行動裝置 App 之安全導覽

黃建隆 / 財金資訊公司安控部資訊安全組高級工程師

一、前言

西元 2008 年 Apple 公司第一代 iPhone 誕生，Google 公司的 Android 手機與微軟公司的 Windows Phone 亦隨之而起，直至今日智慧型手機 (Smart phone) 市場已是百家齊鳴。另一方面，2010 年第一代 Apple iPad 問世，為行動裝置開啓另一新頁，掀起平板電腦的戰場風雲，Google、微軟等公司也紛紛推出搭載自己作業系統的平板電腦。

從全球出貨量亦可觀察行動裝置的變化，根據美國國際數據資訊公司 (International Data Corporation，簡稱 IDC) 的手機市場調查報告顯示，智慧型手機的出貨量在 2013 年第一季首次超過傳統功能手機 (Feature phone)。另一方面，2013 年平板電腦的全球出貨量正式超越筆記型電腦，預估 2014 年有機會超越桌上型電腦與筆記型電腦的總和，在在顯示行動裝置是未來主流趨勢。

在行動應用程式 (Mobile applications，簡稱 App) 方面，Apple 官方於 2013 年 5 月 16 日宣布 App Store 下載次數突破 500 億次，而同時間 Google 也宣布 Play Store 下載量已達 480 億次。行動裝置 App 逐漸融入日常生活，對民生之影響日益加深，尤以智慧型手機 App 為甚。近來常有智慧型手機遭受惡意程式攻擊的相關消息，行動裝置 App 的安全議題實在不容小覷。誠如 Apple 公司在 iOS 安全白皮書中所言，App 已是現代行動作業系統安全體系結構中最關鍵的要素。本文相關討論將以目前市占率最高的 Google Android 與 Apple iOS 兩大陣營為主軸。

二、行動裝置 App 之安全威脅

依據 2012 年智慧型連網裝置 (Smart connected devices) 分布統計，桌上型電腦與筆記型電腦約占 28.7%，平板電腦約 11.8%，智慧型手機約 59.5%。預估 2017 年時，整體電腦所占比例將下降至 13%，平板電腦提升至 16.5%，智慧型手機則高達 70.5%。換言之，未來有高達 87% 的智慧型連網裝置是行動裝置，由於這些裝置有以下特點，其安全威脅將更甚於傳統個人電腦。

- 行動裝置持續處於開機狀態，且可能一直連上網路，不像家中電腦可能閒暇之餘才會開機上網。持續開機時間拉長，風險暴露機會自然竄升。
- 行動裝置可能存有惡意軟體覬覦的標的，例如：通訊錄的個人資料、銀行帳戶資訊等有價值的資訊。
- 行動裝置的輸出入管道多元，例如：電話、藍牙、NFC (Near Field Communication，近場通訊)、相機等，可能遭受攻擊的管道

較多。例如：以相機掃描包含惡意網址的 QR Code (Quick Response Code，一種二維條碼)，手機可能被植入木馬程式，但事前單從 QR Code 本身卻無法分辨內容是否有害；另以 NFC 掃描 Tag (標籤) 亦有類似的風險。

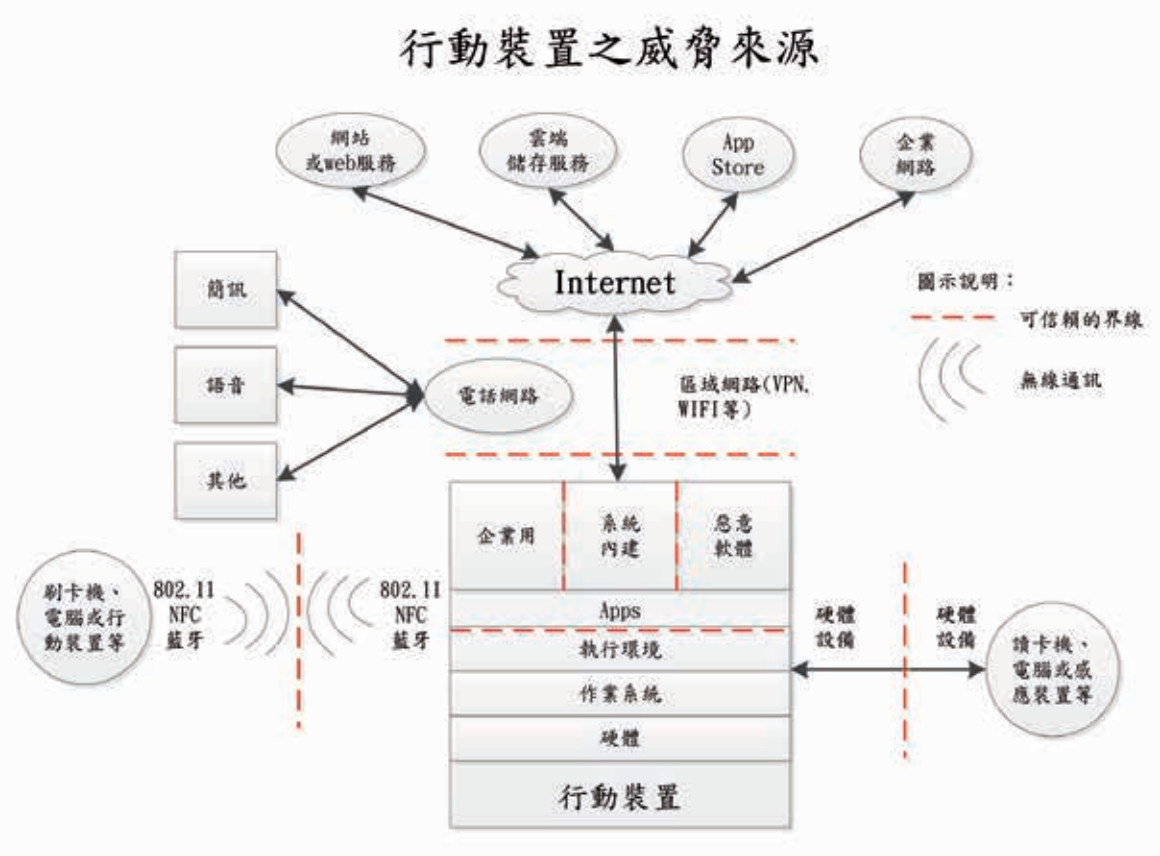

圖 1　行動裝置之威脅來源

Google Play Store 或 Apple App Store 的 App 上架流程與審核方式也是行動裝置安全威脅的一環，概述如下：

(一) Google Play Store

Google Play Store 的前身是 Android Market，於 2012 年改版更名。只要擁有 Google 帳號，並繳交 25 美元 (只須繳一次)，便可註冊成為 App 開發人員。完成註冊 48 小時後，即可將自己的 App 發布至 Play Store，而 App 上架相關作業也大約只要 24 小時就可完成。Google 對於 App 的審核方式主要是採取自動掃描，分析潛在的安全威脅，已上架的 App 則可經由檢舉而下架。對開發人員而言，這種審核方式較為友善且寬鬆，然而惡意軟體趁虛而入的機會也較高。因此，Play Store 的軟體品質較為參差不齊，發現惡意程式的情事偶有所聞。

(二) Apple App Store

Apple App Store 的 App 上架審核非常嚴格，開發人員每年必須繳交 99 美元，Apple 公司不僅審查 App 用途，也會監控程式原始碼，以防範惡意程式上架。此外，App 必須使用 Apple 公司中央控管的憑證進行簽章，不可使用第三方憑證。因此，App 上架所需時間較長，但軟體品質較高，罕有惡意程式。

依據芬蘭網路安全服務商 F-Secure 發布的一份研究報告指出，2013 年 Android 平台共發現 804 個惡意程式，約占全球總量 97%，較 2012 年增加 23%。不過，只由 Google Play Store 下載軟體的使用者不必太擔心，大部分惡意程式會被及時刪除，其實還算安全。第三方應用商店才是惡意程式四處流竄的淵藪。

圖 2　詐騙簡訊

綜上所述，行動裝置的安全威脅來源眾多，無論個人 App 的使用或企業 App 開發的安全機制必須更加審慎，以避免淪為攻擊目標。

以下介紹一些行動裝置惡意程式案例：

- **Super Clean**：一種橫跨行動裝置與個人電腦的 Android 惡意程式，使用者安裝之後，行動裝置 SD 卡的根目錄會出現 autorun.inf、folder.ico、svchosts.exe 等檔案。當行動裝置與個人電腦連結，個人電腦就會自動執行 svchosts.exe，啓動錄音程式進行錄音，並將錄音資料傳送至遠端主機。
- **Find and Call**：一種 iOS 與 Android 均曾出現的惡意程式，也是 iOS 首度發現的惡意程式。該程式會竊取使用者的手機通訊錄，並用以散布垃圾簡訊。
- **小額付款詐騙**：經由簡訊或 Line 訊息，引誘受害者開啓內含惡意程式的網路連結，自動下載安裝惡意程式後，再將小額付款的驗證碼簡訊轉接到詐騙集團，暗中進行交易 (如圖 2、3 所示)。

圖 3　惡意程式下載

三、行動裝置 App 安全機制之建構

傳統的資訊系統開發生命週期 (System Development Life Cycle，簡稱 SDLC) 較注重於短時間內完成系統開發與功能實作，但行動

裝置面臨眾多新的安全挑戰，App 安全機制之建構更應關注安全系統發展生命週期 (Secure SDLC，簡稱 SSDLC)。系統開發之初，除考量系統功能與開發時程外，架構設計亦應納入安全性思維，以適時採取各項安全防護措施。

針對行動裝置 App 安全機制的開發規劃，可參考開放網路應用程式安全計畫 (Open Web Application Security Project，簡稱 OWASP) 就技術角度所發布的行動裝置十大風險，以及歐洲網路與資訊安全機構 (European Network and Information Security Agency，簡稱 ENISA) 就用戶端角度所發布的智慧型手機十大風險，以避免落入相關常見的開發威脅中。

OWASP 組織將行動裝置可能遭遇的威脅分為偽冒 (Spoofing)、拒絕 (Repudiation)、阻斷服務 (Denial of Service)、竄改 (Tampering)、資訊洩漏 (Information Disclosure) 及權限提升 (Elevation of Privilege) 六類，再依這些威脅造成之衝擊 (例如：機密性、完整性或可用性) 訂定十大風險。以下是 2012-2013 年版的行動裝置十大風險：

(一) M1 用戶端資料儲存不安全 (Insecure Data Storage)

用戶端裝置未適當保護機敏資料，例如：機敏資料 (帳號、密碼等) 未加密或誤認資料「編碼」即已加密，因而可能導致機敏資料外洩。

(二) M2 伺服器端控制脆弱 (Weak Server Side Controls)

行動裝置 App 可能會與伺服器端的系統互動，而伺服器端可能存在弱點。以日前沸沸揚揚的 OpenSSL Heartbleed 安全漏洞為例，行動裝置就可能因為 App 連結伺服器和網頁服務執行相關功能而遭波及。「趨勢科技」曾掃描 Google Play Store 上約 39 萬個應用程式，發現大約有 1300 個會連結有安全漏洞的伺服器，其中 15 個與銀行相關，39 個與線上支付有關，10 個與網路購物有關。

(三) M3 傳輸層保護不足 (Insufficient Transport Layer Protection)

未以加密方式傳輸機敏資料，例如：經由網路傳輸交易資料或帳號密碼時，未以 https 或其他加密方式保護，可能遭受中間人攻擊 (Man-in-the-middle attack) 而導致機敏資料外洩或遭竄改。

(四) M4 用戶端注入變造 (Client Side Injection)

這種網路常見的攻擊方式歷久不衰，行動裝置 App 亦無法倖免。如果網頁程式未妥善防範，攻擊者即可利用 SQL 注入 (SQL Injection) 等攻擊方式，提升權限或存取未經授權的資料。

(五) M5 身分辨識認證不嚴謹 (Poor Authorization and Authentication)

部分行動裝置 App 僅以固定數值進行身分驗證與授權，例如：國際行動設備識別碼 (International Mobile Equipment Identity Number，IMEI)、國際行動用戶識別碼 (International Mobile Subscriber Identity，

IMSI) 或通用唯一識別碼 (Universally Unique Identifier，UUID)。

(六) M6 連線處理不適當 (Improper Session Handling)

因應行動裝置連接網路的特性，App 連線逾期 (Session timeout) 的設定通常比較寬鬆，以方便使用。這些連線可能經由 Http Cookies、OAuth tokens 或 Single Sign On (SSO) 等方式維護，建議避免使用裝置的硬體識別碼為連線值，以防攻擊者輕易猜到帳號、密碼等機敏連線內容，進而非法提升權限，存取相關重要資料。

(七) M7 安全決策輸入不受信任 (Security Decisions Via Untrusted Inputs)

經由惡意攻擊者精心佈局，可以略過應用程式的權限檢核或安全控制，各種行動裝置平台 (如：iOS、Andriod) 均可能發生。例如：假設 Skype App 有 HTML 或 Script 注入弱點，攻擊者只要先把含惡意連結的 iframe (<iframe src="skype:17031234567?call"></iframe>) 寫入某特定網頁中，當行動裝置的瀏覽器讀此 iframe 原始碼，Skype App 不需使用者授權，即自動撥打指定的電話號碼。

(八) M8 側通道資料洩漏 (Side Channel Data Leakage)

側通道可能是行動裝置中的第三方程式或函式庫，會自動儲存一些敏感資料，例如：暫存網頁、日誌檔或暫存資料等，因而導致資料洩漏。

(九) M9 加密失效 (Broken Cryptography)

此風險可分為兩種狀況：一是使用過時或金鑰長度不足的加密演算法，二是使用過於簡單的加密演算法。OWASP 指出：編碼 (Encoding)、混淆 (Obfuscation)、序列化 (Serialization) 等方式非屬加密，不可誤用。

(十) M10 敏感資訊洩漏 (Sensitive Information Disclosure)

此弱點是指程式開發人員將輸入或輸出的重要資訊直接寫在 App 原始碼中，攻擊者只要以逆向工程 (Reverse engineering) 手法還原 App 原始碼，即可取得資訊，例如：API 金鑰、帳號密碼、業務邏輯等，導致重要資訊洩漏。

另外，目前許多行動裝置 App 採用混合 (Hybrid) 開發方式，亦即利用某一平台的原生 (Native) 程式包裝 HTML 5 網頁程式，以快速開發跨平台 App。然而 HTML 5 已不是單純 HTML，而是具備強大功能的語言，相當於 HTML + CSS + JavaScript 的組合，已可支援 web socket、task、web DB 及可存取用戶端硬體等功能，可輕易製作內部網路掃描工具，因此必須審慎考量程式開發的安全性。

至於 App 的安全性測試方面，其應包含靜態及動態兩種檢測方式：

(一) 靜態檢測 (白箱)

由用戶端提供或利用 Android 平台的逆向工程工具 (例如 smali) 取得原始碼，再以工具或人工方式進行原始碼檢視。另亦可針對 byte code 或二進位碼進行靜態分析。

（二）動態檢測（黑箱）

於可控制的環境下安裝 App 進行檢測，這是很重要的檢測方式，因為某些弱點可能在執行階段才會出現。因此，動態檢測應是與靜態檢測相輔相成。

有關 App 安全性檢測之工具，可以參考 AppSec Labs 的 AppUse (Android 適用)、HP Fortify (Android 或 iOS 適用) 等工具，或委由專業單位進行。

四、行動裝置 App 安全之預防與修正

針對前述行動裝置 App 常見的十大安全議題，對應的預防或修正措施建議如表 1 所示。

表 1　行動裝置 App 安全之預防修正建議

安全議題	預防或修正措施之建議
敏感資料儲存與保護 (M1, M9, M10)	• 定義資訊的敏感程度，再據以採行適當的保護機制。 • 機敏資料勿存放於用戶端，如確有需要，必須以適當的方式加密保護。 • 為防範行動裝置遺失，可設定自遠端抹除資料的功能。 • 密碼必須以 Hash 方式儲存與比對。
身分識別或認證 (M5)	• 不要使用裝置唯一識別碼。 • 可採多因子 (Multi-factor) 認證方式。 • APK (Application Package File) 程式可以逆向取得原始碼，需要編譯的原始碼中切勿註記連線資訊、帳號密碼等可資利用的資訊。
連線與資料傳輸 (M2, M3, M6)	• 後端伺服器的安全性亦須納入考量。 • 敏感資料的傳輸須以加密方式進行。 • 資料傳輸須先完成身分確認，方可進行。 • 連線應避免使用容易被猜到的數值。
其他 (M4, M7, M8)	• 使用者的輸入值必須進行合理性判斷，以防範 SQL 注入等攻擊手法。 • 安全決策勿以不受信任的輸入為依據。 • 不要記錄帳號密碼之類的敏感資訊，使用第三方函式庫須審慎確認其功能，App 上架前須仔細觀察檔案建立、讀取與寫入相關行為。 • 針對付費的資源應防範未經授權的使用。 • 設計 App 時，用戶端頻寬應列入考量項目。

五、結語

行動裝置 App 已成為日常生活之一部分，其安全有賴使用者自我安全意識的提升，謹提出下列幾點供參：

(一) 可被 Root (Android 平台) 或 Jailbreak (iOS 平台，簡稱 JB) 破解的行動裝置即表示系統存在已知的安全漏洞，完成破解後，可取得系統最高權限，行動裝置便處於未受保護的狀態，伴隨而來的可能是惡意程式更加恣意妄為。

(二) 調整 Android 系統的安全性設定，避免安裝不明來源的 App。

(三) 安裝 Google Play Store 的 App 時，確實檢視其權限需求是否合理，例如：瀏覽圖片的 App 卻要求通訊錄讀取權限，誠屬不合理，應審慎考慮是否安裝。

(四) 來自第三方應用商店或來源不明的 App 安裝應謹慎為之，例如：原須付費使用的 App 免費提供下載，外表看似相同，卻無法確認是否埋藏惡意程式。

(五) 使用 QR Code 或 NFC Tag 之類的掃描軟體時，如掃描內容為網址，建議設定為須經審核確認後再開啓網址，以避免誤蹈惡意網址。經由 Line 或 WhatsApp 等訊息收到的網址連結，亦須謹慎確認後再開啓。

(六) 謹慎選擇欲下載安裝的軟體，以防輕則浪費金錢，買到無用軟體，重則引狼入室，誤裝惡意程式。以近來新聞為例，Google Play Store 下載率第一，獲得4.7顆星評等的付費防毒軟體 Virus Shield 竟是詐欺軟體，其宣稱的防護功能均屬無效，唯一用途只是將畫面上的「×」符號改成「✓」。

另一方面，企業於 App 開發初期，就必須將建構安全機制 (SSDLC) 納入考量，雖然開發時間可能拉長，惟對於整體安全性卻有極大助益。再者，企業應隨時關注行動裝置常見的安全議題 (例如：OWASP 行動裝置十大風險等)，並自我審視原始碼，以提升 App 開發的安全性。最後，委外開發的 App 應委由第三方進行靜態原始碼檢測與動態安全性檢測，以確保其安全性。

※ 參考文獻 / 資料來源：

1. OWASP Mobile Security Project，https://www.owasp.org/index.php/OWASP_Mobile_Security_Project 。
2. 「Mobile App Security 應用與實務」課程教材，恆逸教育訓練中心。
3. Gartner 報告， http://www.gartner.com/technology/home.jsp 。
4. IDC 報告，http://www.idc.com 。
5. F-Secure 的 2013 年下半年安全威脅，http://www.f-secure.com。