You Cannot See Me

unohope [at] chroot.org

講師簡介

- **Unohope (unohope [at] chroot.org)**
- 研究方向
  - Web Application Security
  - Network Security
  - Multimedia Security
- 相關經歷
  - 經歷 Hacks In Taiwan Conference 2005 Speaker
  - 經歷 Hacks In Taiwan Conference 2006~2008 Wargame Designer
  - 經歷 Chroot Security Group (http://www.chroot.org)
  - 經歷 企業、學術及政府等單位資安教育訓練講師
  - 經歷 網駭科技 WARGAME 教育訓練講師
  - 著作 THE WARGAME 駭客訓練基地
  - 證照 EC-Council Certified Ethical Hacker

兩隻蜥蜴還是兩隻壁虎?

- To see is to believe
- Surf the Internet every day
- Maybe you are an accessory

Malicious Web Browser Attack

- 灌籃高手：控制籃下就等於控制了整場比賽
- 駭客高手：控制瀏覽器就等於控制了使用者

Features

- 竄改資料
  - 顯示的資訊
    - 擾亂視聽的資訊
  - 送出的表單
    - 串改傳送數值
    - 修改接收網址
  - 啓用的元件
    - 安裝/執行惡意元件
- 連線劫持

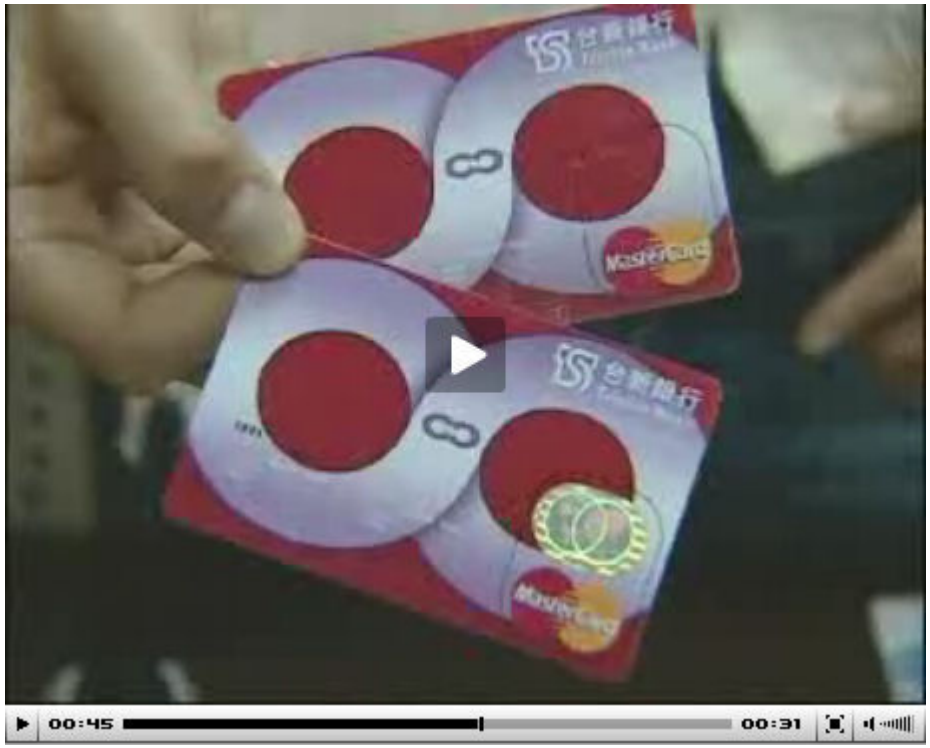
更有效率的攻擊方式

- 優點
  - 免利用任何網站弱點
    - SQL Injection
    - Cross Site Scripting
    - Cross-Site Request Forgery
    - etc …
  - 輕易繞過多種認證
    - Captcha
    - Sign-In Seal
    - One Time Password
    - Certification
    - IC Card
    - etc …
- 缺點
  - 必須用戶端執行 (Software, Plug-in, Spyware, etc…)

DEMO1

- 展示內容: 擾亂使用者視聽
- 適用對象: 所有網站

信用卡側錄與盜刷



在加油站刷卡加油要特別留意，國道公路警察局破一起盜刷集團派遣成員，應徵進入加油站當工讀生，充當盜刷集團的臥底來側錄顧客信用卡內碼，並且製作成偽卡到各大百貨盜刷，盜刷金額高達上億元，警方發現嫌犯當中，竟然還有一位是自稱是參與救治邵曉鈴的醫護人員。

嫌犯被捕時，坐在地上不發一語，隨後警方搜出偽造信用卡數百張，還有內碼燒錄器、印卡機，甚至連防偽標籤都有，可見集團犯眾手法相當精細。

DEMO2

- 展示內容: 竊取傳遞的資訊
- 適用對象:
  - 各種線上金流網站
    - ESafe, GreenWorld, EzPos, etc…
  - 各種線上購物網站
    - PChome, Yahoo, PayEasy, ETMall, etc…

駭客沒晶片金融卡 無法盜領

駭客沒晶片金融卡 無法盜領

【陳毓婷／台北報導】

網路ATM安全出現疑慮的傳言讓銀行公會昨日緊急召開記者會澄清。銀行公會資訊安全小組召集人羅安昌表示，即使電腦已遭駭客入侵，但駭客要同時握有晶片金融卡，才能執行網路ATM轉帳盜領。

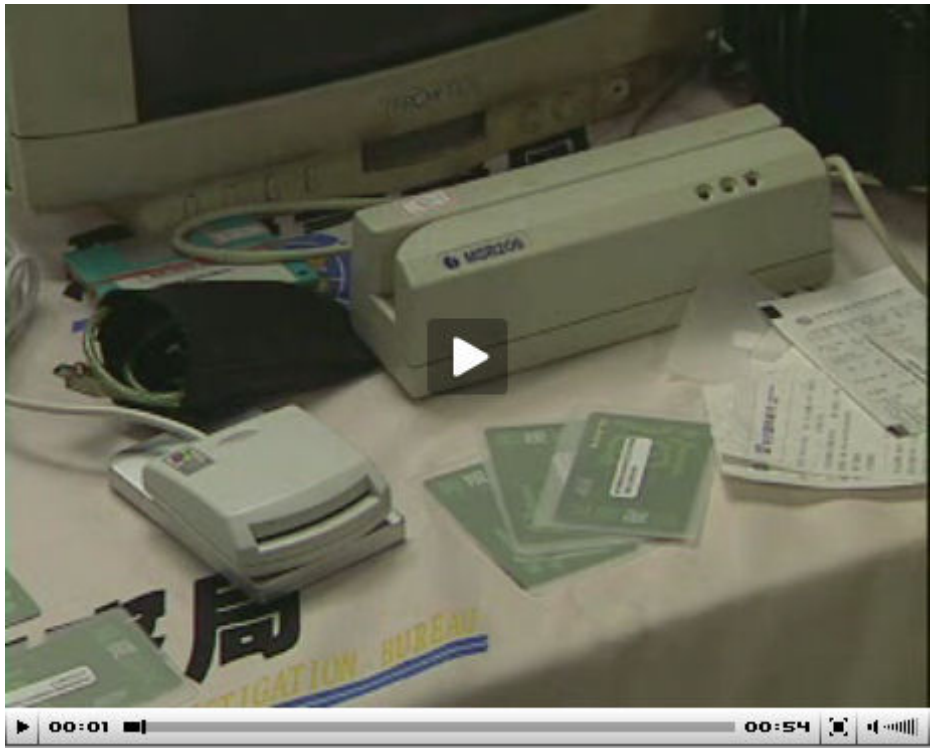
用戶利用網路ATM轉帳必須同時使用晶片金融卡及晶片讀卡機，交易的同時不僅需要輸入密碼，還必須同時插晶片金融卡，所以安全性高於一般的網路銀行。根據統計資料顯示，9月使用網路ATM跨行轉帳的筆數達41萬，總交易金額高達99億元，可見網路ATM的便利性及安全性。

然而在網路ATM逐漸普及時，也有傳言稱，若持卡人在使用後忘了將晶片金融卡從讀卡機抽出，駭客將可啟動電腦盜轉帳戶存款。對此，羅安昌表示，銀行公會曾經模擬測試持卡人遭木馬程式入侵，且將晶片金融卡插在讀卡機上的狀況，但實際上，駭客是無法成功盜轉。

他解釋，因為以目前的網路科技，駭客雖然可以利用木馬程式取得持卡人密碼，並利用遠端遙控方式啟動持卡人的個人電腦，但因為每台電腦都有IP(Internet Protocol)，遠端遙控的範圍有一定權限，在網路ATM的系統上，是不能透過遠端遙控發號指令，而必須要由讀卡機所屬的電腦發出訊息。

而且有別於過去的磁條卡，晶片金融卡還無法被複製，因此不需擔心因為駭客入侵，導致晶片金融卡被側錄的問題。另外，持卡人使用晶片金融卡時，輸入密碼是由晶片在封閉迴路內驗證密碼，確認密碼後再對電腦（或ATM）發出訊號，因此，即使有心人士取得密碼，也必須握有同一張晶片金融卡才能執行盜領轉帳。

鍵盤駭客入侵網路銀行安全堪虞



刑事局17日偵破了一起網路銀行鍵盤側錄密碼的案件。陳姓害客專門在網路上販賣虛擬銀行、ATM的讀卡機，然後在驅動程式中加入自己設計的鍵盤側錄程式，只要民眾在網路上使用晶片卡，條碼就會被完全側錄。還好警方在嫌犯盜刷這些晶片卡前逮捕他，這些被偷取條碼的民眾才沒有損失。要在虛擬的網路世界開戶，使用網路銀行就必須要讀卡機。只有高職畢業目前擔任電腦工程師的陳姓嫌犯就專門在網路上販賣讀卡機。不過，他自己設計了一套鍵盤側錄程式放在讀卡機的驅動程式中，只要民眾一刷卡，卡片的條碼就會完全被複製。

DEMO3

- 繞過複雜的認證
- 適用對象:
  - 各種網路銀行

Bypass ActiveX Object

- Patch ActiveX Object
- Replace Malicious ActiveX Object
- Session Hijacking

THANKS