觸控螢幕是您 POS 安全性的最薄弱環節嗎？

■文：Vivek Tyagi / Microchip

觸控螢幕是每個現代支付系統和銷售點 (POS) 設備的重要組成部分。觸控螢幕大幅提高了支付設備的美感，同時提供了手機、平板電腦和觸控筆電使用者熟悉的現代化操控方式。儘管擁有這些優點，卻同時增加了一些安全漏洞必須克服，以防範頑劣的金融卡盜刷者。遵循支付卡行業資料安全標準 (PCI DSS) 成為設計安全硬體 / 軟體系統的關鍵，在協助客戶建立強大且受保護支付產品的同時，無須犧牲可用性或優美的工業設計。本文介紹了 POS 支付系統的演變、觸控螢幕安全漏洞以及觸控螢幕設備必須滿足的 PCI 認證標準。

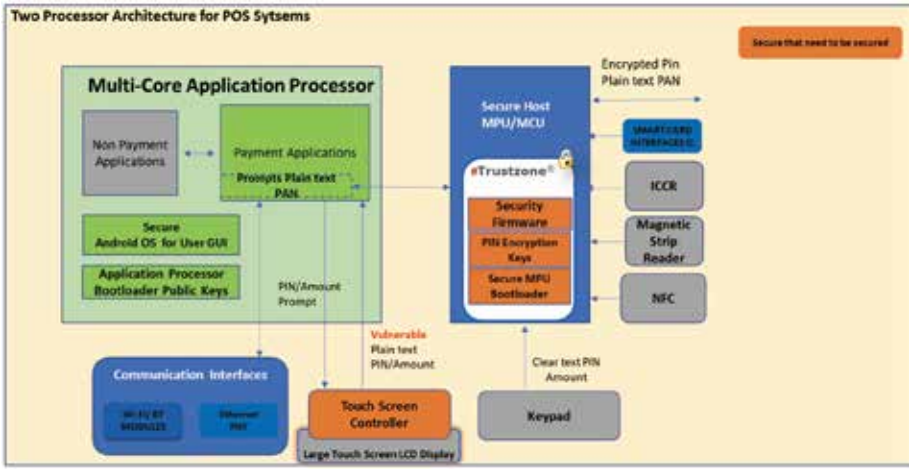
POS 顯示器中的觸控螢幕

幾十年來，全球消費者一直在 POS 設備上使用信用卡為商品和服務付費。這些設備逐漸增加了低成本的小型顯示器，以幫助商戶和消費者更能輕鬆了解交易狀態。也在顯示器的兩側或底部增加了與螢幕上的虛擬按鈕對齊的按鈕，以便使用者快速點選卡片類型 (例信用卡或金融卡)、選擇小費金額和列印收據等選項。同時利用機械鍵盤輸入卡號和 PIN 碼等資料。以上描述幾乎涵蓋了大部分市面上的 POS 設備。

支付行業的一個趨勢是用更大的彩色觸控螢幕替換小型單色無觸控功能顯示器和機械按鈕。這些彩色顯示器更美觀，對商戶和消費者也更有吸引力。有了觸控螢幕顯示器，POS 設備供應商將能取消側面 / 底部的智慧按鈕和機械鍵盤。藉由排除這些會日漸磨損甚至損壞的零件 (包括內部按鍵開關機構以及按鍵表面的印刷)，進而提高系統可靠性。此外，觸控螢幕也不再擔心按鍵可能進水的風險。最後，彩色觸控螢幕可協助商家進行品牌推廣和廣告宣傳，種種趨勢促使現代支付設備上觸控螢幕的尺寸變得越來越大。

另一個驅動更大尺寸觸控螢幕的趨勢是電子收銀機 (ECR) 的興起，作為 POS 設備機的輔助設施，ECR 用於傳統的多結帳通道商場，以及日益流行的自助結帳通道。ECR 系統可協助零售商追蹤銷售、減少銷售錯誤、追蹤庫存資料，並且同時將財務交易記錄到他們的系統中。在輸入產品類型和數量、購買購物袋和選擇支付選項等詳細資訊時，ECR 觸

控螢幕顯示器提供了極高的靈活性。ECR 通常不是一種安全的支付設備，因此它通常與 POS 設備結合使用，以透過卡片、手機和智慧手錶處理支付。



隨著時間的推移，ECR 和 POS 設備開始融合，形成一套基於觸控螢幕的安全支付系統。尺寸約為 3.5 吋至 42 吋的觸控螢幕已成為現代 ECR 和 POS 設備的組成部分。使用者互動方式、非接觸式 NFC 技術的出現、手機的連線性，以及功能整合的需求，這些因素促成了固定牆壁供電的平板電腦 / 自助服務設備或電池供電的移動式 POS 設備的興起，而不是單獨的 ECR-POS 系統。可攜式 POS 設備允許商戶在商店內外任何地方收取付款。非接觸式支付的快速成長趨勢促進了易用性和便利性，導致自動販賣機、停車計時器、自動加油機和電動車充電站中無人看守和自助公共支付設備的興起。更大尺寸的觸控螢幕不僅使商戶能夠顯示更多所購買產品資訊，而且還能透過產品促銷和廣告宣傳刺激更多業績收入。

POS 安全性和 PCI 合規性

保護 PAN 主帳號、信用卡憑證 (卡號、到期日和 CVV) 和使用者 PIN 等使用者資料成為設計支付系統的優先事項。磁條 (刷卡) 卡交易存在固有的安全性漏洞，而且隨著時間的推移，當磁條磨損和暴露在磁場中時，更容易出現故障。Dip (晶片和 PIN) 和 Tap (近場通信：NFC) 等更安全的卡片支付方法是可用的替代方案。這些方法由二維碼 (紙或手機上) 和生物特徵 (如手指、臉或眼睛) 等其他認證機制補充。然而，當觸控螢幕取代機械鍵盤時，它們的引入對 PIN 輸入系統的安全性也造成一種特殊的新影響。

觸控資料 /PIN 的傳輸容易受到通過觸控感測器覆蓋層、底層甚至在觸控 IC 和安全主機 MPU 之間的通信匯流排探測攻擊的影響。觸控控制器上的韌體容易被駭客侵入後門來提取卡片詳細資訊。觸控控制器的配置易於修改，這可能會在已經通過安全認證測試的系統上打開漏洞。

此外，戶外觸控螢幕設計要求包括處理極端環境雜訊、主動 NFC 干擾、極端發射標準、更寬廣溫度範圍、厚手套檢測和極端防水 (包括高導電清潔液體，否則會導致誤觸) 的技術。未經認證的配置和軟體更新漏洞也可能導致與勒索攻擊相結合的拒絕服務 (Denial-of-Service) 攻擊，如果設備連接到中央更新系統，則可能導致整個網路癱瘓，譬如一個帶整合支付設備的電動汽車充電站網路。對於觸控螢幕支付系統開發者而言，這些都意味著額外的挑戰和機會。

PCI 合規性充當救援

由主要的支付卡品牌 (Visa、MasterCard、American Express、Discover 和 JCB) 創建的支付卡行業安全標準委員會 (PCI SSC) 已經開發並管理了全球知名的 PCI DSS，以保護持卡人的資料。支付品牌和收單機構有責任創建符合 PCI 標準的產品，以保護使用者資料的儲存、傳輸和處理。根據支付應用類型，PCI 合規要求可能會有所不同，這可能會影響著開發者考慮硬體 / 軟體 / 系統級設計等不同因素。

大多數 POS 設備供應商現在都符合 PCI 資料

安全標準。PCI 安全機制力圖將 PIN 與 PAN 和其他持卡人資料隔離。這確保了通過軟體應用輸入 PIN 時的安全性和完整性，並且要求對此類軟體進行主動監控，以及使用安全金鑰對使用者資料進行加密。應實施存取控制以對設備使用者或所有者進行身份驗證。建議設置故障警報以針對篡改、駭客攻擊或功能故障發出警告。

如果支付系統使用一個針對 PCI DSS 預先認證的單獨支付模組，以便使用帶有機械鍵盤的讀卡器進行安全卡交易，那麼觸控螢幕不會在通信線路上傳輸任何安全資訊。只有當觸控螢幕用於輸入信用卡和 / 或 PIN 碼資料 (所謂的 PoG，即 PIN on Glass) 時，才需要對觸控螢幕進行 PCI PIN 交易安全 (PTS) 認證。在這種情況下，需要屏蔽觸控控制器的通信介面，或對觸控訊息資料進行加密。加密為 POS 設備供應商提供了將觸控控制器 IC 轉移到連接到觸控感測器的單層柔性印刷電路 (FPC) 尾板的機會，這種尾板結構簡單且經濟高效。這種配置允許觸控感測器供應商設計、測試並向 POS 設備供應商交付整套觸控系統，因而降低成本並簡化供應鏈。

一般的 PCI 認證要求

與觸控螢幕顯示器相關的 PCI 合規指南由 PCI-PTS 管理。PIN 交易安全要求可大致總結如下：

■系統中內置了在發生實體或軟體篡改時關閉的措施
■機密使用者資料必須始終以加密方式傳輸，並且僅在必要時才保留
■只有在可以驗證軟體完整性的情況下，才能進行軟體更新或啓動
■只有經過身份驗證的用戶才能更新軟體
■金鑰應儲存在受保護的區域內，並且應創建安全機制來保護生產中的初始金鑰載入
■設備應進行自檢並報告異常

為了方便遵守最新的 PCI 要求，可以在系統級別將以下功能設計進觸控控制器產品中：

■每隔 24 小時重啓計畫
■手動輸入存在 15 分鐘超時
■採用 ISO 格式 4 的先進加密標準 (AES) PIN 加密
■更嚴格地使用加密金鑰，客戶金鑰層級與製造商金鑰層級之間分離
■ PAN 加密
■ TR-34 遠端金鑰載入 (RKL) 協議

PCI 實驗室會驗證觸控螢幕顯示器，以檢查它能否滿足 PIN 交易安全標準的安全要求。此驗證包括以下測試：

■藉由駭客攻擊評估 PIN 輸入安全性的漏洞
■藉由篡改存取敏感性資料，並檢查系統中使用的回應機制
■驗證生產中的金鑰管理技術和文件。

快速切入重點

支付設備的設計必須瞭解如何實現完整的系統解決方案和堅固的安全標準。像 Microchip 的 maXTouch 控制器產品組合這樣的解決方案具有整合的類比前端和專有韌體，可為任何最終使用者應用配置安全的加密通信，有效解決此類複雜的系統問題。

像 Microchip 的觸控控制器專家這樣的專門支援團隊可以指導客戶進行系統級設計，並在軟體 / 驅動程式整合過程、產品測試和除錯中為他們提供支援。他們在應對一些世界領先的支付設備供應商和認證實驗室方面擁有豐富的經驗，這意味著客戶可以獲得他們需要的協助，順利通過至關重要的認證過程。

關於作者：

Vivek Tyagi 在半導體行業擁有 10 多年的工作經驗，目前是 Microchip 人機界面部門的產品行銷經理。他負責工業產品部分，包括 POS 和電動汽車充電器。

參考資料

■ https://ww1.microchip.com/downloads/aemDocuments/documents/HMID/ApplicationNotes/ApplicationNotes/DS00004863A.pdf CTA