班級：	姓名	座號
單元：3-2 資訊安全		教師：徐惠珠

一、資訊安全的種類：

種類		說明
實體安全		建築物與週遭環境安全考量，如硬體環境控制、天然災害控制（火災、地震、風災）、人為破壞管理控制。
資料安全		確保資料不會被非法入侵者讀取或破壞，如資料的使用權限、分級、備份、加解密、密碼防護、使用紀錄。
軟體安全	程式安全	程式的開發、執行及維護的安全管理。
	系統安全	維護電腦系統的正常運作，防止駭客入侵、病毒及專業訓練不足之人為破壞管理控制。
個人安全防護		包含人身安全、個人隱私安全、通訊（網路）安全。

二、影響資訊安全因素：

1.蓄意破壞　2.意外災害 3.人員疏失 4.軟硬體設備故障 ─ 偶發因素

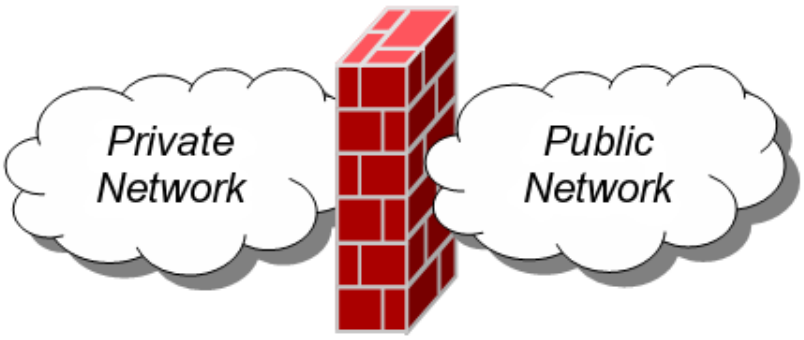
三、電腦犯罪的類型（網路攻擊的模式）

類型	說明
資料竄改	利用一些非法的手段，來改變系統中重要的資料，例如學生成績檔、銀行存款金額。
竊取資料	利用非法手段拷貝資料，以獲得利益，例如信用卡公司的員工盜賣客戶資料。
攔截資料	攔截網路上所傳送的資料，以獲得利益或情報，例如攔截客戶的交易資料。
特洛伊木馬（網頁掛馬）	通常會在免費軟體中加入一些特殊指令，使用者下載使用時，啟動這些特殊指令，而執行了一些未經授權的作業，造成重要資料被竊取、串改或開啟後門程式。
邏輯炸彈	在合法的程式中加上一些特殊的程式，它們被設計成隨時或在某個特定的時刻，執行特定的程式引發破壞的動作。
阻絕服務（DoS）	Denial of Service（DoS），某些有心人士對一些網路伺服器發送大量服務請求封包，進而讓伺服器無法有效處理這些請求而當機，使得伺服器無法運作而造成損失。
電腦蟑螂	專門在網路上登記知名企業的名稱做為網址，然後再以高價向企業兜售的人。
義大利臘腸式犯罪	非法入侵更改程式，從大批交易或多人的帳戶中竊取微小的金額到特定的帳戶中，積少成多。
社交工程	首先取得攻擊目標的背景資訊，利用社交手腕取得被害人信任，再向受害人要求某一些資訊，利用這些資訊向其他人員欺騙，不斷重複這些步驟，以達到最後目標。（常見的詐騙與攻擊手法相當多元，包括：假冒為同事；假冒新進員工；假冒廠商、客戶或政府單位；假冒具有權威的人；假冒系統廠商，表示欲提供系統修補程式或更新程式；假冒好心人士，告訴對方如果電腦發生問題可以找他，然後製造問題，讓受害人打電話來求援…等。）
網路釣魚	利用偽造電子郵件與網站做為誘餌，並且使用社交工程方式騙取使用者洩漏重要資料，例如：銀行帳號密碼、信用卡號碼等個人機密資料。

班級：	姓名	座號
單元：3-2 資訊安全		教師：徐惠珠

網址嫁接	駭客將試用者原本要連接的網站重新導引至一個看似相同的網站，誘騙人們將使用者名稱及密碼輸到偽造網站的資料庫中。
零時差攻擊	利用軟體本身的安全漏洞進行攻擊，因為駭客是趕在軟體業者修護漏洞前發動攻擊，所以稱之零時差攻擊。
BotNet 攻擊（殭屍網路）	Botnet 傀儡網路另一個說法是殭屍網路，顧名思義受害電腦一旦被植入可遠端操控該電腦的惡意程式，即會像傀儡一般任人擺佈執行各種惡意行為，當一部電腦成為傀儡網路 Botnet 的一部份時，意味著 Bot 操縱者可將募集到的龐大網路軍團當作機器人來遠端遙控，從事各種非法入侵近年來尤以藉著「網頁掛馬」(入侵合法網頁植入惡意連結）進行資料竊取危害甚遽。瀏覽網頁者在無法察覺的情況下，連線到殭屍網路背景植入間諜軟體等載惡意程式，並從此成為殭屍網路的一員，繼續壯大殭屍網路軍團。 Bot 殭屍網路是網路犯罪者最常使用來從事詐欺與竊盜的主要管道，除此之外，Bot 網路還可用於針對商業網站發動聯合攻擊，讓這些網站無法使用。由於感染殭屍病毒多數沒有徵兆，一般受害者通常並不知道電腦已經遭受遠端控制。
間諜程式	間諜程式 (spyware) 指的是在你電腦裡偷偷的被植入的軟體, 這些軟體有可能收集你的個人資訊, 或使用電腦習慣.間諜程式與木馬、後門程式不同，它指的是那些具有行銷目的應用程式，會將使用者電腦裡的資訊透過網路傳送給 spyware 撰寫者，卻不事先知會電腦使用者。木馬、後門程式會使駭客從這些管道中，竊取使用者機密資訊。間諜程式不是什麼資訊都要，通常僅收集該間諜程式的行銷目的所需要的資訊，有一些間諜程式只會傳送該電腦使用何種作業系統的資訊，有一些則是將該電腦的使用者上網習性資料傳出去。

四、防火牆



目的	用來過濾資料來源，以維護內部網路安全的軟體或硬體。
常見問題	1.因大量資料流通都須透過防火牆的檢查，會降低網路效率。
	2.無法完全阻絕來自內不可能的攻擊，因為內部不易避免內部人員竊取重要資訊。
	3.無法完全阻絕外來的病毒攻擊、網路詐騙。

班級：	姓名	座號
單元：3-2 資訊安全		教師：徐惠珠

五、常見電腦病毒種類：

類型	說明	實例
開機型 （系統型） （啟動型）	1. 隱藏在**磁碟啟動磁**區（Boot Sector） 2. 會修改磁片的**檔案配置表**（FAT）或硬碟分割表 3. 若以中毒磁碟開機，病毒程式會比作業系統更早進入記憶體（RAM），取得磁碟控制權，感染其他磁片或硬碟。	米開朗基羅
檔案型	1. 隱藏在**可執行檔案中**（附檔名為 com 或 exe），依傳染方式不同，分成非常駐型及常駐型 2 種。 2. 當含有檔案型病毒的程式執行時，非常駐型病毒會嘗試去傳染給一個或多個檔案，而常駐型病毒則會「常駐」在記憶體（RAM）中感染其他可執行檔。	13 號星期五、兩隻老虎
混合型	兼具開機型及檔案型病毒，可加快病毒散播速度	大榔頭
巨集型 （文件型）	1. 以 VBA（Visual Basic Application）語言所寫成的巨集程式。 2. 隱藏在 **Word（.doc）、Excel（.xls）**等應用軟體的文件檔案中。	台灣 NO.1’釣魚台
蠕蟲（worm） 特洛伊木馬	1. 此類病毒或後門程式常隱藏於網頁、電子郵件中。 2. 常利用網路（E-mail、FTP）為傳染媒介。	梅麗莎、紅色警戒
間諜程式	1. 常利用共享軟體或免費軟體、電子郵件、含間諜程式的網頁為傳染媒介。 2. 主動掃瞄電腦系統、監視電腦活動，並進一步將電腦內機密資料（密碼、登入資料、帳號、檔案文件）隱密的傳送到網路上駭客的電腦軟體，造成系統當機、壅塞的網路連線、瀏覽器異常執行、洩漏帳號與密碼。	
隨身碟病毒 （USB 蠕蟲）	1. 利用系統自動播放 USB 隨身碟的功能來傳播，蠕蟲程式自己設定於 Autorun.inf 檔中，以便隨身碟插上電腦就可以自動被執行。 2. 中毒的特徵如隨身碟點兩下無法開啟、用檔案總管才可開啟、或是隨身碟的根目錄中自動產生 Autorun.inf 檔。	

六、電子交易安全：

（一）資料加/解密技術

1. 秘密鑰匙密碼術：對稱性密碼術，使用相同鑰匙加密及解密（DES）。
2. 公開鑰匙密碼術：非對稱性密碼術，具公開鑰匙和私人鑰匙（RSA）。

（1） 數位簽章（確保交易不可否認性）：傳送端以「傳送端私人鑰匙」加密，接收端以「傳送端公開鑰匙」解密，可確定資料由傳送端發出。

（2） 秘密通訊：非對稱性密碼術，傳送端以「接收端公開鑰匙」加密，接收端以「接收端私人鑰匙」解密，確保只有接收方才可看到完整資料。

班級：	姓名	座號
單元：3-2 資訊安全		教師：徐惠珠

（二）安全認證協定：

1.SET 與 SSL

安全機制	SET（電子商務安全交易）	SSL（安全資料傳輸層）
說明	由 VISA、Master 等信用卡公司與某些網路軟硬體公司所共同制定，用來保護網路上付款交易的安全規範。	Netscape 公司為了保護網路上資料傳輸的安全而制定的協定。
用途	線上交易付款過程中資料隱密性及傳輸完整性的保護。	普遍應用於各瀏覽器中的安全協定。定義於「應用層」及「傳輸層」之間，提供客戶端與伺服器端資料傳輸時加密的安全機制及驗證服務。
優點	1. 買賣雙方都必須取得數位憑證才能進行交易，可確認彼此身分的真實性。 2. 可以防範賣方盜用買方信用卡，也能保障買方購物的隱私權。	1. 消費者不需事先取得憑證即可使用，使用上比 SET 方便。 2. 可確保買方傳送給賣方的信用卡卡號不會在傳送過程中被竊取或竄改。
缺點	需向認證中心取得認證，手續較為麻煩。	無法讓賣方確認信用卡卡號是否為買方本人、或由本人親自授權，也無法防止賣方盜刷買方的信用卡。

八、BT 與 FTP 的比較：

比較項目	FTP	BT
網路拓撲	主從式	點對點
檔案所在位置	伺服器	分散在用戶端機器上
下載方式	連上伺服器下載	作為種子用戶端或其他擁有部分檔案片段的用戶端，會上傳資料給其他用戶端進行下載
支援檔案續傳	視伺服器是否支援	有
安全機制	可透過帳號、密碼管制使用，並設定檔案存取權限	沒有
優點	● 下載和上傳速度穩定 ● 可以監控和管制使用者，並限制檔案的存取權限 ● 檔案在固定的伺服器上，可以隨時下載	● 沒有下載人數限制，越多人下載，下載速度越快 ● 分享檔案有效率，可以減輕其他伺服器負擔
缺點	● 有人數限制，超過連線人數上限，要重新連線下載 ● 架設伺服器，需極大頻寬，才能負荷較多使用者下載 ● 愈多人下載，速度越慢	● 檔案來源不穩定，容易出現斷種問題 ● 下載檔案容易夾帶木馬、病毒，有安全上疑慮