資訊安全

保密性(confidentiality)、完整性(integrity)、可用性(availability)、

責任性(accountability)

工控系統(ICS)異常 🡺 在資安防護上最應先考量”可用性”

兩個網路使用者共同用秘密金鑰進行認證程序：

其中一方先產生一組隨機訊息給對方(隨機訊息以secret key加密)

對方以secret key加密後回傳

比較對方加密後回傳的隨機訊息

對稱性加密法(symmetricall key encryption)=單一鍵值加密系統(single key encryption)=秘密金鑰系統(secrect key) 🡺加解密端都有加/解密鑰匙，這個共同鑰匙稱為秘密鑰匙(secrect key)

Ex: DES、Triple DES、IDEA 🡺加/解密速度快。適合長度常跟大量的資料。缺點是不容易管理金鑰

非對稱加密系統(或稱雙鍵加密系統(Double key Encryption)：

目前較普遍，也是金融界應用上最安全的加密系統

🡺公開金鑰(public key)+私密金鑰(private key)

🡺公開金鑰在網路上流傳(必須藉由憑證管理中心來簽發公開金鑰)，私密金鑰由私人保管

Ex:RSA

數位簽章：用自己的私鑰加密HASH過的明文然後再跟明文一起傳送

認證：

用自己的私鑰加密再用對方的公鑰加密，再傳送

SSL和SET：都具有資料傳輸的隱密性、完整性

安全等級： SET > SSL

SET還具有交易的不可否認性

SSL(Secure Sockets Layer)、TLS(Transport Layer Security)：<https://zh.wikipedia.org/wiki/%E5%82%B3%E8%BC%B8%E5%B1%A4%E5%AE%89%E5%85%A8%E6%80%A7%E5%8D%94%E5%AE%9A>

SSL：

網際網路上報密通訊的工業標準

包含紀錄層(確定傳輸層的封裝格式)和傳輸層(安全協定使用X.509認證，之後再利用**非對稱加密演算**來對通訊方做**身分認證**，然後交換**對稱金鑰**作為**會談金鑰**(session key))

2015年，[RFC 7568](https://tools.ietf.org/html/rfc7568) 標準棄用了SSL 3.0。

SET：(電子錢包符合SET交易標準)

[IETF](https://zh.wikipedia.org/wiki/%E4%BA%92%E8%81%94%E7%BD%91%E5%B7%A5%E7%A8%8B%E4%BB%BB%E5%8A%A1%E7%BB%84)將SSL標準化，即 [RFC 2246](https://tools.ietf.org/html/rfc2246) ，並將其稱為TLS（Transport Layer Security）。

TLS協定採用[主從式架構](https://zh.wikipedia.org/wiki/%E4%B8%BB%E5%BE%9E%E5%BC%8F%E6%9E%B6%E6%A7%8B)模型，用於在兩個應用程式間透過網路建立起安全的連線，防止在交換資料時受到[竊聽](https://zh.wikipedia.org/wiki/%E7%AB%8A%E8%81%BD)及篡改。

TLS協定的優勢是與高層的[應用層](https://zh.wikipedia.org/wiki/%E5%BA%94%E7%94%A8%E5%B1%82)協定（如[HTTP](https://zh.wikipedia.org/wiki/%E8%B6%85%E6%96%87%E6%9C%AC%E4%BC%A0%E8%BE%93%E5%8D%8F%E8%AE%AE)、[FTP](https://zh.wikipedia.org/wiki/%E6%96%87%E4%BB%B6%E4%BC%A0%E8%BE%93%E5%8D%8F%E8%AE%AE)、[Telnet](https://zh.wikipedia.org/wiki/Telnet)等）無耦合。應用層協定能透明地執行在TLS協定之上，由TLS協定進行建立加密通道需要的協商和認證。應用層協定傳送的資料在通過TLS協定時都會被加密，從而保證通訊的私密性。



加密技術

非對稱性加密技術：RSA、ECC

對稱性加密技術：DES、AES、3DES

網路安全

零時差攻擊：**所謂零時差攻擊就是利用尚未修補的漏洞進行攻擊。通常，未修補的漏洞在廠商釋出修補更新之前，就是一場駭客與廠商之間的競賽，前者試圖開發漏洞攻擊手法，後者則試圖修補漏洞。**

**所謂的零時差漏洞是指**[**軟體**](https://blog.trendmicro.com/the-patching-problem-best-practices-for-maintaining-up-to-date-systems/)**、**[**韌體**](https://blog.trendmicro.com/trendlabs-security-intelligence/upnp-enabled-connected-devices-in-home-unpatched-known-vulnerabilities/)**或**[**硬體**](https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/meltdown-and-spectre-intel-processor-vulnerabilities-what-you-need-to-know)**設計當中已被公開揭露但廠商卻仍未修補的缺失、弱點或錯誤。或許，研究人員已經揭露這項漏洞，廠商及開發人員也已經知道這項缺失，但卻尚未正式釋出更新來修補這項漏洞。**

這樣的缺失就是所謂的「零時差」漏洞，因為廠商及開發人員 (以及受此漏洞影響的企業和使用者) 才剛知道這個漏洞的存在。隨後，當廠商及開發人員針對這個漏洞提供了修補更新，那這漏洞就會變成「已知」漏洞 (有時亦稱為 N-day 漏洞)。

網路竊聽：擷取並分析網路通訊

現在防火牆的主要功能：DMZ區段設置、SQL Injection阻擋、存取控制

**Heartbleed**

<https://www.ithome.com.tw/news/86593>

<https://zh.wikipedia.org/wiki/%E5%BF%83%E8%84%8F%E5%87%BA%E8%A1%80%E6%BC%8F%E6%B4%9E>

**什麼是Heartbleed臭蟲？**

這個漏洞存在OpenSSL的TLS/DTLS 傳輸安全層的heartbeat（心跳）擴充功能之中，該漏洞受到攻擊時會造成記憶體內容的外洩，可能從伺服器端外洩到客戶端，或者由客戶端外洩到伺服器端，因此研究人員將它命名為Heartbleed bug，Heartbleed也就是「心在淌血」的意思。

這個漏洞並不是SSL/TLS協定的問題，而是OpenSSL函式庫的程式錯誤。

**CVE**

<https://zh.wikipedia.org/wiki/%E5%85%AC%E5%85%B1%E6%BC%8F%E6%B4%9E%E5%92%8C%E6%9A%B4%E9%9C%B2>

可提供資訊安全領域，有關電腦系統弱點及漏洞相關資訊

**公共漏洞和暴露**（英語：CVE, Common Vulnerabilities and Exposures）又稱**通用漏洞披露**、**常見漏洞與披露**，是一個與[資訊安全](https://zh.wikipedia.org/wiki/%E8%B3%87%E8%A8%8A%E5%AE%89%E5%85%A8)有關的[資料庫](https://zh.wikipedia.org/wiki/%E8%B3%87%E6%96%99%E5%BA%AB)，收集各種資安弱點及漏洞並給予編號以便於公眾查閱。此資料庫現由美國非營利組織[MITRE](https://zh.wikipedia.org/w/index.php?title=MITRE&action=edit&redlink=1)所屬的[National Cybersecurity FFRDC](https://zh.wikipedia.org/w/index.php?title=National_Cybersecurity_FFRDC&action=edit&redlink=1)所營運維護[[](https://zh.wikipedia.org/wiki/%E5%85%AC%E5%85%B1%E6%BC%8F%E6%B4%9E%E5%92%8C%E6%9A%B4%E9%9C%B2#cite_note-1)

ISO27001:2013

ISO27001:2005

<https://www.cc.ntu.edu.tw/chinese/epaper/0030/20140920_3003.html>

2013年版本新增了兩個領域分別是

A.10密碼(Cryptography)領域與

A.15供應商關係(Supplier Relationships)領域，並將原本

A.10通訊與作業管理(Communications and operations management)領域分成

A.12作業安全(Operations Security)與A.13通訊安全(Communications Security)兩個領域

Wi-fi加密方式

加密(Encryption)：封包資料在進行無線傳輸時，因為受到密碼保護，所以第三方人士無法讀取其中的資訊

|  |  |
| --- | --- |
| WEP  (wired equivalent privacy) | 最基本的加密方式  安全技術源自於RC4的RSA數據加密技術  採用802.11技術，但現在路由器大多用802.11n技術🡺加密時多少會影響無線網路設備的傳輸速率 |
| WPA/WPA2/WPA3  Wi-fi網路安全存取  (WiFi Protected Access) |  |
| WPA-PSK/WPA2-PSK |  |