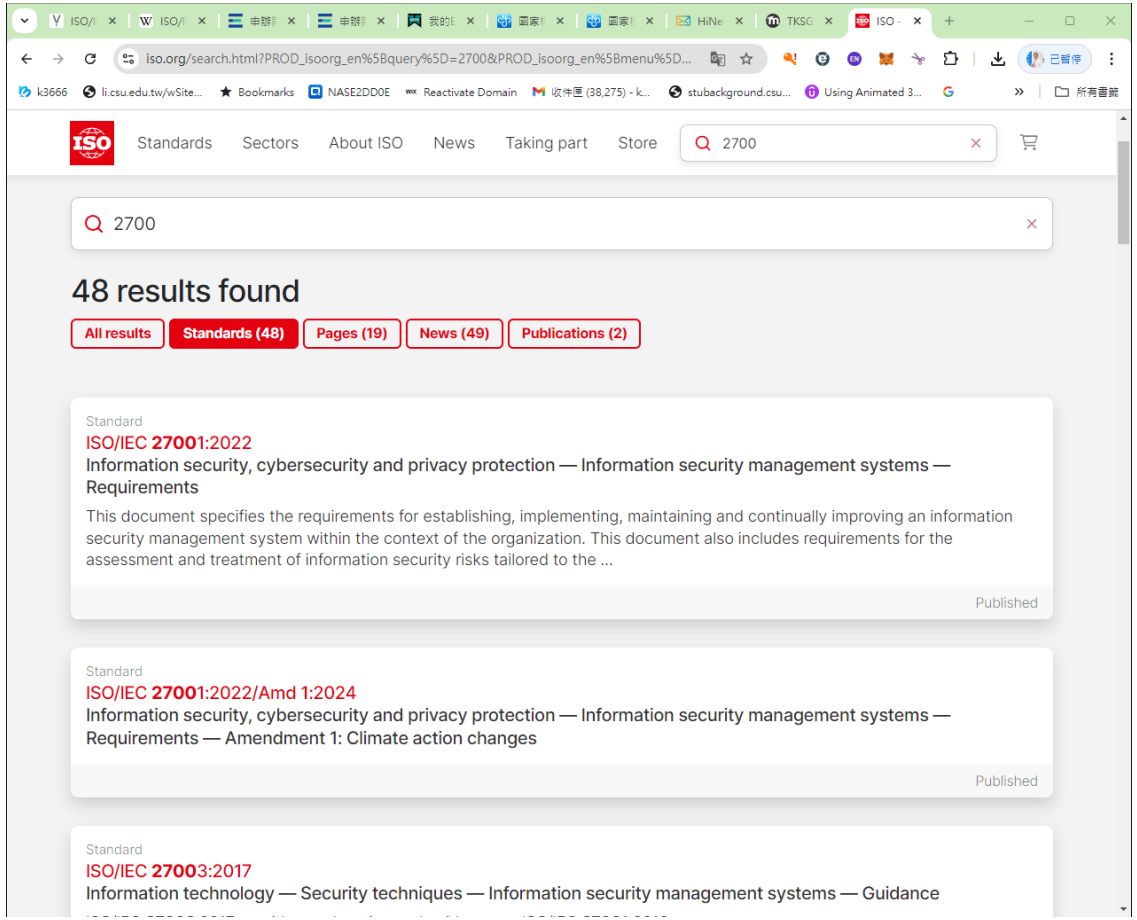
資訊安全管理補充

馬維銘博士

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

270001 site：iso.org > 2700

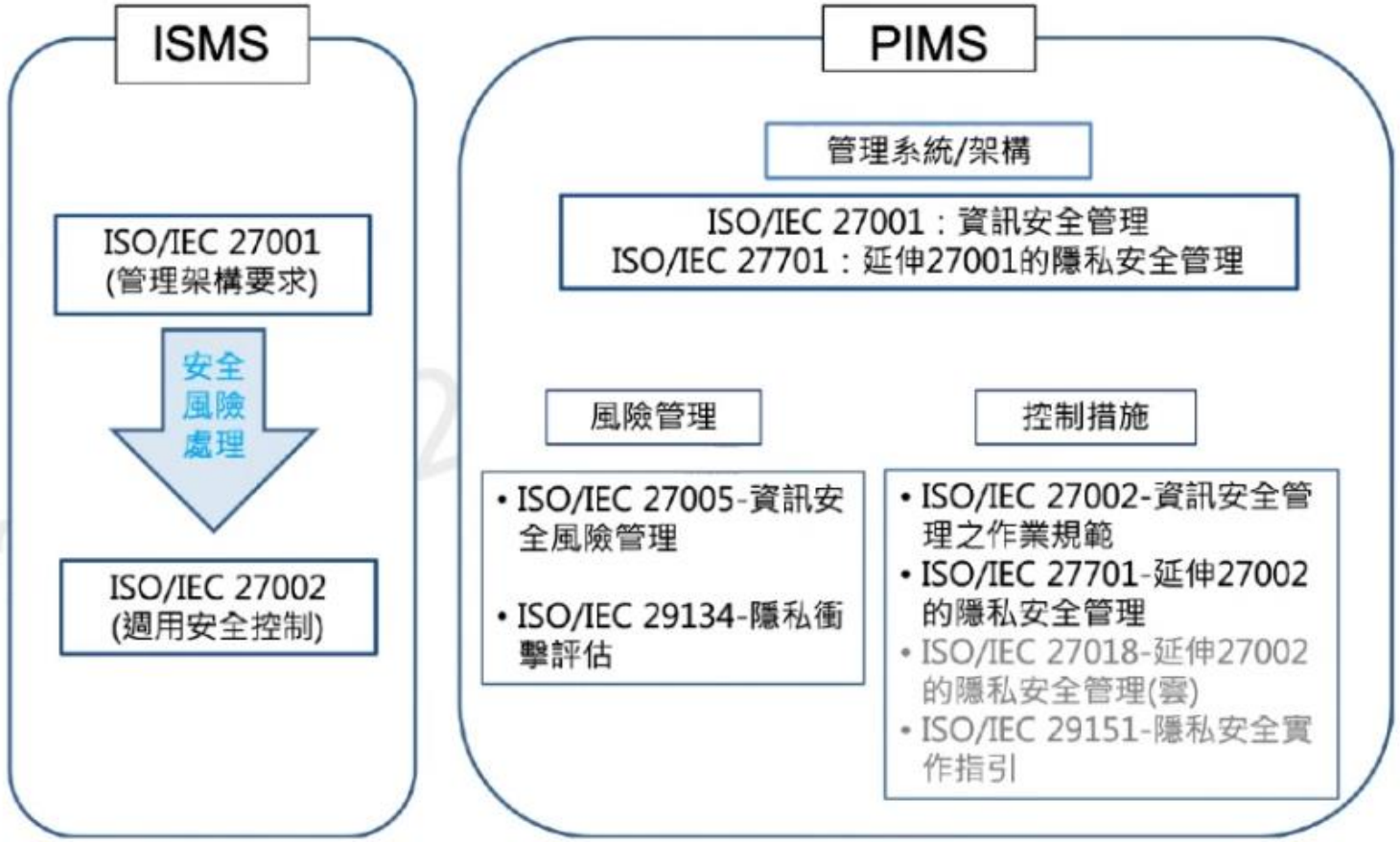


國家標準(CNS)網路服務系統

https://www.cnsonline.com.tw/

CNS 27002　X6040 >預覽

建構以ISMS為基礎框架的PIMS



異地備份/備援機制提及之主機房與異地備援機房之距離？

- 有關不同地點備份，宜朝「不遭受同一風險或事件影響」的方向考量，目前並未設置距離要求
- 有關距離建議，機關亦可參考「我國電腦機房異地備援機制參考指引」中，異地備份/備援機制提及之主機房與異地備援機房之距離應**距離30公里以上**，做為參考依據
- 以期在發生地震等區域性毀損時，仍能夠保存完整之備份資料及縮短回復時間。

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

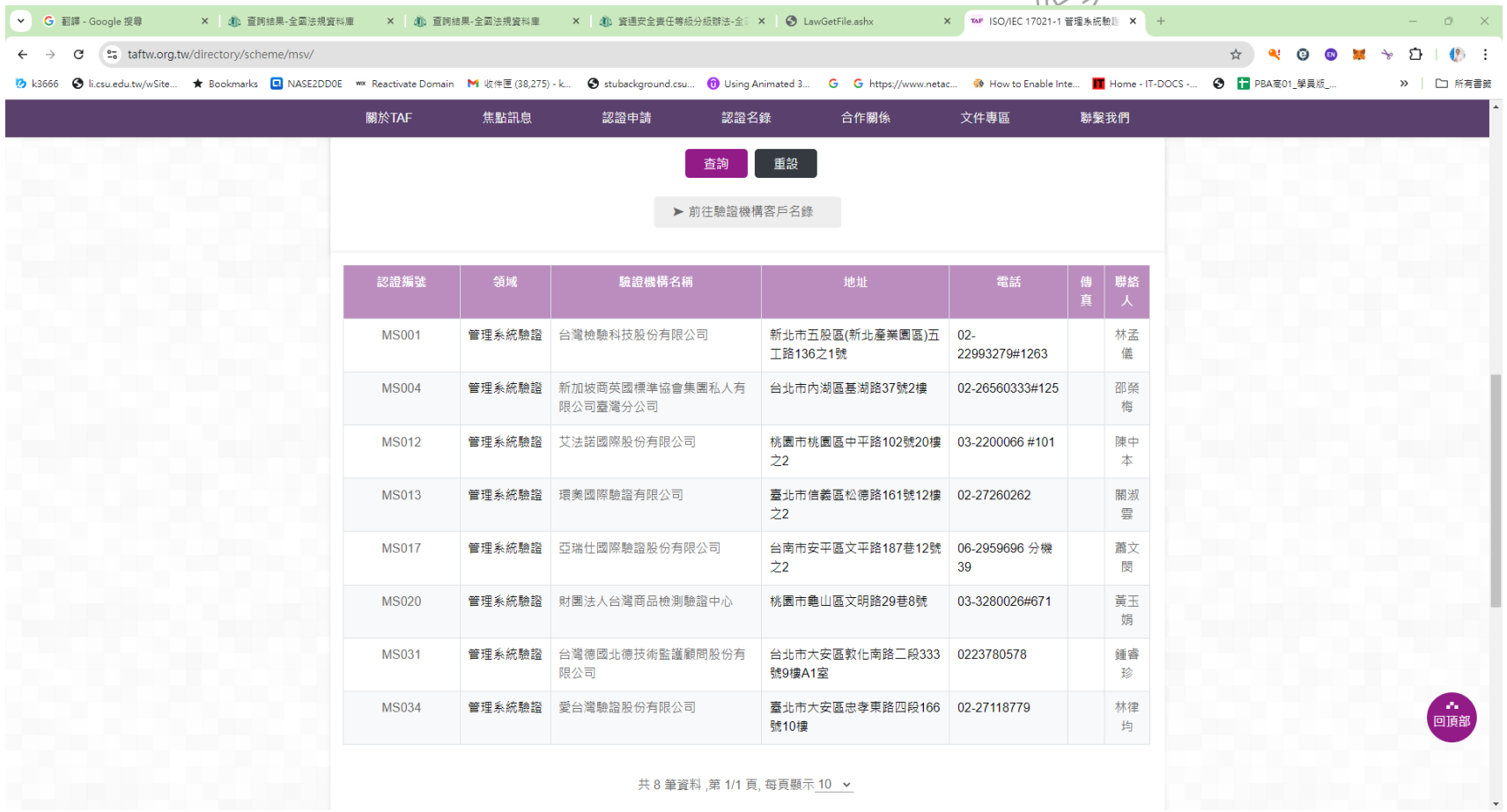
公正第三方

- 有關公正第三方係指通過我國標準法主管機關（經濟部）委託機構（財團法人全國認證基金會，TAF）認證之機構，可至TAF官網之「認證名錄」查詢「管理系統驗證機構」（https://www.taftw.org.tw/directory/scheme/msv）。

- 三、考量第三方驗證作業之公正性及獨立性，機關如委外辦理ISMS輔導及驗證時，輔導案及驗證案之服務契約，應分別招標。

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

財團法人全國認證基金會網站



認證編號	領域	驗證機構名稱	地址	電話	傳真	聯絡人
MS001	管理系統驗證	台灣檢驗科技股份有限公司	新北市五股區(新北產業園區)五工路136之1號	02-22993279#1263		林孟儀
MS004	管理系統驗證	新加坡商英國標準協會集團私人有限公司臺灣分公司	台北市內湖區基湖路37號2樓	02-26560333#125		邵綮梅
MS012	管理系統驗證	艾法諾國際股份有限公司	桃園市桃園區中平路102號20樓之2	03-2200066 #101		陳中本
MS013	管理系統驗證	環奧國際驗證有限公司	臺北市信義區松德路161號12樓之2	02-27260262		關淑雲
MS017	管理系統驗證	亞瑞仕國際驗證股份有限公司	台南市安平區文平路187巷12號之2	06-2959696 分機39		蕭文閔
MS020	管理系統驗證	財團法人台灣商品檢測驗證中心	桃園市龜山區文明路29巷8號	03-3280026#671		黃玉婿
MS031	管理系統驗證	台灣德國北德技術監護顧問股份有限公司	台北市大安區敦化南路二段333號9樓A1室	0223780578		鍾睿珍
MS034	管理系統驗證	愛台灣驗證股份有限公司	臺北市大安區忠孝東路四段166號10樓	02-27118779		林律均

https://www.taftw.org.tw/directory/scheme/msv/

資通安全責任各等級應辦事項(管理面)

責任等級		資通系統分級及防護基準	資訊安全管理系統導入及通過公正第三方驗證	資通安全專責人員	內部資通安全稽核	業務持續運作演練(全部核心資通系統)	資安治理成熟度評估
A	公務機關	1年內完成	• 2年內完成導入 • 3年內完成驗證	1年內完成 配置4人	2次/年	1次/年	1次/年
	特定非公務機關	1年內完成	• 2年內完成導入 • 3年內完成驗證	1年內完成 配置4人	2次/年	1次/年	無
B	公務機關	1年內完成	• 2年內完成導入 • 3年內完成驗證	1年內完成 配置2人	1次/年	1次/2年	1次/年
	特定非公務機關	1年內完成	• 2年內完成導入 • 3年內完成驗證	1年內完成 配置2人	1次/年	1次/2年	無
C	公務機關	• 1年內資通分級 • 2年內控制措施	• 2年內完成導入	1年內完成 配置1人	1次/年	1次/2年	無
	特定非公務機關	• 1年內資通分級 • 2年內控制措施	• 2年內完成導入	1年內完成 配置1人	1次/年	1次/2年	無

資通安全責任各等級應辦事項(技術面)

責任等級	安全性檢測		資通安全健診	資通安全威脅偵測管理機制	政府組態基準	資通安全弱點通報機制	端點偵測及應變機制	資通安全防護	備註
	弱點掃描	滲透測試							
A 公務機關	2次/年	1次/年	1次/年	1年內完成	1年內完成	1年內完成	2年內完成	1年內完成	• 防毒軟體 • 網路防火牆 • 具有郵件伺服器者，應備電子郵 件過濾機制 • 入侵偵測及防禦機制 • 具有對外服務之核心資通系統者，應備應用程式防火牆 • 進階持續性威脅攻擊防禦措施
A 特定非公務機關	2次/年	1次/年	1次/年	1年內完成	無	1年內完成	無	1年內完成	
B 公務機關	1次/年	1次/2年	1次/2年	1年內完成	1年內完成	1年內完成	2年內完成	1年內完成	同上，除進階持續性威脅攻擊防禦措施外
B 特定非公務機關	1次/年	1次/2年	1次/2年	1年內完成	無	1年內完成	無	1年內完成	
C 公務機關	1次/年	1次/2年	1次/2年	無	無	2年內完成	無	1年內完成	同A級公務機關，除： • 入侵偵測及防禦機制 • 具有對外服務之 核 心資 通 系 統 者，應備應用程式防火牆 • 進階持續性威脅 攻擊防禦措施
C 特定非公務機關	1次/年	1次/2年	1次/2年	無	無	2年內完成	無	1年內完成	
D	無	無	無	無	無	無	無	1年內完成	僅 • 防毒軟體 • 網路防火牆

資通安全責任各等級應辦事項(認知與教育訓練面)

責任等級		資通安全教育訓練			資通安全專業證照及職能訓練證書
		資通安全專職人員 (每人每年至少接受)	資通安全專職人員以外之資訊人員 (每人)	一般使用者及主管 (每人每年接受)	
A	公務機關	12小時以上	• 每2年3小時以上專業或全職能訓練 • 每年2小時以通識教育訓練	3小時以上	一年內，至少4名資通安全專職人員，各持有證照及證書各1張以上
	特定非公務機關	12小時以上	• 每2年3小時以上專業或全職能訓練 • 每年2小時以通識教育訓練	3小時以上	一年內，至少4名資通安全專職人員，各持有證照及證書各1張以上
B	公務機關	12小時以上	• 每2年3小時以上專業或全職能訓練 • 每年2小時以通識教育訓練	3小時以上	一年內，至少2名資通安全專職人員，各持有證照及證書各1張以上
	特定非公務機關	12小時以上	• 每2年3小時以上專業或全職能訓練 • 每年2小時以通識教育訓練	3小時以上	一年內，至少2名資通安全專職人員，各持有證照及證書各1張以上
C	公務機關	12小時以上	• 每2年3小時以上專業或全職能訓練 • 每年2小時以通識教育訓練	3小時以上	一年內，至少1名資通安全專職人員，各持有證照及證書各1張以上
	特定非公務機關	12小時以上	• 每2年3小時以上專業或全職能訓練 • 每年2小時以通識教育訓練	3小時以上	一年內，至少1名資通安全專職人員，各持有證照及證書各1張以上
D		無	無	3小時以上	無
E		無	無	3小時以上	無

資料庫安全
(Database Security)

正修科技大學資管系
馬維銘教授

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

資料庫管理系統
(Database Management Systems, DBMS)

- 主要功能就是要管理、維護、及操作資料庫內資料 (Major functions are managing maintaining, and manipulating data in the database)
- 一筆資料交易完成之後，就必須要將資料寫入到資料庫裡面 (Each data transaction is recorded into the Database)
- 具容錯的機制 (Provide fault-tolerance)
- 可以容許很多人一起使用資料庫的資源 (Allow concurrent access on database resources)

資料庫與檔案差異

- 資料庫是由資料庫管理系統(DBMS)管理，而檔案是由作業系統(OS)所管理。
- 資料庫安全比作業系統安全更為明細。
- 資料庫比檔案更經常被存取及更新。
- 資料庫之存取經常須同時關聯到數個資料表，而檔案之存取則一時間僅處理單一檔案。

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

資料庫與檔案差異比較

	資料庫	檔案
管理	資料庫管理系統(DBMS)	作業系統(OS)
安全處理物件	更為彈性與細微	僅處理檔案
存取與更新頻率	經常	較少
存取的關連性	關聯到數個資料表	某一時間僅能處理單一個檔案

資料庫管理系統的類型(1/3)

1. 階層式資料庫管理系統 (Hierarchical database management system)
2. 網路式資料庫管理系統 (Network database management system)
3. 關聯式資料庫管理系統 (Relational database management system)
4. 物件導向資料庫管理系統 (Object-oriented database management system)

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

資料庫管理系統的類型(2/3)

1. 階層式資料庫管理系統
   - 以樹狀結構連結，每一筆記錄僅屬於一位擁有者，較不符實際
2. 網路式資料庫管理系統
   - 較階層式資料庫管理系統有彈性，具有晶格的結構 (lattice) ，每一筆記錄可有多重父記錄或子記錄

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

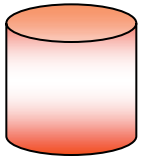
資料庫管理系統的類型(3/3)

3. 關聯式資料庫管理系統
   - 由資料表組成，藉由主鍵建立關聯，使用結構化查詢語言(SQL Structure Query Language)
4. 物件導向資料庫管理系統
   - 採用較新的技術，以克服關聯式資料庫的限制，但不使用SQL

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

資料庫內資料之階層關係

資料庫
Data base



資料表
Table

Id	name	address	tel
96001	周志明	台北市內湖區祥和路500號	02-7654321
96002	李春嬌	台中市北屯區大愛一路8號	04-1234567
96003	汪健鳴	高雄市三民區平等路111號	073416666

資料錄
Record

96001	周志明	台北市內湖區祥和路500號	02-7654321

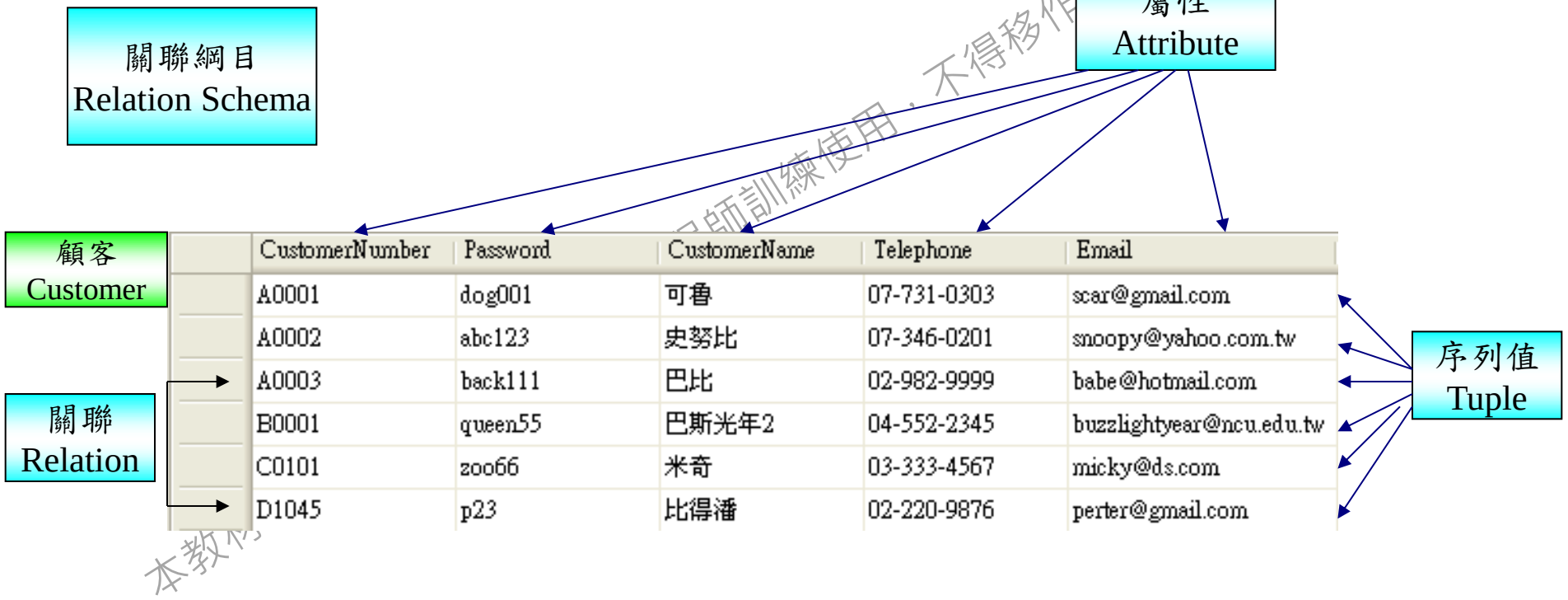
字母
Character

欄位
Fields

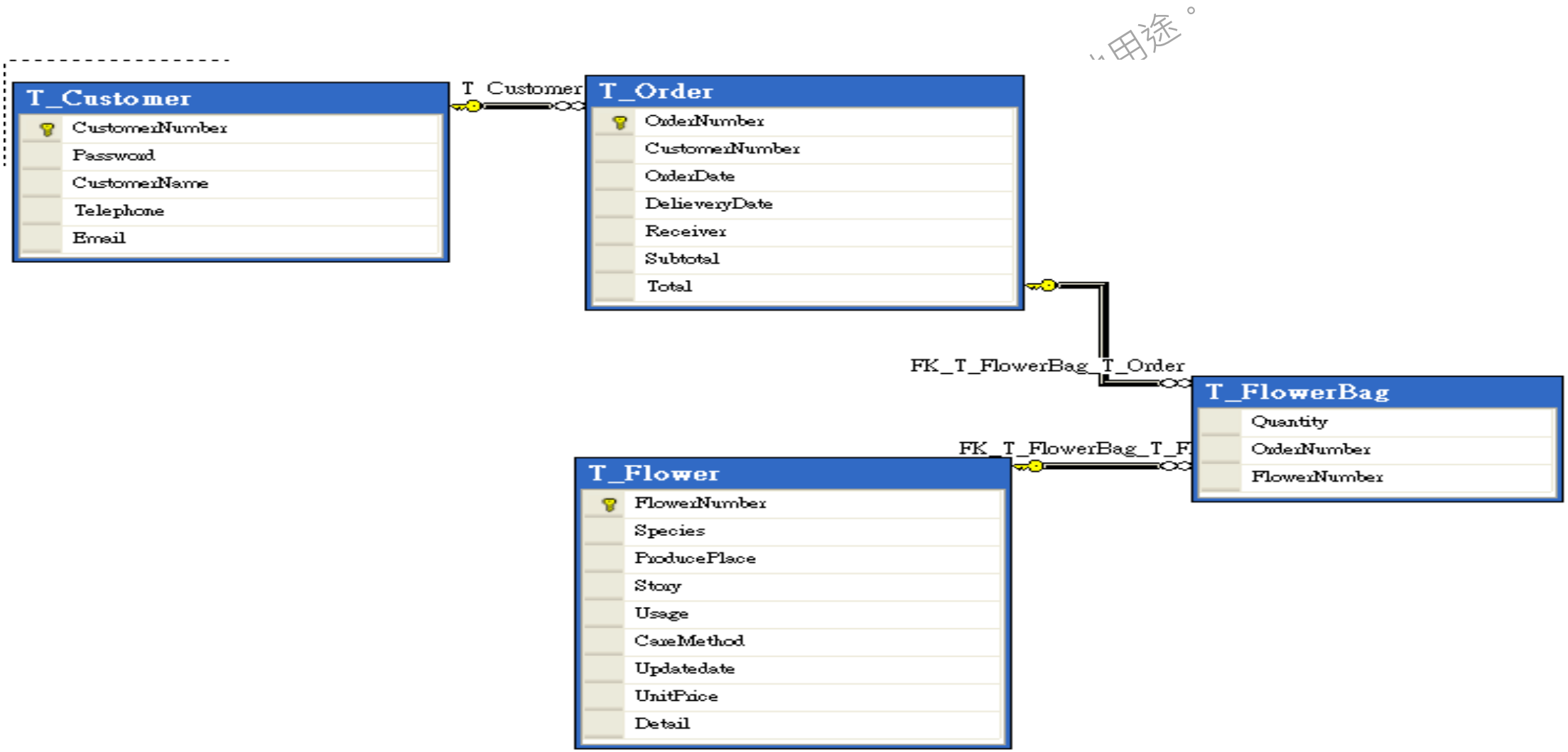
關聯模式的定義(1/2)

- 關聯模式裡的最基本的組成元素稱為關聯
- 一個關聯就好像一個資料表
  - 表中的每一列記載一串資料值，稱為一筆序列值
  - 表中的每一行則用來記載一個屬性的屬性值
  - 一筆序列值是描述真實世界裡的一個實體或一個關係的各個屬性值
- 一個關聯必須有一個相對應的定義，稱為關聯綱目（Relation schema），一個關聯綱目包括了關聯名稱和關聯的屬性

關聯模式的定義(2/2)

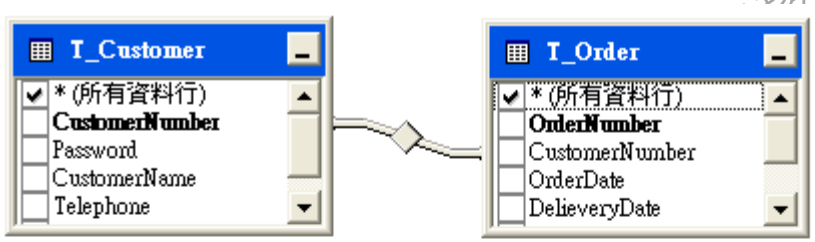


資料表之間的關聯性(1/2)



資料表之間的關聯性(2/2)

圖表



SQL

```
SELECT      *, T_Customer.*, T_Order.*
FROM        T_Customer INNER JOIN
              T_Order ON T_Customer.CustomerNumber = T_Order.CustomerNumber
```

view

CustomerNumber	Password	CustomerName	Telephone	Email
A0001	dog001	可魯	07-731-0303	scar@gmail.com
A0002	abc123	史努比	07-346-0201	snoopy@yahoo.c...
A0003	back111	巴比	02-982-9999	babe@hotmail.com
B0001	queen55	巴斯光年2	04-552-2345	buzzlightyear@nc...
C0101	zoo66	米奇	03-333-4567	micky@ds.com
D1045	p23	比得潘	02-220-9876	perter@gmail.com

常用的資料庫管理系統埠號

Data Base	Port
Oracle Net Listener	1579
Microsoft SQL	1433
MySQL	3306

好的資料庫應該具備下列特性

- 資料分享
- 最小資料重複
- 資料一致性
- 資料完整性
- 資料安全性

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

針對SQL Injection弱點攻擊

- 具有瑕疵的程式設計 (Poor coding practicing)
- 系統未修補更新 (Un-patched systems)
- sa管理者使用空白密碼 (Blank sa password)

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

MS SQL伺服器的弱密碼影響

- MS SQL伺機器的弱密碼不僅導致SQL伺機器的入侵，同時也會導致整個伺服器系統的入侵。

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

SQL Injection資訊隱碼攻擊

將SQL的查詢/行為命令透過「嵌入」模式放入合法的HTTP提交請求中從而達到攻擊的目的：

1.測試主機是否存在SQL Injection漏洞

- ‘ or 1=1—

2.尋找登錄頁面，在ID與密碼輸入文字框或URL輸入

- Login: ‘ or 1=1—
- Password: ‘ or 1=1—
- http://www.***.com/index.asp?id=*** ‘ or 1=1--

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

在客戶端網頁顯示存在SQL弱點訊息的範例

Microsoft OLE DB Provider for SQL Server error ‘80040e14’

Unclosed quotation mark before the character string ‘ and Password= ‘’ .

/login.asp line 42

資訊隱碼攻擊

正常身份認證連線

```
SELECT *
FROM customer
WHERE UID = '& request("ID") &' AND
        Passwd = '& request("Pwd") &';
```

UID = 'E123456789'
Passwd = 'abc123'

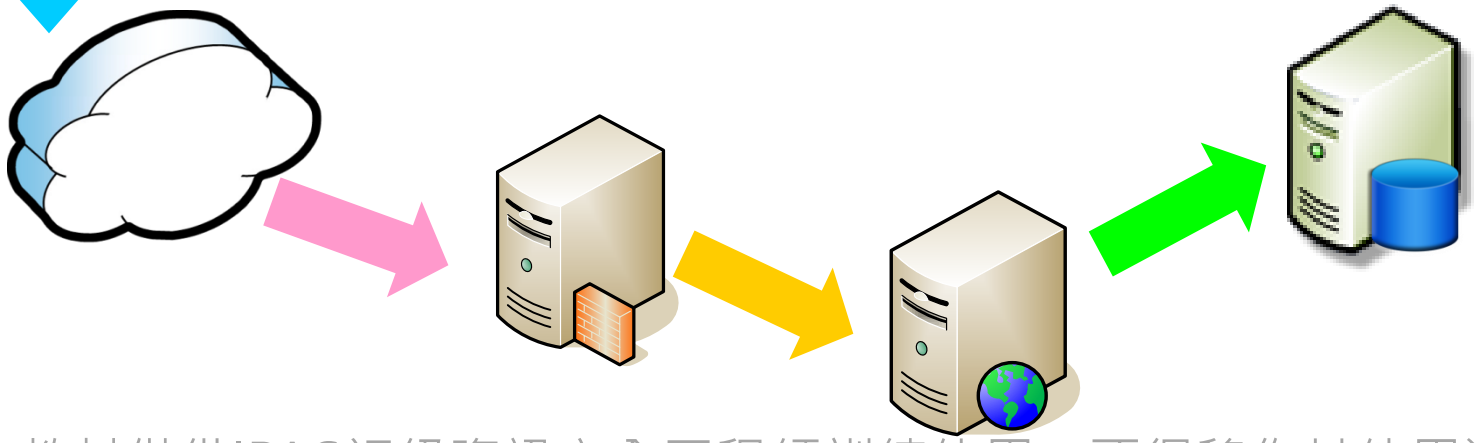
```
SELECT *
FROM customer
WHERE UID = 'E123456789' AND Passwd = 'abc123';
```

正常連線狀態

	CustomerNumber	Password	CustomerName	Telephone	Email
	A0001	dog001	可魯	07-731-0303	scar@gmail.com
	A0002	abc123	史努比	07-346-0201	snoopy@yahoo.com.tw
	A0003	back111	巴比	02-982-9999	babe@hotmail.com
	B0001	queen55	巴斯光年2	04-552-2345	buzzlightyear@ncu.edu.tw
	C0101	zoo66	米奇	03-333-4567	micky@ds.com
	D1045	p23	比得潘	02-220-9876	perter@gmail.com

Customer Number = A002
Password = abc123

Select * from customer where
CustomerNumber = ‘A002’
Passwd = ‘abc123’



SQL Injection攻擊

```
SELECT *
FROM customer
WHERE UID = '& request("ID") &' AND
        Passwd = '& request("Pwd") &';
```

```
UID = 'Admin' -- '
Passwd = ' '
```

```
SELECT *
FROM customer
WHERE UID = 'Admin' --' AND Passwd = ' ';
```

資訊隱碼攻擊工具
(SQL Injection Hacking Tools)

- SQLDict - 使用字典攻擊法
- SQLExec - 執行攻擊指令
- SQLLbf - 使用字典攻擊與暴力破解法
- SQLSmack - 於Linux執行攻擊指令
- SQL2.exe - 使用UDP緩衝區溢位攻擊
- Msadc.pl - 資訊隱碼攻擊探測

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

彌補資料庫安全漏洞的安全技術 (1/2)

- 利用 ASP 或 ASP.NET 在伺服器端檢查與限制輸入變數的型別與長度，過濾掉不需要的內容。
- 登入 SQL Server 的帳號不要使用 sa，或任何屬於 Sysadmin 群組的帳號，以免有過大的權限。
- 管理者 sa 須有強固的密碼。
- 利用 ADO 的 Command 物件或 ADO.NET 的 SqlCommand class 參數執行 SQL

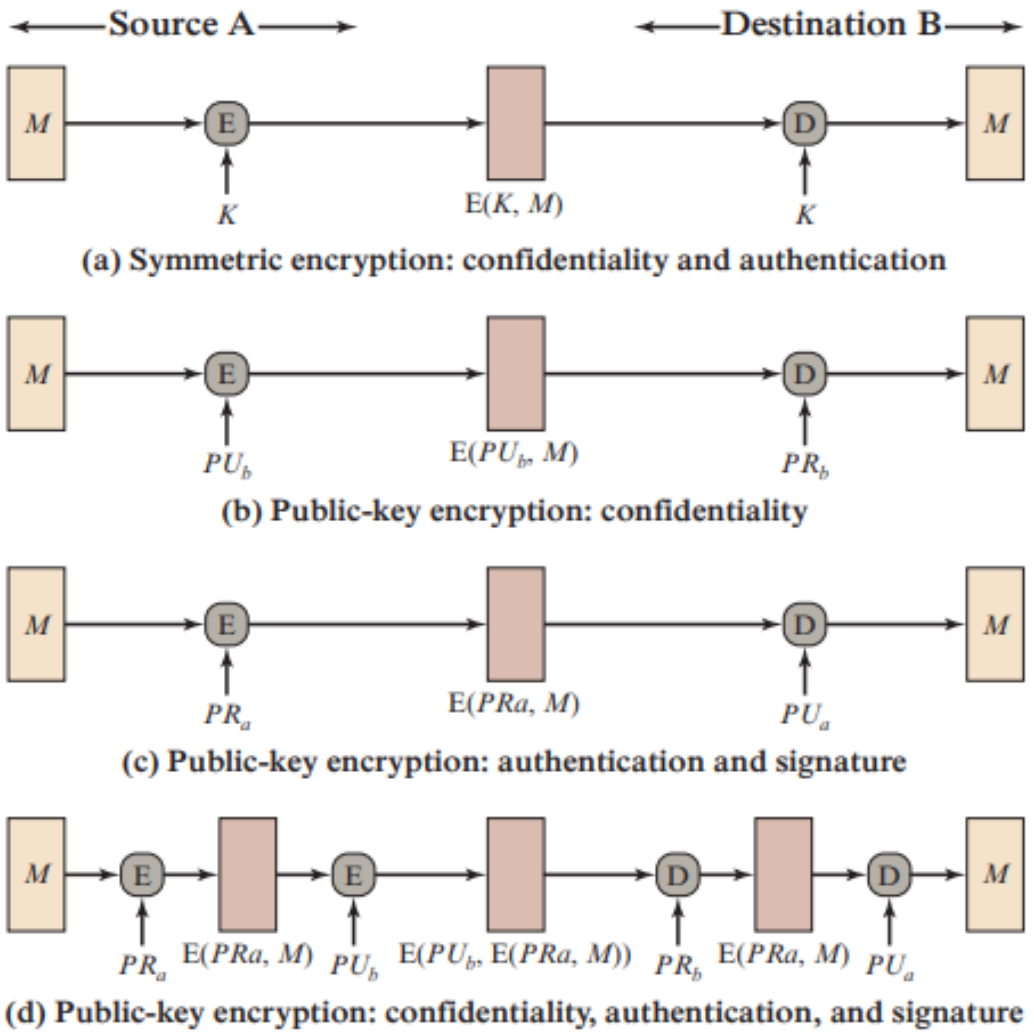
本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

彌補資料庫安全漏洞的安全技術 (1/2)

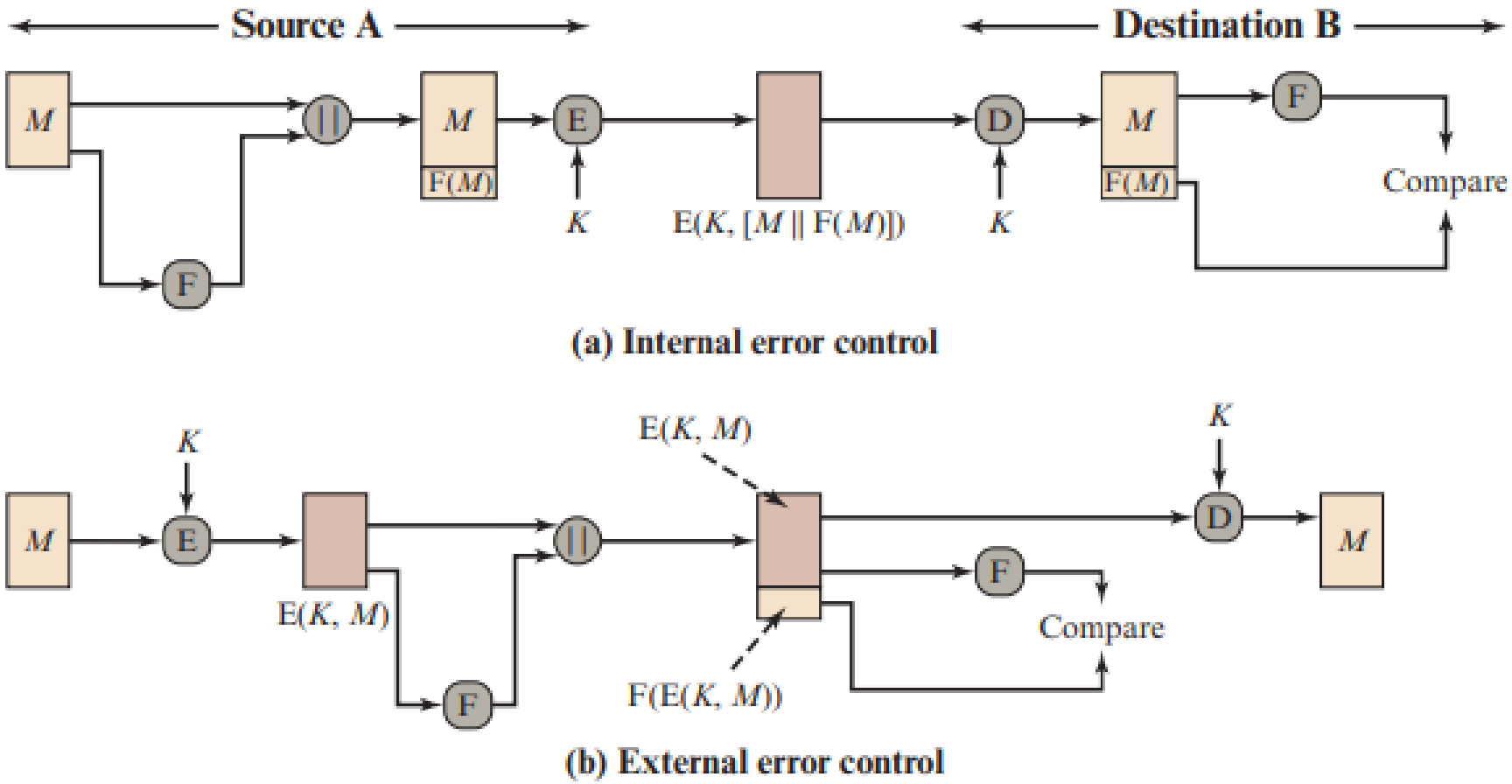
- 更改預設的 Web 虛擬路徑，不要使用 IIS 預設的路徑
- 不要顯示錯誤訊息到客戶端網頁。
- 刪除用不到的延伸預存程序。
- 持續監控系統的執行。
- 防火牆關閉 TCP 1433/UDP 1434 埠(port)對外的連線。
- 隨時注意更新的修補程式。

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

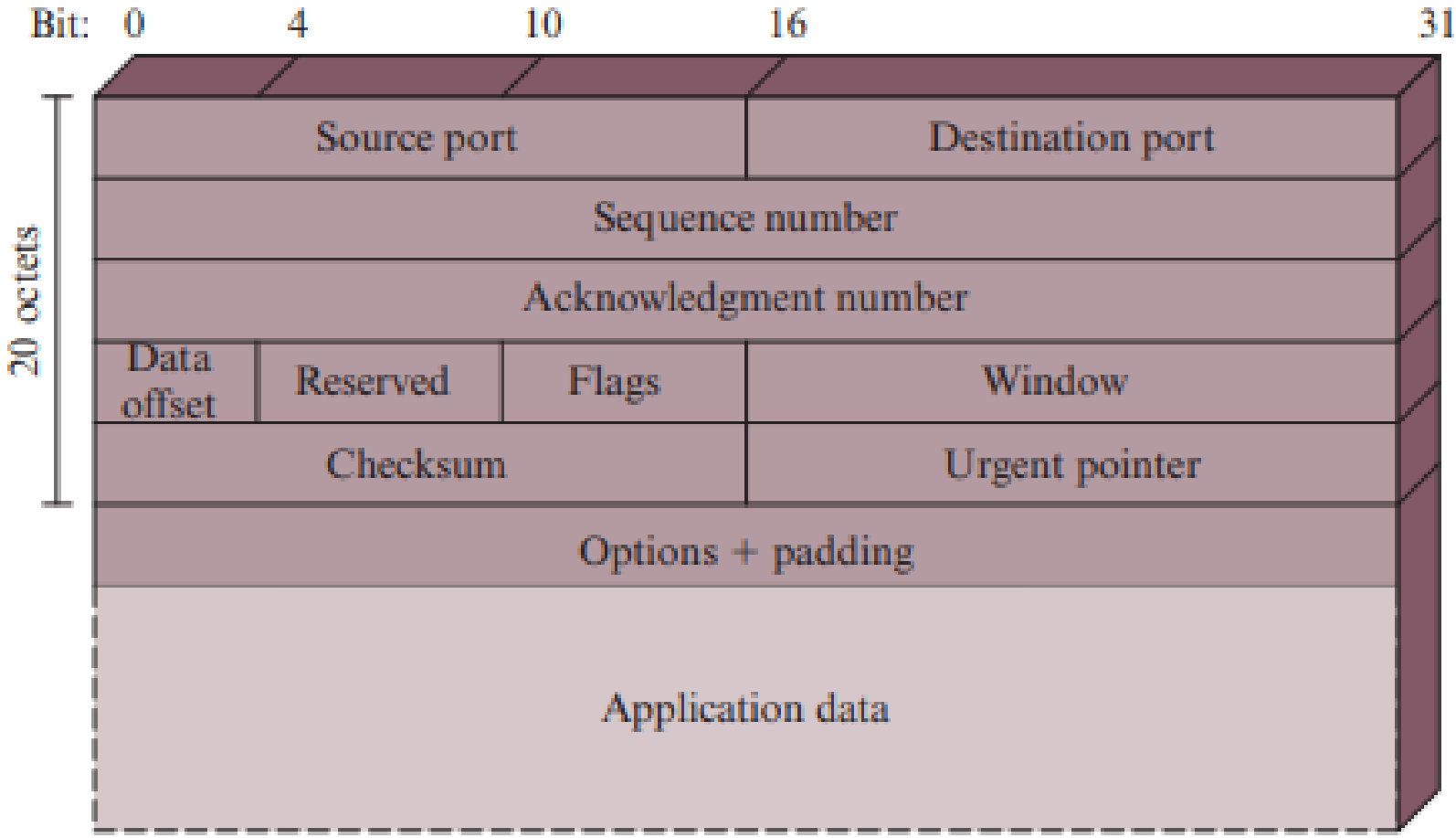
Basic Uses of Message Encryption



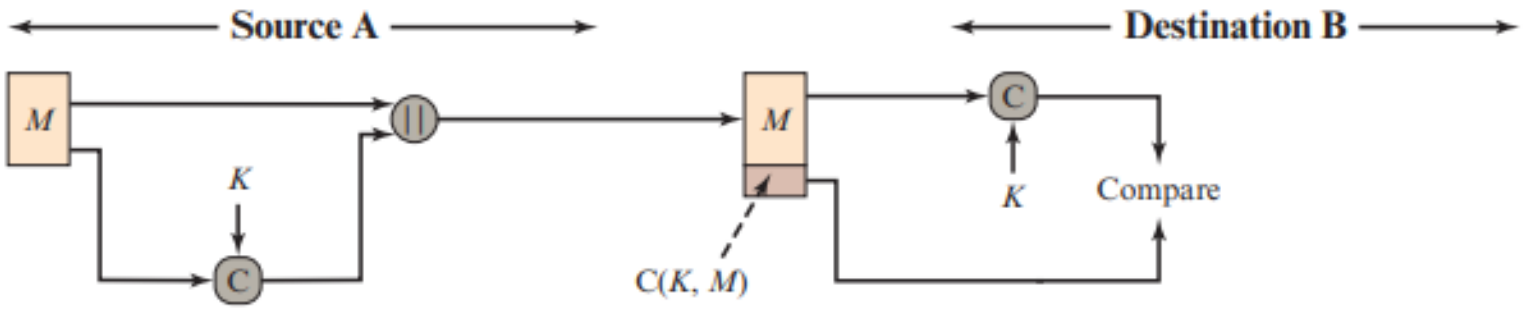
Internal and External Error Control



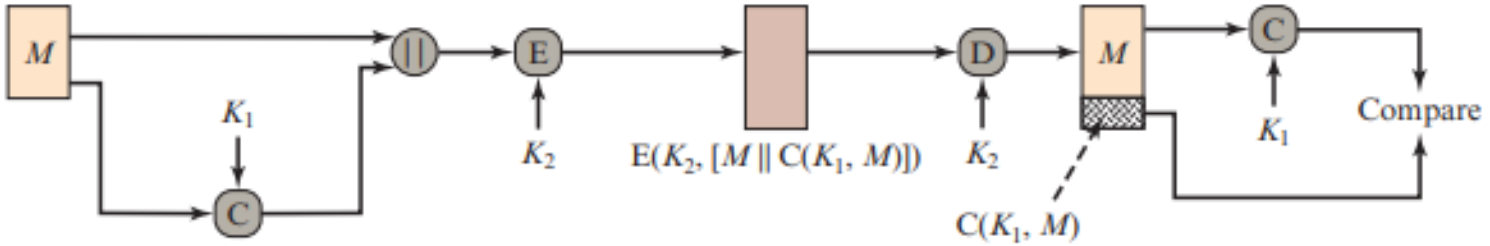
TCP Segment



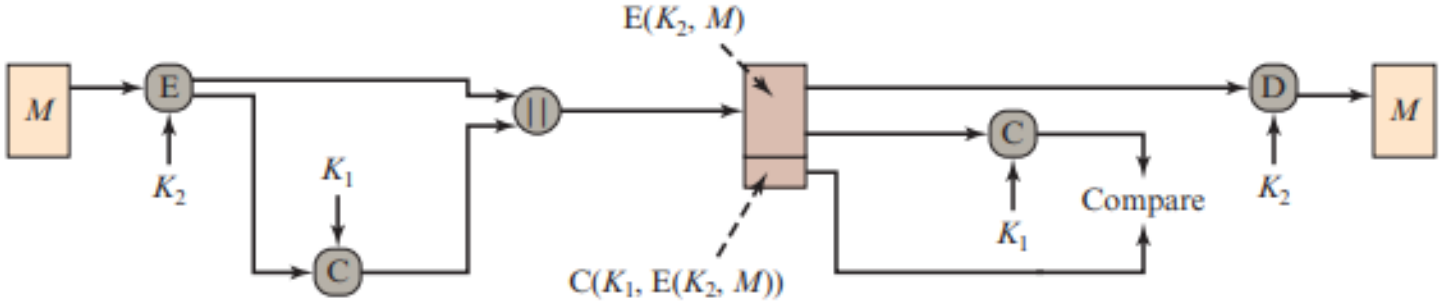
Basic Uses of Message Authentication code (MAC)



(a) Message authentication

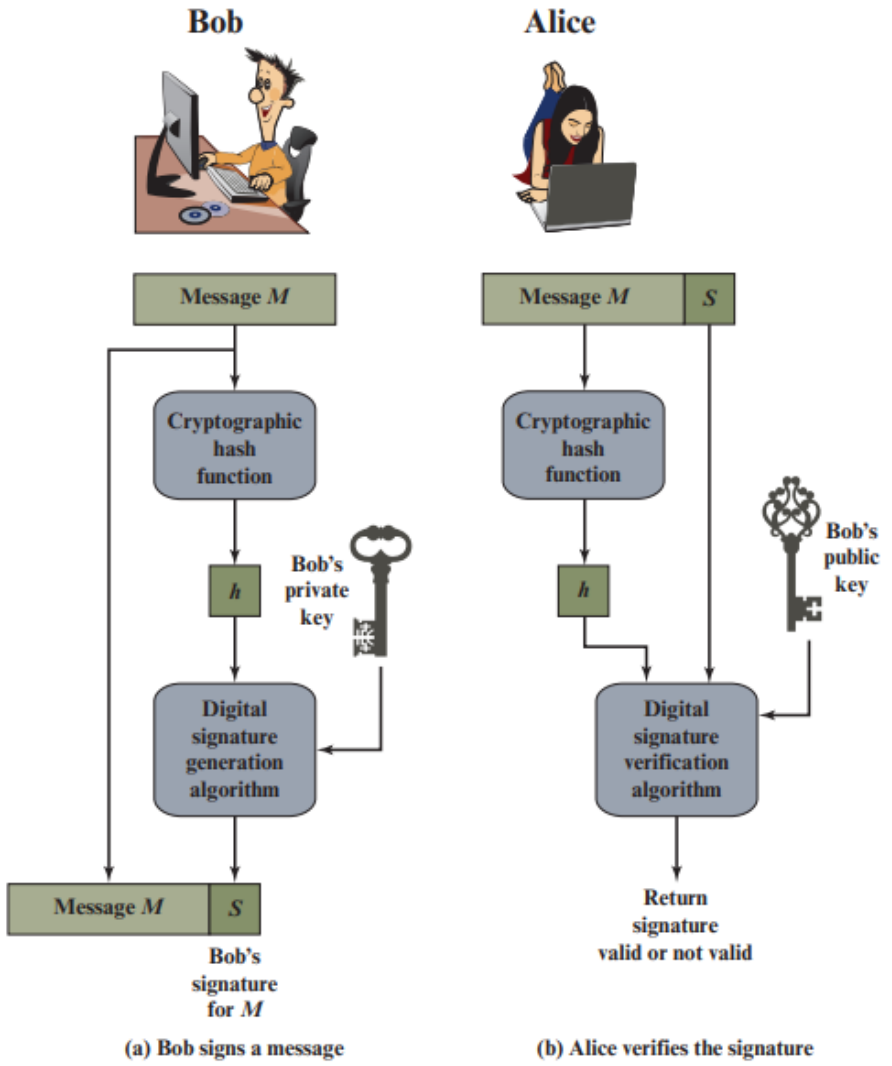


(b) Message authentication and confidentiality; authentication tied to plaintext

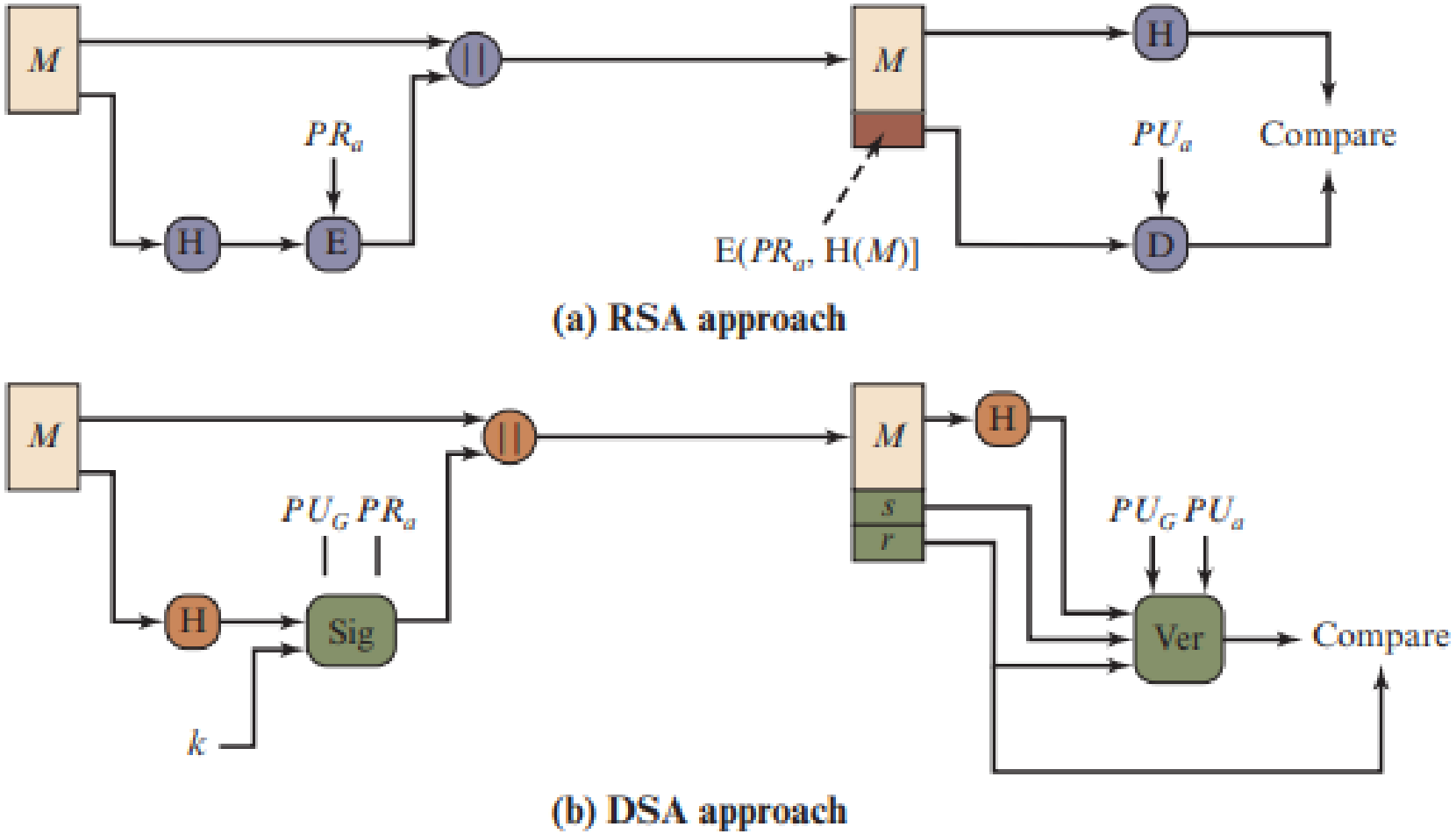


(c) Message authentication and confidentiality; authentication tied to ciphertext

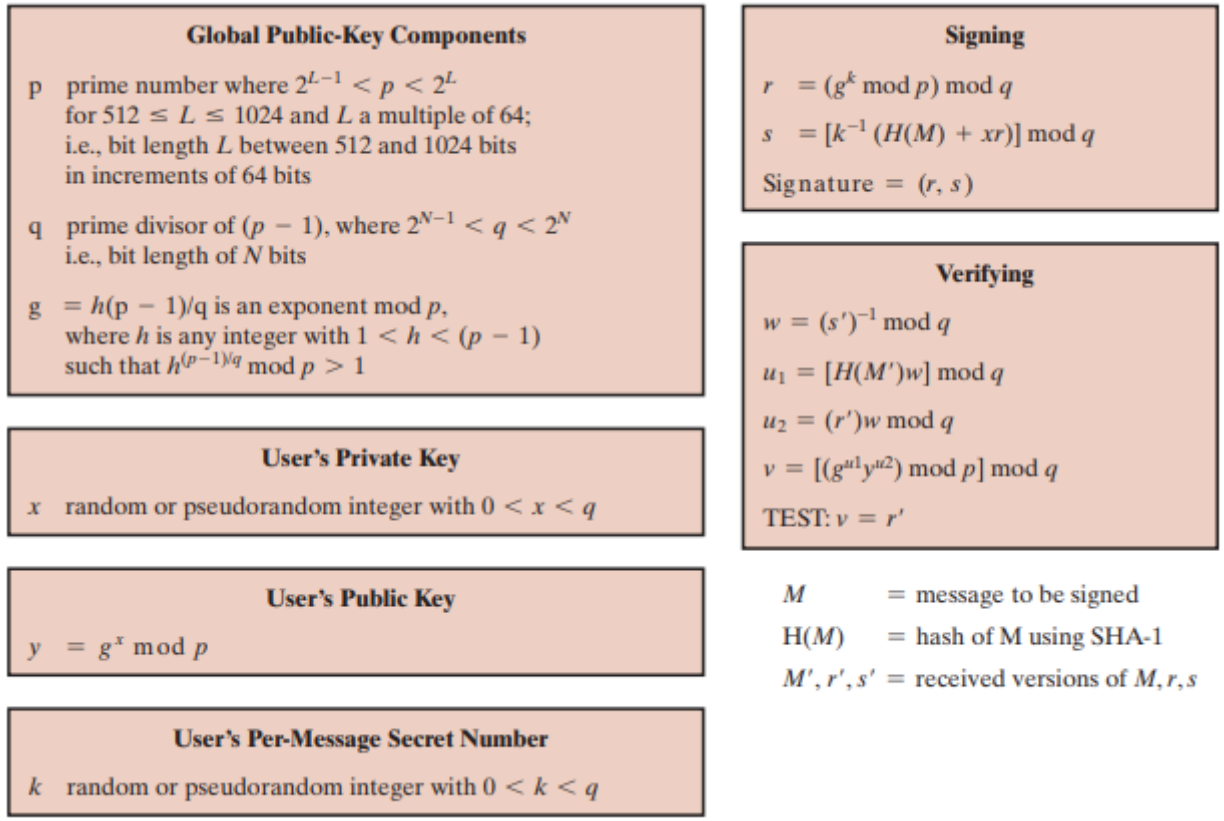
Simplified Depiction of Essential Elements of Digital Signature Process



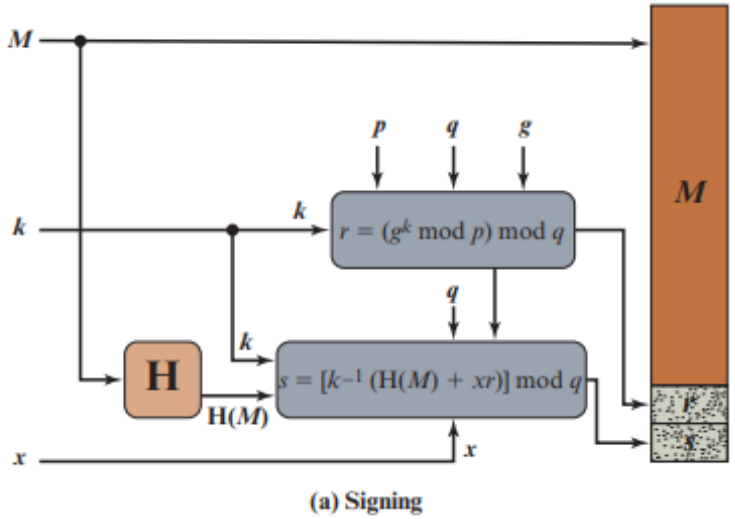
Two Approaches to Digital Signatures



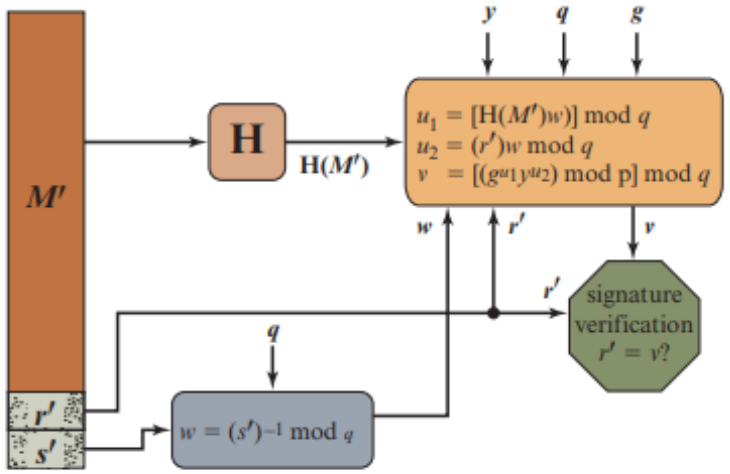
The Digital Signature Algorithm (DSA)



DSA Signing and Verifying

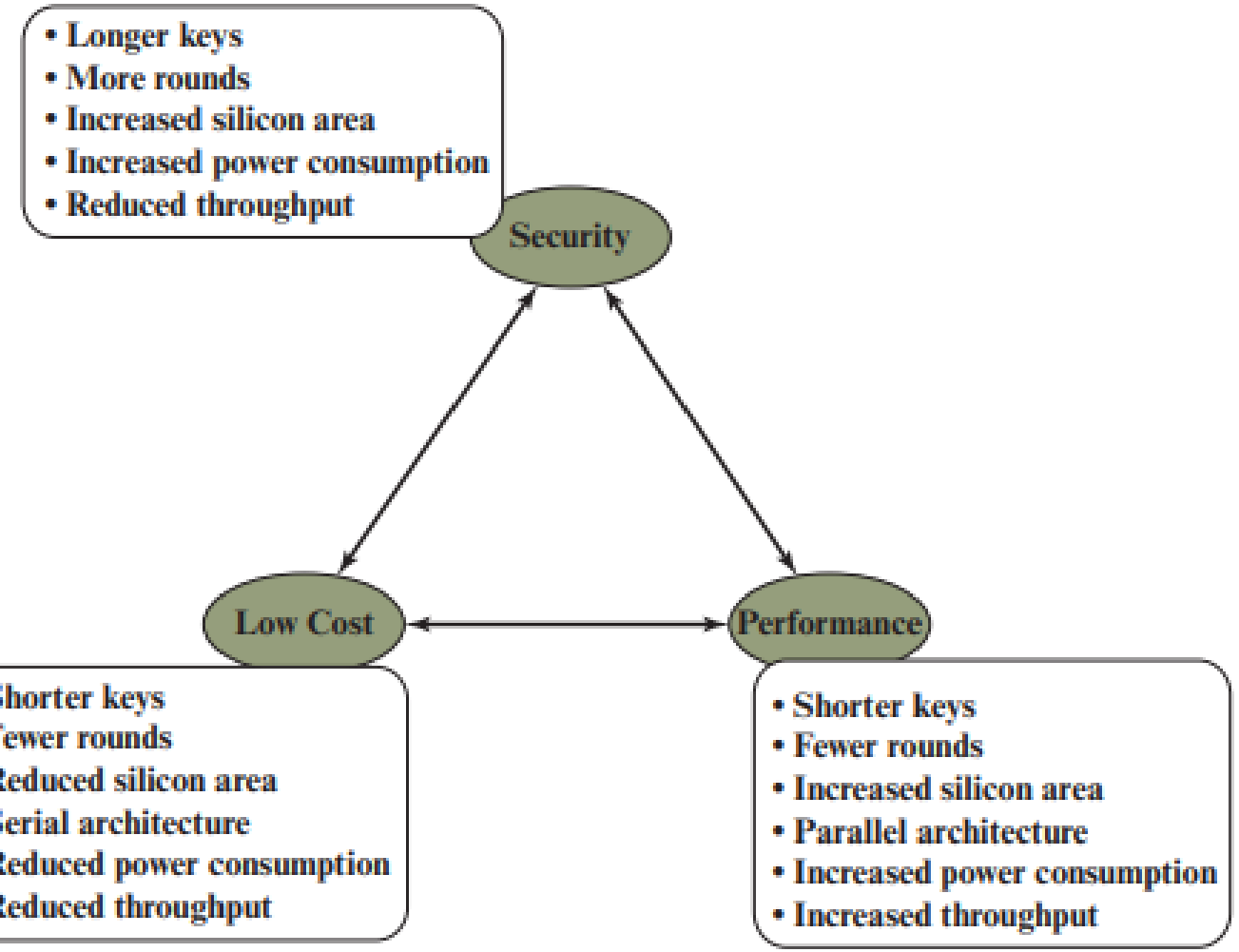


(a) Signing

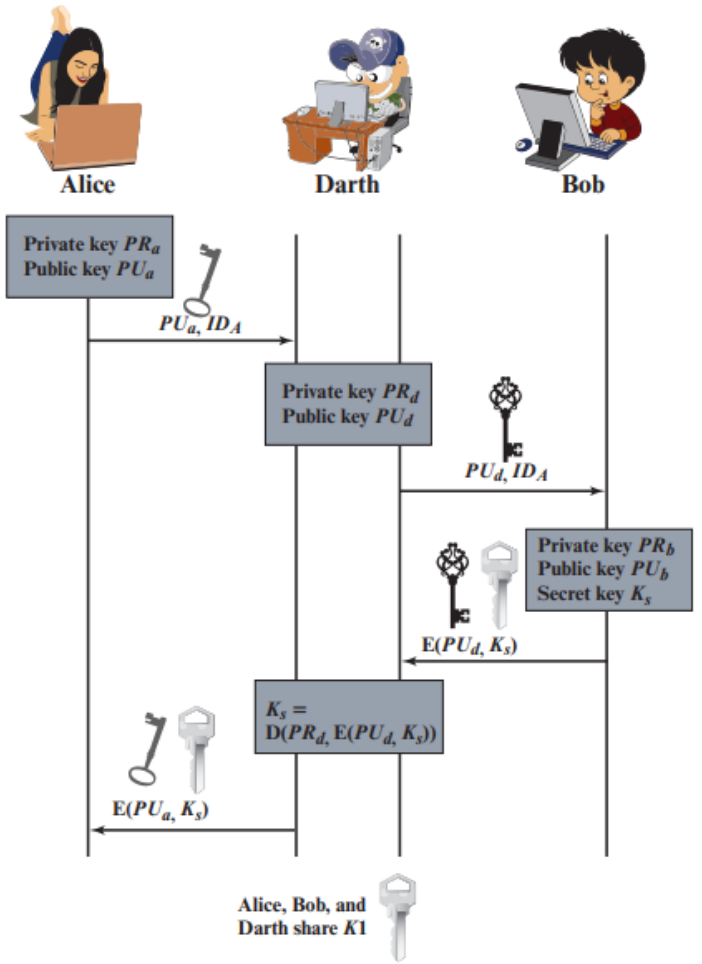


(b) Verifying

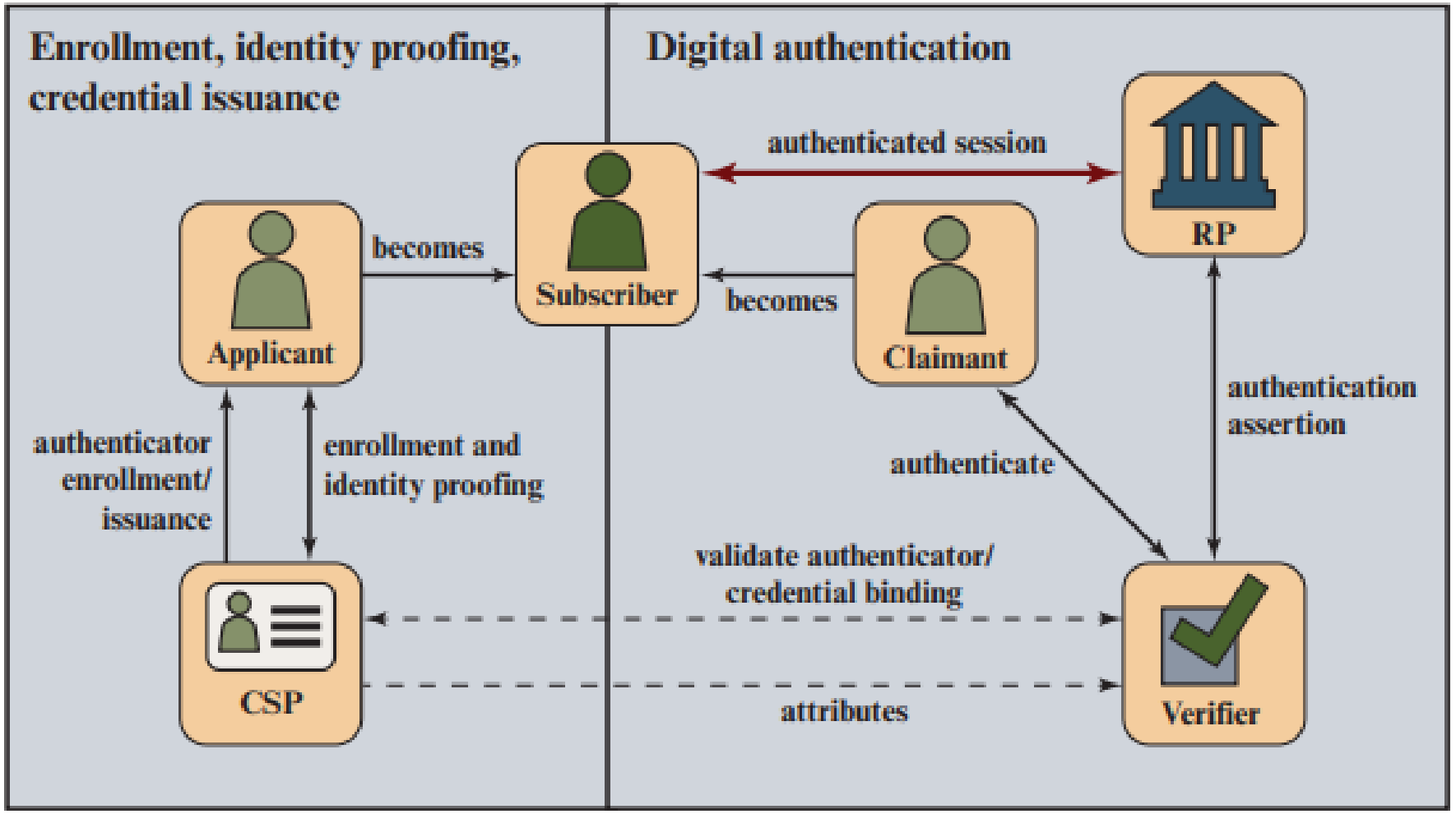
Lightweight Cryptography Trade-Offs



Another Man-in-the-Middle Attack



The NIST 800-63 Digital Identity Model

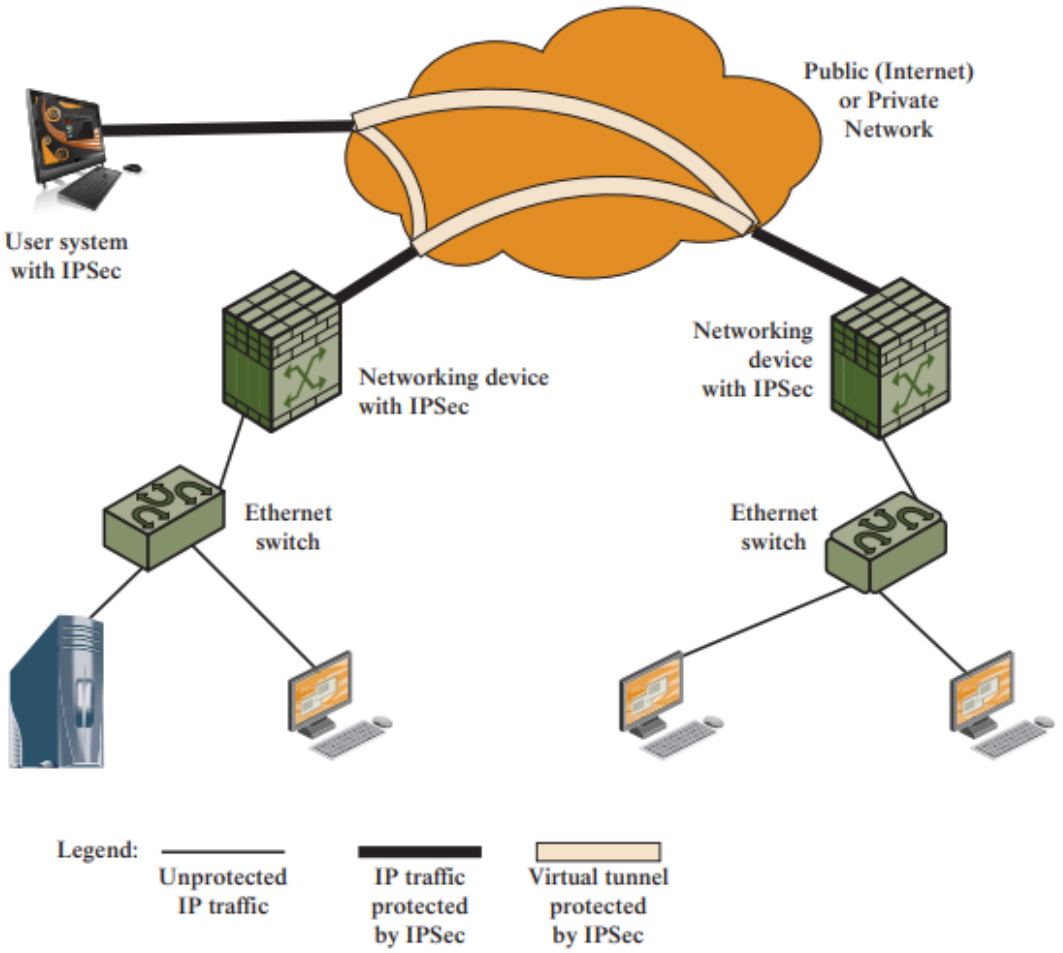


CSP = credential service provider
RP = relying party

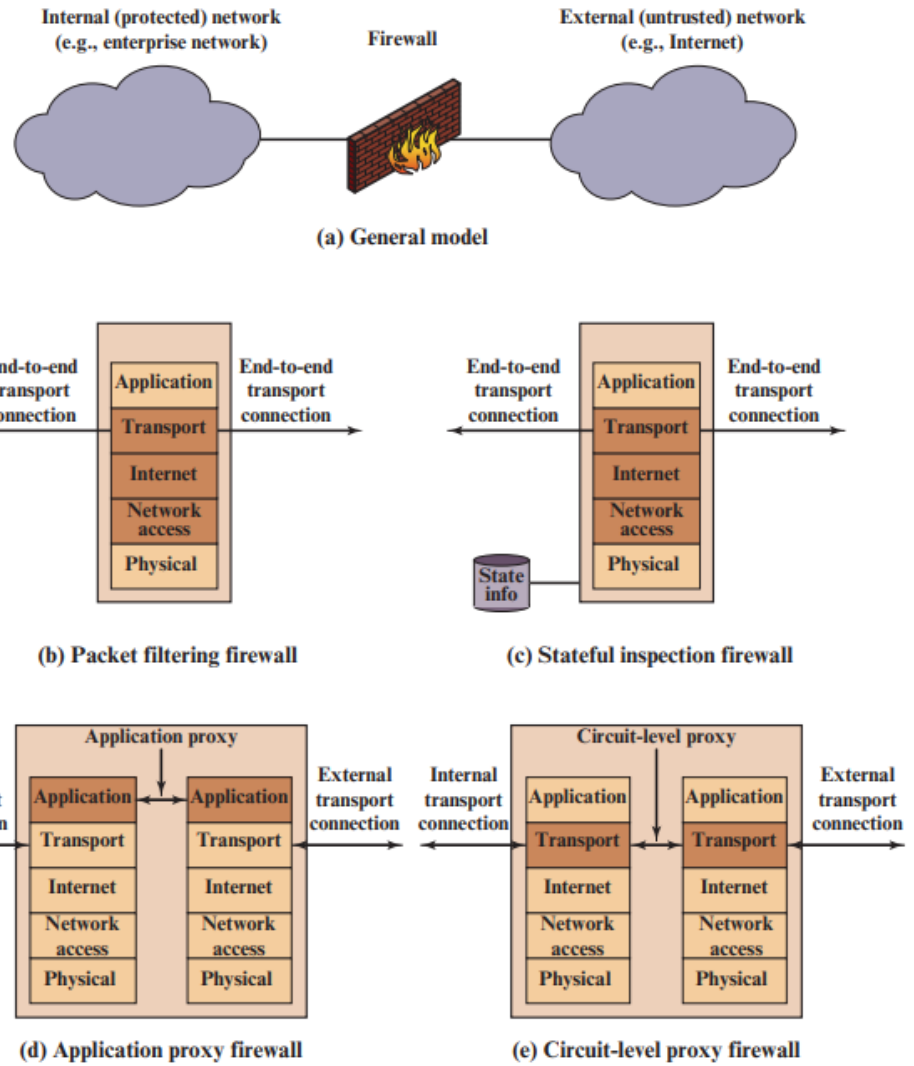
Authentication Factors

Factor	Examples	Properties
Knowledge	User ID Password PIN	Can be shared Many passwords easy to guess Can be forgotten
Possession	Smart Card Electronic Badge Electronic Key	Can be shared Can be duplicated (cloned) Can be lost or stolen
Inherence	Fingerprint Face Iris Voice print	Not possible to share False positives and false negatives possible Forging difficult

Example of Virtual Private Network Implemented with IPsec Tunnel Mode



Types of Firewalls



封包過濾(Packet-Filtering)範例

Rule Set A

action	Ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

Rule Set B

action	Ourhost	port	theirhost	port	comment
block	*	*	*	*	default

Rule Set C

action	Ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

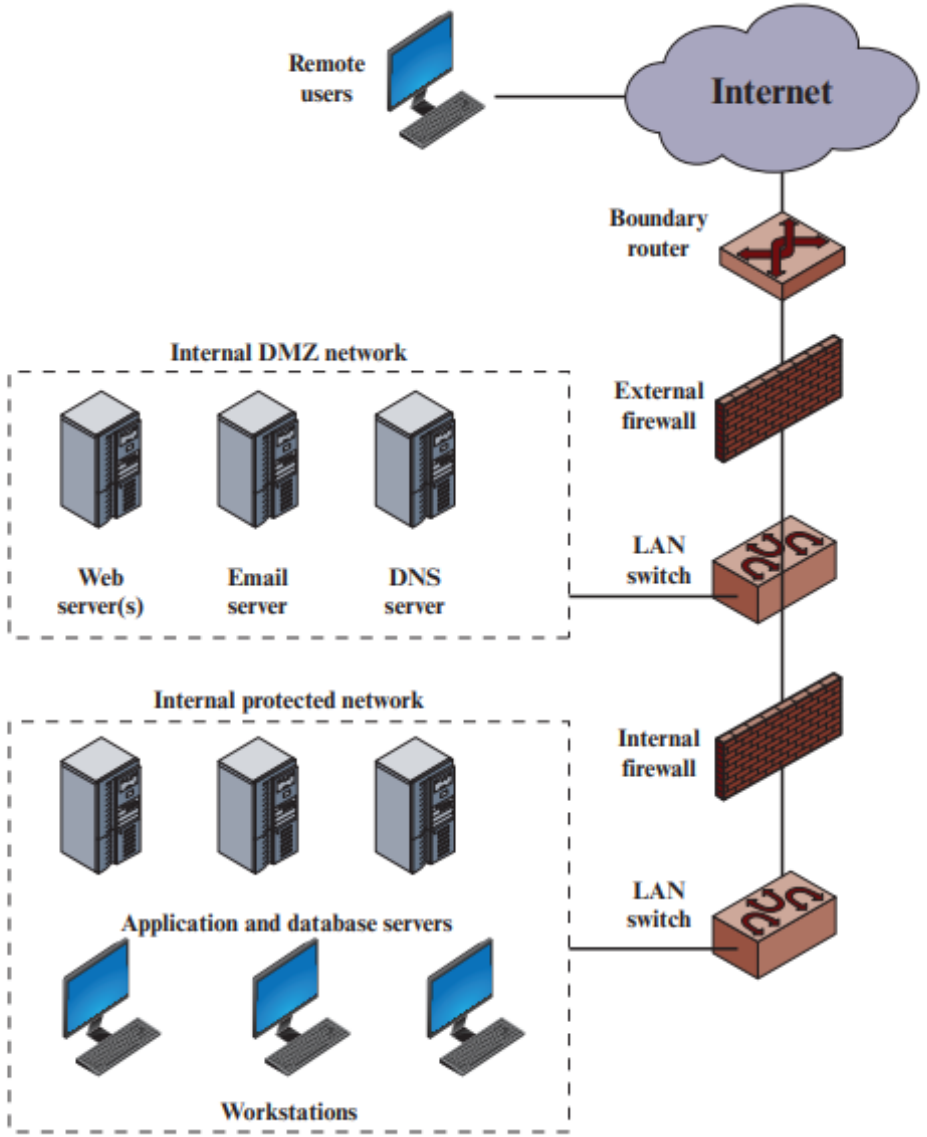
Rule Set D

action	Src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

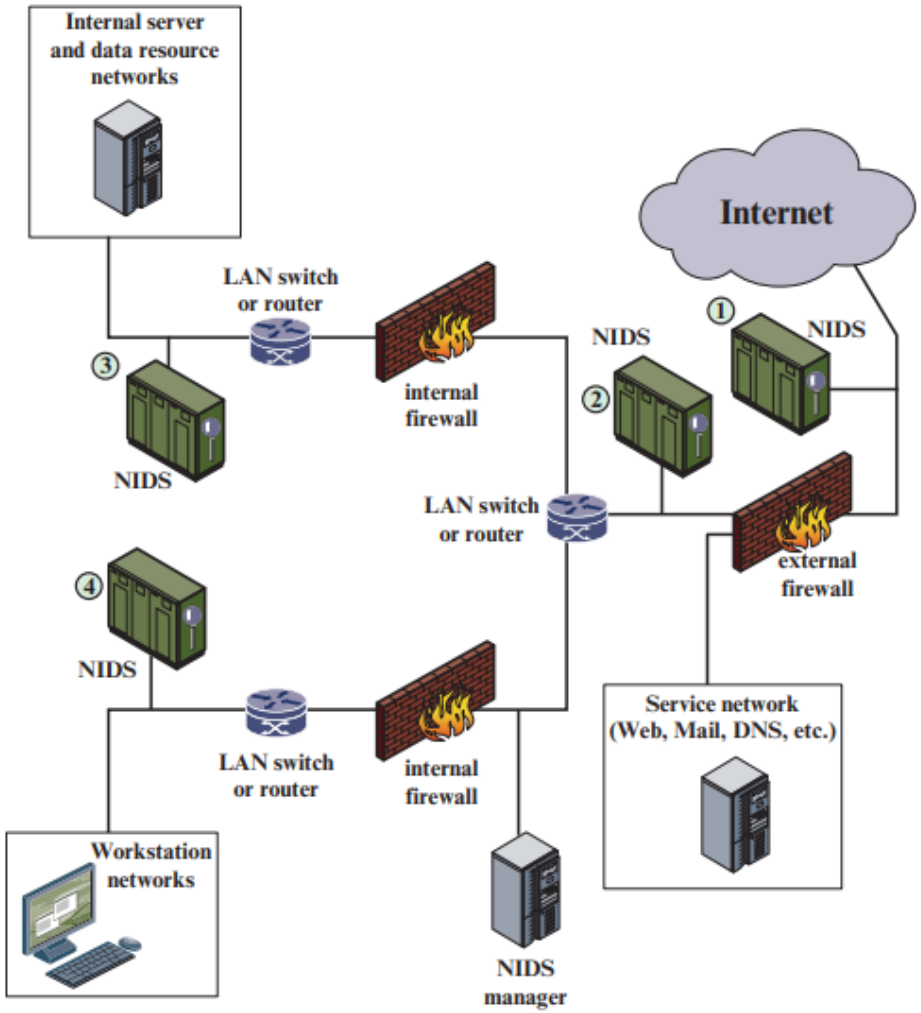
Rule Set E

action	Src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

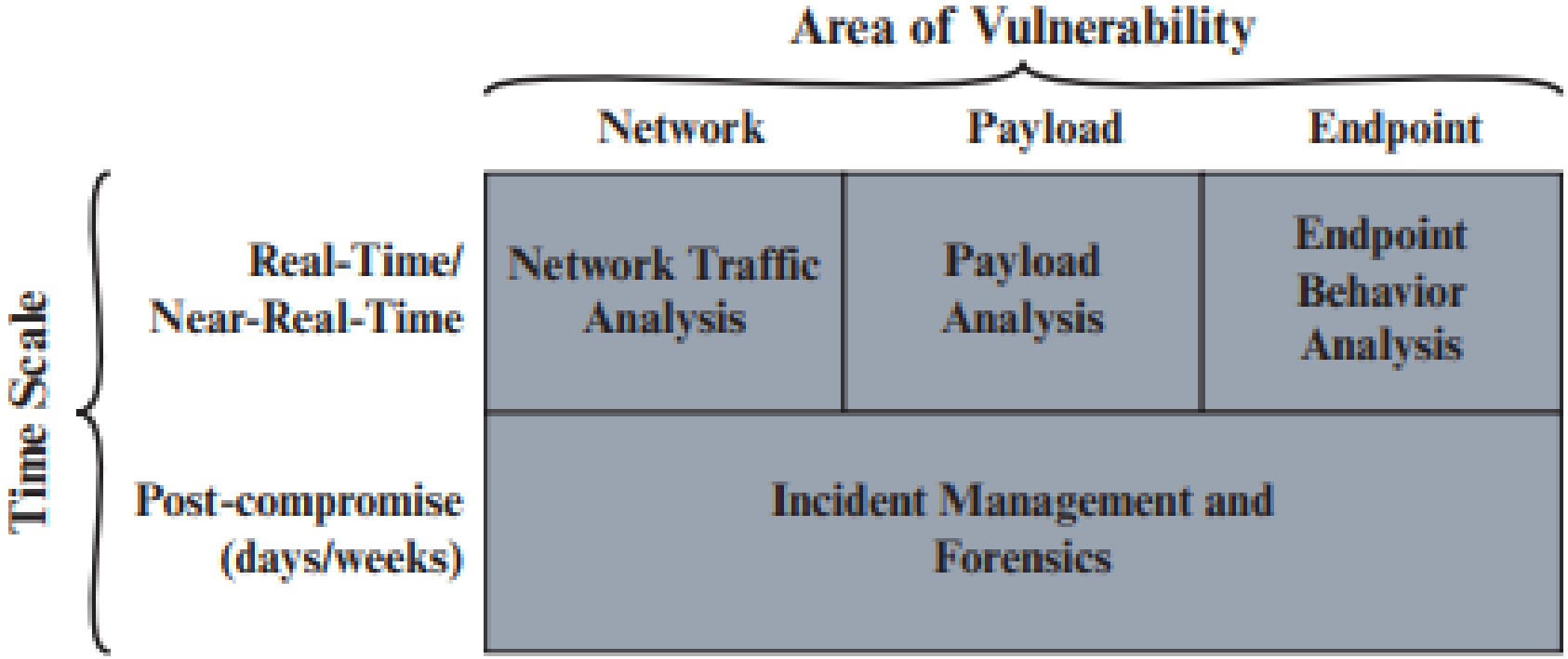
防火牆設定範例



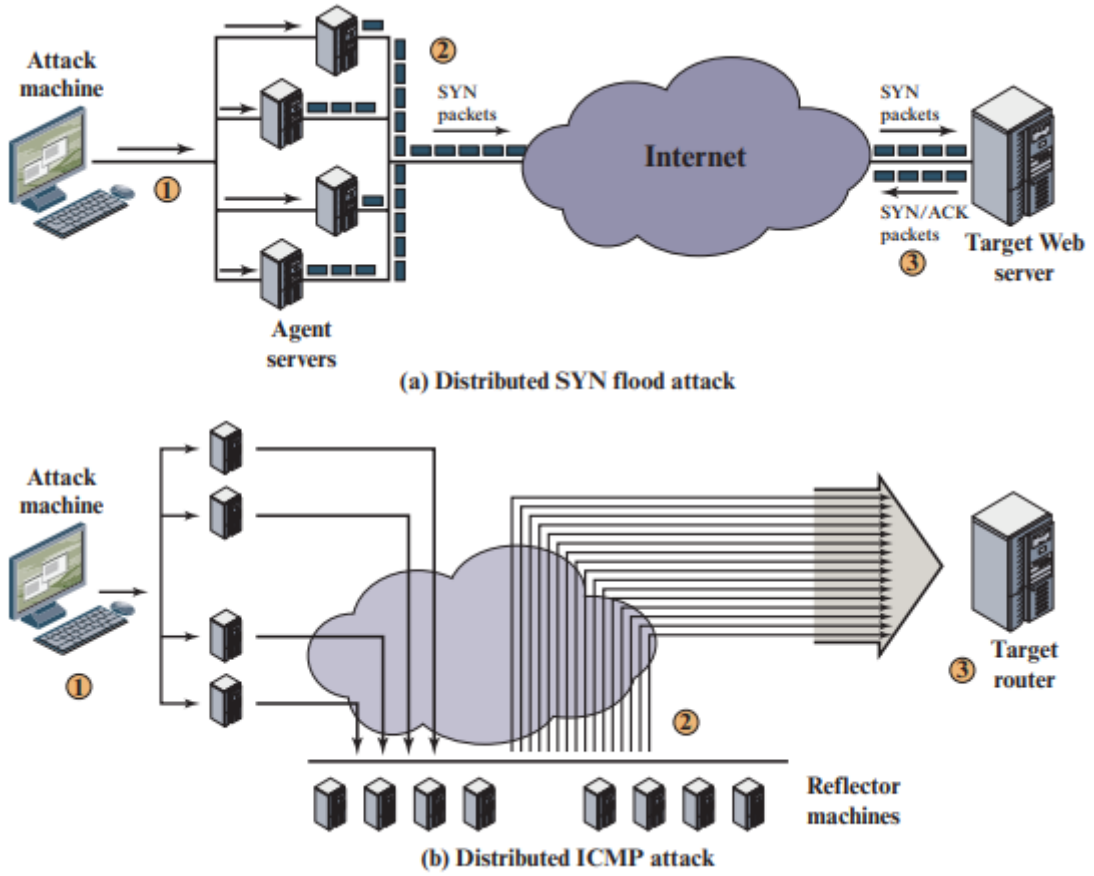
Example of NIDS Sensor Deployment



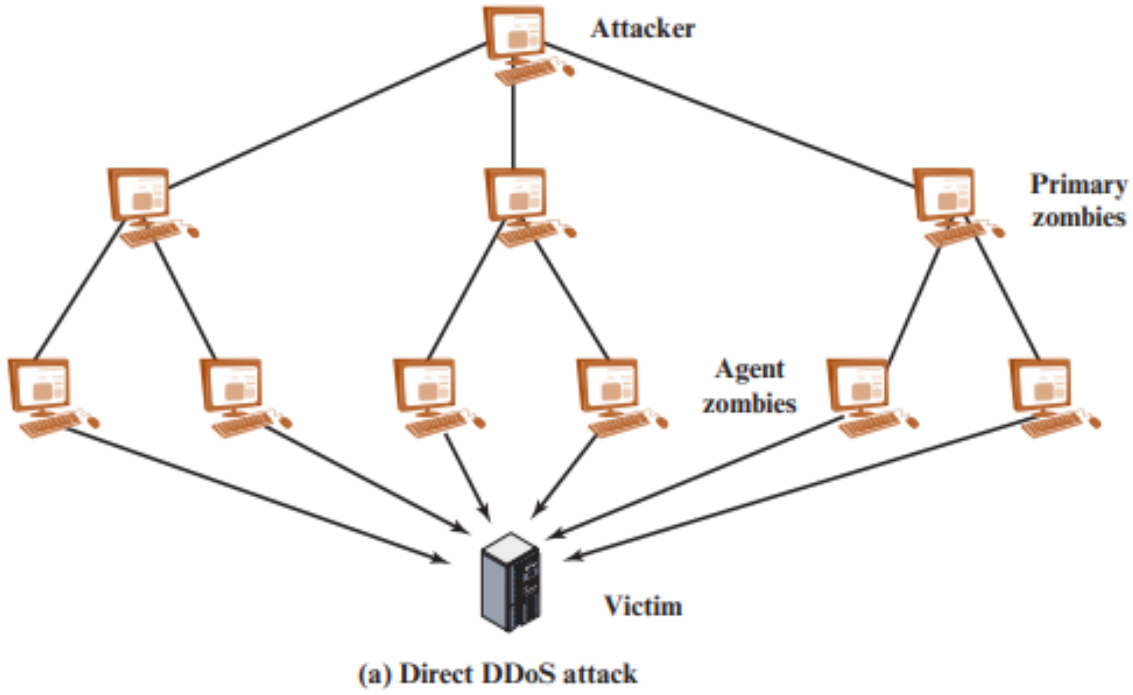
Five Elements of Malware Defense



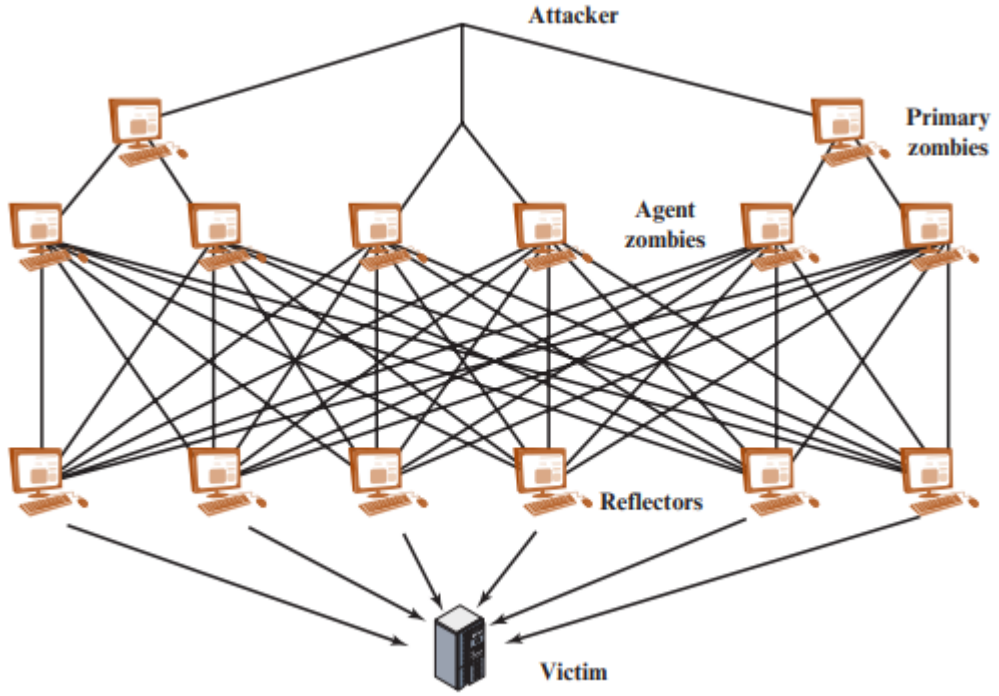
Examples of Simple DDoS Attacks



Types of Flooding-Based DDoS Attacks



(a) Direct DDoS attack



(b) Reflector DDoS attack

Sample Packet Filter Firewall Ruleset

	Source Address	Source Port	Destination Address	Destination Port	Action
1	Any	Any	192.168.1.0	> 1023	Allow
2	192.168.1.1	Any	Any	Any	Deny
3	Any	Any	192.168.1.1	Any	Deny
4	192.168.1.0	Any	Any	Any	Allow
5	Any	Any	192.168.1.2	SMTP	Allow
6	Any	Any	192.168.1.3	HTTP	Allow
7	Any	Any	Any	Any	Deny

因為感冒 聲音辨識系統 無法正確辨識 為哪一型錯誤?

- 「錯誤接受率」（False Acceptance Rate, FAR）
- 「錯誤拒絕率」（False Rejection Rate, FRR）
- Type II error

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

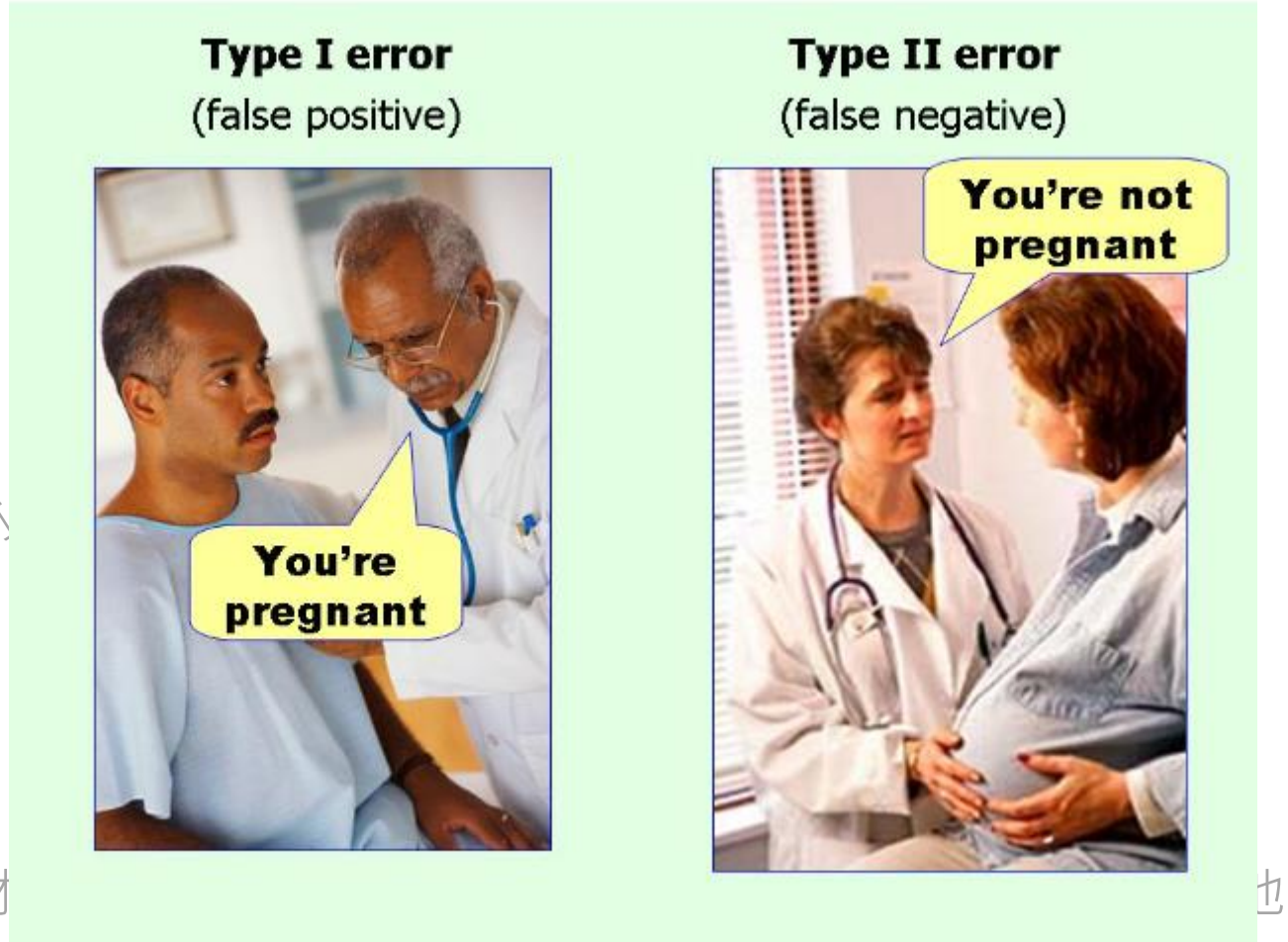
型一錯誤與型二錯誤

- 在假說檢定中，有一種假說稱為「虛無假說」，記為H0假說檢定的目的是利用統計的方式，推翻虛無假說的成立，也就是對立假說（Alternative hypothesis，記為Ha或H1成立。
- 假說檢定涉及選擇兩個相互競爭的命題，稱為虛無假說(Null hypothesis)，用H0表示，另一種對立假說(Alternative hypothesis)，用H1表示。
- 如果測試結果與現實相符，則做出了正確的決定。但是，如果測試結果與實際不符，則發生錯誤。發生錯誤的情況有兩種：虛無假說為真，而我們拒絕H0。另一方面，對立假說H1為真，而我們不拒絕H0。兩種錯誤分別稱為：型一錯誤、型二錯誤[1]
- 若虛無假說事實上成立，但統計檢定的結果拒絕虛無假說（接受對立假說），這種錯誤稱為型一錯誤。
- 若虛無假說事實上不成立，但統計檢定的結果不拒絕虛無假說，這種錯誤稱為型二錯誤。[2]

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

Type I errors and Type II errors

Type I errors, also known as false positives, occur when you see things that are not there. Type II errors, or false negatives, occur when you don't see things that are there (see Figure below).



- 聲音辨識系統無法正確辨識因為感冒而改變的聲音，通常屬於「錯誤接受率」（False Acceptance Rate, FAR）和「錯誤拒絕率」（False Rejection Rate, FRR）中的一種問題。

- 在這種情況下，感冒可能會導致聲音特徵的暫時改變，因此系統可能會出現較高的錯誤拒絕率（FRR），即合法使用者的聲音特徵被系統錯誤地拒絕，因為它與系統中已存儲的聲音特徵不匹配。這通常是因為聲音識別系統對於聲音生物特徵的變化缺乏足夠的靈活性。

- 改善此問題的方法可能包括增加系統的樣本多樣性，確保系統能學習和容忍聲音的正常變動，或使用更複雜的機器學習模型來提高系統的穩健性。

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

- 在統計學中，Type II error（第二類錯誤）指的是當虛無假設為假時，錯誤地不拒絕虛無假設。在語音辨識的情境中，如果我們類比語音辨識的錯誤接受和錯誤拒絕：

- Type I error 可能類比於系統錯誤地接受不正確的聲音（False Acceptance），即系統認為不匹配者為匹配者。
- Type II error 可能類比於系統錯誤地拒絕正確的聲音（False Rejection），即系統認為匹配者為不匹配者。
- 因此，當因為感冒而聲音改變導致系統無法識別你的聲音時，這更接近於第二類錯誤（Type II error），因為系統錯誤拒絕了本應接受的聲音匹配。

		真實情況	
		（虛無假說）為真	Ha（對立假說）為真
根據研究結果的判斷	拒絕H0	錯誤判斷 （**偽陽性、型一錯誤**） 發生機率α（顯著水準）	正確判斷 發生機率1-β（檢定力）
	不拒絕H0	正確判斷 發生機率1-α	錯誤判斷 （**偽陰性、型二錯誤**） 發生機率β

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

		真實情況	
		H_0（虛無假說）為真	H_a（對立假說）為真
根據研究結果的判斷	拒絕H_0	錯誤判斷 （偽陽性、型一錯誤） 發生機率α（顯著水準）	正確判斷 發生機率1-β（檢定力）
	不拒絕H_0	正確判斷 發生機率1-α	錯誤判斷 （偽陰性、型二錯誤） 發生機率β

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

- Default = discard: That which is not expressly permitted is prohibited.
- Default = forward: That which is not expressly prohibited is permitted.

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

6.4 惡意程式

- 惡意程式：電腦病毒、電腦蠕蟲、後門程式、木馬程式、間諜軟體、釣魚網頁等，是能侵害電腦正常操作的程式。

- 惡意程式常造成電腦重大損失，以下介紹常見的惡意程式，如圖6-6。

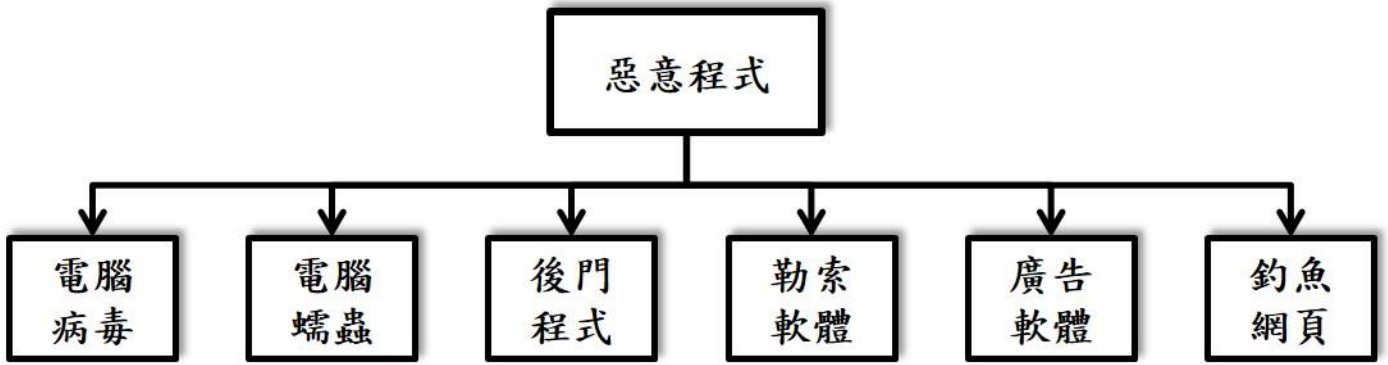


圖6-6常見的惡意程式

惡意程式

- 勒索軟體（Ransomware）：主要透過「社交工程」或其他方式以誘騙使用者上當，像參加抽獎郵件、中獎通知、一般帳單等等。勒索軟體被執行後，會發現電腦的檔案、文件等資料都被鎖住無法開啟，欲開啟檔案或文件時會跳出勒索警告視窗。
- 間諜程式/廣告軟體（spyware / adware）：也是利用各種管道自動安裝在受害者的電腦中，它不會明顯的危害或破壞電腦軟硬體資源，然而它主要目的是竊取電腦內的重要或機密資料，對於資訊安全造成嚴重威脅。
- 釣魚網頁（phishing site）：屬於網路詐騙行為的一種，它並不需要使用複雜的駭客技術，利用電子郵件寄發垃圾郵件，使受害者誤信而連結到一些偽造的網站，竊取受害者的帳號和密碼。

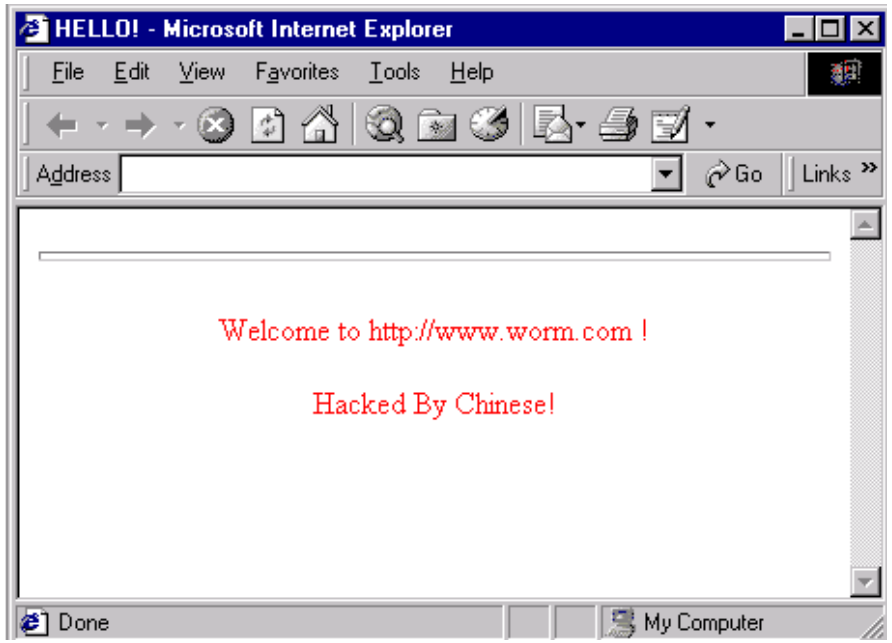


圖 6-7 受 Code Red 病毒感染之伺服器，使用者連線所見的畫面

圖 6–8 勒索程式之警告畫面

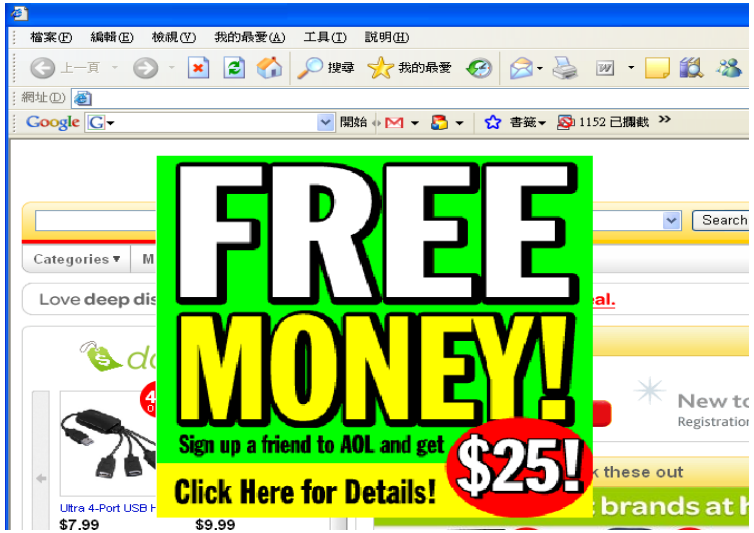


圖 6-9 廣告軟體跳出廣告視窗

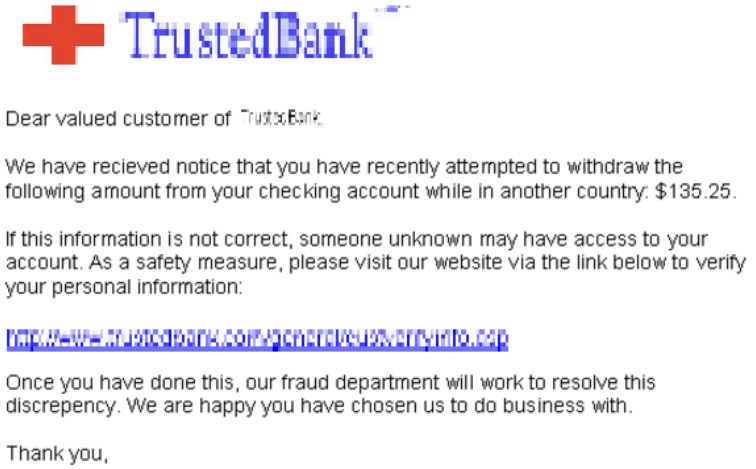


圖 6-10 釣魚郵件

存取控制

- 存取控制 (Access control) 是作業系統中管理系統資源的機制，是控制每一個主體 (subject)依其權限 (Permission) 以存取各項客體 (Object)資源的控管方法。
- 參考存取控制示意圖。

ACL 存取控制方法

- ACL是常用的存取控制方法之一 (如左圖)，每項客體都存有一份清單，主體與權限記錄在清單上，當主體要存取客體資源時，客體查核清單上的主體與權限，作為控管機制。

- 例如： Anna 和 Bart 擁有資料庫之存取權限，在資料庫維護存取控管清單上，Anna 僅有讀取權限，Bart 則擁有讀取、寫入、修改與刪除權限。

- 範例：如右圖 Windows 作業系統 ACL 存取控制設定。

ACL 存取控制方法

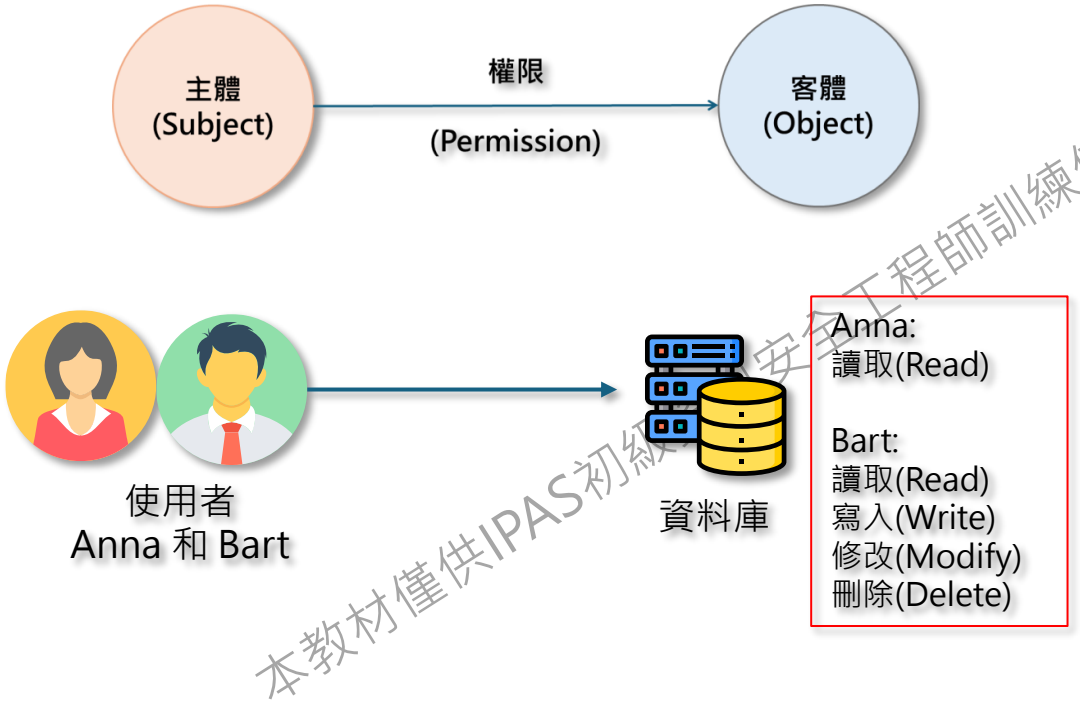


圖 ACL 存取控制方法

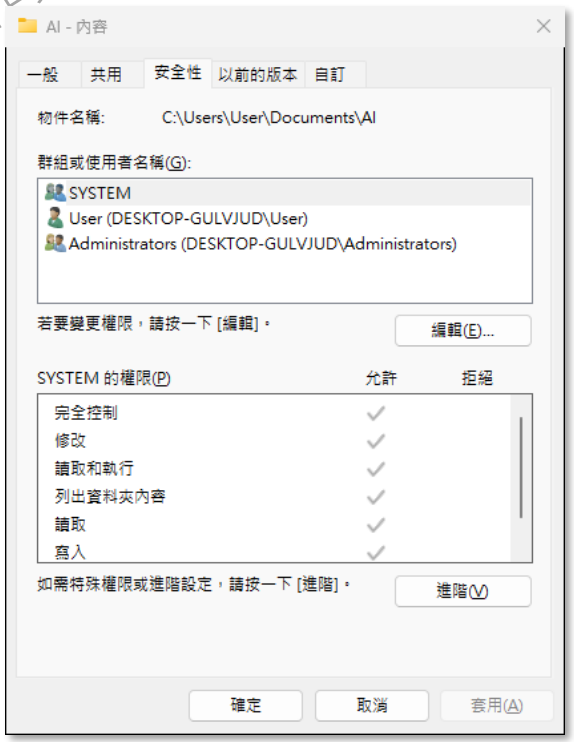


圖 Windows 作業系統 ACL存取控制範例

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

主體功能存取控制

- 主體功能存取控制，是在主體上維護一個表格清單，以控管其可以存取的客體與權限。
- 例如：Anna 可以讀取資料庫之資料，也可以讀取、寫入、修改與刪除檔案系統，參考圖。

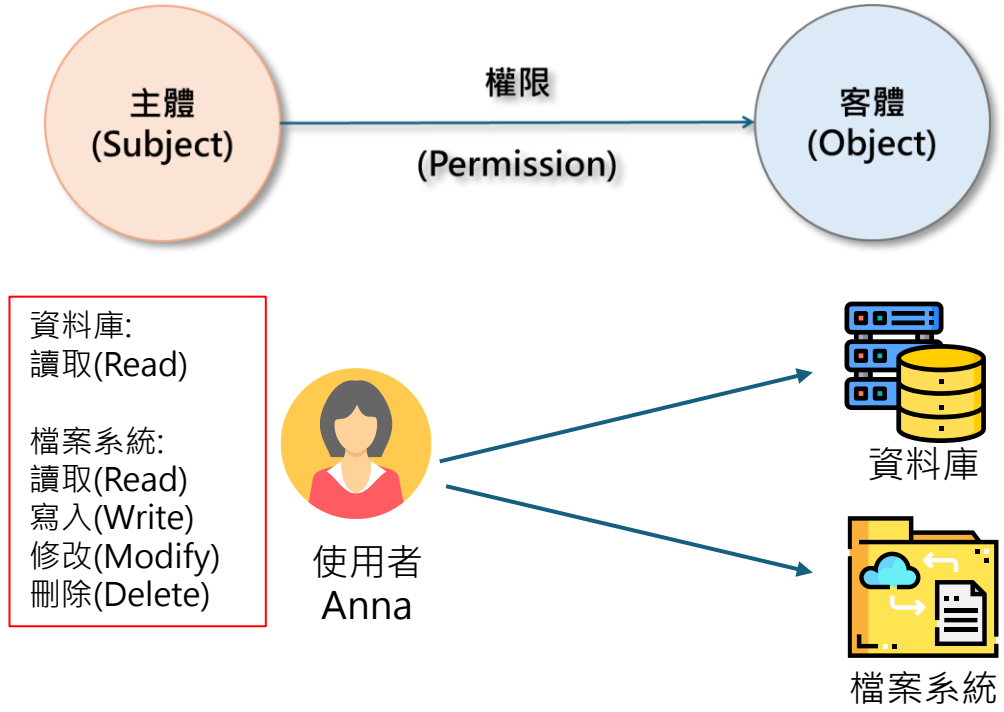


圖　主體功能存取控制

RBAC 存取控制方法

- 例如：某公司有多位業務人員，假若他們使用系統的權限都是一樣的。如果使用ACL 的方法，則需要每一個人都設定權限，操作複雜，又有安全疑慮。

- 反之，若將職務看作一個角色 (role)，依角色分派權限，再將人員指定其角色，此方法稱為角色基存取控制 (RBAC)。如圖 RBAC 存取控制方法。

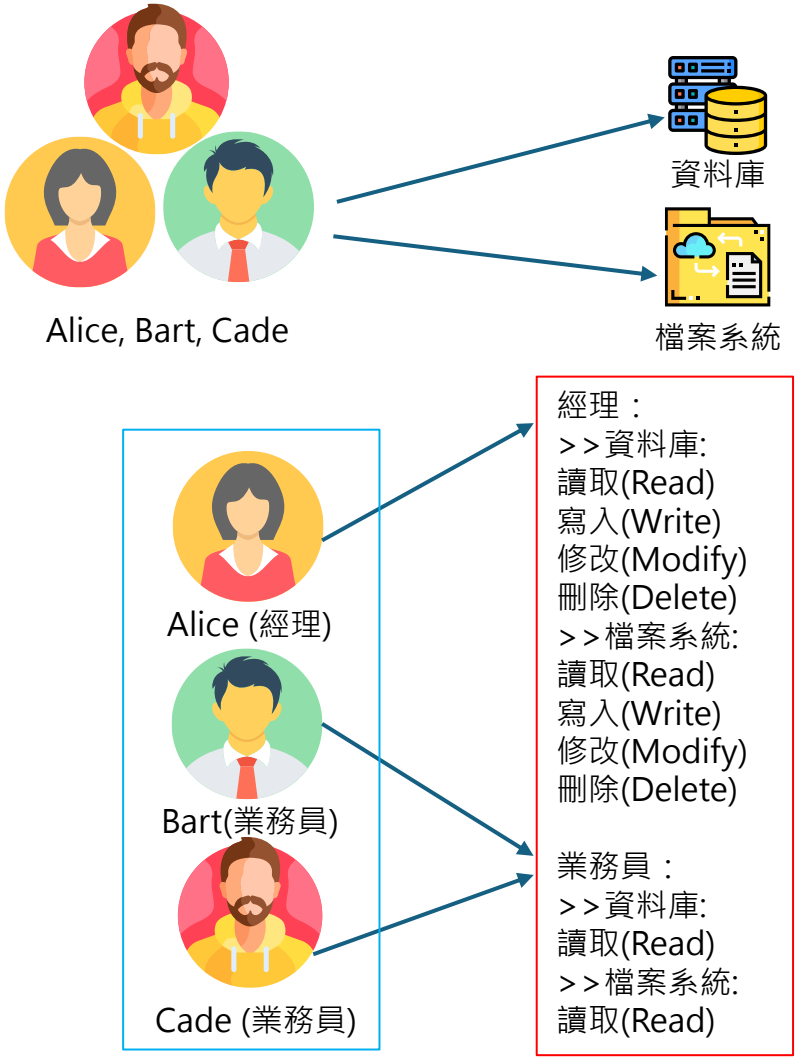


圖 RBAC 存取控制方法

可信賴電腦系統

- 1983 年美國國防部國家電腦安全中心為因應軍事電腦保密的需要，對可信賴電腦基礎 (Trusted Computing Base；TCB) 做較為明確的定義並提出可信賴電腦系統評估準則 (Trusted Computing System Evaluation Criteria；TCSEC)。
- 1991 年，英、法、德、荷等歐洲較先進國家，也提出『資訊技術安全評估準則』(Information Technology Security Evaluation Criteria；ITSEC) 。
- 1999 年由Intel、IBM、HP、Compaq 及Microsoft 發起一個可信賴計算平台聯盟 (Trusted Computing Platform Alliance；TCPA)，隨後於 2002年更名為可信賴電腦組織 (Trusted Computing Group；TCG) 。

TCSEC安全評估準則

- 『 可信賴電腦系統安全評估準則』 (Trusted Computer System Evaluation Criteria；TCSEC)，就是俗稱的『橘皮書』(Orange Book)。

- 橘皮書根據電腦系統採用的安全功能，將電腦系統分為四大類七個安全等級，分別是 D、 C1 、 C2 、 B1 、B2 、 B3 與 A1 七個等級，如表 6-1。

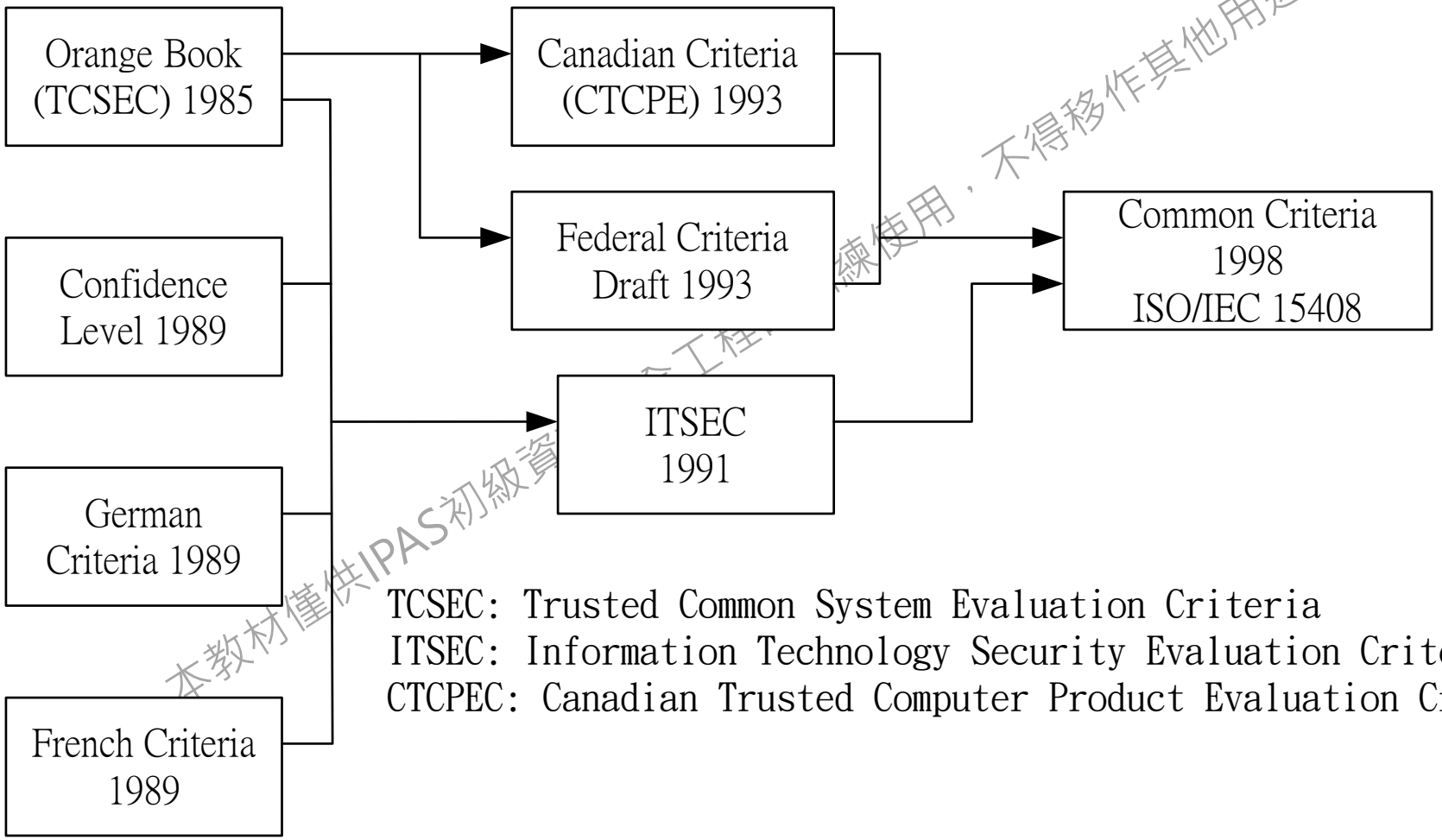
TCSEC 安全標準等級

類別	評估標準	等級	評估準則概要
A	需經認可之保護措施	A1	經許可的系統安全設計，如 Boeing Aerospace SNS 系統
B	強制性系統保護措施	B3	獨立系統安全模組
		B2	結構化系統保護設計，如 Trusted XENIX 系統
		B1	強制進入管制與資料安全標示，如 Solaris 8 作業系統
C	使用者決定系統保護措施	C2	系統管理者可對使用者實施稽核
		C1	使用者決定資料保護措施
D	無保護措施	D	資料無安全保護措施，如 DOS 作業系統

CC安全評估準則

- 共通準則 (Common Criteria；CC) 安全評估，內容涵蓋『加拿大可信賴電腦產品評估準則』(CTCPEC)、『資訊技術安全評估準則』(ITSEC)、以及美國的『可信賴電腦系統評估準則』(TCSEC) 和 『美國聯邦準則』(US Federal Criteria；FC)，如圖。
- CC 共通準則安全評估規範包含三大部分：
  - 簡介及一般模型 (introduction & general model)：敘述資訊技術共通準則，提出整體概念與其各部份的關連性。
  - 功能需求 (functional requirements)：功能需求是描述評估目標的安全性質，這些性質可以由使用者透過與評估目標的直接交談或是觀察評估目標加以偵測。
  - 安全保證需求 (assurance requirements)：介紹安全保證需求、保護分析表、以及安全目標評估標準，定義了七個保證等級。

CC 共通準則的發展歷程



TCSEC: Trusted Common System Evaluation Criteria
ITSEC: Information Technology Security Evaluation Criteria
CTCPEC: Canadian Trusted Computer Product Evaluation Criteria

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

可信賴電腦系統發展

- 可信賴電腦系統的範圍比電腦安全的範圍更廣泛，電腦安全所探討的只是可信賴電腦系統之一部份，如圖可信賴電腦系統的範圍。

- 可信賴電腦系統的發展趨勢有以下幾點：
  - 提升電腦網路環境的安全性，以確保網路資料之安全。
  - 建構一個誠信的電腦系統環境，以及可信賴的電腦處理環境。
  - 具對抗惡意程式的能力，如對後門程式、木馬程式、病毒程式均有防禦能力。
  - 鑑別使用者或網路連線者之身分。
  - 合理舉證、監控與管理意外事件或異常問題。

可信賴電腦系統架構

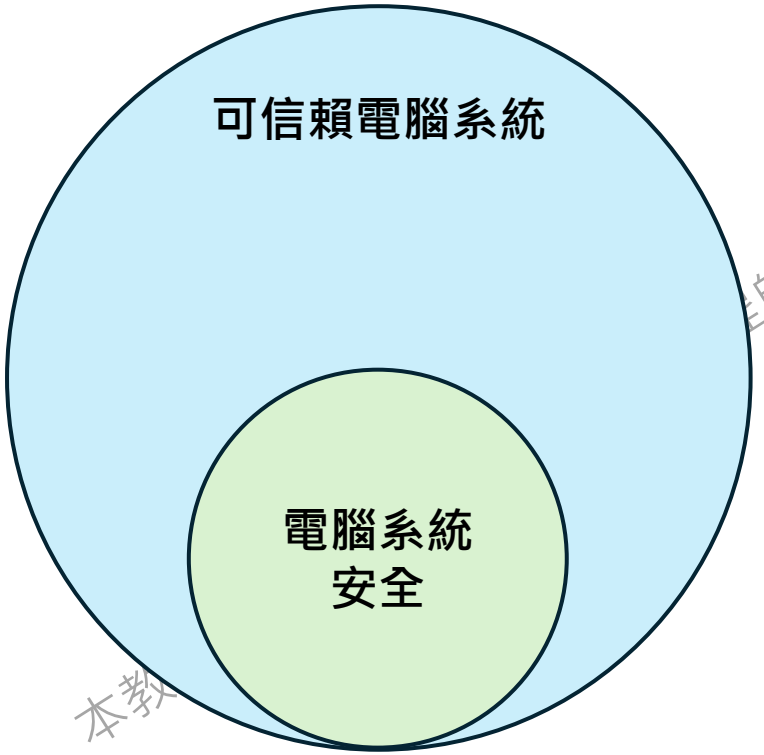


圖 可信賴電腦系統的範圍

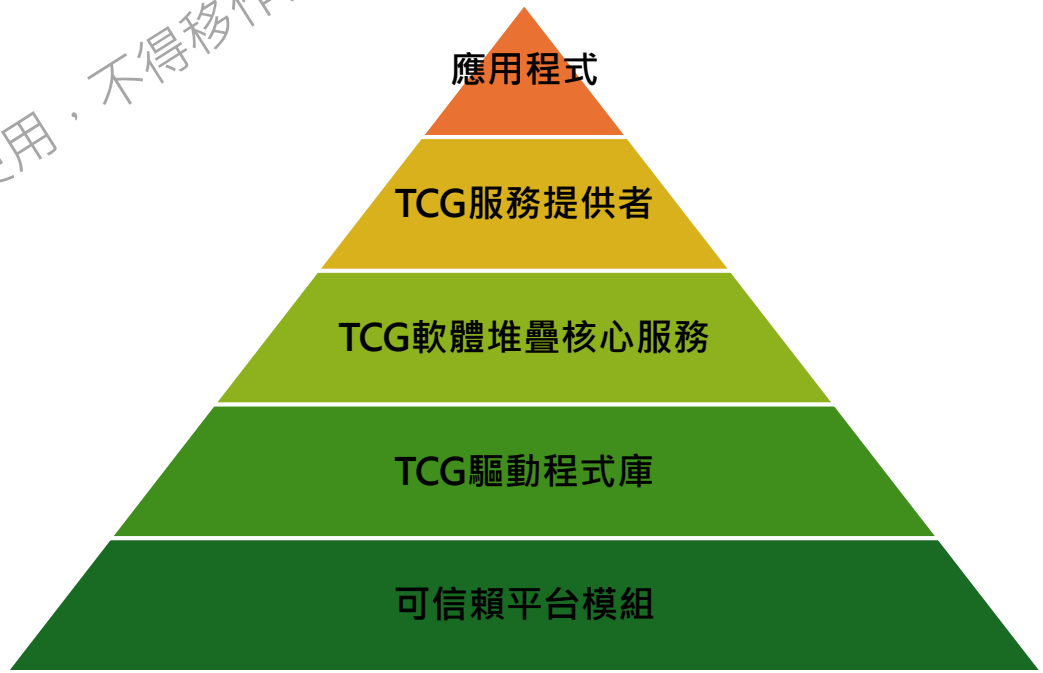


圖 可信賴電腦系統架構

可信賴電腦系統的架構

- TCPA聯盟所制定的TCPA 主規範 (TCPA Main Specification)，定義一個可信賴平台模組 (Trusted Platform Module；TPM)的硬體安全架構標準。
- 可信賴電腦系統的架構，如圖，除最底層的可信賴平台模組外，其上是TCG驅動程式庫，提供標準驅動介面程式模組與軟體界面；再上一層是TCG 軟體堆疊核心服務，提供主要軟體核心服務功能；再上一層 TCG 服務提供者，是標準之功能界面，提供最上層應用程式使用。

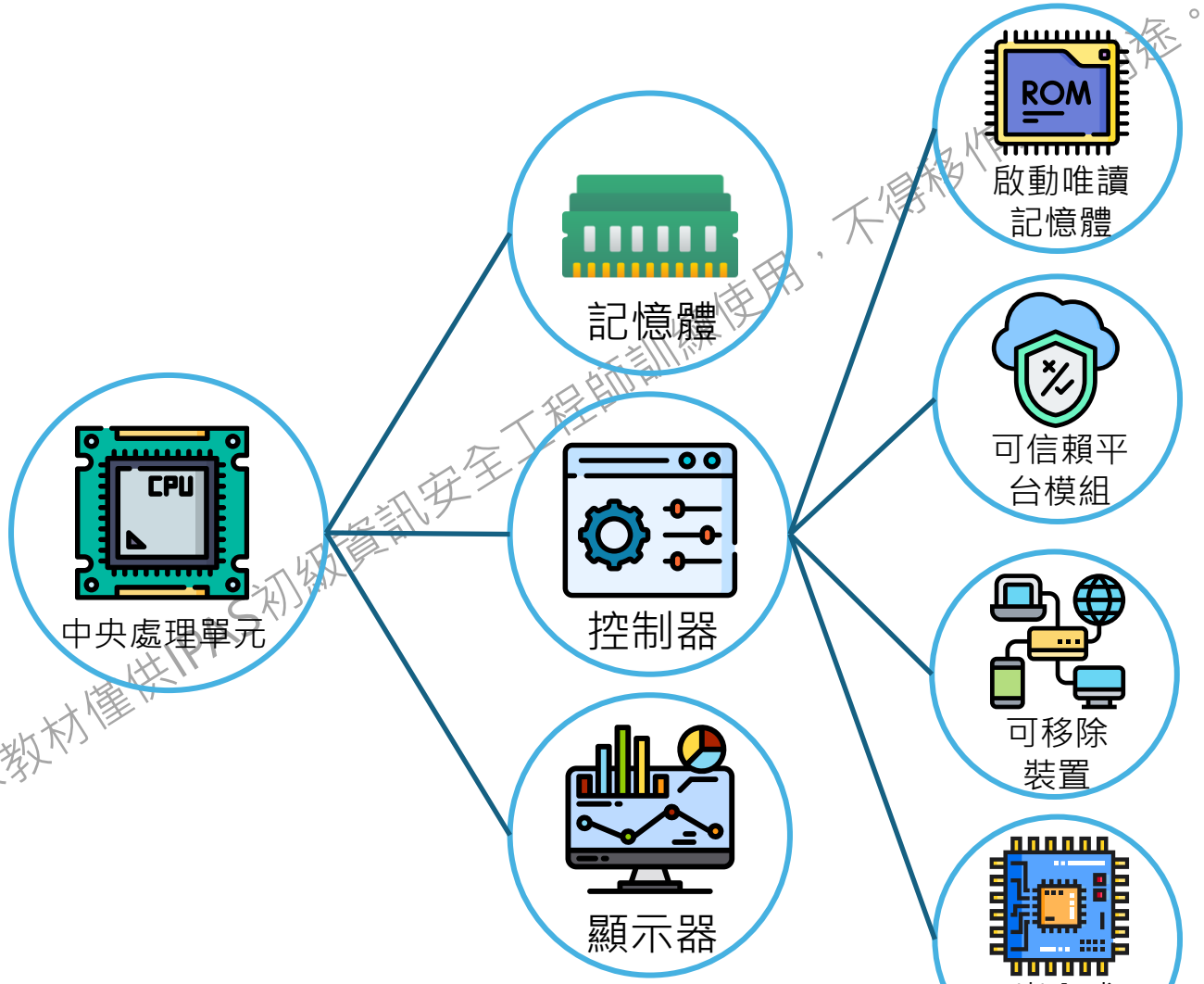
可信賴平台模組

- TCG制定各種規範，以達成可信賴電腦系統的目標，主要有三項機制

- 可信賴平台模組（trusted platform module；TPM）。
- 數位版權管理（digital rights management；DRM）。
- 強制型存取控制（mandatory access control；MAC）。

- 可信賴平台模組提供硬體安全模組並配合軟體使用，其架構如圖6-19可信賴平台模組與電腦周邊。以CPU為核心，控制器控制電腦週邊，記憶體與顯示器則是電腦必備之裝置。Boot ROM為電腦開機時執行之基本程式，放在唯讀記憶體（read-only memory；ROM）；可信賴平台模組，具有安全防護以抵擋攻擊。可移除裝置，是可以移除的各種裝置，並非內建在系統中，系統若無此裝置也不影響系統組態。嵌入式裝置，此裝置之組態完全嵌入在受控制系統之內。

可信賴平台模組與電腦周邊



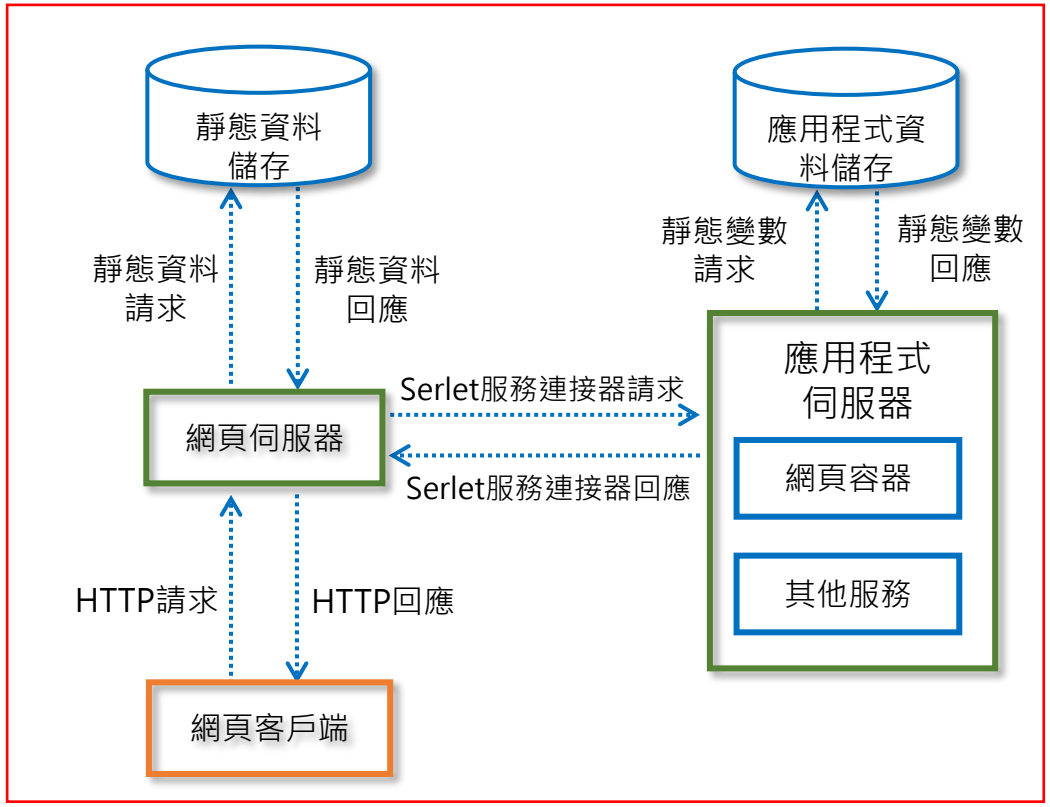
網頁伺服器操作

Web 伺服器是一種資訊系統，它透過 HTTP 儲存、處理和傳送網頁給客戶端

網頁伺服器的組成元素

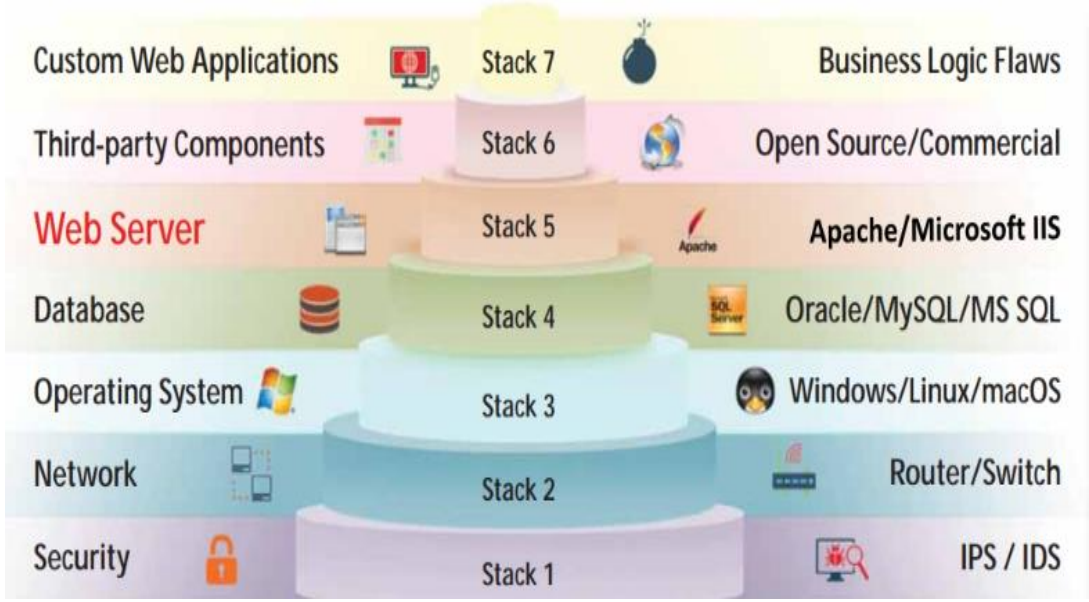
- 檔案根目錄：存儲與將回應請求提供的網域名稱網頁相關的關鍵 HTML檔案
- 根域名稱伺服器：存儲伺服器的設定、錯誤、可執行檔案和日誌檔案
- 虛擬檔案樹：提供原始磁盤寫滿後在不同機器或磁盤上的儲存
- 虛擬機：在同一台伺服器上託管多個域或網站的技術
- 網頁代理伺服器:位於 網頁客戶端和網頁伺服器之間的代理伺服器，用於防止 IP 阻塞並保持匿名

典型的客戶端-伺服器 網頁伺服器操作流程



Web 伺服器安全問題

- 攻擊者通常以軟體漏洞和設定錯誤為目標來破壞 Web 伺服器
- 使用適當的網路安全措施（如防火牆、IDS 等）可以有效地防禦網路和作業系統級別的攻擊。但是，可以透過 Internet 從任何地方存取 Web伺服器，這使得它們極易受到攻擊



Web 伺服器攻擊的影響

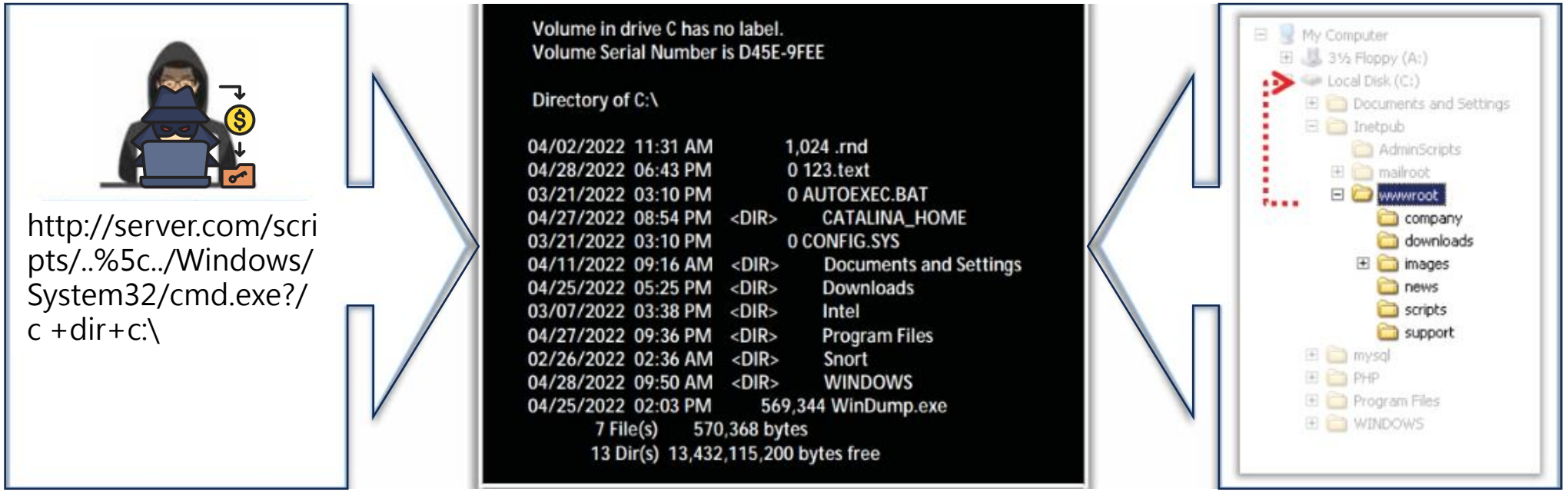
- 使用者帳號的損害
- 網站污損
- 來自網站的二次攻擊
- 對其他應用程式或伺服器的根存取
- 資料篡改和資料竊取
- 公司聲譽受損

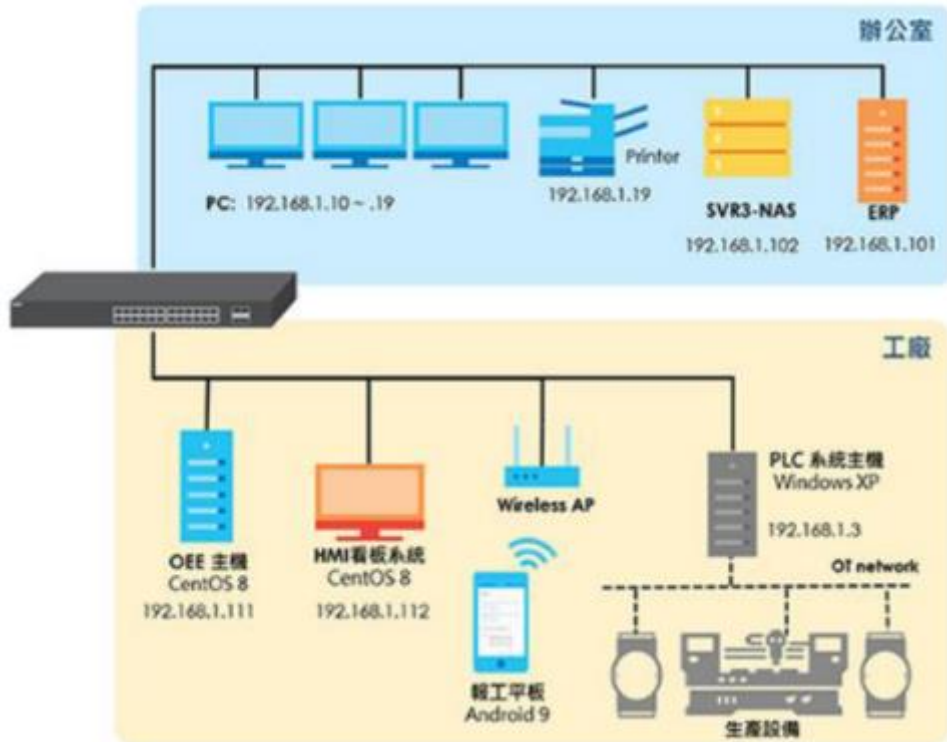
為什麼 Web 伺服器遭受到損害?

- 檔案和目錄權限不當
- 使用預先設置的伺服器安裝
- 啟用不必要的服務，包括內容管理和遠端管理
- 安全與業務易用性衝突
- 缺乏適當的安全政策、程式和維護
- 與外部系統的身份驗證不當
- 具有預設密碼或沒有密碼的預設帳戶
- 不必要的預設、備份或範例檔案
- Web伺服器、作業系統和網路中的錯誤配置
- 伺服器軟體、作業系統和 Web 應用程式中的錯誤
- 配置錯誤的 SSL 憑證和加密設置
- Web 伺服器上啟用或可存取的管理或除錯功能
- 使用自簽名憑證和預設憑證
- 未使用專屬的 Web 伺服器

目錄遍歷攻擊

- 在目錄遍歷攻擊中，攻擊者使用../（點-點-斜線）序列存取網頁伺服器根目錄之外的受限目錄
- 攻擊者可以使用嘗試錯誤法(trial and error)導航到根目錄之外，存取系統中的敏感資訊




辦公室
PC: 192.168.1.10 ~ .19
Printer
192.168.1.19
SVR3-NAS
192.168.1.102
ERP
192.168.1.101
工廠
OEE 主機
CentOS 8
192.168.1.111
HMI看板系統
CentOS 8
192.168.1.112
Wireless AP
PLC 系統主機
Windows XP
192.168.1.3
OT network
報工平板
Android 9
生產設備

數位鑑識實務

https://www.youtube.com/watch?v=J5fSpWBj1No&t=86s

數位鑑識

- 透過一系列的數位鑑識流程，可還原駭客活動軌跡
  - 了解駭客到底如何入侵，入侵後做什麼事情，打包哪些資料，如何擴散等
  - 受害單位也可了解到如何改善其架構，以防駭客再次透過相似手法入侵

NTFS系統架構(1/5)

- 基本上所有Windows的硬碟格式都是NTFS
- 一雖然Windows有支援ex FAT、ReFS格式但相對少見
- -NTFS是非常成熟的硬碟格式，提供多樣功能與紀錄
- NTFS規格相關紀錄

NTFS files

File	Name	$MFT record #	Description
$Mft	Master File Table	0	Contains one base file record for each file and folder on an NTFS volume. If the allocation information for a file or folder is too large to fit within a single record, other file records are allocated as well.
$MftMirr	MFT mirror	1	Guarantees access to the MFT in case of a single-sector failure. It is a duplicate image of the first four records of the MFT.
$LogFile	Log file	2	Contains information used by NTFS for faster recoverability. The log file is used by Windows Server 2003 to restore metadata consistency to NTFS after a system failure. The size of the log file depends on the size of the volume, but you can increase the size of the log file by using the Chkdsk command.
$Volume	Volume	3	Contains information about the volume, such as the volume label and the volume version.
$AttrDef	Attribute definitions	4	Lists attribute names, numbers, and descriptions.
.	Root file name index	5	The
$Bitmap	Cluster bitmap	6	Represents the volume by showing free and unused clusters.
$Boot	Boot sector	7	Includes the BPB used to mount the volume and additional bootstrap loader code used if the volume is bootable.
$BadClus	Bad cluster file	8	Contains bad clusters for a volume.
$Secure	Security File	9	Contains unique security descriptors for all files within a volume.
$Upcase	Upcase table	10	Converts lowercase characters to matching Unicode uppercase characters.
$Extend	NTFS extension file	11	Used for various optional extensions such as quotas, reparse point data, and object identifiers.
		12-15	Reserved for future use.

source: http://technet.microsoft.com/en-us/library/cc781134(WS.10).aspx

NTFS系統架構(2/5)

- 在所有紀錄中，最重要的是$MFT紀錄
- 一該紀錄會標示每個檔案的詳細資訊，例如檔名、內容、時間等
- MFT紀錄

Some $MFT entry attributes

ID	Attribute Type	Description
0x10	Standard Information	Includes information such as time stamp and link count.
0x20	Attribute List	Lists the location of all the attribute records that do not fit in the MFT record.
0x30	File Name	A repeatable attribute for both long and short file names. The long name of the file can be up to 255 Unicode characters. The short name is the MS-DOS-readable, 8.3, case-insensitive name for the file. Additional names, or hard links, required by POSIX can be included as additional file name attributes.
0x40	Object ID	A volume-unique file identifier. Used by the link tracking service. Not all files have object identifiers.
0x50	Security Descriptor	Shows information about who owns the file and who can access the file.
0x60	Volume Name	Used only in the $Volume system file. Contains the volume label.
0x70	Volume Information	Used only in the $Volume system file. Contains the volume version.
0x80	Data	Contains file data. NTFS allows multiple data attributes per file. Each file typically has one unnamed data attribute. A file can also have one or more named data attributes, each using a particular syntax.
0x90	Index Root	Used to implement folders and other indexes.
0xA0	Index Allocation	Used to implement folders and other indexes.
0xB0	Bitmap	Used to implement folders and other indexes.
0xC0	Reparse Point	Used for directory junction points and volume mount points. They are also used by file system filter drivers to mark certain files as special to that driver.
0x100	Logged Tool Stream	Similar to a data stream, but operations on a logged tool stream are logged to the NTFS log file just like NTFS metadata changes. Used by EFS.

NTFS系統架構(3/5)

- 在$MFT中， 有兩個欄位會帶有檔案相關時間
  - Standard Information(SI)欄位會記錄一組(4個)時間，我們經常看到的時間即Standard Information Time
  - 4個時間分別為
    - Creation Time
    - Last Write Time
    - Last Access Time
    - Metadata Time (隱藏欄位)

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

NTFS系統架構(4/5)

- 在$MFT中，有兩個欄位會帶有檔案相關時間
  - File Name(FN)欄位會記錄另一組(4個)時間，但僅能用鑑識工具進行檢視
  - 4個時間分別為
    - Creation Time (隱藏欄位)
    - Last Write Time (隱藏欄位)
    - Last Access Time (隱藏欄位)
    - Metadata Time (隱藏欄位)

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

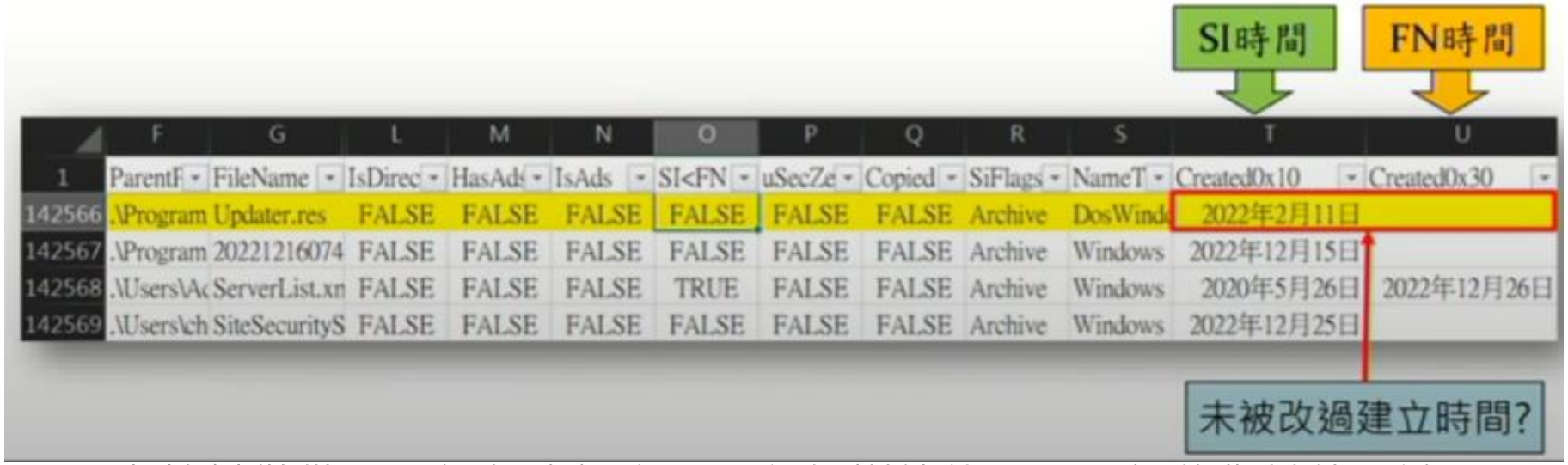
NTFS系統架構(5/5)

- 若要針對檔案時間進行調整，僅能修改Standard Information Time,無法修改File Name Time
  - 使用者可用指令/API輕易修改Standard Information Time
  - 無法修改File Name Time之原因為沒有可用API，修改File Name Time之API 不但為未公開API，使用時更會被微軟的Patch Guard機制擋下
    - 若繞過Patch Guard的保護，等於可以直接控制Windows Kernel，難度非常高，
    - 因此過往的迷思，都是FN無法修改。僅有SI可以修改

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

駭客手法分析與實證(1/9)

- 在本案發現駭客似乎可以修改File Name Time一我們使用鑑識工具對硬碟中$MFT進行分析，竟然發現該惡意程式的Standard Information Time和File Name Time是一樣的，該工具若未顯示FN時間，則代表此檔案的FN時間和SI時間相同，惡意程式為黃色，明顯可看出FN時間和SI時間相同。即未被改過建立時間



駭客手法分析與實證(2/9)

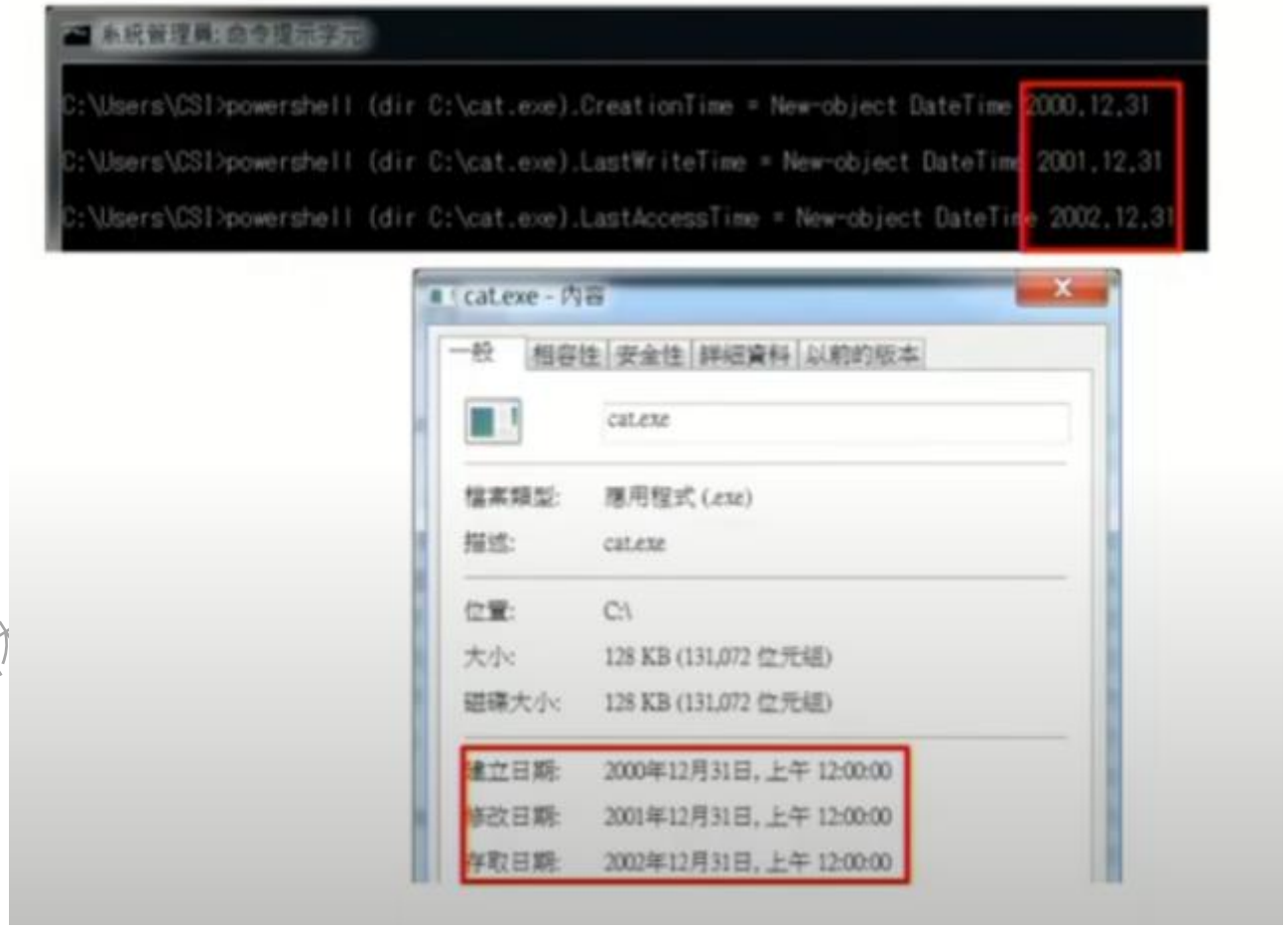
- 我們在分析該惡意程式相關時間，意外發現該程式Standard Information中的Metadata Time很接近正確的植入時間—該程式為12/14~12/26間植入，8個時間中僅有Metadata Time符合此時段

駭客手法分析與實證(3/9)

- 因此我們於實驗環境對此進行實測
  - 隨意準備一個檔案，其時間如下

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

駭客手法分析與實證(4/9)



駭客手法分析與實證(6/9)

- 透過鑑識工具分析MFT的內容，發現僅有Standard Information(SI)的時間改動，而File Name(FN)的時間未改動
  - MFT紀錄之時間均為UTC，故需+8小時始為當前時區

駭客手法分析與實證(6/9)

- 經查SANS公布有關檔案時間之鑑識研究，可知不會更動到SI中3個時間之行為僅有檔案更名與同磁碟區**檔案移動**兩種
- Windows time rules

駭客手法分析與實證(7/9)

- 接著進行檔名變更，Standard Information的Meta data Time會變成修改檔名的時間
  - 同時因為檔名調整的影響，會發現所有的File Name時間均變成其對應的Standard Information時間

駭客手法分析與實證(8/9)

- 由以上實驗可知，駭客修改檔案時間之流程推測如下步驟
- 透過工具**修改**檔案**S1的3個時間**(不包含metadata time)或**4個時間**(包含metadata time)
- 將檔案**更名或移動**
- 再度**修改**檔案**SI的metadata time**，以達成所有SI和FN時間都是駭客想要的內容
- 本案的駭客可能是忘了進行動作3，所以才會有SI的metadata time 與其他時間不同之情形

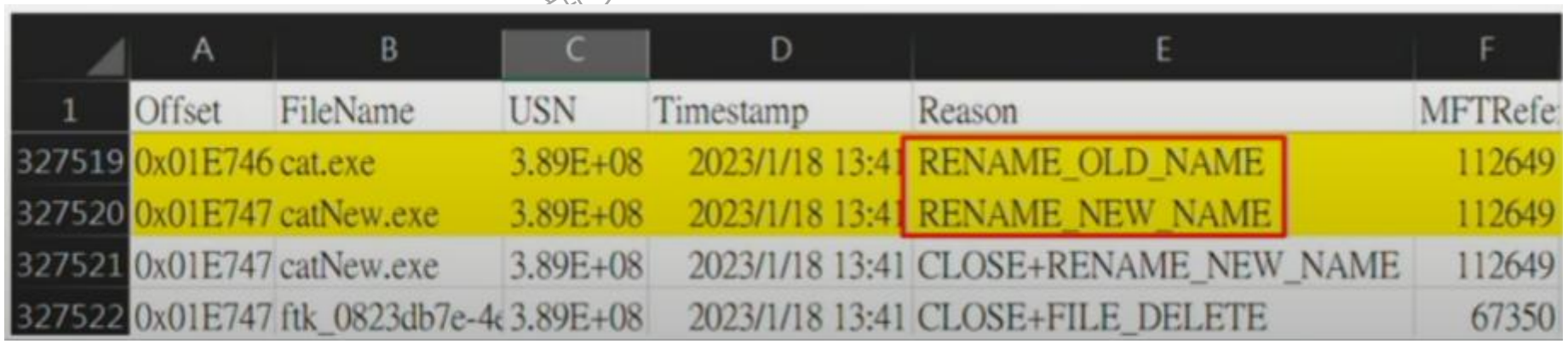
本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

駭客手法分析與實證(9/9)

- SANS新版之檔案操作時間對應表已於今年調整

偵測方式(1/2)

- 由於NTFS檔案格式具有許多日誌紀錄，我們可以透過查找其他日誌了解駭客是否使用前述反鑑識手法
  - 分析NTFS的$Extend\$UsnJrnl日誌，可以知道檔案是否有改名/改路徑的紀錄
  - 但該日誌紀錄的東西較多，通常僅能保存1日，之後便會覆蓋舊有紀錄



	A	B	C	D	E	F
1	Offset	FileName	USN	Timestamp	Reason	MFTRefe
327519	0x01E746	cat.exe	3.89E+08	2023/1/18 13:41	RENAME_OLD_NAME	112649
327520	0x01E747	catNew.exe	3.89E+08	2023/1/18 13:41	RENAME_NEW_NAME	112649
327521	0x01E747	catNew.exe	3.89E+08	2023/1/18 13:41	CLOSE+RENAME_NEW_NAME	112649
327522	0x01E747	ftk_0823db7e-4(	3.89E+08	2023/1/18 13:41	CLOSE+FILE_DELETE	67350

偵測方式(2/2)

- 由於NTFS檔案格式具有許多日誌紀錄，我們可以透過查找其他日誌了解駭客是否使用前述反鑑識手法
  - 分析NTFS的$Extend\$LogFile日誌，可以知道檔案的FN time修改前後之紀錄
  - 但該日誌紀錄的東西過多，通常僅能保存數小時，之後便會覆蓋舊有紀錄

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

結論

- 不只我們懂得做數位鑑識，組織型駭客也很了解這個領域_駭客知道要如何修改跡證以防被我們還原其入侵軌跡
- 過往的知識可能並不是永遠正確
- 一不是FN Time不能修改，只是沒有API可以修改，但駭客可以不透過API修改時間
- 近期有部分組織型駭客開始透過此法修改檔案時間進而干擾跡證分析
- 駭客若操作沒有依照SOP完成所有步驟，就有可能留下痕跡可供分析
- 雖可透過$UsnJrnl。和$LogFile偵測該手法利用之可能性，但相關日誌保存時間均十分短暫，一旦人侵時間較長即難以找出實際遭駭時間

網路威脅比較

	威脅	結果	對策
完整性	• 修改使用者資料 • 木馬瀏覽器 • 修改記憶體 • 修改傳輸中的訊息流量	• 資訊遺失 • 入侵機器 • 對所有其他威脅的脆弱性	加密校驗和
保密性	• 竊聽網路 • 從伺服器竊取資訊 • 竊取客戶資料 • 有關網路設定的資訊 • 有關客戶端與伺服器間對話資訊	• 資訊遺失 • 洩漏隱私	加密、 網頁代理伺服器
阻絕服務	• 抹殺使用者執行緒 • 使用假冒請求洪泛機器 • 填滿磁碟或記憶體 • 透過 DNS 攻擊隔離機器	• 破壞性的 • 惱人的 • 阻止使用者完成工作	難以預防
驗證	• 冒充合法使用者 • 資料偽造	• 使用者的虛假陳述 • 相信偽造資訊有效	密碼技術

William Stallings (2017). CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE. SEVENTH EDITION. GLOBAL EDITION.

A Comparison of Threats on the Web

	Threats	Consequences	Countermeasures
Integrity	• Modification of user data • Trojan horse browser • Modification of memory • Modification of message traffic in transit	• Loss of information • Compromise of machine • Vulnerability to all other threats	Cryptographic checksums
Confidentiality	• Eavesdropping on the net • Theft of info from server • Theft of data from client • Info about network configuration • Info about which client talks to server	• Loss of information • Loss of privacy	Encryption, Web proxies
Denial of Service	• Killing of user threads • Flooding machine with bogus requests • Filling up disk or memory • Isolating machine by DNS attacks	• Disruptive • Annoying • Prevent user from getting work done	Difficult to prevent
Authentication	• Impersonation of legitimate users • Data forgery	• Misrepresentation of user • Belief that false information is valid	Cryptographic techniques

William Stallings (2017). CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE. SEVENTH EDITION. GLOBAL EDITION.

一些潛在的攻擊、易受攻擊的驗證器和典型的防禦

攻擊	驗證器	範例	典型的防禦
客戶端攻擊	密碼	猜測、窮舉搜索	熵很大、有限的嘗試
	權杖	窮舉搜索	熵很大、有限的嘗試、盜竊物品，需要到現場
	生物識別	錯誤匹配	熵很大、有限的嘗試
主機攻擊	密碼	明文竊取、字典/窮舉搜索	雜湊、熵很大、密碼資料庫的保護
	權杖	密碼被盜	與密碼相同、1次性密碼
	生物識別	模板盜竊	擷取裝置、身份驗證、挑戰回應
竊聽、、盜竊以及複製	密碼	“肩窺”	使用者盡力保守秘密、管理員努力快速撤銷洩漏的密碼、多因子身份驗證
	權杖	竊盜、偽造 硬體	多因子身份驗證； 防篡改/明顯的權杖
	生物識別	複製（欺騙）生物特徵識別	擷取設備上的複製檢測和擷取設備身份驗證

註：熵是一個科學概念，通常與沒有次序、隨機或不確定狀態有關。熵（資訊理論），也稱為Shannon熵，是對資訊來源的不可預測性或資訊內容的度量

一些潛在的攻擊、易受攻擊的驗證器和典型的防禦

攻擊	驗證器	範例	典型的防禦
重送	密碼	重送被竊密碼回應	挑戰-回應協定
	權杖	重送被竊密碼回應	挑戰-回應協定；1次性密碼
	生物識別	重送被竊生物識別樣版回應	透挑戰-回應協定擷取設備上的複製檢測和擷取設備身份驗證
特洛伊木馬	**密碼**、權杖、生物識別	安裝惡意使用者端或擷取設備	對可信任安全範圍內的使用者端或擷取裝置進行身份驗證
阻絕馬	**密碼**、權杖、生物識別	多次驗證失敗而鎖定	帶令牌的多因子驗證

William Stallings (2017). CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE. SEVENTH EDITION. GLOBAL EDITION.

Some Potential Attacks, Susceptible Authenticators, and Typical Defenses

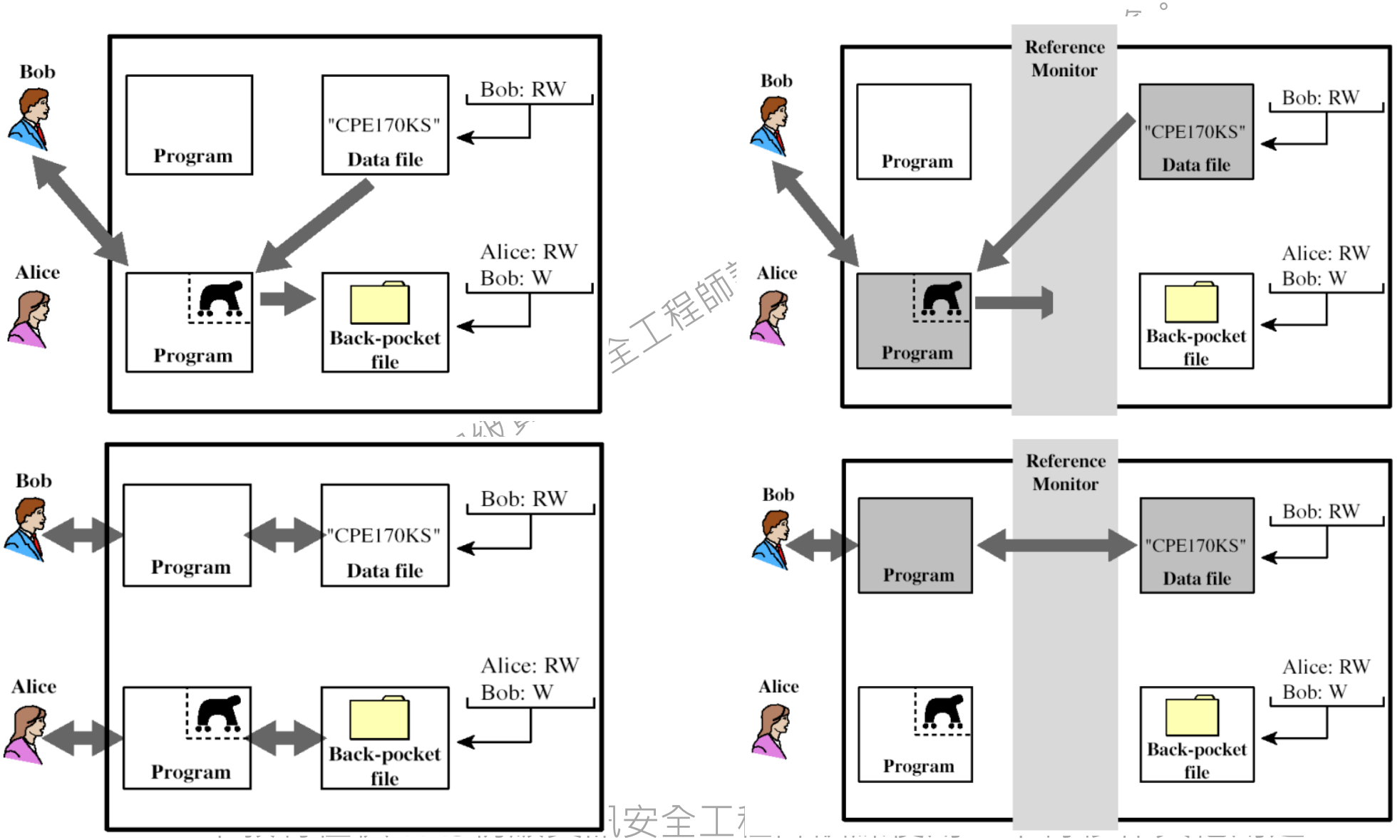
Attacks	Authenticators	Examples	Typical Defenses
Client attack	Password	Guessing, exhaustive search	Large entropy; limited attempts
	Token	Exhaustive search	Large entropy; limited attempts; theft of object, requires presence
	Biometric	False match	Large entropy; limited attempts
Host attack	Password	Plaintext theft, dictionary/exhaustive search	Hashing; large entropy; protection of password database
	Token	Passcode theft	Same as password; 1-time passcode
	Biometric	Template theft	Capture device, authentication; challenge response
Eavesdropping, theft, and copying	Password	"Shoulder surfing"	User diligence to keep secret; administrator diligence to quickly revoke compromised passwords; multifactor authentication
	Token	Theft, counterfeiting hardware	Multifactor authentication; tamper resistant/evident token
	Biometric	Copying (spoofing) biometric	Copy detection at capture device and capture device authentication

William Stallings (2017). CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE. SEVENTH EDITION. GLOBAL EDITION.

Some Potential Attacks, Susceptible Authenticators, and Typical Defenses

Attacks	Authenticators	Examples	Typical Defenses
Replay	Password	Replay stolen password response	Challenge-response protocol
	Token	Replay stolen passcode response	Challenge-response protocol; 1-time passcode
	Biometric	Replay stolen biometric template response	Copy detection at capture device and capture device authentication via challenge-response protocol
Trojan horse	Password, token, biometric	Installation of rogue client or capture device	Authentication of the client or capture device within the trusted security perimeter
Denial horse	Password, token, biometric	Lockout by multiple failed authentications	Multifactor with token

防止木馬竊取資訊


Bob
Alice
Program
"CPE170KS"
Data file
Bob: RW
Alice: RW
Bob: W
Program
Back-pocket
file
Reference
Monitor
Bob
Alice
Program
"CPE170KS"
Data file
Bob: RW
Alice: RW
Bob: W
Program
Back-pocket
file
Bob
Alice
Program
"CPE170KS"
Data file
Bob: RW
Alice: RW
Bob: W
Program
Back-pocket
file
Reference
Monitor
Bob
Alice
Program
"CPE170KS"
Data file
Bob: RW
Alice: RW
Bob: W
Program
Back-pocket
file

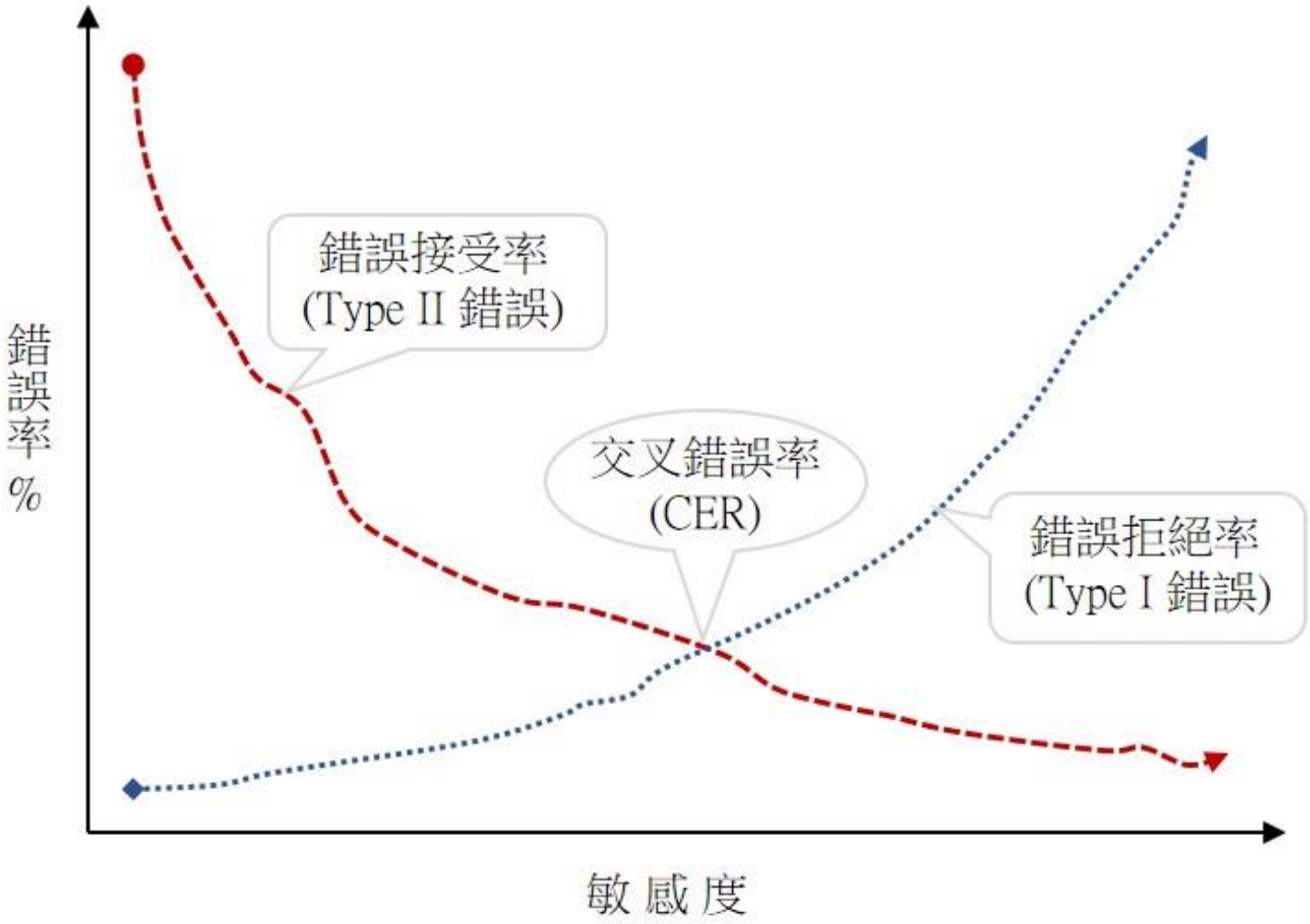
美國電腦倫理協會10條戒律

(1)不應用電腦去傷害別人；
(2)不應干擾別人的電腦工作；
(3)不應窺探別人的文件；
(4)不應用電腦進行偷竊；
(5)不應用電腦作偽證；
(6)不應使用或拷貝沒有付錢的軟體；
(7)不應未經許可使用別人的電腦資源；
(8)不應盜用別人的智力成果；
(9)應該考慮你所編的程式的社會後果；
(10)應該以深思熟慮的方式來使用電腦。

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

機房安全門

敏感度與錯誤率關係圖



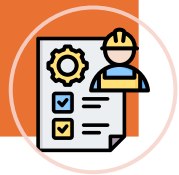
錯誤率

- 原本合法的使用者在認證時卻被判斷為『失敗』，稱為『Type I 錯誤』。所有認證個案中出現『Type I 錯誤』的比率稱為『錯誤拒絕率』(false rejection rate；FRR)。
- 非法使用者被認證為『通過』，稱為 『Type II 錯誤』。所有認證個案中，出現『Type II 錯誤』的比率，稱為『錯誤接受率』(false acceptance rate；FAR)。
- 將設備有效的敏感度調整至錯誤拒絕率與錯誤接受率之交叉點，稱為『交叉錯誤率』(crossover error rate；CER)。

存取控制型式

- 預防型存取控制是要遏止沒有授權的行為發生。

預防型存取控制



- 使用威嚇手段去嚇止違反資安原則之行為，使入侵者了解設施之規範，如果侵入將會有嚴重後果，其目的不是強力去阻止違反資安的行為。

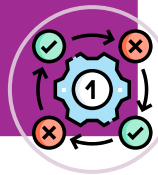
威嚇型存取控制

- 偵查型存取控制的手段是要發現非授權者入侵的證據，一般偵測型存取控制手段用於事實發生後，而不是事情發生當時。

偵查型存取控制

- 矯正型存取控制使用於當系統損害時，修復系統使其恢復正常運作的狀況。

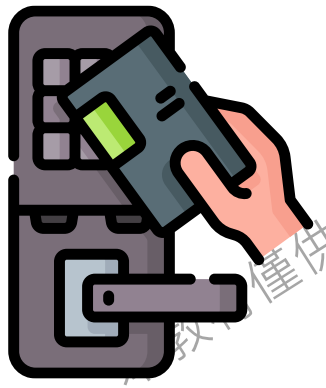
矯正型存取控制



- 回復型存取控制是在系統無法運作時，回復系統之正常功能。

回復型存取控制

門鎖與SSL/TLS 協定之存取控制標語



常見的作業系統與其分類

平台類別	常見的作業系統
個人電腦	Windows、macOS、Chrome OS、Linux (各版本)
行動裝置	iOS、Android、iPadOS、KaiOS、Tizen
伺服器	Unix、Linux (CentOS、Ubuntu)、Windows
嵌入式系統	Linux、Android、Tizen、webOS、FreeBSD FreeRTOS、uC/OS 11、Raspberry Pi

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

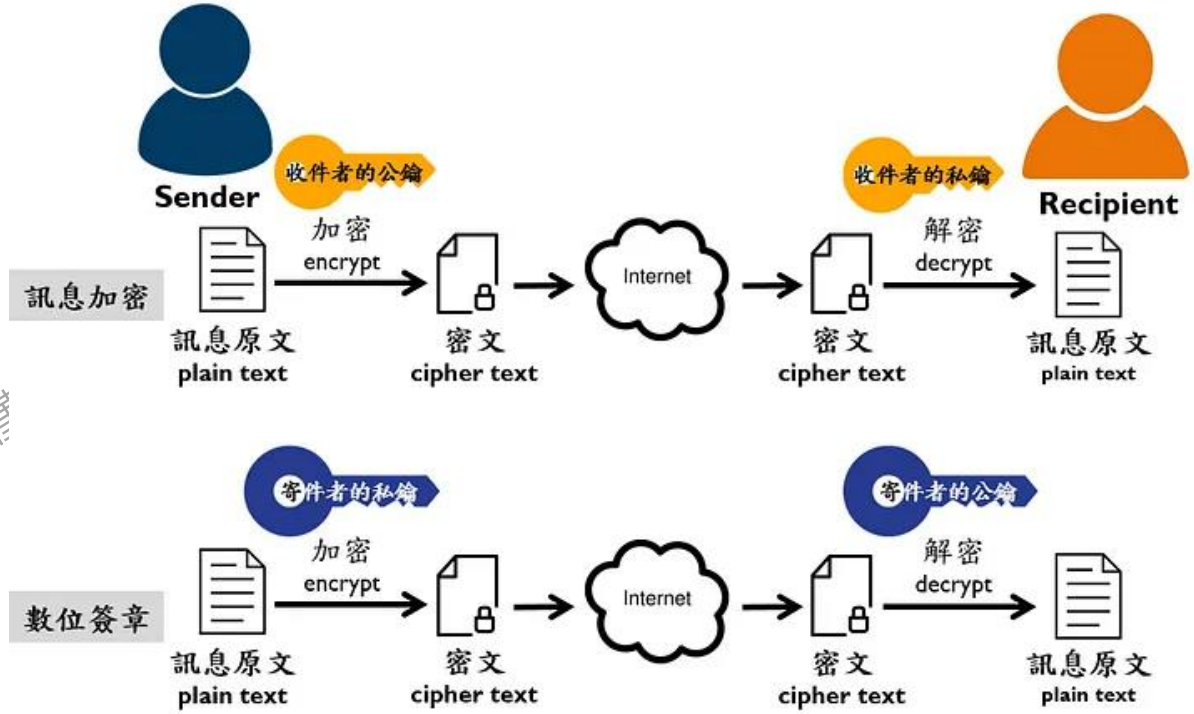
常見瀏覽器及其常用作業系統的對應關係

瀏覽器	支援的作業系統
Google Chrome 	Windows, macOS, Linux, Android, iOS
Mozilla Firefox 	Windows, macOS, Linux, Android, iOS
Safari 	macOS, iOS
Microsoft Edge 	Windows, macOS, Linux, Android, iOS
Opera 	Windows, macOS, Linux, Android, iOS
Brave 	Windows, macOS, Linux, Android, iOS

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

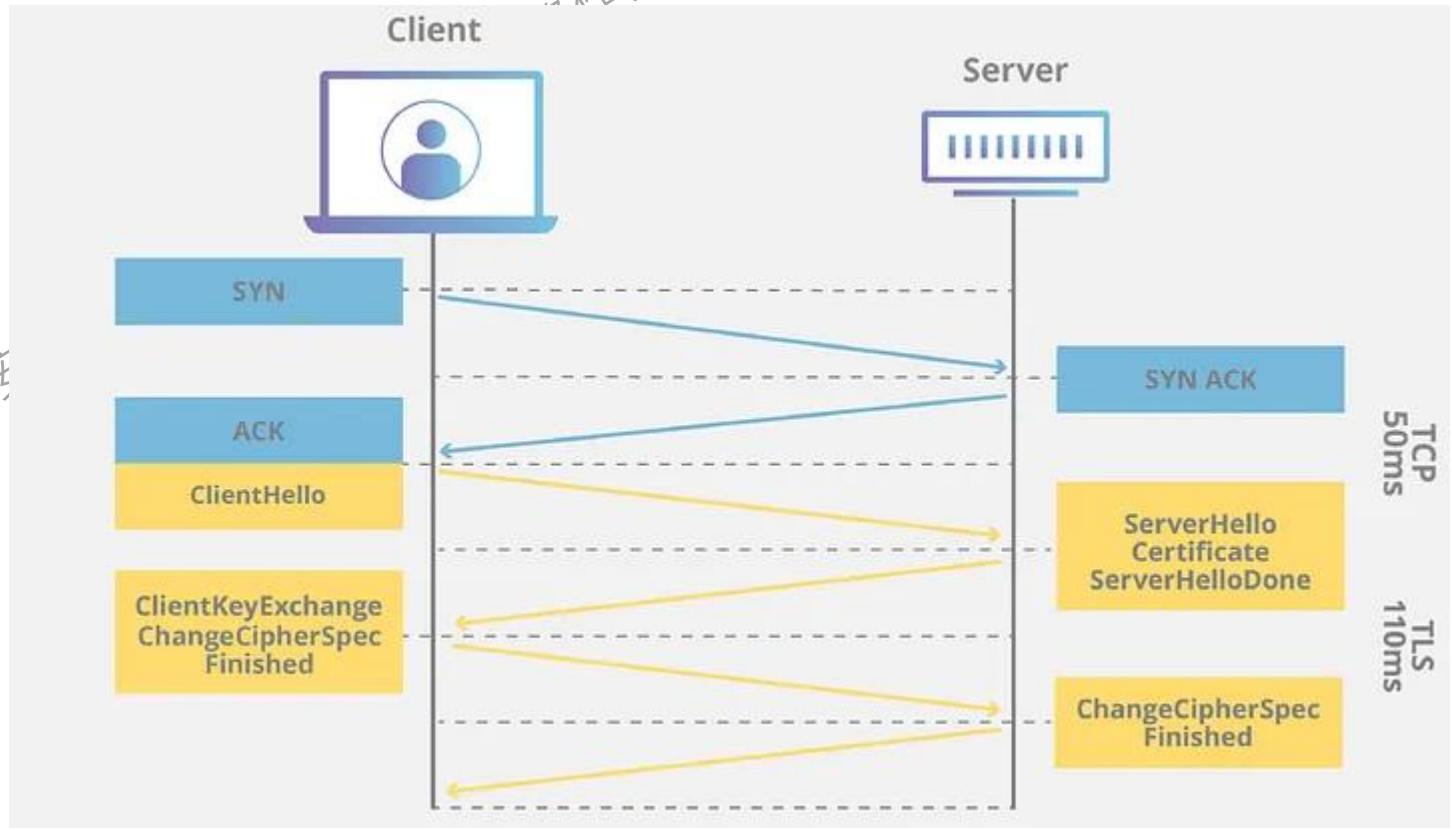
傳輸層安全性協定(SSL/TLS)

- 用於加密、保護和驗證網際網路上的通訊協定。TLS目前廣泛的應用在HTTP連線上，當以「HTTPS」方式連上網站，如果瀏覽器有一個鎖，即代表該網站有支援TLS。加密對稱是 解密非對稱是

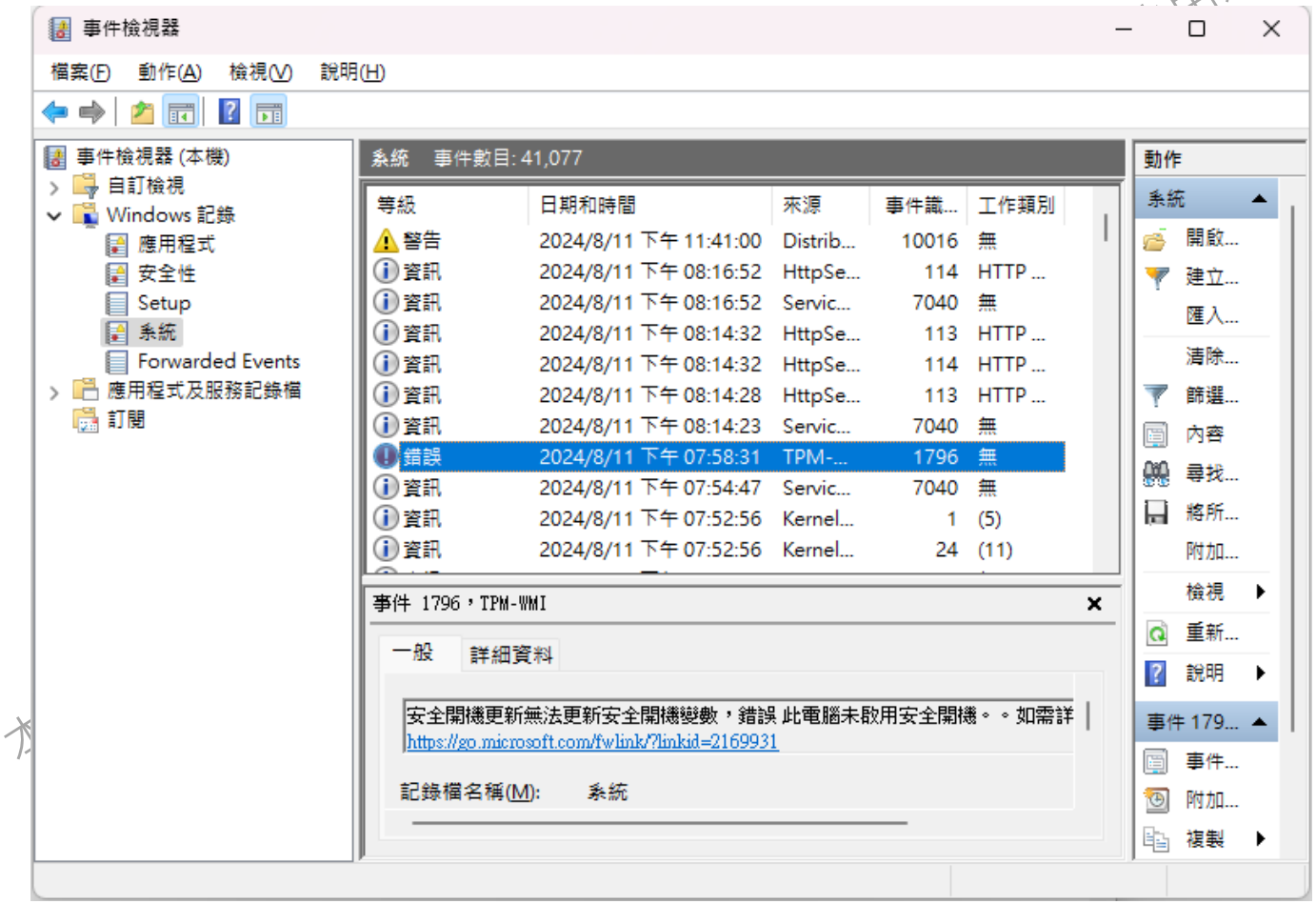


SSL原理

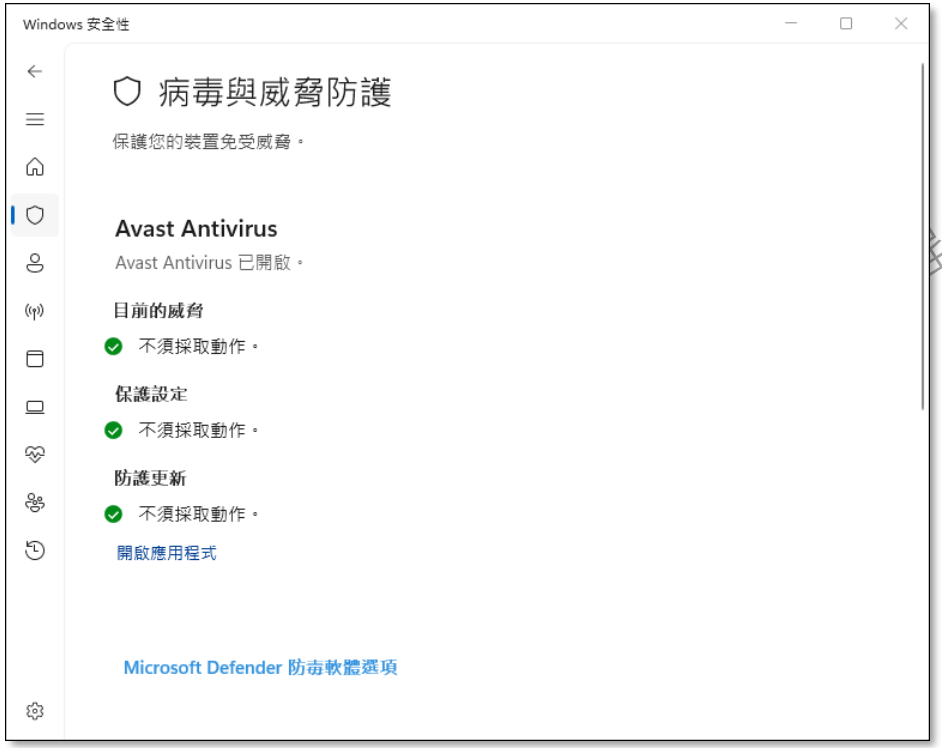
- SSL Handshake
- 在傳輸之前事先用來溝通雙方（client與server）所使用的加密演算法或密鑰交換演算法，或是在伺服器和使用者端之間安全地交換密鑰及雙方的身分認證等相關規則，讓雙方有所遵循，在身分認證方面，SSLHandshake可用來認證伺服器的身分



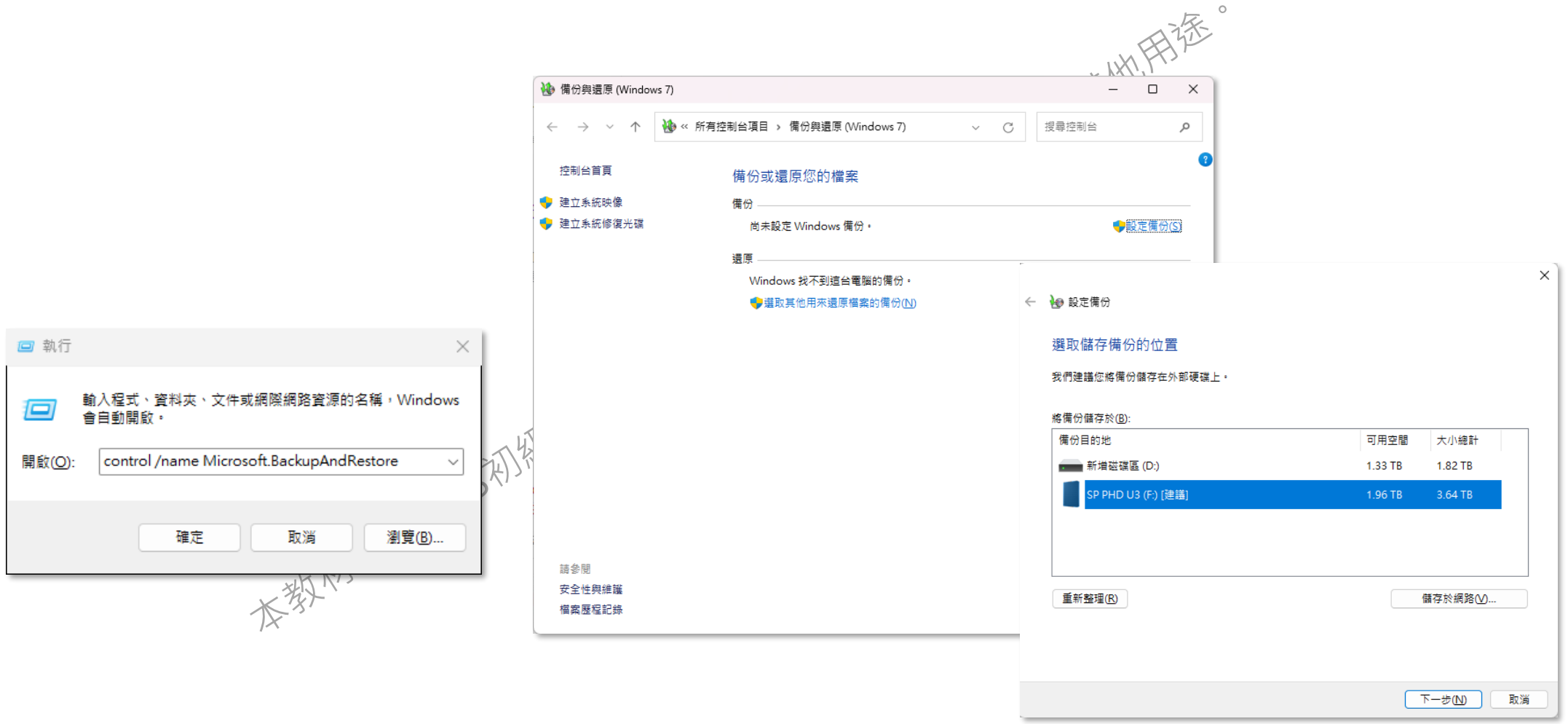
事件稽核紀錄



防毒軟體



Windows 備份與還原工具



透過鍵盤快捷鍵「Windows + R」開啟執行視窗，輸入「control /name Microsoft.BackupAndRestore」後按下確定，會跳出「備份與還原(Windows 11)」程式畫面

存取控制型式 (2/2)

- 補償型存取控制提供另一個存取選擇，或協助現有存取控制，以提高系統安全性，例如，安全政策、人員監督、工作流程等。

補償型存取控制

- 為使系統符合安全政策，依照安全指令作業，並執行安全工作。

指令型存取控制

- 從管理層面執行的存取控制，使各項作業遵循組織的安全政策、安全流程相關的程序。

管理型存取控制

- 從技術層面進行之存取控制，以管理系統資源，防止非法存取資源，技術是指邏輯性技術。

技術型存取控制

- 實體型存取控制是採用實體的障礙，以防止直接接觸系統或設施。例如，警衛、圍牆、籬笆、門鎖、安全窗戶等設施。

實體型存取控制

存取控制題庫1

存取控制（Access Control）決定使用者與作業系統之間的溝通，防止系統資源或資料被未經授權地存取。請問下列何者「不」是存取控制在組織中主要區分的三種操作模式？(1102,26,50)

(A) 強制存取控制（Mandatory Access Control, MAC）

(B) 任意存取控制（Discretionary Access Control, DAC）

(C) 屬性存取控制（Attribute-based Access Control, ABAC）

(D) 角色基準存取控制（Role-based Access Control, RBAC）

答案：(A)

存取控制題庫2

關於存取控制（Access Control），下列敘述何者較「不」正確？(1102,27,50)

(A) 需依據不同角色，賦予不同的資料存取權限 (B) 需依據資料的機密層級不同，去設立存取權限

(C) 將所有存取角色皆設定為共同權限，以方便程式開發操作使用

(D) 記錄所有的存取事件，以便未來追蹤使用

存取控制題庫1

關於系統管理者統一指定使用者對資源之權限存取策略，屬於下列何種安全模式？(1091,31,24)

(A) MAC（Mandatory Access Control）強存取控制

(B) DAC（Discretionary Access Control）自由存取控制

(C) RBAC（Role-Based Access Control）基於角色存取控制

(D) ABAC（Attribute-Based Access Control）基於屬性存取控制

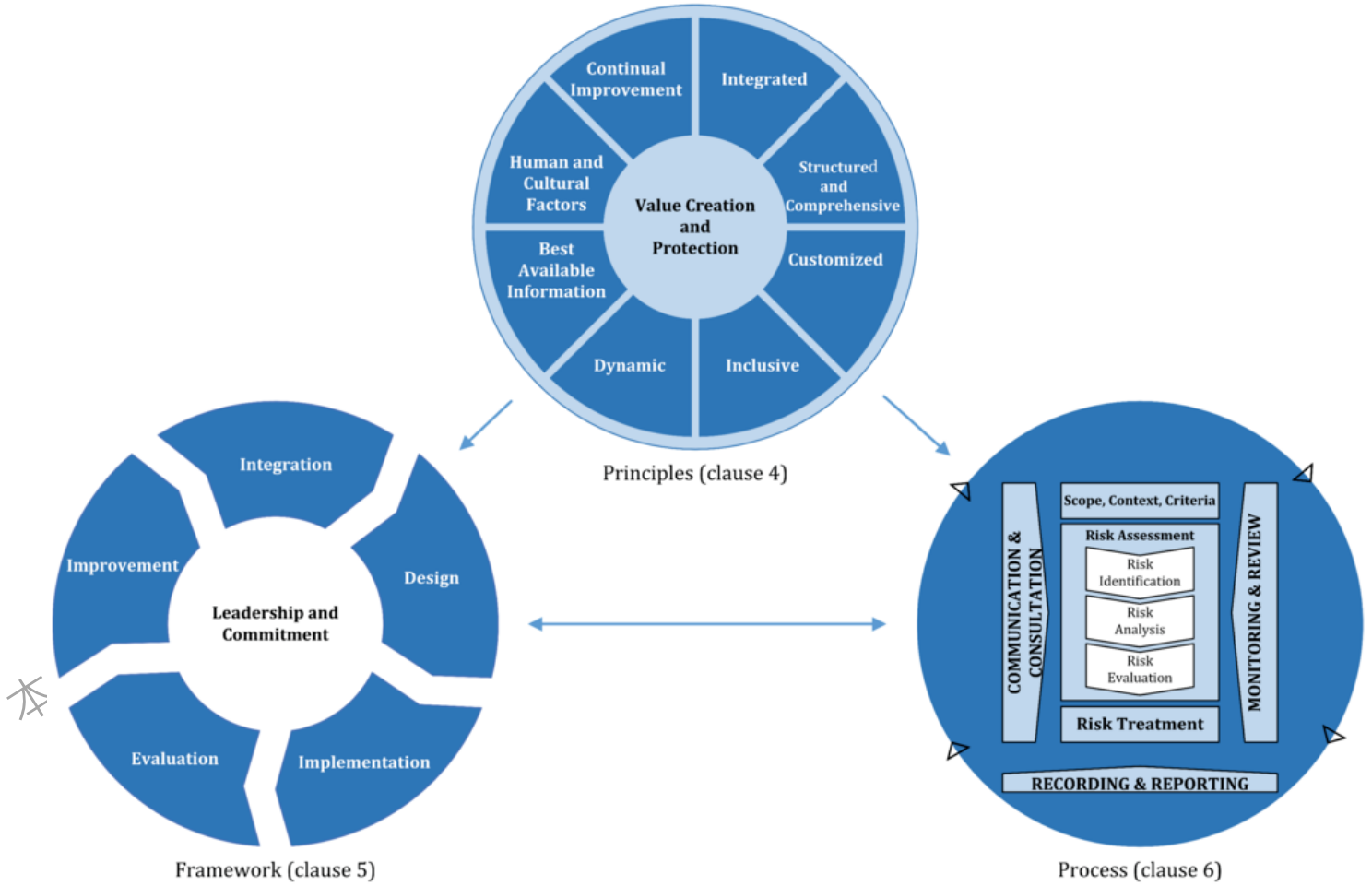
答案：(A)

强制存取控制（MAC）——BIBA模型

- 强制访问控制（MAC）——BIBA模型

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

Principles, framework and process



風險處理題庫

若公司規定超出風險胃納才須進行風險處理，請問依規定須進行處理之風險項目，不可能出現下列何項風險回應方式？

(A) 風險緩解（Risk mitigation）

(B) 風險規避（Risk avoidance）

(C) 風險保留（Risk retention）

(D) 風險分擔（Risk sharing）

答案為 (C) 風險保留（Risk retention）

從題目的描述中公司規定超出風險胃納才須進行風險處理，對風險的認知和做為較為消極，視風險為負向較多，故選項適合(A)(B)(C)任何一項。

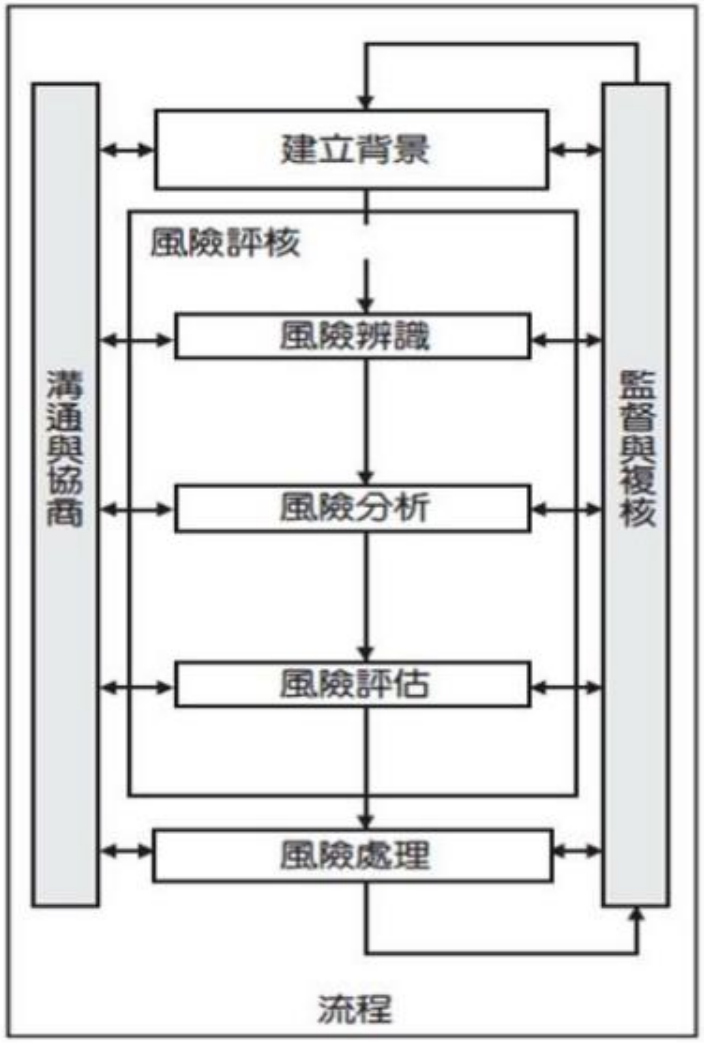
答案(D)風險分擔（Risk sharing）是屬於較正向的風險處理。

建議(D) 風險分擔（Risk sharing）

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

風險處理題庫

- M公司為國內股票上市公司，從事國內資安軟硬體開發銷售相關業務，已追過ISO 27001:2013之驗證，並持續維持證照有效。公司並於每年3月進行年度風險評鑑作業，並規定執行風險回應後最遲須於2個月內確認有效，令年亦以依照預定時程完成相關作業，年亦以依照預定時程完成相關作業。



ISO 30001:2018

3.1風險(risk)

對目標不確定性之效應。

備考1. 效應係與預期之偏離。其可為正向的、負向的或兩者兼具，並且可處理、創造成導致機會與威脅。

6.5.2選擇風險處理選項

選擇最適當的風險處理選項包含相關於達成目標所獲得之潛在利益與實施的成本努力或不利因素間之平衡。

處理風險可能涉及以下1個或多個選項;

藉決定不開始或不繼續會引起風險的活動以規避風險。

承受或增加風險以尋求機會、

移除風險來源。

改變可能性。

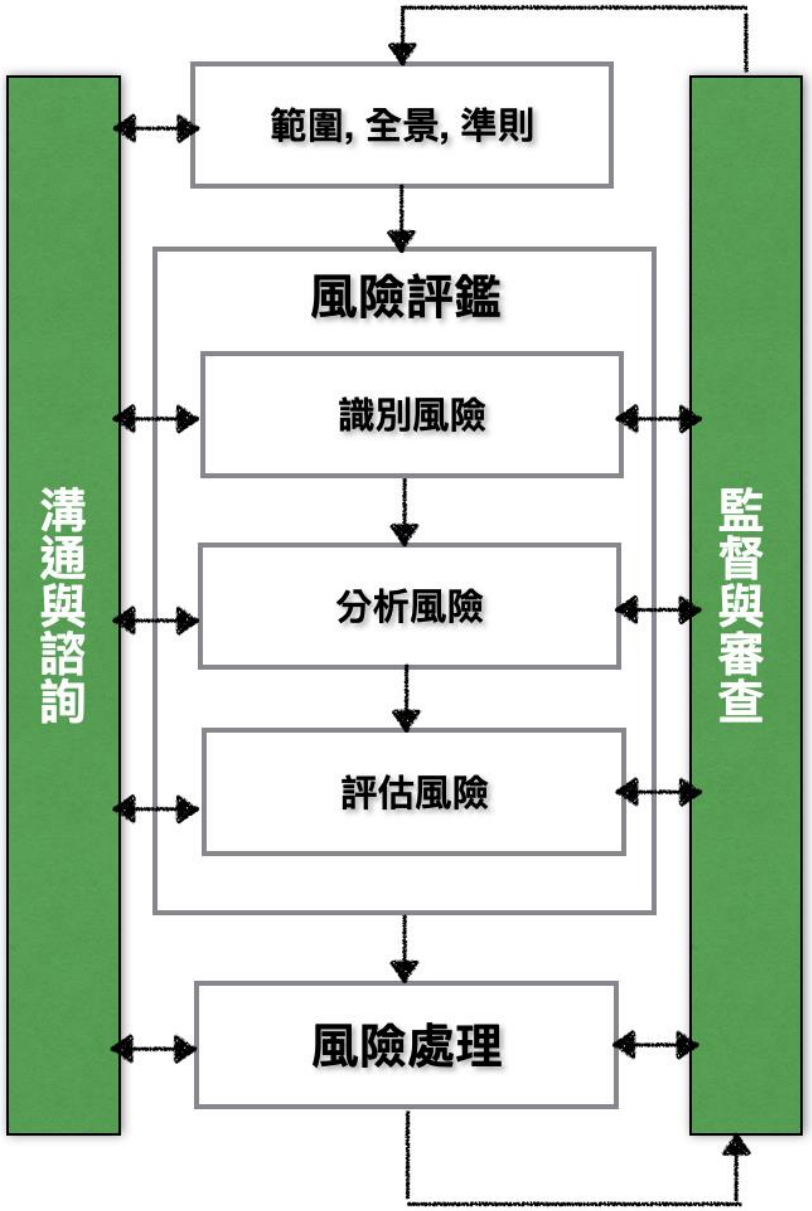
改變後果。

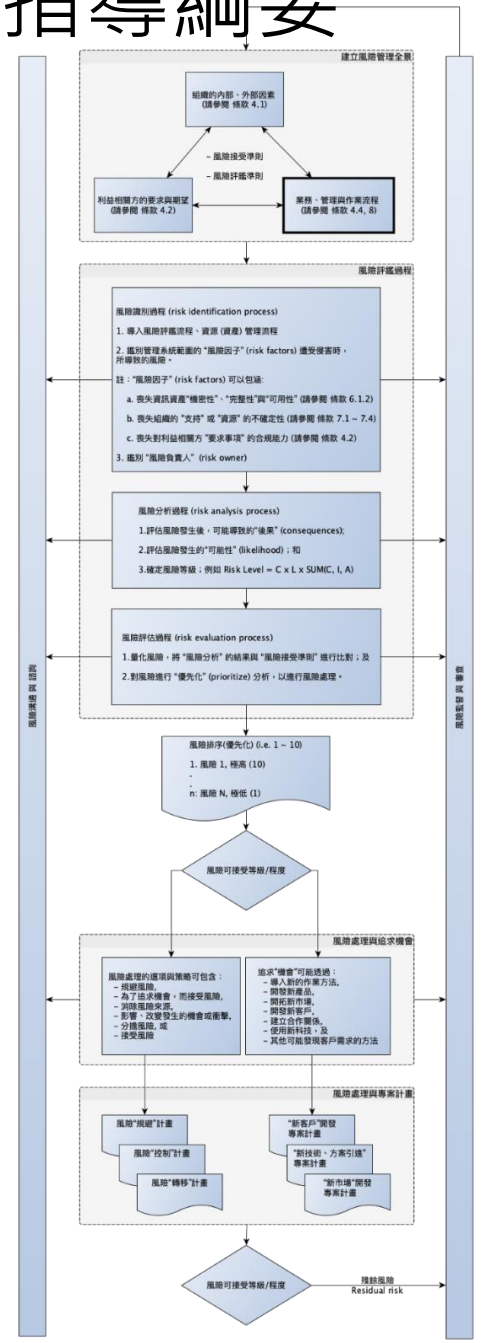
分擔風險(sharing the risk) (例：透過合約、購買保險)。

藉由明智的決定保留既風險。

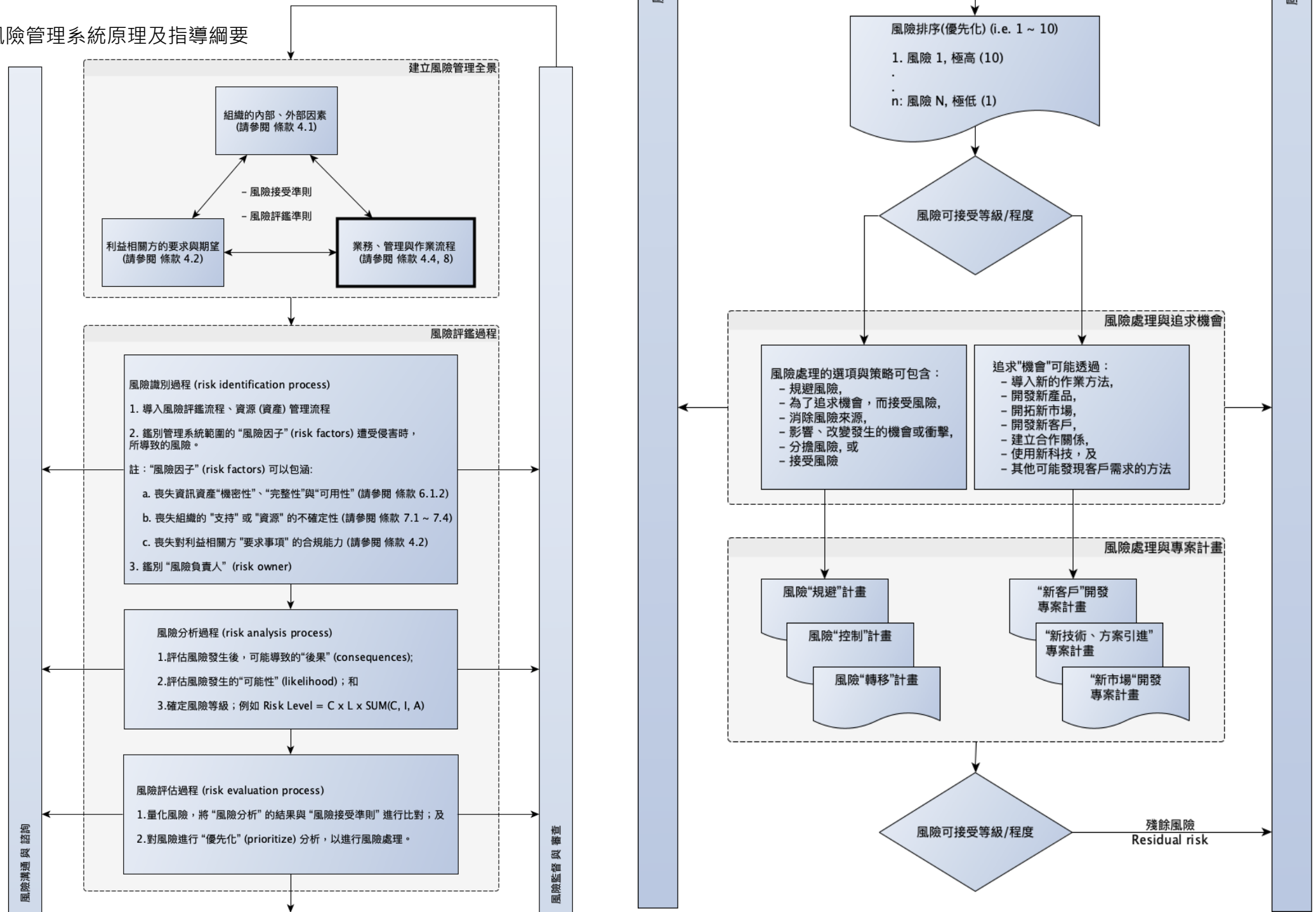
本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。

ISO 31000:2018風險管理系統原理及指導綱要





ISO 31000:2018風險管理系統原理及指導綱要



風險回應規劃

規劃風險回應

負面風險因應策略	正面風險因應策略

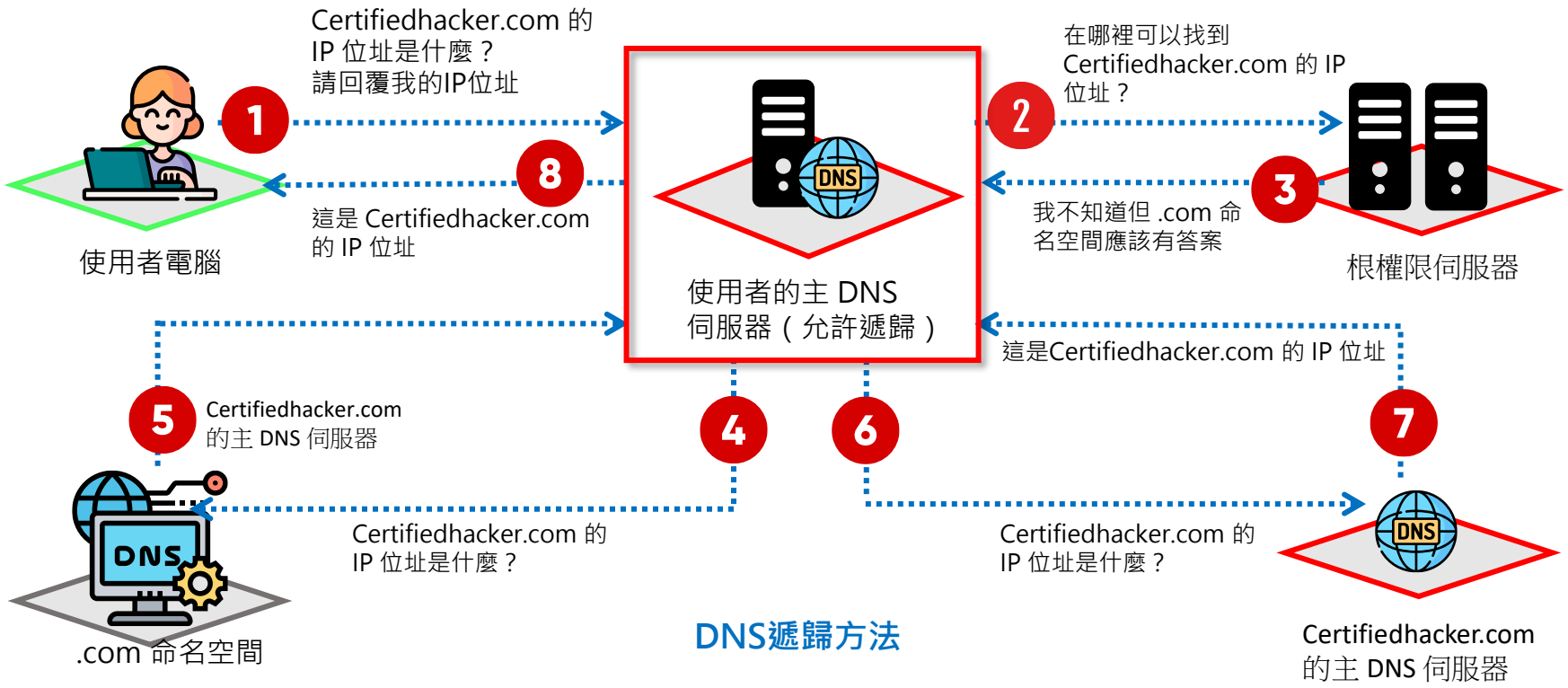
刪除活動 或人員	避免 (消除原因)	原因	利用(開發) (啟用原因)	新增活動 或人員
保險 固定價格 合約	轉移 (第三方責任)	外包	分享 (第三方支援)	投資者 合作
培訓 原型	降低 (降低機率/影響)	機率/影響	提高 (增加機率/影響)	激勵措施

**負面或正面風險
因應策略**

**接受
(沒有可行性的回應)**

DNS放大攻擊

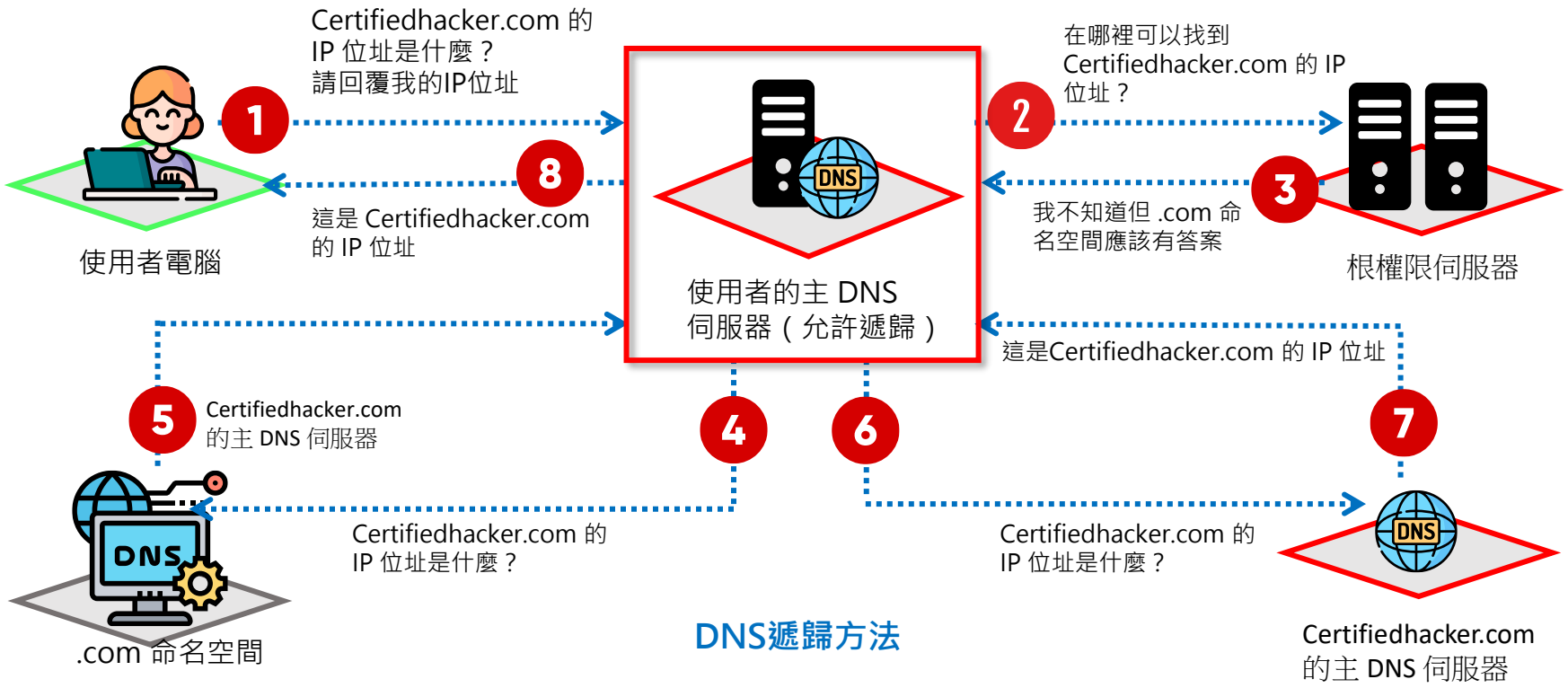
- 攻擊者利用DNS重定向的DNS遞歸方法進行DNS放大攻擊



每個機器人向開放 DNS 解析器提出請求時都提供欺騙性 IP 位址，也就是目標受害者的真實源 IP 位址，目標隨後會收到來自 DNS 解析器的回應。因此，目標接收攻擊者的初始流量的放大結果，其網路被虛假流量堵塞，導致阻斷服務。

DNS放大攻擊

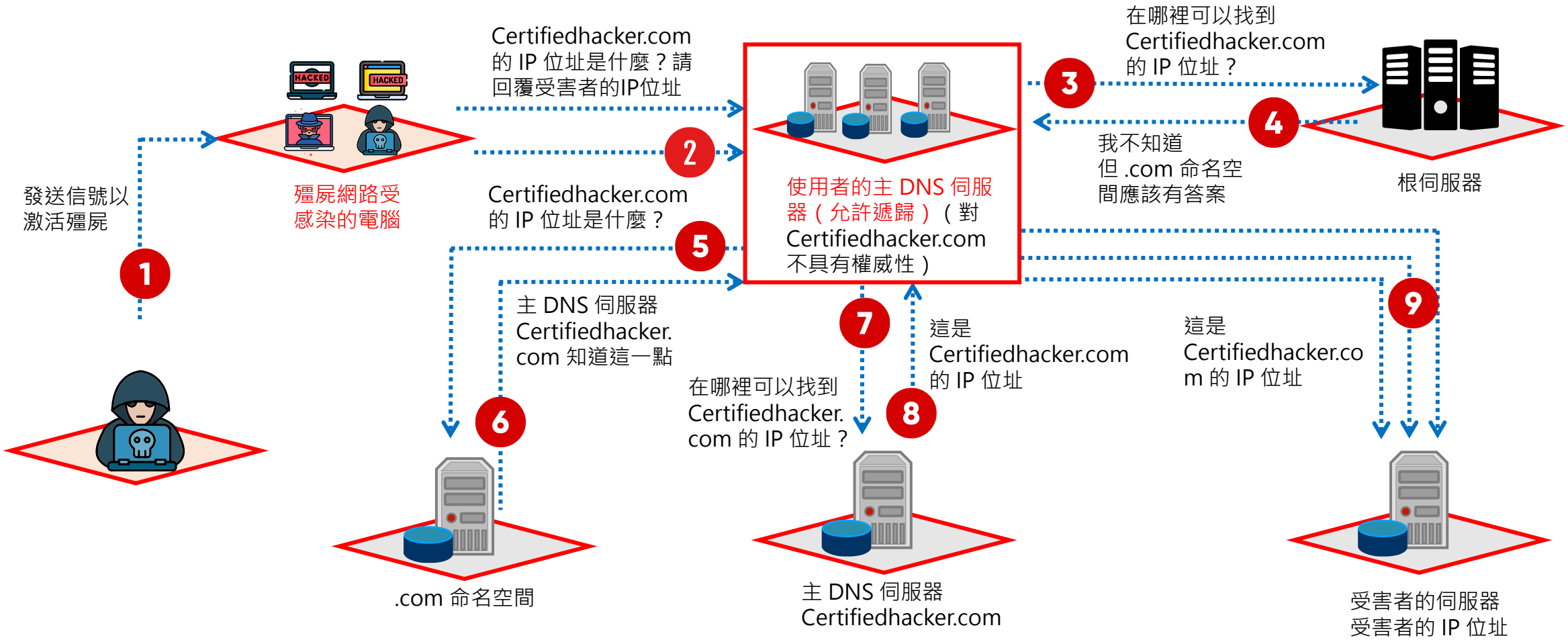
- 攻擊者利用DNS重定向的DNS遞歸方法進行DNS放大攻擊



每個機器人向開放 DNS 解析器提出請求時都提供欺騙性 IP 位址，也就是目標受害者的真實源 IP 位址，目標隨後會收到來自 DNS 解析器的回應。因此，目標接收攻擊者的初始流量的放大結果，其網路被虛假流量堵塞，導致阻斷服務。

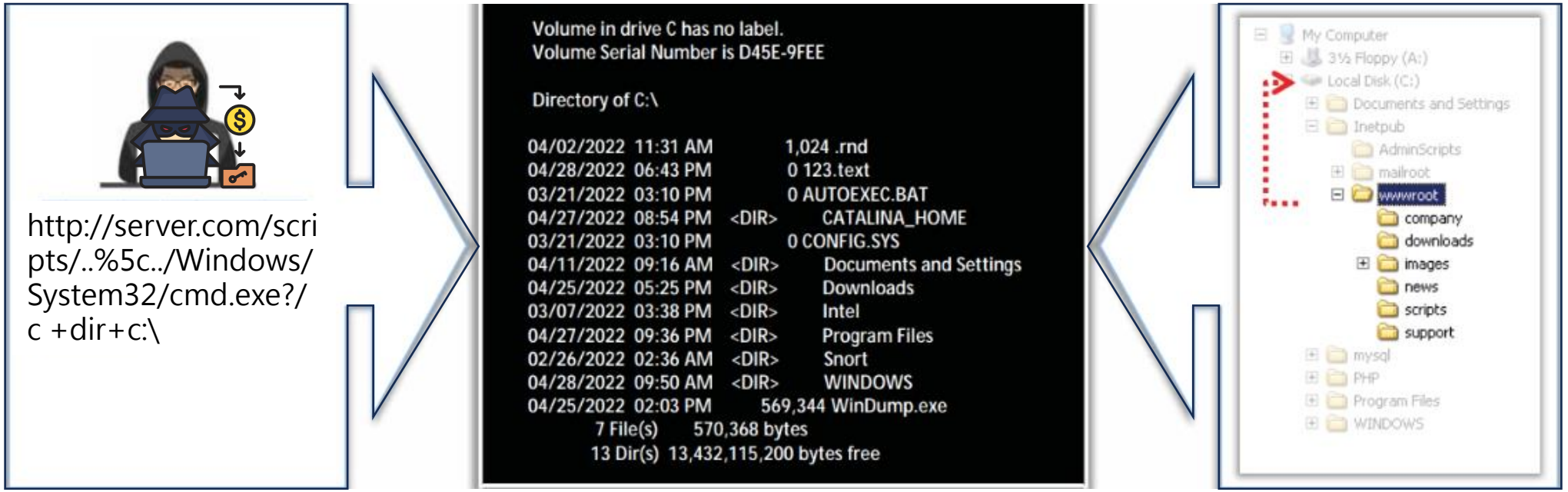
DNS 放大攻擊（續）

- 攻擊者使用具有欺騙性 IP 位址的受感染 PC，利用 DNS 遞歸方法放大對受害者 DNS 伺服器的 DDoS 攻擊



目錄遍歷攻擊

- 在目錄遍歷攻擊中，攻擊者使用../（點-點-斜線）序列存取網頁伺服器根目錄之外的受限目錄
- 攻擊者可以使用嘗試錯誤法(trial and error)導航到根目錄之外，存取系統中的敏感資訊



FIDO

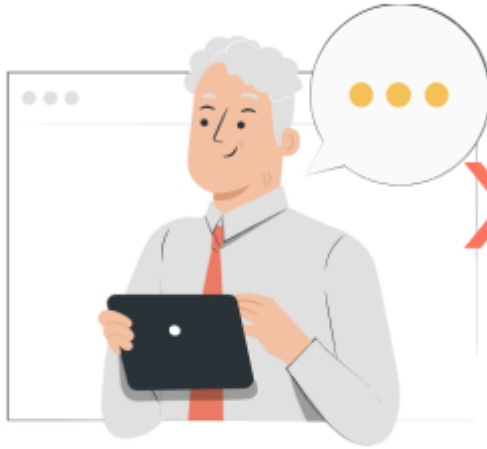
業界對密碼問題的回答

- FIDO（Fast IDentity Online）是一套開放且可延伸的身份驗證標準，目的加強和簡化網上驗證過程，減少對傳統密碼的依賴。FIDO聯盟所推動的這些標準，使得企業和開發者能夠整合更安全的驗證方法，例如：生物識別（指紋、面部識別等）、安全密鑰和設備PIN碼。
- FIDO 聯盟制定以公鑰加密技術為基礎的 FIDO 身份驗證標準，這種身份驗證比密碼和簡訊 OTP 更安全，更便於消費者使用，也更便於服務提供者部署和管理。 FIDO Authentication（FIDO 身份驗證）可在網站和應用程式中以安全、快速的登錄體驗取代僅憑密碼的登錄。

https://fidoalliance.org/fido2/?lang=zh-hans

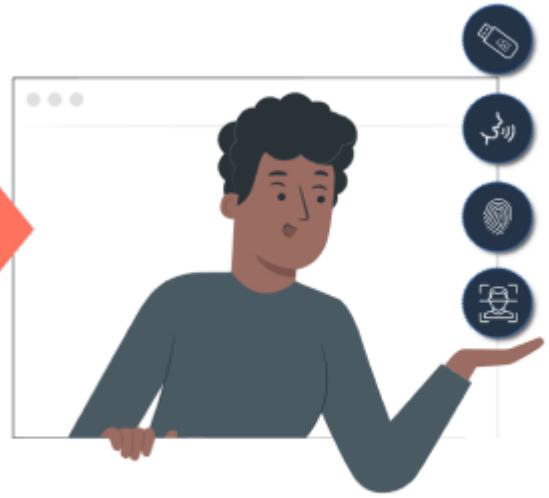
實現向防網路釣魚身份驗證的根本轉變

從傳統的知識型認證



- 存儲在伺服器上
- 短信 OTP
- KBA
- 密碼

到以佔有為基礎的現代認證



- 在裝置上（從不在伺服器上）
- 本地生物識別/PIN 碼
- 檔授權
- 多設備 FIDO 證書

https://fidoalliance.org/fido2/?lang=zh-hans

有關FIDO的參考來源和相關網址的整理

參考來源	說明	網址
FIDO Alliance 官方網站	提供FIDO標準、成員資訊、新聞和活動的詳細資料	FIDO Alliance
FIDO2 標準	關於支持無密碼驗證的FIDO2標準介紹	FIDO2
WebAuthn 指南	由開發者社群建立的WebAuthn使用和實施指南	WebAuthn Guide
W3C WebAuthn 標準	W3C制定的Web Authentication規範的官方文件	W3C Web Authentication

https://fidoalliance.org/fido2/?lang=zh-hans

FIDO Alliance 官方網站

https://fidoalliance.org/?lang=zh-hans

FIDO2 標準


FIDO Alliance - Open Authentica
FIDO2 - FIDO Alliance
https://fidoalliance.org/fido2/?lang=zh-hans
簡體中文
fido ALLIANCE
FIDO聯盟
通行金鑰
設備上載
認證
資源
新聞與活動
About the Alliance – Chinese (Simplified)
聯盟概述
FIDO領導團隊
標識使用與法律事項
行為準則
招賢納士
聯繫我們
業界對密碼問題的回答
FIDO 聯盟制定了基於公鑰加密技術的 FIDO 身份驗證標準，這種身份驗證比密碼和簡訊 OTP 更安全，更便於消費者使用，也更便於服務提供者部署和管理。 FIDO Authentication（FIDO 身份驗證）可在網站和應用程式中以安全、快速的登錄體驗取代僅憑密碼的登錄。
實現向防網路釣魚身份驗證的根本轉變
從傳統的知識型認證
到以佔有為基礎的現代認證
• 存儲在伺服器上
• 短信 OTP
• KBA
• 密碼
• 在裝置上（從不在伺服器上）
• 本地生物識別/PIN 碼
• 檔授權
• 多設備 FIDO 證書
FIDO Enterprise Video
分享
什麼是 FIDO2?
FIDO2 使用戶能夠利用普通設備在行動和桌面環境中輕鬆驗證線上服務。
FIDO2 規範是萬維網聯盟（W3C）的網路驗證（WebAuthn）規範和 FIDO 聯盟相應的用戶端到驗證器協定（CTAP）。
FIDO 身份驗證的優勢
安全
FIDO2 加密登錄憑證在每個網站上都是唯一的，不會離開用戶的設備，也不會存儲在伺服器上。這種安全模式消除了網路釣魚、各種形式的密碼盜竊和重放攻擊的風險。
便利性
用戶可通過設備上的指紋識別器或攝像頭等簡單的內置方法，或利用易於使用的 FIDO 安全密鑰，解鎖加密登錄

FIDO 身份驗證的優勢

- FIDO2 加密登錄憑證在每個網站上都是唯一的，不會離開使用者的設備，也不會儲存在伺服器上。 這種安全模式消除了網路釣魚、各種形式的密碼盜竊和重送攻擊的風險。

安全

- 使用者可透過設備上的指紋識別器或攝影機等簡單的內建方法，或利用易於使用的 FIDO 安全密鑰，解鎖加密登錄憑證。消費者可以選擇最適合自己需求的設備。

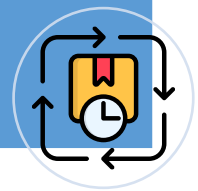
便利性

- FIDO 將認證資料存於使用者端，由於每個網站的 FIDO 密碼金鑰都是獨一無二的，因此不能用於跨網站跟蹤使用者。此外，生物識別資料在使用時永遠不會離開使用者的設備。

隱私權

- 網站可以透過簡單的 JavaScript API資料用啟用 FIDO2，消費者每天使用的數十億台設備上的主流瀏覽器和平臺都支援該 API。

可延伸性



https://fidoalliance.org/fido2/?lang=zh-hans

FIDO題庫1

FIDO 是確保登入流程中伺服器透過與終端裝置協定的安全機制。請問下列何項敘述有誤？

(A) 由 IETF（網際網路工程任務組織）所訂定的一套網路識別標準

(B) 這套識別標準透過公開金鑰加密（Public Key Cryptography）的架構進行多重因素驗證（MFA）以及生物辨識登入來強力且嚴密地保護雲端帳號的個資

(C) FIDO 是 Fast Identity Online 的縮寫

(D) FIDO 是採用公開金鑰基礎架構的驗證模式，在FIDO 認證伺服器端（FIDO Authentication Server）只保存相對應的公鑰，而私鑰則僅保存在使用者的裝置端，因此使用者在登入時只需提供個資給終端裝置解鎖私鑰，再透過這個步驟解鎖公鑰進行登入

答案：(A)

FIDO題庫2

近來 FIDO（Fast Identity Online）標準被廣泛應用在身分識別，下列描述何者錯誤？(1122,27,98)

(A) FIDO 匯集生物識別（指紋、虹膜、聲紋和臉部識別）、Token、晶片卡等各種認證技術方法

(B) FIDO 因具備無密碼身分識別，並無整合多因子驗證

(C) 可透過 FIDO 身分鑑別和身分認證以確認使用者身分，減少帳號盜用

(D) FIDO 將認證資料存於使用者端

答案：(B)

參考文獻

本教材僅供IPAS初級資訊安全工程師訓練使用，不得移作其他用途。