Unauthorized Access and Use

Unauthorized Access and Use

Unauthorized access is the use of a computer or network without permission

未經授權的存取是使用電腦或網路時未經許可

Unauthorized use is the use of a computer or its data for unapproved or possibly illegal activities

未經授權的使用是不允許或非法使用電腦或資料

Unauthorized Access and Use

Safeguards against Unauthorized Access

- Organizations take several measures to help prevent unauthorized access and use

  組織採取一些方來預防未經授權的存取與使用

  – Acceptable use policy (AUP)可接受的使用政策

    - that outlines the activities for which the computer and network may and may not be used.
    - specify the **acceptable use of technology** by employees for personal reasons
    - also should specify the **personal activities**

Page 221
Figure 5-5

Unauthorized Access and Use

Safeguards against Unauthorized Access

- To protect your personal computer from unauthorized intrusions
  - Disable file and printer sharing 禁用檔案和影印機共享
  - Firewalls 防火牆
  - Intrusion detection software 入侵偵測軟體
  - Identifying and authenticating users 識別與驗證使用者

Page 221
Figure 5-5

Unauthorized Access and Use

許多企業使用access control 降低Unauthorized Access and Use 的可能

- **Access controls** define
  who can access a computer,
  when they can access it,
  and what actions they can take

存取控制定義**誰**可以存取電腦，**何時**他們可以存取，可以**作什麼**

P222

Unauthorized Access and Use

- The computer, device, or network should maintain an **audit trail** that records in a file both successful and unsuccessful access attempts
- Audit trail records access attempts
  審核資料會保留存取成功與失敗的紀錄
  - used to monitor and record computer transactions so auditors can trace activity
    可用來監視和記錄電腦交易，使稽核人員能追蹤和辨認可疑的電腦活動
  - Effective audit-control software forces every user to leave a trail of electronic footprints
    有效的稽核軟體會迫使所有的使用者，都要留下電子蹤跡

Unauthorized Access and Use

- Organizations should investigate unsuccessful access attempts immediately to ensure they are not intentional breaches of security.
- They also should review successful access for irregularities, such as use of the computer after normal working hours or from remote computers.
- The security program can be configured to alert a security administrator whenever suspicious or irregular activities are suspected.
- In addition, an organization regularly should review users' access privilege levels to determine whether they still are appropriate.

Unauthorized Access and Use

- Access controls use **two-phase processes** called **identification** and **authentication**
  - **Identification識別**
    verifies that an individual is a valid user.
  - **Authentication驗證**
    verifies that the individual is the person he or she claims to be.
    - User name and Password
    - Passphrase 通關密語
      - CAPTCHA 驗證碼
    - Posses objects 持有物
    - Biometric devices 生物辦識設備

補充

Unauthorized Access and Use

- User name also called a ID
- Password

Single sign-on

- **單一登入**（縮寫為 SSO）
- 一種對於許多相互關連，但是又是各自獨立的軟體系統，提供存取控制的屬性。當擁有這項屬性時，當使用者登入時，就可以取得所有系統的存取權限，不用對每個單一系統都逐一登入。
- 這項功能通常是以輕型目錄訪問協議（LDAP）來實作，在伺服器上會將使用者資訊儲存到LDAP資料庫中。
- 相同的，**單一登出**（single sign-off）就是指，只需要單一的登出動作，就可以結束對於多個系統的存取權限。

LDAP

- 輕型目錄存取協定
  （Lightweight Directory Access Protocol，英語發音：/ˈɛldæp/）
- 一個開放的，中立的，工業標準的應用協議，通過IP協議提供訪問控制和維護分布式信息的目錄信息。
- 目錄服務在開發內部網和與網際網路程序共享用戶、系統、網絡、服務和應用的過程中占據了重要地位。
- 例如，目錄服務可能提供了組織有序的記錄集合，通常有層級結構，例如公司電子郵件目錄。同理，也可以提供包含了地址和電話號碼的電話簿。
- LDAP stands for Lightweight Directory Access Protocol. It is an application protocol used over an IP network to manage and access the distributed directory information service.

Unauthorized Access and Use

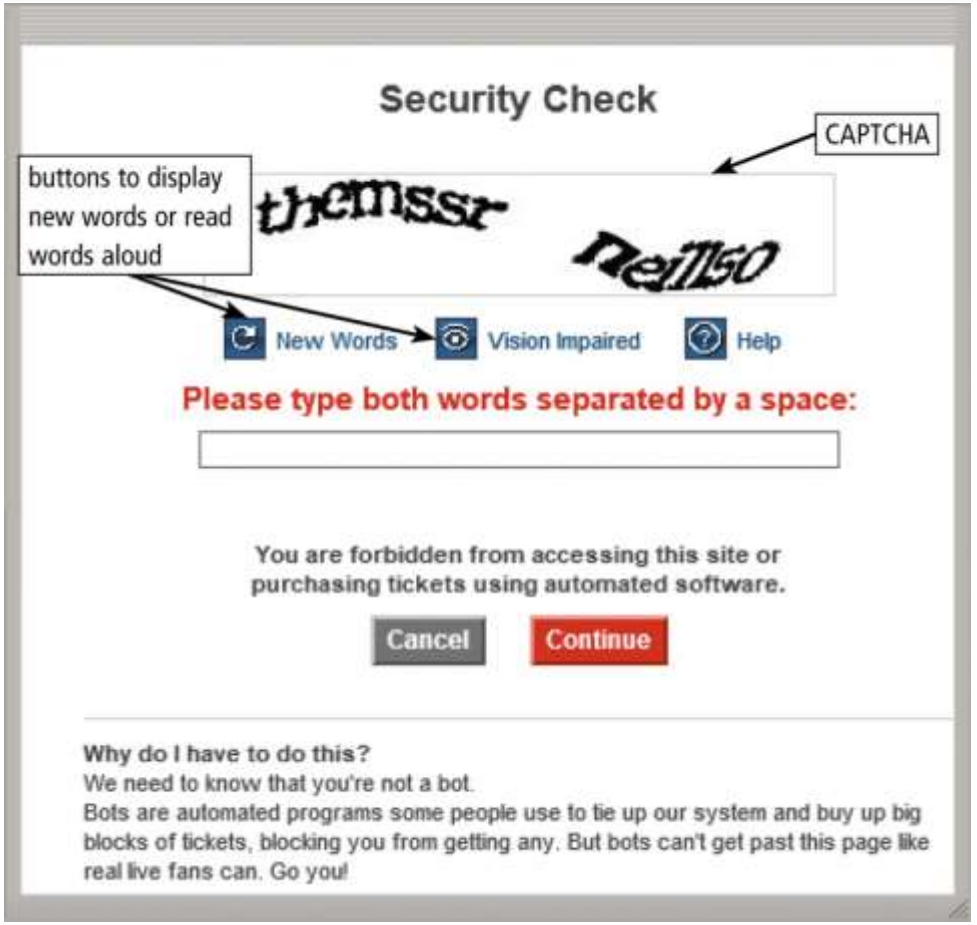
- Passphrase 通關密語
  - A passphrase is a private combination of words, often containing mixed capitalization and punctuation, associated with a user name that allows access to certain computer resources

Unauthorized Access and Use

- A **PIN** (personal identification number), sometimes called a passcode, is numeric password, either assigned by a company or selected by a user

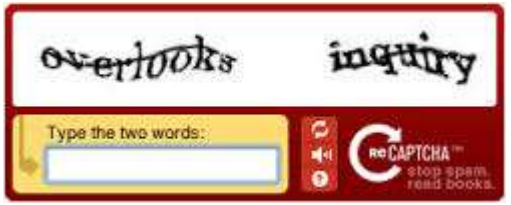
Why Do Some Websites Display Distorted Characters You Must Reenter Along With Your Password?

CAPTCHA



Unauthorized Access and Use

- CAPTCHA驗證碼
  - Completely Automated Public Turing test to tell computers and humans apart
  - is a program developed at Carnegie Mellon University 卡內基美隆大學
  - **to verify that user input is not computer generated**.

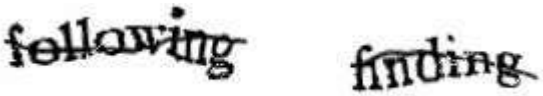


CAPTCHA 驗證碼

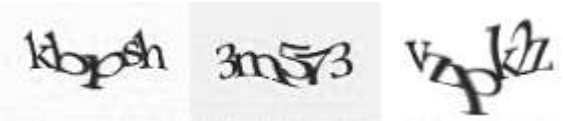
- 全自動區分電腦和人類的Turing Test（英語：Completely Automated Public Turing test to tell Computers and Humans Apart，簡稱CAPTCHA），**俗稱驗證碼**
- 是一種區分使用者是電腦和人的公共全自動程式。在CAPTCHA測試中，作為伺服器的電腦會自動生成一個問題由使用者來解答。這個問題可以由電腦生成並評判，但是必須只有人類才能解答。由於電腦無法解答CAPTCHA的問題，所以回答出問題的使用者就可以被認為是人類。
- CAPTCHA這個詞最早是在2002年由卡內基梅隆大學的路易斯·馮·安、Manuel Blum、Nicholas J.Hopper以及IBM的John Langford所提出。
- 一種常用的CAPTCHA測試是讓使用者輸入一個扭曲變形的圖片上所顯示的文字或數位，扭曲變形是為了避免被光學字元識別（OCR, Optical Character Recognition）之類的電腦程式自動辨識出圖片上的文數字而失去效果。
- 為了無法看到圖像的身心障礙者，替代的方法是改用語音讀出文數字，為了防止語音辨識分析聲音，聲音的內容會有雜音。

CAPTCHA

早期的Captcha驗證碼 "smwm" ，由EZ-Gimpy程式產生，使用扭曲的字母和背景顏色梯度



一種更現代的CAPTCHA，其不使用扭曲的背景及字母，而是增加一條曲線來使得影像分割（segmentation）更困難



另一種增加影像分割難度的方法為將符號彼此擁擠在一起，但其也使得真人使用者比較難以識別

CAPTCHA

- 目前廣泛用於網站的留言板，許多留言板為防止有人利用電腦程式大量在留言板上張貼廣告或其他垃圾訊息，因此會放置CAPTCHA要求留言者必需輸入圖片上所顯示的文數位或是算術題才可完成留言。
- 而一些網路上的交易系統（如訂票系統、網路銀行）也為避免被電腦程式以暴力法大量嘗試交易也會有CAPTCHA的機制。

CAPTCHA

台鐵訂票系統

CAPTCHA

高鐵訂票系統

一般網路訂票 | 信用卡合作優惠專區

起訖站	起程站 請選擇... 到達站 請選擇...
車廂種類	◉ 標準車廂 ○ 商務車廂
訂位方式	◉ 依時間搜尋合適車次 ○ 直接輸入車次號碼
時間	去程 2013/12/10 約 請選擇... 出發 ☐ 訂購回程
票數	全票 1 孩童票(6-11歲) 0 愛心票 0 敬老票(65歲以上) 0
查詢早鳥優惠	☐ 僅顯示尚有早鳥優惠之車次

為了確保交易安全，請輸入右圖中之驗證碼：  重新產生 | 語音播放

開始查詢

Unauthorized Access and Use

- A **possessed object** is any item that you must carry to gain access to a computer or computer facility

possessed object

是任何必需用來獲得存取電腦或電腦設施的物件

  - Often are used in combination with a **personal identification number** (**PIN**)

    通常與**個人身分確認號碼(PIN)** 合併使用
  - Examples of possessed objects are badges, cards, smart cards, and keys.
  - The card you use in an ATM (automated teller machine), for example, is a possessed object that allows access to your bank account.

Unauthorized Access and Use

生物辦識設備Biometric Devices

Fingerprint reader

Face recognition system

Hand geometry system 手幾何學

Voice verification system

Signature verification system

Iris 虹膜 recognition system

Pages 224-225
Figures 5-8 – 5-10

Unauthorized Access and Use

- A **biometric device** authenticates a person's identity by translating a personal characteristic into a digital code that is compared with a digital code in a computer
  生物辨識設備藉由轉換個人特徵成數位碼，並與電腦中的數位碼進行比對，以鑑識個人的身分
  - Fingerprint, hand geometry, voice, signature, and iris
    如指紋、掌形辨視、聲音、簽名、虹膜
  - 虹膜-眼睛構造的一部分，虹膜中心有一圓形開口，稱為瞳孔。
  - hand geometry
    手幾何學 (使用手的幾何形狀驗證使用者身分的一種科學)
    - Measure the shape and size of a person's hand

Pages 225

What is a lock screen

Pages 225

Iris Recognition System虹膜辨識系統

- expensive
- 有時是比對視網膜後方的血管樣式(patterns)

Pages 225

Two-Step Verification

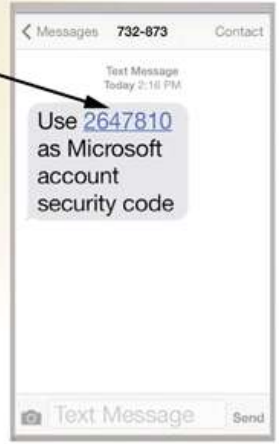
- With two-step verification, also known as two-factor verification, a computer or mobile device uses tow separate methods, one after the next, to verify the identity of a user.
  - ATM
    - ATM Cad
    - PIN
  - Mobile phone and computer
    - Sign to an account on a computer (account and password)
    - Prompted to enter another authentication code which is sent as a text or voice message or via an app on a smartphone.

Two-Step Verification

Step 1
User signs in to an account on a computer.

Step 2
User is prompted to enter an authentication code, received via text message or email message, before being granted access to the account.

Step 3
User receives security code in a text message.



Step 4
User gains entry to account by entering the security code sent in the text message.

Digital forensics

- **Digital forensics** is the discovery, collection, and analysis of evidence found on computers and networks
  數位鑑識是發現，收集，分析電腦中和網路上的證據
- Many areas use digital forensics

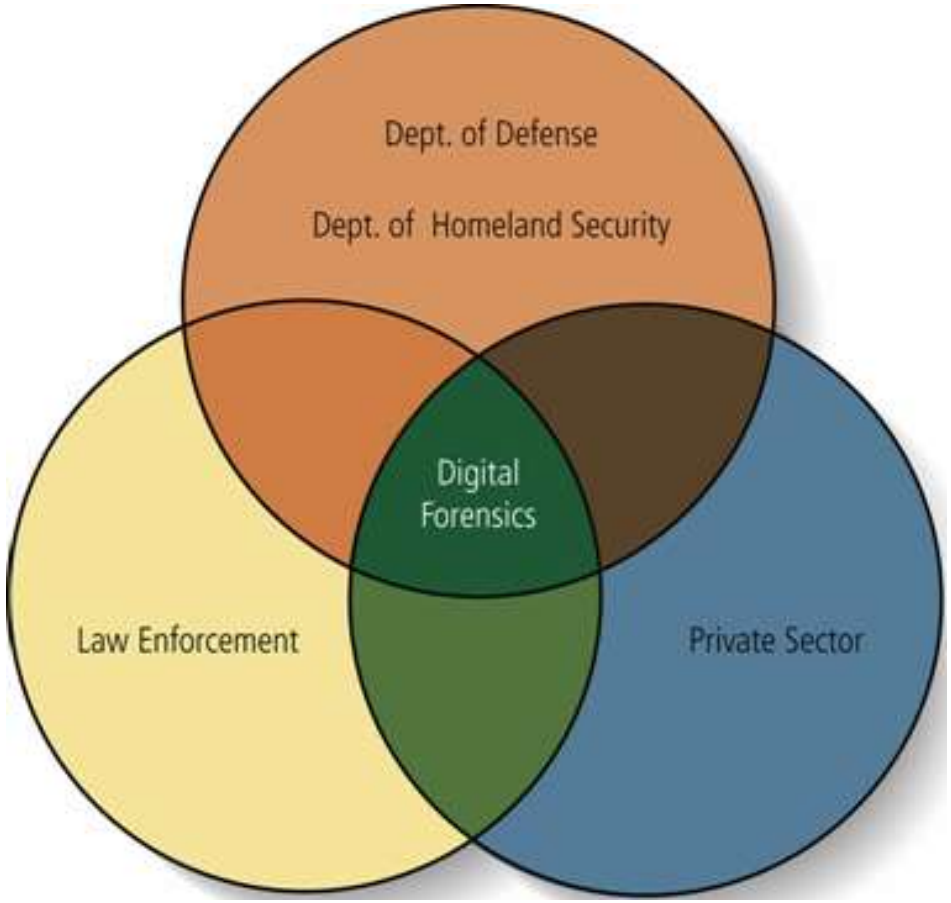
Digital forensics examiner

需具備之能力

- A digital forensics examiner must have
  - knowledge of the law,
  - technical experience with many types of hardware and software products,
  - superior communication skills,
  - familiarity with corporate structures and policies,
  - a willingness to learn and update skills,
  - and a knack for problem solving.

Digital Forensics Examiners

- Digital forensics covers several overlapping areas



Software Theft

- **Software theft** occurs when someone:

Steals software media
偷竊軟體媒介

Intentionally erases programs
故意地消除程式

Illegally registers and/or activates a program
非法註冊或啟動程式

Illegally copies a program
非法拷貝軟體

Pages 228

Software Theft

- **BSA**
  - To promote understanding of software piracy, a number of major worldwide software companies formed the **Business Software Alliance (BSA) .**

    商業軟體聯盟(網業軟體聯盟)推動認知軟體智財問題

    由幾家大型軟體公司組成在美國與40個以國家架設網站和反盜版熱線

Software Theft

- **Illegal registration/activation**非法註冊或啟動程式
  - A perpetrator illegally obtains registration numbers and/or activation codes.
  - A program called a **keygen** , short for key generator, creates software registration numbers and sometimes activation codes. 註冊碼產生器
  - Some unscrupulous individuals create and post keygens so that users can install software without legally purchasing it.

Pages 228

Software Theft

- **Illegal copying 非法複製**
  - A perpetrator copies software from manufacturers.
  - **Software piracy** often referred to simply as **piracy**剽竊, is the **unauthorized and illegal duplication of copyrighted software.** **軟體剽竊**
  - Piracy is the most common form of software theft.
  - Copying, loaning, borrowing, renting, or distributing software can be a violation of copyright law

    複製，出借，借用，租用，或散布軟體都可算是違反著作權法

Pages 228

Safeguards against Software Theft

- Many manufacturers incorporate an **activation process** into their programs to ensure the software is not installed on more computers than legally licensed
- During the **product activation**, which is conducted either online or by phone, users provide the software product's identification number to associate the software with the computer or mobile device on which the software is installed

有些軟體需要**產品啟動**才能完全起作用

讓使用者從網路上或是利用電話輸入一串產品識別碼

Pages 228

Software Theft

- A license agreement(許可協議、授權) is the right to use software.
- A **single-user license agreement** , also called **EULA, E**nd-**U**ser **L**icense **A**greement

Safeguards against Software Theft

- A single-user **license agreement** typically contains the following conditions:單一使用者**授權協議書**通常包含以下情況

Typical Conditions of a Single-User License Agreement

You can…

- Install the software on only one computer. (Some license agreements allow users to install the software on one desktop and one laptop.)
- Make one copy of the software as a backup.
- Give or sell the software to another individual, but only if the software is removed from the user's computer first.

You cannot…

- Install the software on a network, such as a school computer lab.
- Give copies to friends and colleagues, while continuing to use the software.
- Export the software.
- Rent or lease the software.

Pages 228 – 229
Figure 5-13

Safeguards against Software Theft

- 單一使用者授權協議書通常包含以下情況

Permitted to 允許	Not permitted to 不允許
• Install the software on one computer 安裝軟體在一台電腦上 • Make one copy of the software 拷貝一份軟體 • Remove the software from your computer before giving it away or selling it 贈送或賣掉電腦前，移除軟體	• Install the software on a network 在網路上安裝軟體 • Give copies to friends or colleagues while continuing to use the software 使用軟體時，同時拷貝給朋友或同學 • Export the software 出口軟體 • Rent or lease the software 出租或租借軟體

Safeguards against Software Theft

- To support multiple users' access of software, most manufacturers sell **network versions** or **site licenses** of their software, which usually costs less than buying individual stand-alone copies of the software for each computer.
- A **network license** is a legal agreement that allows multiple users to access the software on the server simultaneously.
  - The network license fee usually is based on the number of users or the number of computers attached to the network.
- A **site license** is a legal agreement that permits users to install the software on multiple computers — usually at a volume discount.

Information Theft

Information theft occurs when someone steals personal or confidential information

資訊竊盜發生當某人偷取個人或機密的資訊

Information Theft

Safeguards against Information Theft

- **Encryption** is a process of converting data that is readable by humans into encoded characters to prevent unauthorized access
  加密是一個過程，將可讀的資料轉換成不可讀的字元，預防未經授權的存取
- To read the data, the recipient must decrypt, or decipher, the data讀資料需要解密或是有密碼
- Safeguards against information theft
  防止資料被盜取的方法
- Process of converting plaintext明文 (readable data) into ciphertext密文(unreadable characters)

Pages 229

Safeguards against Information Theft

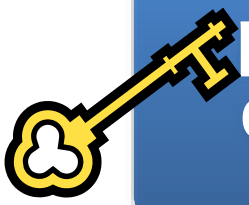
- A **Encryption** algorithm, or **cypher**, is a set of steps that can convert readable plaintext into unreadable ciphertext
- An **encryption key** is a set of characters that the originator of the data uses to encrypt the plaintext and the recipient of the data uses to decrypt the ciphertext.
- **Encryption key** (formula) often uses more than one method

Table 5-2 Simple Encryption Algorithms

Name	Algorithm	Plaintext	Ciphertext	Explanation
Transposition	Switch the order of characters	SOFTWARE	OSTFAWER	Adjacent characters swapped
Substitution	Replace characters with other characters	INFORMATION	WLDIMXQUWIL	Each letter replaced with another
Expansion	Insert characters between existing characters	USER	UYSYEYRY	Letter Y inserted after each character
Compaction	Remove characters and store elsewhere	ACTIVATION	ACIVTIN	Every third letter removed (T, A, O)

P230

The two basic types of encryption



private key encryption

also called **symmetric key encryption**

秘密加密法

對稱式金鑰加密法

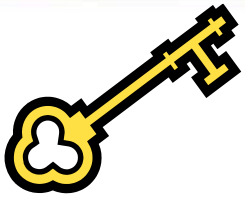
Public key encryption

also called **asymmetric key encryption**

公開金鑰加密法

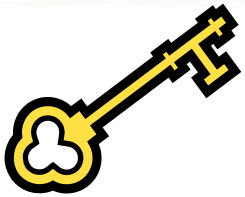
非對稱式加密法

The two basic types of encryption

- **private key** 
  - Also called **symmetric key encryption對稱式金鑰加密法**
  - Both the originator and the recipient **use the same secret key** to encryption and decrypt the data
  - The **most popular** private key encryption system is **advanced encryption standard (AES)**

Symmetric Key Encryption

- 對稱式金鑰加密法



  - 資料傳送過程中使用相同的金鑰進行加密及解密
  - 在雙方交換訊息前，即是先持有一個**共同的密鑰**；當甲方傳輸前，先以該金鑰對明文編碼成密文，乙方收到後，再以同一把金鑰將密文解碼回明文。

The two basic types of encryption

- **Public key**

  - Also called **asymmetric key encryption**
    公開（非對稱式）金鑰加密法
  - Use two encryption keys
    - **Public key**
    - **Private key**
  - A message encrypted with your public key can be decrypted only with your private key, and vice versa.
  - The public key is made known to those with whom you communicate

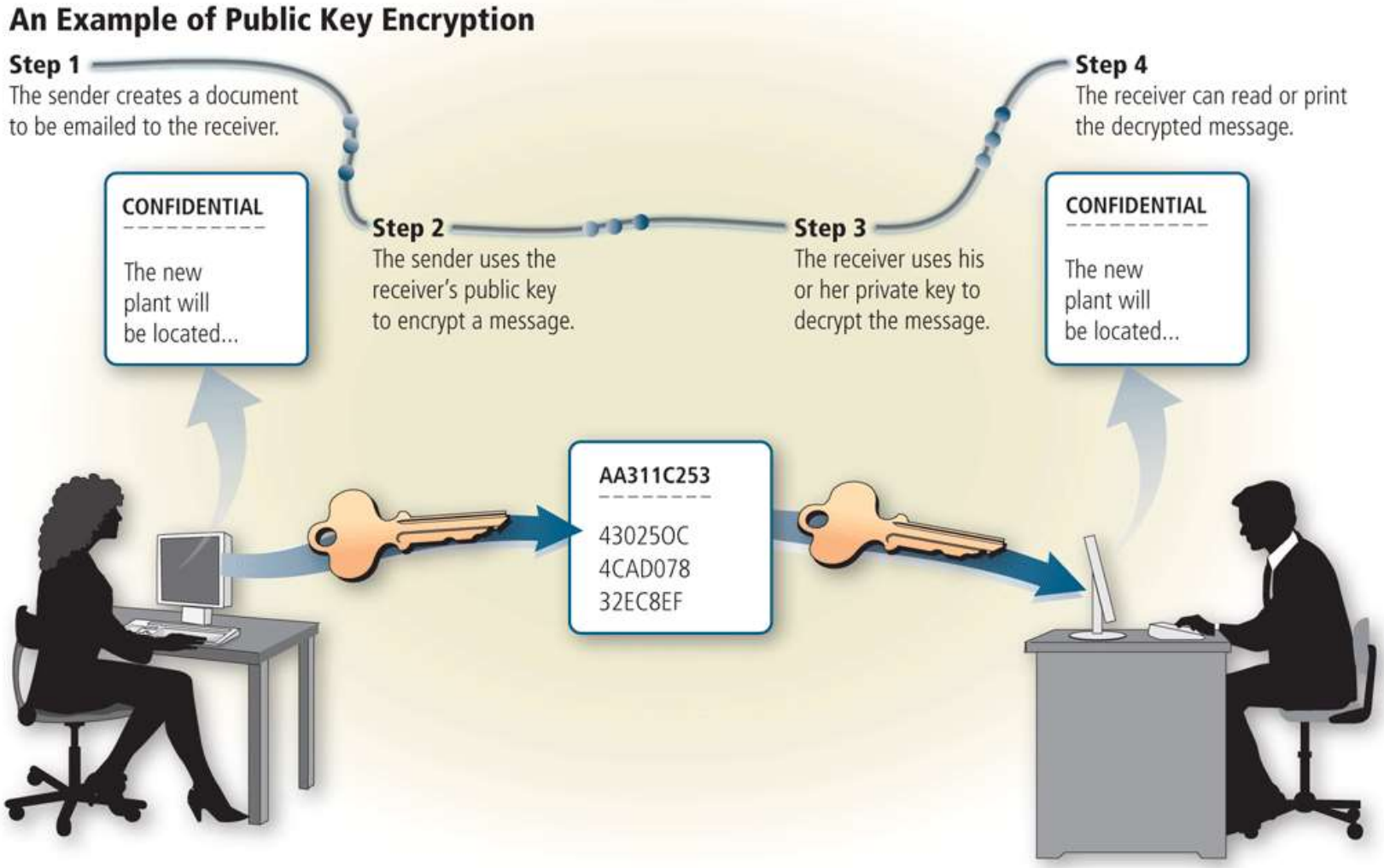
Asymmetric key encryption

- 公開（非對稱式）金鑰加密法
  - 1976年Diffie與Hellman提出；1978Rivest、Shamir及Adlman提出著名的**RSA公開金鑰密碼系統**，遂將此一理念付諸實現。
  - 公鑰（Public Key）
    - 每個參與者會產生一組公鑰，用來對訊息作加密。此公鑰可以公布在一個公開的註冊處或發送給其他人。
  - 私鑰（Private Key）
    - 與公鑰組成金鑰對，由參與者保留私用。

Asymmetric key encryption

- 此加密法需產生兩把金鑰，一把用以加密，另一把用以解密。
  - 此兩把金鑰完全不相同，但具有某種關聯性，有心人士即使知道得知演算與加密金鑰，仍須另一把解密金鑰。
- 範例：
  - 甲乙雙方欲傳送資料，各自產生自己的金鑰組，包含一支公鑰，一支私鑰。
  - 當甲欲傳送資料給乙方，甲用乙方的公鑰來加密（因為乙方的公鑰是公開的，所以可以輕易取得）
  - 當乙方收到加密的文件，再用自己的私鑰來解密。

Information Theft



Page 217
Figure 5-14

Encryption

- Mobile users today often access their company networks through a virtual private network.
- When a mobile user connects to a main office using a standard Internet connection, a **virtual private network (VPN)** provides the mobile user with a secure connection to the company network server, as if the user has a private line.
- VPNs help ensure that data is safe from being intercepted by unauthorized people by encrypting data as it transmits from a laptop, smartphone, or other mobile device.

http://wiki.mbalib.com/zh-tw/VPN

Signatures and Certificates

- A **digital signature** is an encrypted code that a person, website, or organization attaches to an electronic message to verify the identity of the sender
  數位簽章是個人、網站、或組織加密在電子信息上的密碼，**用來驗證傳送者的身分**
  - Often used to ensure that an impostor is not participating in an Internet transaction
    常用來確保冒充者無法參與在網路交易中
  - digital signatures help to prevent e-mail forgery
    數位簽章可以用來預防電子郵件被偽造
  - A digital signature also can verify that the content of a message has not changed.
    數位簽章可以用來預防電子郵件的內容沒有被更改

數位簽章

- 如同書面文件的簽名、蓋章，網路環境中也有數位簽章，作為通信與交易的基礎。
- 由於數位簽章是簽署人向憑證機構申請後核發，且文件傳遞過程亦經**加密與驗證**，所以具有**防止竄改偽造、確認交易對象身份、避免事後否認**等功能。

Information Theft

- A **digital certificate** is a notice that guarantees a **user or a website is legitimate**

  是不種保證使用者或網站為合法的告示

  - 它可以建立擁有者的身份識別，並且可提供擁有者的公開金鑰。
  - 數位憑證是由可信任的機構-憑證管理中心(CA)發出，並且只限用一段時間。
  - **數位認證 (數位憑證)**
  - 可以讓進行電子商務交易的雙方確認彼此的身份。
    而企業也需要有這機制來確認與他交易的另一端是誰，
    才能夠在網路上向顧客收費，或傳送資料給代理商。

certificate authority

- **Certificate authority (CA)** 憑證授權中心
  - Authorized person or company that issues and verifies digital certificates 一個經過授權可核發和驗證數位憑證的個人或中心
  - Users apply for digital certificate from CA
  - Digital certificates typically have these components:
    - version number, serial number, certificate algorithm identifier, issuer name, validity period, subject name, subject public key information, issuer unique identifier, subject unique identifier, extensions, and certification authority's digital signature.
  - The information in a digital certificate is **encrypted**.

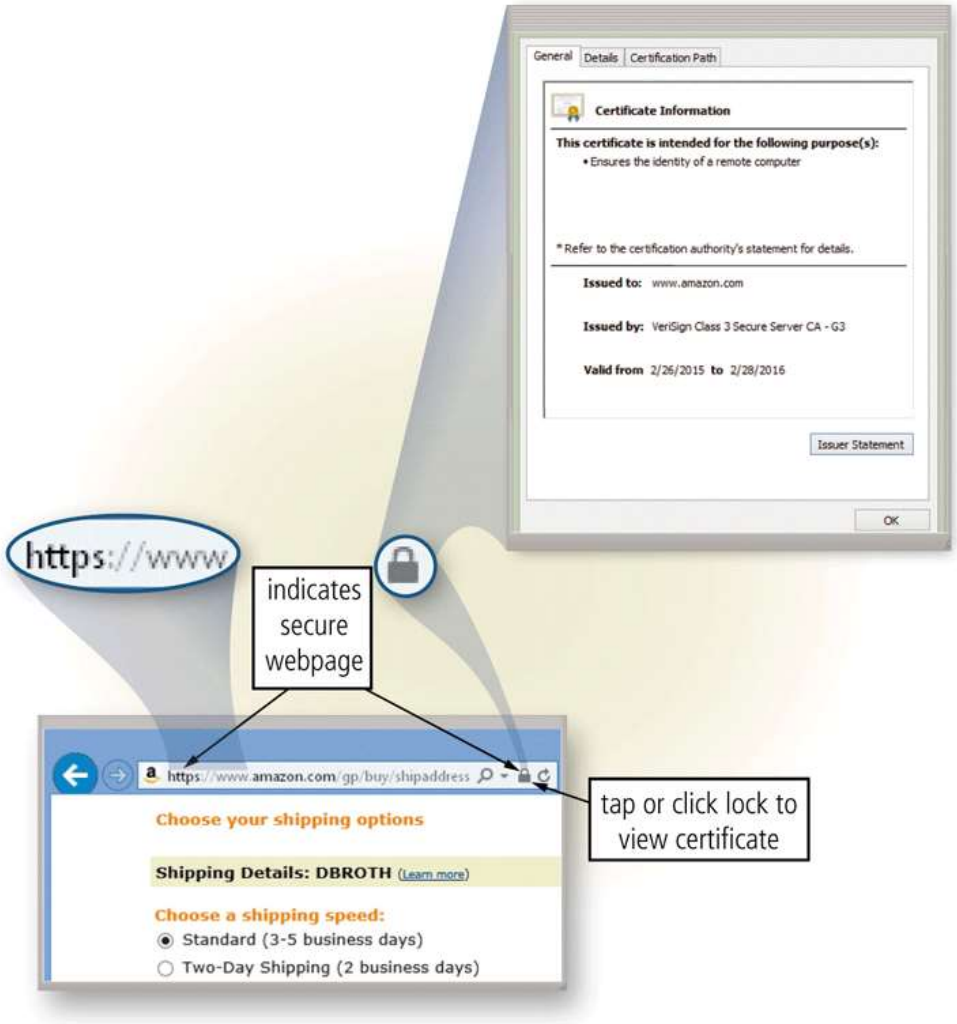
certificate authority

- Online **certificate authority** (Online providers that issue digital certificates.) (CA) providers issue digital certificates.
- Each CA is a trusted third party that takes responsibility for verifying the sender's identity before issuing a certificate.
- Every digital certificate has identical components because it is generated using a standard, called X.509.
- Individuals and companies can purchase digital certificates from one of more than 35 online CA providers.
- The cost varies depending upon the desired level of data encryption, with the strongest levels recommended for financial and e-commerce transactions.

certificate authority

- The certificates can be **valid for a maximum of two years**.
- Digital signatures also tie the signer's identity to the contents of a specific document, but they use an algorithm to detect changes to the file.
- The sender encrypts the file with a private key and creates a digital signature. Then, the receiver decrypts the same file with a public key and uses the same algorithm to open the document.
- A symbol, such as a green check mark, often is used to indicate the document is authentic; a different symbol, such as a yellow triangle, would indicate the document has been altered.

Information Theft



- A website that uses encryption techniques to secure its data is known as a **secure site**
- Web addresses of secure sites often begin with **https** instead of http.
- Secure sites typically use digital certificates along with security protocols.

Page 231
Figure 5-15

Internet Security Risks

- 兩種常見的安全協定
  - TLS (Transport Layer Security)
  - S-HTTP (Secure HTTP)
- 企業也經常使用VPN