M.Sc. IV Sem. (Mathematics)

Paper 2nd - Fundamentals of Computer Science - II

Unit V

Reference Book : **C. Ritchie, *Operating Systems incorporating UNIX and Windows,* BPB Publications, New Delhi.**

Topic : Distributed Systems

A distributed system is a computer system in which the resources reside in separate unit connected by a network, but which presents the user a uniform computing environment. Distributed systems address the difficulties that arise in operating a network which consists of a number of systems with diverse hardware platform, operating system and communication system software and protocols.

Following are the distributed system architectures :

1. **CORBA (OMG)**
2. **DCE (OSF)**
3. **DCOM (Microsoft)**
4. **DSOM (IBM)**
5. **DAIS (ICL)**

1. **CORBA :** CORBA is an acronym for Common Object Request Broker Architecture. This architecture is developed by Object Manager Group (OMG). CORBA provides a peer-to-peer communication infra-structure in which applications are viewed as 'objects'.

2. **DCE :** DCE is an acronym for Distributed Computing Environment. DCE is developed by Open Source Foundation (OSF), which is an organization of several companies including IBM and Hewlett Packard (HP) and so on. DCE

provides services and tools that support the creation, use and maintenance of distributed applications in a heterogeneous computing environment.

3. **DCOM :** DCOM is an acronym for Distributed Common Object Model. It is developed by Microsoft. COM handles interprocess communication within application running on the same computer whereas DCOM is an extended architecture that enables communication between separate machines connected by a network.

4. **DSOM :** DSOM is an acronym for Distributed System Object Model. It is developed by IBM. SOM is a CORBA – Compliant Object Request Broker and hence supports the communication of client and server object across a network independent of languages and other system features whereas DSOM extends this interoperability to remote system.

5. **DAIS :** DAIS is an acronym for Distributed Application Integration System. It is developed by ICL. DAIS is already in use in practical applications.

Security :

The term security refers to all aspects of protecting a computer system from all hazards such as physical damage, loss or corruption of data, loss of confidentiality. The related term integrity is used to refer specifically to maintain the correctness of the data stored.

The effects of the danger facing a computer system can be placed in four categories :

1. **Loss or damage to data :** Loss, corruption, modification or invalid addition to stored data.
2. **Loss of confidentiality :** Access to data by unauthorized person breaching privacy and confidentiality and probably resulting in losses.
3. **Loss of availability of hardware :** This may results in consequential losses to the organization.

4. **Loss of or corruption to software :** This may results in consequential losses to the organization.

Specific threats and their possible consequences are summarized in the following table :

Types of Threats	Example	Effect
Physical Threats	Fire, flood, machine faults etc.	Loss of availability of machine or data.
Accidental Error	Programmer error, user error or operator error.	Corruption of data.
Malicious Misuse	Viruses, worms, Trojan horses etc.	Corruption of data and software. Loss of availability of hardware.
Fraudulent Misuse	Deliberate modification of data or software	Financial loss.
Unauthorized Access	Accessing of confidential data, for example, competitive, commercial data, military data.	Specific to circumstances.

Accidental Error :

Virtually every one working with computers has suffered some accidents resulting in the loss of all or part of a file, or a program. Some accidents are more serious and more public than others. In a recent incident, a major bank ran a program accidently twice which debited monthly standing amounts from its customers' accounts. This was discovered when customers complained to the bank.

Viruses :

A virus is a small program which can invade a computer system by attaching itself to a legitimate program. It can also propagate by creating copies of itself which can

attached to other program. In addition to its reproductive activity, each virus will have some malicious effect.

Worms :

A worm is a variation on the theme of the viruses instead of attaching itself to another program. A worm is an independent process which spans copies of itself. The effect of this is clog up a system with spurious execution of these processes preventing legitimate processes from running properly. Worms are usually associated with propagation through network systems.

Trojan Horse :

A Trojan Horse is a program which ostensibly and eventually performs some useful legitimate function but which also performs some other undesirable activity. A Trojan Horse can be created by subtle modification of a normal program such as a compiler or text editor. When such a modified program is executed, a trojan horse code can perform any invasive, destructive or mischievous activity.

Security Techniques :

1. **Procedural Guards**
2. **Operating System Facilities**
3. **Encryption**
4. **File Access Control**

1. Procedural Guards :

We include in this category any procedures operated by the system administration or by users themselves which reduce the level of security risk. This includes :

a) Access restrictions to system hardware.
b) Program modification control.
c) Backup and Archiving

From the above three, we study the last one.

Backup and Archiving : Backup systems are possibly the most fundamental technique for guarding against loss or corruption of data when all else fails. The ability to recover the data from some earlier point of time provides a general safety net which has saved many systems from disaster. Backups are usually carried out by using a system utility program such as MS-DOS, Backup.exe and Restore.exe. A common procedure is to create backups of files at daily intervals, using a compact disk, hard disk and so on.

2. Operating System Facilities :

The operating system can significantly contribute to the security of resources of a computer. This can be done with the help of password. The characteristics of good password system are characterized below :

- The system should require a password of atleast six characters.
- The system should log all password attempts so that warning of the efforts of an attempted hacker are produced.
- The system should only permitted limited number of attempts on a particular terminal. This places a time obstacle on the persistent hacker.
- Password should be changed every so often in case one has been discovered.
- User should give password which are not easily guessed, but are easy to remember.

3. Encryption :

Encryption is the conversion of data in some intelligible format into unintelligible format to prevent the data from being understood if read by an unauthorized party. A reverse operation called decryption converts the encrypted data back into its original form.

4. File Access Control :

Since the data held within the file system is the principal interest of the computer security system so we must give permission code for each file to prevent data. For example, the permission code which give read access to all user is r, the permission code which gives write access to all user is w, the permission code which give read and write access to all user is rw.