隨著新興科技發展，包括金融3.0、金融科技（FinTech）、行動支付、工業4.0、物聯網等為業務模式帶來改變，使得行動應用App蓬勃發展。未來，企業運用新興科技時，行動應用App所帶來的風險與衝擊，勢必將透過更完整的防護，以保障使用者的資訊安全。

防護行動裝置App安全
ARXAN從軟體保護強化下手

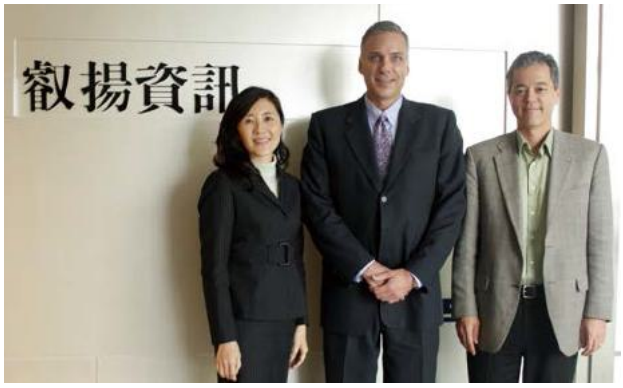
行動支付開啟新應用
也開啟個資遭竊、APP盜版等新風險

事實上，新科技的使用雖然使得人們生活更加便利，卻也使得資安問題層出不窮。

以行動支付為例，App的便利性及下載的簡易性，任何人皆可毫不費力地取得App完整程式碼，進而將其改造成盜版、甚至隱含有惡意程式的App，以及藉由外洩資訊來執行中間人攻擊（MitM），也可能因為App程式本身出現程式碼或流程上的漏洞，造成銀行帳戶資料外洩，使得這項新的支付方式雖然方便，卻處處充滿風險。因此，如何維護App資訊安全，已經成為當前企業在思考運用行動支付，或者是在未來發展物聯網（IoT）時不能忽視的重要關鍵。

長時間協助美國國防部進行資安防護工程的資安廠商ARXAN就觀察到，App開發完成後，儘管歷經弱點掃描等資安測試，一旦原始碼未經防護直接安裝於行動裝置或嵌入式系統，App源碼就能輕易地被取得並任意破壞，造成難以預測的資安威脅。而且，駭客無時無刻都在試探App的安全漏洞，且藉由簡單反組譯工具（逆向工程），即可跳脫驗證機制的手段來篡改程式碼或假冒App，竊取智慧財產造成企業或使用者的巨大損失。

為保護App與智慧財產安全，降低被篡改、破壞、偽造與竊取的風險，全球已有5億台裝置採用ARXAN保護機制，國際上尤其以支付、遊戲、醫療、長照行業已廣泛使用，建立程式與金鑰防護(Code Protection& Key Hiding)效果，降低資安風險。ARXAN產品管理副總裁Lee Cooper就強調，ARXAN專精於防護各式裝置上App的安全，能協助包括行動裝置、電腦、伺服器、嵌入式裝置，甚至由物聯網串聯的物件，提供軟體強化防護機制。



叡揚資訊資安業務處處長范家禎、Arxan Technologies 亞太區副總Richard Lord、Arxan Technologies產品管理副總裁 Lee Cooper

IoT聯網裝置威脅
建議全面、彈性的多層防護架構

根據2015年1月美國聯邦貿易委員會(FTC)針對物聯網設備的安全建議報告中表示，連接上網的智慧型設備，因為其未授權的存取、個人資料濫用、以及有利於駭客藉由物聯裝置而攻擊其它系統的情況下，成為高資安風險。

因此，ARXAN研究當前網路上已知的多種攻擊方式，提出「專利Guards」技術，能防護包括逆向工程中的反組譯程式碼，或者在程式內字串加密，執行防監聽與動態隨機執行保護等功能，同時防護動態、靜態的攻擊。

Lee Cooper表示，Guards還能防護程式碼被竄改或偷取，並執行跨組件認證與監聽模式偵測。如此，當App或物聯網裝置受到攻擊時，能就由變造程式碼區塊，達到防護的功能。最後，Guards更提供客製化防護機制，讓使用者根據自己的使用習慣設定，並可部署在多種區塊模式中，執行修復被竄改的程式碼，或者發出停止App執行訊息，以完成全面且彈性的資安防護。