iOS軟體逆向工程應用 & 手機遠程監控技術

大可(Dark)

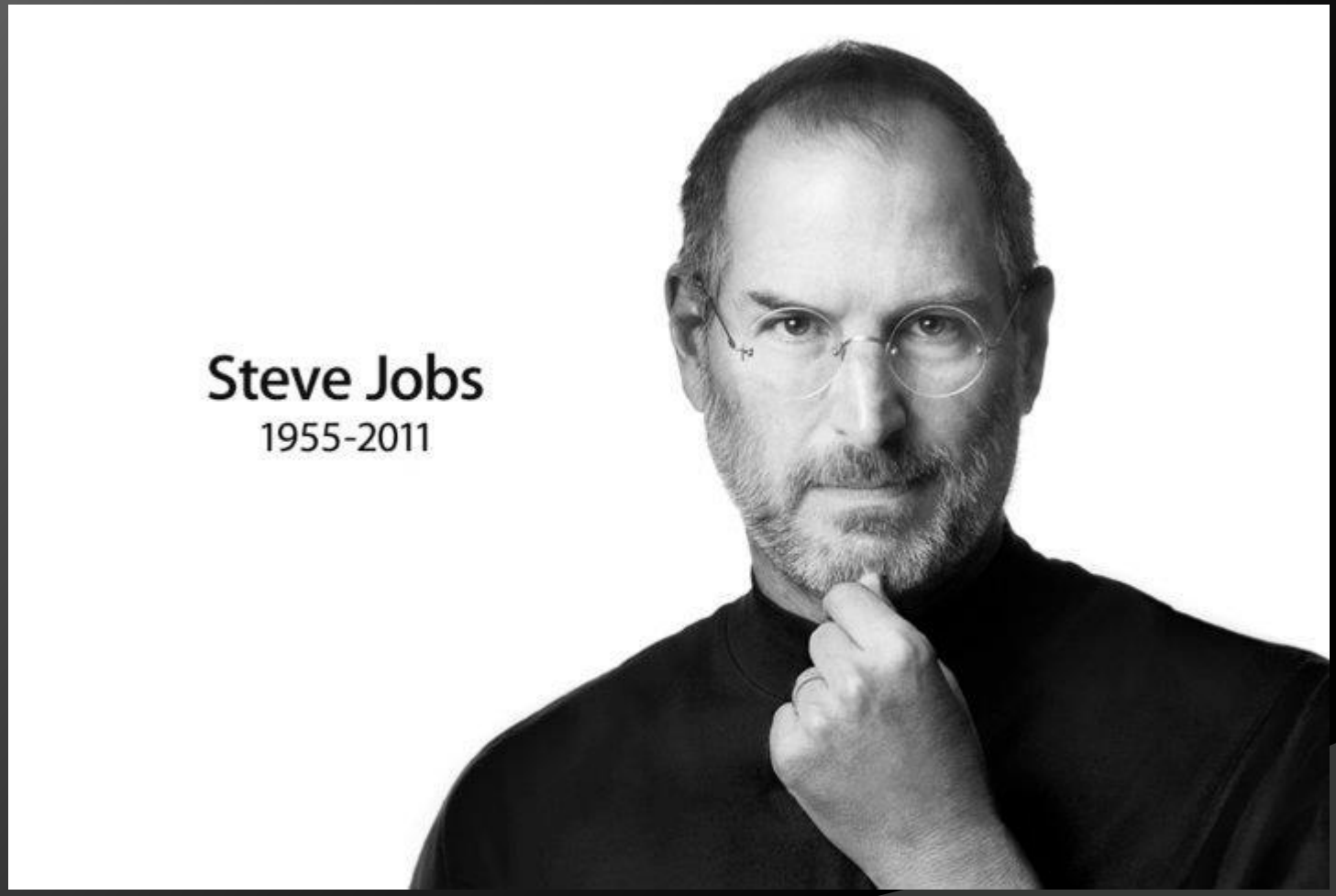
經歷

- PHATE Security- 創辦人
- Zuso Security - 成員
- Chroot - 成員
- 吉瑞科技 - R&D
- 網駭科技 - R&D
- 某警調單位 - 外聘顧問
- 資策會 - 教育訓練講師
- 中科院 - 教育訓練講師

內容簡介

- iOS 軟體逆向工程應用
  - IAP (In-App-Purchases) 破解技術
  - 遊戲作弊引擎設計
- iOS遠程控制軟體設計

謹以此紀念Steve Jobs



iOS 軟體逆向工程技巧

iOS APP簡介

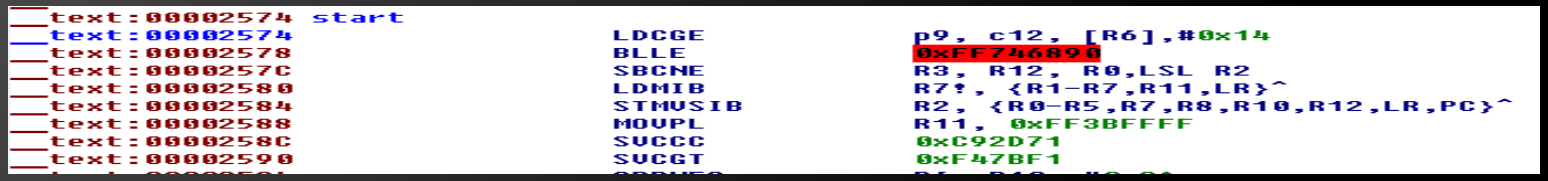
- 執行檔格式
  - Mach-O
- 組合語言格式
  - ARMv6
    - Thumb
  - ARMv7
    - Thumbv2

工具

- 已JB的iphone
- GDB
  - 動態分析
- IDA Pro
  - 靜態分析
- otool
  - 觀察mach-o執行檔結構
- class-dump
  - 將執行檔中的objective C classes輸出成.h

拿IDA Pro開刀前...

- 將加密的code還原
  - otool –l filepath | grep ‘crypt’ (確定加密的位置&大小)
  - 使用gdb將程式執行後~把該區域dump出來
  - 重新塞入執行檔



DEMO

Binary Patching

- 找出要修改的位置
- 利用ARM Assembler組譯
  - 找出對應OP Code
- 修改，並重新簽章

DEMO

繞過IAP (In-App-Purchases)檢查

兩種繞過IAP介面的通用方式

- 從執行檔下手-分析IAP – API
  - -需JB
- 架設假IAP認證伺服器 (MITM SSL Proxy Server)
  - -不需JB

IAP流程 – 從API角度看

建立SKPaymentTransaction class
根據購買狀態將SKPaymentTransaction transactionState區分為
SKPaymentTransactionStatePurchasing
SKPaymentTransactionStatePurchased
SKPaymentTransactionStateFailed
SKPaymentTransactionStateRestored
購買狀態若有變化，則會呼叫
(void)paymentQueue:(SKPaymentQueue *)*queue* updatedTransactions:(NSArray *)*transactions*
Developer可根據transactions的類型來決定內購各種狀態變化所要呈現的東西
Sample:

```
- (void)paymentQueue:(SKPaymentQueue *)queue updatedTransactions:(NSArray *)transactions
{
    for (SKPaymentTransaction *transaction in transactions)
    {
        switch (transaction.transactionState)
        {
            case SKPaymentTransactionStatePurchased:
                if([self putStringToItunes:transaction.transactionReceipt]){
                    //許多developer會認為程式運作到這，就已經購買成功，而沒再做訂單驗證
                }
                  break;
          }
     }
}
```

Apple IAP收據驗證伺服器

- https://buy.itunes.apple.com/verifyReceipt
  - 將訂單轉json傳入伺服器即可驗證
  - 驗證完會收到訂單資訊，status 0代表付款已完成
  - 如下

{"receipt":{"original_purchase_date_pst":"2012-07-12 05:54:35 America/Los_Angeles", "purchase_date_ms":"1342097675882", "original_transaction_id":"170000029449420", "original_purchase_date_ms":"1342097675882", "app_item_id":"450542233", "transaction_id":"170000029449420", "quantity":"1", "bvrs":"1.4", "version_external_identifier":"9051236", "bid":"com.zeptolab.ctrexperiments", "product_id":"com.zeptolab.ctrbonus.superpower1", "purchase_date":"2012-07-12 12:54:35 Etc/GMT", "purchase_date_pst":"2012-07-12 05:54:35 America/Los_Angeles", "original_purchase_date":"2012-07-12 12:54:35 Etc/GMT", "item_id":"534185042"}, "status":0}

Objective-C分析技巧

- b [classname method]
- objc_msgSend
  - objc_msgSend(object_ptr,@selector_name,arg0,arg1)
  - objc_msgSend($r0,$r1,$r2,$r3,…,…)
  - po $r0
- class-dump –H filepath –o output

DEMO

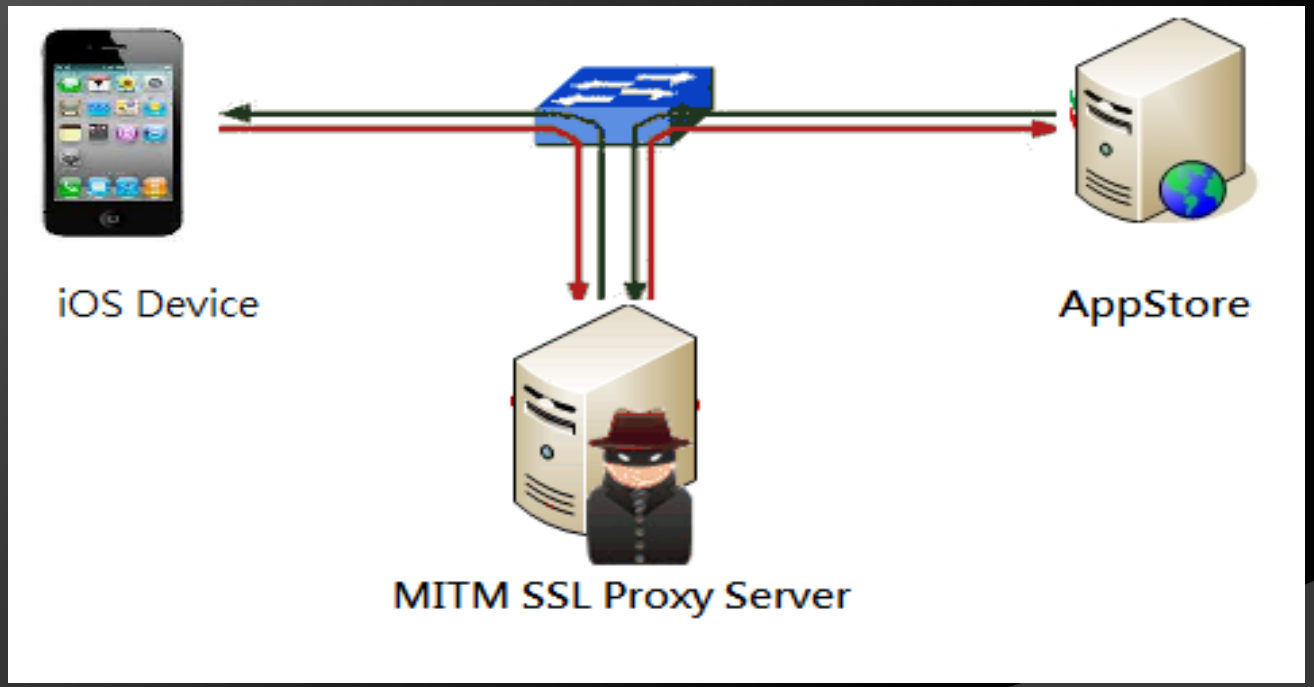
IAP流程 – 從App AppStore看

- App向AppStore發送IAP Request
  - 裡面包含商品資訊
- AppStore向使用者說明付款項目明細
- 使用者確認購買，則從AppStore處理交易 並且回傳訂單收據給APP
- 開發者決定要如何處置訂單收據

```
switch (transaction.transactionState)
    {
        case SKPaymentTransactionStatePurchased:
            if([self putStringToItunes:transaction.transactionReceipt]){
                //許多developer會認為程式運作到這，就已經購買成功，而沒再做訂單驗證
            }
              break;
     }
```

MITM方式繞過IAP機制

- 當App發出IAP Request時攔截該資訊，並取出部分資訊來構造假收據傳回App



其他方式

- 俄羅斯駭客架設DNS Server並把apple server domain name 指向自己ip
  - http://www.in-appstore.com/
  - 優點:
    - 不必擔心別人伺服器會留下自己的IP,或其他紀錄
  - 缺點:
    - 使用時無法上網，因為所有domain name都指向他的ip了
    - 無法購買一些需要網路連線才可購買的東西
    - 架構彈性不夠大，若有除了apple外的額外伺服器驗證，修改會很麻煩

DEMO

iOS遠程控制軟體設計

開發心得

- unix socket
- 關掉螢幕tcp connection會斷掉怎麼辦?
  - 不斷發heartbeat包跟server通訊
- 如何常駐在系統?
  - launchctl load /System/Library/LaunchDaemons/xxx.plist

DEMO

遊戲作弊引擎設計

如何讀寫iOS APP記憶體?

- task_for_pid
  - vm_read_overwrite
  - vm_write
- 設計MobileSubstrate Plugin
  - 就像DLL Injection…

DEMO

參考文獻

- http://developer.apple.com/library/ios/#documentation/StoreKit/Reference/SKPaymentTransaction_Class/Reference/Reference.html
- http://www.iphonedevwiki.net/index.php/MobileSubstrate
- http://www.peter-cockerell.net/aalp/html/frames.html
- http://sources.redhat.com/gdb/documentation/
- iOS.Hackers.Handbook
- Patching_Applications_from_Apple_AppStore_with_additional_protection_by_Reilly
- *感謝皮樂(http://hiraku.tw/)指點repo server架設&打包deb

Thank You!

Q&A

聯絡方式

zusodark@gmail.com