



2016 杭州·云栖大会
THE COMPUTING CONFERENCE

云栖社区
yq.aliyun.com

APP加固新方向 --混淆和瘦身

闵振飞 (陵轩)
2016.10

2016
The Computing Conference

主办单位:



战略合作伙伴:



扫码观看大会视频

目录

CATALOG

□ 加固的意义

□ 传统加固

□ 全量混淆

□ 优化瘦身

□ Q&A



加固的意义

- JAVA语言编写，开发门槛低，容易被反编译
- Android市场混乱，且可自签名，导致大量应用被二次打包，植入广告、木马
- 手机Root后，利用HOOK等技术手段对应用进行动态攻击



目录

CATALOG

□ 加固的意义

□ 传统加固

□ 全量混淆

□ 优化瘦身

□ Q&A



加固和脱壳技术的发展

第一代

1. Dex加密存储，解密时落地
2. 自定义DexClassLoader

脱壳方法

HOOK文件操作函数，read、write、delete



加固和脱壳技术的发展

第一代升级版

1. Dex加密存储，解密时不落地
2. 自定义DexClassLoader

脱壳方法

内存dump法

HOOK dvmDexFileOpenPartial

```
int dvmDexFileOpenPartial(const void* addr, int len, DvmDex** ppDvmDex)
{
    DvmDex* pDvmDex;
    DexFile* pDexFile;
    int parseFlags = kDexParseDefault;
    int result = -1;

    /* -- file is incomplete, new checksum has not yet been calculated
    if (gDvm.verifyDexChecksum)
        parseFlags |= kDexParseVerifyChecksum;
    */

    pDexFile = dexFileParse((u1*)addr, len, parseFlags);
    if (pDexFile == NULL) {
        ALOGE("DEX parse failed");
        goto bail;
    }

    pDvmDex->isMappedReadOnly = false;
    *ppDvmDex = pDvmDex;
    result = 0;

bail:
    return result;
}
```

```
auto fp, dexAddress;
fp = fopen("/Users/mzf/unpack/test.so", "wb");
for ( dexAddress=0x4018d000; dexAddress < 0x401b38e0; dexAddress++)
    fputc(Byte(dexAddress), fp);
```



加固和脱壳技术的发展

第二代

1. Dex Method方法抽离
2. Dex加载不连续

第三代

1. Dex Method方法抽离
2. Dex执行中动态解密

```
CaptureActivity.class  ChangeABTestParam.class  MainActivity.class x
protected void onCreate(Bundle paramBundle)
{
}

protected void onDestroy()
{
}

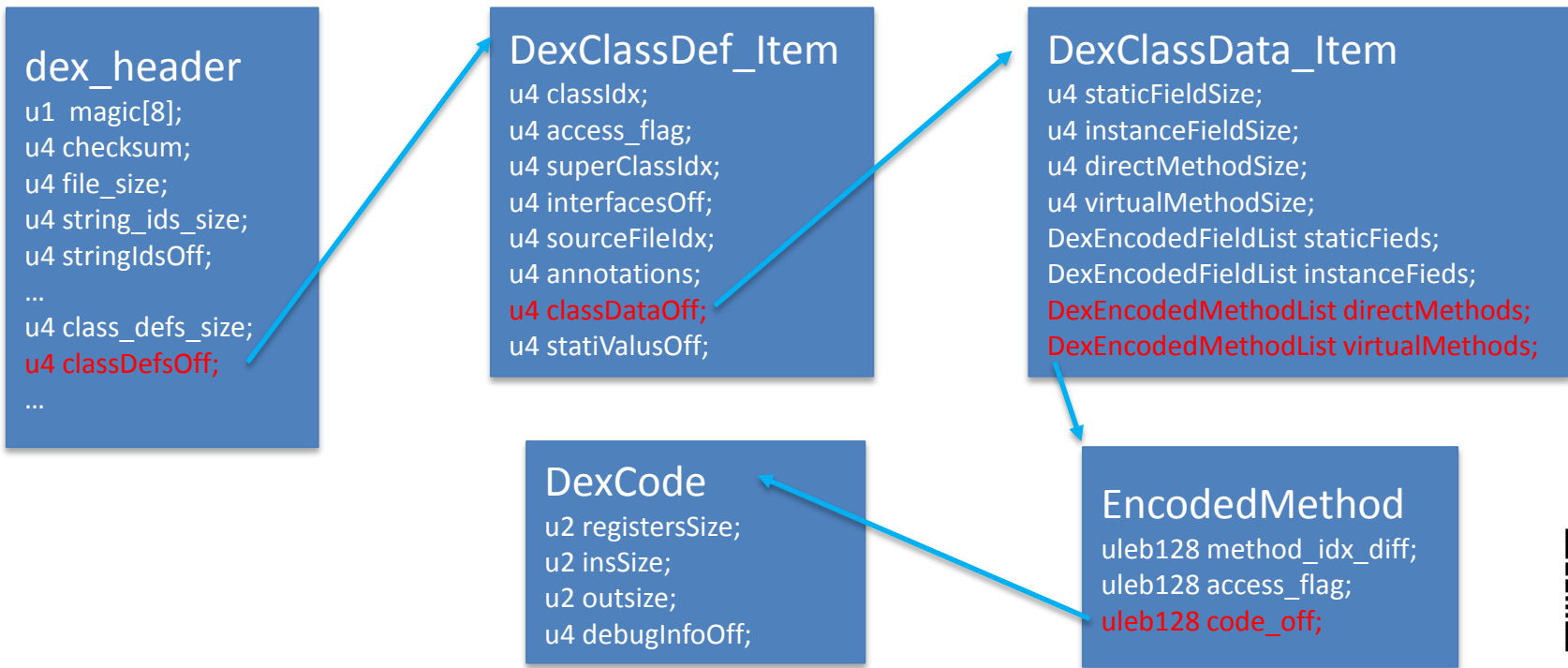
protected void onNewIntent(Intent paramIntent)
{
}

protected void onPause()
{
}

protected void onResume()
{
}
```



DEX结构



传统加固的挑战

容易被脱壳，脱壳类教程非常多

!	原	【原创】腾讯加固脱壳 (1 2)	0
+		【原创】**应用加固的脱壳分析和修复 (1 2 3 4)	0 0 精
!		【原创】360加固成功脱壳 (1 2 3 4)	0 0
!		【招聘】【阿里移动PP助手】马先生给的福利多到你想不到 逆向和安全程序猿快到碗里来	
!		【原创】某加固保动态脱壳 (1 2 3)	0 关注
!	👤	【求助】那位大师帮忙脱壳（阿里加固）	0
!		【原创】几维so加固脱壳 (1 2)	0
!		【求助】360加固	
!		【原创】Xdex（百度版）脱壳工具基本原理 (1 2 3)	0 0 优秀
+		【原创】Android dex文件通用自动脱壳器 (1 2 3 4 5 6 7 ... 10)	0 精

通用脱壳机可轻易脱大部分壳

zjdroid:

<https://github.com/BaiduSecurityLabs/ZjDroid>

DexHunter:

<https://github.com/zyq8709/DexHunter>



扫码观看大会视频

目录

CATALOG

□ 加固的意义

□ 传统加固

□ 全量混淆

□ 优化瘦身

□ Q&A



ProGuard混淆

```
release {
    minifyEnabled true
    proguardFiles getDefaultProguardFile('proguard-android.txt'), 'proguard-rules.pro'
}
```

meilishuo

a

app

a

activity

CaptureActivity

ChangeABTestParam

ChangeStandardEnvironment

EmptyActivity

FirstSellActivity

MainActivity

PrivateMessageThreadActivity

UploadActivity

UserIdActivity

WebActivity

WelcomeActivity

a

aa

ab

ac

af

ag

ah

b

c

d

e

f

CaptureActivity.class

ChangeABTestParam.class

MainActivity.class

```

protected void onCreate(Bundle paramBundle)
{
    g locala = c.b.b.b.b.a(c, this, this, paramBundle);
    a(this, paramBundle, locala, com.meilishuo.app.g.b.a(), null, c, locala);
}

protected void onDestroy()
{
    g locala = c.b.b.b.b.a(h, this, this);
    e(this, locala, com.meilishuo.app.g.b.a(), null, h, locala);
}

protected void onNewIntent(Intent paramIntent)
{
    g locala = c.b.b.b.b.a(i, this, this, paramIntent);
    a(this, paramIntent, locala, com.meilishuo.app.g.b.a(), null, i, locala);
}

protected void onPause()
{
    g locala = c.b.b.b.b.a(f, this, this);
    c(this, locala, com.meilishuo.app.g.b.a(), null, f, locala);
}

protected void onResume()
{
    g locala = c.b.b.b.b.a(e, this, this);
    b(this, locala, com.meilishuo.app.g.b.a(), null, e, locala);
}

```

```

-keepclassmembers class * {
    public <init> (org.json.JSONObject);
}

-keep public class net.secsoft.globalfly.R${
public static final int *;
}

-keepclassmembers enum * {
    public static **[] values();
    public static ** valueOf(java.lang.String);
}

-keep class com.baidu.** {*; }
-keep class vi.com.** {*; }
-dontwarn com.baidu.**

# bugly
-dontwarn com.tencent.bugly.**
-keep public class com.tencent.bugly.** {*; }

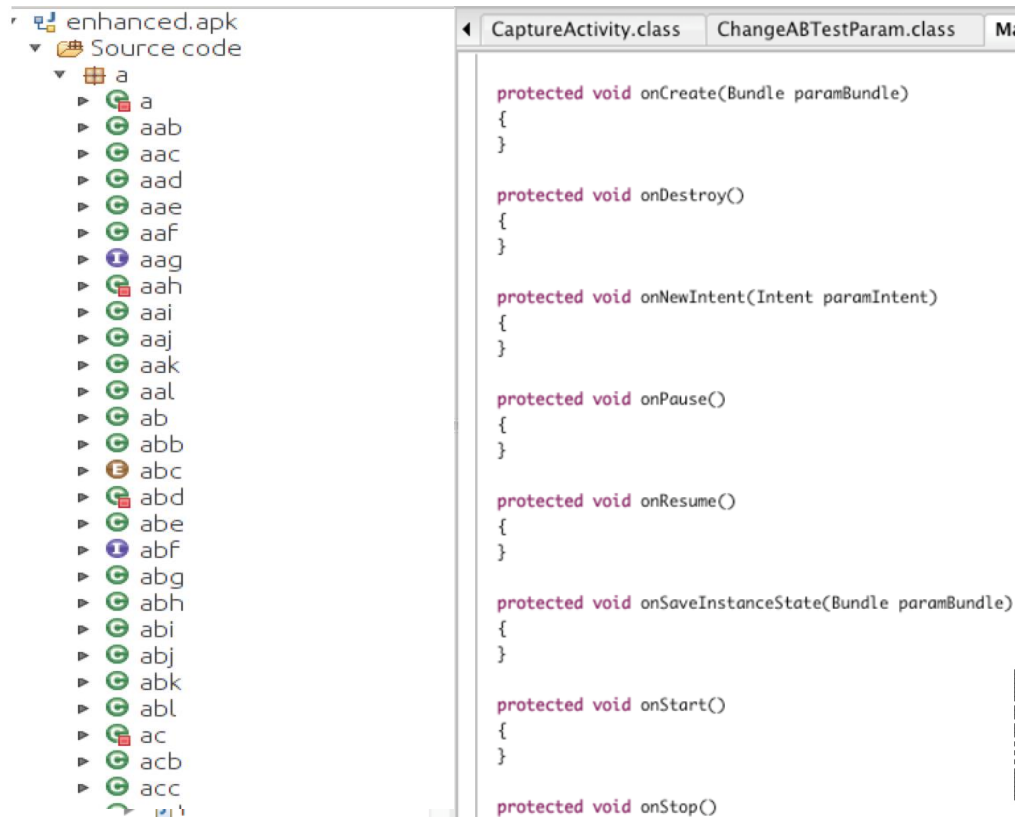
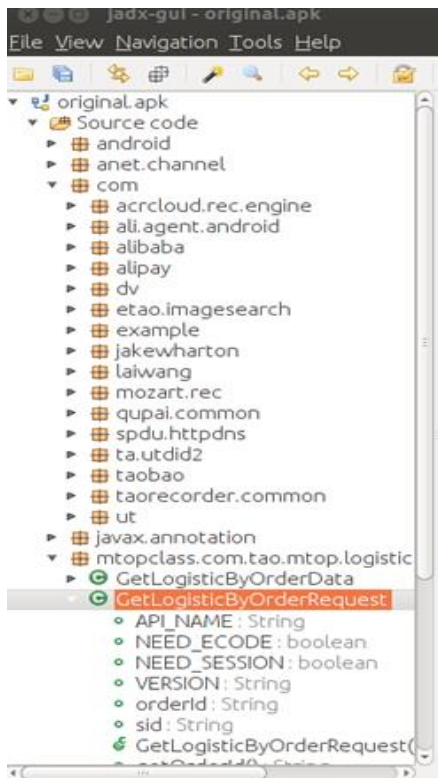
-keep public class c.b.** {*; }
-keep public class c.b.a.** {*; }

-ignorewarnings

-keepattributes Signature
```



全量混淆



目录

CATALOG

□ 加固的意义

□ 传统加固

□ 全量混淆

□ 优化瘦身

□ Q&A

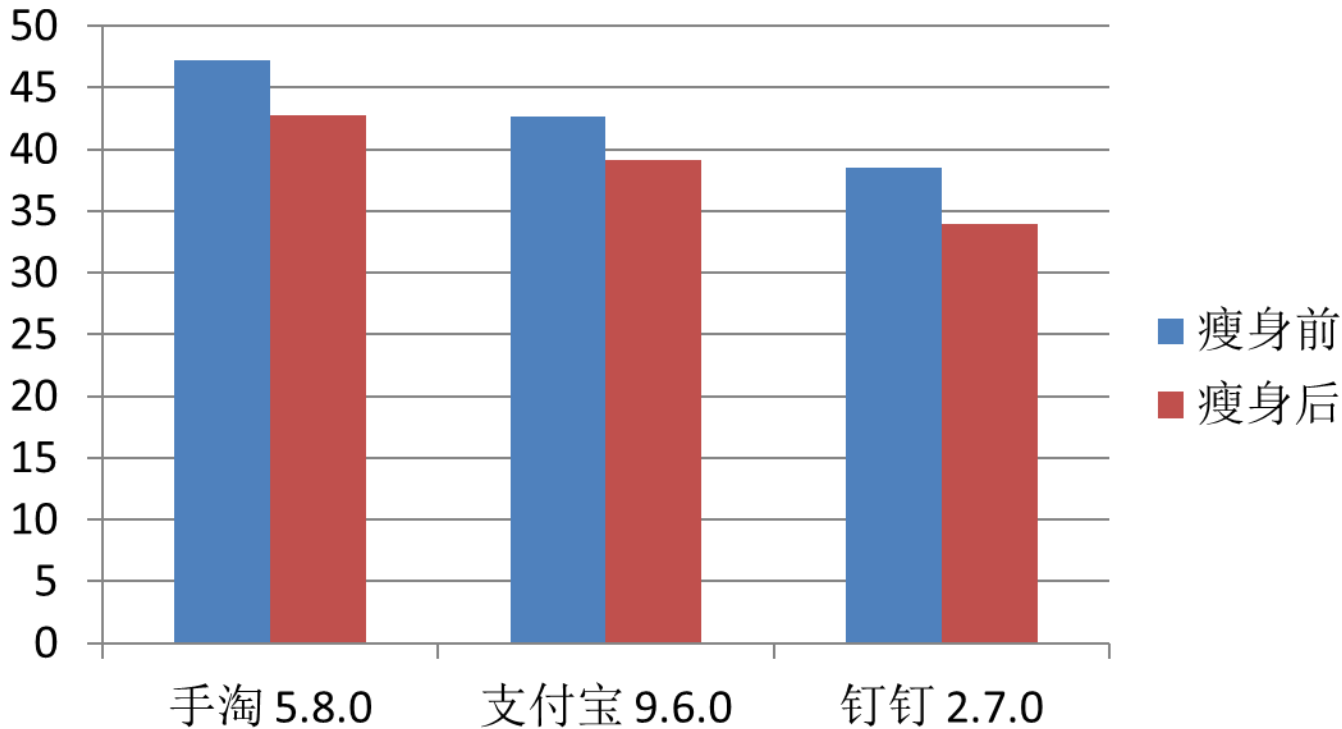


优化瘦身

- Dex文件debug信息清除，减少编译器自动产生的函数，优化性能，减少体积。
- 通过java层拦截技术，对so进行重新打包压缩，减少体积。
- 修改 android 应用资源名称，减少应用体积，提高资源保护强度。
- 开发7z工具，对签名后的apk包重新压缩，达到进一步减少体积的目的。



优化瘦身



注：基准包来源
摩天轮打包平台和
支付宝cp平台



优化瘦身

应用名	原始大小 (字节)	优化后大小 (字节)	减少百分比
微博	49814631	43694900	12.29%
百度地图	56679325	50210909	11.42%
唯品会	24585845	20744044	15.66%
美团外卖	21000244	17473964	16.81%
今日头条	23432134	18681124	20.27%
华为账号	14526281	8117842	44.12%
优酷视频	38464866	28929039	24.78%
大众点评	19965701	15948756	21.18%
百度视频	27116288	23781210	12.32%



目录

CATALOG

□ 加固的意义

□ 传统加固

□ 全量混淆


□ 优化瘦身

□ Q&A




Q & A



 阿里聚安全
官方微博



 阿里聚安全
微信公众号



扫码观看大会视频

2016 The
Computing
Conference
THANKS

