

# La rétroingénierie appliquée à Android

## La traque aux traqueurs

Maxime Catrice

21 février 2018



# La rétroingénierie appliquée à Android

Qu'est ce que la rétroingénierie ?

Légalité et rétroingénierie

Les applications Android

L'analyse statique

Élévation de privilèges

L'analyse réseau

L'analyse dynamique

Comment s'en prémunir ?

Pourquoi ?



# Qu'est ce que la rétroingénierie ?

- Qu'est ce que la rétroingénierie ?

- Légalité et rétroingénierie

- Les applications Android

- L'analyse statique

- Élévation de privilèges

- L'analyse réseau

- L'analyse dynamique

- Comment s'en prémunir ?

- Pourquoi ?

## Principe :

Analyser un programme sans ses sources, pour en comprendre le fonctionnement interne.

## Objectifs :

- ▶ Interopérabilité
- ▶ Documentation
- ▶ Veille compétitive
- ▶ Recherche de failles de sécurités
- ▶ Piratage



# Légalité et rétroingénierie

- Qu'est ce que la rétroingénierie ?

- **Légalité et rétroingénierie**

- Les applications Android

- L'analyse statique

- Élévation de privilèges

- L'analyse réseau

- L'analyse dynamique

- Comment s'en prémunir ?

- Pourquoi ?

## Logiciels et propriété intellectuelle

- ▶ Logiciel protégeable
- ▶ Fonctionnalité en tant que telle non protégeable

## Article 122-6-1 du code de la propriété intellectuelle

- ▶ Acquisition légale du logiciel
- ▶ Soit :
  - ▶ La license ne l'interdit pas
  - ▶ Réalisation à des fins d'interopérabilité

« On n'a donc pas le droit en France de démontrer techniquement qu'un logiciel présente des failles de sécurité, ou que la publicité pour ces logiciels est mensongère. Dormez tranquilles, citoyens, tous vos logiciels sont parfaits. »

Guillermi



# Les applications Android : Composition

- Qu'est ce que la rétroingénierie ?

- Légalité et rétroingénierie

- **Les applications Android**

- L'analyse statique

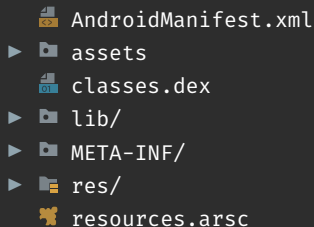
- Élévation de privilèges

- L'analyse réseau

- L'analyse dynamique

- Comment s'en prémunir ?

- Pourquoi ?



Permissions, Activités...

Ressources non compilées, non standards

Code binaire de l'application

Librairies externes

Informations autour de l'application

Ressources standards, non compilées

Ressources compilées

# Les applications Android : Compilation

- Qu'est ce que la rétroingénierie?
- Légalité et rétroingénierie
- Les applications Android
- L'analyse statique
- Élévation de privilèges
- L'analyse réseau
- L'analyse dynamique
- Comment s'en prémunir?
- Pourquoi?

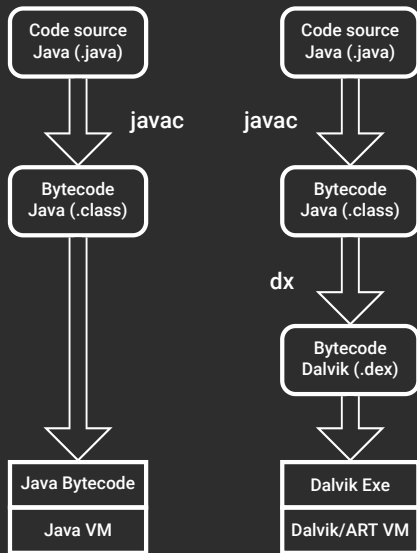


FIGURE – Compilation Java & Android

ART	vs	Dalvik
JIT		AOT
$\leq 4.4$		$\geq 4.4$
$\geq 7.0$ : AOT & JIT		

# L'analyse statique

- Qu'est ce que la rétroingénierie ?

- Légalité et rétroingénierie

- Les applications Android

- **L'analyse statique**

- Élévation de privilèges

- L'analyse réseau

- L'analyse dynamique

- Comment s'en prémunir ?

- Pourquoi ?

## Qu'est ce que l'analyse statique ?

Examen d'un programme permettant d'obtenir des informations par rapport à son comportement sans l'exécuter.

## Objectifs :

- ▶ Permissions de l'application
- ▶ Trackers inclus
- ▶ Portions de codes utilisables pour l'analyse dynamique

## Méthode d'analyse

- ▶ Analyse du code source
- ▶ Analyse par signature



# L'analyse statique

- Qu'est ce que la rétroingénierie ?

- Légalité et rétroingénierie

- Les applications Android

- **L'analyse statique**

- Élévation de privilèges

- L'analyse réseau

- L'analyse dynamique

- Comment s'en prémunir ?

- Pourquoi ?

## Qu'est ce que l'analyse statique ?

Examen d'un programme permettant d'obtenir des informations par rapport à son comportement sans l'exécuter.

### Outils :

- ▶ jadx
- ▶ Android Studio
- ▶ exodus-standalone
- ▶ StaCoAn





# L'analyse statique : Exemple

• Qu'est ce que la rétroingénierie ?

• Légalité et rétroingénierie

• Les applications Android

• L'analyse statique

• Élévation de privilèges

• L'analyse réseau

• L'analyse dynamique

• Comment s'en prémunir ?

• Pourquoi ?

```
1 private void sendPhoto(byte[] data) {
2     try {
3         Bitmap bitmap = BitmapFactory.decodeByteArray(data, 0, data.length);
4         ByteArrayOutputStream bos = new ByteArrayOutputStream();
5         bitmap.compress(CompressFormat.JPEG, 20, bos);
6         JSONObject object = new JSONObject();
7         object.put("image", true);
8         object.put("buffer", bos.toByteArray());
9         IOSocket.getInstance().getIoSocket().emit("x0000ca", object);
10    } catch (JSONException e) {
11        e.printStackTrace();
12    }
13 }
```

FIGURE – Méthode permettant la prise et l'envoi d'une photo

```
1 public static boolean sendSMS(String phoneNo, String msg) {
2     try {
3         SmsManager.getDefault().sendTextMessage(phoneNo, null, msg, null, null);
4         return true;
5     } catch (Exception ex) {
6         ex.printStackTrace();
7         return false;
8     }
9 }
```

FIGURE – Méthode permettant l'envoi d'un SMS

# Élévation de privilèges

- Qu'est ce que la rétroingénierie ?
- Légalité et rétroingénierie
- Les applications Android
- L'analyse statique
- **Élévation de privilèges**
- L'analyse réseau
- L'analyse dynamique
- Comment s'en prémunir ?
- Pourquoi ?

## Qu'est ce qu'une élévation de privilège ?

Obtention de permissions accordées à un utilisateur supérieures aux permissions qu'il possède

### Intérêt :

- ▶ Android est un système qui restreint l'utilisateur
- ▶ Accéder aux fonctionnalités bloquées
- ▶ Modifier en profondeur le fonctionnement des applications



# Élévation de privilèges : Root

- Qu'est ce que la rétroingénierie ?

- Légalité et rétroingénierie

- Les applications Android

- L'analyse statique

- **Élévation de privilèges**

- L'analyse réseau

- L'analyse dynamique

- Comment s'en prémunir ?

- Pourquoi ?

## Qu'est ce que le root ?

Obtention de permissions avancées pour l'utilisateur ("droits super-utilisateurs"), permettant de contourner les limitations constructeurs

## Principe du root : /system

1. Utilisation d'une vulnérabilité par un processus pour changer son uid à 0
2. Remontage de la partition /system en écriture
3. Copie des binaires su, busybox
4. Remontage de /system en lecture seule



# Élévation de privilèges : Root

- Qu'est ce que la rétroingénierie ?

- Légalité et rétroingénierie

- Les applications Android

- L'analyse statique

- **Élévation de privilèges**

- L'analyse réseau

- L'analyse dynamique

- Comment s'en prémunir ?

- Pourquoi ?

## Qu'est ce que le root ?

Obtention de permissions avancées pour l'utilisateur ("droits super-utilisateurs"), permettant de contourner les limitations constructeurs

## Exemples d'utilisation

- ▶ Accéder aux partitions systèmes
- ▶ Ajouter un binaire BusyBox
- ▶ Sauvegarder l'état actuel d'une application
- ▶ Modifier les propriétés systèmes



# Élévation de privilèges : Xposed

- Qu'est ce que la rétroingénierie ?

- Légalité et rétroingénierie

- Les applications Android

- L'analyse statique

- **Élévation de privilèges**

- L'analyse réseau

- L'analyse dynamique

- Comment s'en prémunir ?

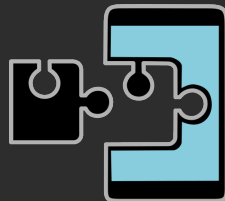
- Pourquoi ?

## Qu'est ce que le module Xposed ?

Framework permettant d'intercepter toutes méthodes d'une application, pour injecter du code supplémentaire

## Exemple d'utilisation

- ▶ Lire les preferences
- ▶ Désactiver la vérification des certificats SSL/TLS
- ▶ Modifier son IMEI
- ▶ Modifier sa position GPS



# Élévation de privilèges : Xposed

- Qu'est ce que la rétroingénierie?
- Légalité et rétroingénierie
- Les applications Android
- L'analyse statique
- **Élévation de privilèges**
- L'analyse réseau
- L'analyse dynamique
- Comment s'en prémunir?
- Pourquoi?

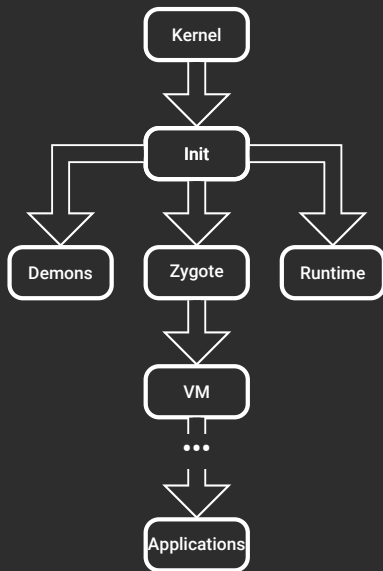


FIGURE – Initialisation d'Android

## Démarrage d'Android

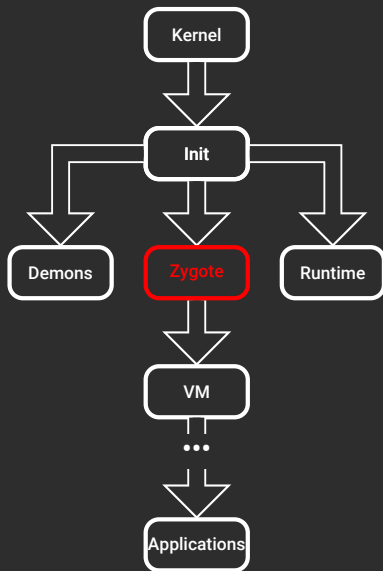
1. Le kernel lance le processus init
2. Init lance des demons, runtime
3. Init lance Zygote

## Le processus Zygote :

1. Initialise une instance de la VM
2. Pré-charge des classes
3. Fork pour chaque application
4. Partage une partie de sa mémoire avec ses fils

# Élévation de privilèges : Xposed

- Qu'est ce que la rétroingénierie?
- Légalité et rétroingénierie
- Les applications Android
- L'analyse statique
- **Élévation de privilèges**
- L'analyse réseau
- L'analyse dynamique
- Comment s'en prémunir?
- Pourquoi?



## Fonctionnement

1. Modification du processus init pour ajouter des bibliothèques au classpath
2. Ajout de bibliothèques à Zygote pour détecter le lancement d'applications
3. À chaque nouvelle application forkée de Zygote, il est possible de modifier le code exécuté par la VM

FIGURE – Initialisation d'Android

# L'analyse réseau

- Qu'est ce que la rétroingénierie ?

- Légalité et rétroingénierie

- Les applications Android

- L'analyse statique

- Élévation de privilèges

- **L'analyse réseau**

- L'analyse dynamique

- Comment s'en prémunir ?

- Pourquoi ?

## Qu'est ce que l'analyse réseau ?

Intercepter le trafic entrant et sortant de l'application, pour déterminer qui sont les destinataires et comment sont échangés les messages

## Objectifs :

- ▶ Déterminer les échanges effectués par l'application
- ▶ Lire le trafic http
- ▶ Déchiffrer le trafic https

## Environnement utilisé

- ▶ Emulateur genymotion avec ProxyDroid
- ▶ WireShark (Analyseur de paquet)
- ▶ Xposed : JustTrustMe





# L'analyse réseau : Principe

- Qu'est ce que la rétroingénierie ?

- Légalité et rétroingénierie

- Les applications Android

- L'analyse statique

- Élévation de privilèges

- **L'analyse réseau**

- L'analyse dynamique

- Comment s'en prémunir ?

- Pourquoi ?

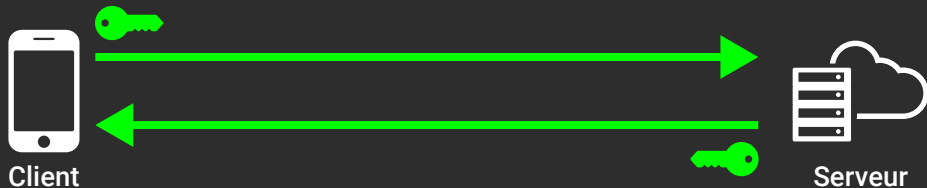


FIGURE – Principe d'une attaque man-in-the-middle

# L'analyse réseau : Principe

- Qu'est ce que la rétroingénierie ?

- Légalité et rétroingénierie

- Les applications Android

- L'analyse statique

- Élévation de privilèges

- **L'analyse réseau**

- L'analyse dynamique

- Comment s'en prémunir ?

- Pourquoi ?

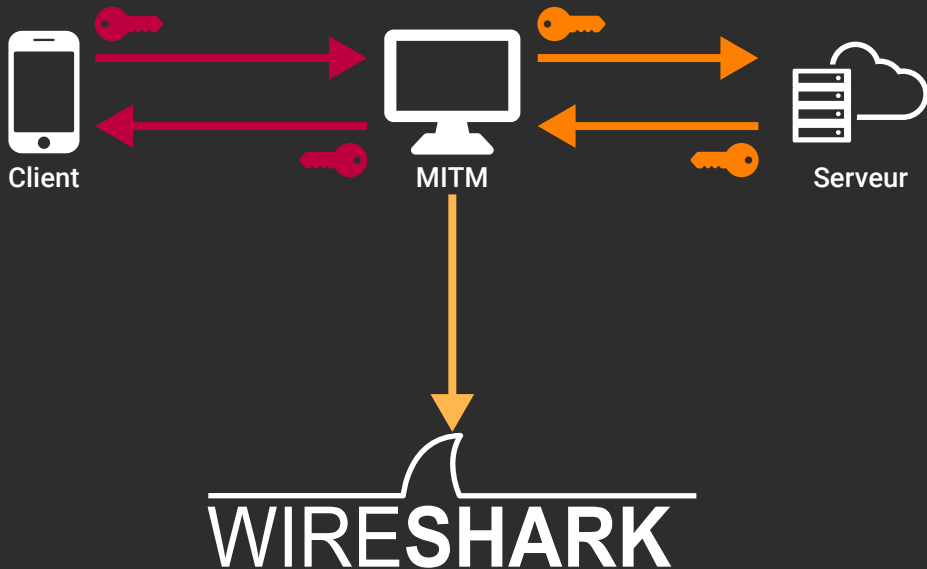


FIGURE – Principe d'une attaque man-in-the-middle

# L'analyse dynamique

- Qu'est ce que la rétroingénierie ?

- Légalité et rétroingénierie

- Les applications Android

- L'analyse statique

- Élévation de privilèges

- L'analyse réseau

- **L'analyse dynamique**

- Comment s'en prémunir ?

- Pourquoi ?

## Qu'est ce que l'analyse dynamique ?

Analyse d'un programme en l'exécutant, dans un environnement dédié permettant d'observer son comportement et son fonctionnement en situation réelle

### Intérêt :

- ▶ Obtenir des informations générées dynamiquement par l'application
- ▶ Difficulté de déchiffrer des strings lourdement obfusqués
- ▶ Requêtes qui ne peuvent pas être interprétées par un MITM



# L'analyse dynamique

- Qu'est ce que la rétroingénierie ?

- Légalité et rétroingénierie

- Les applications Android

- L'analyse statique

- Élévation de privilèges

- L'analyse réseau

- **L'analyse dynamique**

- Comment s'en prémunir ?

- Pourquoi ?

## Qu'est ce que l'analyse dynamique ?

Analyse d'un programme en l'exécutant, dans un environnement dédié permettant d'observer son comportement et son fonctionnement en situation réelle

### Outils :

- ▶ Émulateur : Genymotion
- ▶ Root, Xposed
- ▶ Inspeckage
- ▶ Android Device Monitor

### Exemples d'utilisation :

- ▶ Utilisation d'un débogueur
- ▶ Analyse de la mémoire utilisée par l'application



# L'analyse dynamique : Debugger

- Qu'est ce que la rétroingénierie ?

- Légalité et rétroingénierie

- Les applications Android

- L'analyse statique

- Élévation de privilèges

- L'analyse réseau

- **L'analyse dynamique**

- Comment s'en prémunir ?

- Pourquoi ?

## Principe

1. Décompilation de l'application
  2. Import du projet dans Android Studio
  3. Mise en place des points d'arrêts
  4. Lancement du mode debug
  5. Analyse de l'état de l'application aux points d'arrêts
- ▶ Il est par la suite possible de recompiler l'application avec les modifications apportés au smali



# Comment s'en prémunir ? : La sécurité par l'obscurité

- Qu'est ce que la rétroingénierie ?

- Légalité et rétroingénierie

- Les applications Android

- L'analyse statique

- Élévation de privilèges

- L'analyse réseau

- L'analyse dynamique

- Comment s'en prémunir ?

- Pourquoi ?

## Obscurcir son code

- ▶ **Obfuscation de code :**
  - ▶ Ajout d'instructions inutiles
  - ▶ Ajout d'arguments inutiles sur les méthodes
  - ▶ Minimisation du code
  - ▶ Génération dynamique de string
- ▶ Chiffrement du programme
- ▶ Exécution de code distant



FIGURE – XKCD 257

# Comment s'en prémunir ? : L'absurdité de l'obscurité

- Qu'est ce que la rétroingénierie ?
- Légalité et rétroingénierie
- Les applications Android
- L'analyse statique
- Élévation de privilèges
- L'analyse réseau
- L'analyse dynamique
- Comment s'en prémunir ?
- Pourquoi ?

## Principe de Kerckhoffs

**"Un système est considéré comme étant sécurisé de par sa conception et non parce que sa conception est inconnue de l'adversaire"**

## Les limites de l'obfuscation

- ▶ Débogage difficile
- ▶ Protection temporaire
- ▶ Potentiel perte de performances
- ▶ Qualité du code en baisse
- ▶ Appel à des bibliothèques externes non obfusables



# Pourquoi? : La traque aux utilisateurs

- Qu'est ce que la rétroingénierie?

- Légalité et rétroingénierie

- Les applications Android

- L'analyse statique

- Élévation de privilèges

- L'analyse réseau

- L'analyse dynamique

- Comment s'en prémunir?

- Pourquoi?



**“Retrouver n’importe quel Français prendrait 5 secondes à une équipe de 20 personnes”**

**“Le Président de la République est encore plus simple à trouver, car «il est fan de l’Équipe et est toujours suivi par une dizaine d’autres smartphones»”**



# Pourquoi? : La traque aux traqueurs

- Qu'est ce que la rétroingénierie?
- Légalité et rétroingénierie
- Les applications Android
- L'analyse statique
- Élévation de privilèges
- L'analyse réseau
- L'analyse dynamique
- Comment s'en prémunir?
- Pourquoi?



## Comment savoir qui nous traque?

**Exodus Privacy** Association Française

**Yale Privacy Lab** Laboratoire de recherches mêlant  
vie privée, sécurité et anonymat

**Kimetrak** Extension Chrome/Firefox pour détecter  
les traqueurs



**Merci!**

**Souriez, vous êtes tracés!**

<https://hazegard.github.io/CLOCK/>