漏洞特輯
金融類行動應用程式漏洞現況

撰文及整理｜叡揚資訊資安團隊

Arxan委託 Aite Group 製作“In Plain Sight: The Vulnerability Epidemic in Financial Mobile Apps”，檢查了目前市面上的金融類行動應用程式的漏洞現況。文中闡述了 Aite Group 為期六週的一項研究調查結果，該研究為分析金融機構中所有垂直金融服務的行動應用程式。其中發現的漏洞數量及嚴重程度明確的指出了一個系統性的問題：目前市場上的金融類行動應用程式普遍缺乏安全控制及安全程式碼撰寫，如 Application Shielding 技術、環境檢測技術及反應能力。該研究調查的目標公司從小公司、中型公司，到市值超過 100 億美元的公司皆有，並涵蓋八種金融服務行業：商業銀行、信用卡、行動支付、加密貨幣、HSA、零售業、健康保險和汽車保險，共 30 個受測 App。其開發商包含 72 人的公司至擁有 25 萬名員工的跨國公司。

該研究對目標 App 進行靜態程式分析，於 Android 7.0 的 LG G Pad X2 8.0 Plus 平板下載 Google Play 上的 App，接著使用 APK Extractor 將 Apk 匯出。匯出後使用 ApkTool 2.3.4 版進行反組譯、MobSF 1.0.5-Beta 進行靜態程式分析，最後用 Burp Suite 攔截、分析網路封包。

其測試的 11 項漏洞包含：缺乏執行碼防護、資料儲存不安全、資料外洩、客戶端注入、加密方法強度不足、信任所有憑證、使用 root 權限執行 App、可讀寫所有的文件/資料夾、私鑰外洩、資料庫參數和 SQL 語法外洩、亂數產生法不安全。

調查結果

下方表格列出了各類 App 對 11 種不同的漏洞項目的測試結果：

○ 代表 0% 的測試 App 出現此漏洞
◔ 代表該類有 25% 的測試 App 出現此漏洞
◑ 代表該類有 50% 的測試 App 出現此漏洞
◕ 代表該類有 75% 的測試 App 出現此漏洞
● 代表該類有 100% 的測試App出現此漏洞

App種類	缺乏執行碼保護	資料儲存不安全	資料外洩	客戶端注入	加密方法強度不足	信任所有憑證
商業銀行	●	●	●	◑	●	◔
信用卡發行商	◕	●	●	◕	●	○
行動支付	●	●	●	◕	●	○
HSA	●	◕	◕	◑	◕	○
零售業	◕	◕	●	◑	◕	◔
健康保險公司	●	◑	◕	◔	◕	○
汽車保險公司	●	●	●	◑	◕	○
加密貨幣	◕	◕	◕	◔	◕	◔

App種類	使用root權限執行App	可讀寫所有的文件/資料夾	私鑰外洩	資料庫參數和SQL語法外洩	亂數產生法不安全
商業銀行	◑	◔	◔	●	●
信用卡發行商	◑	○	○	◕	●

其中幾項關鍵項目為：

> **缺乏執行碼保護**：97% 的 App 缺乏執行碼保護，因此可以反組譯 App 以分析、竄改程式碼。

> **資料外洩**：90% 的 App 與該設備上其他 App 共享服務，使得該金融 App 的資料能被測試設備上其他 App 存取。

> **資料儲存不安全**：83% 的 App 將資料儲存在 App 無法掌握的地方，例如：裝置的檔案系統、外部儲存空間、剪貼簿等。使用者可能不小心讓機敏性資訊存到暫存檔或 log 中，導致該資訊能被其他 App 存取。

> **加密方法強度不足**：80% 的 App 使用了強度較弱的加密演算法，如 MD5，或者錯誤使用較強的演算法，使攻擊者能夠將機敏性資訊解密回原始狀態並為所欲為。

> **亂數產生法不安全**：70% 的 App 實作依賴於隨機數的保護機制卻使用了不安全的亂數產生器，使得該亂數值較易猜測及破解。

結論

為了降低這些弱點被分析並最終被利用的風險，金融機構必須全面採用應用程式保護方案—包含Application Shielding、加密及威脅分析—並確保開發人員在撰寫程式時有足夠的安全開發訓練並在軟體開發週期中實作。Application Shielding 是一個過程。其中程式的 source code 會被混淆、防止攻擊者進行反組譯分析以查找程式漏洞，或將惡意程式碼重新打包進程式中並散播。此外 Application Shielding 亦提供其他安全性強化，如應用程式綁定，重新打包檢測，篡改檢測，靜態資料加密以及通過白箱加密進行金鑰防護。應用程式級別的威脅檢測可識別及警告應用程式在何時被攻擊、被使用什麼手法進行攻擊，並觸發即時的反應動作，如關閉程式、隔離使用者、改變業務邏輯等。

更多資訊
請參考