Managing Data Security

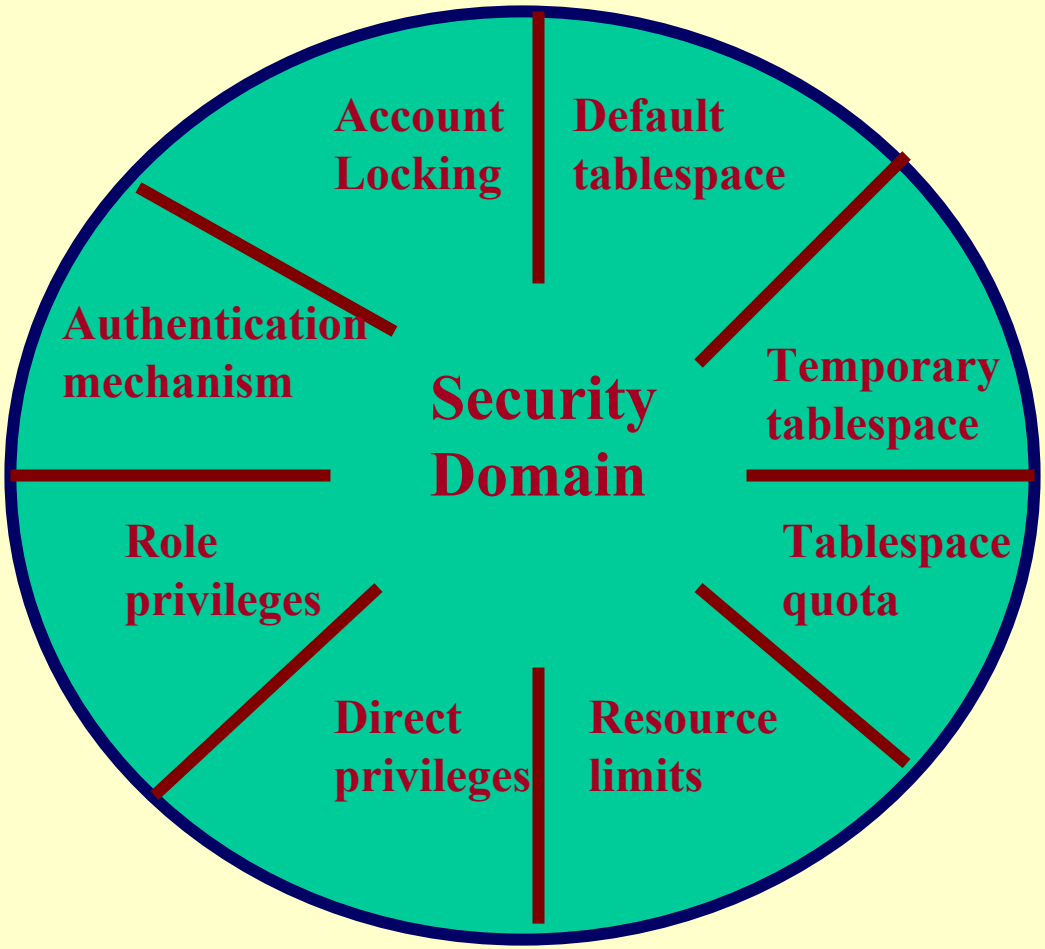
CC Faculty
ALTTC,Ghaziabad

Database Security Aspects

- User Management
- Password Management
- Managing Allocation of Resources to Users
- Backup and Recovery
- Auditing

USER MANAGEMENT

Users and Security



User parameters

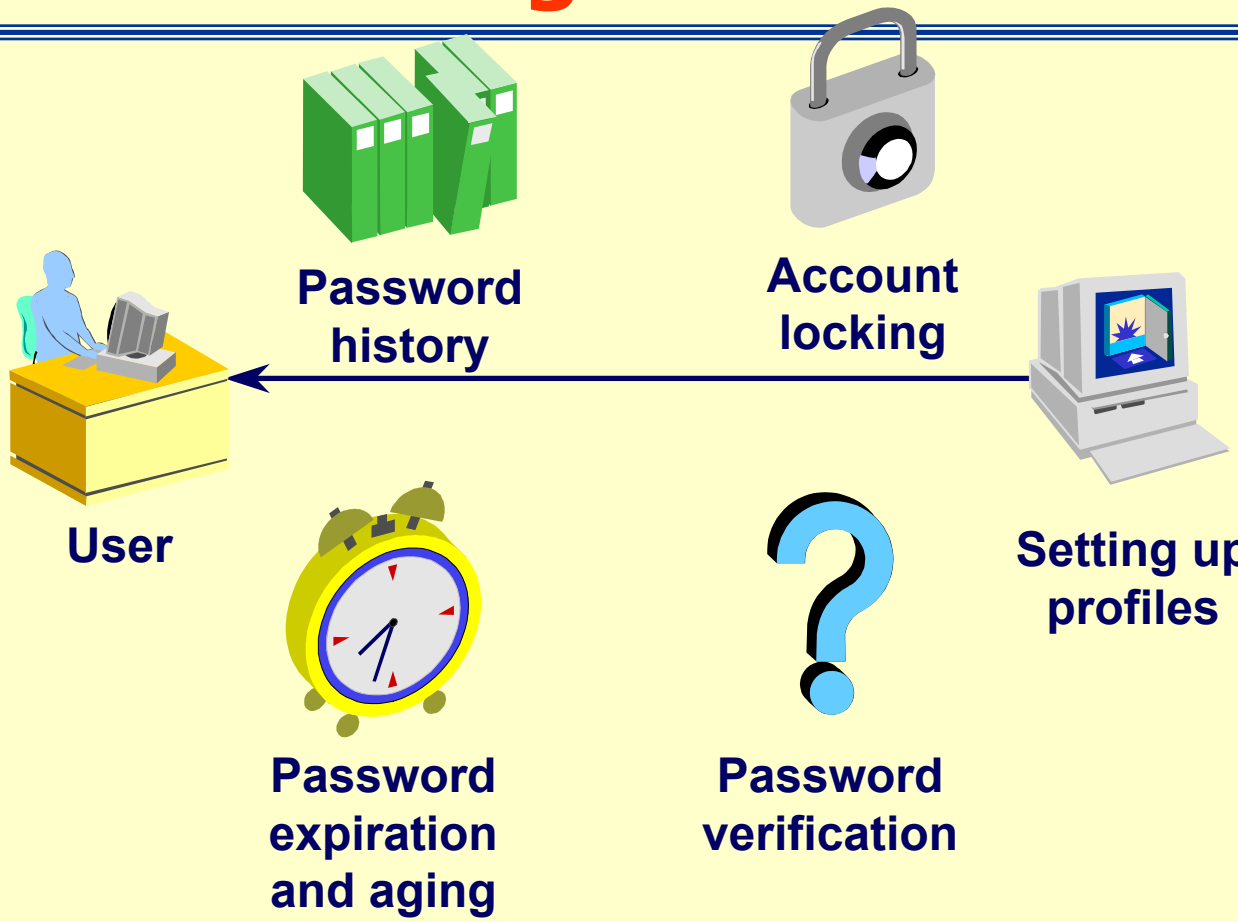
- Authentication at OS level or RDBMS level
- Default space(tablespace)
- Maximum space allocation for user
- Password parameters

Managing Privileges

- System Privileges and Object Privileges

PASSWORD MANAGEMENT

Password Management

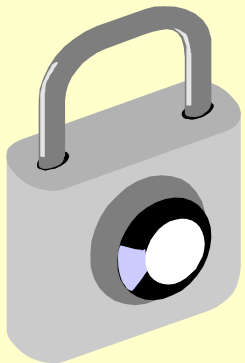


Enabling Password Management

- Set up password management by using profiles and assigning them to users.
- Lock, unlock, and expire accounts using the CREATE USER or ALTER USER command.
- Password limits are always enforced.

Password Account Locking

Parameter	Description
FAILED LOGIN ATTEMPTS	Number of failed login attempts before lockout of the account(3)
PASSWORD LOCK TIME	Number of days the account is locked after the specified number of failed login attempts(1/1440)



Password Expiration and Aging

Parameter	Parameter
PASSWORD LIFE TIME	Lifetime of the password in days after which the password expires(60)
PASSWORD GRACE TIME	Grace period in days for changing the password after the first successful login after the password has expired(10)

Password History

Parameter	Description
PASSWORD REUSE TIME	Number of days before a password can be reused(unlimited)
PASSWORD REUSE MAX	Maximum number of times a password can be reused(unlimited)

Password Verification

Parameter	Description
PASSWORD VERIFY FUNCTION	PL/SQL function that performs a password complexity check before a password is assigned

Password Verification Function

VERIFY_FUNCTION

- Minimum length is four characters.
- Password should not be equal to username.
- Password should have at least one alphabetic, one numeric, and one special character.
- Password should differ from the previous password by at least three letters.

EXAMPLE OF PASSWORD VERIFICATION FUNCTION

```
FUNCTION    my_pwver    (
userid_parameter IN        VARCHAR2 (30),
password_parameter IN        VARCHAR2 (30),
old_password_parameter IN        VARCHAR2 (30)
) RETURN BOOLEAN IS
BEGIN
IF LENGTH(password_parameter ) < 6 THEN
     RAISE_APPLICATION_ERROR(-2001, 'New password too short') ;
ELSE password_parameter = userid_parameter  THEN
     RAISE_APPLICATION_ERROR(-2002, 'New Password Same as username');
ELSEIF password_parameter = old_password_parameter  THEN
          RAISE_APPLICATION_ERROR(-2003, 'New Password same as old');
ELSE
RETURN(TRUE);
END IF;
END;
```

Creating a Profile: Password Settings

```
CREATE PROFILE grace_5 LIMIT
  FAILED_LOGIN_ATTEMPTS 3
  PASSWORD_LOCK_TIME UNLIMITED
  PASSWORD_LIFE_TIME 30
  PASSWORD_REUSE_TIME 30
  PASSWORD_VERIFY_FUNCTION
verify_function
  PASSWORD_GRACE_TIME 5;
```

Altering a Profile: Password Setting

Use ALTER PROFILE to change password limits

```
ALTER PROFILE default LIMIT
FAILED_LOGIN_ATTEMPTS 3
PASSWORD_LIFE_TIME 60
PASSWORD_GRACE_TIME 10;
```

MANAGING ALLOCATION OF RESOURCES TO USERS

Resource Management

- Resource management limits can be enforced at the session level, the call level, or both.
- Limits can be defined by profiles

Setting Resource Limits at Session Level

- Total CPU time measured in hundredths of seconds
- Number of concurrent sessions allowed for each username
- Elapsed connect time measured in minutes
- Periods of inactive time measured in minutes
- Number of data blocks (physical and logical reads)

Setting Resource Limits at Call Level

- CPU time per call in hundredths of seconds
- Number of data blocks that can be read per call

Profiles

- A profile is a named set of password and resource limits.
- Profiles are assigned to users by the CREATE USER or ALTER USER command.
- Profiles can be enabled or disabled.
- Profiles can relate to the DEFAULT profile.

BACKUP & RECOVERY MANAGEMENT

Backup and Recovery Issues

- Protect the database from numerous types of failures
- Increase Mean-Time-Between_Failures (MTBF)
- Decrease Mean-Time-To-Recover
- Minimize Data Loss

Categories of Failures

- Statement Failure
- User Process Failure
- User Error
- Network failure
- Instance Failure
- Media Failure

Defining a Backup and Recovery Strategy

- Business Requirements
- Operational Requirements
- Technical Considerations
- Management concurrence

Business Requirements

- Mean Time to recover
- Mean Time Between Failures
- Evolutionary Process

Operational Requirements

- 24-hour operations
- Testing and validating backups
- Database volatility

Technical Considerations

- Resources: hardware, software, manpower and time.
- Physical image copies of the operating system files
- Logical copies of the objects in the database
- Database configuration
- Transaction volume that affects desired frequency of backups

Disaster Recovery Issues

- How will your business be affected in the event of a major disaster, such as:
  - Earthquake, flood, or fire
  - Complete loss of the machine
  - Loss of key personnel, eg DBA
- Do you have a plan for testing your strategy periodically?

AUDITING

What is Auditing?

- Auditing is the monitoring of selected user data base actions and is used to :-
  - ✓Investigate suspicious database activity
  - ✓Gather information about specific database activities
- Auditing can be performed by session or access

Auditing Guidelines

- Define what you want to audit:
  - Users, statements or objects
  - Statement executions
  - Successful statement executions, unsuccessful or both
- Manage your audit trail
  - Monitor the growth of the audit trail
  - Protect the audit trail from unauthorized access

Auditing categories

- Auditing by default
- Database Auditing
  - Enabled by the DBA
  - Cannot record column values
- Value-based or application auditing
  - Implemented through code
  - Used to track changes to tables

Auditing Options

- Statement Auditing
- Privilege Auditing
- Object Auditing
- Fine-grained auditing provides the monitoring of data access based on content

Thanks!