

L'analyse statique :

Analyse du logiciel réalisée sans exécuter le programme.

But : trouver les défauts présents dans le logiciel.

S'assurer que le code est écrit selon des règles de programmations définis,

L'analyse statique

- L'analyse statique

L'analyse statique :

Analyse du logiciel réalisée sans exécuter le programme.

But : trouver les défauts présents dans le logiciel.

S'assurer que le code est écrit selon des règles de programmations définis,

L'analyse statique

• L'analyse statique

Qu'est ce que l'analyse statique ?

L'analyse statique :

Analyse du logiciel réalisée sans exécuter le programme.

But : trouver les défauts présents dans le logiciel.

S'assurer que le code est écrit selon des règles de programmations définis,

L'analyse statique

• L'analyse statique

Qu'est ce que l'analyse statique ?

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

L'analyse statique :

Analyse du logiciel réalisée sans exécuter le programme.

But : trouver les défauts présents dans le logiciel.

S'assurer que le code est écrit selon des règles de programmations définis,

Méthodes :

- Analyse du code source : peut être illégale
- Analyse par signature : pas de décompilation, ce qui rend l'opération un peu plus légale (mais pas forcément approuvée par les créateurs des applications que l'on analyse)

L'analyse statique

• L'analyse statique

Qu'est ce que l'analyse statique ?

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

Méthode d'analyse

L'analyse statique :

Analyse du logiciel réalisée sans exécuter le programme.

But : trouver les défauts présents dans le logiciel.

S'assurer que le code est écrit selon des règles de programmations définis,

Méthodes :

- Analyse du code source : peut être illégale
- Analyse par signature : pas de décompilation, ce qui rend l'opération un peu plus légale (mais pas forcément approuvée par les créateurs des applications que l'on analyse)

L'analyse statique

• L'analyse statique

Qu'est ce que l'analyse statique ?

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

Méthode d'analyse

- ▶ Analyse du code source

L'analyse statique :

Analyse du logiciel réalisée sans exécuter le programme.

But : trouver les défauts présents dans le logiciel.

S'assurer que le code est écrit selon des règles de programmations définis,

Méthodes :

- Analyse du code source : peut être illégale
- Analyse par signature : pas de décompilation, ce qui rend l'opération un peu plus légale (mais pas forcément approuvée par les créateurs des applications que l'on analyse)

L'analyse statique

• L'analyse statique

Qu'est ce que l'analyse statique ?

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

Méthode d'analyse

- ▶ Analyse du code source
- ▶ Analyse par signature

L'analyse statique :

Analyse du logiciel réalisée sans exécuter le programme.

But : trouver les défauts présents dans le logiciel.

S'assurer que le code est écrit selon des règles de programmations définis,

Objectifs :

- Permissions : déterminer si l'application nécessite des permissions qui semblent incohérentes
- Lister les trackers qui y sont inclus
- Déterminer si des portions de code peuvent être intéressantes pour l'analyse dynamique

Méthodes :

- Analyse du code source : peut être illégale
- Analyse par signature : pas de décompilation, ce qui rend l'opération un peu plus légale (mais pas forcément approuvée par les créateurs des applications que l'on analyse)

L'analyse statique

• L'analyse statique

Qu'est ce que l'analyse statique ?

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

Méthode d'analyse

- ▶ Analyse du code source
- ▶ Analyse par signature

Objectifs :

L'analyse statique :

Analyse du logiciel réalisée sans exécuter le programme.

But : trouver les défauts présents dans le logiciel.

S'assurer que le code est écrit selon des règles de programmations définis,

Objectifs :

- Permissions : déterminer si l'application nécessite des permissions qui semblent incohérentes
- Lister les trackers qui y sont inclus
- Déterminer si des portions de code peuvent être intéressantes pour l'analyse dynamique

Méthodes :

- Analyse du code source : peut être illégale
- Analyse par signature : pas de décompilation, ce qui rend l'opération un peu plus légale (mais pas forcément approuvée par les créateurs des applications que l'on analyse)

L'analyse statique

• L'analyse statique

Qu'est ce que l'analyse statique ?

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

Méthode d'analyse

- ▶ Analyse du code source
- ▶ Analyse par signature

Objectifs :

- ▶ Permissions de l'application

L'analyse statique :

Analyse du logiciel réalisée sans exécuter le programme.

But : trouver les défauts présents dans le logiciel.

S'assurer que le code est écrit selon des règles de programmations définis,

Objectifs :

- Permissions : déterminer si l'application nécessite des permissions qui semblent incohérentes
- Lister les trackers qui y sont inclus
- Déterminer si des portions de code peuvent être intéressantes pour l'analyse dynamique

Méthodes :

- Analyse du code source : peut être illégale
- Analyse par signature : pas de décompilation, ce qui rend l'opération un peu plus légale (mais pas forcément approuvée par les créateurs des applications que l'on analyse)

L'analyse statique

• L'analyse statique

Qu'est ce que l'analyse statique ?

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

Méthode d'analyse

- ▶ Analyse du code source
- ▶ Analyse par signature

Objectifs :

- ▶ Permissions de l'application
- ▶ Trackers inclus

L'analyse statique :

Analyse du logiciel réalisée sans exécuter le programme.

But : trouver les défauts présents dans le logiciel.

S'assurer que le code est écrit selon des règles de programmations définis,

Objectifs :

- Permissions : déterminer si l'application nécessite des permissions qui semblent incohérentes
- Lister les trackers qui y sont inclus
- Déterminer si des portions de code peuvent être intéressantes pour l'analyse dynamique

Méthodes :

- Analyse du code source : peut être illégale
- Analyse par signature : pas de décompilation, ce qui rend l'opération un peu plus légale (mais pas forcément approuvée par les créateurs des applications que l'on analyse)

L'analyse statique

• L'analyse statique

Qu'est ce que l'analyse statique ?

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

Méthode d'analyse

- ▶ Analyse du code source
- ▶ Analyse par signature

Objectifs :

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

L'analyse statique :

Analyse du logiciel réalisée sans exécuter le programme.

But : trouver les défauts présents dans le logiciel.

S'assurer que le code est écrit selon des règles de programmations définis,

Méthodes :

- Analyse du code source : peut être illégale
- Analyse par signature : pas de décompilation, ce qui rend l'opération un peu plus légale (mais pas forcément approuvée par les créateurs des applications que l'on analyse)

Objectifs :

- Permissions : déterminer si l'application nécessite des permissions qui semblent incohérentes
- Lister les trackers qui y sont inclus
- Déterminer si des portions de code peuvent être intéressantes pour l'analyse dynamique

Outils :

- Jadx : décompileur dex vers Java : ne pas avoir à manipuler les fichiers smali (=assembleur pour android), qui sont peu lisibles
- Exodus-standalone : Analyse par signature pour déterminer les permissions ainsi que les trackers utilisés par une application

L'analyse statique

• L'analyse statique

Qu'est ce que l'analyse statique ?

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

Méthode d'analyse

- ▶ Analyse du code source
- ▶ Analyse par signature

Outils :

Objectifs :

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

L'analyse statique :

Analyse du logiciel réalisée sans exécuter le programme.

But : trouver les défauts présents dans le logiciel.

S'assurer que le code est écrit selon des règles de programmations définis,

Méthodes :

- Analyse du code source : peut être illégale
- Analyse par signature : pas de décompilation, ce qui rend l'opération un peu plus légale (mais pas forcément approuvée par les créateurs des applications que l'on analyse)

Objectifs :

- Permissions : déterminer si l'application nécessite des permissions qui semblent incohérentes
- Lister les trackers qui y sont inclus
- Déterminer si des portions de code peuvent être intéressantes pour l'analyse dynamique

Outils :

- Jadx : décompileur dex vers Java : ne pas avoir à manipuler les fichiers smali (=assembleur pour android), qui sont peu lisibles
- Exodus-standalone : Analyse par signature pour déterminer les permissions ainsi que les trackers utilisés par une application

L'analyse statique

• L'analyse statique

Qu'est ce que l'analyse statique ?

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

Méthode d'analyse

- ▶ Analyse du code source
- ▶ Analyse par signature

Outils :

- ▶ jadx

Objectifs :

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

L'analyse statique :

Analyse du logiciel réalisée sans exécuter le programme.

But : trouver les défauts présents dans le logiciel.

S'assurer que le code est écrit selon des règles de programmations définis,

Méthodes :

- Analyse du code source : peut être illégale
- Analyse par signature : pas de décompilation, ce qui rend l'opération un peu plus légale (mais pas forcément approuvée par les créateurs des applications que l'on analyse)

Objectifs :

- Permissions : déterminer si l'application nécessite des permissions qui semblent incohérentes
- Lister les trackers qui y sont inclus
- Déterminer si des portions de code peuvent être intéressantes pour l'analyse dynamique

Outils :

- Jadx : décompilateur dex vers Java : ne pas avoir à manipuler les fichiers smali (=assembleur pour android), qui sont peu lisibles
- Exodus-standalone : Analyse par signature pour déterminer les permissions ainsi que les trackers utilisés par une application

L'analyse statique

• L'analyse statique

Qu'est ce que l'analyse statique ?

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

Méthode d'analyse

- ▶ Analyse du code source
- ▶ Analyse par signature

Outils :

- ▶ jadx
- ▶ Android Studio

Objectifs :

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

L'analyse statique :

Analyse du logiciel réalisée sans exécuter le programme.

But : trouver les défauts présents dans le logiciel.

S'assurer que le code est écrit selon des règles de programmations définis,

Méthodes :

- Analyse du code source : peut être illégale
- Analyse par signature : pas de décompilation, ce qui rend l'opération un peu plus légale (mais pas forcément approuvée par les créateurs des applications que l'on analyse)

Objectifs :

- Permissions : déterminer si l'application nécessite des permissions qui semblent incohérentes
- Lister les trackers qui y sont inclus
- Déterminer si des portions de code peuvent être intéressantes pour l'analyse dynamique

Outils :

- Jadx : décompileur dex vers Java : ne pas avoir à manipuler les fichiers smali (=assembleur pour android), qui sont peu lisibles
- Exodus-standalone : Analyse par signature pour déterminer les permissions ainsi que les trackers utilisés par une application

L'analyse statique

• L'analyse statique

Qu'est ce que l'analyse statique ?

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

Méthode d'analyse

- ▶ Analyse du code source
- ▶ Analyse par signature

Outils :

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

Objectifs :

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

sendPhoto : Méthode qui envoie des photos **à un serveur distant**
sendSMS : Méthode qui envoie un SMS

L'analyse statique : Exemple

- L'analyse statique

sendPhoto : Méthode qui envoie des photos à un serveur distant
sendSMS : Méthode qui envoie un SMS

L'analyse statique : Exemple

• L'analyse statique

```
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

sendPhoto : Méthode qui envoie des photos à un serveur distant
sendSMS : Méthode qui envoie un SMS

L'analyse statique : Exemple

• L'analyse statique

```
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