SUGGESTED SOLUTION

CA INTERMEDIATE NOV'19

SUBJECT- EIS

Test Code – CIM 8290

BRANCH - () (Date :)

Answer 1:
(A)

Operating System protection can be achieved using following steps.

- **Automated terminal identification:** This will help to ensure that a specified session could only be initiated from a certain location or computer terminal.

- **Terminal log-in procedures:** A log-in procedure is the first line of defence against unauthorized access as it does not provide unnecessary help or information, which could be misused by an intruder. When the user initiates the log-on process by entering user-id and password, the system compares the ID and password to a database of valid users and accordingly authorizes the log-in.

- **Access Token:** If the log on attempt is successful, the Operating System creates an access token that contains key information about the user including user-id, password, user group and privileges granted to the user. The information in the access token is used to approve all actions attempted by the user during the session.

- **Access Control List:** This list contains information that defines the access privileges for all valid users of the resource. When a user attempts to access a resource, the system compasses his or her user-id and privileges contained in the access token with those contained in the access control list. If there is a match, the user is granted access.

- **Discretionary Access Control:** The system administrator usually determines; who is granted access to specific resources and maintains the access control list. However, in distributed systems, resources may be controlled by the end-user. Resource owners in this setting may be granted discretionary access control, which allows them to grant access privileges to other users.

- **User identification and authentication:** The users must be identified and authenticated in a fool-proof manner. Depending on risk assessment, more stringent methods like Biometric Authentication or Cryptographic means like Digital Certificates should be employed.

- **Password management system:** An operating system could enforce selection of good passwords. Internal storage of password should use one-way hashing algorithms and the password file should not be accessible to users.

- **Use of system utilities:** System utilities are the programs that help to manage critical functions of the operating system e.g. addition or deletion of users. This utility should not be accessible to a general user. Use and access to these utilities should be strictly controlled and logged.

- **Duress alarm to safeguard users:** If users are forced to execute some instruction under threat, the system should provide a means to alert the authorities.

- **Terminal time out:** Log out the user if the terminal is inactive for a defined period. This will prevent misuse in absence of the legitimate user.

- **Limitation of connection time:** Define the available time slot. Do not allow any transaction beyond this time.

(5 marks)

(B)

Detective controls:

- Are designed to detect errors, omissions or malicious acts that occur and report the occurrence.

- Ex: Hash totals, CCTV, Review of Audit logs, BRS.   **(1 mark)**

Characteristics of Detective Controls

- Clear understanding of lawful activities so that anything which deviates from these is reported as unlawful, malicious, etc.

- An established mechanism to refer the reported unlawful activities to the appropriate person or group

- Interaction with the preventive control to prevent such acts from occurring **(1.5 marks)**

Corrective controls

- Are designed to **reduce the impact** or **correct an error** once it has been detected.
- Ex: Cleaning a file detected to contain virus, data backups, stand by server, failover networks etc. (Business continuity plan)   **(1 mark)**

Characteristics of Corrective Controls

- Minimize the impact of the threat
- Correct error arising from a problem
- Feedback from preventive and detective controls
- Modify the processing systems to minimize future occurrences of the problem.

                                                                              (1.5 marks)

Answer 2:

(A)

- ♦ **Data Diddling:** This involves the change of data before or after they entered the system. A limited technical knowledge is required to data diddle and the worst part with this is that it occurs before computer security can protect the data.
- ♦ **Bomb:** Bomb is a piece of bad code deliberately planted by an insider or supplier of a program. An event, which is logical, triggers a bomb or time based. The bombs explode when the conditions of explosion get fulfilled causing the damage immediately. However, these programs cannot infect other programs. Since, these programs do not circulate by infecting other programs; chances of a widespread epidemic are relatively low.
- ♦ **Christmas Card:** It is a well-known example of Trojan and was detected on internal E-mail of IBM system. On typing the word 'Christmas', it will draw the Christmas tree as expected, but in addition, it will send copies of similar output to all other users connected to the network. Because of this message on other terminals, other users cannot save their half-finished work.
- ♦ **Worm:** A worm does not require a host program like a Trojan to relocate itself. Thus, a Worm program copies itself to another machine on the network. Since, worms are stand-alone programs, and they can be detected easily in comparison to Trojans and computer viruses. Examples of worms are Existential Worm, Alarm clock Worm etc. The Alarm Clock worm places wake-up calls on a list of users. It passes through the network to an outgoing terminal while the sole purpose of existential worm is to remain alive.

Existential worm does not cause damage to the system, but only copies itself to several places in a computer network.

♦ **Rounding Down:** This refers to rounding of small fractions of a denomination and transferring these small fractions into an authorized account. As the amount is small, it gets rarely noticed.

♦ **Salami Techniques:** This involves slicing of small amounts of money from a computerized transaction or account. A Salami technique is slightly different from a rounding technique in the sense a fix amount is deducted. For example, in the rounding off technique, Rs. 21,23,456.39 becomes Rs. 21,23,456.40, while in the Salami technique the transaction amount Rs. 21,23,456.39 is truncated to either Rs. 21,23,456.30 or Rs.21,23,456.00, depending on the logic.

♦ **Trap Doors:** Trap doors allow insertion of specific logic, such as program interrupts that permit a review of data. They also permit insertion of unauthorized logic.

♦ **Spoofing:** A spoofing attack involves forging one's source address. One machine is used to impersonate the other in spoofing technique. Spoofing occurs only after a particular machine has been identified as vulnerable. A penetrator makes the user think that s/he is interacting with the operating system. For example, a penetrator duplicates the login procedure, captures the user's password, attempts for a system crash and makes user login again.

(B)

IS Audit is defined as the process of attesting following objectives;

- **Asset Safeguarding Objectives:** The information system assets (hardware, software, data information etc.) must be protected by a system of internal controls from unauthorized access.

- **Maintenance of Privacy:** Audit of Information Systems ensures that data collected in a business process are adequately guarded and their privacy is maintained.

- **System Effectiveness Objectives:** Audit of Information Systems ensures effectiveness of a system is continuously evaluated by auditing the characteristics and objective of the system to ascertain that it meets substantial user requirements.

- **System Efficiency Objectives:** Control and Audit of Information Systems are required to optimize the use of various information system resources.

(5 marks)

Answer 3:

(A)

(i)   Cache Memory:
- Cache can be used in order to **bridge the speed differences** between Registers and Primary memory (RAM).

- It is a **smaller, faster memory**, which stores copies of the data from the most frequently used main memory locations so that Processor / Registers can access it more rapidly than it's access from main memory.   **(1 mark)**

(ii)   Random Access Memory (RAM):
- This is **Read Write memory**.

- Information can be **read as well as modified** (i.e. write).

- **Volatile** in nature means Information is lost as soon as power is turned off.

- RAM is an **expandable memory** i.e. we can expand the size of RAM.

(1 mark)

(iii) **Read Only Memory (ROM):**

- This is **non-volatile** in nature (content remains even in absence of power).

- Information **can be read, not modified**.

- Generally used by manufacturers to store data & Programmes like startup program and configuration of computer.

- ROM is provided by manufacturer on motherboard and generally it is **not expandable** memory. **(1 mark)**

(iv) **Virtual Memory:**

- Virtual Memory is not an actual Memory, it's an imaginary memory. It is a memory technique which helps to execute big size programs with small size available RAM.

- If a computer lacks the RAM needed to run a Program or operation, Windows uses virtual memory to compensate.

- Virtual memory combines computer's RAM with **temporary space on the hard disk**. When RAM runs low, virtual memory moves data from RAM to a space called a paging file or segmentation on hard disk.

- Moving data to and from the paging file frees up RAM to complete its work.

- Thus, Virtual memory is an **allocation of hard disk space** to help RAM.

(2 marks)

(B)

(Students can write any FIVE points)

Major advantages are as follows:
a) **Permitting data sharing:** One of the advantages is that the same information can be made available to different users. Ex: Railway reservation etc.

b) **Minimizing Data Redundancy: Duplication** of information is carefully **controlled or reduced.** Minimizing redundancy can **reduce the cost of storing information** on hard drives and other storage devices. Ex: By creating centralized database or data in linked tables by DBMS, the data redundancy can be avoided.

c) **Integrity can be maintained:** Data integrity is maintained with accurate, consistent, and up-to-date data. **Updates and changes to the data only have to be made in one place in DBMS ensuring Integrity.** Ex: E106 cannot enter into loan to employee table until the same E106 exist in Employee Master.

d) **User-friendly:** It makes the data access and manipulation **easier for the user**. It also reduces the reliance of users on computer experts.

e) **Improved security:** DBMS provide various security features which can be used for providing a secured database. Ex: User authentication and Access control.

f) **Faster application development:** In DBMS environment the data is already there in databases, application developer has to think of only the logic required to retrieve the data in the way a user needs. **(1 mark x 5 = 5 marks)**

Answer 4:

(A)

<u>**A variety of activities are executed by Operating Systems which include:**</u>

- **Managing hardware functions**: O/Shelps in performing hardware tasks such as obtaining inputs from keyboards and mouse, access of data from hard disk & display of outputs on monitor. It acts as an intermediary between the application program and the hardware.

- **User Interfaces**: O/S provides a user interface for working on a computer. In earlier day's command User Interfaces (CUI) were widely used, but today most of the O/S's are Graphic User Interface (GUI) which uses icons & menus for executing activities on a computer in a user friendly manner. So, how we interface with our system will be provided by O/S.

- **Memory Management**: Allow controlling how memory is accessed and maximize available memory & storage. OS also provides Virtual Memory by improving the capacity of RAM. (Nov 16)

- **Task Management**: O/S can execute many tasks simultaneously and it maintains track of resources used by multiple jobs / tasks being executed simultaneously. In case of multitasking, O/S Helps in allocating resources to make optimum utilization of resources. This facilitates a user to work with more than one application at a time.

- **Networking Capability**: O/S Provide many features & capabilities to help connect computer networks. Like Linux & Windows 8 give us an excellent capability to connect to internet.

- **Logical access security**: It provides logical security by establishing a procedure for identification & authentication using a User ID and Password. It can log the user access thereby providing security control.

- **File management**: O/S does efficient file management by allowing users to give appropriate name to file and provide folders or directories for file management. It keeps a track of where each file is stored and who can access it.

(5 marks)

(B)

A data warehouse should be designed so that it meets the following criteria:

❖ It uses **non-operational data**. This means that the data warehouse is using a copy of data from the active databases that the company uses in its day-to-day operations, so the data warehouse must pull data from the existing databases on a regular, scheduled basis.

❖ The data is **time-variant**. This means that whenever data is loaded into the data warehouse, it receives a time stamp, which allows for comparisons between different time periods.

❖ The data is **standardized**. Because the data in a data warehouse usually comes from several different sources, it is possible that the data does not use the same definitions or units. For example, our Events table in our Student Clubs database lists the event dates using the mm/dd/yyyy format (e.g., 01/10/2013). A table in another database might use the format yy/mm/dd (e.g.13/01/10) for dates. For the data warehouse to match up dates a standard date format would have to be agreed upon and all data loaded into the data warehouse would have to be converted to use this standard format. This process is called **Extraction-Transformation-Load (ETL).**

(5 marks)

Answer 5:   **(1 mark x 10 = 10 marks)**

1) A
2) A
3) C
4) A
5) B
6) D
7) D
8) B
9) C
10) D