電子支付開放 企業主您準備好了嗎？

撰文 | 叡揚資訊 資安事業處資安顧問　趙若雲

我國電子支付發展落後 且資安意識薄弱

目前國內已於104年4月27日由金融監督管理委員會訂定發布「電子支付機構資訊系統標準及安全控管作業基準辦法」全文共24條，並自104年5月3日施行。慶幸的是相關業者終於可以開始拓展相關電子支付業務並提供更為方便的功能給民眾使用，但相對於行動裝置上的資安防護意識，業者是否擁有足夠能量來保障消費者權益？

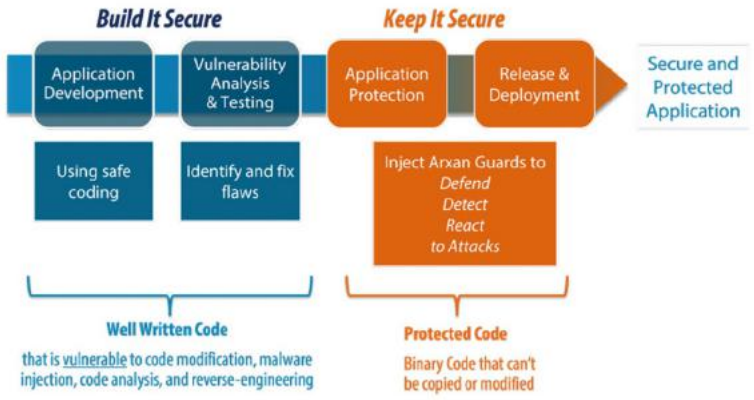
電子支付功能於國外已行之有年，許多對生活更為便利性的應用都在行動APPs上發展，所以對於APPs上的安全防護也都有基本防護觀念去實行，如同國內目前系統上線前都需經過原始碼掃描檢測。在電子支付機構資訊系統標準及安全控管作業基準辦法當中，詳讀內文後能發現，多數規範是針對「主機」端要求，但對APPs的規範寥寥可數，且就行動裝置應用程式部分條文於第十條第四項行動裝置應用程式設計要求中六項規範，就技術層面來看多數處於灰色地帶；而少數國內業者抱持著「資訊安全是為遵循法規而做，而非企業社會責任」，但國內目前行動化應用程式也開始蓬勃發展，就目前觀察分析常見主流APPs來看，多數APPs並無任何防護措施，更何況支付功能已開放，我們的生活必定與APPs息息相關，以及未來IoT（Internet of Things，物聯網）趨勢，無論企業主或消費者，更應多琢磨於行動應用程式安全。

以我們目前的經驗，台灣客戶多數是已被攻擊後才進行相關解決方案的尋找，所以當我們進入專案時面臨的是演算法已外洩、金鑰被竊取或是Web Service被破解，此時所要調整的人力成本遠比原先建置時導入防護高出許多，這點與導入原始碼掃描機制是相同的，受攻擊所面臨最大的挑戰可能不只法律問題而是公司的商譽與客戶信任度已降低。

遵循國際標準 OWASP MOBILE TOP 10

在網頁應用程式開發領域，多數國內業者已將原始碼檢測視為SSDLC必定的一環，許多工程師也培養了撰寫安全程式碼的能力，所以對於OWASP TOP TEN其中A1～A10相關風險已具有一定的防護意識；但APPs所對應的OWASP MOBILE TOP TEN，可以發現其中內容是以針對資料是否落地，主機管控，加密強度是否足夠等，針對行動應用程式常見的風險分類，M1～M10與A1～A10完全不同的風險意識。

↑ M10 Lack of Binary Protection(缺乏執行碼保護) 為 2014 年 OWASP 新增的威脅。



↑單靠原始碼檢測不夠，Arxan 為您 SSSDLC 補足最後高強度的安全防護。

您應該有發現，當進行APPs原碼檢測使用OWASP MOBILE TOP TEN規則時，有些漏洞無法透過程式碼修復，這時您的解決方式為何？行動應用程式我們所面臨到的風險與網站應用程式最大的風險差異性在於，「您的程式在客戶手上」，所以首當其衝的就是面臨反組譯攻擊。

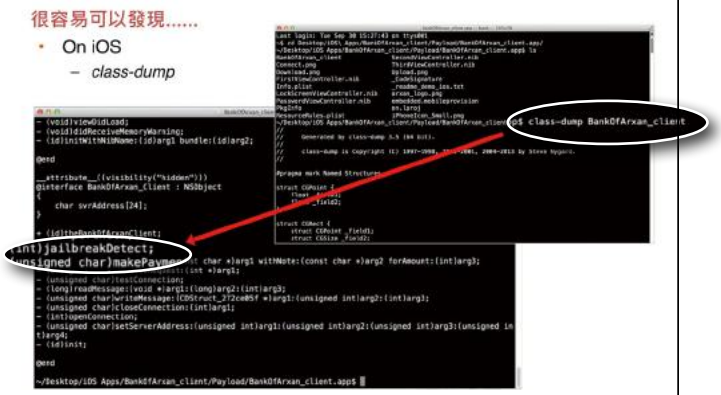
OWASP MOBILE TOP TEN最值得一提的是M10：Lack of Binary Protections，這所謂的Binary指的就是您行動應用程式的APK/IPA的檔案，即使原始碼掃描後修復到都零風險了，但您的Binary是否有做保護？若沒有，請問企業的應用程式程式邏輯、架構、資源檔等，都被看到了，安全嗎？

反組譯工程沒有這麼難

早期我們在進行反組譯工程時，的確需要具備足夠的技術與匹配的工具才能進行，但目前高階語言的盛行（如：JAVA、C#），除了使得程式設計師建立在巨人的背上快速開發之外，也造就了反組譯越來越容易。

如各位所知，Android使用Java語言為Base開發，可以嘗試上網查詢「Android 破解」，等關鍵字，可以顯示出非常多的破解教學或反組譯工具下載，APPs破解已成常態，技術難度低，就連小朋友玩APP遊戲時，也懂得先找破解版，而開發人員對於行動應用程式安全上，無法僅僅由程式碼安全來進行保護，需要有能夠幫助開發人員且不會造成額外負擔的防護工具。

若APPs應用程式沒有做過任何保護，我們可以看到如下圖資訊：



↑未受保護 Apps 不需攻擊工具，亦可分析 Binary 內容。

應用程式中宣告的Function Name非常清楚的顯示出來，當然我們也可以dump出APPs有宣告string的資訊，這兩個動作，決定了攻擊者在分析APPs的掌握度，加上目前破解工具不斷推陳出新，破解速度越來越快，還不保護應用程式嗎？或仍有保護後會降低應用程式效能的思維？

行動APPs實際所面臨的風險

原本在電腦上會遭遇的資安風險，也會在行動裝置上發生，不同的是行動裝置與我們密不可分，使用者行為的改變，操作手機的時間已遠比在電腦上更久，也有更多隱私資料或所依賴的功能性轉移到行動裝置上。試想若有人隨時掌握您的位置、傳送的訊息、照片、通話紀錄、email內容、行事曆等許多個人敏感資訊，想必您應該會非常恐慌。

↑使用者在未知情況下，商用邏輯已被竄改， 駭客可輕易竊取機敏資訊或變更交易行為。

今日多數企業以外包開發APPs藉此降低成本及快速達成業務需求，但風險是應用程式邏輯可能與其他公司一模一樣，當共用元件被破解後，所有APPs將暴露在相同危機當中。此外最近主流APPs開發方式，是利用開發平台撰寫HTML5產生多種平台之應用程式，雖能降低成本、開發快速、但在沒有任何防護的情形下，安全性令人堪憂，如同最新Cordova框架漏洞

（CVE-201501835），攻擊者能利用惡意連結任意竄改相關APP的外觀、內容，甚至讓應用程式當掉。該漏洞可能導致使用者只要點選URL網址，就會遭到攻擊者竄改Android裝置上APP的內容與行為，促使APP完全當掉無法使用。不僅APP可能受影響，只要相關使用Apache Cordova的外掛程式也同樣曝露相同風險中。

透過自動插入Guards技術有效抵抗APPs攻擊

面臨目前已知多種攻擊方式，該如何衡量效能、安全性與成本，達成應盡的企業社會責任；需要的防護機制是完整支援並且擁有多層次架構，可組合多種防護機制進行全面性抵抗攻擊，各功能Guards分類如以下三類說明：

防護技術（Defend）

防護逆向工程反組譯程式碼。在程式執行碼階段進行混淆（obfuscation），程式/字串加密，防監聽（Anti-Debug）與動態隨機執行保護（Guards）。

Arxan Mobile軟體保護 強大與獨特的解決方案

偵測技術（Detect）

防護程式碼竄改與偷取程式碼。包含了checksum確認（竄改偵測）、跨組件認證與監聽模式偵測（debugger detection），其中pre-damage Guards功能能夠當應用程式被攻擊時，破壞程式碼區塊。

反應技術（React）

提供客製化防護機制。Reaction Guards可部署在多種區塊模式，如自行修復程式碼被竄改、或發出訊息給其他元件、結束應用程式等多種可自行彈性設計之技術。

Arxan Mobile軟體保護 強大與獨特的解決方案

Arxan 能保護運行於各式環境之軟體安全，包括行動裝置、電腦、伺服器（server）、嵌入式平台（embedded platforms），以及以物聯網形式串聯的部分。Arxan的設計策略是在Guards及Guard網路，可提供有效與獨特的防護解決方案，以屬性的區分如下：

- **Guard的活動難以追蹤：**Guard能夠自行定義執行階段，執行時可以隨機概率的方式被調用。
- **無單點破壞之問題：**Guard設計使用交互式網路防護，交叉保護之下Guards有足夠能力保護整 體設計架構。
- **可使用多種防護Guards於單一片段程式碼區塊：**Guards可部署多種功能於單一片段，卻可多次執行防護機制。所以當攻擊者辨識出欲攻擊範圍時，需同時將此範圍中的所有Guards移除，除此之外也必須知道這些Guards的設計網路，並一併破解。
- **整合QA：**Guards測試功能可辨識Guard防護是否有效執行，所以當應用程式出現錯誤，可找尋程式碼之問題。

更多客戶案例、資安資源 http://www.gss.com.tw/index.php/focus/security