Solved Question Paper

December 2008

5)Describe the following and also explain their usage[10*2]

x. TFTP

TFTP stands for Trivial File Transfer Protocol.

The TFTP is a minimal protocol for transferring files without authentication. In TFTP, there is no separation of control information and data as in FTP. Therefore TFTP must not be used on computer where sensitive/confidential information is stored. TFTP is frequently used by devices without permanent storage for copying an initial memory image from a remote server when the devices are powered on. Due to the lack of security features, the use of TFTP is generally restricted.

TFTP uses the unreliable transport protocol UDP(User Datagram Protocol) for data transport, whereas FTP uses TCP(Transmission Control Protocol). Each TFTP message is carried in a separate UDP datagram. The first two bytes of a TFTP message specify the type of a message, which can be a request to download a file, request to upload a file, a data message, or an acknowledgement or error message. A TFTP session is initiated when a TFTP client sends a request to upload or download a file from an ephemeral UDP port to the (well-known) UDP port 69 of a TFTP server. When the request is received the TFTP server picks an ephemeral UDP port of its own and uses this port to communicate with the TFTP client. Thus, both client and server communicate using ephemeral ports.

Since UDP does not recover lost or corrupted data, TFTP is responsible for maintaining the integrity of the data exchange. TFTP transfers data in blocks of 512 bytes. Each block is assigned a 2-byte long sequence number and is transmitted in a separate UDP datagram. A block must be acknowledged before the next block can be sent. When an acknowledgment is not received before a timer expires, the block is retransmitted.

vii. Goals of computer security

The goals of computer security are :

1. Integrity
2. Confidentiality
3. Availability

Integrity : it deals with the knowledge that data has not been modified. Data integrity is related to data accuracy, but integrity and accuracy are not the same. For example, if information is entered incorrectly, it will remain incorrect. Integrity means preventing unauthorised modification. To preserve the integrity of an item means that the item is unmodified, precise, accurate, modified in a acceptable way by authorised people, or consistent.

2. Confidentiality :

It means preventing unauthorised access. It ensures that only the authorised person accesses the computer system. Only some data in the computer falls in the category of confidential data. There is data that can be made public and there is data that is considered sensitive. It is this critical or sensitive data that will require confidentiality. Data confidentiality cannot be enforced unless data integrity is present. The following items could require data confidentiality : credit card files, medical records, personnel data, mission-critical data, and R&D data etc.

3. Availability :

A computer system is available if :

- The response time is acceptable
- There is a fair allocation of resources

- Fault tolerance exists
- It is user friendly
- Concurrency control and deadlock management exists.

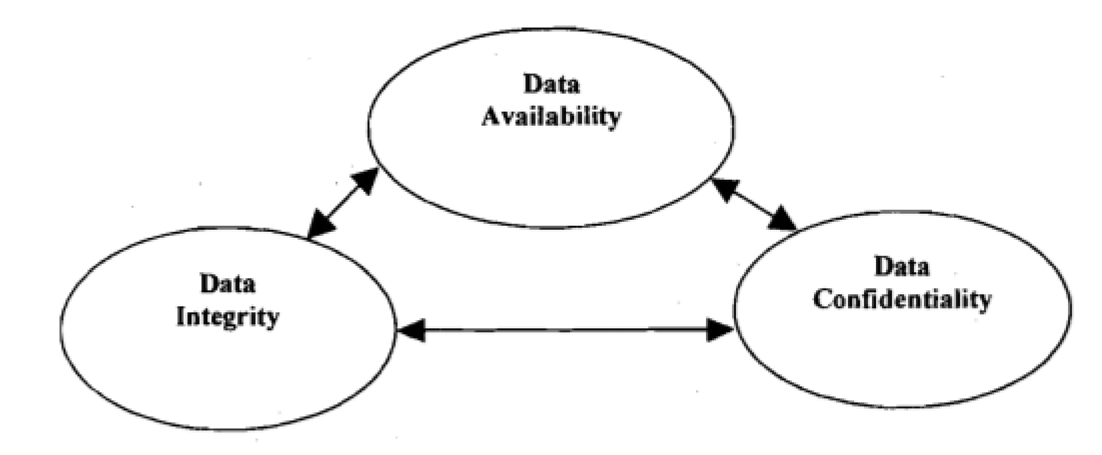

Figure 1: Relationship between Confidentiality, Integrity, and Availability