



# Penetration Testing Practice

## 滲透測試實務應用

### 05 系統通行碼

孫士勝

Shi-Sheng Sun, Ph.D.

[sssun@nccu.edu.tw](mailto:sssun@nccu.edu.tw)

# 課程聲明

## Disclaimer

- 本課程所教授之滲透測試相關技術僅能於課堂中進行，若有任何超出範圍的動作，皆屬個人行為。  
The penetration testing techniques taught in this course are only to be used within this course. Any actions taken outside of this scope are the sole responsibility of the individual.
- 學員於課後使用任何網路攻擊技術對任何資訊設備進行攻擊，皆屬個人行為。  
Students are solely responsible for any network attacks carried out on any equipment after the course using any network attack techniques.

法規名稱：中華民國刑法 EN

法規類別：行政 > 法務部 > 檢察目

所有條文

編章節

條號查詢

條文檢索

沿革

立法歷程(附帶決議)

※如已配合行政院組織改造，公告變更管轄或停止辦理業務之法規條文，請詳見沿革

### 第二編 分則

#### 第三十六章 妨害電腦使用罪

- 第 358 條 無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。
- 第 359 條 無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。
- 第 360 條 無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。
- 第 361 條 對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。
- 第 362 條 製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。
- 第 363 條 第三百五十八條至第三百六十條之罪，須告訴乃論。

# ACM 道德與專業行為準則

## ACM Code of Ethics and Professional Conduct

- 1.1 增進人類社會福祉(Contribute to society and human well-being.)
- 1.2 避免傷害任何人(Avoid harm to others.)
- 1.3 誠實與值得信任(Be honest and trustworthy.)
- 1.4 公平且無犯罪意圖的行動(Be fair and take action not to discriminate.)
- 1.5 尊重智慧財產權(Honor property rights including copyrights and patent.)
- 1.6 維持智慧財產的完整性(Give proper credit for intellectual property.)
- 1.7 尊重他人隱私(Respect the privacy of others.)
- 1.8 遵守保密原則(Honor confidentiality.)



# 課前問券

- 系統通行碼 課前問券
- <https://forms.gle/9f5JUDU4uPyTeY2i7>



# 什麼是通行碼(Password)

- A confidential string used for authentication, protecting privacy and preventing unauthorized operations.



歡迎使用iNCCU單一認證窗口，您正在登入的系統是：

**Moodle 數位教學平台**

您多次登入失敗，請輸入下圖中的驗證碼，再輸入帳號。若驗證碼難以辨識，請按F5重新產生。

0338 輸入圖中數字(0~9)

請輸入在上圖中顯示之數字(0~9)。

帳號/學號

@nccu.edu.tw

密碼

☐ 記住我的帳號密碼

登入

建立帳戶

無法登入?



帳號/學號

@nccu.edu.tw

密碼

☐ 記住我的帳號密碼

登入

建立帳戶

無法登入?

了解更多 | 誰可以登入

校內分機67599・校外直撥(02)29387599

校址：11605 台北市文山區指南路二段64號

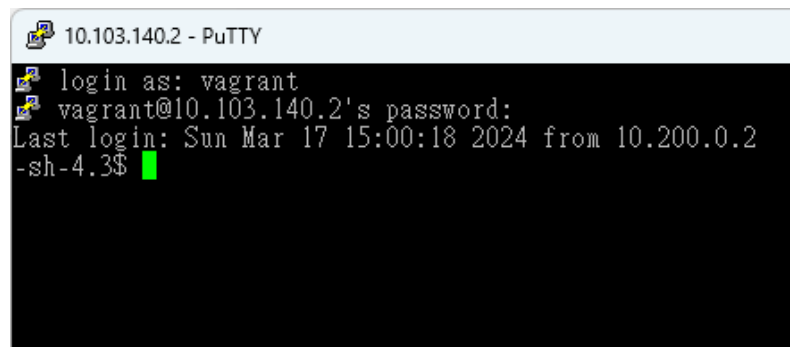
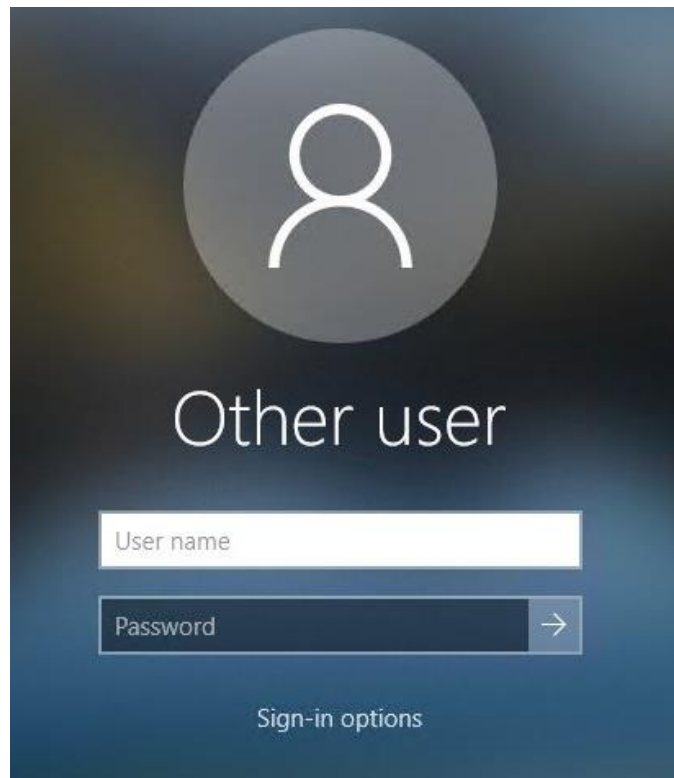
・總機電話：02-29393091

・傳真：02-29379611

The NCCU Web Mail login page. It has a blue header with the text "國立政治大學Web Mail系統" and "NCCU Web Mail". The main content area is a white box with a light blue background. It contains the text "請登入帳號密碼" and "Login with your NCCU mail account". Below this are two input fields: "帳號 Account" and "密碼 Password". At the bottom of the box is a "Login" button. Below the box are links for "忘記密碼" and "Need Help?". At the very bottom, there are four links: "建立帳號 Registry", "信箱App Mail App", "信箱安全 Security", and "系統說明 Manual".

# 通行碼應用

- 通行碼使用於：
  - 作業系統登入
    - Windows based
    - Unix-like based
  - 應用系統登入
    - Web applications
    - Apps
    - BBS...etc.



# 通行碼管理

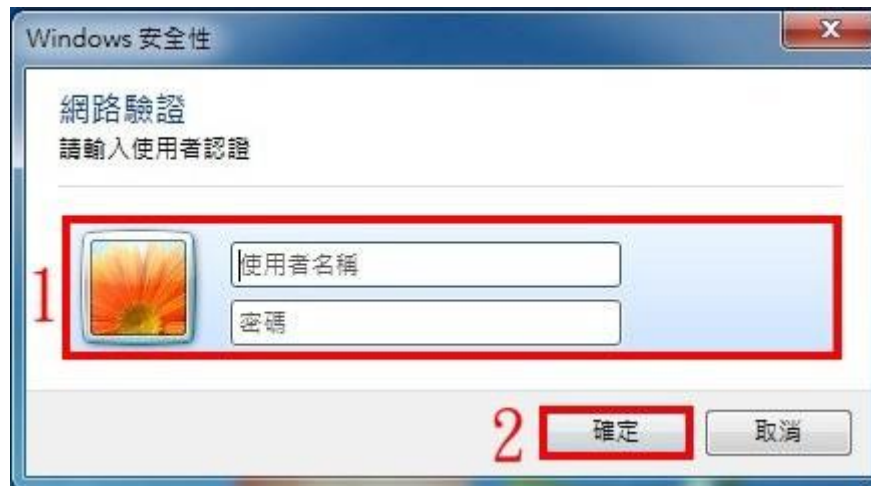
- 使用者認證
- 傳統通行碼認證
- Token認證
- 生物特徵認證





# 使用者認證 (1)

- 資訊安全基礎建設
  - 基於存取控制及使用者責任制
- 對於系統控管權，需有一套驗證使用者的程序，分為兩個步驟
  - **識別**：明確的使用者ID
  - **核實**：將個體(使用者)與ID綁定，並確認該ID屬於所屬之使用者





# 使用者認證 (2)

- 使用者認證概分四類
  - Something you know：個體所**認知**，如密碼、通行片語及PIN碼
  - Something you have：個體所**擁有**，如智慧卡、USB token、手機
  - Something you are：個體之**特徵**，如指紋、臉、虹膜及視網膜
  - Something you do：個別之**行為**，如聲音波型、筆跡、輸入習慣

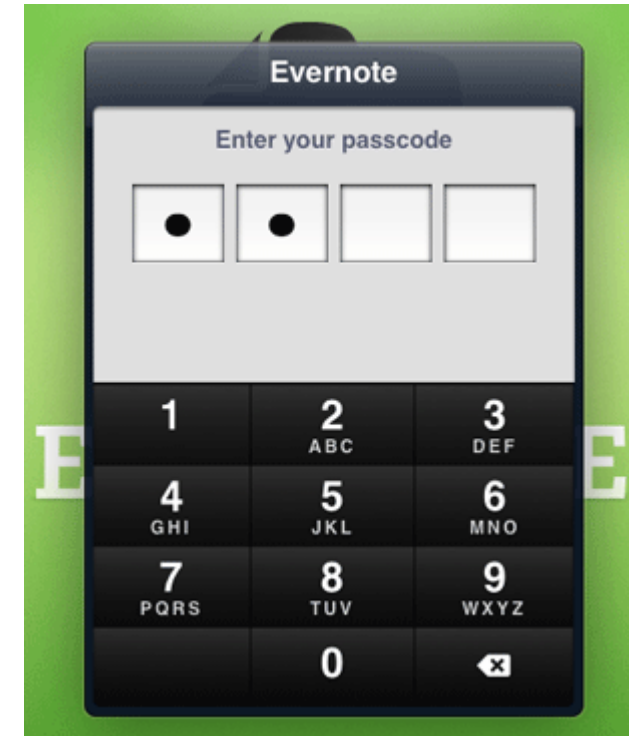


# 傳統通行碼認證

- 最常被使用的一種認證機制
  - 登入
    - 使用者輸入ID與Password
  - 查驗
    - 系統自動去資料庫或使用者密碼檔比對ID與Password是否正確配對

# ID & Password

- 一般來說，帳號分成：
  - 管理者帳號(admin account)
  - 一般帳號(normal account)
  - 來賓帳號(guest account)
- 脆弱的通行碼(weak password)
  - 容易猜測(easy to guess)
  - 容易知道(easy to know)
  - 有規則性，容易找到對應(easy to find)
  - 容易破解(easy to crack)



- 
- Department of Computer Science  
National Chengchi University



# Unix帳號雜湊通行碼的產生

- 系統會將通行碼與一個產生的salt結合，經過一個hash function後儲存

ID	Salt	Hash code
----	------	-----------

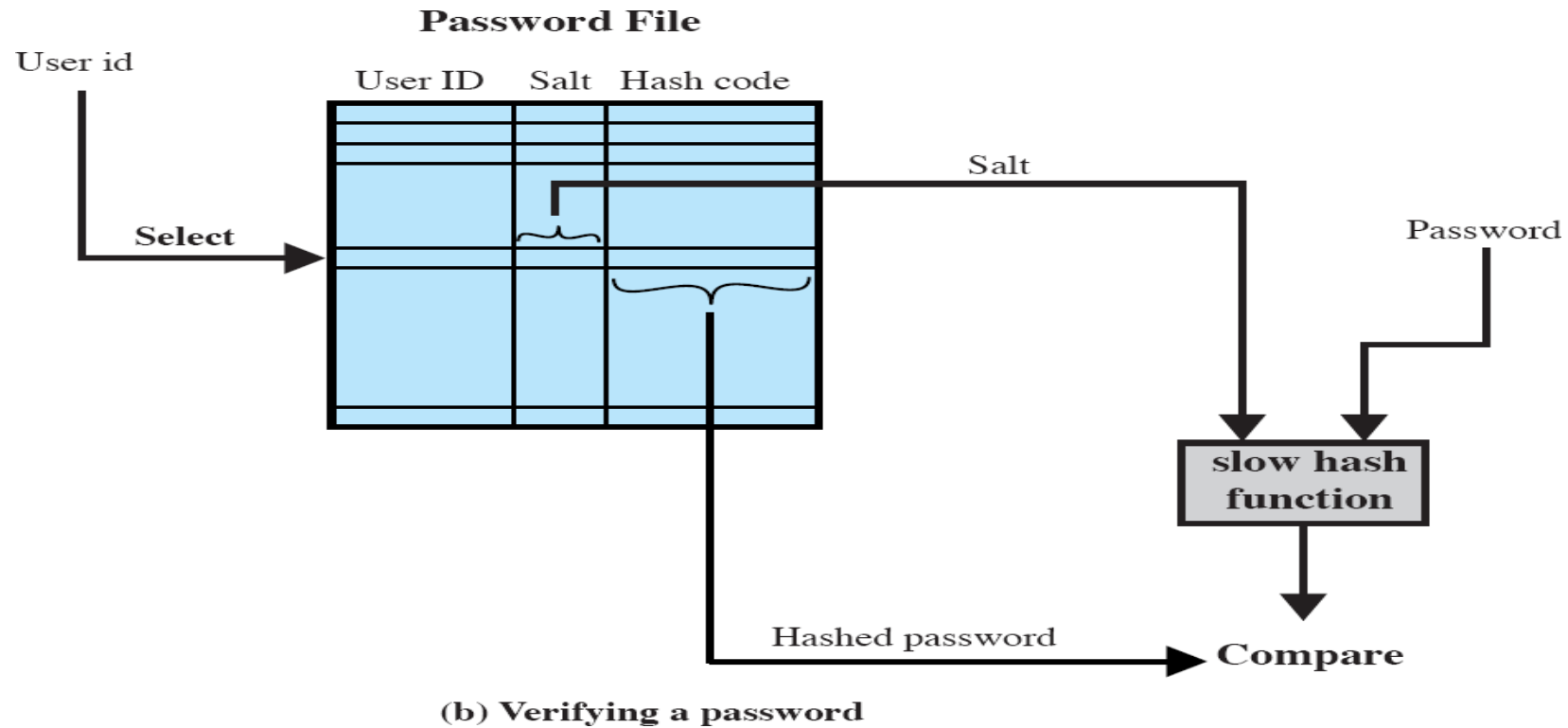


# Unix帳號雜湊通行碼的認證

- 當使用者輸入帳號與通行碼後，系統會到對應的帳號中取出salt數值，與使用者輸入的通行碼再次執行hash function 並比對產生的hash code，若是相符就是正確通行碼



# Unix帳號雜湊通行的認證



# Unix帳號雜湊通行碼的產生及認證

- 早期的系統設計使用修改過的1970年代DES加密演算法
  - 此方法目前已被破解：使用超級電腦，破解近億筆資料僅需數分鐘
- 現在有其他更完善的雜湊涵式和改進的亂數產生，過去有許多系統都用到MD5演算法
  - 使用48-bit的亂數(Salt value)
  - 通行碼長度不再受限制
  - 使用單向雜湊Hashing
  - 遞迴使用雜湊函數1000次
  - 產生128-bit的數列
- 目前較新的Linux亦已採用SHA 來取代MD5，更不易被破解
- 從BSD衍生出的類Unix作業系統--OpenBSD使用Crypt演算法加密
  - 使用128-bit salt 去產生192-bit 的雜湊值

# MD5演算法

- MD5( Message-Digest algorithm 5)雜湊演算法，是電腦常用的一種加密演算法，簡而言之，使用者可將任意長度的資料，以MD5雜湊演算法運算，得到一組固定長度為128位元(16位元組)的結果
- MD5為一個**單向雜湊演算法**，亦即不易以逆向運算得到原始資料，例如：要計算字串 “NCCU” 的MD5結果很簡單，但是要將MD5計算後的結果逆向運算得到 “NCCU” 卻相當困難。
  - $X = \text{MD5}(\text{"NCCU"}) = \text{DD8DA3F743717C4D}$
  - $X = \text{MD5}(\text{"nccu"}) = \text{40934B65D36C1BB5}$
  - $X = \text{MD5}(\text{"CCU"}) = \text{A375EB5F4E56D174}$
- MD5由MIT EECS教授羅納德·李維斯特(Ronald Linn Rivest，亦為RSA)設計，於1992年公開，用以取代MD4演算法，並由MD4、MD3、MD2改進而來，主要增強演算法的複雜度和不可逆性。這套演算法的程序在 RFC 1321 中被加以規範，將數據透過hash運算變為另一固定長度值，是雜湊算法的基礎原理
  - 1996年後被證實存在弱點，可以被加以破解，對於需要高度安全性的資料，專家一般建議改用其他演算法，如SHA-1。2004年，MD5演算法被證實無法避免碰撞，因此無法適用於安全性認證，如SSL公開金鑰認證或是數位簽章等用途



# UNIX下Password File的控管

- 只有特定權限的ID才能對password file做存取的動作
- 通常會另存一個shadow password file
- 雖然如此，但仍有下列幾項弱點
  - 駭客可能從作業系統的Bug下手
  - 可能會有使用者把Password File權限開啟，變成可讀
  - 使用者可能在別的作業系統使用同樣的通行碼
  - 可能被安裝了後門木馬程式
  - 從未受保護的網路上竊聽到通行碼

# UNIX系統下的使用者帳號與通行碼

## Storing UNIX Passwords

UNIX passwords were kept in a publicly readable file, `etc/passwords`.  
Now they are kept in a `"shadow"` directory and only visible by `"root"`.

PASSWD	SHADOW
sna:x:501:501:sna:/home/sna:/bin/bash cnyang:x:500:500:/home/cnyang:/bin/bash lily:x:502:502:/home/lily:/bin/bash	sna:\$1\$nP15UQFw\$15aD.J92mOEpnE2G/9owT0:12147:0:99999:7::: cnyang:\$1\$rTbmtV/Q\$usCiGXihKMH2jzEqG3pc6.:12207:0:99999:7::: lily:\$1\$8TomJ6..\$Qgr50Mkl6g8WtbSigr59A/:12207:0:99999:7:::
Username: passwd: UID: GID: user_information :directory:shell  username The user (login) name passwd The encoded password UID Numerical user ID GID Numerical default group ID User_information User's full name etc. directory User's home directory (Full pathname) shell User's login shell (Full Pathname)	Username: password: last: may: must: warn: expire: disable: reserved  username The User Name passwd The Encoded password last Days since Jan 1, 1970 that password was last changed may Days before password may be changed must Days after which password must be changed warn Days before password is to expire that user is warned expire Days after password expires that account is disabled disable Days since Jan 1, 1970 that account is disabled reserved A reserved field

# UNIX系統下的使用者帳號與通行碼

- `/etc/shadow` 以冒號 (:) 分成 9個欄位，各欄位功能如下 (詳細資料可查詢 `man 5 shadow`)
  1. 帳號名稱
  2. 密碼：目前大多使用 SHA 的格式來取代舊的 md5，因為其hash code長度較長，較不容易被破解
  3. 最近更動密碼的日期：主要以 1970/01/01 累積來的總日數
  4. 密碼不可被更動的天數：修改好密碼後，幾天內不能變更之意，0 代表沒限制
  5. 密碼需要重新變更的天數：修改好密碼後，幾天內一定要變更的意思，0 代表沒限制
  6. 密碼需要變更期限前的警告天數：第 3 與第 5 欄位相加後的幾天內，當使用者登入系統時，會警告該修改密碼了
  7. 密碼過期後的帳號寬限時間(密碼失效日)：密碼有效日期為『更新日期(第3欄位)』+『重新變更日期(第5欄位)』，過了該期限後使用者依舊沒有更新密碼，那該密碼就過期了
  8. 帳號失效日期：亦使用 1970/01/01 累加的總日數，這個欄位表示，此帳號在此欄位規定的日期之後，將無法再使用
  9. 系統保留尚未使用

# UNIX系統下的使用者帳號與通行碼

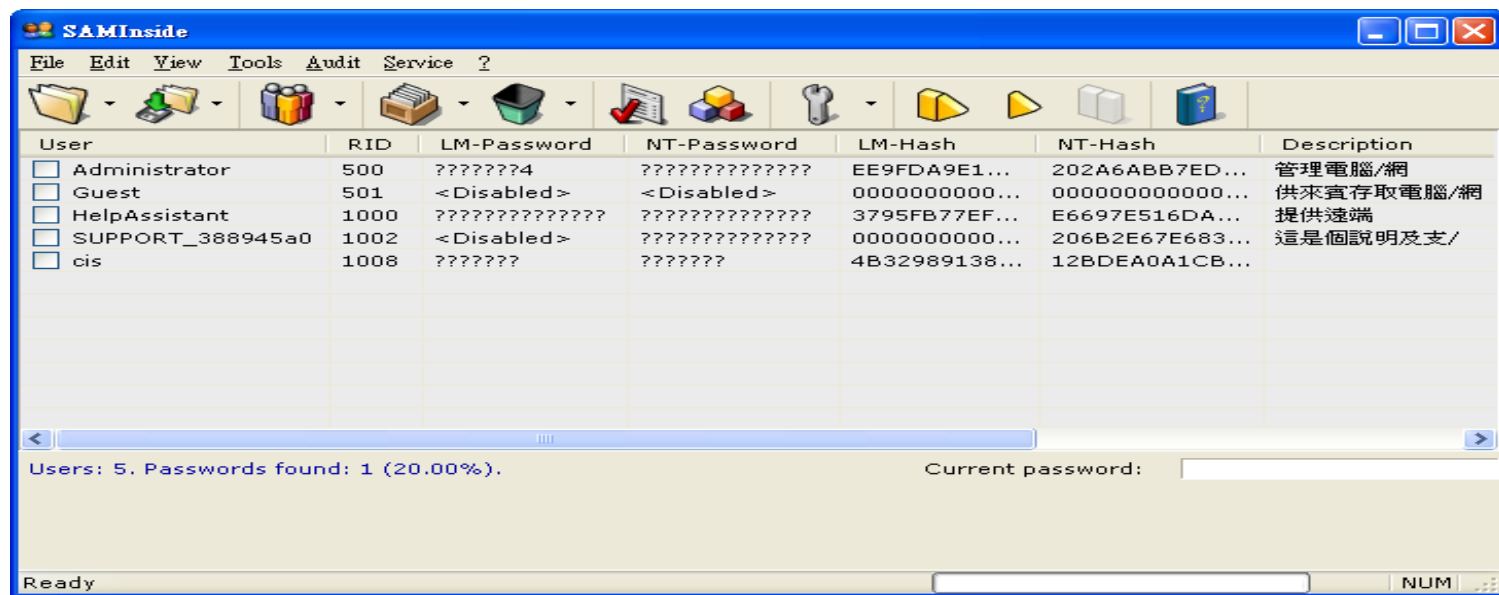
```
root@kali: ~  
root@kali:~# cat /etc/passwd  
root:x:0:0:root:/root:/bin/bash  
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin  
bin:x:2:2:bin:/bin:/usr/sbin/nologin  
sys:x:3:3:sys:/dev:/usr/sbin/nologin  
sync:x:4:65534:sync:/bin:/bin/sync  
games:x:5:60:games:/usr/games:/usr/sbin/nologin  
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin  
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin  
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin  
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin  
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin  
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin  
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin  
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin  
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin  
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin  
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin  
_lapt:x:100:65534::/nonexistent:/usr/sbin/nologin  
systemd-timesync:x:101:102:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin  
systemd-network:x:102:103:systemd Network Management,,:/run/systemd:/usr/sbin/nologin  
systemd-resolve:x:103:104:systemd Resolver,,:/run/systemd:/usr/sbin/nologin  
mysql:x:104:109:MySQL Server,,:/nonexistent:/bin/false  
Debian-exim:x:105:110:/var/spool/exim4:/usr/sbin/nologin  
uidd:x:106:112:/run/uidd:/usr/sbin/nologin  
rwhod:x:107:65534:/var/spool/rwho:/usr/sbin/nologin  
redsocks:x:108:113:/var/run/redsocks:/usr/sbin/nologin  
usbmux:x:109:46:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin  
miredo:x:110:65534:/var/run/miredo:/usr/sbin/nologin  
ntp:x:111:114:/nonexistent:/usr/sbin/nologin  
stunnel4:x:112:116:/var/run/stunnel4:/usr/sbin/nologin  
postgres:x:113:117:PostgreSQL administrator,,:/var/lib/postgresql:/bin/bash  
dnsmasq:x:114:65534:dnsmasq,,:/var/lib/misc:/usr/sbin/nologin  
messagebus:x:115:118:/nonexistent:/usr/sbin/nologin  
iodine:x:116:65534:/var/run/iodine:/usr/sbin/nologin  
arpwatch:x:117:120:ARP Watcher,,:/var/lib/arpwatch:/bin/sh  
Debian-snmp:x:118:123:/var/lib/snmp:/bin/false  
sshd:x:119:124:/nonexistent:/usr/sbin/nologin  
rtkit:x:120:125:RealtimeKit,,:/proc:/usr/sbin/nologin  
inetsim:x:121:126:/var/lib/inetsim:/usr/sbin/nologin
```

```
root@kali: ~  
root@kali:~# cat /etc/shadow  
root:$6$qvhlq171$/0wh10Y9i55tzFatxkzafR7n7KA2P2nRh7kMS082KR6V89ujtSTPEJ0QjXsRGpSEFuFKnCT0a0.g92kCst0P1:17938:0:99999:7:::  
daemon:*:17926:0:99999:7:::  
bin:*:17926:0:99999:7:::  
sys:*:17926:0:99999:7:::  
sync:*:17926:0:99999:7:::  
games:*:17926:0:99999:7:::  
man:*:17926:0:99999:7:::  
lp:*:17926:0:99999:7:::  
mail:*:17926:0:99999:7:::  
news:*:17926:0:99999:7:::  
uucp:*:17926:0:99999:7:::  
proxy:*:17926:0:99999:7:::  
www-data:*:17926:0:99999:7:::  
backup:*:17926:0:99999:7:::  
list:*:17926:0:99999:7:::  
irc:*:17926:0:99999:7:::  
gnats:*:17926:0:99999:7:::  
nobody:*:17926:0:99999:7:::  
_lapt:*:17926:0:99999:7:::  
systemd-timesync:*:17926:0:99999:7:::  
systemd-network:*:17926:0:99999:7:::  
systemd-resolve:*:17926:0:99999:7:::  
mysql!:17926:0:99999:7:::  
Debian-exim!:17926:0:99999:7:::  
uidd:*:17926:0:99999:7:::  
rwhod:*:17926:0:99999:7:::  
redsocks!:17926:0:99999:7:::  
usbmux:*:17926:0:99999:7:::  
miredo:*:17926:0:99999:7:::  
ntp:*:17926:0:99999:7:::  
stunnel4!:17926:0:99999:7:::  
postgres:*:17926:0:99999:7:::  
dnsmasq:*:17926:0:99999:7:::  
messagebus:*:17926:0:99999:7:::  
iodine:*:17926:0:99999:7:::  
arpwatch!:17926:0:99999:7:::  
Debian-snmp!:17926:0:99999:7:::  
sshd!:17926:0:99999:7:::  
rtkit:*:17926:0:99999:7:::  
inetsim:*:17926:0:99999:7:::
```



# Windows系統下的帳號與通行碼檔

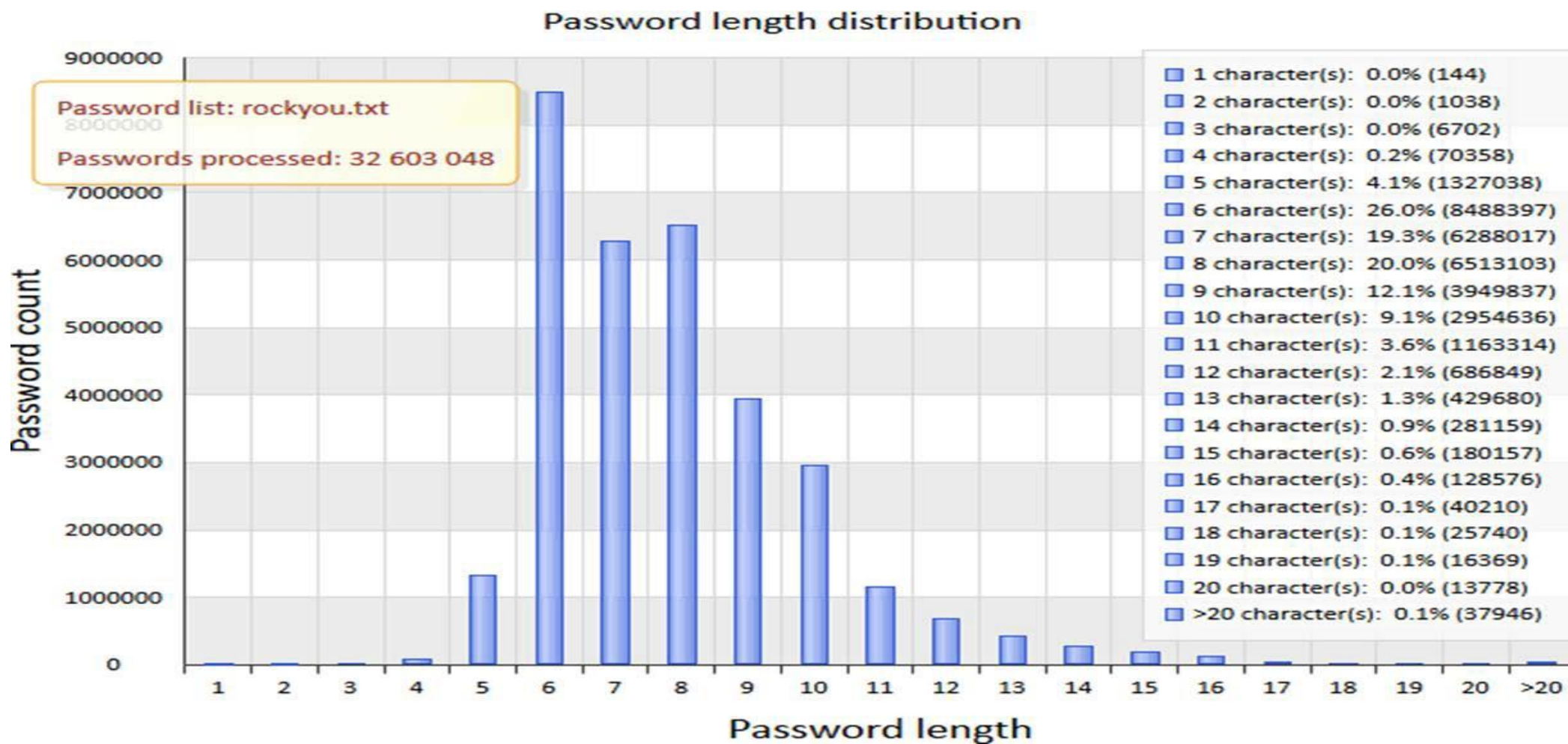
- Windows會將使用者帳號與通行碼的檔案鎖住不能開啟且更動，以下是一個已擷取過後的Windows帳密的簡單頁面
- 視窗中顯現的User、LM-Password、NT-Password為Windows的帳號與通行碼檔
- 過去的Windows所使用的LM hash(LAN Manager Hash)即為一個例子，以下為運作方式：
  - 將通行碼中的所有小寫字元轉換成大寫。使用 NULL 字元填補通行碼，直到通行碼的長度正好是**14 個字元**，分成各 7 個字元的兩個區塊，使用上述區塊作為**DES 機碼**，來加密特定字串。將兩段通行碼文字串連成 128 位元的字串，並儲存結果。



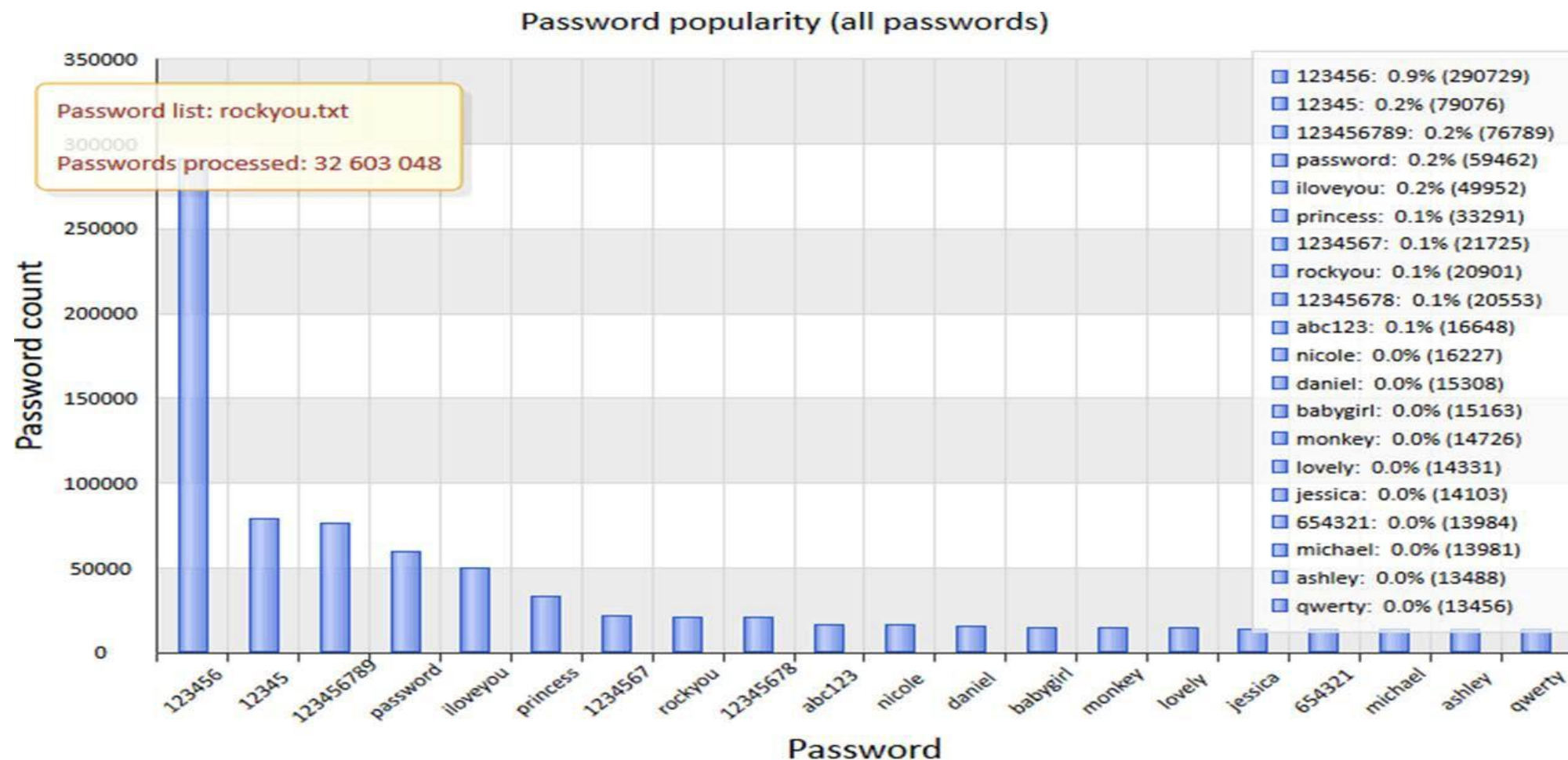
# 通行碼的選擇

- 使用者可能會選擇短通行碼以方便記憶
  - 例：有人會選擇3個字元或以下的通行碼，易被猜測
  - 有的系統會拒絕太短的通行碼，增加安全性
- 使用者可能會選擇可被猜測的通行碼
  - 攻擊者可能會列出一系列的可能通行碼
  - 通行碼可能為使用者的名字，預設密碼，帳戶名稱，或其它各種可能的個人相關資料(生日、電話)
  - 可能是上述資料的相關延伸，例如：John變成John0912345678

# 使用的通行碼長度統計



# 使用的通行碼統計



# However...

## 15 年前發明煩死人的密碼規則，Bill Burr：抱歉浪費大家時間

2023/10/19 · Mia · 密碼、規則、設定

相信大家都心有戚戚焉，每次碰到這些落落長的要求，心裡就有底，這組密碼防止自己登入的次數將比防止被盜的次數還來得多。

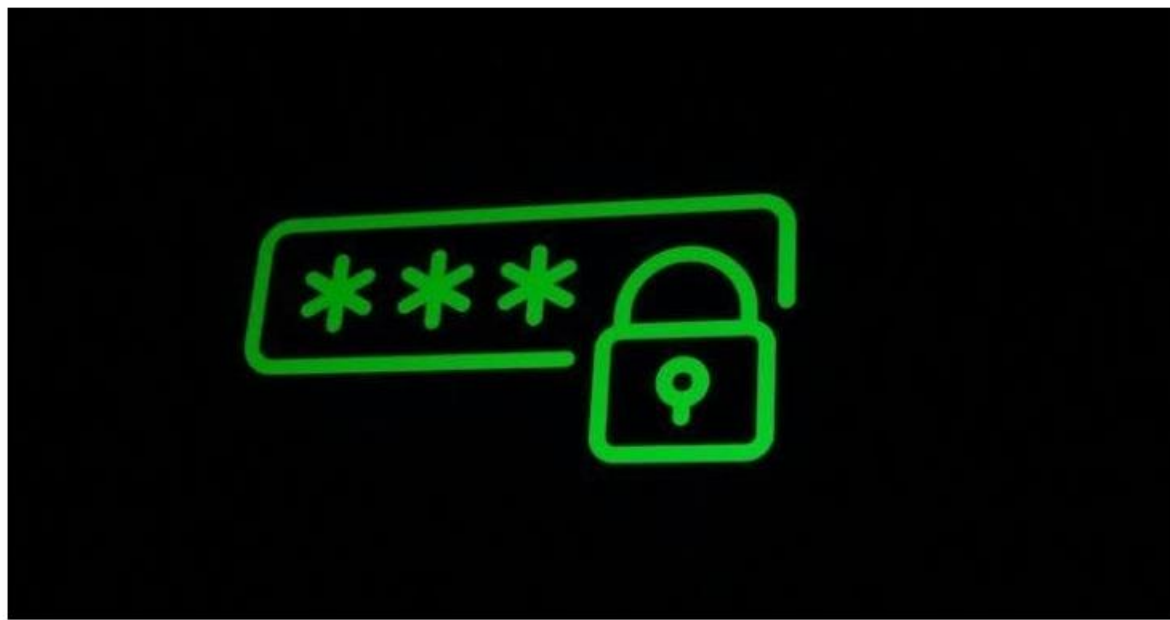


Photo Credit: Christiaan Colen on Flickr

大家是不是都有這樣的經驗呢？當你要設定新密碼的時候，出現了這樣的一行提示：密碼長度不得低於 8 位數、必須同時包含大小寫英文、數字、符號，且相同字元不得重複超過 3 次、英文或數字間不得連續…… 相信大家都心有戚戚焉，每次碰到這些落落長的要求，心裡就有底，這組密碼防止自己登入的次數將比防止被盜的次數還來得多。

那你知道這種規則是誰創造的嗎？一切都始於近 15 年前，一名叫 Bill Burr 的美國國家標準技術研究所（NIST，National Institute of Standards and Technology）主管。Bill Burr 2003 年草擬了一份 8 頁的指南，教大家怎麼建立安全的密碼，這份文件就叫做「NIST 特別刊物 800-63. 附錄 A」。裡面建議大家設定密碼要用奇怪而無意義的字加上罕見的字元、大寫英文和數字，並且時常更換密碼。

# 使用更安全的通行碼

- 有意義的通行碼易被猜測，但不規律的通行碼卻不易被使用者記下
- 使用讓使用者更容易記得，也必須是要不易被猜測的通行碼，例如：
  - 電腦產生的通行碼
    - 使用密碼管理器或線上密碼產生器，生成隨機且複雜的通行碼
    - 這些工具通常可以設置密碼長度、包含的字元類型（大小寫字母、數字、符號）等
  - 可使用通行碼提示，方便自己記憶
    - 建立容易記住的提示或規則，幫助您記住複雜的通行碼
    - 可以使用一句話的首字母組成通行碼，或者將多個單字組合起來，並加入數字和符號
    - 注音符號或是各類輸入法的對應鍵盤位置輸入



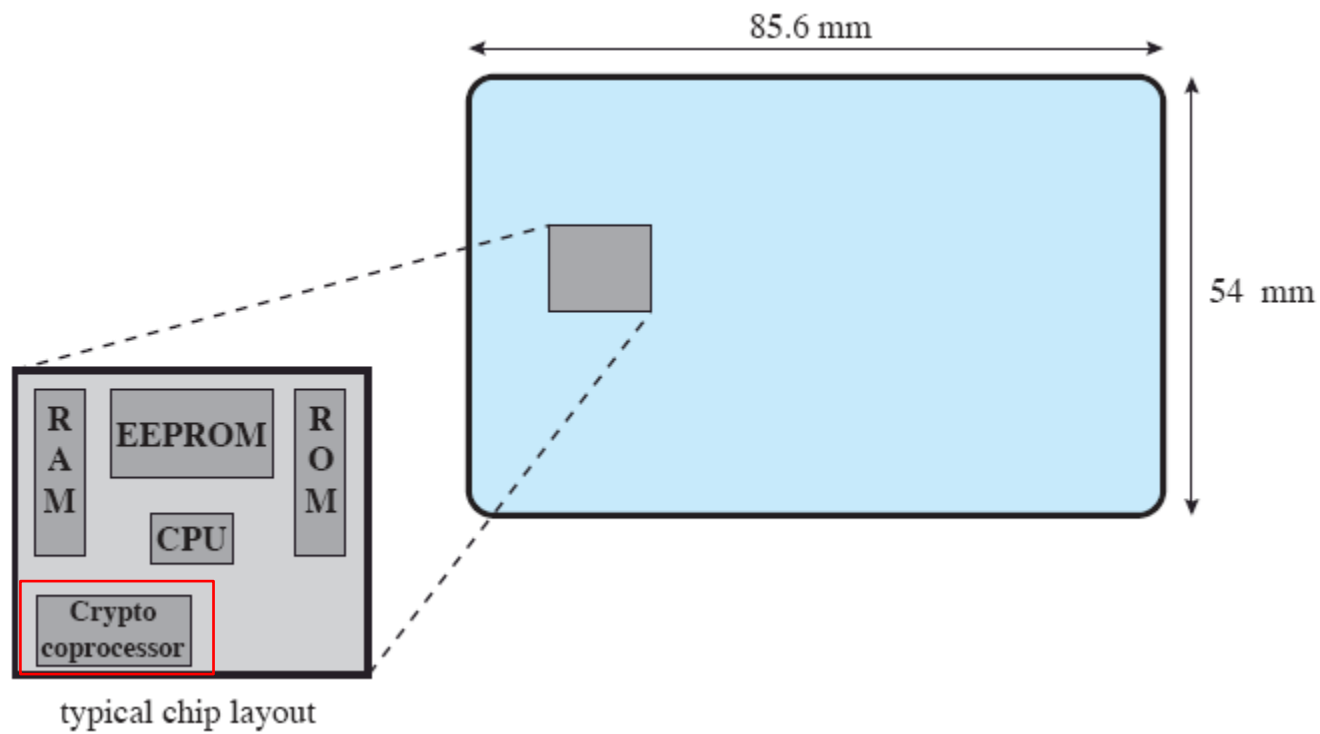
# Token認證 - 記憶卡(Memory Card)

- 單純儲存資料而不對其內容做處理
  - 磁條卡，如部份銀行卡與鑰匙卡
  - 電子記憶卡
- 單獨用於實體上的存取
- 配合電腦使用則可搭配ID/Password
- 不方便的地方
  - 需搭配特定的讀卡機
  - 使用者的不便



# Token認證 - 智慧卡(Smart Card)

- 智慧卡內的積體電路，包含了處理器(CPU)、唯讀記憶體(ROM)、隨機存取記憶體(RAM)以及電壓消除式可程式化唯讀記憶體 (EEPROM)。IC採用環氧化物嵌入，再透過導線連到電子接觸點，以便觸通讀卡機內部的接觸點；或是連到天線，透過無線電波與讀卡機通訊；或是兩者兼具。



# 非接觸式智慧卡

- 台灣現今的非接觸式智慧卡大部分都是使用ISO/IEC 14443 標準，NFC 可提供完全相容ISO/IEC 14443 的非接觸式智慧卡，它可以藉由快速感應及自動辨識功能達到身份驗證目的。

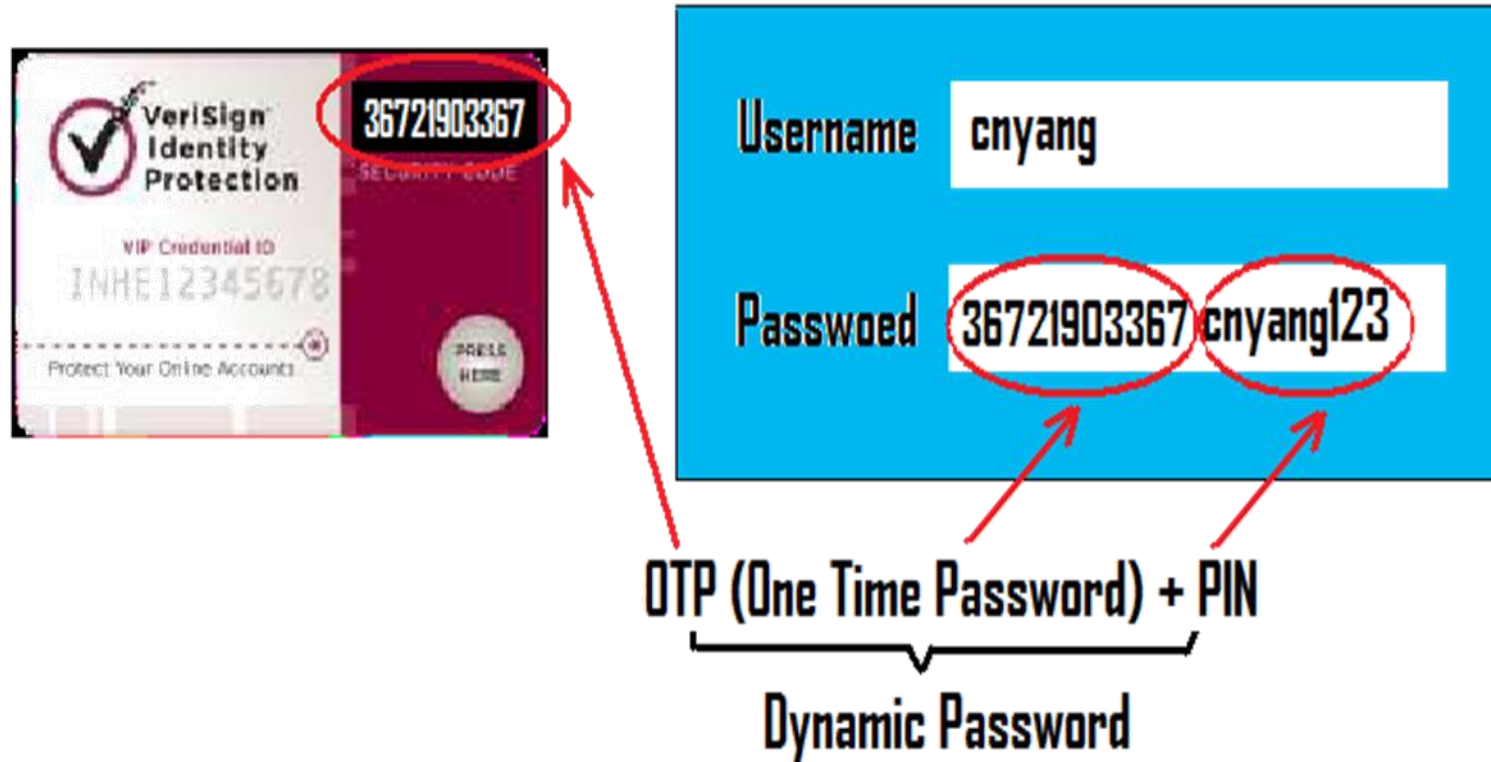
	傳輸速率	通訊距離	頻段	方向性	網路型態	國際標準	安全協定
RFID	106、212、424Kbps	3至10cm	13.56MHz	全向性	點對點	ISO/IEC 14443、10536、15693	ISO/IEC 7816、EMV
NFC	106、212、424Kbps	20cm	13.56MHz	±15度	點對點	ISO/IEC 18092、21481	ISO/IEC 7816、EMV

# Token認證 - 一次密碼智慧卡(One Time Password, OTP)

- 將信用卡提供顯示的功能，顯示的可能是時刻在改變、安全性較高的動態密碼，也可顯示信用餘額或累積紅利點數等。每次登入使用時，除詢問使用者PIN密碼外，系統會隨機產生一隨機密碼，使用者依此密碼取得使用權限。因此，每次登入系統密碼均不相同，藉此提高安全性



# 動態通行碼Dynamic Password

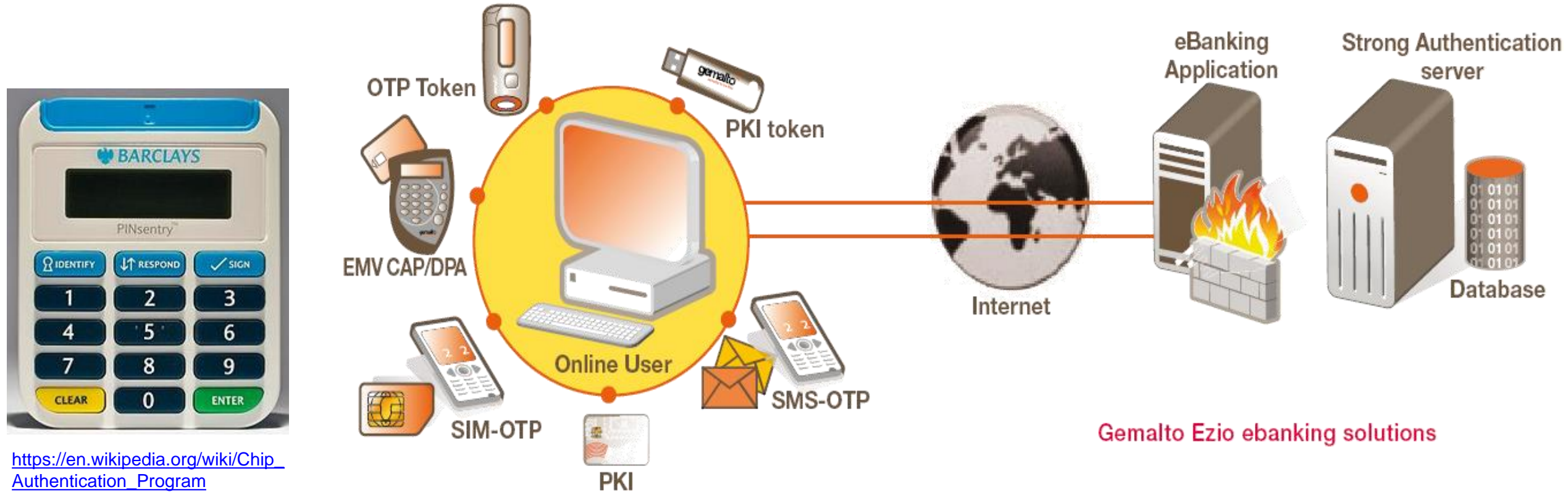


# Authenex A-key

- 內建晶片運算為核心的多功能認證硬體
- 獨一無二的32位元ESN碼(Electronic Serial Number，電子序列號)
- 隨機產生的4096-bit共用密碼
- OTP演算法：AES，SHA-1，HMAC-1
- 符合FIPS140-2 Level3標準
- 依循OATH所產生的160-bit OTP

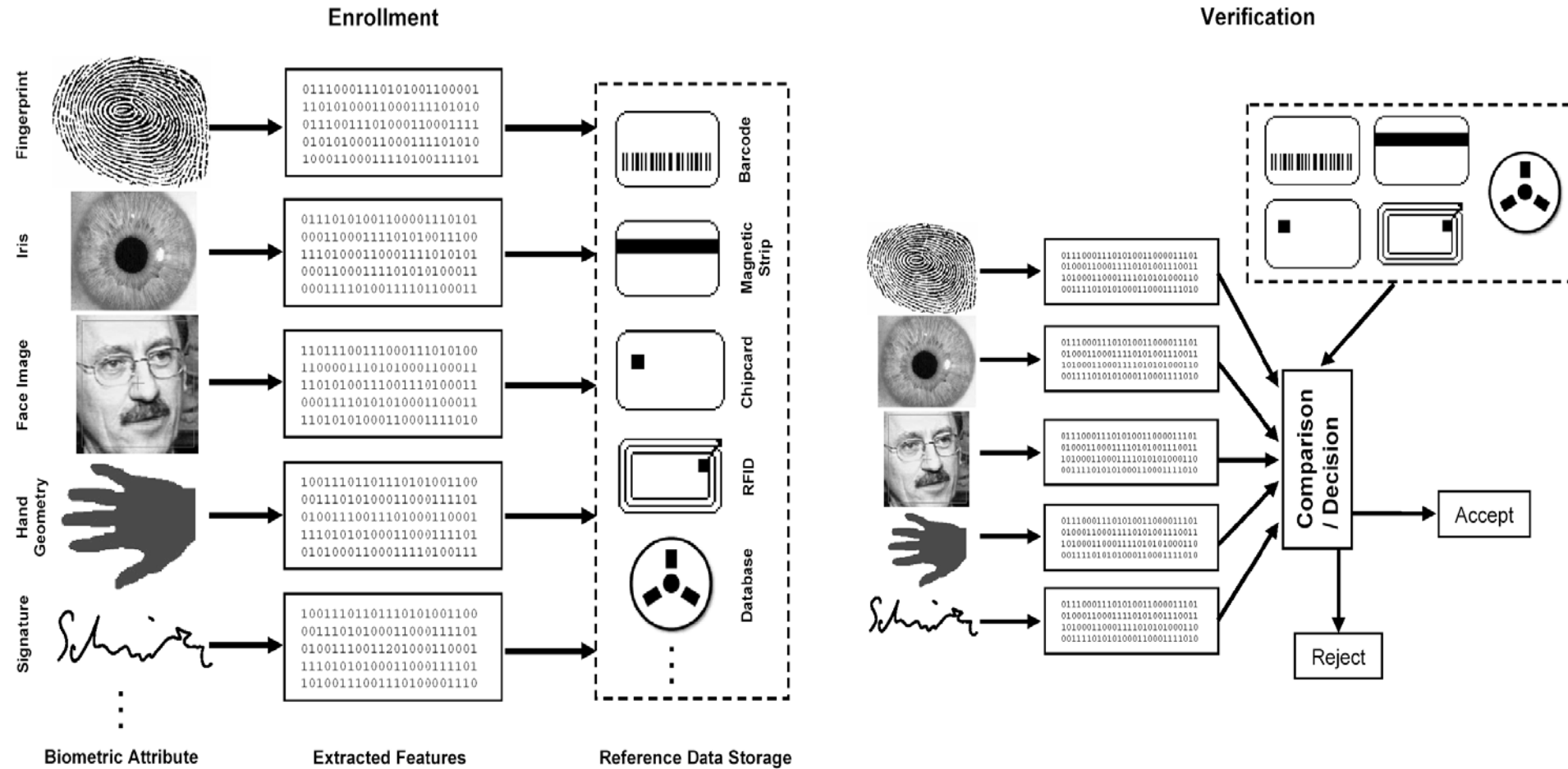


# OTP : E-Banking Solution





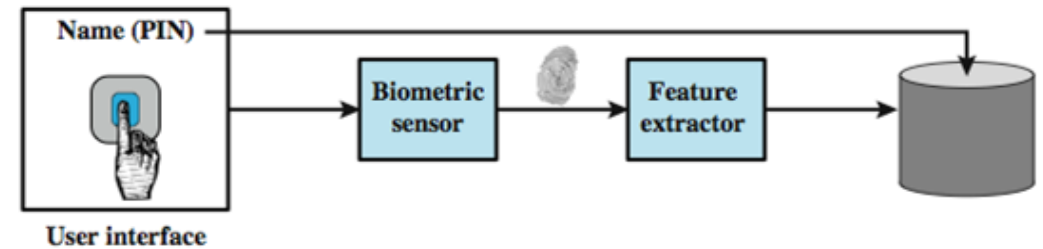
# 生物特徵認證



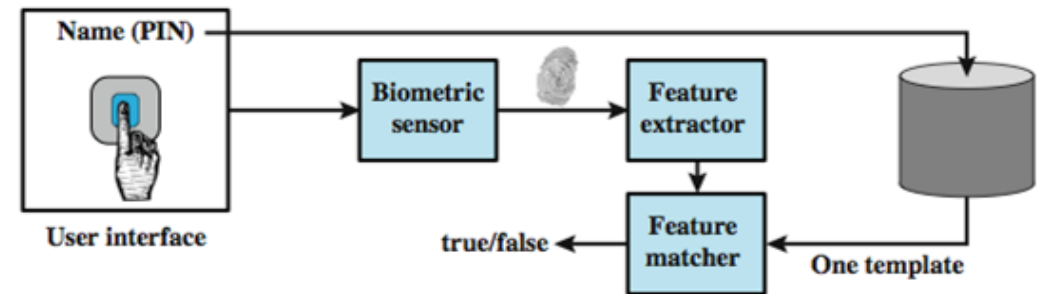


# 生物特徵認證 - 指紋

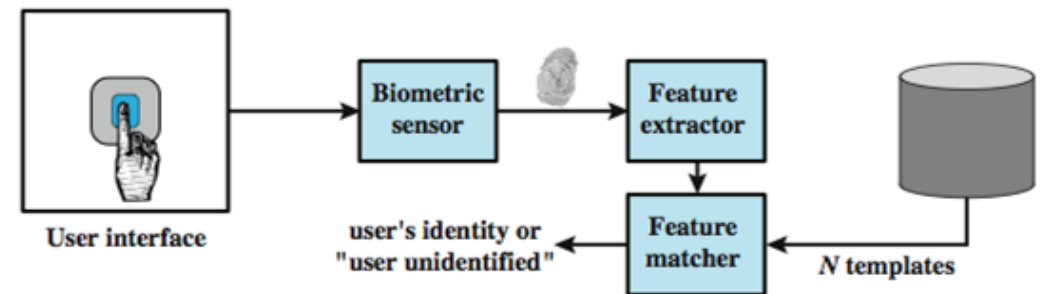
- 辨識速度快、正確性高
  - 相關設備普及容易取得
  - 國際標準
    - ISO/IEC JTC 1/SC 37 19794-2



(a) Enrollment



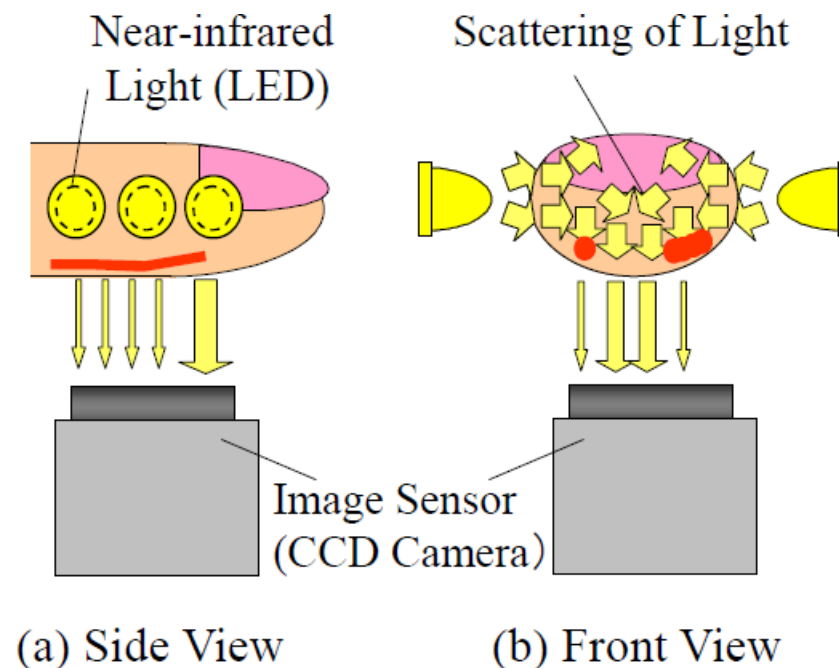
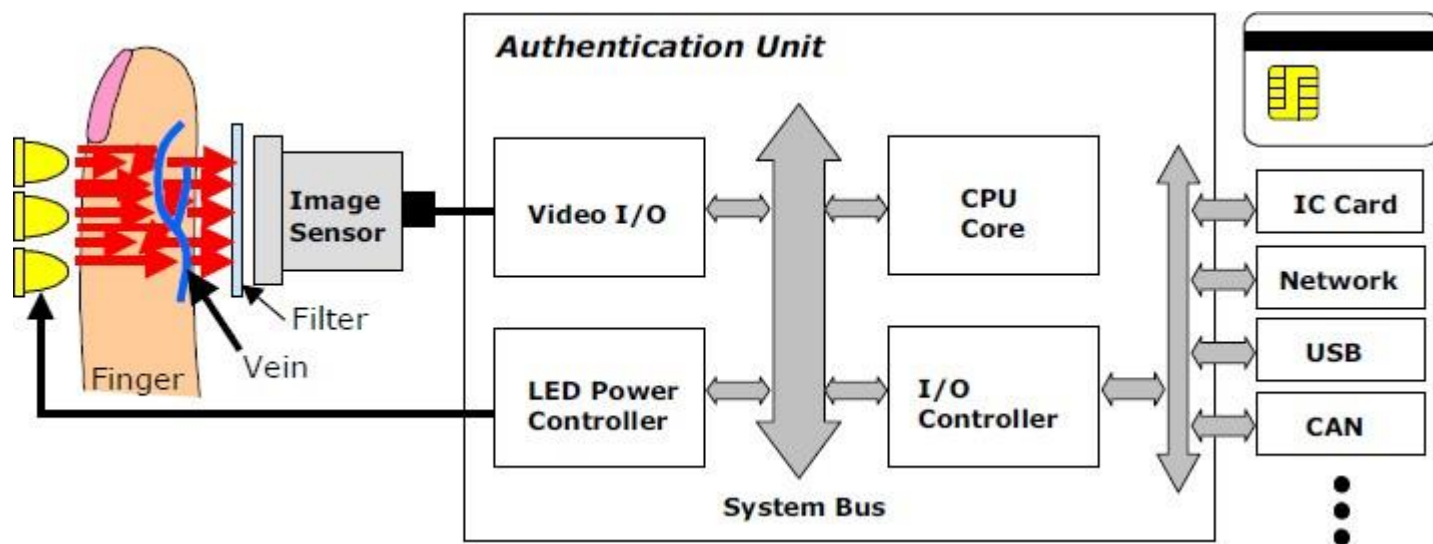
(b) Verification



(c) Identification

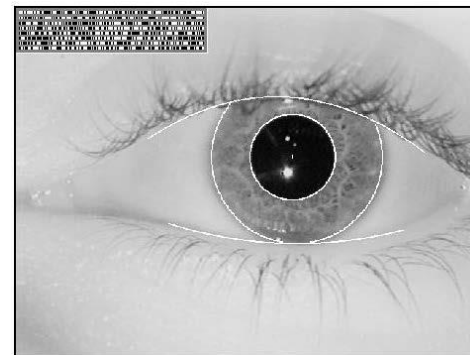
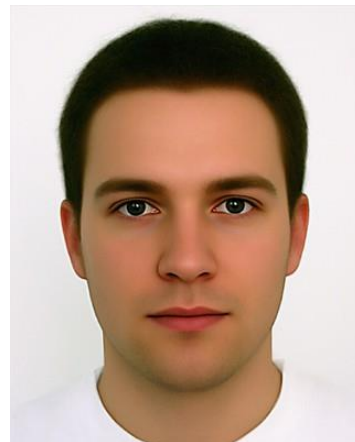
# 生物特徵認證 - 指靜脈辨識

- 適用於機場等出入複雜區域
- 指靜脈獨一無二，永久性，無法複製性



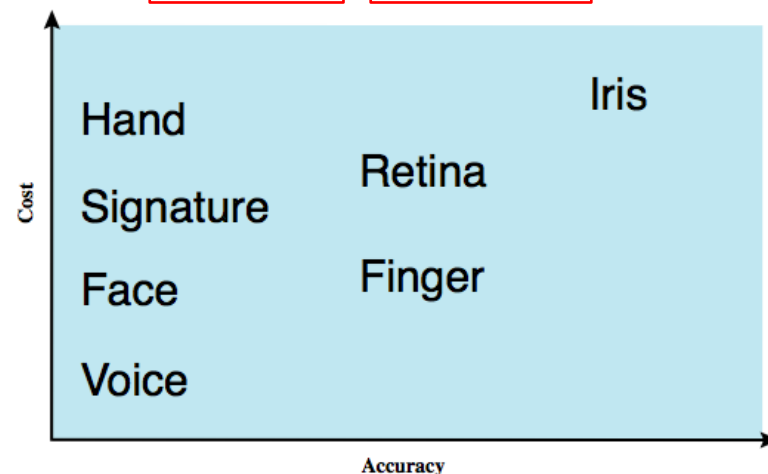
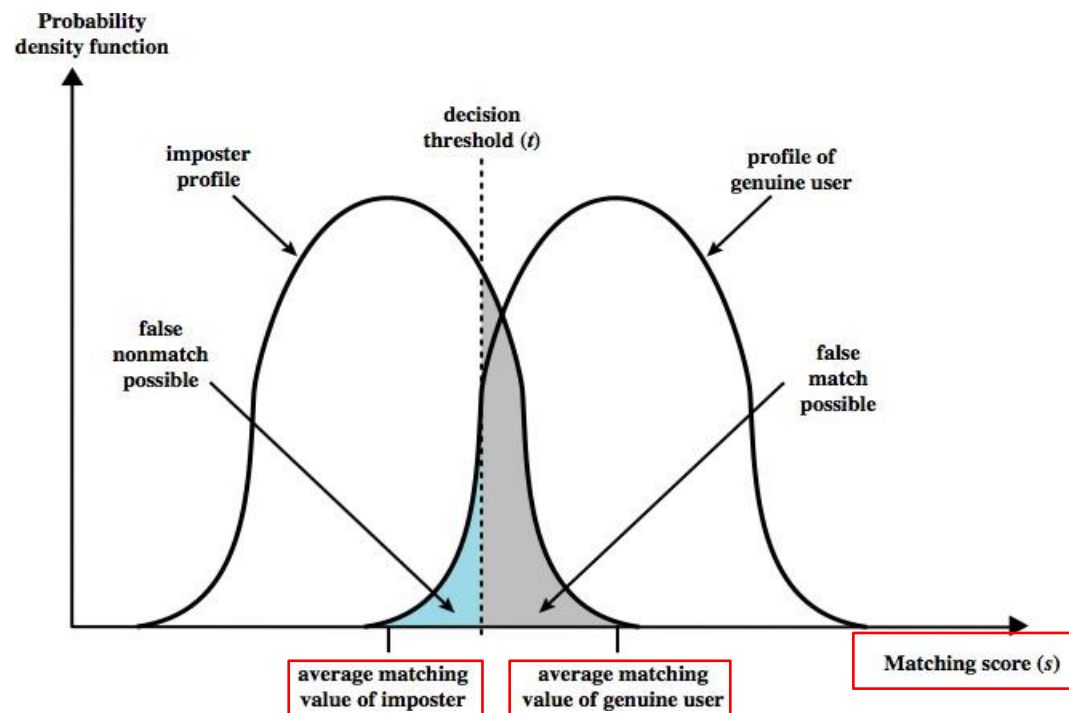
# 生物特徵認證 - 人臉辨識與人眼虹膜

- 不需接觸，適用於機場等出入複雜或是疾病易傳播區域
- 國際標準
  - ISO/IEC JTC 1/SC 37 19794-5
- 需要精準攝影機
- 比對技術較為複雜
- 隱私性問題
  - 可能由虹膜得知相關疾病



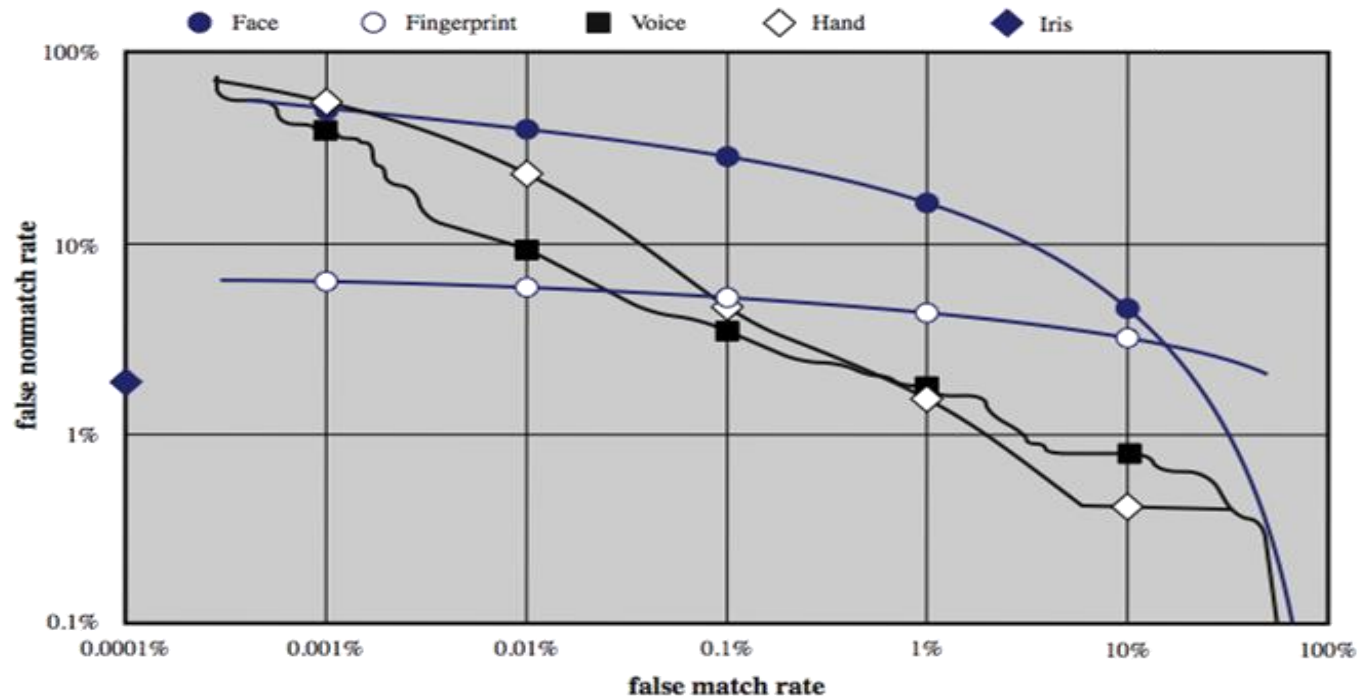
# 生物特徵認證的準確性(1)

- 不會有重複的樣本
- 目前在一些精準度指標上仍有爭議以及待改善空間：
  - False Non-Match Rate (FNMR) :
    - 錯誤不符率，可視為False Rejection Rate (FRR，錯誤拒絕率)，為生物特徵認證系統將合法使用者誤判為不合法使用者的機率
    - 應該為TRUE的卻判斷錯誤 / 所有TRUE，代表系統的便利程度
  - False Match Rate (FMR) :
    - 錯誤匹配率，可視為False Acceptance Rate (FAR，錯誤接受率)，為生物辨識系統誤將不合法使用者辨認為合法使用者的機率
    - 應該為FALSE的卻判斷錯誤 / 所有FALSE，代表系統的安全程度
  - Decision threshold該如何選擇？



# 生物特徵認證的準確性(2)

- 可以繪出特徵曲線
- 藉由選出適當的臨界值，可降低錯誤率





# 通行碼破解

- Popular Password攻擊法與猜測法
- 字典攻擊法
- 暴力法
- 網路竊聽
- 社交工程

# Popular Password攻擊法與猜測法

- Popular Password 攻擊法
  - 正如字面意義所說，此攻擊法能對多數範圍的ID做密碼猜測。因為 Popular password可能指的是某電影明星、某個樂團、某個偉人，範圍相當廣。而這些可能是大家都耳熟能詳的，所以都有可能拿來做通行碼。例如：Taiwan、The Beatles、Tom Cruise、Jay Chou、BTS、BLACKPINK...
- 猜測法
  - 攻擊者在破解通行碼時可以透過使用者個人資訊來猜測。例如生日、身份證號碼、電話號碼、及使用者有關之紀念日等

# Dictionary Attack字典攻擊法 (1)

- 對於字典攻擊法意指在一組小範圍的字典檔中，攻擊者從中嘗試 使用各種可能的通行碼，利用這些可能的帳號通行碼登入伺服器，直到找到正確的通行碼為止
- 例：John the Ripper字典模式，可以指定字典檔，並使用進階指令加入規則，可將字典檔內的資料做有規則的排列或是重組等等，之後再跟通行碼檔比對，有效地破解通行碼

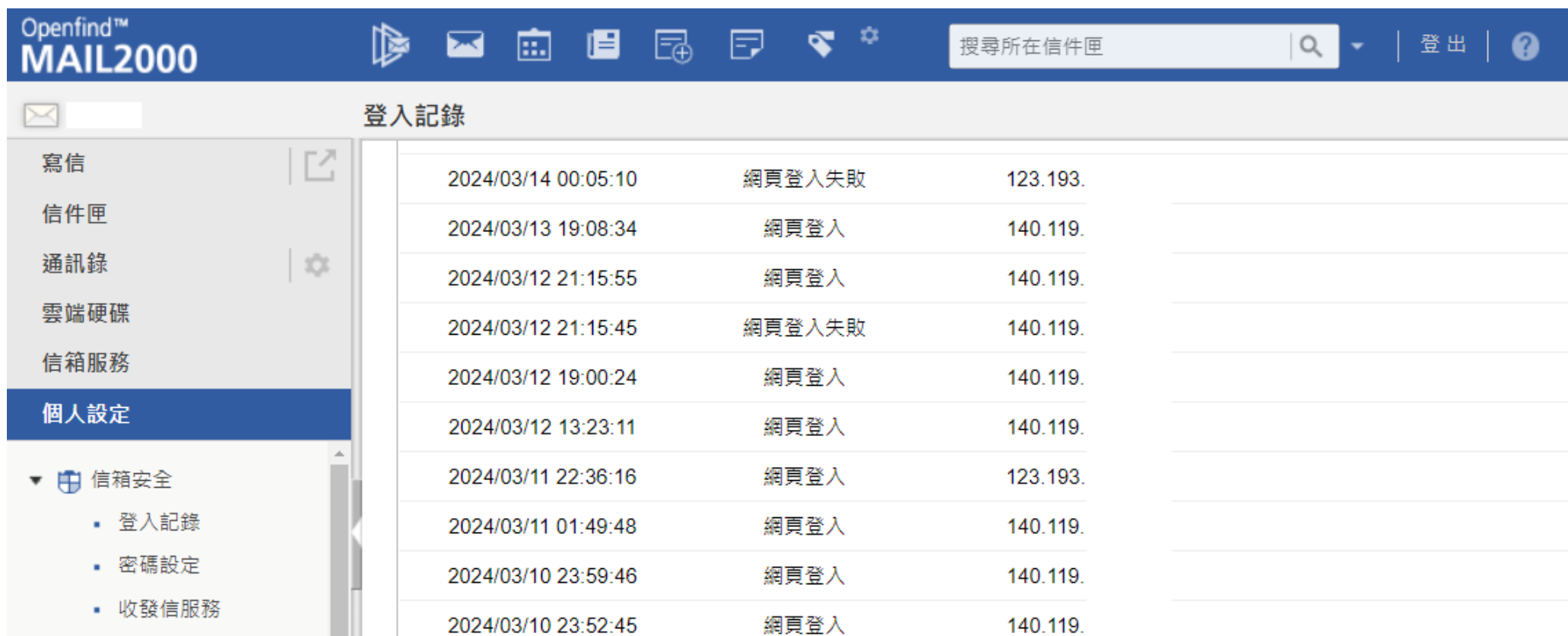


# Dictionary Attack字典攻擊法 (2)

- 線上(Online) - 字典攻擊
  - 攻擊者在網路上直接對伺服器做帳號通行碼登入驗證，以便檢查猜測的通行碼是否可正確登入
  - 線上字典攻擊會在伺服器日誌紀錄檔中留下大量的通行碼登入錯誤紀錄
- 離線(Offline) - 字典攻擊
  - 不需與伺服器做互動帳號通行碼驗證，攻擊者透過伺服器中其他系統漏洞盜取伺服器的通行碼檔。取得通行碼檔後，可讓攻擊者不需透過登入伺服器的程序，來進行破解

# Dictionary Attack字典攻擊法 (3)

- 以NCCU Webmail為例，當連續輸入錯誤通行碼，會被伺服器記錄下來，內容包括日期、IP、登入狀態等。

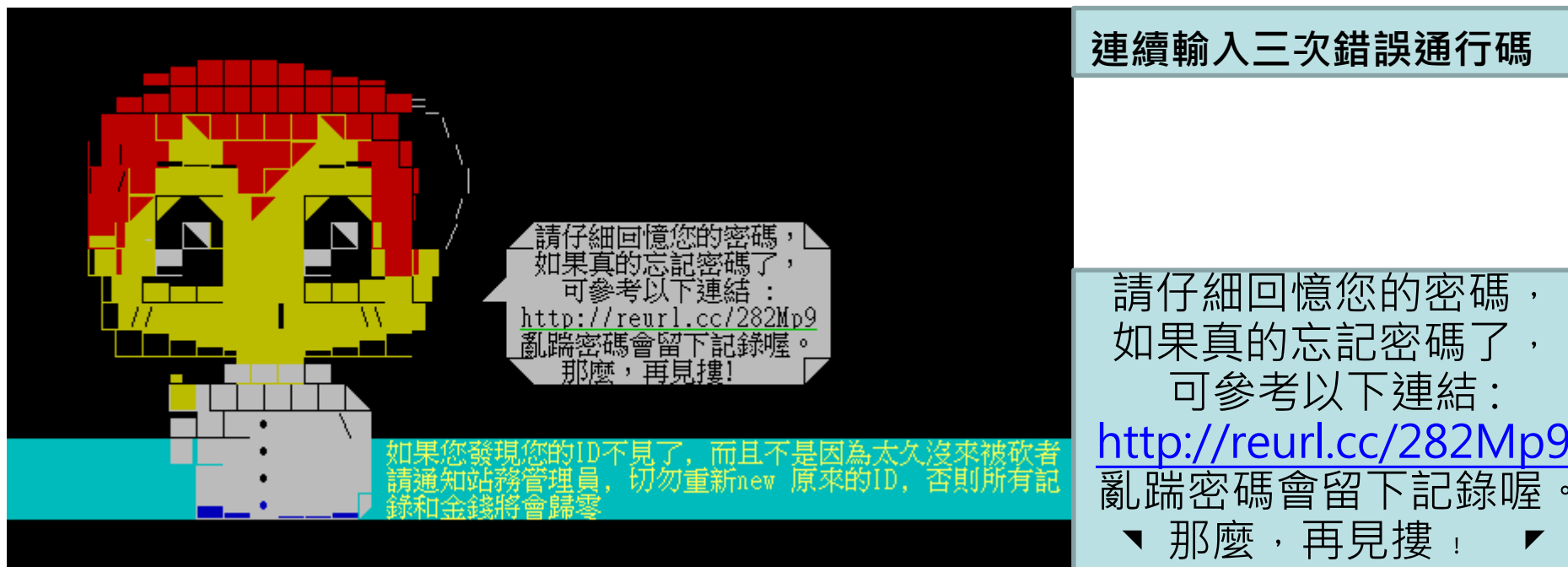


The screenshot shows the NCCU Webmail interface. The top navigation bar includes the 'Openfind™ MAIL2000' logo, several icons for mail functions, a search bar labeled '搜尋所在信件匣', and links for '登出' (Logout) and help. The left sidebar contains a menu with options: '寫信' (Compose), '信件匣' (Inbox), '通訊錄' (Address Book), '雲端硬碟' (Cloud Drive), '信箱服務' (Mailbox Services), and '個人設定' (Personal Settings). Under '信箱安全' (Mailbox Security), there are sub-options: '登入記錄' (Login Records), '密碼設定' (Password Settings), and '收發信服務' (Mail Services). The main content area is titled '登入記錄' (Login Records) and displays a table of login attempts.

時間	登入狀態	IP
2024/03/14 00:05:10	網頁登入失敗	123.193.
2024/03/13 19:08:34	網頁登入	140.119.
2024/03/12 21:15:55	網頁登入	140.119.
2024/03/12 21:15:45	網頁登入失敗	140.119.
2024/03/12 19:00:24	網頁登入	140.119.
2024/03/12 13:23:11	網頁登入	140.119.
2024/03/11 22:36:16	網頁登入	123.193.
2024/03/11 01:49:48	網頁登入	140.119.
2024/03/10 23:59:46	網頁登入	140.119.
2024/03/10 23:52:45	網頁登入	140.119.

# Dictionary Attack字典攻擊法 (4)

- 以PTT BBS為例，當連續輸入三次錯誤通行碼後，系統判斷可能為攻擊，會中斷使用者連線，並於正常登入時顯示通行碼輸入錯誤訊息。讓使用者知道有人在嘗試破解他的密碼。



# 暴力法

- 將全部的有效鍵盤字符(大概95個)進行隨機的組合，去猜解通行碼。此模式效率極低，非常耗時
- 若通行碼使用8個字元，而鍵盤上可以輸入的字元變化全部有95個，若用暴力法破解的話就需要 $6.7 \times 10^{15}$ (次)
- John the Ripper提供的Incremental mode模式，就是一種暴力攻擊法

# 網路竊聽

- 最初網路封包擷取軟體是被設計做為網路分析的工具，擷取網路封包再分析封包上的內容，可方便網路工程師除錯、監控網路流量或診斷網路異常等問題
- 而現今的網路竊聽攻擊法是基於資料經由未加密的通道傳送，每個人都可以拿取這通道上的封包，利用封包擷取軟體來分析所抓取的封包，便可得知此封包中的訊息
- 如刻意分析含有使用者登入訊息的封包，便可竊聽到使用者的帳號與通行碼
- 網路竊聽是網路攻擊一種簡單但有效的攻擊方式，一般而言，攻擊者能夠藉由竊聽作為攻擊手段，主要是資料在Layer 2 Data Link Layer未經加密(即在不安全之通道上)傳送
- 因此若使用者未使用IPSEC、HTTPS、SSH、SFTP等加密方式傳送資料，攻擊者可輕易地使用網路封包擷取軟體，獲得帳號與通行碼

# 如何避免網路竊聽通行碼 (1)

- 回到網路封包竊聽這個議題上，我們並不能改變網路封包的傳送路徑，但是我們可以提升傳送的通道的安全性，傳輸機密資料時，以加密軟體進行傳輸，此時就算資料被竊聽程式所擷取，惡意的第三者也只能看到密文，而無法分析所擷取的密文資料
- 此外仍應做好電腦的安全設定，杜絕所有木馬後門程式，安裝防毒軟體是必備的；並且除了隨時更新病毒碼外，也需定時的掃描，如此可維持基本的電腦資訊安全

# 如何避免網路竊聽通行碼 (2)

透過https網頁並透過有效憑證進行安全連線以保護通行碼，避免駭客竊取通行碼

The screenshot shows a web browser interface with the address bar displaying `https://mail.google.com/mail/u/0/#inbox`. A security overlay on the left indicates a secure connection to `mail.google.com` and lists permissions for camera, microphone, pop-ups, and auto-download, all of which are currently enabled. A 'Reset permissions' button is also visible.

On the right, a 'Certificate Inspector' window for `mail.google.com` is open, showing the following details:

憑證檢視者 : mail.google.com	
一般(G)	詳細資訊(D)
<b>核發對象</b>	
一般名稱 (CN)	mail.google.com
組織 (O)	<不是憑證的一部分>
組織單位 (OU)	<不是憑證的一部分>
<b>發行者</b>	
一般名稱 (CN)	WR2
組織 (O)	Google Trust Services
組織單位 (OU)	<不是憑證的一部分>
<b>有效期間</b>	
發行日期	2025年2月26日 星期三 晚上11:34:45
到期日	2025年5月21日 星期三 晚上11:34:44
<b>SHA-256 指紋</b>	
憑證	1ecf63cdf003d0d158f3d2c4422cb8957a71db52b01ff7b77188e90409b8bad1
公開金鑰	4e6f31c84ae5290da70b457ae7e0dc7dfb5ead697db23634bbad55a45061e8f0

# 社交工程(Social Engineering)

- 社交工程是以影響力或說服力來欺騙他人以獲得資訊。它是利用人性弱點的詐騙技術，避開嚴密的安全技術防護，是一種非常 難以防範的攻擊模式
- 以下將介紹「網路釣魚」與「網路刺魚」兩種方式，來說明如何利用社交工程騙取帳號通行碼



# 社交工程 - 網路釣魚(Phishing)

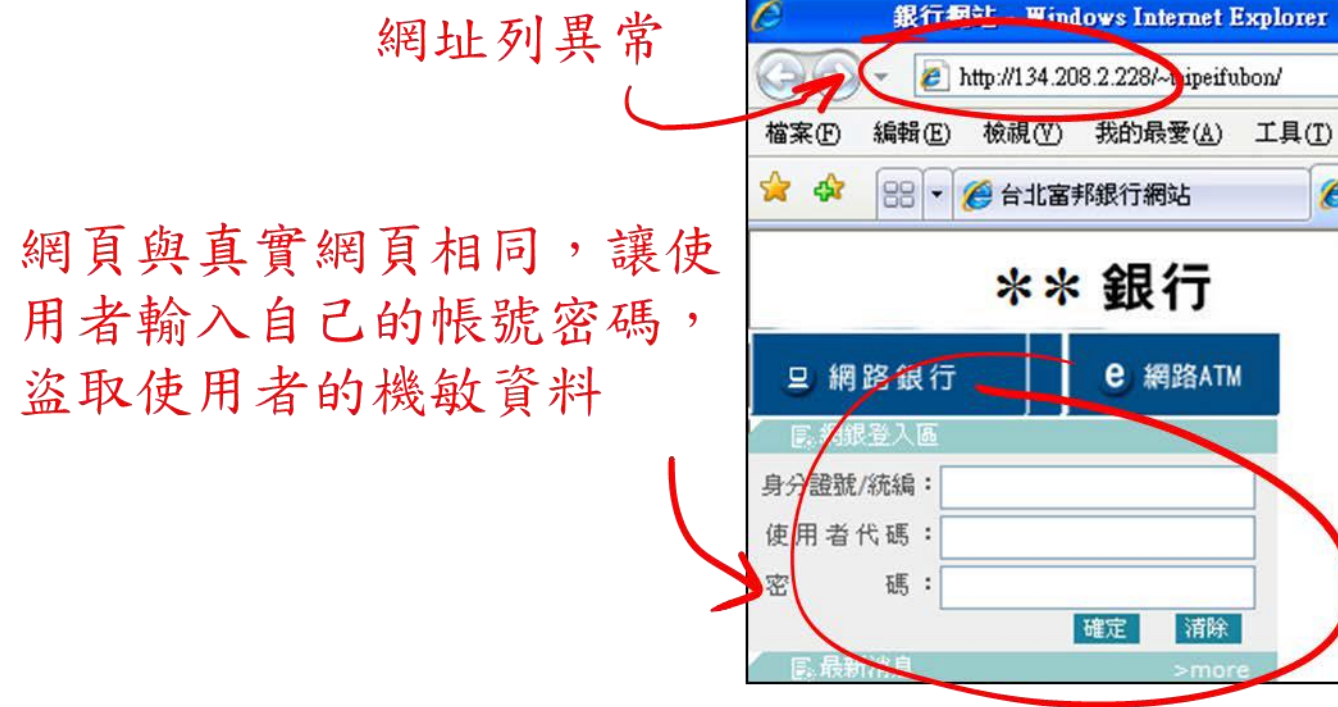
- 網路釣魚一詞最早出現於1996年，起因是因為駭客利用電話線犯案，因而結合Fishing與Phone創造Phishing一詞
- 惡意者製造一個與真實相同的網頁來假冒真實網站，讓使用者輸入自己的帳號通行碼，盜取使用者的敏感資料

# 社交工程 - 網路刺魚

- 網路釣魚經由宣導以後，許多使用者已經產生警覺，於是出現新型態手法，也就是網路刺魚(Spear-phishing)，也有人稱為「魚叉式網路釣魚」。
- 這種型態不再是漫無目的的攻擊，而是有計畫的針對某些特定的人攻擊。網路刺魚者通常攻擊公司行號、學校、公務機關等，發送與公務機關或是公司行號相似的E-mail，讓使用者上網填寫或是更新資料，一旦輸入通行碼填寫資料以後，網路刺魚者就取得使用者的機密資料。

# 網路釣魚(Phishing)盜取使用者通行碼

- 一個與真實網站相同的網頁的網站，讓使用者輸入自己的帳號通行碼，盜取使用者的通行碼。



# 網路刺魚(Spear-Phishing)盜取使用者通行碼

- 發送與政府機關或公司行號相似的E-mail，讓使用者上網更新資料，一旦輸入通行碼、填寫資料以後，網路刺魚者就取得使用者機密資料。



# 網路刺魚(Spear-Phishing)盜取使用者通行碼

請各位留意假借院長名義之冒名詐騙信 ➤

2月20日 週四 下午5:07 ☆ 😊 ↶ ⋮

🗨 翻譯成中文 (繁體) ✕

各位師長好，

近期有出現冒用多位校內一級主管的詐騙信(有回信的話，會向您借錢)，請大家切勿理會此信件

信件內容如下所示，它寄信來源的email和英文名字拼法都不是很正確(看起來像對岸的拼音方式)。

--

Hello

Are you available at the moment?

I need your quick assistance now.

Await your reply.

Regards

**Professor Jixuan Liu**

Dean, College of Informatics

Professor

College of Informatics

National Chengchi University

No. 64, Sec. 2, Zhinan Rd.,

Wenshan Dist.,

Taipei City 11605, Taiwan (R.O.C)

# 社交工程演練

受文者：國立政治大學

發文日期：中華民國114年3月6日

發文字號：臺教資通字第1142700703號

速別：普通件

密等及解密條件或保密期限：

附件：114年度社交工程演練計畫 (A09000000E\_1142700703\_senddoc2\_Attach1.pdf)

說明：

一、依資通安全事件通報及應變辦法第8條及臺灣學術網路管理規範相關規定辦理。

二、演練計畫摘要如下：

(一)演練對象：本部各單位、所屬公務機關（部屬機關（構）、公法人、國立大專校院及其資通安全責任等級屬C級以上之附屬機關）及臺灣學術網路連線單位（公立大專校院、區域網路中心、直轄市、縣（市）教育網路中心等）。

(二)演練時程自114年4月至12月止，期間辦理2次演練。

(三)演練方式：每次演練針對受測人員寄送5封社交工程演練郵件。

(四)演練目標：每次演練作業，各演練對象社交工程由件開啟率應低於10%（含），社交工程郵件點閱率應低於6%（含）。

三、請於114年3月21日前，將貴機關、學校之專案聯絡人（含姓名、公務電話、公務電子郵件）、演練人員名單（csv電子檔）及自我檢核表（含簽核紀錄），以電子郵件方式回復至本部演練作業窗口。

四、本部演練作業窗口如下：

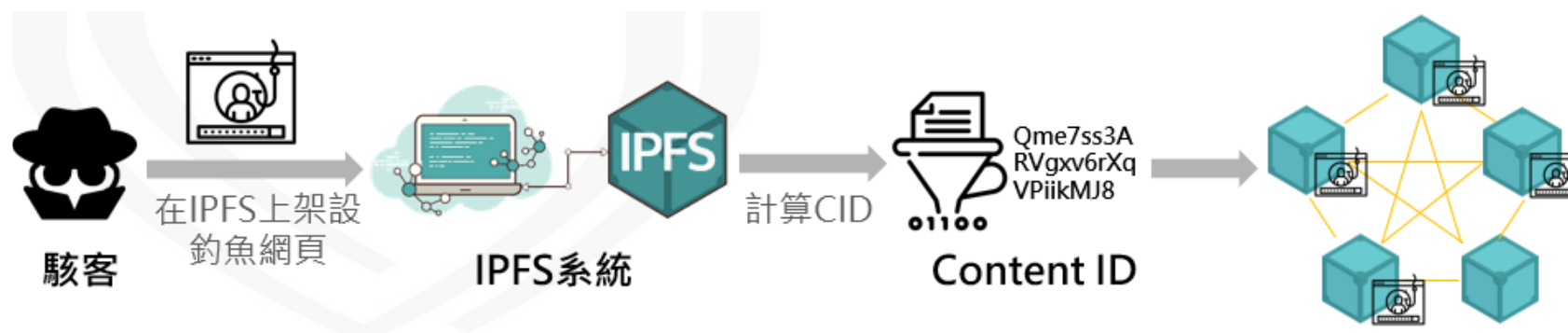
# IPFS相關惡意郵件威脅趨勢與案例分析 (1)

- 有別於傳統之主從式架構，IPFS為一點對點(Peer-to-peer, P2P)分散式檔案系統，主要用於實現檔案之分散式儲存、共享及持久化之網路傳輸協定。傳統網際網路檔案傳輸，以集中式主從架構之HTTP協定進行，因此若伺服器停擺或連線中斷，則無法傳輸檔案。運用IPFS檔案系統，則可輕易利用多個網路節點上傳送，因此內容將可以分散式存放且維持其存續性。
- IPFS自問世以來，廣泛應用於各項網路服務，如串流平台、網路文獻典藏及線上市集等，現今也被視為一項新興Web3技術，如新創公司Fleek.co，該公司去中心化開放式之Web3開發者平台已被大量廣泛使用，產品包含各式IPFS與區塊鏈服務，可窺見未來可能取代傳統雲端平台如AWS與DNS基礎設施等Web2服務。
- IPFS於網路中各檔案預設使用SHA256演算法建立其雜湊值，以辨識是否為相同檔案，傳遞內容時不僅可節約頻寬用量，且因其分散式架構可避免單點故障並防止分散式阻斷服務(DDoS)攻擊，另一IPFS服務被廣泛利用之原因為可運用星際命名系統IPNS (Inter Planetary Name System)將網路域名(DNSLink機制)對應至特定IPFS之內容定址Content ID (CID)，以方便人們以易記的網址取代CID複雜的雜湊值。對使用者而言，可透過安裝軟體成為IPFS網路節點或使用公開IPFS閘道經HTTP協定以CID取得資料。
- 多起資安事件顯示駭客利用多項IPFS服務展開惡意攻擊，如設立釣魚網站、或於合法服務中暗藏惡意程式及利用IPFS作為通訊管道，以進行惡意C2(Command and Control)命令控制。



# IPFS相關惡意郵件威脅趨勢與案例分析 (2)

- IPFS釣魚網站之所以無法於第一時間阻擋最主要的原因為其去中心化之特性，如內容雜湊定址、檔案分散儲存至多個網路空間及結合URL轉址導向，導致無法即時追蹤分析特定URL特徵，並進行攔截。
- 雖然部分IPFS閘道服務商，已開始針對此類釣魚網頁或惡意程式下載進行過濾阻擋，惟只需變更IPFS閘道，CID內容保持不變，則依然可瀏覽與存取資料，因此無法成功以域名黑名單進行連線阻擋。



IPFS釣魚網站攻擊手法



# IPFS相關惡意郵件威脅趨勢與案例分析 (3)



利用IPFS合法服務掩飾非法網址

# IPFS相關惡意郵件威脅趨勢與案例分析 (4)



利用翻譯服務轉址功能取得合法憑證之網址



潛藏惡意連結之郵件

# IPFS相關惡意郵件威脅趨勢與案例分析 (5)



利用合法網站服務取得合法憑證之網址



# 通行碼分析工具介紹

- 通行碼破解軟體
  - John the Ripper
  - Hydra

# 通行碼分析工具 - John the Ripper (1)

- John the Ripper 最早是只有發展於UNIX平台的通行碼破解工具，但是現今它可以運行的平台包含了UNIX、DOS、Windows、BeOS及OpenVMS等等
- 因為有著自動偵測通行碼雜湊函式的格式、可自行定義的破密模組與支援數種破密模組等等優點，讓John the Ripper成為最受歡迎的通行碼測試破解工具。
- John the Ripper可破解的雜湊函式格式包含DES、MD5、Blowfish、Kerberos AFS及各版本之LM-hash等，功能相當的強大

# 通行碼分析工具 - John the Ripper (2)

- 指令介紹：
  - --single : "single crack" mode
  - --wordlist=FILE -stdin : wordlist mode, read words from FILE or stdin
  - --rules : enable word mangling rules for wordlist mode
  - --incremental[=MODE] : "incremental" mode [using section MODE]
  - --external=MODE : external mode or word filter
  - --stdout[=LENGTH] : just output candidate passwords [cut at LENGTH]
  - --restore[=NAME] : restore an interrupted session [called NAME]
  - --session=NAME : give a new session the NAME
  - --status[=NAME] : print status of a session [called NAME]
  - --make-charset=FILE : make a charset, FILE will be overwritten

# 通行碼分析工具 - John the Ripper (3)

- 指令介紹：
  - --show : show cracked passwords
  - --test[=TIME] : run tests and benchmarks for TIME seconds each
  - --users=[-]LOGIN|UID[,..] : [do not] load this (these) user(s) only
  - --groups=[-]GID[,..] : load users [not] of this (these) group(s) only
  - --shells=[-]SHELL[,..] : load users with[out] this (these) shell(s) only
  - --salts=[-]COUNT : load salts with[out] at least COUNT passwords only
  - --save-memory=LEVEL : enable memory saving, at LEVEL 1..3
  - --format=NAME : force hash type NAME: des/bsdi/md5/bf/afs/lm/trip/



# 通行碼分析工具 - John the Ripper (4)

- 常用指令

- : 對wordlist不做任何動作
- C 將字首大寫，如：" crack" -> "Crack"
- c 將字首小寫其餘大寫，如："Crack" -> "cRACK"
- r 反向，如："crack" -> "kcarc"
- d 複製，如："crack" -> "crackcrack"
- f 鏡射，如："crack" -> "crackkcarc"
- { 往左shift，如："crack" -> "rackc"
- } 往右shift，如："crack" -> "kcrac"
- \$X 在字串後面串接一個字母，如：\$4: "crack" -> "crack4"
- ^X 在字串前面先置一個字母，如：^4: "crack" -> "4crack"
- <N 字串大小必須大於N
- >N 字串大小必須小於N

# 通行碼分析工具 - John the Ripper (5)

- (X 只對第一個字是X的字串做rule的動作
- )X 只對最後一個字是X的字串做rule的動作
- p 複數，如：“crack” -> “cracks”
- P 過去式，如：“crack” -> “cracked”
- l 現在式，如：“crack” -> “cracking”
- [ 將第一個字刪除，如：“crack” -> “rack”
- ] 將最後一個字刪除，如：“crack” -> “crac”  
(由於“[”和在“]” rule裡有另外的用法，為了區分使用，必須在之前加 “\” )
- R 根據鍵盤上的位置往右移一格，如：“crack96” -> “vtsvl07”
- L 根據鍵盤上的位置往左移一格，如：“crack96” -> “xeaxj85”

# 通行碼分析工具 – Hydra (1)

- THC-Hydra 是一款可平行化登錄的工具，已內建於Kali Linux
- 可以用來對需要網路登入的系統進行快速的字典攻擊，包括Samba、FTP、POP3、IMAP、Telnet、HTTP Auth、LDAP、NNTP、MySQL、VNC、Socks5、PCNFS、Cisco等，支持SSL加密。包括了對 Socks5 和 SSL 的支援。
- 範例(需要字典)：
  - `hydra -l login -P /tmp/passlist 192.168.0.1 ftp login` 為要破解的用戶名，`passlist`為通行碼字典

# 通行碼分析工具 – Hydra (2)

- 指令介紹：

- `hydra [[[-I LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e ns] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-f] [-s PORT] [-S] [-vV] [service type :server IP]`
- `-R` 繼續從上一次進度接著破解
- `-S` 採用SSL連接 ( 大寫的S )
- `-s PORT` 如果非預設port，可通過這個參數指定
- `-I LOGIN` 小寫，用於指定破解的用戶，對特定用戶破解
- `-L FILE` 大寫，用於指定用戶的用戶名字典
- `-p PASS` 小寫，用於指定通行碼破解。少用，一般是採用通行碼字典
- `-P FILE` 大寫，用於指定通行碼字典

# 通行碼分析工具 – Hydra (3)

- `-e ns` 額外的選項，`n`：空通行碼試探，`s`：使用指定帳戶和通行碼試探
- `-C FILE` 使用冒號分割格式例如 “登錄名:通行碼” 來代替`-L/-P`參數
- `-M FILE` 指定目標列表文件一行一條
- `-o FILE` 指定結果輸出文件
- `-f` 在使用`-M`參數以後找到第一對登錄名或者通行碼的時候中止破解
- `-t TASKS` 同時運行的`threads`數，預設為16
- `-w TIME` 設置最大超時的時間，單位秒，預設是30s
- `-v / -V` 顯示詳細過程
- `server` 目標IP

# 練習

- 請自行於CDX平台啟用CDX-Linux-kali-2024.1-v2-TMPL-custom
  - 帳/密：kali/kali

# htpasswd

htpasswd指令是Apache的Web server的內建工具，用於建立和更新儲存使用者名稱、網域和使用基本認證的密碼檔案

- 利用htpasswd指令加入用戶
  - 在目錄下產生一個testpw文件，使用者名稱hello，密碼：goodluck
  - `htpasswd -bc testpw hello goodluck`
- 在原有密碼檔案testpw中增加下一個用戶hihi，密碼123456
  - 去掉-c選項，即可在第一個用戶之後再增加第二個用戶，以此類推
  - `htpasswd -b testpw hihi 123456`

# 使用John the Ripper

- cat testpw

```
# cat testpw
hello:$apr1$E9w0.EqM$bBrn4TkXLdZVH5tOYtjmW0
hihi:$apr1$gSjPdmMT$mL.eprnJcem/yxLugxJTH0
```

- john --wordlist=/usr/share/wordlists/john.lst testpw

— --wordlist指定使用哪個字典檔爆破密碼，亦可不指定

```
# john --wordlist=/usr/share/wordlists/john.lst testpw

Created directory: /root/.john
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16x3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
goodluck      (hello)
123456        (hihi)
2g 0:00:00:00 DONE (2025-03-17 09:35) 100.0g/s 38400p/s 76800c/s 76800C/s 123456..bigben
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```



- 若再次爆破同一密碼檔，會出現No password hashes left to crack (see FAQ)，原因是該次爆破的結果已存在自身目錄下的~/.john/john.pot檔案內

```
(root@kali)-[/home/kali]
# john --wordlist=/usr/share/wordlists/john.lst testpw

Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16x3])
No password hashes left to crack (see FAQ)

(root@kali)-[/home/kali]
# cat ~/.john/john.pot
$apr1$E9w0.EqM$bBrn4TkXLdZVH5tOYtjmW0:goodluck
$apr1$gSjPdmMT$mL.eprnJcem/yxLugxJTH0:123456
```

- 移除~/.john/john.pot後，即可再次爆破

```
(root@kali)-[/home/kali]
# rm ~/.john/john.pot

(root@kali)-[/home/kali]
# john --wordlist=/usr/share/wordlists/john.lst testpw

Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16x3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
goodluck      (hello)
123456        (hihi)
2g 0:00:00:00 DONE (2025-03-17 09:40) 100.0g/s 38400p/s 76800c/s 76800C/s 123456..bigben
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

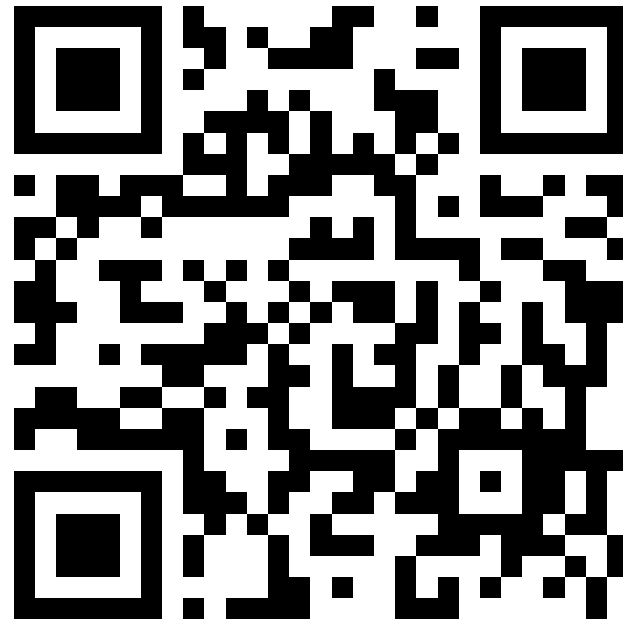
# 結論

- 慎選通行碼，方便、易記的通行碼容易遭受攻擊
- 結合生物特徵認證雖需額外認證設備，但可達到更安全的認證
- 動態通行碼可使用一次性加密智慧卡，每次登入系統通行碼均不同，藉此提高安全性



# 課後問券

- 系統通行碼 課後問券
- <https://forms.gle/reNe2tgBRYLakWjk7>



# Reference Materials

- Thanks to 「教育部資訊安全人才培育計畫」 & 「國網中心雲端資安攻防平臺（Cyber Defense eXercise，CDX）」



# Q & A