

iOS安全研究及实践分享

信息安全部 高雪峰



MAC地址随机化

在设备安全防丢失方面Find my iphone里增加了“send last location”，

信息收取的详细信息增加了请勿打扰模式，信息黑名单还会远么...

Touch ID的API接口开放，肯定带来内部安全认证和授权的新方式，但不可能出现密码认证取代密码

Beta2版本新增来电归属地显示

原有iOS7安全特性：

电话号码黑名单

iMessage垃圾信息处理机制

Activation Lock：绑定apple ID，防丢失

iOS不支持java和Flash，减少受攻击面

iOS精简代码 /bin/sh

权限分离 不同的user group分离进程 mobile用户权限

代码签名 苹果安全审核

DEP 不允许数据的执行

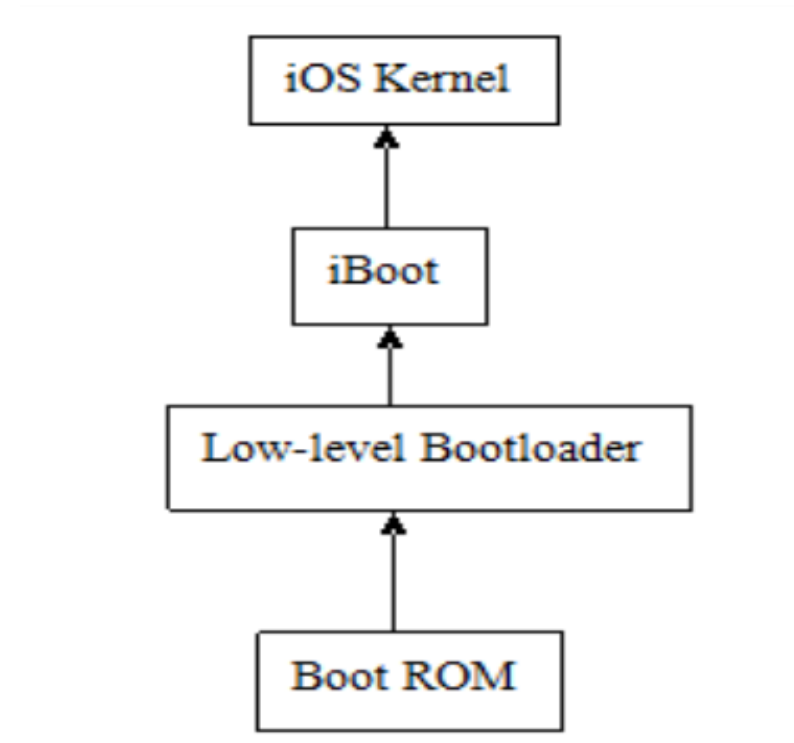
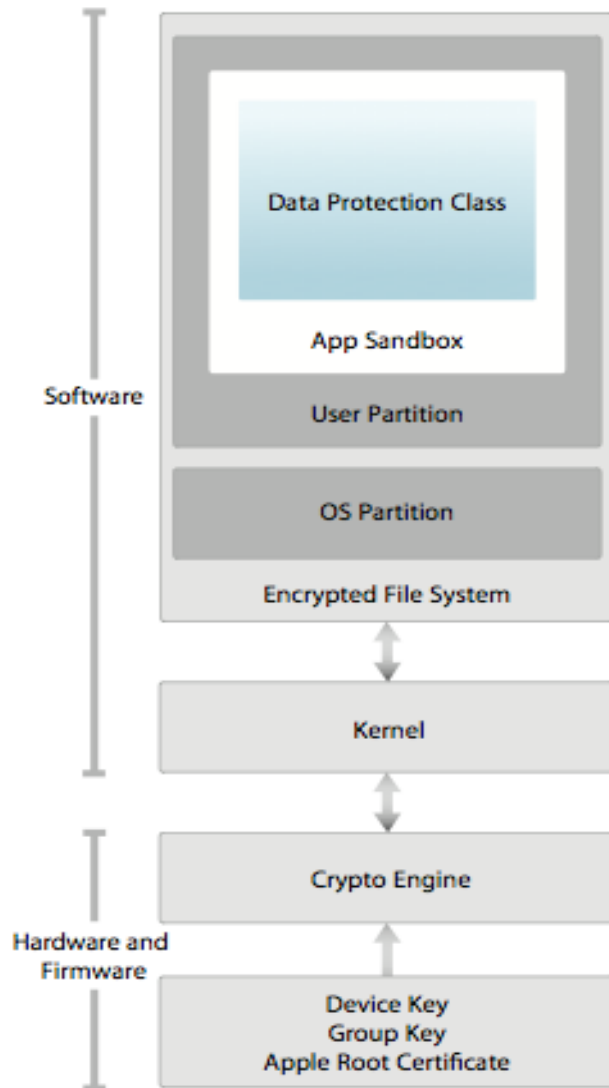
ASLR 二进制文件，库文件，动态链接文件，栈和堆内存地址全部随机化

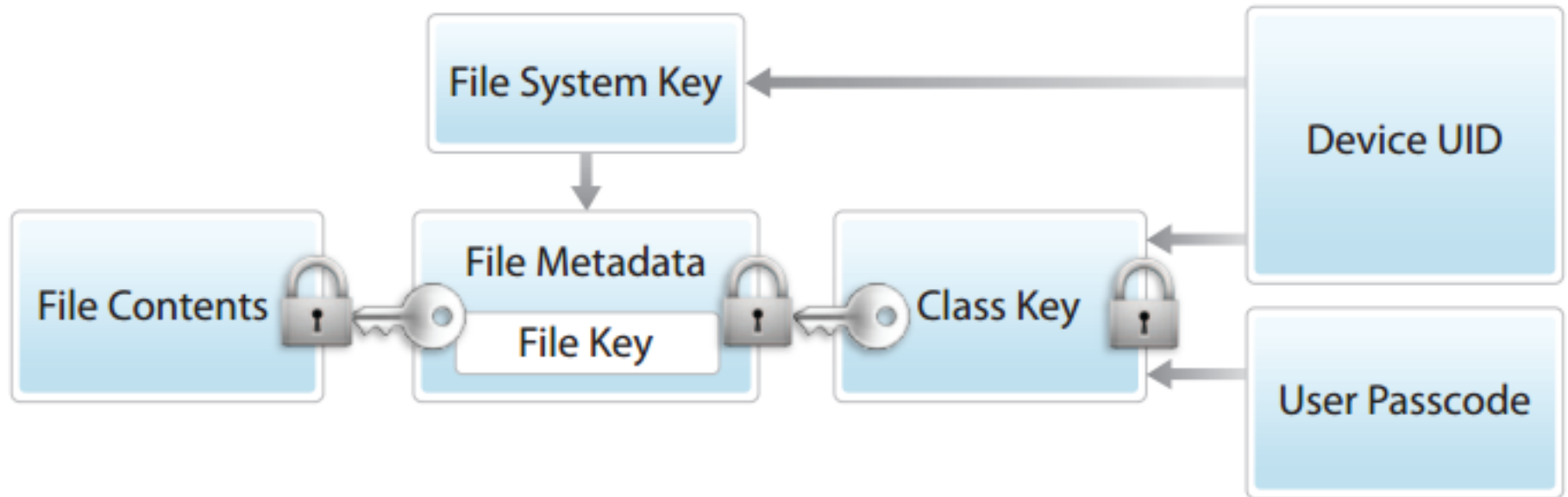
Sandbox 限制对设备造成破坏，增加攻击难度

iOS安全发展史：

iOS 1.x无沙盒及内存保护措施 iOS 3.x 引入沙盒，DEP，代码签名

iOS 4.3 ASLR保护 iOS 5.X ASLR保护改进 iOS 6.0 内核ASRL保护





Availability	File Data Protection	Keychain Data Protection
When unlocked	NSFileProtectionComplete	kSecAttrAccessibleWhenUnlocked
While locked	NSFileProtectionCompleteUnlessOpen	N/A
After first unlock	NSFileProtectionCompleteUntilFirstUserAuthentication	kSecAttrAccessibleAfterFirstUnlock
Always	NSFileProtectionNone	kSecAttrAccessibleAlways

设置-密码-抹掉数据(连续输错十次抹掉所有数据)

```
iphone4:~ root#  
iphone4:~ root# ./FileDP -f early_random-paper.pdf  
2014-06-23 18:14:16.866 FileDP[785:707] prot type is NSFileProtectionCompleteUnlessOpen  
iphone4:~ root#
```

```
iphone4:~ root#  
iphone4:~ root# xxd early_random-paper.pdf  
xxd: early_random-paper.pdf: Operation not permitted  
iphone4:~ root#
```

7.X版本的漏洞，7.1.1修复

```
<@appleimap.163.com/INBOX.imapmbbox/Attachments/151/2 root# ./FileDP -f early_random-paper.pdf  
2014-06-23 18:50:55.518 FileDP[8584:507] prot type is NSFileProtectionCompleteUntilFirstUserAuthentication
```

```
<30@appleimap.163.com/INBOX.imapmbbox/Attachments/151/2 root# xxd early_random-paper.pdf  
0000000: 2550 4446 2d31 2e35 0a25 d0d4 c5d8 0a31  %PDF-1.5.%.....1  
0000010: 3020 3020 6f62 6a20 3c3c 0a2f 4c65 6e67  0 0 obj <<./Leng  
0000020: 7468 2032 3430 3220 2020 2020 200a 2f46  th 2402 ./F  
0000030: 696c 7465 7220 2f46 6c61 7465 4465 636f  ilter /FlateDeco
```

Keychain的实体是sqlite: 用户保存手机上的敏感信息, wifi/mail/vpn帐号密码等, 也提供API供第三方程序保存登录凭据

NSFileProtectionNone类别存储

/usr/libexec/securityd决定进程访问

```
Generic Password
-----
Service: AirPort
Account: 360-ZS366A
Entitlement Group: apple
Label: (null)
Generic Field: (null)
Keychain Data: 12345678

Generic Password
-----
Service: AirPort
Account: Xingfusanqianli
Entitlement Group: apple
Label: (null)
Generic Field: (null)
Keychain Data: xingfusanqianli
```

Apple configurator

功能禁用

(仅对属于企业的iOS设备以及被监管的Android设备)

- ☒ 禁用摄像头   (iOS设备禁用摄像头会同时禁用FaceTime)
- ☒ 禁用FaceTime 
- ☐ 禁用WIFI 
- ☐ 禁用移动数据网络(2G/3G/4G) 
- ☐ 禁用蓝牙 
- ☒ 禁止进入个人区  (仅对Android4.2以下设备生效)
- ☐ 禁用屏幕快照 
- ☐ 禁止安装应用程序 
- ☐ 禁止移除应用程序  (监管设备有效)
- ☐ 禁止应用程序内购买 
- ☐ 禁止iCloud云备份 
- ☐ 禁止iCloud文稿与数据 
- ☐ 禁止iCloud钥匙串 
- ☐ 强制对备份进行加密 

keychain查看工具：keychain dumper

socket连接监控：lsock需越狱设备，只有源码，需编译成arm版本的二进制文件

逆向分析工具：

otool 分析lib库，头文件

class-dump-z dump头文件

Clutch 自动破解ipa还是有帮助的

cycrypt 动态调试，和GDB各有好处，GDB在arm64不好调

IDA 破解版不支持arm的F5功能

Hopper 这个还是ida核心改的，ida在arm的F5功能反编译出来的源码

removePIE 去除ASLR

安全审计：iAuditor 初级审计

网络分析：

ssl kill switch + BurpSuite

Rvictl

tcpdump

文件系统监控工具：filemon.iOS

文件加密类型检测工具：FileDP

Cookies.binarycookies读取工具 BinaryCookieReader.py

文件取证分析：

APP行为分析：

网络通信分析：

runtime分析：

IPC通信（Protocol handler）：URLScheme

逆向APP可以看到，应用、框架、驱动等都是以bundle的形式存储在磁盘上

bundle目录结构：

Info.plist - 对该bundle的描述（XML格式）

Mach-o – 可执行文件 (OS X)

Resource - 资源文件，一般是图片和界面资源

_CodeSignature - 签名信息

通讯数据包分析:

监听HTTP/HTTPS/UIWebView

1.http代理工具iOS SSL kill switch + Burp Suite

2.程序Hook方式: httppeek.dylib httppeek.plist对应app的bundle

UDID 数据泄漏和校验:

UDID = SHA1(Serial Number + ECID + LOWERCASE (WiFi Address) +
LOWERCASE(Bluetooth Address))

[UIDevicecurrentDevice].uniqueIdentifier变为私有API

```
otool -v -s __TEXT __objc_methname /Applications/360safe.app/360safe | grep  
uniqueIdentifier
```

代码如使用 [UIDevicecurrentDevice].uniqueIdentifier 将会被提示

```
maxde-iPhone:~ root# otool -v  
00651d2e uniqueIdentifier
```

通讯安全:

与服务器之间的通信采用HTTPS

使用了一些不安全的方法如allowAllowsAnyHTTPSCertificate,使得用户可以在没有警告的提示下接受无效证书

```
===== BEGINNING OF PROCEDURE =====  
  
; Basic Block Input Regs: lr - Killed Regs: r0  
+[NSURLRequest(NSURLRequestWithIgnoreSSL) allowsAnyHTTPSCertificateForHost:]_88020:  
00088020 0120      movs     r0, #0x1  
00088022 7047      bx       lr  
; endp
```

URL Schemes

提供了一个应用程序间或者safari可以启动他的方法


URL Schemes可能带来漏洞

键盘缓存

/private/var/mobile/Library/Keyboard/dynamic-text.dat

```
DynamicDictionary-5baidunbdeyesitecnadmmmscomonternetvduyetsinahttplocalhosthttpqghttplocalhosthttpsohtmlweixinmailcorpqihoonetwhat'smatte
rI'mChineseahackerqihoosslcercomcomcomcomcomwxqqcomqqcommailcomcomcomimperialvioletorgorgorghsocomworkftpdriveftphttpshowrunleegmailhideshowrun
leegmailftpdoubandoubancomqqcomcomWhatsAppgaoxuefengxaaxdexbfcomimperialvioletorgorgcomcomcomgocomorggohttpsgotofailgotocomcomSBbeevilcomwhatsa
ppimagexyzwhatsappimagexyzwhatsappimagexyzwhatsappimagexyzGuDongimagexyzGuDongiamgecallframesrcGuDongimagexyzlxapiqihucassetpngiframesrctelifr
ameiframeteliframesrcteliframeiscanonlineoniscanbincombyodzwqihootelcomJadminapiassetbaidubebinbyodccallcerChineseecncomcorpdoubandriveevilftpg
aoxuefengmailgoqotogotofailGuDonghackerhomehtmlhttphttpsiamgeiframetI'mimageimperialvioletiscanleelocalhostlxmmailmattermmmscomonternetnbdedaven
```

keymonitor 类似与木马程序

360云盘	 @163.com	2014-03-06 23:31:34
360云盘	123355	2014-03-06 23:31:37
360云盘	123355	2014-03-06 23:31:38

NSUserDefaults、Sqlite保存用户名密码

knowledgeBaseUrl	String	115.29.236.21	
lastLoginAddress	Data	<1002f4fb d3977e62 00000000 00000000>	
password	Data	<d93ae659 92caf6a8 751e334d 0a716ad8>	
phoneNumber	String	13811016304	0

10	RequirePasswordLock	0
11	PasswordForLockScreen	1236
12	GesturePasswordLock	1
13	ClassifyAlbumListType	0

破壳mach-o: dumpdecrypted.dylib、clutch、手动解密

removePIE去掉app的ASLR地址随机化

▼ Linking

Setting	Calculator
Bundle Loader	
Compatibility Version	
Current Library Version	
Dead Code Stripping	Yes ↕
Display Mangled Names	No ↕
► Don't Create Position Independent Executables	No ↕
Don't Dead-Strip Inits and Terms	No ↕

```
childsafe (architecture armv7s):
```

```
Mach header
```

magic	cputype	cpusubtype	caps	filetype	ncmds	sizeofcmds	flags
MH_MAGIC	ARM	V7S	0x00	EXECUTE	44	5008	NOUNDEFS DYLDLINK TWOLEVEL WEAK_DEFINES BINDS_TO_WEAK PIE

```
childsafe (architecture armv7):
```

```
Mach header
```

magic	cputype	cpusubtype	caps	filetype	ncmds	sizeofcmds	flags
MH_MAGIC	ARM	V7	0x00	EXECUTE	44	5008	NOUNDEFS DYLDLINK TWOLEVEL WEAK_DEFINES BINDS_TO_WEAK PIE

```
iPhone5S:/var/mobile/Applications/4A2C3A72-1213-4F89-9C18-0633CE83E5AF/childsafe.app root#
```


GADBannerView

```
ldr    r1, [r0]                ; @selector(setAdUnitID:)
add    r2, pc                  ; 0x21c0
mov    r0, r6
add    r7, sp, #0xc
blx    imp__symbolstub1__objc_msgSend

function sub_1328 {
    r5 = r1;
    [r6 setAdUnitID:@"a152ae87a0c0cfb"];
    Pop();
    Pop();
    Pop();
    Pop();
    Pop();
    r0 = (*_logos_orig$_ungrouped$GADBannerView$loadRequest$)(r6, r5, r4,
*_logos_orig$_ungrouped$GADBannerView$loadRequest$);
    return r0;
}
```

方法1: 动态链接库注入, set DYLD_INSERT_LIBRARIES

```
void *dlopen( const char * pathname, int mode)
```

```
void *dlsym(void* handle,const char* symbol)
```

```
export DYLD_INSERT_LIBRARIES=dumpdecrypted.dylib
```

方法2: Cypcript, 利用objc_msgSend消息机制



```
cy# a.visibleViewController.videoAlbum->isa.messages  
{isOnlyFromSOHU:0x38da85,selectedVideoSource:0x38e4d9,isFromSOHU:0x38e605,  
SelectedVideoSource:"":0x38e605,"initWithAlbumInfoJSONDictionary:"":0x38dae5,  
sources:"":0x38dae5,selectedVideoSourceID:0x38e389,"setSelectedVideoSource:  
e:"":0x38e491,dealloc:0x38d801,cid:0x37fb81,albumInfo:0x386441,cateCod  
Vid:0x38c181,"initWithSingleVideoItemJSONDictionary:"":0x37f601,"setCid:  
":0x3863bd,hasOriginal:0x388f15,"initWithSingleVideoItem:"":0x37f4a9,canBe  
vailable:0x386121,canBeDownloaded:0x75efc1,"setCid:"":0x386375,currSiteId:  
x386311,"setAlbumInfo:"":0x386451,"loadRecommendWithVid:pageSize:siteId:
```

```
cy# a.visibleViewController.videoAlbum->isa.messages ['canBeDownloaded'] = function() {return YES;}
function () {return YES;}
cy#
```

Thoes

```
NIC 2.0 - New Instance Creator
-----
[1.] iphone/application
[2.] iphone/cyldget
[3.] iphone/framework
[4.] iphone/library
[5.] iphone/notification_center_widget
[6.] iphone/preference_bundle
[7.] iphone/sbsettingstoggle
[8.] iphone/tool
[9.] iphone/tweak
[10.] iphone/xpc_service
Choose a Template (required):
```

```
#define kYearInterval 1161536000.0

%hook UserModel

- (BOOL)isVip
{
    return YES;
}

- (NSString *)vipExpire
{
    NSDate *date = [[NSDate date] dateByAddingTimeInterval:kYearInterval];
    NSDateFormatter *dateFormatter = [[[NSDateFormatter alloc] init] autorelease];
    [dateFormatter setDateFormat:@"yyyy-MM-dd HH:mm:ss"];
    return [dateFormatter stringFromDate:date];
}

%end
```

Method Swizzling



Jaibreak -- iOS安全永恒的主题

