

4.2 Data Security Technologies And Standards

4.2.1 Encryption

Encryption is the transformation of data into a form unreadable by anyone without a confidential decryption key. Its purpose is to ensure privacy by keeping the information unusable from anyone for whom it is not intended, even those who can see the encrypted data. For example, one may wish to encrypt files on a hard disk to prevent an intruder from reading them.

4.2.2 Data Encryption Standard (DES)

Data Encryption Standard (DES) is an encryption block cipher defined and endorsed by the U.S. government in 1977 as an official standard. It is also the most well-known and widely used cryptosystem in the world.

DES is a secret-key, symmetric encryption system. When used for communication, both sender and receiver must know the same secret key, which is used both to encrypt and decrypt the message. DES can also be used for single-user encryption, such as to store files on a hard disk in an encrypted form. In a multi-user environment, the secure key distribution may be difficult. It was designed to be implemented in hardware, and therefore its operation is relatively fast. It also works well for bulk encryption such as for encrypting a large set of data.

4.2.3 C2 Security

The requirements for a C2 secure system were articulated by the U.S. Department of Defense's National Computer Security Center (NCSC) in the publication *Trusted Computer System Evaluation Criteria*. Some of the most important requirements of C2-level secure system are:

1. The owner of a resource (such as a file) must be able to control access to the resource.
2. The operating system must protect data stored in memory for one process so that it is not randomly reused by other processes.
3. Each user must uniquely identify himself or herself. The system must be able to use the unique identification to track the activities of the user.
4. System Administrators must be able to audit security-related events and the actions of individual users. Access to this audit data must be limited to authorized administrators.
5. The system must protect itself from external interference or tampering, such as modification of the running system or of system files stored on disk.