Security Services

The following is a list of terms that is defined for the Security Infrastructure Working Group. It has only basic terms, plus those terms with controversial or multiple meanings. For a more complete glossary of security terms, see Network Security by Charlie Kaufmann, Radia Perlman & Mike Speciner; Computer Security Basics by Deborah Russell & G. T. Gabgemi Sr; or The Directory, CCITT Recommendations of the X.500 Series, 89/267

Basic Concepts

1 *AAA*: Overall term for security. The three A's are generally taken to be Authentication, Authorization, and Auditing although it may mean Authentication, Authorization & Accounting in some contexts.
2 *Authentication*: The process of reliably determining the identity of a communicating party. There are three classic ways of authenticating oneself: something you know, something you have and something you are. The two entities involved in the communication could use the following two ways to authenticate themselves.
    - Single entity authentication. Only one of the entities is authenticated by the other. It could be either data origin or data recipient authentication.
    - Mutual authentication. Both the parties authenticate each other.
3 *Authorization*: The granting of rights to a user, program or process. Permission to access a resource. It is used to protect a resource from unauthorized use. This can be achieved by the use of access control lists (ACL) or capabilities.
4 *Auditing*: Keep a record of events that might have some significance, such as when access to resources occurred. To record independently and later examine system activity. Audit data is generally used for security concerns (e.g. intrusion detection and consistency checks).
5 *Accounting*: Keep a record of events that might have some significance, such as when access to resources occurred, who accessed it, what was accessed and for how long. Accounting data is generally used for commercial concerns (e.g. billing and charges).

Security Service Attributes

1. *Anonymity*: The ability to communicate so that the other principal can't find out the identity of the sender.
2. *Integrity*: Keeping information from corruption or unauthorized modification either maliciously or accidentally. Integrity protects against forgery or tampering.
3. *Non-Repudiation*: There is proof who sent a message that a recipient can show to a third party and the third party can independently verify the source.
4. *Privacy (Confidentiality)*: Protection from the unauthorized disclosure of data.

Encryption Concepts

1. *Encryption*: To scramble information so that only someone knowing the appropriate secret can obtain the original information.
2. *Public Key*: Dual key (RSA/PGP style) cryptography. Uses two different keys, either one for encryption and the other for decryption. Also called a asymmetric cryptography.
3. *Secret Key*: Single key cryptography. Also called symmetric cryptography.
4. *Session Key*: A short lived Secret Key used by two principals for the purpose of secure communications between them.

Authorization Concepts

ACL: Access Control List. A list of the subjects authorized to access that object. The list usually indicates what type of access is allowed for each user.

Groups: A named set of users, created for convenience in stating authorization policy.

Roles: A specific function a principal plays with respect to another principal. Examples include a system administrator of a individual computer system, and a bank teller at a particular bank. If a principal has multiple functions with respect to another principal, it has multiple roles (e.g. A person can have both the bank teller role and the customer role at a particular bank).

Capability: An identifier that specifies an object and the access rights for the subject who possess the capability. See also "Certificate / Ticket / Token"

Proxy Agent: A principal that has been authorized to work on the behalf of another.

Proxy: A token that grants the rights of a principal to another.

Restricted Proxy: A token that grants the rights of a principal to another while placing restrictions on the privileges granted.

Certificate / Ticket / Token: Different names for a object used to grant privileges. While these terms have individual meanings in specific contexts (Kerberos generates tickets, physical objects are tokens), there is no general agreement on how they differ. We will use Certificate / Ticket / Token largely interchangeably. Capability & Proxy are related terms, but with narrower focus.

CRL: Certificate Revocation List. A list of revoked certificates.

Miscellaneous

Denial of Service: An action that prevents a system or its resources from functioning efficiently and reliably.

S.No	Services	HTTP/1.1	SSL (V2)	SSL (V3)	LDAP (X.509)
1.	Authentication				
	• Client only	Yes	Yes	Yes	--
	• Mutual	--	--	Yes	--
2.	Authorization				
	• ACL	--	--	--	--
	• Capability	--	--	--	Yes
3.	Non-repudiation	--	--	--	--
4.	Integrity	--	Yes	Yes	--
5.	Confidentiality	--	Yes	Yes	--
6.	Administration				
	• Certificate Mgmt.	--	--	--	Yes