App Extension的脱壳办法

时间：15-03-12 10:56:42 点击：3379 来源:念茜的博客

从app store下载的app和app extension是加过密的，可以通过otool查看:

```
$ otool -l binary_name | grep crypt

cryptoff  16384
cryptsize 294912
cryptid   1
```

iPhone applications的解密办法

dumpdecrypted 是个出色的app脱壳开源工具，它的原理是：将应用程序运行起来（iOS系统会先解密程序再启动），然后将内存中的解密结果dump写入文件中，得到一个新的可执行程序。

iPhone app extensions的特别之处

app extension虽是独立进程，但不可独立运行

iPhone app extensions的解密办法

通过对dumpdecrypted稍作修改，更改其写入dump结果的path，变通启动方式就可实现对app extension的解密，详见：Carina's dumpdecrypted

使用方法很简单，用微信的Share Extension为例

1）本地编译好 dumpdecrypted.dylib

2）指定作用的Extension Bundle

```
{
Filter = {
Bundles = ("com.tencent.xin.sharetimeline");
};
```

```
}
```

3）将 dumpdecrypted.plist 和 dumpdecrypted.dylib 拷贝至越狱机的 /Library/MobileSubstrate/DynamicLibraries/ 下

4）利用系统相册启动微信的Share Extension

当微信的Share Extension被启动时，解密插件自动工作。值得注意的是，如果你的越狱机是armv7架构，那么也就只dump armv7那部分；如果越狱机是arm64架构，那么也就只dump arm64那部分。So，最后你需要:

```
$ lipo -thin armv7 xxx.decrypted -output xxx_armv7.decrypted
```

或

```
$ lipo -thin armv64 xxx.decrypted -output xxx_arm64.decrypted
```

来得到干净的dump结果