ЗАЩИТА ANDROID-ПРИЛОЖЕНИЙ

Александр Княжев

«СофтИнвент», Пенза

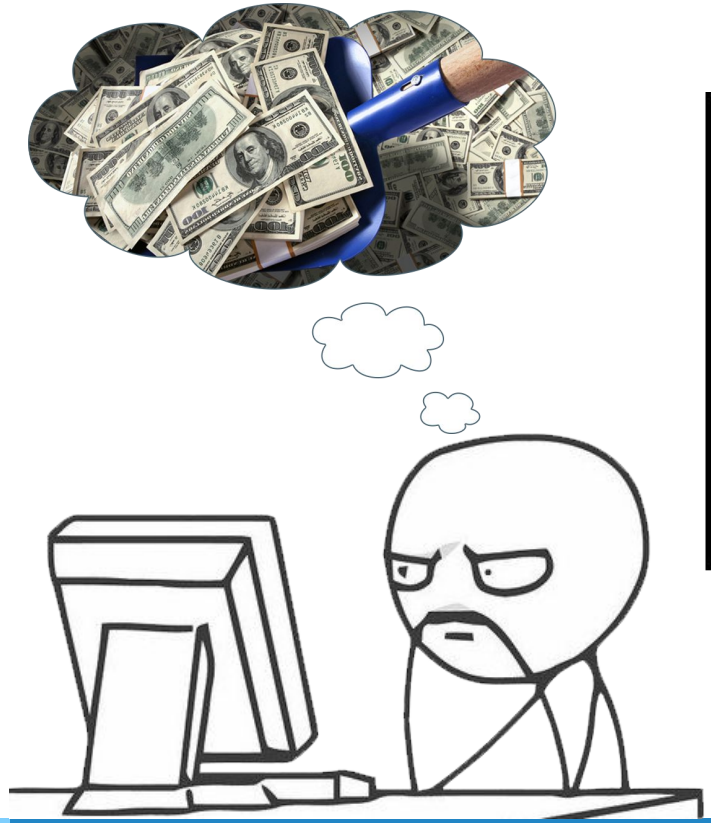
#SECONRU

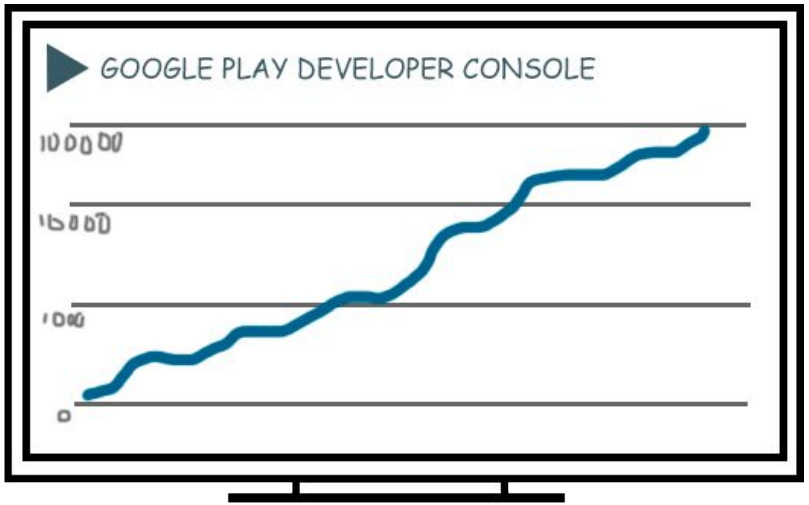
1.

С ЧЕГО ВСЁ НАЧИНАЕТСЯ

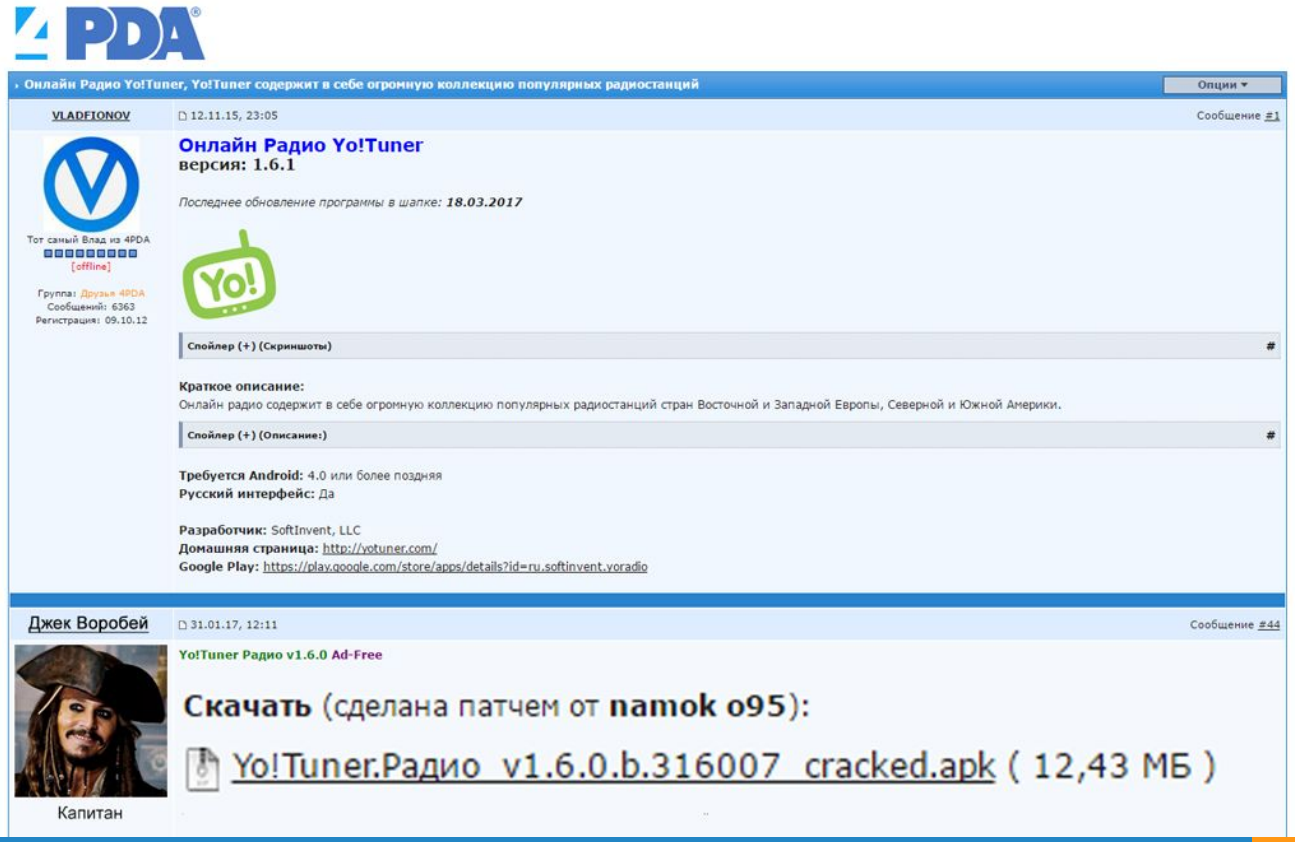
Основано на реальных событиях

Опубликовали приложение...

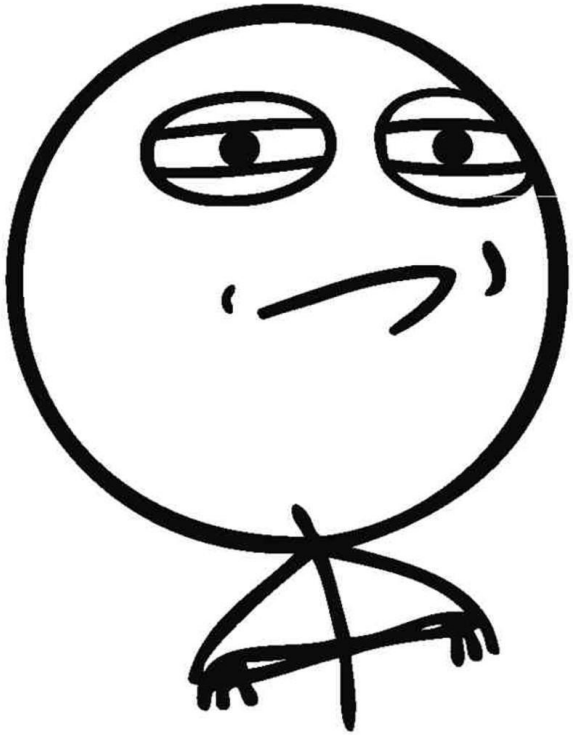




Внезапно


4PDA
Онлайн Радио Yo!Tuner, Yo!Tuner содержит в себе огромную коллекцию популярных радиостанций
Опции
VLADFIONOV
12.11.15, 23:05
Сообщение #1
Онлайн Радио Yo!Tuner
версия: 1.6.1
Последнее обновление программы в шапке: 18.03.2017
Yo!
Тот самый Влад из 4PDA
[offline]
Группа: Друзья 4PDA
Сообщений: 6363
Регистрация: 09.10.12
Спойлер (+) (Скриншоты)
Краткое описание:
Онлайн радио содержит в себе огромную коллекцию популярных радиостанций стран Восточной и Западной Европы, Северной и Южной Америки.
Спойлер (+) (Описание:)
Требуется Android: 4.0 или более поздняя
Русский интерфейс: Да
Разработчик: SoftInvent, LLC
Домашняя страница: http://yotuner.com/
Google Play: https://play.google.com/store/apps/details?id=ru.softinvent.yoradio
Джек Воробей
31.01.17, 12:11
Сообщение #44
Yo!Tuner Радио v1.6.0 Ad-Free
Скачать (сделана патчем от namok o95):
Yo!Tuner.Радио_v1.6.0.b.316007_cracked.apk (12,43 МБ)
Капитан

Вызов принят

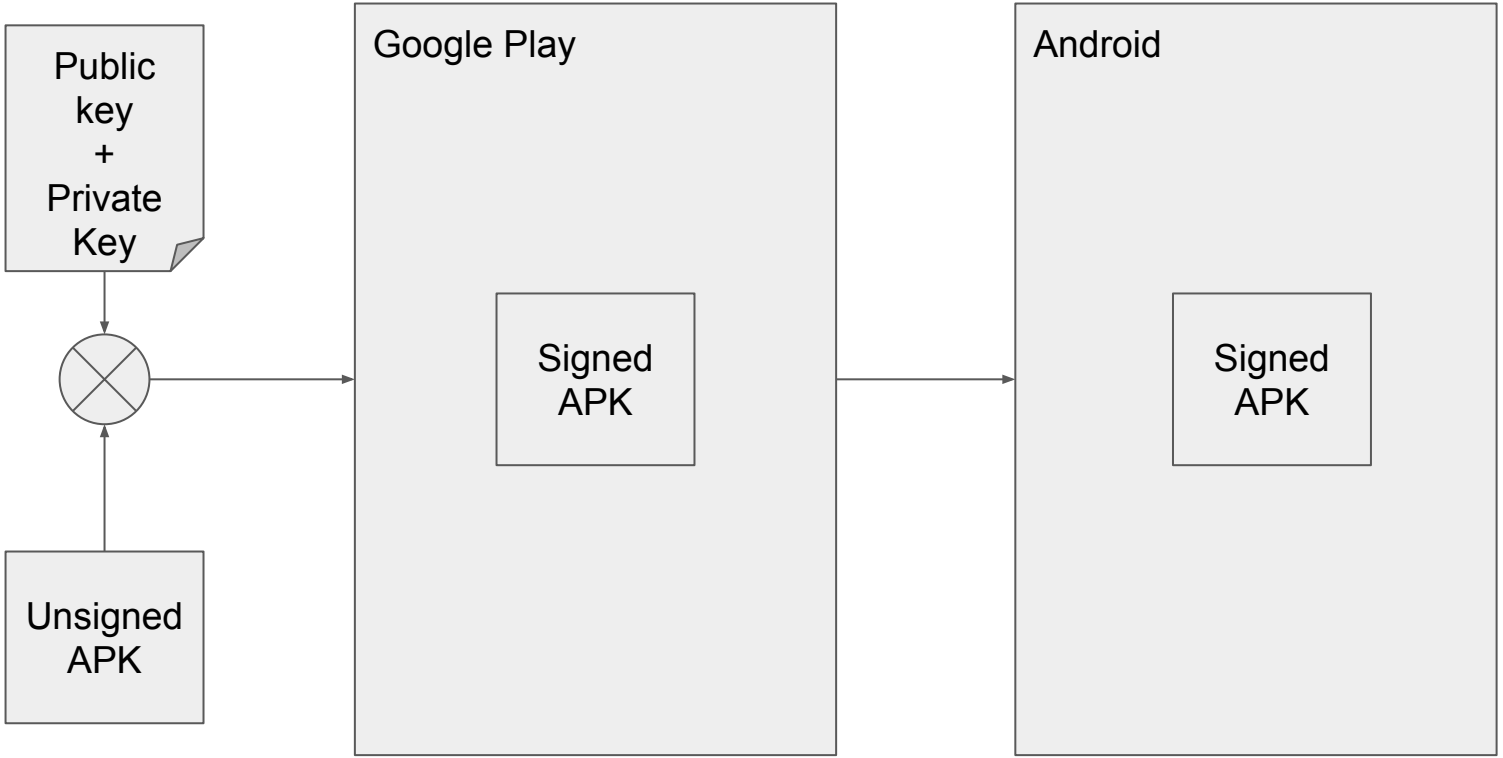


2.

НЕМНОГО ТЕОРИИ

Про подпись приложений в Android

Как всё устроено



Внутри APK

- META-INF/
  - CERT.RSA
  - CERT.SF
  - MANIFEST.MF

Это подпись приложения

3.

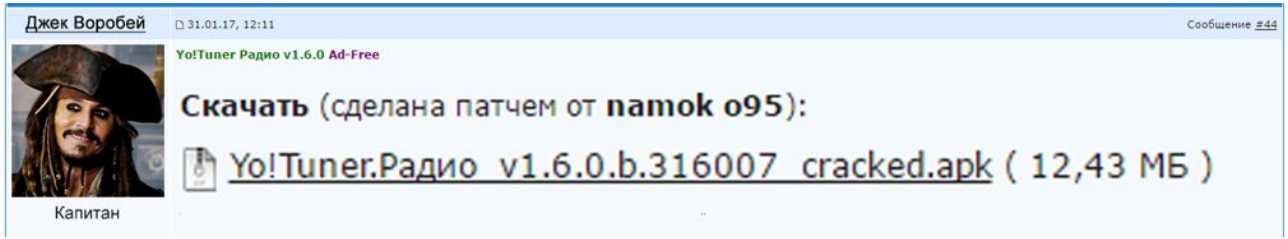
ПРИНИМАЕМСЯ ЗА ДЕЛО

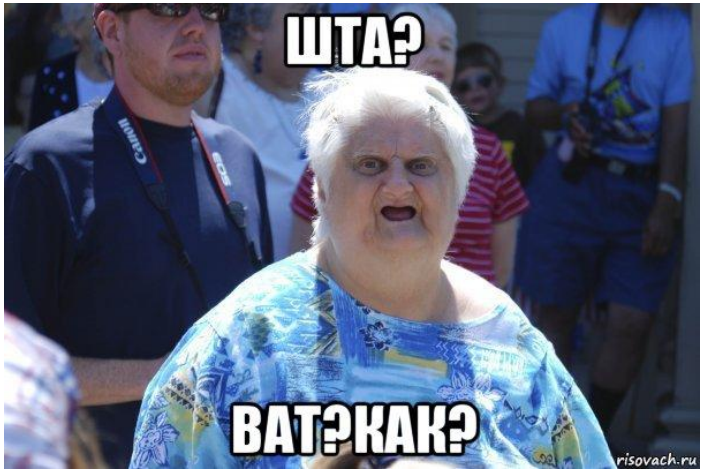
Первая реализация

Проверка подписи

```
PackageInfo info = ctx.getPackageManager().getPackageInfo(
                        ctx.getPackageName(),
                        PackageManager.GET_SIGNATURES);
String[] fingerprints = new String[info.signatures.length];
int i = 0;
for (Signature signature : info.signatures) {
    MessageDigest md = MessageDigest.getInstance("SHA");
    md.update(signature.toByteArray());
    fingerprints[i++] = toHex(md.digest());
}
```

Публикуем обновление и…





We need to go deeper

4.

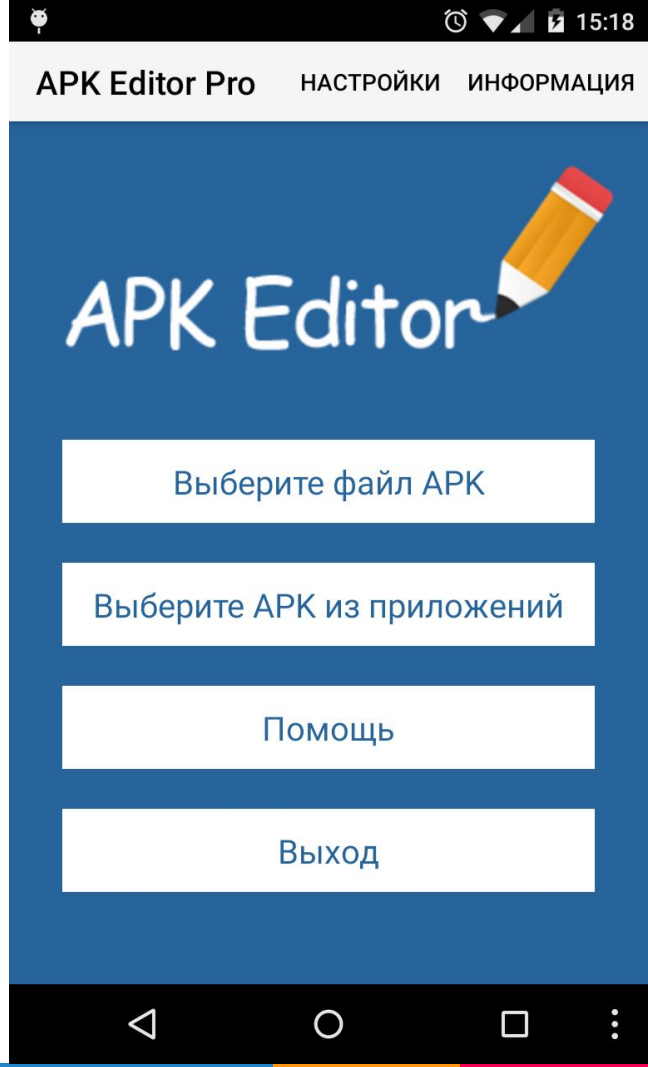
ИДЁМ В СТАН ВРАГА

Как они это делают?!

APK EDITOR PRO и патчи:

- Удаление рекламы
- Удаление\добавление локализаций
- Удаление отладочной информации
- Удаление проверки подписи
- Подмена аккаунта Google
- Подмена серийного номера\IMEI\Android ID
- Для конкретных приложений

Google Play — https://goo.gl/NFROzl



Структура патчей

- [PACKAGE]
- [MATCH_REPLACE]
  - TARGET:
  - MATCH:
  - REGEX:
  - REPLACE:
- [ADD_FILES]
  - SOURCE:
  - TARGET:
- [SIGNATURE_REVISE]
  - TARGET:

Патч удаления рекламы #1

[MATCH_REPLACE]

TARGET:

```
res/layou*/*.xml
```

MATCH:

```
(<\S*[^<]*)(android:id=\"@id/(?:[Aa][Dd][Ss]|[Bb][Aa][Nn][Nn][Ee][Rr]|[Aa][Dd]
[Vv][Ii][Ee][Ww]|[Aa][Dd][Vv][Ii][Ee][Ww]Layout)\")[^<]*(\"\s?/?>)
```

REGEX:

```
true
```

REPLACE:

```
${GROUP1}${GROUP2} android:layout_width="0.0dip"
android:layout_height="0.0dip" android:visibility="gone${GROUP3}
```

[/MATCH_REPLACE]

Патч удаления рекламы #2

[MATCH_REPLACE]

TARGET:

*.smali

MATCH:

\".*doubleclick\.net.*\"|\".*googleadservices\.com.*\"| …|\"https://rri\.appodeal\.com/api/stat.*\"|\"https://settings\.crashlytics\.com/spi/v2/platforms/android/apps/%s/settings.*\"|\"https://startup\.mobile\.yandex\.net.*\"|\"https://target.my\.com.*\"|\"https://www\.googleapis\.com/auth/plus\.me.*\"

REGEX:

true

REPLACE:

"="

[/MATCH_REPLACE]

Патч удаления рекламы #2

```
[MATCH_REPLACE]
TARGET:
*.smali
MATCH:
ca-app-pub
REGEX:
true
REPLACE:
=
[/MATCH_REPLACE]
```

Патч проверки подписи #1

```
.class public Lapkeditor/patch/signature/Fix;
.super Ljava/lang/Object;
.source "Fix.java"

.method public static
getSignatures(Landroid/content/pm/PackageInfo; )[Landroid/content/pm/Signature;
    .registers 15
    .param p0, "pi"    # Landroid/content/pm/PackageInfo;
    .prologue
    const/4 v8, 0x0

    .line 22
    const-string v7, "%PACKAGE_NAME%"

    .line 23
    .local v7, "target":Ljava/lang/String;
    const-string v4, "%RSA_DATA%"
```

…

Патч проверки подписи #2

```
[MATCH_REPLACE]
TARGET:
*.smali
MATCH:
iget-object ([pv]\d+), ([pv]\d+),
Landroid/content/pm/PackageInfo;->signatures:\[Landroid/content/pm/Signature;
REGEX:
true
REPLACE:
invoke-static {${GROUP2}},
Lapkeditor/patch/signature/Fix;->getSignatures(Landroid/content/pm/PackageInfo;)
[Landroid/content/pm/Signature;
move-result-object ${GROUP1}
[/MATCH_REPLACE]
```

Патч проверки подписи #3

…

[ADD_FILES]

SOURCE:

Fix.smali

TARGET:

smali/apkeditor/patch/signature/Fix.smali

[/ADD_FILES]

[SIGNATURE_REVISE]

TARGET:

smali/apkeditor/patch/signature/Fix.smali

[/SIGNATURE_REVISE]

Идея!

Если патчится Java-код, нужно вынести проверку подписи из Java-кода

5.

Решение #1: JNI

Будем проверять подпись из нативного кода

Проверка подписи через JNI

- Android NDK
- CPP:
  - JNIEnv -> GetObjectClass()
  - JNIEnv -> GetMethodId()
  - JNIEnv -> CallObjectMethod()
  - JNIEnv -> GetFieldId()
- Java:
  - System.loadLibrary("mylib")

Проверка через JNI

Плюсы

- Простота
- Не тянет зависимости
- Работает без интернета

Минусы

- Нужно уметь в C++
- Чуть дольше сборка проекта
- SO можно вытащить и дизассемблировать

6.

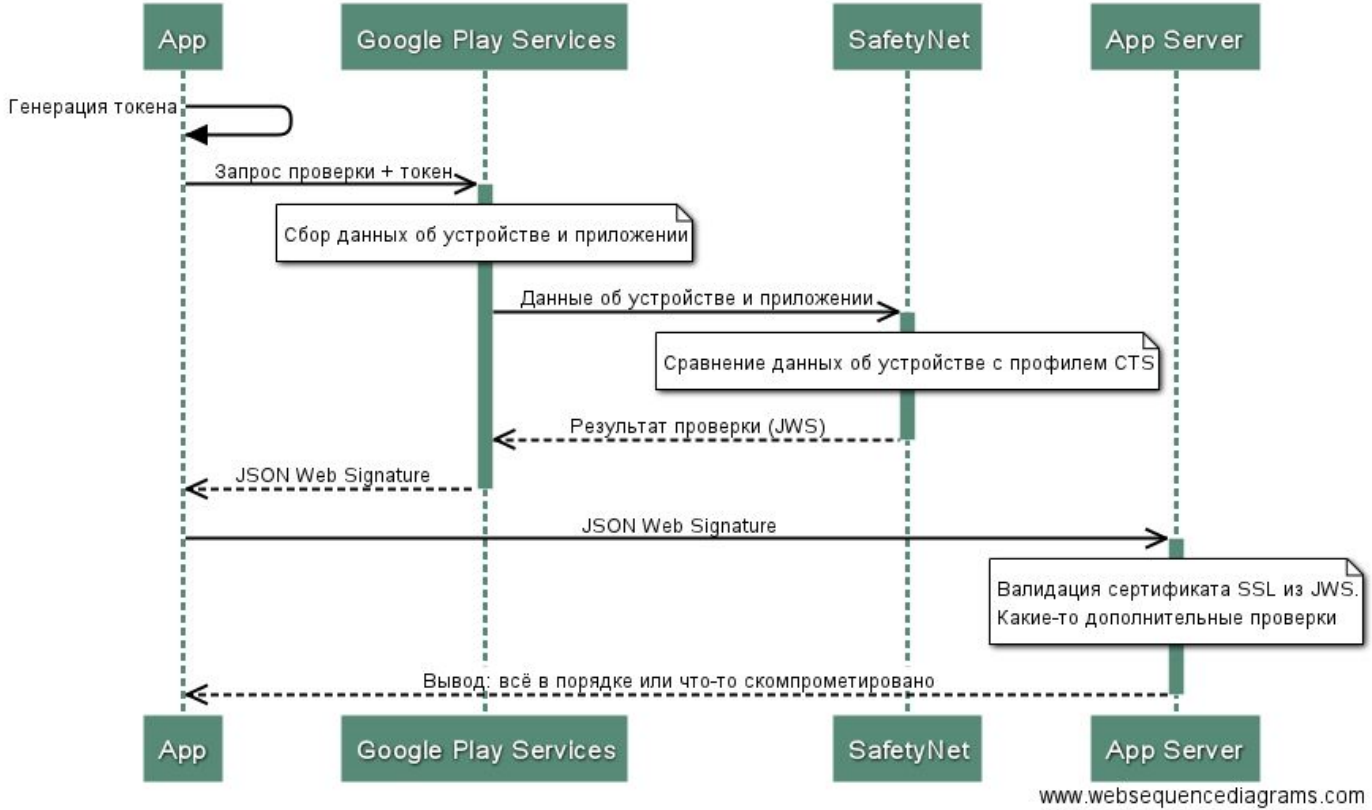
Решение #2: SafetyNet

Пусть проверяет подпись Google

SafetyNet от Google это

- Проверка целостности устройства
- Проверка целостности приложения
- Проверка безопасности URL

Как это работает



SafetyNet — не панацея

Ideally, you should use the SafetyNet Attestation API as an additional in-depth defense signal as part of an anti-abuse system, rather than the sole anti-abuse signal for your app.

Проверка через SafetyNet

Плюсы

- Достаточно высокая степень защиты
- Можно распознать "root"

Минусы

- Зависимость от сервисов Google Play
- Нужен интернет
- Сложнее в реализации

7.

ОБЩИЕ РЕКОМЕНДАЦИИ

Что ещё нужно делать, чтобы вас не ломали

Пара советов от КО

ProGuard

Всегда обфусцируйте релизные сборки - это бесплатно!

SSL

Используйте SSL и делайте это правильно!

Аналитика

Узнайте всё о пользователях взломанной версии

Если есть деньги

Используйте коммерческие обфускаторы: DexGuard, DexProtector, DashO, Shield4J

Спасибо!

Вопросы?

Александр Княжев
руководитель компании «СофтИнвент»

zoidberg@softinvent.ru
fb.com/alexandr.knyazhev.9

Credits

Special thanks to all the people who made and released these awesome resources for free:

- Presentation template by SlidesCarnival
- Photographs by Unsplash