

某宝系 tb tm sgmain x-sign 分析 - unidbg

📅 2021/9/7 6:09:19

编程Tag: import new com TM VM Sign public sgmain unidbg

整套多商户商城源码打包售卖
秒变SaaS服务商

手机号(微信) :
13816330315

二维码

.NetCore最新技术栈 +Uni-app 多端小程序源码

本文主要是介绍某宝系 tb tm sgmain x-sign 分析 - unidbg，对大家解决编程问题具有一定的参考价值，需要的程序猿们随着小编来一起学习吧！

仅供学习研究。请勿用于非法用途，本人将不承担任何法律责任。

前言

apk 版本，天猫 8.11.0，本次主要说分析下如何使用 unidbg 跑通 x-sign，博主也是初学者，有啥问题可以加博主一起讨论哈，非常欢迎

charles 数据包分析

OverviewContentsSummaryChartNotes

POST /gw/mtop.alibaba.cro.umid.networksdk.saveweb/1.0/ HTTP/1.1
f-refer mtop
x-ttid 231200%40tmall android 8.11.0
x-sign ab205400901bb70b74bfc385d3713ea8b41aca3a0fb1f2bbf
x-c-traceid YSznz%2FgMpXu8DAD6xvGUyIWS1630139450634000416811
x-nettype WIFI
x-pv 6.2
x-nq WIFI
x-features 27
x-app-conf-v 0
a-orange-q appKey=23181017&appVersion=8.11.0&clientAppIndexVersion=0&clientVersio
x-mini-wua HHnB_QID45Y0o55WS4syYEmlanRi01sT6CasO71HrGW%2FIgA4%3D
x-utdid YSznz%2FgMpXu8DAD6xvGUyIWS
c-launch-info 0,0,1630139450634,0

主要分析这个 x-sign，知道目标后，直接开始使用 unidbg

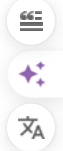
unidbg

具体的函数定位就不说了，各位看官应该都知道 JNICLibrary.doCommandNative 这个是 so 入口

```
1 package com.xiayu;
2
3 import com.github.unidbg.AndroidEmulator;
4 import com.github.unidbg.Emulator;
5 import com.github.unidbg.LibraryResolver;
6 import com.github.unidbg.file.FileResult;
7 import com.github.unidbg.file.IOResolver;
8 import com.github.unidbg.file.linux.AndroidFileIO;
9 import com.github.unidbg.linux.android.AndroidEmulatorBuilder;
10 import com.github.unidbg.linux.android.AndroidResolver;
11 import com.github.unidbg.linux.android.dvm.AbstractJni;
12 import com.github.unidbg.linux.android.dvm.DvmClass;
13 import com.github.unidbg.linux.android.dvm.DvmObject;
14 import com.github.unidbg.linux.android.dvm.VM;
```

区域3
广告位
QQ: 2300

区域3
广告位
QQ: 2300



```

15 import com.github.unidbg.memory.Memory;
16 import com.github.unidbg.spi.SyscallHandler;
17 import com.github.unidbg.virtualmodule.android.AndroidModule;
18 import org.json.JSONException;
19 import org.json.JSONObject;
20
21 import java.io.File;
22 import java.io.IOException;
23 import java.util.LinkedHashMap;
24 import java.util.Map;
25
26 public class TianMaoXSign1 extends AbstractJni implements IOResolver<AndroidFileIO>
27 {
28     private final AndroidEmulator emulator;
29     private final VM vm;
30     private long slot;
31
32     public String sgMain = "unidbg-
33 android/src/test/resources/test_so/tianmao8110/libsgmainso-6.4.156.so";
34     public String sgSecurityBody = "unidbg-
35 android/src/test/resources/test_so/tianmao8110/libsgsecuritybodyso-6.4.90.so";
36     public String sgAvMp = "unidbg-
37 android/src/test/resources/test_so/tianmao8110/libsgavmpso-6.4.34.so";
38     public String sgMisc = "unidbg-
39 android/src/test/resources/test_so/tianmao8110/libsgmiscso-6.4.44.so";
40
41     public File sgMainFile = new File(sgMain);
42     public File sgSecurityBodyFile = new File(sgSecurityBody);
43     public File sgAvMpFile = new File(sgAvMp);
44     public File sgMiscFile = new File(sgMisc);
45
46     public String dataAppPath = "/data/app/com.tmall.wireless-
47 NsaOVgz2fomXJNoPTrbOwg==";
48     public String packageName = "com.tmall.wireless";
49     public String methodSign =
50 "doCommandNative(I[Ljava/lang/Object;)Ljava/lang/Object;";
51     public DvmClass JNICLibrary;
52     public DvmObject<?> context;
53     public DvmObject<?> ret;
54
55     public String APK_INSTALL_PATH = dataAppPath + "/base.apk";
56     public File APK_FILE = new File("/Users/admin/Desktop/android/file/tianmao-
57 8.11.0.apk");
58     private static LibraryResolver createLibraryResolver() {
59         return new AndroidResolver(23);
60     }
61
62     private static AndroidEmulator createARMEulator() {
63         return AndroidEmulatorBuilder
64             .for32Bit()
65             .setRootDir(new File("appFile/tianmao-xsign1"))
66             .setProcessName("com.tmall.wireless")
67             .build();
68     }
69
70     public TianMaoXSign1() {
71         emulator = createARMEulator();
72
73         Map<String, Integer> iNode = new LinkedHashMap<>();
74         iNode.put("/data/system", 671745);
75         iNode.put("/data/app", 327681);
76         iNode.put("/sdcard/android", 294915);
77         iNode.put("/data/user/0/com.tmall.wireless", 655781);
78         iNode.put("/data/user/0/com.tmall.wireless/files", 655864);
79         emulator.set("inode", iNode);
80         emulator.set("uid", 10074);
81
82         Memory memory = emulator.getMemory();
83         memory.setLibraryResolver(createLibraryResolver());
84         SyscallHandler<AndroidFileIO> handler = emulator.getSyscallHandler();
85         handler.setVerbose(false);
86         handler.addIOResolver(this);
87
88         vm = emulator.createDalvikVM(APK_FILE);
89         vm.setJni(this);
90         vm.setVerbose(true);
91
92         new AndroidModule(emulator, vm).register(memory);
93
94         JNICLibrary =
95 vm.resolveClass("com/taobao/wireless/security/adapter/JNICLibrary");
96         context = vm.resolveClass("android/content/Context").newObject(null);
97     }
98
99     public static void main(String[] args) throws IOException {
100         TianMaoXSign1 tm2 = new TianMaoXSign1();
101         tm2.destroy();
102     }
103

```

```

104 |     public void destroy() throws IOException {
        emulator.close();
    }

    @Override
    public FileResult<AndroidFileIO> resolve(Emulator<AndroidFileIO> emulator,
String pathname, int oflags) {
        System.out.println("resolve.pathname: " + pathname);
        return null;
    }
}

```

这里先把框架搭起来, `IOResolver<AndroidFileIO>` 这个接口类可以直接使用 `unidbg` 的虚拟文件系统, 方便补文件。运行, 如果没啥错误就说明一切正常, 继续下一步

下面开始对各个 `so` 进行初始化, 具体的初始化流程, 可以使用 `frida hook` 查看整体流程, 使用 `jnitrace` 不全, 比较容易出问题

libsgmainso

```

1 | public void initMain() {
2 |     DalvikModule dm = vm.loadLibrary(sgMainFile, true);
3 |     dm.callJNI_OnLoad(emulator);
4 |
5 |     ret = JNICLibrary.callStaticJniMethodObject(
6 |         emulator, methodSign, 10101,
7 |         new ArrayObject(
8 |             context,
9 |             DvmInteger.valueOf(vm, 3),
10 |             new StringObject(vm, ""),
11 |             new StringObject(vm, "/data/user/0/" + packageName +
12 | "/app_SGLib"),
13 |             new StringObject(vm, "")
14 |         ));
15 |     System.out.println("xiayu, initMain.ret-10101: " + ret.getValue().toString());
16 |
17 |     ret = JNICLibrary.callStaticJniMethodObject(
18 |         emulator, methodSign, 10102,
19 |         new ArrayObject(
20 |             new StringObject(vm, "main"),
21 |             new StringObject(vm, "6.5.156"),
22 |             new StringObject(vm,
23 | "/data/user/0/com.tmall.wireless/app_SGLib/app_1627957761/main/libsgmainso-
24 | 6.5.156.so")
25 |         ));
26 |     System.out.println("xiayu, initMain.ret-10102: " + ret.getValue().toString());
27 | }

```

这里是初始化 `sgmain` 具体流程是 `frida hook` 的结果, 写好后在 `main` 函数里调用一下, 开始运行

```

JNIEnv->NewGlobalRef(class android/content/Context) was called from RX@0x40839ab5[libmain.so]@0x39ab5
JNIEnv->GetMethodID(android/content/Context.checkSelfPermission(Ljava/lang/String;)I) was called from RX@0x40839b23[libmain.so]@0x39b23
JNIEnv->FindClass(class com/alibaba/wireless/security/open/umid/UHIDComponent) was called from RX@0x4083878b[libmain.so]@0x3878b
JNIEnv->NewGlobalRef(class com/alibaba/wireless/security/open/umid/UHIDComponent) was called from RX@0x40838753[libmain.so]@0x38753
JNIEnv->GetMethodID(class com/alibaba/wireless/security/open/umid/UHIDComponent.sendUmidChangedNotification(Ljava/lang/String;)V) was called from RX@0x408387f5[libmain.so]@0x387f5
JNIEnv->FindClass(class com/alibaba/wireless/security/mainplugin/SecurityGuardMainPlugin) was called from RX@0x40858a51[libmain.so]@0x58a51
JNIEnv->GetMethodID(class com/alibaba/wireless/security/mainplugin/SecurityGuardMainPlugin.getMainPluginClassLoader()Ljava/lang/ClassLoader;) was called from RX@0x40858a51[libmain.so]@0x58a51
[23:06:28 835] WARN [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:457) - handleInterrupt intno=2, NR=-1073744240, svcNumber=0x132, PC=unidbg.java.lang.UnsupportedOperationException: com/alibaba/wireless/security/mainplugin/SecurityGuardMainPlugin->getMainPluginClassLoader()Ljava/lang/ClassLoader;
at com.github.unidbg.linux.android.dvm.AbstractJni.callStaticObjectMethod(AbstractJni.java:357)
at com.github.unidbg.linux.android.dvm.AbstractJni.callStaticObjectMethod(AbstractJni.java:352)
at com.github.unidbg.linux.android.dvm.DvmMethod.callStaticObjectMethod(DvmMethod.java:55)
at com.github.unidbg.linux.android.dvm.DalvikVM$51.handle(DalvikVM.java:1286)
at com.github.unidbg.linux.ARM32SyscallHandler.hook(ARM32SyscallHandler.java:182)
at com.github.unidbg.arm.backend.UnicornBackend$6.hook(UnicornBackend.java:292)

```

```

@Override
public DvmObject<?> callStaticObjectMethod(BaseVM vm, DvmClass dvmClass, String signature, VarArg varArg) {
    switch (signature) {
        case "com/alibaba/wireless/security/mainplugin/SecurityGuardMainPlugin->getMainPluginClassLoader()Ljava/lang/ClassLoader;":
            return vm.resolveClass("java/lang/ClassLoader").newObject(signature);
    }

    return super.callStaticObjectMethod(vm, dvmClass, signature, varArg);
}

```

这里就开始报常见的环境错误了, 我们给他加上

```
Find native function Java_com_tmbao_wireless_security_adapter_JNICLibrary_doCommandNative(I[Ljava/lang/Object;)Ljava/lang/Object;
JNINEnv->GetObjectArrayElement([android.content.Context@567d299b, java.lang.Integer@2eafffde, "", "/data/user/0/com.tmall.wireless-nsa0vgz2fomXJNoPTrb0wg==/base.apk") was called from RX@0x400b5297[libmain.so]0xb5297
JNINEnv->GetObjectArrayElement([android.content.Context@567d299b, java.lang.Integer@2eafffde, "", "/data/user/0/com.tmall.wireless-nsa0vgz2fomXJNoPTrb0wg==/base.apk") was called from RX@0x400b5297[libmain.so]0xb5297
JNINEnv->GetMethodID(java.lang.Integer.intValue()I) was called from RX@0x400b5921[libmain.so]0xb5921
JNINEnv->CallIntMethod(java.lang.Integer@2eafffde, intValue() => 0x3) was called from RX@0x400b187eb[libmain.so]0x187eb
JNINEnv->GetMethodID(android.content.Context.getPackageCodePath()Ljava/lang/String;) was called from RX@0x4001130d[libmain.so]0x1130d
[23:08:39 284] WARN [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:457) - handleInterrupt intno=2, NR=-107374328, svcNumber=0x1130d
java.lang.UnsupportedOperationException: android.content.Context->getPackageCodePath()Ljava/lang/String;
    at com.github.unidbg.linux.android.dvm.AbstractJni.callObjectMethod(AbstractJni.java:778)
    at com.github.unidbg.linux.android.dvm.AbstractJni.callObjectMethod(AbstractJni.java:786)
    at com.github.unidbg.linux.android.dvm.DvmMethod.callObjectMethod(DvmMethod.java:78)
    at com.github.unidbg.linux.android.dvm.DalvikVM$28.handle(DalvikVM.java:489)
    at com.github.unidbg.linux.ARM32SyscallHandler.hook(ARM32SyscallHandler.java:182)
```

```
@Override
public DvmObject<?> callObjectMethod(BaseVM vm, DvmObject<?> dvmObject, String signature, VarArg varArg) {
    switch (signature) {
        case "android/content/Context->getPackageCodePath()Ljava/lang/String;": {
            return new StringObject(vm, APK_INSTALL_PATH);
        }
    }

    return super.callObjectMethod(vm, dvmObject, signature, varArg);
}
```

这里继续，返回 apk 的 base.apk 路径

```
JNINEnv->GetStringUTFChars("/data/app/com.tmall.wireless-nsa0vgz2fomXJNoPTrb0wg==/base.apk") was called from RX@0x400b537d[libmain.so]0xb537d
JNINEnv->ReleaseStringUTFChars("/data/app/com.tmall.wireless-nsa0vgz2fomXJNoPTrb0wg==/base.apk") was called from RX@0x400b53c7[libmain.so]0xb53c7
JNINEnv->GetMethodID(android.content.Context.getFilesDir()Ljava/io/File;) was called from RX@0x400114e9[libmain.so]0x114e9
[23:09:34 988] WARN [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:457) - handleInterrupt intno=2, NR=-107374328, svcNumber=0x114e9
java.lang.UnsupportedOperationException: android.content.Context->getFilesDir()Ljava/io/File;
    at com.github.unidbg.linux.android.dvm.AbstractJni.callObjectMethod(AbstractJni.java:778)
    at com.xiaoyu.TianMaoXSign1.callObjectMethod(TianMaoXSign1.java:157)
    at com.github.unidbg.linux.android.dvm.AbstractJni.callObjectMethod(AbstractJni.java:786)
    at com.github.unidbg.linux.android.dvm.DvmMethod.callObjectMethod(DvmMethod.java:78)
    at com.github.unidbg.linux.ARM32SyscallHandler.hook(ARM32SyscallHandler.java:182)
```

```
@Override
public DvmObject<?> callObjectMethod(BaseVM vm, DvmObject<?> dvmObject, String signature, VarArg varArg) {
    switch (signature) {
        case "android/content/Context->getPackageCodePath()Ljava/lang/String;": {
            return new StringObject(vm, APK_INSTALL_PATH);
        }
        case "android/content/Context->getFilesDir()Ljava/io/File;": {
            return new StringObject(vm, vm.getFilesDir().getAbsolutePath());
        }
        case "java/lang/String->getAbsolutePath()Ljava/lang/String;": {
            return new StringObject(vm, vm.getFilesDir().getAbsolutePath());
        }
    }

    return super.callObjectMethod(vm, dvmObject, signature, varArg);
}
```

Run: TianMaoXSign1

```
JNINEnv->CallIntMethod(java.lang.Integer@2eafffde, intValue() => 0x3) was called from RX@0x400b187eb[libmain.so]0x187eb
JNINEnv->GetMethodID(android.content.Context.getPackageCodePath()Ljava/lang/String;) was called from RX@0x4001130d[libmain.so]0x1130d
JNINEnv->CallObjectMethod(android.content.Context@567d299b, getPackageCodePath() => "/data/app/com.tmall.wireless-nsa0vgz2fomXJNoPTrb0wg==/base.apk") was called from RX@0x4001130d[libmain.so]0x1130d
JNINEnv->GetStringUTFChars("/data/app/com.tmall.wireless-nsa0vgz2fomXJNoPTrb0wg==/base.apk") was called from RX@0x400b537d[libmain.so]0xb537d
JNINEnv->ReleaseStringUTFChars("/data/app/com.tmall.wireless-nsa0vgz2fomXJNoPTrb0wg==/base.apk") was called from RX@0x400b53c7[libmain.so]0xb53c7
JNINEnv->GetMethodID(android.content.Context.getFilesDir()Ljava/io/File;) was called from RX@0x400114e9[libmain.so]0x114e9
JNINEnv->CallObjectMethod(android.content.Context@567d299b, getFilesDir() => "/data/user/0/com.tmall.wireless/files") was called from RX@0x40011509[libmain.so]0x11509
JNINEnv->GetMethodID(java/lang/String->getAbsolutePath()Ljava/lang/String;) was called from RX@0x40011509[libmain.so]0x11509
[23:10:46 186] WARN [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:457) - handleInterrupt intno=2, NR=-107374328, svcNumber=0x11509
java.lang.UnsupportedOperationException: java/lang/String->getAbsolutePath()Ljava/lang/String;
    at com.github.unidbg.linux.android.dvm.AbstractJni.callObjectMethod(AbstractJni.java:778)
    at com.xiaoyu.TianMaoXSign1.callObjectMethod(TianMaoXSign1.java:162)
    at com.github.unidbg.linux.android.dvm.AbstractJni.callObjectMethod(AbstractJni.java:786)
    at com.github.unidbg.linux.android.dvm.DvmMethod.callObjectMethod(DvmMethod.java:78)
```

这里连续报的两个错误，可以统一处理，返回 files 文件夹路径

```
@Override
public DvmObject<?> getObjectField(BaseVM vm, DvmObject<?> dvmObject, String signature) {
    if ("android/content/pm/ApplicationInfo->nativelibraryDir()Ljava/lang/String;".equals(signature)) {
        return new StringObject(vm, vm.dataAppPath + "/lib/arm");
    }

    return super.getObjectField(vm, dvmObject, signature);
}
```

Run: TianMaoXSign1

```
JNINEnv->GetStringUTFChars("/data/app/com.tmall.wireless-nsa0vgz2fomXJNoPTrb0wg==/base.apk") was called from RX@0x400b537d[libmain.so]0xb537d
JNINEnv->ReleaseStringUTFChars("/data/app/com.tmall.wireless-nsa0vgz2fomXJNoPTrb0wg==/base.apk") was called from RX@0x400b53c7[libmain.so]0xb53c7
JNINEnv->GetMethodID(android.content.Context.getFilesDir()Ljava/io/File;) was called from RX@0x400114e9[libmain.so]0x114e9
JNINEnv->CallObjectMethod(android.content.Context@567d299b, getFilesDir() => "/data/user/0/com.tmall.wireless/files") was called from RX@0x40011509[libmain.so]0x11509
JNINEnv->GetMethodID(java/lang/String->getAbsolutePath()Ljava/lang/String;) was called from RX@0x40011509[libmain.so]0x11509
JNINEnv->CallObjectMethod("/data/user/0/com.tmall.wireless/files", getAbsolutePath() => "/data/user/0/com.tmall.wireless/files") was called from RX@0x400b537d[libmain.so]0xb537d
JNINEnv->GetStringUTFChars("/data/user/0/com.tmall.wireless/files") was called from RX@0x400b537d[libmain.so]0xb537d
JNINEnv->ReleaseStringUTFChars("/data/user/0/com.tmall.wireless/files") was called from RX@0x400b53c7[libmain.so]0xb53c7
JNINEnv->GetMethodID(android.content.Context.getApplicationInfo()Landroid/content/pm/ApplicationInfo;) was called from RX@0x40011715[libmain.so]0x11715
JNINEnv->CallObjectMethod(android.content.Context@567d299b, getApplicationInfo() => android.content.pm.ApplicationInfo@64cee07) was called from RX@0x40011715[libmain.so]0x11715
[23:11:29 601] WARN [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:457) - handleInterrupt intno=2, NR=-107374328, svcNumber=0x11715
java.lang.UnsupportedOperationException: android/content/pm/ApplicationInfo->nativelibraryDir()Ljava/lang/String;
    at com.github.unidbg.linux.android.dvm.AbstractJni.getObjectField(AbstractJni.java:136)
    at com.github.unidbg.linux.android.dvm.AbstractJni.getObjectField(AbstractJni.java:188)
    at com.github.unidbg.linux.android.dvm.DvmField.getObjectField(DvmField.java:56)
```


这里需要返回 apk 的 native lib/arm 路径

```
@Override
public DvmObject<?> newObject(BaseVM vm, DvmClass dvmClass, String signature, VarArg varArg) {
    switch (signature) {
        case "com/alibaba/wireless/security/open/SecException-><init>(Ljava/lang/String;)V": {
            StringObject msg = varArg.getObjectArg( index: 0);
            int value = varArg.getIntArg( index: 1);

            System.out.println("SecException.msg : " + msg);
            System.out.println("SecException.value: " + value);

            return dvmClass.newObject( value: msg.getValue() + " " + value + "");
        }
    }

    return super.newObject(vm, dvmClass, signature, varArg);
}
}
```

这个是 `sgmain` 抛异常的类，我们需要把 `msg code` 打印下，看看报了啥错误

```

↑
↓
⏮
⏭
⏴
⏵
⏶
⏷
resolve.pathname: /data/app/com.tmall.wireless-Nsa0Vgz2fomXJNoPTrb0wg==/base.apk
[23:15:50 508] INFO [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:19)
resolve.pathname: /data/app/com.tmall.wireless-Nsa0Vgz2fomXJNoPTrb0wg==/base.apk
[23:15:50 509] INFO [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:19)
JNIEnv->FindClass(com/alibaba/wireless/security/open/SecException) was called from RX@0x40
JNIEnv->GetMethodID(com/alibaba/wireless/security/open/SecException.<init>(Ljava/lang/Stri
JNIEnv->NewStringUTF("") was called from RX@0x40b587f[libmain.so]@xb587f
SecException.msg : ""
SecException.value: 123
JNIEnv->NewObject(class com/alibaba/wireless/security/open/SecException, <init>("", 0x7b)
[23:15:50 511] WARN [com.github.unidbg.linux.android.dvm.DalvikVM] (DalvikVM$3:116) - Thr
Exception in thread "main" java.lang.NullPointerException
    at com.xiayu.TianMaoXSign1.initMain(TianMaoXSign1.java:106)
    at com.xiayu.TianMaoXSign1.main(TianMaoXSign1.java:122)

```

继续执行，果然报错了 `code = 123`。这里查找错误原因有两种，第一种是 百度搜索 阿里聚安全 123 是啥错误，第二种是自己查看 `log` 日志，猜测试错。过程还是比较坑的，我这里踩了很多坑，就直接说答案吧是缺少了文件。具体缺少啥文件，搜索 `resolve.pathname`：这个字眼，不知道补哪些就能补的都补下

The screenshot displays the Android Studio environment. On the left, the 'Project' tab of the file explorer shows the package structure: `com.tmall.wireless` containing `NsaOvg2fomXNoPTrbDwgw`. The right pane shows the Java code for a class. The `main` method takes a `String[] args` and throws `IOException`. The `destroy` method also throws `IOException` and overrides a method. It calls `resolve` with parameters: `Emulator<AndroidFileIo> emulator`, `String pathname`, `int oflags`, and `System.out.println("resolve.pathname: " + pathname);`. The `resolve` method is highlighted with a red box. It checks if the `pathname` equals `"/data/app/com.tmall.wireless-NsaOvg2fomXNoPTrbDwgw-base.apk"`. If true, it returns `FileResult.success(emulator.getFileSystem().createSimpleFileIo(APK_FILE, oflags, pathname));`. Otherwise, it returns `null`. The `@Override` annotation is also visible above the `destroy` method.

我这里是补了左侧的几个文件，跟 `base.apk`，文件就在手机里对应的目录下，`pull` 下来就行，运行后发现不再报 123 错误了

```

196
197
198 @Override
199 public void callStaticVoidMethod(BaseVM vm, DvmClass dvmClass, String signature, VarArg varArg) {
200     switch (signature) {
201         case "com.alibaba/wireless/security/securitybody/LifeCycle->registerCallBack()V":
202             return;
203         case "com.alibaba/wireless/security/open/edgecomputing/ECMiscInfo->registerAppLifeCycleCallBack()V":
204             return;
205     }
206     super.callStaticVoidMethod(vm, dvmClass, signature, varArg);
207 }
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000

```

这里报了两个错误，可以一起补

```

public DvmObject<?> callStaticObjectMethod(BaseVM vm, DvmClass dvmClass, String signature, VarArg varArg) {
    switch (signature) {
        case "com.alibaba/wireless/security/mainlogin/SecurityGuardMainPlugin->getMainPluginClassLoader()Ljava/lang/ClassLoader;": { ... }
        case "com.taobao/wireless/security/adaptor/common/SPUtility2->readFromSPUnified(Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;)Ljava/lang/String;": {
            String temp = null;
            String key = varArg.getObjectArg(0).getValue() + "." + varArg.getObjectArg(1).getValue();
            System.out.println("readFromSPUnified: " + key);
            try {
                temp = data.getString(key);
            } catch (Exception ignored) {
            }
            return temp == null ? varArg.getObjectArg(2) : new StringObject(vm, temp);
        }
    }
    return super.callStaticObjectMethod(vm, dvmClass, signature, varArg);
}

```

```

resolve.pathname: /data/app/com.tmall.wireless-Nsa0Vgz2fomX3NoPTrb0wg==/base.apk
resolve.pathname: /data/user/0/com.tmall.wireless/files
resolve.pathname: /data/user/0/com.tmall.wireless/files/spFile.lock
resolve.pathname: /data/user/0/com.tmall.wireless/app_56Lib/SG_INNER_DATA
[23:28:43 899] INFO [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:1913) - openat dirfd=-100, pathname=/data/user/0/com.tmall.wireless/app_56Lib/SG_INNER_DATA, flags=O_RDONLY, mode=0, result=0
JNIEnv->NewStringUTF("Soft") was called from RX@8x400b5561[libmain.so]@xb5561
JNIEnv->NewStringUTF("SGSAFETOKEN_IN") was called from RX@8x400b5561[libmain.so]@xb5561
[23:28:43 101] WARN [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:457) - handleInterrupt intno=2, NR=-1073746096, svcNumber=0x132, PC=un
java.lang.UnsupportedOperationException: com.taobao/wireless/security/adaptor/common/SPUtility2->readFromSPUnified(Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;)Ljava/lang/String;
    at com.github.unidbg.linux.android.dvm.AbmootJni.callStaticObjectMethod(AbmootJni.java:157)
    at com.xiyu.TianMaoXSign1.callStaticObjectMethod(TianMaoXSign1.java:153)
    at com.github.unidbg.linux.android.dvm.AbmootJni.callStaticObjectMethod(AbmootJni.java:152)
    at com.github.unidbg.linux.android.dvm.DvmMethod.callStaticObjectMethod(DvmMethod.java:55)

```

```

data = new JSONObject(("{\"SGTAGIC\":\"jniPwHvUgUgCgQgPwUfPkFALSJaAEbHFSJ2ImKc8=\",\"SGSAFETOKEN_IN\":\"34e56Q7ML/\"}"));
JNICLibrary = vm.resolveClass( className: "com.taobao/wireless/security/adaptor/JNICLibrary");
context = vm.resolveClass( className: "android/content/Context").newObject( value: null);

```

中间又补了几个错误之后，这里是读取文件里的 json 内容，因为是固定的我就直接取出来了，这个补完之后再补一个常见的就 OK 了

```

JNIEnv->GetMethodID(java/lang/Integer.<init>(I)V) was called from RX@0x...
JNIEnv->NewObject(class java/lang/Integer, <init>(0x0)
xiayu, initMain.ret-10101: 0
Find native function java_com_taobao_wireless_security...
JNIEnv->GetArrayLength(["main", "6.5.156", "/data/user/0/com.tmall.wireless...
JNIEnv->GetObjectArrayElement(["main", "6.5.156", "/data/user/0/com.tmall.wireless...
JNIEnv->GetStringUtfChars("main") was called from RX@0x...
JNIEnv->ReleaseStringUtfChars("main") was called from RX@0x...
JNIEnv->GetObjectArrayElement(["main", "6.5.156", "/data/user/0/com.tmall.wireless...
JNIEnv->GetStringUtfChars("6.5.156") was called from RX@0x...
JNIEnv->ReleaseStringUtfChars("6.5.156") was called from RX@0x...
JNIEnv->GetObjectArrayElement(["main", "6.5.156", "/data/user/0/com.tmall.wireless...
JNIEnv->GetStringUtfChars("/data/user/0/com.tmall.wireless...
JNIEnv->ReleaseStringUtfChars("/data/user/0/com.tmall.wireless...
JNIEnv->GetMethodID(android/content/Context.getPackageName()Ljava/lang/String;)Ljava/lang/String;) was called from RX@0x...
JNIEnv->CallObjectMethod(android.content.Context@510160, java/lang/String;)Ljava/lang/String;) was called from RX@0x...
JNIEnv->GetStringUtfChars("/data/app/com.tmall.wireless...
JNIEnv->ReleaseStringUtfChars("/data/app/com.tmall.wireless...
[23:32:58 060] INFO [com.github.unidbg.linux.ARM32SyscallHandler] syscall 10102
JNIEnv->GetMethodID(java/lang/Integer.<init>(I)V) was called from RX@0x...
JNIEnv->NewObject(class java/lang/Integer, <init>(0x0)
xiayu, initMain.ret-10102: 0

```

这里算是 `sgmain` 就补完了，全都正常返回了 0，这个结果我是 `frida call` 出来的结果

libsgsecuritybodyso

```

1 public void initSecurityBody() {
2     DalvikModule securityBody = vm.loadLibrary(sgSecurityBodyFile, true);
3     securityBody.callJNI_OnLoad(emulator);
4
5     ret = JNICLibrary.callStaticJniMethodObject(
6         emulator, methodSign, 10102,
7         new ArrayObject(
8             new StringObject(vm, "securitybody"),
9             new StringObject(vm, "6.4.90"),
10            new StringObject(vm,
11                "/data/user/0/com.tmall.wireless/app_SGLib/app_1627957761/main/libsgsecuritybodyso-
12                6.4.90.so")
13            ));
14     System.out.println("xiayu, initSecurityBody.ret-10102: " +
15         ret.getValue().toString());
16 }

```

新增个函数，`main` 函数里调用


```

@Override
public void setStaticLongField(BaseVM vm, DvmClass dvmClass, String signature, long value) {
    System.out.println("setStaticLongField.signature: " + value);

    if ("com/alibaba/wireless/security/framework/SGPluginExtras->slot:J".equals(signature)) {
        this.slot = value;
    } else {
        super.setStaticLongField(vm, dvmClass, signature, value);
    }
}
}
}

TianMaoXSign1
xiayu, initMain.ret-18182: 0
JNIEnv->FindClass(java/lang/Boolean) was called from RX@0x418643a5[libsecuritybody.so]@x253a5
JNIEnv->NewGlobalRef(class java/lang/Boolean) was called from RX@0x418643af[libsecuritybody.so]@x253af
JNIEnv->FindClass(java/lang/Integer) was called from RX@0x418643bf[libsecuritybody.so]@x253bf
JNIEnv->NewGlobalRef(class java/lang/Integer) was called from RX@0x418643c9[libsecuritybody.so]@x253c9
JNIEnv->FindClass(java/lang/String) was called from RX@0x418643d9[libsecuritybody.so]@x253d9
JNIEnv->NewGlobalRef(class java/lang/String) was called from RX@0x418643e3[libsecuritybody.so]@x253e3
JNIEnv->FindClass(com/alibaba/wireless/security/framework/SGPluginExtras) was called from RX@0x4186681d[libsecuritybody.so]@x2781d
[23:39:59 358] WARN [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:457) - handleInterrupt intno=2, NR=-1873744848, svcNumbe
java.lang.UnsupportedOperationException: com/alibaba/wireless/security/framework/SGPluginExtras->slot:J
    at com.github.unidbg.linux.android.dvm.AbstractJni.setStaticLongField(AbstractJni.java:845)
    at com.github.unidbg.linux.android.dvm.AbstractJni.setStaticLongField(AbstractJni.java:846)
    at com.github.unidbg.linux.android.dvm.DvmField.setStaticLongField(DvmField.java:189)
    at com.github.unidbg.linux.android.dvm.DalvikVM$42.handle(DalvikVM.java:1426)

```

```

@Override
public int getStaticIntField(BaseVM vm, DvmClass dvmClass, String signature) {
    if ("android/content/pm/PackageManager->PERMISSION_GRANTED:I".equals(signature)) {
        return 0;
    }

    return super.getStaticIntField(vm, dvmClass, signature);
}

TianMaoXSign1
JNIEnv->GetMethodID(android/content/Context.checkSelfPermission(Ljava/lang/String;)I) was called from RX@0x4185bb23[libsecuritybody.so]@x1c1cb
JNIEnv->GetMethodID(android/content/Context.checkCallingOrSelfPermission(Ljava/lang/String;)I) was called from RX@0x4185bb55[libsecuritybody
JNIEnv->GetMethodID(android/content/Context.registerReceiver(Landroid/content/BroadcastReceiver;Landroid/content/IntentFilter;)Landroid/cont
JNIEnv->GetMethodID(android/content/Context.getContentResolver()Landroid/content/ContentResolver;) was called from RX@0x4185bbbf[libsecurity
JNIEnv->FindClass(android/content/pm/PackageManager) was called from RX@0x4185bbe7[libsecuritybody.so]@x1cbe7
[23:41:17 619] WARN [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:457) - handleInterrupt intno=2, NR=-1873744856, svcN
java.lang.UnsupportedOperationException: android/content/pm/PackageManager->PERMISSION_GRANTED:I
    at com.github.unidbg.linux.android.dvm.AbstractJni.getStaticIntField(AbstractJni.java:184)
    at com.github.unidbg.linux.android.dvm.AbstractJni.getStaticIntField(AbstractJni.java:185)
    at com.github.unidbg.linux.android.dvm.DvmField.getStaticIntField(DvmField.java:49)
    at com.github.unidbg.linux.android.dvm.DalvikVM$42.handle(DalvikVM.java:1426)

```

```

@Override
public long getStaticLongField(BaseVM vm, DvmClass dvmClass, String signature) {
    if ("com/alibaba/wireless/security/framework/SGPluginExtras->slot:J".equals(signature)) {
        return this.slot;
    } else {
        return super.getStaticLongField(vm, dvmClass, signature);
    }
}

TianMaoXSign1
JNIEnv->ReleaseStringUTFChars("6.4.98") was called from RX@0x408b5485[libmain.so]@xb5485
JNIEnv->GetObjectArrayElement(["securitybody", "6.4.98", "/data/user/0/com.tmall.wireless/app_SGLib/app_1627957761/main/libsgsecuritybodyso-6.4
JNIEnv->GetStringUTFChars("/data/user/0/com.tmall.wireless/app_SGLib/app_1627957761/main/libsgsecuritybodyso-6.4.98.so") was called from RX@0x4
JNIEnv->ReleaseStringUTFChars("/data/user/0/com.tmall.wireless/app_SGLib/app_1627957761/main/libsgsecuritybodyso-6.4.98.so") was called from RX
JNIEnv->FindClass(com/alibaba/wireless/security/framework/SGPluginExtras) was called from RX@0x40818dfd[libmain.so]@x18dfd
JNIEnv->NewGlobalRef(class com/alibaba/wireless/security/framework/SGPluginExtras) was called from RX@0x40818e09[libmain.so]@x18e09
[23:41:58 841] WARN [com.github.unidbg.linux.ARM32SyscallHandler] (ARM32SyscallHandler:457) - handleInterrupt intno=2, NR=-1873744168, svcNumbe
java.lang.UnsupportedOperationException: com/alibaba/wireless/security/framework/SGPluginExtras->slot:J
    at com.github.unidbg.linux.android.dvm.AbstractJni.getStaticLongField(AbstractJni.java:855)
    at com.github.unidbg.linux.android.dvm.AbstractJni.getStaticLongField(AbstractJni.java:856)
    at com.github.unidbg.linux.android.dvm.DvmField.getStaticLongField(DvmField.java:116)
    at com.github.unidbg.linux.android.dvm.DalvikVM$48.handle(DalvikVM.java:1628)

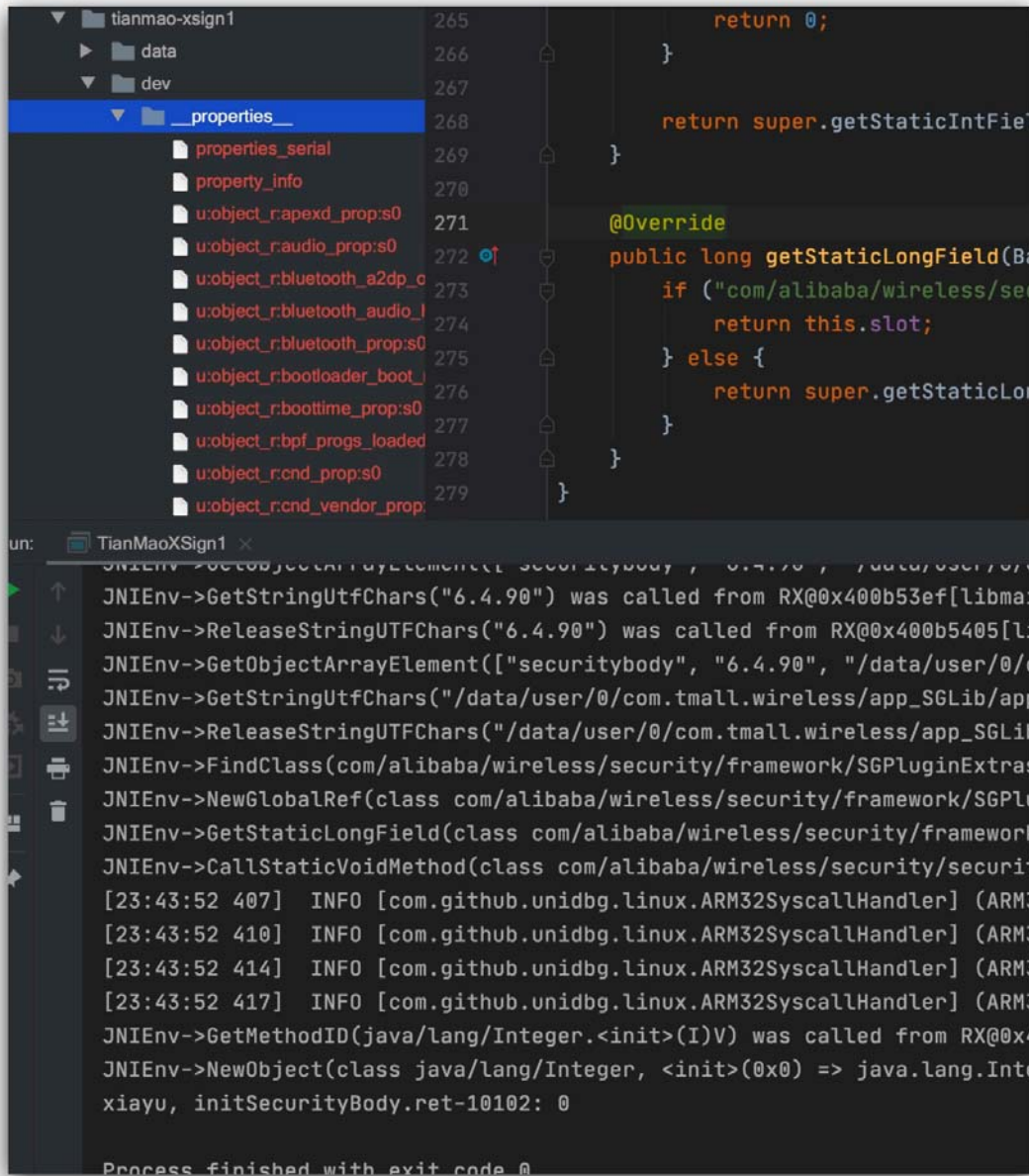
```

上图都是执行结果却啥啥啥，就行

```

JNIEnv->FindClass(java/lang/String) was called from RX@0x418534bb[libsecuritybody.so]@x144bb
JNIEnv->NewGlobalRef(class java/lang/String) was called from RX@0x418534cd[libsecuritybody.so]@x144cd
JNIEnv->GetMethodID(java/lang/String.<init>()V) was called from RX@0x418534e9[libsecuritybody.so]@x144e9
[23:42:31 972] WARN [com.github.unidbg.arm.AbstractARMEulator] (AbstractARMEulator$1:58) - memory failed: address=0x1cb9c121, size=4, value=0x0, PC=RX
[23:42:31 973] WARN [com.github.unidbg.AbstractEmulator] (AbstractEmulator:389) - emulate RX@0x00018269[libmain.so]@x18269 exception sp=unidbg@0xbffff58
Exception in thread "main" java.lang.NullPointerException
    at com.xiaoyu.TianMaoXSign1.initSecurityBody(TianMaoXSign1.java:132)
    at com.xiaoyu.TianMaoXSign1.main(TianMaoXSign1.java:140)

```

补到最后报了个指针错误，因为啥也不知道，还是使用相同的方法补文件，经过测试补 `dev/.__properties__` 即可，继续运行，OK 了

libsgavmpso

```

1 public void initAvMp() {
2     DalvikModule avMp = vm.loadLibrary(sgAvMpFile, true);
3     avMp.callJNI_OnLoad(emulator);
4
5     ret = JNICLibrary.callStaticJniMethodObject(
6         emulator, methodSign, 10102,
7         new ArrayObject(
8             new StringObject(vm, "avmp"),
9             new StringObject(vm, "6.4.34"),
10            new StringObject(vm,
11                "/data/user/0/com.tmall.wireless/app_SGLib/app_1627957761/main/libsgavmpso-
12                6.4.34.so")
13        ));
14     System.out.println("xiayu, initAvMp.ret-10102: " + ret.getValue().toString());
15 }

```

这个比较简单，跟上诉逻辑差不多，就不说了，缺啥补啥

get x-sign

```

1 public void getXSign() {
2     Map<String, String> map = new HashMap<>();
3     map.put("INPUT",
4         "&&231817&1c9d79ea8dd4bc56fb7a7727a30366&1629886&mtop.tmall.inshopsearch.searchitems&1.
5         DvmObject<?> ret = JNICLibrary.callStaticJniMethodObject(
6             emulator, methodSign, 10401,
7             new ArrayObject(

```

```

8         vm.resolveClass("java/util/HashMap").newObject(map),
9         new StringObject(vm, "23181017"),
10        DvmInteger.valueOf(vm, 7),
11        null,
12        DvmBoolean.valueOf(vm, true)
13    ));
14
15    System.out.println("xiayu, getXSign.ret-10401: " + ret.getValue().toString());
}

```

```

    case "java/util/HashMap->keySet()Ljava/util/Set;": {
        HashMap<?, ?> map = (HashMap<?, ?>) dvmObject.getValue();
        return vm.resolveClass("java/util/Set").newObject(map.keySet());
    }
}

JNIEnv->GetStaticLongField(class com/alibaba/wireless/security/framework/SGPluginExtras, slot => 0x4146e0ee) was called from RX@0
[23:48:35 278] INFO [com.github.unidbg.linux.ARM32SyscallHandler:829] - pthread_clone child_stack=RW@0x415
JNIEnv->GetMethodID(java/lang/Integer.<init>(I)V) was called from RX@0x408b5aa7[libmain.so]@xb5aa7
JNIEnv->NewObject(class java/lang/Integer, <init>(<0x0>) => java.lang.Integer@5c0369c4) was called from RX@0x40811007[libmain.so]@
xiayu, initAvMp.ret-10102: 0
Find native function Java_com_taobao_wireless_security_adapter_JNICLibrary_doCommandNative(I[Ljava/lang/Object;)Ljava/lang/Object;
JNIEnv->GetObjectArrayElement([Ljava.util.HashMap@d70c189, "23181017", java.lang.Integer@17ed40e0, null, true], 0) was called from
[23:48:35 271] WARN [com.github.unidbg.linux.ARM32SyscallHandler:457] - handleInterrupt intno=2, NR=-10737
java.lang.UnsupportedOperationException: java/util/HashMap->keySet()Ljava/util/Set;
    at com.github.unidbg.linux.android.dvm.AbstractJni.callObjectMethod(AbstractJni.java:770)
    at com.xiaoyu.TianMaoXSign1.callObjectMethod(TianMaoXSign1.java:229)
    at com.github.unidbg.linux.android.dvm.AbstractJni.callObjectMethod(AbstractJni.java:786)

```

```

    case "java/util/Set->toArray()Ljava/lang/Object;": {
        Set<?> set = (Set<?>) dvmObject.getValue();
        Object[] array = set.toArray();
        DvmObject<?>[] objects = new DvmObject[array.length];
        for (int i = 0; i < array.length; i++) {
            if (array[i] instanceof String) {
                objects[i] = new StringObject(vm, (String) array[i]);
            } else {
                throw new IllegalStateException("array=" + array[i]);
            }
        }
        return new ArrayObject(objects);
    }
}

TianMaoXSign1
JNIEnv->GetStringUTFChars("6.4.34") was called from RX@0x408b53ef[libmain.so]@xb53ef
JNIEnv->ReleaseStringUTFChars("6.4.34") was called from RX@0x408b5405[libmain.so]@xb5405
JNIEnv->GetObjectArrayElement([Ljava.util.HashMap@d70c189, "23181017", java.lang.Integer@17ed40e0, null, true], 0) was called from RX@0x408b5405
JNIEnv->GetStringUTFChars("/data/user/0/com.tmall.wireless/app_SGLib/app_1627957761/main/libsgavmpso-6.4.34.so") was called from RX@0x408b5405
JNIEnv->ReleaseStringUTFChars("/data/user/0/com.tmall.wireless/app_SGLib/app_1627957761/main/libsgavmpso-6.4.34.so") was called from RX@0x408b5405
JNIEnv->GetStaticLongField(class com/alibaba/wireless/security/framework/SGPluginExtras, slot => 0x4146e0ee) was called from RX@0x40811007
[23:49:28 303] INFO [com.github.unidbg.linux.ARM32SyscallHandler:829] - pthread_clone child_stack=RW@0x41599938, th
JNIEnv->GetMethodID(java/lang/Integer.<init>(I)V) was called from RX@0x408b5aa7[libmain.so]@xb5aa7
JNIEnv->NewObject(class java/lang/Integer, <init>(<0x0>) => java.lang.Integer@5c0369c4) was called from RX@0x40811007[libmain.so]@xb11007
xiayu, initAvMp.ret-10102: 0
Find native function Java_com_taobao_wireless_security_adapter_JNICLibrary_doCommandNative(I[Ljava/lang/Object;)Ljava/lang/Object; => RX@0
JNIEnv->GetObjectArrayElement([Ljava.util.HashMap@d70c189, "23181017", java.lang.Integer@17ed40e0, null, true], 0) was called from RX@0x408b5405
JNIEnv->CallObjectMethod(java.util.HashMap@d70c189, keySet() => java.util.Set@50675690) was called from RX@0x408b6e43[libmain.so]@xb6e43
[23:49:28 305] WARN [com.github.unidbg.linux.ARM32SyscallHandler:457] - handleInterrupt intno=2, NR=-1073744232, sv
java.lang.UnsupportedOperationException: java/util/Set->toArray()Ljava/lang/Object;
    at com.github.unidbg.linux.android.dvm.AbstractJni.callObjectMethod(AbstractJni.java:770)
    at com.xiaoyu.TianMaoXSign1.callObjectMethod(TianMaoXSign1.java:233)
    at com.github.unidbg.linux.android.dvm.AbstractJni.callObjectMethod(AbstractJni.java:786)

```

```

    case "java/util/HashMap->get(Ljava/lang/Object;)Ljava/lang/Object;": {
        HashMap<?, ?> map = (HashMap<?, ?>) dvmObject.getValue();
        Object key = varArg.getObjectArg(index 0).getValue();
        Object obj = map.get(key);
        if (obj instanceof String) {
            return new StringObject(vm, (String) obj);
        } else {
            throw new IllegalStateException("array=" + obj);
        }
    }
}

TianMaoXSign1
JNIEnv->CallObjectMethod(java.util.HashMap@d70c189, keySet() => java.util.Set@50675690) was called from RX@0x408b6e43[libmain.s
JNIEnv->CallObjectMethod(java.util.Set@50675690, toArray() => ["INPUT"]) was called from RX@0x408b6e5f[libmain.so]@xb6e5f
JNIEnv->GetArrayLength(["INPUT"] => 1) was called from RX@0x408b6e6f[libmain.so]@xb6e6f
JNIEnv->GetObjectArrayElement(["INPUT"], 0) was called from RX@0x408b6f0d[libmain.so]@xb6f0d
JNIEnv->GetStringUTFChars("INPUT") was called from RX@0x408b537d[libmain.so]@xb537d
JNIEnv->ReleaseStringUTFChars("INPUT") was called from RX@0x408b53c7[libmain.so]@xb53c7
[23:50:08 682] WARN [com.github.unidbg.linux.ARM32SyscallHandler:457] - handleInterrupt intno=2, NR=-107
java.lang.UnsupportedOperationException: java/util/HashMap->get(Ljava/lang/Object;)Ljava/lang/Object;
    at com.github.unidbg.linux.android.dvm.AbstractJni.callObjectMethod(AbstractJni.java:770)
    at com.xiaoyu.TianMaoXSign1.callObjectMethod(TianMaoXSign1.java:246)
    at com.github.unidbg.linux.android.dvm.AbstractJni.callObjectMethod(AbstractJni.java:786)
    at com.github.unidbg.linux.android.dvm.DvmMethod.callObjectMethod(DvmMethod.java:78)
    at com.github.unidbg.linux.android.dvm.DalvikVM$28.handle(DalvikVM.java:487)

```

```

resolve.pathname: /data/user/0/com.tmall.wireless/files
resolve.pathname: /data/user/0/com.tmall.wireless/files
JNIEnv->NewStringUTF("ab205408098c7675f4cbd71d4b0f2791f34ceb601508fe63966") was called from RX@0x408b5561[libmain.so]@xb55
xiayu, getXSign.ret-10401: ab205408098c7675f4cbd71d4b0f2791f34ceb601508fe63966

```

上图环境报错全部补完之后, 就可以出结果了, 经过测试, 这个结果是可以使用的

这篇关于某宝系 tb tm sgmain x-sign 分析 - unidbg的文章就介绍到这儿，希望我们推荐的文章对大家有所帮助，也希望大家多多支持为之网！

原文链接: https://blog.csdn.net/qq_40000081/article/details/120147710

相关编程文章		更多>
别再手动处理数据了！FastGPT 这个新功能让你提前下班		2024-11-08
大厂算法入门详解		2024-11-05
朴素贪心算法入门详解		2024-11-05
深度优先遍历算法详解与实践教程		2024-11-05
初学者指南：轻松理解树形模型		2024-11-05
搜索算法入门指南：轻松掌握基础概念与实现方法		2024-11-05
算法入门指南：轻松掌握编程基础		2024-11-05
算法高级入门教程：从基础到进阶		2024-11-05
随机贪心算法入门教程		2024-11-05
贪心算法入门详解		2024-11-05