haute école neuchâtel berne jura arc ingénierie www.he-arc.ch

MODÈLE DE SÉCURITÉ TECHNIQUE D'ANDROID

Simon Meier

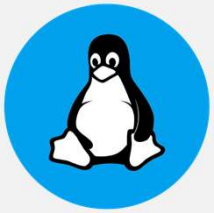
INF 3 DLM-a

haute école neuchâtel berne jura arc ingénierie www.he-arc.ch

Table des matières

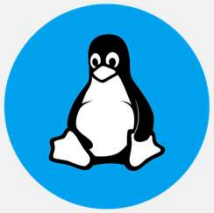
ANDROID

- Système open-source basé sur un noyau linux



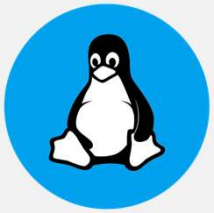
ANDROID

- Système open-source basé sur un noyau linux
- Rachat par Google en 2005



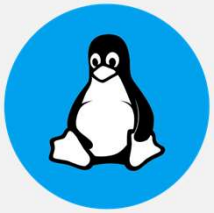
ANDROID

- Système open-source basé sur un noyau linux
- Rachat par Google en 2005
- 2015, 80% de parts du marché.



ANDROID

- Système open-source basé sur un noyau linux
- Rachat par Google en 2005
- 2015, 80% de parts du marché.
- Version actuelle: 12

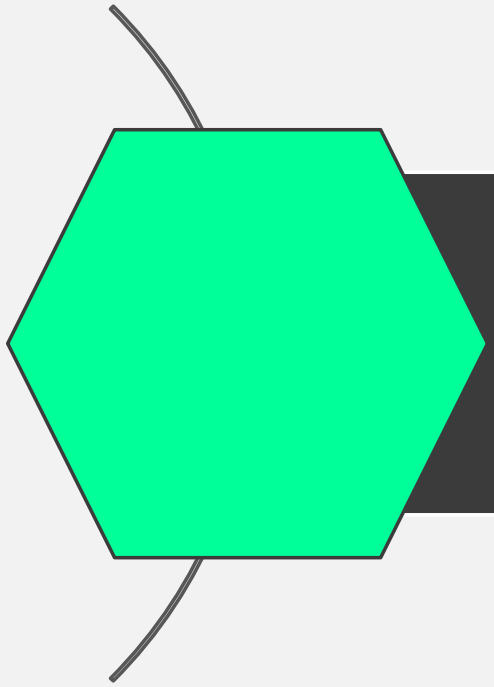


ANDROID

Part actuelle:

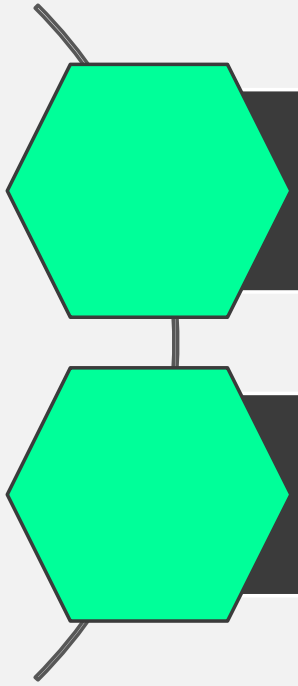
Source: https://gs.statcounter.com/os-market-share/mobile/worldwide

COUCHES LOGICIELLE



1. Linux Kernel

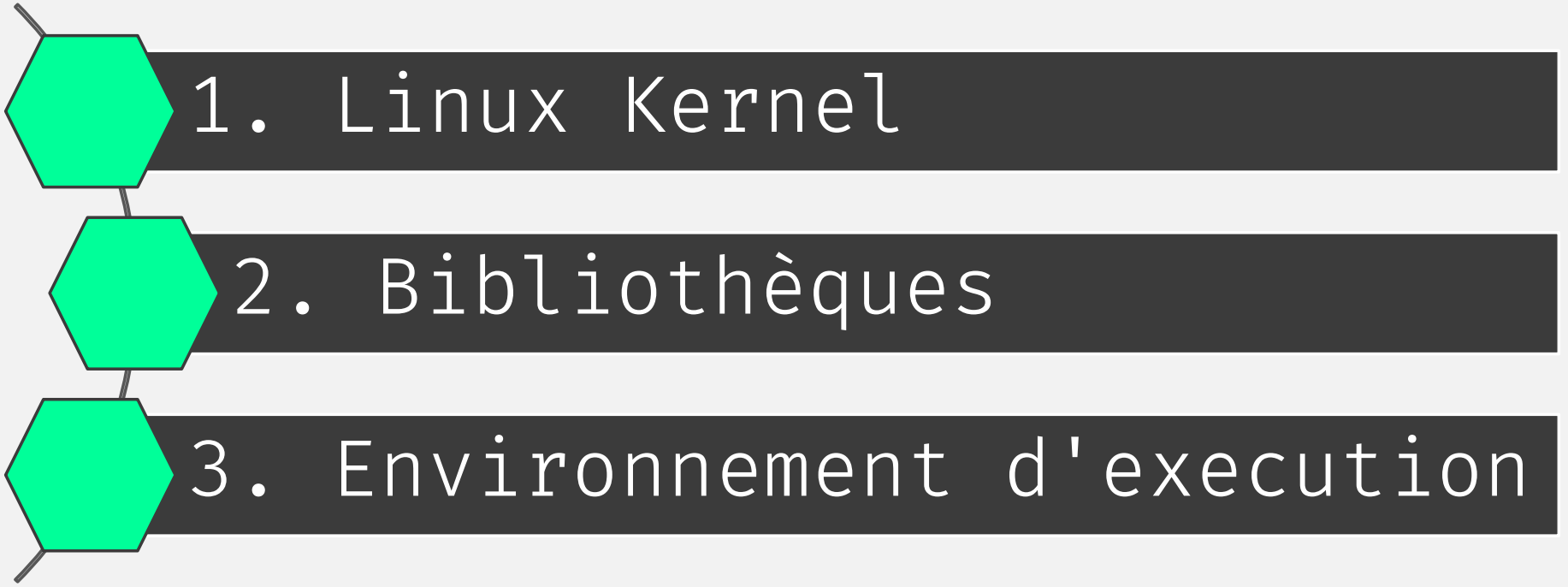
COUCHES LOGICIELLE



1. Linux Kernel

2. Bibliothèques

COUCHES LOGICIELLE



COUCHES LOGICIELLE

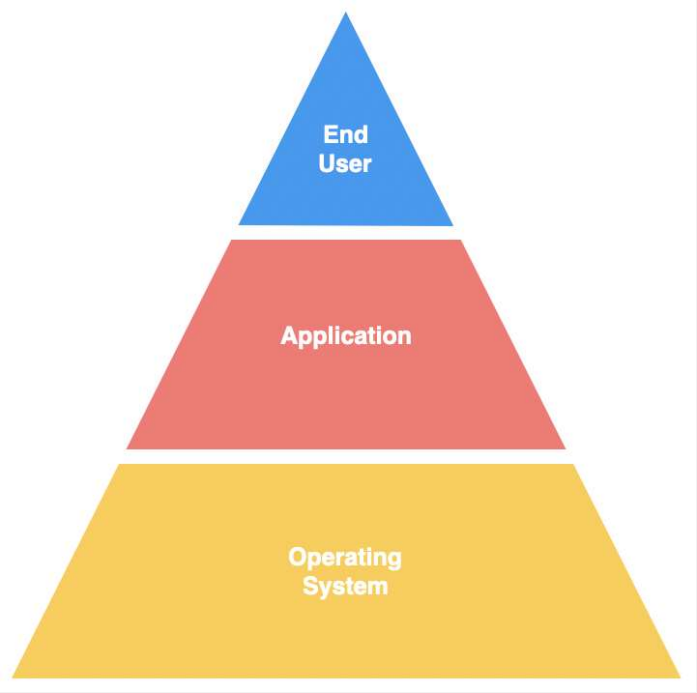
1. Linux Kernel
2. Bibliothèques
3. Environnement d'execution
4. Kit de développement

Source: https://gs.statcounter.com/os-market-share/mobile/worldwide

COUCHES LOGICIELLE

MODÈLE DE SÉCURITÉ

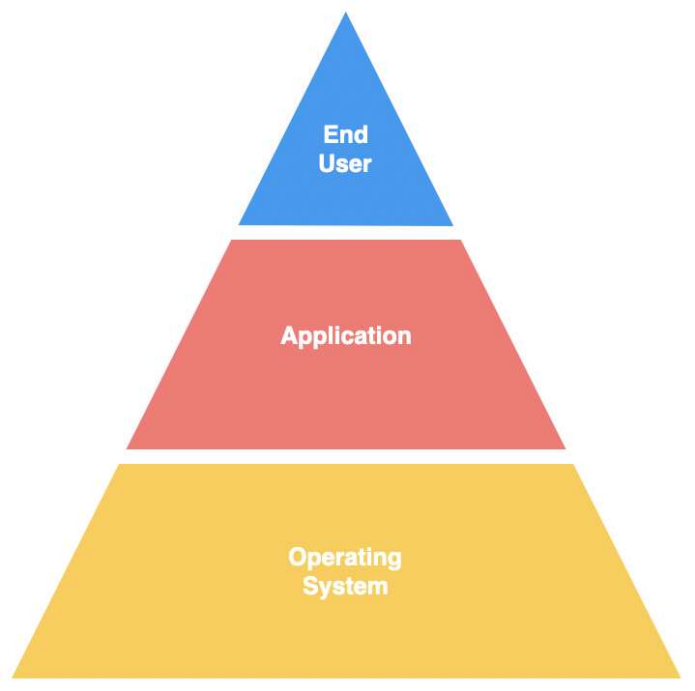
1. **End-user**: l'utilisateur.



MODÈLE DE SÉCURITÉ

1. **End-user**: l'utilisateur.

2. **Application**: le(s) software(s) utilisés

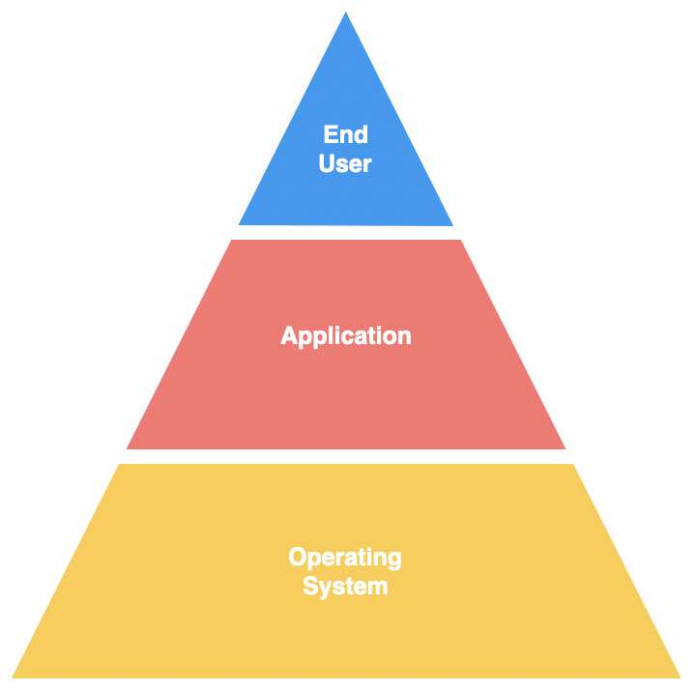


MODÈLE DE SÉCURITÉ

1. **End-user**: l'utilisateur.

2. **Application**: le(s) software(s) utilisés

3. **OS**: le kernel et fonctionnalités de bases.



SÉCURITÉ DE L'OS

Isolation de processus

SÉCURITÉ DE L'OS

Isolation de processus

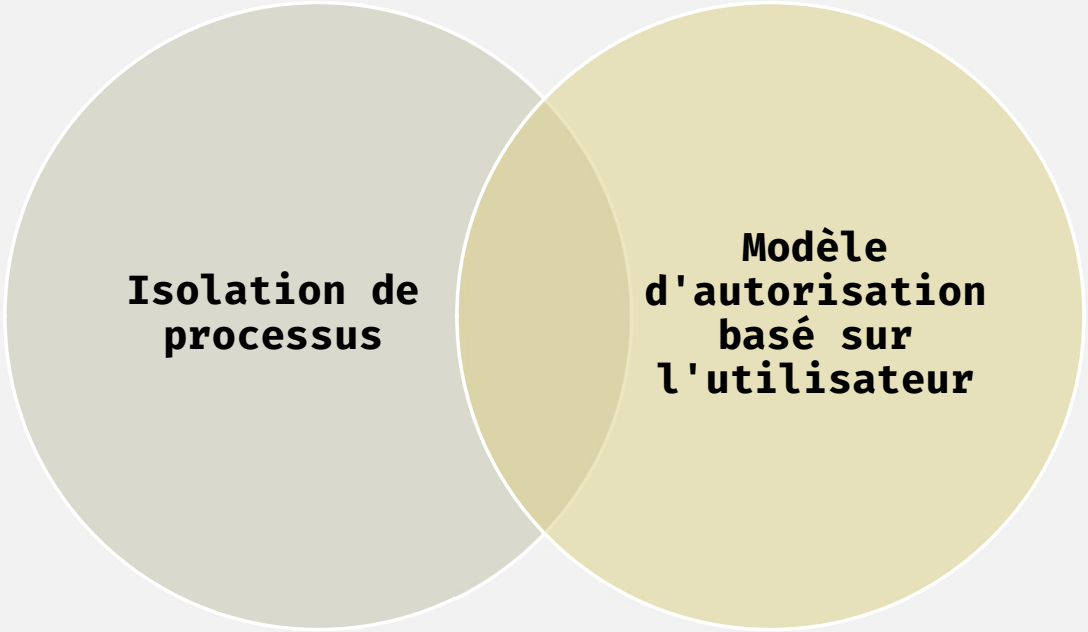
Accès limité à l'OS

SÉCURITÉ DE L'OS

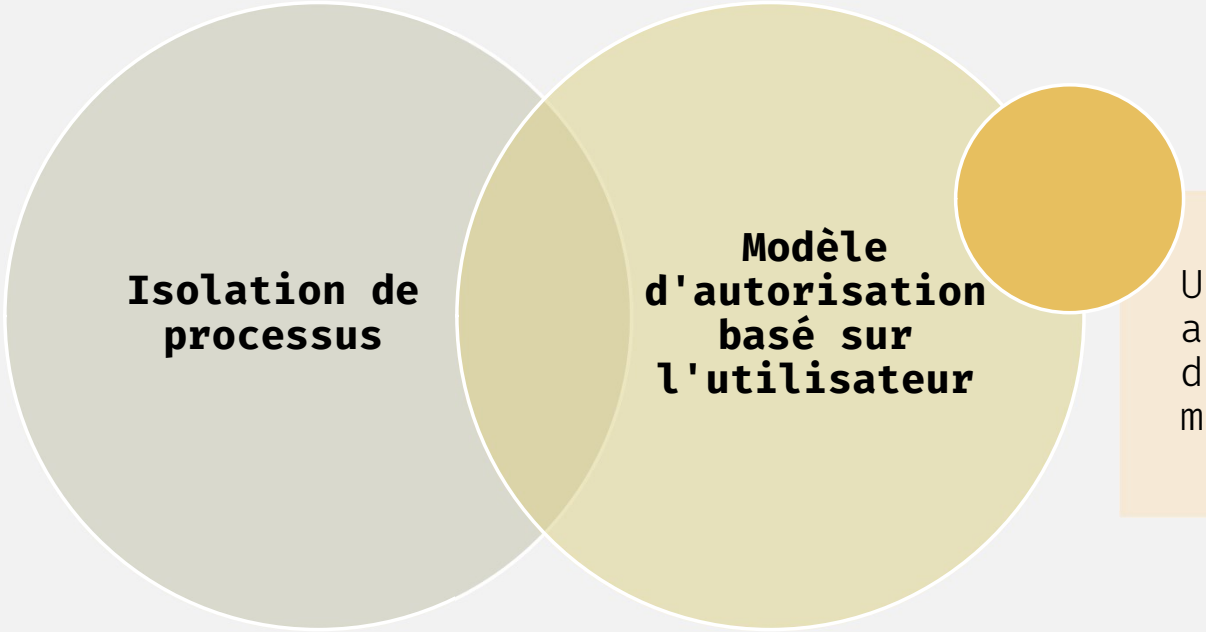
Isolation de processus

- Accès limité à l'OS
- Sandboxing

SÉCURITÉ DE L'OS

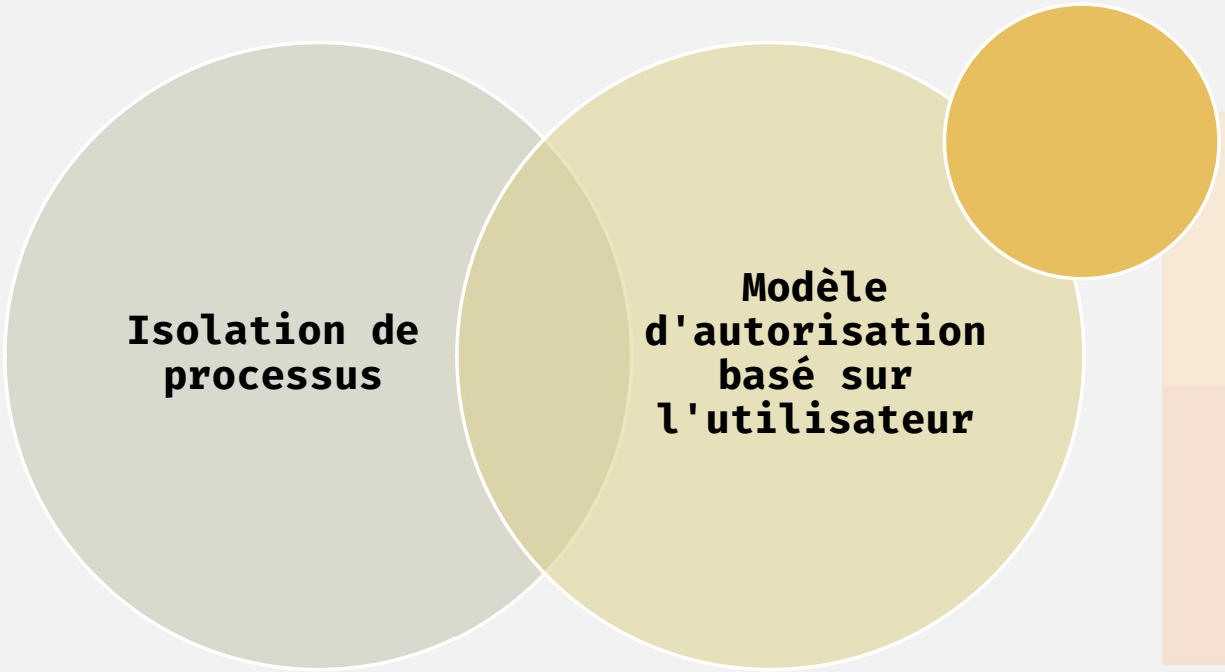


SÉCURITÉ DE L'OS



Utilisateur a le dernier mot.

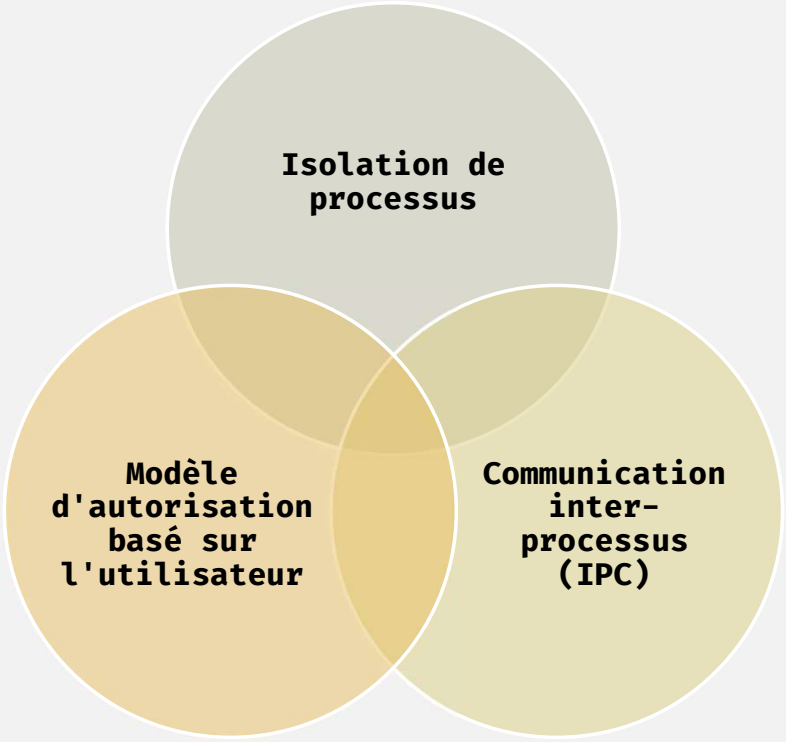
SÉCURITÉ DE L'OS



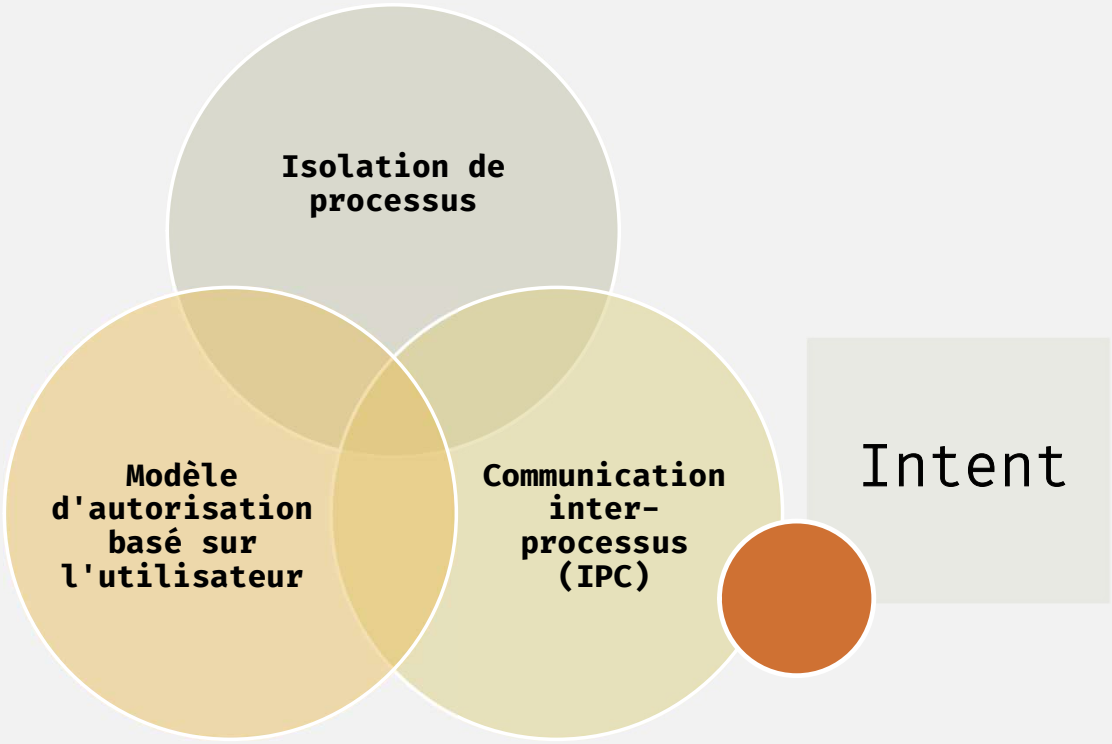
Utilisateur a le dernier mot.

Rooting

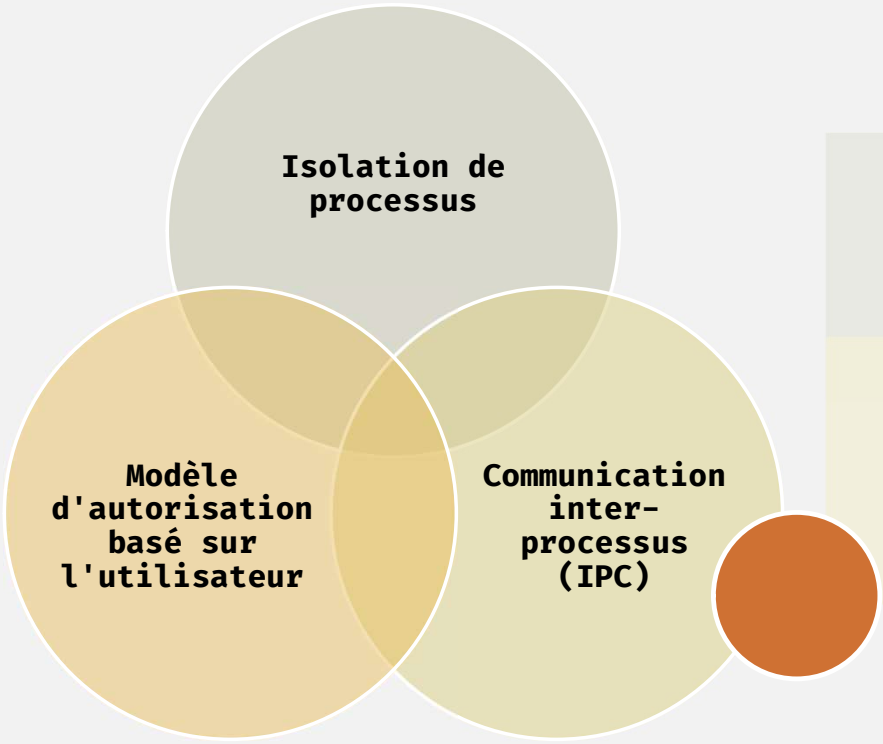
SÉCURITÉ DE L'OS



SÉCURITÉ DE L'OS



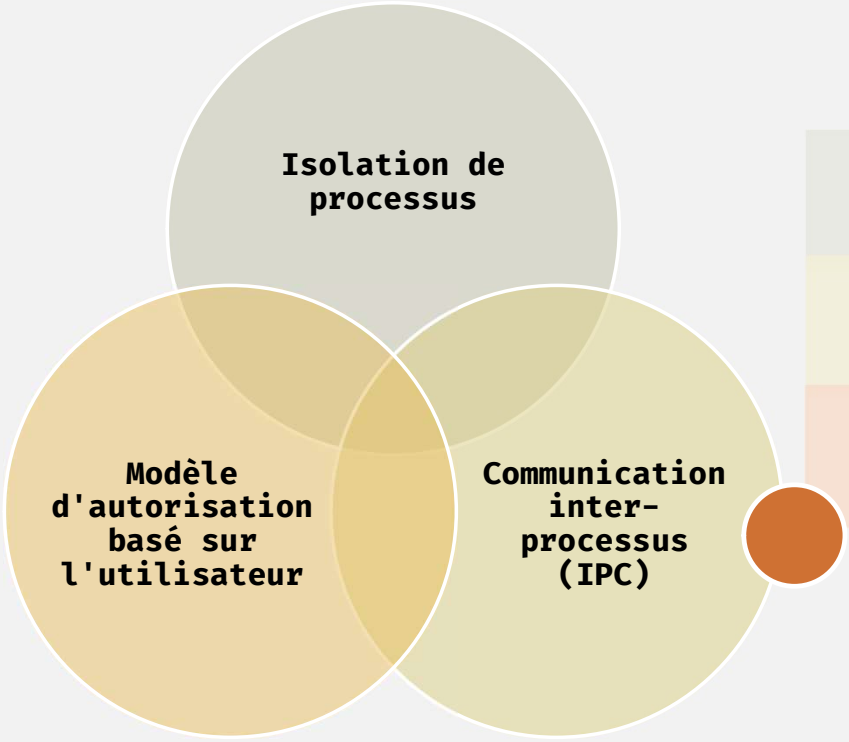
SÉCURITÉ DE L'OS



Intent

Binder

SÉCURITÉ DE L'OS



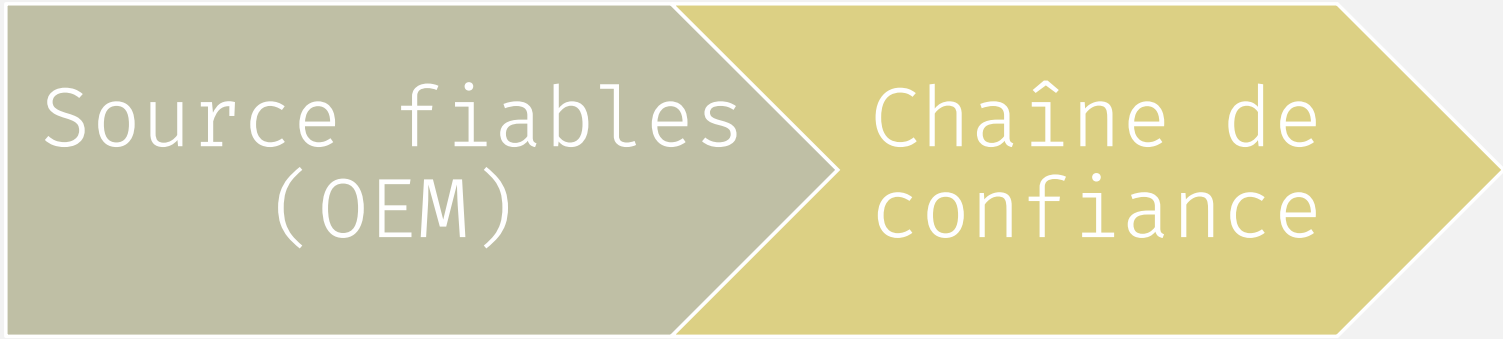
- Intent
- Binder
- Messenger

Certification des données entre activités

ANDROID VERIFIED BOOT

Source fiables (OEM)

ANDROID VERIFIED BOOT



ANDROID VERIFIED BOOT

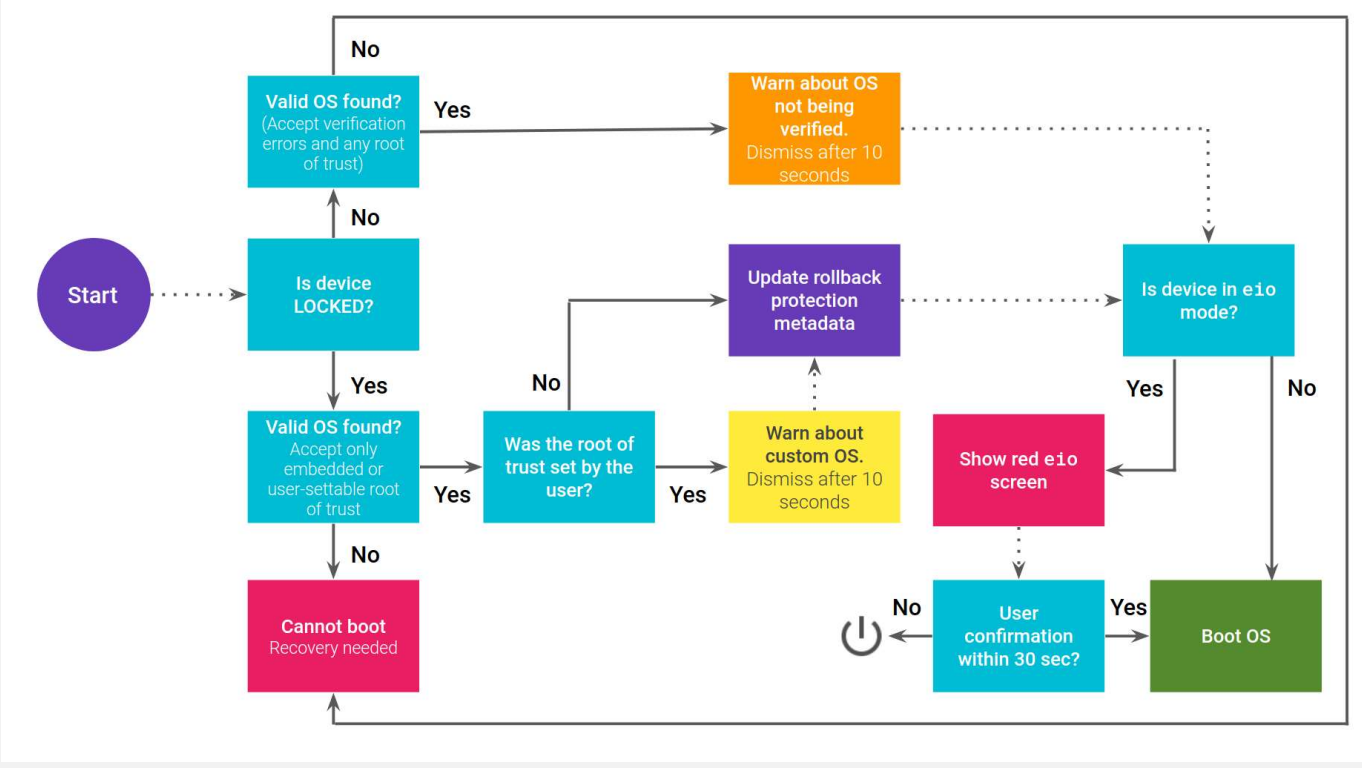
ANDROID VERIFIED BOOT

ANDROID VERIFIED BOOT

ANDROID VERIFIED BOOT

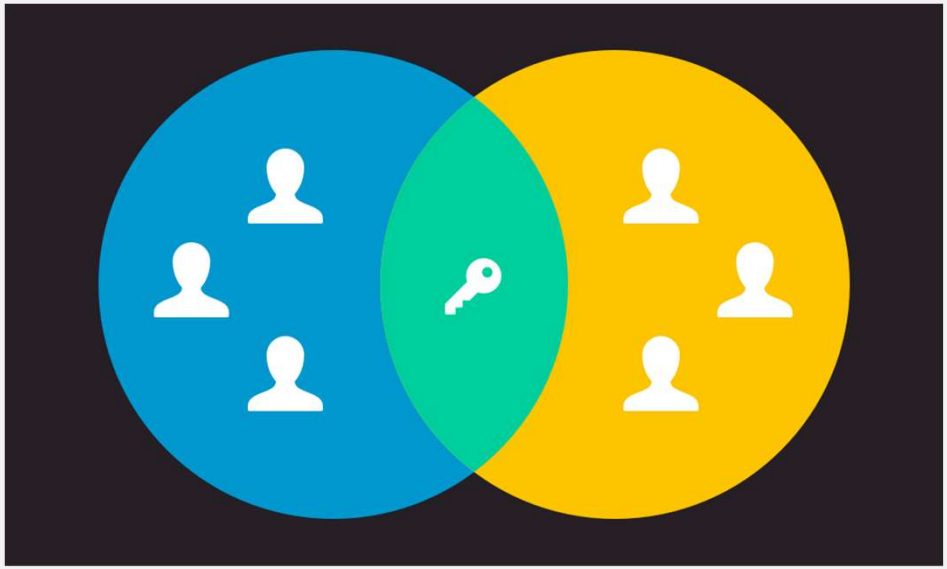
ANDROID VERIFIED BOOT

Plus en détail:



SÉCURITÉ DES APPLICATIONS

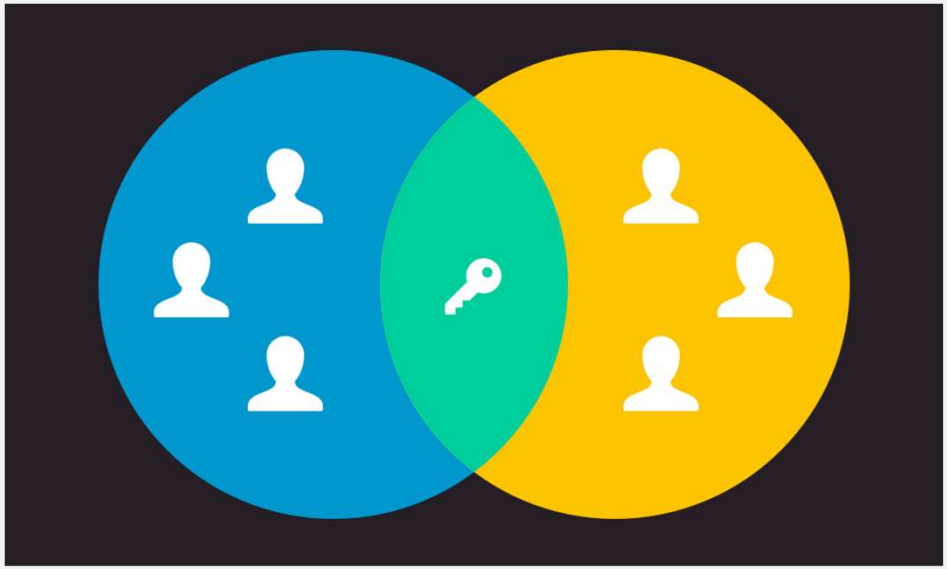
- Système de permission



SÉCURITÉ DES APPLICATIONS

- **Système de permission**

  Autorisations au moment de l'installation.

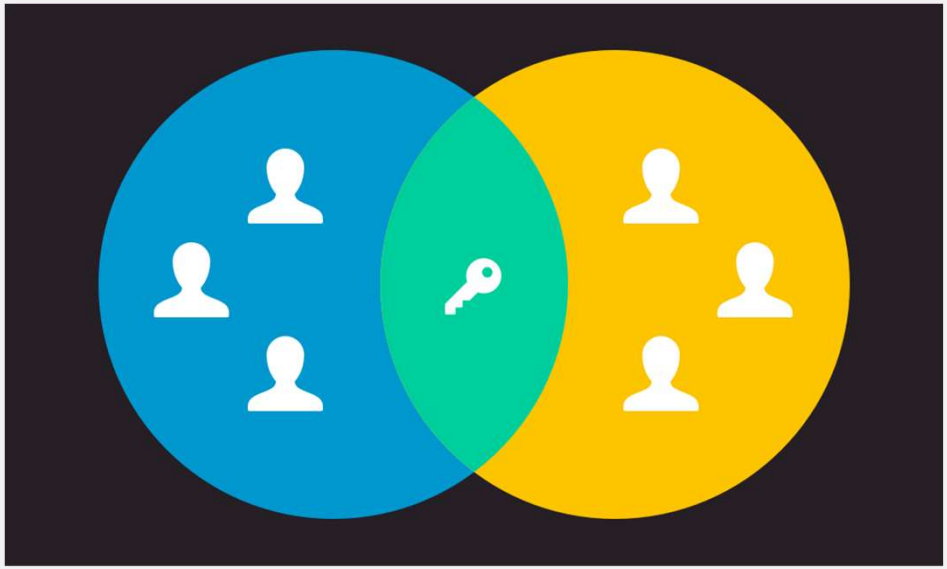


SÉCURITÉ DES APPLICATIONS

- **Système de permission**

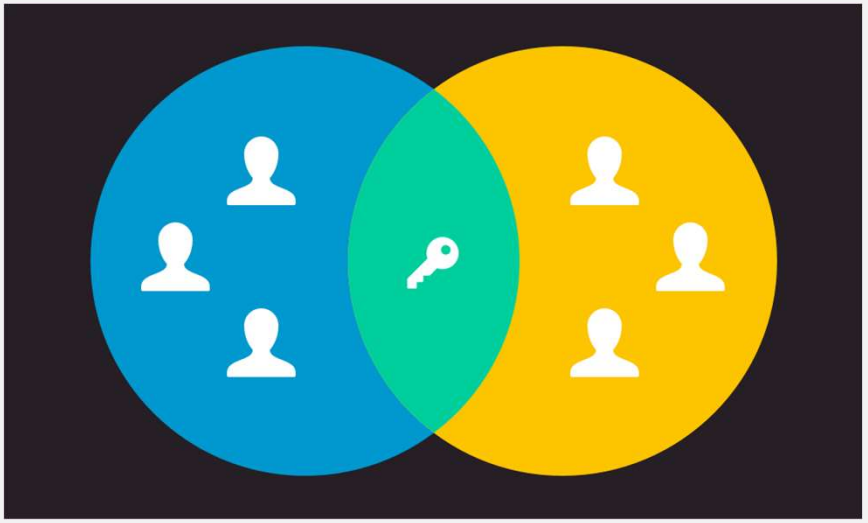
  Autorisations au moment de l'installation.

  Autorisations d'exécution.



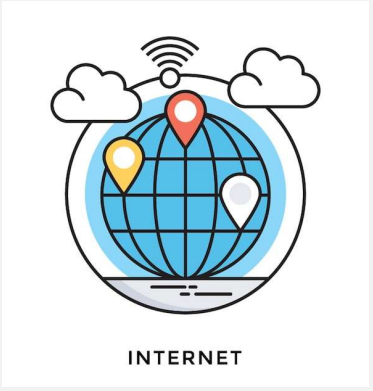
Système de permission

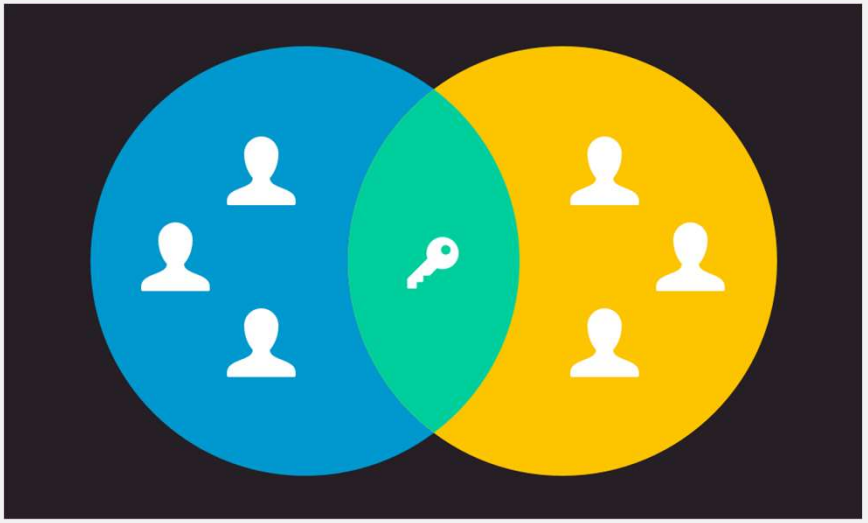
- Accès:
  - Appareil photo



Système de permission

- Accès:
  - Appareil photo
  - Internet

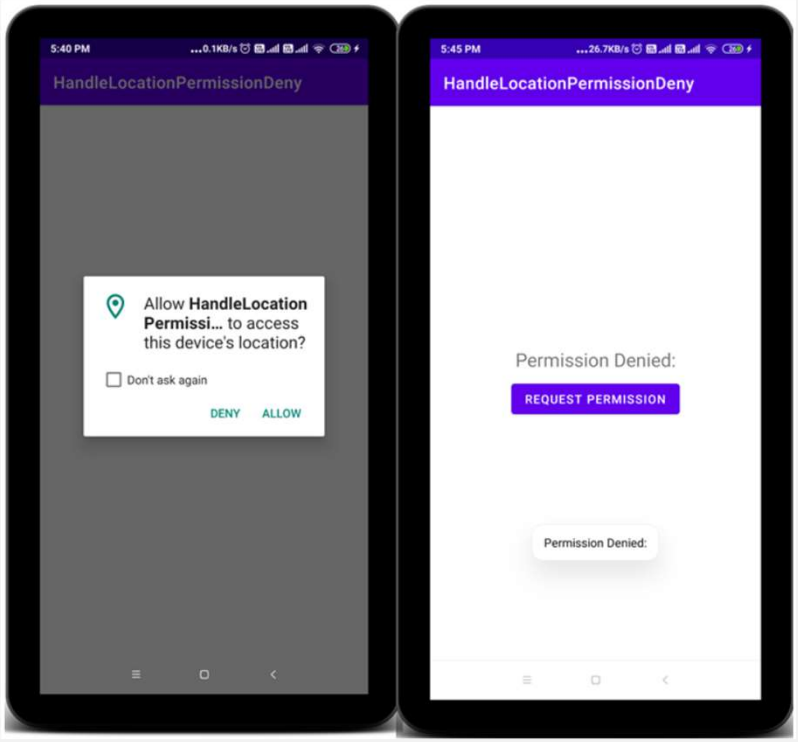




Système de permission

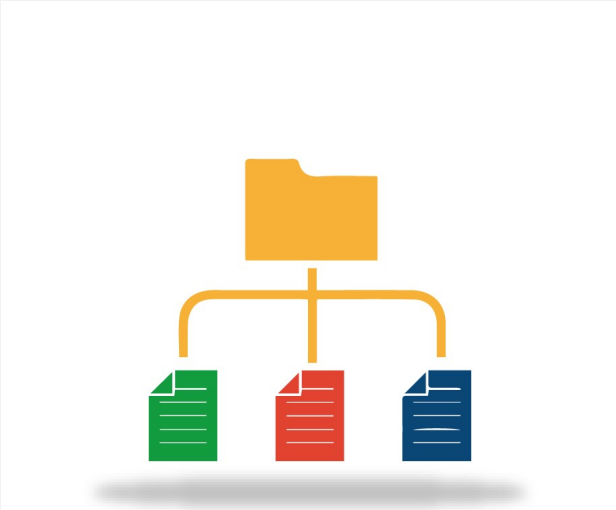
Exemple:

Demande et rejet de la requête de l'accès à la localisation.



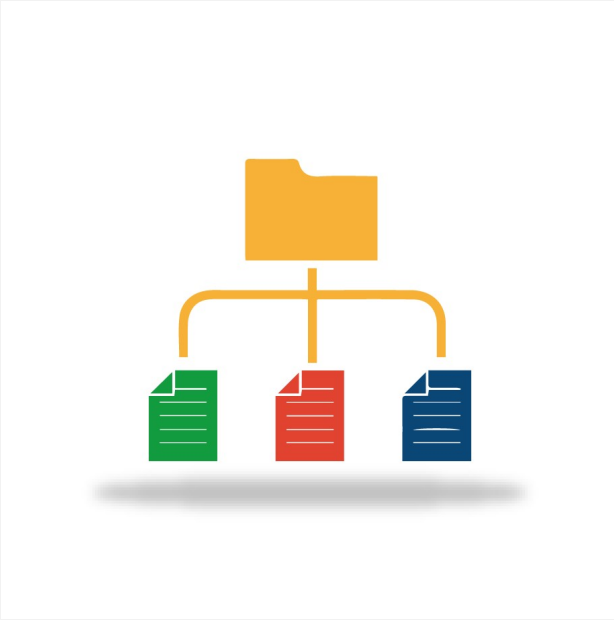
STOCKAGE

- Système de permission
- Stockage des données



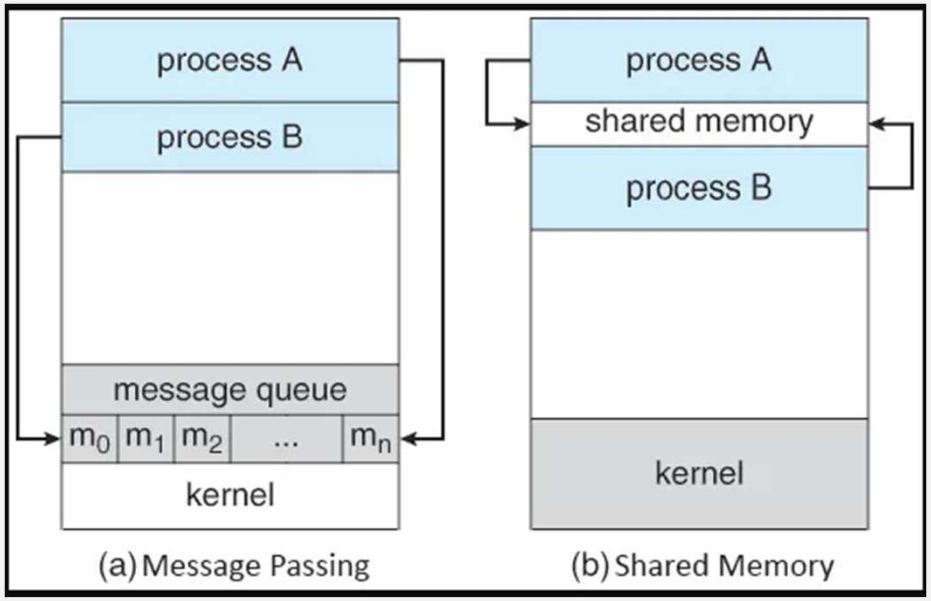
STOCKAGE

- **Système de permission**
- **Stockage des données**
  - Stockage interne.
  - Stockage externe.
  - Fournisseurs de contenu.



IPC

- Système de permission
- Stockage des données
- Interprocess communication

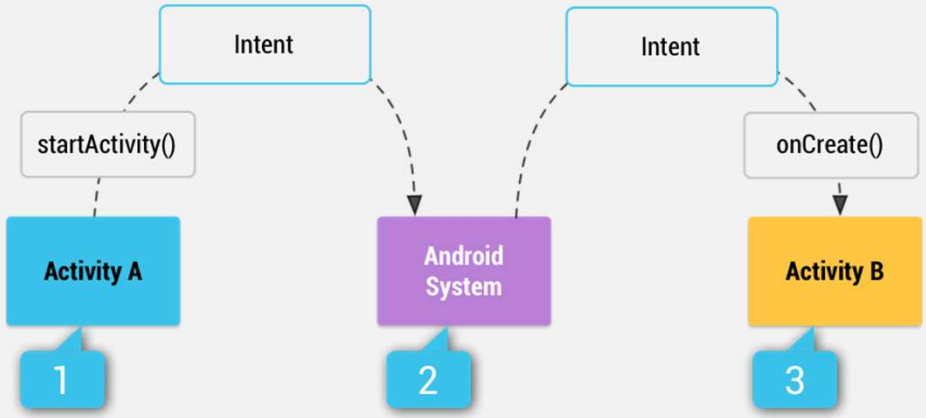


IPC

- Système de permission
- Stockage des données
- Interprocess communication

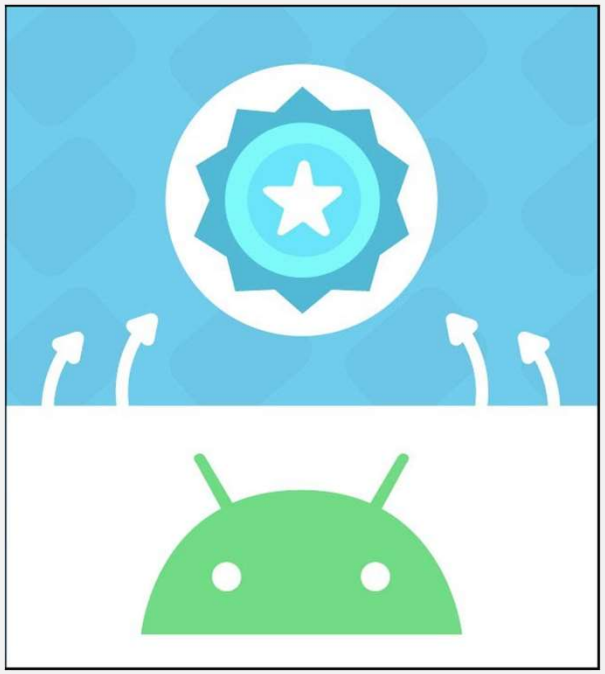
  Intent explicites -> envoyer des données entre les activités

  Intent implicites -> action générale à effectuée



SIGNATURE DE L'APPLICATION

- Système de permission
- Stockage des données
- Interprocess communication
- Signature de l'application

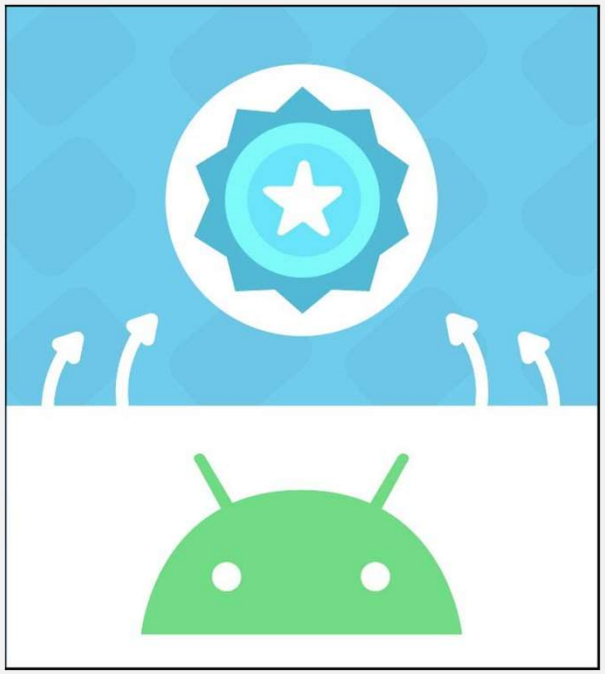


SIGNATURE DE L'APPLICATION

- Système de permission
- Stockage des données
- Interprocess communication
- Signature de l'application

  Si non signée, non-téléchargeable sur Google Play.

  UID est attribué en fonction du certificat utilisé pour signer l'application



EXEMPLE DE MALWARE

HummingBad (2016)

Affichage des publicités et simulation de clics dessus.

Installation d’applications frauduleuses sur l’appareil.

EXEMPLE DE MALWARE

HummingBad (2016)

- **USER PRESENT** – se déclenche lorsque l'appareil est déverrouillé

- **BOOT COMPLETED** - se déclenche une fois que l'utilisateur a terminé le démarrage

- **SCREEN ON** – se déclenche lorsque l'appareil se réveille et devient interactif

- **USER PRESENT** — se déclenche lorsque l'appareil est déverrouillé
- **BOOT COMPLETED** - se déclenche une fois que l'utilisateur a terminé le démarrage
- **SCREEN ON** — se déclenche lorsque l'appareil se réveille et devient interactif

Lorsqu n'importe lequel des événements mentionnés précédemment est reçu par le récepteur de diffusion, le service **Se** démarre.

Receiver.java

```java
public void onReceive(Context context, Intent intent) {
        Editor editor = UtilsClass.getInstance().
            getSharedPreferences(context).edit();
        if (Utilstools.ACTIONIAD.equals(intent.getAction())
                || Utilstools.ACTIONZDT.equals(intent.getAction())
                    ||
                "android.intent.action.USER_PRESENT".equals(intent
                    .getAction()) ||
                "android.intent.action.BOOT_COMPLETED".equals(
                    intent.getAction()) ||
                "android.intent.action.SCREEN_ON".equals(intent.
                    getAction())) {
            if ("android.intent.action.BOOT_COMPLETED".equals(
                intent.getAction())) {
                MobclickAgent.onEvent(context, "SSP_ReCreate");
            }
            if (!Utilstools.getInstance().isServiceRunning(context
                )) {
                context.startService(new Intent(context, Se.class)
                    );
            }
        }
  //...
}
```

Lorsqu'une publicité est affichée, le processus capture l'événement *KeyDownEvent* et ne l'envoie pas plus loin si le *keycode* est l'un des suivants :

- KEYCODE HOME (3)
- KEYCODE BACK (4)
- KEYCODE MENU (82)

KeyCapture.java

```java
public boolean onKeyDown(int keyCode, KeyEvent event) {
    if (keyCode == 4 || keyCode == 82 || keyCode == 3) {
        return false;
    }
    return super.onKeyDown(keyCode, event);
}
```

Sans pouvoir utiliser les commandes de navigation, l'utilisateur est **obligé** de traiter l'annonce.

Cependant, si l'utilisateur essaie de fermer la publicité, l'événement de clic est intercepté et un événement de clic au milieu de l'écran est envoyé à la place.

```
1  public void setSimulateClick(final Activity activity) {
2      activity.runOnUiThread(new Runnable() {
3          public void run() {
4              DisplayMetrics dm = activity.getResources().
                   getDisplayMetrics();
5              int x = dm.widthPixels / 2;
6              int y = dm.heightPixels / 2;
7              long downTime = SystemClock.uptimeMillis();
8              MotionEvent downEvent = MotionEvent.obtain(downTime,
                   downTime,
9                      0, (float) x, (float) y, 0);
10             MotionEvent upEvent = MotionEvent.obtain(downTime,
                   downTime,
11                     1, (float) x, (float) y, 0);
12             activity.getWindow().getDecorView().dispatchTouchEvent
                   (downEvent);
13             activity.getWindow().getDecorView().dispatchTouchEvent
                   (upEvent);
14             downEvent.recycle();
15             upEvent.recycle();
16         }
17     });
18 }
```

CONCLUSION

- **Avantage**
  - Ouverture, qualité, SELinux, moderne.

- **Défauts**
  - OEM, ~permissivité (ROMs custom, rooting), grande distribution

QUESTIONS

Merci pour votre attention

Source : Fallout picture https://bethesda.net/fr/store/product/FA4SP1PCDG01

BIBLIOGRAPHIE

https://www.playhooky.fr/technologie/stockage-donnees/

https://www.frandroid.com/culture-tech/securite-applications/367259_hummingbad-surement-lun-malwares-android-plus-vicieux-plus-intelligents-moment

https://wonderfall.space/modele-securite-mobile/

https://arxiv.org/pdf/1904.05572.pdf

https://networkencyclopedia.com/interprocess-communication-ipc/

https://developer.android.com/guide/components/intents-filters

https://i.ytimg.com/vi/c4e-jOFTPhA/maxresdefault.jpg