

ITE420 FINAL EXAM ANSWERS

FARDINA KABIR 1910080005



COURSE INSTRUCTOR : Ajarn Ilogu Ikechukwu

**Section1**

1.

DAC

DAC stands for **Discretionary Access Control**. The owner of the resource has the complete control over who can have access to a specific resource. The resource can be a file, directory, or any other, which can be accessed via the network. He can grant permission to other users to access the resource. He can also allow them to perform operations such as read, write, execute or share the resource. Moreover, he can transfer the ownership and determine the access type of other users.

In general, DAC is an easy and flexible access control method. However, it is not very secure. As the owner of the resource has the full control, one slip from him can give full control to others.

## MAC

MAC stands for **Mandatory Access Control**. In this method, access is determined by the system, not by the owner. Systems that contain highly sensitive data such as government or military based systems use this access control type.

In this control, all users (subjects) and resources should have a label assigned to them. It is a security label and specifies the level of trust.  To access the resource, the user must have equal or higher sensitivity level than the level of the required resource. For example, if the user requires accessing a secret file, he should have a secret clearance or a higher clearance to access the resource.

## Difference Between DAC and MAC

### **Definition**

DAC is a type of access control in which the owner of a resource restricts access to the resource based on the identity of the users. MAC is a type of access control that restricts the access to the resources based on the clearance of the subjects.

### **Full Name**

The DAC stands for Discretionary Access Control (DAC) and the MAC stands for Mandatory Access Control.

### **Basis**

In DAC, the resource owner determines who can access and what privileges they have. MAC provides access to the users depending on the clearance level of the users.  Access is determined by the system.

### **Flexibility**

Furthermore, DAC is more flexible than MAC.

### **Security**

Also, MAC is more secure than DAC.

### **Implementation**

Moreover, DAC is easier to implement than MAC

2.

.Authorization usually comes after authentication which confirms your privileges to perform. In simple terms, it’s like giving someone official permission to do something or anything.

Access to a system is protected by both authentication and authorization. Any attempt to access the system might be authenticated by entering valid credentials, but it can only be accepted after successful authorization. If the attempt is authenticated but not authorized, the system will deny access to the system.Authorization usually comes after authentication which confirms your privileges to perform. In simple terms, it’s like giving someone official permission to do something or anything.

For example, the process of verifying and confirming employees ID and passwords in an organization is called authentication, but determining which employee has access to which floor is called authorization. Let’s say you are traveling and you’re about to board a flight. When you show your ticket and some identification before checking in, you receive a boarding pass which confirms that the airport authority has authenticated your identity. But that’s not it. A flight attendant must authorize you to board the flight you’re supposed to be flying on, allowing you access to the inside of the plane and its resources.

Access to a system is protected by both authentication and authorization. Any attempt to access the system might be authenticated by entering valid credentials, but it can only be accepted after successful authorization. If the attempt is authenticated but not authorized, the system will deny access to the system.

1. I. Identity Verification is the much more in-depth step of linking an individual to the information that they provide. In the validation step, companies are seeing if the data is real, in this step a customer is tied directly to the information and verified as genuine by additional checks including official databases such as driver license files, electoral registers and the credit bureau. This level of check is often associated when companies have a regulatory obligation to prove that you exist – for example as part of setting up a bank account or applying for a loan. Verification has more friction than validation however this is good when more certainty is needed that the individual’s data links, e.g. their address matches their name. Experian research shows that some friction, caused by fraud controls, are valued by customers, especially when high value products are involved such as mortgages.

Authentication is the process by which a customer’s identity is qualified against something that only the user should have or know. This process determines that the individual is who they say they are by utilising existing user-provided information, e.g. the individual is asked a series of questions which would only be known to them, that they must answer correctly to log onto an existing account, or a onetime password is sent to their mobile phone. This process can provide friction in the customer journey however developments in this area, like using biometrics, are improving the customer experience and providing greater certainty for businesses

II. There are three common factors used for authentication:

Something you know (such as a password)

Something you have (such as a smart card)

Something you are (such as a fingerprint or other biometric method)

A key would be described as the authentication factor "something that you have". In order to open a door you MUST have a key.

**Section 2**

1. SLE=45000\*4+45000=225000

ARO=0.45

ALE= SLE\*ARO=$101250

1. SLE=$12\*2=$24

Aro=52weeks \*0.4=20.8

ALE=SLE\*ARO=$24\*20.8=$499.2

**Section3**

**6.**

**Shift 7 a to h**

**Ans: AIIX FIWE CH SIOL ZCHUF YRUGM**

7.   What are the main differences between symmetric and asymmetric key

         cryptography?

| **Symmetric key cryptography** | **Asymmetric key cryptography** |
| --- | --- |
| In symmetric key cryptography, single or same key is used for both encryption as well as decryption | In asymmetric key cryptography, two separate keys are used, one for encryption and the other for decryption |
| It is also called a secret key cryptography or private key cryptography | It is also called as Conventional cryptography system or Public key cryptography |
| Mathematically it is represented as: P=D(K,E(P)) Where K=Encryption and decryption key P=Plain text D=Decryption E(P)=Encryption of plain text | Mathematically it is represented as:P=D(Kd,E(Ke,P)) Where Ke=Encryption key Kd=Decryption key D=Decryption E(Ke,P)=Encryption of plain text using encryption key P=Plain text |
| It is faster than asymmetric key cryptography | Because of different keys used for encryption and decryption, it is slower than symmetric key cryptography |
| It utilizes less resources as compared to asymmetric key cryptography | It uses more resources as compared to symmetric key cryptography |
| AES and DES are examples of symmetric key cryptography | Diffie hellman and RSA are examples of asymmetric key cryptography |

8. The difference between them:

|  |  |  |
| --- | --- | --- |
| S.NO | Block Cipher | Stream Cipher |
| 1. | Block Cipher Converts the plain text into cipher text by taking plain text’s block at a time. | Stream Cipher Converts the plain text into cipher text by taking 1 byte of plain text at a time. |
| 2. | Block cipher uses either 64 bits or more than 64 bits. | While stream cipher uses 8 bits. |
| 3. | The complexity of block cipher is simple. | While stream cipher is more complex. |
| 4. | Block cipher Uses confusion as well as diffusion. | While stream cipher uses only confusion. |

**SECTION 4:     Operations Security**

9. The OPSEC process involves five steps, which will be discussed in greater depth later in this section. These steps are:

Identification of Critical Information

Analysis of Threats

Analysis of Vulnerabilities

Assessment of Risks

Application of Appropriate Countermeasures.

Identification of Critical Information. Critical information is factual data about an organization's intentions, capabilities, and activities that the adversary needs to plan and act effectively to degrade operational effectiveness or place the potential for organizational success at risk. The OPSEC process identifies critical information and determines when that information may cease to be critical in the life cycle of an operation, program, or activity.

Analysis of Threats. Threat analysis consists of determining the adversary's ability to collect, process, analyze, and use information. The objective of threat analysis is to know as much as possible about each adversary and their ability to target the organization. It is especially important to tailor the adversary threat to the actual activity and, to the extent possible, determine what the adversary's capabilities are with regard to the specific operations of the activity or program.

10.I). Operational security (OPSEC), also known as procedural security, is a risk management process that encourages managers to view operations from the perspective of an adversary in order to protect sensitive information from falling into the wrong hands.

Though originally used by the military, OPSEC is becoming popular in the private sector as well. Things that fall under the OPSEC umbrella include monitoring behaviors and habits on social media sites as well as discouraging employees from sharing login credentials via email or text message.

10. II)Three laws of OPSEC

If you don’t know the threat, how do you know what to protect.

If you don’t know what to protect, how do you know you’re protecting it.

If you are not protecting it, the dragon wins.