SCS 2209 Database II

Isuru Nanayakkara
University of Colombo School of Computing

Course Content

1. Use access control to secure relational databases – NHP
   i. Introduction to DB security issues
   ii. Discretionary access control based on granting and revoking privileges
   iii. Role Based access control
2. Describe indexing methods – NHP
   i. Types of single level ordered indexes
   ii. Multilevel indexes
3. Explain object relational mapping – NHP
   i. Overview of object DB concepts
   ii. Object relational features

Course Content cont.

4. Explain transaction processing and constraints – HNK
    i. Introduction to transaction processing
    ii. Serializability
    iii. Transaction support in SQL
5. Write stored procedures, constraints and triggers in SQL - HNK
    i. Constraints & Triggers
    ii. Database Stored Procedures
6. NoSQL Data Stores - VL

Learning Objectives

- Use access control to secure relational databases
- Describe indexing methods
- Explain object relational mapping
- Explain transaction processing and constraints
- Write stored procedures and triggers in SQL

Rubric

- Evaluation
  - 70% Final Examination
  - 30% Assignments

- References
  - Fundamentals of Database Systems (6th Edition) RamezElmasri , ShamkantNavathe
  - NoSQL Distilled, by Martin Fowler and Pramod Sadalage (http://martinfowler.com/books/nosql.html)

1.Database Security

Learning Objectives

- Explain the need for security in an organization.
- Identify basic security problems.
- Discuss the types of control measures.
- Discuss techniques for securing databases against a variety of threats.
- Apply schemes of providing access privileges to authorized users'.

Topic Overview

- Introduction to Database Security
- Database security goals and threats
- Security countermeasure
- DBA
- Security vs Privacy
- Security mechanisms
    - Discretionary Security
    - Mandatory and role based security

Introduction to Database Security

- Protect the database from **intentional** or **unintentional** (accidental) **threats**
- **Security Threats**
  - Unauthorized access to data
  - Data alteration
  - Malwares
  - Privilege abuse etc.

Types of Security Issues

- **Legal and ethical issues** regarding right to access information
- **Policy issues** on the kind of information that should not be publicly available at governmental, institutional level etc.
- **System related issues** such as the system levels at which various security functions should be enforced
  - DBMS, OS, HW
- Identify **multiple security levels** and to categorize the data and users based on these classifications

Security Goals - CIA

- Confidentiality - protection of data from **unauthorized disclosure**.
- Integrity - information be protected from **improper modification.**
  - Consistency, accuracy, trustworthiness etc
- Availability - Information requested is **readily available** to **authorized entity.**

- **Database threats violate one or mo**

Activity 01 - CIA

1. A hacker encrypt the whole database
2. DBA uses his account to retrieve the email addresses of co workers to run scams
3. Access to school database and change the grades
4. NMRA incident 2021

Threats to Database

- Loss of confidentiality
  - **Unauthorized, unanticipated, or unintentional disclosure** could result in loss of public confidence, embarrassment or legal action against the organization.
- Loss of integrity
  - Integrity is lost if **unauthorized changes** are made to the data by either **intentional or accidental acts**.
- Loss of availability
  - Making objects **not available** to a human user or a program to which they have a **legitimate right.**

Security Countermeasures

- To protect DB against these types of threats, four kinds of counter measures can be implemented
  - Access control
  - Inference control
  - Flow control
  - Encryption

Access Control

- The security mechanism that **restricts unauthorized access** by handling **user accounts and passwords**
- A security policy that informs;
  - Who are authorized
  - What roles are assigned
- Types of Access Controls
  - Discretionary Access Controls - DAC
  - Mandatory Access Controls – MAC
  - Role Based Access Controls - RBAC

Access Control List

User	Read	Write	Add	Delete
jsmith	x			
rlee	x			
knguyen	x	x	x	x
mroberts	x	x		
manderson	x	x		

Role-Based Access Control

Role	Read	Write	Add	Delete
Reader	x			
Editor	x	x		
Administrato	x	x	x	x

Role Assignments

User	Role
jsmith	Reader
rlee	Reader
knguyen	Admin
mroberts	Editor
manderson	Editor

Inference Control

- Inference control for **statistical databases.**
- Statistical databases are used to provide **statistical information or summaries.**
  - Ex: population statistics DB – statistics based on age, education level, income
- Should **not give access** to the **detailed confidential information** about **specific individuals**.

Flow Control

- Prevents information from **flowing** in such a way that it **reaches unauthorized users.**
- Channels that are **pathways for information to flow implicitly** in ways that **violate the security policy** of an organization are called **covert channels**

Data Encryption

- To **protect sensitive data** that transmit over a communication network.
- Data is **encrypted** using **some encrypting algorithm.**
- Unauthorized user who **accesses encrypted data** will have difficulty deciphering it,
- But authorized users are given **decrypting algorithms** (and keys) to **decrypt the data.**

Database Administrator

- DBA is the **central authority** to manage databases.
- The DBA's responsibilities include **granting privileges to users** who need to **use the system** and **classifying users and data** in accordance with the **policy of the organization**.
- The DBA has a DBA account in the DBMS, sometimes called a system or **super user account**.
- Type of actions
  - Account creation
  - Privilege granting
  - Privilege revocation
  - Security level assignment

Database Administrator Cont.

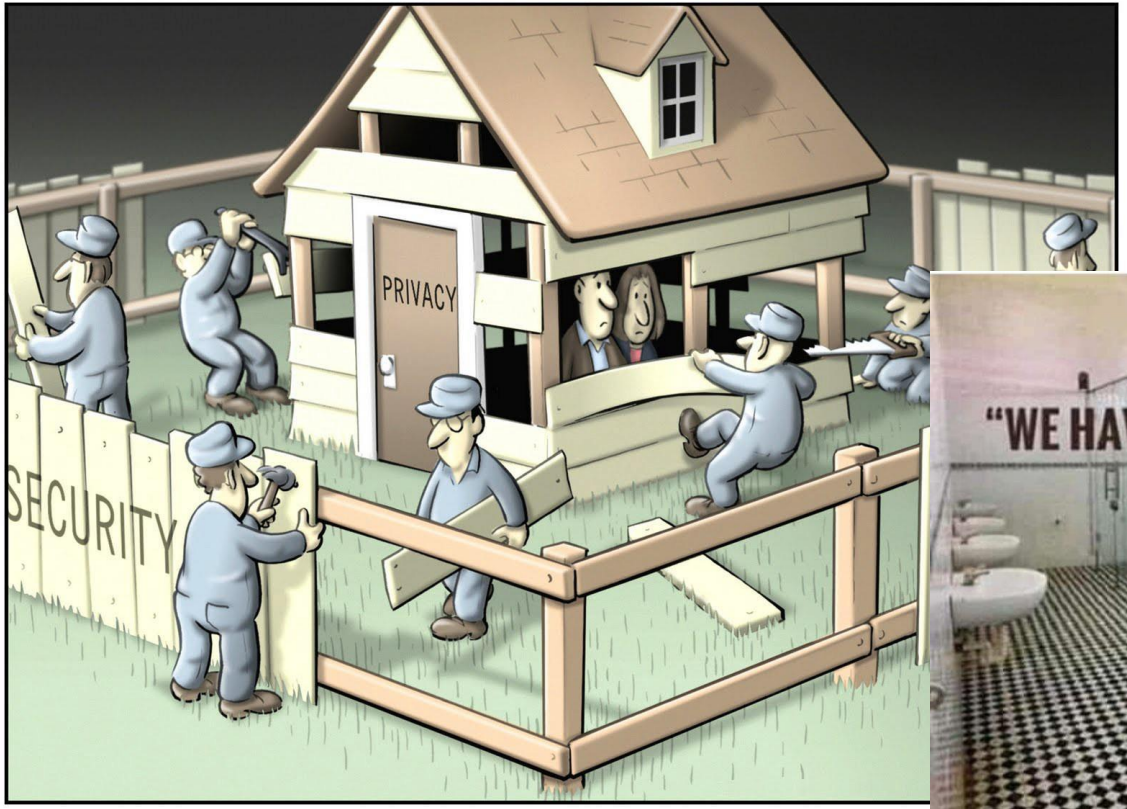
- Provide access through **accounts and login credentials**.
- **Keep track of all actions** by each user through each login session.
  - Ex: User account number, device identity
- System log - includes an **entry for each operation** applied to the database that may be **required for recovery** from a **transaction failure or system crash**
- **Database audit** to identify malicious work
- Audit trail - A database log that is used **mainly for security purposes**

Access to Data

Factors to be considered before revealing data

- Data availability
  - If a user is updating a field, then this field becomes inaccessible and other users should not be able to view this data temporary and only to ensure that **no user sees any inaccurate data.**
- Access acceptability
  - Data should only be **revealed to authorized users**. No sensitive data to unauthorized people.
- Authenticity assurance
  - Before granting access, **certain external characteristics** about the user may also be considered.
  - Ex: Access during working hours

Security Vs. Privacy



Security Vs. Privacy

- Security – Information is **protected from unauthorized** access and modification.
- Privacy - The ability of individuals to **control the terms** under which their personal **information is acquired and used**.
- One basic principle is that people should be informed about information collection, told in advance what will be **done with their information**, and given a reasonable opportunity to approve of such use of the information.

Database Security Mechanisms

- **Database security and authorization** subsystem is responsible for ensuring the **security of portions of a database against unauthorized access.**
- Multiuser database, DBMS must provide techniques to enable **certain users** or **user groups to access selected portions** of a database **without gaining access** to the **rest of the database**.
  - Ex: Salary, Performance reviews

Database Security Mechanisms Cont.

Two types

- Discretionary security
  - used to **grant privileges to users**, including the capability to access specific data files, records, or fields in a specified mode (such as read, insert, delete, or update).
- Mandatory and role based security
  - used to **enforce multilevel security** by classifying the **data and users** into **various security levels**
  - Ex: Role based security

Access Control List

User	Read	Write	Add	Delete
jsmith	x			
rlee	x			
knguyen	x	x	x	x
mroberts	x	x		
manderson	x	x		

Role-Based Access Control

Role	Read	Write	Add	Delete
Reader	x			
Editor	x	x		
Administrato	x	x	x	x

Role Assignments

User	Role
jsmith	Reader
rlee	Reader
knguyen	Admin
mroberts	Editor
manderson	Editor

End of Lecture 01