L'élévation de privilège résulte de l'octroi à un intrus d'autorisationssupérieures à celles initialement accordées.Par exemple, un intrus avecun jeu de privilèges contenant des autorisations « en lecture seule »élèvent d'une façon ou d'une autre le jeu pour inclure des autorisations« en lecture et en écriture ».

Élévation de privilèges

centralelille
ÉCOLE CENTRALE DE LILLE

L'élévation de privilège résulte de l'octroi à un intrus d'autorisationssupérieures à celles initialement accordées.Par exemple, un intrus avecun jeu de privilèges contenant des autorisations « en lecture seule »élèvent d'une façon ou d'une autre le jeu pour inclure des autorisations« en lecture et en écriture ».

Élévation de privilèges

Qu'est ce qu'une élévation de privilège ?

L'élévation de privilège résulte de l'octroi à un intrus d'autorisationssupérieures à celles initialement accordées.Par exemple, un intrus avecun jeu de privilèges contenant des autorisations « en lecture seule »élèvent d'une façon ou d'une autre le jeu pour inclure des autorisations« en lecture et en écriture ».

Élévation de privilèges

Qu'est ce qu'une élévation de privilège ?

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

L'élévation de privilège résulte de l'octroi à un intrus d'autorisationssupérieures à celles initialement accordées.Par exemple, un intrus avecun jeu de privilèges contenant des autorisations « en lecture seule »élèvent d'une façon ou d'une autre le jeu pour inclure des autorisations« en lecture et en écriture ».

Élévation de privilèges

Qu'est ce qu'une élévation de privilège ?

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

Intérêt :

L'élévation de privilège résulte de l'octroi à un intrus d'autorisationssupérieures à celles initialement accordées.Par exemple, un intrus avecun jeu de privilèges contenant des autorisations « en lecture seule »élèvent d'une façon ou d'une autre le jeu pour inclure des autorisations« en lecture et en écriture ».

Élévation de privilèges

Qu'est ce qu'une élévation de privilège ?

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

Intérêt :

- Android est un système qui restreint l'utilisateur

centralelille
ÉCOLE CENTRALE DE LILLE

L'élévation de privilège résulte de l'octroi à un intrus d'autorisationssupérieures à celles initialement accordées.Par exemple, un intrus avecun jeu de privilèges contenant des autorisations « en lecture seule »élèvent d'une façon ou d'une autre le jeu pour inclure des autorisations« en lecture et en écriture ».

Élévation de privilèges

Qu'est ce qu'une élévation de privilège ?

Obtension 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

centralelille
ÉCOLE CENTRALE DE LILLE

L'élévation de privilège résulte de l'octroi à un intrus d'autorisationssupérieures à celles initialement accordées.Par exemple, un intrus avecun jeu de privilèges contenant des autorisations « en lecture seule »élèvent d'une façon ou d'une autre le jeu pour inclure des autorisations« en lecture et en écriture ».

Élévation de privilèges

Qu'est ce qu'une élévation de privilège ?

Obtension 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

centralelille
ÉCOLE CENTRALE DE LILLE

Root :
Utilisation de privilèges avances, permettant de limiter des limitationsimposées par le système
Par exemple, cela permet de supprimer les applications systèmes,qui ne sont pas désinstallables en tant que simple utilisateur.

Principe du root :
Utilisation du'une faille d'android, ou alors du mode récupération d'android pourobtenir temporairement un uid à , c'est à dire root
Remontage de la partition système en écriture, afin de pouvoir la modifier
Copie de nouveaux binaires, tels que su, busybox
Remontage de la partition système en lecture seuls**Exemples d'utilisation :**

- Accéder aux partitions systèmes
- Installation de busybox
- Sauvegarder une application en conservant l'état de l'applicationau moment de la sauvegarde
- Modifier des propriétés systèmes (densité d'écran, adresse mac...)

Élévation de privilèges : Root

Root :
Utilisation de privilèges avances, permettant de limiter des limitationsimposées par le système
Par exemple, cela permet de supprimer les applications systèmes,qui ne sont pas désinstallables en tant que simple utilisateur.

Principe du root :
Utilisation du'une faille d'android, ou alors du mode récupération d'android pourobtenir temporairement un uid à , c'est à dire root
Remontage de la partition système en écriture, afin de pouvoir la modifier
Copie de nouveaux binaires, tels que su, busybox
Remontage de la partition système en lecture seuls**Exemples d'utilisation :**

- Accéder aux partitions systèmes
- Installation de busybox
- Sauvegarder une application en conservant l'état de l'applicationau moment de la sauvegarde
- Modifier des propriétés systèmes (densité d'écran, adresse mac...)

Élévation de privilèges : Root

Qu'est ce que le root ?

Root :
Utilisation de privilèges avances, permettant de limiter des limitationsimposées par le système
Par exemple, cela permet de supprimer les applications systèmes,qui ne sont pas désinstallables en tant que simple utilisateur.
Principe du root :
Utilisation du'une faille d'android, ou alors du mode récupération d'android pourobtenir temporairement un uid à , c'est à dire root
Remontage de la partition système en écriture, afin de pouvoir la modifier
Copie de nouveaux binaires, tels que su, busybox
Remontage de la partition système en lecture seuls**Exemples d'utilisation :**
- Accéder aux partitions systèmes
- Installation de busybox
- Sauvegarder une application en conservant l'état de l'applicationau moment de la sauvegarde
- Modifier des propriétés systèmes (densité d'écran, adresse mac...)

Élévation de privilèges : Root

Qu'est ce que le root ?

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

Root :
Utilisation de privilèges avances, permettant de limiter des limitationsimposées par le système
Par exemple, cela permet de supprimer les applications systèmes,qui ne sont pas désinstallables en tant que simple utilisateur.
Principe du root :
Utilisation du'une faille d'android, ou alors du mode récupération d'android pourobtenir temporairement un uid à , c'est à dire root
Remontage de la partition système en écriture, afin de pouvoir la modifier
Copie de nouveaux binaires, tels que su, busybox
Remontage de la partition système en lecture seuls**Exemples d'utilisation :**
- Accéder aux partitions systèmes
- Installation de busybox
- Sauvegarder une application en conservant l'état de l'applicationau moment de la sauvegarde
- Modifier des propriétés systèmes (densité d'écran, adresse mac...)

Élévation de privilèges : Root

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`

centralelille
ÉCOLE CENTRALE DE LILLE

Root :
Utilisation de privilèges avances, permettant de limiter des limitationsimposées par le système
Par exemple, cela permet de supprimer les applications systèmes,qui ne sont pas désinstallables en tant que simple utilisateur.
Principe du root :
Utilisation du'une faille d'android, ou alors du mode récupération d'android pourobtenir temporairement un uid à , c'est à dire root
Remontage de la partition système en écriture, afin de pouvoir la modifier
Copie de nouveaux binaires, tels que su, busybox
Remontage de la partition système en lecture seuls**Exemples d'utilisation :**
- Accéder aux partitions systèmes
- Installation de busybox
- Sauvegarder une application en conservant l'état de l'applicationau moment de la sauvegarde
- Modifier des propriétés systèmes (densité d'écran, adresse mac...)

Élévation de privilèges : Root

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

Root :
Utilisation de privilèges avances, permettant de limiter des limitationsimposées par le système
Par exemple, cela permet de supprimer les applications systèmes,qui ne sont pas désinstallables en tant que simple utilisateur.
Principe du root :
Utilisation du'une faille d'android, ou alors du mode récupération d'android pourobtenir temporairement un uid à , c'est à dire root
Remontage de la partition système en écriture, afin de pouvoir la modifier
Copie de nouveaux binaires, tels que su, busybox
Remontage de la partition système en lecture seuls**Exemples d'utilisation :**
- Accéder aux partitions systèmes
- Installation de busybox
- Sauvegarder une application en conservant l'état de l'applicationau moment de la sauvegarde
- Modifier des propriétés systèmes (densité d'écran, adresse mac...)

Élévation de privilèges : Root

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

Root :
Utilisation de privilèges avances, permettant de limiter des limitationsimposées par le système
Par exemple, cela permet de supprimer les applications systèmes,qui ne sont pas désinstallables en tant que simple utilisateur.
Principe du root :
Utilisation du'une faille d'android, ou alors du mode récupération d'android pourobtenir temporairement un uid à , c'est à dire root
Remontage de la partition système en écriture, afin de pouvoir la modifier
Copie de nouveaux binaires, tels que su, busybox
Remontage de la partition système en lecture seuls**Exemples d'utilisation :**
- Accéder aux partitions systèmes
- Installation de busybox
- Sauvegarder une application en conservant l'état de l'applicationau moment de la sauvegarde
- Modifier des propriétés systèmes (densité d'écran, adresse mac...)

Élévation de privilèges : Root

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

Root :
Utilisation de privilèges avances, permettant de limiter des limitationsimposées par le système
Par exemple, cela permet de supprimer les applications systèmes,qui ne sont pas désinstallables en tant que simple utilisateur.
Principe du root :
Utilisation du'une faille d'android, ou alors du mode récupération d'android pourobtenir temporairement un uid à , c'est à dire root
Remontage de la partition système en écriture, afin de pouvoir la modifier
Copie de nouveaux binaires, tels que su, busybox
Remontage de la partition système en lecture seulsExemples d'utilisation :
- Accéder aux partitions systèmes
- Installation de busybox
- Sauvegarder une application en conservant l'état de l'applicationau moment de la sauvegarde
- Modifier des propriétés systèmes (densité d'écran, adresse mac...)

Élévation de privilèges : Root

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

Root :
Utilisation de privilèges avances, permettant de limiter des limitationsimposées par le système
Par exemple, cela permet de supprimer les applications systèmes,qui ne sont pas désinstallables en tant que simple utilisateur.
Principe du root :
Utilisation du'une faille d'android, ou alors du mode récupération d'android pourobtenir temporairement un uid à , c'est à dire root
Remontage de la partition système en écriture, afin de pouvoir la modifier
Copie de nouveaux binaires, tels que su, busybox
Remontage de la partition système en lecture seuls**Exemples d'utilisation :**
- Accéder aux partitions systèmes
- Installation de busybox
- Sauvegarder une application en conservant l'état de l'applicationau moment de la sauvegarde
- Modifier des propriétés systèmes (densité d'écran, adresse mac...)

Élévation de privilèges : Root

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

centralelille
ÉCOLE CENTRALE DE LILLE

Root :
Utilisation de privilèges avances, permettant de limiter des limitationsimposées par le système
Par exemple, cela permet de supprimer les applications systèmes,qui ne sont pas désinstallables en tant que simple utilisateur.
Principe du root :
Utilisation du'une faille d'android, ou alors du mode récupération d'android pourobtenir temporairement un uid à , c'est à dire root
Remontage de la partition système en écriture, afin de pouvoir la modifier
Copie de nouveaux binaires, tels que su, busybox
Remontage de la partition système en lecture seuls**Exemples d'utilisation :**
- Accéder aux partitions systèmes
- Installation de busybox
- Sauvegarder une application en conservant l'état de l'applicationau moment de la sauvegarde
- Modifier des propriétés systèmes (densité d'écran, adresse mac...)

Élévation de privilèges : Root

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

centralelille
ÉCOLE CENTRALE DE LILLE

Root :
Utilisation de privilèges avances, permettant de limiter des limitationsimposées par le système
Par exemple, cela permet de supprimer les applications systèmes,qui ne sont pas désinstallables en tant que simple utilisateur.
Principe du root :
Utilisation du'une faille d'android, ou alors du mode récupération d'android pourobtenir temporairement un uid à , c'est à dire root
Remontage de la partition système en écriture, afin de pouvoir la modifier
Copie de nouveaux binaires, tels que su, busybox
Remontage de la partition système en lecture seuls**Exemples d'utilisation :**
- Accéder aux partitions systèmes
- Installation de busybox
- Sauvegarder une application en conservant l'état de l'applicationau moment de la sauvegarde
- Modifier des propriétés systèmes (densité d'écran, adresse mac...)

Élévation de privilèges : Root

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

Root :
Utilisation de privilèges avances, permettant de limiter des limitationsimposées par le système
Par exemple, cela permet de supprimer les applications systèmes,qui ne sont pas désinstallables en tant que simple utilisateur.
Principe du root :
Utilisation du'une faille d'android, ou alors du mode récupération d'android pourobtenir temporairement un uid à , c'est à dire root
Remontage de la partition système en écriture, afin de pouvoir la modifier
Copie de nouveaux binaires, tels que su, busybox
Remontage de la partition système en lecture seuls**Exemples d'utilisation :**
- Accéder aux partitions systèmes
- Installation de busybox
- Sauvegarder une application en conservant l'état de l'applicationau moment de la sauvegarde
- Modifier des propriétés systèmes (densité d'écran, adresse mac...)

Élévation de privilèges : Root

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

centralelille
ÉCOLE CENTRALE DE LILLE

Root :
Utilisation de privilèges avances, permettant de limiter des limitationsimposées par le système
Par exemple, cela permet de supprimer les applications systèmes,qui ne sont pas désinstallables en tant que simple utilisateur.
Principe du root :
Utilisation du'une faille d'android, ou alors du mode récupération d'android pourobtenir temporairement un uid à , c'est à dire root
Remontage de la partition système en écriture, afin de pouvoir la modifier
Copie de nouveaux binaires, tels que su, busybox
Remontage de la partition système en lecture seuls**Exemples d'utilisation :**
- Accéder aux partitions systèmes
- Installation de busybox
- Sauvegarder une application en conservant l'état de l'applicationau moment de la sauvegarde
- Modifier des propriétés systèmes (densité d'écran, adresse mac...)

Élévation de privilèges : Root

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

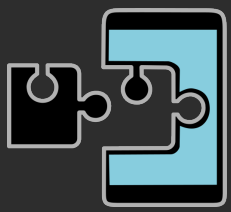
- Accéder aux partitions systèmes
- Ajouter un binaire BusyBox
- Sauvegarder l'état actuel d'une application
- Modifier les propriétés systèmes

centralelille
ÉCOLE CENTRALE DE LILLE

Xposed :
Framework permettant d'intercepter toutes méthodes d'une application, pour injecterdu code suplémentaireExemple d'utilisation
Ne fonctionne qu'avec les applications java, mais pas avec les bibrairies natives, par exemple

Exemples d'utilisation de Xposed :
- Lire les paramètres des applications
- Désactiver la vérification SSL, pour par exemple, pouvoir déchiffre le traffic
- Modifier son IMEI
- Simuler sa position GPS

Élévation de privilèges : Xposed

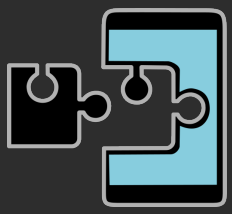


Xposed :
Framework permettant d'intercepter toutes méthodes d'une application, pour injecterdu code suplémentaireExemple d'utilisation
Ne fonctionne qu'avec les applications java, mais pas avec les bibrairies natives, par exemple

Exemples d'utilisation de Xposed :
- Lire les paramètres des applications
- Désactiver la vérification SSL, pour par exemple, pouvoir déchiffre le traffic
- Modifier son IMEI
- Simuler sa position GPS

Élévation de privilèges : Xposed

Qu'est ce que le module Xposed ?



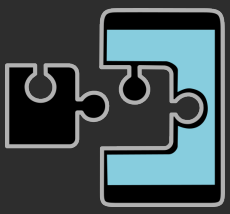
Xposed :
Framework permettant d'intercepter toutes méthodes d'une application, pour injecterdu code suplémentaireExemple d'utilisation
Ne fonctionne qu'avec les applications java, mais pas avec les bibrairies natives, par exemple

Exemples d'utilisation de Xposed :
- Lire les paramètres des applications
- Désactiver la vérification SSL, pour par exemple, pouvoir déchiffre le traffic
- Modifier son IMEI
- Simuler sa position GPS

Élévation de privilèges : Xposed

Qu'est ce que le module Xposed ?

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



Xposed :
Framework permettant d'intercepter toutes méthodes d'une application, pour injecterdu code suplémentaireExemple d'utilisation
Ne fonctionne qu'avec les applications java, mais pas avec les bibrairies natives, par exemple

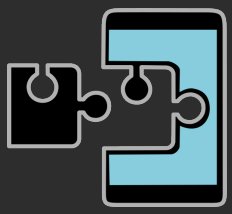
Exemples d'utilisation de Xposed :
- Lire les paramètres des applications
- Désactiver la vérification SSL, pour par exemple, pouvoir déchiffre le traffic
- Modifier son IMEI
- Simuler sa position GPS

Élévation de privilèges : Xposed

Qu'est ce que le module Xposed ?

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

Exemple d'utilisation



Xposed :
Framework permettant d'intercepter toutes méthodes d'une application, pour injecterdu code suplémentaireExemple d'utilisation
Ne fonctionne qu'avec les applications java, mais pas avec les bibrairies natives, par exemple

Exemples d'utilisation de Xposed :
- Lire les paramètres des applications
- Désactiver la vérification SSL, pour par exemple, pouvoir déchiffre le traffic
- Modifier son IMEI
- Simuler sa position GPS

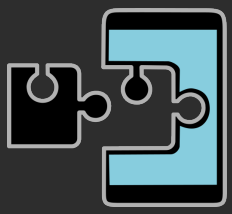
Élévation de privilèges : Xposed

Qu'est ce que le module Xposed ?

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

Exemple d'utilisation

- Lire les preferences



Xposed :
Framework permettant d'intercepter toutes méthodes d'une application, pour injecterdu code suplémentaireExemple d'utilisation
Ne fonctionne qu'avec les applications java, mais pas avec les bibrairies natives, par exemple

Exemples d'utilisation de Xposed :
- Lire les paramètres des applications
- Désactiver la vérification SSL, pour par exemple, pouvoir déchiffre le traffic
- Modifier son IMEI
- Simuler sa position GPS

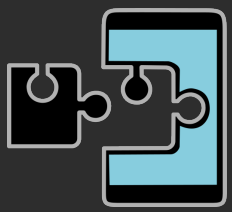
Élévation de privilèges : Xposed

Qu'est ce que le module Xposed ?

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

Exemple d'utilisation

- Lire les preferences
- Désactiver la vérification des certificats SSL



Xposed :
Framework permettant d'intercepter toutes méthodes d'une application, pour injecterdu code suplémentaireExemple d'utilisation
Ne fonctionne qu'avec les applications java, mais pas avec les bibrairies natives, par exemple

Exemples d'utilisation de Xposed :
- Lire les paramètres des applications
- Désactiver la vérification SSL, pour par exemple, pouvoir déchiffre le traffic
- Modifier son IMEI
- Simuler sa position GPS

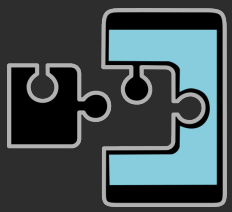
Élévation de privilèges : Xposed

Qu'est ce que le module Xposed ?

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

Exemple d'utilisation

- Lire les preferences
- Désactiver la vérification des certificats SSL
- Modifier son IMEI



Xposed :
Framework permettant d'intercepter toutes méthodes d'une application, pour injecterdu code suplémentaireExemple d'utilisation
Ne fonctionne qu'avec les applications java, mais pas avec les bibrairies natives, par exemple

Exemples d'utilisation de Xposed :
- Lire les paramètres des applications
- Désactiver la vérification SSL, pour par exemple, pouvoir déchiffre le traffic
- Modifier son IMEI
- Simuler sa position GPS

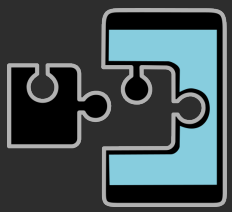
Élévation de privilèges : Xposed

Qu'est ce que le module Xposed ?

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

Exemple d'utilisation

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



Le démarrage d'Android :

- On s'intéresse au processus une fois le lancement du kernel
- Le kernel initialise le processus Init
- Init lance à son tour des démons (usb, adb, ril), et le runtime
- Init lance aussi Zygote

Élévation de privilèges : Xposed

centralelille
ÉCOLE CENTRALE DE LILLE

Le démarrage d'Android :

- On s'intéresse au processus une fois le lancement du kernel
- Le kernel initialise le processus Init
- Init lance à son tour des démons (usb, adb, ril), et le runtime
- Init lance aussi Zygote

Élévation de privilèges : Xposed

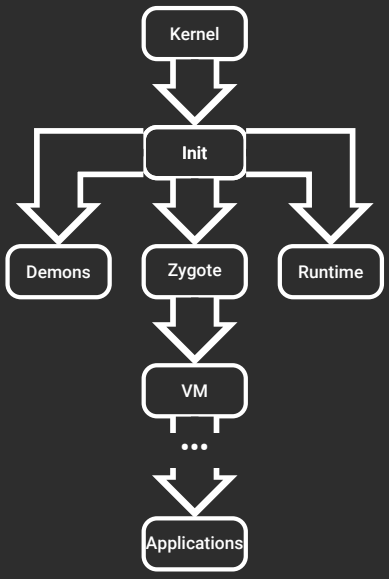


FIGURE – Initialisation d'Android

Le démarrage d'Android :

- On s'intéresse au processus une fois le lancement du kernel
- Le kernel initialise le processus Init
- Init lance à son tour des démons (usb, adb, ril), et le runtime
- Init lance aussi Zygote

Élévation de privilèges : Xposed

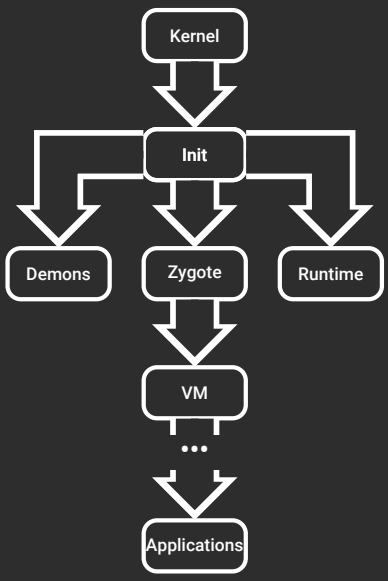


FIGURE – Initialisation d'Android

Démarrage d'Android

Le démarrage d'Android :

- On s'intéresse au processus une fois le lancement du kernel
- Le kernel initialise le processus Init
- Init lance à son tour des démons (usb, adb, ril), et le runtime
- Init lance aussi Zygote

Élévation de privilèges : Xposed

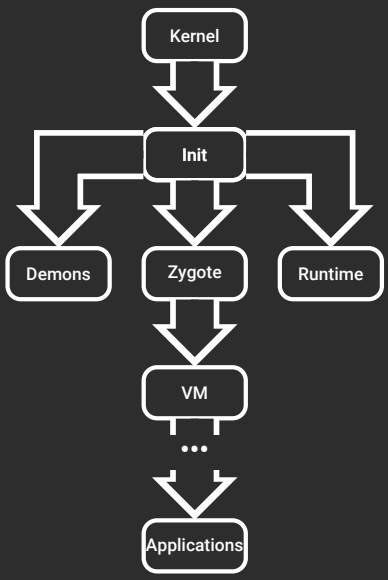


FIGURE – Initialisation d'Android

Démarrage d'Android

1. Le kernel lance le processus init

Le démarrage d'Android :

- On s'intéresse au processus une fois le lancement du kernel
- Le kernel initialise le processus Init
- Init lance à son tour des démons (usb, adb, ril), et le runtime
- Init lance aussi Zygote

Élévation de privilèges : Xposed

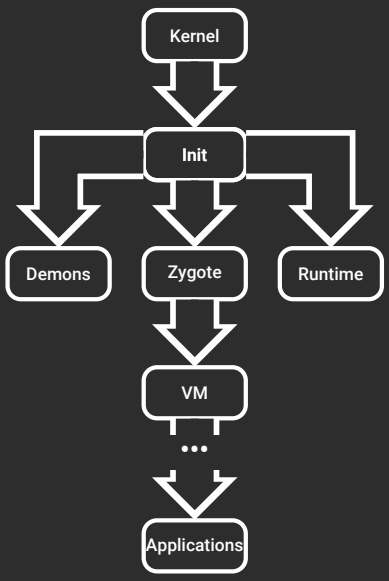


FIGURE – Initialisation d'Android

Démarrage d'Android

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

Le démarrage d'Android :

- On s'intéresse au processus une fois le lancement du kernel
- Le kernel initialise le processus Init
- Init lance à son tour des démons (usb, adb, ril), et le runtime
- Init lance aussi Zygote

Zygote :

Zygote est un processus primordiale pour Android :

- Il initialise la machine virtuelle
- pré-charges des classes communes aux applications
- Se fork pour chaque nouvelle application lancée
- Partage une partie de sa mémoire avec les applications forkées

Élévation de privilèges : Xposed

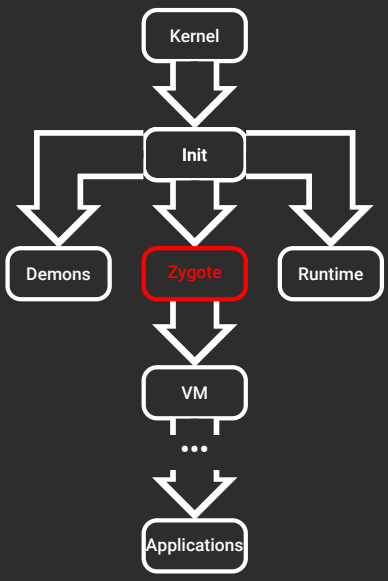


FIGURE – Initialisation d'Android

Démarrage d'Android

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

Le démarrage d'Android :

- On s'intéresse au processus une fois le lancement du kernel
- Le kernel initialise le processus Init
- Init lance à son tour des démons (usb, adb, ril), et le runtime
- Init lance aussi Zygote

Zygote :

Zygote est un processus primordiale pour Android :

- Il initialise la machine virtuelle
- pré-charges des classes communes aux applications
- Se fork pour chaque nouvelle application lancée
- Partage une partie de sa mémoire avec les applications forkées

Élévation de privilèges : Xposed

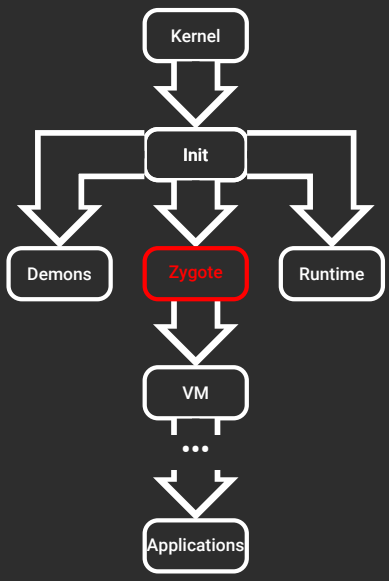


FIGURE – Initialisation d'Android

Démarrage d'Android

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

Le processus Zygote :

Le démarrage d'Android :

- On s'intéresse au processus une fois le lancement du kernel
- Le kernel initialise le processus Init
- Init lance à son tour des démons (usb, adb, ril), et le runtime
- Init lance aussi Zygote

Zygote :

Zygote est un processus primordiale pour Android :

- Il initialise la machine virtuelle
- pré-charges des classes communes aux applications
- Se fork pour chaque nouvelle application lancée
- Partage une partie de sa mémoire avec les applications forkées

Élévation de privilèges : Xposed

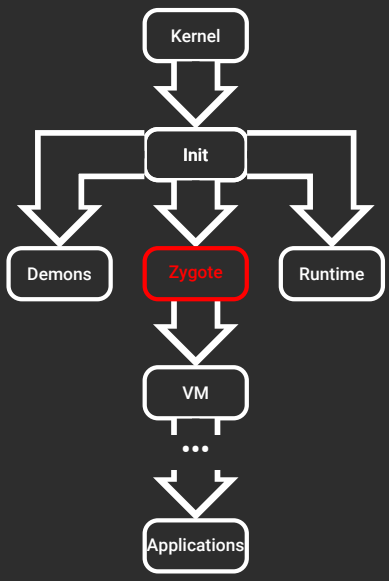


FIGURE – Initialisation d'Android

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

Le démarrage d'Android :

- On s'intéresse au processus une fois le lancement du kernel
- Le kernel initialise le processus Init
- Init lance à son tour des démons (usb, adb, ril), et le runtime
- Init lance aussi Zygote

Zygote :

Zygote est un processus primordiale pour Android :

- Il initialise la machine virtuelle
- pré-charges des classes communes aux applications
- Se fork pour chaque nouvelle application lancée
- Partage une partie de sa mémoire avec les applications forkées

Élévation de privilèges : Xposed

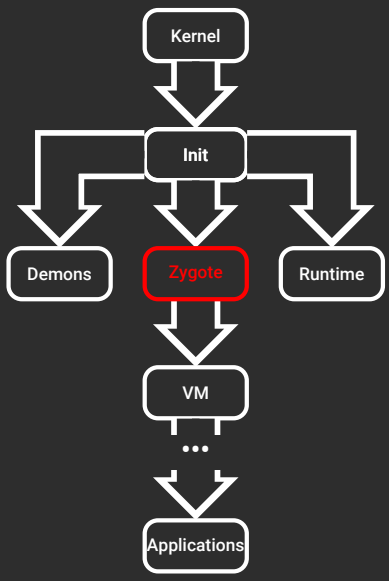


FIGURE – Initialisation d'Android

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

Le démarrage d'Android :

- On s'intéresse au processus une fois le lancement du kernel
- Le kernel initialise le processus Init
- Init lance à son tour des démons (usb, adb, ril), et le runtime
- Init lance aussi Zygote

Zygote :

Zygote est un processus primordiale pour Android :

- Il initialise la machine virtuelle
- pré-charges des classes communes aux applications
- Se fork pour chaque nouvelle application lancée
- Partage une partie de sa mémoire avec les applications forkées

Élévation de privilèges : Xposed

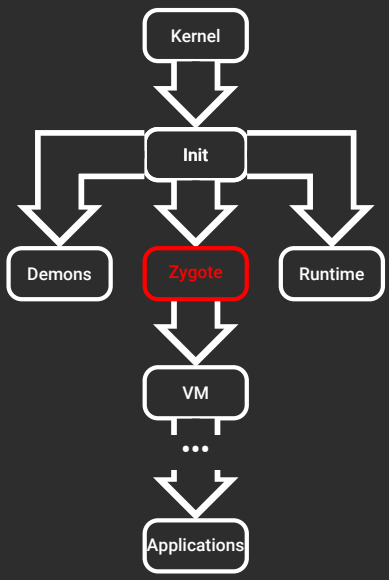


FIGURE – Initialisation d'Android

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

centralelille ÉCOLE CENTRALE DE LILLE

Le démarrage d'Android :

- On s'intéresse au processus une fois le lancement du kernel
- Le kernel initialise le processus Init
- Init lance à son tour des démons (usb, adb, ril), et le runtime
- Init lance aussi Zygote

Zygote :

Zygote est un processus primordiale pour Android :

- Il initialise la machine virtuelle
- pré-charges des classes communes aux applications
- Se fork pour chaque nouvelle application lancée
- Partage une partie de sa mémoire avec les applications forkées

Fonctionnement de Xposed :

- Le processus init est modifié pour changer le comportement de Zygote en ajoutantdes librairies au classpath
- Ajout de librairies à Zygote permettant de détecter le lancement d'application
- A chaque lancement d'une application, Zygote va remplacer le code de l'application-pour injecter du code externe

Élévation de privilèges : Xposed

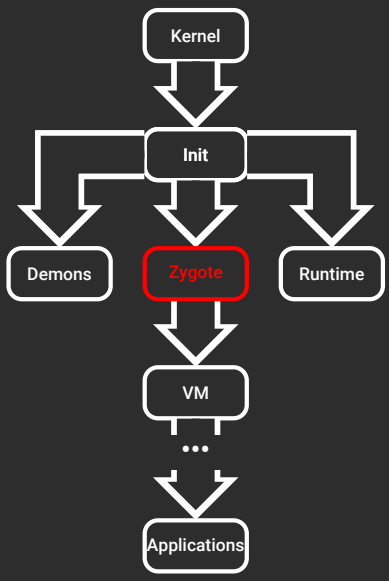


FIGURE – Initialisation d'Android

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

Le démarrage d'Android :

- On s'intéresse au processus une fois le lancement du kernel
- Le kernel initialise le processus Init
- Init lance à son tour des démons (usb, adb, ril), et le runtime
- Init lance aussi Zygote

Zygote :

Zygote est un processus primordiale pour Android :

- Il initialise la machine virtuelle
- pré-charges des classes communes aux applications
- Se fork pour chaque nouvelle application lancée
- Partage une partie de sa mémoire avec les applications forkées

Fonctionnement de Xposed :

- Le processus init est modifié pour changer le comportement de Zygote en ajoutantdes librairies au classpath
- Ajout de librairies à Zygote permettant de détecter le lancement d'application
- A chaque lancement d'une application, Zygote va remplacer le code de l'application-pour injecter du code externe

Élévation de privilèges : Xposed

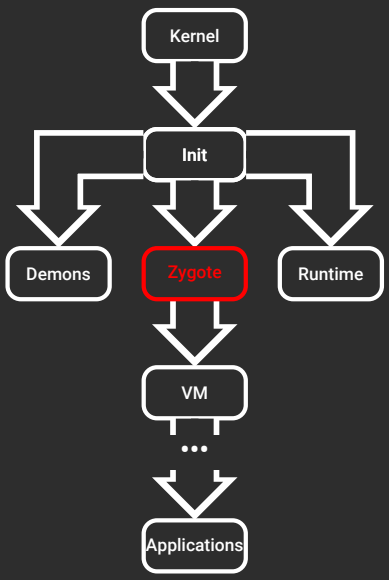


FIGURE – Initialisation d'Android

Fonctionnement

Le démarrage d'Android :

- On s'intéresse au processus une fois le lancement du kernel
- Le kernel initialise le processus Init
- Init lance à son tour des démons (usb, adb, ril), et le runtime
- Init lance aussi Zygote

Zygote :

Zygote est un processus primordiale pour Android :

- Il initialise la machine virtuelle
- pré-charges des classes communes aux applications
- Se fork pour chaque nouvelle application lancée
- Partage une partie de sa mémoire avec les applications forkées

Fonctionnement de Xposed :

- Le processus init est modifié pour changer le comportement de Zygote en ajoutantdes librairies au classpath
- Ajout de librairies à Zygote permettant de détecter le lancement d'application
- A chaque lancement d'une application, Zygote va remplacer le code de l'application-pour injecter du code externe

Élévation de privilèges : Xposed

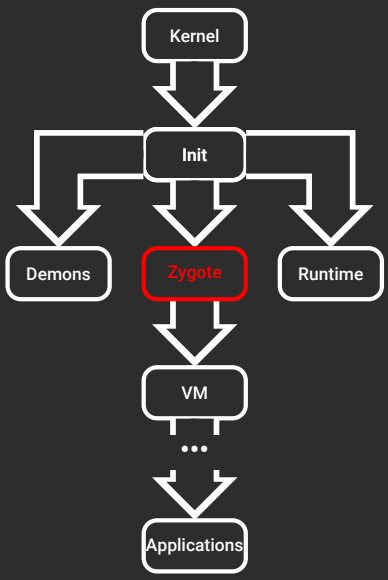


FIGURE – Initialisation d'Android

Fonctionnement

1. Modification du processus init pour ajouter des librairies au classpath

Le démarrage d'Android :

- On s'intéresse au processus une fois le lancement du kernel
- Le kernel initialise le processus Init
- Init lance à son tour des démons (usb, adb, ril), et le runtime
- Init lance aussi Zygote

Zygote :

Zygote est un processus primordiale pour Android :

- Il initialise la machine virtuelle
- pré-charges des classes communes aux applications
- Se fork pour chaque nouvelle application lancée
- Partage une partie de sa mémoire avec les applications forkées

Fonctionnement de Xposed :

- Le processus init est modifié pour changer le comportement de Zygote en ajoutantdes librairies au classpath
- Ajout de librairies à Zygote permettant de détecter le lancement d'application
- A chaque lancement d'une application, Zygote va remplacer le code de l'application-pour injecter du code externe

Élévation de privilèges : Xposed

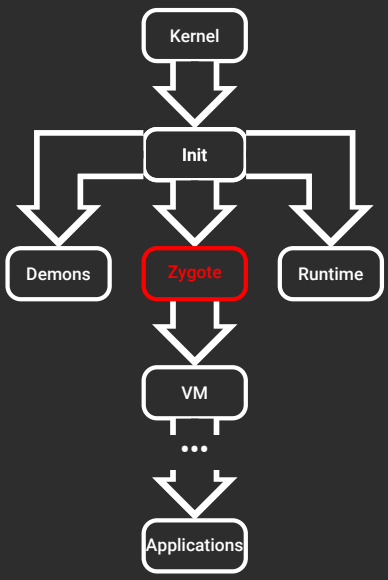


FIGURE – Initialisation d'Android

Fonctionnement

1. Modification du processus init pour ajouter des librairies au classpath
2. Ajout de librairies à Zygote pour détecter le lancement d'applications

Le démarrage d'Android :

- On s'intéresse au processus une fois le lancement du kernel
- Le kernel initialise le processus Init
- Init lance à son tour des démons (usb, adb, ril), et le runtime
- Init lance aussi Zygote

Zygote :

Zygote est un processus primordiale pour Android :

- Il initialise la machine virtuelle
- pré-charges des classes communes aux applications
- Se fork pour chaque nouvelle application lancée
- Partage une partie de sa mémoire avec les applications forkées

Fonctionnement de Xposed :

- Le processus init est modifié pour changer le comportement de Zygote en ajoutantdes librairies au classpath
- Ajout de librairies à Zygote permettant de détecter le lancement d'application
- A chaque lancement d'une application, Zygote va remplacer le code de l'application-pour injecter du code externe

Élévation de privilèges : Xposed

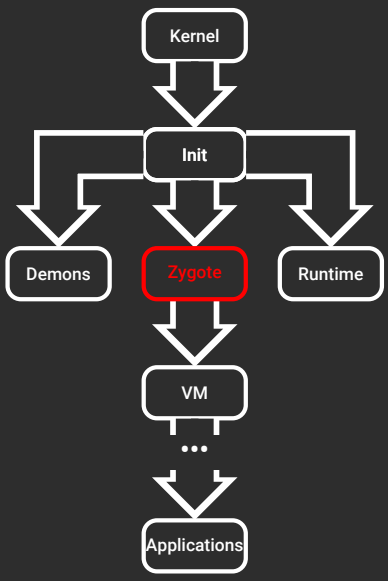


FIGURE – Initialisation d'Android

Fonctionnement

1. Modification du processus init pour ajouter des librairies au classpath
2. Ajout de librairies à Zygote pour détecter le lancement d'applications
3. A chaque nouvelle aplication forké de Zygote, il est possible de modifier le code exécuté lar la VM