破解Revealapp的试用时间限制

Revealapp作为分析iOS app UI结构的利器，还是非常称手的，89刀的价格也是物有所值。本文分析其试用版时间限制，只是用于学习，如果一直用，还是买个licence支持一下吧。

试用版有30天的时间限制，既然是30天时间限制，肯定每次启动是要读当前时间的啰。所以最简单的hack方法就是修改系统时间。如果这种方法可以接受，就不用往下看了。

如果你的工作严重依赖于Calendar，那么修改系统时间的方法就是不可以接受的。下面的追踪过程包含了对双精度浮点数在内存中的表示、ObjC对象模型等问题的讨论，如果不感兴趣可直接跳到文末查看最终的解决方案。

开始的尝试

用dtruss看了下启动时调用的syscall，是没有网络通讯的，说明app的安装时间不可能是从网络读下来的，那么这个时间肯定是写在本地的文件系统。

用opensnoop看了下启动时Reveal读过的所有文件，没有值得注意的地方。最后的发现证实这个思路忽略了一个问题，一个app读的文件并不一定是它自己打开的，可以是进程间通信。

这些简单的尝试失败后，就只能老老实实的分析代码了。

从关键字开始

试用版的Reveal有提醒试用剩余时间的信息在窗口的右上角”Free trial ends in xx days”（我觉得这不是一个好的设计，这句话似乎时刻挑衅着使用者：“来呀，你来hack我呀”）。“trial”是我感兴趣的关键字，除了在数据段肯定能找到这个关键字以外，说不定在ObjC的运行时类型系统中还能有意外的收获。果真，Reveal没有对类型信息进行模糊处理，在class-dump生成的头文件中发现了：
-[IBARegistrationPreferencesViewController messageForTrialDaysRemaining:(long long)arg1]
从函数名来看它应该就是生成试用剩余时间字符串的。

上GDB，单步跟踪，

0x000000010008bd34 push rbp
0x000000010008bd3f move rbx, rdx ; rdx 就是还剩下的试用天数，也就是函数的参数arg1

以此为突破口，发现下面的小段代码。

0x00000001000872cd call 0x100086ec2
0x00000001000872d2 mov rcx, rax ; rax中是上面函数返回的已过去的天数
0x00000001000872d7 mov eax, 0x1e ; 0x1e=30 30天的限制
0x00000001000872dc sub rax, rcx ; 30减去已经过去的天数的，减出来就是还剩下的天数

再往下走，需要分析的数据不再像是“天数”这样的整数，而是像软件安装日期NSDate这样的对象，特征不明显。所以就有必要清楚NSDate这个对象中日期的表示方法。

内存中的NSDate对象

NSDate对象应该有两个域，第一个“isA”是所有ObjC对象都有的类型指针，指向NSDate类型对象。第二个是个双精度浮点数，表示从2001年1月1日到现在的时间间隔，单位是秒。

pointer: isA
double: _timeIntervalSinceReferenceDate

其实isA指针就是NSDate对象的特征，所有的NSDate对象都是以相同的8个字节开始。第二个域是一个浮点数，分两步把它转换为一个日期。

第一步，十六进制浮点数转换为十进制

双精度浮点数由8个字节构成，1个bit表示符号，11个bit表示指数，剩下的52位用来表示底数。
使用python可以方便的把8字节的十六进制浮点数转换为十进制数：
struct.unpack('<d','c3b72c7a9ebfb841'.decode('hex'))[0]

在gdb中，可以直接使用命令
p *(double*)(NSDate指针地址+8)

第二步，秒数转换为日期

NSDate *date = [NSDate
dateWithTimeIntervalSinceReferenceDate:415285808.20822901];
NSLog(@"\n%@", date);

使用上面的方法，可以在跟踪汇编代码的时候检查内存中的NSDate对象，以及它所表示的日期。（这需要点耐心）

最终，安装Reveal的时间第一次出现在内存中的位置被找到，这个位置所在的函数显然负责把存在文件某处的一个magic number转换为软件安装日期。

但是意料之外的是，这个想像中的magic number并不magic，它仅仅是存在user default的plist文件中的一项，而且就是安装日期的双精度浮点数的十六进制表示。

结论

所以，要想永久试用Reveal，只需要打开

~/Library/Preferences/com.ittybittyapps.Reveal.plist

把IBAApplicationPersistenceData这一项删除就是了。

后记

有同学留言说上面的方法不起作用(问题的原因请参考另一篇blog谁动了我的plist)，于是叽歪刘写了个补丁。

补丁是用10.9的SDK编译的，在Reveal1.0.3（2287）上测试通过。

下载解压后，用右键的“打开”菜单运行程序。亲，叽歪刘只能帮你到这里了。

更多叽歪：

- 2015-06-17 » 一种应用内付费(IAP)的破解方法
- 2015-04-19 » 谁动了我的plist
- 2015-02-19 » 羊年大年初一阳澄湖飞行

被顶起来的评论

wangjiebo
可惜来晚了点，现在更新1.0.4了，这个方法不管用了
2014年5月9日 回复 顶(1) 转发

33 条评论 12 条新浪微博 最新 最早 最热


移动开发小冉
逆向思维值得学习，建议大家买licence
2014年3月10日 回复 顶 转发

coder
貌似不起作用。
2014年3月10日 回复 顶 转发

Aster0id
Preferences下没有找到这个pist文件
2014年3月12日 回复 顶 转发

迅乎电驰
不起作用。
2014年3月20日 回复 顶 转发

迅乎电驰
试试你编译的这个，谢啦
2014年3月20日 回复 顶 转发

IOS-Coding
博主V5
2014年3月20日 回复 顶 转发

可可不是糖
这...
2014年3月24日 回复 顶 转发

lonelysoul
膜拜
2014年3月25日 回复 顶 转发

Aster0id
博主V5, 博主能不能把注册机的源码放一下,我想学习学习
2014年3月25日 回复 顶 转发

磊哥在纽约

博主，plist方法不管用，不过用了你的注册机，果然可用。
我想问一下，学习汇编是否对开发有帮助？有时候出错代码都是汇编，看不懂，找了很久也不一定找出错误。比如我的CoreData多线程下面的错误，用了别人的库文件，出错了也不知道什么原因，找了很多天，最后还是通过找到了人家的开源代码才调试成功。如果能从单步跟踪找出错误，是不是会更加好？所以想请教一下，有哪些是值得学习能帮助开发的知识？ 这里不常来，如果方便也可邮件赐教：derek.designer[at]gmail.com

2014年4月6日 回复 顶 转发

叽歪刘

回复 磊哥在纽约: 回答你的第一个问题： “学习汇编是否对开发有帮助？”
我的回答是肯定的.
从小处讲，在调试代码的时候是用得着汇编的知识的。举两个例子：
1. v = func1() + func2()
如果有人写了上面的语句，func1()和func2()都是没有源代码的库函数，调试的时候得出来的v的值跟想像的不一样，怎么知道两个函数分别返回的是多少呢？
当然好点的IDE会给出两个函数的返回值，不过如果懂汇编的话，自己就能分析。

2. crash stack
对于从用户那里拿到的crash stack，会指出最后crash的地方是某个函数 + 一个地址偏移。如果懂汇编，我们就能知道crash的地方大概在函数的哪个位置。

从大处讲，汇编是软件和硬件之间的接口，如果要对整个计算机系统有个全面清晰的认识，而不是仅仅做个Code Monkey，懂得汇编是必须的。

回答你的第二个问题，对于你遇到的CoreData多线程下的一个开源库的错误。
对于这类问题，可以试着看看出错处的汇编是否对解决问题有帮助，如果答案是否定的，不需要纠结在汇编上，因为其实你有更好的选择，那就是能够得到源代码。得到所有能得到的源代码，并且建立起便于调试的开发环境，虽然要费点精力和时间，但是对以后的排错是大有裨益的，正所谓磨刀不误砍柴工。

回答你的第三个问题， “有哪些是值得学习能帮助开发的知识？”
在用RevealApp的同学，我想都是开发Native Application的，所以Web App就不在讨论之列。对于开发Native App，我想到的能帮助开发的知识，无非就是操作系统、编译原理、语言本身和要解决问题的领域知识。

希望我的回答对你有帮助。

2014年4月6日 回复 顶 转发

Esay

貌似把 ~/Library/Preferences/com.ittybittyapps.Reveal.plist 删除了就能再用 30 天。

2014年4月9日 回复 顶 转发

刘云鹏

博主，请教一下，为什么我这边昨天用的时候还正常，今天再用的时候发现真机怎么也连接不上，两个设备确定连的都是同一个无线网，用模拟器的话能连接上

2014年4月9日 回复 顶 转发

isaced

过程值得学习，但鼓励正版！

2014年4月10日 回复 顶 转发

Mrshyi

赞 亲测注册机可用 已转载到：http://iosre.com/forum.php?mod=viewthread&tid=133&extra=page%3D1

2014年4月10日 回复 顶 转发

东邪向东斜

JY实在太可爱了。

2014年4月10日 回复 顶 转发

阿弥妥佛

对应reveal的试用版要放到application中去才能成功，放在桌面上去破解不成功。不懂注册机的具体原理，是否能讲解下！

2014年4月11日 回复 顶 转发

挡不住的君文

电脑还是ML的，注册没法使用，能够打包一个支持10.8的？楼主

2014年4月14日 回复 顶 转发

开心赚

不错,支持

2014年4月14日 回复 顶 转发

风云

多谢博主！

2014年4月17日 回复 顶 转发

风云

多谢博主！

2014年4月17日 回复 顶 转发

勇敢有力

楼主你好，我想请问下你怎么用gdb调试reveal的，因为我试着用lldb的 attach -p （pid）命令，reveal的进程都会自动关闭掉，不知道怎么下手

2014年4月18日 回复 顶 转发

zhouleyu

逆向思维值得学习，建议大家买licenc

2014年4月25日 回复 顶 转发

wangjiebo

可惜来晚了点，现在更新1.0.4了，这个方法不管用了

2014年5月9日 回复 顶(1) 转发

墨和米说

有人放一个1.0.3的版本下载地址吗?

2014年5月29日 回复 顶 转发

郭琦

坐等更新

2014年6月17日 回复 顶 转发

随变混混

果然是IOS UI分析神器，求10.4版的注册机

2014年6月19日 回复 顶 转发

随变混混

求楼主给个 10.3的reveal,网上下不到了，邮箱hhlai1990@163.com

2014年6月19日 回复 顶 转发

李剑飞

求楼主给个 10.3的reveal,网上下不到了，280820669@qq.com

2014年6月20日 回复 顶 转发

于满洋

1.0.3的reveal：http://pan.baidu.com/wap/link?uk=2466567715&shareid=2220438916&third=0
不过不支持最新版的xcode喽
楼主能写个1.0.4版的注册机吗?

2014年7月8日 回复 顶 转发

→→→点我*推倒萝莉或者被御姐推到

呵呵

2014年7月9日 回复 顶 转发

emp_heng

能给讲下注册机的原理吗？楼主

2014年7月18日 回复 顶 转发

L

回复 叽歪刘: 博主，我来当一次伸手党吧，能帮忙破解一下Reveal1.0.5吗？实在找不到1.0.3了，个体户不给力，买不起软件，很可怜的

2014年9月19日 回复 顶 转发

社交帐号登录: 微博 QQ 人人 豆瓣 更多»