**風險向量**

攻擊者發出威脅的方式，可以是攻擊者用來對付你的工具或所採用的攻擊路徑

**平均故障間隔(MTBF)**

估量預期中的系統或元件失效與意外，他計算元件預期壽命

**平均故障時間(MTTF)**

不可修復系統的平均故障時間，若可修復以MTBF來衡量

**平均回復時間(MTTR)**

一旦發生故障多久才能修復系統或元件

**復原時間目標(RTO)**

能夠承受最大停機或停止服務時間

**復原點目標(RPO)**

系統復原的時間點，越接近當機時間點成本越高

**安全性稽核項目**

檢查安全性日誌

檢視規定以及規定落實

檢查安全性裝置的組態

檢查事故回應報告

**嚴重程度分類**

輕微:不會立即威脅到安全性

嚴重:足以產生立即危脅，但可能性不高或難以被突破產生危害

重大:產生立即威脅，必須馬上處理

**蜂蜜罐(honeypot)**

設計用來作為攻擊標靶的電腦，在受害過程中系統可用來收集攻擊的資訊

**TCP/IP四層**

應用層:應用程式存取服務或通訊協定以交換資料;HTTP、HTTPS、FTP

傳輸層:提供應用層session與數據的通訊服務;TCP、UDP

網際網路層:負責找尋路徑，IP定位與包裝

網路存取層負責透過主機上的網路卡發出或接收實體網路上通訊用的封包

**封裝**

讓傳輸層通訊協定可以跨越網路傳送並被接收端的主機上對等的服務或通訊協定處理

**DMZ**

設置公開伺服器給未受信任使用者存取的區域

**穿隧通訊協定**

PPTP:

支援點對點的環境，PPTP將PPP封包封裝並加密，連線兩端點皆以明文交涉，交涉完後改以加密傳輸，使用TCP1723port

L2TP:

PPTP與L2F的混合，可在IPX、SNA與IP上運作，主要問題是不支援資料安全性，資訊並未加密，使用UDP1701port

SSH:

起初是在Unix上的穿隧通訊協定，以加密來建立兩系統間的安全連線，使用TCP22port

IPSec:

非穿隧通訊協定，但用來與穿隧通訊合作，主要用於區域網路對區域網路的連線，提供資料與標頭的全認證與加密

**遠端存取服務(RAS)**

任何提供遠端存取的服務，VPN、ISDN、DSL等技術達成，RAS連線可以是加密或明文

**網路轉址(NAT)**

用來輔助網路的安全性，提供IP位址給網路的主機或系統並追蹤出入境流量，如同本地網路可使用私用的網路位址

**防火牆功能類型**

封包過濾防火牆:根據應用程式類型，允許通過或拒絕，例如:HTTP 80port

代理伺服器防火牆:網路與其他網路間的中介，用來處理外部網路來的請求，檢視資料並根 據規則做出是否要轉發或拒絕的決定，通常使用兩塊網卡，一塊連結外 部，一塊連結內部

內容感知型封包檢查防火牆:紀錄以追蹤每個通訊通道的狀態表保存，他會記得封包從何處 來以及下一個應該從何處而來

**IDS四種主要方法**

行為檢測:觀察各種不同行為，例如:異常流量、違反規定

特徵檢測:根據檢測特徵與稽核紀錄來評估攻擊手法

異常檢測:查詢正常之外的事物，對不尋常的行為採取行動

啟發式:使用演算法來分析穿越網路流量，容易產生偽正面

**欺騙**

讓攻擊者以為攻擊成功，而系統持續監控並將攻擊者導向用來被突破的系統，可讓管理 者收集攻擊者的手法及相關資訊，例如使用honeypot

**認證系統的五個要素**

* 知悉:密碼或PIN
* 持有:智慧卡、記號或辨識裝置
* 生物:人臉或指紋
* 動作:完成認證要素所必須採取的動作
* 位置:根據地理位置

**認證協定**

* PAP:不再使用的系統，以直白文字送出帳號密碼給認證伺服器
* SPAP:取代PAP，主要差別是會將帳號密碼加密
* CHAP:連線的機器會被要求產生一個hash數字，送出給伺服器，伺服器會週期性的 要求用戶端出示該數字，攻擊者無法知道該數字並且無法認證
* TOTP:用於以時間要素所建構的密碼
* HOTP:依據HMAC演算法運作

**RADIUS**

可讓遠端透過NAS伺服器認證與其他網路連線的機制，使用IETF標準的AAA協定

**AAA**

指的是驗證(Authentication)，帳號管理(Accounting)與授權(Authorization)

**TACACS**

是一種安全控管的協定，使用在負責控管安全的伺服器與網路設備間溝通存取控制的資訊。當遠端使用者想要透過網路使用公司內部的資源時，必須 先經過安全伺服器的檢查與放行後，才能夠在網路上取得被授權的資源

**Kerberos**

kerberos 就是一種計算機網路的授權協議，可以用在非安全的網路環境中， 對個人通信以安全的手段進行身份認證。同時，客戶端與伺服器端均可向對方進行身份認證，因此可用於防止竊聽，保護資料完整性的應用中。 基本上， kerberos 是透過對稱式金鑰的方式來進行資料加密的

**單一簽入(SSO)**

使用者在登入後可以存取所需的程式與系統，不需要記住多組帳號密碼

**有線等效加密(WEP)**

無線網路的通訊協定，提供與有線網路等同的隱私性，使用RC4加密演算法，安全性非常低，可使用TKIP所產生的128位元加密鍵來加強，舊型裝置才用WEP

**無線應用協議(WAP)**

設計給無線裝置使用，是資料的傳輸標準，WAP功能等同於TCP/IP

**WPA與WPA2**

用來解決WEP問題，實作802.11i標準，WPA與WPA2差別在於WPA只實作出802.11i的部分標準，以便跟舊型裝置通訊，WPA使用RC4演算法與TKIP，WPA2則完整實作802.11i標準，並使用CCMP加密，難以破解並降低重放攻擊

**802.11i**

此標準提供認證以加強無線網路安全性

**軟體即服務(SaaS)**

讓消費者使用雲基礎上執行應用程式，可從各種裝置存取，例如:網頁郵件

**平台及服務(PaaS)**

讓消費者建立或購買應用程式，也可佈署應用程式在供應上的平台上執行

**基礎建設即服務(IaaS)**

供應商替消費者準備處理器、儲存空間、網路等硬體元件，消費者可在平台上佈署作業系統

**雲端四種運作方式**

私有:為組織企業自行建立自行使用

公用:為一般大眾公開準備的雲基礎建設

社群:由一個或多個社群中組織建立的服務

混合:由兩種以上不同的雲基礎建設所組成的個體

**存取控管清單(ACL)**

哪些使用者可以使用哪種權限存取哪些資源的清單

**叢集**

將多台電腦合併當作一台電腦運作，系統是利用平行處理

替代加密術

可將一個字元換成另外一個字元，或者將字母右移三位，A→D

多字母替代

將第一個字母右移三，第二個右移二，第三個右移一

轉位加密術

以特定方式轉位或打亂字母的順序

ROT13

將字母右移13個位置，A→N

對稱加密

加密與解密都是同一把金鑰，對稱加密演算法比非對稱快

常見對稱加密演算法

DES:使用56位元金鑰，因密鑰太小被認為不安全

3DES:DES的升級版，使用168位元密鑰

AES:支援128、192與256位元金鑰，預設為128位元

CAST:常使用於微軟與IBM產品，有CAST-128與CAST-256

RC4:常用在無線與WEP/WPA加密上，使用介於40~2048密鑰，也用在SSL/TLS

IDEA:使用128位元的密鑰，速度與功能類似DES，但更為安全

單次密碼本:真正安全的密碼實作，使用與明文一樣長的金鑰，使用一次立即拋棄

密鑰交換

同頻交換:密鑰是在被加密的同一個通訊通道上進行交換，IPSec使用此方式

異頻交換:使用被加密通道以外的其他通道交換

非對稱加密

發送方始用公鑰加密，接收方使用私鑰解密，公鑰可公開或私有，密鑰則擁有者或接收方知道，公鑰無法用來解密

四種非對稱系統

RSA:早期的公鑰加密系統，使用大整數作為運算的基礎

橢圓曲線加密(ECC):類似RSA的功能，但使用較小的密鑰以取得相同程度的安全性

雜湊演算法三個特質

必須是單向:表示無法逆向還原，一旦雜湊就無法反雜湊

不定長輸入產生定長輸出:兩個字元或兩百字元作雜湊，輸出大小都相同

必須有最小或沒有碰撞:雜湊兩個不同輸入不會產生相同輸出

SHA

是單向雜湊，此演算法產生160個位元的雜湊值，目前標準是SHA-3，但是SHA-2沒有發現問題所以還是被廣泛使用，SHA-2有224、256、334與512這幾種大小

MD

同樣也是單向雜湊，最常見的為MD5，他產生128位元的雜湊，最大弱點是沒有很強的防碰撞，因此不再推薦使用，替代方案為SHA-1或SHA-2

密碼破解技術

頻率分析:查詢加密過的訊息以判斷是否有重複的樣式

選定明文:攻擊者以自行選定的明文取得相對應的密文，這讓攻擊者推論出對方所使用的密 鑰以破解其他使用該密鑰的密文

暴力攻擊:透過嘗試每個可能字元組合來進行，但可能會花費很長時間

找尋人為失誤:密鑰交付給錯誤對象，洩漏密鑰內容

WIFI加密

WPA與RC4加密演算法組成TKIP而WPA2偏好CCMP，CCMP使用128位元的AES

加密系統存在原因

保密性:防止網路上洩漏未授權的資訊，即使不小心洩漏也無法看到加密內容

完整性:訊息在傳輸過程中不會被修改，一般方法是在訊息加入訊息認證碼(MAC)

認證:檢驗發送方是否如宣稱的身分，檢驗方法可使用數位簽章

不可否認性:防止一方否認自己所執行的動作，發送方可使用憑證來證明自己身分

數位簽章

類似文件上標準簽章的功能，使得完整性與送件者的可信，訊息使用加密系統加密，數位簽章被加入訊息中

SSL

用於兩台TCP機器之間建立安全通訊連線，使用握手建立session，session會保持開啟直到某一端發出指令將其關閉，通常是關閉瀏覽器

TLS

由SSL所衍生出的安全性協定

SSH

主要運用在終端機交談，握手程序與SSL類似，使用兩階段建立連線

階段一:以安全通道協調通道連線

階段二:以安全通道建立連線

PGP

是免費的郵件加密系統，使用對稱與非對稱加密作為程序的一部分，加密過程中，文件以公鑰與session key加密建立密文，session key在以公鑰加密並與密文一起送出，接收端使用私鑰來解開session key，之後再以session key與私鑰解開密文，成原始文件

IPSec

目前是VPN通道加密標準，且內建IPV6，被認為是高度安全，主要用途是建構VPN，IPSec在OSI第三層運作，主要協定是AH與ESP

PPTP

支援點對點環境中的封裝，PPTP將PPP封包封裝並加密，是網路上最常見的低階通訊協定，

PPTP兩端的連線皆以明文完成，之後才改以加密傳輸，這是PPTP主要弱點，使用1723port的TCP連線

L2F

由Cisco所開發，功能類似PPP，不能用於WAN，僅提供認證功能沒有提供加密

L2TP

是PPTP與L2F的混合，主要作為點對點的通訊協定，支援多種網路通訊協定且可以用於TCP/IP外的網路，主要問題是不支援資料安全性，資訊並未加密，安全性可透過IPSec提供

**公鑰基礎建設(PKI)**

提供大範圍訊息與交易安全性的方法，支援電子商務、安全交易、資訊隱私等需求，PKI是雙鑰非對稱系統，有四個主要元件:

憑證中心

註冊中心

RSA

數位憑證

**憑證中心(CA)**

負責發出、撤銷、分發憑證的組織，憑證會攜帶使用者資訊，可以是私用或公開的

**註冊中心(RA)**

分擔CA的工作，可以分發密鑰幫CA接受註冊與驗證個體，RA並不發出憑證

**PKI四種主要信任模式**

階層:頂端為根CA，中介CA只信任根CA提供的資訊，根CA也只信任中介CA，根CA系 統間可以互相信任，中介CA與葉CA也可互相信任

橋接:根CA之間存在用戶對用戶關係，根CA可與其他CA通訊以達成認證，每個中介CA 只信任以上或以下的CA

嚙合:每個根CA可與其他根CA交互認證，又被稱為網狀結構

混合:使用一種以上的結構

Dos攻擊

伺服器忙於回應假的請求，而沒時間處理正常的請求

常見Dos攻擊類型

ping of death:送出比系統所能處理更大的ICMP封包

緩衝區溢流:嘗試填入比緩衝區所能儲存更多的資料

DDos

透過多個電腦實行Dos攻擊，通常都是利用殭屍網路

欺騙攻擊

使用假的登入系統，無論使用者輸入什麼都會顯示錯誤，再竊取使用者輸入的資料

常見欺騙攻擊

IP spoofing:讓資料看起來像是來自信任的主機

ARP spoofing:使用假的MAC位址，取得網路存取權限，能夠通過白名單

DNS spoofing:讓DNS伺服器給出假的名稱解析，使用者會進入不是原本要去的網站

網址嫁接攻擊

重新導向將某主機的流量導向另一個主機

目錄遍歷攻擊

攻擊者透過HTTP存取受限目錄

資料政策

清除:資料如何從媒體上移除

處理:不再需要的媒體如何拋棄

保留:資料要保存多久

儲存:資料保存何處，有什麼存取安全機制

安全性概念

保密:防止未授權使用者存取資料

完整:確保資料未受到更改

可用:確保資料與系統對授權者可以使用

備份類型

完整備份:儲存所有檔案的備份

累積備份:只儲存上次完整備份後或累積備份後有異動的部分，星期日晚上執行完整備份， 周一晚上只會備份周日晚上之後的異動

差異備份:備份從上次完整備份後的異動檔案，但會重複備份上次異動備份後沒有異動過的 檔案，周日晚上執行完整備份，周一晚上差異備份會備份周日晚上之後的異動， 周二晚上的差異備份會備份周一與周二異動過的檔案

階層儲存管理:新的備份類型，可設定為最接近當前資料的即時備份