iOS代码加密的几种方式

技术那些事 / 2017-09-13 08:59:29 / 浏览数 3011 安全技术 技术讨论 顶(0) 踩(0)

众所周知的是大部分iOS代码一般不会做加密加固，因为iOS
APP一般是通过AppStore发布的，而且苹果的系统难以攻破，所以在iOS里做代码加固一般是一件出力不讨好的事情。万事皆有例外，不管iOS、adr还是js，加密的目的是为

iOS代码加密的几种方式

1.字符串加密
字符串会暴露APP的很多关键信息，攻击者可以根据从界面获取的字符串，快速找到相关逻辑的处理函数，从而进行分析破解。加密字符串可以增加攻击者阅读代码的难度以
一般的处理方式是对需要加密的字符串加密，并保存加密后的数据，再在使用字符串的地方插入解密算法。简单的加密算法可以把NSString转为byte或者NSData的方式，还

2.符号混淆
符号混淆的中心思想是将类名、方法名、变量名替换为无意义符号，提高应用安全性；防止敏感符号被class-dump工具提取，防止IDA
Pro等工具反编译后分析业务代码。目前市面上的IOS应用基本上是没有使用类名方法名混淆的。

a. 别名
在编写代码的时候直接用别名可能是最简单的一种方式，也是比较管用的一种方式。因为你的app被破解后，假如很容易就能从你的类名中寻找到蛛丝马迹，那离hook只是一

b.C重写
编写别名的方式不是很易读，而且也不利于后续维护，这时你可能需要升级一下你的保护方式，用C来重写你的代码吧。这样把函数名隐藏在结构体中，用函数指针成员的形
from 念茜)。如下例子：

c.脚本处理
稍微高级一点的是脚本扫描处理替换代码，因为要用到linux命令来编写脚本，可能会有一点门槛，不过学了之后你就可以出去吹嘘你全栈工程师的名头啦。。。
linux脚本比较常用的几个命令如下：

脚本混淆替换是用上述几个命令扫描出来需要替换的字符串，比如方法名，类名，变量名，并做替换，如果你能熟练应用上述几个命令，恭喜你，已经了解了脚本的一点皮毛
如以下脚本搜索遍历了代码目录下的需要混淆的关键字：

替换的方式可以直接扫描文件并对文件中的所有内容替换，也可以采用define的方式定义别名。例如：

d.开源项目ios-class-guard
该项目是基于class-dump的扩展，和脚本处理类似，是用class-dump扫描出编译后的类名、方法名、属性名等并做替换，只是不支持隐式C方法的替换，有兴趣的同学可以

3.代码逻辑混淆
代码逻辑混淆有以下几个方面的含义：
对方法体进行混淆，保证源码被逆向后该部分的代码有很大的迷惑性，因为有一些垃圾代码的存在；
对应用程序逻辑结构进行打乱混排，保证源码可读性降到最低，这很容易把破解者带到沟里去；
它拥有和原始的代码一样的功能，这是最最关键的。
一般使用obfuscator-llvm来做代码逻辑混淆，或许会对该开源工具做个简单介绍。

4.加固SDKadr中一般比较常见的加固等操作，iOS也有一些第三方提供这样的服务，但是没有真正使用过，不知道效果如何。当然还有一些第三方服务的加固产品，基本上都
iOS加密可能市场很小，但是存在必有道理，在越狱/开源/极客的眼中，你的APP并没有你想像的那么安全，如果希望你的代码更加安全，就应给iOS代码加密。

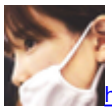
上一篇：Catfish-4.5.7利用TP... 下一篇：关于浏览器的一些问题

1. 2 条回复

技术那些事 2017-09-20 07:57:39

菜鸟初入门槛，水平所限，写的比较浅显，还请大神勿喷。

0 回复Ta

 hades 2017-09-20 09:22:02

不喷~在某些领域 都是菜鸡

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板