

Hide Android Applications in Images

Axelle Aprville - FortiGuard Labs, Fortinet
Ange Albertini, Corkami

BlackHat Europe, Amsterdam, NH
October 2014

00001160	8d eb 6b 46	fb e2 2b 0e	13 f5 5e 93	85 9c 1f da	.xkF+.+.+.x	00001160	30 00 41 28	00 00 00 61	65 61 62 69	00 01 1e 00	0.A(._.seabi....
00001170	5d e8 6b 1f	cc d2 86 78	13 07 1e 4d	f4 63 c7 a...x...M.c.	00001160	00 00 05 35	54 45 00 06	04 08 01 09	01 12 04 14	...5TE.....	
00001180	99 b1 90 06	96 46 89 0d	78 4f 07 0c	1b aa 0e 85	a...FY.30....	00001170	01 15 01 17	03 18 01 19	01 1a 02 00	2e 73 68 73	...tntab..interp..h
00001190	61 08 a1 9e	99 5e d9 19	7c 81 ba 54	55 05 92 8d	.7.S.&.....TU..	00001180	74 72 74 61	62 00 2e 69	64 75 62 70	00 00 2e 68	tntab..interp..h
000011a0	fb 21 24 c2	9b 26 0d 02	22 9a 8a	aa 76 2e 1c 8f	/S.&.....TU..	00001190	61 73 68 00	2e 64 79 6e	73 79 6d 00	2e 64 79 6e	tntab..interp..h
000011b0	b4 03 1d 7d	12 3f 0f 6e	54 37 57	c6 4b 76 36 cf	.7.?.nT7M.Kv6..	000011a0	73 74 72 00	2e 72 65 6c	2e 70 6c 74	00 2a 74 65	tntab..interp..h
000011c0	8d 45 94 9e	47 4b 7e da	55 37 63	c0 99 ce a5 77	.E.. G..U.c..Ew	000011b0	78 74 00 2e	72 6f 64 61	74 61 00 2e	70 72 65 69	tntab..interp..h
000011d0	43 98 6f 2e	50 89 c0 92	1 f2 ae af	af 96 44 6f	C8.P.....Do	000011c0	6e 69 74 5f	61 72 72 61	79 00 2e 69	6e 69 74 5f	tntab..interp..h
000011e0	49 36 c2 61	66 c6 40 e8	Fe 6a 44	2c 54 88 47	L..af..B..jD.T	000011d0	61 72 72 61	79 00 2e 66	69 6e 69 5f	61 72 72 61	tntab..interp..h
000011f0	17 aa c1 92	7e 9b 4c f8	05 67 19	53 0c 06 0f	...3F..l.g..S..	000011e0	63 00 2e 67	67 74 00 2e	62 73 73 00	2e 63 6f 69	tntab..interp..h
00001200	c1 b4 0d 33	46 8e da 73	22 43 7f	5c f8 da 12 b6	...Bu..C.N....	00001200	6d 65 6e 74	00 2a 41 52	4d 2e 61 74	74 72 69 62	tntab..interp..h
00001210	a3 93 e5 b5	38 79 96 f0	22 43 7f	5c f8 da 12 b6	...Bu..C.N....	00001210	75 74 65 73	00 00 00 00	00 00 00 00	00 00 00 00	tntab..interp..h
00001220	de 67 3b 6b	02 b3 70 4a	90 18 04	86 03 20 01 1e	.g.kj..p.j....	00001220	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	tntab..interp..h
00001230	76 29 3c 26	e6 ee 85 32	02 11 35	a4 a4 1f 3a 78	v)<R..Z.....x	00001230	06 00 00 00	01 00 00 00	02 00 00 00	d4 80 00 00	tntab..interp..h
00001240	36 42 f1 5a	24 86 1f 9e	33 35 ff	82 b3 06 05 2e	6B.Z...35....	00001240	06 00 00 00	01 00 00 00	02 00 00 00	d4 80 00 00	tntab..interp..h
00001250	ea b6 f6 20	c4 c4 c4 c4	11 90 00	04 00 00 00	00001250	06 00 00 00	01 00 00 00	02 00 00 00	d4 80 00 00	tntab..interp..h
00001260	1e 89 92 e2	e5 e5 e5 e5	49 06 05	0f 9d 9e fc 0c	...3F..s1..U..	00001260	04 01 00 00	10 00 00 00	21 00 00 00	03 00 00 00	tntab..interp..h
00001270	03 27 d1 a5	64 64 64 64	44 34 e2	6b 5c 3b bc 91	.U..m...4....	00001270	03 00 00 00	00 00 00 00	04 00 00 00	04 00 00 00	tntab..interp..h
00001280	df 9e 38 04	9f bc fc 2c	77 d2 73	ba ea c2 39 72	...m...s...9P	00001280	19 00 00 00	0b 00 00 00	02 00 00 00	04 81 00 00	tntab..interp..h
00001290	f5 0a 83 34	3a b5 de 83	68 32 4d	50 c3 b6 9a deh2MP....	00001290	04 01 00 00	00 02 00 00	04 00 00 00	01 01 00 00	tntab..interp..h
000012a0	c0 24 e7 68	23 75 83 83	1e 8a e2	ad c5 17 ac 56	.\$.huu.....V	000012a0	04 00 00 00	10 00 00 00	21 00 00 00	03 00 00 00	tntab..interp..h
000012b0	1a 17 83 0e	b6 9c 17 0c	84 ad 3c	2d 03 ff 1a 82<.....	000012b0	02 00 00 00	b4 83 00 00	b4 03 00 00	05 01 00 00	tntab..interp..h
000012c0	f1 e2 9f 9c	fb e6 2e a5	66 97 71	99 da 6e c3 88f..q..n..	000012c0	00 00 00 00	00 00 00 00	01 00 00 00	00 00 00 00	tntab..interp..h
000012d0	8b 3a b4	b3 38 67 8a 84	af af 88	f8 14 56 1d 40 823.g...V.8	000012d0	29 00 00 00	09 00 00 00	02 00 00 00	00 bc 84 00 00	tntab..interp..h
000012e0	e2 c3 87	58 0f 9a 9c 81	b7 88 8b	fd a2 85 96 73	...b...8...8...	000012e0	06 04 00 00	98 00 00 00	03 00 00 00	06 00 00 00	tntab..interp..h
000012f0	62 c3 87	58 0f 9a 9c 81	b7 88 8b	fd a2 85 96 73	...b...8...8...	000012f0	06 04 00 00	98 00 00 00	03 00 00 00	06 00 00 00	tntab..interp..h
00001300	e2 74 73	f4 0a 33 ca c2	4e 10 5d	6d 82 09 10 28	...3..N.e...S	00001300	00 00 00 00	00 00 00 00	04 00 00 00	04 00 00 00	tntab..interp..h
00001310	64 1b ec	dd b0 4a c7 1e 12	50 a3 4a	65 17 86 16 6b	d.....2....S	00001310	32 00 00 00	01 00 00 00	06 00 00 00	50 86 00 00	tntab..interp..h
00001320	8f 59 1b	88 ab c8 d8 69	bb 41 48	e2 e8 e3 6e 63 6e	d.....2....S	00001320	32 00 00 00	01 00 00 00	06 00 00 00	50 86 00 00	tntab..interp..h
00001330	85 a7 1c	32 55 24 de d1	e2 84 3c	b9 1e 7d 9d 1f	U..2....S...	00001330	32 00 00 00	01 00 00 00	06 00 00 00	50 86 00 00	tntab..interp..h
00001340	a5 55 9f	5e 0b 9a c8 3e	89 64 21	61 62 16 d6 06	U..2....S...	00001340	32 00 00 00	01 00 00 00	06 00 00 00	50 86 00 00	tntab..interp..h
00001350	df 6f c1	e1 5e 1d 9b c8	32 15 2b	09 42 c5 53 91	...o.q...2.+B.S.	00001350	00 00 00 00	00 00 00 00	04 00 00 00	01 00 00 00	tntab..interp..h
00001360	01 09 2a	c2 9e 1e 85 93	59 f9 e5	f1 18 7d 20 29	...*.Y...j..	00001360	40 00 00 00	10 00 00 00	03 00 00 00	00 90 00 00	tntab..interp..h
00001370	4b 06 1c	d8 bc f2 7f 65	54 aa a3	84 91 45 77 95	K.....FT...E..	00001370	00 10 00 00	08 00 00 00	00 00 00 00	00 00 00 00	tntab..interp..h
00001380	5e 1f 5a	f6 fc fd bc 05 60	fd d5 6f	41 6e bc 1a feo.n....	00001380	01 00 00 00	00 00 00 00	4f 00 00 00	0e 00 00 00	tntab..interp..h
00001390	1a 17 83 0e	b6 9c 17 0c	84 ad 3c	2d 03 ff 1a 82<.....	00001390	03 00 00 00	08 90 00 00	08 10 00 00	08 00 00 00	tntab..interp..h
000013a0	93 e2 77	ca 55 ed 0a ba	6e 40 58	08 bf 09 77 8b	...U..n..X..w..	000013a0	00 00 00 00	00 00 00 00	01 00 00 00	01 00 00 00	tntab..interp..h
000013b0	e1 dd 6b	6c 77 27 1e d5	22 4f 4c	b5 66 9f 79 b6	.kmu'..KL.f.y..	000013b0	5b 00 00 00	0f 00 00 00	03 00 00 00	10 90 00 00	tntab..interp..h
000013c0	0e 3a 48	71 28 81 d6 11	74 48 5e	a4 f3 e4 e9 27	.Hn'..tH'....	000013c0	10 10 00 00	08 00 00 00	00 00 00 00	00 00 00 00	tntab..interp..h
000013d0	6d 8e 44	52 e4 bb c4 42	a5 ba 09	42 c5 53 91	...*.Y...j..	000013d0	00 00 00 00	00 00 00 00	04 00 00 00	01 00 00 00	tntab..interp..h
000013e0	1a 17 83 0e	b6 9c 17 0c	84 ad 3c	2d 03 ff 1a 82<.....	000013e0	00 00 00 00	00 00 00 00	04 00 00 00	01 00 00 00	tntab..interp..h
000013f0	ff c9 33	80 33 30 33	8a 2e 0c	ec 2c 2c 2c 2c	000013f0	00 00 00 00	00 00 00 00	01 00 00 00	00 00 00 00	tntab..interp..h
00001400	4d 21 47	c5 af 03 de e0	8a 2e 0c	91 70 d8 db da	.IG.....p..	00001400	0e 00 00 00	06 00 00 00	00 00 00 00	20 90 00 00	tntab..interp..h
00001410	48 f9 9e	18 d8 e8 26 b9	f7 aa 0e	47 01 5c d2 43	H.....	00001410	10 00 00 00	c8 00 00 00	04 00 00 00	00 00 00 00	tntab..interp..h
00001420	fd 57 0f	ca ee c3 6f	d2 59 95	15 31 55 0d 51	.U..	00001420	00 00 00 00	08 00 00 00	00 00 00 00	01 00 00 00	tntab..interp..h
00001430	04 b7 46	ae af ab 9a 17	d4 79 9d	97 05 95 1e c2	.F.....	00001430	03 00 00 00	e8 90 00 00	e8 10 00 00	58 00 00 00	tntab..interp..h
00001440	4c 8d 75	fc 6c 36 f7	d9 66 a5	ad 66 8b e1 8d	.U.. B..F..F..	00001440	00 00 00 00	00 00 00 00	04 00 00 00	04 00 00 00	tntab..interp..h
00001450	a5 70 73	d7 d7 d7 d7	d7 d7 d7	d7 d7 d7	00001450	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	tntab..interp..h





- ▶ What is this all about? (quick)
- ▶ Who are we? (quick)
- ▶ Demo
- ▶ Details!

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

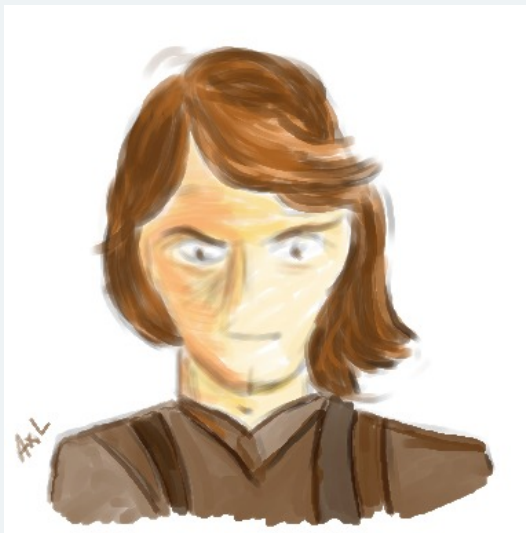
Axelle

```
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!



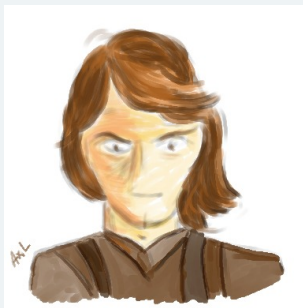
file says...

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

PNG file format

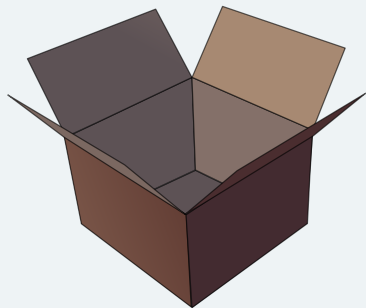
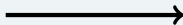
```
89 50 4e 47 0d 0a 1a 0a 00 01 b4 40 61 61 61 61 |.PNG.....0a
25 ed 23 3a 52 80 fb c6 13 cc 54 4d 74 f5 78 87 |%.#:R.....Tmt
ba 7d b5 f6 93 63 43 f0 e0 b9 99 9b 37 06 cc 8f |.}...cC.....7
32 59 5b 55 da 14 e2 87 68 f7 89 e5 88 14 fe 76 |2Y[U...h...
3e 0b cd 65 ec c4 7a 71 4d 95 c0 4e de 48 30 91 |>..e...zqM..N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

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*...



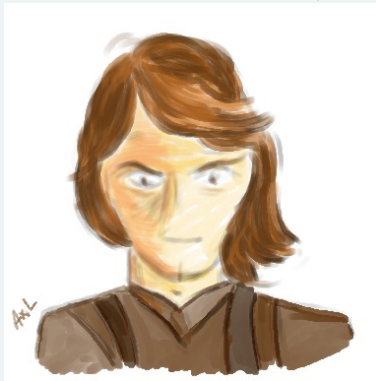
Party time!
Demo!
Wake up!

The APK looks genuine

Archive: PocActivity-debug.apk

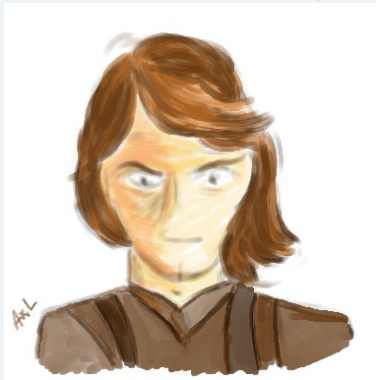
Length	Date	Time	Name
508720	2014-09-11	13:41	assets/anakin.png
1272	2014-09-11	14:03	res/layout/main.xml
1988	2014-09-11	14:03	AndroidManifest.xml
1444	2014-09-11	14:03	resources.arsc
7515	2014-09-11	14:03	res/drawable-hdpi/logo.png
2455	2014-09-11	14:03	res/drawable-ldpi/logo.png
4471	2014-09-11	14:03	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

The image looks genuine: `assets/anakin.png`



In case the demo crashes - lol

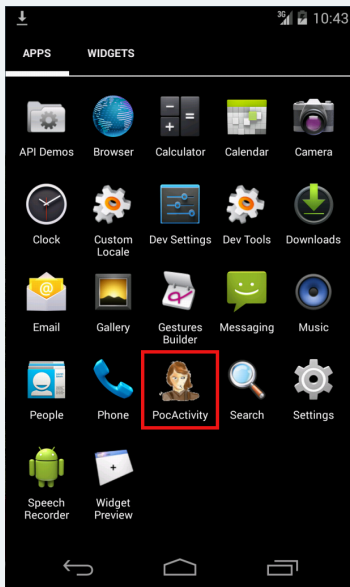
The image looks genuine: assets/anakin.png



Perhaps a bit 'fat'

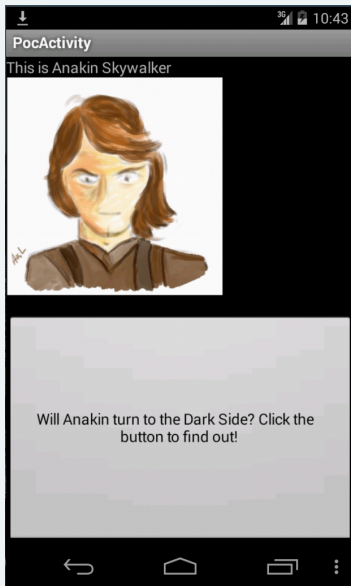
508720 bytes (\approx 500K) for 382x385 pixels

In case the demo crashes - lol

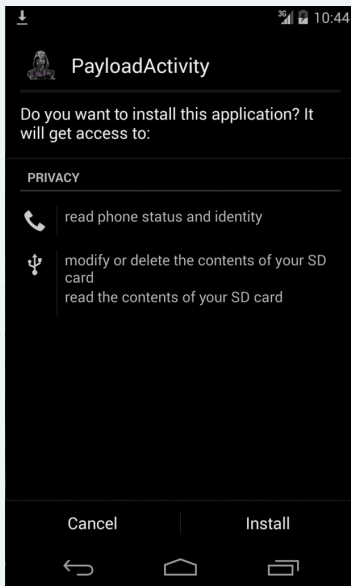


```
adb install  
WrappingApk.apk
```

In case the demo crashes - lol

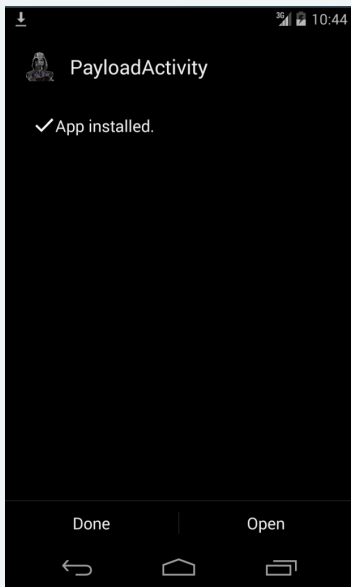


In case the demo crashes - lol



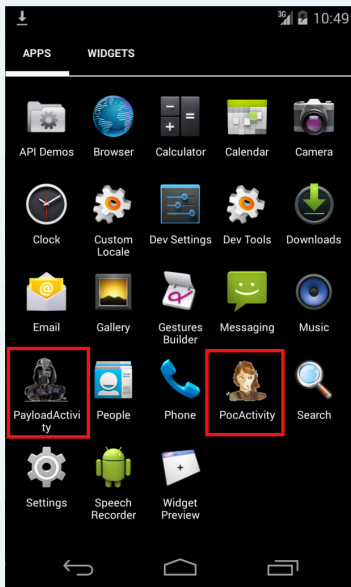
We could use
DexClassLoader to
hide this

In case the demo crashes - lol



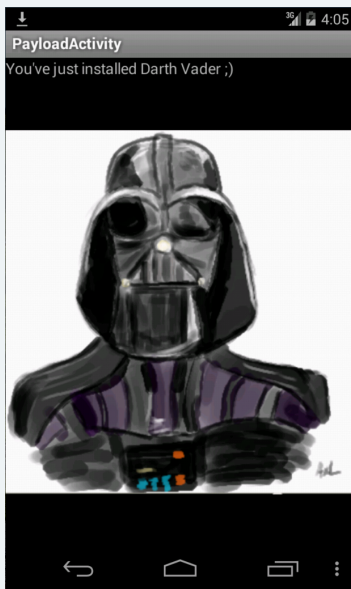
We could use
DexClassLoader to
hide this

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?



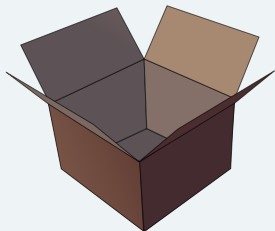
1. We write a payload APK
2. We encrypt it using AngeCryption: it looks like a valid PNG
3. We hack it (a little)

How do we do that?

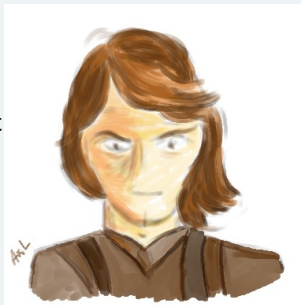


1. We write a payload APK
2. We encrypt it using AngeCryption: it looks like a valid PNG
3. We hack it (a little)
4. We implement another APK containing the PNG

Power: controlling encryption!



encrypt
.....→



Android Package (APK)
Plaintext

Genuine PNG
Ciphertext

Is this possible?

key: 'MySecretKey12345'

block: 'a block of text.'

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

key: 'MySecretKey12346'

block: 'a block of text.'

gO†⌈ 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@ααφ♣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'

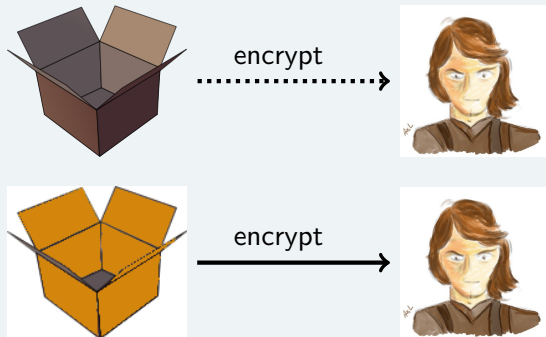
Yes, we can!
But there's a **trick** - **AngeCryption**

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

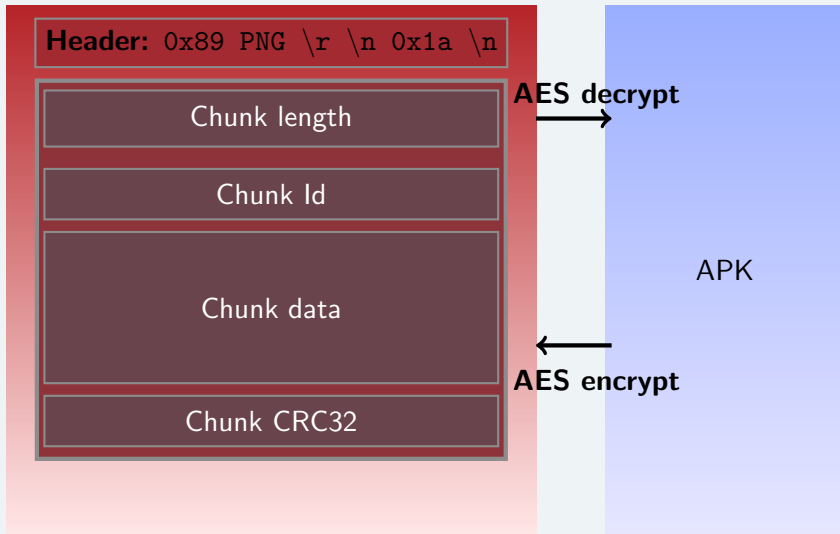
Header: 0x89 PNG \r \n 0x1a \n

Chunk length

Chunk Id

Chunk data

Chunk CRC32





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

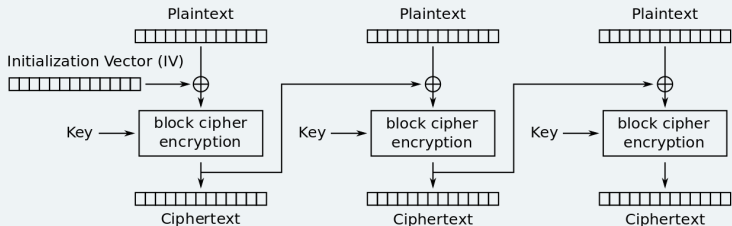
What if my plaintext is longer?!

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) mode encryption

IV is Initialization Vector

First block

- ▶ We have our **plaintext** P_0 and **ciphertext** C_0
- ▶ $C_0 = AES_K(P_0 \oplus IV)$
- ▶ We can choose the **key** K and **IV**!!!

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

Chunk length

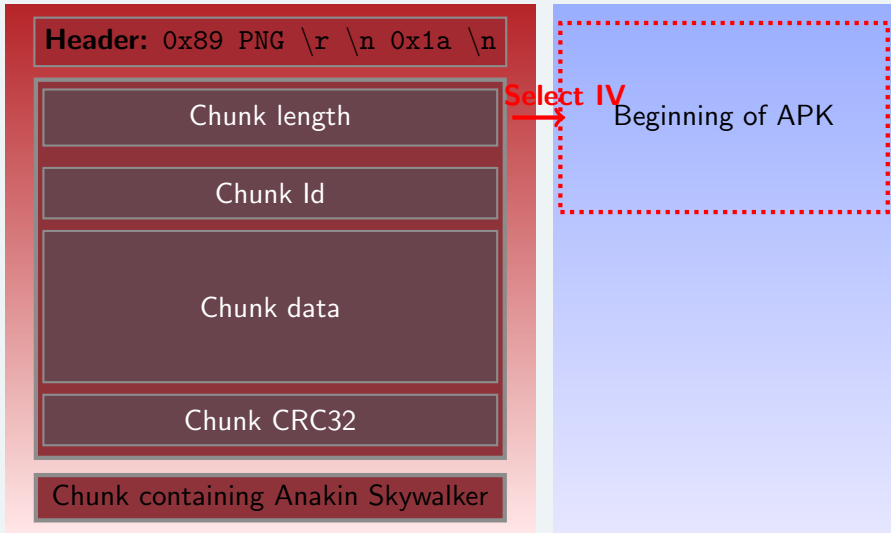
Chunk Id

Chunk data

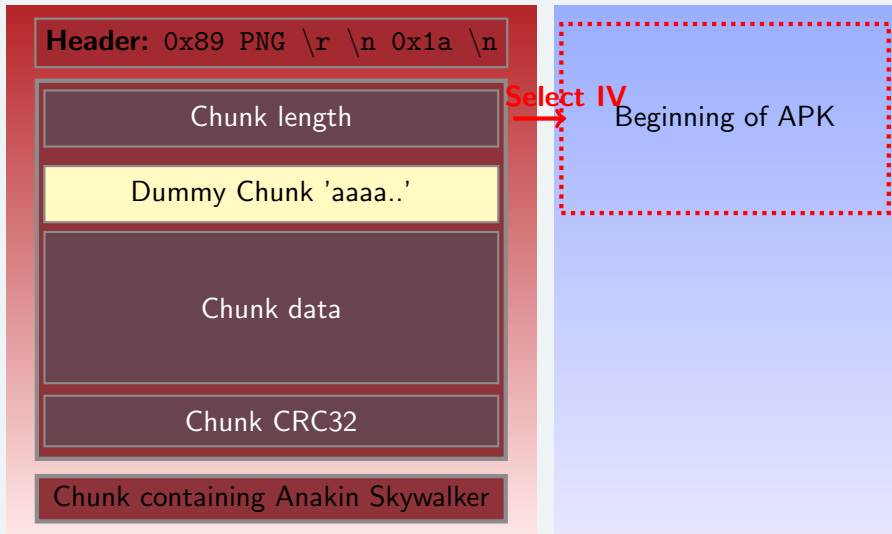
Chunk CRC32

Chunk containing Anakin Skywalker

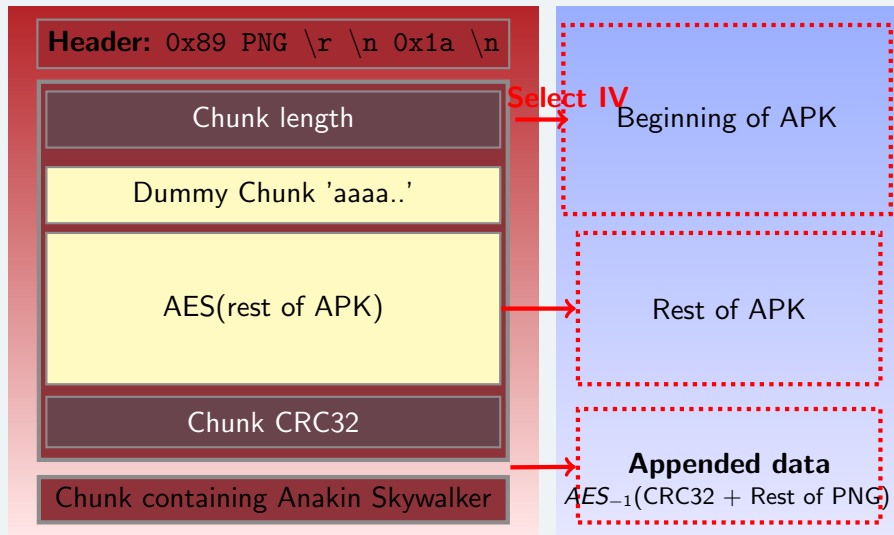
AngeCryption Explained



AngeCryption Explained



AngeCryption Explained



The 'similar' APK is 'perfect'... except Android won't load it!
(unzip does not like it either)

```
EOCD not found, not Zip  
file 'payload-similar.apk' is not a valid zip file
```

Why?

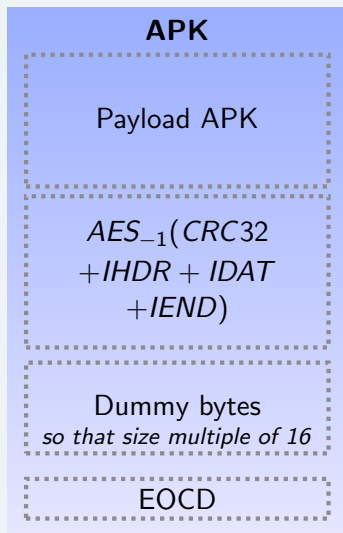
- ▶ EOCD is **End of Central Directory**: zip marker
- ▶ No EOCD at the end
- ▶ Too much appended data after EOCD

Solution

Let's add another EOCD at the end!

Will the APK still correspond to Anakin Skywalker?

YES



Will the APK still correspond to Anakin Skywalker?

YES

PNG



APK

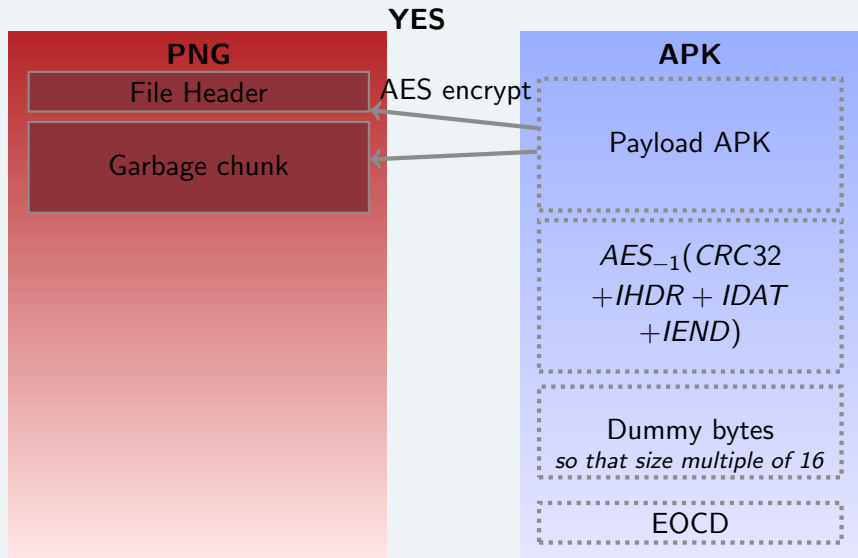
Payload APK

$AES_{-1}(CRC32$
 $+ IHDR + IDAT$
 $+ IEND)$

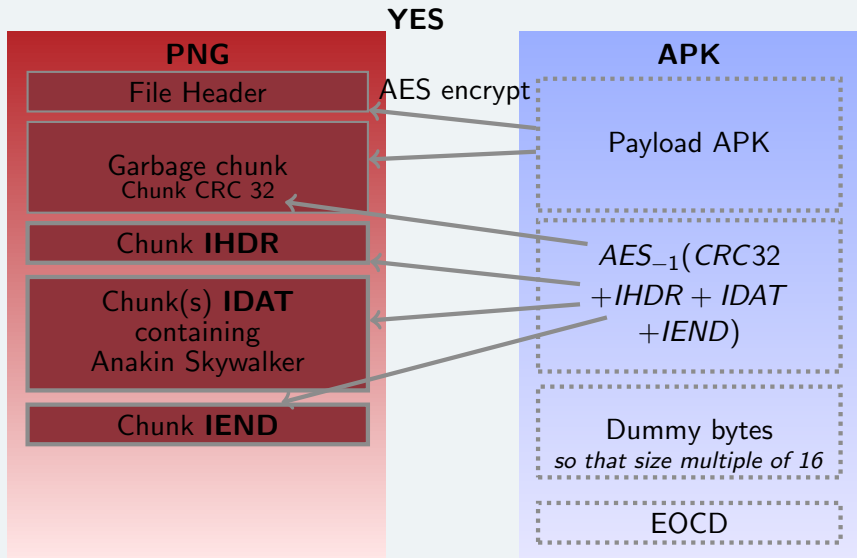
Dummy bytes
so that size multiple of 16

EOCD

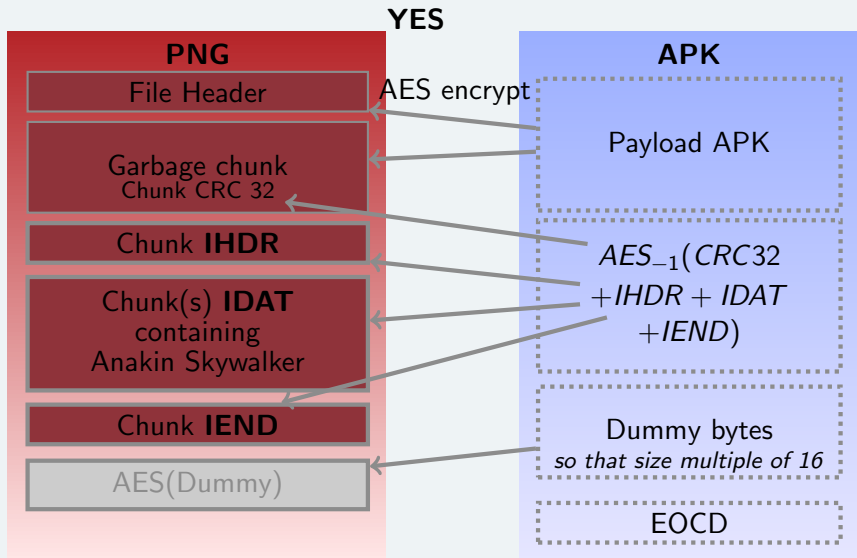
Will the APK still correspond to Anakin Skywalker?



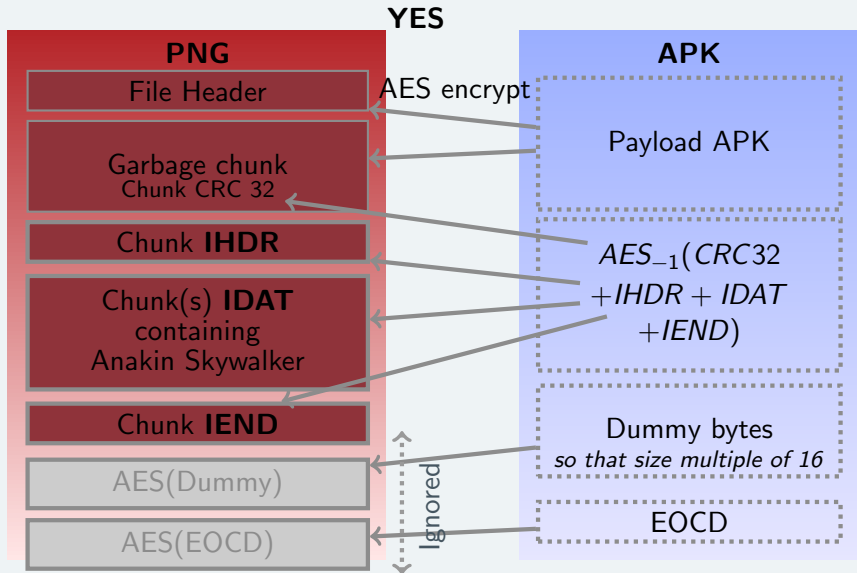
Will the APK still correspond to Anakin Skywalker?



Will the APK still correspond to Anakin Skywalker?



Will the APK still correspond to Anakin Skywalker?



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/angepryption/>

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

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

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

Thanks to : @veorq, Android Security Team