

2019

美团

APT检测设备的扩展研究

演讲人：朱学文 (Ju Zhu)



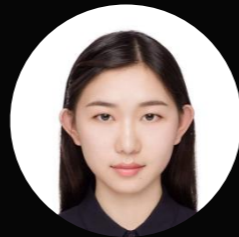


团队介绍



朱学文 (Ju Zhu)
美团/高级安全研究员

9+年的安全研究经验
7+年主要从事高级威胁的研究，包括0Day、nDay和漏洞挖掘
一直致力于使用自动化系统来Hunt野外的高级威胁
多次获得CVE，且受到Google、Apple、Facebook等厂商的致谢
多次作为Speaker受邀参加BlackHat、CodeBlue、CSS等国内外的顶级安全会议



郭梦圆 (Mabel Guo)
上海交通大学/美团实习安全研究员

上海交通大学在读硕士
研究生阶段致力于视频隐写/隐写分析研究
擅长iOS逆向以及虚拟化技术



目录

CONTENTS

01

PART 01

设备选型对比

02

PART 02

解决方案对比

03

PART 03

iOS动态沙箱

04

PART 04

一些实践

PART
01

业界主流APT检测设备的选型对比





业界主流APT检测设备的选型对比

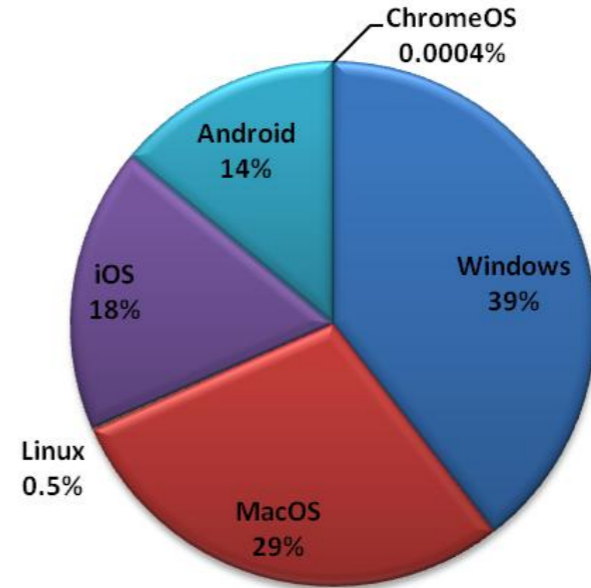
概述

平台支持性

文件类型支持性

内网接入设备类型统计

BYOD (Bring Your Own Device)





业界主流APT检测设备的选型对比

平台支持性

	Windows	MacOS	iOS	Android	其它
厂商1	✓	✗	✗	✗	✗
厂商2	✓	✗	✗	✗	✗
厂商3	✓	✗	✗	✓	✗

Win7、Win10、。。。

32位、64位

自定义导入



业界主流APT检测设备的选型对比

文件类型支持性

	PE	Office	PDF	Mach-O	plist	APK
厂商1	✓	✓	✓	✗	✗	✗
厂商2	✓	✓	✗	✗	✗	✗
厂商3	✓	✓	✗	✓	✗	✓

Mach-O <- 静态分析

plist : iOS Ransomware (Death Profile)

PART
02

可参考的解决方案对比





可参考的解决方案对比

动态沙箱技术解决方案对比

MacOS

iOS、Android



动态沙箱技术解决方案对比

	MacOS	iOS	Android
可参考的动态沙箱	Darling 或 Cuckoo Sandbox	Corellium	Anbox 或 Cuckoo Droid
使用方式（云或本地）	本地	云	本地
开源？	是	否	是
实现成本	中	极高	中



MacOS



阶梯式部署

Darling--大部分指标

Cuckoo Sandbox--剩下少部分



PART
03

iOS动态沙箱（蜜罐）





iOS动态沙箱（蜜罐）

总体架构流程

轻量级虚拟化设计

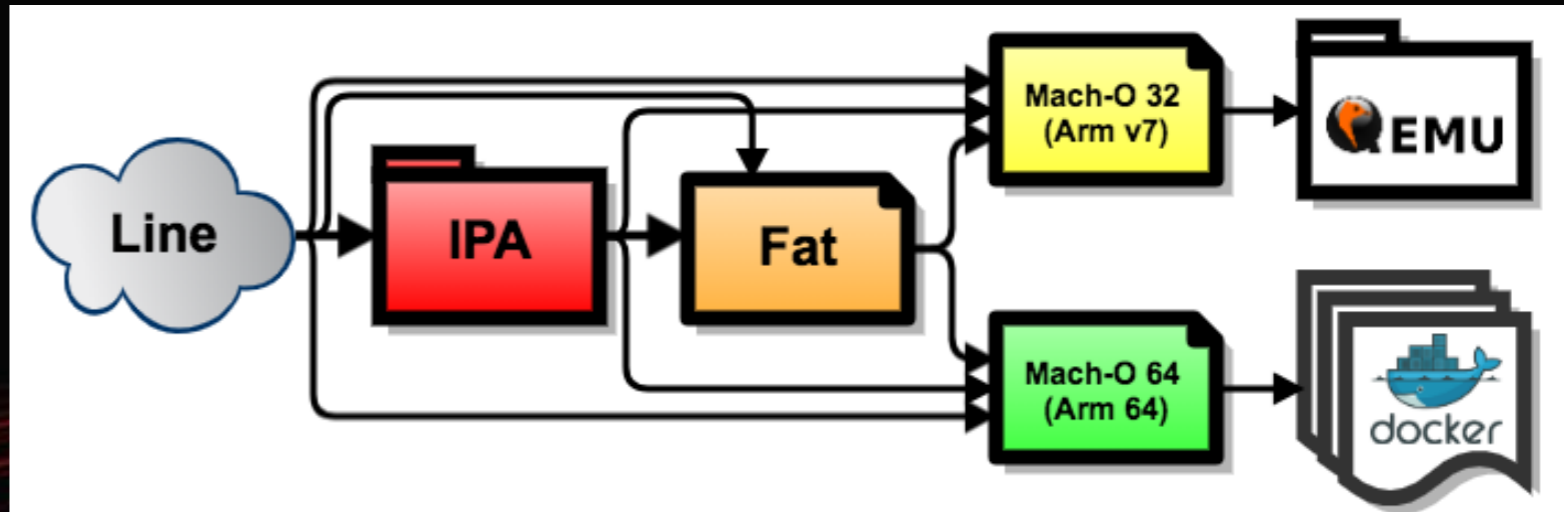
实现、部署



总体架构流程

针对Mach-O

考虑攻击面（影响面）

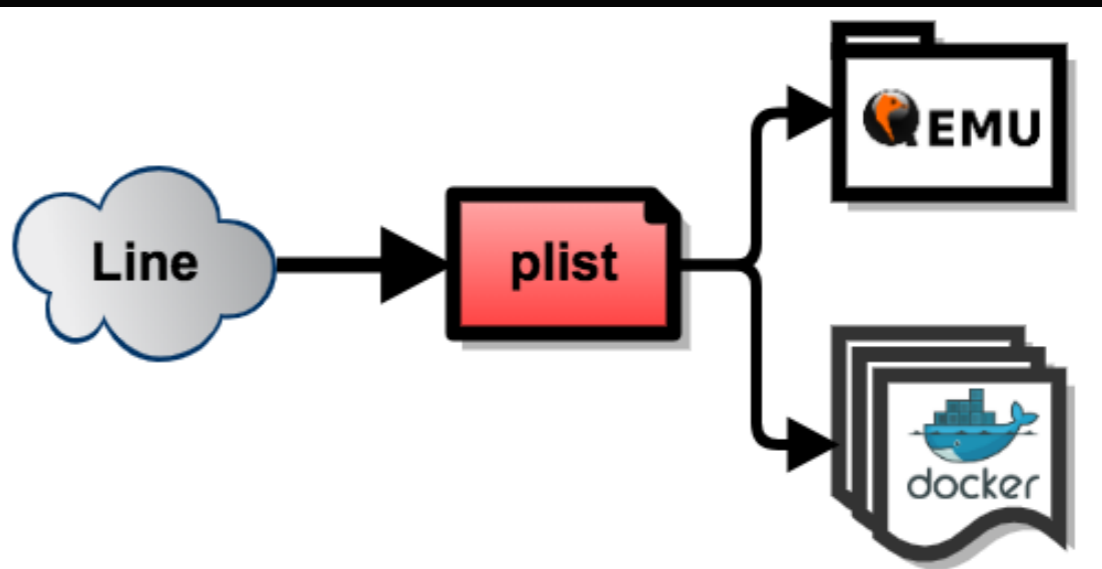




总体架构流程

针对plist

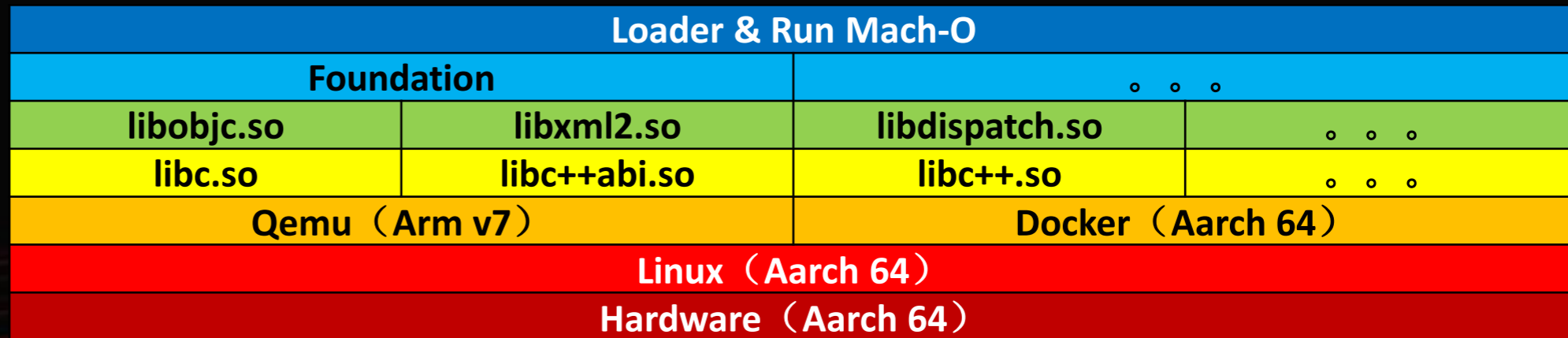
类似Death Profile的攻击





轻量级虚拟化设计

API重定向





轻量级虚拟化设计



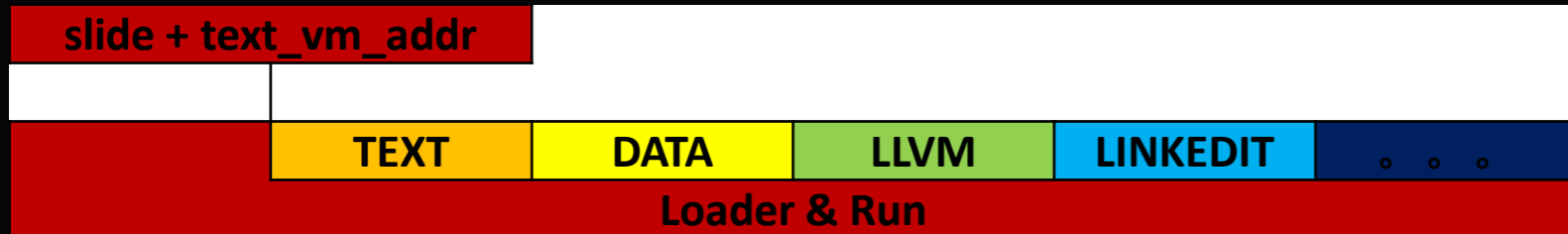
简单运行效果

```
QEMU
pi@raspberrypi: ~/Desktop/iosvm
File Edit Tabs Help
pi@raspberrypi:~/Desktop/iosvm $ uname -a
Linux raspberrypi 4.4.1 #3 SMP Sun Sep 25 13:12:50 CEST 2016 armv7l GNU/Linux
pi@raspberrypi:~/Desktop/iosvm $
pi@raspberrypi:~/Desktop/iosvm $ file pios
pios: Mach-O armv7 executable, flags:<NOUNDEFS|DYLDLINK|TWOLEVEL|PIE>
pi@raspberrypi:~/Desktop/iosvm $
pi@raspberrypi:~/Desktop/iosvm $ ./run_macho pios
Hello, World!
/run_macho: relocation error: /run_macho: symbol version GLIBC_2.4 not def
```

```
[root@localhost ju]#
[[root@localhost ju]# uname -a
Linux localhost.localdomain 4.14.36-6.1.hxt.aarch64 #1 SMP Tue Jul 17 07:01:42 UTC 2018 aarch64 aarch64 aarch64 GNU/Linux
[[root@localhost ju]#
[[root@localhost ju]# docker run iosvm-debian9 /usr/bin/file /root/ios64
/root/ios64: Mach-O 64-bit arm64 executable, flags:<NOUNDEFS|DYLDLINK|TWOLEVEL|PIE>
[[root@localhost ju]#
[[root@localhost ju]# docker run iosvm-debian9 /bin/run-macho /root/ios64
Hello World!
[[root@localhost ju]#
[[root@localhost ju]#
```

Segment数据映射到虚拟内存

VM Protection值 -> 虚拟内存VMP属性



Segment名称	Segment信息	实际虚拟内存地址范围
TEXT	Segment Name: __TEXT VM Address: 4294967296 VM Size: 32768 File Offset: 0 File Size: 32768 Maximum VM Protection: 00000001: VM_PROT_READ 00000004: VM_PROT_EXECUTE	(slide + text_vm_addr) -> (slide + text_vm_addr + 0x8000)
DATA	Segment Name: __DATA VM Address: 4295000064 VM Size: 16384 File Offset: 32768 File Size: 16384 Maximum VM Protection: 00000001: VM_PROT_READ 00000002: VM_PROT_WRITE	(slide + text_vm_addr + 0x8000) -> (slide + text_vm_addr + 0xC000)
LLVM	Segment Name: __LLVM VM Address: 4295016448 VM Size: 16384 File Offset: 49152 File Size: 16384 Maximum VM Protection: 00000001: VM_PROT_READ 00000002: VM_PROT_WRITE	(slide + text_vm_addr + 0xC000) -> (slide + text_vm_addr + 0x10000)
LINKEDIT	Segment Name: __LINKEDIT VM Address: 4295032832 VM Size: 32768 File Offset: 65536 File Size: 20496 Maximum VM Protection: 00000001: VM_PROT_READ	(slide + text_vm_addr + 0x10000) -> (slide + text_vm_addr + 0x15010)



导入相关依赖库

模拟实现

(比如Foundation.framework)



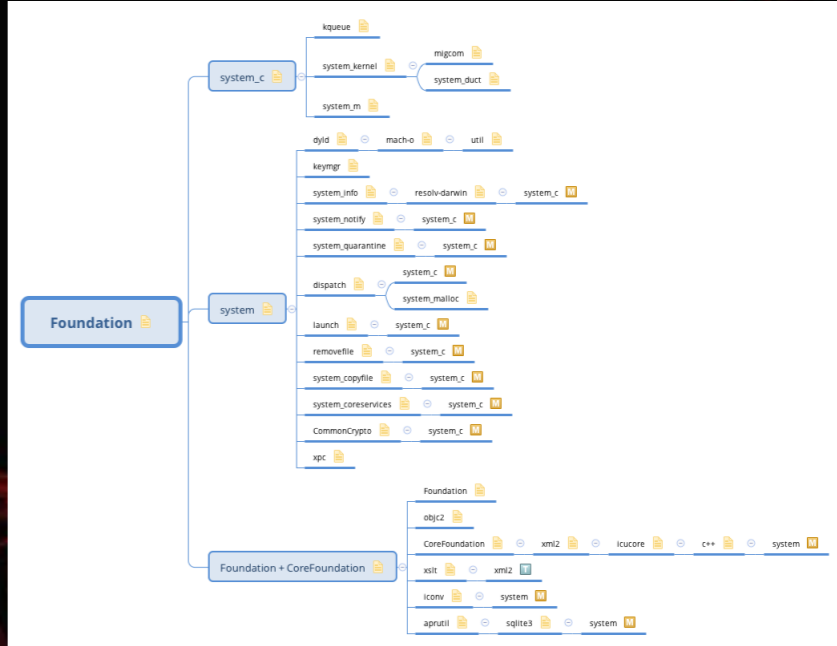
The GNUstep Base Library is a library of general-purpose, non-graphics Objective C objects. <https://www.gnustep.org/>

Foundation glibc base-library objective-c

10,700 commits 34 branches 109 releases 38 contributors View license

Search master New pull request Find File Clone or download

Commit	Message	Time
twidaler	large pull request #64 from twidaler/Foundation-header-additions	Latest commit: c62841 6 days ago
Documentation	release-chore: Bump version to 1.26.0 and update release notes.	4 months ago
Examples	Implement OSX compatible non-keyed arch encoding	2 years ago
Headers	Include CoreFoundation and libdispatch in Foundation if available.	5 days ago
NSCharacterSet	OSX compatibility fixes for zero width space character and initial...	8 years ago
NSTimeZones	Updated zone info and corrected preferred abbreviation mappings to me...	10 months ago
Resources	Fix wrong 'i' sequence for letter 'l' and short weekdays.	2 months ago
Source	Cleanups to avoid code conflicts and buffer overrun fixes.	8 months ago
Support/Foundation	Add OSX foundation support files	6 years ago
Tests	Cleanups to avoid code conflicts and buffer overrun fixes.	8 months ago
Tools	Fix crash in glibmap when an invalid hostname is given for the -M option	2 months ago
base.codeproj	Added NSUserNotification (new in OSX 10.8) and Infrastructure. It's c...	5 years ago
config	Use pkg-config to detect lua	6 months ago
macosx	removal of garbage collection	2 years ago
objcignore	ignore automatic cache; removed unused blank lines at the beginning of...	16 years ago
glibignore	chore: create glibignore file	2 years ago
travis.yml	Tweak Travis build matrix after sort algorithm changes.	3 years ago
ANNOUNCE	release-chore: Bump version to 1.26.0 and update release notes.	4 months ago
COPYING	allow developers more time to adapt to LGPLv3	11 years ago
COPYING.LIB	allow developers more time to adapt to LGPLv3	11 years ago
COPYINGv3	Added back in the v3 version of the license since the tools are still...	10 years ago
ChangeLog	Cleanups to avoid code conflicts and buffer overrun fixes.	8 months ago
ChangeLog.1	Further copyright/license updates.	14 years ago
ChangeLog.2	fix spelling errors / typos (patch by heitzmann.eric@heo.fr)	3 years ago
GNUmakefile	Remove the obsolete gspend bundle code.	3 years ago
INSTALL	Release new version	2 years ago
Makefile	allow developers more time to adapt to LGPLv3	11 years ago
Makefile.optional	preparations for release and Yavor's make distclean patch	4 years ago
NEWS	release-chore: Bump version to 1.26.0 and update release notes.	4 months ago
README	Release new version	2 years ago
README.HITable	doc: tweaks	5 years ago
Version	release-chore: Bump version to 1.26.0 and update release notes.	4 months ago
base.make.in	simplifications suggested by Yavor	5 years ago
config.mak.in	Various configure/build tweaks	3 years ago
configure	Fixed libdispatch configuration switch.	12 days ago
configure.ac	Fixed libdispatch configuration switch.	12 days ago
cross.config	When cross-compiling, obeying an additional setting for Objective-C 2...	6 years ago
gnustep-base.org.spec.in	Some cleanup for make-2.0 changes	12 years ago
gnustep-base.spec.in	Update License field	12 years ago
gnustep-base.spec.old	Updated	10 years ago
Install.sh	Update Install.sh	7 years ago





运行

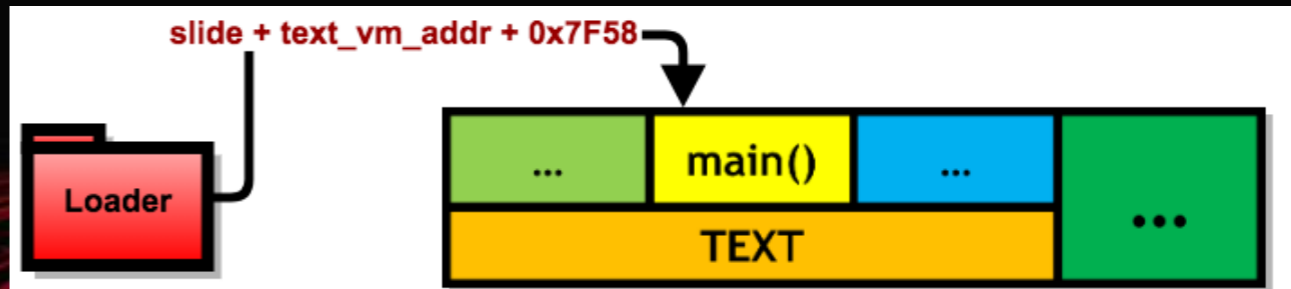
找到入口地址 (比如main函数)

Load Commands--LC_MAIN

绝对地址 = 入口地址

+ slide + text_vm_addr

80000028	Command	LC_MAIN
00000018	Command Size	24
00000000000007F58	Entry Offset	32600
0000000000000000	Stacksize	0



地址 (Rebase数据) 修正

Lazy Symbol Pointer、CFString

	原数据 (Pointer)		新数据 (Pointer)
Lazy Symbol Pointer	0x100007F9C	->	slide + 0x100007F9C
CFString	0x100007FA8	->	slide + 0x100007FA8

Dynamic Loader Info		Description	
Rebase Info	__DATA __la_symbol_ptr	0x100008010	Pointer
Opcodes	__DATA __cfstring	0x100008028	Pointer
Actions			

Section64 (__DATA,__la_symbol_ptr)	Address	Data	Description	Value
Lazy Symbol Pointers	100008010	0000000100007F9C	Indirect Pointer	[0x100008010->_NSLog]

Section64 (__DATA,__cfstring)	Address	Data	Description	Value
ObjC CFStrings	100008018	0000000000000000	CFString Ptr	___CFConstantStringClassReference
	100008020	00000000000007C8		0x7C8
	100008028	0000000100007FA8	String	0x100007FA8:"Hello World!"



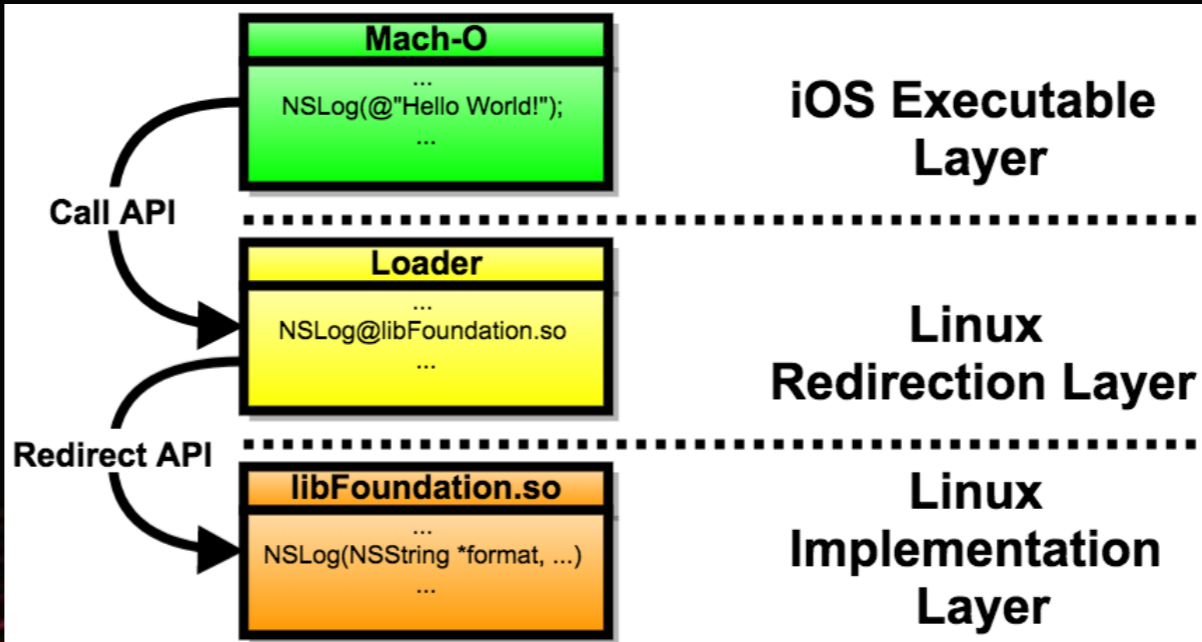
地址 (API) 重定向

Lazy Symbol Pointer数据 <- 模拟实现函数地址

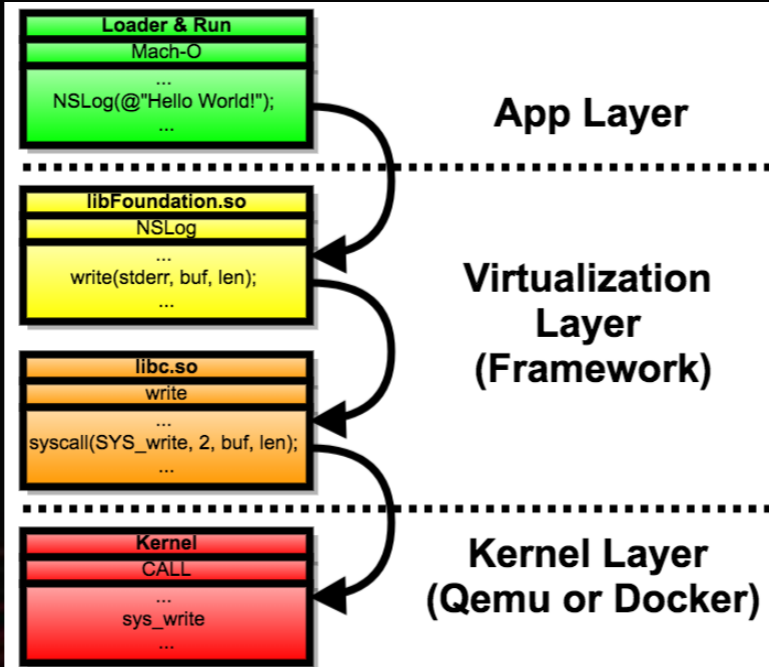
▼ Section64 (__DATA,__la_symbol_ptr)	Address	Data	Description	Value
Lazy Symbol Pointers	100008010	0000000100007F9C	Indirect Pointer	[0x100008010->_NSLog]

	原地址		新地址
NSLog	slide + 0x100007F9C	->	NSLog@libFoundation.so

API重定向流程



完整运行流程

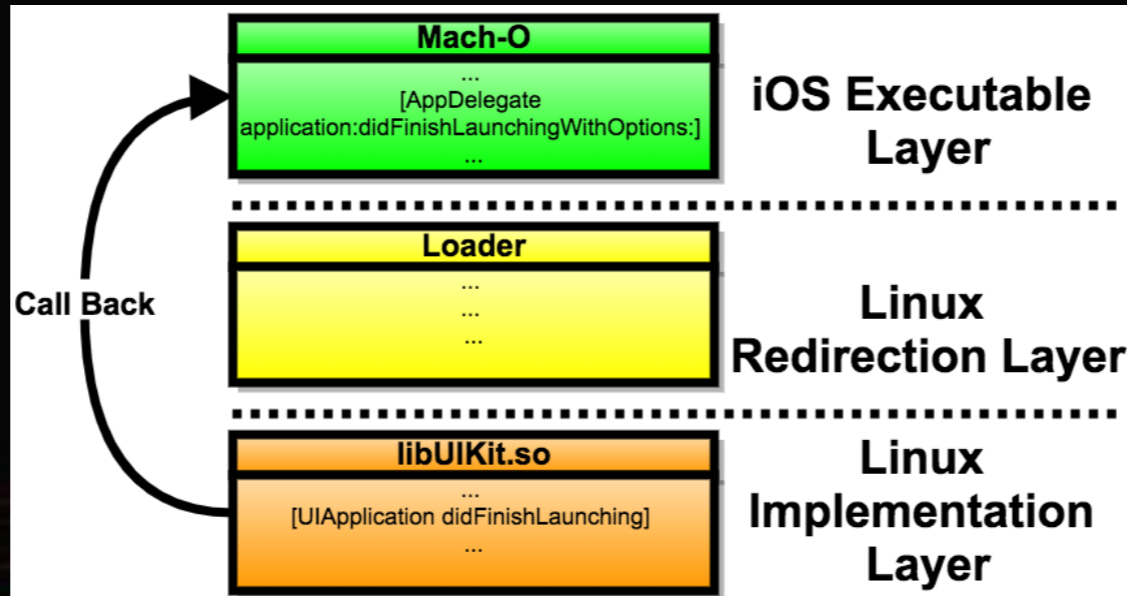


```
root@raspberrypi:~#
root@raspberrypi:~# uname -a
Linux raspberrypi 4.4.1 #3 SMP Sun Sep 25 13:12:50 CEST 2016 armv7l GNU/Linux
root@raspberrypi:~#
root@raspberrypi:~# file /root/iosvm/nslog32
/root/iosvm/nslog32: Mach-O armv7 executable, flags:<NOUNDEFS|DYLDLINK|TWOLEVEL|PIE>
root@raspberrypi:~#
root@raspberrypi:~# run-macho /root/iosvm/nslog32
4 = open$NOCANCEL$UNIX2003(/dev/urandom@0x755dbfa2, 0, 3)
-1 = open$NOCANCEL$UNIX2003(/etc/localtime@0x755dbb7c, 0, 0)
4 = open$NOCANCEL$UNIX2003(/usr/share/zoneinfo/UTC@0x7ef279cf, 0, 48040)
4 = open$NOCANCEL$UNIX2003(/usr/share/zoneinfo/posixrules@0x7ef2790f, 0, 48011)
4 = open$NOCANCEL$UNIX2003(/dev/random@0x755db1f0, 0, 0)
-1 = open$NOCANCEL$UNIX2003(/etc/master.passwd@0x757e0d98, 0, 438)
-1 = open$NOCANCEL$UNIX2003(/etc/master.passwd@0x757e0d98, 0, 438)
-1 = open$NOCANCEL$UNIX2003(/etc/master.passwd@0x757e0d98, 0, 438)
-1 = open$NOCANCEL$UNIX2003(/etc/master.passwd@0x757e0d98, 0, 438)
-1 = open$NOCANCEL$UNIX2003(/etc/master.passwd@0x757e0d98, 0, 438)
-1 = open$NOCANCEL$UNIX2003(/usr/share/locale/en_GB.UTF-8/LC_COLLATE@0x7ef2959e, 0, 438)
3 = open$NOCANCEL$UNIX2003(.@0x755d8791, 0, 34705)
-1 = open$NOCANCEL$UNIX2003(/usr/share/locale/en_GB.UTF-8/LC_COLLATE@0x7ef296fe, 0, 438)
-1 = open$NOCANCEL$UNIX2003(/usr/share/locale/en_GB.UTF-8/LC_COLLATE@0x7ef2942e, 0, 438)
3 = open$NOCANCEL$UNIX2003(/etc/timezone@0x74f081b0, 0, 438)

Unable to create time zone for name: 'E'
(source '(null)').
61 = write$NOCANCEL$UNIX2003(2, 0x74f08780, 61)

You can override the timezone name by setting the 'Local Time Zone'
NSUserDefaults via the 'defaults' command line utility, a Preferences
application, or some other utility.
eg "defaults write NSGlobalDomain 'Local Time Zone' 'Africa/Nairobi'"
See '(null)'
for the standard timezones such as 'GB-Eire' or 'America/Chicago'.
324 = write$NOCANCEL$UNIX2003(2, 0x74f08f90, 324)
2019-05-20 11:10:52.883 nslog32[5736:1961886520] Using time zone with absolute offset 0.
2019-05-20 11:10:52.824 nslog32[5736:1961886520] Hello World!
root@raspberrypi:~#
```

回调流程



```
root@raspberrypi:~# uname -a
Linux raspberrypi 4.4.1 #3 SMP Sun Sep 25 13:12:50 CEST 2016 armv7l GNU/Linux
root@raspberrypi:~# file /root/iosvm/uiapplicationmain32
/root/iosvm/uiapplicationmain32: Mach-O armv7 executable, flags:<NOUNDEFS|DYLDLINK|TWOLEVEL|PIE>
root@raspberrypi:~#
root@raspberrypi:~# run-macho /root/iosvm/uiapplicationmain32
4 = open$NOCANCEL$UNIX2003(/dev/urandom@0x755bcfaa, 0, 3)
-1 = open$NOCANCEL$UNIX2003(/etc/localtime@0x755bcb84, 0, 0)
4 = open$NOCANCEL$UNIX2003(/usr/share/zoneinfo/UTC@0x7e8ba9bf, 0, 52144)
4 = open$NOCANCEL$UNIX2003(/usr/share/zoneinfo/posixrules@0x7e8ba8ff, 0, 52115)
4 = open$NOCANCEL$UNIX2003(/dev/random@0x755bc1f8, 0, 0)
objc_msgSendSuper2: undefined symbol
3 = open$NOCANCEL$UNIX2003(./@0x755b9799, 0, 38809)
-1 = open$NOCANCEL$UNIX2003(/etc/master.passwd@0x757cd198, 0, 438)
-1 = open$NOCANCEL$UNIX2003(/etc/master.passwd@0x757cd198, 0, 438)
-1 = open$NOCANCEL$UNIX2003(/etc/master.passwd@0x757cd198, 0, 438)
-1 = open$NOCANCEL$UNIX2003(/etc/master.passwd@0x757cd198, 0, 438)
-1 = open$NOCANCEL$UNIX2003(/etc/master.passwd@0x757cd198, 0, 438)
-1 = open$NOCANCEL$UNIX2003(/etc/master.passwd@0x757cd198, 0, 438)
-1 = open$NOCANCEL$UNIX2003(/etc/master.passwd@0x757cd198, 0, 438)
-1 = open$NOCANCEL$UNIX2003(/usr/share/locale/en_GB.UTF-8/LC_COLLATE@0x7e8bc02e, 0, 438)
-1 = open$NOCANCEL$UNIX2003(/usr/share/locale/en_GB.UTF-8/LC_COLLATE@0x7e8bc18e, 0, 438)
-1 = open$NOCANCEL$UNIX2003(/usr/share/locale/en_GB.UTF-8/LC_COLLATE@0x7e8bbebe, 0, 438)
6 = open$NOCANCEL$UNIX2003(/etc/timezone@0x74f08eb0, 0, 438)

Unable to create time zone for name: 'E'
(source '(null)').
61 = write$NOCANCEL$UNIX2003(2, 0x74f09480, 61)

You can override the timezone name by setting the 'Local Time Zone'
NSUserDefaults via the 'defaults' command line utility, a Preferences
application, or some other utility.
eg "defaults write NSGlobalDomain 'Local Time Zone' 'Africa/Nairobi'"
See '(null)'
for the standard timezones such as 'GB-Eire' or 'America/Chicago'.
324 = write$NOCANCEL$UNIX2003(2, 0x74f09cd0, 324)
2019-08-14 02:52:42.997 uiapplicationmain32[32545:1961886520] Using time zone with absolute offset 0.
2019-08-14 02:52:42.950 uiapplicationmain32[32545:1961886520] Unable to get name of current host - using 'localhost'
-1 = open$NOCANCEL$UNIX2003(/usr/share/locale/en_GB.UTF-8/LC_CTYPE@0x7e8bc5e0, 0, 438)
7 = open$NOCANCEL$UNIX2003(/root/slide@0x72a13d3d, 0, 438)
2019-08-14 02:52:44.687 uiapplicationmain32[32545:1961886520] AppDelegate-application:didFinishLaunchingWithOptions:
2019-08-14 02:52:44.708 uiapplicationmain32[32545:1961886520] AppDelegate-applicationDidBecomeActive:
||
```



部署

更好适配

ODM (Original Design Manufacturer)



PART
04

一些实践





谢谢观看

演讲人：朱学文 (Ju Zhu)

