Unit 8-Database Security

Subject Code: 303105203

Prof. S.W.Thakare
Assistant Professor,
Computer science & Engineering

Parul®
University

DIGITAL LEARNING CONTENT

CHAPTER-8

Database Security

Data Security

- It is protecting data from unauthorized access or allowing only authorized access.
- Only DBA is allowed to access any data or update any data while other users are permitted to access any record or update any data according to their relevance or authority level.

Data Security …

- Keeps your information safe
- Helps keep your reputation clean
- Gives you a competitive edge
- Saves on support and development costs

Data Integrity

- The overall precision, completeness, and continuity of data is known as data integrity.
- Data integrity also applies to the data's protection and security in terms of regulatory enforcement, such as GDPR compliance.
- It is kept up to date by a set of procedures, guidelines, and specifications that were put in place during the design phase.
- Data integrity also ensures that the information is protected from outside influences.

Data Integrity

Different Kinds of data integrity

- Physical and logical data integrity are the two forms of data integrity. Both are a collection of procedures and methods for maintaining data integrity in hierarchical and relational databases.

- Physical integrity

Physical integrity refers to the safeguarding of data's completeness and precision during storage and retrieval. It is jeopardized when natural disasters occur, electricity goes out, or hackers interrupt database functions.

- Logical integrity

In a relational database, logical consistency ensures the data remains intact as it is used in various ways. Logical integrity, like physical integrity, defends data from human error and hackers, but in a different way.

Authentication

- Process of using credentials for validating user
- Its main objective is to provide security and integrity control to data

  - Integrity : It is all about validity of data either to make sure data is not corrupt and incorrect
  - Security : It is to protect data and making sure data access is to only those who are allowed to access that data.

Authorization

- Process of validation the access of the user for any data.
- It checks what data a particular user can access for example accessing a file from hard disk
- It ensures data privacy as well as access control of data.

Access Control

- Access control is a strategy for ensuring that clients are who they state they are and that they have the fitting access to data.

- There are mainly three access control model
- That is DAC,MAC, RBAC

DAC : Discretionary access control

- Here the data access control is availed by the user who has created that data either the owner of particular data.
- Here single user can have multiple permission and multiple users can have same permission all according to the owner of the data often referred as object.
- Discretionary access control is supported by SQL with help of following two command:

  1) Grant :- It is used to assign specific access to any user. Syntax:- GRANT privilege ON object TO user [WITH GRANT OPTION]

  2) Revoke :- It is used to remove any permission from the user. Syntax:- REVOKE privilege ON object FROM user {RESTRICT/CASCADE}

DAC : Discretionary access control

Examples:
1) GRANT SELECT, INSERT, UPDATE, DELETE ON Student TO abc;

User “abc” can perform select, insert, update and delete on the table “Student”.
2) GRANT ALL ON Student TO def;

User “def” can perform all operations on the table “Student”.
3) GRANT SELECT ON Student TO PUBLIC;

Any user can perform only select operations on the table “Student”.
4) REVOKE ALL ON Student FROM abc;

Permissions are taken back from user “abc”.

MAC: Mandatory Access Control

- Here individual access is not assigned.
- The access permission are bifurcated into particular levels according to sensitivity or importance of data for the respective organization.
- The users are also divided into several groups which has different clearance by which they can access the data of different levels
- Higher the clearance level more levels of data can be accesed.

MAC: Mandatory Access Control

- Four Components for implement multilevel Mandatory access control.

1. Subjects
1. Objects
1. Clearance Level
1. Security Level

MAC: Mandatory Access Control

- Database management system determines which user can read or do write operation based on some object rule.
- These rule make sure that sensitive data are protected and are not received by unwanted entities
- User Can Access data by following two rules :-
  1) Security Property
  2) Star Security Property

MAC: Mandatory Access Control

DAC vs MAC:

DAC	MAC
DAC stands for Discretionary Access Control.	MAC stands for Mandatory Access Control
DAC is easier to implement.	MAC is difficult to implement
DAC is less secure to use.	MAC is more secure to use.
In DAC, the owner can determine the access and privileges and can restrict the resources based on the identity of the users.	In MAC, the system only determines the access and the resources will be restricted based on the clearance of the subjects.
DAC has high flexibility with no rules and regulations.	MAC is not flexible as it contains lots of strict rules and regulations
DAC has complete trust in users.	MAC has trust only in administrators.
Decisions will be based only on user ID and ownership.	Decisions will be based on objects and tasks, and they can have their own ids.

RBAC:- Role Based Access Control

- In this model role of user in an organization plays an important role to define the access to the data.
- Roles in this model defines access level of a employee have to the network.
- User is allowed to access only those data which is needed to perform his duties effectively.
- Factors on which access may be based: Authority, Responsibility, Job Competency

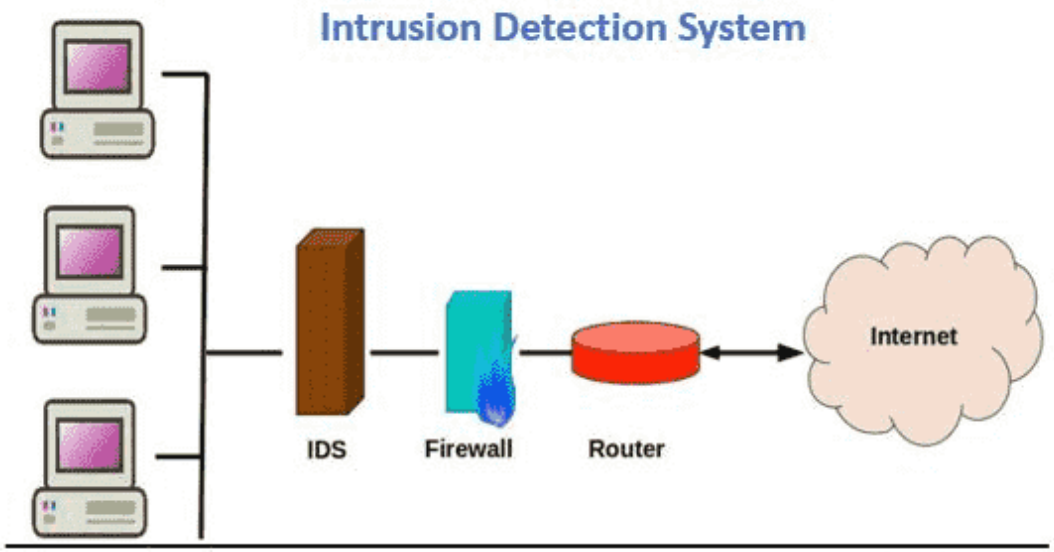
Intrusion Detection System

- An Intrusion Detection System (IDS) is a system or programming application that screens network traffic or system for dubious action or strategy infringement and issues alarms at the point when such action is found.
- It is a software application that scans a network or a system for hurtful movement or strategy breaking.
- Any malicious endeavor or infringement is typically revealed either to a head or gathered centrally utilizing a security information and event management (SIEM) system.

Intrusion Detection System

Different Intrusion Detection Systems:

1. Network Intrusion Detection System,
2. Host Intrusion Detection System,
3. Protocol-based Intrusion Detection System,
4. Application Protocol-based Intrusion Detection System,
5. Hybrid Intrusion Detection System.



Intrusion Detection System

Detection Method of IDS:

1. Signature-based Method:

- Signature-based IDS detects the attacks on the basis of the specific patterns such as number of bytes or number of 1's or number of 0's in the network traffic.
- It also detects on the basis of the already known malicious instruction sequence that is used by the malware.
- The detected patterns in the IDS are known as signatures. Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it is quite difficult to detect the new malware attacks as their pattern (signature) is not known.

Intrusion Detection System

2. Anomaly-based Method:

- Anomaly-based IDS was introduced to detect unknown malware attacks as new malware are developed rapidly.
- In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model.
- Machine learning-based method has a better-generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

Intrusion Detection System

IDS vs Firewall:

- IDS and firewall both are related to network security but an IDS differs from a firewall as a firewall looks outwardly for intrusions in order to stop them from happening.
- Firewalls restrict access between networks to prevent intrusion and if an attack is from inside the network it doesn't signal.
- An IDS describes a suspected intrusion once it has happened and then signals an alarm.

SQL Injection

- Also known as SQLI
- Its an common attack done on any database using SQL CODE which manipulates the background code of any database and reveals sensitive or un intended data.
- This Reveal data can be any costly or private data like user profiles, customers detail etc.
- A successfully implemented attack may result in alteration of data or deletion of entire tables or acquiring administrative rights to database etc. which all are highly hazardous to any organization.

SQL Injection

Example 1

In SQL: `select id, firstname, lastname from authors`

If one provided: `Firstname: evil'ex` and `Lastname: Newman`

the query string becomes:

`select id, firstname, lastname from authors where firstname = 'evil'ex' and lastname ='newman'`

which the database attempts to run as:

`Incorrect syntax near il' as the database tried to execute evil.`

A safe version of the above SQL statement could be coded in Java as:

```
String firstname = req.getParameter("firstname");
String lastname = req.getParameter("lastname");
// FIXME: do your own validation to detect attacks
String query = "SELECT id, firstname, lastname FROM authors WHERE firstname = ? and lastname = ?";
PreparedStatement pstmt = connection.prepareStatement( query );
pstmt.setString( 1, firstname );
pstmt.setString( 2, lastname );
try
{
    ResultSet results = pstmt.execute( );
}
```

Data Encryption

- Its an way to achieve data security by encoding the data so that even if unintended access is done data remains useless for the unauthorized user.
- Here some encryption algorithm is used to encode the data and this encoded data is known as cipher text.
- Basically its an process that only authorized user are only able to read it and its unreadable for unauthorized user.

Data Decryption

- It’s a process to decrypt the cipher text rather saying converting unreadable text to readable or original data.
- As for encryption algorithm is used similarly the same algorithm is designed to decrypt the cipher text in to original data

Types of encryption

- Mainly two types of encryption :

  1) Symmetric key encryption / Private key encryption

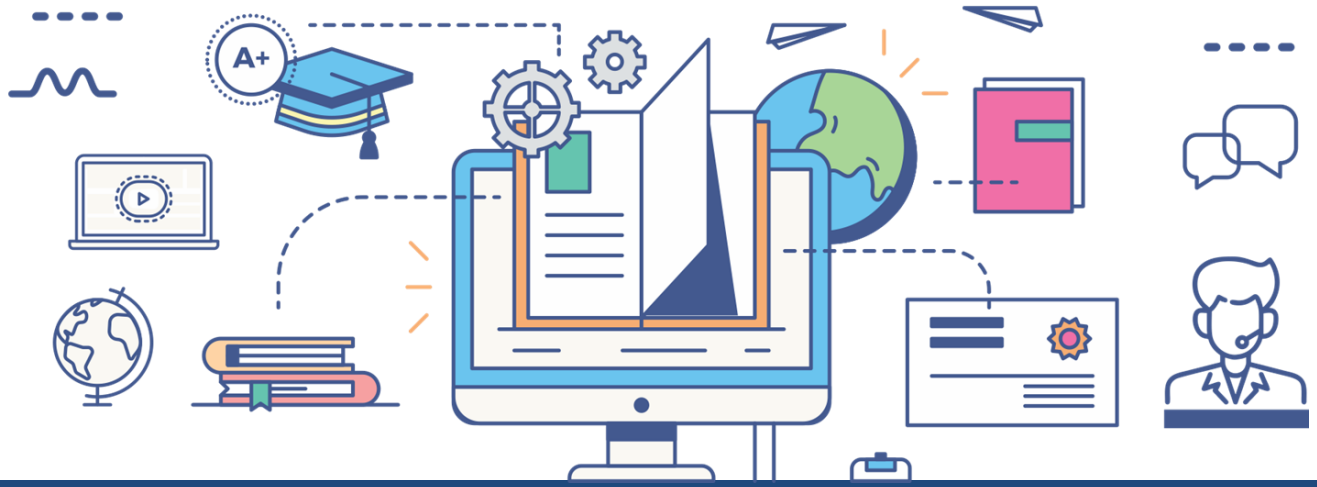
  2) Asymmetric key encryption / Public key encryption

Types of encryption

- Symmetric Key Encryption:-
  - Encryption and decryption key are same.
  - Sender an receiver need to share the key securely.

- Asymmetric Key Encryption:-
  - Encryption and decryption key are different.
  - Encryption is done by the public key of the receiver by the sender.
  - While decryption is done by the receiver by its own private key.

DIGITAL LEARNING CONTENT



Parul® University

www.paruluniversity.ac.in