Database Security Notes:

- Introduction
- Brief description of the whole concept

Objectives:

- Threats
- Countermeasures
- Authorization and authentication
- Access Control
- Bell-La Padula Model in Database security(using MAC)
- Encryption

INTRODUCTION:

Database security within network security refers to the collection of measures and practices designed to protect a database from unauthorized access, misuse, corruption, or loss. It is crucial in safeguarding sensitive data, preventing data breaches, and ensuring data integrity and availability.

BRIEF DESCRIPTION OF THE WHOLE CONCEPT

Database security involves various strategies, including:

1. **Access Control:** Ensures that only authorized users and applications can access certain parts of the database. This can involve role-based access control (RBAC), multi-factor authentication (MFA), and user permissions.
2. **Encryption:** Protects data in storage and in transit by converting it into unreadable formats for unauthorized users. Strong encryption algorithms help to secure sensitive data like personal information, credit card numbers, and health records.
3. **Auditing and Monitoring**: Regular tracking of database activity allows detection of unauthorized access, suspicious behavior, or unusual patterns. Database logs and alerts play a significant role here.
4. **Database Firewalls:** Acts as a barrier between the database and potential malicious traffic, filtering out unauthorized access attempts and potential threats.
5. **Data Masking:** Protects sensitive information by obscuring it in non-production environments. Masked data remains usable in testing or development without revealing real data.
6. **Patch Management:** Regularly updating database systems to patch vulnerabilities. Many cyberattacks exploit unpatched software vulnerabilities, so keeping database software current is critical.
7. **Backup and Recovery:** Regular backups and robust recovery plans protect data integrity and availability in the event of data corruption, hardware failure, or cyberattacks like ransomware.
8. **Firewall Configuration**: Block unauthorized access to database servers and allow connections only from trusted IPs.

9. **Network Segmentation**: Place the database in a separate network segment (e.g., a private subnet) and limit inbound and outbound traffic.
10. **Virtual Private Network (VPN)**: Use VPNs to provide secure remote access to databases.

Objectives:

- Threats
- Countermeasures
- Authorization and authentication
- Access Control
- Encryption

Threats

A threat is any situation or event, whether intentional or accidental, that may adversely affect a system Sample threats: An attack

1. Unauthorized amendment or copying of data
2. Using another person's means of access
3. Program alteration
4. Wire tapping
5. Illegal entry by hacker
6. Blackmail
7. Theft
8. Failure of security mechanisms

Countermeasures to the database threats:

Countermeasures range from the physical controls to the administrative controls

Security of Database Management System (DBMS) is as good as security of an operating system running DBMS

We consider the following computer-based security controls in a multiuser environment

- Authorization and authentication
- Encryption
- **Vulnerability Management**
- Backup and recovery
- Integrity

- **Authorization**

  Authorization means granting a right or a privilege to have a legitimate access to a system or the resources operated by a system

Authorization is usually built into the software and it determines what system or object a user can access and what a user is allowed to do with it

In a process of authorization a subject representing a user or a program requests and obtains access to an object that represent relational table, relational view, etc.

Authentication

Authentication is a mechanism that determines whether a user is who he or she claims to be.

A system administrator is responsible for allowing the users to have access to a computer system by creating the individual user accounts.

When an account is created a user is given a unique identifier and a user picks a password associated with the identifier

Access Control

It ensures that only authorized users and applications can access certain parts of the database.

A typical way to control access to a database system is based on granting and revoking privileges

A privilege allows a user to create, to drop, or to access in read or write mode some database objects like relational tables, relational views, index, etc or to perform certain operations.

DBMS keeps track of all granted privileges to ensure that only selected user can access and can perform operations on the database objects.

There are two different strategies of access control:

- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)

Discretionary Access Control (DAC)

It is a model that allows the owner of a resource to control who can access it and what rights they have.

In **Discretionary Access Control** each user is given the access rights (privileges) on the specific database objects

A user obtains the privileges in a moment when he/she creates an object and the access of other users to the object is at a discretion of an owner.

It is an effective system with some weaknesses, for examples:

1. In operating systems like Windows and UNIX, the owner of a file or folder can specify who can access it and what rights they have.

2. Google Docs

The owner of a Google Doc can create an access control list (ACL) that includes relevant employees. Some members of the group may be able to edit the document, while others may only be able to view it.

Mandatory Access Control

It is based on system-wide policies that cannot be changed by the individual users.
Mandatory Access Control (MAC) is a cybersecurity system that limits access to resources in a database management system (DBMS) based on the sensitivity of the information and the user's authorization level:

- **Examples**

1. For example, in the military, a data owner does not decide who has clearance or change the classification of an object.

2. **Banking and insurance**

MAC is used to limit who can access financial information, such as customer records. This reduces the risk of data breaches

THE BELL-LAPADULA MODEL

It is a security model in a database management system (DBMS) that protects the confidentiality of data by preventing users with lower security levels from accessing objects with higher security **levels:**

1. Clearance and

2. Classification Levels

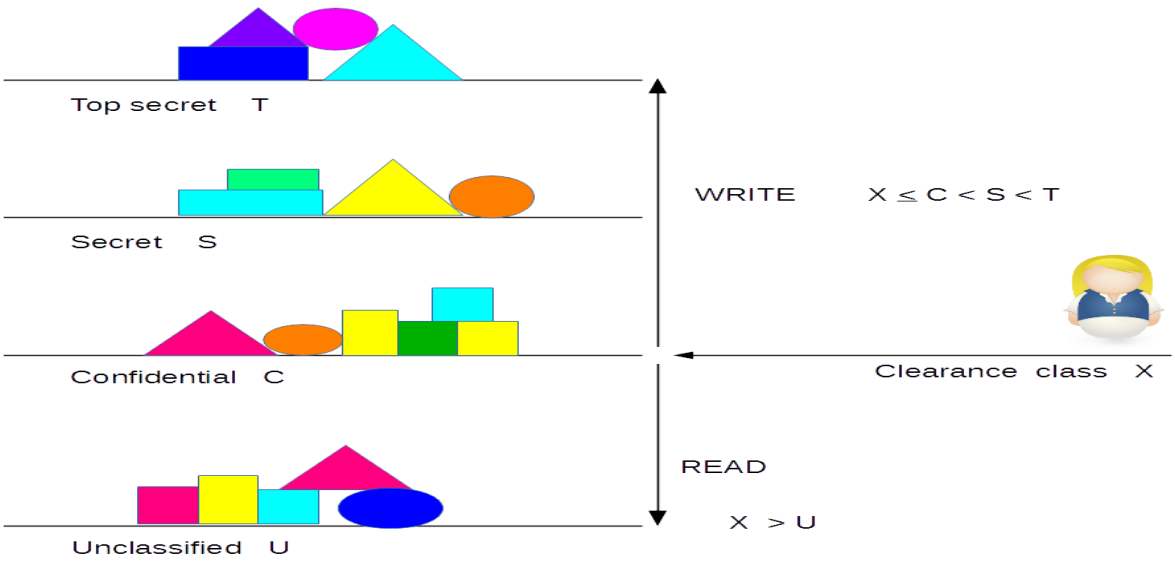
There are two types of levels in the Bell-LaPadula model: classification and clearance levels.

1. Classification levels are used to protect information from unauthorized disclosure. These levels are used to assign a security label to an object. The security labels are used to control access to the object. Examples of classification levels in the Bell-LaPadula model could include Top Secret, Secret, Confidential, and Unclassified, with Top Secret holding the highest level of trust/classification and unclassified being the lowest (available to the public).

2. Clearance levels are used to protect information from unauthorized modification and unauthorized use/access.

A multilevel security system that helps maintain confidentiality by controlling access to classified information.

A MODEL OF MAC IN BELL LA PADULA:



The Bell-LaPadula model uses **mandatory access control (MAC)** rules to restrict access to objects based on the security levels of subjects and objects:

- **Simple Security Property**: A subject cannot read an object with a higher security level.
- **Star Security Property**: A subject cannot write to an object with a lower security level.
- **Discretionary Security Property**: Uses an access matrix to specify discretionary access control.

These levels are used to assign a security level to a subject.

They mimic the classification levels in their structure.

For example:

- **Top Secret:** Subjects with this clearance level would have access to all objects with a classification level of Top Secret and below.
- **Secret:** Subjects with this clearance level have access to all objects with a classification level of Secret and below.
- **Confidential:** Subjects with this clearance level would have access to all objects with a classification level of Confidential or Unclassified.
- **Unclassified:** Subjects with this clearance level could only access unclassified/public information. They would have no access to information classified as Top Secret, Secret, or Confidential.

The model's main Access control rules are:

1. **Simple Security Property**
   Also known as "no read up", this rule states that a subject cannot read an object at a higher classification level.
2. **Star Property**

a. Also known as "no write down", this rule states that a subject cannot write to an object at a lower classification level.

3. **Star Property Rule**

   This rule prevents a subject from writing down to a lower classification level. For example, someone with Top Secret clearance can read down to all other clearance levels, but can only write to objects with a Top Secret classification.

4. **Strong Star Property Rule**

   This rule states that only a subject with the same clearance level as an object can read and write to that object.

NB: It only focuses on confidentiality only but rather talks on Integrity and Availability.

Encryption

Encryption of data means encoding of data by a special algorithm, that renders the data unreadable by any program without the decryption key Sensitive data can be encoded to protect it against external threats or access.

Strong encryption algorithms help to secure sensitive data like personal information, credit card numbers, and health records.

Some DBMS provide special facilities to encrypt data and to access encrypted data after decoding it

Usually there is a degradation in performance because of time needed to decode data

A typical cryptosystem includes:

- An encryption key to encrypt data (plaintext)
- An encryption algorithm that with the encryption key transfroms plaintext into ciphertext
- A decryption key to decrypt the ciphertext
- A decryption algorithm to use decryption key with cipher text and to create the original plaintext.

Types of database encryption are: **Symmetric, Asymmetric and Hashing**

Here are some examples of encryption in databases:

- **Encryption plug-in API**

This plug-in can provide different keys for tables with different security needs. For example, tables with low security can use short keys for fast encryption, while tables with high security needs can use longer keys.

- **One-way encryption**

This algorithm is used to encrypt passwords before saving them. The encrypted password is not similar to the original plaintext, and it cannot be reversed to get the original password.

➢ **Important note:**

The Bell-LaPadula model uses classification and clearance levels to manage a multi-level security system:

- Classification levels

These levels are used to assign security labels to objects.
Examples of classification levels include Top Secret, Secret, Confidential, and Unclassified. Top Secret is the highest level of classification, and Unclassified is the lowest.

- Clearance levels

These levels are used to assign security levels to subjects. The clearance levels mimic the classification levels in structure.
For example, a subject with a Top Secret clearance level can access all objects with a classification level of Top Secret or below.
These levels are used to assign a security label to an object. The security labels are used to control access to the object.