Ministry of Higher Education A.C. Year : 2022/2023
Modern Academy Term : May
For Computer Science and Spec : 4th CS $_{CS}$
Management Technology in Maadi Code : CS 405
Subject: DCNS Total Degrees: 50 Degrees
Examiner: Examination Boa ,) Time : 2 Hours

Ans Questions for Final Examination *No of Questions: 5*

<u>Q:1-a</u>

- **Bacteria**

Bacteria are programs that duplicate themselves. While these programs do not directly attack any software, they consume resources simply by replicating themselves.

- **<u>Viruses</u>**

These programs cannot exist by themselves; they need some application utility, or system program. Viruses, for example, need a host program and can also replicate them-selves, as described earlier.

- **Intrusion Detection**

Intrusion detection is the process of detecting and identifying unauthorized or unusual activity on the system. By using the audit records, the intrusion detection system should identify any undesirable activity.

- **<u>A *firewall*</u>**

Provides controlled access between a private network and the Internet. It intercepts each message between the private network and the Internet. Depending on the configuration, the firewall determines whether a data packet or a connection request should be permitted to pass through the firewall or be discarded.

<u>Q:1-b</u>

<u>Profiles</u>

Profiles characterize the behavior of a subject (or a group of subjects) on an object (or a group of objects).

Profiles include the description of normal behavior of subjects with respect to the objects. So profiles can be detect and report any abnormal activity as recorded in the audit records.

<u>A-Logon and Session Activity</u>

Logon and session activity is represented in the audit records as follows:

The subject is the user, the object is the user's logon location, and action is log on or log off.

<u>B-Command or Program Execution</u>

For these profiles, the audit records show the subject as a user, the object as the name of the program, and the action is execute. Measures for these profiles include execution frequency, resource usage, and execution denied.

<u>C-File Access Activity</u>

File access activity is reflected in audit records where the subject is a user, the object is the name of a file, and the action is read, write, create, delete, or append.

<u>Q:2-a</u>

Authentication: The word authentic means being actually and precisely what is claimed to be. Authentication is the process of verifying something, Such as a user's identity, a network address, or the integrity of a data string.

authenticated based on one or more of the following:

- Something the user knows
- Something the user has
- Something the user is .

<u>Q:2-b</u>

<u>Access Rights:</u>

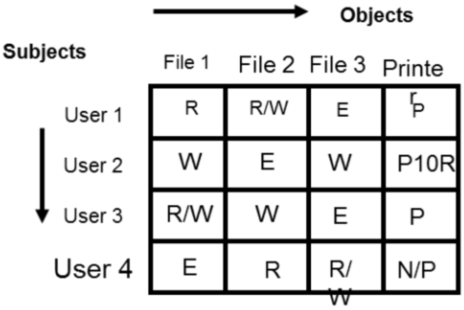
Access rights define the ways in which a subject can access the object. Access rights are specified for each pair of subjects and objects.

<u>An Access Control List ACL</u>

For a given object defines the access rights for each subject.

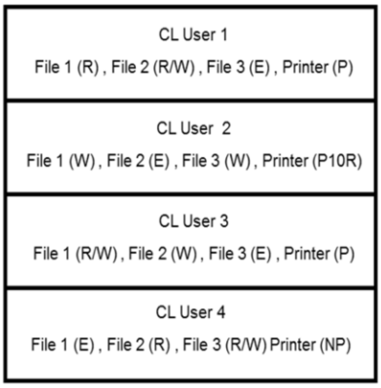
<u>A Capability List CL</u>

For a subject specifies the rights to access each object.


Objects
Subjects

	File 1	File 2	File 3	Printer
User 1	R	R/W	E	P
User 2	W	E	W	P10R
User 3	R/W	W	E	P
User 4	E	R	R/W	N/P

Access matrix



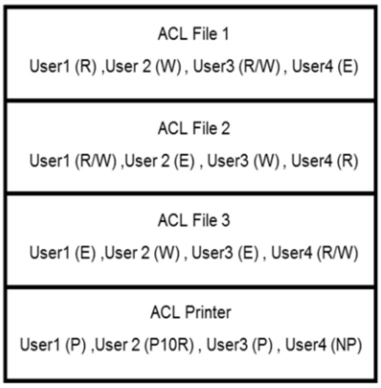
CL User 1
File 1 (R) , File 2 (R/W) , File 3 (E) , Printer (P)

CL User 2
File 1 (W) , File 2 (E) , File 3 (W) , Printer (P10R)

CL User 3
File 1 (R/W) , File 2 (W) , File 3 (E) , Printer (P)

CL User 4
File 1 (E) , File 2 (R) , File 3 (R/W) Printer (NP)

Capability lists



ACL File 1
User1 (R) ,User 2 (W) , User3 (R/W) , User4 (E)

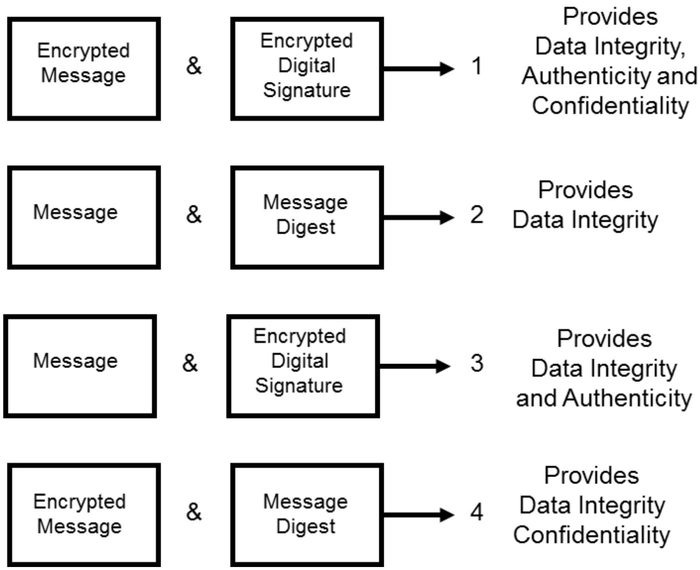
ACL File 2
User1 (R/W) ,User 2 (E) , User3 (W) , User4 (R)

ACL File 3
User1 (E) ,User 2 (W) , User3 (E) , User4 (R/W)

ACL Printer
User1 (P) ,User 2 (P10R) , User3 (P) , User4 (NP)

Access Control Lists

Q:3-a


Encrypted Message
&
Encrypted Digital Signature
1
Provides Data Integrity, Authenticity and Confidentiality
Message
&
Message Digest
2
Provides Data Integrity
Message
&
Encrypted Digital Signature
3
Provides Data Integrity and Authenticity
Encrypted Message
&
Message Digest
4
Provides Data Integrity Confidentiality

Q:3-b

Audit Requirements

Some of the important requirements for an audit system follow:

- Automatically collects information on all the security – sensitive activities. These activities are often selected by the administrator at installation time.
- Stores the information using a standard record format.
- Creates and saves the audit records automatically without requiring any action by the administrator.
- Protects the audit records log under some security scheme. For example, encrypt the audit log using the root password as the encryption key, or require entry of the root password to access the audit log.
- Minimally affects the normal computer system operation and performance.

Q:4-a

Security Concepts

1- Identification

Users are identified to an application through a user identifier or user-id.

2- Authentication

Authentication is the process used to verify the identity claimed by the user.

3- Authorization

Authorization is the process of assigning access rights to each user (ID).

4- Access Control

Access control pertains to the process of enforcing access rights for network resources.

5- Confidentiality

Confidentiality is the process used to protect secret information from unauthorized disclosure.

6- Data Integrity

Data integrity allows detection of unauthorized modification of data. Typically, data integrity detects whether the data has been modified during, transmission.

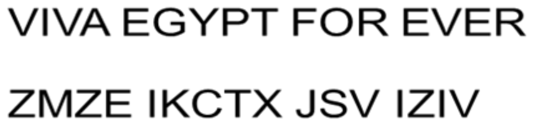
7- Non-repudiation

Non-repudiation is the capability to provide proof of the origin of data or proof of the delivery of data.

8- Denial of Service

A denial of service attack is one in which the attacker takes over or consumes a resource so that no one else can use it.

Q:4-b



VIVA EGYPT FOR EVER

ZMZE IKCTX JSV IZIV

Q:5-a

Distributed Security Services

1- Data confidentiality requires that given information must be protected from disclosure to unauthorized recipients.
   Solved by Encryption
2- Data integrity pertains to protection of information from modification by unauthorized users.
   Solved by hash function
3- Change data through transfer
   Solved by **Digital Signature**

Q:5-b

One-Way Hash Function requirements.

The requirements to be satisfied by one-way hash functions:

1- The one-way hash function *H* can be applied to a data block *M* of arbitrary size.

2- The resulting message digest, *d*, is of fixed size, the message digest size is usually 128 bits or 160 bits.

3- The one-way hash function *H* is easy to implement in both hardware and software.

4- Given the message digest *d*, it is very hard to find the original message *M*.

5- Given the message *M*, it is very hard to find a data block *N* such that *H* (N) = *H* (*M*).

6- It is very hard to find any two data blocks x and y such that:

H (x) = H (y).

Q:6

1. **Audit trail**: Procedures that automatically create a record for every security-sensitive workstation event and store the record in a secure log.
2. **Profiles:** The description of normal behavior of subjects with respect to the objects, so can detect and report any abnormal activity.
3. **An anomaly record**: Created when the audit records show some abnormal behavior compared to that in the profiles.
4. **logic bomb:** A fragment of software that is set to inflict damage when a certain set of conditions exist.
5. **A Trojan horse**: A piece of code that hides inside a program and performs a disguised function.
6. **Trapdoors**: Used legitimately by programmers to test, monitor, or fix programs. Some programmer has instantly gained special privileges to change the program.
7. **The firewall** Depending on the configuration, determines whether a data packet or a connection request should be permitted to pass or be discarded.
8. **The digital signature** establishes the authenticity of the originator of the data, able to authenticate the contents of the document.
9. **Viruses**: fragment of software that is not an independent program, self-reproducing often have the capability to gain control of the computer when it is executed causes harmful.
10. **Third party authentication**: Is the only trusted location where passwords are stored, every user or application will send the ID and the password for authentication. This approach improves the security and simplifies the storage and maintenance of passwords.