Reverse Engineering (/archive/?tag=Reverse+Engineering) Frida (/archive/?tag=Frida)

Frida 学习笔记

Posted by API Caller on March 30, 2019

本文环境

- Google Nexus/Pixel
- iPhone 6sp

Android

环境

```
# 用 magiskfrida 之类的插件代替
export PATH=~/Android/Sdk/platform-tools/:$PATH
adb push frida-server-12.4.8-android-arm64 /data/local/tmp/fserver
# adb shell su -c "mount -o rw,remount /system"
# adb shell su -c "mv /data/local/tmp/fserver /system/bin/fserver"
# adb shell su -c "chmod 777 /system/bin/fserver"
# adb shell su -c "mount -o ro,remount /system"

adb shell su -c "mv /data/local/tmp/fserver /sbin/fserver"
adb shell su -c "chmod 777 /sbin/fserver"
adb shell su -c "fserver --help"
```

- pip 安装指定版本 (virtualenv)

```
cd ~/frida
virtualenv --no-site-packages frida-12.0.7
source ~/frida/frida-12.0.7/bin/activate
pip3 install frida==12.0.7
pip3 install frida-tools==1.1.0
```

vscode 里添加

```
"python.venvPath": "F:\\path\\to\\Frida",
"python.venvFolders": [
    "envs",
    ".pyenv",
    ".direnv"
],
```

即可在 vscode 中选择 venv 中的解释器.

虚拟机堆栈

```
console.log(Java.use("android.util.Log").getStackTraceString(Java.use("java.lang.Throwable
```

相当于 java 的

```
android.util.Log.getStackTraceString(new java.lang.Throwable())
```

注入 Dex (https://www.jianshu.com/p/ca8381d3e094)

- **先用 sdk - build-tools 中的 dx 制作 dex, push 到手机里**
- **注入代码**

```
var currentApplication = Java.use("android.app.ActivityThread").currentApplication();
var context = currentApplication.getApplicationContext();
var pkgName = context.getPackageName();
var dexPath = "/data/local/tmp/guava.dex";
Java.openClassFile(dexPath).load();
console.log("inject " + dexPath + " to " + pkgName + " successfully!")
console.log(Java.use("com.google.common.collect.Maps")); //
```

Non-ASCII

比如说

```
int ֏(int x) {
    return x + 100;
}
```

甚至有一些不可视, 所以可以先编码打印出来, 再用编码后的字符串去 hook.

```
Java.perform(
    function x() {
        var targetClass = "com.example.hooktest.MainActivity";
        var hookCls = Java.use(targetClass);
        var methods = hookCls.class.getDeclaredMethods();
        for (var i in methods) {
            console.log(methods[i].toString());
            console.log(encodeURIComponent(methods[i].toString().replace(/^.*?\.([^\s\.\(\)]+)
        }
        hookCls[decodeURIComponent("%D6%8F")]
            .implementation = function (x) {
                console.log("original call: fun(" + x + ")");
                var result = this[decodeURIComponent("%D6%8F")](900);
                return result;
            }
    }
)
```

TracerPid

```
console.log("anti_fgets");
var fgetsPtr = Module.findExportByName('libc.so', 'fgets');
var fgets = new NativeFunction(fgetsPtr, 'pointer', ['pointer', 'int', 'pointer']);
Interceptor.replace(fgetsPtr, new NativeCallback(function (buffer, size, fp) {
    var retval = fgets(buffer, size, fp)
    var bufstr = Memory.readUtf8String(buffer)
    if (bufstr.indexOf('TracerPid:') > -1) {
        Memory.writeUtf8String(buffer, 'TracerPid:\t0')
        // console.log('tracerpid replaced: ' + bufstr)
    }
    if (bufstr.indexOf(':' + 27042..toString(16).toUpperCase()) > -1) {
        Memory.writeUtf8String(buffer, '')
        console.log('27042 replaced: ' + bufstr)
    }
    if (bufstr.indexOf('frida') > -1) { // frida
        Memory.writeUtf8String(buffer, '')
        console.log('frida replaced: ' + bufstr)
    }

    return retval
}, 'pointer', ['pointer', 'int', 'pointer']))
```

System.loadLibrary

```
const SDK_INT = Java.use('android.os.Build$VERSION').SDK_INT.value
const System = Java.use('java.lang.System')
const Runtime = Java.use('java.lang.Runtime')
const VMStack = Java.use('dalvik.system.VMStack')

System.loadLibrary.implementation = function (library: string) {
   try {
      console.log('System.loadLibrary("' + library + '")')
      if (SDK_INT > 23) {
         return Runtime.getRuntime().loadLibrary0(VMStack.getCallingClassLoader(), library)
      } else {
         return Runtime.getRuntime().loadLibrary(library, VMStack.getCallingClassLoader())
      }
   } catch (e) {
      console.warn(e)
   }
}

System.load.implementation = function (library: string) {
   try {
      console.log('System.load("' + library + '")')
      if (SDK_INT > 23) {
         return Runtime.getRuntime().load0(VMStack.getCallingClassLoader(), library)
      } else {
         return Runtime.getRuntime().load(library, VMStack.getCallingClassLoader())
      }
   } catch (e) {
      console.warn(e)
   }
};

```

也可以:

```
function readStdString(str) {
  const isTiny = (str.readU8() & 1) === 0
  if (isTiny) {
    return str.add(1).readUtf8String()
  }
  return str.add(2 * Process.pointerSize).readPointer().readUtf8String()
}

var mod_art = Process.findModuleByName("libart.so")
if (mod_art) {
  for (var exp of mod_art.enumerateExports()) {
    if (exp.name.indexOf("LoadNativeLibrary") != -1) {
      console.log(exp.name, exp.address)

      Interceptor.attach(exp.address, {
        onEnter: function (args) {
          this.pathName = readStdString(args[2])
          console.log("[*] [LoadNativeLibrary] in  pathName =", this.pathName)
        },
        onLeave: function (retval) {
          console.log("[*] [LoadNativeLibrary] out pathName =", this.pathName)
        }
      })

      break
    }
  }
}

var mod_dvm = Process.findModuleByName("libdvm.so")
if (mod_dvm) {
  for (var exp of mod_dvm.enumerateExports()) {
    if (exp.name.indexOf("dvmLoadNativeCode") != -1) {
      console.log(exp.name, exp.address)
      //    bool dvmLoadNativeCode(const char * pathName, void * classLoader, char ** det

      Interceptor.attach(exp.address, {
        onEnter: function (args) {
          this.pathName = args[0].readUtf8String()
          console.log("[*] [dvmLoadNativeCode] in  pathName =", this.pathName)
        },
        onLeave: function (retval) {
          console.log("[*] [dvmLoadNativeCode] out pathName =", this.pathName)
        }
      })
```

```

                break
            }
        }
    }
```

SDK_INT

```
const SDK_INT = Java.use('android.os.Build$VERSION').SDK_INT.value;
```

dump so

```
// Process.enumerateModules();
var fd = new File("/sdcard/Android/data/com.example/files/libxx.so","wb"); fd.write(new N
```

找 interface 的实现 (估计有谬误, 有空再找一下对应的 Java 代码翻译一下)

```
Java.enumerateLoadedClasses(
    {
        "onMatch": function (className) {
            if (className.indexOf("com.example.hooktest.") < 0) {
                return
            }
            var hookCls = Java.use(className)
            var interFaces = hookCls.class.getGenericInterfaces()
            if (interFaces.length > 0) {
                console.log(className)
                for (var i in interFaces) {
                    console.log("\t", interFaces[i])
                }
                var methods = hookCls.class.getDeclaredMethods()
                for (var i in methods) {
                    console.log(methods[i].toString(), "\t", encodeURIComponent(methods[i].toStrir
                }
            }
        },
        "onComplete": function () { }
    }
)
```

打印 il2cpp 中返回的 c# string

> **第三个四字节是长度, 第四个四字节开始存放 utf-16 字符串.**

```
// public string DecryptString(string stringId); // RVA: 0x3D270 Offset: 0x3D270
function attach_DecryptString(){
    var func = Module.getBaseAddress("libil2cpp.so").add(0x3D270)
    console.log('func addr: ' + func)
    Interceptor.attach(func, {
        onEnter: function (args) {

        },
        onLeave: function (retval) {
            print_dotnet_string("onLeave", retval)
        }
    }
    )
}
```

```
function print_dotnet_string(tag, dotnet_string) {
   console.log(JSON.stringify({
      tag: tag,
      len: dotnet_string.add(8).readU32(),
      data: dotnet_string.add(12).readUtf16String(-1)
   }))
}
```

读取 std::string

> Frida and std::string (https://stek29.rocks/2017/08/07/frida-stdstring.html)

PREVIOUS
V2RAY + CLOUDFLARE 配置
(/2019/03/01/V2RAY-WITH-CDN/)

NEXT
RUST 学习笔记 (/2019/07/19/RUST-NOTE/)

FEATURED TAGS (/archive/)

Reverse Engineering (/archive/?tag=Reverse+Engineering)
(/archive/?tag=Reverse+Engineering)

LINKS

(/archive/?tag=Reverse+Engineering)
(/archive/?tag=Reverse+Engineering)
(/archive/?tag=Reverse+Engineering)女朋友 (https://www.google.com/search?
q=%E6%80%8E%E4%B9%88%E5%8F%AF%E8%83%BD%E6%9C%89%E5%A5%B3%E6%9C%8B%E5%8