Network security

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Encryption algorithms:

Encryption algorithms are commonly used in computer communications, including FTP transfers. Usually they are used to provide secure transfers. If an algorithm is used in a transfer, the file is first translated into a seemingly meaningless cipher text and then transferred in this configuration; the receiving computer uses a key to translate the cipher into its original form. So if the message or file is intercepted before it reaches the receiving computer it is in an unusable (or encrypted) form.

Here are some commonly used algorithms:

DES/3DES or TripleDES

This is an encryption algorithm called Data Encryption Standard that was first used by the U.S. Government in the late 70's. It is commonly used in ATM machines (to encrypt PINs) and is utilized in UNIX password encryption. Triple DES or 3DES has replaced the older versions as a more secure method of encryption, as it encrypts data three times and uses a different key for at least one of the versions.

Blowfish

Blowfish is a symmetric block cipher that is unpatented and free to use. It was developed by Bruce Schneier and introduced in 1993.

AES

Advanced Encryption Standard or Rijndael; it uses the Rijndael block cipher approved by the National Institute of Standards and Technology (NIST). AES was originated by cryptographers Joan Daemen and Vincent Rijmen and replaced DES as the U.S. Government encryption technique in 2000.

Twofish

Twofish is a block cipher designed by Counterpane Labs. It was one of the five Advanced Encryption Standard (AES) finalists and is unpatented and open source.

IDEA

This encryption algorithm was used in Pretty Good Privacy (PGP) Version 2 and is an optional algorithm in Open PGP. IDEA features 64 bit blocks with a 128 bit key.

MD5

MD5 was developed by Professor Ronald Riverst and was used to create digital signatures. It is a one way hash function and intended for 32 bit machines. It replaced the MD4 algorithm.

SHA 1

SHA 1 is a hashing algorithm similar to MD5, yet SHA 1 may replace MD5 since it offers more security

HMAC

This is a hashing method similar to MD5 and SHA 1, sometimes referred to as HMAC MD5 and HMAC SHA1.

RSA Security

- **RC4** RC4 is a variable key size stream cipher based on the use of a random permutation.
- **RC5** This is a parameterized algorithm with a variable block, key size and number of rounds.
- **RC6** This an evolution of RC5, it is also a parameterized algorithm that has variable block, key and a number of rounds. This algorithm has integer multiplication and 4 bit working registers