APPENDIX L
GLOSSARY

William Stallings

Copyright 2014
Supplement to
Computer Security, Third Edition
Pearson 2014
http://williamstallings.com/ComputerSecurity

access control The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities.

access control list (ACL) A discretionary access control technique organized by object. For each object, an ACL lists users and their permitted access rights.

access matrix A matrix whose two dimensions are subjects and objects. Each cell in the matrix lists the access permissions of that subject for that object.

access right Describes the way in which a subject may access an object.

active attack An attempt to alter system resources or affect their operation.

adversary An entity that attacks, or is a threat to, a system.

anomaly detection Involves the collection of data relating to the behavior of legitimate users over a period of time. Then statistical tests are applied to observed behavior to determine with a high level of confidence whether that behavior is not legitimate user behavior.

asset A major application, general support system, high impact program, physical plant, mission critical system, or a logically related group of systems.

assurance The degree of confidence one has that the security measures, both technical and operational, work as intended to protect the system and the information it processes.

asymmetric encryption A form of cryptosystem in which encryption and decryption are performed using two different keys, one of which is referred to as the public key and one of which is referred to as the private key. Also known as public-key encryption.

attack A threat that is carried out (threat action) and, if successful, leads to an undesirable violation of security

audit Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

authentication Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

authenticator Additional information appended to a message to enable the receiver to verify that the message should be accepted as authentic. The authenticator may be functionally independent of the content of the message itself (e.g., a nonce or a source identifier) or it may be a function of the message contents (e.g., a hash value or a cryptographic checksum).

authenticity The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.

availability The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them.

backdoor Any mechanisms that bypasses a normal security check; it may allow unauthorized access to functionality.

bacteria Program that consumes system resources by replicating itself.

base-rate fallacy Occurs when there is an attempt to detect a phenomenon that occurs rarely. The frequency of occurrence is referred to as the base rate. When the base rate is very low, it is difficult to achieve low levels of both false positives and false negatives.

biometric A physical or behavioral characteristic of a human being.

block chaining A procedure used during symmetric block encryption that makes an output block dependent not only on the current plaintext input block and key, but also on earlier input and/or output. The effect of block chaining is that two instances of the same plaintext input block will produce different ciphertext blocks, making cryptanalysis more difficult.

block cipher A symmetric encryption algorithm in which a block of plaintext bits (typically 64 or 128) is transformed as a whole into a ciphertext block of the same length.

brute force attack A cryptanalysis technique or other kind of attack method involving an exhaustive procedure that tries all possibilities, one-by-one.

buffer overflow A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Attackers exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system.

capability ticket A discretionary access control technique organized by subject. For each subject, the capability ticket lists objects and their permitted access rights by this subject.

certificate authority A trusted entity that issues and revokes public key certificates.

challenge-response An authentication process that verifies an identity by requiring correct authentication information to be provided in response to a challenge. In a computer system, the authentication information is usually a value that is required to be computed in response to an unpredictable challenge value.

cipher An algorithm for encryption and decryption. A cipher replaces a piece of information (an element in plaintext) with another object, with the intent to conceal meaning. Typically, the replacement rule is governed by a secret key.

ciphertext The output of an encryption algorithm; the encrypted form of a message or data.

closed access control policy Only accesses that are specifically authorized are allowed.

collision resistant A property of a hash function such that it is computationally infeasible to find any pair (x, y) such that H(x) = H(y). Also referred to as strong collision resistant.

confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

copyright Protects the tangible or fixed expression of an idea, not the idea itself.

corruption An attack on system integrity. Malicious software in this context could operate in such a way that system resources or services function in an unintended manner. Or a user could gain unauthorized access to a system and modify some of its functions.

countermeasure Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system.

covert channel A communications channel that enables the transfer of information in a way unintended by the designers of the communications facility.

cryptanalysis The branch of cryptology dealing with the breaking of a cipher to recover information, or forging encrypted information that will be accepted as authentic.

cryptographic checksum An authenticator that is a cryptographic function of both the data to be authenticated and a secret key. Also referred to as a message authentication code (MAC).

cryptography The branch of cryptology dealing with the design of algorithms for encryption and decryption, intended to ensure the secrecy and/or authenticity of messages.

cryptology The study of secure communications, which encompasses both cryptography and cryptanalysis.

data confidentiality The property that information is not made available or disclosed to unauthorized individuals, entities, or processes

data integrity The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.

database A collection of interrelated data, often with controlled redundancy, organized to serve multiple applications. The data are stored so that they can be used by different programs without concern for the internal data structure or organization.

database management system (DBMS) A suite of programs for constructing and maintaining a database and for offering ad hoc query facilities to multiple users and applications.

decryption The translation of encrypted text or data (called ciphertext) into original text or data (called plaintext). Also called deciphering.

denial of service The prevention of authorized access to resources or the delaying of time-critical operations.

digital signature An authentication mechanism that enables the creator of a message to attach a code that acts as a signature. The signature is formed by taking the hash of the message and encrypting the message with the creator's private key. The signature guarantees the source and integrity of the message.

discretionary access control An access control service that enforces a security policy based on the identity of system entities and their authorizations to access system resources. This service is termed "discretionary" because an entity might have access rights that permit the entity, by its own volition, to enable another entity to access some resource.

disruption A threat to availability or system integrity.

elliptic curve cryptography A cryptographic technique based on the use of a mathematical construct known as the elliptic curve.

encryption The conversion of plaintext or data into unintelligible form by means of a reversible translation, based on a translation table or algorithm. Also called enciphering.

evaluation The process of examining a computer product or system with respect to certain criteria.

exposure Can be deliberate, as when an insider intentionally releases sensitive information, such as credit card numbers, to an outsider. It can also be the result of a human, hardware, or software error, which results in an entity gaining unauthorized knowledge of sensitive data.

false positive In the context of intrusion detection, an authorized user identified as an intruder.

false negative In the context of intrusion detection, intruders identified as an authorized user.

falsification The altering or replacing of valid data or the introduction of false data into a file or database.

firewall A dedicated computer that interfaces with computers outside a network and has special security precautions built into it in order to protect sensitive files on computers within the network. It is used to service outside network, especially Internet, connections and dial-in lines.

hash function A function that maps a variable-length data block or message into a fixed-length value called a hash code. The function is designed in such a way that, when protected, it provides an authenticator to the data or message. Also referred to as a message digest or one-way hash function.

hashed password A hash value of a password stored in place of the password in a password file.

honeypot A decoy system designed to lure a potential attacker away from critical systems. A form of intrusion detection.

identification The means by which a user provides a claimed identity to the system.

identity management A centralized, automated approach to provide enterprise-wide access to resources by employees and other authorized individuals.

incapacitation An attack on system availability. This could occur as a result of physical destruction of or damage to system hardware. More typically, malicious software, such as Trojan horses, viruses, or worms, could operate in such a way as to disable a system or some of its services.

inference A threat action whereby an unauthorized entity indirectly accesses sensitive data by reasoning from characteristics or byproducts of data to which the entity does have access.

inline sensor An intrusion detection sensor inserted into a network segment so that the traffic that it is monitoring must pass through the sensor.

inside attack An attack initiated by an entity inside the security perimeter (an "insider"). The insider is authorized to access system resources but uses them in a way not approved by those who granted the authorization.

integrity A term that covers the related concepts of data integrity and system integrity.

interception A threat action whereby an unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations.

intruder An individual who gains, or attempts to gain, unauthorized access to a computer system or to gain unauthorized privileges on that system.

intrusion A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system (or system resource) without having authorization to do so.

intrusion detection system A set of automated tools designed to detect unauthorized access to a host system.

intrusion prevention system A set of automated tools designed to prevent unauthorized access to a host system.

key distribution center A system that is authorized to transmit temporary session keys to principals. Each session key is transmitted in encrypted form, using a master key that the key distribution center shares with the target principal.

key exchange A procedure whereby two communicating parties can cooperate to acquire a shared secret key.

least privilege This is the principle that access control should be implemented so that each system entity is granted the minimum system resources and authorizations that the entity needs to do its work. This principle tends to limit damage that can be caused by an accident, error, or fraudulent or unauthorized act.

logic bomb Logic embedded in a computer program that checks for a certain set of conditions to be present on the system. When these conditions are met, it executes some function resulting in unauthorized actions.

logical security Protects computer-based data from software-based and communication-based threats.

malicious software Software that exploits vulnerabilities in computing system to create an attack. Also called *malware*.

mandatory access control A means of restricting access to objects based on fixed security attributes assigned to users and to files and other objects. The controls are mandatory in the sense that they cannot be modified by users or their programs.

masquerade A type of attack in which one system entity illegitimately poses as (assumes the identity of) another entity.

master key A long-lasting key that is used between a key distribution center and a principal for the purpose of encoding the transmission of session keys. Typically, the master keys are distributed by noncryptographic means. Also referred to as a key-encrypting key.

memory card A plastic card that can store but not process data. The most common such card is the bank card with a magnetic stripe on the back.

message authentication A process used to verify the integrity of a message.

message authentication code (MAC) An authenticator that is a cryptographic function of both the data to be authenticated and a secret key. Also referred to as a cryptographic checksum.

message digest see *hash function*.

misappropriation A threat action whereby an entity assumes unauthorized logical or physical control of a system resource.

misuse A threat action that causes a system component to perform a function or service that is detrimental to system security.

mode of operation A technique for enhancing the effect of a cryptographic algorithm or adapting the algorithm for an application, such as applying a block cipher to a sequence of data blocks or a data stream.

multilevel security A capability that enforces access control across multiple levels of classification of data.

non-repudiation Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.

object In the context of access control, a resource to which access is controlled.

obstruction A threat action that interrupts delivery of system services by hindering system operations.

one-way hash function Same as secure hash function.

one-way function A function that is easily computed, but the calculation of its inverse is infeasible.

OSI security architecture A management-oriented security standard that focuses on the OSI model and on networking and communications aspects of security.

outside attack An attack initiated by an entity outside the security perimeter (an "outsider").

passive attack An attempt to learn or make use of information from the system that does not affect system resources.

passive sensor An intrusion detection sensor that monitors a copy of network traffic; the actual traffic does not pass through the device.

password A secret data value, usually a character string, that is used as authentication information. A password is usually matched with a user identifier that is explicitly presented in the authentication process, but in some cases the identity may be implicit.

patent The grant of a property right to the inventor of an invention.

permission Same as access right.

physical security Protects the information systems that house data and the people who use, operate, and maintain the systems. Physical security also must prevent any type of physical access or intrusion that can compromise logical security. Also called *infrastructure security*.

plaintext The input to an encryption function or the output of a decryption function.

preimage resistant A property of a hash function such that for any given code h, it is computationally infeasible to find x such that $H(x) = h$.

premises security Protects the people and property within an entire area, facility, or building(s), and is usually required by laws, regulations, and fiduciary obligations. Premises security provides perimeter security, access control, smoke and fire detection, fire suppression, some environmental protection, and usually surveillance systems, alarms, and guards.

privacy Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

private key One of the two keys used in an asymmetric encryption system. For secure communication, the private key should only be known to its creator.

pseudorandom number generator A function that deterministically produces a sequence of numbers that are apparently statistically random.

public key One of the two keys used in an asymmetric encryption system. The public key is made public, to be used in conjunction with a corresponding private key.

public-key certificate Consists of a public key plus a User ID of the key owner, with the whole block signed by a trusted third party. Typically, the third party is a certificate authority (CA) that is trusted by the user community, such as a government agency or a financial institution.

public-key encryption Asymmetric encryption.

public-key infrastructure (PKI) The set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography.

query language Provides a uniform interface to the database for users and applications.

relational database A database organized as a set of tables (relations). A table is a collection of rows or records and each row in a table contains the same fields. Certain fields may be designated as keys, which means that searches for specific values of that field will use indexing to speed them up. Keys also provide a way of linking one table to another.

replay An attack in which a service already authorized and completed is forged by another, duplicate request in an attempt to repeat authorized commands.

repudiation Denial by one of the entities involved in a communication of having participated in all or part of the communication.

risk An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

role-based access control Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.

rootkit Set of hacker tools used after attacker has broken into a computer system and gained root-level access.

salt A random value that is concatenated with a password before applying the one-way encryption function used to protect passwords that are stored in the database of an access control system.

second preimage resistant A property of a hash function such that For any given block x, it is computationally infeasible to find $y \neq x$ with $H(y) = H(x)$. Also referred to as weak collision resistant.

secret key The key used in a symmetric encryption system. Both participants must share the same key, and this key must remain secret to protect the communication.

secure hash function A hash function with certain additional security properties to make it suitable for use as a primitive in various information security applications, such as authentication and message integrity.

security attack see *attack*

security audit An independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures. The basic audit objective is to establish accountability for system entities that initiate or participate in security-relevant events and actions. Thus, means are needed to generate and record a security audit trail and to review and analyze the audit trail to discover and investigate attacks and security compromises. Also known as a *security log*.

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

security mechanism A mechanism that is designed to detect, prevent, or recover from a security attack.

security policy A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

security service A service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

separation of duty The practice of dividing the steps in a system function among different individuals, so as to keep a single individual from subverting the process.

session key A temporary encryption key used between two principals.

signature detection Involves an attempt to define a set of rules or attack patterns that can be used to decide that a given behavior is that of an intruder.

smart card A plastic card that can store and process data.

static biometric A biometric that is captured without a time component, such as a fingerprint, retina, or face.

statistical database A database that provides data of a statistical nature, such as counts and averages.

stream cipher A symmetric encryption algorithm in which ciphertext output is produced bit-by-bit or byte-by-byte from a stream of plaintext input.

subject In the context of access control, an entity capable of accessing objects.

symmetric encryption A form of cryptosystem in which encryption and decryption are performed using the same key. Also known as conventional encryption.

system integrity Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

system resource see *asset*

threat A potential security harm to an asset.

token An item possessed by an individual and used for authentication. Examples include electronic keycards, smart cards, and physical keys.

trademark A word, name, symbol, or device that is used in trade with goods to indicate the source of the goods and to distinguish them from the goods of others.

traffic analysis Inference of information from observable characteristics of data flow(s), even when the data is encrypted or otherwise not directly available. Such characteristics include the identities and locations of the source(s) and destination(s), and the presence, amount, frequency, and duration of occurrence.

Trojan horse A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

trusted system A computer and operating system that can be verified to implement a given security policy.

unauthorized disclosure An event involving the exposure of information to entities not authorized access to the information.

user authentication The process of verifying an identity claimed by or for a system entity.

usurpation: A circumstance or event that results in control of system services or functions by an unauthorized entity.

verification Presenting or generating authentication information that corroborates the binding between an entity and an identifier**.**

virtual private network Consists of a set of computers that interconnect by means of a relatively unsecure network and that make use of encryption and special protocols to provide security.

virus Code embedded within a program that causes a copy of itself to be inserted in one or more other programs. In addition to propagation, the virus usually performs some unwanted function.

vulnerability Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

worm Program that can replicate itself and send copies from computer to computer across network connections. Upon arrival, the worm may be activated to replicate and propagate again. In addition to propagation, the worm usually performs some unwanted function.

zombie A program that secretly takes over another Internet-attached computer and then uses that computer to launch attacks that are difficult to trace to the zombie's creator.