The different security principles and there terminology are as below

1. Confidentiality: The confidentiality principle means that only the sender and the intended recipient should be able to access the message. Confidentiality is not achieved if an unauthorized person is able to access a message.
2. Authentication: The authentication principle help to establish proof of identities. The authentication process makes sure sure that the sender of a electronic message or document is correctly identified.
3. Integrity: The integrity principle protects data against active threats like those that may alter it.
4. Non-repudation: The principle of non-repudation prevents either sender or receiver from denying a transmitted message. Therefore, whenever a message is send by the sender, the receiver can prove that the message was sent by that the sender. When a message is received, the sender can prove that the message was received by the receiver.
5. Access control: The principle of access control means the ability to limit and control the access to host systems and applications through communication links. To achieve this, a user attempting to access must first be identified, or authenticated.
6. Availability: The principle of availability means that system resources must be available to authorized entities at all times.

Related posts:

1. Types of Attack
2. Security threats
3. Computer and cyber security
4. Introduction to network security
5. Intrusion detection tool

6. Categories of security assessments
7. Intoduction to intrusion
8. Intrusion detection tool
9. Categories of security assessments
10. Intrusion terminology
11. Cryptography attacks
12. Cryptography
13. SSH
14. MD5
15. Message digest functions
16. Digital signature
17. Authentication Functions
18. One way hash function
19. Hash function in network web security
20. Digital signature standard
21. SSL Secure socket layer