# 資訊安全常見詞彙補充

### Access Control

```

存取控制(Access Control):強制存取權限的各種機制。

防止未授權而使用資源,例如沒有權限便不能存取檔案。

```

### Active Attacks

```

主動式攻擊(Active Attacks)可以分成四類:偽裝、修改訊息內容、重送和阻絕服務。

被動式攻擊(Passive Attacks)的重點是在竊取資訊,或者監控資訊傳輸;

例如司法調查人員取得法官的監聽票所採取的監聽行為,就是一種被動式攻擊。

面對被動式攻擊,我們可以採用加密的技術來保護資訊,縱使攻擊者取得了資訊,

也無法或必須曠時費日才能得知資訊內容。

被動式攻擊偵測起來很困難,因為攻擊者不會變更任何資料。

因此在面對被動式攻擊時,處理的重點是預防而非偵測。

```

### ActiveX

```

Activex 控制項是一種小型軟體程式,有時候也稱為「附加元件」·適用於網際網路。

它們可藉由允許動畫提升您的瀏覧體驗,或是協助您的工作,例如安装Microsoft Update 上的安全性更新。

有些網站會要求您安裝Active控制項,以便看到網站內容或是執行網站上的特定工作。

當您造訪這類網站時,Internet Explorer會詢問您是否想要安裝Activex 控制項。

```

### ASLR 隨機記憶體編排

```

藉助 ASLR (Address Space Load Randomization,位址空間配置隨機化)功能。

ASLR以前在Unix系統中就有,在電腦一開機時,就可以將一些重要的系統檔案下載到不同的記憶體位置。

以前駭客只要完成某一個語系作業系統的攻學程式,就可以攻擊同一語系的電腦,

對於其他語系電腦的入侵,有時候甚至也不需要多加修改即可適用。

Vista加入 ASLR功能,讓每個作業系統記憶體空間位置編排隨機化,

「未來,Vista很難出現蠕蟲,也很難有大規模的病毒擴散,

「即使是緩衝區溢位攻鹦的漏洞,也很難利用透過推論記憶體位置的手法,再次成功攻擊,」

因為,ASR的功能讓開發人員連除錯(Debug)都很難」,「ASLR 功能讓駭客撰寫攻擊程式的難度變高,」

```

### Authentication

```

認證(Authentication ):確保通訊方的身份。

```

### Authentication Exchange

```

驗證交換(Authentication Exchange):藉由資訊交換的方法確認身份的機制。

```

### Availability Service

```

可用性(Availabiliy Service):系統的易用或可用的程度。

許多攻擊會導致系統失去或減少可用性,而有些攻擊可以經由認證(Authentication)和加密(Encryption)的方式來降低。

```

### CAIN

```

CAIN原則(CAIN principle),資訊安全關係密切的四項基本概念:

機密(confidentiality)

存取(access)

完整(integrity)

不可否認(nonrepudiation )

```

### Clandestine user

```

秘密客(Clandestine user):非法奪取系統管理員控制權限,並以此控制能力去逃避稽核和存取控制的人。

偽裝者有可能是企業外部的人,濫權者通常都是企業內部的人,

而不論企業內部或是外部的人都有可能是秘密客。

```

### Data Integrity

```

資料完整性(Data lntegrity):確保收到的資料和送出的內容完成相同。

```

### Digital Signature

```

數位簽章(Digital Signature):讓接收者可以證明資料的來源與完整性,並確保資料不被偽造。

```

### Event Detection

```

事件偵測(Event Detection ):偵測安全相關的事件。

```

### Masquerade

```

偽装(Masquerade)是相當基本的主動是攻擊類型,因此通常不會單獨使用,而會包

含其他類型的主動式攻擊。

```

### Misfeasor

```

濫權者(Misfeasor):雖然是合法使用者,但卻在未經授權的情況下增自存取,或是

有權可以存取但卻濫用特權的人。

```

### Modification of Message Content

```

修改訊息內容(Modification of Message Content) 會更改訊息的某一部份,或者延遲訊,息送出的時間。

```

### Nonrepudiation

```

不可否認性(Nonrepudiation):可防止發送端或者接收端否認發送的訊息。

```

### Notarization

```

公證(Notarization):利用信任的第三者來確保某些資料。

```

### Replay

```

重送(Replay)通常需要以上兩種攻擊來配合,例如先偽裝成另一個使用者的身份,

然後竊取並修改資訊內容,再重送給第三位使用者。

入侵者記錄檔在使用者和伺服器之間的網路交換程序,並在稍后時間重覆這一程序以偽裝成此使用者

```

### Rule-based detection

```

規則偵測法( Rule-based detection):這種方法定義了一組規則,然后比對規則與使用者的行為,

藉以決定使用者是否符合入侵者條件,這種方法會使用者以往的行為與目前行為之差異。

此外,也可以利用專家系統來辨識可疑的行為。

```

### Security Audit Trail

```

安全稽核追蹤(Security Audit Trail): 收集可能幫助安全稽核的資料。

```

### Security Label

```

安全標纸(Security Label):附於資源之上,用來表示資源安全属性的標記。

```

### Security Recovery

```

安全復原(Security Recovery):根據事件處理或管理功能等機制的要求,進行復原的動作。

```

### Threat

```

威脅(Threat):可能破壞系統安全的情況、能力或行為。

```

### Titan Rain

```

既雨計劃(Titan Rain)是從2003年起,一系列針對美國政府、軍火商、科學研究室

的電腦進行攻擊的行動。

普遍認為這些攻擊是源自於中國,但中國政府或解放軍是否涉入其中,至今仍然無從查證。

```

### Trusted Functionality

```

受信任的功能(Trusted Functionality):符合某些準則的功能,例如是依照安全原則所建立的功能。

```

### 存取控制

```

一種安全性機制,用以決定使用者、群組、服務或電腦已獲授權,

可在電腦或特定物件(例如檔案、印表機、登錄子機碼或目錄服務物件)上哪些作業。

```

### 存取控制清單(ACL)

```

套用到整個物件、一組物件的內容或一個物件的個別内容之安全性保護清單。

有兩種類型的存取控制清單:判別與系統。

```

### Active Directory

```

Windows 型的目錄服務·Active Directory 會儲存網路上物件的相關資訊,

並讓使用者及網路系統管理員可以使用此資訊。Active Directory使用單一登入處理程序,

授與網路使用者對網路上任意地方允許之資源的存取權。

它向系統管理員提供網路的直觀階層檢視及所有網路物件的單點系統管理。

```

### 防毒軟體(AV)

```

一種電腦程式,其設計目的為偵測及回應諸如病毒與蠕蟲等惡意軟體。

回應可能包括:阻止使用者存取受感染的檔案、清理受感染的檔案或系統,或者通知使用者已偵測到受感染的程式。

```

### 驗證

```

用以驗證某個實禮或物件是否與其所宣告者相同的程序,範例包括確認資訊的來源與完整性,

例如驗證數位簽章,或是駛證使用者或電腦的身分。

```

### 基本驗證

```

一種廣泛使用的業界標準方法,可用以收集使用者名稱和密碼資訊。大部分瀏覽器都支援基本驗證。

此驗證方法會提示使用者提供使用者名稱與密碼(也稱為認證),以未加密的形式透過網路傳送。基本驗證又稱為純文字驗證。

```

### 憑證

```

用來確認身分以及建立安全連結之使用者或伺服器識別資訊的加密檔案。

```

### 憑證授權單位(CA)

```

負責建立及擔保隸屬於主體(通常為使用者或電腦)或其他憑證授權單位之公開金錦真實性的實體。

憑證授權單位的活動包括:透過簽署的憑證將公開金鑰繋結至辨別名稱、管理憑證序號,以及撤銷憑證。

```

### 無類別網域間路由選擇(CIDR)

```

一種IP位址與路由管理方法,可藉由降低儲存於任何個別路由器上之路由數目、同時並增加可用IP位址數的方式,來配置IP位址。

CIDR 會取代以類別為基礎的P位址配置。

```

### 深度防禦

```

在網路中的多個點上使用安全性技術,以降低攻擊貫穿企業重要資源的整體可能性。

在電子郵件環境中,深度防翼可協助系統管理員確保惡意程式碼或活動可在電子郵件基礎結構中的多重「檢查點」上遭到攔截

進而降低某項威脅入侵的可能性。

```

### 阻絕服務攻撃(DoS)

```

攻擊資訊系統中的弱點或設計限制,藉以讓合法使用者無法存取資源(通常為網路服務)的惡意(或粗心的)使用者、處理程序或系統。

DoS 攻擊的範例包括建立大量網路連線、填滿磁碟儲存、停用通訊埠或移除電源。

```

### 字典攻撃

```

此方法會誉試以字典中的每個文字來猜測使用者密碼或 PIN,直到成功為止。

```

### 目錄搜集攻擊

```

一種嘗試,會從特定組織收集有效的電子郵件地址,以便將電子郵件地址加入垃圾郵件資料庫中。

```

### 網域名稱系統(DNS)

```

一種階層分散式資料庫,含有各種資料類型(如IP位址)的DNS網域名稱對應。

DNS 可讓您使用好記的名稱來設定電腦與服務的位置,也可讓您探索資料庫中儲存的其他資訊。

```

### 網路釣魚

```

誘使電腦使用者洩漏其個人或金融資訊的技術,常見的線上網路釣魚詐騙手法是,

寄出看似來自信任來源的電子郵件訊息,但實際上曾誘使收件者提供資訊給偽造的網站。

```

### 公開金鑰

```

密碼編譯金鑰組中不屬於機密的部分,可與公開金鑰演算法搭配使用。

公開金鑰通常用於加密工作階段金鑰、驗證數位簽章、或為可使用對應秘密金鑰加以解碼的資料進行加密等情況。

```

### 規則

```

執行郵件原則之單一功能點的概念,此規則中含有一些一般設定、

何時觸發此規則的相關設定,以及騰發規則時將如何因應的相關動作集(依序排列)。

此外,每個規則均可有例外狀況,以指定要排除在條件外的項目。

例外狀況通常會識別條件中所識別的搜尋條件子集。

```

### 規則集合

```

用以執行郵件原則的規則集(依序排列)。規則集合的數目是在設計期間所定。

```

### 安全通訊端層(SSL)

```

一項建議的公開標準,可用以建立安全通訊通道,防止重要資訊(如信用卡號碼)遭

到截取。其主要功能在於促使全球資訊網上的安全電子金融交易,但根據設計,它也可運用在其他網際網路服務上。

```

### 寄件者原則架構(SPF)

```

SMTP 通訊協定的延伸,藉由驗證SMTP Received:標頭中的IP位址有權傳送寄件者網域的電子郵件

,可防止濫發垃圾郵件者在電子郵件訊息中偽造[寄件者]欄位。

```

### 簡易郵件傳送通訊協定

```

(SMTP) TCP/IP 通訊協定組的成員之一,負責管理郵件傳輸代理程式間的電子郵件交換。

```

### 垃圾郵件

```

未經同意的廣告郵件。也稱為垃圾電子郵件。

```

### 冒名郵件

```

此類電子郵件的傳送地址已遭修改,使其看似來自實際郵件寄件者以外的寄件者。

```

### 詐騙

```

電子郵件寄件者、IP連線或網域的模擬,讓電子郵件看似來自實際郵件寄件者以外的奇件者。

```

### 三重要素驗證

```

需要三種驗證方法的驗證方法,其中可能包括下列項目:使用者所提供的內容(如認證)、

使用者具備的資訊(如使用者名稱、密碼或密語)、實體屬性(如指紋),以及個人屬性(如個人簽章)。

```

### 傳輸層安全性(TLS)

```

通訊協定,提供兩個應用程式透過網路通訊時的通訊隱私權及安全性TLS加密可進行通訊,

並讓用戶端駛證伺服器,且選擇性地讓伺服器驗證用戶端,TLS 是較安全的安全通訊端層(SSL)通訊協定版本。

```

### 特洛伊木馬

```

看來有用或無害的程式,但是包含的隱藏程式碼是設計來惡意探索或破壞所執行的系統。

特洛伊木馬(Trojan Horse)程式最常透過假造程式用途及功能的電子郵件傳遞給使用者。

也稱為特洛伊木馬程式(Trojan Code )。

```

### 雙重要素驗證

```

需要兩種驗證方法的驗證方法,其中可能包括下列項目:使用者所提供的内容(如認證)、

使用者具備的資訊(如使用者名稱、密碼或密語)、實體屬性(如指紋),以及個人屬性(如個人簽章)。

```

### 使用者資料包通訊協定(UDP)

```

TCP/IP 内的不連線通訊協定,

會對應到International Standard Organization's OpenSystem Interconnect(ISO/OI)參考模型中的傳翰層。

UDP 将應用程式產生的資料訊息轉換成透過IP傳送的封包,但它並不可靠,

因為它在傳輸之前並没有在寄件者和收件者之間建立路徑,且不會駛證訊息是否正確傳遞。

UDP比TCP更有效,因此可用於多種用途,包括簡易網路管理通訊協定(SNMP)。

可靠性會視產生訊息的應用程式而定。

```

### 虚擬私人網路(VPN)

```

使用網際網路,將一或多部電腦連接至大型網路(如公司網路)的網路。

VPN 會加密,因此只有授權的人員才可加以存取。

```

### 病毒

```

惡意電腦程式,特別設計來複寫它自己並擴散到不同電腦。病毒可能會破壞硬體、軟體或資料。

```