6.1 : Types of Security and Threats to Database Systems

IT2306 - Database Systems

Level I - Semester 2

Introduction to Database Security Issues

Types of Security

- Legal and ethical issues
  - Various legal and ethical issues regarding the right to access certain information.
  - Some information may be deemed to be private and cannot be accessed legally by unauthorized organizations or persons.
  - There are several laws governing privacy of information.

Introduction to Database Security Issues

- Policy issues
  - Policy issues at the governmental, institutional, or corporate level regarding what kinds of information should not be made publicly available.

Example : Credit ratings and personal medical records.

Introduction to Database Security Issues

- System related issues
  - System related issues such as the system levels at which various security functions should be enforced.

  Example : Whether a security function should be handled at the physical hardware level, the operating system level or the DBMS level.

Introduction to Database Security Issues

- Multiple security levels
  - The need in some organizations to identify multiple security levels and to categorize the data and users based on these classifications.

  Example : Top secret, secret, confidential, and unclassified.

  - The security policy of the organization with respect to permitting access to various classifications of data must be enforced.

Introduction to Database Security Issues

Threats to databases

- Loss of integrity
  - Database integrity refers to the requirement of protecting information from improper modifications such as creating, inserting, and updating data; changing the status of data; and deleting data.
  - Integrity is lost if unauthorized changes are made to the data by either intentional or accidental acts.
  - If data integrity is continued, use of the contaminated system could result in inaccuracy, fraud, or erroneous decisions.

Introduction to Database Security Issues

- Loss of availability
  - Database availability refers to making objects available to a human user or a program who/which has a legitimate right to those data objects.
  - Loss of availability occurs when the user or program cannot access these objects.

Introduction to Database Security Issues

- Loss of confidentiality
  - Database confidentiality refers to the protection of data from unauthorized disclosure.
  - Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

Introduction to Database Security Issues

- Objectives to be considered when designing a secure database application:
  - Integrity
  - Availability
  - Secrecy