嘗試新金融攻擊法…駭客破解悠遊卡 超商消費露餡

更新日期:2011/09/28 04:21

|  |
| --- |
|  |

〔[自由時報](http://tw.news.yahoo.com/article/url/d/a/110928/78/)記者劉慶侯、張文川、蔡偉祺、楊雅民／綜合報導〕敦陽科技資訊安全顧問吳東霖涉嫌以[駭客](http://tw.news.yahoo.com/article/url/d/a/110928/78/)手法成功竄改三張悠遊卡[盜刷](http://tw.news.yahoo.com/article/url/d/a/110928/78/)六○八元，扣除原本卡片內已儲值五百六十九元，僅Ａ走[悠遊卡](http://tw.news.yahoo.com/article/url/d/a/110928/78/)公司卅九元，廿三日遭警方逮獲。

「我是為了嘗試新的金融攻擊手法，才會去竄改悠遊卡！」吳嫌在警訊中坦承犯案，他說為了讓自己更精進，「了解怎麼破，未來才知怎麼防」。

複訊後無保請回 最高可判刑十年

警方查出他六次的刷卡、儲值、消費動作，均是測試，沒有對外流通、牟利，應是「單純的駭客行為」，只為「證明實力」，也沒有前科紀錄，[台北市](http://tw.news.yahoo.com/article/url/d/a/110928/78/)刑大以詐欺、違反電子票證發行管理條例罪嫌移送士林地檢署偵辦，檢方複訊後無保請回。

台北市交通局長林志盈表示，依「電子票證發行管理條例」第卅條規定，變造電子票證者，處一年以上十年以下有期徒刑，得併科一千萬元以上兩億元以下罰金。

花399[美元](http://tw.news.yahoo.com/article/url/d/a/110928/78/)買讀卡機+網路資訊就破解

警方調查，今年五月間，吳嫌選定具有兩千七百萬持用戶的悠遊卡公司，作為研究攻擊對象，吳東霖挑選美國某駭客撰發的資訊，認為可符合台灣悠遊卡內碼程式，花費三百九十九美元（約新[台幣](http://tw.news.yahoo.com/article/url/d/a/110928/78/)一萬兩千元），透過美國網站郵購型號TQ2SA\_5V的讀卡機；吳嫌八月初自製一個感應線圈，與讀卡機做合體連結，形成一個可置放悠遊卡的「感應平台」。

檢警解釋，吳嫌先自製無線天線，用來取代超商、[捷運](http://tw.news.yahoo.com/article/url/d/a/110928/78/)閘門的感應讀碼器，將卡片資料掃進電腦，再以進口解碼器讀取、破解晶片的安全防護程式碼，即可隨意更改儲值金額。

吳嫌向警方指出，完全破解悠遊卡四道程序（即所謂的鑰匙）、三十二道密碼後，便可修改內部程式；要竄改完每張悠遊卡至少需要二至三個工作天。

悠遊卡公司總經理鄭有欽說，吳嫌共竄改三張票卡，每張票卡都是自行加值到九千元，並在九月十日持票卡到超商第一次消費。悠遊卡公司說，吳嫌當天使用的第一張卡片因破解技術不佳，讀卡後立刻被鎖卡無法消費，但第二、三張卡則通過票卡和讀卡機的認證，在超商消費成功。

非合法加值 資料被後台查核鎖定

信用卡交易都需經系統確認才有效；悠遊卡則是使用者先行使用扣款，約一天半之後才上傳到系統確認。但是悠遊卡公司表示，悠遊卡每筆消費、加值都留有紀錄，吳嫌私自加值，雖消費成功，但從當天回傳的資料，立刻被後台查核機制鎖定。

警方指出，悠遊卡公司事後彙整刷卡資料時才驚覺有異，已延遲至少一到兩天，悠遊卡公司鎖定吳嫌持用的兩張竄改悠遊卡，並調閱特定時間出入超商的監視錄影帶畫面，廿二日向台北市刑警大隊偵八隊報案。

警方同步清查，發現位在內湖路二段的統一便利超商，曾有吳嫌兩次刷卡紀錄，經派人埋伏，九月廿三日果然逮到住便利超商後方巷內的吳嫌，吳東霖嗜菸，成功刷卡三次共買五包菸。

吳東霖小檔案

年齡：24歲

學歷：龍華科大機械系一年級肄業

現職：敦陽科技資訊安全顧問

專長：國中開始當駭客，專長為網頁應用程式相關安全技術，負責滲透測試、資安事件應變，具CEH v6證照

製表：記者劉慶侯、張文川

<http://tw.news.yahoo.com/article/url/d/a/110928/78/2zhwy.html>

**悠遊卡遭破解　專家：防護密碼落後**

更新日期:2011/09/27 18:14 *楊鎮全　侯力元*

|  |
| --- |
|  |

悠遊卡成功被人破解加值，究竟卡片安全性有沒有問題？其實早在2年前，就有[台北市](http://tw.news.yahoo.com/article/url/d/a/110927/8/)議員拿荷蘭大學的研究報告，質疑卡片安全係數不夠，有心人很容易破解，而且國內大學也有類似實驗，只要一台監聽設備和模擬器，就能破解[悠遊卡](http://tw.news.yahoo.com/article/url/d/a/110927/8/)的密碼，甚至完成卡片複製；智慧卡專家就說，這是因為悠遊卡採用的是早期的卡片系統，安全防護已經跟不上新型電腦的運算速度。

沒有門禁卡，進不了門，沒關係，只要有人拿跟悠遊卡相同的門禁卡刷卡開門，在旁邊的2台筆記型電腦，第一台負責監聽，擷取卡片資訊，再利用另外一台的模擬器，就能現場破解，成功開門，這是[台大](http://tw.news.yahoo.com/article/url/d/a/110927/8/)電機系破解實錄，悠遊卡採用的，就是這種Mifare卡，因為是比較早期的智慧卡，密碼防護恐怕不太夠。

智慧卡專家倪萬昇：「因為密碼已經被破解出來，而且這卡金鑰長度是不夠的，你只要去買一個市面上現有的讀卡機，你就可以不斷嘗試，去(破解)金鑰。」

不只台大破解，有民代2年前，就以荷蘭大學生透過讀卡設備，就能破解密碼的影片，質疑悠遊卡安全性，不過悠遊卡公司強調，現在的卡片本身就有設密碼，加上不斷變換的密碼系統，以及防偽驗證碼，最後還有後台判讀，總共有4層把關。

悠遊卡公司科長林諭林：「以交易完整性來講，這樣的交易，不算是一個完整的交易。」

話雖這樣說，但卡片密碼一旦被破解，資訊很容易就被複製，尤其悠遊卡現在又跟不少企業合作，變成識別證，裡頭建立的個人資料，恐怕也有外流疑慮。林諭林：「我們之後會發行，所謂的晶片悠遊卡。」

考慮發行安全係數更高的晶片卡，但還沒發行之前，該怎麼防止有心人破解，恐怕是個大麻煩。

<http://tw.news.yahoo.com/article/url/d/a/110927/8/2zha1.html>

**二代悠遊卡 金鑰密碼難度升級**

更新日期:2011/09/28 05:30 *林佩怡、潘欣彤／台北報導*

中國時報【林佩怡、潘欣彤／台北報導】

悠遊卡遭竄改消息曝光，[台北市](http://tw.news.yahoo.com/article/url/d/a/110928/4/)長[郝龍斌](http://tw.news.yahoo.com/article/url/d/a/110928/4/)強調「對[悠遊卡](http://tw.news.yahoo.com/article/url/d/a/110928/4/)安全防護有信心」；曾任悠遊卡公司董座的北市府交通局長林志盈則說，所有交易均在電腦內留存紀錄，呼籲民眾勿心存僥倖。悠遊卡公司則強調，系統擁有四道防弊機制，未來二代卡上路後，安全性將更加提高。

台北市長郝龍斌昨強調，對悠遊卡安全防護有信心，該工程師九月十日竄改悠遊卡時，第一時間就被鎖定，警方短時間破案，基於偵查不公開，也擔心尚有共犯，才沒有對外公布。

林志盈強調，悠遊卡是自己竄改金額，或到加值機加值，公司的電腦可查得出來，消費時間、地點或金額，全都一清二楚，民眾千萬不要心存僥倖，違者違反《電子票證發行管理條例》，可處一年到十年的有期徒刑併科一千萬到兩億的罰鍰。

悠遊卡公司總經理鄭有欽強調，悠遊卡設計四道關卡，包括每張票卡都有專屬金鑰、且擁有多樣化基碼、防偽驗證機制，系統後台更可完整判斷、查核每張卡資料，若上述任一關卡未過，系統現場便可註記為問題票卡，立即停用。

鄭有欽說，上月剛發兩萬張測試的二代晶片悠遊卡，雖然上市日期未定，但該卡最大特色為內建記憶體容量擴增八倍，可容納更複雜密碼機制，若有心人要破解「光拆解出金鑰密碼，恐得花上龐大時間」，由於難度提升，不符成本效益，應可大幅降低資料遭竄改可能。

<http://tw.news.yahoo.com/article/url/d/a/110928/4/2zibu.html>

討論議題

1. 新聞所敘說的悠遊卡破解手法的正確性為何？請使用自己的觀念嘗試解說這次駭客事件使用的手法。
2. 悠遊卡公司所說的「四道程序」是哪四道？請簡單介紹。
3. 目前悠遊卡所使的應用技術與晶片卡所使用的應用技術有何差別？
4. RFID是什麼？請簡單敘說原理與應用。
5. 台灣資訊科技是否落後？否則怎麼一台特規讀卡機就可破解悠遊卡？
6. 上文提到新的晶片悠遊卡可是卻沒有說明其用途，若使用晶片悠遊卡請試著構想如用應用晶片悠遊卡。
7. 為什麼此次駭客只消費了39元卻有可能被罰千萬罰款，到底「電子票證發行管理條例」是一個怎麼樣的條款。
8. 整組討論此次悠遊卡破解事件對社會有甚麼樣的影響？