Database Security

Protecting data is at the heart of many secure systems, and many users (people, programs, or systems) rely on a database management system (DBMS) to manage the protection.

A **database** is a collection of data and a set of rules that organize the data by specifying certain relationships among the data.

Security Requirements

- Physical database integrity. The data of a database are immune to physical problems, such as power failures, and someone can reconstruct the database if it is destroyed through a catastrophe.

  .

- Logical database integrity. The structure of the database is preserved. With logical integrity of a database, a modification to the value of one field does not affect other fields, for example.

  .

- *Element integrity.* The data contained in each element are accurate.

  .

- **Auditability.** It is possible to track who or what has accessed (or modified) the elements in the database.

  .

- Access control. A user is allowed to access only authorized data, and different users can be restricted to different modes of access (such as read or write).

  .

- *User authentication.* Every user is positively identified, both for the audit trail and for permission to access certain data.

  .

- Availability. Users can access the database in general and all the data for which they are authorized.

Reliability and Integrity

When software engineers say that software has **reliability**, they mean that the software runs for very long periods of time without failing. Users certainly expect a DBMS to be reliable, since the data usually are key to business or organizational needs. Moreover, users entrust their data to a DBMS and rightly expect it to protect the data from loss or damage. Concerns for reliability and integrity are general security issues, but they are more apparent with databases.

Sensitive data

Sensitive data is confidential information that must be kept safe and out of reach from all outsiders unless they have permission to access it.

Examples of Sensitive Data

Sensitive Personal Data
Protected Health Information (PHI)
Education Records
Customer Information
Card Holder Data
Confidential Personnel Information

What Does Inference Mean?

Inference is a database system technique used to attack databases where malicious users infer sensitive information from complex databases at a high level. In basic terms, inference is a data mining technique used to find information hidden from normal users.

Multilevel Database

Databases that contain objects with different levels of confidentiality and register subjects with different abilities.

Proposals for Multilevel Security

implementing multilevel security for databases is difficult, probably more so than in operating systems, because of the small granularity of the items being controlled.

Separation

Partitioning

Encryption