable'

Can we control the output?



With a **tiny change** in the key in the key or the block, the output block is **completely different**

We can't control the output
The output block is (more or less) 'unpredictable'

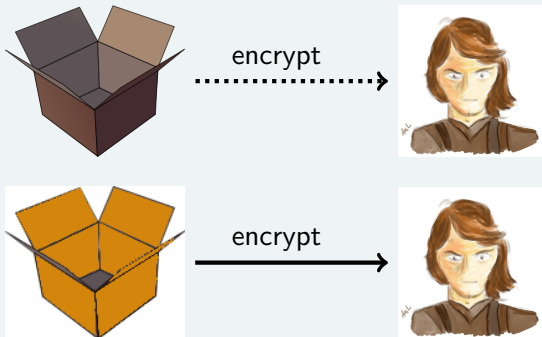
Yes, we can!
But there's a **trick** - **AngeCryption**

Controlling AES with AngeCryption

It will look the same ... but be slightly different

The APK **will look the same** to Android

The PNG **will look the same** to our eyes



Android does not see the diff Your eye does not see the diff
Manipulate Plaintext so that it encrypts to this PNG

Trick no. 1: dummy PNG chunk

Header: 0x89 PNG \r \n 0x1a \n

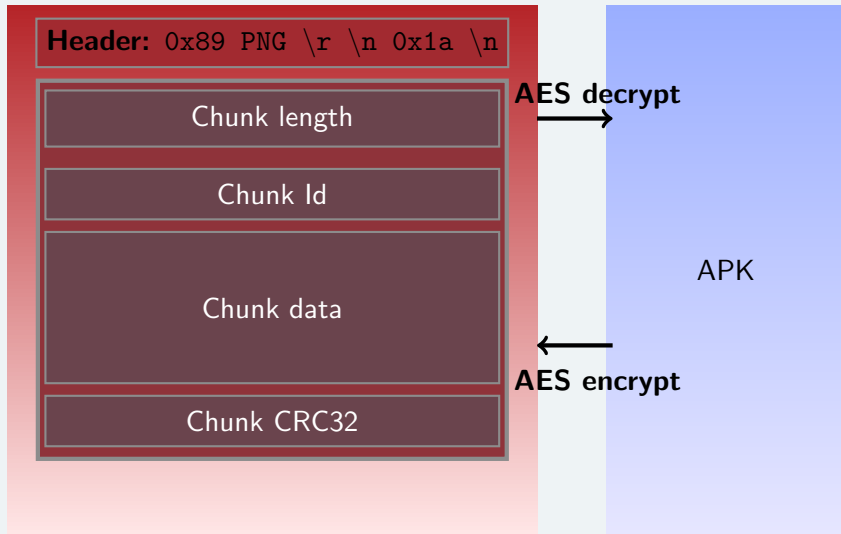
Chunk length

Chunk Id

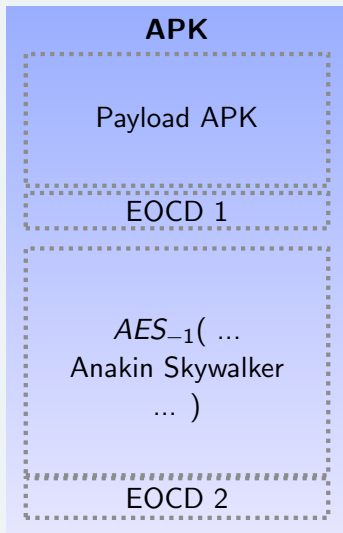
Chunk data

Chunk CRC32

Trick no. 1: dummy PNG chunk



Trick no. 2: appended zip data





- ▶ AES is a **block cipher**
- ▶ It can only process a **block of 16 bytes**

What if my plaintext is longer?!

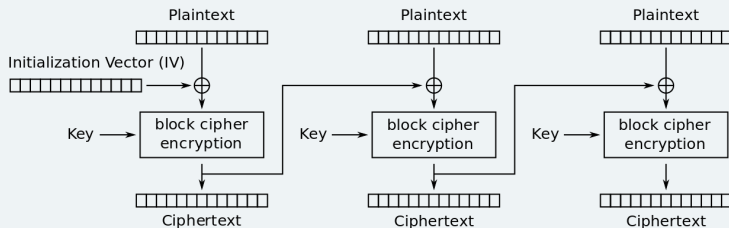
Chaining - 101

- ▶ We use **chaining**
- ▶ We apply **AES** on **block**
- ▶ ... well, that's for ECB (Electronic Code Book). Not very good.

Other chainings

- ▶ CBC, CFB, OFB... (see FIPS 81)
- ▶ We'll use **CBC** : **C**ipher **B**lock **C**haining

Cipher Block Chaining (CBC) - 101



Cipher Block Chaining (CBC) mode encryption

IV is **Initialization Vector**

Trick no.3: controlling first block

- ▶ We have our **plaintext** P_0 and **ciphertext** C_0
- ▶ We select a **key** K
- ▶ We compute **IV**: $IV = AES_K^{-1}(C_0) \oplus P_0$

Trick no.4: controlling other blocks

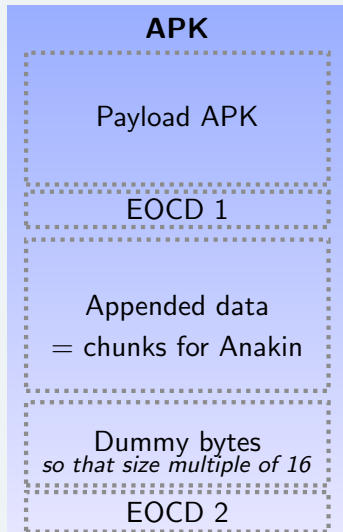
Basically... obvious!

Encrypting then decrypting is like doing nothing and reciprocally

Want ciphertext to be bitmap of Anakin?

Select $plaintext = AES_{-1}(bitmapofAnakin)$

$AES(plaintext) = AES(AES_{-1}(bitmapofAnakin)) = \text{bitmap of Anakin}$



PNG

APK

Payload APK

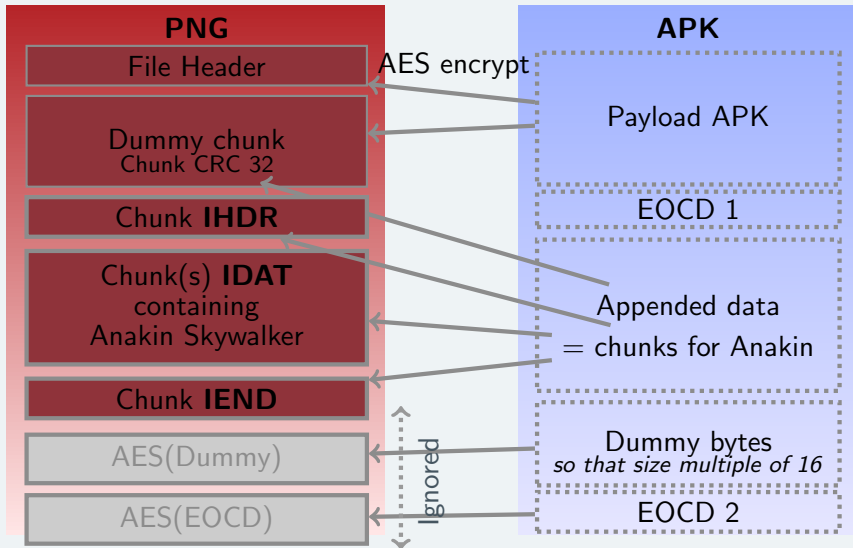
EOCD 1

Appended data
= chunks for Anakin

Dummy bytes
so that size multiple of 16

EOCD 2

Full picture



Thank You !

Status

Works on Android 4.4.2

June 2014: Android Security Team notified \approx fixed

Contact info

Me: **@cryptax** or aapvrille at fortinet dot com

Ange: **@angealbertini** or ange at corkami dot com

References

AngeCryption:

<http://corkami.googlecode.com/svn/trunk/src/angecryption/>

Code: <https://github.com/cryptax/angeapk> - *soon after conf'*

Corkami: <https://code.google.com/p/corkami/>

Fortinet's blog: <http://blog.fortinet.com>

Thanks to : @veorq, Android Security Team