Data Security Fundamentals

Length: 2 Days

Audience: Application Developers, Database Administrators, Business Analysts, Managers, or anyone concerned with data security.

Prerequisites: Experience working with a relational database system including a basic understanding of SQL.

Overview: This course explores the issues associated with providing database security. In general, database security encompasses logical, physical, and organizational issues. The goal is to provide secrecy, integrity, and availability of data, and address system threats from both insiders and outsiders.

This course provides both a theoretical or conceptual overview of security techniques and mechanisms as well as an applied component addressing approach to implementing security in Oracle and SQL Server systems.

Topics discussed include:

- Motivation for Data Security
  - Potential Risks
  - Internal Security Mechanisms
    - Access
    - Flow
    - Inference
    - Encryption
- Access Control
  - Mandatory Access Control
  - Multilevel Secure Databases
  - Discretionary Access Control
    - Authentication
    - Privileges
    - Grant and Revoke operations
  - Case Study: Oracle
  - Case Study: SQL Server
  - Case Study: DB2
- Inference
  - Inference in General Purpose Databases
  - Inference in Statistical Databases
  - Data mining and Knowledge Discovery
  - Privacy-Preservation Techniques
  - Database Obfuscation
- Data Encryption

- Overview of Data Encryption and Cryptography
- Encryption Algorithms
- Transparent Data Encryption (TDE)
- Column Encryption
- Tablespace Encryption
- Database Encryption
- Case Study: Oracle
- Case Study: SQL Server
- Case Study: DB2