Communications of the CCISA
Vol.30 No. 2 May. 2024

惡意商家利用新型 COTS 裝置實現小額收款之研究

林敬皇[1*]、曾大衛[2]、黎德謙[3]
[1,2,3]國立臺北科技大學資訊與財金管理系
[1]gbox@ntut.edu.tw、[2]112ab8005@cc.ntut.edu.tw、[3]111ab8002@cc.ntut.edu.tw

摘要

隨著支付方式的演進，商業買賣交易從傳統現金交易演進至信用卡交易，紀錄商品的交貨付款也從原本銀貨兩訖轉變到出現大型銷售時點(POS, Point of Sale)機器至小型的行動付款裝置，這些金融工具的出現不僅提供更便利的消費者體驗、提升消費的速度，還幫助商家解決問題，不斷帶給整個消費環境全新風貌。近年來甚至出現更方便的以行動裝置：手機(又可稱為新型態的商業現貨（Commercial off-the-shelf, COTS）裝置)整合收款功能工具，分別為 Android tap on phone 以及 iPhone tap to pay，讓手機變成行動收款裝置，取代原有的銷售點收款裝置。然而，新型 COTS 裝置收款服務帶來的效益，相對地隱藏潛在的風險，從申請 COTS 裝置收款服務的個人資料審核變成惡意商家，到惡意商家利用這些 COTS 收款裝置大量部署攻擊者在人潮擁擠地區進行小額惡意收款，形成容易執行且成本極低的攻擊模式。

本研究從現有新型 COTS 裝置收款服務流程中發現一個潛藏的問題及攻擊模型，並探討實施此攻擊所需的條件與可能性。透過設計實驗模擬攻擊者如何從申請 iPhone tap to pay 並且通過個資與商家審核，到使用 iPhone 對受害者進行小規模且未經授權的收款接觸攻擊，隨後評估利用此攻擊作為小額惡意收款的可行性和影響，本研究將其定義為 Merchant's COTS Fraud Attack(MCFA)的攻擊模型，其可以作為金融領域增強利用 COTS 裝置收款服務安全性的研究及參考。

關鍵詞：數位支付、行動裝置收款、非接觸支付、金融資訊安全、惡意商家

* 通訊作者 (Corresponding author.)

Communications of the CCISA
Vol.30 No. 2 May. 2024

A study on the use of the new COTS device to implement a small-scale fraud attack by merchants

Ching-Huang Lin[1*], Ta-Wei Tseng[2] , De-Cian Li[3]
[1,2,3]Department of Information and Finance Management, National Taipei University of Technology
[1]gbox@ntut.edu.tw,[2]112ab8005@cc.ntut.edu.tw,[3]111ab8002@cc.ntut.edu.tw

Abstract

With the evolution of payment methods, commercial payment methods have evolved from traditional cash purchase to current credit card transactions. The recording of goods delivery and payment has also transformed from a cash billing to the use of large point-of-sale (POS) machines and small mobile payment devices. The emergence of these financial tools not only provides a more convenient consumer experience and helps merchants solve problems but brings a new appearance to the entire consumer environment. In recent years, even more convenient mobile integrated payment tools named as Android Tap on Phone and iPhone Tap to Pay have emerged, which turns mobile phones into mobile payment devices and offers a different look for commercial off-the-shelf (COTS) devices. However, there are potential risks hidden under the benefits brought by new COTS device payment services. The personal information audit for application of COTS device payment services may become a gateway for malicious merchants who can use these COTS payment devices to deploy small-scale malicious payment attacks in crowded areas and form an easy-to-execute and low-cost attack model.

This study not only discovers an attack model from the hidden problems of the new COTS device payment services but explores the factors and success rate required for implementing this attack. Moreover, we conduct an experiment to simulate how an attacker passes personal and merchant audit, which is applied for iPhone tap to pay. After that, we use the iPhone to carry out small-scale and unauthorized payment acceptance attacks on victims. Subsequently, we assess the feasibility and the impact of using this attack for small-scale malicious payments and substantiate an attack model named Merchant's COTS Fraud Attack (MCFA), which can be regarded as a foundational reference to enhance the security of payment acceptance services using COTS devices.

Keywords: digital payment, mobile device billing, financial cybersecurity, malicious merchant

壹、前言

過去幾年來，隨著購物環境與消費者習慣資訊化，行動裝置的普及化，民眾對於行動支付、數位支付的需求與接受度都逐年提高[16]。信用卡作為民眾日常生活中最常見的非現金支付方法之一，也已從磁條卡，晶片卡，感應卡，發展到今日如 Apple Pay、Samsung Pay 等手機數位信用卡，透過技術的發展與演進不斷提升民眾支付的方便性與安全性，提升民眾對行動支付的使用意願[14]。不僅如此，商業買賣交易的結帳流程已經從過去傳統的收銀機與現金交易，演進為使用實體 Point of Sales（POS）機來掃描物品與紀錄服務，並可讓消費者以信用卡或電子支付的方式感應付款，改變了消費者的支付習慣。近年來，更有 Mobile Point of Sales（mPOS）這類強調輕巧性與便利性的小型行動 POS 機，提供餐廳、攤販等有可攜性需求的場景使用，促使從購物商場到市場商家都可以減少龐大的體積佔用空間放置 POS 機。

2023 年蘋果公司（Apple Inc.）在台灣市場推出新型收款工具「iPhone 卡緊收（iPhone Tap to Pay）」服務，為我國商業現貨（Commercial Off-the-Shelf, COTS）行動裝置支援非接觸式支付收款服務帶來新潮流，所謂商業現貨（COTS）指的是消費者能從一般通路購買到的消費級電子產品，如行動電話裝置等。「iPhone 卡緊收（iPhone Tap to Pay）」這項服務提供讓 iPhone 作為收款 mPOS 裝置的創新功能，提供台灣眾多的小型商家與攤販更多元的收款管道，開拓更多非現金支付的消費者市場與機會，為行動裝置收款的未來支付場景帶來全新的可能性[20]。

儘管如此，行動裝置例如手機、平板面臨許多威脅和攻擊，與大型零售商店中不斷維護、監控且專門用作銷售時點的 POS 裝置不同，行動裝置並非專門用於支付或收款服務。行動裝置通常會被安裝多種應用程式，像是管理電子郵件、文字處理和娛樂，對於行動裝置的系統安全有時也取決於使用者是否更新作業系統，或是廠商有無發行最新的安全修補程式[18]，而以 iPhone 當作刷卡機的新型收款服務「iPhone 卡緊收（iPhone Tap to Pay）」服務，由於其主打小額支付、人人都能申請的特性，在提升便利性的同時亦帶來了對應的風險。過去有關信用卡支付攻擊的相關研究，主要集中在受害者身上，並假設商家通常不涉及惡意行為，但隨著每個人都能夠申請 iPhone Tap to Pay，將可能有攻擊者利用申請的盲點成為惡意商家，並在擁擠地區使用 iPhone 作為刷卡機進行小額惡意收款，使「惡意商家收款詐欺」成為一種新型的攻擊模式。

過去雖然有許多研究討論支付方行動裝置風險與解決辦法[10, 11, 17, 18]，卻較少探討收款方行動裝置所帶來的風險與對應方法。因此本研究從收款方的觀點著手，以我國現況分析惡意商家利用 iPhone 實現小額惡意收款攻擊的可行性，探討申請 iPhone Tap to Pay 的審核機制，收款後的相關金流機制是否存在交易斷點，付款過程中持卡人、惡意商家、銀行和第三方支付平台等多方的角色關係，多方分析惡意商家運用行動裝置實現惡意收款的攻擊與成功的可能性。

貳、文獻探討

為了完整理解信用卡交易付款的型態演進，以更全面的分析 COTS 裝置可能存在的潛在問題，本文探討過去信用卡在傳統接觸式交易與 NFC 非接觸式感應交易時的相關盜刷與攻擊手法。並說明現行新型商業 COTS 裝置收款的相關背景與運作原理，再將過去的攻擊跟新型商業 COTS 裝置收款進行比較，以解析目前 COTS 裝置收款的新型信用卡交易型態中可能存在哪些尚未解決之潛在問題。

2.1 過去信用卡現場交易的盜刷攻擊方法與現行解決方案

信用卡作為短期商業賒借行為的紀錄主體，其發展最早可追溯至 19 世紀，經歷過去逾百年的發展，紀錄「信用卡資訊」的方式也已從最初的手寫紀錄、凸字拓印式刷卡機、1990 年代主流的感應磁條、2000 年代主流的插入式晶片、直至今日的非接觸式感應交易與手機虛擬卡片，有過了多次紀錄資訊形態上的改進，也為信用卡交易帶來不少變革[15]。

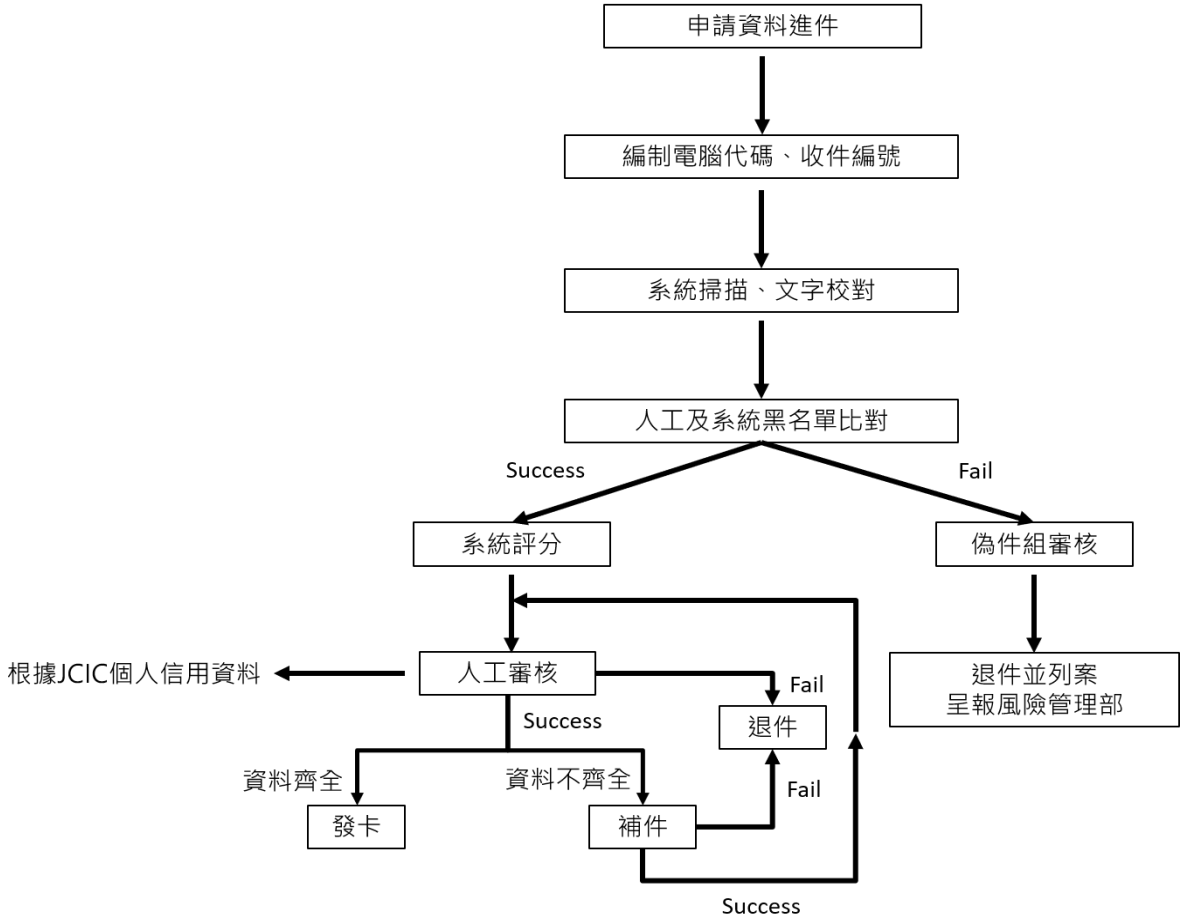
2.1.1 傳統接觸式交易

在使用接觸式交易的場域（即刷卡或插入卡片讀取），早期被廣泛使用的感應式磁條因其容易被複製與偽造的問題，逐漸改由支援進階加密演算法的晶片信用卡取代。雖然接觸式交易在改用晶片信用卡之後已解決多數問題，但仍存在一些實體卡片本質上難以被解決的問題，以下將說明接觸式交易中的攻擊手法與解決方案。

2.1.1.1 申請詐欺（Application Fraud）

申請詐欺指的是攻擊者利用盜取真實存在之他人身分資訊或持偽造證件，以他人的名義及其相關的資料向發卡機構申請信用卡所為之詐欺行為[29, 30]。圖一為信用卡徵審流程圖。

我國發卡機構在防堵這種攻擊時，會先由偽件組初次審核，發現可疑名單會立刻註記可疑的原因，並且登錄到系統黑名單內啟動比對作業，再去徵信系統查詢該筆申請書是否真實正確，接著會分成兩個程序。（一）審查單位確認是偽冒證件，會把可疑且確定是偽冒證件的資料建立到黑名單系統內，最後將偽冒證件退件並呈報給風險管理部。（二）審查單位發現無異常，會透過人工審核到財團法人信用徵信中心（Joint Credit Information center, JCIC）取得個人信用資料，再搭配申請書與黑名單核對，若確定是偽冒證件則直接退件，若依然無異常則會視資料完整度通知申請者是否審核成功或是通知補件[28, 29]。

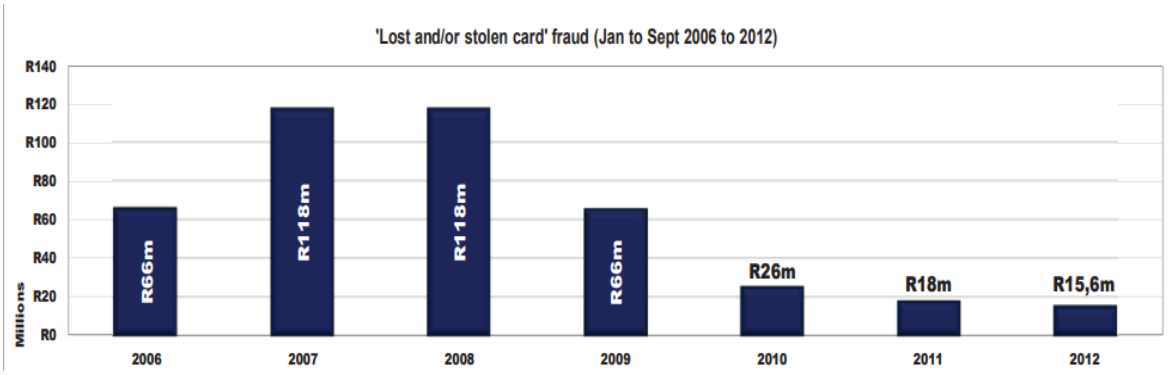


圖一：信用卡徵審流程圖[29]

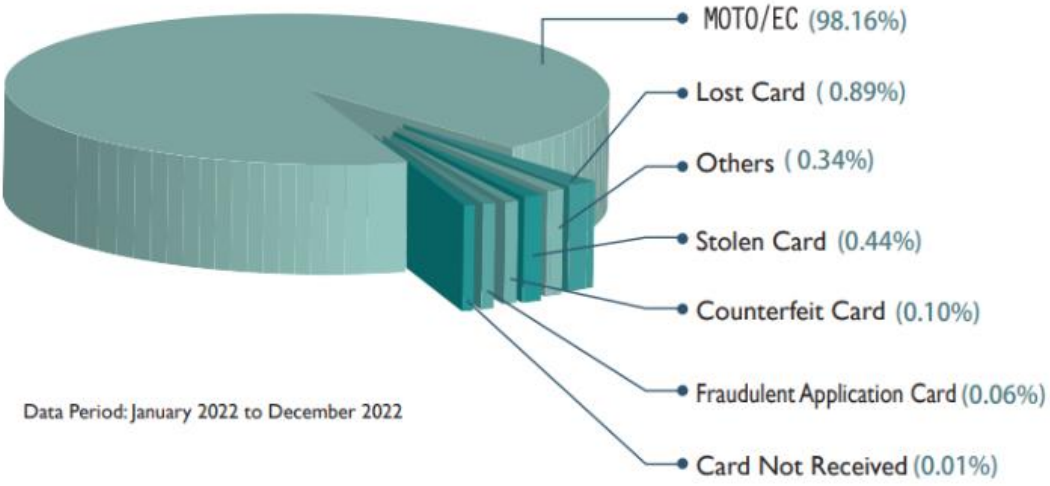
2.1.1.2 丟失被盜卡交易（Lost or Stolen Card Fraudulent）

攻擊者在未經持卡人授權或同意的情況下，冒用或盜用持卡人遺失的信用卡進行欺騙性交易[30]。此類攻擊至目前為止每年仍有一定發生的比例，根據歐洲中央銀行（European Central Bank, ECB）統計在 2021 年此攻擊發生在 ATM 和 POS 機的比率分別為 88%和 56%[27]，而南非銀行風險資訊中心（South Africa Banking Risk Information Center, SABRIC）統計於 2007 年此攻擊在南非的比率為 68%，圖二為 2005 年至 2008 年在南非因為此攻擊所損失的金額，之後持續下降。於 2010 年後此攻擊的比例大幅度降低 60%以上[6, 25]，此外如圖三我國聯合信用卡中心（National Credit Card Center of R.O.C, NCCC）在 2022 年統計，此攻擊佔國內信用卡發行機構整理的詐欺交易種類中比率為 1.33%[26]，歸因於晶片信用卡（Chip-and-Pin Card）及 EMV（Europay、MasterCard 與 Visa）標準的問世，由於使用晶片信用卡交易前需要輸入 PIN 碼，使丟失或被盜取的信用卡無法被使用，也讓此攻擊發生的次數愈來愈少。

我國應對此攻擊的方式是在 24 小時內向發卡銀行提出被盜刷通知，則持卡人不需負擔任何金額，若超過 24 小時，則必須負擔 3,000 元自付額。不僅如此，發卡銀行在對爭議款項的處理，通常也會透過信用卡上的簽名核對是否為本人[31, 33, 34]，但現今小額交易已逐漸減少刷卡消費要簽名的動作[32]，因此 3,000 元以下的交易在這類情境下可能存在的盜刷問題。在網路交易的部分，也更多轉向使用密碼驗證的方式審核，透過向手機發送一次性簡訊（One-Time Password, OTP）來確認是否為本人的交易行為，解決此攻擊的問題。



圖二：丟失被盜卡交易損失金額統計圖[25]



圖三：我國詐欺交易種類統計圖[26]

2.1.1.3 受控制的 PoS 攻擊（A Compromised PoS Attack）

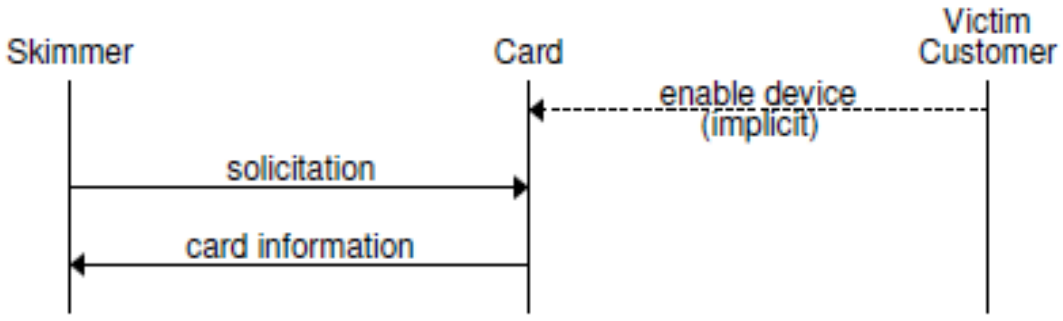
攻擊者透過惡意第三方，實際上侵入並控制了零售商的 POS 系統，竊取儲存在交易訊息的信用卡資訊，並再次利用該資訊進行盜刷[9]。此攻擊的預防包含將 POS 的資料加密、讓 POS 的軟體時常更新、讓防毒軟體經常性檢查 POS、加裝防火牆並且使用 SSL 來傳輸資料、對使用 POS 人員進行足夠的安全操作及防護訓練[13]。

2.1.2 非接觸式感應交易

隨著技術的進步與演進，為了解決實體卡片在接觸式交易需要經手多人，導致可能被抄寫卡號、到期日與安全碼資訊的問題，現場信用卡交易慢慢轉向以 RFID 與 NFC 技術為主的非接觸式感應交易（Contactless Payment）。非接觸式交易除了解決了過去實體卡交易的部分問題，也提升了消費者支付時的交易體驗，更在 2020 年 COVID-19 疫情期間扮演了降低接觸風險的重要角色。然而，由於非接觸式交易基於 NFC（Near Field Communication）與 RFID（Radio Frequency Identification）等無線技術的運作原理，也出現了相對應的盜刷攻擊手法，以下將說明非接觸式感應交易中的攻擊手法與解決方案。

2.1.2.1 掠讀攻擊（Skimming Attack）

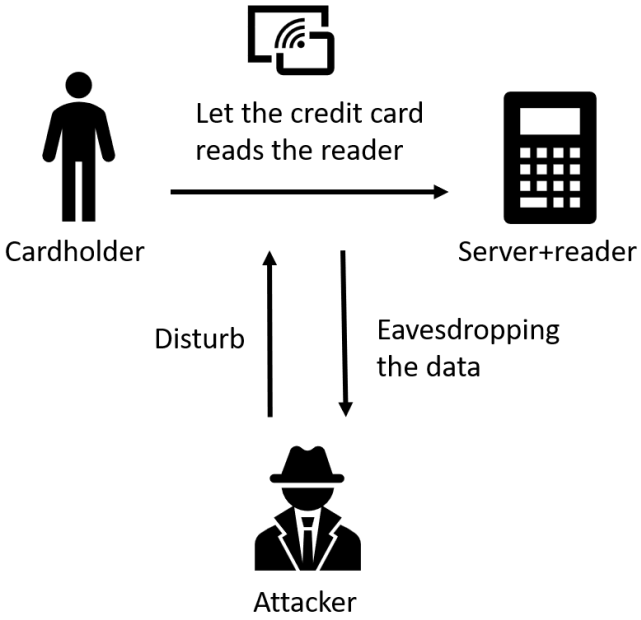
掠讀攻擊指的是攻擊者透過讀取信用卡的敏感資訊，將該資訊複製之後進行重製，以用來進行欺詐性購買[2, 6, 9]。掠讀攻擊最早常見於感應磁條（Magnetic Strip）的信用卡，因感應磁條不具備加密功能，並能被輕易的讀取、重製，攻擊者就能以偽卡進行惡意交易。隨著接觸式交易從感應磁條進展到晶片信用卡，晶片信用卡以加密的方式解決了容易被複製的問題。雖然在感應磁條進展到晶片型信用卡時已解決了當時的掠讀攻擊問題，但隨著信用卡無線化，透過 NFC 或 RFID 讀取信用卡資訊，竊取信用卡的相關訊息，再將竊取來的信用卡訊息進行欺詐性購買，也再次成為非接觸交易中的一項問題。此攻擊的先決條件是必須在 NFC 感應範圍內（大約 10 公分以內），接著如圖四為掠讀攻擊 （Skimming Attack）流程圖[9]，受害者（Victim Customer）讓信用卡直接在感應範圍內被攻擊者（Skimmer）感應，最後攻擊者（Skimmer）獲取信用卡資訊。此攻擊有兩種解決方法，其一是在卡片內放置可形成法拉第籠（Farady Cage）的金屬隔絕高頻訊號，使感應失效，其二是當靠近卡片感應時，需要輸入持卡人知道的密碼如 PIN 碼，從持卡人端阻隔攻擊[5, 8]。



圖四：掠讀攻擊（Skimming Attack）流程圖[9]

2.1.2.2 竊聽攻擊（Eavesdropping Attack）

竊聽攻擊指的是在具備 NFC 功能的信用卡與讀卡機間建立一個私人通道，並利用天線擷取資料，攻擊的範圍從 10 公分到 18 公尺，即攻擊者可在商店內竊聽又或是在更遠的公共場所監聽信用卡交易的資訊[2, 9, 12]。圖五為竊聽攻擊（Eavesdropping Attack）的示意圖，此攻擊會有三個角色，分別是持卡人受害者（Cardholder）、商家讀卡機（Reader）以及中間人攻擊者（Attacker），當持卡人受害者（Cardholder）要感應信用卡並傳遞資料給商家讀卡機（Reader）時，其中中間人攻擊者（Attacker）會在兩人之間建立私人通道竊聽傳遞資訊[1]。此攻擊的解決方式為在 NFC 感應讀卡機時，將信用卡要傳遞給讀卡機的資料進行加密，並且在信用卡跟讀卡機間建立安全通道傳遞加密後的資料[1, 5, 7, 8]。

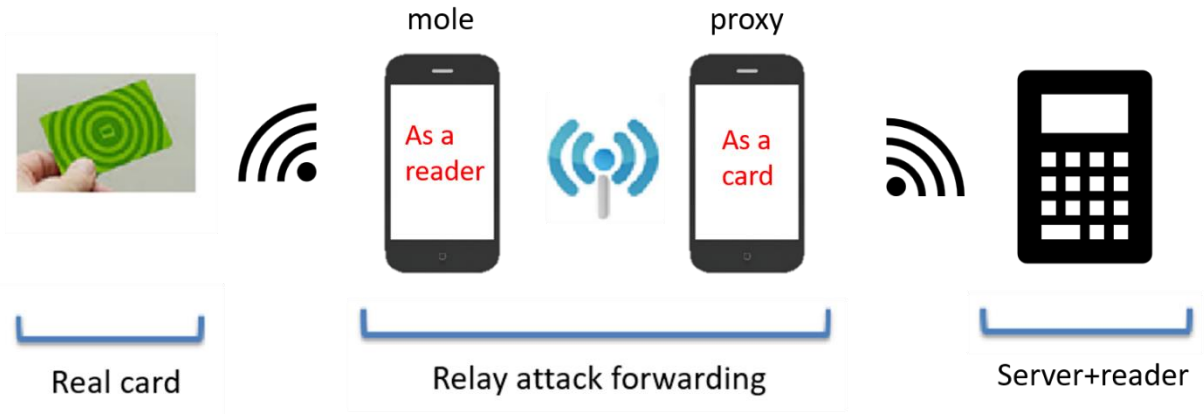


圖五：竊聽攻擊（Eavesdropping Attack）流程圖[1]

2.1.2.3 中繼攻擊（Relay Attack）

攻擊者利用兩個具備 NFC 功能的設備，一個充當讀卡機（mole），另一個充當 NFC 卡片模擬機（proxy），將讀卡機（mole）靠近受害者的卡片，並通過網路將卡片資訊中繼到 NFC 卡片模擬機（proxy），此時 NFC 卡片模擬機（proxy）將被放置在實際交易的讀卡機（transaction reader）附近，並模擬受害者的卡片來完成交易，此外，此攻擊也會欺騙不知情的商家，造成受害者和商家雙方損失[2, 3, 8, 9, 19]。此攻擊有距離與設備的限制，在理想情況下，信用卡在可知時間內回應信用卡資訊給讀卡機（mole），並且讀卡

機（mole）再將資訊中繼給另一個 NFC 卡片模擬機（proxy），但實際情況下須視讀卡機（mole）竊取的時間以及對微波頻率的影響，且在感應期間需要針對卡片資訊解析並中繼到另一端，取決於網路通訊速度，圖六為中繼攻擊（Relay Attack）的流程圖[3]。此攻擊可以透過降低感應取得信用卡資訊的逾時時間（time out）[5, 8]，或是利用深度學習警覺此攻擊的發生機率並提醒受害者[19]，以達到預防中繼攻擊（Relay Attack）。



圖六：中繼攻擊（Relay Attack）流程圖[3]

2.1.2.4 各類攻擊之說明與對應解決方法

為了更容易理解目前傳統接觸式交易與非接觸式交易的攻擊種類以及對應的解決措施，本研究整理成如下表一的各項攻擊與其解決方式或緩解措施，用以提供傳統信用卡和 NFC 感應攻擊彙整資訊。

表一:各項攻擊與其解法表

交易類型	種類	說明	解決方式或緩解措施
傳統接觸式交易	申請詐欺 (Application Fraud)	攻擊者利用盜取真實存在之他人身分資訊或持偽造證件，以他人的名義及其相關的資料向發卡機構申請信用卡所為之詐欺行為[29, 30]。	發卡機構偽件組初次審核，發現可疑名單立刻註記可疑的原因，並且登錄到系統黑名單內啟動比對作業，再經徵信系統查詢該筆申請書是否真實正確，審查單位若確定是偽冒證件則直接退件，若依然無異常則會視資料完整度通知申請者是否審核成功或是通知補件[28, 29]。

交易類型	種類	說明	解決方式或緩解措施
	丟失被盜卡 (Lost or Stolen Card Fraudulent)	攻擊者在未經持卡人授權或同意的情況下，冒用或盜用持卡人遺失的信用卡進行欺騙性交易[30]。	在 24 小時內向發卡銀行提出被盜刷通知，持卡人不需負擔任何金額。此外，發卡銀行在對爭議款項的處理，通常會透過信用卡上的簽名核對是否為本人[31, 33, 34]，在網路交易的部分，也更多轉向使用密碼驗證的方式審核，透過向手機發送一次性簡訊(OTP)來確認是否為本人的交易行為。
	受控制的 PoS 攻擊 (A Compromised PoS Attack)	攻擊者透過惡意第三方，實際上侵入並控制了零售商的 POS 系統，竊取儲存在交易訊息的信用卡資訊，並再次利用該資訊進行盜刷[9]。	將 POS 的資料加密、讓 POS 的軟體時常更新、讓防毒軟體經常性檢查 POS、加裝防火牆並且使用 SSL 來傳輸資料、對使用 POS 人員進行足夠的安全操作及防護訓練[13]。
非接觸式交易	掠讀攻擊 (Skimming Attack)	攻擊者透過讀取信用卡的敏感資訊，將該資訊複製之後進行重製，以用來進行欺詐性購買 [2, 6, 9]。	此攻擊有兩種解決方法，其一是在卡片內放置可形成法拉第籠（Farady Cage）的金屬隔絕高頻訊號，使感應失效，其二是當靠近卡片感應時，需要輸入持卡人知道的密碼如 PIN 碼，從持卡人端阻隔攻擊[5, 8]。
	竊聽攻擊 (Eavesdropping Attack)	攻擊者在具備 NFC 功能的信用卡與讀卡機間建立一個私人通道，並利用天線擷取資料，範圍從 10 公分到 18 公尺，即攻擊者可在商店內竊聽又或是在更遠的公共場所監聽信用卡交易的資訊[2,	在 NFC 感應讀卡機時，將信用卡要傳遞給讀卡機的資料進行加密，並且在信用卡跟讀卡機間建立安全通道傳遞加密後的資料[1, 5, 7, 8]。

交易類型	種類	說明	解決方式或緩解措施
		9, 12]。	
	中繼攻擊（Relay Attack）	攻擊者利用兩個具備NFC功能的設備，一個充當讀卡機（mole），另一個充當 NFC 卡片模擬機（proxy），將讀卡機（mole）靠近受害者的卡片，並通過網路將卡片資訊中繼到 NFC 卡片模擬機（proxy），此時 NFC 卡片模擬機（proxy）將被放置在實際交易的讀卡機（transaction reader）附近，並模擬受害者的卡片來完成交易，此攻擊也會欺騙不知情的商家，造成受害者和商家雙方損失[2, 3, 8, 9, 19]。	透過降低感應取得信用卡資訊的逾時時間（time out）[5, 8]，或是利用深度學習來警覺此攻擊的發生機率並提醒受害者[19]。

2.2 新型態信用卡交易：COTS 裝置的付款與收款

在信用卡交易從接觸式走向非接觸式感應交易之後，隨著行動裝置的市占率與接受率逐年攀升，近年來使用手機內建的 Apple Pay、Samsung Pay、Google Wallet 等「虛擬信用卡」行動支付服務的趨勢也逐年攀升。除了消費者以手機進行付款之外，目前更有將手機作為刷卡機系統的收款服務[20, 23, 24]。本節將說明目前以 COTS 裝置付款與收款的相關技術與趨勢。

2.2.1 COTS 裝置付款（行動支付）

COTS 裝置付款指的是使用商業市場上通用、現成可購得的裝置來進行支付交易，如 Apple Pay、Google Wallet 和 Samsung Pay 都屬於 COTS 裝置付款的應用，也稱為「行動支付」[4]。由於目前市面上的大多數的智慧型裝置都支援近場通信（NFC）技術，因此使用者只需將裝置靠近支援 NFC 的終端機，即可完成支付交易。在安全性上，目前主流的行動支付服務除了支援生物識別技術，以指紋辨識、臉部辨識等方式確保持卡人

的同意與確認，也透過動態安全碼為每筆交易生成一個單獨的隨機碼有效減少詐騙風險。除此之外，使用這些服務也無須將實際的信用卡號儲存於裝置本身或伺服器上，相反地，它們使用安全元素（Secure Element）或其他類似的技術，為用戶生成一個代碼，如 Apple Pay 的「Device Account Number」，以確保相關支付資訊即使被截獲，也無法取得真實的信用卡號碼，增強了整體支付系統的安全性[18]。

2.2.2 COTS 裝置收款（行動收款）

除了消費者利用手機進行付款，近年亦開始推出以手機進行收款的便利服務。目前可將手機作為刷卡機系統的收款服務主要有兩種，分別是 Android Tap on Phone 與 iPhone Tap to Pay。我國首先推出 Android Tap on Phone 交易服務且主要運用於 Android 系統上，並隨之增加信用卡機構的交易服務，如台新銀行開發的「台新手付」，結合 Mastercard 運用在小型商家與大都會計程車[35]，還有 Visa、JCB 結合環匯亞太信用卡股份有限公司開發的「Mobile Tap 手機付」，並導入送貨服務與食品餐車[35, 36]，不久後更推出 iPhone Tap to Pay 服務，在我國命名為「iPhone 卡緊收」並主要運用於 iOS 系統上[20]。同樣地，持有 Visa、Mastercard、JCB 與 American Express 的消費者也能透過 iPhone Tap to Pay 交易服務與小型商家進行商業買賣[37]。

現行 COTS 裝置收款都是提供手機當作 mPOS 的功能服務，讓商家無須另外申請實體刷卡機，免去實體刷卡機的體積、佈線等問題，讓小型店家也能提供消費者刷卡付款的功能，同樣在交易上能提供電子發票，並可能需要收取月租費跟手續費，一切都能在手機上完成，希望簡化小型店家的申請流程與操作複雜度，提升整體信用卡交易體驗。我國在 COTS 收款裝置的申請過程中，目前 Android 只有傳統金融機構可以申請，申請過程中一定需要申請人資料、商家資訊以及預約聯絡方式以開通 COTS 裝置收款服務，讓整個申請過程有專人在審核，但是對於 iPhone 來說，除了傳統金融機構以外，商家可向第三方支付平台申請，與 Android 不同，申請過程中不一定需專人審核，且審核時間迅速，這使得 Android Tap on Phone 相較 iPhone Tap to Pay 在新型 COTS 裝置收款服務更為安全。

2.2.3 COTS 裝置收款的潛在問題

雖然以手機當作 mPOS 進行收款可以讓商家為消費者提供更方便的收付款服務，但這樣的應用也衍生一些潛在的風險。其中，特別以「缺乏持卡人驗證」的問題最需要關注，即交易過程中持卡人輸入 PIN 碼或簽名的動作。以目前主流的兩大 COTS 裝置收款服務而言，在其開發者框架中都有提供輸入 PIN 碼的功能[21, 23]，或由收款服務供應商（Payment Service Provider, PSP）提供因地制宜的持卡人驗證方案[22]，但以我國的信用卡交易環境而言，信用卡低於 3,000 元以下的消費多數情況是不需要簽名的，且多數民

眾也並沒有為信用卡或 NFC 感應付款卡片設定 PIN 碼的習慣，使得持卡人驗證作為防盜刷保護機制之一成為交易流程中較脆弱的一環。

綜論前述，過去有關於信用卡交易的攻擊手法相當多種，也已經有許多研究與解決方案，然而大部份主題仍聚焦於竊取信用卡資訊、仿造信用卡、入侵零售商系統等議題，其攻擊假設是從「消費者與商家不知情」角度的行為。然而，隨著主打簡化申請流程的 COTS 收款裝置上市，本研究認為「商家即是攻擊者（惡意商家）」的情況應納入考慮，透過分析針對惡意商家利用新型 COTS 收款裝置如 iPhone Tap to Pay 服務進行惡意收款的威脅，我們將其命名為惡意商家利用 COTS 裝置進行惡意收款的詐欺攻擊(MCFA)。

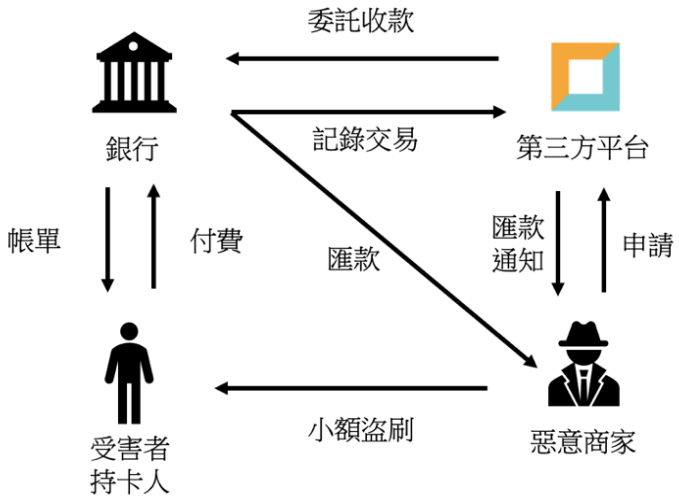
參、Merchant's COTS Fraud Attacks（MCFA）

MCFA(Merchant's COTS Fraud Attacks)指的是惡意商家利用新型 COTS 裝置收款服務進行惡意收款的攻擊或詐欺行為。由於其主打小額支付、人人都能申請的特性，將能使攻擊者利用大量申請 mPOS 的情況成為惡意商家，加上 COTS 裝置收款在小額無須持卡人驗證的情況下，便能透過在人潮擁擠地區以 NFC 感應進行惡意收款，僅需要在 10 公分以內就有機會感應成功，對受害者造成威脅[17, 18]。

在本章節中，將首先於 3.1 節說明 MCFA 的攻擊模式圖，解析交易流程中銀行、第三方收款服務供應商、惡意商家與持卡人的關係。接著於 3.2 節說明要成功執行 MCFA 攻擊所需要的三項條件，包含（1）成功申請商家身分、（2）成功感應收款、（3）成功取回帳款，多方分析 MCFA 攻擊的流程與細節。

3.1 MCFA 攻擊模式中的角色關係圖

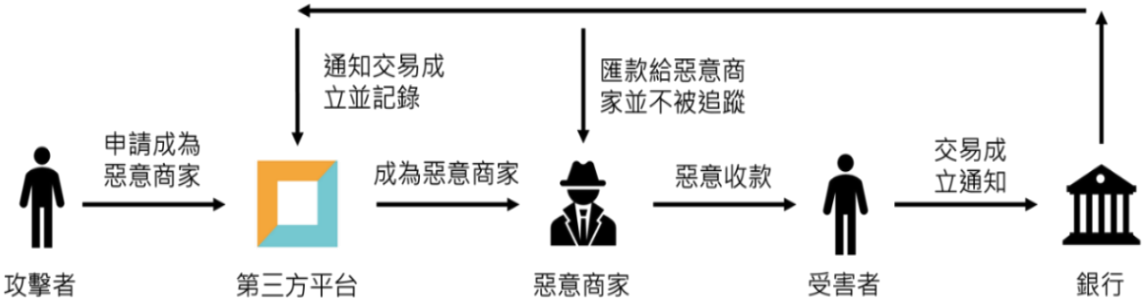
在 COTS 裝置惡意收款 MCFA 攻擊中，主要包含四種角色：銀行、第三方平台（收款服務供應商 PSP）、惡意商家、受害人（持卡人）。結構上使用 iPhone Tap to Pay 的第三方平台需與銀行合作收付款，而攻擊者則須向第三方平台申請 iPhone Tap to Pay 的手機端末機服務，將必要資料填妥並申請完畢，才能成為有收款資格的惡意商家。在攻擊者成為惡意商家後，接著便能持有搭載 iPhone Tap to Pay 軟體的 iPhone 端末機向受害者進行小額惡意收款。圖七展示了 COTS 裝置惡意收款中 MCFA 攻擊的角色關係。



圖七：COTS 裝置惡意收款中 MCFA 攻擊角色關係圖

3.2 實現 MCFA 攻擊的所需條件

要實現「惡意商家利用 COTS 裝置進行惡意收款的詐欺攻擊」，主要需要三個條件，包含（1）獲取商家身份、（2）實現成功惡意收款、（3）成功拿回金錢並且無法被追蹤，本研究將依序做詳細說明，圖八為攻擊者從申請成為惡意商家後到向受害者惡意收款到最後不被追蹤並獲取款項的攻擊流程圖。



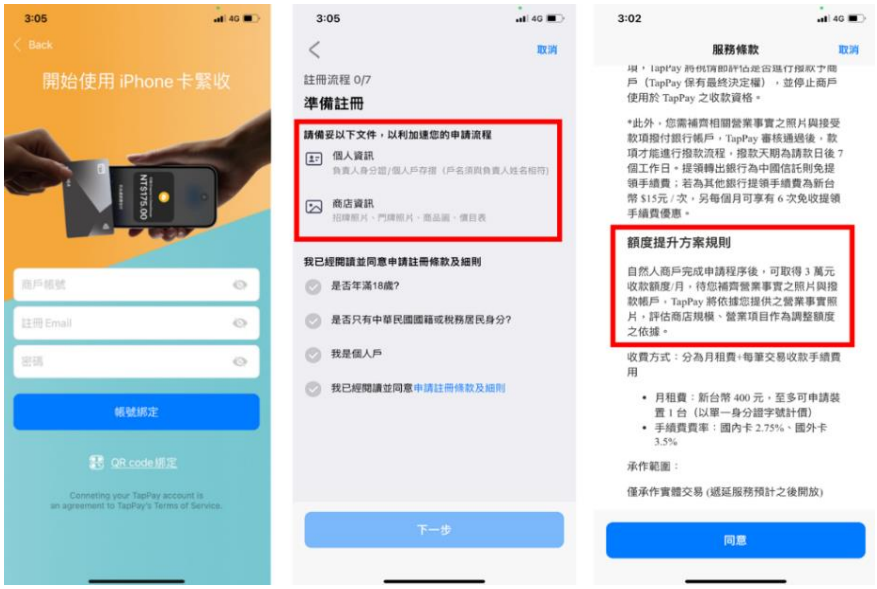
圖八：獲取款項並不被追蹤攻擊流程

3.2.1 獲取商家身份

依據蒐集與分析現況，申請使用 iPhone tap to pay 的方式分為：金融機構申請與第三方支付平台申請，以我國金融機構來說有中信銀行、富邦銀行、香港商台灣環匯亞太信用卡公司，而第三方支付平台有 TapPay。如果選擇用金融機構開發的應用程式當作

iPhone 刷卡機，以中信銀為例，申請者必須提供公司名稱、公司統編、營業內容等的資訊，對於商家身分的真實性具有特定之審核管控機制。

然而，如果選擇用第三方平台申請 iPhone 刷卡機制，通常審核會較為鬆散。以 TapPay 為例，申請流程通常只需要個人資訊即可，而營業事實也能透過假造的方式處理，如抓取網路上的攤販照片、或使用生成式 AI 製作相關影像等。換言之，對於惡意的商家較為容易就能申請到 iPhone tap to pay 的服務，圖九為「TapPay 收款吧」服務申請的所需資料，而鬆散的審核機制也讓攻擊者可進行詐欺行為，騙取具備可收款之商家身分，有利於進行後續的攻擊。



圖九：TapPay 收款吧申請資料與相關規定

3.2.2 實現成功惡意收款

若申請 iPhone tap to pay 是容易且大多數能夠通過審核，那麼對於惡意商家來說也是一樣，惡意商家可以向第三方支付平台如 TapPay 申請 iPhone 刷卡機，然後部署多名攻擊者在擁擠地區，例如夜市、商圈、聚會場所等，透過 NFC 感應放在受害者背包內的信用卡，並利用 iPhone tap to pay 在小額（通常為 3,000 元以下）不用數位簽名和不用輸入信用卡 PIN 碼的特性，實現小額惡意收款，遂行詐欺行為，本研究綜整實現流程示意圖如圖十。

圖十：實現攻擊流程圖

3.2.3 可從銀行或從第三方支付平台拿回金錢並且無法被追蹤

MCFA 的成功的關鍵為：(1)當 iPhone 端末機（COTS 裝置）向受害者發起惡意收款後，受害者的信用卡需等待發卡銀行的授權。一旦授權完成，該筆交易才被視為成功。(2)銀行和第三方支付平台會記錄這筆交易，在匯款期限內將惡意收款金額轉至惡意商家指定的銀行帳戶。成功進行 MCFA 攻擊，惡意商家獲得款項，而留存在系統的資料的卻是偽造或是盜取的惡意商家資訊，使得銀行和第三方支付平台難以追蹤，從而實現利用 iPhone 做為端末機近距離接觸受害者進行小額惡意收款的詐欺或攻擊行為。

此一部分亦是最為關鍵的金流，若攻擊者無法成功的獲取金錢回報，則該類攻擊將較不具備探討價值。經資料蒐集金融相關流程，信用卡交易成功後，會有一段銀行及第三方支付平台付款予商家的時間差。若是無法追蹤交地的商家，則損失由受害者或銀行、第三方支付平台承擔。而此一時間差，通常為 7 至 30 日。根據本研究前述分析的攻擊架構，雖攻擊不易成功，但仍有機會透過多樣、少量的偽冒個人零售商店成功地利用付款金流時間差從銀行或第三方支付平台獲取特定或小量的利益，且不被追蹤。

肆、Merchant’s COTS Fraud Attacks 可行性評估

新型 COST 裝置收款如 iPhone tap to pay 的進展，使得本研究所提的惡意攻擊模式 MCFA 可能成功。然而在實際情況中，如何進行 MCFA 攻擊是否容易、可行，我們設計進行下列實證實驗分析，發現在偽冒商家身分的取得與透過 NFC 小額惡意收款是容易、可行的，且在特定條件下詐欺及攻擊行為可獲取利益，這顯示 MCFA 在現行金流與環境下是存在潛在可行性的。

4.1 透過偽冒資訊通過商家身份審核

本研究以實驗方式建構惡意店家角色向第三方平台 Tap Pay 申請 iPhone Tap to Pay 服務，可分為（1）申請帳號與營業資訊驗證、（2）申請人資訊與營業資訊驗證，共兩個階段。在第一階段需要提交帳號密碼、Email、店家名稱、負責人姓名跟負責人身份證等資訊，並在送出申請後得到一組 Email 驗證碼，以 Email 進行驗證。在第二階段需要申請人姓名（可與負責人姓名不同）、申請人手機號碼、負責人身份證資訊、營業照片、商店資訊與收款銀行帳號等資訊。

對於申請 iPhone 端末機的資料須有申請人姓名、帳號密碼、email、店家名稱、營業照片、商店資訊與收款銀行帳號。其中，負責人的身分證可透過偽造、招募大量車手或是盜取身份證來取得，而驗證個人資料時只需 email 驗證，但 email 也可大量申請，且 email 與申請人身份間無關聯。如圖十一、十二。負責人可與申請人的身分證不同，換言之，只要偷取任意身份，攻擊者能透過招募車手當作申請人來申請 iPhone 端末機成為惡意商家，而負責人就是這些被盜取身份的受害者，當被發現有盜刷嫌疑時，第三方支付平台會先找負責人（受害者），而申請人（攻擊者）將有時間做應對並逃走，因此可以驗證是有可能利用偽冒或盜取的身份證資料做惡意利用，成功取得商家身分。再者商店資訊與照片也能透過 AI 生成。整體來說，利用偽冒的商家資訊通過審核以開通使用 iPhone 端末機是具有可行性的，如圖十二申請成功畫面可資證明。

圖十一：申請人與負責人資料不同圖

圖十二：申請成功畫面

4.2 能否在人潮擁擠的地區實現小額惡意收款

為了驗證在 3.2.2 節所說明的 NFC 攻擊模式所需條件，本研究也透過設計 2 個小型實驗證明攻擊可行，模擬在人潮擁擠地區的小額惡意收款，透過 TapPay 收款吧模擬惡意收款，發現確實可以透過 iPhone 端末機感應放於皮夾內的信用卡，並且還能在兩人模擬惡意收款情境下，讓惡意商家跟隨受害者成功感應放於背包側邊的信用卡。圖十三為透過 iPhone 端末機感應放於皮夾內的信用卡成功畫面，而圖十四為模擬人潮擁擠地區進行小額惡意收款，以兩個實際人員當作範例，其中一人作為惡意商家，另一人作為受害者，感應放置於背包內的皮夾，也能成功感應收款。

非接觸式卡片的刷卡動作僅需感應設備近距離靠近卡片即可完成，本研究透過上述實驗證實，只要攻擊者順利成為惡意商家，被攻擊的受害人在一定距離內，儘管有背包、皮夾的隔層，在感應收款的環節中相對遭遇到的阻礙可能不多，仍然能夠順利感應到。

圖十三：成功感應放於皮夾內的信用卡收款

圖十四：成功感應置於背包內皮夾的信用卡收款

4.3 能否從銀行或第三方支付平台拿回金錢

在成功惡意收款之後，發卡銀行授權受害者的信用卡使交易成功，並且銀行與第三方支付平台都會記錄交易。但是在現實正常情況下，銀行與第三方支付平台匯款給商家的交易款項是需要時間的，並且匯款時也可能需要審核商家身份，因此在多數情況都會造成惡意商家無法成功在惡意收款後順利獲取款項，然而在特定情況下也可能讓攻擊成功，本研究個別分析與闡明不容易成功與特定條件下可能成功的原因，最後彙整可能成功實現 MCFA 的條件並建立一個可行性條件表格說明。

4.3.1 大部份不容易成功的原因

4.3.1.1 商家通常要身份審核

一般情況下，銀行或第三方支付平台在匯款前都會審核合作商家的資料，以確保匯款流程無誤，但這也讓惡意商家拿著 iPhone 端末機惡意收款後獲取款項的機會降低，因為此項審核會讓惡意商家得到款項的時間增加，讓銀行或第三方支付平台發現惡意收款事件，進而使交易失效，最終停止付款，則 MCFA 失敗。

4.3.1.2 銀行或第三方支付平台有匯款時間差

除商家身份審核之外，另造成惡意收款失敗的原因是匯款時間差，不論銀行或是第三方支付平台，支付予合作商家的匯款時間大部分在 8 至 14 天左右，然而對於惡意商家來說，進行惡意收款後最迫切的就是儘速獲取金錢，匯款時間差也讓利用 iPhone 端末機實現 MCFA 的機會降低。

4.3.2 特定條件下可能成功

4.3.2.1 攻擊者透過申請眾多帳號並部署大量人力進行惡意收款

攻擊者可以向第三方支付平台申請大量帳號成為惡意商家身分，而且這些帳號的申請成本極低，並部署大量人力去人潮擁擠的地區進行小額惡意收款。如此攻擊者就可能拿回金錢，儘管部分作為偽冒的惡意商家帳號會被發現進而被終止或停用，但也可能就只有幾個裝置被視為警告或停用，而其他沒被發現的裝置（偽冒商家），就會被銀行或第三方支付平台視為正常，最終將金錢匯款到惡意商家的銀行，攻擊者就能迅速提領或移轉，透過積少成多，仍可能造成銀行、第三方支付平台及受害者的損失。

4.3.2.2 消費者針對小額付款金額未開啟推播通知

現今手機 APP 於刷卡消費時大多都會傳送推播訊息到手機畫面上，以通知消費者此筆交易紀錄，但是目前信用卡的消費通知金額基本上設定在 3,000 元以上才會通知。換句話說，若消費者沒有設定消費推播，且金額微小到不足以注意的程度，將有可能造成攻擊成功。

對惡意商家來說，若滿足表二的條件，則只要透過大量申請商家帳號，並且在人潮眾多的地方，利用 NFC 近場感應攻擊特性，大量進行每次設定金額低於 3,000 元以下的惡意收款，儘管大部分手機都有開啟推播通知，但依然有受害者未察覺被刷卡的通知，等到發現時，惡意商家可能已經獲取款項，而受害者則可能因為超過通知銀行信用卡被盜刷的期限，只能使得自行吸收虧損。

表二：MCFA 可行性條件

階段	條件	實證可行性	原因
申請	個人資訊 商店資訊	✓	1.商店資訊可假造 2.申請人與負責人可為不同人 3.只需 email 驗證 4.申請成本低
惡意收款	人潮擁擠地區	✓	1.NFC 近場感應攻擊 2.可穿透部分材質感應信用卡
金流	獲取金錢 不被追蹤	特定條件可行	1.眾多帳號佈署並大量惡意收款 2.消費通知沒有在手機推播

4.4 緩解措施

以我國現況而言，目前避免惡意攻擊者變成惡意商家並利用新型 COTS 裝置收款服務進行不法獲利的防堵機制，主要為此收款服務的供應商(金融機構、第三方支付平台)，然而透過小型實驗也得知，申請流程的相關審核機制仍有缺失的部分，從表二可得知，從申請階段不嚴謹的流程，到攻擊者申請成變成惡意商家，然後在擁擠地區進行近場感應攻擊，且感應的頻率可穿透部份材質如皮夾等，最終在特定條件下，因為大量佈屬惡意商家進行惡意收款以及消費者無消費推播功能的因素，造成 MCFA 攻擊最後可被實現，讓未來數位支付的安全性令人疑慮，因此從流程面來改善交易安全是重要做法之一。

本研究以我國使用信用卡習慣，對新型 COTS 裝置收款服務進行分析，並提出三項潛在風險與建議緩解措施，如表三，其中包含(1)小額交易、(2)持卡人交易授權與(3)收款服務申請資料審核。針對小額交易的問題，我們認為應該在驗證信用卡交易時，應不限金額或對於連續多筆小額交易列為異常，而持卡人交易授權的問題，金融機構或主

觀機關應訂定明確保護機制，像是交易時皆需要數位簽名或輸入 PIN 碼以及制定簽名保護的相關機制，最後在申請此收款服務時的資料審核，應設計規範制度，嚴謹確認商家申請資料的真實性。

儘管此研究提出的緩解措施會讓交易便利性與交易體驗降低，但期望透過本研究提供金融機構及主管機關對於新型態金融交易便利性與可接受風險的相關議題，並有助於制定我國數位支付相關政策與制度設計的參考。

表三：COTS 裝置收款服務的潛在風險與緩解措施

潛在風險	建議緩解措施
1.小額交易	驗證信用卡交易應不限金額或對於連續多筆小額交易列為異常等
2.持卡人交易授權	金融機構或主管機關應訂定明確保護機制，如交易時皆需數位簽名或輸入 PIN 碼及制定簽名保護相關標準
3.收款服務申請資料審核	設計規範制度，嚴謹確認商家申請資料的真實性

伍、結論

本研究介紹新型 COTS 裝置收款服務的背景與功能，以及過去對於接觸式及非接觸式盜刷、詐欺等攻擊及解決方法，同時探討在新型 COTS 裝置收款服務出現後，加速攻擊者申請 COTS 裝置收款服務成為惡意商家，並可能佈署大量攻擊者向受害者進行惡意收款的新型攻擊模型，命名為 MCFA，隨後提出在現實情況中實現此攻擊的必要條件與可行性評估，最終整理並提出可行性條件。

透過以惡意商家的角度討論新型 COTS 裝置收款的攻擊模式與必要條件，本研究結果發現針對 COTS 裝置收款服務的安全機制主要是（1）PIN 碼驗證以及（2）固定金額簽名驗證。要達成 MCFA 攻擊所需的條件包含（1）獲取商家身份、（2）實現成功惡意收款、（3）可從銀行或從第三方支付平台拿回金錢並且無法被追蹤，接著利用這些條件進行小型實驗驗證，並探討這些條件下在現實情景中的可行性評估，可以得知若要滿足實現 MCFA 攻擊，首先攻擊者需要透過偽造或盜取的身分證來申請惡意商家，並且利用申請人與負責人可為不同人，以及只需要 email 驗證的審核機制下，順利取得惡意商家的身份還有 iPhone 端末機收款服務，接著惡意商家部屬大量人力在人潮擁擠的地區，進行大規模且小額的惡意收款，最終從銀行或第三方支付平台取回款項。

儘管從現實情況中我們發現不容易達成此攻擊，原因在於商家在匯款時需要身份審核以及匯款會有時間差，然而惡意商家還是能透過（1）在人潮擁擠地區大量部屬擁有收款服務的 iPhone 端末機，以及（2）利用消費者未注意小額付款通知的心理，最終在匯款期限內取得盜取的款項，綜合 iPhone 小型實驗與可行性條件的歸納因素，證實惡意商

家利用新型 COTS 裝置實現小額惡意收款是可以達成的。就目前我國信用卡交易習慣而言，我們建議（1）持卡人驗證信用卡交易應不限金額、（2）金融機構或主管機關應針對 COTS 裝置收款，需要有持卡人確認等明確保護機制標準、（3）嚴謹審核申請 COTS 裝置收款服務的資料真實性，以應對此類小額近場惡意收款(MCFA)的問題。

目前研究範圍聚焦於 COTS 裝置收款服務的安全議題，闡述利用行動裝置收款服務的主要風險和實現小額近場惡意收款的條件，並針對這些問題提出相關的應對建議措施。然而科技日新月異，未來的行動收付款場景將愈來愈便利，因此後續的工作可針對金融機構或第三方支付平台能否及時偵測或警覺惡意申請行為，且利用 AI 協助分析惡意商家行為的研究。現在的研究成果提供後續研究人員對新型 COTS 裝置收款服務的交易便利性與可能問題研究的方向，期望研究成果提供銀行與第三方支付平台運用於收款金流等機制的安全考量，據以修正現有機制，強化與保障交易安全。

參考文獻

[1] A. Allah and M. Mostafa, "Strengths and Weaknesses of Near Field Communication (NFC) Technology", *Global Journal of Computer Science and Technology*, vol. 11 Issue Version 1.0, March 2011.

[2] A. Alrawais, "Security Issues in Near Field Communications (NFC)", *(IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 11, no. 11, 2020.

[3] X. Chu, "Relay attacks of NFC smart cards", *Norwegian University of Science and Technology*, June 2014.

[4] T. Dahlberg, J. Guo and Jan Ondrus, "A critical review of mobile payment research", *Electronic Commerce Research and Applications*, vol. 14, Issue 5, September–October 2015, pp. 265-284.

[5] B. B. Gupta and S. Narayan, "A Survey on Contactless Smart Cards and Payment System: Technologies, Policies, Attacks and Countermeasures", *Journal of Global Information Management*, 2020.

[6] Y. Han, "The Credit Card Fraud", *International Conference on Economic Administration and Information Systems (EAIS)*, 2022.

[7] G. P. Hancke, "Practical Eavesdropping and Skimming Attacks on High-Frequency RFID Tokens", *University of London*, 2011.

[8] T. Huizinga, "Using NFC enabled Android devices to attack RFID systems", *Radboud University*, 2018.

[9] O. Jensen, T. O'Meara, and M. Gouda, "Securing NFC Credit Card Payments",

University of Texas at Austin, 2016.

[10] I. Lacmanović, B. Radulović, and D. Lacmanović, "Contactless payment systems based on RFID technology", in the 33rd International Convention MIPRO, *2010: IEEE*, pp. 1114-1119.

[11] W. Liu, X. Wang, and W. Peng, "State of the art: Secure mobile payment" *IEEE Access*, vol. 8, pp. 13898-13914, 2020.

[12] R. Nandakumar, K. K. Chintalapudi, V. N. Padmanabhan and R. Venkatesan, "Dhwani: Secure Peer-to-Peer Acoustic NFC", *ACM SIGCOMM COMPUTER COMMUNICATION REVIEW*, OCT 2013.

[13] E. Njogela, J. Ally, B. Lufyagila, "Investigation of Cyber Security Risks, Practices, and Capability:A Point of Sale Perspective in Local Government Authorities of Tanzania", *MUST Journal of Research and Development (MJRD)*, vol. 2 Issue 3, May 2023.

[14] H. Qasim and E. Abu-Shanab, "Drivers of mobile payment acceptance: The impact of network externalities", *Information Systems Frontiers*, vol. 18, pp. 1021-1034, 2016.

[15] I. Sakharova, "Payment card fraud: Challenges and solutions", *IEEE*, 2012.

[16] P. G. Schierz, O. Schilke and B. W. Wirtz, "Understanding consumer acceptance of mobile payment services: An empirical analysis" *Electronic commerce research and applications*, vol. 9, no. 3, pp. 209-216, 2010.

[17] E. Taylor, "Mobile payment technologies in retail: a review of potential benefits and risks," *International Journal of Retail & Distribution Management*, vol. 44, no. 2, pp. 159-177, 2016.

[18] Y. Wang and C. Hahn, K. Sutrave, "Mobile payment security, threats, and challenges," *in 2016 second international conference on mobile and secure services (MobiSecServ)*, 2016: IEEE, pp. 1-5.

[19] Y. Wang, J. Zou and K. Zhang, "Deep-Learning-Aided RF Fingerprinting for NFC Relay Attack Detection", *ELECTRONICS*, FEB 2023.

[20] Apple."使用「iPhone 卡緊收」為顧客提供一致且可靠的收款體驗", https://developer.apple.com/tw/tap-to-pay/ (2023/7/23).

[21] Apple. "iPhone 卡緊收商家常見問題集", https://register.apple.com/tap-to-pay-on-iphone/faq/ (2023/7/23).

[22] TapPay. "『iPhone 卡緊收』常見問題", https://cherritech.atlassian.net/wiki/spaces/FAQ/overview (2023/7/23).

[23] VISA. "VISA Tap to Phone", https://usa.visa.com/visa-everywhere/innovation/connected-commerce/tap-to-phone.html (2023/7/23).

[24] VISA. "Tap to Phone 手機感應收款-收款從此更加輕鬆簡單", https://www.visa.com.tw/visa-everywhere/innovation/tap-to-phone.html (2023/7/23).

[25] South Africa Banking Risk Information Center. “Card Fraud South Africa”, https://www.sabric.co.za/media/c2ljwaww/2011-to-2012-card-fraud-booklet.pdf (2012)
[26] National Credit Card Center of R.O.C. “Fraud Prevention Operation”, https://www.nccc.com.tw/wps/wcm/connect/en/home/BusinessOperations/fraudPreventionOperation# (2022)
[27] European Central Bank. “Report on card fraud in 2020 and 2021”, https://www.ecb.europa.eu/pub/pdf/cardfraud/ecb.cardfraudreport202305~5d832d6515.en.pdf
[28] 白豐榮, “銀行經營信用卡業務與風險管理之研究”, *銘傳大學*, 2002
[29] 李炎和、杜炎明, “台灣信用卡徵審作業風險之探討”, *績效與策略研究*, 2005
[30] 鄭可婕, “網路盜刷信用卡交易犯罪偵防策略之研究”, *中央警察大學刑事警察研究所*, 2021
[31] 施宇宸, 「信用卡被盜刷，銀行不認帳怎麼辦？學霸律師教你申訴 6 管道「找這個單位最有效」：1 個星期就解決了」, *今周刊*, 2023
[32] 黎德謙、林敬皇, “我國商用現貨行動裝置支援感應支付收款的安全性問題”, *TANET*, 2023
[33] 信用卡定型化契約範本第 17 條第 3 項：「辦理掛失手續前持卡人被冒用之自負額以新臺幣__元為上限。(各發卡機構得自行視本身狀況約定收取不超過新臺幣三千元之金額，且應明定於契約中。)但有下列情形之一者，持卡人免負擔自負額：一、持卡人於辦理信用卡掛失手續時起前二十四小時內被冒用者。二、冒用者在簽單上之簽名，以肉眼即可辨識與持卡人之簽名顯不相同或以善良管理人之注意而可辨識與持卡人之簽名不相同者。」
[34] 信用卡定型化契約範本第 17 條第 4 項：「持卡人有本條第二項但書及下列情形之一，且發卡機構能證明已盡善良管理人之注意義務者，其被冒用之自負額不適用前項約定：一、持卡人得知信用卡遺失或被竊等情形而怠於立即通知發卡機構，或持卡人發生信用卡遺失或被竊等情形後，自當期繳款截止日起已逾二十日仍未通知發卡機構者。二、持卡人違反第八條第一項約定，未於信用卡簽名致他人冒用者。三、持卡人於辦理信用卡掛失手續後，未提出發卡機構所請求之文件、拒絕協助調查或有其他違反誠信原則之行為者。」
[35] 孫彬訓, “萬事達卡、Visa 擴大手機感應收款服務”, 工商時報, https://www.ctee.com.tw/news/20210901700209-430301 (2021/9/1).
[36] 環滙亞太. “環滙亞太與 JCB、大都會車隊攜手合作，增設【Mobile Tap】手機感應收款方式”, https://www.media-outreach.com/news/taiwan/2023/04/18/214517/%E7%92%B0%E6%BB%99%E4%BA%9E%E5%A4%AA%E8%88%87jcb%E3%80%81%E5%A4%A7%E9%83%BD%E6%9C%83%E8%BB%8A%E9%9A%8A%E6%94%9C%E6%89%8B%E5%90%88%E4%

BD%9C%EF%BC%8C%E5%A2%9E%E8%A8%AD%E3%80%90mobile-tap%E3%80%91/ (2023/4/18).
[37] 遠傳電信. “Apple 全新「Tap to Pay」功能，讓手機直接當成刷卡機使用！” https://www.fetnet.net/content/cbu/tw/lifecircle/tech/2022/02/tap_to_pay.html (2022/2).