



Пользу Android так небезопасен

@SergejKomlach

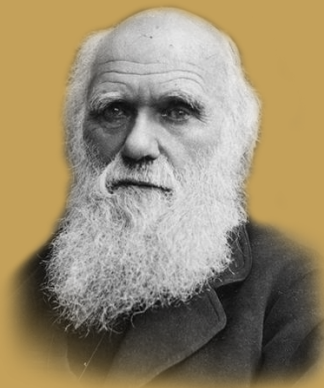


Sticky Password



и поэтому это неправда

(R)Evolution



На дворе был 2008 год....

Ға гворе дыл 2008 зод....

symbian
OS

На дворе был 2008 год....

symbian
OS



На дворе был 2008 год....

symbian
OS



- Wild Wild West, Chaos, Anarchy
- PC- like (way) SW
- C/C++
- No limits (include apps installation)
- Apps on the wild (forums, file sharing)
- ETC.

Newbies...



Android 1.5 Cupcake

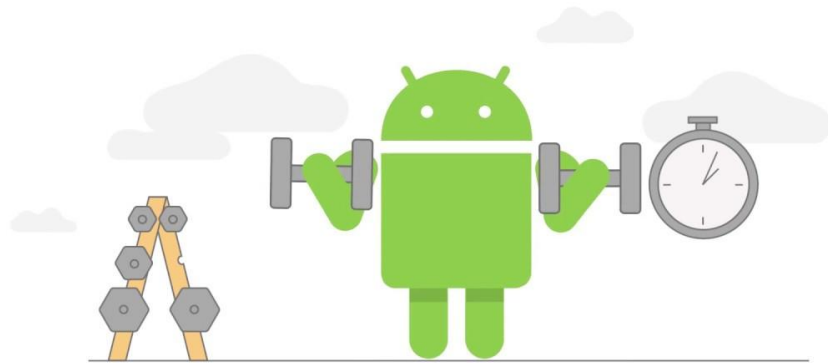


- Apps Store
- Manual app installation
- Apps in Sandbox
- Permissions
- Java
- SELinux
- Non-Rooted Linux
- Protected System dirs



Security





1. Android 1.5 - 3.x - “Детский” период становления
2. Android 4 - 5 - “Набор массы” - количество API растёт, расширяется функционал и возможности для приложений, фрагментация
3. Android 6-Q - работа над оптимизацией (ART, батарея, безопасность)

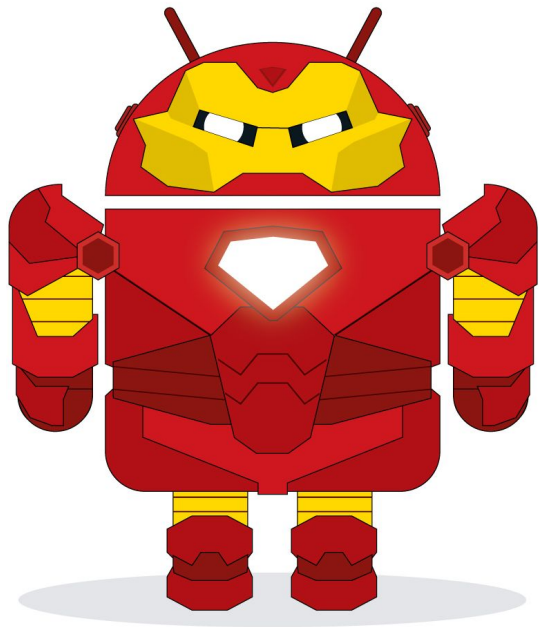


Android 1.5 - 3.x - “Детский”
период становления



Android 4 - 5 - “Набор массы” -
количество API растёт,
расширяется функционал и
возможности для приложений,
фрагментация

В этот период возникли
большинство из проблем с
безопасностью



Android 6-Q - работа над
оптимизацией (ART, батарея,
безопасность)



**- У НАС ДЫРА В
БЕЗОПАСНОСТИ!**

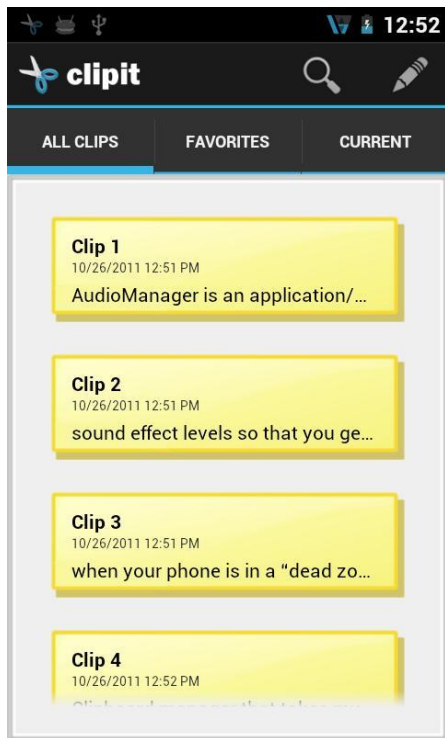
- НУ ХОТЬ ЧТО-ТО У НАС В БЕЗОПАСНОСТИ...

С ростом количества Android устройств и разработчиков, стали очевидны проблемы, оставшиеся с "Детского периода"

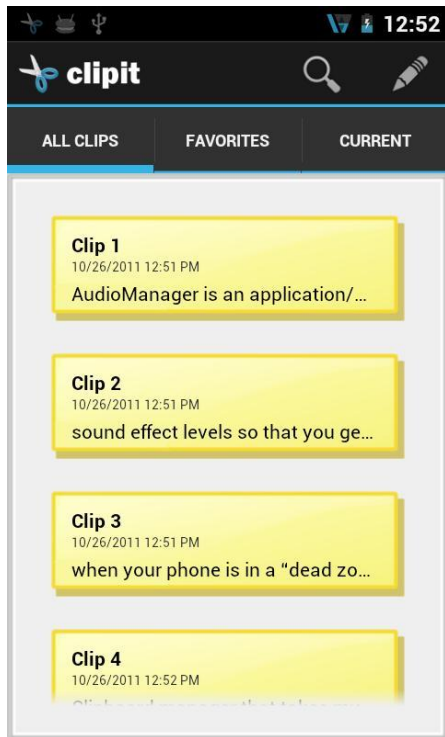
Basic Problems

- PackageID's:
com.facebook.katana VS *com.facebook.myphishingapp.v2*
- Dev.certificates (Keys) -> Google Sign-In (partial fix)

ClipboardManager



ClipboardManager



Android Q

<https://developer.android.com/preview/privacy/data-identifiers#clipboard-data>

“Access to clipboard data

Unless your app is the default [input method editor \(IME\)](#) or is the app that currently has focus, your app cannot access clipboard data.”

Toast/Window Manager

✕ This is an error toast.

✓ Success!

i Here is some info for you.

! Beware of the dog.



Normal toast w/o icon

paw Normal toast w/ icon

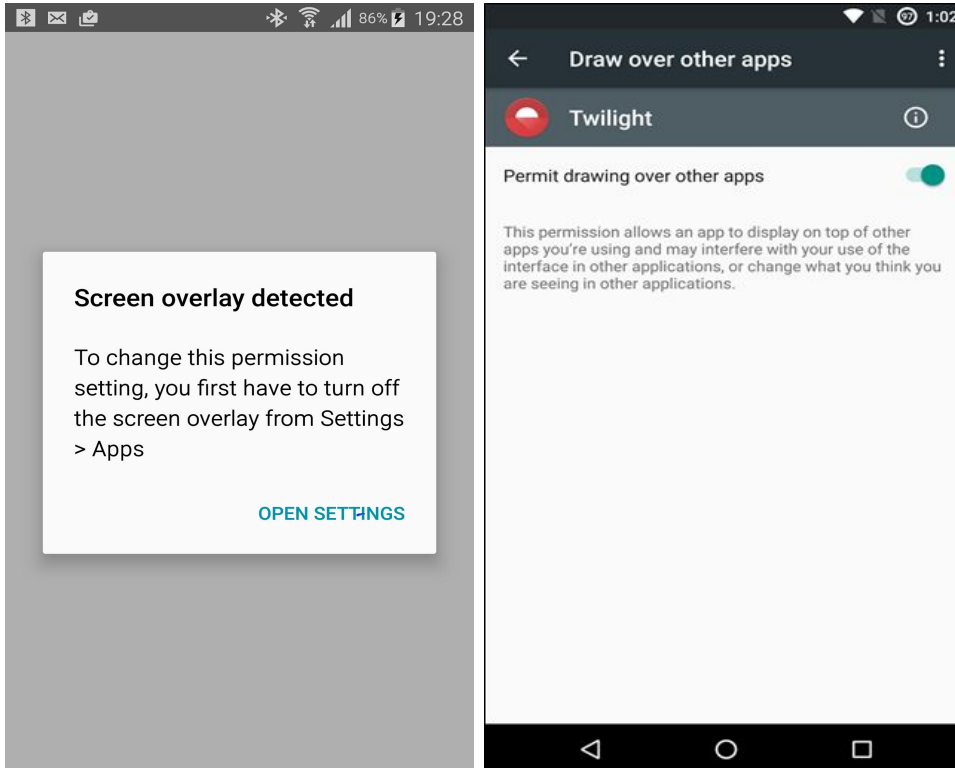
i Formatted ***bold italic*** text

💻 `sudo kill -s everyone`



Toast/WindowManager

Android 6 (Marshmallow)



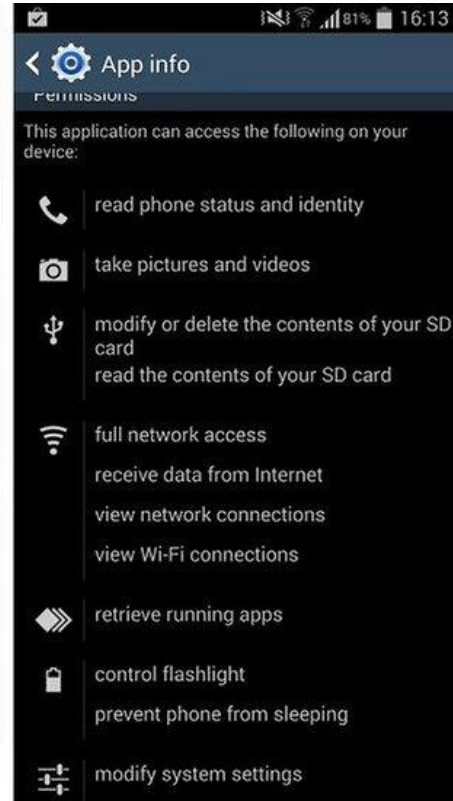
Android 8 (Oreo)

- 1) Toast from BG now crashed, yep :)
- 2) `TYPE_APPLICATION_OVERLAY`

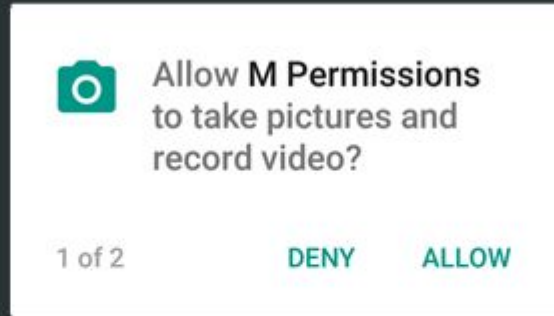
```
public static final int WINDOW_TYPE =  
(Build.VERSION.SDK_INT < 26 ?  
WindowManager.LayoutParams.TYPE_SYSTEM_ALERT :  
WindowManager.LayoutParams.TYPE_APPLICATION_OVER  
LAY);
```

```
public static final int TOAST_TYPE =  
(Build.VERSION.SDK_INT < 26 ?  
WindowManager.LayoutParams.TYPE_TOAST :  
WindowManager.LayoutParams.TYPE_APPLICATION_OVER  
LAY);
```

Permissions (Android 1.5-5.1)



Permissions (Android 6-9)



A N D R O I D

Marshmallow Permissions

Permissions (Android Q)



**Allow App 1 to access this
device's location?**

Allow all the time

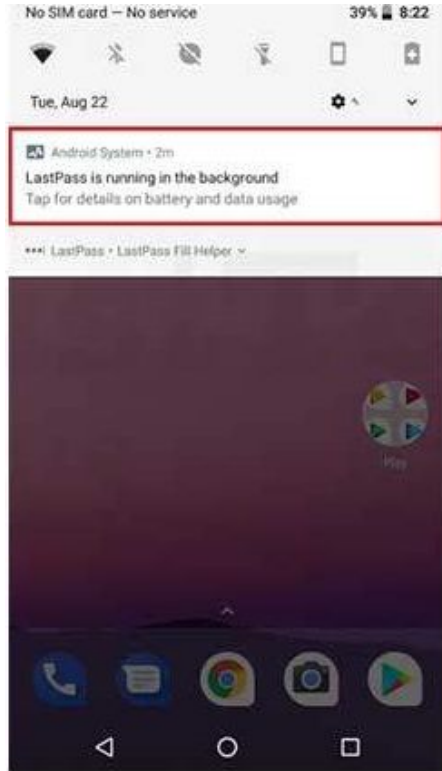
Allow only while the app is in use

Deny

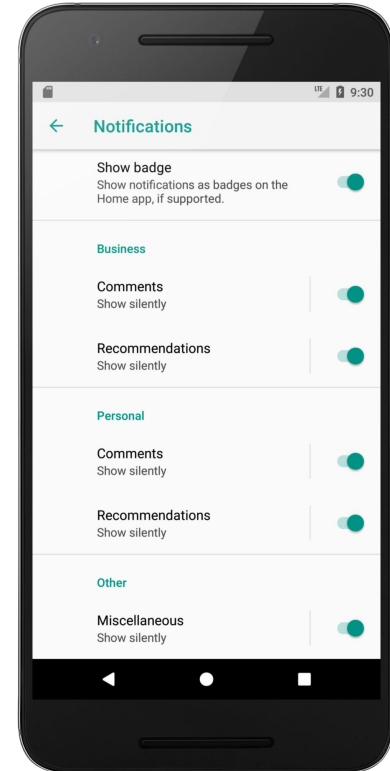
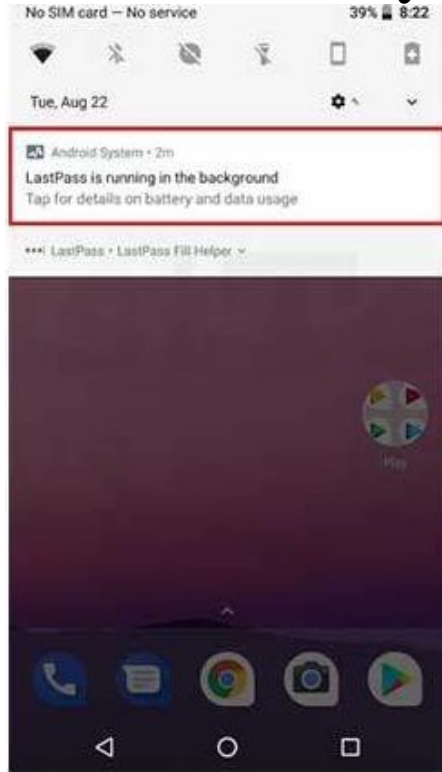
Accessibility



Background Services



Background Services VS Notifications



Instant Apps



INSTANT APPS

Private API usage

- Reflection API
- ClassLoader
- ByteBuddy
- ***.SO - *dlopen()***

1. white, black and grey list (Android 8+)
2. Limitation in GooglePlay

Issues with Crypto

Issue:

Obsolete Crypto (BoringSSL, TLSv1/SSLv3)

Fixes:

1. OpenSSL, Conscrypt (Android 6)
2. Moving away from BouncyCastle (Android 9)
3. Use updates from GooglePlay:
`com.google.android.gms.security.ProviderInstaller.installIfNeeded()`



Updates

Updates VS Fragmentation

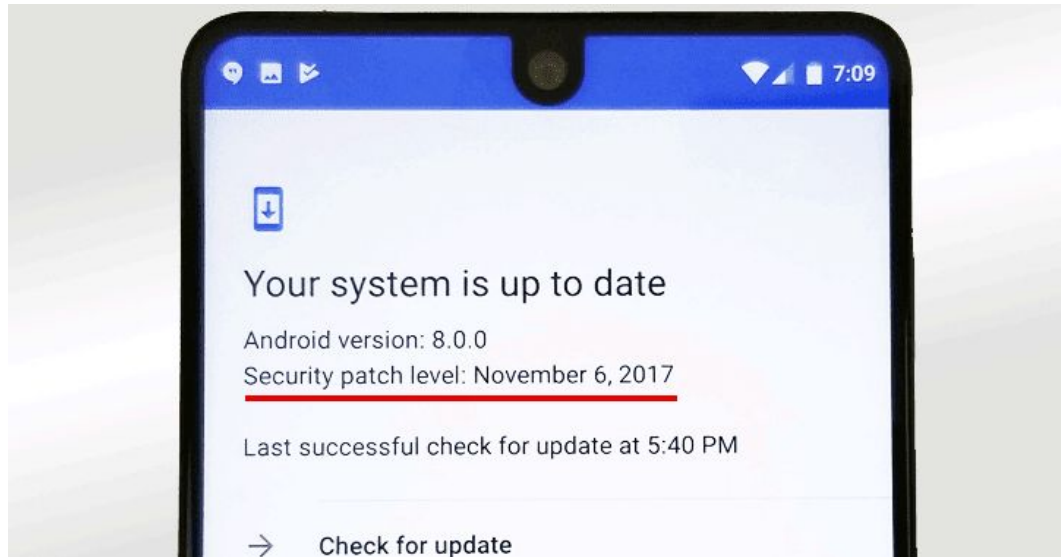
Google Play:

- WebView (Android 5+)
- System Apps (Calendar, Clock, Browser etc)
- Apps updates (!!!!!!!!!!!)



Updates VS Fragmentation

System - Security Patches



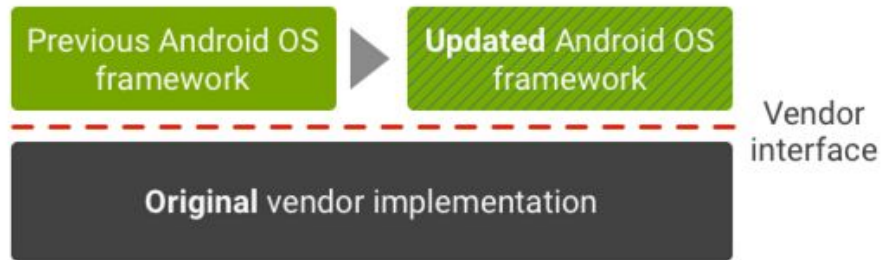
Updates VS Fragmentation

System - Project Treble

ANDROID UPDATES BEFORE TREBLE



ANDROID UPDATES WITH TREBLE





Google Play Market

1. Actual minAPI version
2. Strict verification of apps with Accessibility API
3. Strict verification of apps with **DANGEROUS** permissions (like Calls, SMS etc)
4. Strict rules for apps publishing





Summary

Android OS постоянно меняется и эволюционирует

- **Вначале пути, это была очень безопасной для своего времени OS**
- **Накопив функциональности и популярности - она подверглась проверке на прочность в плане безопасности**
- **Сейчас мы видим этап исправления проблем и улучшений**



[@SergejKomlach](#)
Sticky Password