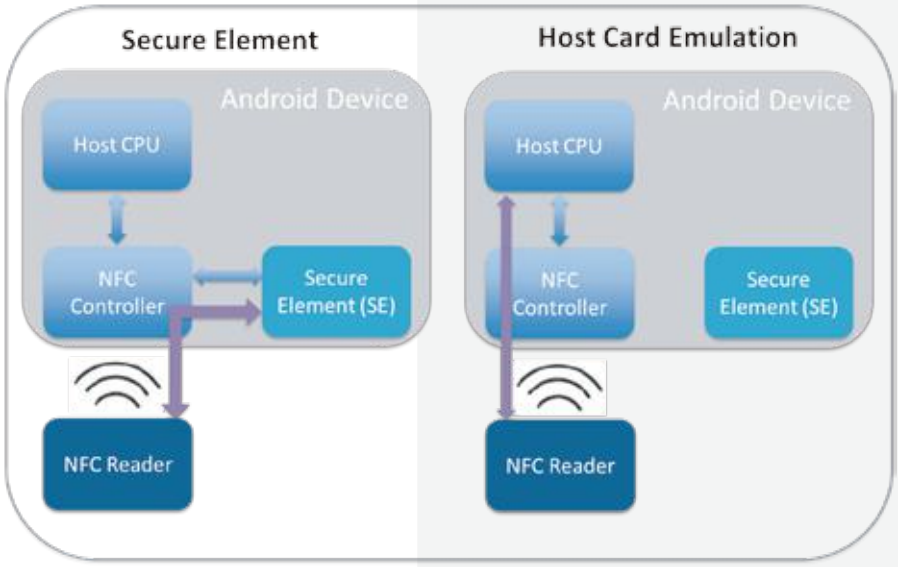
信用卡巨頭透過Arxan來保護HCE手機行動支付

Case Study

（某知名）信用卡公司正在展開雙臂迎接新的手機行動支付技術-主機卡模擬（Host Card Emulation, HCE）技術。HCE 技術提供了一種新的支付方式，可以透過 APP 或是雲端服務來模擬 SIM Card 的安全元件 SE（Secure Element），利用 HCE 技術繞過了手機中內置的安全元件（SE）限制，讓行動支付系統有更大的自由。並且透過 HCE 的研發團隊開發了一款軟體開發套件（SDK），為希望開發自己的手機支付應用程式來提升現有手機銀行應用程式的客戶提供支援。



上圖為在配備 NFC 功能的手機在實現手機行動支付時有兩種方式。
圖片左方：為基於硬體的 NFC 服務，需要透過安全元件SE做存取控管。
圖片右方：透過 HCE 技術，無需嵌入安全元件 SE，即可完成手機行動支付技術。

在 HCE 技術誕生之前，付款憑證需要被儲存在手機中特定的安全元件（SE）上，而手機營運商在產業鏈中掌握有重要的籌碼，當有支付行為發生時需要透過營運商的安全元件（SE）提供對敏感訊息的安全儲存與提供一個安全的交易環境。當 HCE 技術的出現，透過軟體模擬支付卡，手機可以在無安全元件（SE）的情況下實現行動支付，不再需要使用安全元件（SE），換句話說 HCE 技術的出現讓營運商無法在控制與約束手機移動支付的行為。

HCE技術的挑戰

HCE 技術允許透過軟體模擬支付卡，可在無安全元件（SE）的情況下進行手機移動支付。相較於傳統基於硬體的安全模塊 NFC 服務，基於軟體的 HCE 技術可能會面臨以下的安全風險：

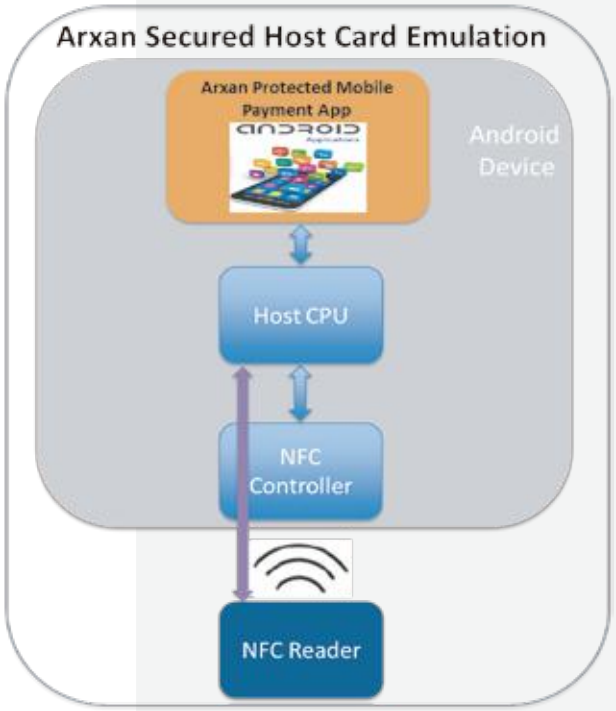
- 攻擊者可以獲取敏感資訊，如付款憑證和持卡人資料。
- 惡意軟體應用程式可以攻擊作業系統和行動支付應用程式，並且利用這些設備。
- 如果手機遺失或被盜取，惡意用戶可以獲取儲存於應用程式中的資訊，並且利用這些資訊來偽造詐欺付款。

HCE 技術面臨最大的難題主要還是安全性的問題，因此無安全模塊的情況下進行行動支付安全風險與便利性間需要有所取捨。

Arxan 提供了降低安全風險的解決方案和彌補基於硬體所缺少的安全，並彌補基於 HCE 的 NFC 應用程式服務所缺乏的安全機制。

ARXAN

Case Study



透過 Arxan 來保護使用 HCE 技術的手機行動支付。

解決方案

為了減輕HCE關鍵的安全風險，Arxan 提供了一個全面性的保護解決方案：

1. 透過健全的白箱加密技術（TransformIT®），來保護持卡人敏感資訊和付款資訊。
2. 自動化安全解決方案（EnsureIT®），包括獨特的專利守衛技術來保護應用程式，並透過以下的方法來抵抗對於應用程式有危害的攻擊：

- 防護技術：防止逆向工程反組譯程式碼。
- 偵測技術：防護程式碼竄改與偷取程式碼。
- 反應技術：提供客製化防護機制。

結果

Arxan 提供了降低安全風險的解決方案以及補強基於軟體的安全機制，並彌補基於 HCE 的 NFC 應用程式服務所缺乏的安全機制。
Arxan 提供了全面性的應用程式防護，保護應用程式以及加密金鑰的完整性與機密性。

Arxan 提供了全球最先進的白箱解決方案，確保程式的金鑰與關鍵邏輯不會出現在靜態形式或者程式運行中。
Arxan 的 EnsureIT 解決方案透過「硬化」應用程式，增加攻擊者獲取程式碼的困難度，以及防止被攻擊者控制所有的安全控制和防止程式在運行中被修改。

關於Arxan

Arxan 提供了世界上最強大的應用程式保護解決方案。
透過獨有的專利防護技術（1）防護應用程式遭受攻擊（2）偵測程式是否遭受攻擊（3）反應檢測到的攻擊。
Arxan 提供的解決方案可運行在手機裝置、桌面應用程式、伺服器、客戶端的應用軟體保護與嵌入式平台上運行的軟體解決方案，包括連結物聯網IoT網路，目前保護300萬台以上設備運作應行的行業包括：金融服務、高科技/獨立軟件供應商（ISV）、製造業、醫療保健、數字媒體、遊戲產業。

Arxan 的總公司與研發團隊設在美國，在 EMEA 和亞太地區的全球辦事處。
欲了解更多訊息可參考 www.arxan.com。

GSS 叡揚資訊 Galaxy Software Services
台北總公司：10461台北市中山區德惠街9號5樓　TEL：+886-2-2586-7890　FAX：+886-2-2586-8787
高雄辦公室：80453高雄市明華路317號6樓　TEL：+886-7-586-6195
海外據點：上海　營業範圍：兩岸三地及日本　www.gss.com.tw