Доподписывались...

Mikhail Dudarev

Licel Corporation

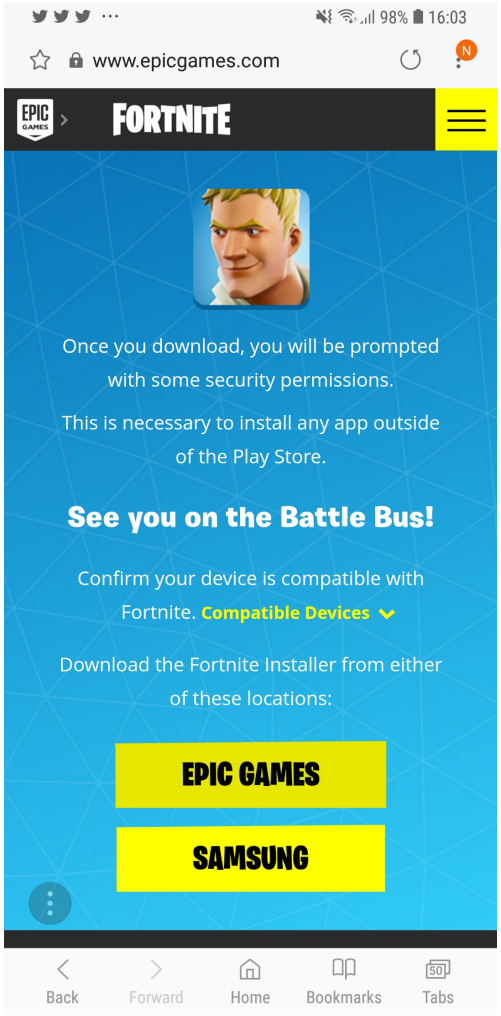
О нас

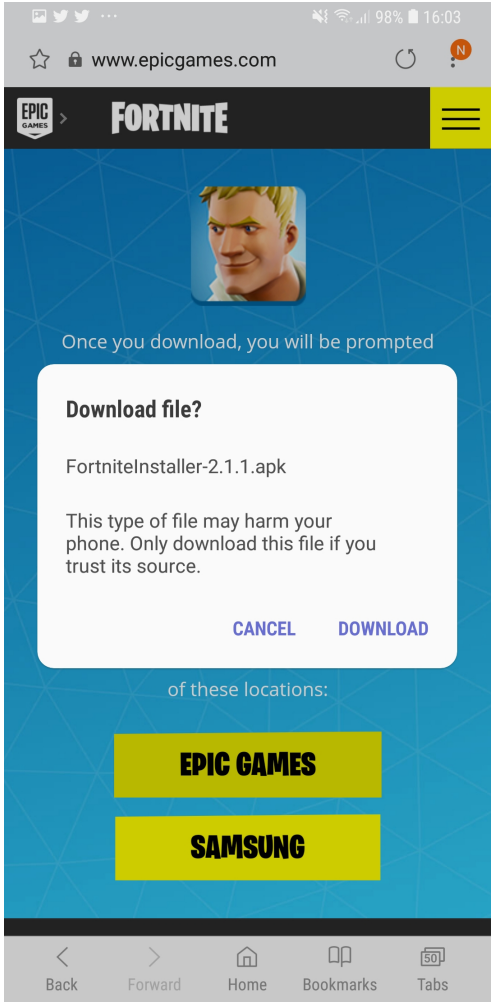
Licel Corporation

Web: https://licelus.com


FORTNITE

To get started, please visit fortnite.com/android on an Android device, or scan the QR code below.


98% 16:03
www.epicgames.com
FORTNITE
Once you download, you will be prompted with some security permissions.
This is necessary to install any app outside of the Play Store.
See you on the Battle Bus!
Confirm your device is compatible with Fortnite. Compatible Devices
Download the Fortnite Installer from either of these locations:
EPIC GAMES
SAMSUNG
Back
Forward
Home
Bookmarks
Tabs


98% 16:03
www.epicgames.com
FORTNITE
Once you download, you will be prompted
Download file?
FortniteInstaller-2.1.1.apk
This type of file may harm your phone. Only download this file if you trust its source.
CANCEL
DOWNLOAD
of these locations:
EPIC GAMES
SAMSUNG
Back
Forward
Home
Bookmarks
Tabs

Тест на переподпись

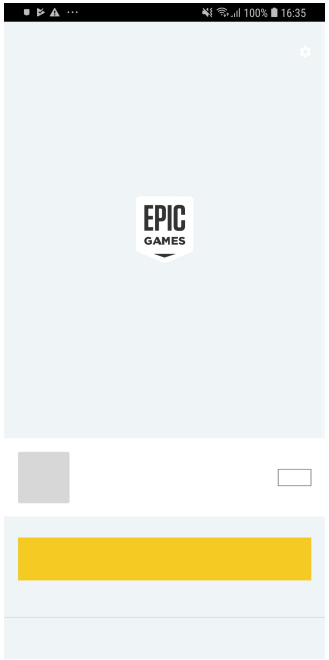
$ adb pull /sdcard/Download/FortniteInstaller-2.1.1.apk

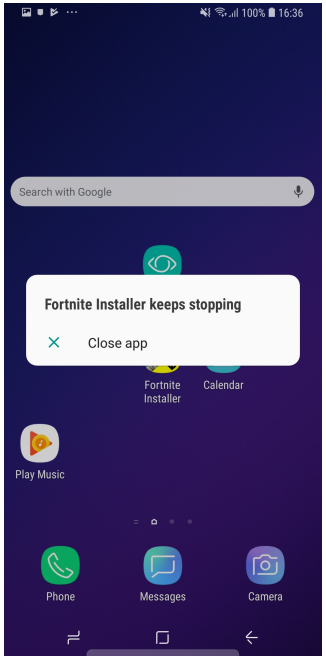
$ cp FortniteInstaller-2.1.1.apk HackedFortniteInstaller-2.1.1.apk

$ jarsigner -keystore sample.keystore HackedFortniteInstaller-2.1.1.apk -storepass android -keypass android android

$ adb install -r HackedFortniteInstaller-2.1.1.apk

Запускаем…


100% 16:35
EPIC
GAMES


100% 16:36
Search with Google
Fortnite Installer keeps stopping
Close app
Fortnite Installer
Calendar
Play Music
Phone
Messages
Camera

adb logcat

```
OkHttp  : {
OkHttp  :   "elements" : [ {
OkHttp  :     "appName" : "EpicGamesLauncher",
OkHttp  :     "labelName" : "Live-AnarchyAcres-Android",
OkHttp  :     "buildVersion" : "2.1.1-804d43d.b25+releaselive-Android",
OkHttp  :     "hash" : "708e3eadc80782eb49c53ca2655d928c27066603",
OkHttp  :     "metadata" : {
OkHttp  :       "androidSigningFingerprintSHA1" :
"70:75:66:F8:B0:9B:4C:8B:FD:77:2E:1B:53:6D:58:1F:19:BC:30:12",
OkHttp  :       "androidPackageVersionCode" : "6",
OkHttp  :       "buildTime" : "2018-08-22T19:09:28Z",
OkHttp  :       "androidPackageName" : "com.epicgames.portal"
OkHttp  :     }
```

Выводы

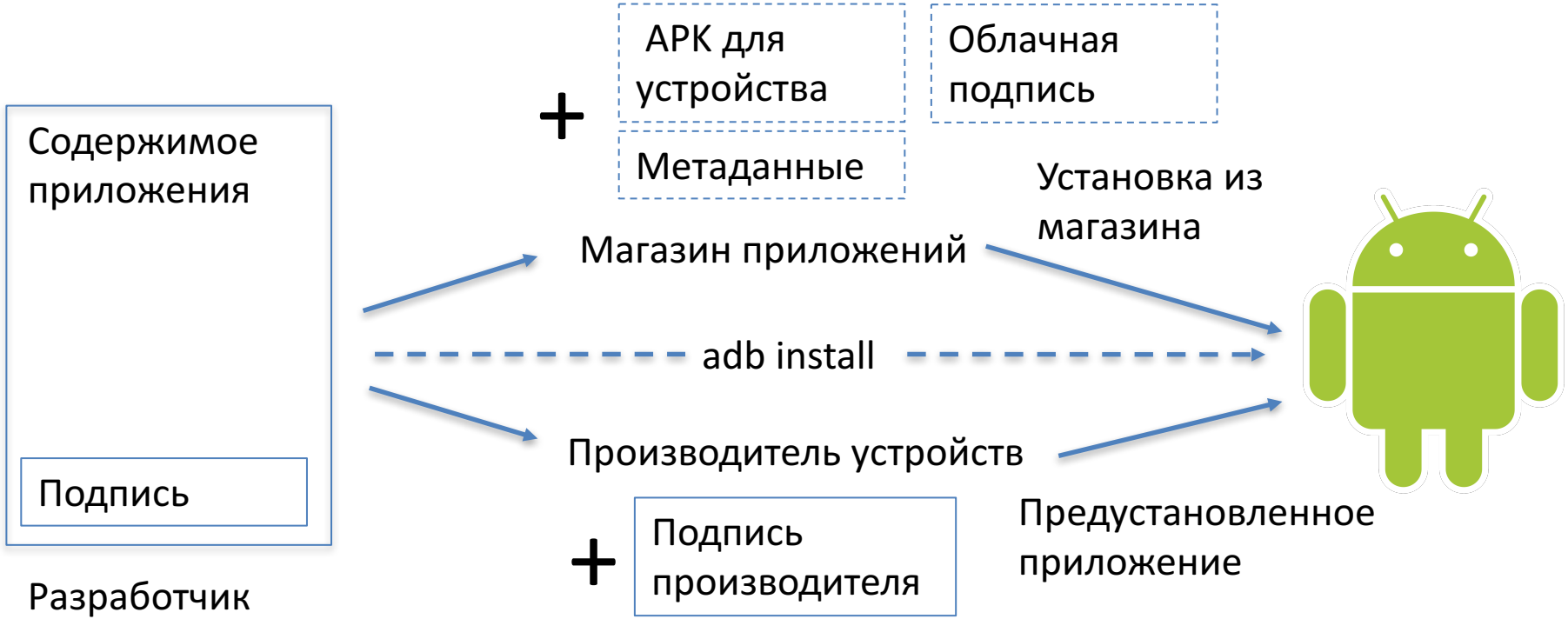
Цифровая подпись необходима, ЕСЛИ есть надежные способы проверить

- Владельца
- Права владельца
- Техническую корректность

Содержание

- Способы доставки приложений
- Контейнеры и их форматы
- Схемы подписи
- Google Play
- Выводы

Доставка приложений в Android



AAпчхи

APK

AAR

AAB

APKS

ZIP == JAR == APK ?

Структура JAR-архива

- META-INF
  - MANIFEST.MF
  - …
- Набор файлов

```
Manifest-Version: 1.0
Created-By: X.X.X _X (Test Corporation)
Attribute-1: ..
..
Atttribute-N: ..
```

Структура подписанного JAR-архива

- META-INF — Без подписи
  - MANIFEST.MF
  - …..
  - ALIAS.<RSA|DSA|ECDSA> — Подпись
  - ALIAS.SF
- Набор файлов — Подписано

ALIAS.<RSA|DSA|ECDSA>

```
> less META-INF/CERT.SF
```

Owner: CN=Epic Games, OU=Online, O=Epic Games, L=Cary, ST=North Carolina, C=US
Issuer: CN=Epic Games, OU=Online, O=Epic Games, L=Cary, ST=North Carolina, C=US
Serial number: 7ff9c6ee
Valid from: Thu Apr 19 20:28:25 MSK 2018 until: Fri Apr 06 20:28:25 MSK 2068
Certificate fingerprints:
MD5: D5:9C:16:5B:0E:1D:27:DF:97:C1:53:CC:8E:DE:EC:4D
SHA1: 70:75:66:F8:B0:9B:4C:8B:FD:77:2E:1B:53:6D:58:1F:19:BC:30:12
SHA256: 67:69:9A:6B:3D:31:5D:EE:51:53:6A:67:B4:F1:C6:E7:E2:17:5F:98:4B:09:6B:C2:97:6E:51:2D:22:94:08:71
Signature algorithm name: SHA256withRSA
Version: 3

ALIAS.SF

```
> less META-INF/CERT.SF
```

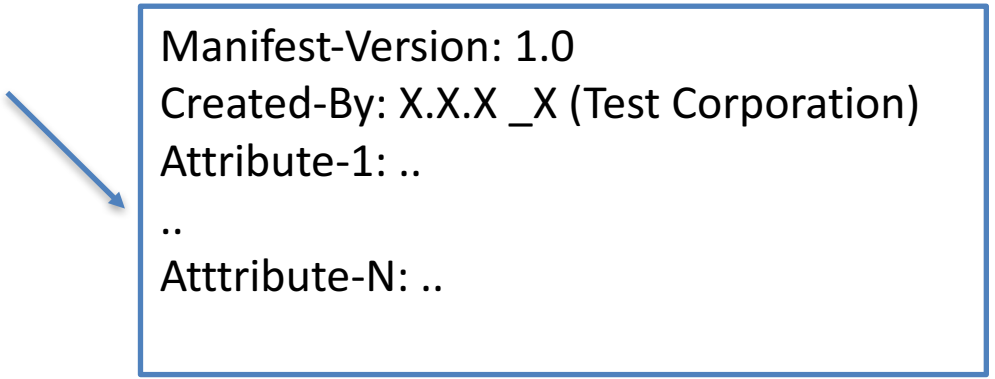
Signature-Version: 1.0
SHA1-Digest-Manifest-Main-Attributes: wx7wAKbM7DDeNhBgV2mNRTX9IN4=
SHA1-Digest-Manifest: pFsXCDP9sfW7FnlJ6BIcA14G8dA=
Created-By: 1.8.0_181 (Oracle Corporation)

Name: kotlin/collections/MapWithDefault.kotlin_metadata
SHA1-Digest: jsFC98b5KzSCNFy2T8vBNXVY810=

Name: res/anim/design_snackbar_in.xml
SHA1-Digest: EWX2SCUo5H5R93jvpTSxVoUJWQ0=

Структура подписаного APK-архива

- META-INF
  - MANIFEST.MF
  - …
- Набор файлов
  - AndroidManifest.xml
  - …




UFC
1

Создаем и подписываем Jar-архив

```
$ touch 1.txt
$ jar -vcf 1.jar 1.txt
$ jarsigner -keystore sample.keystore 1.jar android
```

Проверяем подпись

```
$ jarsigner -verify 1.jar
jar verified.
```

```
$ apksigner verify 1.jar
Exception in thread "main" com.android.apksig.apk.ApkFormatException: Missing
AndroidManifest.xml
```


UFC
2
WWW.UFC.COM
UFC

Добавляем пустой AndroidManifest.xml

```
$ touch 1.txt
$ touch AndroidManfist.xml
$ jar -vcf 1.jar 1.txt AndroidManfist.xml
$ jarsigner -keystore sample.keystore 1.jar android
```

Проверяем подпись

```
$ jarsigner -verify 1.jar
jar verified.
```

```
$ apksigner verify 1.jar
Exception in thread "main" com.android.apksig.apk.MinSdkVersionException: Failed to determine APK's minimum supported platform version.
Caused by: com.android.apksig.internal.apk.AndroidBinXmlParser$XmlParserException: No XML chunk in file
```


UFC
3
WWW.UFC.COM

JarSigner VS ApkSigner

Минимальный AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<manifest
xmlns:android="http://schemas.android.com/apk/res/android"
package="com.dexprotector.detector.envchecks"
platformBuildVersionCode="18" platformBuildVersionName="1.0”
/>
```

Добавляем минимальный AndroidManifest.xml

```
$ touch 1.txt
$ cp minimalAndroidManifest.xml AndroidManfist.xml
$ jar -vcf 1.jar 1.txt AndroidManfist.xml
$ jarsigner -keystore sample.keystore 1.jar android
```

Проверяем подпись

```
$ jarsigner -verify 1.jar
jar verified.

$ apksigner verify 1.jar
OK
```

ApkSigner под микроскопом

$ apksigner verify --minSdk 16 1.jar
JAR signer ANDROID.RSA: JAR signature META-INF/ANDROID.RSA uses digest algorithm SHA-256 and signature algorithm RSA which is not supported on API Level(s) 16-17 for which this APK is being verified

$ apksigner verify --verbose 1.jar
Verifies
Verified using v1 scheme (JAR signing): true
Verified using v2 scheme (APK Signature Scheme v2): false

Zip-архив

```
    00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
    -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
00: 50 4B 03 04 0A 00 00 00 00 00 DB 65 90 4C 53 FC
10: 51 67 02 00 00 00 02 00 00 00 01 00 1C 00 31 55
20: 54 09 00 03 0E 71 D4 5A C7 72 D4 5A 75 78 0B 00
30: 01 04 F5 01 00 00 04 14 00 00 00 31 0A 50 4B 01
40: 02 1E 03 0A 00 00 00 00 00 DB 65 90 4C 53 FC 51
50: 67 02 00 00 00 02 00 00 00 01 00 18 00 00 00 00
60: 00 01 00 00 00 A4 81 00 00 00 00 31 55 54 05 00
70: 03 0E 71 D4 5A 75 78 0B 00 01 04 F5 01 00 00 04
80: 14 00 00 00 50 4B 05 06 00 00 00 00 01 00 01 00
90: 47 00 00 00 3D 00 00 00 00 00
```

Zip-архив

```
     00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
     -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
00:  50 4B 03 04 0A 00 00 00 00 00 DB 65 90 4C 53 FC
10:  51 67 02 00 00 00 02 00 00 00 01 00 1C 00 31 55
20:  54 09 00 03 0E 71 D4 5A C7 72 D4 5A 75 78 0B 00
30:  01 04 F5 01 00 00 04 14 00 00 00 31 0A 50 4B 01
40:  02 1E 03 0A 00 00 00 00 00 DB 65 90 4C 53 FC 51
50:  67 02 00 00 00 02 00 00 00 01 00 18 00 00 00 00
60:  00 01 00 00 00 A4 81 00 00 00 00 31 55 54 05 00
70:  03 0E 71 D4 5A 75 78 0B 00 01 04 F5 01 00 00 04
80:  14 00 00 00 50 4B 05 06 00 00 00 00 01 00 01 00
90:  47 00 00 00 3D 00 00 00 00 00
```

End of Central Directory Record

File Data

Central Directory Record

Local File Header

Zip-архив (играем в прятки)

```
     00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
     -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
00:  50 4B 03 04 0A 00 00 00 00 00 DB 65 90 4C 53 FC
10:  51 67 02 00 00 00 02 00 00 00 01 00 1C 00 31 55
20:  54 09 00 03 0E 71 D4 5A C7 72 D4 5A 75 78 0B 00
30:  01 04 F5 01 00 00 04 14 00 00 00 31 0A .. .. ..
40:  50 4B 01 02 1E 03 0A 00 00 00 00 00 DB 65 90 4C
50:  53 FC 51 67 02 00 00 00 02 00 00 00 01 00 18 00
60:  00 00 00 00 01 00 00 00 A4 81 00 00 00 00 31 55
70:  54 05 00 03 0E 71 D4 5A 75 78 0B 00 01 04 F5 01
80:  00 00 04 14 00 00 00 .. .. .. 50 4B 05 06 00 00
90:  00 00 01 00 01 00 47 00 00 00 40 00 00 00 00 00
```

End of Central Directory Record

File Data

Central Directory Record

Local File Header

APK Signature 2

```
    00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
    -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
XX: FILE HEADER1 + DATA1, .. FILE HEADERN + DATAN
XX: 15 06 00 00 00 00 00 00 .. .. .. .. .. .. .. ..
XX: 66 85 63 86 66 AC D4 BA 5E 27 AA D3 9C 24 61 EF
XX: 9A E7 E5 86 6D 3A BE 1F 92 D8 3B A0 0A F3 5A 64
XX: 72 B7 15 02 03 01 00 01 15 06 00 00 00 00 00 00
XX: 41 50 4B 20 53 69 67 20 42 6C 6F 63 6B 20 34 32
XX: 50 4B 01 02 1E 03 0A 00 00 00 00 00 DB 65 90 4C
```

First Central Directory Record

APK Signature 2 Magic

Size of APK Signature Block

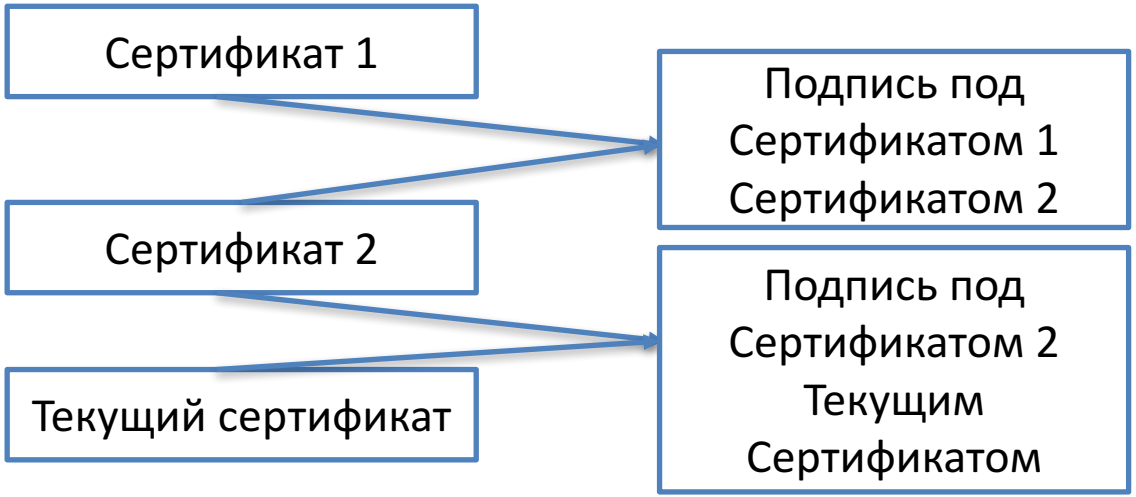
Signature Block Data (ID-Value pairs)

APK Signature v1 + v2

- V1 – для совместимости со старыми устройствами (minSdk < 24)
- V2 – ускорение старта приложения
- V2 – более надежный способ контроля содержимого

APK Signature v3

Цепочка доверия сертификатов



APKSigner в действии

$ apksigner rotate --out.lineage --old-signer --ks 1.keystore --new-signer --ks 2.keystore

$ apksigner sign --ks 1.keystore --next-signer -ks 2.keystore --lineage out.lineage app.apk

Android API

Получение сертификатов

```
Signature[] sigs = context.getPackageM...ger().
      getPackageInfo(context.getPackage...ame(),
PackageManager.GET_SIGNATU...S).sign...ures;
```

Работа с сертификатами

- java.s...ty.*
- java.security.cert.*

Android: He protec, but he also attac

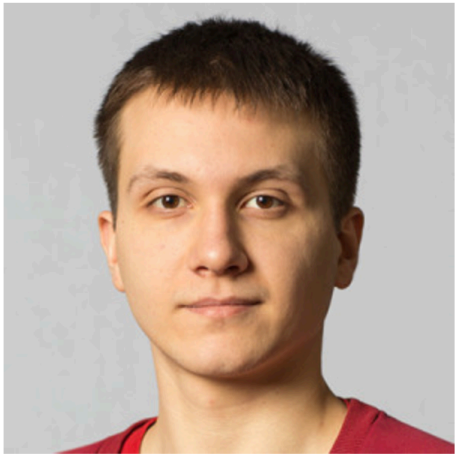
День 2 / 12:00 / Зал 2 / RU /

9 декабря 12:00 Зал 2

> Комментарий Программного комитета:
>
> *Доклад спускается до уровня ассемблера, раскапывая глубокие детали механизма работы Android-приложений и операционной системы. То, что надо для Mobius!*

Последнее время всё больше компаний заботятся о безопасности, но все знают способы защиты не дальше, чем «не палить логи в проде», и уж точно единицы знают, как их могут взломать. Александр расскажет про базовые способы защиты, покажет способ взлома через method hooking, объяснит, что это такое, и расскажет, как от него защититься.

Все доклады



JACKS0N23

Александр Гузенко

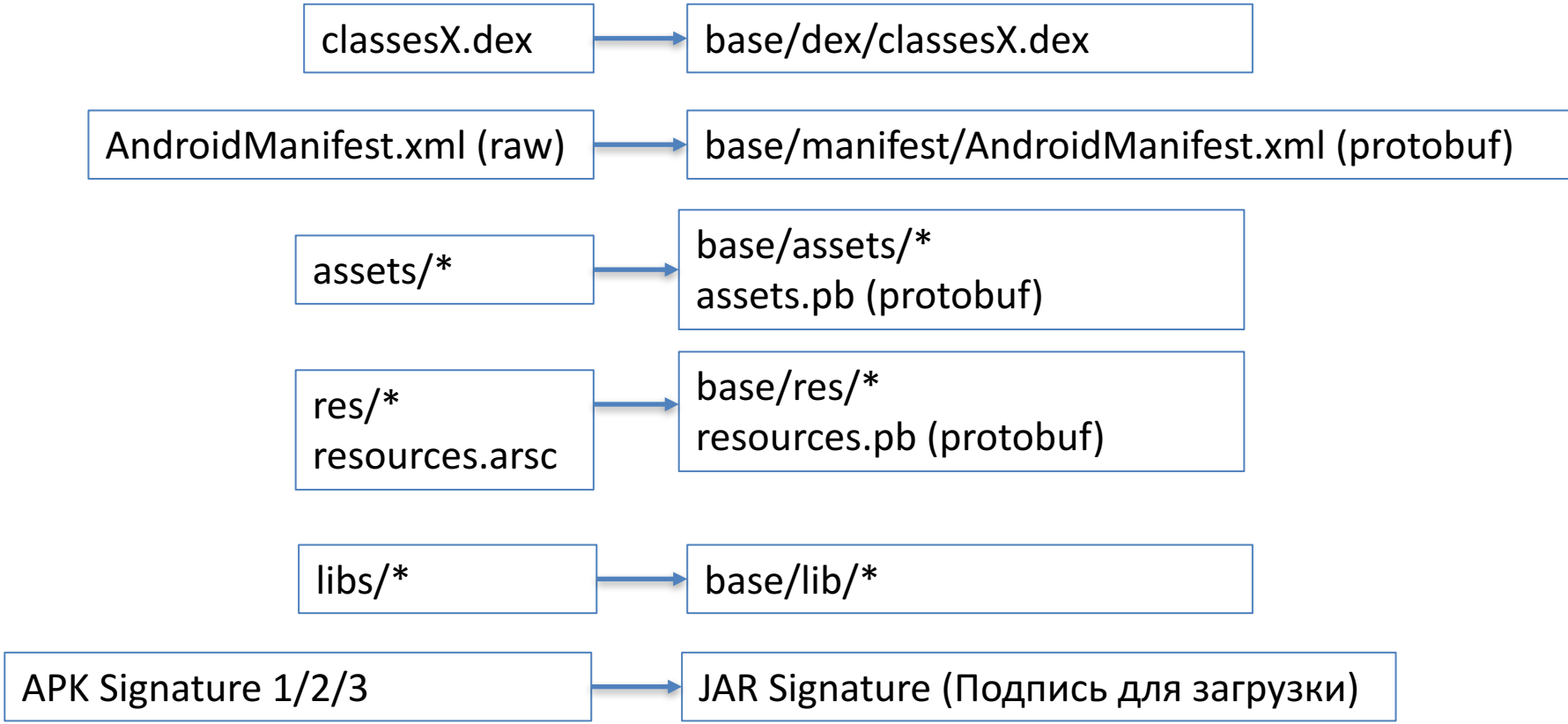
Tinkoff.ru

С детства был увлечён компьютерами, буквально рос вместе с этой индустрией, попал в самый её рассвет. С 2015 года пишет приложения под Android. Работал в QIWI, писал главное приложение кошелька, рассказывал людям о финтехе. Сейчас работает в Tinkoff.ru, пишет приложение «Клиенты». Александр всегда интересовался безопасностью, в том числе мобильных приложений, поэтому ему есть что вам рассказать в этой области.

AABs


Thank You!
@ceruleanotter
Get started
g.co/androidappbundle
#BuildBetterApps

APK vs AAB

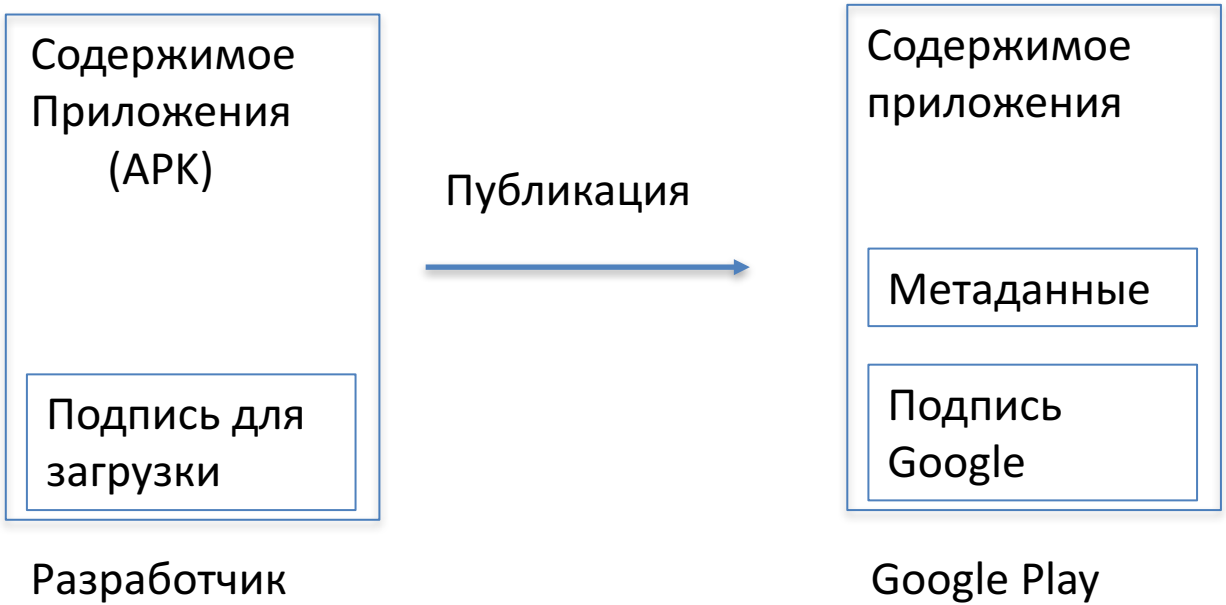

classesX.dex
base/dex/classesX.dex
AndroidManifest.xml (raw)
base/manifest/AndroidManifest.xml (protobuf)
assets/*
base/assets/*
assets.pb (protobuf)
res/*
resources.arsc
base/res/*
resources.pb (protobuf)
libs/*
base/lib/*
APK Signature 1/2/3
JAR Signature (Подпись для загрузки)

JAR Signature (Подпись для загрузки)

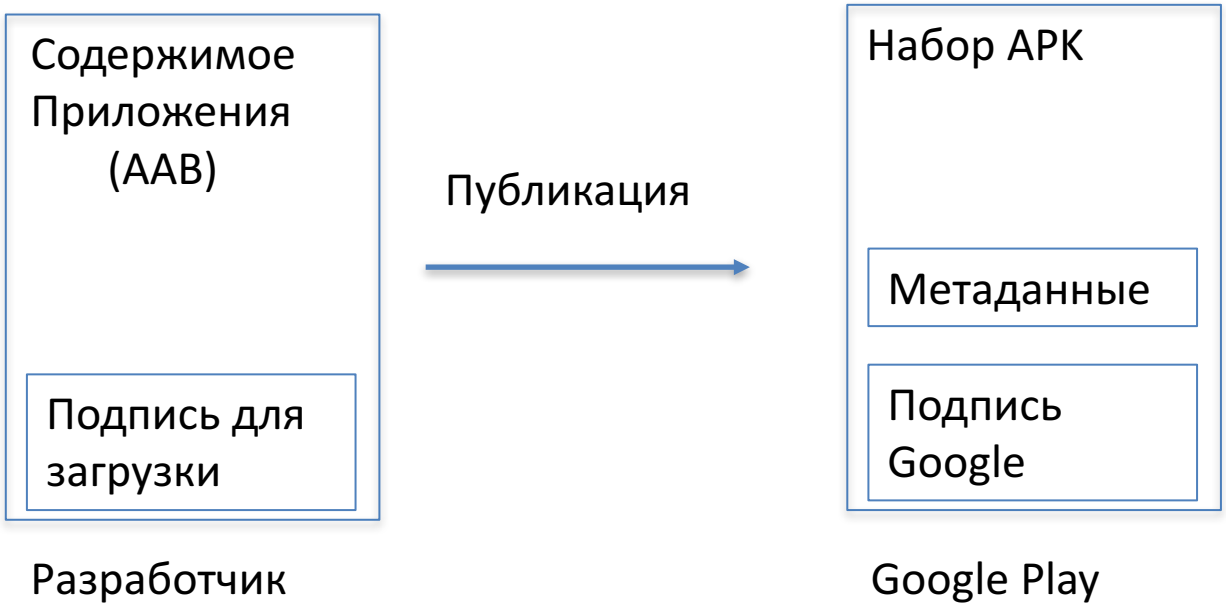
```
$ jarsigner -verify app-google.aab
jar verified.

$ apksigner verify app-google.aab
Exception in thread "main" com.android.apksig.apk.ApkFormatException: Missing
AndroidManifest.xml
```

Google Play Signing APK



Google Play Signing AAB



Текущая ситуация

1. Загружаем AAB в Google Play
2. Загружаем APK из Google Play
3. Проверяем подпись

????

DOES NOT VERIFY
ERROR: APK Signature Scheme v2 signer #1: Malformed additional attribute #1

Выводы

- Включите APK Signature 2
- Контролируйте содержимое приложения и подпись самостоятельно + на серверной части
- Задумайтесь об использовании SafetyNet Attestation API
- Берегите ваши ключи
  - Серверная подпись на Jenkins
  - Google Play Signing

Ну пока! Пишите письма!..

Email: kinash@licelus.com
Twitter: @ivan_kinash

Email: dudarev@licelus.com
Twitter: @MikhailDudarev

Licel Corporation
Web: https://licelus.com