Android 前三大安全技巧

文章來源：Checkmarx blog 翻譯整理：叡揚資訊 資訊安全事業處

Android 市場呈現指數性成長。據估計， Android 智慧手機於 2013 年出貨量已突破十億支大關。但這個開放原始碼平台有許多安全問題。建議使用者加強本身的安全意識。

Android 行動平台在 2008 年底進入智慧手機市場。儘管落後了 iOS 和 Windows Mobile 幾年，但現在卻是全球的領先平台（在 2013 年第三季超過 80%的市佔率）。採用 Android 內建的安全功能，經常更改密碼，安裝防毒軟體是非常有用且建議的。但對於進一步的保護，你可以且應該做得更多。讓我們來仔細看看。

1 - 小心使用 APPs

許多使用者安裝非原廠正式的 Apps。這樣的私有安裝 .APK 檔，被稱為“sideloading”。這些“破解”的 Apps 雖是免費的但其安全風險是非常高的，建議使用者只有先設定好 PIN 鎖定後，才從 Google Play 下載 Apps。

使用者也必須在安裝過程中格外小心，安裝過程前的權限指定不應忽視，惡意 Apps 通常要求額外不需要的存取權限以取得最多的手機資源，還會研究其他的 Apps 發布者，並檢查他們提供哪些功能服務。

2 - 避免安裝客製化 ROM

Android，作為一個開放原始碼平台，是非常客製化。地下市場充滿了第三方 ROM，自稱可提升系統效能和改善使用者體驗。但 Android 的擁有者必須知道的事實：這些“cooked”的 ROM 是不安全，且存在許多可被利用的漏洞。

官方 ROM 配有標誌 RO（只可讀）的系統分割區，但”cooked”ROM 設定成 RW（可重新寫入），系統資料的修改變得非常容易。這樣的存取權限設定也導致惡意軟體和病毒可以容易地利用該設備。

3 - 避免連結未知的公共 WiFi 熱點

Android 使用者連結上未知的公共 WiFi 熱點是極度危險的。一旦你使用到駭客建立的網路，市場上充斥許多間諜軟體產品，可以很容易地接入你的手機。免費的無線網絡是誘人的，且非常方便的，但它值得我們冒這個險嗎？

同樣建議需留意加密類型，如果你看到的 WEP（Wired Equivalent Privacy），你很可能遇到了麻煩，這是一個十年之久的不安全系統。WPA（WiFi Protected Access），這可以藉由安全的 SDLC 和適當的安全掃描，盡可能的關閉安全漏洞，特別是靜態應用程式安全測試（SAST）和源碼分析（SCA），確保傳輸層的安全性，良好的加密標準和沙箱也是極力推薦。