

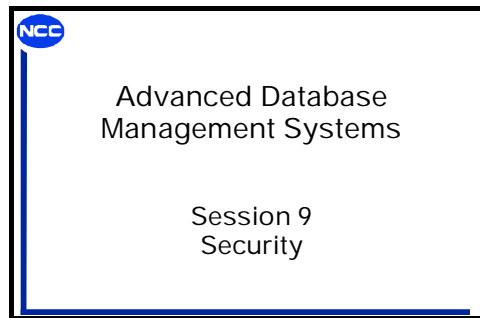
Session 9

Security

1 Introduction

(5 minutes)

V9. 1



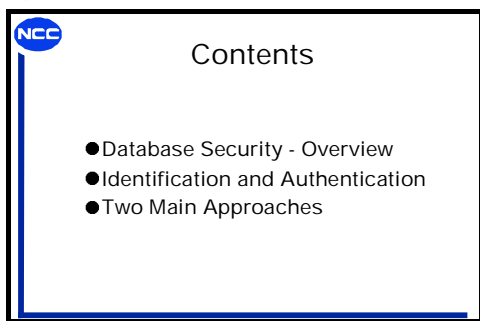
The widespread use of multi-user database systems has certainly increased productivity and efficiency for many organisations. However, it also exposes the organisations to a greater vulnerability to the misuse of databases.

The overall objective of database security is to protect data in the databases against unauthorised use, disclosure, alteration, or destruction.

Inform students that a handout containing a full set of visuals will be provided to them at the end of this lecture.

1.1 Summary of Topics to be Covered

V9. 2



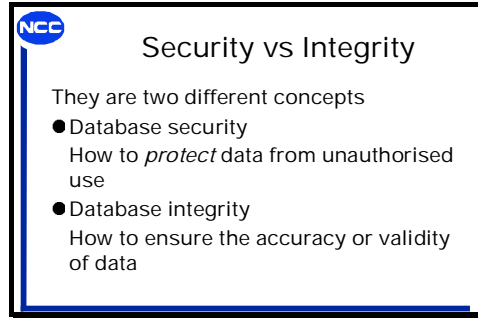
The topics detailed in the visual will be discussed during this session.

2 Database Security - Overview

(20 minutes)

2.1 Security and Integrity

V9.3



Database security and database integrity are two different concepts as described in the visual.

2.1.1 Security

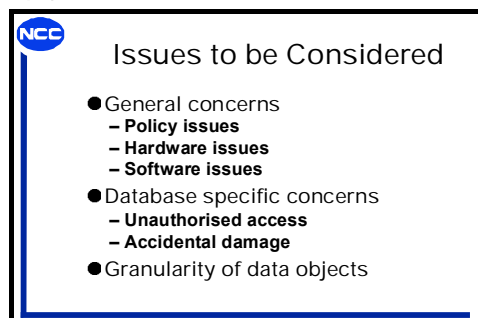
Security deals with the issue of how to protect data from unauthorised use. That is, to ensure that only authorised personnel are permitted to use the database in question, and they do so under the access right control imposed by the system.

2.1.2 Integrity

Integrity deals with how to ensure data in the database remains accurate and valid. That is, to ensure that what the users are permitted to do are correct.

2.2 Issues to be Considered

V9.4



The issues to be considered are as shown in Visual V9.4 and described in more detail now.

2.2.1 General Concerns

There are many issues of general concern. They include:

- *Policy issues* - For example, an organisation has to decide how to protect its database and what scheme to use.
- *Hardware issues* - For example, the physical security of the computer and database has to be ensured, as well as the reliability of the computer hardware.
- *Software issues* - They range from the actual implementation of the security schemes adopted, to the reliability and functions of the operating systems.

2.2.2 Database Specific Concerns

There are issues specific to the database system itself. They include:

- *Unauthorised access* - This refers to unauthorised users attempting to access the database, or authorised users doing unauthorised operations on certain data objects. Therefore, it covers three aspects: user, data and operations.
- *Accidental damage* - This could be a combination of software, hardware and human errors/failures.


2.2.3 Granularity of Data Objects

Depending on the granularity of the security schemes used, the scope of the term *data objects* ranges from the entire database, a set of relations, tuples, to a particular attribute value within a tuple.

3 Identification and Authentication

(10 minutes)

V9. 5



Identification and Authentication

- Before accessing the database users must:
 - **identify themselves**
 - **authenticate their identification**
- Additional identification and authentication may be required during the session

The first facility which should be provided by a database security mechanism, is to check and verify users' identity before accepting them to access the system.

Before accessing the database the user must:


- identify themselves, for example, user-id;
- authenticate their identification, for example, password.

These are the common procedures adopted by systems (for example, bank cashpoint machines). For database systems, additional identification and authentication may be required during the session.

4 Two Main Approaches

(50 minutes)

V9. 6



Two Main Approaches

- Discretionary access control
– **control is exercised by assigning** users different access rights
- Mandatory access control
– **control is exercised by assigning** data objects different classification levels

As pointed out, the purpose of database security is to make sure that only an authorised person can access authorised data objects through a set of authorised operations.

There are many access control methods available to implement database security. They are generally classified into two main approaches (Date), depending on the type of object (user or data) through which the access control is exercised.

- *Discretionary access control* - Control is exercised by assigning users different access rights.
- *Mandatory access control* - Control is exercised by assigning data objects different classification levels.

Modern database systems typically support either or both approaches, but the discretionary control approach is more widely used than the other, due to its flexibility.

4.1 Discretionary Control

There are various methods in this group, different in styles but the same in their approach. We introduce two methods:

- Access matrix;
- Security rules.

4.1.1 Access Matrix

V9. 7

NCC Discretionary Control - 1

Access Matrix - Example

	User	Data Object				
		Table 1	Attribute 1	Attribute 2	Table 2	Attribute 1 etc
A		Select		Update	Select	
B			Select			Update
C					Select	
D					Select Insert	
		*	*	*	*	*
		*	*	*	*	*
		*	*	*	*	*

This method uses a table or tables to specify processing permissions for different users on different data objects. The visual provides an example of this method.

4.1.2 Security Rules

This method is discussed by Date, who uses a hypothetical language to generalise the discretionary control approach.

V9. 8


NCC Discretionary Control - 2

- Definition of Security Rules
 - name
 - privilege
 - scope
 - user-id
 - violation response
- Deletion of Security Rules
- Enforcement of Security Rules

- *Definition of security rules* - This deals with the set-up of security rules for the systems. In this approach, the components for defining access control generally include the following:
 - *Name* - Name of the rule (some systems do not use names for rules), under which the rule is registered in the system catalogue.

- *Privilege* - This specifies which operations are permitted using a GRANT clause. Typical operations are retrieve, insert, update and delete.
- *Scope* - This specifies where the rule applies using an ON clause (for example, some subset of a relation, some tuples, *etc.*).
- *User* - This specifies who is to be granted the specified access right using a TO clause.
- *Violation response* - This specifies the action to be taken in the event of access violation.

V9. 9



Rule Definition Example (Date)

```
CREATE SECURITY RULE SR3
GRANT RETRIEVE (S*, SNAME, CITY), DELETE
ON S WHERE S.CITY <> 'London'
TO FRED, MARY
ON ATTEMPTED VIOLATION REJECT;
```


One example of this rule definition is given by Date:

- *Deletion of security rules* - The deletion of security rules created can be realised by using a DESTROY command.

- *Enforcement of security rules* - The security rules are enforced by a system which checks the user identity before accepting, then checks against the security rules (permissible operations and data objects) assigned to that user. Appropriate actions specified in the rules are taken if an unauthorised access is attempted.

4.2 Mandatory Control

V9. 10



Mandatory Control - 1

Key Points

- Data Object
 - Assigned a classification level
- User
 - Assigned a clearance level
- For retrieve operations
- For update operations

Again, this approach can be generalised into the following key points:

- *Data object* - Each data object is assigned a classification level.
- *User* - Each user is assigned a clearance level.

The scheme works as follows:

- *For retrieve operations* - Users with a clearance level i can only access data objects whose classification level j is less than or equal to i .
- *For update operations* - Users with a clearance level i can only modify data objects whose classification level j is equal to i .

Compared with discretionary control, mandatory control is more rigid.

V9.11

Mandatory Control - 2			
Security Classification - Example			
	Select	Update	Insert
Table 1	2	2	3
Attribute 1	1	2	2
Attribute 2	1	2	3
Table 2	1	1	2
Attribute 1	0	1	1
...

User:	Class
Directors	4 top secret
Senior Managers	3
Managers	2
Authorised clerks	1
Anybody	0

An example of how mandatory control may be implemented is illustrated in the *Security Classification* example shown in Visual V9.11.

5 Summary

(5 minutes)

V9.12

Summary	
● Importance of database security	
● Difference with database integrity	
● Two main approaches:	
– definition	
– implementation	

This session discussed the concept of database security. The emphasis should be on the following points:

- Importance of database security.
- Difference to database integrity.
- Two main approaches: their definition and implementation.

Describe and discuss the security facilities and commands used in the SQL language, since, by this session, students will have considerable knowledge and practice in using SQL.