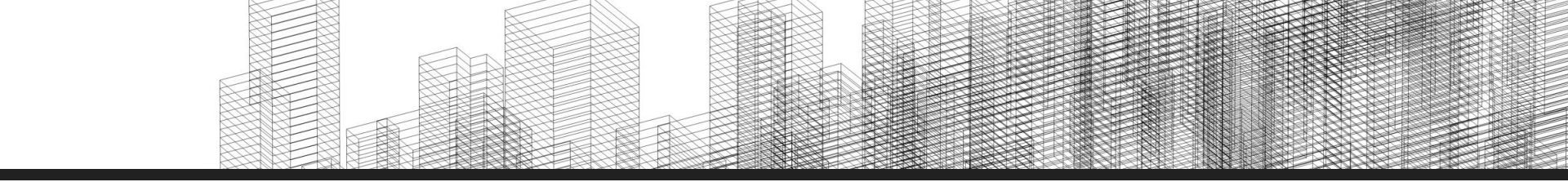
Sécurité Applicative

AppSec Mobile
Ve. 7 Déc. 2018 - PHELIZOT Yvan

Sommaire

- Contexte
- Android
- OWASP Top 10 Mobile
- Mauvaises pratiques de développement

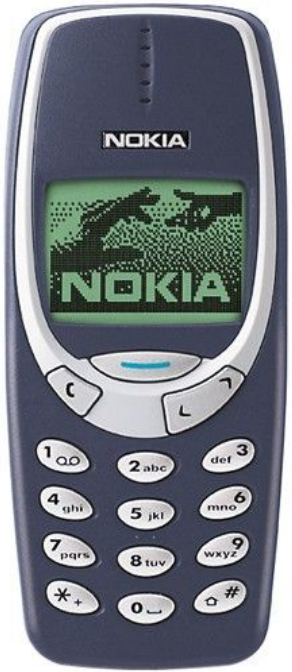


Long story made short...

Is a mobile secured?

Contexte

Evolution des mobiles



Mobile vs. Smartphone

- Comparaison puissance
- Mini PC
- Connecté via 4G, WiFi, Bluetooth, NFC, USB, …
- GPS, Camera, Accéléromètre,
- Lecteur d’empreintes
- Fonctions
  - Terminal de paiement
  - EMails
  - Authentification (SMS, Google Authenticator, …)

LCL, PayPal, BNP… : MysteryBot, le malware Android qui vise les applis bancaires

Julien Lausson - 19 juin 2018 - Tech

Des failles...

Android

Android lockscreen can be bypassed by overloading with massive password

Security bug means Android smartphones running Android Lollipop can be broken into by simply entering a very long password causing the lockscreen to crash

Nouveaux problèmes

FACE ID | By Joseph Cox | Oct 12 2018, 5:05pm

Cops Told 'Don't Look' at New iPhones to Avoid Face ID Lock-Out

**After five failed attempts with th
Apple's Face ID system will fall
a passcode; a tricky situation fo**

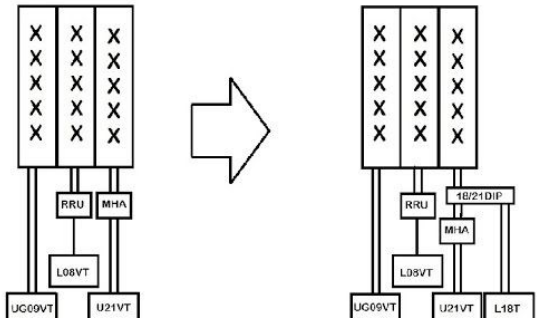
Police use dead man's fingers to try to unlock his iPhone

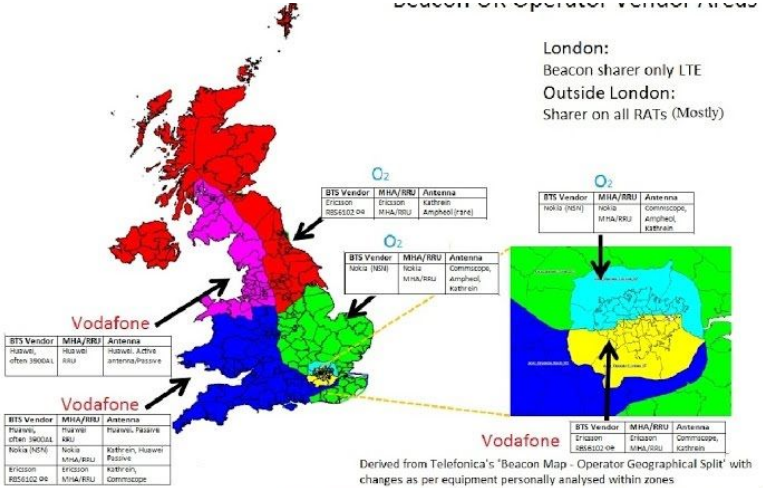
26 MAR 2018 5

Apple, iOS, Law & order, Mobile, Privacy


Rooting &
Jailbreaking

Sécurité des réseaux mobiles

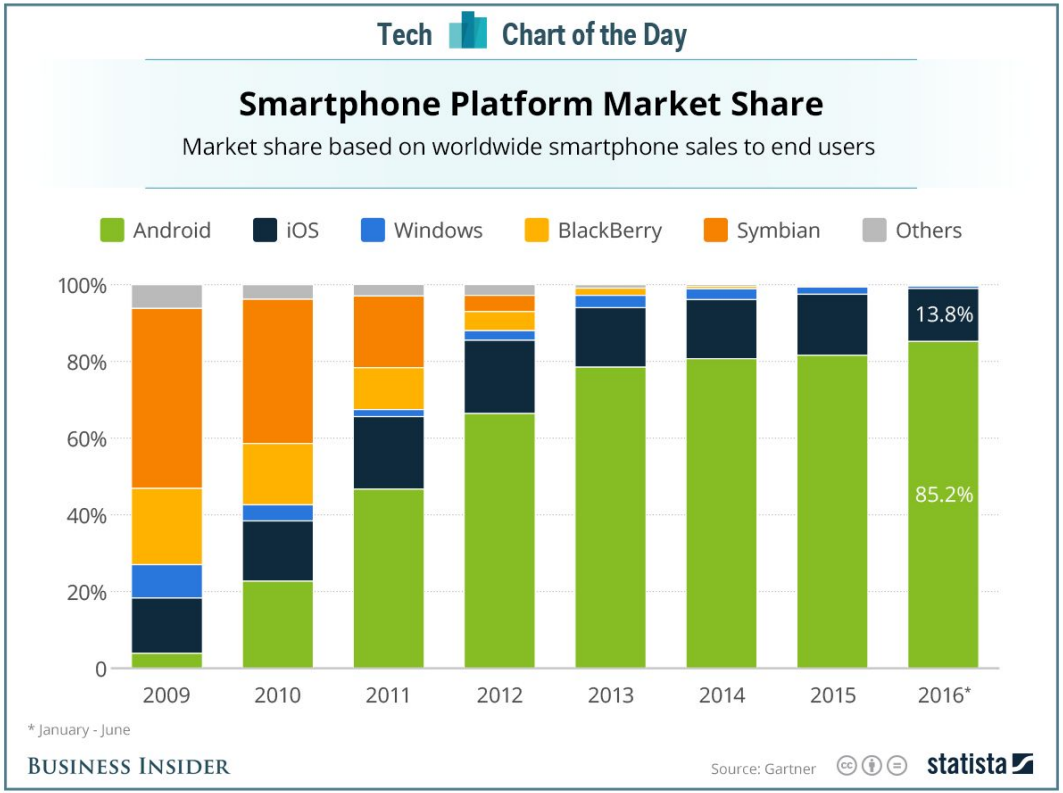




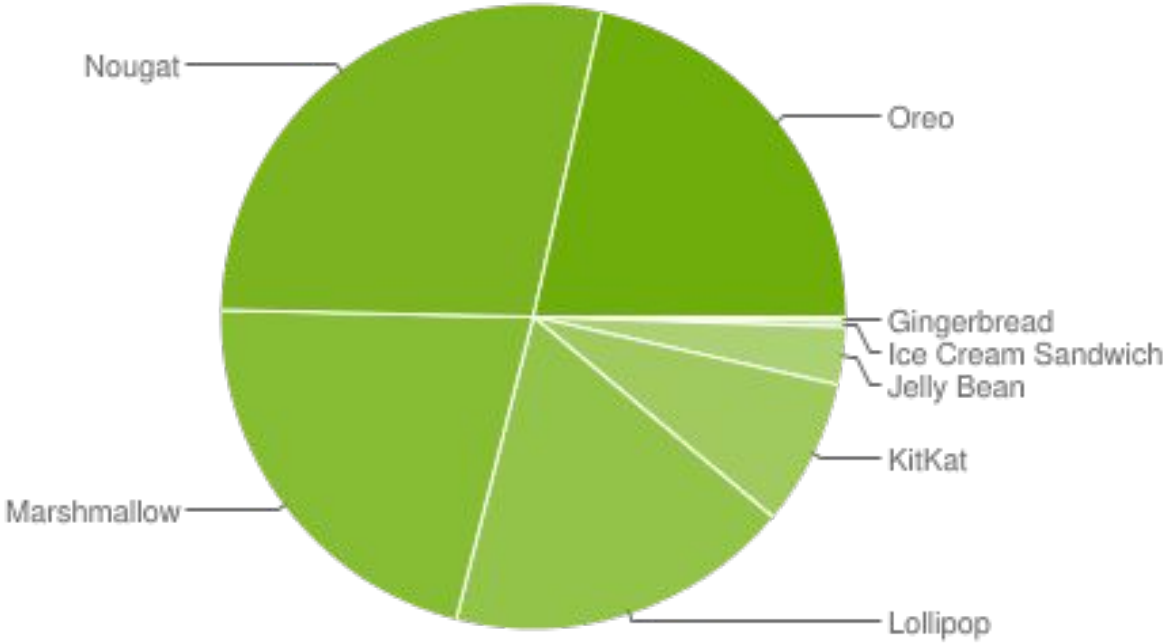
Une cible privilégiée

Backup to the cloud

Fragmentation du marché



Fragmentation



Nouvelles Menaces, Nouveaux Modèles

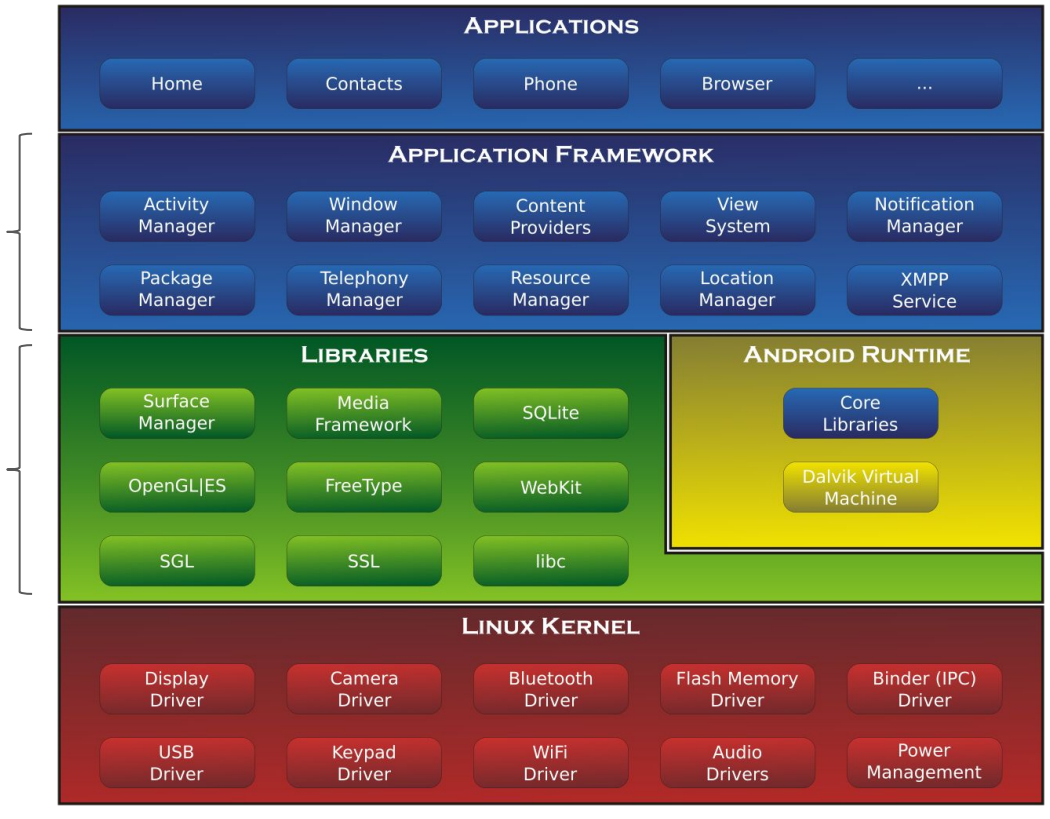
OWASP Top 10 Mobile

Android

Histoire

- 2008: Android 1.0
- 2010: Gingerbread 2.3
- 2011: Ice Cream Sandwich 4.0
- 2012: Jelly Bean 4.1
- 2013: KitKat 4.4
- 2014: LollyPop 5.0
- 2015: Marshmallow 6.0
- 2016: Nougat 7.0
- 2017: Oreo 8.0
- 2018: Pie 9.0

Architecture



API Android

Librairies utilisant le noyau

Application

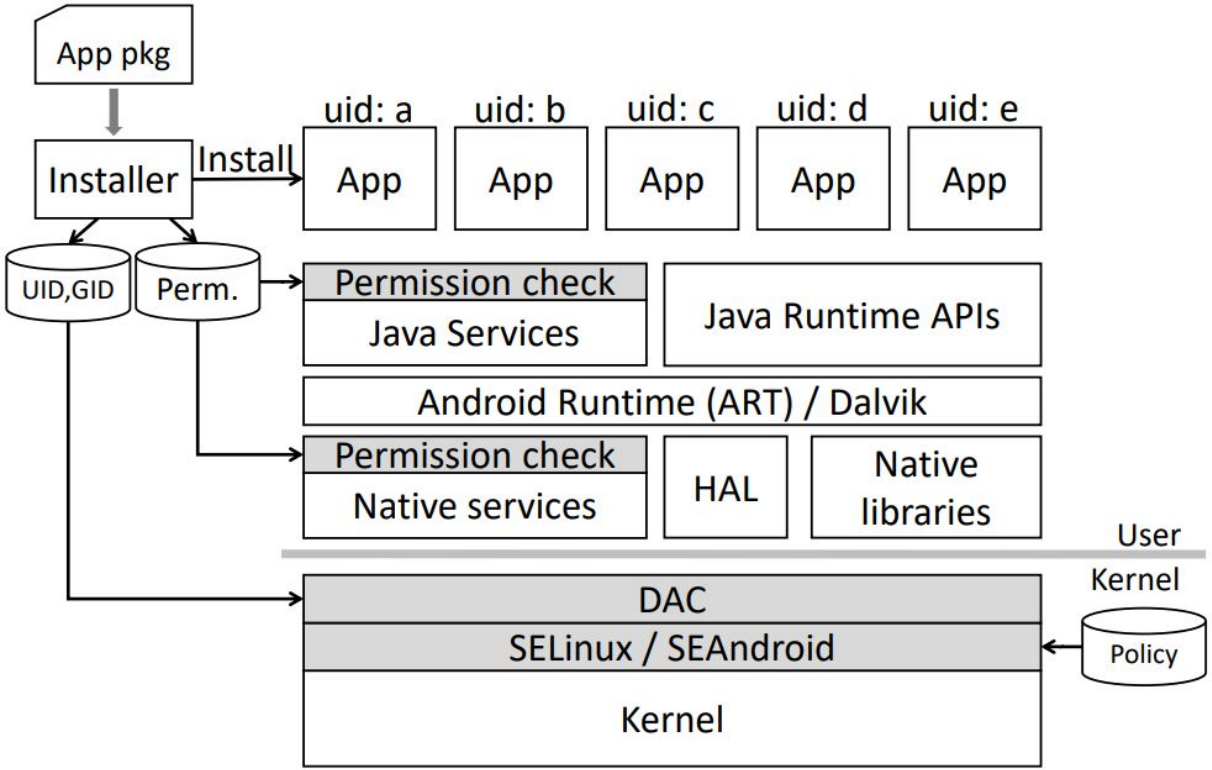
Remplacer par ART

Noyau Linux
Interface avec le matériel

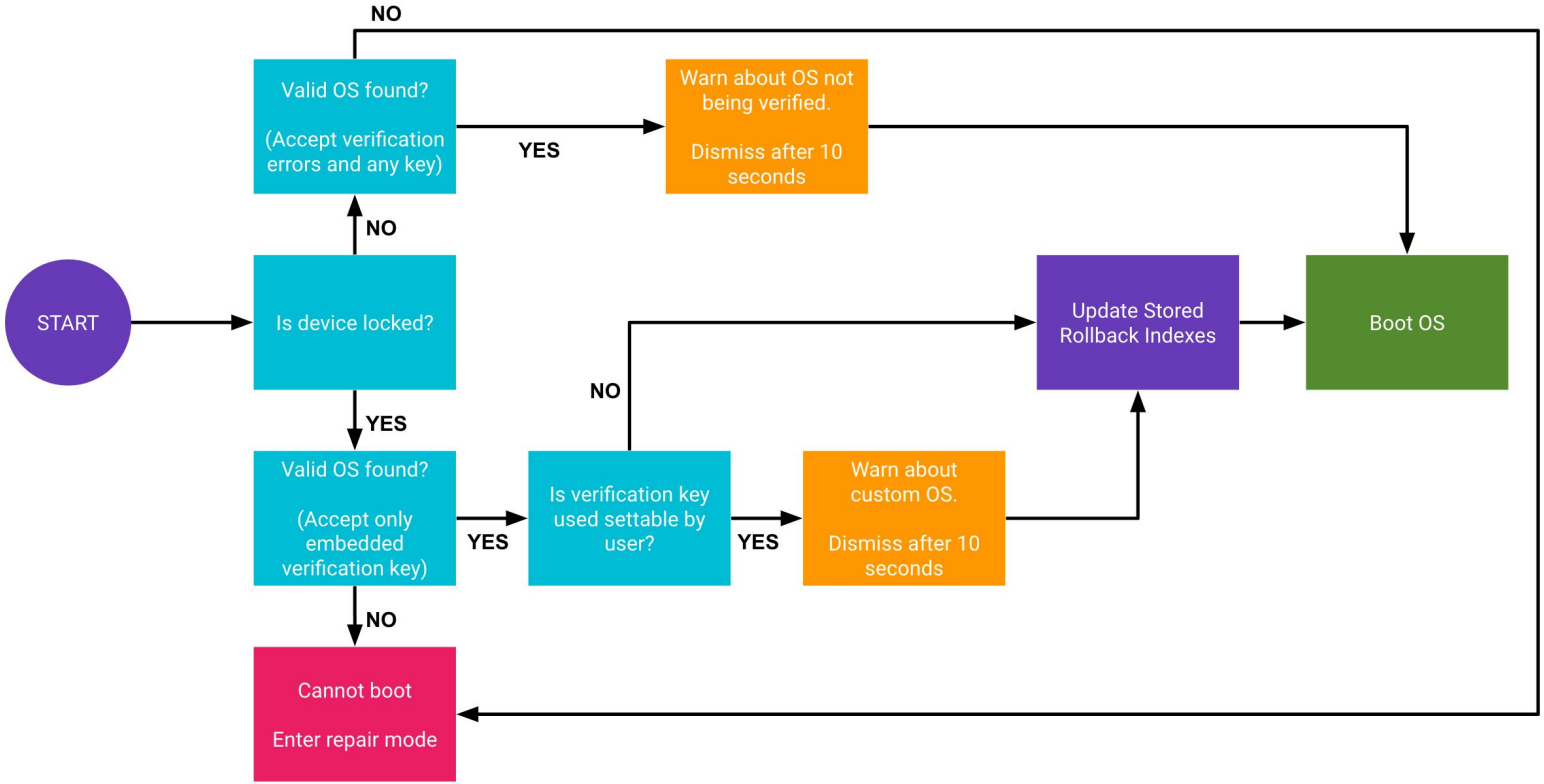
Noyau Linux

- Classic Linux
  - Permission par utilisateur
  - Isolation des processus
  - root
- Hardened Kernel
- Security-Enhanced Linux (SELinux)

Architecture de sécurité Android



Verified Boot



Storage

- Différents types de stockage
  - Internal file storage
  - External file storage
- Full-Disk Encryption
- KeyStore: protected with a password

Storage

- Différents types de stockage
  - Internal file storage
    - App binary: /data/app/[app-name]
    - App data: /data/data/[app-name]
    - System app: /data/system/
  - External file storage
- Full-Disk Encryption
- KeyStore: protected with a password

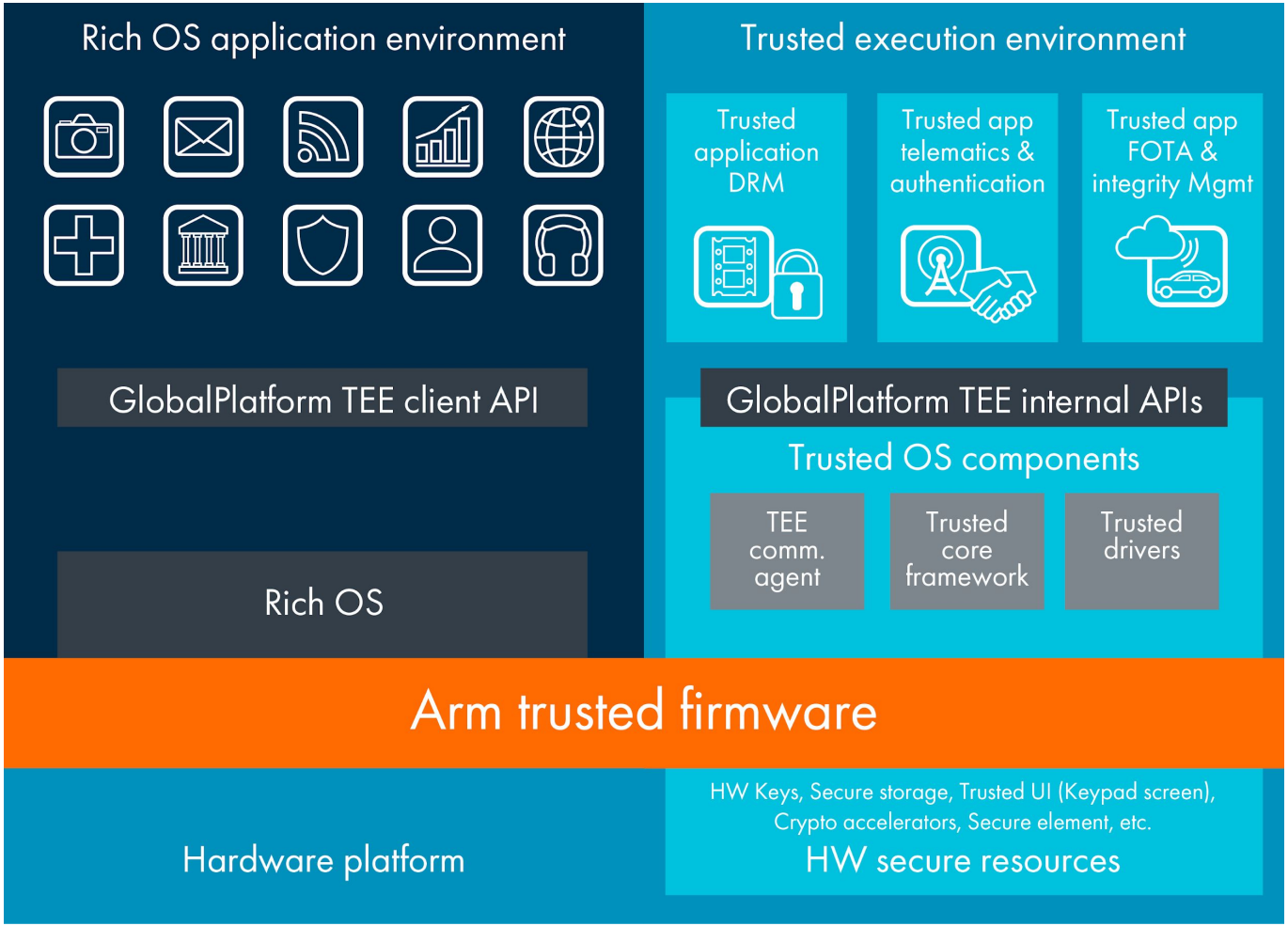
Chiffrement

- Java Cryptography Architecture (JCA)
- Android Key Store
  - Stocke les clé
  - Protège si compromission application
- Certificate Pinning
- TrustManager
- Trusted Execution Environment (TEE)
  - Zone d’exécution privilégiée

Android KeyStore Provider

- Cryptographic operation
- Fed to a system process
  - In case of software compromission ⇒ no compromission of key
- Secure Hardware : TEE/SE

TEE

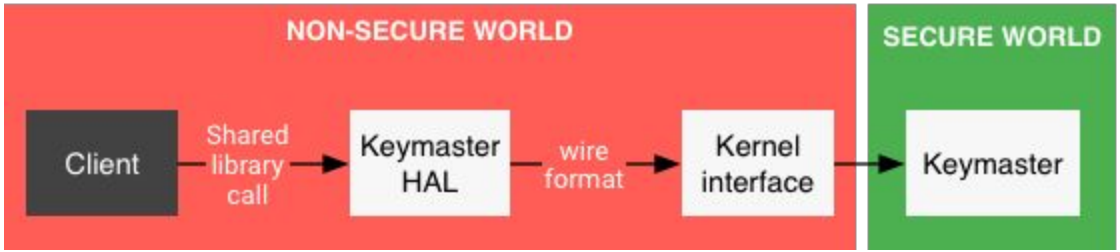

Rich OS application environment
Trusted execution environment
Trusted application DRM
Trusted app telematics & authentication
Trusted app FOTA & integrity Mgmt
GlobalPlatform TEE client API
GlobalPlatform TEE internal APIs
Trusted OS components
TEE comm. agent
Trusted core framework
Trusted drivers
Rich OS
Arm trusted firmware
HW Keys, Secure storage, Trusted UI (Keypad screen), Crypto accelerators, Secure element, etc.
Hardware platform
HW secure resources

Authentication

- Biometrie
- Mot de passe/PIN

Architecture

- Java
  - android.security.keystore



Google

- Google SafetyNet
- Google Play Security
- Google Play/Sources tiers

Android App

Exemple de projet

- AndroidManifest.xml
- Classes.dex : packages/classes
- assets/
- lib/
- res/
- APK: Android Packaging
- Signature : apksigner
- Proguard

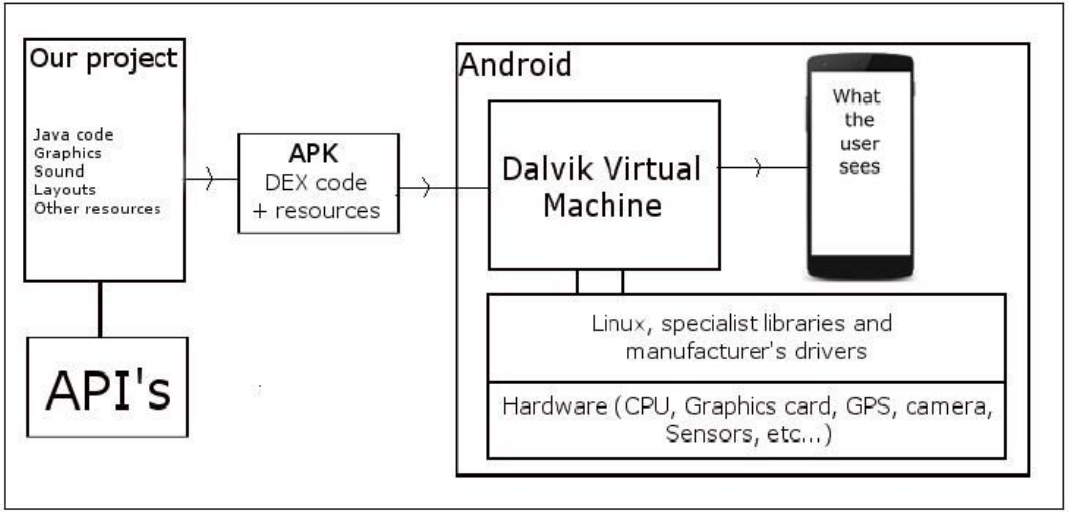
Dalvik/ART

Dalvik

- VM
- Just-In-Time

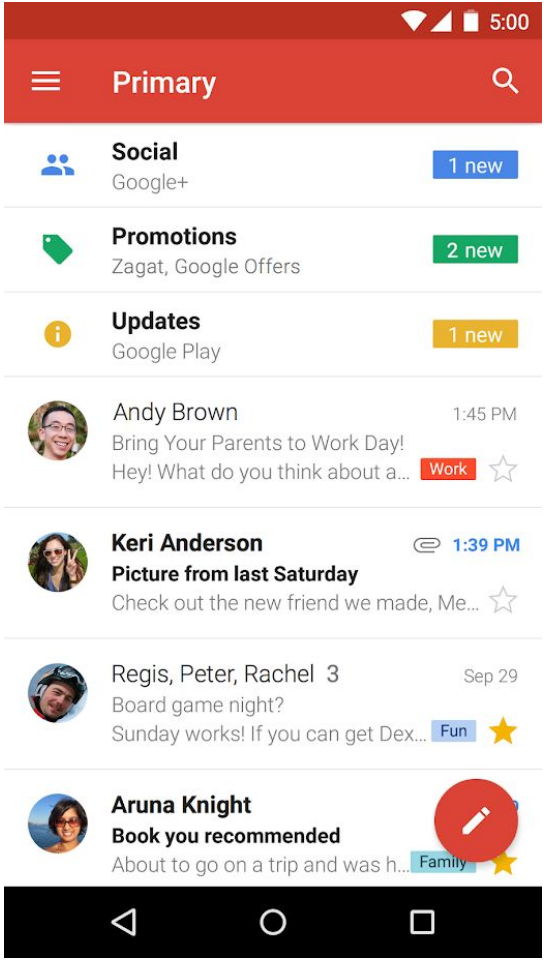
ART

- Ahead-of-Time (AoT)

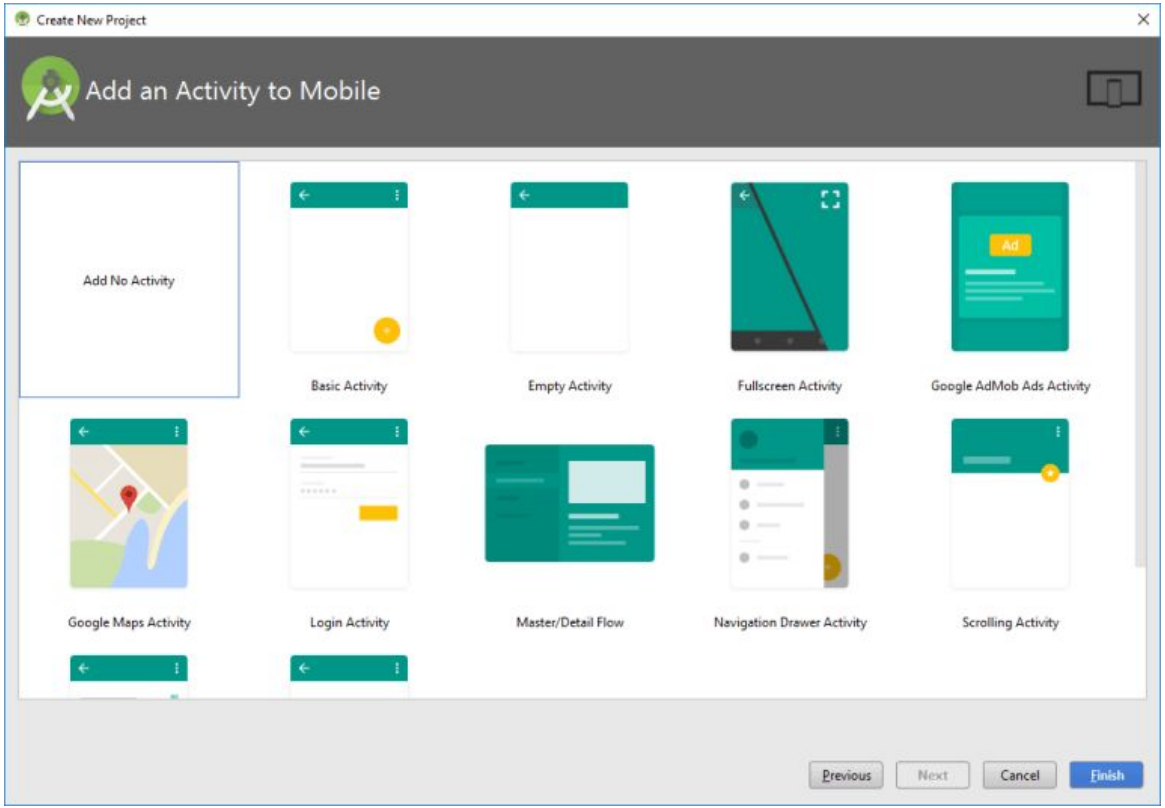


Composants

- Activity
- Intent
- ContentProvider
- Service
- Broadcast receiver



Activity

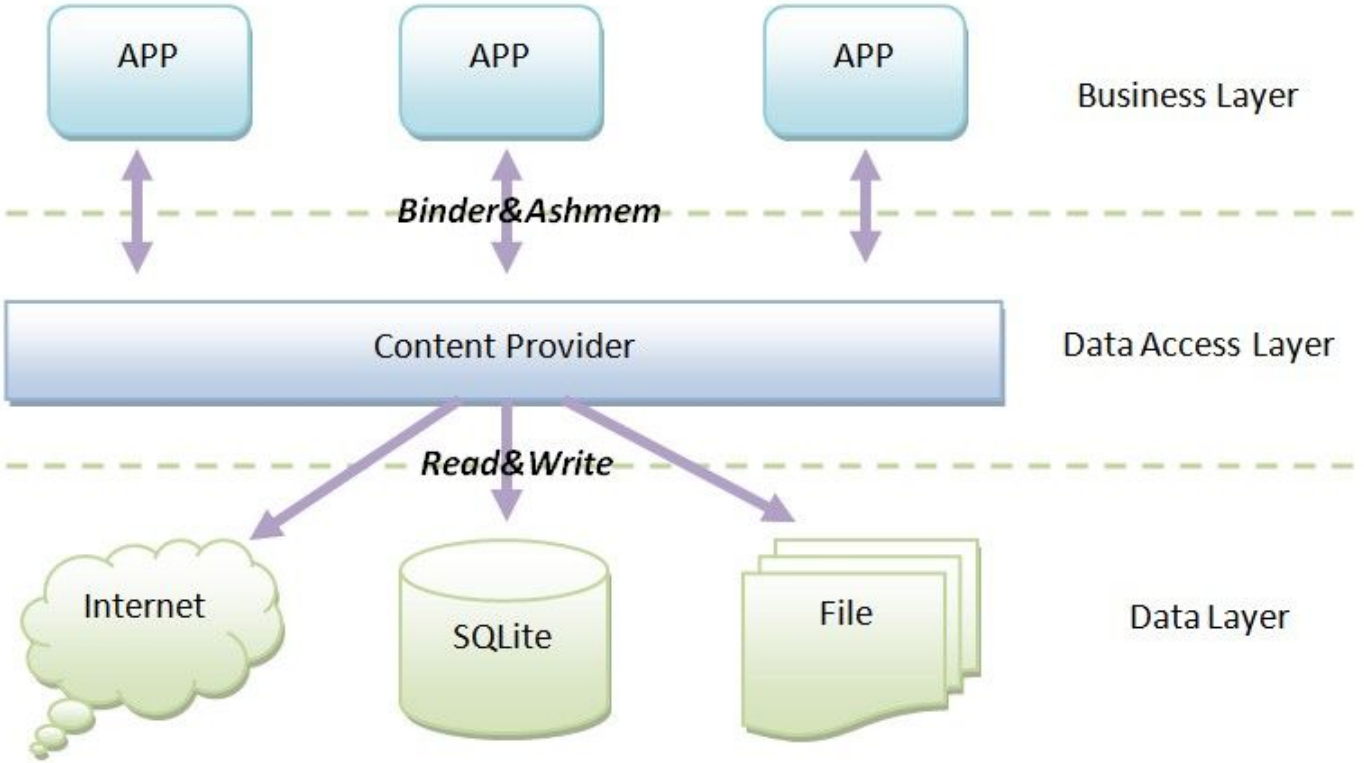

Create New Project
Add an Activity to Mobile
Add No Activity
Basic Activity
Empty Activity
Fullscreen Activity
Ad
Google AdMob Ads Activity
Google Maps Activity
Login Activity
Master/Detail Flow
Navigation Drawer Activity
Scrolling Activity
Previous
Next
Cancel
Finish

Intent


7:00
My First App
Hello world!
SEND
7:00
My First App
Hello world!

Android Service

ContentProvider

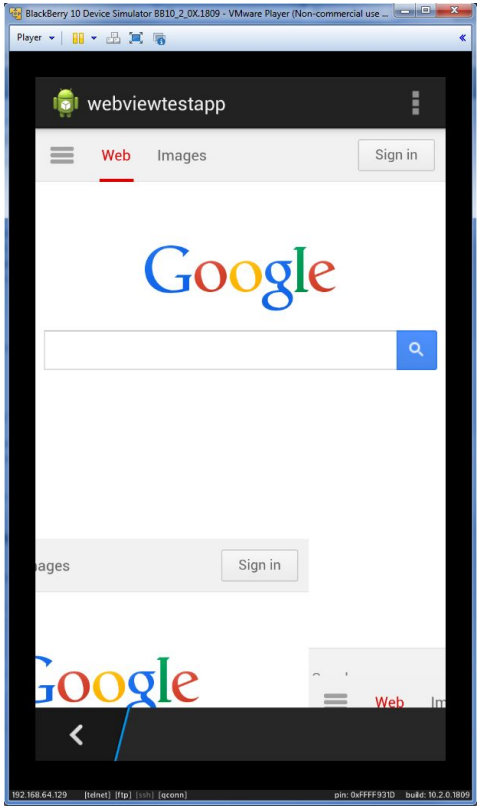


Permissions

- Accéder à des fonctions particulières: identité du téléphone, SMS, Contacts, position GPS
- Demande d’autorisation à l’utilisateur pour les permissions dangereuses

WebView

- WebPage in App
  - Problème des pages Web
    - XSS
    - CRSF
    - SSRF



OWASP Top 10
Mobile

Insecure Logging

- Sensitive Data stored in logs
- On older android versions, even permission
- Log.d, Log.w, … ⇒ Static analysis

    - DIVA : INSECURE LOGGING

      adb logcat

Insecure Data Storage

- Shared Preferences
- Database
- Storage
- Misuse: hard-coded crypto keys

    - DIVA : INSECURE DATA STORAGE 1-4

Local Authentication

- Front JS: Authentification
- Access to the device
- Bruteforce password
- Skip authentication all together

Exposing Sensitive Information

Provider android:exported = true

Any activity with an intent-filter can be triggered by other applications

Exposing Sensitive Information

```
adb shell am start -n fr.hitema/.MainActivity

adb shell am start -n fr.hitema/.MainActivity
-e param1 xxx

adb shell content query –uri
content://fr.hitema.CustomProvider/secretdata
adb shell am start -n
“jakhar.aseem.diva/.APICredsActivity”
```

Endpoint Identity Verification

- TLS
- MitM or install untrusted certificates
- Self-signed certificate
- TrustManager ⇒ Accept everything
- Accept invalid certificates

Endpoint Identity Verification

Certificate Pinning (HKPK)

- Verify that a certificate from a trusted source CA
- Terminate if the certificate is not the one expected
- Verify the hash from the certificate server and you compare from the locally store hash

Frida

- Dynamic Instrumentation Framework
- Installation du serveur sur le téléphone

```
$ adb push frida-server /data/local/tmp/
$ adb shell "chmod 755 /data/local/tmp/frida-server"
$ adb shell "/data/local/tmp/frida-server &"
```

- Vérification

```
$ frida-ps -R
```

Frida

Fichier hook.js:

```
Java.perform(function () {
    const RootDetector = Java.use('sg.vantagepoint.a.c');
    RootDetector.a.overload().implementation = function (arg) {
        return false;
    }
});
```

```
$ frida -R -f be.nviso.application -l hook.js
```

Common Security Threats

- Unpatched security vulnerabilities due to lack of updates and support.
- Backup
- Permission Re-Delegation
- Native: buffer overflows, use after free, off-by-one errors, ...

Mauvaises pratiques
De développement

Insufficient Attack Protection

- Unreliable Information Sources
- Untrustworthy Libraries
- Outdated Library
- Native Code
- Open to Piggybacking
- Unnecessary Permissions

Security Invalidation

- Weak Crypto Algorithm
- Weak Crypto Configuration
- Unpinned Certificate
- Improper Certificate Validation
- Unacknowledged Distribution

Broken Access Control

- Unauthorised Intent Receipt
- Unconstrained Inter-Component Communication
- Unprotected Unix Domain Socket
- Exposed adb-level Capabilities
- Debuggable Release
- Custom Scheme Channel

Sensitive Data Exposure

- Header Attachment
- Unique Hardware Identifier
- Exposed Clipboard
- Exposed Persistent Data
- Insecure Network Protocol
- Exposed Credentials
- Data Residue

Lax Input Validation

- XSS-like Code Injection
- Broken WebView’s Sandbox
- Dynamic Code Loading
- SQL Injection