iOS8应用安全新挑战

李俱顺
<s1mbily@557.im>

开放 合作 共赢

个人简介

- 支付宝安全工程师
- 关注客户端安全/开发
  - Windows客户端
  - 移动/无线端安全
- 偶尔写写服务端程序，也喜欢搞搞渗透测试
- 伪Geek

iOS8新变化

- Swift新语言
- App的新存在形式：扩展(Extension)
- 4000+新API
- and etc...

Swift

- 新的语言
  - 五仁月饼？
- 号称更快的执行速度
  - 比Objective-C快
- 更丰富的语法糖
  - 一辈子的中括号终于不会用光了

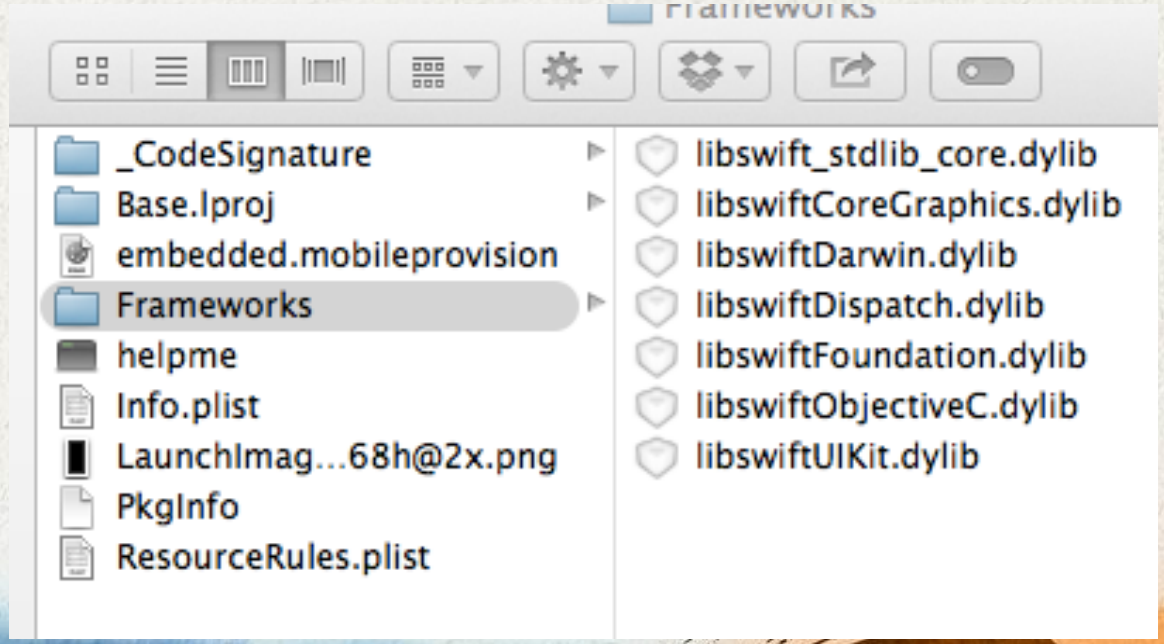
```
import UIKit

class RootViewController: UIViewController, UIPa

    var pageViewController: UIPageViewController


    override func viewDidLoad() {
        super.viewDidLoad()
        // Do any additional setup after loading
        // Configure the page view controller an
        self.pageViewController = UIPageViewCont
            navigationOrientation: .Horizontal,
        self.pageViewController!.delegate = self

        let startingViewController: DataViewCont
            viewControllerAtIndex(0, storyboard:
        let viewControllers: NSArray = [starting
        self.pageViewController!.setViewControll
            animated: false, completion: {done i

        self.pageViewController!.dataSource = se

        self.addChildViewController(self.pageVie
        self.view.addSubview(self.pageViewContro
```

Swift

- 编译过程新变化
  - swift->clang替代了clang->clang
  - 再见rewrite-objc：除了逆向外更难进行实现分析

Swift

- 结构变化
  - 嘿，我有自己的Framework了！



Swift

- 运行时新变化：
  - 再见，objc_msgSend
  - 或者叫Objective-C without message?

Swift

- Swift逆向Tips
  - Name mangling: _TFC10swift_204811AppDelegate27applicationWillResignActivefS0_FCSo13UIApplicationT_/_TToC10swift_204811AppDelegate27applicationWillResignActivefS0_FCSo13UIApplicationT_
  - 参数传递顺序：type method(arg1,..., id self)
  - Object struct/vtables

Swift

- 如何攻击？
  - 再见，method swizzling
  - 感谢Mobile Substrate，还可以用
    - No MSHookMessage

Swift

- 如何防御
  - 一些针对OC的动态特性的加固方法已经不再适用(如: #define trick)
  - 增强调用间验证机制(anti-hook)
- 建议谨慎选择Swift

扩展

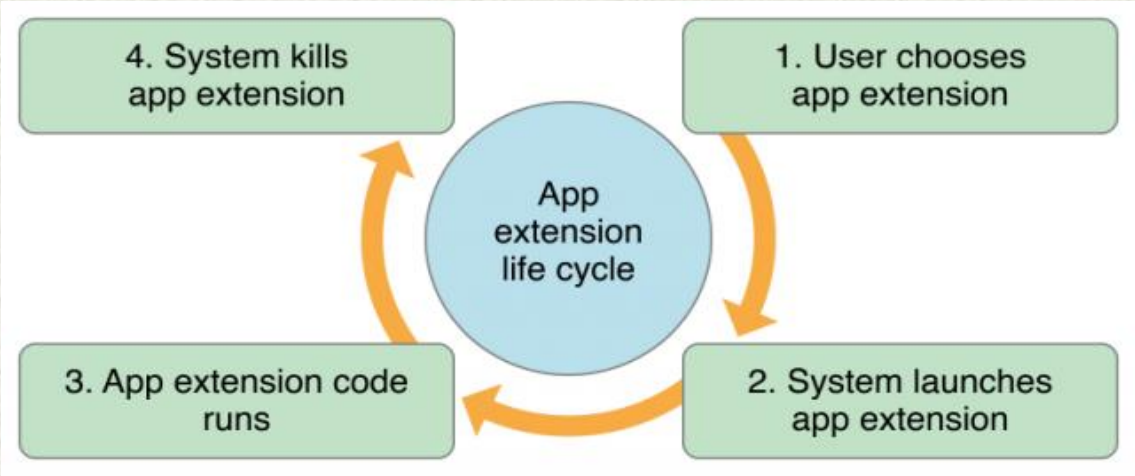
- 不同于应用的架构
- 更加紧密的应用间交互
  - 我：不越狱用上第三方输入法了
  - 产品经理：终于不用应用间跳转啦

扩展

- 扩展的本质
  - Plugins本质是一个普通的binary程序的bundle，主程序包含Entitlements声明。
  - 借助XPC Services唤起，可以展示一个UIViewController
  - 比如之前的MFMessageComposeViewController？

扩展

- 生存周期



- 无法与主程序直接通讯
  - 当然也不在调用者程序空间

扩展

- 安装路径变化
  - Base: private/var/mobile/Containers
  - 应用：Bundle/Application/<uuid>
  - 扩展：<appPath>/PlugIns/
  - 资源文件：Data/Application/<UUID>/

扩展

- 安全威胁
  - 希望XPC不出什么问题
  - 共享数据的安全性
    - NSFileCoordination
    - CoreData
    - sqlite
    - keychain
    - NSUserDefaults

扩展

- 安全威胁
  - 第三方键盘，用户输入隐私怎么办？

扩展

- 防御方案
  - 对第三方键盘 say no
  - Keychain安全数据共享
  - 信息加密安全共享

APIs

- 新增4000+API
  - Wow！
  - 不是全部与安全有关 (谢天谢地!)

CloudKit

- iCloud云端存储API
  - 创建共享存储空间/私有存储空间
  - 私有敏感数据应选择 CKContainer.privateCloudDatabase

LocalAuthentication

- TouchID开放API
  - [LAContext evaluatePolicy:localizedReason:reply:]
- 获取不到指纹内容，只有一个结果block
  - 应用场景：本地认证

WKWebView

- 更快的WebView，更多的H5应用
- 当心JSBridge
  - -[WKUserContentController addScriptMessageHandler:name:]
  - -[WKUserContentController addUserScript:]

其他变化

- Xcode不再提供完全iOS framework

```
→ Current  ARCH=armv7 jtool -v -l IOKit

LC 00: LC_SEGMENT              Mem: 0x00000000-0x0005c000      File: 0x00000000-0x00000000     r-x/r-x __TEXT
       Mem: 0x00000000-0x00000000      File: 0x00000000-0x00000000            __TEXT.__text                    (Normal)
       Mem: 0x00000000-0x00000000      File: 0x00000000-0x00000000            __TEXT.__picsymbolstub4__TEXT
       Mem: 0x00000000-0x00000000      File: 0x00000000-0x00000000            __TEXT.__stub_helper             (Normal)
       Mem: 0x00000000-0x00000000      File: 0x00000000-0x00000000            __TEXT.__cstring                 (C-String Literals
       Mem: 0x00000000-0x00000000      File: 0x00000000-0x00000000            __TEXT.__const
LC 01: LC_SEGMENT              Mem: 0x0005c000-0x00061000      File: 0x00000000-0x00000000     rw-/rw- __DATA
       Mem: 0x00000000-0x00000000      File: 0x00000000-0x00000000            __DATA.__nl_symbol_ptr
       Mem: 0x00000000-0x00000000      File: 0x00000000-0x00000000            __DATA.__la_symbol_ptr
       Mem: 0x00000000-0x00000000      File: 0x00000000-0x00000000            __DATA.__const
       Mem: 0x00000000-0x00000000      File: 0x00000000-0x00000000            __DATA.__cfstring
       Mem: 0x00000000-0x00000000      File: 0x00000000-0x00000000            __DATA.__data
       Mem: 0x00000000-0x00000000      File: 0x00000000-0x00000000            __DATA.__common                  (Zero Fill)
       Mem: 0x00000000-0x00000000      File: 0x00000000-0x00000000            __DATA.__bss                     (Zero Fill)
LC 02: LC_SEGMENT              Mem: 0x00061000-0x0008048c      File: 0x00000648-0x0001fad4     r--/r-- __LINKEDIT
LC 03: LC_ID_DYLIB             /System/Library/Frameworks/IOKit.framework/Versions/A/IOKit (compatibility ver: 1.0.0, current ver
```

致谢

- 系统安全的各位小伙伴们
- 感谢程君、火翼[CCG]、nekizhang对内容的建议
- 感谢Evan Swick、John McCall、Jonathan Levin的无私分享

END

Q&A 谢 谢！

开放 合作 共赢