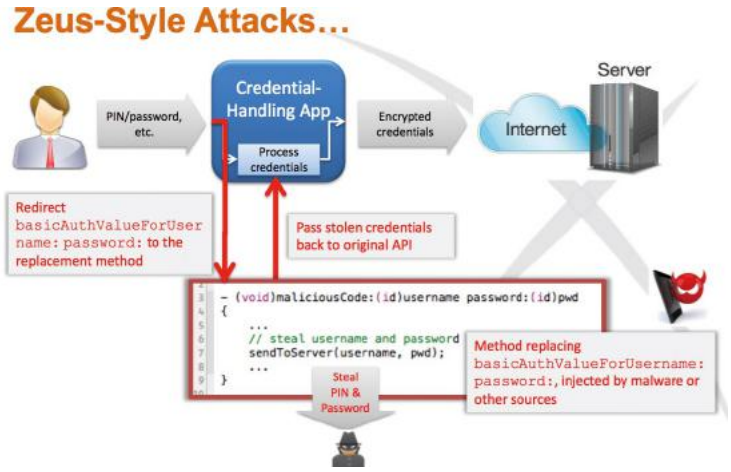
市場風險教育與客戶導入之困難與心得

台灣行動應用程式安全防護

撰文 | 叡揚資訊 資安事業處資安顧問

近年來台灣行動安全應用程式推動，到今年才陸續看到實際的作為，如：電子支付法的實施或金管會等主管機關的推動，但對於條文內容並未實際規定業者於客戶應用程式端（APPs）須符合何種安全強度、或是避免安全風險發生的必要措施，僅僅於舊有觀念來限制基礎設施上的安全防護或傳輸加密演算法之強度，但這些辦法與WEB應用程式的防護機制無差異，並非是實際針對 APPs 的安全威脅所擬訂出來能真正保護企業端及客戶端的辦法條例。



↑國外銀行 APPs 常見攻擊方式：利用反組譯得知交易邏輯後竄改交易行為，後端主機收到為正常交易，但於前端客戶機敏資訊已被盜取。

實際上，台灣的行動應用程式的發展，的確慢了鄰近國家 2 至 3 年，更別提 APPs 的安全防護觀念是否夠普及。在今年，香港已經通過相關法規限制業者需達到 APPs 相對應的安全防護。

不論是否為 IT 人員也能感受到台灣這一兩年 APPs 的市場結構與客戶行為模式的大幅度改變，如：銀行業者開始推動行動 ATM 或金流業者也整合了許多支付方式、小朋友們玩的手機遊戲也一再呼應 APPs 的蓬勃發展、而最近被熱烈討論的 IOT 產業，其中也利用了大量的行動應用程式的技術。

Apps 技術發展迅速 傳統資安思維無法 100%直接套用

叡揚資訊在 2014 年引進 Arxan Mobile 軟體保護技術到台灣，在初期教育市場觀念時期，我們面臨到以下幾個問題：

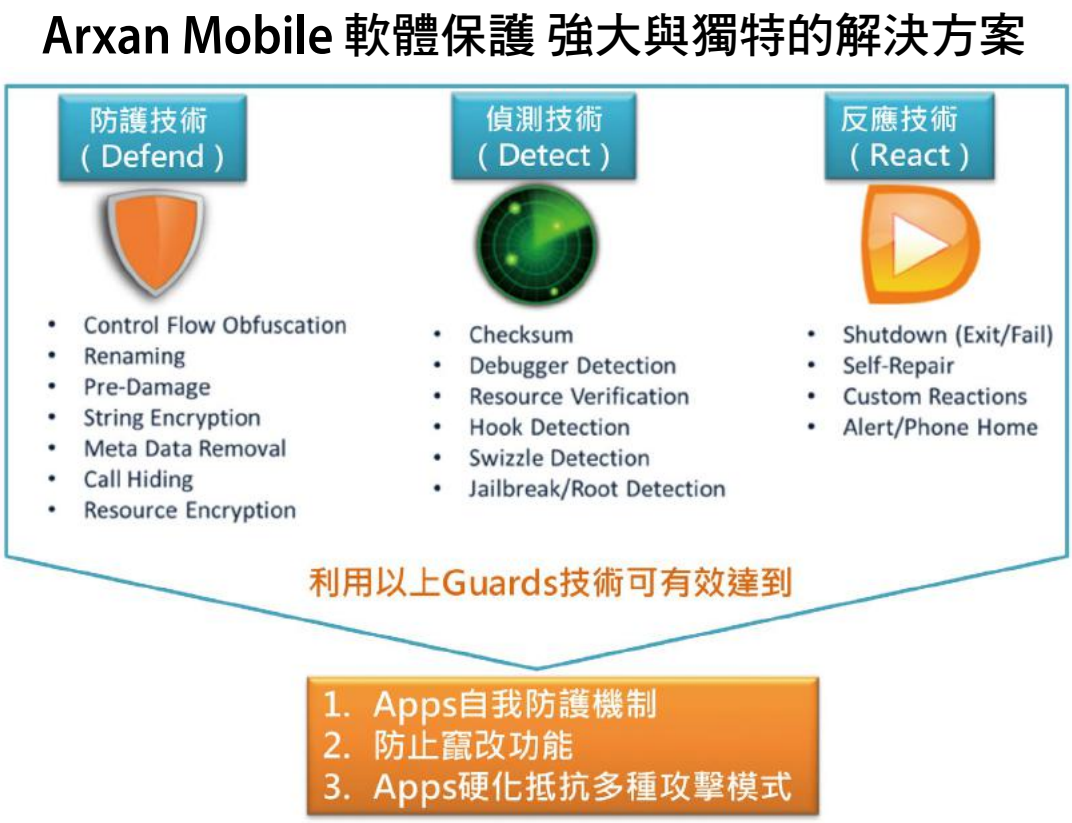
① 國內無相關法規限制業者
② 多數產業不了解行動應用程式風險
③ 技術人員對於 APPs 風險無任何經驗
④ 保守派人員固有思維認為後端主機防護即可
⑤ 對於無此觀念的技術人員，很難表達出產品之間技術性差異
⑥ 要求驗證產品有效性

我們遇到的客戶常會有兩種極端，一種毫無任何觀念，一種可能因為產業因素促使技術人員必須了解相關安全機制。就後者而言，他們回應給我們的資訊是已經尋找相關防護機制許久，只是在台灣一直未曾聽到有相關全面的防護技術，所以只能暫時使用，如：ProGuard（程式碼混淆）等的免費機制，但也了解其實像這樣初階的防護方式對於有心想要攻擊的駭客來說完全無用武之地。

APPs 的攻擊方式就像一般網站入侵一樣，有各種各樣的方式變化，不單單只是很多人在討論的反組譯。

經過一年多的努力，相信在台灣已經有不少企業聽過我們介紹相關的風險以及何謂有用並適當的防護機制；但仍有部分客戶，聽完介紹後並沒有認知到此類的風險真的會發生，然而不幸地是當我們再度接到電話時，客戶回應遇到攻擊需要協助。此篇文章主要也在闡述客戶面臨被攻擊後遭受到的損失，以及我們的導入機制與困難。

各位是否曾經思考過，手機會被入侵？若曾經想過上述問題，是否知道手機被入侵是非常容易的呢？或是否意識到手機被入侵後，造成的損失比電腦被入侵更大？



其實任何安全防護產品機制都類似，需要在發生攻擊前就被導入，但台灣許多客戶無法認同買保險的防護方式，常需等到攻擊事件發生或產生損失後才願意花錢進行防護，這也是進行專案時常聽到技術人員的無奈。

面對台灣客戶 Apps 遭破解 Arxan 防護實錄

國內目前有兩個客戶遭遇到相同問題，一位為交通運輸相關，一位為消費行為應用，但基於保護客戶立場以及此類防禦機密等級較高，不便於此說明客戶名稱。

這兩個客戶打電話給我們的時候 APPs 皆已被破解了，演算法、金鑰與安全邏輯的機制也都被翻出，所以任何人都可以直接連線到後端資料庫進行查詢，一旦類似事件發生，受害公司可能面臨客戶個資外洩、智慧財產或營業祕密被竊取等，不但會因為資安防護不夠嚴密造成實質上損失，也將會面臨相關的法律責任，但所有的風險損失中，公司商譽將會是最難以彌補及挽救的一環。

當我們接手開始進行防護時，一律要求客戶必須配合進行下列步驟：

Step 1 **修改現有演算法邏輯與更換金鑰**

Step 2 **討論應用程式行為與風險因素**

Step 3 **提供效能需求，如 APPs 執行反應速度或與主機資料傳遞回應**

與一般專案導入不同的是，多了請客戶修改程式碼內安全機制的過程，而這點對大多數的客戶來說是最大的負擔，尤其許多客戶的 APPs 都是委外開發，所以基於安全的角度還是建議企業認知到風險時即刻進行相對應之防護方式，避免資安問題發生後防護的成本攀升。

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