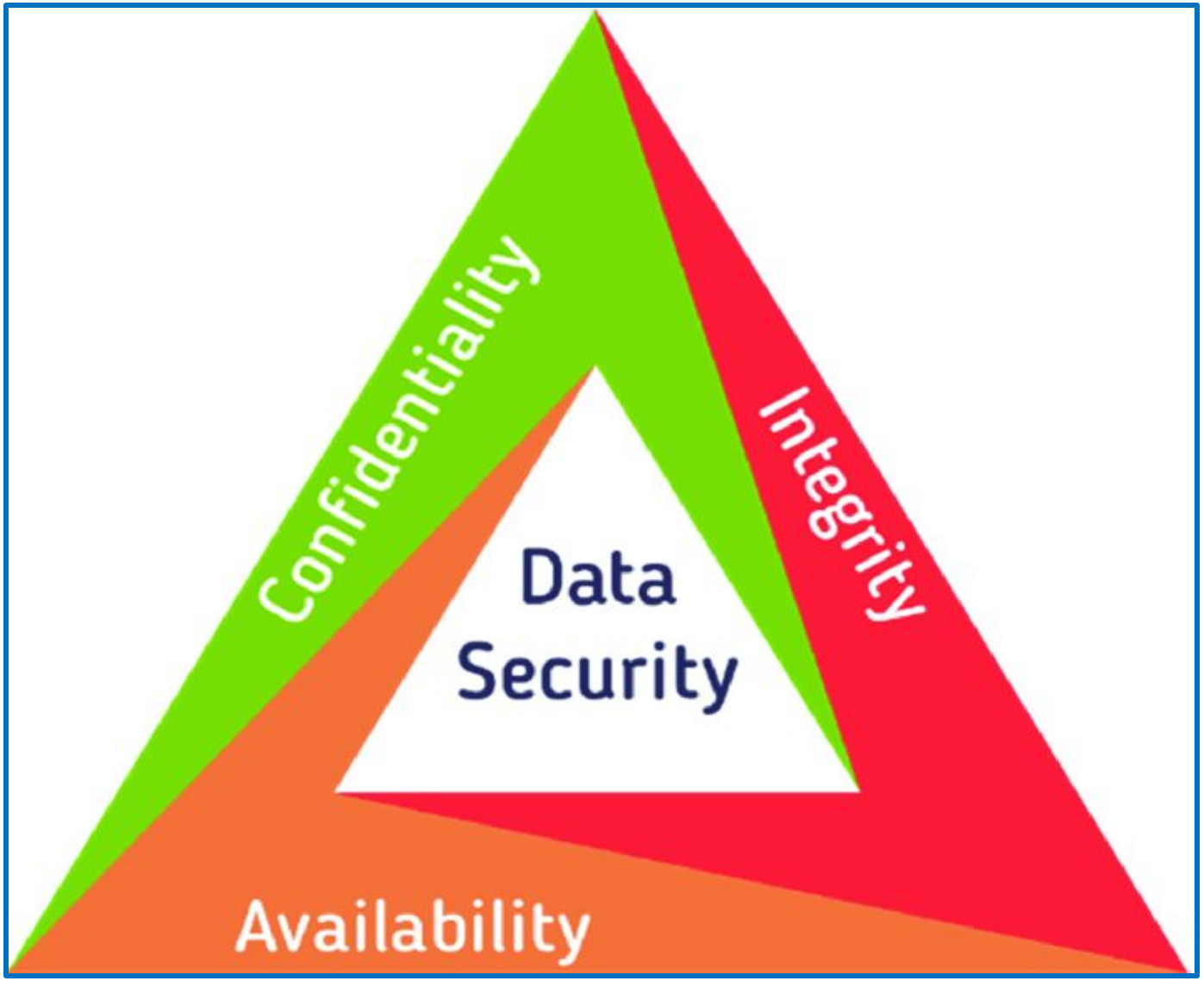
Unit 5. Database Security and Auditing

- Database Security and Auditing;
- Database Authentication Methods;
- Database Authorization Methods;
- Data Encryption Techniques, Virtual Private Database;
- Managing Users and Security: Profiles, managing users, managing privileges, managing roles,


Confidentiality
Integrity
Data
Security
Availability

Database Security

- Database security entails allowing or disallowing user actions on the database and the objects within it. Oracle uses schemas and security domains to control access to data and to restrict the use of various database resources.
- Oracle provides comprehensive discretionary access control. Discretionary access control regulates all user access to named objects through privileges. A privilege is permission to access a named object in a prescribed manner; for example, permission to query a table. Privileges are granted to users at the discretion of other users.

Database Auditing

- **Auditing** is the monitoring and recording of selected user database actions. It can be based on individual actions, such as the type of SQL statement executed, or on combinations of factors that can include user name, application, time, and so on. Security policies can trigger auditing when specified elements in an Oracle database are accessed or altered, including the contents within a specified object.

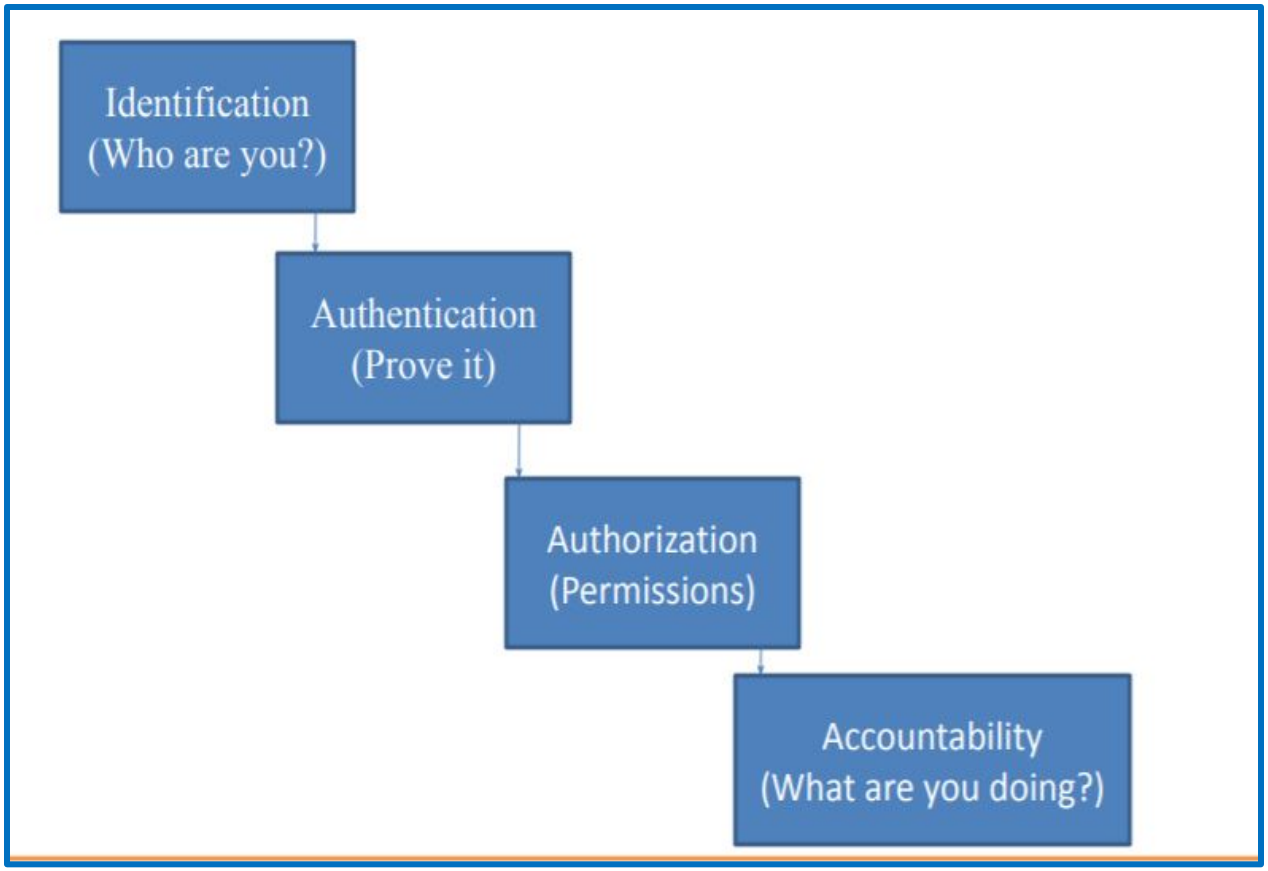
- **Auditing is typically used to:**
  - Enable future accountability for current actions taken in a particular schema, table, or row, or affecting specific content
  - Deter users (or others) from inappropriate actions based on that accountability
  - Investigate suspicious activity
  - Notify an auditor that an unauthorized user is manipulating or deleting data and that the user has more privileges than expected which can lead to reassessing user authorizations
  - Monitor and gather data about specific database activities
  - Detect problems with an authorization or access control implementation

Oracle Database Security Solutions

Defense-in-Depth for Maximum Security

PREVENTIVE	DETECTIVE	ADMINISTRATIVE
Encryption	Activity Monitoring	Privilege Analysis
Redaction and Masking	Database Firewall	Sensitive Data Discovery
Privileged User Controls	Auditing and Reporting	Configuration Management

ORACLE


Identification
(Who are you?)
Authentication
(Prove it)
Authorization
(Permissions)
Accountability
(What are you doing?)

Database Authentication Methods

- Authentication means verifying the identity of someone (a user, device, or other entity) who wants to use data, resources, or applications. Validating that identity establishes a trust relationship for further interactions.
- Authentication also enables accountability by making it possible to link access and actions to specific identities. After authentication, authorization processes can allow or limit the levels of access and action permitted to that entity.

- To validate the identity of database users and prevent unauthorized use of a database user name, you can authenticate using any combination of the methods described in the following sections:
  - Authentication by the Operating System
  - Authentication by the Network
  - Authentication by the Oracle Database
  - Multitier Authentication and Authorization
  - Authentication by the Secure Socket Layer Protocol
  - Authentication of Database Administrators

Authentication by the Operating System

- Once authenticated by the operating system, users can connect to Oracle more conveniently, without specifying a user name or password.
- With control over user authentication centralized in the operating system, Oracle need not store or manage user passwords, though it still maintains user names in the database.
- Audit trails in the database and operating system use the same user names.
- When an operating system is used to authenticate database users, managing distributed database environments and database links requires special care.

Authentication by the Network

- If network authentication services are available to you then Oracle can accept authentication from the network service. If you use a network authentication service, then some special considerations arise for network roles and database links.

Authentication by the Oracle Database

- Oracle can authenticate users attempting to connect to a database by using information stored in that database.
- To set up Oracle to use database authentication, create each user with an associated password that must be supplied when the user attempts to establish a connection. This prevents unauthorized use of the database, since the connection will be denied if the user provides an incorrect password. Oracle stores a user's password in the data dictionary in an encrypted format to prevent unauthorized alteration, but a user can change the password at any time.
- Database authentication includes the following facilities:
  - Password Encryption
  - Account Locking
  - Password Lifetime and Expiration
  - Password Complexity Verification

Multitier Authentication and Authorization

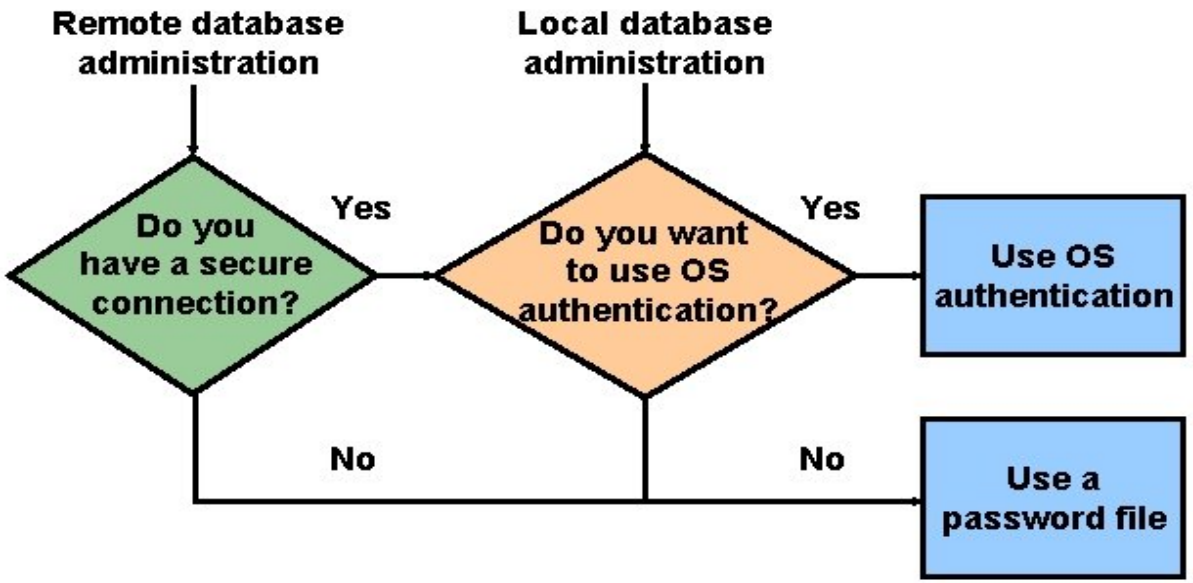
- In a multitier environment, Oracle controls the security of middle-tier applications by limiting their privileges, preserving client identities through all tiers, and auditing actions taken on behalf of clients. In applications that use a heavy middle tier, such as a transaction processing monitor, the identity of the client connecting to the middle tier must be preserved. Yet one advantage of a middle tier is **connection pooling**, which allows multiple users to access a data server without each of them needing a separate connection. In such environments, you must be able to set up and break down connections very quickly.
- For these environments, Oracle database administrators can use the Oracle Call Interface (OCI) to create **lightweight sessions**, allowing database password authentication for each user. This preserves the identity of the real user through the middle tier without the overhead of a separate database connection for each user.
- You can create lightweight sessions with or without passwords. However, if a middle tier is outside or on a firewall, then security is better when each lightweight session has its own password. For an internal application server, lightweight sessions without passwords might be appropriate.

- **Authentication by the Secure Socket Layer Protocol**
  - The Secure Socket Layer (SSL) protocol is an application layer protocol. Users identified either externally or globally (external or global users) can authenticate to a database through SSL.

Authentication of Database Administrators

- Database administrators perform special operations (such as shutting down or starting up a database) that should not be performed by normal database users. Oracle provides a more secure authentication scheme for database administrator user names.
- You can choose between operating system authentication or password files to authenticate database administrators.

Authentication Methods for Database Administrators



ORACLE

- **Database Authorization Methods**
- Authorization is the process where the database manager gets information about the authenticated user. Part of that information is determining which database operations the user can perform and which data objects a user can access.

- **Profiles**
  - In the context of system resources, a profile is a named set of specified resource limits that can be assigned to a valid user name in an Oracle database. Profiles provide for easy management of resource limits.
- **Privilege**
  - A **privilege** is a right to run a particular type of SQL statement or to access another user's object.

There are two distinct categories of privileges:

- System Privileges
  - A system privilege is the right to perform a particular action, or to perform an action on any schema objects of a particular type. For example, the privileges to create tablespaces and to delete the rows of any table in a database are system privileges. There are over 100 distinct system privileges.
- Schema Object Privileges
  - A **schema object privilege** is a privilege or right to perform a particular action on a specific schema object:
  - Different object privileges are available for different types of schema objects. For example, the privilege to delete rows from the departments table is an object privilege.

Roles

- Managing and controlling privileges is made easier by using **roles**, which are named groups of related privileges that you grant, as a group, to users or other roles. Within a database, each role name must be unique, different from all user names and all other role names. Unlike schema objects, roles are not contained in any schema.
- In general, you create a role to serve one of two purposes:
  - To manage the privileges for a database application
  - To manage the privileges for a user group

Data Encryption Techniques

- Encryption is a process of transforming plaintext (unencrypted data) to ciphertext (encrypted data) so that only people having a secret key (formally known as the decryption key) can have access to that encrypted data and will be able to decode the information.
- Data encryption is a popular security method used by organizations for protecting an organization's data.
- There are several data encryption approaches available to choose from. Most internet security (IS) professionals break down encryption into three distinct methods: symmetric, asymmetric, and hashing. These, in turn, are broken down into different types. We'll explore each one separately.

Virtual Private Database

- Virtual Private Database (VPD) is a database security feature that is built into an Oracle database server, as opposed to being part of an application that is accessing the data. The user is only allowed to see the data they have been given permission to see.
- VPD uses application contexts to provide row-level security and fine-grained access control based on a company's security policies. Application contexts are simply key value pairs that are created in a defined namespace. VPD was first introduced in Oracle8i.

- Example: A customer can only see his orders in the 'orders' table (below), when he is listed in the 'customers' table (below)

CUST_FIRST_NAME	CUST_LAST_NAME	CUSTOMER_ID
Matthias	Hannah	106

ORDER_DATE	CUSTOMER_ID	ORDER_TOTAL
31-AUG-99 09.19.37.811132 AM	105	22150.1
20-MAR-96 05.18.21.862632 PM	106	5546.6
01-AUG-00 10.22.48.734526 AM	106	2075.2
31-AUG-99 08.53.06.008765 PM	107	70576.9

Thank You