Nuwa详解

贾吉鑫

Android 类加载

ClassLoader

```
protected Class<?> loadClass(String className, boolean resolve) throws ClassNotFoundException {
    Class<?> clazz = findLoadedClass(className);
    if (clazz == null) {
        try {
            clazz = parent.loadClass(className, false);
        } catch (ClassNotFoundException e) {
            // Don't want to see this.
        }
        if (clazz == null) {
            clazz = findClass(className);
        }
    }
    return clazz;
}
```

BaseDexClassLoader(API 14)

```
@Override
protected Class<?> findClass(String name) throws ClassNotFoundException {
    Class clazz = pathList.findClass(name);
    if (clazz == null) {
        throw new ClassNotFoundException(name);
    }
    return clazz;
}
```

DexPathList

```
public Class findClass(String name) {
    for (Element element : dexElements) {
        DexFile dex = element.dexFile;
        if (dex != null) {
            Class clazz = dex.loadClassBinaryName(name, definingContext);
            if (clazz != null) {
                return clazz;
            }
        }
    }
    return null;
}
```

热补丁

思路

patch.dex插入到dexElements的最前面

问题

```
E/AndroidRuntime: java.lang.IllegalAccessError: Class ref in pre-verified class resolved to unexpected implementation
E/AndroidRuntime:     at cn.jiajixin.nuwasample.MainActivity.onCreate(Unknown Source)
E/AndroidRuntime:     at android.app.Activity.performCreate(Activity.java:5274)
E/AndroidRuntime:     at android.app.Instrumentation.callActivityOnCreate(Instrumentation.java:1087)
E/AndroidRuntime:     at android.app.ActivityThread.performLaunchActivity(ActivityThread.java:2158)
E/AndroidRuntime:     at android.app.ActivityThread.handleLaunchActivity(ActivityThread.java:2253)
E/AndroidRuntime:     at android.app.ActivityThread.access$800(ActivityThread.java:145)
E/AndroidRuntime:     at android.app.ActivityThread$H.handleMessage(ActivityThread.java:1206)
E/AndroidRuntime:     at android.os.Handler.dispatchMessage(Handler.java:102)
E/AndroidRuntime:     at android.os.Looper.loop(Looper.java:136)
E/AndroidRuntime:     at android.app.ActivityThread.main(ActivityThread.java:5128)
E/AndroidRuntime:     at java.lang.reflect.Method.invokeNative(Native Method) <1 internal calls>
E/AndroidRuntime:     at com.android.internal.os.ZygoteInit$MethodAndArgsCaller.run(ZygoteInit.java:893)
E/AndroidRuntime:     at com.android.internal.os.ZygoteInit.main(ZygoteInit.java:702)
E/AndroidRuntime:     at dalvik.system.NativeStart.main(Native Method)
```

原因

1. A和所有直接引用类同dex，则ISPREVERIFIED

2. A引用B，替换B，则报错

如果没有类直接引用A，或者直接引用A的类没有被标记，则A可被直接替换

新思路

防止CLASS_ISPREVERIFIED：

1. hack.dex中Hack.class

2. 所有类构造函数中引用Hack.class

3. application中加载hack.dex,不引用Hack.class

实现

Nuwa Gradle

1. 构造函数中引用Hack类

怎么找到全部Class?

PreDex

ProGuard

MultiDex

如何修改字节码?

Grade>Lint>ASM

自动生成ASM代码?

```
java -classpath asm-all-3.2.jar:asm-util-3.2.jar:nb.jar
org.objectweb.asm.util.ASMifierClassVisitor
com.dianping.v1.NB
```

引用Hack类

```
private static byte[] referHackWhenInit(InputStream inputStream) {
    ClassReader cr = new ClassReader(inputStream);
    ClassWriter cw = new ClassWriter(cr, 0);
    ClassVisitor cv = new ClassVisitor(Opcodes.ASM4, cw) {
        @Override
        public MethodVisitor visitMethod(int access, String name, String desc,
                                         String signature, String[] exceptions) {

            MethodVisitor mv = super.visitMethod(access, name, desc, signature, exceptions);
            mv = new MethodVisitor(Opcodes.ASM4, mv) {
                @Override
                void visitInsn(int opcode) {
                    if ("<init>".equals(name) && opcode == Opcodes.RETURN) {
                        super.visitLdcInsn(Type.getType("Lcn/jiajixin/nuwa/Hack;"));
                    }
                    super.visitInsn(opcode);
                }
            }
            return mv;
        }

    };
    cr.accept(cv, 0);
    return cw.toByteArray();
}
```

2. 生成Patch

ProGuard

- mapping.txt，混淆前后对照表
- 同样的代码混淆，mapping.txt相同

applymapping

C>a：

加入B，则B>a,C>b

加入B，-applymapping，则C>a,B>b

Class Hash

- 记录引用Hack类的sha1
- 增加或者改变

dx

dx --dex --output=patch.apk patch

如何编写Gradle Plugin?

参考资料

1. 构建神器Gradle：http://t.cn/RLHdj57

2. Writing Custom Plugins：http://t.cn/RUQtnJp

numa extension

- includePackage:HashSet<String> //只fix自己代码
- excludeClass:HashSet<String> //去除Application
- debugOn:boolean //nuwa几秒额外耗时

Nuwa

1. 注入hack.apk

- library project支持assets，.jar结尾不好使
- attachBaseContext注入

2. 注入patch.jar

类已加载，需要重启生效

Later Plan

- 版本管理
- 安全性，加签名，dex and odex
- 新增Task，加快编译
- dex inject支持V14以下

Q&A