TCS332 Fundamental of Information Security and Blockchain

B. Tech CSE III Semester

Instructor:

Dr Mohammad Wazid

Professor, Department of CSE

Graphic Era (Deemed to be University), Dehradun, India

(Research h-index: 43, i10-index:71)

Email: wazidkec2005@gmail.com

Homepage: https://sites.google.com/site/mwazidiiith/home

Unit 1. Introduction to information security

Topics for this lecture

- **Cyber attacks and defense**

Protection against Unauthorized Modification/ Deletion and Unauthorised Access

Data (message) modification attack

- A kind of active attack on a system.
- It simply means that some portion of a authorized data message is altered/deleted, or that messages are delayed or reordered, to cause harm.
- Example, message meaning “Allow Alice” to read confidential file accounts” is changed to “Allow Eve” to read confidential file accounts”.
- In case of deletion message becomes garbled. Suppose “Allow Alice” changed to “Allow Eve”.
- Note: Here Alice is a genuine user and Eve is the guy with malicious mind (attacker) who can misuse the confidential file accounts.

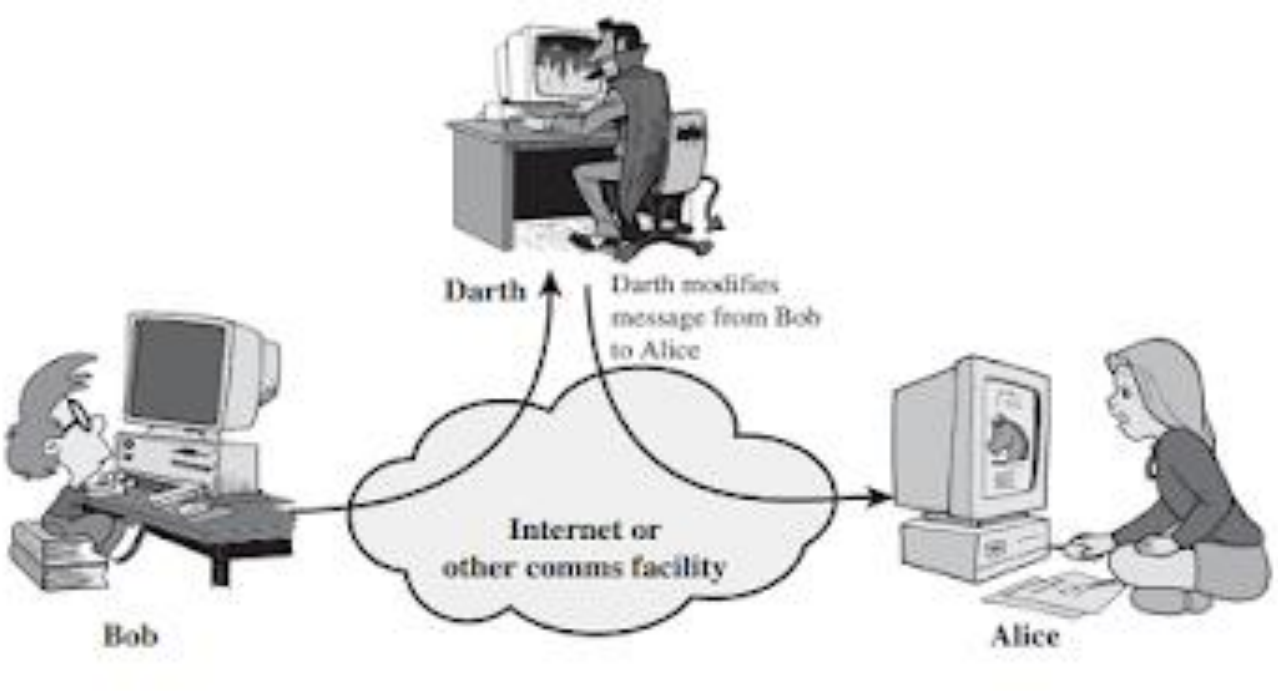

Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

Fig2. Data (message) modification attack scenario

Protection against data (message) modification attack

- To protect the data against the data modification certain algorithms are used. For example Hash, MAC, HMAC.
- Hash algorithm i.e., SHA1, SHA256.
- By using these algorithm we compute hash value (in case of hash algorithm) and append that with the original message and send the [message||hash value] to the receiver.
- At the receiver's end receiver will also compute the hash value from the received message and compare it with the appended hash value.
- If both hash values matches then data message is original; otherwise message was modified in the communication channel.

Protection against data (message) modification attack

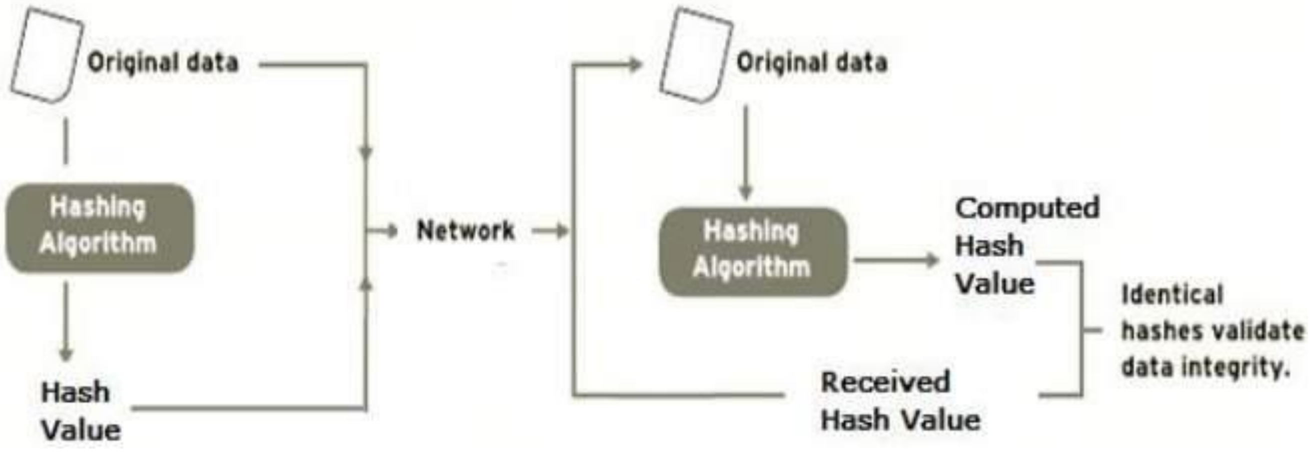


Fig3. Protection against data (message) modification attack using the hash function

Note: Same mechanism also works for data message deletion.

Unauthorised access

- Unauthorized access is when someone gains access to a website, server, running service, or other system using someone else’s account or other methods (i.e., by using malware).
- For example, if someone kept guessing a password or username for an account that was not theirs until they gained access, it is considered unauthorized access **(Protection: Authentication mechanism).**

Unauthorised access

- Unauthorized access could also occur if a user attempts to access an area of a system which they are not allowed access.
- When attempting to access that area, they would be denied access and possibly see an unauthorized access message **(Protection: Access control mechanism).**

Protection against unauthorised access

Following are the possible ways.

1. Authentication

2. Access control

Protection against unauthorised access

- Additionally system administrators set up alerts to let them know when there is an unauthorized access attempt, so that they may investigate the reason **(in case if control mechanism (i.e., authentication fail to prevent).**
- These alerts stops attackers from gaining access to the system.
- Many secure systems may also lock an account that has had too many failed login attempts (i.e., Online banking accounts).

End of lecture

What is authentication?

- The process of proving or showing something to be true, genuine, or valid.
- The action of verifying the identity of a user (or process, sender).

Authentication procedure

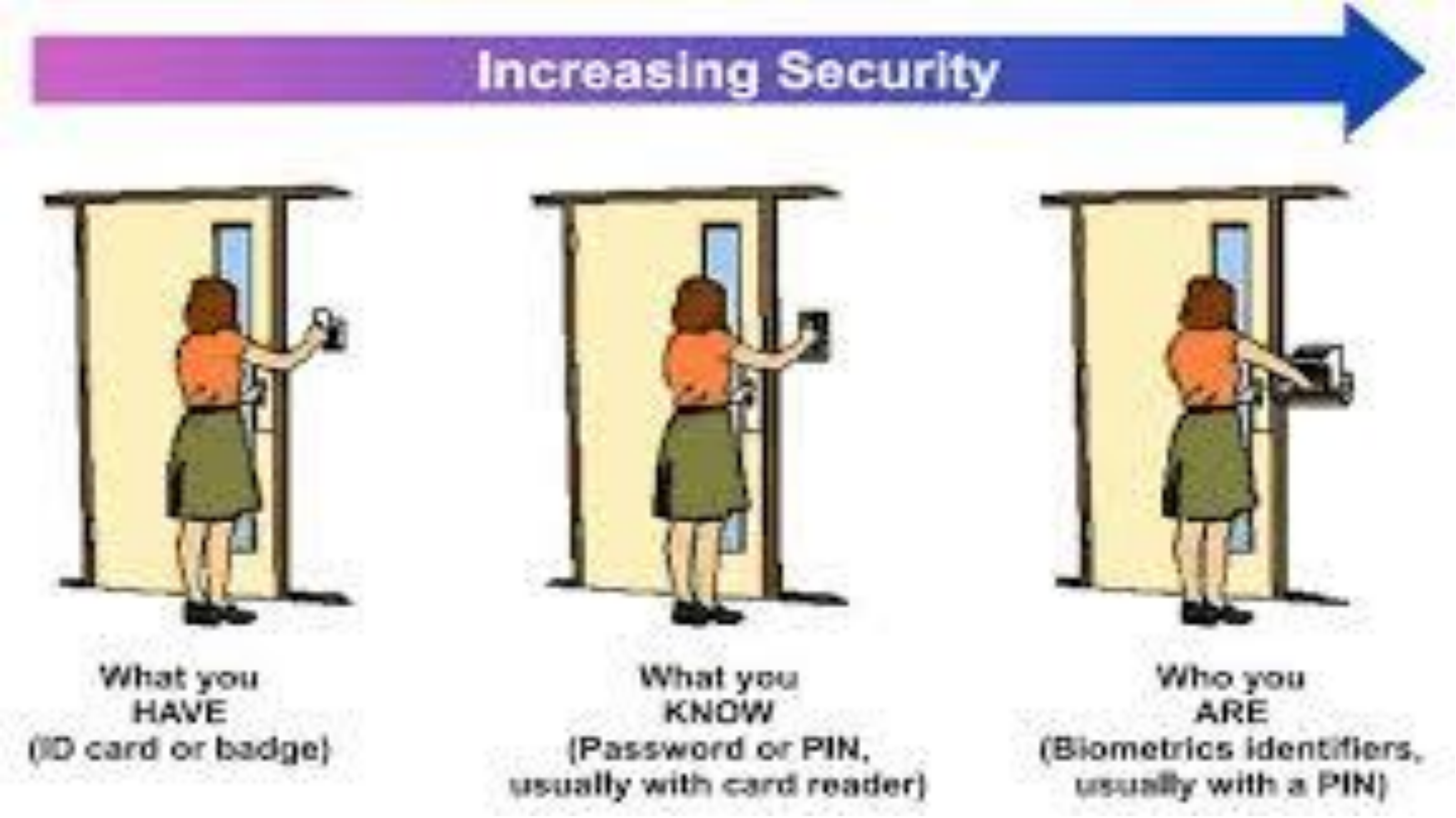


Fig. Authentication procedure (Image source: researchgate.net)

Authentication procedure

Types:

- **1-Factor authentication protocol**
- **2-Factor authentication protocol**
- **3-Factor authentication protocol**

Authentication procedure

- Positive verification of identity (man or machine)
- Verification of a person’s claimed identity
- Who are you? Prove it.
- It has three categories:
    - What you know (i.e., password)
    - What you have (i.e., smart card)
    - Who you are (i.e., biometric data-finger prints etc.)

2. Access Controls

- Access controls are used specifically address admission of a user into a trusted area of organization.
- Putting restriction on the invalid user.

Access Matrix

- The access matrix model is the policy for user authentication, and has several implementations such as access control lists (ACLs) and capabilities.

- **It is used to describe which users (subject) have access to what resource (objects).**

Access Matrix

❖The access matrix model consists of four major parts:

I. A list of objects

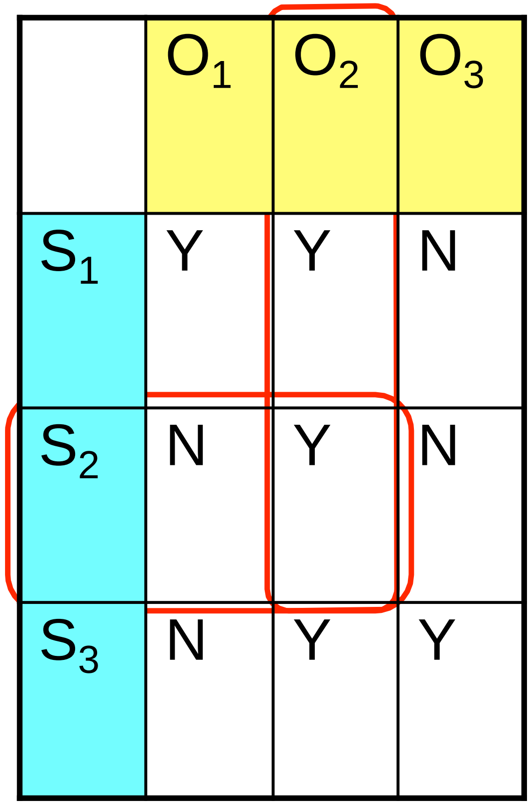
II. A list of subjects

III. A function T which returns an object’s type

IV. The matrix itself, with the objects making the columns and the subjects making the rows

Example of Access Matrix

- Subjects (i.e., user)
- Objects (i.e., some file)
- Operations (i.e., read, write)
- Can determine
  - Who can access an object
  - What objects can be accessed by a subject
  - What operations a subject can perform on an object



	O_1	O_2	O_3
S_1	Y	Y	N
S_2	N	Y	N
S_3	N	Y	Y

Access Controls

- Access controls can be:
  - **Mandatory access controls (MAC):** Give users and data owners limited control over the access to information.

Access Controls

Mandatory Access Control (MAC)

- Mandatory Access Control (MAC) is the **strictest of all levels of control**.
- The design of MAC was defined, and is primarily used by the government.

Access Controls

Mandatory Access Control (MAC)

- MAC takes a hierarchical approach to control access to resources.
- Under a MAC enforced environment access to all resource (i.e., data file) is controlled by settings defined by the system administrator.

Access Controls

Mandatory Access Control (MAC)

- For example, all access to resource is strictly controlled by the operating system based on system administrator configured settings.

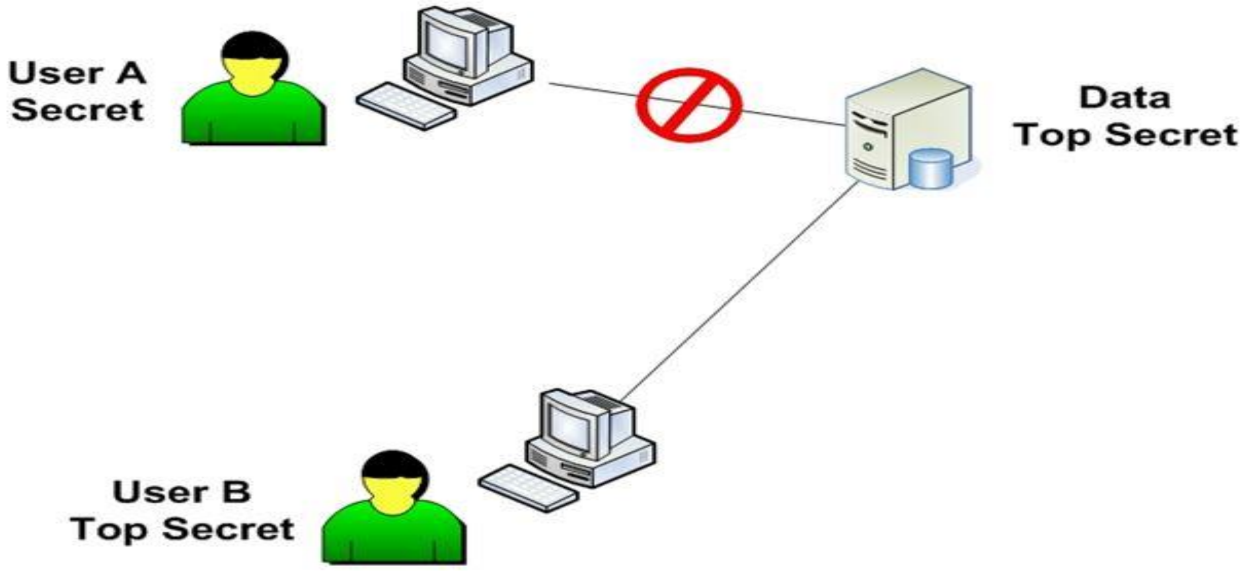


Fig. Mandatory Access Control (MAC) (Source: brighthub.com)

No matter who is user A, only authority (i.e., Government) decides who is going to access this top secret data.

Access Controls

- **Nondiscretionary controls**:

- Can be on an individual's role (role-based) or a specified tasks the individual is assigned (task-based). **(Role-based, task-based).**

Access Controls

- **Nondiscretionary controls**
- **Role based access control (RBAC):** Users are assigned to a particular role. For example, an accountant in a company will be assigned to the Accountant role, gaining access to all the resources permitted for all accountants on the system.
- Similarly, a software engineer might be assigned to the developer role.

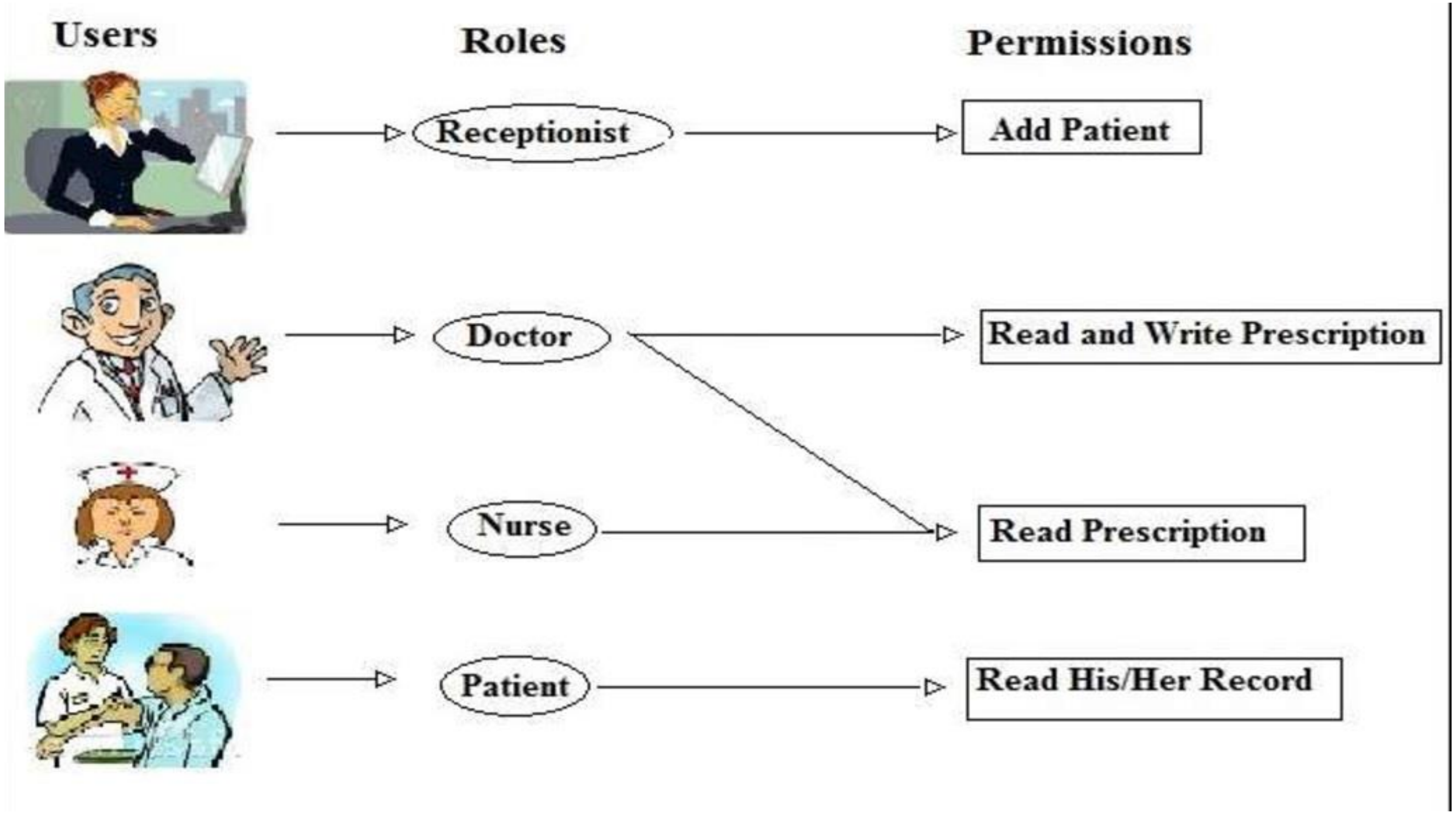


Fig. Role based access control (RBAC) scenario
(Source: semanticscholar.org)

Access Controls

Discretionary access controls (DAC)

- Unlike Mandatory Access Control (MAC) where access to system resources is controlled by the operating system (under the control of a system administrator).

Access Controls

Discretionary access controls (DAC)

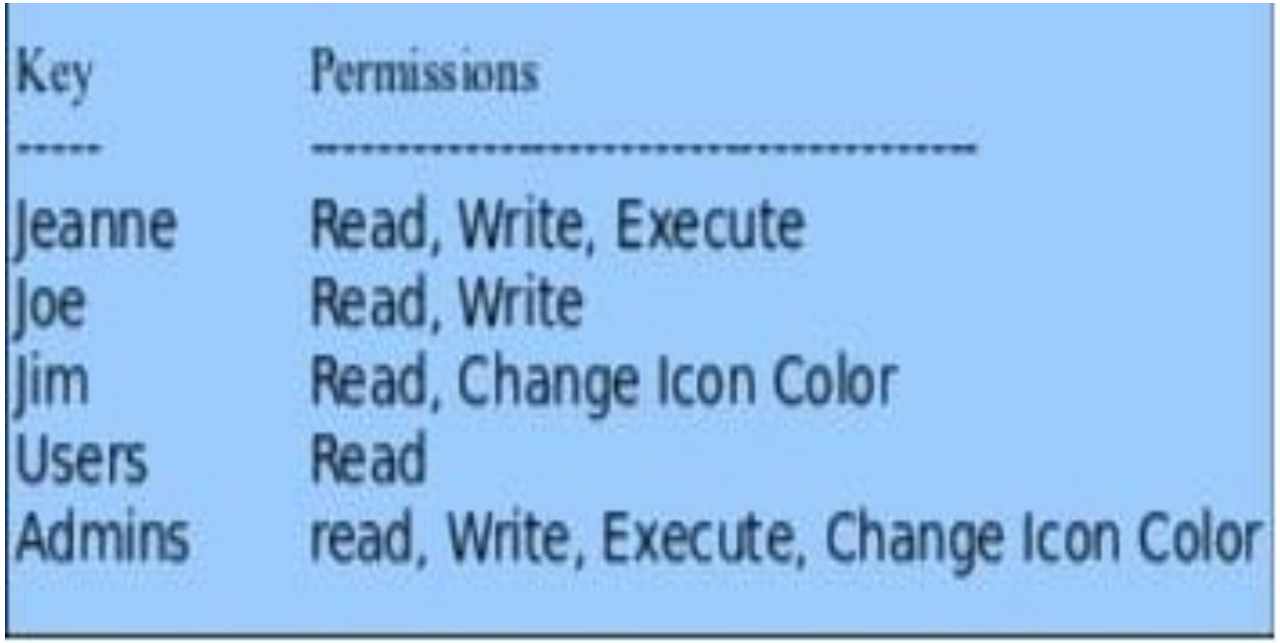
- ❑ DAC allows each user **to control access to their own data.**
- ❑ DAC is typically the default access control mechanism for most desktop operating systems.

Discretionary access controls (DAC)

- Each resource object on a DAC based system has an Access Control List (ACL) associated with it.
- An ACL contains a list of users and groups to which the user has permitted access together with the level of access for each user or group.

Discretionary access controls (DAC)

- For example, User A may provide read-only access on one of her files to User B, read and write access on the same file to User C and full control to any user belonging to Group 1.



Key	Permissions
Jeanne	Read, Write, Execute
Joe	Read, Write
Jim	Read, Change Icon Color
Users	Read
Admins	read, Write, Execute, Change Icon Color

Fig. Discretionary access controls (DAC) scenario

Exercises

Create a access matrix for the following scenario

- There are three users (i.e., U1, U2, U3) in the system.
- There are three objects/resources (i.e., R1, R2, R3) in the system.
- User U1 can only access resource R3 but not the other resources.
- User U2 can access both resource R1 and R2 but not resource R3.
- User U3 can access all resources.

Solution:

Users/ Resources	R1	R2	R3
U1	No	No	Yes
U2	Yes	Yes	No
U3	Yes	Yes	Yes

Create a access matrix for the following scenario

- There are three users (i.e., U1, U2, U3) in the system.
- There are three objects/files (i.e., F1, F2, F3) in the system.
- User U1 can not access F1, can read F2, and read/write F3.
- User U2 can read/write F1 and F2 and can read/write/execute F3.
- User U3 can read/write/execute all files.

Solution:

Users/ Resources	F1	F2	F3
U1	NA	R	R/W
U2	R/W	R/W	R/W/E
U3	R/W/E	R/W/E	R/W/E

Abbreviations:

R= Read operation

W= Write operation

E=Execute operation

NA=Can not access

Predict who may be the administrator ?

Answer: U3

MCQ round

To secure a system we can use following technique

a) IDS

b) Firewall

c) Access control

d) All of above

To secure a system we can use following technique

Answer: (d) is correct

To secure a system which technique we should use first

a) Authentication mechanism

b) Access control mechanism

c) Any of above

d) None

To secure a system which technique we should use first

Answer: (a) is correct

Which of the following is not a access control technique

a) Role based

b) Identity based

c) Task based

d) All of them are access control techniques

Which of the following is not a access control technique

Answer: (d) is correct

References

- Zero Trust Model: Can Trusting No One Be the Answer to Your Cybersecurity Problems (Information available at: https://www.ekransystem.com/en/blog/zero-trust-security-model
- Textbook: Penetration Testing: A Hands-on Introduction to Hacking by Georgia Weidman
- Textbook: Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives by Sunit Belapure and Nina Godbole
- Michael E. Whitman and Herbert J. Mattord, Principles of Information Security, (2e), Thomson Learning, 2007
- psu.edu
- Pen test. Information available at: https://www.imperva.com/learn/application-security/penetration-testing/

❑ Identifying, Analyzing, and Evaluating Cyber risks. Information available at: https://www.securityforum.org/uploads/2017/05/ISF_c07.pdf