**Chapter 8: DATABASE SECURITY**

**Data Security**

* Protection from unauthorized access.
* DBA decides who will access what.

**Benefits Data Security Offers**

* Keeps your reputation clean.
* Resists potential damage to client accounts.

**Data Integrity**

* Stable, non-scattered, as it is data.
* Or in simple language, making sure that data is not corrupt.
* It helps keeping data safer.
* Security is built-in during database designing phase.

**Physical Integrity**

* Basic definition of data integrity.
* Can be destroyed in natural disasters, or when electricity goes off.

**Logical Integrity**

* Protection from human error and hackers.

**Access Control**

* Ensures that clients are who they claim to be.
* Three models: **DAC**, **MAC**, **RBAC**

**Discretionary Access Control (DAC)**

* This access is given to creator/owner of the data.
* He controls access control too.
* SQL commands for this are **GRANT**, **REVOKE**.

**Mandatory Access Control (MAC)**

* Here one person does not control everything.
* Access permission is bifurcated to various levels.
* Users at each level have different level of control as per their access.
* Users at higher level have more access to data.
* These permissions include **read & write** operations.

**Role Based Access Control (RBAC)**

* Similar to MAC.
* It is the level of access an employee of an organization has.
* User can only access data that is required to perform his job.
* Access is granted on the basis of authority of the employee.

**Intrusion Detection System (IDS)**

* A safety application.
* Alarms the authority when any malicious activity is noticed.
* Scans for suspicious patterns in network/system.
* **SIEM:** Security information & event management

**Different IDS**

* Network IDS
* Host IDS
* Protocol-based IDS
* Application protocol-based IDS
* Hybrid IDS

**Working of IDS**

* General information chaining order:
  + Internet
  + Router
  + Firewall
  + IDS
  + System
* After information passed through firewall, IDS immediately checks it.

**Detection Methods by IDS**

* **Signature based detection:-**
  + Binary computing **pattern** formed on network traffic.
  + Pre-programmed malicious instruction sequence readings.
  + Signature based detection lacks at detecting new malicious patterns.
* **Anomaly based detection:-**
  + Detects unknown malware attacks.
  + Uses machine learning.
  + These ML models can be trained for particular hardware.

**IDS vs Firewall**

* Firewall looks for **outward** intrusion, IDS looks for **inside** intrusion.
* Firewall restricts access between networks.

**SQL Injection**

* Can alter/ manipulate background code.
* May cost revelation of sensitive/ unintended data.

**Data Encryption**

* Data is made unreadable.
* So that if someone accesses data, it would be useless for him.
* **Cipher text:** Encoded data.
* Readable for authorized users however.

**Data Decryption**

* Uses similar algorithm to encryption.
* Conversion of encrypted data is not same as decrypting data.

**Types of Encryptions**

* **Symmetric key encryption:**
  + Also known as private key encryption.
  + Encryption and decryption have same keys.
  + Sender and receiver must be careful when sharing the key.
* **Asymmetric key encryption:**
  + Also known as public key encryption.
  + Encryption and decryption keys are different.
  + The sender keeps the encryption key.
  + The receiver keeps the decryption key.