資安意識先進 走在業界前端

遠傳電信防駭導入 Arxan APPs 安全保護沒有談判空間

撰文 | 叡揚資訊 行銷部

一分鐘看問題

導入單位

遠傳電信

導入產品

Arxan Mobile 程式碼保護解決方案—GuardIT

導入契機

2015 年大陸 SDK 資安事件以及台灣電子錢包 APP 遭惡意攻擊事件，加深遠傳了解 APP 資安議題故加強防護。

導入效益

- 解決 ProGuard 混淆機制不夠完善的問題，透過 Arxan 混淆演算法保護後，即便 APP 被反組譯也無法辨識。
- 強化電子錢包 APP 的防護機制。
- 防護 Client 端，提升遠傳的 APPs 資安防護等級，也提升公司正面形象。
- 導入 Arxan 可按需求彈性調整資安等級，且不影響開發速度、及不影響系統效能。

秉持「只有遠傳 沒有距離」的品牌精神，遠傳電信自 1997 年成立以來跨足 2G、3G、4G 以及 Wifi 各式接取技術，近期更陸續推出多項網路應用產品與服務。遠傳電信多媒體暨後勤服務開發處游文賢經理表示：「隨著行動 APPs 的多元及多樣化，遠傳電信對行動 APPs 的安全防護等議題也越來越重視。」尤其去年連續發生兩個重大的 APPs 資安事件，一個是大陸行動廣告商提供的第三方廣告SDK（軟件開發工具包），利用專有 API 收集用戶個人資料；另一個則是台灣某電子錢包 APP 遭惡意攻擊事件。因此遠傳電信決心導入 APPs 安全防護軟體，為行動應用服務多加一層保障。

ProGuard 混淆機制不夠完善 導入 Arxan 程式安全再升級

事實上，遠傳電信在導入 Arxan 之前是藉由 ProGuard 進行程式碼擾亂及混淆，避免被逆向工程解出原始碼，雖然 ProGuard 是免費軟體，但是功能太過簡易，防護不夠複雜，還需自行寫程式才能進行防護，因此希望更強大的 Arxan 取代原有的 ProGuard。

遠傳電信多媒體暨後勤服務開發處游文賢經理（右）、叡揚資訊資安團隊工程師洪任佐（左）

游經理解釋：「去年台灣發生電子錢包 APP 被惡意攻擊之後，我們就檢視過遠傳電信所有 APPs 的防護機制，和該公司不同，遠傳在 Server 上多做了一層保護，雖然相對安全很多，但仍無法保證這樣就是 100% 的保護。」在這樣的契機之下，叡揚資訊資安團隊建議導入優於業界的 APPs 防護解決方案-Arxan，在通過遠傳電信內部 POC 及反組譯測試後，便選擇導入 Arxan 作為 APPs 安全防護的最佳防線。

團隊自行開發 APPs 電子錢包安全為首要之急

游經理表示：「我們團隊對 APPs 非常熟悉，所以知道要破解一支 APP 實在太容易了。」不過游經理也坦言，目前市面上種類繁多的 APPs 確實不見得每個都需要加以防護，而且業界普遍對 APPs 安全的意識較為薄弱，所以容易發生 APP 資安事件。遠傳電信所有的 APPs 都自行開發，尤其是電子錢包的 APP 牽涉金流及個人機密資料，資安規範要求更為嚴謹，不能不注重資安問題，因此需要透過 Arxan 將整體 APP 資安提升到更高的境界。

Arxan 搭配嚴謹系統測試 確保不被駭客攻擊

遠傳電信有極為嚴謹的系統測試流程，在所有程式開發完上線前都必須經過 Code Review 、資安團隊的滲透測試及效能測試（內容包含壓測、黑白箱及反組譯測試），務必要讓所有程式都通過嚴謹的資安規範，才能上線服務。除了通過上述測試之外，防護工具也必須符合開發團隊三大需求：依需求彈性調整資安等級、不影響開發速度、不影響系統效能。游經理笑著說：「在 POC後，我們內部曾經進行效能和反組譯測試。在效能方面，我們把一個 APP

包了Arxan，另一個沒有，經過測試效能並沒有甚麼差別；在程式保護方面，Arxan的混淆演算法（Obfuscation Algorithm）相當有效，即便反組譯APP後也無法解碼。Arxan 不但達到我們的需求，也確實能夠保護 APPs 不被駭客攻擊。」

APPs 資安意識抬頭 高層及同仁支持導入 Arxan

根據經驗，電信公司一向是駭客攻擊的對象，一旦發生資安事件，除了損失之外，也會影響公司形象。因此遠傳電信高層及執行同仁對於導入 APPs 防護機制都抱持支持且正面的態度，導入Arxan 後，提升了資安防護等級，從原本只保護 Server 端，到現在從 Client 端保護，強化 APPs 資安防護機制，主要是因為 APPs 本身就很容易被攻擊，增加資安工具保護資訊安全，再搭配不定期動態調整資安防護策略，適時轉換保護重點和等級，才是最佳資安實作方式。

游經理補充說：「從整體資安層面來說，遠傳電信在 APPs 的防護不只是導入 Arxan，而是整個流程都有制式的安全規範。」從開發環境建置開始，遠傳電信一律採用標準軟體，主要是要預防第三方軟體或開放軟體內被預埋的間諜軟體，在開發過程中也有設有標準的測試流程和規範，再加上當初導入 Arxan 時，叡揚資安團隊協助建置環境和技術設定，並提供工具之外的專業教育訓練及相關技巧，不斷地動態更新資安防護的技術與新知，才能夠知己知彼，達到 APPs 防駭的最高等級。

Tips

APP 防護技術大解密

目前市面上常見的 APP 防護技術大致可以分為 4 種，除了常見的加殼與命名混淆外，還有程式碼混淆及插入動態防護的防禦方式，以下為幾種技術簡述：

1. 加殼（Wrapper）

在原有的 APP 上加上一層殼作為保護。

優點：實作簡單、便宜、基本的防護。

缺點：容易被單點破解、影響效能、且可能會被部分防毒軟體判為惡意活動。

2. 命名混淆（Rename）

針對 Class、Method、Field 名稱重新命名。

優點：輕量化的防護、可以降低程式碼可讀性、有開源的實作方式。

缺點：只進行重新命名，防護強度有限。

3. 程式碼混淆（Obfuscate）

插入或重寫原有的程式碼邏輯。

優點：大幅降低程式碼可讀性、增加逆向工程的難度。

缺點：根據混淆程度不同，影響效能及檔案大小。

4. 插入動態防護（Attack Detection）

在 APP 中散佈各種不同的防護點，以抵禦不同的攻擊手法。

優點：可以針對多種不同的攻擊手法進行防護、能夠設定多個防護點達到多重防護的效果，有些產品更可以構成網狀防護。

缺點：影響效能、防護的設計需要一定的專業知識。

各種防護方式其實多少都會影響程式運行的效能及檔案大小，但是其中有些方法，可以根據使用方式的不同，將影響降至微乎其微。Arxan 可提供的防護方案包括命名混淆、程式碼混淆、及插入動態防護。