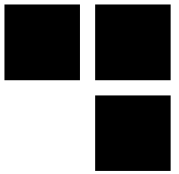
SYNACKTIV
DIGITAL SECURITY



Frida

Comment ça marche, comment l'utiliser

Présenté 14/06/2016

Pour OSSIR

Par Eloi Vanderbeken

Whoami

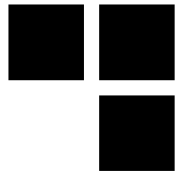
- **Eloi Vanderbeken – @elvanderb**
- **Synacktiv – www.synacktiv.ninja**

- Utilisateur et contributeur de Frida

Plan

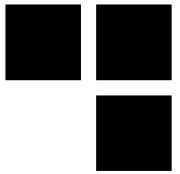
- **Intro**
- **Pourquoi l'instrumentation dynamique de code ?**
- **Pourquoi Frida ?**
- **Description des outils et de l'API**
- **DEMO !**
- **Questions**

Frida



- **En quelques mots :**
  - Du python…
  - ...ou du JavaScript…
  - ...ou du QML, du Swift, du .NET...
  - ...qui injecte du C/C++…
  - …scripté en JavaScript...
  - ...pour reverser de l'assembleur (x86, x86_64, ARM, ARM64)…
  - ...ou de l'Objective-C…
  - ...ou du Dalvik…
  - ...sur Windows, Mac, Linux, iOS, Android et... QNX.

A quoi ça sert ?



- **Instrumentation**
  - Modification du flot d'exécution du programme
  - Pour lire / écrire des données
  - Pour modifier le comportement du programme
- **Dynamique**
  - Les modifications sont faites dynamiquement, en mémoire
  - Plus discret

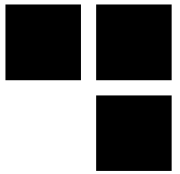
    Pas de modification des fichiers
  - Plus facile

    modifier et reconstruire un exécutable pour y ajouter du code est compliqué, voire impossible
  - Plus pratique

    possibilité de modifier l'instrumentation à la demande

    Possibilité d'instrumenter facilement du code généré dynamiquement (programmes packés)
- **Code binaire**
  - Inutile d'avoir les sources

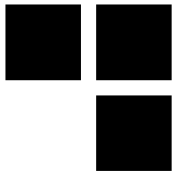
Pourquoi ?



- **Intercepter des données**
  - Interception des données avant chiffrement / après déchiffrement
  - Lecture de valeurs calculées pendant l'exécution / dépendantes de l'environnement
- **Injecter des données**
  - Fuzzing d'un client lourd, du serveur associé...
- **Modifier le comportement du programme**
  - Contourner une vérification coté client
  - Utiliser des fonctions du programme

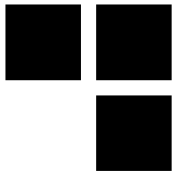
    Utilisation d'une méthode de chiffrement / compression propriétaire, fuzzing en mémoire, émulation d'un serveur, etc.
- **Créer des traces d'exécution**
  - Vue d'ensemble de l'exécution du programme
  - Localisation de code utile
- **...**

Pourquoi Frida ?



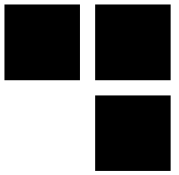
- **Multi-plateforme**
  - Windows, Mac, Linux, iOS, Android et QNX
- **VRAIMENT multi-plateforme**
  - Réutilisation de code directe ou avec très peu de modifications
- **Installation SIMPLE**
  - Pas plus de 3 commandes par plateformes
- **Prototypage rapide**
  - JavaScript
    - Pas de compilation
    - Toutes les bibliothèques JavaScript sont utilisables directement
  - Résilient
    - Pas de crash en cas d'erreur
    - Nettoyage du processus à la fin du script
    - On peut injecter 1000 versions d'un script à la suite dans 1 process
- **Licence permissive**
  - wxWindows Library Licence
  - LGPLv2 + exception du linkage statique

Pourquoi Frida ? – cont'd



- **Piles incluses**
  - Les briques de bases pour l'étude dynamique de code binaire sont incluses
  - Des modules pour l'Objective-C et le Dalvik sont intégrés
- **Modulaire**
  - Il est possible d'utiliser ou de remplacer des briques de Frida de manière indépendante
  - Frida peut utiliser 3 moteurs JavaScript différents
  - Le support QNX a été ajouté par un tiers
  - BLACKBUCK de Immunity est basé sur frida-gum
- **Bien codé**
  - Mais pas très commenté...
- **API documentée**
  - L'architecture interne l'est un peu moins...
- **Communauté réactive**
  - #frida sur irc.freenode.net
- **Projet actif**
  - Plusieurs contributeurs, commits fréquents

Un projet tenu d'une main de fer



oleavr added a note on Nov 10, 2015

- Missing spaces around `*`
- Missing space after sizeof
- Continuation (hanging indents) should be 4 spaces instead of 2

oleavr added a note on Nov 10, 2015

Declarations should be at the beginning of the scope (no declarations after the first statement), ordered chronologically.

```
279 +  if (priv->access_mask & GUM_PAGE_READ)
```

oleavr added a note on Nov 12, 2015

For consistency this should be:

```
if ((priv->access_mask & GUM_PAGE_READ) != 0)
```

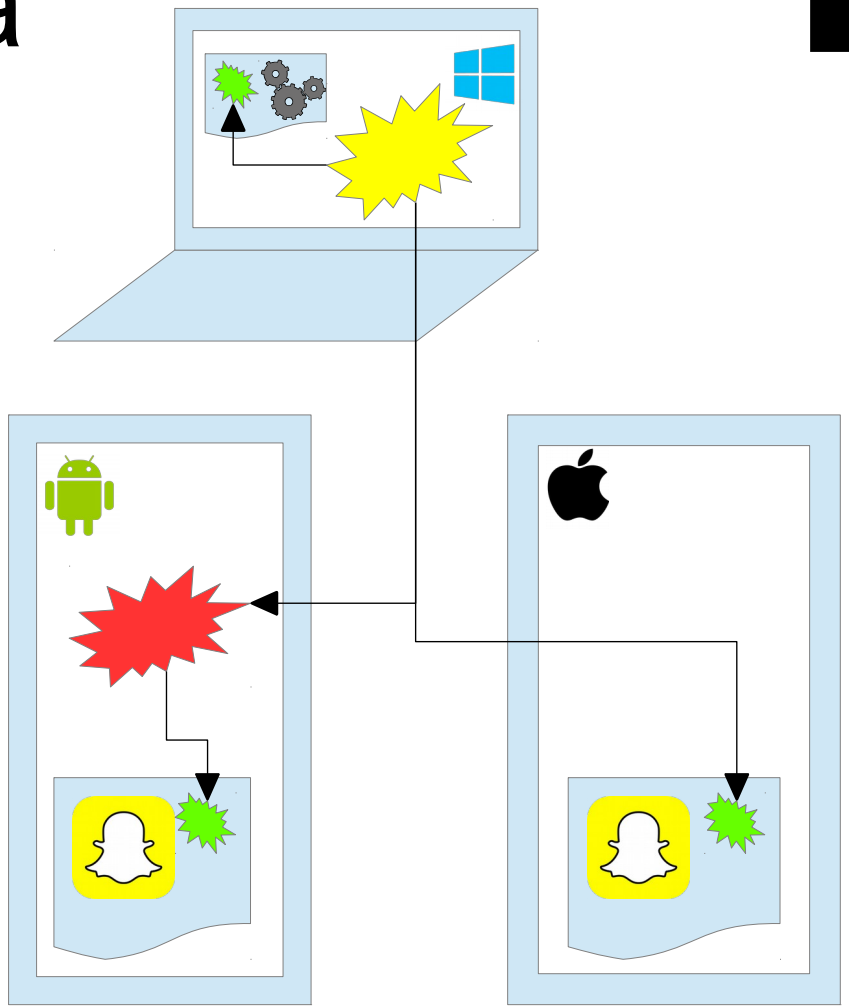
The rest of the code tries to be very explicit, so unless it's a gboolean we check explicitly against a value.

oleavr added a note on Dec 8, 2015

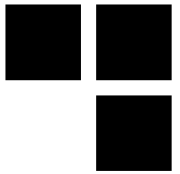
Includes should be sorted alphabetically within each group of includes.

Architecture de Frida

- **Client**
  - Sur la machine du reverser
  - Pilote les servers
  - Python / node-js / Swift / QML...
- **Serveurs**
  - Sur la machine cible
  - Chargés de l'interaction avec l'OS cible
    liste des processus / injection / création
  - Communiquent via TCP ou des pipes
    support natif de usbmuxd et adb pour les communications
- **Agents**
  - Injectés dans le processus cible
    LD_PRELOAD / insert_dylib / ptrace / CreateRemoteThread
  - Communiquent avec le client directement ou via le serveur
  - Cœur codé en C avec la glib (frida-gum)
  - Scriptés en JavaScript (V8, Duktape)
  - Exposent un serveur RPC



Outils CLI

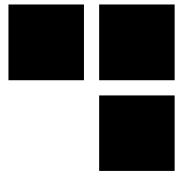


- **frida-ls-devices**
  - Liste les devices accessibles
- **frida-ps**
  - Liste les processus sur les devices
- **frida-trace**
  - Hooks des APIs / méthodes suivant des templates
  - Génère des traces d'exécution
  - Avec des couleurs !
- **frida**
  - Console JavaScript avec auto-complétion
  - Et des couleurs !

API – Interceptor

- **Permet de poser des hooks**
- **Interceptor.attach - callbacks**
  - Callbacks appelées avant et après l'exécution de la fonction
  - Accès aux arguments, au contexte et à la valeur de retour
- **Interceptor.attach – watch-point**
  - Callback appelée lors de l'exécution de l'instruction
  - Accès au contexte
- **Interceptor.replace**
  - Remplace une fonction par une autre fonction
  - Potentiellement en JavaScript
  - Possibilité d'appeler la fonction originale

API – NativeXXX



- **Permet d'interagir avec le système**
- **NativePointer / Int64 / UInt64**
  - Équivalent de void * / int64_t / uint64_t
  - Supporte les opérations arithmétiques de base
  - ⚠ **Entiers JavaScript : float ou Int32** ⚠
- **NativeFunction**
  - Permet d'appeler des fonctions natives depuis du JS
  - Utilisation de fonctions de chiffrement custom / in-memory fuzzing / etc.
- **NativeCallback**
  - Permet d'appeler des fonctions JS depuis du code natif
  - Utilisation de fonctions nécessitant des callback / modifications de v-tables / utilisation avec Interceptor.replace etc.

API – Interaction avec le système

- **Process**
  - Contient toutes les informations sur le process

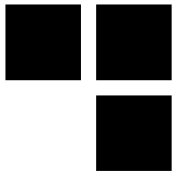
    arch, platform, pageSize, pointerSize, isDebuggerAttached, threads, modules, page / malloc ranges etc.
- **Thread**
  - Manipulation du thread courant

    backtrace, sleep
- **Module**
  - Informations sur le module

    nom, adresse de base, exports, imports, pages mémoire etc.
- **Memory**
  - Permet la manipulation de la mémoire

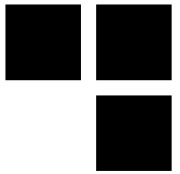
    Allocation, scan, protection, manipulation etc.
- **MemoryAccessMonitor (Windows only)**
  - Surveille les accès mémoire

API – Utils



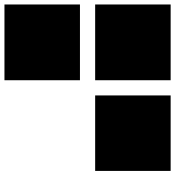
- **DebugSymbol**
  - Parse les informations de debug à l'aide des API natives (dbghelp / libunwind / CoreSymbolication.framework)
- **Instruction.parse**
  - Binding pour capstone
- **Stalker (x86 / x86_64)**
  - Fonctionne comme Pin / DynamoRIO
  - Capture l'exécution des {JMP, CALL, instructions}
- **ObjC**
  - Accès à **TOUTE** l'API Objective-C
  - Création de classes en JS, support de l'héritage, hook de méthodes, création d'instances, recherche d'objets en mémoire etc.
  - Sur MacOS et iOS
- **Java**
  - Même chose que ObjC mais pour Java et Android

API – Helpers

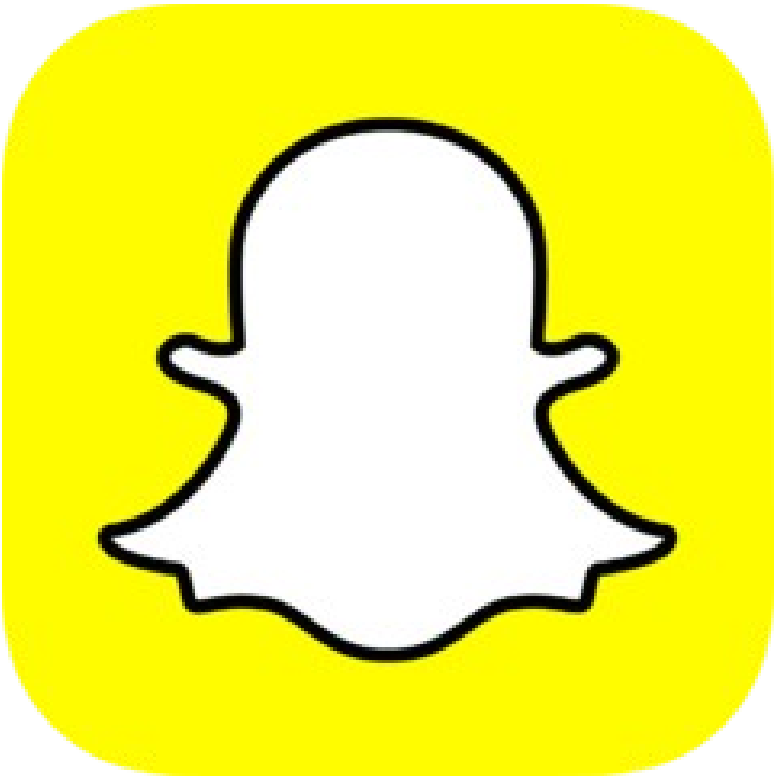


- **Socket**
  - Inspection des sockets

    Type / adresse locale / adresse distante
- **Stream**
  - Lecture / écriture asynchrones sur des fd / handles (UNIX / Windows)
- **File**
  - Manipulation de fichiers
- **ApiResolver**
  - Facilite l'énumeration de fonctions
  - Ex : `new ApiResolver('objc').enumerateMatches('-[NSURL* *HTTP*]', {onMatch: function (match) { … }, onComplete: function () { … }});`



DEMO !



Pour en savoir plus...

- **http://www.frida.re**
- **#frida sur irc.freenode.net**
- **https://groups.google.com/d/forum/frida-dev**

AVEZ-VOUS DES QUESTIONS ?

MERCI DE VOTRE ATTENTION,

SYNACKTIV
DIGITAL SECURITY