

This glossary will help you to understand all the terminology associated with Information Security.

Accountability

The ability to identify who or what was responsible for taking a particular action. Typically requires a logging system to record activity and authentication to verify that the user was actually the originator/instigator.

Access Control List (ACL)

An explicit set of permissions for users (or groups of users) detailing who can access specific items.

Asynchronous Digital Subscriber Line (ADSL)

A fast mechanism for accessing the Internet using conventional copper telephone lines.

Algorithm

A mathematical function used in Encryption to make the retrieval of information by unauthorised users more difficult.

Anti virus software

Software tools for detecting, blocking and/or removing viruses from files, emails or network communications. Sometimes referred to as Virus Defence Software. Anti virus software can be loaded on workstations, servers and used by application proxies to check for viruses in real-time, or (in the case of files on servers), by sweeping the entire system according to a preset schedule. Anti virus systems must be regularly updated with new virus signatures to protect against the release of new viruses.

Applet

A segment of programme code, usually embedded within a web page which runs within the browser of the user system.

Application

At the lowest level, a set of instructions that a computer system uses to perform a task. More commonly referred to as a software package. In web-based systems there may be an application in the form of a set of web pages and executable scripts or applets.

Audit Trail

Audit trails provide a date and time stamped record of the usage of a system. They record what a computer was used for, allowing a security manager to monitor the actions of every user. Audit trails can help to establish an alleged fraud or security violation.

Authentication

The process of accepting a user's claimed identity (their username) and verifying they are actually that user.

Back Door

An entry point to a programme or a system that is hidden or disguised, often created by the software's author for maintenance purposes. A certain sequence of control characters permits access to the system manager account. If the back door becomes known, unauthorised users (or malicious software) can gain entry and cause damage.

Baseline Security

Method of selecting security measures for implementation within a company, based upon measures used in similar organisations that are generally accepted to be well-run. Implementation of Baseline Security throughout a company provides a common basis for units to develop, implement and measure effective information security management and practice. It also provides confidence in inter-unit/inter-company trading.

The British Standard for Information Security Management, BS 7799 (now ISO/IEC 17799) provides a list of baseline controls which should be implemented. Many of these basic principles apply to smaller organisations as well as to large companies.

Browser

An application that is used to access a web server.

Buffer

A block of memory used by a computer to hold inputted or submitted data pending its processing, storage or onward transmission.

Business Continuity Planning

Prepared (and tested) measures for protection of critical business operations from the effects of a loss, damage or other failure of operational facilities which provide crucial functions (e.g. programmes and data). In terms of information security, this comprises backups and archiving, stand-in hardware etc.

Cipher

An algorithm for encryption or decryption. A cipher replaces a piece of information (an element of plain text) with another object, with the intent to conceal its meaning. Typically, a secret key governs the replacement rule.

Content Checking

Content checking is a process that uses software to read the contents of incoming files, normally e-mail. The content can be scanned for Malicious Code (See Viruses and Anti Virus Software), obscenities and dubious programme files.

Cookie

A mechanism through which a web server can store and retrieve client information in order to identify users. This information allows a web site to personalise content for returning visitors.

Credentials (authentication)

A combination of the claimed identity (username) together with required verification information (such as a password or PIN).

Cryptography

Cryptography is the study and practice of scrambling information in a manner that makes it difficult to unscramble, and makes scrambled information intelligible. It is used as the basis for much computer security in that it can keep information confidential, and can also preserve the integrity of data, particularly when being stored or transmitted.

Cyberliabilities

Cyberliabilities is an emerging term that describes liability issues, normally relating to the Internet and email use (and abuse). The term refers less to the actual offence (which is little different from standard liability) than to the means by which the offence manifests itself.

Database

A system or programme in which structured data is stored.

Decrypt/Decryption

The reverse process of encryption, i.e. to turn scrambled data back into its original form.

Digital Signature

The process of adding an electronic marker to the information to validate both the content and the originator of the data.

Dialup

The use of a computer and modem to connect to a computer or the Internet using standard telephone lines. It normally describes slow speed narrowband connections rather than Broadband.

Encryption

Scrambling information to prevent unauthorised disclosure or modification using mathematical techniques. Techniques normally use an encryption algorithm with a key to ensure that only the intended recipient can read the information.

Encryption can be either:

- Symmetric (where the same key is used to encrypt and decrypt)
- Asymmetric (where two mathematically related keys are used, one (the public key) to encrypt, and the other (the private key) to decrypt).

File Permissions

Security information that details which users or user groups have access to files or folders.

Access rights might include the ability to read, write, modify, delete etc.

Filter

A technique for checking a number of items (e.g. file types, user commands, web site addresses), allowing only those who are acceptable to pass through a barrier such as a firewall.

Firewall

A Firewall is a device or software package that provides a secure gateway between two networks. Some network devices such as routers have firewalls built in. There are also 'personal firewalls' that do the same job but only protect one system (such as a laptop or PC). Firewalls ensure that certain network traffic (e.g. from certain applications) is allowed to pass from one network to another according to a set security policy. Firewalls can prevent network-based attacks that are often targeted against systems.

Firewalls can log connection attempts and traffic and authenticate users trying to make network connections. They can inspect network packets, e-mail viruses and web pages, and track the state of connections to ensure they are behaving as expected. Firewalls also protect internal networks by performing Network Address Translation (NAT). Firewalls fall into three main types: Stateful Inspection, Application Proxy or Packet Filtering.

File Transfer Protocol (FTP)

A protocol for the transfer of files (programmes and/or data) by programmes or users.

Gateway

A bridge between two networks, often another name for a firewall or application proxy.

Host

Either a workstation or server i.e. any computer system connected to a network.

Hyper Text Mark-up Language (HTML)

HTML is code inserted in files intended for display on a Web browser. It tells the browser how to display the information.

Hyper Text Transfer Protocol (HTTP)

HTTP is a protocol for exchanging information (text, graphics, sound, video, etc) on the World Wide Web.

Hub

A network device that allows a number of computers to be connected. All systems on a hub can see all the traffic on that network.

Internet Control Message Protocol (ICMP)

A protocol used to verify that the network is working correctly.

Information Assets

Stored data which is pertinent to business processes. In the case of personal information, this is subject to data protection considerations.

Integrated Emergency Management

A term that describes an overall practice covering Business Continuity Management and Crisis Management, aiming to integrate and enhance their individual effectiveness.

Intrusion Detection

Detection of break-ins or attempted break-ins by manual means or by software expert systems operating on the basis of logs or other information available on the network.

An Intrusion Detection System (IDS) effectively acts as a “burglar alarm” for a network or a system. It can identify someone “casing” the system and can detect the “rattling of door knobs” to see if the house is unlocked. It can also “hear the shattering of glass” as entry is gained and can “sound the alarm” and “call the police”. Additionally, it can monitor and log forensic evidence to support any legal case.

Internet Protocol (IP) Address

The network address of a computer system or host.

Internet Protocol Security (IPsec)

A protocol to implement a Virtual Private Network. This comprises a number of sub-protocols such as IKE (Internet Key Exchange).

Integrated Services Digital Network (ISDN)

This is a system of digital transmission over telephone lines which provides faster response times than using a normal telephone line and modem.

Key

A string of characters used in encryption to give unique results.

Local Multipoint Distribution Systems (LMDS)

This is a wireless broadband technology that provides connections over a few kilometres for multiple subscribers. This can prove useful in isolated communities or difficult terrain.

Leased Line

A fixed, permanent connection (e.g. to the Internet).

Local Area Network (LAN)

An interconnected system of computers and peripherals. LAN users share data stored on hard discs and can also share printers connected to the network.

Log

A list of events (security related or otherwise) that have occurred on a system. The logs may be used for troubleshooting purposes to try to identify what went wrong, when and why an incident occurred (i.e. recovery). Alternatively,

logs may be used to spot suspicious activity on a system (i.e. detection).

Macro Virus

A computer virus that is embedded within word processing documents or spreadsheets that will activate when the file is opened. The effect can range from minor inconvenience to substantial corruption. This form of virus is currently the most prolific.

Malicious Code

A term for a virus, hostile applet or code fragment downloaded from a web server or sent directly from one system to another.

Mobile Code

A programme downloaded from the Internet that runs automatically on a computer, with little or no user interaction.

Modulator Demodulator (Modem)

A device which allows a computer to connect to another computer or network over a normal telephone line.

Narrowband

A term to describe slow speed dialup connections. The term contrasts with broadband.

Network Address Translation (NAT)

An internet standard that increases security by enabling a Local Area Network (LAN) to use one set of Internet Protocol (IP) addresses for internal traffic and a second set for external traffic. A NAT box located where the LAN meets the Internet makes all necessary IP address translations. This feature is often built into routers.

Network

The physical and logical infrastructure that allows for the connection of a set of computers.

Network Protocol

A standard way for two elements on a network (servers, hosts, workstations etc.) to communicate.

Network-Level Firewall

A firewall in which traffic is examined at the network protocol packet level.

Operating System

The underlying package that allows a computer to function and provides the basic services required for a user to run an application. The operating system is normally responsible for the configuration and enforcement of the security of the system itself. Functions such as authentication of users, file permissions and logging of events will be under its direct control.

Packet Filtering

A type of firewall that, although fast, has little intelligence. This reduces its effectiveness and flexibility. It is a powerful tool when used in conjunction with other types of Firewall Stateful Inspection and Application Proxy.

Partition

To divide computer memory or storage into different sections. Each partition can behave as a separate disc drive.

Password

A secret string which is known only to the user and the system which the user can enter. It is used for identification and authentication purposes. The strength of a password (and thus the level of security it provides) is directly related to its length and how easy it would be for an attacker to guess it.

Username/Passwords should never be disclosed or shared as this would mean there is no accountability within the system. A variant is a PIN which is normally numeric only and is used in conjunction with an authentication token (e.g. a smart card).

Patch

A patch is updated computer code that is published either as part of ongoing development, or to meet known vulnerabilities and other problems in code. Most software vendors have sites that provide patches and hotfixes. All systems should be patched to the level recommended by the vendor as unpatched systems are like an open window into your environment. Many commercial operations and hacker sites provide online databases of known vulnerabilities and exploits.

Penetration Testing

The portion of security testing in which the testers attempt to circumvent the security features of a system. The testers sometimes use system design and implementation documentation, which may include listings of system source code, manuals, and circuit diagrams. They can also work under the same constraints applied to ordinary users. This practice is sometimes called 'ethical hacking'.

PIN

A short numeric password, normally fairly insecure in its own right, but often used in conjunction with some form of authentication token such as a smart card.

Packet Internet Groper (PING)

A type of Internet Control Message Protocol (ICMP) message used to verify a computer is connected to the network and is responding to it.

Proxy

A computer (server) that sits between a client application (for example, a web browser) and a real server. The proxy intercepts all requests to the real server to see if it can fulfil the requests itself. If not, it forwards the request to the real server.

Registry

This is the central database which is a collection of files that make up the user configuration and local PC configuration settings. The registry is made up of Registry Hives files which contain the Registry Keys (the configuration settings for programmes).

Remote Access

The connection of a device, through communication lines such as phone lines or Wide Area Networks (WANs), to access applications and information hosted elsewhere.

Routing

The method by which information (Internet Protocol packets) is transferred from one system on a network to another. Routers perform this function.

Server

The computer on a local area network that acts as a store for data and software. It also controls access to workstations, printers and other parts of the network.

Smart Card

A card with an embedded chip used for a variety of purposes such as proving the user is valid (authentication). It does this by storing authentication credentials and submitting them, or by actually performing an operation on the card itself (using a specific key), to demonstrate the validity of the user.

Simple Mail Transfer Protocol (SMTP)

The protocol used to exchange e-mail messages between servers in order to transfer a message from the sender to the recipient.

Sniffing

Passive interception and reading of network traffic.

Structured Query Language (SQL)

A language to interrogate database systems.

Secure Sockets Layer (SSL)

A network protocol which provides security to web-based network traffic. A connection is established with the server which sends a digital certificate to the browser/user system to verify its authenticity. The client then generates a random session encryption key which it sends to the server. The latter uses its own private key to decrypt the client's session key. This results in both parties having a shared secret key to protect encrypted information. The SSL also allows each party to check that data has not been modified in transit (i.e. check its integrity) by using a hash function.

SSL is used to secure web server accesses, but it should be noted that it only protects information in transit; once decrypted and processed or stored by the web server (e.g. in a database), the information is no longer protected.

Stateful Inspection

A type of firewall which relies on tracking the status of a network connection and a rulebase. The handshake at the start of a network connection is observed and monitored, and if a successful connection is established, the firewall then makes an entry in a table to allow all future traffic for that connection to pass freely. The advantage is that a very high degree of

security can be achieved and virtually all network based attacks can be thwarted with minimal performance impact.

Many stateful inspection firewalls also provide some application proxy capabilities for various types of network traffic. This allows them to filter requests and screen content.

Switch

A more sophisticated version of a hub that ensures each system only sees its own traffic.

Transmission Control Protocol/Internet Protocol (TCP/IP)

These are network protocols used to communicate over the Internet. IP defines how a packet of information can be exchanged and routed across the network. TCP uses IP to allow two systems to establish a session (similar to a telephone conversation), in order to exchange or transfer data.

Trojan Horse

A programme that causes unexpected and usually undesirable effects when installed or run by an unsuspecting user. These effects may be immediate or they may wait for some predetermined time or condition before they are triggered.

Trusted

Those systems or networks that meet an organisation's security requirements for configuration and operation.

User Datagram Protocol (UDP)

A protocol that uses Internet Protocol (IP) to send a single block of information from one system to another.

Untrusted

Those systems or networks that do not meet an organisation's security requirements.

Uniform Resource Locator (URL)

A URL contains a web address. It is also used to specify information for retrieval or to pass instructions to another computer.

User Group

A set of users with equivalent access rights, roles or levels of privilege.

Username

A name or string that uniquely identifies an individual user. It is normally accompanied by a password, or PIN and token to provide authentication. Usernames/Passwords should never be disclosed or shared as this would mean there is no accountability within the system.

Virtual Private Network (VPN)

A secure network that connects entirely or in part over insecure public links (i.e. the Internet or dial-up via PSTN the Public Switched Telephone Network). It uses tunnelling technology.

Virus Defence Software

Software tools for detecting, blocking and/or removing viruses from files, emails or network communications. Sometimes referred to as Anti Virus Software.

Virus Defence Software can be loaded on workstations, servers and used by application proxies to check for viruses in real-time, or (in the case of files on servers), by sweeping the entire system according to a preset schedule. Anti virus systems must be regularly updated with new virus signatures to protect against the release of new viruses.

Wide Area Network (WAN)

A network of Local Area Networks (LANs), which provides communication and services over a geographic area larger than that served by an individual LAN.

Web Server

A specific type of server that contains pages, images and files that are accessed and displayed by a browser. Each page can contain links to other pages which a user clicks on to move from one page to another.

Wireless Network

A method by which a number of systems or computers communicate with a base station to provide network functionality, but without physical cables between them.

GENERAL BUSINESS ADVICE

For more information on achieving best practice in your business contact your local Business Link advisor by visiting the website at <http://www.businesslink.gov.uk> or calling 0845 600 9 006.

Published by the Department of Trade and Industry. <http://www.dti.gov.uk> © Crown Copyright