免 iDP 编译 iPhone app 真机执行

2010 年 9 月 15 日代码罐头发表评论阅读评论

因为尝试了很多资料.所以这篇不光是转载了
我把所有尝试方法和最终步骤都记录下来.
网上的资料要不是少步骤要不就是太老
我在 IOS SDK 4.1 下面测试
环境是

Mac OS X 10.6.4
iPhone 1,1 whited00r 3.1.5(firmware 3.1.3)
iOS SDK 4.1 final

测试下来方法 1 和方法 2 都不能通过编译
两种方法结合起来也不行
后来找到方法 3
使用方法 3 终于可以编译通过.产生了 release 代码
但是复制到 iphone 上之后只要执行就立刻退出
在 ssh 下面执行的时候直接返回 Killed
查阅之后感觉是签名还是有问题,被 SpringBoard 直接杀掉了
尝试过在 iPhone 上执行 ldid
但是返回如下的错误

```
codesign_allocate: for architecture armv6 object: ./test malformed object (unknown load command 4)
util/ldid.cpp(582): _assert(0:WEXITSTATUS(status) == 0)
```

最终使用如下方法关闭 iphone 证书检测

```
sysctl -w security.mac.proc_enforce=0
sysctl -w security.mac.vnode_enforce=0
```

==========总结:真正运行自己的 app 过程==========

1.iPhone 安装 openssl 以及 openssh,这个方便以后连接上来操作.当然用 91 之类的文件管理也可以将编译后的程序放上来

2.iPhone 的 ssh 默认密码是 alpine,不要用 passwd 去改.直接修改/etc/passwd 文件和备份.具体方法这里不说了.

3.修改 Developer/Platforms/iPhoneOS.platform/Developer/SDKs/iPhoneOS[SDK 版本].sdk/SDKSettings.plist 文件,将 CODE_SIGNING_REQUIRED 对应的值设置为 NO.

4.打开项目,在 Xcode 右上角的 info 里面,选择 Building 项,Configuration 选择 Release,在 Code Signing->Code Signing Identity->Any iOS device 设置为 Don't Code Sign

5.这时候项目选择 Device 就可以正常编译通过了

6.将文件上传,这里使用 scp,可以使用其他方法
mac$scp -r [项目名.app] root@[你的 iphone 的 IP 地址]/Applications

7.登录 iphone 进行操作,给程序可执行权限并且重启 SpringBoard 让程序图标可以出现.

mac$ssh root@[你的 iphone 的 ip 地址]

iphone$cd /Applications
iphone$chmod +x [项目名.app]

iphone$killall SpringBoard

8.关闭 iphone 的合法性检查关闭

iphone$sysctl -w security.mac.proc_enforce=0
iphone$sysctl -w security.mac.vnode_enforce=0

9.执行程序成功

==========总结:测试过程==========

1.iPhone 安装 openssl 以及 openssh,这个方便以后连接上来操作.当然用 91 之类的文件管理也可以将编译后的程序放上来

2.iPhone 的 ssh 默认密码是 alpine,不要用 passwd 去改.直接修改/etc/passwd 文件和备份.具体方法这里不说了.

3.修改 Developer/Platforms/iPhoneOS.platform/Developer/SDKs/iPhoneOS[SDK 版本].sdk/SDKSettings.plist 文件,将 CODE_SIGNING_REQUIRED 对应的值设置为 NO.

4.打开项目,在 Xcode 右上角的 info 里面,选择 Building 项,Configuration 选择 Release,在 Code Signing->Code Signing Identity->Any iOS device 设置为 Don't Code Sign

5.这时候项目选择 Device 就可以正常编译通过了

6.在 Mac OS X 中下载 ldid,以下使用 mac$标识在 mac 机执行的指令,iphone$标识在 iphone 中执行的指令

mac$wget http://svn.telesphoreo.org/trunk/data/ldid/ldid-1.0.610.tgz

7.解压这个包并编译

mac$tar -zxf ldid-1.0.610.tgz
mac$cd ldid-1.0.610
mac$g++ -I . -o util/ldid{,.cpp} -x c util/{lookup2,sha1}.c

8.进入[项目目录]/build/Release-iphoneos/

9.使用 ldid 对应用程序进行签名

mac$ldid -S [项目名.app]/[项目名]

10.将文件上传,这里使用 scp,可以使用其他方法

mac$scp -r [项目名.app] root@[你的 iphone 的 IP 地址]/Applications

11.登录 iphone 进行操作,给程序可执行权限并且重启 SpringBoard 让程序图标可以出现.

mac$ssh root@[你的 iphone 的 ip 地址]

iphone$cd /Applications
iphone$chmod +x [项目名.app]

iphone$killall SpringBoard

12.在 iphone 上执行程序就直接退出了.

13.从手机的 Cydia 上搜索下载 ldid,登录 ssh 之后执行
iphone$ldid -S [项目名.app]/[项目名]
报错

codesign_allocate: for architecture armv6 object: ./test malformed object (unknown load command 4)
util/ldid.cpp(582): _assert(0:WEXITSTATUS(status) == 0)
14.从 cydia 的网站找到 ldid 官方的方法
只能将检查关闭

iphone$sysctl -w security.mac.proc_enforce=0
iphone$sysctl -w security.mac.vnode_enforce=0

15.执行程序成功

==========方法 1:制作自己证书==========
1. 產生證書
由於 XCode 後面的版本都要求應用程式必須經過簽署,也因此你必須要
多花 99 美元加入 Developer Program (真是黑呀),反正我又不放到 App Store 賣錢,乾脆自己簽個證書來用不就好了

打開 Key Access 這個工具程式(在應用程式->工具程式內),並建立一個 “iPhone Developer” 名稱的證書(這個名稱不要改,否則你得在專案內改變)

類型選擇”編碼簽名”
輸入憑證資訊
最後選擇存放在”系統”內(不是 “登入”,否則會找不到)
這樣就大功告成了,你已經省下$99 了!

2. 專案建立好了後,打開 Project Setting,並在 User-Defined Settings 輸入:

PROVISIONING_PROFILE_ALLOWED = NO
PROVISIONING_PROFILE_REQUIRED = NO

3. 打開 Info.plist,這個檔案主要存放應用程式的相關描述,按右鍵 Add Row,新增 SignerIdentity = “Apple iPhone OS Application Signing” (要一樣的,亂輸好像不行)

11. 選擇要使用的設備,在此我們選擇 Device – iPhone OS 2.2,XCode 會幫我們簽署,按下”允許”(不能按”總是允許”)就可以輸出到你的 iPhone 了(第一次跑可能會出現 Security policy error,再跑一次
就不會出現了)

==========方法 2:直接生成 app==========
开发安装环境 mac OS,并且有 wifi,经过越狱(破解)的 iphone 或者 ipod touch.
下面所提到的 scp 是 mac OS 的终端命令.
ssh,ldid 和 chmod 等是 iphone 的终端命令行,需要安装,cydia 等工具

直接进行编译,必会出现错误提示:
CodeSign error: no certificate found in keychain for code signing identity ‘iPhone Developer’

下面我们先跳过 Xcode 的签名检查.打开工程文件夹下的*.xodeproj 为后缀名的文件(右键点击显示包内容”Show Package Contents”),一般会看到三个文件,以文本方式打开 project.pbxproj 这个文件,

此時, 打開工程文件夾下*.xcodeproj 為後綴名的文件(右鍵點擊, 選擇”Show Package Contents”),搜索 iPhone Developer,找到后删除,一共有 2 处,然后保存,重新进入 Xcode 编译即可生成 App 程序.生成的结果在 build 目录下.

把编译好的 release for device 的程序拷贝到 iphone

先进入 MyApp.app 所在的目录,然后执行如下命令

siu-andrewde-macbook:release-iphoneos siuandrew$ scp -r MyApp.app root@192.168.0.2:/Applications
提示输入密码

root@192.168.0.2's password:
然后开始拷贝.

拷贝完成后再次登入 Iphone:

siu-andrewde-macbook:release-iphoneos siuandrew$ ssh root@192.168.0.2
root@192.168.0.2's password:
登入后执行签名工作

iPhone:~ root# cd /Applications
iPhone:/Applications root# ldid -S MyApp.app/MyApp
ldid 这一步非常重要,注意-S 要大写,耐心等待签名结束.

签名完成进行把整个目录权限设置 755

iPhone:/Applications root# chmod +x MyApp.app
设置权限这一步也必不可少,或者用 chmod -R 755 MyApp.app

上传及签名工作完成,如果 iphone 安装了 91 关机助手,注销并修复图标即可,否则在 iphone 机子上要删除 installation.plist 文件

iPhone:~ root# rm /private/var/mobile/Library/Caches/com.apple.mobile.installation.plist
然后重启动手机即可看到程序的图标.

运行你自编译的 App 程序.

==========方法 3:不签名 app,使用 ldid==========

如果你不是 iPhone 开发者，但是恰好有 mac 和 iphone 在身边，又恰好是个喜欢“hello world”的 IT 民工，那你一定会想在自己的 iPhone 上 hello world 一下。由于你只是玩票，所以肯定不会去弄 iPhone Development Program ，官方文档自然没有任何供你参考的信息，目前网络上介绍的各种 sdk 版本的方法大多都已经失效或是混乱，所以发一个简单的说明：

本文测试环境：Snow leopard 10.6.3 + Xcode 3.2.2 + iPhone 3G(3.1.2 固件)

前提条件：在 Xcode 中已经有可以在模拟器上正常运行的 Hello World 程序 + iPhone 已经越狱 + 本身是个没进行过 iPhone 开发的小白

方案思路：build 一个不需要签名的应用，在 mac 上用 ldid 伪造签名，通过 SSH 上传到 iPhone 上

操作步骤：
sudo vi /Developer/Platforms/iPhoneOS.platform/Developer/SDKs/iPhoneOS[SDK 版本].sdk/SDKSettings.plist , 把 CODE_SIGNING_REQUIRED 对应的值设置为 NO。 – 这是告诉 Xcode 使用这个 SDK build 时不用必须签名应用;

在 Xcode 中修改应用的”info”->”build” -> “Release” -> “Code Signing Identity”,设置为”Don’t Code Sign”,选择构建目标为”iPhone Device – [SDK 版本] | Release”，build 应该提示无错误。(第一步的配置生效需要重启 Xcode) – 此步构建了一个没有签名的 app，路径为[项目位置]/build/Release-iphoneos/HelloWorld.app

安装 ldid

```
wget http://svn.telesphoreo.org/trunk/data/ldid/ldid-1.0.610.tgz
tar -zxf ldid-1.0.610.tgz
cd ldid-1.0.610
g++ -I . -o util/ldid{,.cpp} -x c util/{lookup2,sha1}.c
```

util/ldid 下面就是我们需要用来伪造签名的 ldid 程序了

给程序签名

ldid -S [项目位置]/build/Release-iphoneos/HelloWorld.app/HelloWorld (注意这里要写到.app 下面的执行文件)

SSH 上传到 iPhone 的/Applications 下面，respring 一下就可以看到并使用 HelloWorld 应用了（SSH 应该在大家越狱时都有装，如果没有，到 Cydia 或 Rock 中都能装上，不会 respring 就重启 iPhone）

参考资料:

http://bbs.weiphone.com/read-htm-tid-222380.html

http://www.blogjava.net/sealyu/archive/2010/09/14/331968.html

http://blog.robaggio.net/2010/04/idpiphone.html

http://techxter.com/62/code-signing-iphone-applications-using-ldid/

http://www.saurik.com/id/8