



## Brief glossary excerpt of terms used in security knowledge areas

### A

#### **Advanced Encryption Standard (AES)**

An encryption standard being developed by NIST. Intended to specify an unclassified, publicly-disclosed, symmetric encryption algorithm.

#### **Asymmetric Cryptography**

Public-key cryptography; A modern branch of cryptography in which the algorithms employ a pair of keys (a public key and a private key) and use a different component of the pair for different steps of the algorithm.

#### **Asymmetric Warfare**

Asymmetric warfare is the fact that a small investment, properly leveraged, can yield incredible results.

#### **Auditing**

Auditing is the information gathering and analysis of assets to ensure such things as policy compliance and security from vulnerabilities.

#### **Authentication**

Authentication is the process of confirming the correctness of the claimed identity.

#### **Authenticity**

Authenticity is the validity and conformance of the original information.

#### **Authorization**

Authorization is the approval, permission, or empowerment for someone or something to do something.

#### **Availability**

Availability is the need to ensure that the business purpose of the system can be met and that it is accessible to those who need to use it.



## Brief glossary excerpt of terms used in security knowledge areas

### **B**

#### **Basic Authentication**

Basic Authentication is the simplest web-based authentication scheme that works by sending the username and password with each request.

#### **Bit**

The smallest unit of information storage; a contraction of the term "binary digit;" one of two symbols "0" (zero) and "1" (one) - that are used to represent binary numbers.

#### **Block Cipher**

A block cipher encrypts one block of data at a time.

#### **Byte**

A fundamental unit of computer storage; the smallest addressable unit in a computer's architecture. Usually holds one character of information and usually means eight bits.

### **C**

#### **Chain of Custody**

Chain of Custody is the important application of the Federal rules of evidence and its handling.

#### **Checksum**

A value that is computed by a function that is dependent on the contents of a data object and is stored or transmitted together with the object, for the purpose of detecting changes in the data.

#### **Cipher**

A cryptographic algorithm for encryption and decryption.

#### **Ciphertext**

Ciphertext is the encrypted form of the message being sent.



## Brief glossary excerpt of terms used in security knowledge areas

### **Circuit Switched Network**

A circuit switched network is where a single continuous physical circuit connected two endpoints where the route was immutable once set up.

### **Client**

A system entity that requests and uses a service provided by another system entity, called a "server." In some cases, the server may itself be a client of some other server.

### **Competitive Intelligence**

Competitive Intelligence is espionage using legal, or at least not obviously illegal, means.

### **Confidentiality**

Confidentiality is the need to ensure that information is disclosed only to those who are authorized to view it.

### **Corruption**

A threat action that undesirably alters system operation by adversely modifying system functions or data.

### **Cost Benefit Analysis**

A cost benefit analysis compares the cost of implementing countermeasures with the value of the reduced risk.

### **Countermeasure**

Reactive methods used to prevent an exploit from successfully occurring once a threat has been detected. Intrusion Prevention Systems (IPS) commonly employ countermeasures to prevent intruders from gaining further access to a computer network. Other counter measures are patches, access control lists and malware filters.

### **Cryptographic Algorithm or Hash**

An algorithm that employs the science of cryptography, including encryption algorithms, cryptographic hash algorithms, digital signature algorithms, and key agreement algorithms.



## Brief glossary excerpt of terms used in security knowledge areas

### **Cyclic Redundancy Check (CRC)**

Sometimes called "cyclic redundancy code." A type of checksum algorithm that is not a cryptographic hash but is used to implement data integrity service where accidental changes to data are expected.

### **D**

#### **Data Custodian**

A Data Custodian is the entity currently using or manipulating the data, and therefore, temporarily taking responsibility for the data.

#### **Data Encryption Standard (DES)**

A widely-used method of data encryption using a private (secret) key. There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used. For each given message, the key is chosen at random from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key.

#### **Data Mining**

Data Mining is a technique used to analyze existing information, usually with the intention of pursuing new avenues to pursue business.

#### **Data Owner**

A Data Owner is the entity having responsibility and authority for the data.

#### **Decapsulation**

Decapsulation is the process of stripping off one layer's headers and passing the rest of the packet up to the next higher layer on the protocol stack.

#### **Decryption**

Decryption is the process of transforming an encrypted message into its original plaintext.

#### **Diffie-Hellman**

A key agreement algorithm published in 1976 by Whitfield Diffie and Martin Hellman. Diffie-Hellman does key establishment, not encryption. However, the



## Brief glossary excerpt of terms used in security knowledge areas

key that it produces may be used for encryption, for further key management operations, or for any other cryptography.

### **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. 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.

### **Digital Envelope**

A digital envelope is an encrypted message with the encrypted session key.

### **Digital Signature**

A digital signature is a hash of a message that uniquely identifies the sender of the message and proves the message hasn't changed since transmission.

### **Digital Signature Algorithm (DSA)**

An asymmetric cryptographic algorithm that produces a digital signature in the form of a pair of large numbers. The signature is computed using rules and parameters such that the identity of the signer and the integrity of the signed data can be verified.

### **Due Care**

Due care ensures that a minimal level of protection is in place in accordance with the best practice in the industry.

### **Due Diligence**

Due diligence is the requirement that organizations must develop and deploy a protection plan to prevent fraud, abuse, and additional deploy a means to detect them if they occur.

## **E**

### **Eavesdropping**

Eavesdropping is simply listening to a private conversation which may reveal information which can provide access to a facility or network.



## Brief glossary excerpt of terms used in security knowledge areas

### **Encapsulation**

The inclusion of one data structure within another structure so that the first data structure is hidden for the time being.

### **Encryption**

Cryptographic transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used.

### **Exposure**

A threat action whereby sensitive data is directly released to an unauthorized entity.

### **F**

### **Fragment Offset**

The fragment offset field tells the sender where a particular fragment falls in relation to other fragments in the original larger packet.

### **Fragmentation**

The process of storing a data file in several "chunks" or fragments rather than in a single contiguous sequence of bits in one place on the storage medium.

### **Frames**

Data that is transmitted between network points as a unit complete with addressing and necessary protocol control information. A frame is usually transmitted serial bit by bit and contains a header field and a trailer field that "frame" the data. (Some control frames contain no data.)

### **Full Duplex**

A type of duplex communications channel which carries data in both directions at once. Refers to the transmission of data in two directions simultaneously. Communications in which both sender and receiver can send at the same time.



## Brief glossary excerpt of terms used in security knowledge areas

### H

#### **Hardening**

Hardening is the process of identifying and fixing vulnerabilities on a system.

#### **Hash Function**

An algorithm that computes a value based on a data object thereby mapping the data object to a smaller data object.

#### **Hash Functions**

(cryptographic) hash functions are used to generate a one way "check sum" for a larger text, which is not trivially reversed. The result of this hash function can be used to validate if a larger file has been altered, without having to compare the larger files to each other. Frequently used hash functions are MD5 and SHA1.

#### **Header**

A header is the extra information in a packet that is needed for the protocol stack to process the packet.

### I

#### **Identity**

Identity is whom someone or what something is, for example, the name by which something is known.

#### **Incident**

An incident as an adverse network event in an information system or network or the threat of the occurrence of such an event.

#### **Incident Handling**

Incident Handling is an action plan for dealing with intrusions, cyber-theft, denial of service, fire, floods, and other security-related events. It is comprised of a six step process: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.



## Brief glossary excerpt of terms used in security knowledge areas

### **Information Warfare**

Information Warfare is the competition between offensive and defensive players over information resources.

### **Integrity**

Integrity is the need to ensure that information has not been changed accidentally or deliberately, and that it is accurate and complete.

### **Internet Standard**

A specification, approved by the IESG and published as an RFC, that is stable and well-understood, is technically competent, has multiple, independent, and interoperable implementations with substantial operational experience, enjoys significant public support, and is recognizably useful in some or all parts of the Internet.

### **ISO**

International Organization for Standardization, a voluntary, non-treaty, non-government organization, established in 1947, with voting members that are designated standards bodies of participating nations and non-voting observer organizations.

### **Issue-Specific Policy**

An Issue-Specific Policy is intended to address specific needs within an organization, such as a password policy.

### **ITU-T**

International Telecommunications Union, Telecommunication Standardization Sector (formerly "CCITT"), a United Nations treaty organization that is composed mainly of postal, telephone, and telegraph authorities of the member countries and that publishes standards called "Recommendations."

### **J**

#### **Jitter**

Jitter or Noise is the modification of fields in a database while preserving the aggregate characteristics of that make the database useful in the first place.



## Brief glossary excerpt of terms used in security knowledge areas

### L

#### **Log Clipping**

Log clipping is the selective removal of log entries from a system log to hide a compromise.

### M

#### **Md5**

A one way cryptographic hash function. Also see "hash functions" and "sha1"

#### **Measures of Effectiveness (MOE)**

Measures of Effectiveness is a probability model based on engineering concepts that allows one to approximate the impact a give action will have on an environment. In Information warfare it is the ability to attack or defend within an Internet environment.

### N

#### **National Institute of Standards and Technology (NIST)**

National Institute of Standards and Technology, a unit of the US Commerce Department. Formerly known as the National Bureau of Standards, NIST promotes and maintains measurement standards. It also has active programs for encouraging and assisting industry and science to develop and use these standards.

#### **Non-Repudiation**

Non-repudiation is the ability for a system to prove that a specific user and only that specific user sent a message and that it hasn't been modified.

### O

#### **Octet**

A sequence of eight bits. An octet is an eight-bit byte.



## Brief glossary excerpt of terms used in security knowledge areas

### **One-Way Encryption**

Irreversible transformation of plaintext to cipher text, such that the plaintext cannot be recovered from the cipher text by other than exhaustive procedures even if the cryptographic key is known.

### **One-Way Function**

A (mathematical) function,  $f$ , which is easy to compute the output based on a given input. However given only the output value it is impossible (except for a brute force attack) to figure out what the input value is.

### **OSI**

OSI (Open Systems Interconnection) is a standard description or "reference model" for how messages should be transmitted between any two points in a telecommunication network. Its purpose is to guide product implementers so that their products will consistently work with other products. The reference model defines seven layers of functions that take place at each end of a communication. Although OSI is not always strictly adhered to in terms of keeping related functions together in a well-defined layer, many if not most products involved in telecommunication make an attempt to describe themselves in relation to the OSI model. It is also valuable as a single reference view of communication that furnishes everyone a common ground for education and discussion.

### **P**

#### **Packet**

A piece of a message transmitted over a packet-switching network. One of the key features of a packet is that it contains the destination address in addition to the data. In IP networks, packets are often called datagrams.

#### **Packet Switched Network**

A packet switched network is where individual packets each follow their own paths through the network from one endpoint to another.

#### **Patch**

A patch is a small update released by a software manufacturer to fix bugs in existing programs.



## Brief glossary excerpt of terms used in security knowledge areas

### **Patching**

Patching is the process of updating software to a different version.

### **Payload**

Payload is the actual application data a packet contains.

### **Plaintext**

Ordinary readable text before being encrypted into ciphertext or after being decrypted.

### **Possession**

Possession is the holding, control, and ability to use information.

### **Program Policy**

A program policy is a high-level policy that sets the overall tone of an organization's security approach.

### **Proprietary Information**

Proprietary information is that information unique to a company and its ability to compete, such as customer lists, technical data, product costs, and trade secrets.

### **Protocol**

A formal specification for communicating; an IP address the special set of rules that end points in a telecommunication connection use when they communicate. Protocols exist at several levels in a telecommunication connection.

### **Protocol Stacks (OSI)**

A set of network protocol layers that work together.

### **Public Key**

The publicly-disclosed component of a pair of cryptographic keys used for asymmetric cryptography.



## Brief glossary excerpt of terms used in security knowledge areas

### **Public Key Encryption**

The popular synonym for "asymmetric cryptography".

### **Public Key Infrastructure (PKI)**

A PKI (public key infrastructure) enables users of a basically unsecured 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.

### **Public-Key Forward Secrecy (PFS)**

For a key agreement protocol based on asymmetric cryptography, the property that ensures that a session key derived from a set of long-term public and private keys will not be compromised if one of the private keys is compromised in the future.

## **R**

### **Radiation Monitoring**

Radiation monitoring is the process of receiving images, data, or audio from an unprotected source by listening to radiation signals.

### **Request for Comment (RFC)**

A series of notes about the Internet, started in 1969 (when the Internet was the ARPANET). An Internet Document can be submitted to the IETF by anyone, but the IETF decides if the document becomes an RFC. Eventually, if it gains enough interest, it may evolve into an Internet standard.

### **Response**

A response is information sent that is responding to some stimulus.

### **Risk**

Risk is the product of the level of threat with the level of vulnerability. It establishes the likelihood of a successful attack.



## Brief glossary excerpt of terms used in security knowledge areas

### **Risk Assessment**

A Risk Assessment is the process by which risks are identified and the impact of those risks determined.

### **Risk Averse**

Avoiding risk even if this leads to the loss of opportunity. For example, using a (more expensive) phone call vs. sending an e-mail in order to avoid risks associated with e-mail may be considered "Risk Averse"

### **Rivest-Shamir-Adleman (RSA)**

An algorithm for asymmetric cryptography, invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman.

## **S**

### **S/Key**

A security mechanism that uses a cryptographic hash function to generate a sequence of 64-bit, one-time passwords for remote user login. The client generates a one-time password by applying the MD4 cryptographic hash function multiple times to the user's secret key. For each successive authentication of the user, the number of hash applications is reduced by one.

### **Safety**

Safety is the need to ensure that the people involved with the company, including employees, customers, and visitors, are protected from harm.

### **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.

### **Sensitive Information**

Sensitive information, as defined by the federal government, is any unclassified information that, if compromised, could adversely affect the national interest or conduct of federal initiatives.



## Brief glossary excerpt of terms used in security knowledge areas

### **Session**

A session is a virtual connection between two hosts by which network traffic is passed.

### **Session Key**

In the context of symmetric encryption, a key that is temporary or is used for a relatively short period of time. Usually, a session key is used for a defined period of communication between two computers, such as for the duration of a single connection or transaction set, or the key is used in an application that protects relatively large amounts of data and, therefore, needs to be re-keyed frequently.

### **SHA1**

A one way cryptographic hash function. Also see "MD5"

### **Stream Cipher**

A stream cipher works by encryption a message a single bit, byte, or computer word at a time.

### **Symmetric Cryptography**

A branch of cryptography involving algorithms that use the same key for two different steps of the algorithm (such as encryption and decryption, or signature creation and signature verification). Symmetric cryptography is sometimes called "secret-key cryptography" (versus public-key cryptography) because the entities that share the key.

### **Symmetric Key**

A cryptographic key that is used in a symmetric cryptographic algorithm.

## **T**

### **Tamper**

To deliberately alter a system's logic, data, or control information to cause the system to perform unauthorized functions or services.



## Brief glossary excerpt of terms used in security knowledge areas

### **Threat**

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

### **Threat Assessment**

A threat assessment is the identification of types of threats that an organization might be exposed to.

### **Threat Model**

A threat model is used to describe a given threat and the harm it could do a system if it has a vulnerability.

### **Threat Vector**

The method a threat uses to get to the target.

### **Triple DES**

A block cipher, based on DES, that transforms each 64-bit plaintext block by applying the Data Encryption Algorithm three successive times, using either two or three different keys, for an effective key length of 112 or 168 bits.

### **U**

A person, organization entity, or automated process that accesses a system, whether authorized to do so or not.

### **User Contingency Plan**

User contingency plan is the alternative methods of continuing business operations if IT systems are unavailable.

### **V**

Vulnerability

A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.



## Brief glossary excerpt of terms used in security knowledge areas

### W

#### **War Chalking**

War chalking is marking areas, usually on sidewalks with chalk, that receive wireless signals that can be accessed.

#### **War Driving**

War driving is the process of traveling around looking for wireless access point signals that can be used to get network access.

#### **Wired Equivalent Privacy (WEP)**

A security protocol for wireless local area networks defined in the standard IEEE 802.11b.

#### **Wiretapping**

Monitoring and recording data that is flowing between two points in a communication system.

#### **Wrap**

To use cryptography to provide data confidentiality service for a data object

---

#### **Document reference**

<http://www.sans.org/resources/glossary.php>