



看雪安全论坛 > 移动平台 > 『iOS安全』  
【原创】lldb + debugserver调试环境部署(一)

用户名  记住 ☒  
密码  登录论坛 忘记密码?

KSSD

注册账号

搜索论坛

日历事件

论坛帮助

发新话题

回复话题

主题工具 显示模式

小调调



初级会员

资料:

注册日期: Jul 2010  
帖子: 201  
精华: 0  
现金: 111 Kx  
致谢数: 6  
获感谢文章数: 6  
获会员感谢数: 6

1 2014-07-15, 17:04:35 【原创】lldb + debugserver调试环境部署(一)

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 (以下操作在iPhone 5, iOS 7.0.4上测试, 应该也适用于arm64, 如果不行, 请参照iphonedevwiki)。

使用的工具

Otool ——查看程序依赖哪些动态库信息, 反编代码段.....等等等等  
Ldid ——签名工具, 通过plist文件指定了授予一应用的一组特权  
Gdbserver ——调试工具  
SSH ——远程控制  
Lipo ——合并拆分对支持不同芯片的mach-o

一.定制一个可以调试的debugserver

1.下载编译ldid

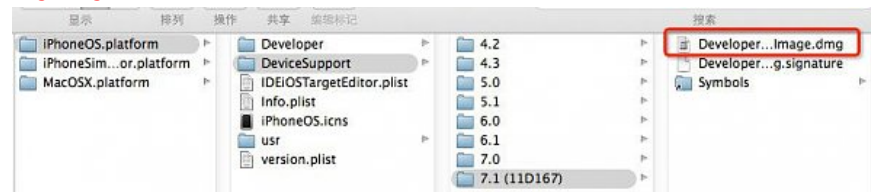
```
git clone git://git.saurik.com/ldid.git  
cd ldid  
git submodule update --init  
./make.sh
```

完成以上操作会在ldid目录下生产一个mac 可执行程序 ldid。

2.获取debugserver和ARMDisassembler.framework

我这以xcode 5.1.1的版本为例。

找到/Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/DeviceSupport/7.1 (11D167)/DeveloperDiskImage.dmg



如果你在Mac那双击它, 你会看到如下目录:

Applications	2014年2月10日 下午2:19	--	文件夹
Library	2014年3月1日 下午12:35	--	文件夹
Daemons	2014年3月1日 下午12:35	--	文件夹
Frameworks	2014年3月1日 下午12:35	--	文件夹
LaunchDaemons	2014年3月1日 上午9:33	--	文件夹
Lockdown	2014年2月10日 下午12:08	--	文件夹
PreferenceBundles	2014年3月1日 上午9:33	--	文件夹
PrivateFrameworks	2014年3月1日 下午12:35	--	文件夹
AppleProfileFamily.framework	2014年3月1日 上午9:26	--	文件夹
ARMDisassembler.framework	2014年2月10日 上午11:19	--	文件夹
CoreProfile.framework	2014年3月1日 下午12:35	--	文件夹
DevToolsBundleInjection.framework	2014年2月10日 上午11:23	--	文件夹
DTInstrumentsCP.framework	2014年2月10日 下午12:05	--	文件夹
DTInstrumentsServer.framework	2014年2月10日 下午12:06	--	文件夹
DTMessageQueueing.framework	2014年2月10日 下午12:02	--	文件夹
DTXConnectionServices.framework	2014年2月10日 下午12:02	--	文件夹
GPUTools.framework	2014年2月10日 下午2:18	--	文件夹
GPUToolsCore.framework	2014年2月10日 下午2:18	--	文件夹
RemotelInjection.framework	2014年2月10日 下午12:05	--	文件夹
UIAutomation.framework	2014年2月11日 下午2:33	--	文件夹
Tools	2014年2月10日 下午12:02	--	文件夹
otest	2014年2月10日 下午12:02	84 KB	Unix 可执行文件
usr	2014年3月1日 下午12:35	--	文件夹
bin	2014年3月1日 下午12:35	--	文件夹
debugserver	2013年11月22日 下午1:36	1 MB	Unix 可执行文件
heap	2014年2月22日 下午12:07	171 KB	Unix 可执行文件
reg	2014年2月10日 下午12:03	377 KB	Unix 可执行文件
sample	2014年2月22日 下午12:07	119 KB	Unix 可执行文件
ScreenShot	2014年2月10日 下午2:35	121 KB	Unix 可执行文件
XcodeDeviceMonitor	2014年2月10日 下午2:21	537 KB	Unix 可执行文件
xctest	2014年2月10日 下午12:02	84 KB	Unix 可执行文件
libexec	2014年3月1日 下午12:35	--	文件夹

红色框圈起来的就是我们需要使用到的部分, 此时你一定很高兴的看到了debugserver, 但是别高兴的太早了, 我们还要对这个debugserver做下处理, 使其能正常的调试起来。

将ARMDisassembler.framework 拷贝到手机上/System/Library/PrivateFrameworks目录下。

很多人一定奇怪为啥要这步骤，你们可以自己试试，去掉ARMDisassembler.framework与存在ARMDisassembler.framework，在LLDB调试的过程看ARM反汇编的质量和效果。  
我这边使用scp拷贝到设备上：

```
# cd /Volumes/DeveloperDiskImage/Library/PrivateFrameworks
# scp -r -p 22 ARMDisassembler.framework root@192.168.20.21:/System/Library/PrivateFrameworks
```

3.提取对应设备版本的debugserver，并对其签名授予特权

1) 提取对应的debugserver（由于Idid不支持对FAT文件格式的mach-o签名，所以需要提取对应版本）

```
lipo -thin armv7 /Developer/usr/bin/debugserver -output ~/debugserver
lipo -thin armv7S /Developer/usr/bin/debugserver -output ~/debugserver
lipo -thin armv64 /Developer/usr/bin/debugserver -output ~/debugserver
```

以上根据自己手机支持的armv7、armv7s、arm64提取，我这边以iphone5为例，是armv7，所以我使用

```
# cd Development/DeveloperDiskImage/usr/bin/
# mv debugserver _debugserver
# lipo -thin armv7 _debugserver -output debugserver
```

2) 保存以下授予特权内容为entitlement.xml

```
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>com.apple.springboard.debugapplications</key>
  <true/>
  <key>get-task-allow</key>
  <true/>
  <key>task_for_pid-allow</key>
  <true/>
  <key>run-unsigned-code</key>
  <true/>
</dict>
</plist>
```

3) 使用Idid对debugserver签名授予特权

```
# Idid -Sentitlement.xml debugserver
将签名授予特权的debugserver拷贝到手机/usr/bin目录下
# scp -p 22 debugserver root@192.168.20.21:/usr/bin/
```

4) 测试debugserver是否安装成功(如下正常)

```
# debugserver 192.168.40.45:12345 -a "PAppInstall"
debugserver-310.2 for armv7.
Attaching to process PAppInstall...
Listening to port 12345 for a connection from 192.168.40.45...
```

参考链接：  
<http://www.iphonedevwiki.net/index.php/Debugserver>

PDF下载: [lldb + debugserver调试环境部署\(一\).pdf](#)

此帖于 2014-07-25 11:40:22 被 小调调 最后编辑

[公告]如果你觉得有人语言挑衅，请点每帖右上角的“举报”按钮！



感谢 小调调  
此篇文章之用户: grok (2015-06-30)

kuang110  
☺☺☺☆☆☆

☆☆☆☆☆  
中级会员

资 料:

注册日期: Jun 2004

帖子: 296

精华: 6

现金: 72 Kx

致谢数: 0

获感谢文章数: 0

获会员感谢数: 0

2 2014-07-15, 19:01:37

不错。支持，加油加油

[招生]15PB软件安全培训开始接受第007期报名（05.05开课）！



lookzo







★

密码学小组（见习）  
信息及实践组


资 料:

注册日期: Jan 2007  
帖子: 312   
精华: 0  
现金: 233 Kx  
致谢数: 1  
获感谢文章数: 2  
获会员感谢数: 2

3




2014-07-15, 22:26:21



支持ios上的技术文章

[招生]15PB软件安全培训开始接受第007期报名（05.05开课）！

 引用

TOP

white、




★

初级会员


资 料:

注册日期: May 2011  
帖子: 270   
精华: 0  
现金: 47 Kx  
致谢数: 37  
获感谢文章数: 1  
获会员感谢数: 2

4




2014-07-16, 09:04:08



嗯 赞一个，

[培训]"麦洛克菲"内核底层开发培训，看雪会员报名减免200元！

 引用

TOP

dkxzl






★ ★ ★

普通会员

资 料:

注册日期: Jun 2009  
帖子: 211   
精华: 1  
现金: 172 Kx  
致谢数: 2  
获感谢文章数: 5  
获会员感谢数: 11

5



2014-07-17, 11:11:20



我来顶宝珠姐的～～

[公告]如果你觉得有人语言挑衅，请点每帖右上角的“举报”按钮！

 引用

TOP

snakeninny

☆☆☆


★

初级会员


资 料:

注册日期: Nov 2010  
帖子: 42   
精华: 0  
现金: 12 Kx  
致谢数: 1  
获感谢文章数: 2  
获会员感谢数: 5


6



2014-07-23, 16:19:07



引用:

最初由 小调调发布 

这边先给一篇吧,懒得排版,后续会陆续补全.(有地方有细节补充)

90685

90686

90687

90688

90689

PDF下载: 90690...

前辈你好，请问你原创PDF的第一段话，是否参考了小弟的帖子？

[招生]15PB软件安全培训开始接受第007期报名（05.05开课）！


 引用

TOP

dkxzl



7



2014-07-23, 17:46:57





普通会员

资 料:

注册日期: Jun 2009  
帖子: 211  
精华: 1  
现金: 172 Kx  
致谢数: 2  
获感谢文章数: 5  
获会员感谢数: 11

引用:

最初由 **snakeninny** 发布  
前辈你好，请问你原创PDF的第一段话，是否参考了小弟的帖子？

近距离抚摸大神啊！我砸app壳的时候还是参考大神的发的那工具源码！大神快到我碗里来吧

[公告]如果你觉得有人语言挑衅，请点每帖右上角的“举报”按钮！

引用 TOP

Carina



初级会员

资 料:

注册日期: Mar 2014  
帖子: 19  
精华: 0  
现金: 5 Kx  
致谢数: 0  
获感谢文章数: 0  
获会员感谢数: 0

8 2014-07-24, 15:31:53

使用的工具，我也有点眼熟。

[培训]"麦洛克菲"内核底层开发培训，看雪会员报名减免200元！

引用 TOP

小调调



初级会员

资 料:

注册日期: Jul 2010  
帖子: 201  
精华: 0  
现金: 111 Kx  
致谢数: 6  
获感谢文章数: 6  
获会员感谢数: 6

9 2014-07-24, 18:50:31

引用:

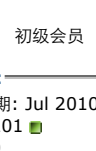
最初由 **snakeninny** 发布  
前辈你好，请问你原创PDF的第一段话，是否参考了小弟的帖子？

哈哈，大神就别折磨我了，就是参考你的

[公告]如果你觉得有人语言挑衅，请点每帖右上角的“举报”按钮！

引用 TOP

小调调



初级会员

资 料:

注册日期: Jul 2010  
帖子: 201  
精华: 0  
现金: 111 Kx  
致谢数: 6  
获感谢文章数: 6  
获会员感谢数: 6

10 2014-07-24, 18:51:32

引用:

最初由 **Carina** 发布  
使用的工具，我也有点眼熟。

借鉴念茜的排版哈，我看挺好的，就拿来用了，罪过罪过，不过内容货真价实是我自己有补充的~

[培训]"麦洛克菲"内核底层开发培训，看雪会员报名减免200元！

引用 TOP

Carina



初级会员

资 料:

注册日期: Mar 2014  
帖子: 19

11 2014-07-24, 18:56:20

引用:

最初由 **小调调** 发布  
借鉴念茜的排版哈，我看挺好的，就拿来用了，罪过罪过，不过内容货真价实是我自己有补充的~

我看到很开心呀~~ 让你误会啦~~



精华: 0  
现金: 5 Kx  
致谢数: 0  
获感谢文章数: 0  
获会员感谢数: 0

[培训]"麦洛克菲"内核底层开发培训，看雪会员报名减免200元！

引用 TOP

goabout



初级会员

资料:

注册日期: Sep 2012  
帖子: 8  
精华: 0  
现金: 15 Kx  
致谢数: 0  
获感谢文章数: 0  
获会员感谢数: 0

12 2014-08-21, 10:02:17

请问一下，我把debugger放进手机后，运行debugserver \*:1234 -a "OPlayer Lite"后，出现一下错误  
dyld: Symbol not found: \_BKSAcivateForEventOptionTypeBackgroundContentFetching  
Referenced from: /usr/bin/debugserver  
Expected in: /System/Library/PrivateFrameworks/BackBoardServices.framework/BackBoardServices  
in /usr/bin/debugserver  
Trace/BPT trap: 5  
请问怎么解决呀

[培训]"麦洛克菲"内核底层开发培训，看雪会员报名减免200元！

引用 TOP

伊邪那美



初级会员

资料:

注册日期: Dec 2014  
帖子: 41  
精华: 0  
现金: 100 Kx  
致谢数: 1  
获感谢文章数: 1  
获会员感谢数: 6

13 2015-01-14, 16:38:05

楼主你好，能不能给我个8.1（12B411）的DeveloperDiskImage.dmg，先谢谢你了

[招生]15PB软件安全培训开始接受第007期报名（05.05开课）！

引用 TOP

SnowNight



初级会员

资料:

注册日期: Jul 2014  
帖子: 51  
精华: 0  
现金: 5 Kx  
致谢数: 3  
获感谢文章数: 0  
获会员感谢数: 0

14 2015-01-16, 10:28:01


http://bbs.iosre.com/forum.php?mod=viewthread&tid=52&extra=page%3D1&page=1这里的一篇文章也不错


[培训]"麦洛克菲"内核底层开发培训，看雪会员报名减免200元！


引用 TOP


发新话题 回复话题


添加到书签


 Digg


 del.icio.us

 StumbleUpon

 Google

 百度收藏

 QQ 书签

 雅虎收藏

« 上一主题 | 下一主题 »

发帖规则

您不可以发表主题  
您不可以回复帖子  
您不可以上传附件  
您不可以编辑自己的帖子

论坛论坛启用 VB 代码  
论坛启用 表情图标  
论坛启用 [IMG] 代码  
论坛规则

『iOS安全』 执行

相似的主题				
主题	主题作者	论坛	回复	最后发表
【原创】gikdbg v1.1携手lldb震撼来袭，求内测伙伴！	GeekNeo	『iOS安全』	14	2014-10-29 14:01:14

所有时间均为北京时间, 现在的时间是 08:44:25.

-- VBB3

-- 简体中文

[联系我们](#) - [看雪学院](#) - [文字模式](#) - [返回顶部](#)