香港中文大學研究發現流動支付系統保安漏洞

http://www.CRNTT.com 2017-09-28 21:13:33

中評社香港9月28日電／香港中文大學28日宣佈，該校研究人員發現流動支付系統一大保安漏洞。

新華社消息，在流動支付過程中，作為身分驗證的支付令牌是手機客戶端與商戶收款機溝通的核心。目前最為業界廣泛使用的4種支付令牌傳輸渠道分別為：近場通訊（NFC）、二維碼（QR Code）掃描、磁條讀卡器驗證（MST）和聲波轉化。

中大信息工程學系教授張克環領導的系統保安研究實驗室，積極就各種流動支付系統的保安問題進行長達兩年的深入研究及分析，並率先發現一大保安漏洞。

張克環表示，除NFC外，其餘3項皆屬單向式溝通，換言之，一旦交易失敗，商戶收款機無法通知手機客戶端，而已經產生的支付令牌也無法被收回或取消，讓不法分子有機可乘。

QR Code掃描是現時普及度最高的流動支付系統。研究團隊發現，不法分子可利用一種惡意裝備遠程從收款機屏幕上探得付款人的支付令牌，將之用於另一項交易。由於其支付令牌的特性，用戶無法收到交易失敗的信號，便會在不知不覺間蒙受損失。

至於專屬於三星流動支付系統的MST，一般來說，用戶在進行交易時需要將手機移到商戶收款機附近7.5厘米內進行身分確認。然而，經過團隊多番測試，發現實際接收範圍可遠至兩米。如不法份子混入超市付款者的隊伍中，即可伺機發起攻擊，竊取並盜用支付令牌。

研究團隊已將研究結果向相關的第三方支付平台報告。張克環提醒一般手機用戶要時刻警覺，避免下載來歷不明的手機應用程式。一旦有惡意程式被安裝至手機，程式能夠控制前置鏡頭，當用戶採用QR Code付款時，程式便有機可乘，拍攝反射在掃瞄器玻璃面上的QR Code倒影，再經網絡傳送至不法份子，被盜取使用。

這一研究成果已於上月在加拿大溫哥華舉行的國際頂級網絡安全學術會議上發表，以促進流動支付系統保安技術的發展。