Computer audit & infosec jargon buster

This glossary lists common computer audit and information security terms with their usual definitions in that context.

Please be patient - it takes quite a while to download!

Contact us with any additions or corrections, we update it frequently.

Term	Definition
	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Abacus Sentry	Public-domain UNIX utility to detect the use of a port scanner in real time.
Abuse	See computer abuse or breach.
Access control, access rights, access rules	The technique of limiting access to a sensitive and/or valuable resource, such that only authorised subjects (typically users, systems or programs) can reach the resource. Having gained access to the resource, the system may limit the subject's rights (abilities) by rules, typically using an ACL.
Access router	A router used to connect directly to the Internet or other external network. Generally forms the first layer of network perimeter controls.
Account	See username.
Accountability	The concept of holding individuals personally responsible for their actions. Implies the ability to trace actions uniquely to individuals, generally through the use of audit trails (recording what happened) and user authentication (identifying the perpetrator). Also used in the wider sense of management responsibilities *e.g.* to implement appropriate governance controls.
ACL (Access Control List)	In most operating systems, an object (*e.g.* a network port, service, file, directory, memory location or device) may have a set of access control rules attached to it. When a subject (normally a process acting on behalf of a user) attempts to access the object, the system's security kernel checks down the access list until it matches the subject's ID in which case it executes the rule. There may also be a default or implicit rule (*e.g.* "allow full access" or "disallow all access") in case there is no explicit matching entry.
ActiveX	Microsoft software technology for downloading and running signed COM (Component Object Model) code, Win32 programs *etc*. ("controls") embedded within web pages. The author of each ActiveX control can optionally mark it "safe for scripting", thereby allowing it *unrestricted* access to the client operating system. If a user inadvertently accepts and executes a malicious or bug-ridden ActiveX control downloaded directly from a hacked web page, or indirectly via a hyperlink to another website, security of the user's client machine and LAN may be severely compromised. See also Java.
Administrator (ID)	The default username of the main system management account on Windows NT systems, broadly equivalent to ROOT for UNIX. System managers or hackers who gain access to this privileged account can bypass practically any automated controls on the system.
AES (Advanced Encryption Standard)	An encryption algorithm (Rijndael) chosen by the US National Institute of Science and Technology to replace DES (but not triple-DES) as a new Federal Information Processing Standard (FIPS) by summer 2001.
AIDE (Advanced Intrusion Detection Environment)	Public domain UNIX utility, similar to Tripwire, used to detect changes in important files.
	A UNIX-based public domain read-only anonymous FTP server.

Anonftpd	
Anti-virus control	Special security software and procedures designed to detect and prevent the introduction and spread of computer viruses and similar malware into (and sometimes out of) an organisation.
Anton Pillar order	In the UK, a copyright holder with reliable information that another party is infringing their copyright may approach the courts for a so-called Anton Pillar order giving the right to search the other party's premises without prior notice in order to obtain further evidence.
Application, application program	Computer program/s in software or firmware performing one or more useful data processing functions for users of a system. Relies on hardware and operating system software to operate.
Application-level firewall	A type of firewall that maintains the complete TCP connection state and sequencing but performs security processing at the application layer (*e.g.* automatic address translation to hide internal IP addresses from the outside world).
Argus	A UNIX-based public domain IP network monitoring tool. Provides facilities to compare network activities against security policies *etc*.
Arpwatch	A UNIX-based public domain utility to track and cross-reference IP addresses against Ethernet addresses on a LAN *e.g.* for signs of spoofing.
ASP (Active Server Page)	Microsoft software (built-in to IIS) that allows web pages to be generated dynamically by the server. As with other similar systems, ASP security vulnerabilities have been abused by hackers to gain unauthorised access to server- or client-side resources.
Assurance	A measure of confidence that the information security and control features and architecture of a computer system (collectively or individually) satisfy the security requirements, policies *etc.* Assurance is rarely absolute.
Attack	A deliberate, active attempt by a perpetrator to breach security controls on a computer. The attack may actually alter, release, delete or deny access to data and/or systems, or the perpetrator may simply gain unauthorised access. There may or may not be any direct material impact as a result. The success of a particular attack depends on the vulnerability of the computer system *i.e.* the effectiveness of existing controls at the time.
Audit, auditing	The independent examination of a sample of records, activities and/or systems to assess the state of governance, to ensure compliance with established controls, policies and procedures, and to recommend control improvements where judged necessary to reduce risks. Role performed by Internal and External Auditors and, for computer systems, Computer Auditors.
Audit (auditable) event	A discrete action detected by the system that may or may not generate an record in the audit log. Depending on audit rules (parameters) comprising the system's logical security policy, the system determines whether or not to record each audit event in the audit log.
Audit log, audit trail, audit record, activity log	A chronological record of audit events, linked to the corresponding user IDs, used to reconstruct and verify an historical sequence of actions. May also include (or be cross-related to) other logs and records *e.g.* system security logs, change logs (records of authorised system changes), error logs *etc.*
Authenticate, authentication, authenticity	The process positively to establish (beyond all reasonable doubt) the validity of a user, device or other object's claimed identity, often as a prerequisite to allowing access to controlled resources in a system. Normally involves verifying a distinctive (digital) signature, password, fingerprint *etc.* and/or the possession of a token, that would be practically impossible for anyone else to forge.

Authorisation, authorised, unauthorised	The granting of permission by a resource owner to an authenticated individual to access the resource for a specific purpose. Access which is not covered by an explicit authorisation may be covered by an all-encompassing default rule (*e.g.* "all access is deemed unauthorised unless specifically authorised by management") – this kind of catch-all condition is commonly used in ACLs including access rules for firewalls.
Automated controls, technical controls	Security controls enforced and enacted automatically by a computer/network system *e.g.* the login process (*c.f.* procedural controls).
Automated security monitoring	Automatic system processes that continuously or periodically confirm the correct operation of security controls *e.g.* by scanning intrusion logs for intruder alerts, re-calculating and comparing against stored hash values for critical files *etc.*
Availability	The assurance that data/information, data processing functions and communications services will in fact be ready for use by authorised users when and where expected or required, without unacceptable delay. See also threat, vulnerability, impact and risk.
	A **B** C D E F G H I J K L M N O P Q R S T U V W X Y Z
Backdoor, trapdoor	A hole in the system access controls deliberately installed by designers, maintainers or hackers. Hidden software or hardware mechanism used to circumvent security controls *e.g.* the "Back Orifice" Trojan. Some backdoors, originally installed for legitimate purposes (*e.g.* for support access to a database), are now being exploited illicitly by hackers.
Backup, restore	The process of making a duplicate copy of data and/or systems for safe storage (normally in a fire-safe, often off-site), such that if the original data or systems are lost or unavailable, the backups may be retrieved and reloaded, possibly at a secondary (recovery) site.
Bastion host	A hardened server, specifically designed to resist hacker attack and located on the network in a position likely to come under attack (*e.g.* in the DMZ or outside on the public Internet).
Bindview	Well-known UNIX networking program that implements DNS services. Has been the target of numerous security exploits and patches.
Black hats	Figurative term for 'the bad guys' – fraudsters, crackers or hackers with malicious intent towards a target network or system (*c.f.* 'white hats').
Block cypher	A type of encryption function that encodes plaintext in fixed-bit blocks using a key whose length is also fixed in length (*c.f.* stream cipher).
Blowfish	A 64-bit block cypher having key lengths of 32 to 448 bits.
Bomb, crash, Blue Screen of Death, bugcheck, crashdump	A gross software, firmware or operating system failure that completely stops execution of the function, program or entire system, *i.e.* it reduces system availability. 'Blue Screen of Death' (BSoD) refers to the typical colour of an exception (system failure) message reporting a complete failure of a computer operating system (also known as a bugcheck or crashdump).
Breach, compromise, exploit, incident, intrusion, violation	The materialisation of a risk *i.e.* the defeat of defensive security controls which actually does result in unauthorised penetration of the system, a loss of system/data integrity, loss of availability *etc.* A violation of the defensive controls in a particular information system such that information assets or system components are unduly exposed. An intrusion into a computer system where unauthorised disclosure, modification or destruction of sensitive information has or may have occurred. Can include probes, physical events (vandalism, computer room floods/fires, power outages *etc.*), virus infections, worms *etc.*
Bridge	A network device interconnecting two or more networks that passively transfers data packets between them at the data link or network layers. In contrast to a brouter or router, a bridge has very limited data processing functionality except for the decoding of packet addresses and basic packet integrity checking. It generally does not filter out traffic.

Brouter	A network device interconnecting two or more networks which passively transfers certain types or classes of data between the networks but actively filters, blocks or modifies others – a combination of bridge and router.
Browse, browser, browsing	Someone who casually looks around a computer system's files and parameters, looking for 'interesting' files or security vulnerabilities. Often precedes a hacking attempt.
Brute-force attack	Describes a direct frontal method of attacking a target head-on *e.g.* trying all possible combinations of characters to guess encryption keys or passwords (*e.g.* see Crack), or 'ram-raiding' (thieves who use cars to smash through windows or walls).
BS7799, ISO/IEC 13335	BS7799, the British Standard Code of Practice for Information Security Management, defines a control framework for establishing and maintaining an adequate level of information security. Due to become an international standard called ISO/IEC 13335.
Buffer overflow	This happens when more data is put into a buffer or holding area than it can handle, normally due to a mismatch in processing rates or data length between the producing and consuming processes. Buffer overflows can simply cause system crashes (*e.g.* in Denial of Service attacks) or may be deliberately exploited by skilled hackers to modify (overwrite) program code or data in normally inaccessible areas of memory and thereby penetrate security defences (*e.g.* to gain privileged access).
Bug	An unintended property of a program or piece of hardware, especially one that obviously causes a gross malfunction (overt bug) but also one that causes an unrecognised or what seems a relatively trivial problem (cryptic bug). It has been estimated that less than 10% of the bugs in commercial software known by developers are ever noticed and reported by users. Bugs in commercial software that expose security vulnerabilities are frequently being reported through Internet security news groups *etc.*
Bugtraq	Internet newsgroup through which recent exploits are discussed. Also available on the WWW at www.bugtraq.com
	A B **C** D E F G H I J K L M N O P Q R S T U V W X Y Z
CD-ROM	Compact Disk – Read Only Memory data storage device. Useful to store a known good copy of operating system and application program files on a hardened server, as the CD-ROM itself cannot be modified or replaced without physical access to the drive (although it may potentially be bypassed or modified in software if the system is insecurely configured).
CERT (Computer Emergency Response Team)	Worldwide organisation of white-hats dedicated to disseminating information about exploits and fixes through www.cert.org
Certificate	See digital certificate.
Certification authority (CA)	The trusted top-level function/s in a PKI that actually creates valid digital certificates, issues them to authenticated users through registration authorities, and revokes them when necessary using the certificate revocation list, according to the Certification Practice Statement. Usually generates the users' asymmetric key pairs.
Certification Practice Statement (CPS)	Formal document describing the structure and operating rules of a PKI.
Challenge-response	Refers to the sequential process commonly followed to authenticate a user or system to another, whereby: (a) one party issues a challenge, expecting a particular response, (b) the other party duly responds, (c) the first party validates the response to confirm the other's identity. Typical examples are the conventional login process and the establishment of an encrypted network session *e.g.* using SSL.
Checksum, parity check	An error-control (data validation) technique that typically uses a hashing function to identify a loss of message or file integrity (*i.e.* if the data content has been altered in transit or storage). The simplest form is a parity check – a single bit which is set if the number of other set bits in the byte is even, or is reset if there are an odd number of other set bits (although this would not necessarily identify message truncation or other multiple bit changes). 'Cryptographic checksums' are more reliable.

Check total	Another simple data validation technique, comparing a key parameter (such as the total number of data items) before and after another function. Separately calculating and comparing column- and row-wise grand totals is a common control in spreadsheet systems, for example.
CGI (Common Gateway Interface) scripts	Programs used to generate dynamic/interactive HTML web pages according to the content of data obtained from the web server. A common cause of website vulnerabilities.
Chosen plaintext attack	Cryptanalysis technique in which the cryptanalyst possesses both the section of plaintext and the corresponding cyphertext. The known plaintext forms a 'crib' that indicates when the decryption is complete.
Coding, decoding	The straightforward conversion of a message or other data to or from a defined format, generally by a published and freely-available simple algorithm or method (*c.f.* encryption, decryption). The term 'computer coding' usually refers to application programming.
Common-mode failure	Where redundant parts of an information system/network share certain characteristics, they may both be simultaneously vulnerable to the same common threat (*e.g.* multiple systems sharing a power feed may all fail if the supply fails).
Compliance	Conforming with security policies, procedures *etc*. A compliance audit, then, seeks to verify that the subject has not 'broken the rules'.
Compromise	See breach.
Computer abuse/misuse	The wilful or negligent unauthorised activity that affects the confidentiality, integrity and/or availability of computer resources, including fraud, embezzlement, theft, malicious/accidental damage, unauthorised use, denial of service, misappropriation, data modification, disclosure or destruction.
Computer audit	Specialised branch of auditing concerned with examining and advising on the information security controls environment (technical and procedural controls) within and surrounding computer systems and networks. Typically includes reviewing, testing and advising on information security control frameworks, system security designs, logical controls, software development projects, operational systems, end-user and system administrator procedures, computer room facilities, computer security incidents *etc.*
Computer fraud	Crime involving deliberate misrepresentation and/or alteration of computer data in order to obtain unauthorised access to valuable assets (*e.g.* logging on to a bank system through another person's user ID or sending a forged EMAIL to authorise an illegitimate money transfer).
Computer security	Technical and managerial/operational procedures applied to computer and network systems to ensure the confidentiality, integrity and availability of data and data processing systems.
Confidentiality	Assuring that information will be kept secret, with access limited to appropriate authorised persons, program functions *etc.* using access controls such as limited logical access rights and restrictive clauses in employment contracts limiting disclosure of trade secrets *etc.*
[Information security] Control, countermeasure	Action, device, procedure, technique or other measure that reduces the vulnerability of a computer system or network to one or more threats or reduces those threats (preventive controls), or reduces the impact should breaches occur (detective and/or corrective controls).
[Information security] Control framework	The set of laws, objectives, rules, policies, standards, guidelines and practices that regulate how the organisation manages, protects and distributes sensitive information and other valuable IT assets. See also BS7799.
COPS (Computer Oracle and Password System)	Public domain program that identifies certain security risks on a UNIX system, such as null (non-existent) passwords, world-writeable files, mis configured anonymous FTP and many others. See also SATAN.

Copyright	Apart from true public-domain software or freeware, computer software is generally subject to the laws of copyright to protect it against theft and abuse. Software purchasers rarely end up owning the software as such, but are granted certain limited rights to copy and use it by the true owner, the copyright holder.
Corrective control	A class of infosec controls designed to reduce the impact of certain breaches by restoring the system more-or-less to the unbreached condition *e.g.* restoring from backups (*c.f.* preventive and detective controls).
Courtney	A public-domain UNIX-based utility that attempts to identify the use of SATAN.
Crack	Hacker program that tries to 'guess' passwords by brute-force attack *i.e.* it sequentially hashes words from a dictionary or formed from random characters, and compares the result with the values stored in a password file (usually stolen). On a fast system, Crack can guess hundreds of passwords per second.
Cracker, cracking	Some people refer to hackers with malicious intent as 'crackers' to distinguish them from so-called 'benevolent hackers who merely seek the intellectual challenge'. In practice, it can be very difficult to tell them apart. Both types create information security threats.
CRL (Certificate Revocation List)	List within a PKI of digital certificates that are no longer valid. After a given certificate is presented but prior to being accepted, the recipient is supposed to check against the CRL in case it has been revoked (withdrawn or invalidated).
Cryptanalysis, cryptanalyst	The analysis of a cryptographic system and/or its inputs and outputs to derive confidential variables and/or sensitive data such as keys and plaintext. Operations performed in converting encrypted messages (cyphertext) to plaintext without initial knowledge of the crypto-algorithm and/or key employed in the encryption, *e.g.* chosen plaintext attack.
Cryptographic system	Specification and/or embodiment of the process and algorithms for encrypting and decrypting data.
Cryptography ('crypto')	The mathematical science concerning the principles, means and methods for rendering plaintext unintelligible by a defined algorithm and for converting cyphertext back into intelligible form. Includes the study of encryption strength and theoretical proofs.
CUG (Closed User Group)	A club of certain individuals, organisations or systems that are invited to join together for common interest, excluding others (typically connected by a VPN or similar mechanism).
Cyphertext	The encrypted and unintelligible output version of a plaintext input having been fed through an encryption algorithm. Provided a 'strong' encryption algorithm is used (*i.e.* one that is highly resistant to cryptanalysis), it should be virtually impossible to reconstruct the plaintext from the cyphertext without knowledge of the secret encryption key/s.
	A B C **D** E F G H I J K L M N O P Q R S T U V W X Y Z
Daemon	The name of a resident, normally-running program or process that monitors a system for certain events (*e.g.* the arrival of network traffic), then acts on them (*e.g.* passes the data to the appropriate destination service). A typical security daemon monitors all logical access attempts and intercepts those which are unauthorised, creating a security log entry and denying access.
Data	The electronic, symbolic representation of information (descriptions, values, pictures, commands *etc.*) as a sequential series of discrete digital bits or of arbitrary analogue values within a certain range, grouped together in bytes, words, files, packets, messages *etc*. For fellow pedants, 'data' is the plural form of 'datum'.
Denial of Service (DoS) attack	An attack which prevents any part of a computer or network system from functioning in accordance with its intended purpose by denying or delaying access to the service, its inputs or outputs *i.e.* it reduces availability.

DES (Data Encryption Standard, also known as DEA - Data Encryption Algorithm)	A symmetric cryptographic algorithm, a block cipher, popular in the finance industry. DES survived public scrutiny since the 1970s and was therefore widely trusted, especially in triple-DES (3DES) form, a more secure, albeit slower, algorithm that repeats the DES encryption three separate times with different keys (most purportedly triple-DES implementations, however, in fact use only two keys: key A for the first round of encryption, key B for the second, and key A again for the third). Soon to be replaced by AES.
Detection	Establishment of the occurrence of an information security incident.
Detective control	A class of infosec controls designed to identify particular security breaches, such as Tripwire (*c.f.* preventive or corrective controls).
Diffie-Hellman	Public-key encryption algorithm used mostly for exchanging symmetric encryption keys. Its security rests on the difficulty of computing discrete logarithms in a finite field generated by a large prime number.
Digital certificate	Electronic representation of an identification certificate or passport, issued by a certification authority to a *bona fide* PKI user, stating identification information, validity period, the holder's public key, the identity and digital signature of the issuer, and the purpose/s for which it was issued (*e.g.* encryption, signature *etc.*). Certificates are digitally-signed by the issuer to guarantee their authenticity.
Digital fingerprint	Data that allows the source of an information asset to be verified, for example the particular nature, sequence and timing of a hacker's activities recorded in the system security logs may reveal the hacker's tools, or copyright information may be hidden within a computer image (steganography).
Digital signature	Data including a hashword encrypted with the issuer's private key and appended to a file or digital certificate, that can be verified by decrypting with the issuer's public key to prove the integrity and source.
Disaster Contingency Plan (DCP)	Plan describing the initial responses (at least) to a physical or logical disaster scenario affecting valuable resources and services. Generally links to other emergency plans (*e.g.* crisis plans, emergency services call-outs) to stabilise and assess the immediate post-disaster situation, before calling on specific disaster recovery plans for long term restitution.
Disaster Recovery Plan (DRP)	Plan describing the steps required to recover particular resources and services to a usable state in the aftermath of a more-or-less specific disaster (*e.g.* by retrieving data from backups, installing replacement LAN equipment *etc.*) and to minimise the impacts. Common DRP variants cover situations such as data loss, major frauds, virus infections, unauthorised systems accesses (hacks) *etc.*
Discretionary access controls	Access control rules that may be modified and/or bypassed by users (*c.f.* mandatory access controls).
Distributed Denial of Service (DDoS) attack	A form of Denial of Service attack using hundreds or thousands of 'slave' machines simultaneously targeting the system/s under attack, all initiated and/or co ordinated in concert by one or more 'master' systems.
DMZ (Demilitarized Zone)	Section of network between outer (Internet-facing) and inner (LAN-facing) firewalls, in which hardened web servers, DNS servers *etc.* are generally located. The outer firewall provides a degree of perimeter access control but permits certain TCP/IP traffic to reach the DMZ servers. The inner firewall provides additional isolation for the LAN.
DNS (Domain Name Service) server	DNS servers, typically running Bindview, communicate over the network to establish and update a distributed database linking the IP addresses of hosts and other network resources with their corresponding URLs. If a DNS server is compromised, calls to specific IP addresses or URLs may be redirected to spoofs, and network performance and availability may be degraded.

Dual-control	A control step in a process requiring the co-operation of (at least) two trusted people or systems to authorise the next step *e.g.* 'management authorisation' of transactions initiated by staff. Reduces the probability of errors, theft or fraud unless there is collaboration between the individuals.
Dual-homed gateway	A server with two (or more) network interfaces connected to different networks, acting as a router between those networks and generally implementing security controls (*e.g.* packet filtering).
Duress function	A user being threatened or forced to use a system incorporating a duress function may surreptitiously enter a secret code (*e.g.* a special password or key sequence) to trigger a silent alarm, alerting security staff, whilst appearing to use the system normally.
	A B C D **E** F G H I J K L M N O P Q R S T U V W X Y Z
Encrypt, encryption, decrypt, decryption	The mathematical process of converting a plaintext input string into cyphertext output string using a cryptographic function (*e.g.* DES) and one or more encryption keys. Cryptographic functions may have holes *e.g.* the hashing algorithm MD4 was originally believed to be strong but has since been shown to be insecure. See also PKI.
Encryption key, key pair	A string of symbols, characters or bits used to determine the way the encryption function converts the plaintext to the cyphertext or *vice versa*, or to set the encryption algorithm to a known starting state (seed value). The length of the key, coupled with the particular algorithm used, determines the strength of the encryption function since small keys may be guessed much more readily by brute-force attacks. Note: public key encryption uses matched complementary public and private key pairs.
Escrow	Control against accidental or deliberate loss or destruction of a vital piece of data (*e.g.* proprietary source code or encryption key) by maintaining one or more copies in secure locations, often provided and maintained by a trusted third party such as a commercial escrow agent, lawyer *etc*.
Ethernet	The most popular LAN protocol. Devices on an Ethernet LAN are identified by unique Ethernet addresses, generally hard-coded into their firmware, making it difficult to spoof Ethernet devices. However, as all data packets normally pass all interconnected nodes in a given Ethernet LAN segment, a sniffer in promiscuous mode can readily read them even if they are *en route* somewhere else.
Exploit	The description of a deliberate information security breach or hacking method. Information concerning the exploit may be published by hackers to encourage further systems abuse and/or by information security experts to encourage vendors to fix the vulnerabilities.
	A B C D E **F** G H I J K L M N O P Q R S T U V W X Y Z
Fail-over, fault tolerance, redundancy	The ability of a system or component to continue or recommence more-or-less normal operation despite experiencing hardware or software faults or other breaches/control failures, generally by transferring operations to an alternate device or location. Fail-over may be automated or manual (*i.e.* someone has to select the alternate system). Fault tolerance techniques include RAID disks, 'voting' systems and other multiple/redundant system arrangements, but may remain vulnerable to common-mode failures. A corrective control.
Firewall	A specialised router (or equivalent functionality within a dual-homed gateway or network host) that enforces a controlled gateway (security boundary) for data packets passing between networks according to security policies enshrined in its operating system and ACL parameters, *e.g.* "only pass packets to certain destination addresses", "disallow access to particular IP services or ports".

Firmware	A hardware device, such as a Read Only Memory chip, containing low level software, typically a device controller and/or boot sequence (operating system loader or BIOS). Potentially vulnerable to attack by a hacker with physical access to the system, hence the need for physical access controls to protect sensitive systems from compromise.
Forgery	The unauthorised generation of authentic-looking copies of negotiable instruments (cash, company cheques, share certificates *etc*.) and similar items, including electronic versions (electronic money transactions, digital certificates *etc*.). Forged EMAILs, for example, may be used as part of a fraud by purporting to authorise money transfers.
Fraud	An illegal act involving deliberate misrepresentation. For frauds involving the use of computers, see computer fraud.
Fraudster	A person who commits a fraud. Often, a trusted long-serving member of staff, sometimes an outsider.
FTP (File Transfer Protocol)	Part of the TCP/IP suite of protocols concerned with transferring data files between systems over a network. In its standard format, FTP incorporates minimal security *e.g.* message contents, plus usernames and passwords used for access control, are transferred in plaintext.
	A B C D E F **G** H I J K L M N O P Q R S T U V W X Y Z
Governance	An organisation's total system (corporate governance) or information security controls framework (information security governance) or other process of controlling operations to limit risks and prevent adverse impacts.
	A B C D E F G **H** I J K L M N O P Q R S T U V W X Y Z
Hardened server	A server that has been specifically configured to maximise security *e.g.* by removing all non-essential applications, running a secure operating system with a broad range of security monitors and alarms *etc*.
Hardware	Computer equipment and peripherals. Vulnerable to physical damage (vandalism, fire, flood), interference and theft, hence the need for physical access controls to protect sensitive hardware such as shared servers, encryption devices containing stored keys, communications lines, automated teller machines *etc*.
Hack, hacker, hacking	Broadly, hacking is the intellectual challenge of exploring computers and networks, stretching their capabilities, trying to discover information *etc*. More specifically, it is attacking a system with malicious intent to break (circumvent or bypass) the controls (also known as cracking). Media exposure leads the public to believe that most security violations are the results of hackers or "outsiders", however many unauthorised acts, including malicious acts, are carried out by disgruntled employees or other insiders.
Handshake	Typically, a simple form of challenge-response process.
Hash, hashing, hashword	A mathematical function that generates a particular small value (the hashword) from a larger data unit by a form of 'one-way encryption'. A given hashword is extremely unlikely to be generated from any other input string. Even a tiny change in the input string creates a radically different hashword, disclosing that an unspecified change has occurred. Changes to the data in storage or in transit can be detected by recalculating the hashword on retrieval or receipt and comparing it to the original (generally included within the message packet), provided the hashword is itself protected against compromise. This virtually guarantees message integrity.
Hijack	Type of attack in which a hacker takes control of, or interferes with, a legitimate user's active session, typically by using a logged-in but unattended terminal or by spoofing the user's IP address and injecting malicious packets.
Hoax	A malicious attempt to persuade someone that a fictional threat is real. Hoax EMAILs concerning fictional viruses tend to spread through the Internet in similar fashion to worms, albeit without a destructive payload.

Honeypot	A network host deliberately configured to entice hackers into attacking it in order to learn about their techniques and delay them or divert their attention from other potential targets. A form of proactive defence.
Host, host-based	A single computer server or workstation system, generally connected to a network. Host-based security consists of operating system software configurations *etc*. designed to secure a single system from attack.
	A B C D E F G H **I** J K L M N O P Q R S T U V W X Y Z
ID (identifier or identity), user ID, username, account	Within a computer system, processes owned by users and other objects are identified by ID codes. Access rights are assigned to user IDs to determine which assets a user may access, and what type of access they are granted (RWEDC). Users are generally authenticated at logon time to ensure they are in fact as indicated by their IDs.
IDEA (International Data Encryption Algorithm)	Encryption algorithm which uses a 128-bit key. IDEA is viewed as a good algorithm for all except the best-funded attacks. It is used in PGP and Speak Freely (a program that allows encrypted digitised speech to be sent over the Internet).
Impact	The adverse outcome (direct and indirect costs) on the resource owner of a compromise to the security controls *i.e.* the loss of confidentiality, integrity or availability. This may include direct financial losses (*e.g.* thefts of valuable data or systems), consequential damages, recovery/restitution costs, loss of credibility and reputation, loss of business, liability to prosecution *etc*.
Incident	An actual or attempted breach.
Information security (infosec)	The result of implementing appropriate policies, standards and procedures for identifying, controlling and protecting from unauthorised disclosure, disruption or loss, information and other assets requiring such protection. The totality of the information controls environment.
Insider	Someone who works within an organisation, either a permanent member of staff/management, temporary staff, contractors, consultants *etc*. Most security breaches and frauds (in terms of number of incidents if not their severity) are caused by insiders in positions of trust (*c.f.* outsiders).
Integrity	Prevention of the unauthorised modification of data (data integrity), computer systems and networks (network/systems integrity), data processing functions/operations (systems/database integrity) and/or the information controls environment (information security integrity). A person or system with integrity is trustworthy and can be relied upon.
Internal Audit, External Audit	Function within (Internal Audit) or without (External Audit) an organisation concerned with the independent examination of records and systems of control, and advising management on how to reduce risks to the organisation. Modern Audit functions include information security control specialists, generally known as computer auditors.
[The] Internet	The Internet (with a capital I) is a global public TCP/IP network interconnecting billions of users with millions of hosts and their information resources. Originating with ARPAnet and academic networks (like JANET), the Internet was founded on the principle of open access to resources, so access control was not a design goal. It is also operated by a community largely without formal central control, leading to a degree of diversity. However, it has proven extremely resilient with very few widespread failures (*e.g.* when someone accidentally deleted the entire .COM master domain name server database by mistake …).
Intrusion	An attempt to compromise the confidentiality, integrity or availability of a protected or sensitive resource (network, system, data *etc.*) by accessing it without proper authority. A successful unauthorised access (penetration) into a computer or network. See also breach.

Intrusion detection system (IDS)	Techniques and systems to detect intrusion into hosts and/or networks by logging and responding to suspicious (potentially unauthorised) activities. Generally involves the generation of security alarms/alerts and sometimes the initiation of active countermeasures.
Invalid	The opposite of valid.
IP (Internetworking Protocol)	A datacommunications protocol for interconnecting networks, part of TCP/IP. IP traffic uses IP addresses (*e.g.* 10.0.0.1) to identify source and destination systems.
IPsec	A secure (encrypted) version of IP.
IP splicing	An attack whereby an active, established IP session is intercepted and co opted. Splicing attacks typically occur during or after an authorised user has been authenticated, permitting the attacker to assume the legitimate user's identity and hence his/her role and access rights. See also hijack.
IP spoofing	A spoofing attack whereby a system attempts illicitly to impersonate another system using its IP network address. Typically achieved by compromising a DNS server.
ISS (Internet Security Scanner)	Program that checks hosts within a specified range of IP addresses for various security vulnerabilities in sendmail, anonymous FTP, NFS *etc.* See also COPS and SATAN.
	A B C D E F G H I **J** K L M N O P Q R S T U V W X Y Z
Java, JavaScript, Javabeans	Java provides a 'virtual machine' *i.e.* a standardised computer operating system environment that runs within various other host operating systems. Java programs are thus highly portable. Unfortunately, there are certain weaknesses in the Java security model that may be exploited by malware to attack the host system. JavaScript and Javabeans are essentially subset languages derived from Java. See also ActiveX.
	A B C D E F G H I J **K** L M N O P Q R S T U V W X Y Z
Kerberos	An authentication system using encryption. Windows 2000 uses Kerberos v5 to authenticate users at login time.
Key	See encryption key. Also, of course, the device used to open a physical lock.
Key escrow	The system of giving pieces of an encryption key to each of a certain number of trustees such that the whole key can only be recovered with the collaboration of all the trustees (a form of dual-control).
Key management	The generation, storage, distribution, deletion, archival and use of encryption keys.
Klaxon	This is a UNIX daemon that is used to identify the use of port scanners like ISS and SATAN.
A B C D E F G H I J K **L** M N O P Q R S T U V W X Y Z	
LAN (Local Area Network)	A communications network linking computers in one location (typically a single building) using high-speed connections (*e.g.* 1 to 100 megabits per second). *C.f.* WAN
Layered security	See security-in-depth.
Logical security control	Security control in software operating on data, as opposed to procedural and physical controls. Anti-virus software, user rights and access permissions, data backups, encryption and data entry validation routines are typical examples.
Logic bomb	A computer program (or function within another program) which, when executed, checks for a particular condition or state of the system (or else may be remotely triggered over a network connection) and performs an unauthorised act causing an impact. See also payload.

Login, logon	The process whereby a user identifies his/herself to the system and is authenticated, generally by a password and/or security token. Hackers often try to subvert the login process *e.g.* by bypassing the login process, brute-force attack (guessing passwords), exploiting weak or missing passwords and backdoors, or modifying/replacing the login programs. Once logged-in, the system grants access to resources according to the access rights assigned to the user ID, generally without further authentication.
	A B C D E F G H I J K L **M** N O P Q R S T U V W X Y Z
Malicious code, malware	Hardware, software or firmware that is intentionally included in or introduced into a system for an unauthorised purpose *e.g.* logic bomb, Trojan horse, virus. 'Malware' typically refers to software that combines the properties of a virus and a worm *i.e.* instead of being a standalone executable program that replicates, it is a piece of software that uses a popular host like JavaScript, VBScript or some application macro language to do its work, and replicates via the network connections. ExploreZip, Happy99, Melissa and the ILOVEYOU variants are examples.
Mandatory access controls	Access control rules that are automatically enforced by the system and cannot normally be circumvented by users (*c.f.* discretionary access controls).
Manual controls	See procedural controls.
Masquerade	A person or system that assumes a false identity (see also spoof).
MD5	Message digest hash function developed in 1991 which is used to hash a file of arbitrary length into a 128-bit value. Used by PGP.
Message Authentication Code (MAC)	A data field used to verify the authenticity of a message (*i.e.* its integrity and origin) using public key encryption and/or hashing.
Multi-level security/system (MLS)	A computer system incorporating rules determining the permissible access rights for data/messages according to their classification. A practical implementation of the concept of security-in-depth.
	A B C D E F G H I J K L M **N** O P Q R S T U V W X Y Z
Nak attack	Nak is the TCP/IP 'Negative Acknowledgement' message. A Nak attack is a hacker system/network penetration technique that capitalises on an operating system vulnerability concerning improper handling of asynchronous interrupts, leaving the system in an unprotected state during such interrupts.
Network level firewall	A firewall in which traffic is examined and controlled at the network protocol (packet) level, primarily on the basis of source and destination IP addresses and possibly services or ports requested (*c.f.* proxy firewall).
Network security	Protection of networks, data in transit and the network services from information security risks such as unauthorised modification, destruction, disclosure or disruption. Gives assurance that the network performs its critical functions correctly with no harmful side-effects, and provides an adequate level of data integrity.
Non-repudiation	Method by which the sender of data is provided with proof of delivery and the recipient is assured of both the sender's identity and message integrity, so that neither can later deny having exchanged the data. Generally provided through a reciprocal system of public key cryptography.
	A B C D E F G H I J K L M N **O** P Q R S T U V W X Y Z
Operating procedures, system/network management procedures	Processes by which system/network operators, managers and other staff operate, manage, maintain, update, monitor and secure computer systems and networks. Normally documented (to some degree) in formal standards, operations manuals, training guides *etc.* Incorporate procedural controls.
Operating system	A suite of software and firmware programs linking the application programs to the computer hardware, networks and peripheral devices. Provides a wide range of services and functions, including many logical security controls.

Outage	Period during which a service, data, system or network is unavailable. May either be pre-planned and authorised (*e.g.* for routine database maintenance), or represent a control failure (*e.g.* the unplanned but accidental result of a bug, power cut, flood or lightening strike, or due to the system being deliberately compromised by an attacker).
Outsider	Someone who does not work within an organisation *i.e.* a member of the general public. Outsiders such as hackers, spies or undercover agents from another organisation may represent a realistic information security threat to an organisation but often need insider assistance to complete an effective attack.
	A B C D E F G H I J K L M N O **P** Q R S T U V W X Y Z
Packet	A block of data sent over a network, containing the identities (network addresses) of the sending and receiving stations, error-control information (*e.g.* checksum, message length), and some message content or payload.
Packet filter	A feature incorporated into routers, brouters and bridges to limit the flow of information based on pre-determined communications parameters, generally in the packet headers, such as source or destination IP address or type of service being provided by the network. A packet filter is one of the least secure types of firewall, being generally vulnerable to IP spoofing attacks *etc.*
Passive attack	An attack that does not result in an unauthorised state change, such as the interception (monitoring and/or recording) of data on a network (*c.f.* an active attack which alters data, triggers security alarms *etc.*).
Password	The traditional means of authenticating someone is to challenge them (*e.g.* “Halt! Who goes there?”) to reveal a known pass word (character string) that the person is otherwise meant to keep secret. If the pass word is correct, the person is assumed authentic and is permitted access. However, if the pass word has been disclosed to, or guessed by, an unauthorised person, it is useless as an authentication check without further information on the person’s identity (*e.g.* something physical they possess - a token or key - or some distinctive bodily characteristic such as a fingerprint or retina pattern).
Payload	The ‘business end’ of a virus, Trojan horse or logic bomb: the program code delivered by the malware that generally causes some unauthorised activity on the recipients’ systems, ranging from nothing detectable to extreme data loss, disk corruption *etc*. Alternatively, the data content of a message.
Penetration	Successful unauthorised access to a computer system or network.
Penetration signature	A situation or set of conditions in which a penetration could occur, or system events that in conjunction can indicate the occurrence of a penetration in progress or after the event (*e.g.* access log file entries).
Penetration test, pen test	A form of security testing in which ‘white hat’ evaluators (the tiger team) attempt to circumvent the security controls (primarily the perimeter access controls) to gain access to one or more networked systems. The testers may or may not be given system documentation (source code listings, network diagrams *etc.*) but normally work under the same constraints as ordinary users or members of the public.
Perimeter (security) controls	The technique of securing a network by controlling access to all entry and exit points of the network, normally using firewalls, or more broadly limiting physical access to sensitive resources (computer systems *etc.*) by installing walls, doors, door-locks, intrusion detection systems *etc.* Contributes to the concept of defence in depth by supplementing internal/logical controls.
Perpetrator, culprit	The entity (generally, the person) from the external or internal environment that originates or causes a deliberate information security attack, typically a hacker, cracker, browser or fraudster.
Personal data	Any information (not necessarily sensitive or private) relating to an identifiable individual person.

PGP (Pretty Good Privacy)	Public key encryption scheme, used widely for secure Internet EMAIL. Available free for non-commercial use (albeit with limited key lengths outside the US). Uses IDEA and MD5 algorithms.
Phrack, phracker, phracking	An individual who combines phone phreaking with computer hacking, typically using phreaking techniques to conceal his original point of entry into a network prior to launching a hacking attack.
Phreak, phreaker, phreaking	An individual fascinated by the telephone system, just as hackers and crackers are fascinated by (breaking into) computer systems. Commonly, an individual who uses his knowledge of the telephone system, telephone exchanges *etc.* to make phone calls at the expense of legitimate phone users, to redirect calls *etc.* See also phracker.
Physical security	Physical control measures (*e.g.* door locks and strong walls to prevent theft of or damage to systems, air conditioning and fire protection to prevent overheating damage and consequent loss of service) used to protect computer hardware *etc.* against deliberate and accidental threats. Includes perimeter controls.
Piggyback attack	The gaining of unauthorised access to a system via intercepting and taking control of another user's legitimate network connection. See also spoofing.
PIN (personal identification number) code	Generally, a numeric password technique first popularised by the banks for use with automated teller machines. Due to their simplicity, PIN codes are often vulnerable to guessing or brute force attacks, although most such systems now at least limit the number of invalid PIN attempts allowed before logging an intrusion event and preventing access.
Ping of death attack	The abuse of the IP 'Ping' service (meant to be used to test whether a remote device is responding) with over-sized packets (albeit still within the formal specification) causes a Denial of Service attack on many systems.
PKI (Public Key Infrastructure)	The total system (protocols, encryption algorithms, procedures/processes, systems *etc.*) described by a Certification Practice Statement through which public key cryptography is established and used by one or more organisations. Generally includes a certification authority that issues key pairs to authenticated users using digital certificates, a mechanism for checking the validity of certificates and digitally-signed messages *etc.*
Plaintext, cleartext	Unencrypted (generally directly human- or machine-readable) data *c.f.* *cyphertext* that must first be decrypted to be intelligible.
[Infosec] Policies, standards guidelines	A sound information security controls framework includes a comprehensive set of documentation describing the controls, both technical and procedural, that have been reviewed, approved and authorised by management to satisfy the organisation's governance requirements.
Port	TCP/IP network devices and applications communicate through numbered logical ports. If a certain port is 'opened' by a network application, then messages for the corresponding port number (as defined in the headers) will normally be passed to the application. By convention, certain ports numbers are reserved for well-known applications, therefore if the port is available the corresponding application is probably running (although it may not respond).
Port scanner	A program that probes network services by attempting to communicate through various TCP/IP ports. SATAN and ISS are well-known examples. See also Klaxon.
Preventive control	A class of infosec controls designed to reduce the probability of certain breaches *e.g.* logical or physical access restrictions (*c.f.* corrective and detective controls).
Privacy	The right of individuals to control or influence the collection, use and disclosure of their personal information.
Private key, secret key	The member of a pair of asymmetric encryption keys which is kept confidential (hence also known as the secret key) (*c.f.* public key).

Private key (symmetric) cryptography	An encryption methodology in which encryption and decryption use exactly the same key, that must therefore be kept private to the parties involved (*c.f.* public key cryptography). DES and RC4 are common symmetric algorithms. In terms of resistance to brute force cryptanalysis, a good 128-bit symmetric encryption algorithm is about as strong as 2043-bit public-key algorithm. Realistically, though, the public key should be even longer because the same public and private key pair is used to protect *all* messages to the same recipient.
Privilege	On most operating systems, certain 'privileged' users or processes are permitted to override security controls (such as file access controls). Typical examples are Administrator, ROOT and SYSTEM. Privileged access is often required for administering and configuring a system but should be limited as far as practicable to trusted users to maintain system security.
Probe	An effort to gather information about a machine, network or its users with the likely intention of hacking the system later. Normally uses network/system browsing, port scanning and/or social engineering techniques.
Procedural controls, manual controls	Controls embedded in operating procedures *etc.* and enacted by humans *e.g.* keeping passwords secret (*c.f.* automated controls).
Promiscuous mode	An Ethernet interface in promiscuous mode decodes all data packets on the network, not just those bearing its own network address. Sniffers operate in this mode.
Protocol	Agreed-upon method of communication used by networked computers or linked organisations *e.g.* TCP. A specification that describes the rules and procedures that products should follow to perform activities on a network, such as formatting data for transmission or encryption.
Proxy firewall	A firewall mechanism that replaces the actual IP address of hosts on the internal (protected) network with synthetic addresses, whilst maintaining session integrity for all traffic passing through it. May also use higher-level processing in the communications stack to control access to network services *etc.*, perhaps using additional authentication or other criteria (hence the actual service requested is replaced with a substitute incorporating additional security controls).
Public key	The member of a pair of asymmetric encryption keys which is generally published or readily available to others (*c.f.* private key).
Public key (asymmetric) cryptography	Type of cryptography invented by Whitfield Diffie and Martin Hellman in 1976, involving matched and complementary public and private key pairs. A plaintext message encrypted with either key can only be decrypted with the other. RSA is a famous example of an asymmetric algorithm, commonly used for PKI (*c.f.* private key (symmetric) cryptography).
	A B C D E F G H I J K L M N O P Q **R** S T U V W X Y Z
'r' (remote) commands: rlogin, rsh, rcp *etc*.	The 'r' series UNIX programs were originally written to allow access into a system by remote users *e.g.* to share local resources over the network amongst a trusted community. Hackers soon discovered however that they could abuse the 'r' commands very easily to gain unauthorised access to other UNIX systems having successfully hacked one or more systems in the community, or could exploit vulnerabilities in the 'r' commands directly (the user/system authentication is very weak).
RA (Registration Authority)	The function within a PKI that authenticates and registers users using the CA.
RAID (Redundant Array of Inexpensive Disks)	A disk-mirroring architecture designed to increase data availability and/or integrity (depending on the exact type of RAID used) by dispersing data over multiple redundant disks. Using error-correction techniques, data lost through failure of a single disk may be recreated automatically from information stored on the remainder.
RC4	An encryption algorithm. A stream cipher that adds the output of a pseudorandom number generator bit by bit to the sequential bits of the digitized plaintext.

Redundancy	Risk reduction or fail-over technique whereby key parts of an information system/network architecture are duplicated such that failure of one item may hopefully be mitigated by automatically or manually transferring processing to the other *e.g.* RAID. Note however that redundant systems may still be vulnerable to common-mode failures.
Rijndael (pronounced Rhine-doll)	Encryption algorithm adopted by the US National Institute of Standards and Technology as the new public Advanced Encryption Standard to replace DES. Uses keys of 128, 192 or 256 bits.
Risk	The chance combination of a threat acting on a vulnerability to cause an impact. Incorporates the concepts of probability and coincidence *i.e.* certain threats are more likely to occur, certain vulnerabilities are more likely to exist, and certain impacts are larger, therefore certain risks are of greater concern than others.
Risk assessment, risk analysis	The study of threats, vulnerabilities and impacts to assess the likelihood of their occurrence. Usually used to specify, define and/or establish the theoretical effectiveness of actual or proposed security controls (also called information security architecture/design).
Risk management	The total management process to identify, control and minimise the probability and/or impact of uncertain adverse events.
ROOT	As the ROOT account on a UNIX system is fully privileged and owns many of the key system resources, anyone who gains ROOT access can thus bypass practically any technical information security controls. This makes ROOT access a primary target for most UNIX hackers. See also SYSTEM and Administrator.
Router	A network interconnection device similar to a bridge but with higher level processing serving packets or frames containing certain protocols. Routers link LANs at the network layer.
RPC (Remote Procedure Call)	TCP/IP application, originally developed by Sun Microsystems, that allows a procedure or function on a network server to be remotely called over the network. Vulnerabilities in the RPC authentication process have been exploited by hackers.
RSA	One of the most commonly used public-key algorithms. Named after its creators: Rivest, Shamir and Adleman. Its security derives from the mathematical difficulty of factoring very large numbers (*i.e.* calculating their prime factors) compared to the ease of generating such numbers. A key length of at least 1024 bits is generally held secure enough but RSA may still be vulnerable to chosen plaintext attacks.
RWEDC	Refers to types of access control rights given to users and other objects in the system *i.e.* usually Read (read-only), Write (modify data, add new data), Execute (run programs), Delete or Control (take ownership of, change access rights to) [the C sometimes stands for Create (insert new records in a database)].
	A B C D E F G H I J K L M N O P Q R **S** T U V W X Y Z
Sandbox	Refers to a logical systems environment or enclosure (security perimeter) within which users can be permitted greater access than they are allowed elsewhere on the system *e.g.* a testing environment, or a virtual machine such as Java or ActiveX.
SATAN (Security Administrator Tool for Analyzing Networks)	A powerful freeware program for remotely probing and identifying the vulnerabilities of systems on IP networks. SATAN was released into the public domain ostensibly for honourable reasons (as a tool for busy network administrators to check out security on their own systems) but was quickly exploited by hackers to find weaknesses in public Internet hosts. SATAN can flood a network with probes, hence the need for defences against SATAN, such as Klaxon.
Script kiddie	Derogatory term for a hacker whose technical skills barely exceed the ability to run generic hacking scripts, tools and utilities written by others.

Secure erasure	By default, most operating systems do not actually erase a file's data contents from disk when it is deleted, but merely update the directory entry to save time. 'Unerase' programs (*e.g.* the 'retrieve from wastebasket' function in Windows) can therefore simply retrieve supposedly deleted data by resetting the directory entry. Using special hardware, it may even be possible to retrieve underlying data after the disk has been overwritten by using residual magnetism effects, although this is not very likely or reliable. Secure erasure, then, involves overwriting the disk several times to delete all traces of the original data.
Secure smartcard	Smartcard incorporating various tamper-resistant features and used to perform encryption and other functions such as user authentication and storage of private encryption keys, electronic money *etc.*
Security-in-depth, defence-in-depth	Having multiple overlapping layers of protection, such that an attacker would have to compromise several successive security controls to reach a target. In mediaeval castles, this involved a readily defended hill-top location, a moat, a strong and tall perimeter wall, battlements with skilled archers, an inner keep and so forth. In network security, it means using firewalls, hardened servers, intrusion detection systems *etc.*
Secret key	See private key.
[Information] Security	The result of specifying, establishing and maintaining appropriate protective measures (controls) to reduce the information security risks to an acceptable degree.
[Information] Security architecture, framework, design	A detailed description of all aspects of the system that relate to information security, along with a set of principles to guide the design. The information security technical architecture describes how the system is assembled to satisfy the information security requirements.
[Information] Security audit	An independent examination of the controls within a computer/network system and/or the supporting audit logs, procedures *etc.* for information security risks, failure to comply with authorised policies, evidence of breaches *etc.* Leads to the recommendation of improvements to the controls, policies, procedures *etc.* to reduce risks, improve efficiency *etc.*
[Information] Security countermeasures	Controls that are aimed at one or more specific information security threats and vulnerabilities. May involve active defensive techniques (*e.g.* silent alarms), and measures to ensure integrity and availability as well as activities traditionally perceived as information security (*i.e.* achieving confidentiality through access control).
[Information] Security domain	The sets of objects that a subject has the ability to access, which are within a defined (logical and/or physical) security perimeter, or are subject to the same information security policies, procedures *etc.*
[Information] Security exploit	Generally refers to a particular security vulnerability and the corresponding attack method and/or hacking tools that will lead to a compromise. Information on exploits is widely and rapidly circulated amongst the hacker community via Internet newsgroups, EMAIL *etc.*
[Information] Security features, security functions	The security-relevant mechanisms and characteristics of computer hardware and software systems.
[Information] Security incident	An actual or potential breach in security *i.e.* an act or circumstance involving compromise, possible compromise, inadvertent disclosure or other deviation from the security requirements or policies.
[Information] Security kernel	The kernel of an operating system contains core functions and commands which govern all use of the CPU, memory *etc.* In many operating systems, a special 'inner' secure part of the kernel is dedicated to information security functions and commands.

[Information] Security log	Most computer systems can be configured to record details of security-relevant events, such as failed logins, filed file accesses *etc*., in one or more log files. If properly configured and secured, these can provide a valuable audit trail recording what actually happened during an incident, with reliable time stamps providing evidence of the sequence of events.
[Information] Security patch	After software vendors have supposedly solved security vulnerabilities in their products, they typically release the fixes as 'patches' *i.e.* utilities which replace or modify parts of the defective programs. These are generally released quite quickly to reduce the 'window of opportunity' for hackers, but unfortunately, many patches are not so quickly installed and some even introduce further vulnerabilities.
Security perimeter, boundary, domain	The physical and/or logical boundary or limits within which security controls are in effect to protect assets. For example, a collection of networked hosts sharing an encryption system.
[Information] Security requirements	Specification of the types and levels of controls necessary to protect computer equipment, data, information, applications and facilities.
Sendmail	A well-known UNIX EMAIL application program that has been the target of numerous security exploits and patches over the years.
Sensitive	Describes valuable information or other assets requiring protection against unauthorised disclosure, modification/damage or non-availability.
Server	A computer system that provides one or more network services such as disk storage and file transfer, or a program that provides such services. Alternatively, a kind of daemon that performs a remote service for a requester or client normally running on another computer. See also host and hardened server.
SHA (Secure Hash Algorithm)	A commonly-used hash function published by the U.S. government in 1995, which hashes a file into a 160-bit value.
Silent alarm	A security alarm (*e.g.* triggered by an intrusion detection system or duress condition) need not necessarily alert the perpetrator when triggered, lulling them into a false sense of security. Meanwhile, security staff may be quickly despatched to intercept them, or other security countermeasures may be triggered (*e.g.* additional audit logging, transfer of a network session to a honeypot, taking their photograph *etc*.).
Smartcard	Credit-card sized hardware device containing an embedded microprocessor (or other programmable unit), memory and input/output connector, capable of being programmed and storing user data. Normally used for user authentication *etc.* in the form of a secure smartcard.
SMTP (Simple Mail Transfer Protocol)	Simple EMAIL protocol widely used on the Internet. Many information security vulnerabilities have been reported in SMTP server software over the years, and users are advised to install the latest versions and security patches as soon as practicable after release.
Smurf attack	A Denial of Service attack in which an attacker spoofs the source address of an echo-request ICMP (ping) packet to the broadcast address for a network, causing the machines in the network to respond *en masse* to the victim, thereby clogging its network.
[Packet] Sniffer	A device or program that monitors or audits the data on a network. Used legitimately by network operations/support staff to monitor the state of a network *e.g.* for network collisions and overloads, or illegitimately by hackers to capture data (a passive attack). Depending on its sophistication, a packet sniffer may simply save data to disk or send a copy to another network device, or it may selectively filter and decode packets according to rules listing source or destination addresses and/or data content (*e.g.* "capture all packets from 129.223.31.33 containing the text 'Password'").
SNMP (Simple Network Management Protocol)	Protocol used for remote management of network devices. Has numerous information security implications and vulnerabilities, some of which are addressed in an updated version of SNMP called SNMP 2.

Social engineering	The use of techniques such as subterfuge, deception and concealment by an attacker to trick or persuade users, system/network administrators *etc.* to reveal supposedly secret passwords, grant unauthorised systems access *etc.* This method of attack plays directly on what is often the weakest point of any system of information security controls – the human/procedural element.
Software	Computer program/s. Vulnerable to unauthorised access and manipulation, theft, bugs, viruses, worms, inaccurate/incomplete or fraudulent data input *etc.*, hence the need for controls such as logical access restrictions, testing, validation, copyright protection, embedded error-trapping and auditing *etc.*
Spam	Nondescript pink-coloured processed meat product, the subject of a famous Monty Python sketch about blandness.
Spoof, spoofing	Pretending to be someone or something else. The deliberate inducement of a user or a resource to take an incorrect action (permit unauthorised access *etc.)* by masquerading as or impersonating or mimicking an authorised user, system *etc.* See also IP spoof.
SSL (Secure Sockets Layer)	An encryption protocol that provides authentication and confidentiality to applications at the IP communications session layer. Recently updated to SSL2. A client system negotiates and establishes an SSL-encrypted session with a host through a challenge-response process involving the mutual exchange and authentication of digital certificates.
Steganography	System for surreptitiously hiding data within another object or data stream, for instance copyright information may be hidden as a 'digital watermark' (a form of digital fingerprint) within a computer image file without noticeably affecting image quality.
Stream cypher	A type of encryption function that encodes a continuous stream of plaintext sequentially without segmenting it into blocks (see block cipher). Typically used to encrypt network traffic.
Subversion	Surreptitious attack on a system, generally involving fraud and concealment, to undermine the security controls and obtain unauthorised access *e.g.* when an intruder interferes with the operation of an intrusion detector or infiltrates an organisation through social engineering.
SYN flood	Type of TCP/IP Denial of Service attack in which the SYN (synchronise communications) queue is flooded by hackers with spurious calls, such that no new legitimate connections can be opened.
SYSTEM	The default username of the main system management account on VAX VMS systems, the equivalent to ROOT and Administrator. System managers or hackers who have or obtain access to this fully-privileged account can bypass practically any technical security control on the system.
	A B C D E F G H I J K L M N O P Q R S **T** U V W X Y Z
Tamper, tampering	Unauthorised modification of data, system parameters *etc.*, or unauthorised interference with/damage to/disclosure of system hardware, internal operations, peripherals, networking equipment *etc.*
Tamper-resistant	Systems that have been specifically designed to reduce their vulnerability to tampering are said to be tamper-resistant *e.g.* secure smartcards and hardware encryption devices generally incorporate hardened enclosures that trigger the embedded chip to self-destruct if exposed to light.
Tamper-proof	Theoretical state of invulnerability to tampering – unattainable in practice (even well-designed secure smartcards are being compromised in practice by determined hackers using electron microscopes *etc.* to reveal their inner workings).
Target	The object of attack by hackers *etc.* Normally a network system, service, database, password file, credit-card data or similar data resource, sometimes a person (as in social engineering).

TCP (Transmission Control Protocol)	The datacommunications protocol that defines basic data packet structures and procedures *e.g.* the format of packet headers. Part of TCP/IP.
TCP/IP	Originally a precise technical term, this has gradually become a generic name encompassing the complete suite of datacommunications protocols and conventions on which the Internet is based (including, of course, TCP and IP, plus numerous others such as SMTP, URLs, RIP *etc. etc.*).
Technical controls	See automated controls.
Testing	One of the most important computer controls, testing offers the opportunity for an organisation to gain assurance that a system (including its automated and procedural controls) will operate as intended. Well-organised and structured testing regimes ensure reasonably comprehensive coverage in an isolated test environment, separate from development and production environments to avoid compromise, and involve competent testers (including information security experts and/or computer auditors) familiar with topical exploits who test using a risk-based approach (*e.g.* penetration testing).
TFTP (trivial FTP)	Completely insecure form of FTP that lacks even the basic username and password access control.
Threat	A person, system, event or circumstance outside the system under consideration, whose action, if it occurred and acted on a *vulnerability*, would result in an impact (see also risk).
Tiger team	Group of information security experts who test and/or attempt to break the defences of a computer system in an effort to uncover and demonstrate exploitation of vulnerabilities (see also penetration test).
(Date and) Time stamp	Most time-relevant events (*e.g.* entries in security and audit logs) are automatically date-and-time-stamped by the systems. However, these need to be treated with caution as system clocks may be manipulated by privileged users (or hackers who have gained sufficient privilege), unless linked to a secure time source. In a PKI, a trusted master clock may be designated to generate and digitally sign time stamps using public key encryption.
[Security] Token	A portable security device used to authenticate the bearer to another system, typically a smartcard, key or digital certificate. Generally performs a challenge-response function using encryption. Some also incorporate the ability to identify the human bearer (*e.g.* demanding a PIN-code or checking a physical fingerprint) prior to authenticating them.
Traffic analysis	The process of examining statistics and other characteristics relating to data traffic flows to/from the subject's organisation or locations to glean information about their nature or contents *etc.* For example, the systematic use of encryption implies that the subject has something to hide, whilst identifying communications counterparties can indicate accomplices.
Tripwire	A UNIX software auditing tool that generates a database of the byte counts or hash values of files. If the byte counts or hash words have changed between program runs, tripwire will record the change event in a log file and may alert the system security manager. A detective control.
Trojan horse	An apparently useful and/or innocent program containing additional hidden code that subverts the security controls, allowing unauthorised access to data and systems.
Trust	Implicit or explicit belief that someone or something will perform as expected at all times, acting in your best interests. A trusted system, for instance, is treated as if it does not present a security threat, generally because it has been hardened and is operated by trusted staff.

Trusted third party (TTP)	Applies to the situation where an independent organisation (X – typically a bank, government body or similar) has trust relationships with two or more organisations (A, B) that may not directly trust each other to the same degree. If A trusts X, and X trusts B, then A may transact business with B via X, even if it is reluctant to deal directly with B.
Twofish	Reputedly a very strong encryption algorithm, one of the final five candidates short-listed for AES but rejected in favour of Rijndael.
	A B C D E F G H I J K L M N O P Q R S T **U** V W X Y Z
Über hacker	Highly skilled hacker.
UDP (User Datagram Protocol)	Part of the TCP/IP protocol suite, UDP allows for 'connectionless' communications – essentially data broadcasts. As there is no handshaking to confirm receipt of each packet, the connection is fast but is liable to drop packets. Used for Voice-Over-IP and streaming video.
URL (Universal Resource Locator)	Protocol for uniquely naming information resources on the Internet, based on a hierarchical schema.
	A B C D E F G H I J K L M N O P Q R S T U **V** W X Y Z
Valid, validate, validation, invalid …	Valid items pass some test of authentication, truth, completeness, appropriateness, timeliness *etc*. whereas invalid items do not. May apply, for instance, to data within a certain range of values and types (*e.g*. digital certificates are only acceptable between defined start and end dates).
Virus	A program that can "infect" other programs by modifying them to include or distribute a copy of itself. A virus may consume significant system resources and may include a payload. Some viruses are cryptic *i.e*. they use encryption techniques, self-modifying code, variable sequences, normally inaccessible areas of the disk *etc*. in an attempt to evade anti-virus controls.
VPN (Virtual Private Network)	Describes the use of encryption to provide a secure datacommunications route between parties over an insecure or public network, such as the Internet. SSL is commonly used to establish a VPN for secure Internet transactions (*e.g*. submitting credit card details to an eCommerce site).
Vulnerable, vulnerability	Hardware, firmware, software, process or other flaw (an inherent weakness) that leaves a system open for potential exploitation by a threat, causing an impact on the organisation. (See also risk).
	A B C D E F G H I J K L M N O P Q R S T U V **W** X Y Z
WAN (Wide Area Network)	A computer network between locations, typically using links over a public telephone or telecommunications network (*c.f*. LAN). Public networks are vulnerable to various security threats such as interception and redirection of traffic, unplanned service outages *etc*.
Web browser vulnerabilities	Many recent exploits concern security vulnerabilities in common web browsers that can be duped by hackers into loading and executing malicious code (*e.g*. by calling privileged functions within web-integrated office products and databases).
Whistleblower	Someone who discloses an illegal activity (such as a fraud) to management, internal auditors, regulators or even 'the media'. May be protected against retribution by the accused party through confidentiality arrangements, depending on the organisation concerned and/or relevant legislation.
White hats	Figurative term for 'the good guys' - information security professionals who have been explicitly authorised to examine a system's security, often by attempting logical access via public networks (penetration testing) (*c.f*. 'black hats').
Whois	TCP/IP application that interrogates the DNS to identify the registered owner of a domain name and other such information. These days, memorable domain names are valuable assets. Enterprising hackers have been known to compromise the DNS system to hijack other organisations' domain names, sending browsers to their own websites.

W.O.R.M. drive	A data storage device that has been configured to 'Write Once Read Many' *i.e.* once data have been written to the device, they cannot be overwritten or deleted. Can be useful for storing tamper-resistant audit trails and system security logs, if properly configured & secured to prevent their subsequent destruction or removal.
Worm	Independent program that replicates itself from machine to machine across network connections, often clogging networks and information systems as it spreads. Worms mostly use EMAIL *e.g.* the infamous "Morris" and "I Love You" worms that spread widely via Internet EMAIL. See also malware and virus.
	A B C D E F G H I J K L M N O P Q R S T U V W **X** Y Z
X windows	'Universal' graphical interface, common on UNIX systems. Security vulnerabilities in the X windows environment have been exploited by hackers to gain unauthorised access to systems.
	A B C D E F G H I J K L M N O P Q R S T U V W X Y **Z**
Zero-knowledge attack	Penetration testing scenario in which the testers are given no prior knowledge of the target environment but have to establish the facts as part of their tests as if they were members of the general public.

** *End of glossary* **

Sources & references

This is a living hypertext document, edited and generally updated from time to time by Gary.Hinson@CCCL.net Please send me your suggested updates, additions and corrections!

Information in this glossary has been compiled primarily from various public sources on the Internet, including the following useful sources:

· an NSA-sponsored list at www.sans.org/newlook/resources/glossary.htm

· the European Telecommunications Standards Institute (ETSI) Technical Report ETR232 - TC Security - Security Techniques Advisory Group (STAG) glossary of security terminology (which includes numerous formal definitions gleaned from ISO and other published infosec standards)

· the Microsoft security website at www.microsoft.com/security

· Marcus Ranum's FAQ on Firewalls at www.clark.net/pub/mjr/pubs/fwfaq or www.interhack.net/pubs/fwfaq

· The NATO "PKI Working Glossary of Terms" at nra.nacosa.nato.int/pki/hdocs/pkiahwg3.htm

We have also used information from colleagues such as Graeme Jennings, as well as our own material.

Copyright

This glossary is copyright 2000 Corporate Computer Consultants Ltd., all rights reserved. Please refer freely to the maintained public version on-line here at www.cccl.net or contact us for permission to copy and use it off-line.

Contact us

Copyright © 2000 CCCLtd All rights reserved