



Information Security Glossary

March 2003

Access Control

The ability to do something with a computer resource (e.g., read, create, modify or delete a file, execute a program, or use an external connection).

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.

Administration

Tools to help enforce user access security policies.

AES (Advanced Encryption Standard)

A newly developed standard symmetric encryption algorithm aimed to replace DES.

AIS (Automated Information System)

Any equipment of an interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, control, display, transmission, or reception of data and includes software, firmware, and hardware.

Algorithm

A mathematical function used in encryption to increase the difficulty of retrieving the information if not authorised.

Application

A program or system that allows you to process certain types of data.

Antivirus

Antivirus software is a class of program that searches your hard drive and floppy disks for any known or potential viruses. The market for this kind of program has expanded because of Internet growth and the increasing use of the Internet by businesses concerned about protecting their computer assets.

Audit Trail

A technical mechanism that assists the security officer to ensure individual accountability of system users. Users are less likely to attempt to circumvent security policy if they know their name will show up in an audit log.

ATM (Automated teller machine)

A machine that bank customers use to make transactions without a human teller.

Authentication

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done through the use of logon

passwords. Knowledge of the password is assumed to guarantee that the user is authentic. Each user registers initially (or is registered by someone else), using an assigned or self-declared password. On each subsequent use, the user must know and use the previously declared password. The weakness in this system for transactions that are significant (such as the exchange of money) is that passwords can often be stolen, accidentally revealed, or forgotten.

For this reason, Internet business and many other transactions require a more stringent authentication process. The use of digital certificates issued and verified by a Certificate Authority (CA) as part of a public key infrastructure is considered likely to become the standard way to perform authentication on the Internet.

Logically, authentication precedes authorization (although they may often seem to be combined).

Authorization

Authorization is the process of giving someone permission to do or have something. In multi-user computer systems, a system administrator defines for the system which users are allowed access to the system and what privileges of use (such as access to which file directories, hours of access, amount of allocated storage space, and so forth). Assuming that someone has logged in to a computer operating system or application, the system or application may want to identify what resources the user can be given during this session. Thus, authorization is sometimes seen as both the preliminary setting up of permissions by a system administrator and the actual checking of the permission values that have been set up when a user is getting access. Logically, authorization is preceded by authentication.

Backups

Media stored on tapes or diskettes and maintained in an offsite location to be used to restore an automated system in the event of a disaster.

Baseline Security

Method of selecting security measures for implementation within a company based upon measures used in similar companies 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, and also provides confidence in inter-unit/inter-company trading.

The British Standard for Information Security management, BS 7799 (now ISO 1-7799) provides a list of baseline controls which should be implemented in all circumstances, and it is salutary to see how many of these basic principles apply to the smallest of organisations, not just large companies.

Biometrics

Identification of people by measuring some aspect of individual anatomy or physiology (such as hand geometry or fingerprint), some deeply ingrained skill, or other behavioural characteristic (such as handwritten signature), or something that is a combination of the two (such as voice).

BoE

Bank of England

BPO

Business Process Outsourcing

Buffer

A block of memory used by a computer to hold input or submitted data pending 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 providing crucial functions (e.g. programs and data) to them, In terms of Information Security this comprises backups and archiving, stand-in hardware etc.

Business Impact

The consequences to the business (financial, reputation or operational) that could result from a breach in security.

CAGR

Cumulative Annual Growth Rate

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 meaning. Typically, the replacement rule is governed by a secret key.

Content Checking

A process that uses software to read the contents of incoming files, normally e-mail. The content can be scanned for Malicious Code, obscenities and dubious programme files.

Computer System

One or more computers and attached peripherals that may be connected to other computers by a telecommunications network.

Confidentiality

Assurance that sensitive data are kept private and are accessible only by authorized personnel on a need-to-know basis.

CRM

Customer Relationship Management

Cryptography

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

Cyber Liabilities

Cyber Liabilities 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.

Cyber Security

The branch of Security dealing with digital or information technology.

Cyber Terrorism

According to the U.S. Federal Bureau of Investigation, cyber terrorism is any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents."

Unlike a nuisance virus or computer attack that result in a denial of service, a cyber terrorist attack is designed to cause physical violence or extreme financial harm. According to the U.S. Commission of Critical Infrastructure Protection, possible cyber terrorist targets include the banking industry, military installations, power plants, air traffic control centres, and water systems.

Cyber terrorism is sometimes referred to as electronic terrorism or information war.

Decryption

The reverse process of encryption to turn scrambled data back into original form.

Demutualization

The process through which a member-owned company becomes shareholder-owned; frequently this is a step toward the initial public offering (IPO) of a company. Insurance companies often have the word "mutual" in their name, when they are mutually owned by their policy holders as a group. In recent years, however, there has been a strong trend for these companies to demutualize, converting to a shareholder ownership base. Worldwide, stock exchanges have offered another striking example of the trend towards demutualization, as the London Stock Exchange (LSE), New York Stock Exchange (NYSE), Toronto Stock Exchange (TSE) and most other exchanges across the globe have either recently converted, are currently in the process, or are considering demutualization.

Distributed Denial of Service (DDoS)

On the Internet, a distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

A hacker (or, if you prefer, cracker) begins a DDoS attack by exploiting a vulnerability in one computer system and making it the DDoS "master." It is from the master system that the intruder identifies and communicates with other systems that can be compromised. The intruder loads cracking tools available on the Internet on multiple -- sometimes thousands of -- compromised systems. With a single command, the intruder instructs the controlled machines to launch one of many flood attacks against a specified target. The inundation of packets to the target causes a denial of service.

While the press tends to focus on the target of DDoS attacks as the victim, in reality there are many victims in a DDoS attack -- the final target and as well the systems controlled by the intruder.

Demand Side

Financial Services banks, security houses, and insurers that buy Primode's products and services.

Digital Certificate

A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Some digital certificates conform to a standard, X.509. Digital certificates can be kept in registries so that authenticating users can look up other users' public keys.

DMZ (De-Militarised Zone)

An area that exists between 'Trusted' and 'Untrusted' networks to provide additional levels of security whilst enabling external access to information.

E-Business

E-Business (electronic business) derived from such terms as "e-mail" and "e-commerce," is the conduct of business on the Internet, not only buying and selling but also servicing customers and collaborating with business partners.

E-Commerce

E-Commerce (electronic commerce or EC) is the buying and selling of goods and services on the Internet, especially the World Wide Web. In practice, this term and a newer term, e-business, are often used interchangeably. For online retail selling, the term e-tailing is sometimes used.

E-Mail

E-mail (electronic mail) is the exchange of computer-stored messages by telecommunication.

Encryption

Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.

Ecosystem

The global and regional environment comprising any and all entities (private, public, or quasi) firmly in or straddling the IT security and financial services sectors.

EU

European Union

Federal Computer System

The Computer Security Act of 1987 defines a "Federal computer system" as a computer system operated by a Federal agency, by a contractor of a Federal agency, or any other organization that processes information on behalf of the Federal Government to accomplish a Federal function.

Filter

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

File Transfer Protocol (FTP)

FTP enables users to copy files to or from other computers on the Internet.

Financial Services (FS)

The umbrella market segmentation term for banking, insurance, and securities.

Firewall

A firewall is a set of related programs, located at a network gateway server that protects the resources of a private network from users from other networks. (The term also implies the security policy that is used with the programs.) An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users have access to.

Gateway

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

Gramm-Leach-Bliley Act 1999

Requires US financial institutions to ensure that customer data is private and secure.

Hardening

Operating systems contain a vast number of settings, features and options; if these are set incorrectly it can lead to attack and compromise. Hardening the system involves changing setting to help ensure the system is secure.

Hot-fixes

A bug fix that provides a temporary quick fix to a crucial problem.

HR

Human Resources

Hub

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

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 that aims to integrate both to enhance their effectiveness.

Integrity

Safeguarding the accuracy and completeness of information and computer software.

Intranet

A "localized" network of computers used to communicate electronically.

Internet

A global "network of networks" used to communicate electronically that is linked by a common set of protocols. These protocols allow computers from one network to communicate with a computer on another network.

Internet Protocol

The protocol that enables information to be routed from one network to another in packets and then reassembled into information when the packets reach the destination computer.

Internet Control Message Protocol

A protocol used to verify the network is working correctly.

Intrusion Detection

Intrusion detection (ID) is a type of security management system for computers and networks. An ID system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID uses vulnerability assessment (sometimes referred to as scanning), which is a technology developed to assess the security of a computer system or network.

IP

Intellectual Property

IP Address

The network address of a computer system or host.

IPSec

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

IT

Information Technology

IT Security

See Cyber Security

IT Security Hub

Primode's portal of products and services.

Key

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

KPI

Key Performance Indicator

LAN

Local Area Network

Linux

Linux is a UNIX-like operating system that was designed to provide personal computer users a free or very low-cost operating system comparable to traditional and usually more expensive UNIX systems. Linux has a reputation as a very efficient and fast-performing system.

Log File

A file that contains functions and activities performed by the computer.

M&A

Merger and Acquisition

Marco Virus

A computer virus that is embedded within word processing documents or spreadsheet 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 used to either mean a virus, hostile applet or code fragment downloaded from web server or sent directly from one system to another.

Mobile Code

A program downloaded from the internet that runs automatically on a computer with little or no user interaction.

Managed Security Service Provider (MSSP)

Specialist firms providing comprehensive IT security related outsourced or consulting services.

Monitoring Assessment

See Vulnerability Assessment

MOU

Memorandum of Understanding

Network

The physical and logical infrastructure that allows a set of computers to be connected together.

Network Address Translation (NAT)

An internet standard that increases security by enabling a local area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses 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 Level Firewall

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

Network Management

Specialist IT security firms delivering on an outsourcing or consulting basis the management of IT networks.

Network Protocol

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

Network File System (NFS)

A distributed file system that allows a person to work with files on a remote host as though working on the actual host computer.

Offsite Storage

Any place physically located a significant distance away from the main processing environment, such as a locked box at the bank, another office several blocks or miles away from the primary site, or in another State. Magnetic media shall be maintained in a temperature-controlled offsite environment.

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.

Password

A secret string which is known only to the user and the system which the user can enter to prove their identity and thus authenticate themselves to the system.

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 hot fixes. All systems should be patched to the level recommended by the vendors as un-patched systems are likely 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. The practice is sometimes called 'ethical hacking'.

PC

Personal Computer

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 smart card.

PKI

A PKI (public key infrastructure) enables users of a basically un-secure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates. Although the components of a PKI are generally understood, a number of different vendor

approaches and services are emerging. Meanwhile, an Internet standard for PKI is being worked on.

POS

A point-of-sale (POS) terminal is a computerized replacement for a cash register. Much more complex than the cash registers of even just a few years ago, the POS system can include the ability to record and track customer orders, process credit and debit cards, connect to other systems in a network, and manage inventory.

Policy Management

IT Security policy-based management is an administrative approach that is used to simplify the management of a given endeavour by establishing policies to deal with security situations that are likely to occur. Policies are operating rules that can be referred to as a means of maintaining order, security, consistency, or other ways of successfully furthering a goal or mission.

Post Delivery Access Control

See Access Control

Privacy

On the Internet, privacy and associated software products, a major concern of users, can be divided into these concerns:

- What personal information can be shared with whom;
- Whether messages can be exchanged without anyone else seeing them;
- Whether and how one can send messages anonymously.

Protocol

A set of rules for information to be transferred over the network so that your computer will know what to do when it receives the information from another computer.

Provisioning

The process enabling administrators to assign system resources and privileges to users, including employees, contractors and business partners. IT managers may also enforce security policy through provisioning software.

QoS

On the Internet and in other networks, QoS (Quality of Service) is the idea that transmission rates, error rates, and other characteristics can be measured, improved, and, to some extent, guaranteed in advance. QoS is of particular concern for the continuous transmission of high-bandwidth video and multimedia information. Transmitting this kind of content dependably is difficult in public networks using ordinary "best effort" protocols.

ROI

Return on Investment

ROSI

Return on Security Investment

Rulebase

A set of rules which is used by a security device (such as a firewall) to make decisions about what access/traffic to allow and what to block. Also known as the firewall security policy.

Scalability

The ability to expand a computing solution to support large numbers of users without impacting performance.

SCM

Supply Chain Management

Security

A condition that results from the establishment and maintenance of protective measures that ensures a state of inviolability from hostile acts or influences.

Security Awareness

An initiative that sets the stage for training by changing organizational attitudes to realize the importance of security and the adverse consequences of security failure. Further, awareness reminds users of the importance of security and the procedures to be followed.

Security Management

IT security specialist firms such as Symantec offering bundled products and services to retail, corporate, and government.

Sensitive Data

Any information, which through loss, unauthorized access, or modification could adversely affect the national interest, the conduct of Federal programs, or the privacy of individuals (which is protected under the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defence or foreign policy.

SLA

A Service Level Agreement (SLA) is a contract between a customer and the vendor of a system(s) to provide a range of support services, up to an agreed minimum standard. SLAs will usually specify precisely what the support procedures are to be and the way in which a support call will be escalated through the vendor's support organisation to achieve resolution.

Smart Cards

A smart card is a plastic card about the size of a credit card, with an embedded microchip that can be loaded with data, used for telephone calling, electronic cash payments, and other applications, and then periodically refreshed for additional use.

Sniffing

Passive interception and reading network traffic.

SQL

A language to interrogate database systems.

SSL

The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet.

STP

Straight Through Processing (STP) defines business processes in such a way that transactional data is entered only once. Its goal is to eliminate inefficiencies in business processes, such as manual re-keying of data (for example, re-keying a purchase order into a credit verification system) or unnecessary batching of data (such as batching of transactions for periodic processing).

Switch

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

T + 1 (Trade Date Plus One)

The United States Securities and Exchange Commission (SEC) is working with the securities industry to shorten the trade settlement cycle from three days to a maximum of one day through system improvements.

Telnet

A TCP/IP service that allows a user to establish an interactive terminal session with a remote host.

Tokens

A security token (sometimes called an authentication token) is a small hardware device that the owner carries to authorize access to a network service. The device may be in the form of a smart card or may be embedded in a commonly used object such as a key fob.

Trojan Horse

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

User Datagram Protocol

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

Username

A name string that unique identifies an individual user. Normally accompanies 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.

Virus

An unauthorized program that replicates itself and spreads onto various data storage media (diskettes, disks, magnetic tapes, etc.) and/or across a network for malicious intent. The symptoms of virus infection include considerably slower computer response time, inexplicable loss of files, changed modification dates for files, increased file sizes, and total failure of computers.

VPN

A VPN (virtual private network) is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A virtual private network can be

contrasted with an expensive system of owned or leased lines that can only be used by one organization. The goal of a VPN is to provide the organization with the same capabilities, but at a much lower cost.

Vulnerability Assessment

Systematic examination of an AIS or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.