(Не)Безопасность 101

Григорий Джанелидзе

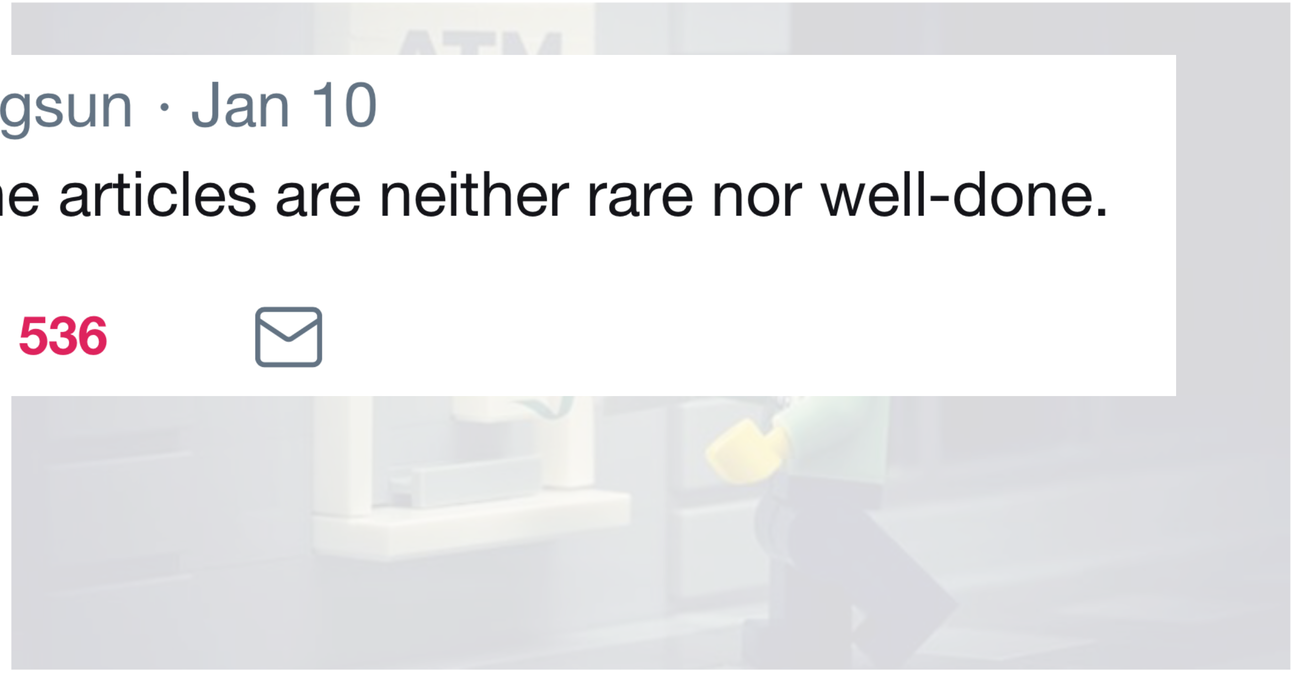
Danil Kravchenko
Dec 6, 2016 · 8 min read

How To Make Your Android Application Secured

li Muzaffar

Yonatan V. Levin
CO-Founder & CTO of KolGene, Founder of Android Academy, Google Developer Expert
Jan 3 · 11 min read

Bang! Bang! You have been hacked.



pretty hate machine @fuckingsun · Jan 10

It's called Medium because the articles are neither rare nor well-done.

2 211 536

Ah the sweet, enticing world of Android. My first true love, always beckoning me, whispering seductively in my ear:

Про что поговорим:

- Как делать точно не надо
- Как делать скорее всего не надо
- Какие инструменты существуют для разных задач
- Как с этим всем жить

101 is a topic for beginners in any area.

It has all the basic principles and concepts that is expected in a particular field.

– Wikipedia

Вся информация представлена исключительно в ознакомительных и образовательных целях.

— Я

Храним ключи

Demo

Храним ключи

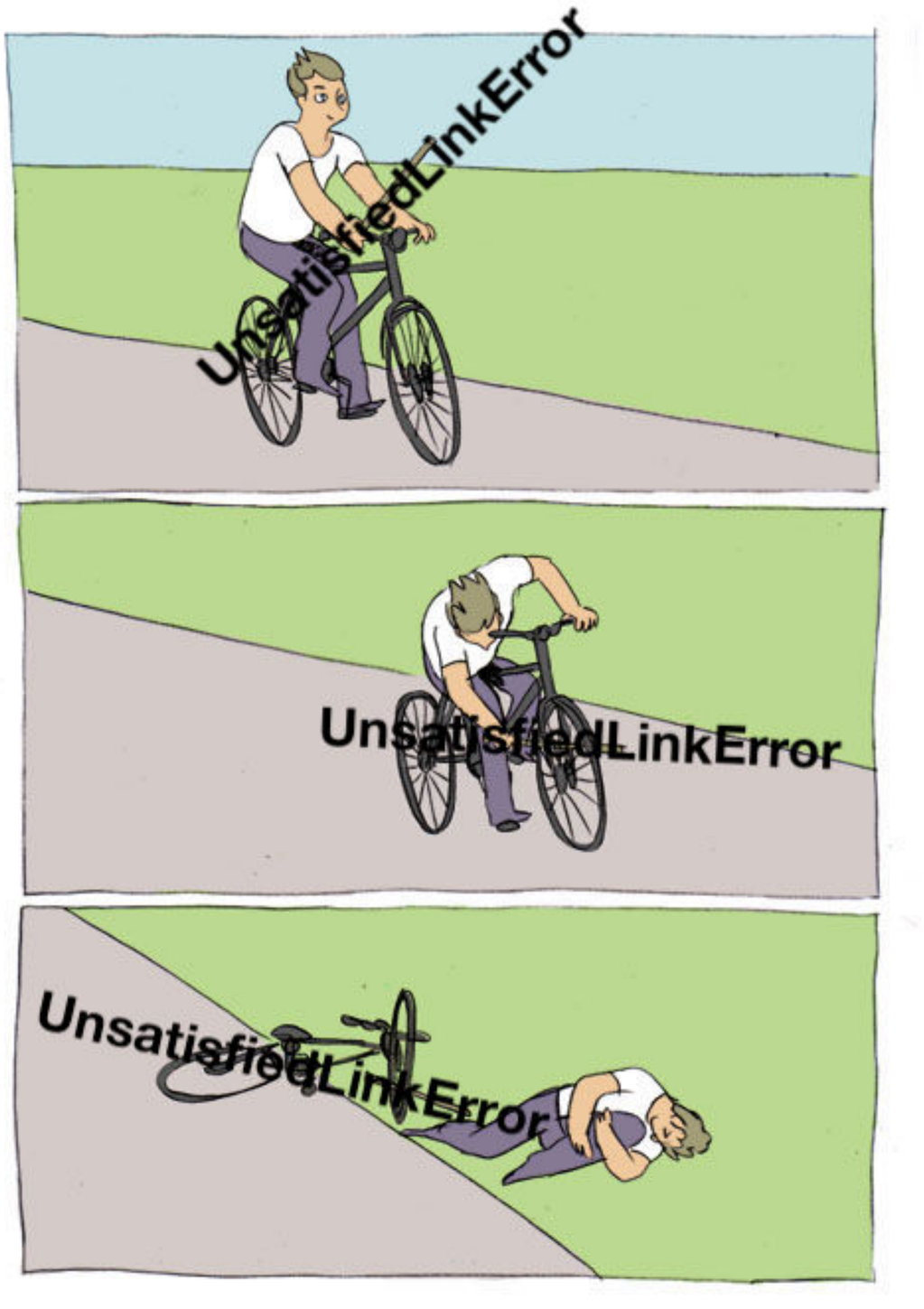
Or you can use Java Native Interface (JNI). It is harder to decompile C/C++ compiled code. Decompilers like JaDx, dex2jar won't help because they are Java-oriented decompilers.

All the methods above can add extra time to the "health" of your app. Use something is better than use nothing.

Храним ключи

Demo

Храним ключи



Храним ключи

https://github.com/KeepSafe/ReLinker

Храним ключи
Итоги

Хранить в коде и шифровать

Хранить в коде

Хранить в манифесте/ресурсах

Хранить в нативной библиотеке и доставать через JNI

Храним ключи
Инструменты

- apktool
- JD-GUI, ByteCode Viewer, …
- IDA Pro, Hopper, …
  - если нужны только строчки: man 1 strings

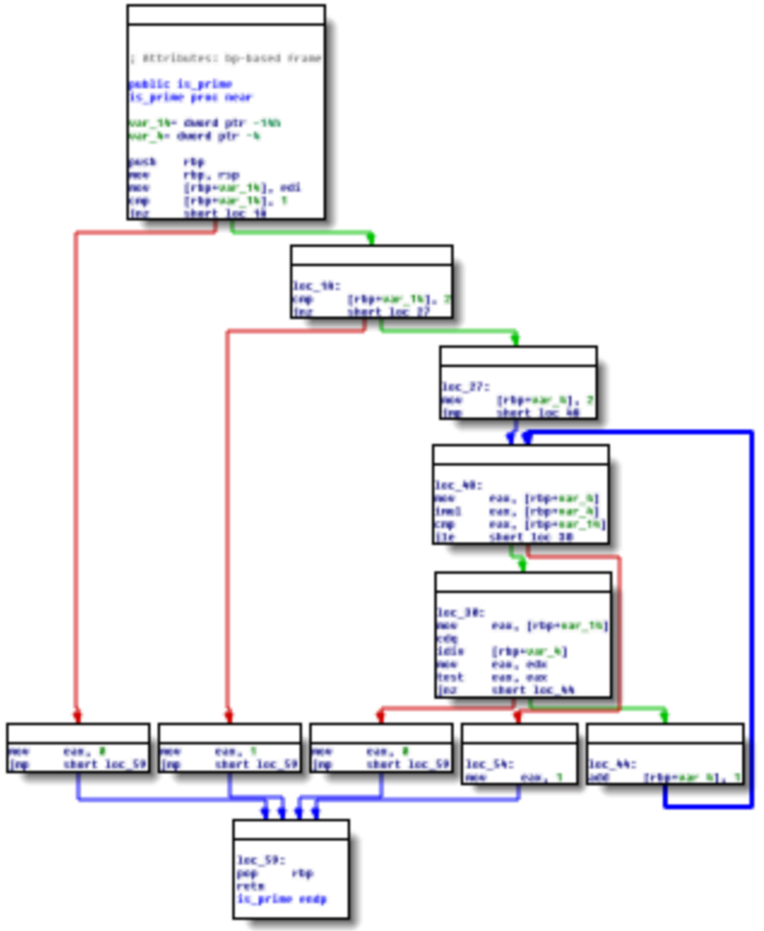
Обфусцируем

Demo

Обфусцируем
Инструменты

- smali / backsmali
- https://github.com/CalebFenton/simplify
- frida, xposed, …
- https://github.com/xoreaxeaxeax/movfuscator

Control flow graphs:

GCC	M/o/Vfuscator
	

Обфусцируем
Итоги

- ProGuard полезный и его в любом случае надо включить
  - Но он не спасет
- Ревью любых изменений в конфиге ProGuard’a ≠ обычное кодревью
  - декомпилируйте и пытайтесь реверсить

Обфусцируем
Итоги

- Я уже говорил, что не надо использовать JNI для «безопасности»?
  - ProGuard не трогает все методы с модификатором native
- Выпиливайте логи, имена переменных, …

Обфусцируем Зло

- Consumer ProGuard Files

Обфусцируем Зло

¯_(ツ)_/¯

(спасибо Google, стало удобнее)

Сопротивляемся

Demo

Сопротивляемся
Итоги

- `Debug.isDebuggerConnected()`
  - не надо
- лайфхаки с ptrace
  - могут быть полезными
- миграция с json’a на protobuf, flatbuf, …
  - поможет, но не сильно

Сопротивляемся
Итоги

- SSL pinning нужен и спасёт
  - …но не от реверсинжиниринга

Сопротивляемся
Инструменты

- man 1 ps
- gdb, lldb, …
- frida, xposed, …

Как быть?

- Пользоваться проприетарными решениями
  - DexGuard, SecNeo, DexProtector, …
- Если есть ресурсы и время, то делать свое

Заключение

- Всегда нуж
- Проверяйте
-

на практике

ить

И если что:

На iOS всё не сильно лучше

(но это тема отдельного выступления)

Спасибо за внимание

t.me/androidguards