

zhangmiaoping23的专栏

目录视图

摘要视图

RSS 订阅

个人资料

访问: 267629次

积分: 4745

等级:

排名: 第2690名

原创: 176篇

转载: 235篇

译文: 1篇

评论: 84条

文章搜索

文章分类

C++与汇编 (75)

LINUX 内核编程 (6)

MFC学习 (17)

STL学习 (1)

代码阅读 (6)

工作经验 (86)

毕业设计--C++异常处理机制的实现 (8)

面试题目录 (10)

黑客-攻与防 (11)

windows驱动 (2)

QT编程 (4)

设计模式 (8)

看雪转载笔记 (39)

逆向 (47)

android 逆向 (52)

反调试 (7)

ios (17)

加解密算法 (5)

ios逆向 (26)

反编译 (2)

android root技术 (12)

漏洞 (3)

android 安全 (7)

爱加密 (2)

Windows开发 (1)

Windows逆向 (5)

协议分析 (1)

Android加固 (5)

梆梆加固 (1)

爱加密 (1)

CSDN博乐 举荐之美 公益活动, 感谢你们 3D游戏引擎实战班4个月只需1999元! 新版极客头条上线, 每天一大波干货

[软件工具] 一步一步用debugserver + lldb代替gdb进行动态调试

分类: ios逆向 2014-06-25 20:24 1908人阅读 评论(0) 收藏 举报

因为Apple已经弃gdb投lldb, 所以随着我动态调试的次数越来越频繁, gdb上一个接一个的bug经常会让人很恼火。既然苹果打算建立自己的调试器王国, 也投入了钱力精力, 那我们干脆也上手lldb玩玩, 看看lldb是不是比gdb要更好用 (以下按照iphonedevwiki)

一、定制lldb

1. 下载一个能用的ldid, 位置, 如/opt/theos/bin/ldid;

2. 将iOS中的/Developer/debugserver拷贝到OSX中, 为其减肥。假定你的iDevice处理器是armv7s, 则运行

01. lipo -thin armv7s /path/to/debugserver -output /path/to/debugserver

复制代码

生成只包含armv7s指令的debugserver;

3. 将下面的内容另存为一个名为ent.xml的文件

01. <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">

02. <plist version="1.0">

03. <dict>

04. <key>com.apple.springboard.debugapplications</key>

05. <true/>

06. <key>get-task-allow</key>

07. <true/>

08. <key>task_for_pid-allow</key>

09. <true/>

10. <key>run-unsigned-code</key>

11. <true/>

12. </dict>

13. </plist>

复制代码

4. 给debugserver签上必须的entitlements。运行

01. /path/to/ldid -S/path/to/ent.xml /path/to/debugserver

复制代码

5. 将定制好的debugserver拷贝回iOS, 笔者习惯放在/usr/bin/debugserver下。

二、在iOS上用debugserver来attach进程

debugserver + lldb调试方法跟gdb最大的不同, 在于前者是用OSX中的lldb远程连接debugserver, 由debugserver作为lldb和iOS的中转, 在执行命令和返回结果; 而后者是gdb直接运行在iOS上。但对于一般的开发者来说, 这个区别跟我们没有鸟关系, 只管用就好~

在iOS上运行下面的命令来attach进程, 其中1234是我们指定的端口号:

http://blog.csdn.net/zhangmiaoping23/article/details/34501837

1/4

文章存档

2015年07月 (6)

2015年06月 (12)

2015年05月 (14)

2015年04月 (10)

2015年03月 (17)

展开

阅读排行

美女薄情馆6.7.0破解VIP (8163)

CFileFind类 (5945)

安卓微信数据库解密 (4003)

常用android的smali注入 (3759)

破解中国移动android游戏 (3543)

生成浮点数的随机函数 (3449)

爱加密和梆梆加固的破解 (3164)

编译Lua库并配置开发环 (3008)

修改VC++6.0生成的EXE (2965)

NTFS文件格式 (2857)

评论排行

apk文件添加AlertDialog (5)

修改VC++6.0生成的EXE (4)

CFileFind类 (4)

调试器攻击技术 - Threac (4)

Object - C中使用NSKey (3)

按钮中添加位图和图标 (3)

IDA pdb 自动下载 (3)

【原创】10分钟破解subl (3)

C++设计模式13: Templ (2)

if(**|| ** || ** || ** ||)的变 (2)

推荐文章



最新评论

[以早期版本为例]快速Dump爱加abcggvg: 你好我试过了, 但是查看寄存器时出现, oop! internel erro 的情况, 我的QQ是2960...

爱加密和梆梆加固的破解方法双刃剑客: 有人说爱加密现在 在内存中展开的都是odex需要找odex的头, 而不是dex的头, dump之后还要还...

爱加密和梆梆加固的破解方法双刃剑客: PTRACE_POKEDATA = 5PTRACE_CONT = 7PTRACE_ATTACH = ...

基于ARM的Ptrace FindAllBlue: good啊啊啊啊啊啊

01. debugserver *:1234 -a "SpringBoard"

复制代码

成功后会显示:

三、在OSX上用lldb远程调试

首先在Terminal中运行lldb, 然后输入以下命令:

01. platform select remote-ios

复制代码

成功后会显示下图类似信息:

接着输入以下命令:

01. process connect connect://iOSIP:1234

复制代码

注意, 这条命令执行耗时比较长, 很多读者可能会以为iOS/OSX死掉了, 其实没有, 耐心等一会, 看看@iOS应用逆向工程有没有刷新微博, 或在论坛里逛逛吧~

执行成功后会显示:

四、获取ASLR的offset

首先在lldb里输入"c"并回车, 让进程继续执行; lldb有一个gdb没有的优点, 就是可以在进程运行的过程中执行一些命令, 这样就可以有效避免SpringBoard这样的进程在暂停过久后被WatchDog给kill掉。在lldb里输入

01. image list -o -f

复制代码

显示如下图片:

其中第一列[X]是image的序号, 不用管; 第二列是ASLR的offset (也就是对应image的虚拟内存slide); 第三列是image的全路径和slide之后的基地址, 也不用管~所以第二列就是我们需要的信息。

五、在内存地址上下断点

假如我们在SpringBoard这个image的0xb446 (在_menuButtonDown:中) 处下断点, 则此地址在内存中的实际位置是0xb446 + 0x9a000 = 0xa5446, 在lldb中对应的命令是:

01. br s -a 0xA5446

复制代码

执行成功后显示:

值得注意的是, lldb好像不支持两个地址相加, 即

01. br s -a (0x0009a000 + 0xb446)

复制代码

是无法成功执行的。这样的话, 我们只好在计算器中算好地址的值, 再下断点了, 略麻烦啊.....

六、更改寄存器的值

按下home键, 触发断点, 显示如图:

可以看到, lldb把包括断点在内的4条指令显示了出来, 方便我们调试。这里, 我们将r0的值设为0, 让其跳转到0xa5470 (0xb470 + 0x9a000) 处。更改r0值的lldb命令是:

01. register write r0 0

http://blog.csdn.net/zhangmiaoping23/article/details/34501837

2/4

啊啊啊啊好啊

windows下gdb与gdb_server调试
双刃剑客: adb shell "su -c
"chmod 4777
/data/local/tmp/gdbse...

ARM的B,BL跳转指令偏移值计算
双刃剑客: 不同于微编码的处理
器, ARM (保持它的 RISC 性)是
完全硬布线的。为了加速 ARM 2
和 3...

ARM的B,BL跳转指令偏移值计算
双刃剑客: ldr 1字节换算公式:偏
移量: B - (A+8)

常用android的smali注入代码
savage407:
Work\com.uroad.yxw\smali\com\urc

IOS第十天——Obj - C的属性
双刃剑客: @property(copy,
nonatomic) NSString *Name;//声
明属性Na...

Object - C中使用NSKeyedArchiv
双刃剑客:
//*****
对应的解归...

新开的论坛

新开的论坛(适合于新手,高手,有
空去看看)

复制代码

接着” ni “两次，我们就可以看到程序执行到了0xa5470处，如图：

七、用lldb启动一个App

01. debugserver -x backboard *:1234 /path/to/app/executable

复制代码

如

01. debugserver -x backboard *:1234 /Applications/MobileNotes.app/MobileNotes

复制代码

此命令会启动记事本，并断在程序的第一条指令上。相较attach的半路出家，这种方式更有助于我们从头调试一个程序，可以观察到一些变量的初始化过程。

八、更多lldb命令

经过上面的操作，我们可以看到，lldb还是比较方便的，用惯了gdb而对它不熟悉的朋友可以通过lldb与gdb命令对照表来熟悉lldb的命令。其实有了上面的几个操作，我们就可以开始简单动态分析程序了，相信能把上面六步走通的朋友，已经具备了举一反三的能力，其他需要用到的功能都可以Google到，当然更欢迎你到论坛里发帖提问或分享。好了，debugserver + lldb的简单介绍到此结束，接下来赶紧打开Terminal，hack起来吧~！

- 上一篇
- iphone用GDB修改游戏教程！详细的图文教程！
- 下一篇
- iPhone 新手必看 新机激活基本教程

主题推荐 gdb 处理器 调试 iphone 苹果

猜你在找

APP内置IM 系统——从入门到千万级在线	iOS安全攻防五使用Cycrypt修改支付宝app运行时
iOS8开发技术（Swift版）：iOS基础知识	iOS安全攻防八键盘缓存与安全键盘
C语言及程序设计初步	CordovaPhoneGap 30 Android开发环境注意事项
Android应用的调试	ubuntu1004 LTS升级git 版本
微信公众平台开发入门	卖冰激凌的程序猿

准备好了么？跳 吧！

更多职位尽在 CSDN JOB

3D引擎以及工具链研发工程师	我要跳槽	C/C++ 软件开发工程师	我要跳槽
北京永航科技有限公司	15-30K/月	上海惠普	16-20K/月
C/C++软件工程师	我要跳槽	C/C++软件开发工程师（社交系统服务	我要跳槽
沈阳美行科技有限公司	4-8K/月	广州朗桥维视通信技术有限公司	10-15K/月

查看评论

暂无评论

您还没有登录,请[登录]或[注册]

* 以上用户言论只代表其个人观点，不代表CSDN网站的观点或立场


核心技术类目

- 全部主题
- Hadoop AWS 移动游戏 Java Android iOS Swift 智能硬件 Docker OpenStack
- VPN Spark ERP IE10 Eclipse CRM JavaScript 数据库 Ubuntu NFC WAP jQuery
- BI HTML5 Spring Apache .NET API HTML SDK IIS Fedora XML LBS Unity
- Splashtop UML components Windows Mobile Rails QEMU KDE Cassandra CloudStack FTC
- coremail OPhone CouchBase 云计算 iOS6 Rackspace Web App SpringSide Maemo
- Compuware 大数据 aptech Perl Tornado Ruby Hibernate ThinkPHP HBase Pure Solr
- Angular Cloud Foundry Redis Scala Django Bootstrap

[公司简介](#) | [招贤纳士](#) | [广告服务](#) | [银行汇款帐号](#) | [联系方式](#) | [版权声明](#) | [法律顾问](#) | [问题报告](#) | [合作伙伴](#) | [论坛反馈](#)

[网站客服](#) [杂志客服](#) [微博客服](#) [webmaster@csdn.net](#) 400-600-2320 | 北京创新乐知信息技术有限公司 版权所有 |

江苏乐知网络技术有限公司 提供商务支持

京 ICP 证 070598 号 | Copyright © 1999-2014, CSDN.NET, All Rights Reserved 

2