

Glossary of Information Security Terms

The definitions used come from the Common Criteria, Orange Book, and Whatis.com.

A

access—A specific type of interaction between a subject and an object that results in the flow of content from one to the other.

access control—The process of limiting access to the resources of a system only to authorized users, programs, processes or other systems.

access control mechanism—Hardware or software features, operating procedures, management procedures and various combinations of these designed to detect and prevent unauthorized access and to permit authorized access in an automated system.

access list—A list of users, programs and/or processes and the specifications of access categories to which each is assigned.

accountability—The property that enables activities on a system to be traced to individuals who may then be held responsible for their actions.

aggregator—An organization that combines content such as news, sports scores, weather forecasts and reference materials from various sources and makes it available to its customers.

assessment—Surveys and inspections; an analysis of the vulnerabilities of an automated content system. Content acquisition and review process designed to assist a customer to determine how best to use resources to protect content in systems.

assets—Content or resources to be protected by the countermeasures of a system.

assignment—The specification of an identified parameter in a component.

assurance—A measure of confidence that the security features and architecture of an automated information system (AIS) accurately mediate and enforce the security policy.

attack—The act of trying to bypass security controls on a system. An attack may be active, resulting in the alteration of data, or passive, resulting in the release of data. *Note:* The fact that an attack is made does not necessarily mean that it will succeed. The degree of success depends on the vulnerability of the system or activity and the effectiveness of existing countermeasures.

attack potential—The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation.

auditing—Creating a chronological record of the user, the systems, application, and network activities of all transactions.

audit trail—A chronological record of system activities that is sufficient to enable the reconstruction, reviewing and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure or an event in a transaction from its inception to final results.

authenticate—(1) To verify the identity of a user, device or other entity in a computer system, often as a prerequisite to allowing access to resources in a system. (2) To verify the integrity of data that has been stored, transmitted or otherwise exposed to possible unauthorized modification.

authentication data—Content used to verify the claimed identity of a user.

authorization—Determining what access privileges have been granted to a user, group, application or process, and enforcing these privileges.

authorized user—A user who may, in accordance with the system security policy, perform an operation.

automated information system (AIS)—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; includes software, firmware and hardware.

availability—Timely, reliable access to data and content services for authorized users.

availability of data—The state when data is in the place needed by the user, at the time the user needs it, and in the form needed by the user.

B

business continuity planning—Process of developing advance arrangements and procedures that enable an organization to respond to an event in such a manner that critical business functions continue with planned levels of interruption or essential change. Similar terms include contingency planning and disaster recovery planning.

business intelligence (BI)— A broad category of applications and technologies for gathering, storing, analyzing and providing access to data to help enterprise users make better business decisions. BI applications include the activities of decision support systems, query and reporting, online analytical processing (OLAP), statistical analysis, forecasting and data mining.

C

capability—A protected identifier that both identifies the object and specifies the access rights to be allowed to the accessor who possesses the capability. In a capability-based system, access to protected objects such as files is granted if the would-be accessor possesses a capability for the object.

category—A restrictive label that has been applied to classified or unclassified data as a means of increasing the protection of the data and further restricting access to the data.

certification—The comprehensive evaluation of the technical and nontechnical security features of an AIS and other safeguards, made in support of the accreditation process, which establishes the extent to which a particular design and implementation meet a specified set of security requirements.

class—A grouping of families that share a common focus.

Common Criteria (CC)—The name used historically for the multipart standard, ISO/IEC 15408, in lieu of its official ISO (International Standards Organization) name of Evaluation Criteria for Content Technology Security.

component—The smallest selectable set of elements that may be included in a requirement.

compromise—A violation of the security policy of a system such that unauthorized disclosure of sensitive content may have occurred.

computer abuse—The misuse, alteration, disruption or destruction of data processing resources. The key aspect is that it is intentional and improper.

confidentiality—The concept of holding sensitive data in confidence, limited to an appropriate set of individuals or organizations.

configuration control—The process of controlling modifications to the system's hardware, firmware, software and documentation that provides sufficient assurance that the system is protected against the introduction of improper modifications prior to, during and after system implementation.

configuration management—The management of security features and assurances through control of changes made to a system's hardware, software, firmware, documentation, test, test fixtures and test documentation throughout the development and operational life of the system.

content flow control—A procedure to ensure that content transfers within a system are not made from a higher-security-level object to an object of a lower security level.

covert channel—A communications channel that allows two cooperating processes to transfer content in a manner that violates the system's security policy. Synonymous with *confinement channel*.

CRM (customer relationship management)—A content industry term for methodologies, software, and usually Internet capabilities that help an enterprise manage customer relationships in an organized way. For example, an enterprise might build a database about its customers that describes relationships in sufficient detail so that management, salespeople, people providing service and perhaps the customer directly could access content, match customer needs with product plans and offerings, remind customers of service requirements, know what other products a customer had purchased and so forth.

cryptography—The principles, means and methods for rendering content unintelligible, and for restoring encrypted content to intelligible form.

D

data integrity—The property that data meets an a priori expectation of quality—refers to the validity of data.

data mining—Sorting through data to identify patterns and establish relationships. Data mining parameters include

- association—looking for patterns where one event is connected to another event;
- sequence or path analysis—looking for patterns where one event leads to another later event;
- classification—looking for new patterns;
- clustering—finding and visually documenting groups of facts not previously known; and
- forecasting—discovering patterns in data that can lead to reasonable predictions about the future.

data security—The protection of data from unauthorized (accidental or intentional) modification, destruction or disclosure.

decryption—The process by which only the intended recipient of an encrypted message can change the unintelligible message back into a readable content.

denial of service—Any action or series of actions that prevent any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized destruction, modification or delay of service.

digital rights management (DRM)—A system for protecting the copyrights of digital content that is distributed online. It may also include the accounting for paying royalties to the authors of the material.

digital signature—A digital guarantee that a file has not been altered, as if it were carried in an electronically sealed envelope. The “signature” is an encrypted digest (one-way hash function) of the text message, executable or other file. The recipient decrypts the digest that was sent and also recomputes the digest from the received file. If the digests match, the file is proven intact and tamper free from the sender.

disaster recovery—The ability to respond to an interruption in services and to restore an organization’s critical business functions. Measures employed include the prevention, detection or containment of incidents, which if unchecked could result in disaster.

E

element—An indivisible security requirement.

encryption—The process of transforming readable content into a scrambled and unintelligible format so that no one but the intended recipient can decrypt the content.

environment—The aggregate of external procedures, conditions and objects that affect the development, operation and maintenance of a system.

F

fault—A condition that causes a device or system component to fail to perform in a required manner.

file protection—The aggregate of all processes and procedures in a system designed to inhibit unauthorized access, contamination or elimination of a file.

file security—The means by which access to computer files is limited to authorized users only.

firewall— A system or combination of systems that enforces a boundary between two or more networks. Gateway that limits access between networks in accordance with local security policy. The typical firewall is an inexpensive micro-based Unix box kept clean of critical data, with many modems and public network ports on it, but just one carefully watched connection back to the rest of the cluster.

formal development methodology—A collection of languages and tools that enforces a rigorous method of verification. This methodology uses the Ina Jo specification language for successive stages of system development, including identification and modeling of requirements, high-level design and program design.

formal security policy model—A mathematically precise statement of a security policy. To be adequately precise, such a model must represent the initial state of a system, the way in which the system progresses from one state to another and a definition of a “secure” state of the system. To be acceptable as a basis for a system, the model must be supported by a formal proof that if the initial state of the system satisfies the definition of a “secure” state and if all assumptions required by the model hold, then all future states of the system will be secure. Some formal modeling techniques include state transition models, denotational semantics models and algebraic specification models.

FTP (file transfer protocol)—A standard Internet protocol and the simplest way to exchange files between computers on the Internet. Like the hypertext transfer protocol (HTTP), which transfers displayable Web pages and related files, and the simple mail transfer protocol (SMTP), which transfers e-mail, FTP is an application protocol that uses the Internet’s TCP/IP protocols. FTP is commonly used to transfer Web page files from their creator to the computer that acts as their server for everyone on the Internet. It’s also commonly used to download programs and other files to your computer from other servers.

H

HTTP (hypertext transfer protocol)—The set of rules for exchanging files (text, graphic images, sound, video and other multimedia files) on the World Wide Web. Relative to the TCP/IP suite of protocols (which are the basis for content exchange on the Internet), HTTP is an application protocol.

I

IDX (Internet Data Exchange)—NAR-created voluntary data display policy.

impersonating—Synonymous with *spoofing*.

infostructure—

integrity—Providing assurance of the correctness of the content.

intellectual property—Property that derives from the work of the mind or intellect. Specifically, an idea, invention, trade secret, process, program, data, formula, patent, copyright or trademark or application, right or registration relating thereto.

M

malicious code—Hardware, software, or firmware that is intentionally included in a system for an unauthorized purpose; e.g., a Trojan horse.

metric—A standard of measurement.

MISMO (Mortgage Industry Standards Maintenance Organization)—Established by the Mortgage Bankers Association of America (MBA) to coordinate the development and maintenance of Internet-based extensible markup language (XML) real estate finance specifications.

N

nonrepudiation—Ensuring that no party involved in a transaction(s) can deny their involvement in the transaction(s).

O

object—A passive entity that contains or receives content. Access to an object potentially implies access to the content it contains. Examples of objects are records, blocks, pages, segments, files, directories, directory trees and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers and network nodes.

object reuse—The reassignment and reuse of a storage medium (e.g., page frame, disk sector, magnetic tape) that once contained one or more objects. To be securely reused and assigned to a new subject, storage media must contain no residual data (magnetic reminisce) from the object(s) previously contained in the media.

Orange Book—Alternate name for the Department of Defense's Trusted Computer Security Evaluation Criteria.

overt channel—A path within a computer system or network that is designed for the authorized transfer of data. Compare *covert channel*.

P

password—A protected/private character string used to authenticate an identity.

penetration—The successful act of bypassing the security mechanisms of a system.

personnel security—The procedures established to ensure that all personnel who have access to sensitive content have the required authority as well as appropriate clearances.

physical security—The application of physical barriers and control procedures as preventive measures or countermeasures against threats to resources and sensitive content.

PKI (public-key infrastructure)—The set of standards and services that enable the use of public-key cryptography, certificates and certificate authorities in a distributed environment.

privilege—The principle that requires that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error or unauthorized use.

protocols—A set of rules and formats, semantic and syntactic, that permits entities to exchange content.

R

read—A fundamental operation that results only in the flow of content from an object to a subject.

read access—Permission to read content.

recovery procedures—The actions necessary to restore a system's computational capability and data files after a system failure.

reliability—The probability of a given system performing its mission adequately for a specified period of time under the expected operating conditions.

residue—Data left in storage after processing operations are complete, but before degaussing or rewriting has taken place.

RETS (real estate transaction standard)—The open standard for exchanging real estate transaction content. Consisting of a transaction specification and a standard extensible markup language (XML) document type definition (DTD).

risk—The probability that a particular threat will exploit a particular vulnerability of the system.

risk analysis—The process of identifying security risks, determining their magnitude and identifying areas needing safeguards. Risk analysis is a part of risk management. Synonymous with *risk assessment*.

risk management—The total process of identifying, controlling and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost-benefit analysis, selection, implementation and test, security evaluation of safeguards and overall security review.

S

security-critical mechanisms—Those security mechanisms whose correct operation is necessary to ensure that the security policy is enforced.

security evaluation—An evaluation done to assess the degree of trust that can be placed in systems for the secure handling of sensitive content. One type, a product evaluation, is an evaluation performed on the hardware and software features and assurances of a computer product from a perspective that excludes the application environment. The other type, a system evaluation, is done for the purpose of assessing a system's security safeguards with respect to a specific operational mission and is a major step in the certification and accreditation process.

security features—The security-relevant functions, mechanisms and characteristics of system hardware and software. Security features are a subset of system security safeguards.

security flaw—An error of commission or omission in a system that may allow protection mechanisms to be bypassed.

security policy—The set of laws, rules and practices that regulates how an organization manages, protects and distributes sensitive content.

security requirements—The types and levels of protection necessary for equipment, data, content, applications and facilities to meet security policy.

security requirements baseline—A description of minimum requirements necessary for a system to maintain an acceptable level of security.

security test and evaluation—An examination and analysis of the security safeguards of a system as they have been applied in an operational environment to determine the security posture of the system.

sensitive content—Any content, the loss, misuse, modification of or unauthorized access to, could affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U.S. Code, but that has not been specifically authorized under criteria established by an executive order or

an act of Congress to be kept classified in the interest of national defense or foreign policy.

sensitivity label—A piece of content that represents the security level of an object. Sensitivity labels are used by the system as the basis for mandatory access control decisions.

SOAP (standard object access protocol)—A way for a program running in one kind of operating system (such as Windows 2000) to communicate with a program in the same or another kind of an operating system (such as Linux) by using the World Wide Web's hypertext transfer protocol (HTTP) and its extensible markup language (XML) as the mechanisms for content exchange.

software security—General purpose (executive, utility or software development tools) and applications programs or routines that protect data handled by a system.

software system test and evaluation process—A process that plans, develops and documents the quantitative demonstration of the fulfillment of all baseline functional performance, operational and interface requirements.

spoofing—An attempt to gain access to a system by posing as an authorized user. Synonymous with *impersonating* and *masquerading*.

subject—An active entity, generally in the form of a person, process or device, that causes content to flow among objects or changes the system state. Technically, a process/domain pair.

system integrity—The quality that a system has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

T

tampering—An unauthorized modification that alters the proper functioning of equipment or a system in a manner that degrades the security or functionality it provides.

technical attack—An attack that can be perpetrated by circumventing or nullifying hardware and software protection mechanisms, rather than by subverting system personnel or other users.

technical vulnerability—A hardware, firmware, communication or software flaw that leaves a computer processing system open for potential exploitation, either externally or internally, thereby resulting in risk for the owner, user or manager of the system.

threat—Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure or modification of data and/or denial of service.

threat agent—A method used to exploit a vulnerability in a system, operation or facility.

threat analysis—The examination of all actions and events that might adversely affect a system or operation.

trusted computer system—A system that employs sufficient hardware and software assurance measures to allow its use for simultaneous processing of a range of sensitive or classified content.

U

unforgeable authentication—Authentication that cannot be copied or forged by reconstructing or generating content from a legitimate source.

user—Person or process accessing a system either by direct connections (i.e., via terminals) or indirect connections (i.e., prepare input data or receive output that is not reviewed for content or classification by a responsible individual).

user ID—A unique symbol or character string that is used by a system to identify a specific user.

user profile—Patterns of a user's activity that can be used to detect changes in normal routines.

V

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.

VOW (virtual office Web site)—Literally an online real estate office. VOWs can display real-time listings straight from the MLS database.

W

Web services—Services (usually including some combination of programming and data, but possibly including human resources as well) that are made available from a business's Web server for Web users or other Web-connected programs. Providers of Web services are generally known as application service providers. Web services range from such major services as storage management and customer relationship management (CRM) down to much more limited services such as the furnishing of a stock quote and the checking of bids for an auction item.

X

XML (extensible markup language)—A formal recommendation from the World Wide Web Consortium (W3C) that is similar to the language of today's Web pages, the hypertext markup language (HTML). Both XML and HTML contain markup symbols to describe the contents of a page or file. HTML, however, describes the content of a Web page (mainly text and graphic images) only in terms of how it is to be displayed and interacted with. For example, the letter "p" placed within markup tags starts a new

paragraph. XML describes the content in terms of what data is being described. For example, the word “phonenum” placed within markup tags could indicate that the data that followed was a phone number. This means that an XML file can be processed purely as data by a program or it can be stored with similar data on another computer or that, like an HTML file, it can be displayed. For example, depending on how the application in the receiving computer wanted to handle the phone number, it could be stored, displayed or dialed.

