

Glossary for Information Security Terms

資訊保安詞彙表

A

Access Control System 接達控制系統

The system of preventing unauthorised access to the resources of an IT product, programs, processes, systems, or other IT products. Some suppliers consider preventing unauthorised users from logging on to the system to be access control. In reality, access control should also stop logged on users accessing objects (files, devices, etc) for which they have no authorisation.

該等系統用以防止未經授權接達資訊科技產品、程式、程序、系統等的資源，又或其他的科技產品。部分供應商認為接達控制乃防止未獲授權用戶登入系統。事實上，接達控制也應阻止已獲接達的用戶接達到未獲授權的物件（檔案、設備等）。

Active Jamming 主動干擾

Active jamming of RF signals refers to the use of a device that actively broadcast radio signals in order to disrupt the operation of any nearby RFID readers.

主動干擾即使用儀器頻密地廣播無線電訊號以干擾 RF 訊號，從而擾亂附近 RFID 閱讀器的運作。

Address Spoofing 位址仿冒

It's simply an action to forging an address. One example is IP spoofing.

位址仿冒即假冒他人位址，例如 IP 仿冒。

Administrative Security 行政性保安

It refers to the use of management procedures and mechanisms to prevent unauthorized access to a system.

運用管理程序和機制以防止未獲授權接達系統。

Adware 廣告軟件

Adware is software that displays advertising banners while the program is running. A lot of adware is also spyware.

當廣告軟件運行時會顯示廣告標語。很多廣告軟件同時也是偵測軟件。

AES Algorithm

AES algorithm is a symmetric block cipher (encryption algorithm) that is based on Rijndael algorithm and uses key sizes of 128, 192, or 256 bits to operate on a 128-bit block.

AES 加密算法是以 Rijndael 算法為基礎的對稱分區加密（加密算法），採用 128、192 或 256 位元的密碼匙在 128 位元的區塊運作。

Alias 別名

An assumed or alternate name. Some viruses are given multiple names since there is no real standard for naming computer viruses.

假名或另一名稱。由於電腦病毒命名並無實際準則，因此有些病毒有多個名稱。

Anti-antivirus Virus 反防毒病毒

A virus that attacks, disables, or avoids infecting specific anti-virus software. Also called a retrovirus.

會攻擊某種防毒軟件、令其失效或會避開防毒軟件的病毒。亦稱 retrovirus。

Anti-spyware Software 間諜防護程式

Anti-spyware software is computer software that detects and cleans spyware.

間諜防護程式是偵測及清理間諜軟件的電腦軟件。

Anti-virus Software 抗電腦病毒軟件

A software that is designed to stop viruses, eliminate viruses, and/or recover data affected by viruses.

該等軟件乃設計來阻止和消滅電腦病毒，及／或把受到電腦病毒感染的數據復原。

Antivirus Virus 防毒病毒

A virus that specifically looks for and removes another virus.

專門尋找並移除另一種病毒的病毒。

Application Gateway 應用通訊閘

A system used to restrict access to services or functions across a firewall boundary.

該等系統用以限制穿越防火牆範圍來接達服務或功能。

Asymmetric Encryption 非對稱加密法

Two different keys are used with one for encryption and the other for decryption. The decryption key cannot be derived from the encryption key.

使用兩條不同的密碼匙分別用以加密和解密的加密法，但不能根據用以加密的密碼匙計算出解密的密碼匙。

Audit Trail 審計追蹤

Audit trail is defined as a chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event.

審計追蹤被定義為按系統活動的時間先後記錄，可以用作重組和檢查一組事件的發生次序，及／或一事件的連串變化。

Authentication 認證

A process or method to identify and to prove the identity of a user/party who attempts to send message or access data. Message authentication refers to a process used to prove the integrity of specific information.

用以辨識及證明嘗試發出信息或接達數據的用戶／一方身份的程序或方法。信息認證指用以證明特定資訊的完整性的程序。

Authentication Token 認證權標

A portable device operates by using challenge/response, time sequence, or other techniques in order to authenticate a user.

採用質疑／應答、時間順序或其它技巧以認證用戶的可攜式設備。

Authorisation 授權

A process to grant rights to a person for accessing data or using specific information resources.

把接達數據或使用特定資訊資源的權利批給某人的程序。

Availability 可用性

A condition in which information or processes are reasonably accessible and used by an authorised party including timely and critical operations.

獲授權一方可合理地接達及使用資訊或程序的狀態，包括及時和重要的運作。

B

Backdoor

Backdoor is a general term for a malicious program that listens for commands on a certain network port. Most backdoors consist of a client component and a server component. The client resides on the intruder's remote computer, and the server resides on the infected system. When a connection between client and server is established, the remote intruder has some degree of control over the infected computer.

Backdoor 指惡意程式以某網絡端口竊聽指令。大部份 backdoor 分為客戶端和伺服器兩部份，入侵者的遙距電腦便是客戶端，伺服器則附於受感染的系統上。當客戶端和伺服器連接起來，遙距的入侵者便可以某程度控制受感染電腦。

Backup 備份

Copies of programs, databases and other files made with the purpose of allowing the information to be restored if it is lost due to computer failure, virus infection or other unforeseen event.

程式、數據庫或其它檔案的副本。在因電腦發生故障、受病毒感染或其它無法預計的事件而令資料遺失時，可利用備份資料進行資料復原。

Biometric Identification 生物特徵識別技術

Use of measurable physiological characteristics to authenticate a user such as fingerprints or facial characteristics.

使用可量度的生理特徵，例如：指紋或面部特徵，以認證用戶的身份。

Blocker Tag 阻塞器標籤

A blocker tag is a device that uses a sophisticated algorithm to simulate many ordinary RFID tags simultaneously.

阻塞器標籤是裝置以先進的算法同時地模擬多個普通的 RFID 標籤。

Botnet 殭屍網絡

A botnet is a network of zombie computers under the remote control of a master.

殭屍網絡即主機遙距控制殭屍電腦所組成的網絡。

Brute Force Attack 暴力攻擊

Brute force attack is a technique used to break an encryption or authentication system by trying all possibilities.

暴力攻擊是嘗試所有可能性以破解加密或認證系統的技術。

Buffer-overflow Attack 緩衝區滿溢攻擊

An attack exploits a process to read in data beyond the boundary of a fixed-length buffer, with an aim to overwrite computer memory by a carefully crafted data and execute privilege instructions in an unintended way.

利用程式在指定長度的緩衝界限以外讀取資料所構成的攻擊，目的是以特別編寫的資料蓋寫電腦記憶體，並且不正當地以特別權限執行指令。

C

Captive Portal 捕獲門戶

A landing page is shown whenever the user starts a new browser session on the wireless network from their client device.

每當用戶透過無線網絡在自己的設備啟動一個新的瀏覽器對話時，登陸頁面便會顯示出來。

Centralised Identity Management 集中化身份管理

Centralised identity management a model of identity management in which the same identifier and credential are used by each service provider.

集中化身份管理是身份管理模式的一種，在此模式中，每一個服務提供者可使用相同身份認證工具和憑證。

Certificate 證書

An electronic document attesting to the binding of a public key to an individual or entity. It allows verification of the claim that a specific public key belongs to a specific individual. A certificate is issued and digitally signed by a trusted third party or Certification Authority.

用以核實公開密碼匙與個人或實體關係的電子文件。該文件可核證某特定公開密碼匙屬於特定人士的聲稱，並由獲信任的第三方或核證機關發出和加上數碼簽署。

Certification Authority 核證機關

A trusted authority or party that digitally signs certificates in order to validate the identity of a person or party.

在證書加上數碼簽署以核實某人或某一方身份的獲信任機構或一方。

Certificate Management 證書管理

A management mechanism includes tasks of storage, dissemination, publication,

revocation and suspension of certificates.

包括貯存、分發、公布、撤銷及暫時吊銷證書的管理機制。

Certificate Revocation List (CRL) 證書撤銷清單

Certificate Revocation List (CRL) is periodically issued list, digitally signed by the Certification Authority, of identified certificates that have been suspended or revoked prior to their expiration dates. It normally shows information such as the CRL issuer's name, date of issue, suspended or revoked certificate's serial numbers.

證書撤銷清單是一份經核證機關加上數碼簽署的定期發出的清單，載列在屆滿日期前遭暫時吊銷或撤銷的經辨識的證書。這份清單一般載列的資訊計有證書撤銷清單發出人姓名、發出日期、暫時吊銷或撤銷證書的編號。

Certificate Server 證書伺服器

A server which performs the certification process of public keys.

執行公開密碼匙核證程序的伺服器。

Challenge / Response 質疑／應答

An authentication technique used by a system/server to authenticate a user. A server usually sends an unpredictable challenge (a set of numbers or letters) to the user, and the client/user will then compute a response using some special form of authentication token.

系統／伺服器採用的用以認證用戶身份的認證技巧。伺服器通常會發出不可預測的質疑（一組數字或字母）給用戶，而客戶／用戶會使用某種特別形式的認證權標計算應答。

Ciphertext 加密文本

A scrambled / cryptic content derived from plaintext using an encryption algorithm.

使用加密算法把原文轉為混亂和不可閱讀內容的信息或數據。

Client Authentication 客戶認證

It refers to the process in which a server verifies the identity of a client before allowing it to gain access.

指伺服器在准許客戶接達前核證其身份的程序。

Code Injection Attack 代碼插入攻擊

An attack technique to introduce code into a computer program or system to form an unexpected action. The attack is usually accomplished by taking advantage of an un-enforced or loosely implemented input validation process.

在電腦程式或系統中插入代碼所構成的攻擊，通常利用薄弱或容易受攻擊的輸入確認程式來達成入侵目的。

Common Criteria 通用條件

Please see ISO/IEC 15408.

請參閱 ISO/IEC 15408。

Companion Virus 伴隨病毒

A virus that creates a new program with the same file name as an existing program, but in a different place or with a different file type, so that typing the program's name on the command line causes the virus program to be executed instead of the original program.

此病毒建立一個與現有程式名稱相同的新程式，並將新程式放置於不同地方或具有不同檔案類型。在指令行輸入該程式名稱時，會執行病毒程式而取替執行原有程式。

Compromise 破解

A violation of a security policy in which an unauthorised access to a system, disclosure or lost of sensitive information may be resulted.

一種違反保安政策的情況，可能導致敏感資訊遭未獲授權的披露或遺失。

Computer Emergency Response Team (CERT) 電腦緊急應變小組

An organisation that provides incident response services, publishes alerts and threats, about vulnerabilities, as well as other information on computer and network security.

這個組織提供事故應變服務、發布保安警告和威脅，以及其它電腦和網絡保安的資訊。

Confidentiality 機密性

The condition in which the sensitive data is protected and disclosed to authorised parties only, e.g. assurance of privacy using encryption or other methods.

敏感數據受到保護及只向獲授權一方披露的情況，例如：使用加密法或其它方法以確保私隱受到保護。

Control Objectives for Information and related Technology (COBIT) 資訊系統稽核與控制標準

The Control Objectives for Information and related Technology (COBIT) is a control framework that links IT initiatives to business requirements, organises IT activities into a generally accepted process model, identifies the major IT resources to be leveraged and defines the management control objectives to be considered.

資訊系統稽核與控制標準（COBIT）是一個連結 IT 主導與商業需要的控制架構，組織 IT 活動令其成為廣受接納的程序模式，指出重要的 IT 資源並予以善用，同時定義要考慮的管理控制標準。

Cracker 電腦破壞者

An individual with malicious intent who attempts to gain unauthorised access to other's system.

個別人士嘗試在未獲授權情況下進入他人電腦並作出破壞。

Cross-certification 互相核證

A condition in which two or more different certificate issuing authorities trust among themselves by issuing certificates having the other as the subject of the certificate.

兩間或以上的不同發出證書的機關，彼此透過信任向對方發出以對方為主體的證書的情況。

Cross Site Request Forgery 跨網站請求偽造

Cross site request forgery is an attack that forces a logged-on victim's browser to send a pre-authenticated request to a vulnerable web application, which then forces the victim's browser to perform a hostile action to the benefit of the attacker.

跨網站請求偽造是網上攻擊的一種，它強迫登入者的瀏覽器寄發預先驗證的要求給具保安漏洞的網上應用系統後，強迫使用者的瀏覽器執行惡意行為而使攻擊者獲利。

Cross Site Scripting 跨網址程式編程

Cross site scripting is a flaw in web application that allows the execution of scripts in the victim's browser to hijack user sessions, deface websites, and possibly introduce worms, etc.

跨網址程式編程攻擊（XSS）是網上應用系統保安漏洞的一種，它允許在受害者的瀏覽器執行手稿程式（Script），導致劫持用戶對話、竄改網站並可能植入蠕蟲等等。

Cryptography 密碼學

Cryptography is the art of keeping messages secret by using different methods. It normally deals with all aspects of secure messaging, authentication, digital signatures, and electronic money. Cryptanalysis is the art of breaking these methods. Cryptology is the study of cryptography and cryptanalysis.

密碼學是指把信息保密的技術。它處理與穩妥信息傳送、認證、數碼簽署及電子貨幣等所有範疇的工作。加密分析指破解這些方法的技術。加密學是有關加密法和加密分析的研究。

Cyclic Redundancy Code (CRC) 循環冗餘碼

A CRC is a type of checksum. A checksum algorithm takes a file (or other string of bytes) and calculates from it a few bytes (the checksum) that depend on the entire file. The idea is that, if anything in the file changes, the checksum will change. CRC checksums are usually used to detect random, uncorrelated changes in files.

循環冗餘碼 (Cyclic Redundancy Code)，是一種檢驗和 (Checksum)。檢驗和算法取出檔案 (或其它字元串) 並根據整個檔案而計算其少量字元 (檢驗和)。其意念是，若檔案中有任何轉變，檢查和亦會轉變。循環冗餘碼檢驗和通常用以偵測檔案中隨意、不相關的改變。

D

Data Driven Attack 數據導引式攻擊

A form of attack encoded in innocuous-seeming data which is then executed by a user or software to enforce the attack.

這是一種隱藏在似乎是無害的數據內的攻擊形式，一旦用戶或軟件執行編碼便會發動攻擊。

Data Encryption Algorithm (DEA)

Data Encryption Algorithm (DEA) is a symmetric block cipher (encryption algorithm) which uses a 64-bit key. The DEA is specified by the Data Encryption Standard (DES). Therefore, the DEA algorithm is usually referred to as "DES".

數據加密算法（DEA）使用 64 位元的密碼匙，是對稱的分區加密（加密算法）。DEA 由數據加密標準（DES）而來，因此，DEA 算法通常被指為「DES」。

Decryption 解密

The reverse process of encryption in which encoded messages or ciphertext is decoded from its protected, scrambled form into original plaintext so that they can be easily readable.

把文本加密的相反程序，即把經加密的信息或加密文本從受保護和混亂的形式轉回原文形式，以便閱讀。

Defence-in-Depth 縱深防禦

Defence-in-depth represents the use of multiple information security techniques as well as security guidelines, policies and safeguarding procedures to help prevent a shortfall in any one defence leading to a wider failure.

縱深防禦是利用多重資訊保安技術和保安指引、政策及保衛程序，幫助防止受攻擊，以免引致更大的傷害。

Denial of Service 拒絕服務

A prevention of the use of information resources either intentionally or unintentionally, which affects the availability of the information resources. Examples of such attacks are SYN flood, Ping O death, packet flooding and Ping flooding.

蓄意或並非蓄意的引致資訊資源的使用受阻，以致資訊資源的可用性受到影響。這類攻擊的例子計有大量的 SYN，「致命小包」，小包氾濫及 Ping 氾濫等。

Detective Control 偵測性措施

Detective controls are used to identify undesirable events that have occurred.

偵測性措施是用來識別已發生的不利事件。

Dictionary Attack 字典攻擊

Dictionary attack is a technique used to break an encryption or authentication system by trying words that can be found in a dictionary.

字典攻擊是使用字典中可找到的字，用以破解加密或認證系統的一種技術。

Diffie Hellman Algorithm [Diffie Hellman 機制]

It is an algorithm for key agreement. The key established can be further used as a key for encryption or other cryptographic operations.

這是密碼匙協議的機制，密碼匙可用作加密的密碼匙或其它加密工序。

Digital Certificate 數碼證書

A file in electronic format in which data stored can be used to verify the identity of the certificate owner. The certificate usually contains information such as user's public key, name and email address.

以電子形式發出的證書，其所儲存的數據可用以核實證書擁有人的身份。證書通常包含的資訊包括用戶的公開密碼匙、姓名及電子郵件地址。

Digital Signature 數碼簽署

A block of fixed-length data computed with a cryptographic algorithm that can be used by recipient of the data to verify the data's origin and integrity.

一個區塊的固定長度數據以加密算法運算，使數據接收者可核實數據的來源和完整性。

Direct Infector 直接傳播病毒程式

It is a virus that activates when an infected file is executed.

直接傳播病毒程式指在執行已受感染的檔案時所發作的電腦病毒。

Discretionary Access Control (DAC) 自主接達控制

Discretionary Access Control (DAC) is an authorisation mechanism in which users own the objects under their control, and the granting and revoking of access control privileges are left to the discretion of individual users.

自主接達控制是一授權機制，用戶擁有可以控制的物件，個別用戶有權決定接達控制權的許可或是撤回。

Distributed Denial of Service (DDoS) Attack 分佈式拒絕服務攻擊

An attack using multiple computers to launch denial-of-service (DoS) attacks at the same time against a targeted system.

利用多台電腦向同一目標系統同時發動 DoS 攻擊。

DNS Spoofing 領域名稱系統仿冒

Pretend to be the DNS name of another system by compromising the domain name server for a valid domain.

某有效域名的領域名稱伺服器的資料被他人盜用，藉此假冒另一個系統的領域名稱系統的域名。

Drive-by attack [Drive-by 攻擊]

Drive-by attack is used by attackers who construct URL(s) embedded with malicious scripts in a website, where the users are tricked to click on the URL allowing the embedded script running on their web browsers and resulting in more malignant attacks (such as downloading a Trojan Horse or sending cookie information to the attacker).

Drive-by 攻擊是由攻擊者在網頁中編制一個或數個已嵌入惡性手稿程式的劃一資源定位，藉此引誘目標用戶點擊此劃一資源定位，讓隱藏在內的手稿程式在用戶的瀏覽器開始運作，造成更惡性的攻擊如下載木馬程式或把 cookie 資訊傳送給攻擊者。

Dropper 病毒安裝程式

A dropper is a program that installs a virus or Trojan Horse. Dropper by itself is not a virus.

這是一種用以安裝電腦病毒或特洛伊木馬的程式，但它本身不是一種病毒。

E

Encryption 加密

A process to encode the contents of message so as to hide it from outsiders. That is, it is a process of scrambling and transforming data from an easily readable and understandable format (plaintext) into an unintelligible format that seems to be useless and not readily understandable (ciphertext).

把信息內容編碼以防止外人讀取程序，即把易於讀取和了解的數據格式（原文）加以更改及轉變，使其轉為不可讀取的格式（加密文本），令人看起來是一組無用及難以了解的文本。

Extensible Access Control Markup Language (XACML) 可擴展接達控制標記語言

XACML is an OASIS standard for expressing policies for information access over the Internet using XML. It is based on the access control matrix model and allows for defining authorisation rules for each element of an XML document, or the document as a whole.

可擴展接達控制標記語言（XACML）是 OASIS 以 XML 來表達在互聯網上信息接達政策的一個標準。在接達控制矩陣模型的基礎上，讓使用者可定義 XML 文件中每一要素或文件本身的授權規則。

Error Log 誤差記錄

The log which records all the errors encountered in a system.

記載系統遇到的所有誤差的記錄。

F

Faraday Cage 法拉第籠

Faraday Cage is a container made of metal mesh or foil that can shield an RFID tag.

法拉第籠是一個用金屬或鋁質製成、有屏蔽的容器，可用來掩蓋 RFID 標籤的訊號。

Federal Information Processing Standards (FIPS) 聯邦資訊處理標準

The Federal Information Processing Standards (FIPS) Publication Series of the National Institute of Standards and Technology (NIST) is an official series of publications relating to standards and guidelines adopted and made available under the provisions of the FISMA.

由 NIST 出版的聯邦資訊處理標準（FIPS）系列是官方刊物，內容是關於 FISMA 所規定採用的和已推出的標準和指引。

Federal Information Security Management Act (FISMA) 聯邦資訊安全管理法案

FISMA is a part of the US E-Government Act (Public Law 107-347) that became legislation in 2002. It requires US federal agencies to develop, document, and implement an agency-wide programme to provide information security for the information (and information systems) that support the operations and assets of the agency.

FISMA 是美國 E-Government Act（Public Law 107-347）的一部份，在 2002 年立法。它需要美國聯邦機構去發展、整理文件，並實施跨機構計劃，在資訊（和資訊系統）方面提供資訊保安，以支援機構的運作和資產。

Federated Identity Management 聯邦身份管理

Federated identity management is a model of identity management in which a group of service providers recognise user identifiers from one another. A customer of one particular service provider could access all services provided by

another service provider in the group with only a single identifier.

聯邦身份管理是身份管理模式的一種，在一群不同的服務提供者中，服務提供者可以互相認可其用戶的身份認證。一個特定服務提供者的客戶可使用一個身份認證，便可接達另外一個服務提供者所提供的全部服務。

File Infector Virus 檔案型病毒

It is a virus that infects executable files. Usually, the virus will get control when the program is first executed. In most cases, the virus will return control to the original program after it has completed its own execution.

有些病毒可感染執行檔案。它們通常會在程式首次執行時奪取控制權。在大部分情況下，病毒會在達到目的後把控制權交回予原有程式。

Filtering Router 過濾路由器

A router or system that selectively permits or denies passage of data packets according to security policies.

一個根據保安政策來選擇准許或拒絕數據包通過的路由器或系統。

Firewall 防火牆

A firewall is a system or combination of systems that helps to prevent outsiders from obtaining unauthorised access to internal information resources. The firewall enforces the access control policy, i.e. permit or deny, between two networks. It provides a single point where access control and audit can be imposed.

防火牆是一個或一組系統，協助防止外人在未獲授權情況下接達內部的資訊資源。防火牆執行接達控制政策，即負責准許或拒絕兩個網絡之間接達的工作。防火牆只提供單一點以進行接達管制和審計。

G

N/A

H

Hacker 黑客

In computer security, a hacker is someone with a strong interest in understanding and manipulating computer systems, and specialises in work with the security mechanisms for these systems. Nowadays, it is most commonly used by the mass media to refer to a person who maliciously uses computer knowledge to gain unauthorised access and cause damage to computers and data.

從電腦保安層面看，黑客是對電腦系統有很大興趣去了解和探討，並擁有對系統保安機制的專門知識。時至今日，大眾傳媒形容以電腦知識去得到未獲授權的接達並破壞電腦和數據的人，都稱之為黑客。

Hacking 黑客入侵

Hacking means illegally accessing other people's computer systems for destroying, disrupting, stealing files or carrying out illegal activities on the network or computer systems.

黑客入侵意思是非法接達他人的電腦系統，以進行破壞、瓦解，或在網絡或電腦系統從事非法活動。

Hardening 強化

Hardening is a process to secure a system, including an operating system or servers such as web servers, by removing the unnecessary system components, disabling unnecessary services, tightening the system configurations, etc.

強化是加強系統保安的過程，這些系統包括操作系統或伺服器如網頁伺服器。強化系統的過程包括停止不用的系統組件和服務、加強系統設定等。

Hash 雜湊函數

A one-way algorithm which maps or translates one set of bits into another (generally smaller) in such a way that the algorithm yields the same hash results every time for the same message, and it is computationally infeasible for a message to be reconstituted from the hash result. Also, two different messages

cannot produce the same hash results.

可以配對或轉化一組位元為另一組位元（通常是較小的）的單向算法，使每次均可得出該信息的同一個雜湊函數，而且不可以經由雜湊函數重整得出該信息。此外，兩個不同的信息不會得出相同的雜湊函數。

Hash-lock 雜湊函數鎖

Hash-lock is a hash value (or meta-ID) of the corresponding key that lock a tag.

雜湊函數鎖是利用有關鑰匙用以鎖定雜湊函數（或 meta-ID）。

Health Insurance Portability and Accountability Act (HIPAA) 健康保險便利及責任法案

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a US law designed to improve the portability and continuity of health insurance coverage in both the group and individual markets, and to combat waste, fraud, and abuse in health insurance and health care delivery as well as other purposes.

美國於 1996 年制定健康保險便利及責任法案（HIPAA），其設計主要用來改善團體和個人的健康保險保障範圍之可轉移性（Portability）和持續性（Continuity），且防止浪費、詐騙和濫用的行為發生在健康保險、實施醫療護理及其它用途上。

Heuristic 試探

This is a technique for assessing the probability that a file contains a computer virus.

用於評估檔案含有病毒可能性的一項技術。

Hoax 惡作劇電子郵件

This usually consists of an email message warning recipients about a new and terribly destructive virus. It ends by suggesting that the reader should warn his or her friends and colleagues, perhaps by simply forwarding the original message to everyone in their address book. The result is a rapidly growing proliferation of pointless emails that can increase to such an extent that they overload systems.

惡作劇電子郵件通常包含一個電子郵件信息，警告收件者提防一種新型、破壞力驚人的電腦病毒。郵件末段會建議讀者應警告他／她的朋友及同事，例如簡單地把原來信息轉寄給通訊錄中的所有人等。結果，該等無意義的電子郵件迅速擴散，其增長程度足以令系統負荷過重。

Honeypot 誘捕系統

A honeypot is a decoy system put on a network as bait for attackers. The attackers believe the honeypot is a legitimate system and attack on it, without being known that their activities are being monitored.

誘捕系統是佈置在網絡上引誘攻擊者的誘餌，令攻擊者誤以為它是真實的系統，他們攻擊系統時並不知道正被秘密監察。

Honeynet 誘捕網絡

In a honeynet, a network of honeypots is connected to imitate an actual or fictitious network. It appears to attackers that many different types of applications are available on several different platforms.

誘捕網絡是誘捕系統組成的網絡，模擬及複製真實或虛構的網絡。誘捕網絡在攻擊者看來，就像在幾個不同的平台運行各種應用程式。

Host-based Scanner 主機掃描軟件

Host-based scanner is installed in the host to be scanned, and can direct access to low-level details, such as the specific services and configuration details of the host's operating system.

主機掃描軟件是安裝在需要掃描的主機上，可以直接接達低層次數據，例如主機操作系統的具體服務及配置細節。

I

Identity Management 身份管理

Identity management is a management process of deciding who should have access to resources, and to what resources; providing, changing and terminating such access when appropriate; managing the process and monitoring it for compliance with internal and external policies.

身份管理是一個管理過程，決定誰可使用資源的接達權力和使用何種資源；適當地授予、改變和終結該項接達權力；管理和監控過程，以符合內部和外部政策。

Inoculate 抗毒辨識

To generate information or data about a file that can be used to verify the integrity of the file at a later time.

指記錄檔案特徵的步驟，用以在稍後時間核證檔案是否已受到病毒感染。

Injection Flaws 插入弱點

Injection flaw is a flaw in web application that allows an attacker to trick the web application into executing unintended commands or into changing system data.

插入弱點是網上應用系統的，它的潛在威脅是攻擊者可透過非預期的命令或改變系統數據藉以欺騙應用系統。

Insider Attack 內部攻擊

An attack originating from the inside of an organisation.

源自機構內部進行的攻擊。

Integrity 完整性

A condition in which the data has not been changed or destroyed in an unauthorised way, such that the current state is identical with the original state before transmission.

數據沒有遭到未獲授權而作出的更改或毀壞的情況，因此，數據的現有狀態與傳輸前的原本狀態相同。

Integrity Check 完整性查核

A mechanism to verify that the present state of data has not been tampered or modified, often using digital signatures or hashing algorithms.

用以核實數據的現有狀態未曾遭受竄改或更改的機制，一般採用的方法是數碼簽署或雜湊函數算法。

Intrusion Detection 入侵偵測

A method or process to detect the break-ins or attempts to attack via the use of software systems which operate on the network. Intrusion detection systems often combine the network monitoring with real-time capture and analysis in order to identify for attacks.

對透過使用在網絡上運作的軟件系統進行的入侵或攻擊嘗試作出的偵測的方法或程序。入侵偵測系統通常與網絡一起進行監察，並且具有即時收集及分析的功能，以找出網絡遭受攻擊的情況。

Intrusion Prevention System (IPS) 網絡入侵防禦系統

Intrusion prevention system (IPS) helps to detect if there is an attack happening on the network. IPS also provides active response to stop the source of attacks or to minimize the impact of the attacks.

網絡入侵防禦系統（IPS）幫助偵測網絡上的攻擊情況，並主動提供停止攻擊源頭的措施或減低攻擊所帶來的影響。

IPsec (IP Security)

IPsec provides interoperable, high quality and cryptographically based security services for traffic at the IP layer, such as authenticity, integrity, confidentiality and access control to each IP packet.

IPsec 為互聯網規約層 (IP layer) 上的傳輸，提供互用、高品質及以加密為基礎的保安服務，如認證、完整性、保密性以及對每個 IP 小包的接達控制等。

ISO/IEC 15408

ISO/IEC 15408 is the international standard that is commonly known as the “Common Criteria” (CC). It consists of three parts: ISO/IEC 15408-1:2005 (introduction and general model), ISO/IEC 15408-2:2005 (security functional requirements) and ISO/IEC 15408-3:2005 (security assurance requirements). This standard helps to evaluate, validate, and certify the security assurance of a technology product against a number of factors, such as the security functional requirements specified in the standard.

ISO/IEC 15408 此項國際標準一般稱為通用條件 (CC)，包括三個部分：ISO/IEC 15408-1:2005 (介紹和一般模式)、ISO/IEC 15408-2:2005 (保安功能要求)和 ISO/IEC 15408-3:2005 (保安保證要求)。該標準有助評估、確認和認證科技產品的保安保證，檢視這些科技產品是否有遵守一連串的要求，例如在標準中定明的保安功能要求。

ISO/IEC 27001:2005

ISO/IEC 27001:2005 is an international standard that specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System (ISMS) within an organisation.

ISO/IEC 27001:2005 國際標準指出機構內已文件化的資訊保安管理系統 (ISMS) 在訂立、推行、操作、監察、覆檢、維護和改善上的要求。

ISO/IEC 27002:2005

ISO/IEC 27002:2005 is an international code of practice for information security management, and is intended as a common basis and practical guideline for developing organisational security standards and effective management practices.

ISO/IEC 27002:2005 可被視為資訊保安管理的作業實務守則，並預期為發展機構的保安標準和有效管理實踐的共同原則與作業實務指引。

Isolated Identity Management 獨立身份管理

Isolated identity management is a model of identity management which requires that each user possess an identifier for access to each isolated service.

獨立身份管理是身份管理模式的一種，此模式要求每一個用戶都擁有身份認證工具，以便接達每一個獨立的服務。

J

N/A

K

Kerberos [Kerberos 安全系統]

A ticket-based, peer entity authentication system that uses passwords and symmetric cryptography to provide access control service in a client-server environment.

這個以票據為基礎、同級認證的系統，使用密碼和對稱的加密法，在客戶端及伺服器應用的環境中提供接達控制服務。

Key Distribution System 密碼匙分發系統

A security facility for the purpose of generating and distributing key in electronic form.

為以電子形式產生和分發密碼匙而設的保安設施。

Key Escrow 信賴鍵值加密法

An arrangement for storing cryptographic key under the custody of third parties so that the key can be available and used in special circumstances..

由第三方貯存密碼匙的安排，在特別情況下便可使用該密碼匙。

Key Exchange 密碼交換

A mechanism that use cryptographic algorithm such as Diffie-Hellman algorithm to securely exchange key keys between two entities.

使用加密算法例如 Diffie-Hellman 算法的機制，讓雙方安全地交換密碼匙。

Key Generation 產生的密碼匙

A process of creating a sequence of symbols that would become a cryptographic key.

產生一連串符號的過程，這一連串的符號就成為密碼匙。

Key Length 密碼匙的長度

The number of symbols that compose of a cryptographic key. Usually it is stated in number of bits.

密碼匙的符號數目，通常以位元為單位。

Key Management 密碼匙的管理

The process of storing, managing or distributing keys to authorised parties.

貯存、管理或分發密碼匙給獲授權各方的程序。

Key Recovery 密碼匙的復原

A process through which the value of a cryptographic key used for cryptographic operation can be obtained.

把在加密過程中使用的密碼匙復原。

Keylogger 鍵盤側錄程式

Keylogger is a device or program that captures activities from an input device. Malicious people can make use of keyloggers to capture personal information being input into a computer system.

鍵盤側錄程式是一個裝置或程式，用作擷取輸入裝置的活動。懷有惡意的人會利用鍵盤側錄程式去擷取輸入到電腦系統的個人資料。

L

Least Privilege Principle 最小權限原則

Least privilege principle is a concept in internal control that includes restricting a user's access (e.g. to data files, to processing capability, or to peripherals) or type of access (e.g. read, write, execute, delete) to the minimum necessary to perform his or her duties.

最小權限原則是一種內部控制概念，將用戶可接達的資訊系統資源（例如數據檔案、資料處理能力或外圍設備）或接達的種類（例如讀、寫、執行、刪除），限制在履行其職責所需的最低限度。

Logic Bomb 邏輯炸彈

A piece of code left within a computing system with the intent of it executing when some condition occurs. The logic bomb could be triggered by a change in a file, by a particular input sequence to the program, or at a particular time or date. Logic bombs get their name from malicious actions that they can take when triggered.

邏輯炸彈是一些駐留在電腦系中並在特定情況下執行的編碼。這些特定情況它可以是更改檔案、特別的程式輸入序列、或在特定的時間或日期。邏輯炸彈這個名稱正是因其發作時的惡意行為而來。

Logical Control 技術性措施

It refers to technological control using passwords, encryption, protocols, anti-virus software, firewall, etc.

指技術性的措施，例如密碼、加密、規約、抗電腦病毒軟件、防火牆等。

M

Macro Virus 巨集病毒

Macro virus is a program written in the macro language which is provided with some software applications (word processors, spreadsheets, etc.) To propagate, macro viruses exploit the capabilities of the macro languages to transfer themselves from one infected file (document or spreadsheet) to another.

巨集病毒是以巨集語言編寫的程序。某些軟件應用程式（如文字處理程式、製表軟件等）提供巨集語言。巨集病毒會利用巨集語言功能，從一個受感染檔案（文件或製表軟件）轉移至另一檔案，以達到傳播目的。

Mail Bomb 電郵炸彈

A mail bomb is the sending of a massive amount of email to a specific person or system. A huge amount of mail may simply fill up the recipient's disk space on the server or, in some cases, may be too much for a server to handle and may cause the server to stop functioning.

電郵炸彈是指向某一特定人士或系統發出大量電子郵件。數量龐大的電子郵件或會輕易地耗盡收件人伺服器上的磁碟空間，或在某些情況下，會使伺服器負荷過重而可能引致伺服器停止運作。

Malicious Code Attack 惡性程式碼攻擊

Malicious code refers to viruses, worms, spyware, Trojan Horses and other undesirable software. Attack made by using such software is to cause disruption either by deleting files, sending emails, or rendering the host system inoperable.

惡性程式碼指電腦病毒、網蟲、特洛伊木馬及其它不良軟件。利用此等軟件來作出的攻擊，會透過刪除檔案、發送電子郵件或使主機系統無法運作來造成破壞。

Man in the Middle (MITM) Attack 中間人攻擊

A man-in-the-middle attack (MITM) is an attack in which an attacker sits between two parties (the sender and receiver), captures and modify the communication messages of the two parties, and then sends the modified

messages to the two parties.

攻擊者在雙方（發送者和接收者）之間，截取並修改雙方的通訊信息，然後發送修改過的信息到雙方，稱之為中間人攻擊。

Mandatory Access Control (MAC) 強制接達控制

Mandatory Access Control (MAC) is an authorisation approach in which access to objects is based on the sensitivity of the information contained in the objects.

強制接達控制是授權機制的一種，限制用戶接達到具敏感性資訊的物件。

Message Digest 信息摘要

A compact representative of a message that is created by a cryptographic algorithm. It changes with the original message.

根據原本信息經加密算法後得出的摘要。它會隨著原本信息的變更而改變。

Multipartite 多元分裂複合型

A multipartite virus uses more than one mechanism to infect, such as combining the capabilities of both boot sector viruses and file infector viruses.

多元分裂複合病毒使用一個或以上的機制作出感染，例如結合開機磁區病毒及檔案感染病毒的特性。

N

Network-based Scanner 網絡掃描軟件

Network-based scanner is installed on a single machine that scans a number of other hosts on the network. It helps detect critical vulnerabilities such as mis-configured firewalls, vulnerable web servers, risks associated with vendor-supplied software, and risks associated with network and systems administration.

網絡掃描軟件通常安裝在一部電腦上，掃描網絡上其它主機。它可以偵測重大的保安漏洞，例如配置不當的防火牆、有保安漏洞的互聯網伺服器、供應商提供的軟件所附帶的風險，以及網絡及系統管理附帶的風險等。

Non-repudiation 不可否認性

Provide proof of the origin such that the sender cannot deny sending the message, and the recipient cannot deny the receipt of the message.

提供原本的證據，使發件人不能否認曾發出信息，而收件人也不能否認曾收取信息。

Q

One-time Password 限用一次密碼

A password which is generated and used only once for authentication, and will not be reused in next authentication.

為認證而產生並只使用一次的密碼，在下次認證時，不會再使用同一個密碼。

Open System Authentication 開放式系統認證

Open System Authentication is the default authentication protocol for 802.11 standard. It consists of a simple authentication request containing the station ID and an authentication response containing success or failure. On success, both stations are considered mutually authenticated.

開放式系統認證是 802.11 標準的預設認證規約，包含了簡單的認證要求，內有工作站 ID 和含有成功或失敗數據的認證應答。成功認證後，兩台工作站便被視為已互相認證。

Opt-in Approach 選用／選擇接受方案

It is an arrangement that requests a sender of promotional messages to provide recipients with some means to take affirmative steps to permit the sender to send promotional messages.

這方案要求推廣信息發出者提供回條，藉此獲得收信者的批准確認，以便日後繼續發出推廣信息。

Opt-out Approach 棄用／選擇不接受方案

It is an arrangement that requires senders of promotional messages to provide recipients with a means to inform the sender if they do not wish to receive further promotional messages.

這方案要求推廣信息發出者提供回條，藉此詢問收信者願意日後收取信息與否。

Overwriting Virus 蓋寫病毒

This is a type of file virus which overwrites the contents of a target file with its own code, destroying the original contents of the target file.

這類病毒會以其代碼重寫某一目標檔案的內容，以破壞該檔案的原來內容。

P

Packet Filtering 小包過濾法

A type of filtering to permit or deny network traffic based on the data source, destination, service or protocol of the data packets.

一種根據數據小包的数据來源、目的地、服務或規約的過濾方法，從而准許或拒絕網絡數據的交換。

Packet Sniffing 小包探取法

Packet sniffing refers to the collection and examination of data packets as they transit over the network.

小包探取法即數據包在網絡上傳輸時進行採集和分析。

Parasitic Virus 寄生蟲病毒

A type of virus which changes the contents of the target file while infecting it. This leaves the original contents of the file completely or at least partly not usable.

這類病毒會在感染目標檔案時修改檔案內容，令檔案原來內容完全或部分無法可用。

Parking Lot Attack 停車場攻擊

Parking lot attack is an attack against wireless network in which the attackers can sit in the organisation's parking lot and try to access the internal hosts via the wireless network.

停車場攻擊是對無線網絡的攻擊，攻擊者可安坐機構的停車場，通過無線網絡嘗試接達內部電腦系統。

Password 密碼

A private and unique series of numbers or letters which enable a user to gain access to a system or service. A passphrase is a longer password.

一組私人及獨有的數字或字母，用以協助用戶接達系統或服務。密碼組指較長的密碼。

Patch 修補程式

A patch is a program that repairs a bug or a security vulnerability of an existing software.

修補程式是用於修補現存軟件的程式錯誤或保安漏洞。

Payload 破壞力

This is a term used to describe the activity initiated by a virus. Typical virus payloads include displaying a message or deleting files.

這個術語用以形容病毒的所作所為。典型的破壞力包括顯示信息或刪除檔案。

Pharming 域欺騙

An attack redirects users to a bogus website such as fraudulent websites or proxy servers, typically through DNS server hijacking or poisoning.

這攻擊通過騎劫或破壞 DNS 伺服器，把用戶引領到仿冒網站，例如欺詐網站或代理伺服器。

Phishing 仿冒詐騙

Phishing is a kind of social engineering attack that tricks legitimate users into revealing private details, such as e-banking login names and passwords by using e-mails or fraudulent websites.

仿冒詐騙是一種社交工程的攻擊，犯罪者利用電子郵件或欺詐網站，引誘毫無戒心的網絡用戶透露私人資料，例如網上銀行之登入名稱和密碼。

Plaintext 原文

A message text or data that is freely readable and understandable by anyone.

可供任何人讀取或了解的信息文本或數據。

Polymorphic Virus 多構式病毒

A type of virus that changes its telltale code segments so that it "looks" different from one infected file to another, thus making detection more difficult.

多構式病毒指一種可改變本身指示代碼段的病毒，使它的「外表」在每一個受感染的檔案都有所不同，增加了偵測的困難程度。

Pretty Good Privacy (PGP) [PGP 程式]

Pretty Good Privacy (PGP) is a computer program that uses cryptography to help secure data in electronic mail and other applications.

PGP 是使用密碼學來保障電子郵件及其它應用程式數據的電腦程式。

Preventative Control 預防性措施

Preventative control aims to deter and avoid undesirable events from taking place.

預防性措施旨在阻嚇及避免不愉快事件發生。

Privacy Enhanced Mail (PEM) 增強型私隱郵件

Privacy Enhanced Mail (PEM) is a standard for secure exchange of electronic mail including message encryption and authentication of senders.

增強型私隱郵件是發件人的信息加密及認證標準。

Private Key 私人密碼匙

A data file storing a mathematical key which is assigned and known only to a single individual, used for creating digital signature and decrypting messages

previously encrypted by the sender, using the individual's own public key.

用以貯存數學密碼匙的數據檔案，該數學密碼匙是支配及告知予某個別人士的，用以產生數碼簽署及在收取電子郵件時，把由發件人以該收件人本身的公開密碼匙加密的信息解密。

Proxy Server 代理伺服器

A system that can accept or reject the connection of a user to the target destination with some kind of rules or authentication mechanisms.

藉某些規則或認證機制以接受或拒絕用戶接達目的地的系統。

Public Key 公開密碼匙

Asymmetric cryptography involves a pair of cryptographic keys for each user. The component that can be made publicly known is the public key.

每個用戶使用一對密碼匙以進行不對稱加密法，可公開的部份稱為公開密碼匙。

Public Key Cryptography Standard (PKCS) 公開密碼匙密碼學標準

A series of specifications for asymmetric cryptography applications published by RSA Laboratories.

由 RSA 實驗室發布的一系列不對稱加密法應用程式的標準。

Public Key Infrastructure (PKI) 公開密碼匙基礎建設

A Public Key Infrastructure (PKI) consists of protocols, services and standards supporting the public key cryptography applications. It often includes services and protocols for managing the public keys through the use of Certification Authority.

公開密碼匙基礎建設是由支援公開密碼匙加密應用系統的規約、服務或標準組成的架構，通常包括透過核證機關管理公開密碼匙的服務和規約。

Q

N/A

R

Reactive Control 應變性措施

Reactive controls are used to respond to undesirable events that have occurred.

應變性措施乃用以應付已發生的不愉快事件。

Registration Authority 註冊機關

An entity trusted to register other entities in applying for certificate and revoking their certificates. The authority may assign each applicant a relative distinguished value or name for the new certificate applied.

一個獲信託的機構，負責替申請證書或撤銷證書的其它機構註冊。該機構可為每名申請人所申請的新證書指配一個相對的獨特數值或名稱。

Remote File Inclusion 遠程文件包含

Remote file inclusion is a technique used by attacker to include hostile code and data to a web application.

攻擊者利用遠程文件包含的方法，把惡性程式碼與數據引進網上應用系統中。

Replay Attack 中繼攻擊

A replay attack is an attack in which the attacker intercepted a communication session from a legitimate user and then repeated in a later time the captured session in an attempt to impersonate the legitimate user.

中繼攻擊使攻擊者可從一名合法用戶截取傳送中的對話，然後試圖重覆扮演合法用戶。

Repudiation 否認性

Denial by an entity involved in a communication / transaction that s/he has participated in the activity.

即曾經參與通訊或交易活動的一方作出否認。

Rivest-Shamir-Adleman (RSA) Algorithm [RSA 加密法]

RSA (Rivest-Shamir-Adleman) is an algorithm for asymmetric cryptography invented in 1977.

RSA (Rivest-Shamir-Adleman) 加密法於 1977 年發明，常用於不對稱加密法。

Robot (or Bot) 漫遊器

A robot is a computer program that runs over the Internet to perform specific task. An example is search engine robot that searches the web for content and links.

漫遊器是互聯網程式，用於特別任務，例如搜尋漫遊器，可用於搜尋網頁內容和連結。

Rogue Device 虛假設備

It refers to devices introduced into the network that are not authorised.

指網絡上未經授權的設備。

Role-based Access Control (RBAC) 基於角色接達控制

Role-based access control (RBAC) is an authorisation mechanism in which access decisions are based on the roles that individual users have as part of an organisation.

基於角色接達控制是一種授權機制，接達決定權建立於個別用戶在組織中的角色。

Rootkit

A rootkit is a program/tool designed to gain the root / administrator access of a system. It often refers to that of malicious intent without going through proper authorization and/or authentication processes.

Rootkit 是一種程式／工具，用作奪取系統的根本目錄／管理員身份接達權。Rootkit 亦指沒有通過正常授權及／或認證過程的惡意入侵。

S

Sarbanes-Oxley Act (SOX) 沙賓法案

Sarbanes-Oxley Act of 2002 (SOX) is a legislation enacted in US in 2002. This act is also known as the “Public Company Accounting Reform and Investor Protection Act”. The purpose is to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes. This regulation affects all companies listed on stock exchanges in the US.

沙賓法案是美國在 2002 年頒布的法例，此法案也被稱為「Public Company Accounting Reform and Investor Protection Act」，其用途是透過改善遵守證券法規之企業披露的正確性和可信賴性來保護投資者，並可應用在其它用途上。此規例影響了所有在美國上市的公司。

Scam Email 騙案郵件

Unsolicited email which is deceptive and deliberately fraudulent in nature, leading to infection by viruses, identity theft, or even financial loss if instructions described in the messages are followed.

未經收件人同意的電子郵件，除了對收件人造成滋擾外，也可能含有行騙及欺詐的成分。如果跟從郵件裡的指令，可能會使電腦感染病毒，身份被盜，甚至是損失金錢。

Seals of Approval 評價認證

Symbols of security granted by an independent audit organisation to assure that proper security measures have been put into place.

由一個獨立審計機構簽發的保安標記，以保證某網站有採用適當的資訊保安措施。

Secure Channel 保密渠道

A communication path which can provide some means of protection from security threats.

保密渠道指可提供一些保護措施，以免受到保安威脅的通訊路徑。

Secure Multi-purpose Internet Mail Extension (S/MIME) 保密／多功能互聯網郵遞伸延

Secure Multi-purpose Internet Mail Extension (S/MIME) is a specification for encrypting and authenticating MIME data using public key technology.

保密／多功能互聯網郵遞伸延是一種用以把多功能互聯網郵遞伸延數據加密及認證的規格。

Secure Sockets Layer (SSL) 保密插口層

Secure Sockets Layer (SSL) is a protocol designed to enable encrypted, authenticated communications across the Internet. It is a security layer between the application and transport layers, which protects the application-layer protocols such as HTTP and is transparent to application developers or users. It provides privacy, authentication and message integrity.

保密插口層是設計用以協助把透過互聯網通訊的信息加密和認證的規約。保密插口層位於應用層和傳輸層之間，以保護應用層的規約，例如：超文本傳輸規約，而發展應用系統的人及用戶則不受其限制。保密插口層提供保護私隱，作出認證和保持信息完整性等功能。

Security Assertion Markup Language (SAML) 安全斷言標記語言

SAML is an XML-based framework from OASIS for communicating user authentication, entitlement, and attribute information.

安全斷言標記語言是 OASIS 為傳送用戶認證、授權和屬性 (attribute) 資訊的 XML 框架。

Security Incident 保安事故

It is any event that could pose a threat to the availability, integrity and confidentiality of an information system.

指可能對資訊系統或資訊資源的可用性完整性及機密性構成威脅的任何事件。

Security Management System 保安管理系統

Security management systems are responsible for controlling access to network resources, such as functions that enable the changing of passwords and alter the identifications and security classes of communications channels including integrity and resilience of the management capability.

保安管理系統負責控制接達網絡資源，例如更改密碼、改變通訊渠道的辨識和保安級別的功能，包括管理能力的完整性和彈性。

Security Policy 保安政策

A top-level directive statement that guide and determine decisions concerning security in a system.

用作引導及決定系統保安方面最高層次的指令文件。

Security Risk Assessment 保安風險評估

Security Risk Assessment can be defined as a process of evaluating security risks, which are related to the use of information technology. It can be used as a baseline for showing the amount of change since the last assessment, and how much more changes are required in order to meet the security requirements.

保安風險評估定義為用於資訊科技的保安風險測試程序，是上一次評估後作出轉變的基準，釐定還需要多少轉變才能夠達到保安要求。

Segregation of Duties 職務分工

Segregation of duties is a concept in internal control that requires critical functions to be divided into steps among different individuals so as to prevent a single individual from subverting a critical process.

職務分工是一種內部控制的概念，指將一項重要工作的各個步驟分別交由不同人員處理，以杜絕重要程序被一人破壞的可能性。

Server Authentication 伺服器認證

It allows a client to identify that it is communicating with the target party, not a malicious third party.

協助客戶辨識與其通訊的一方並非懷著惡意的第三方。

Service Set Identifier (SSID) 服務設定識別碼

Service Set Identifier (SSID) is a configurable identification that allows wireless clients to communicate with an appropriate access point. With proper configuration, only clients with the correct SSID can communicate with access points.

服務設定識別碼 (SSID) 是可設定的識別碼，無線客戶端可憑識別碼跟適當的無線接駁點通訊。只要配置正確，客戶端擁有正確的 SSID 便可與無線接駁點通訊。

Session Key 對話密碼匙

A session key is a symmetric key which encrypts a message or session, in order to protect data during transmission. It is created at the beginning of a communications session.

對話密碼匙是對稱密碼匙，用以把信息加密，使數據在傳輸時受到保護。對話密碼匙是在開始進行通訊加密時產生的。

Shared Key Authentication 分享式密碼匙認證

Shared Key Authentication is a standard challenge and response mechanism that makes use of WEP and the shared secret key to provide authentication.

分享式密碼匙認證是採用 WEP 和分享式密碼匙的標準質疑應答機制，用於提供認證功能。

Shoulder Attack 肩窺

Shoulder attack is an attack in which attacker might be able to observe what one types and hence steal the password by direct observation by looking over one's shoulder, or indirect monitoring by using a camera when one types in his

password.

攻擊者在用戶輸入密碼時，在其肩膊後方直接觀看所鍵入字符，或非直接地從閉路電視監察，繼而竊取密碼。這種攻擊方法稱為肩窺。

Simple Key Management for Internet Protocol (SKIP) 簡單密碼匙管理規約

Simple Key Management for Internet Protocol (SKIP) is an authentication / encryption system that secures the network at the IP packet level.

簡單密碼匙管理規約是一個認證／加密系統，在聯網規約小包層面確保網絡穩妥可靠。

Single Sign-On (SSO) 單一登入

Single sign-on is an access control mechanism that requires a user to login only once and be authenticated automatically by all other service providers.

單一登入是接達控制的一種，它要求用戶登入一次，然後其它服務提供者會自動認證該用戶身份。

Smart Card 智能卡

A tamper-resistant card with a chip storing an encrypted password or the private key which makes it difficult to be sniffed or stolen by the intruder.

貯存了經加密的密碼或私人密碼匙的唯讀晶片，入侵者難以採取或竊取咭上的資料。

SMiShing 短訊仿冒詐騙

SMiShing is phishing by means of Short Message Service (SMS). Similar to the Internet phishing attack, attackers are attempting to fool mobile users with bogus text messages that connect to websites where malicious codes can be downloaded to their mobile devices.

SMiShing 是利用短訊作媒介的仿冒詐騙，它跟互聯網的仿冒詐騙攻擊相似，攻擊

者嘗試以偽造的文字訊息愚弄流動電話用戶連接至短訊中提供的網頁，因而被誘騙下載惡意軟件至流動電話中。

Social Engineering 社會工程

An act using social interactions such as lie, play acting or verbal wordings to trick legitimate users for secrets of the systems such as the user lists, user passwords and network architecture.

以社交手法例如說謊、假扮或言語用字等方式欺騙用戶，藉此套取系統秘密，譬如用戶名單、用戶密碼和網絡結構。

Spam 濫發訊息

Spam refers to bulk unsolicited electronic messages sent in the form of e-mail, fax or short messages, etc. regardless of whether the recipients have given any consent to receive such or even after the recipients have requested not to receive such any more.

濫發電子訊息是指在不管收件人同意與否或在收件人已要求發件者停止送訊息的情況下，通過電子郵件、傳真或電話短訊等形式而發出的大量訊息。

SPam over Internet Telephony (SPIT) Attack 濫發網絡電話攻擊

SPIT is the spamming which targeted at VoIP. It leaves unsolicited marketing voice messages at the target IP phones.

濫發網絡電話攻擊是利用 VoIP 作濫發 (spamming) 用途，在目標 IP 電話中留下非應邀促銷的語音訊息。

Spam Honeypot 誘捕濫發電郵系統

Spam honeypot is a honeypot designed to attract spammers to attack, and hence to study spam and email harvesting activities.

誘捕濫發電郵系統設計來吸引濫發電郵者攻擊，用以研究濫發電郵及收集他人電郵地址的行為。

Spammer 濫發電郵者

Spammer is a person who sends spam messages.

濫發電郵者是發出濫發訊息的人。

SPIM

SPIM is a spam spread via instant messaging (IM). It is sometimes called IM spam.

SPIM 是透過即時通訊 (IM) 散播的濫發訊息。它有時又稱為 IM spam.

Spyware 間諜軟件

Spyware is software that secretly forwards information about a user's online activities to third parties without the user's permission.

間諜軟件在未經用戶允許的情況下，便把用戶網上活動的資料秘密地轉送至別人的軟件。

SSL VPN 保密插口層虛擬私有網絡

An SSL VPN allows users to connect to the VPN devices using their Web browsers. The SSL (Secure Sockets Layer) protocol or TLS (Transport Layer Security) protocol is used to encrypt the traffic between the Web browser and the SSL VPN device.

SSL VPN 讓用戶使用互聯網瀏覽器便可以連接 VPN 裝置，互聯網瀏覽器與 SSL VPN 裝置之間會使用 SSL (保密插口層) 規約或 TLS (傳輸層保安) 規約來加密通訊。

Stealth Virus 隱形病毒

A virus that actively seeks to conceal itself from discovery or defends itself against attempts to analyze or remove it.

隱形病毒是一種刻意隱藏免被發現，或防止被人分析或移除的電腦病毒。

T

Third-party Mail Relay 第三者郵件驛遞

A mail relay that configured in a manner that people from third-party, who are not local users, can send email through this email server.

一個電郵伺服器允許不屬於該電郵系統用戶的第三方通過此伺服器發送電子郵件。

Threat 威脅

A potential violation of security that may cause harm to an organisation and its assets.

可能對機構及其資產有害的潛在保安因素。

Time Bomb 計時炸彈

A logic bomb activated at a certain time or date.

在某一時間或日期啟動的邏輯炸彈。

Timestamp 時間標示

A time mark or notation that indicates the date and the time of an action / event.

顯示行動的日期和時間，及發出或收取該時間標籤的人的身份或裝置的時間標記或標示。

The Payment Card Industry (PCI) Data Security Standard (DSS) [支付卡行業數據安全標準]

The Payment Card Industry (PCI) Data Security Standard (DSS) is a standard developed by PCI Standards Council to enhance payment account data security. The standard consists of 12 core requirements, which include security management, policies, procedures, network architecture, software design and other critical measures.

Payment Card Industry Data Security Standard (PCIDSS) 是由 PCI 標準會議 (Standards Council) 所發展出來以加強付款帳戶資料的保安標準，該標準含 12 項核心要求，包括保安管理、政策、程序、網絡設計、軟件設計和其它重要措施。

Trojan Horse 特洛伊木馬

A software which pretends to provide legitimate function, but actually carries malicious function exploiting legitimate authorisations of a person who invokes the program.

假裝提供正常功能，實際上帶有惡意破壞功能的軟件。

Trusted Third Party 獲信賴的第三方

An independent third party that contributes to the trustworthiness of computer-based information transfers.

協助達致以穩妥可靠方式傳輸電腦資訊的獨立第三方。

Two-factor Authentication 雙重認證

Two-factor authentication is an access control mechanism in which a successful authentication would require the user to provide two of the following factors: (a) something you know (e.g. password), (b) something you have (e.g. a smart card), and (c) something you are (e.g. fingerprint).

雙重認證是接達控制的一種，它要求用戶具備下列最少兩種要素才可成功認證：(1) 使用者所知道的東西（例如密碼），(2) 使用者所擁有的東西（例如智能卡），(3) 使用者本身即有的東西（例如指紋）。

U

N/A

V

Variant 變種

A modified version of a virus that is usually produced on purpose by a virus author or by someone who modifies the original virus. Variants may be very similar to their parent virus, or may be fairly different. Some are text variants, which means that the only differences between them and their parent virus are in internal program comments that are never displayed, or in text that is displayed to the screen. Some are the result of small changes made to the original virus, apparently to create a new virus which is not detected by certain anti-virus programs. Some are the result of large changes, such as combining the spreading part of one virus with the damage part of another.

病毒的修改版本，通常由病毒作者或修改原病毒的人士製造。變種可與原病毒非常類似，亦可以有很大的區別。有些變種是文字變種，其與原病毒的唯一區別是不顯示程式內部註解或顯示於螢幕的文字。某些變種來自對原病毒的細微修改，令其看起來像是某個防毒工具並未偵測出來的新病毒；某些變種則來自較大的改動，例如將一個病毒的散播部分與另一個的破壞部分結合。

Virtual Private Network (VPN) 虛擬私有網絡

Virtual Private Network (VPN) establishes a secure connection over un-trusted network by using a technique called tunnelling, which encapsulates a message packet within an IP (Internet Protocol) packet for transmission across a network.

虛擬私有網絡 (Virtual Private Network, VPN) 在不安全的網絡上，利用隧道技術，建立一條安全連接，在網絡傳送過程中，它把信息小包壓縮（包裹）在 IP（互聯網規約）包內。

Virus 電腦病毒

A computer virus is a block of executable code that would replicate itself by attaching to other files or replacing another program.

電腦病毒指一組執行代碼，可透過附於其它檔案或取代其它程式而自行複製。

Virus Signature 病毒識別碼

Specific strings of binary code in most viruses (except polymorphic ones) that allow antivirus software to identify the virus. New viruses contain new signatures, which is why it is essential to keep signature files up to date.

大部分病毒（除多構式病毒外）中的特定二進制碼字串，防毒軟件可藉此偵測出病毒。新的病毒有新的病毒碼，因此必須定期更新防毒軟件的病毒碼。

Vishing 語音網絡仿冒詐騙

Vishing is a type of phishing attack that targeted VoIP. It can be used by the attacker to steal the identities or money of the victim.

語音網絡仿冒詐騙是利用 VoIP 技述的仿冒詐騙攻擊。攻擊者可藉此竊取受害人的身份或金錢。

Vulnerability 保安漏洞

A flaw or weakness in a system that could be exploited by intruders to violate the security policy.

系統的缺點或弱點，讓入侵者有機可乘加以破壞，違反保安政策。

Vulnerability Scanner 保安漏洞掃描軟件

Vulnerability scanner is software that assesses security vulnerabilities in networks or host systems and produces scan results.

保安漏洞掃描軟件是用於評估網絡或主機系統的保安漏洞，並得出一套掃描結果。

W

Web Application Firewall 網上應用系統防火牆

According to the Web Application Security Consortium, a web application firewall (WAF) is an intermediary device, sitting between a web-client and a web server, analysing OSI Layer-7 messages for violations in the programmed security policy.

根據 Web Application Security Consortium (WASC), 網上應用系統防火牆 (WAF) 是一種介於網絡客戶端和網絡伺服器之間的裝置, 作為分析在 OSI 第七層違反保安政策之訊息。

Web Defacement 網頁竄改

Change of the content (usually the main page) of a website with some messages by intruder or by virus.

指網站內容 (通常是主頁) 變成了由入侵者或電腦病毒發放的一些信息。

Web Service Security (WS-Security) 網絡服務保安

WS-Security is a specification by OASIS to provide message integrity and confidentiality to web service.

網上服務保安是由 OASIS 提供網絡服務上信息完整性和保密性的規格。

Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) is a wireless security protocol to fix known security issues of WEP. WPA provides users with a high level of assurance that their data will remain protected by using Temporal Key Integrity Protocol (TKIP) for data encryption.

Wi-Fi Protected Access (WPA) 是針對 WEP 的缺陷而設計的無線保安規約。WPA 為用戶提供高度保證, 確保用戶的數據透過暫時密碼匙完整性規約 (TKIP) 進行數據加密後得到保護。

Wi-Fi Protected Access 2 (WPA2)

Wi-Fi Protected Access 2 (WPA2) is a new wireless security protocol, based on IEEE 802.11i, in which only authorized users can access their wireless with the features of supporting stronger cryptography (Advanced Encryption Standard AES), stronger authentication control (Extensible Authentication Protocol EAP), key management, replay attack protection and data integrity.

Wi-Fi Protected Access 2 (WPA2) 是依據 IEEE802.11i 標準的嶄新無線保安規約，只有獲授權的用戶才可接達無線裝置，並支援更強的加密法(高級加密標準 AES)、更強的認證控制(可擴展認證規約 EAP)、密碼匙管理、中繼攻擊保護和數據完整性的功能。

Wired Equivalent Privacy (WEP) 有線等效保密規約

Wired Equivalent Privacy Protocol (WEP) is a basic security feature of IEEE 802.11 standard that was intended to provide confidentiality over a wireless network by encrypting information sent over the network. After the key-scheduling flaw was found in the WEP, it is now considered to be fully broken because the WEP key can be cracked in minutes with the aid of automated tools.

有線等效保密規約 (WEP) 是 IEEE802.11 標準的基本保安功能，可在無線網絡中替傳輸資料進行加密，提供保密性。由於 WEP 密碼匙的 key-scheduling 弱點已被發現，WEP 密碼匙已可被自動破解工具於數分鐘內破解。

Worm 蠕蟲

A worm is a program that spreads over network. Unlike a virus, worm does not attach itself to a host program.

蠕蟲是一種經由網絡擴散的程式。它跟病毒有所不同，因為它不會附在一個主程式內。

X

XML Encryption [XML 加密]

XML encryption is a specification developed by W3C that provides a process for encrypting data and representing the result in XML.

XML 加密是 W3C 開發的規範，提供一個為數據加密的過程和以 XML 表示其結果。

XML Key Information Service Specification (X-KISS) [XML 金鑰資訊服務規範]

X-KISS is a protocol developed by W3C to support the delegation by an application to a service of the processing of key information associated with an XML signature, XML encryption, or other usage.

X-KISS 是 W3C 開發的規約，支援應用系統在處理金鑰資訊所連結的 XML 簽署、XML 加密，或其它用途。

XML Key Management Specification (XKMS) [XML 金鑰管理規範]

XKMS is a protocol developed by W3C which describes the public key management for Web service. It defines a way to distribute and register public keys used by the XML Signature and XML Encryption specifications. XKMS comprises two sub-protocols: XML Key Registration Service Specification (X-KRSS) and XML Key Information Service Specification (X-KISS).

XKMS 是 W3C 開發的規約，定義了公開密碼匙管理規約，也定義了分配和登錄公開密碼匙的方法，而公開密碼匙是使用 XML 簽署和 XML 加密算法規格的，XKMS 包含了兩個子協定：XML 金鑰註冊服務規範（Key Registration Service Specification, X-KRSS）和 XML 金鑰資訊服務規範（Key Information Service Specification, X-KISS）。

XML Key Registration Service Specification (X-KRSS) XML [金鑰註冊服務規範]

X-KRSS is a protocol developed by W3C to support the registration of a key pair by a key pair holder, with the intent that the key pair subsequently is usable in conjunction with the XML Key Information Service Specification or a Public Key Infrastructure (PKI) such as X.509.

X-KRSS 是 W3C 開發的規約，支援金匙持有人註冊其配對密碼匙，使其配對密碼匙隨後可與 XML 金鑰資訊服務規範或如 X.509 的公匙基建（PKI）上使用。

XML Signature [XML 簽署]

XML signature is a specification developed by W3C that provides a process for XML digital signature processing.

XML 簽署是 W3C 開發的規範，提供一個處理 XML 數碼簽署的過程。

Y

N/A

Z

Zero-day Attack 零日攻擊

An attack exploiting a newly discovered vulnerability appears before the release of the corresponding patch by the software vendor.

在軟件供應商發放相對應的修補程式前，可利用這些新發現的保安漏洞而進行的攻擊。

Zombie Computer (or Zombie) 殭屍電腦

A computer attached to the Internet that has been compromised by intruder with computer viruses or Trojan Horses and manipulated without the knowledge of the computer owner. The computer is usually used to perform malicious attacks such as denial of service attack under remote control.

指連接互聯網而已經受入侵者、電腦病毒或木馬程式影響的電腦。該等電腦通常被用作惡意用途，例如在接收遠程指令後作出拒絕服務攻擊。一般而言，擁有者並不知道該等用途。