IOS逆向

1. 简介

1.1什么是逆向工程

逆向工程是从任何人造的东西中提取知识或者设计规划的过程。逆向工程和传统的科学研究很相似，存在的差异，逆向工程的研究对象说人造的，而传统科学研究的对象是自然现象。

1.2 软件逆向工程

软件逆向工程就是要打开程序的“外壳”，观察其内部，分享软件产品的设计模式，源代码。

1.3 意义

1 开发竞争软件

一般来说对整个产品进行逆向工程是不值得对，花费对代价太大。独立开发一款软件是相对简单的，只有在某些难度较大或复杂的设计和算法下，可以进行逆向。

2 评估软件对质量及健壮性

当掌握逆向工作后，可以通过检查二进制代码去检测和评估代码当质量。

1.4 汇编语言

汇编是底层语言，是逆向语言，为了掌握逆向，必须全面理解所选平台的汇编语言。汇编语言是一类语言，而不是一门语言，在每个平台下的都有不同于其他平台的汇编语言。

还有个重要的概念，机械码（也称为二进制码或目标代码），有人会错误的任务机械码是比汇编语言更底层的语言，其实是个错误的概念，机械码和汇编语言是同一事物的两种不同表现，cpu读的是机械码，它是包含了cpu将要执行的命令的位序列，汇编语言则是那些位序列的文本表示－我们对位序列中所包含对元素命名为便于人理解的名称。这样我们看到的就不再是神秘的十六进制数，而是mov，xchg等文本指令了。

二、工具

2.1 theos开发工具

Theos是由DHowett大神开发的。大幅简化了编写越狱程序的流程。下面介绍theos的使用。

2.1.1、安装theos

sudo xcode-select -s /Applications/Xcode.app/Contents/Developer

export THEOS=/opt/theos

sudo git clone git://github.com/DHowett/theos.git $THEOS

2.1.2、配置ldid

从http://joedj.net/ldid下载ldid，把它放在 /opt/theos/bin/下面

2.1.3、配置 CydiaSubstrate.

iOS上在cydia中安装“CydiaSubstrate”。将iOS上“/Libarary/Frameworks/CydiaSubstrate.framework/CydiaSubstrate” 重命名为libsubstrate.dylib，放到“/opt/theos/lib/libsubstrate.dylib”下面

2.1.4、配置dpkg-deb

从<https://raw.githubusercontent.com/DHowett/dm.pl/master/dm.pl>下载dm.pl 重命名为dpkg-deb，放到“opt/theos/bin”目录下 修改其权限 sudo chmod 777 /opt/theos/bin/dpkg-deb

2.1.5、下载更多模版

[https://github.com/DHowett/theos-nic-templates/archive/master.zip](https://github.com/DHowett/theos-nic-templates/archive/masterzip) 解压后将五个.tar放到“/opt/theos/templates/iphone ”

简单实用theos创建tweak模板。终端输入 /opt/theos/bin/nic.pl 选择 9 根据提示，输入信息，会简单在当前目录创建一个模板

2.2 class-dump

它其实是个命令，下载镜像class-dump-3.5.dmg，双击，之后将里面的class-dump放在/usr/bin目录下面。这样就可以使用class-dump命令了。命令如下，

class-dump -S -s -H yourapp -o yourpath

2.3 dyld\_decache

dyld\_decache从越狱手机中导出软件私有api

第一步：将/System/Library/Caches/com.apple.dyld/dyld\_shared\_cache\_armx拷贝出来

第二步：下载dyld\_decache 网址https://github.com/downloads/kennytm/Miscellaneous/dyld\_decache[v0.1c].bz2

解压后赋予权限 chmod +x /path/to/dyld\_decache

提取命令 /path/to/dyld\_decache -o /path/to/store /path/to/dyld\_shared\_cache\_armx

倒出来的库可以使用class－dump查看头文件，和使用ida分析。

2.4 ssh-keygen

ssh-keygen 用于生成、管理和转换认证密钥,当使用ssh连接设备时，经常要输入密码，较为麻烦，可使用ssh-keygen生成无密码公钥id\_rsa.pub，重命名为authorized\_keys后放入设备路径/var/root/.shh/下。具体操作如下，

1）删除“/Users/yourcount/.ssh/known\_hosts”中对于设备ip的哪一行,没有就不用删除

2）生成authorized\_key： 命令

ssh-keygen -b 1024 -t rsa

cp /Users/gaozhimin/.ssh/id\_rsa.pub ~/authorized\_keys 拷贝至用户目录

3)配置iOS

在iOS终端输入 ssh-keygen 按几个回车

在mac终端输入 scp ~/authorized\_keys root@10.61.137.120:/var/root/.ssh

如果使用不了scp，就直接使用工具拖入。

2.5 调试工具

目前ios下常用的调试工具有gdb和lldb。目前苹果已经废弃使用gdb，转向自己研发的lldb，所以建议使用lldb的方式去调试。使用lldb需要配置debugserver。

1、在默认情况下，ios上并没有安装debugserver，只有在设备连接过xcode后，debugserver才会被xcode安装到ios的/developer/usr/bin目录下。

2、帮助debugserver瘦身

命令如下lipo -thin armv7 ~/debugserver -output ~/debugserver

3、给debugserver配置task\_for\_pid权限

下载http://iosre.com/ent.xml ,放置和debugserver相同路径，运行终端，cd该路径，运行命令

/opt/theos/bin/ldid -Sent.xml debugserver

4、将debugserver重新拷贝回设备路径/usr/bin/debugserver，并修改权限

chmod +x /usr/bin/debugserver

2.6 cycript

cycript是大神saurik开发的一个非常强大的工具，可以让开发者在命令行下和应用交互，在运行时查看和修改应用。它确实可以帮助你破解一些应用，但这个工具主要还是用来学习其他应用的设计（主要是UI的设计及实现）。

查看ui命令

cycript -p MobileSMS

?expand

[[UIApp keyWindow] recursiveDescription]