各種身分鑑別(Authentication)技術

Password authentication 通行碼身分鑑別
一次性通行碼(One-time Password)

Biometric authentication

Authentication tokens 符記

Network Authentication Protocol

單一登入(Single Sign-On, SSO)
Lightweight Directory Access Protocol (LDAP)
Windows Active Directory(AD)
Kerberos Authentication
RADIUS(Remote Authentication Dial In User Service)
Security Assertion Markup Language (SAML)安全聲明標記語言
OAuth 2.0….
Extensible Authentication Protocol (EAP)
Challenge-Handshake Authentication Protocol (CHAP)

	1	下列何種管控技術較「不」適合用來作為身分認證使用？ (A) SNMP（Simple Network Management Protocol） (B) RADIUS（Remote Authentication Dial In User Service） (C) LDAP（Lightweight Directory Access Protocol） (D)TACACS（Terminal Access Controller Access-Control System）

Password authentication 通行碼身分鑑別

- 使用「最廣泛」也「最簡便」的身分鑑別技術
- 最不安全的身分鑑別技術
  - 由於使用者端的防護疏失，也是最不安全的身分鑑別技術
  - 使用者選用「**懶人通行碼**」
    - 通行碼與帳號相同
    - 字典可以查到的英文單字
    - 用自己的電話號碼
  - 與其他**使用者 共用通行碼** == >導致可歸責性被破壞
  - 為了怕忘記，將通行碼貼在螢幕上，讓其他人可以很容易知道其通行碼
  - 使用者怕忘記通行碼，因而**從不更改通行碼**
  - 輸入通行碼時被別人看到所輸入的通行碼
  - 太長的通行碼理論上較安全，但由於大部分人無法記憶太長的通行碼，因而造成使用者將通行碼抄寫在紙張上的狀況，反而易使通行碼外洩

Password 通行碼: 攻擊與防禦

Password Attacks - 密碼攻擊

1. 字典猜測法Dictionary attack：直接用字典上的單字來猜測
2. 暴力式通行碼猜測Brute-Force attack：
   透過字元的組合變化，一一猜測通行碼
3. 通行碼監聽：在網路上直接監聽使用者輸入的通行碼封包

```
Dictionary Attack

Trying apple        : failed
Trying blueberry    : failed
Trying justinbeiber : failed
              ...
Trying letmein      : failed
Trying s3cr3t       : success!
```

```
Brute Force Attack

Trying aaaa : failed
Trying aaab : failed
Trying aaac : failed
          ...
Trying acdb : failed
Trying acdc : success!
```

Rainbow Table Attack

防禦Rainbow Table Attack
Salted Password Hashing - Doing it Right

通行碼檢測工具
Password cracker

hydra
John 暴力破解弱密碼
hashcat能用GPU來快速產生並比對雜湊值
hash-identifier
.....族繁不及備載

Hashcat offers multiple attack :

Brute-Force attack
Combinator attack
Dictionary attack
Fingerprint attack
Hybrid attack
Mask attack
Permutation attack
Rule-based attack
Table-Lookup attack
Toggle-Case attack
PRINCE attack

Hashcat

hydra

https://www.kali.org/tools/hydra/

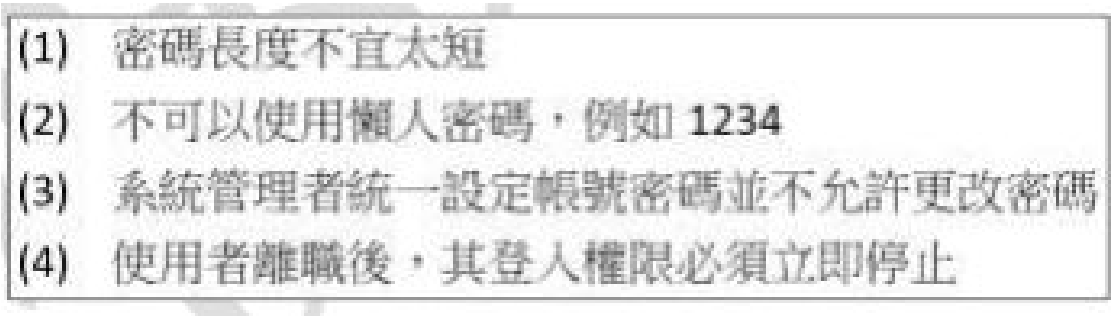
```
hydra -l user -P passlist.txt ftp://192.168.0.1
hydra -L userlist.txt -p defaultpw imap://192.168.0.1/PLAIN
hydra -C defaults.txt -6 pop3s://[2001:db8::1]:143/TLS:DIGEST-MD5
hydra -l admin -p password ftp://[192.168.0.0/24]/
hydra -L logins.txt -P pws.txt -M targets.txt ssh
```

https://ithelp.ithome.com.tw/articles/10278386

Password 通行碼: 防護措施

避免通行碼被破解的防護措施如下：

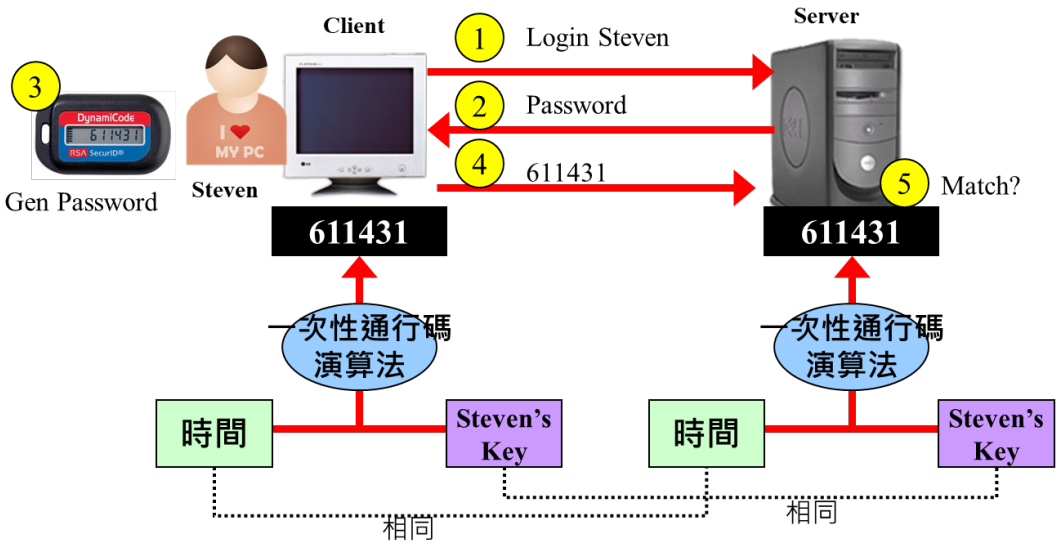
1. 系統強制要求長度**至少8碼**
2. 應包含大小寫字、數字及符號，且在字典中查不到
3. 系統強制要求使用者**定期更換通行碼**
4. 系統判斷通行碼**不重覆使用**
5. 可限制通行碼容許**簽入失敗的次數**，對於連續失敗的簽入應發出警告通知給管理者，也可以自動封鎖該帳號或延遲簽入一段時間
6. 簽入成功或失敗都應被**記錄**
7. 使用**通行碼檢測工具**尋找脆弱通行碼，若系統自動要求通行碼長度與複雜度可不必進行這項檢測
8. 通行碼**不以明碼方式儲存**，可採用**雜湊(Salted)**與加密方式來儲存
9. 通行碼不以明碼方式在網路上傳送，可採用加密方式傳送
10. 加強保護集中存放通行碼雜湊值的伺服器，一旦身分鑑別伺服器被破解，所有存取控管機制便會失效

	1	關於使用者帳號存取管理，下列敘述何者正確？ (A) 外部人員無需管理存取權限 (B) 隨時更新使用者資訊 (C) 職務無異動的人員無需定期檢視使用者帳號權限 (D) 高階主管可自訂密碼長度
	2	如附圖所示，使用帳號及通關密碼（Password）來登入 資訊系統，為了確保安全起見，必須採取何項措施？ (A) (1)、(2)、(3) (B) (1)、(2)、(4) (C) (1)、(3)、(4) (D) (2)、(3)、(4)  (1) 密碼長度不宜太短 (2) 不可以使用懶人密碼，例如 1234 (3) 系統管理者統一設定帳號密碼並不允許更改密碼 (4) 使用者離職後，其登入權限必須立即停止
	3	為防止身分認證使用的帳號及密碼遭到攻擊破解，下列敘述何者最「不」正確？ (A) 密碼應與使用者帳號有關連，以免自身忘記 (B) 至少 8 個字元以上長度，包含數字、英文字母大小寫及特殊符號 (C) 密碼應定期更換，並不可重複使用 (D) 不可與人分享密碼或是使用懶人密碼
	4	若想採用暴力攻擊的方式破解以小寫英文和數字所組成的八位密碼，至多總共要嘗試多少次？(A) $(26+10)^8$ (B) 26^8+10^8 (C) (10+26)x8 (D) $c_8^{(10+26)}$

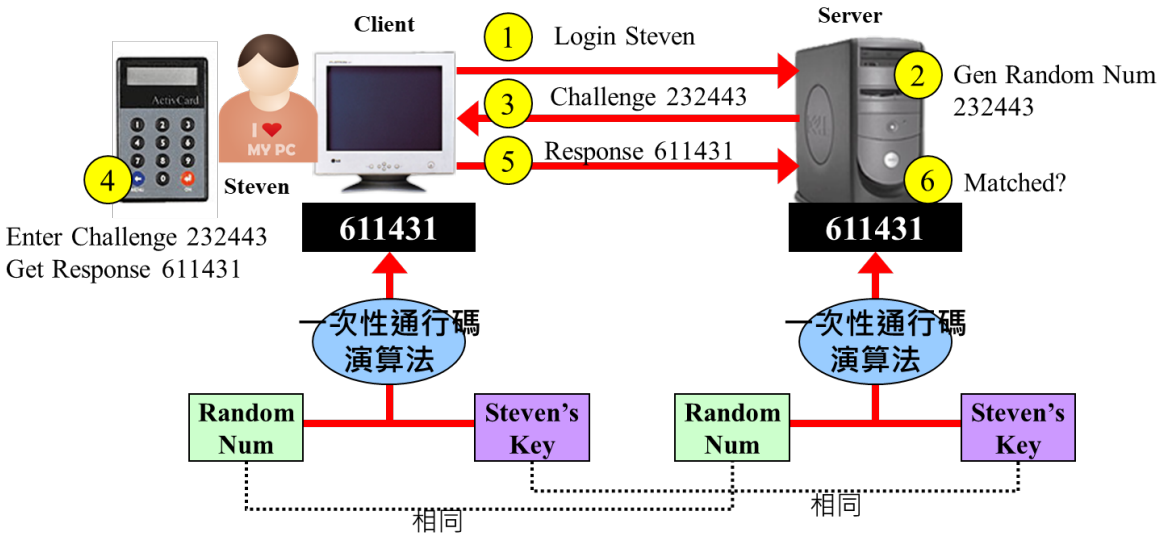
One-time Password 一次性通行碼身分鑑別

- 一次性通行碼(One-time Password)|動態通行碼
- 由隨身攜帶的符記(Token)或軟體自動產生簽入用通行碼
- 簽入時每次產生的通行碼只能使用一次
- 可防止**通行碼被竊聽**而偽冒簽入的問題
- 可防止**通行碼猜測**攻擊
- 可區分為同步式或非同步式兩類

✓ 同步式一次性通行碼技術：使用者持有的一次性通行碼產生符記與鑑別伺服器間有同步機制



✓ 非同步式一次性通行碼技術：一次性通行碼產生符記與鑑別伺服器沒有同步機制，因此需要採用**Challenge/Response的機制**傳送動態的參數



Biometric authentication 生物特徵鑑別

- 生物特徵鑑別技術採用**人類本身即具備的屬性(指紋、掌紋、視網膜、虹膜、聲紋及面容)**進行識別與鑑別
- 它是目前最昂貴、最複雜、但也最能識別人員身分的鑑別技術。
- 對這種技術的接受性較低
  - 主要原因是生物特徵鑑別技術可能需要取得人類的隱私資訊
  - 有些技術(例如：血液)需進行身體侵入動作
  - 在鑑別過程中因身體接觸而有傳染病感染的疑慮

指紋(Fingerprint)	掌紋(Hand Geometry)	面容(Facial)	虹膜(Iris)
可接受程度較高 辨識精準度高 指紋辨識設備較便宜	非侵入性，可接受程度高 辨識誤判率仍高 掌紋辨識設備較貴	可接受程度較高(非侵入與非接觸) 辨識精準度較差 目前尚無標準的特徵值作法 面容辨識設備較便宜 特殊化裝後可以輕易欺騙辨識機制 適用於長距離辨識 外部干擾因素多(眼鏡、頭髮及帽子等)	可接受程度一般(非侵入與非接觸) 辨識精準度高 虹膜辨識設備成本高 與面容辨識相較，需較近的距離

更多生物特徵鑑別技術 == >請參看 https://kknews.cc/zh-tw/science/kyqr28q.html

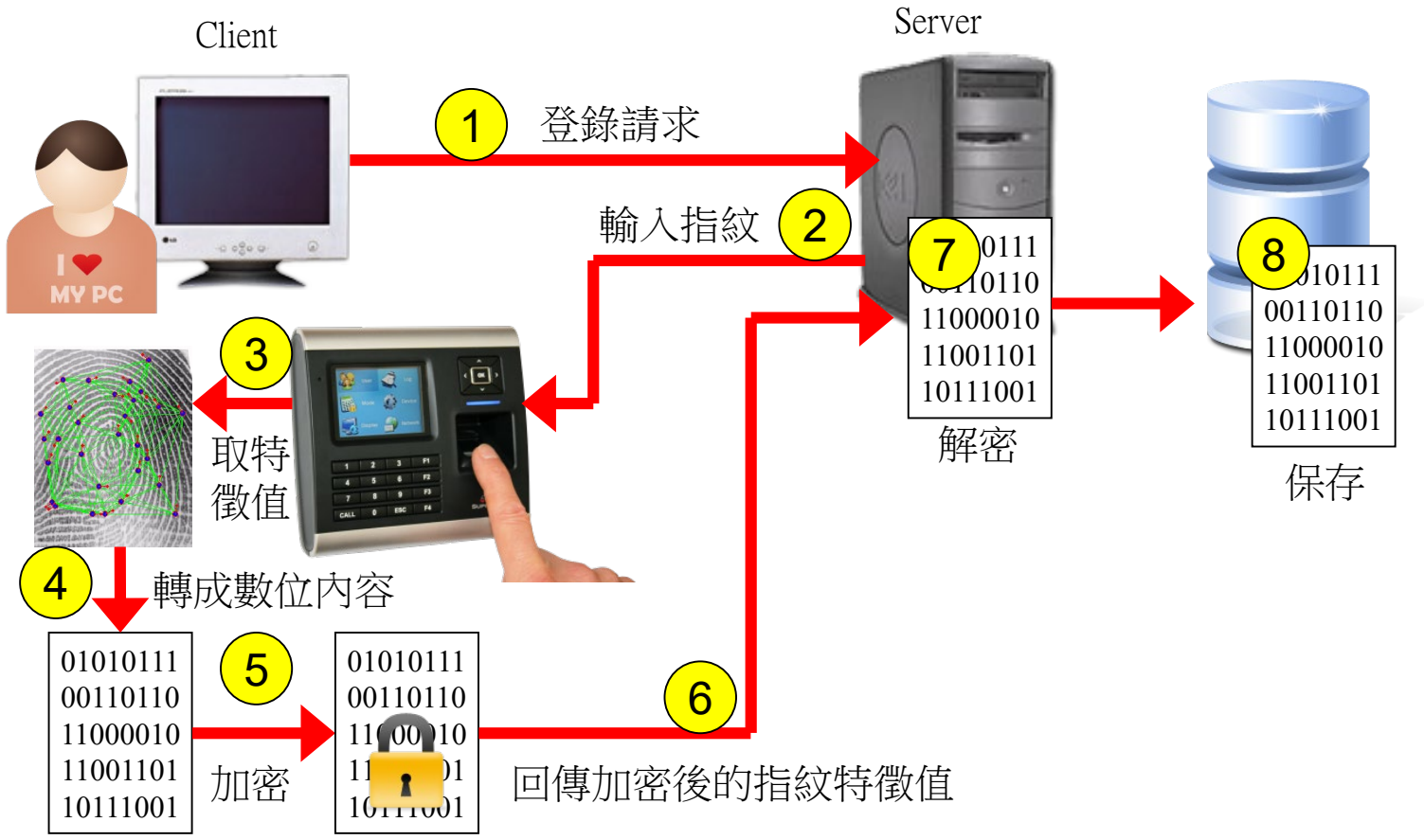
視網膜(Retina)　聲紋(Voice)　簽名(Signature)　血液(Blood)　靜脈(Vein)　DNA　手型　人耳

Biometric authentication: 登錄

在使用生物特徵鑑別技術時，每一個使用者必須先完成生物特徵的登錄步驟，將其生物特徵值存放在伺服器端，以供未來的比對與驗證

生物特徵登錄步驟如下
(以指紋為例)

1. 登錄請求：使用者透過網路向伺服器送出生物特徵登錄的請求
2. 輸入指紋：伺服器要求使用者在指紋辨識設備上按壓指紋
3. 取特徵值：指紋辨識設備取得指紋影像後，並不是將指紋的影像直接存檔，而是採取指紋的特徵
4. 轉成數位內容：將指紋特徵轉換成數位內容(指紋特徵值)，以利後續使用
5. 加密：將指紋特徵值在傳送前進行加密動作
6. 回傳加密後的指紋特徵值：透過網路將加密後的指紋特徵值傳回伺服器
7. 解密：將加密後的指紋特徵值進行解密
8. 保存：將指紋特徵值保存在資料庫，以利後續鑑別比對使用

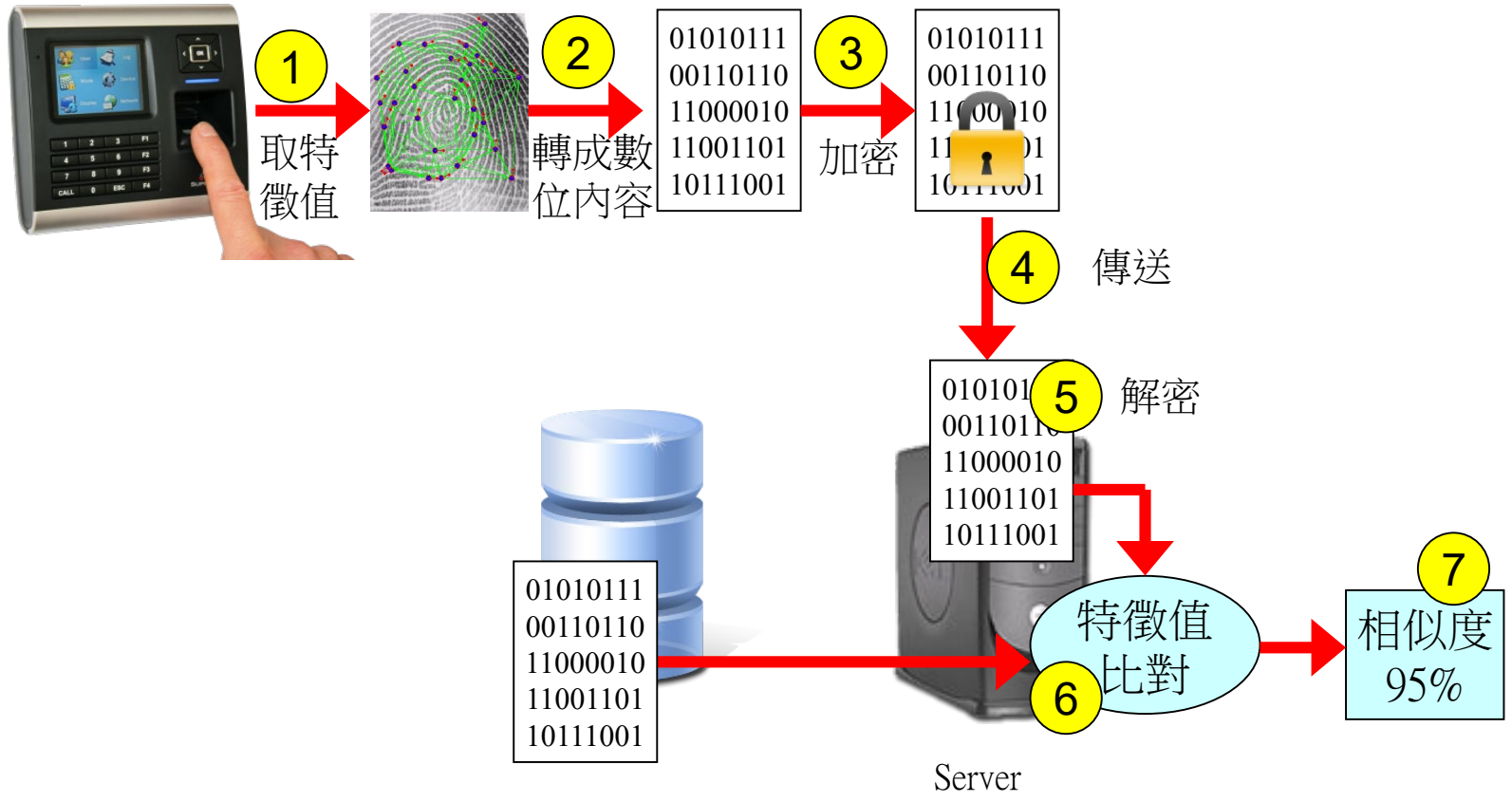


Biometric authentication：鑑別

使用者完成生物特徵登錄後即可使用其指紋進行身分的鑑別

生物特徵**鑑別**步驟如下(以指紋為例)

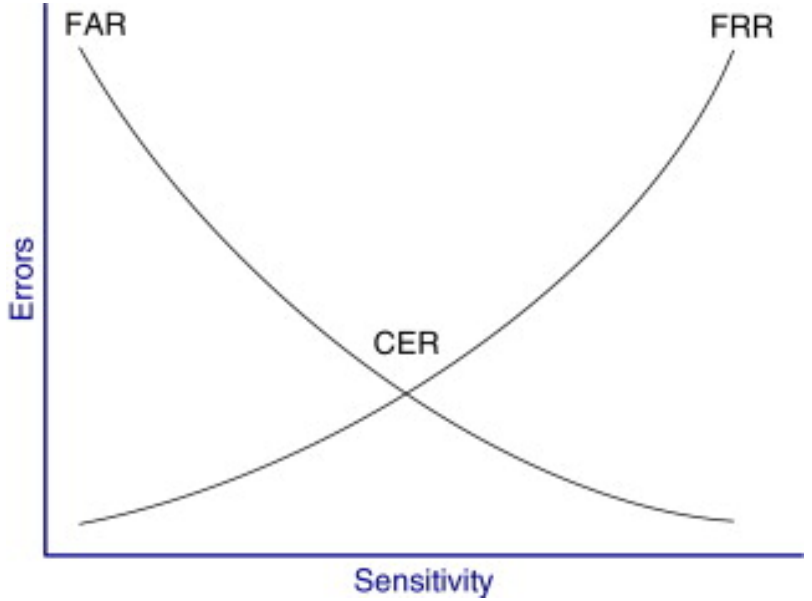
1. 取得特徵值：使用者在指紋辨識設備上按壓後，取得指紋影像並轉換成指紋的特徵
2. 轉成數位內容：將指紋特徵轉成數位內容，稱為指紋特徵值
3. 加密：將使用者的指紋特徵值加密
4. 傳送：透過網路將加密後的指紋特徵值傳回伺服器
5. 解密：伺服器將加密後的指紋特徵值解密
6. 特徵值比對：將解密後的指紋特徵值與資料庫中原登錄的特徵值進行比對
7. 判斷相似度：特徵值的比對並非是1對1的完全比對，而是比對其相似程度，若其相似程度愈高則愈能代表為原來的使用者



Biometric security: FRR | FAR | CER

- 生物特徵鑑別技術的錯誤問題與**設備的敏感度**相關
  - 設定太嚴謹，那麼真實使用者進行辨識時，容易出現錯誤判斷。(False **Reject** Rate, FRR)
  - 設定太寬鬆，那麼偽冒的使用者進行辨識時，容易被誤判是合法使用者(False Acceptance Rate, FAR)

- 可區分為兩個類型的錯誤:
  - ✓ Type I錯誤：**拒絕**合法授權的使用者(False **Reject** Rate, FRR)
    - ◆ 敏感度愈高，發生FRR的比率就愈高
  - ✓ Type II錯誤：**允許**不合法的使用者(False **Acceptance** Rate, FAR)
    - ◆ 敏感度愈高，發生FAR的比率就愈低



- CER(Cross Error Rate)交叉錯誤率
  - ✓ Type I = Type II錯誤時的值
  - ✓ CER值愈低的產品代表其精準度愈高
  - ✓ 當選購生物特徵辨識產品時可比較CER值

	1	以現行科技發展而言，下列何種生物特性較「不」適合 拿來作為身份鑑別使用？ (A) 指紋 (B) 虹膜 (C) 臉部特徵 (D) 身高
	2	如果運用生物特徵來做身分認證，生物特徵可區分為靜態特徵及動態特徵，請問下列哪些屬於「靜態特徵」？(1)指紋、(2)聲音模式、(3) 視網膜 (A) (1)(2) (B) (1)(3) (C) (2)(3) (D) (1)(2)(3)
	3	若運用「生物特徵」來做身分認證時，儀器的最佳靈敏度必須調整在誤殺(False Reject)與誤放(False Accept)兩條曲線的交叉點，此交叉點被稱為下列何種錯誤率？ (A) 位元錯誤率（Bit Error Rate） (B) 封包錯誤率（Packet Error Rate） (C) 測試錯誤率（Test Error Rate） (D) 交點錯誤率（Crossover Error Rate）
	4	在挑選以生物辨識（Biometrics）為主的驗證設備時，下列何種評估要素「不」是常用來比較設備間的優劣性？ (A) 錯誤接受率（False Acceptance Rate, FAR） (B) 正確拒絕率（True Rejection Rate, TRR） (C) 錯誤拒絕率（False Rejection Rate, FRR） (D) 交叉錯誤率（Crossover Error Rate, CER）
	5	若公司的門禁出入管制已使用生理特徵認證（Biometric Authentication） 設備進行身分驗證，為更加嚴格管制，建議應如何調整生理特徵設備？ (A) 選擇交叉錯誤率（Crossover Error Rate, CER） (B) 提高錯誤拒絕率（False Rejection Rate, FRR） (C) 提高錯誤接受率（False Acceptance Rate, FAR） (D) 選擇相等錯誤率（Equal Error Rate, EER）
	6	關於生物特徵認證中之 CER、FRR 與 FAR 三種評比指標，下列敘述 何者「不」正確？ (A) CER：交叉錯誤率，集合 FRR 及 FAR 兩個曲線的交叉點 (B) FRR：錯誤拒絕率，把對的驗證為錯誤的屬於 Type I error (C) FAR：錯誤接受率，把錯誤的驗證為對的屬於 Type II error (D) 生物特徵認證，最好的是 CER 及 FAR 愈高的愈好

Authentication tokens 符記

Hardware tokens

- 符記(Token)是一種適合隨身攜帶的卡片或感應器
- 用來實作「基於所有(Something You Have)」的身分鑑別技術
- 通常可分為「記憶卡(memory card)」與「智慧卡(Smart Card) 」兩種類型
  - ✓ 記憶卡中只有記憶儲存功能，例如：磁條卡
  - ✓ 智慧卡則具有**運算能力**與**記憶能力**，例如：自然人憑證與晶片金融卡等
    - 本身具備**微處理器**與**積體電路(IC)**
    - 有記憶空間也可進行運算
    - 為了防止智慧晶片中的私密金鑰被破解讀出，須具備**防拆解與竄改的保護機制**，只要晶片一被拆開其資料自動銷毀
    - 要啟動智慧卡功能必須輸入PIN或通行碼
- 依其感應或資料傳輸的方式又可分為「接觸式」與「非接觸式」
  - 磁條卡需要與刷卡機接觸
  - 悠遊卡不需接觸，只需要近距離感應即可
- 符記的外型設計基本上都需要能隨身攜帶

記憶卡(memory card)

晶片金融卡

	1.	關於智慧卡(Smart Card)，下列敘述何者較「不」正確？ (A) 智慧卡可攜帶方便 (B) 智慧卡不會遭到實體攻擊 (C) 智慧卡可以儲存人腦無法記憶的密碼長度 (D) 大部分智慧卡都設計三次 PIN 輸入錯誤就會卡片鎖死