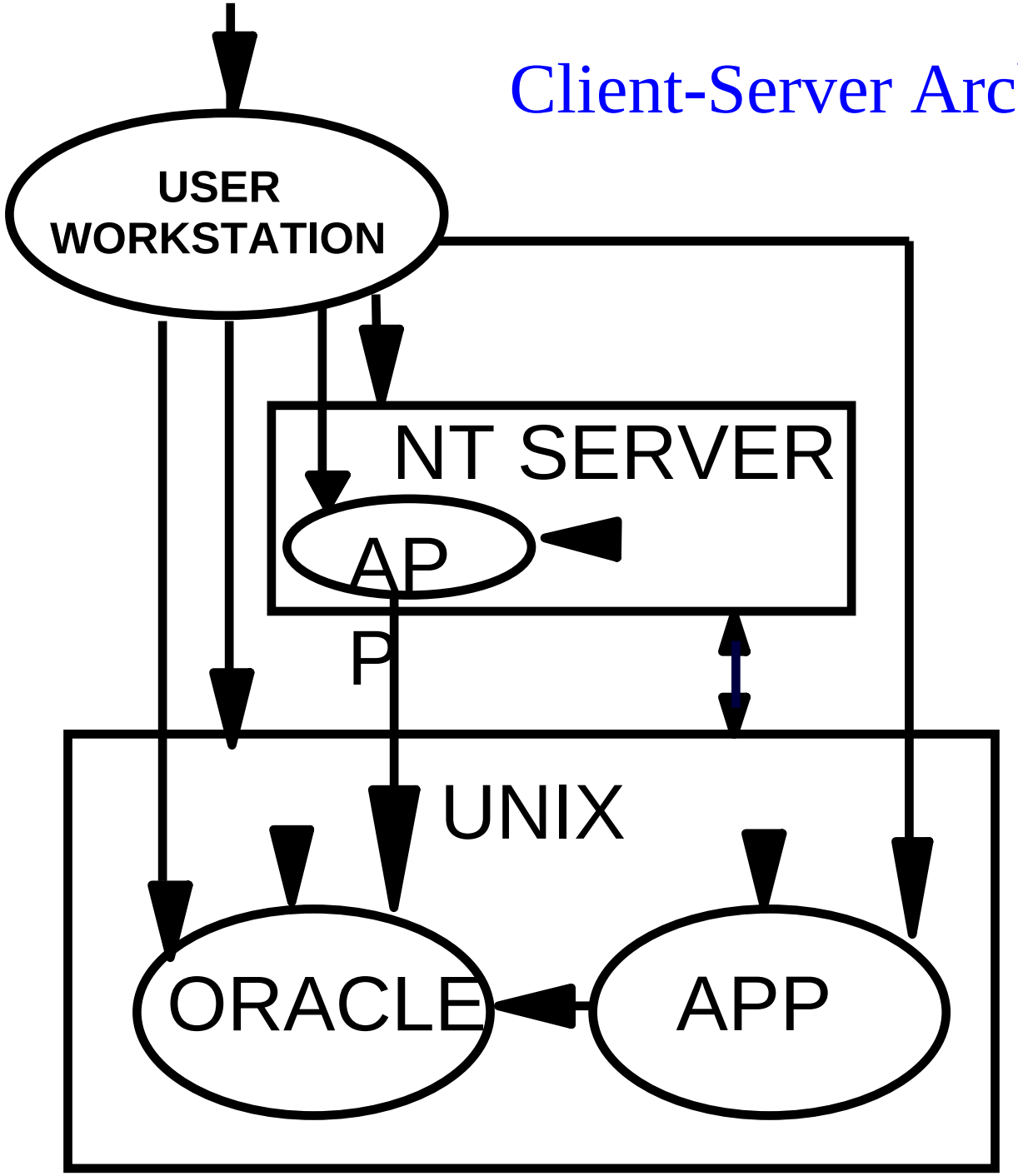
Oracle Database Control Issues

Jennifer L. Bayuk
jennifer_bayuk@attcapital.com

AT&T Capital Corporation

Client-Server Architecture

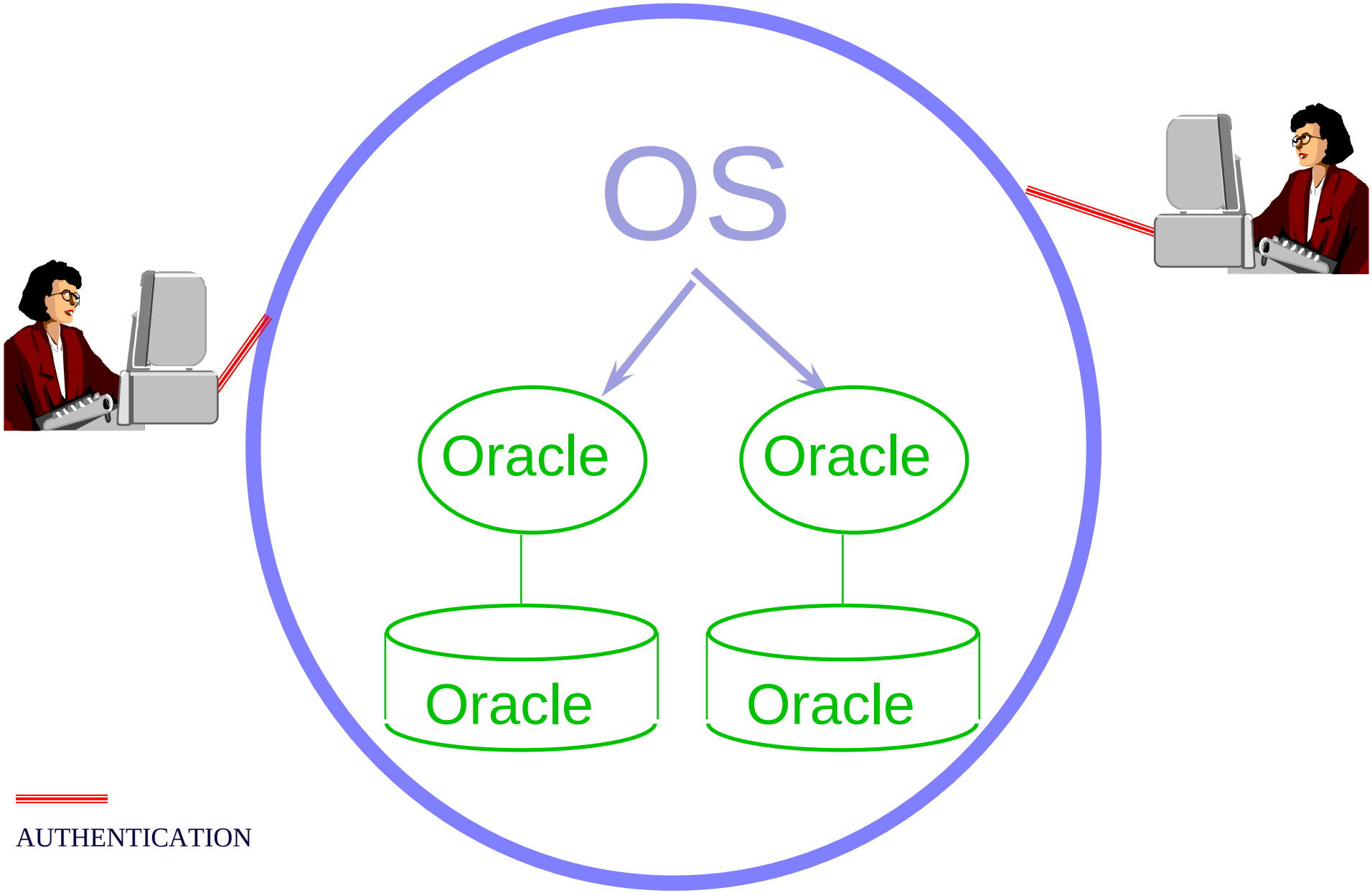


Connectivity Option

Access Control Option

AT&T Capital Corporation

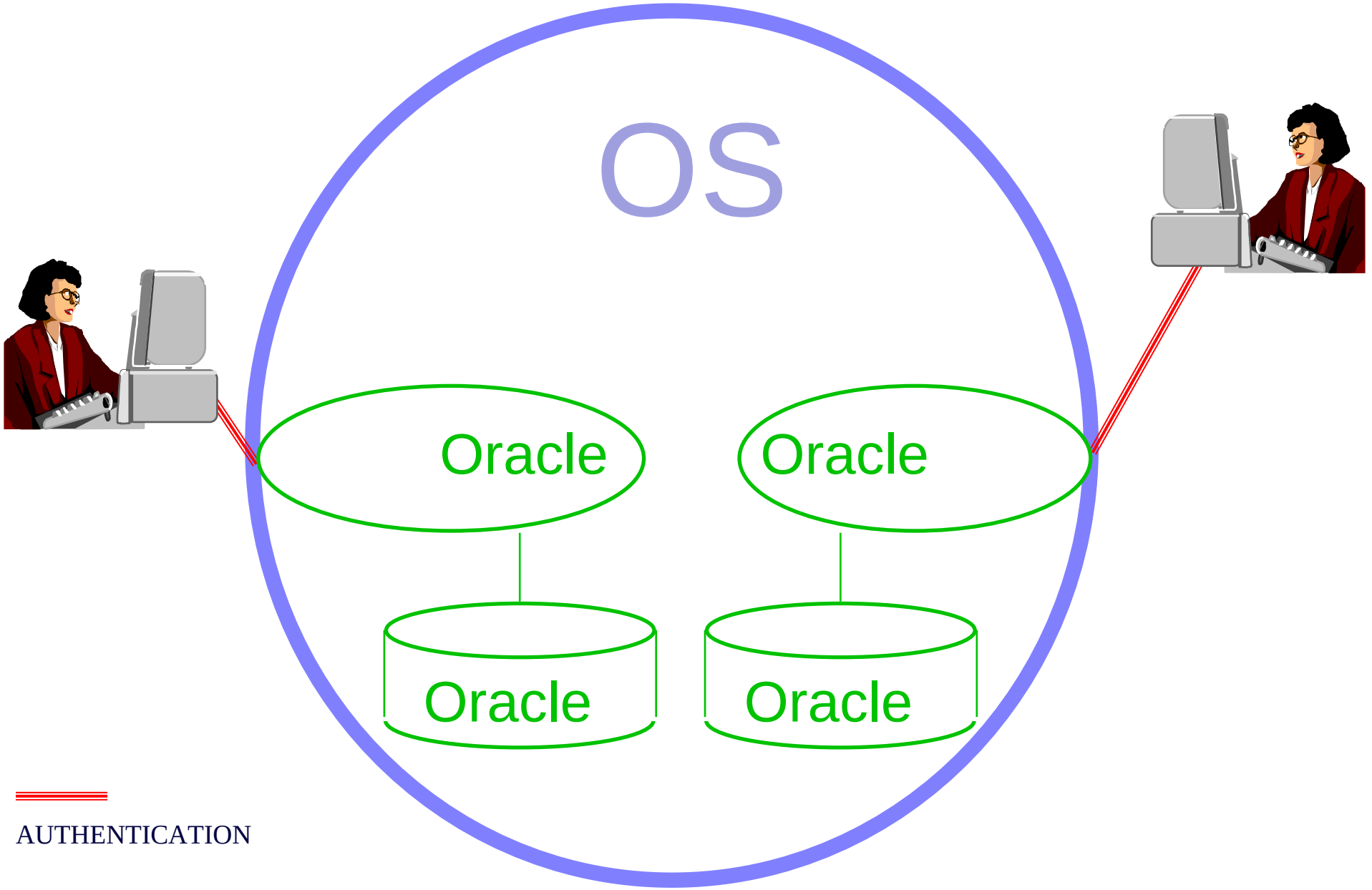
Architecture Example 1: Host-based Access Control



AUTHENTICATION

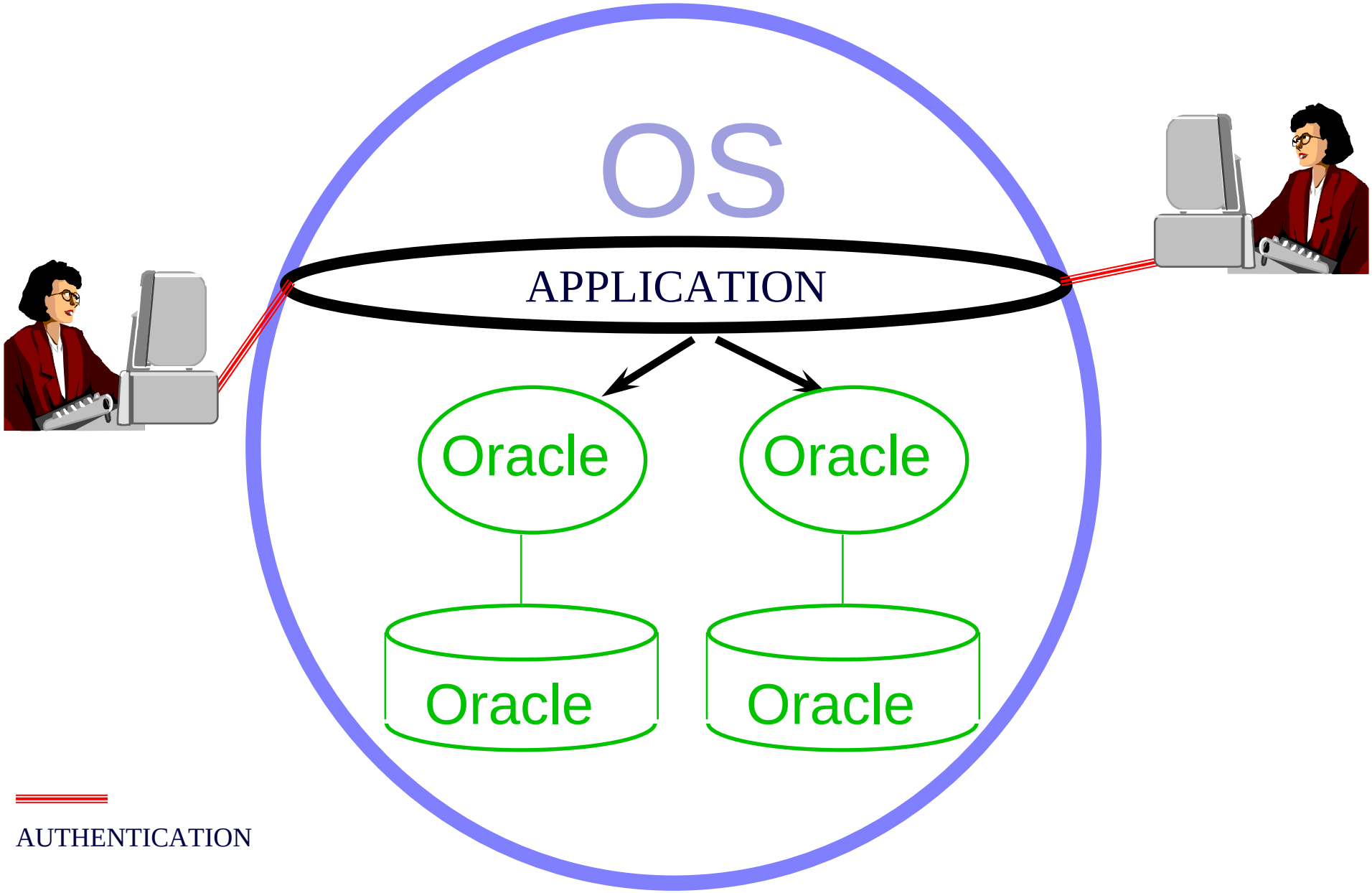
AT&T Capital Corporation

Architecture Example 2: DBMS-based



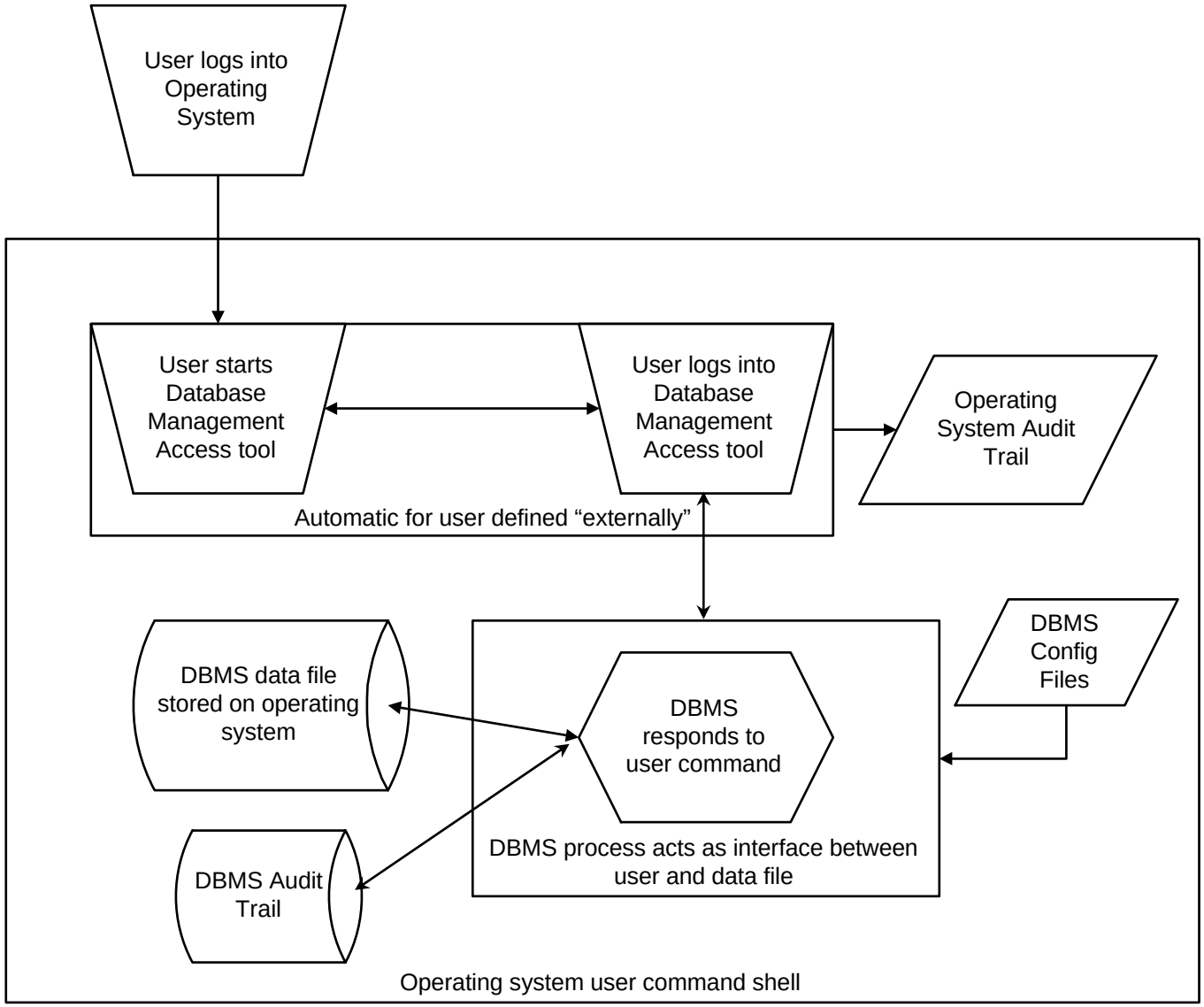
AUTHENTICATION

Architecture Example 3: Application-based

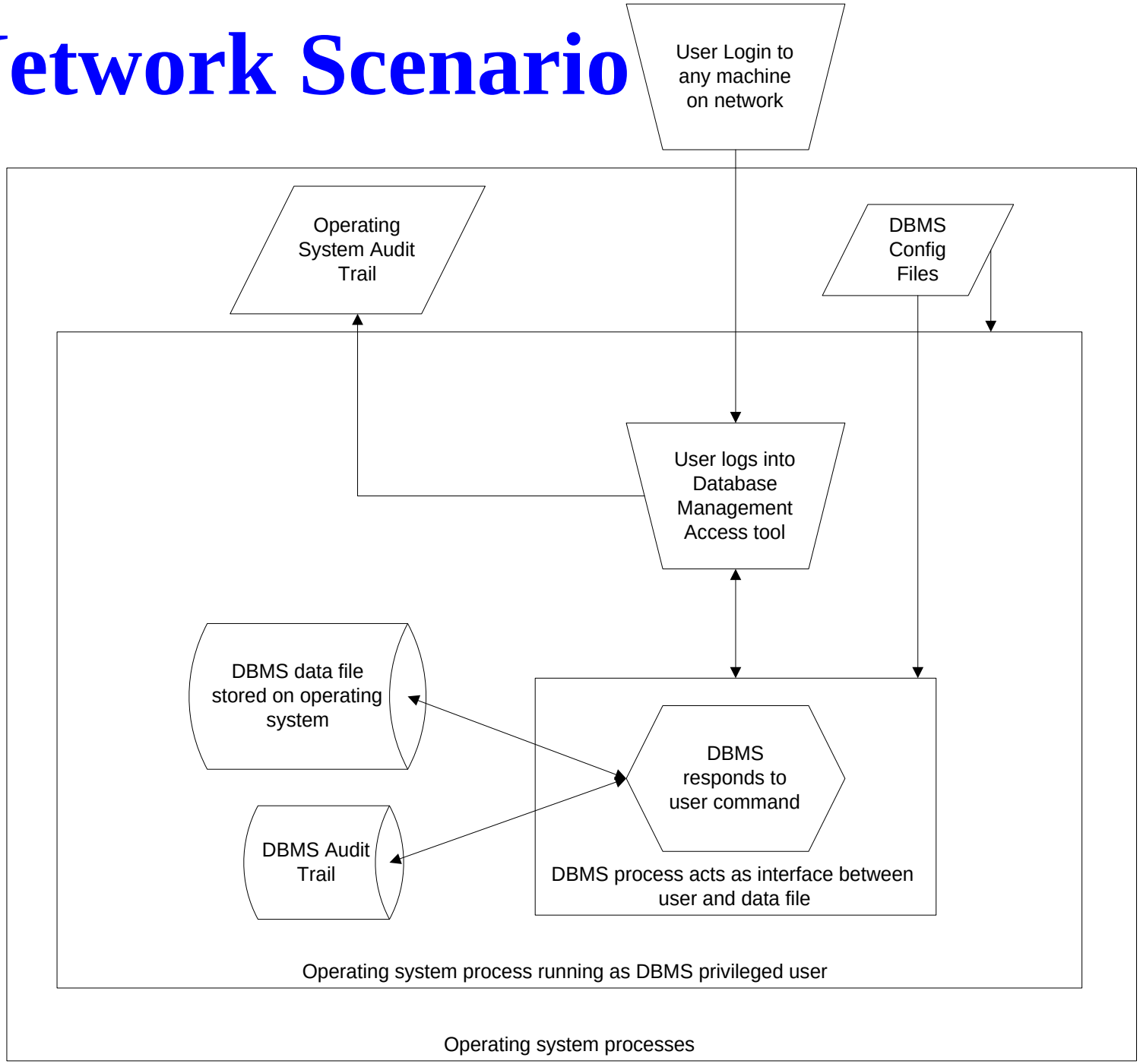


AUTHENTICATION

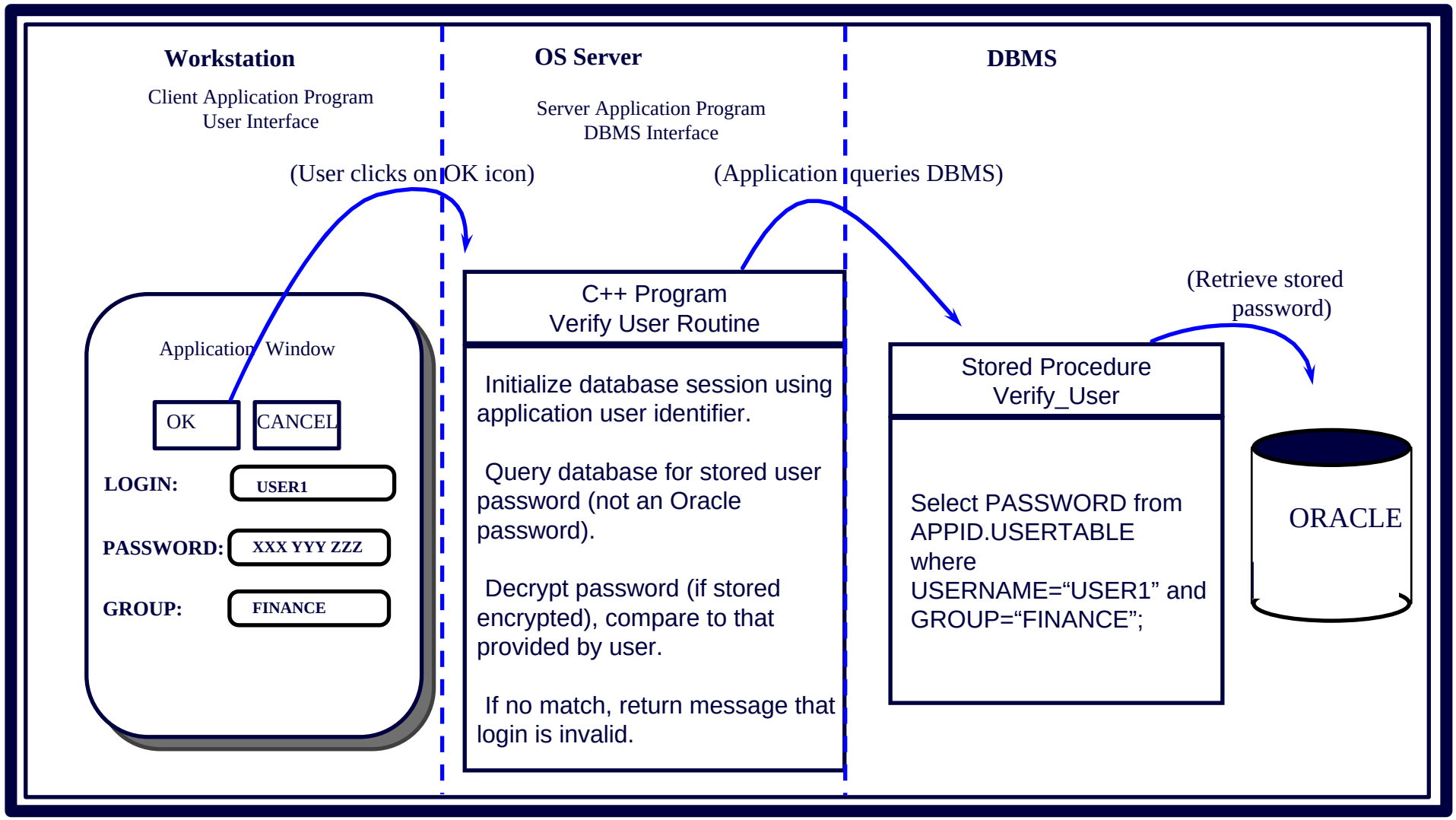
Operating System Scenario



Network Scenario



Application Scenario



AT&T Capital Corporation

Operating System Security vs Oracle Security

- Operating System
  - Rights to restrict, execute and/or manipulate Oracle program files
  - Rights to copy, rename, or delete Oracle data files stored as OS files
- Oracle
  - Rights to tables within Oracle data files
  - Rights to create and execute procedures that manipulate table structure and data

Oracle Access Control Issues:

- Applications embed security in code rather than database
- Non-application-controlled database access can result in corruption of transaction data
- DBMS generic application user access may be uncontrolled
- Database management systems transmit all transactions, data, user IDs and passwords in cleartext, vulnerable to Network analysis (sniffer) software
- Standard installation contain generic passwords
  - sys/change_on_install
  - system/manger
  - scott/tiger

Access Control using Roles

- Oracle DBAs may create any number of roles

- Oracle roles (groups) may be assigned any set of permissions

- Users may be assigned to multiple roles.

- Application privilege assignments may not correspond to Oracle role assignments (but they should)

Access Control using Application Handshakes

Stored procedure key-based authentication

- Prevents users from running stored procedures from a command line

Implementations

- Code conditional into procedure or trigger that forbids execution unless it is passed a secret key from the application
- Code conditional into procedure or trigger that forbids execution if process ID does not = application name.

Access Control using Product User Profiles

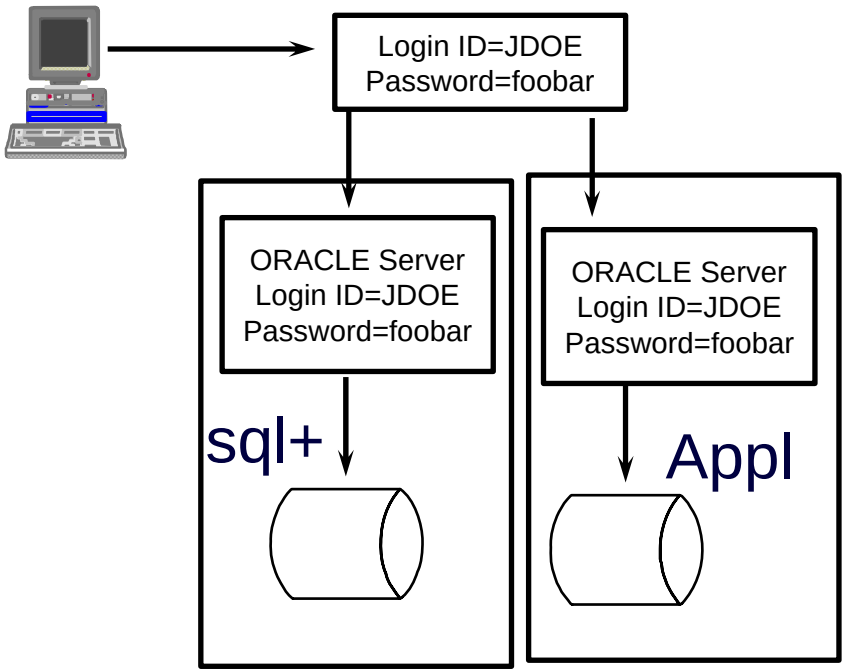
Can be used to limit ad-hoc access by SQL-Plus
- Enforced by SQL-Plus, not by Oracle.
- May be used where operating system access is granted to users with no database access.

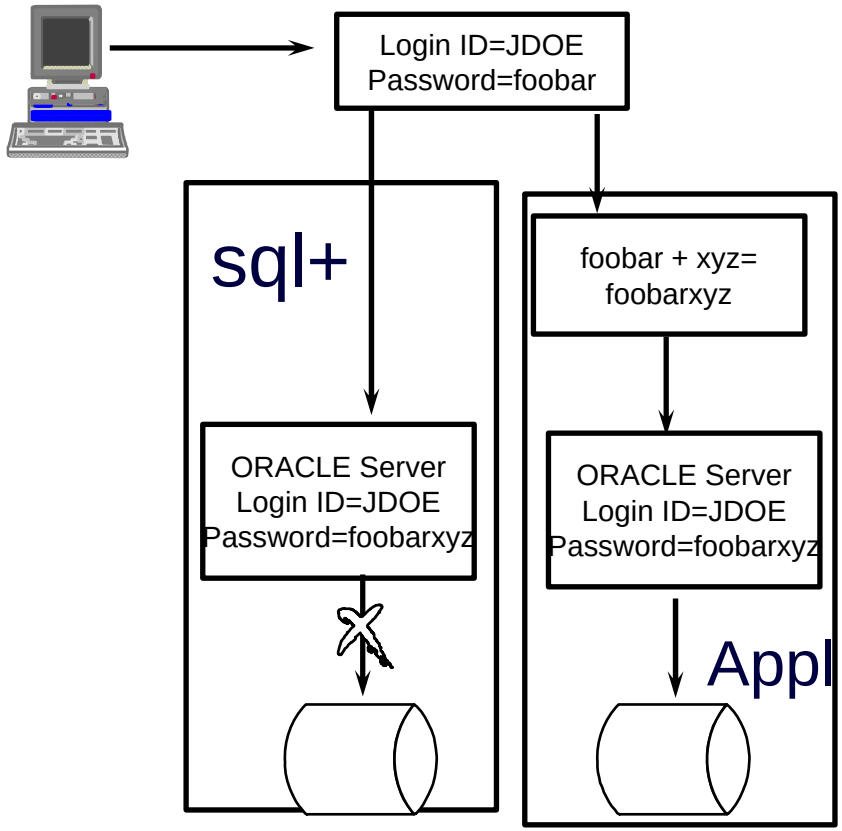
```
select * from sys.product_user_profile;

PRODUCT    USERID     ATTRIBUTE    SCOPE    NUMERIC VALUE  CHAR VALUE  DATE VALUE
---------- ---------- ------------ -------- -------------- ----------- ----------
SQL*Plus   JDOE       GRANT                                 DISABLE
SQL*Plus   JSMITH     AUDIT                               D DISABLE
SQL*Plus   JSMITH     SET ROLE                            D DISABLE
SQL*Plus   %          INSERT                              D DISABLE
SQL*Plus   %          UPDATE                              D DISABLE
SQL*Plus   %          DELETE                              D DISABLE
SQL*Plus   %          SELECT                              D DISABLE
SQL*Plus   ROLES                                          D CLERK
SQL*Plus   ROLES                                            ADMIN
```

Access Control using Password Masking

Protects from ad-hoc access to stored procedures and database tables. Will not protect against spoofing of application access.

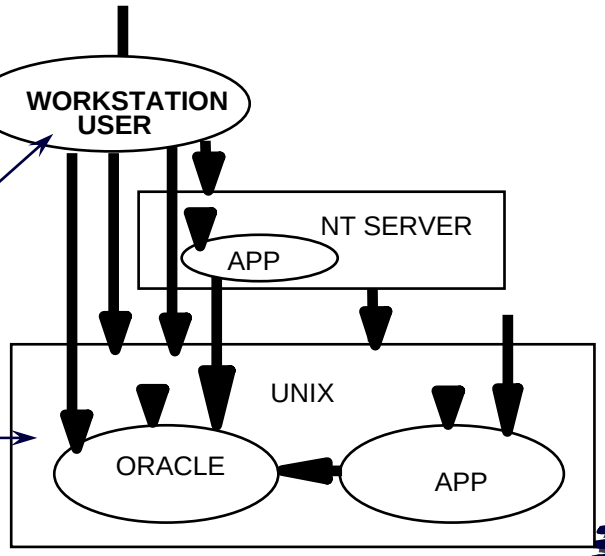




Common Sense
Access Control Mechanisms

- Always change initial passwords.
- Wherever possible, change the names of all generic accounts or disable them and grant the necessary privileges to an account of a different name.
- Use token or biometric authentication devices if network is unsecure.
- Use hardware or software encryption if disclosure is also an issue.

Note: in order for token, biometrics or encryption controls to work, the encryption and decryption of the authentication string or data must be here:
and here:
Not all on one side or in the middle!
Do not assume this is the case!



Detection: Oracle Audit Systems

Problems:

- Default configuration has all auditing disabled
- Comprehensive audit requires considerable CPU and storage

Solution:

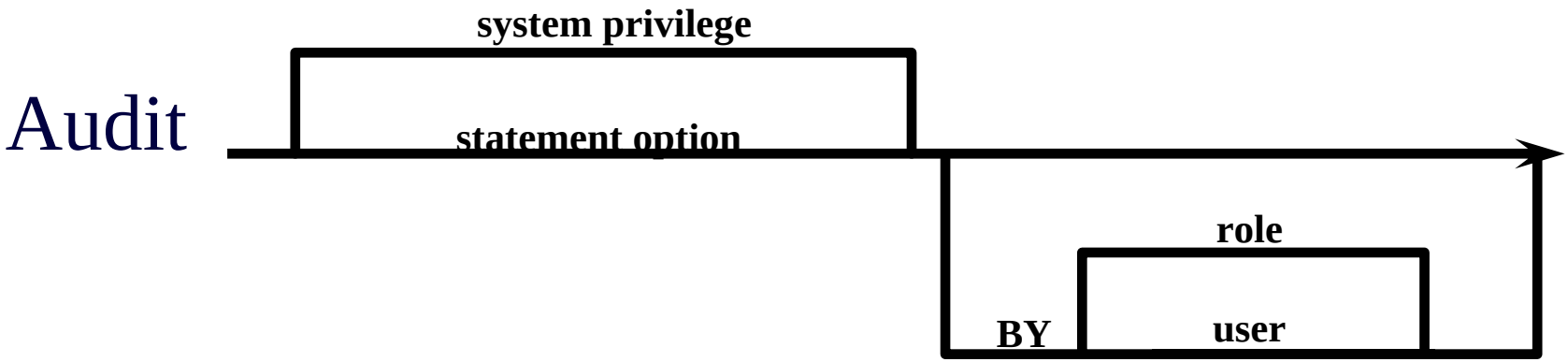
develop targeted monitoring via a combination of:

- System-level audits
- Object-level audits
- Statement-level audits

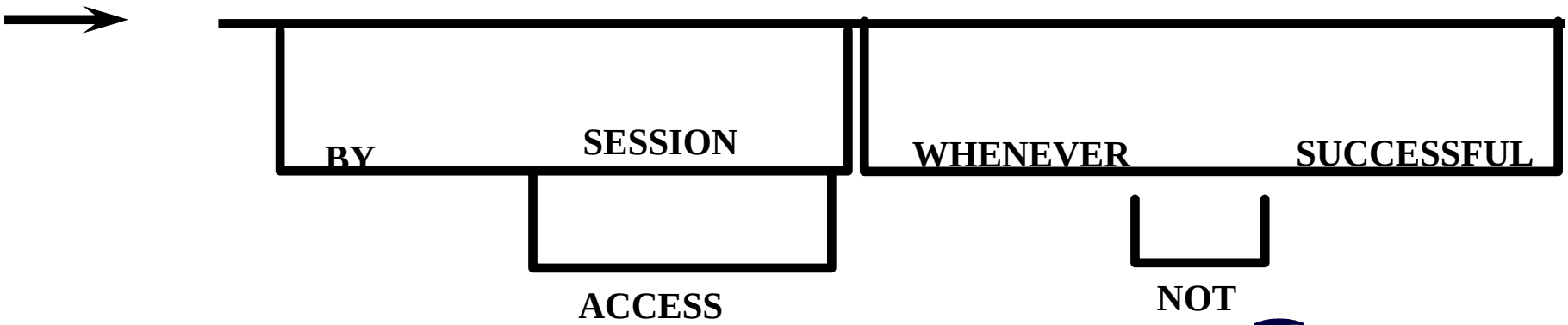
Types of Oracle Audits

- System
  - Audits of activity other than data access
- Object
  - Audits that are recorded whenever a given object is accessed
- Statement
  - Audits record commands issued (not necessarily that they were issued successfully)
  - Recommended for very critical functions and all database administrator actions.

Detection Options:



Audit <privilege> on Object



Oracle Recovery

Challenges:

- Database operation relies on operating system and application configuration
- Operating system backup may not cover most recent database transactions

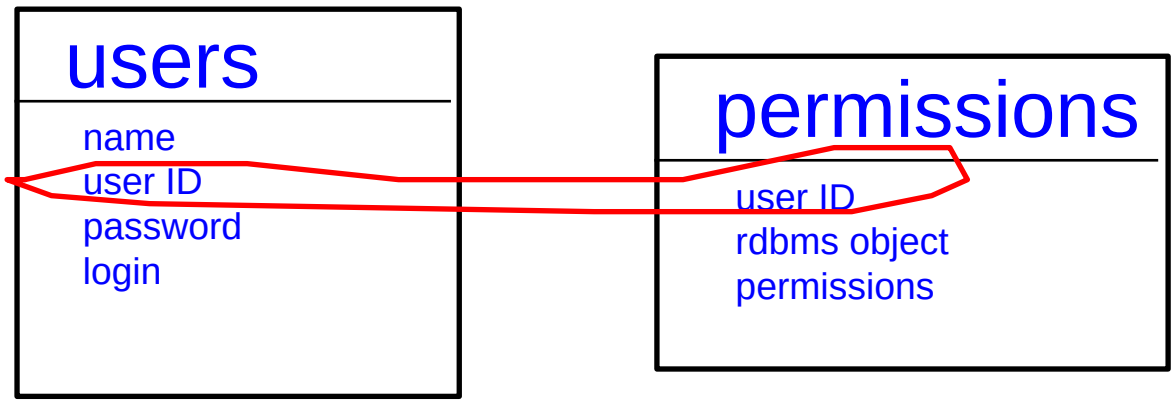
Backup must include:

- Operating System backup
- Application backup
- Data file backup
- Transaction-based backup

Transaction-based backup

- Database transactions are written to a separate file in addition to the database itself: a **transaction log**
- If the database is corrupted, and no current backup exists, transaction logs may be applied to a database backup rather than re-entering all data since last backup. Data will restored to the time of the last available transaction log.
- To ensure recoverability:
  - Ensure the transaction log is updated well within the minimum recovery time interval required.
  - Periodically back up the transaction log
  - Ensure that the transaction log is backed up before it is truncated.

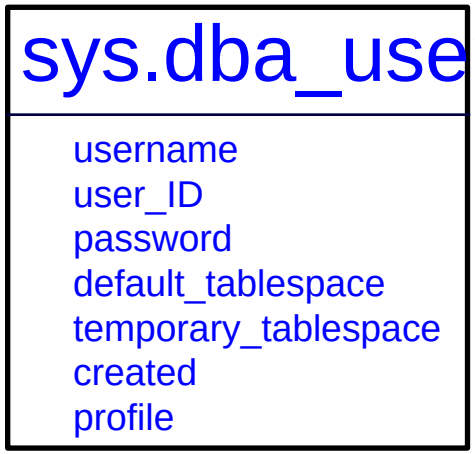
INFORMATION ON CONTROLS WITHIN ORACLE



IS STORED JUST LIKE THE RELATIONAL DATA

AT&T Capital Corporation

Oracle table of users: sys.dba_users



Question:

How to use an RDBMS to list this data?

ANSWER: SQL

SQL (Structured Query Language)

Select Statement

select **X** from **Y**

X=column name of data item

Y=table name

select **username** from **sys.dba_users**

SQL (Structured Query Language)

More about the Select Statement

select **Y.X** from **Y,Z where Y.X=Z.X**

Y=table name

Z=table name

X=column name of data item where the
value of the data is the same in both tables **Y** and **Z**

Y.X = the column **X** in the table **Y**
Z.X = the column **X** in the table **Z**

Oracle SQL query tool is “sqlplus”.
e.g.: ***sqlplus <username>***

To look at users:
```
select username,profile,password,user_id,created from sys.dba_users order by username;
```
To look at profiles:
```
select distinct profile from sys.dba_profiles order by profile;
select * from sys.dba_profiles order by profile;
```
To look at roles:
```
select distinct grantee,role,admin_option,default_role,password_required from sys.dba_roles,
sys.dba_role_privs where sys.dba_roles.role=sys.dba_role_privs.granted_role order by grantee;
```
To look at system privileges granted to users:
```
select * from sys.dba_sys_privs order by grantee;
```
To look at table privileges:
```
select table_name,privilege,grantee,grantable from sys.dba_tab_privs;
```
To look at column privileges:
```
select table_name,column_name,privilege,grantee,grantable from sys.dba_col_privs;
```
To look at audit options:
```
select user_name,audit_option,success,failure from sys.dba_stmt_audit_opts;
```
To look at system privilege audit options:
```
select * from sys.dba_priv_audit_opts;
```
To look at object privilege audit options:
```
select * from sys.dba_obj_audit_opts
where  (ALT != '-/-') or (AUD != '-/-') or (COM != '-/-') or (DEL != '-/-') or (GRA != '-/-')
or (IND != '-/-') or (INS != '-/-') or (LOC != '-/-') or (REN != '-/-') or (SEL != '-/-')
or (UPD != '-/-') or (REF != '-/-') or (EXE != '-/-') order by owner,object_type;
```
To read Oracle audit options:
< Whenever successful >/<Whenever not successful>
S = By session, A= By access

To look at statement audit options:

```
select * from sys.dba_stmt_audit_opts;
```

AT&T Capital Corporation