Database Security

Objectives

- The scope of database security.
- Why database security is a serious concern for an organization.
- The type of threats that can affect a database system.
- How to protect a computer system using computer-based controls.
- The security measures provided by Microsoft Office Access and Oracle DBMSs.
- Approaches for securing a DBMS on the Web

Database Security

- Data is a valuable resource that must be strictly controlled and managed, as with any corporate resource.

- Part or all of the corporate data may have strategic importance and therefore needs to be kept secure and confidential.

Database Security

- Mechanisms that protect the database against intentional or accidental threats.

- Security considerations do not only apply to the data held in a database. Breaches of security may affect other parts of the system, which may in turn affect the database.

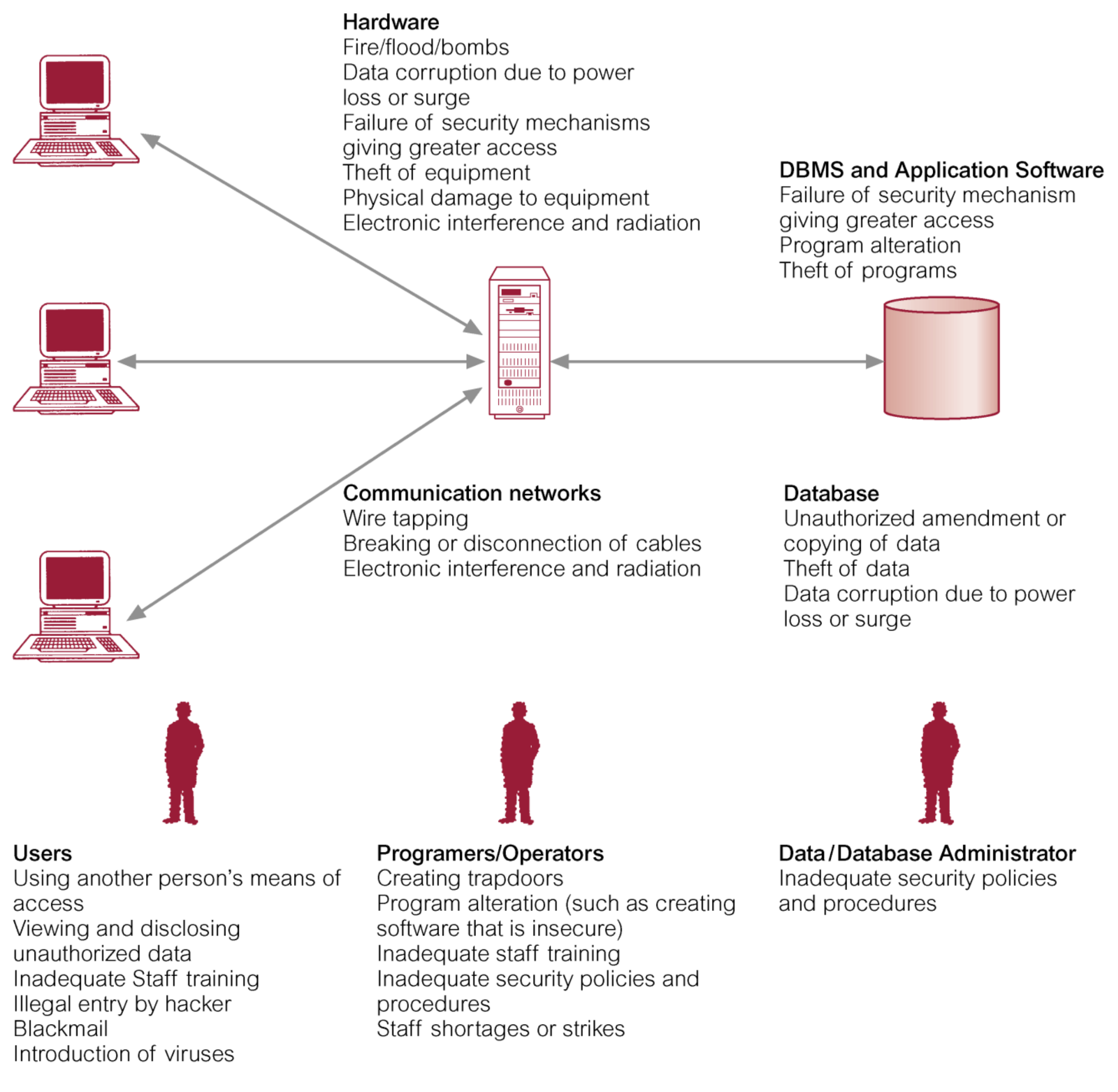
Database Security

- Involves measures to avoid:
  - Theft and fraud
  - Loss of confidentiality (secrecy)
  - Loss of privacy
  - Loss of integrity
  - Loss of availability

Database Security

- Threat
  - Any situation or event, whether intentional or unintentional, that will adversely affect a system and consequently an organization.

Summary of Threats to Computer Systems



Hardware
Fire/flood/bombs
Data corruption due to power loss or surge
Failure of security mechanisms giving greater access
Theft of equipment
Physical damage to equipment
Electronic interference and radiation

DBMS and Application Software
Failure of security mechanism giving greater access
Program alteration
Theft of programs

Communication networks
Wire tapping
Breaking or disconnection of cables
Electronic interference and radiation

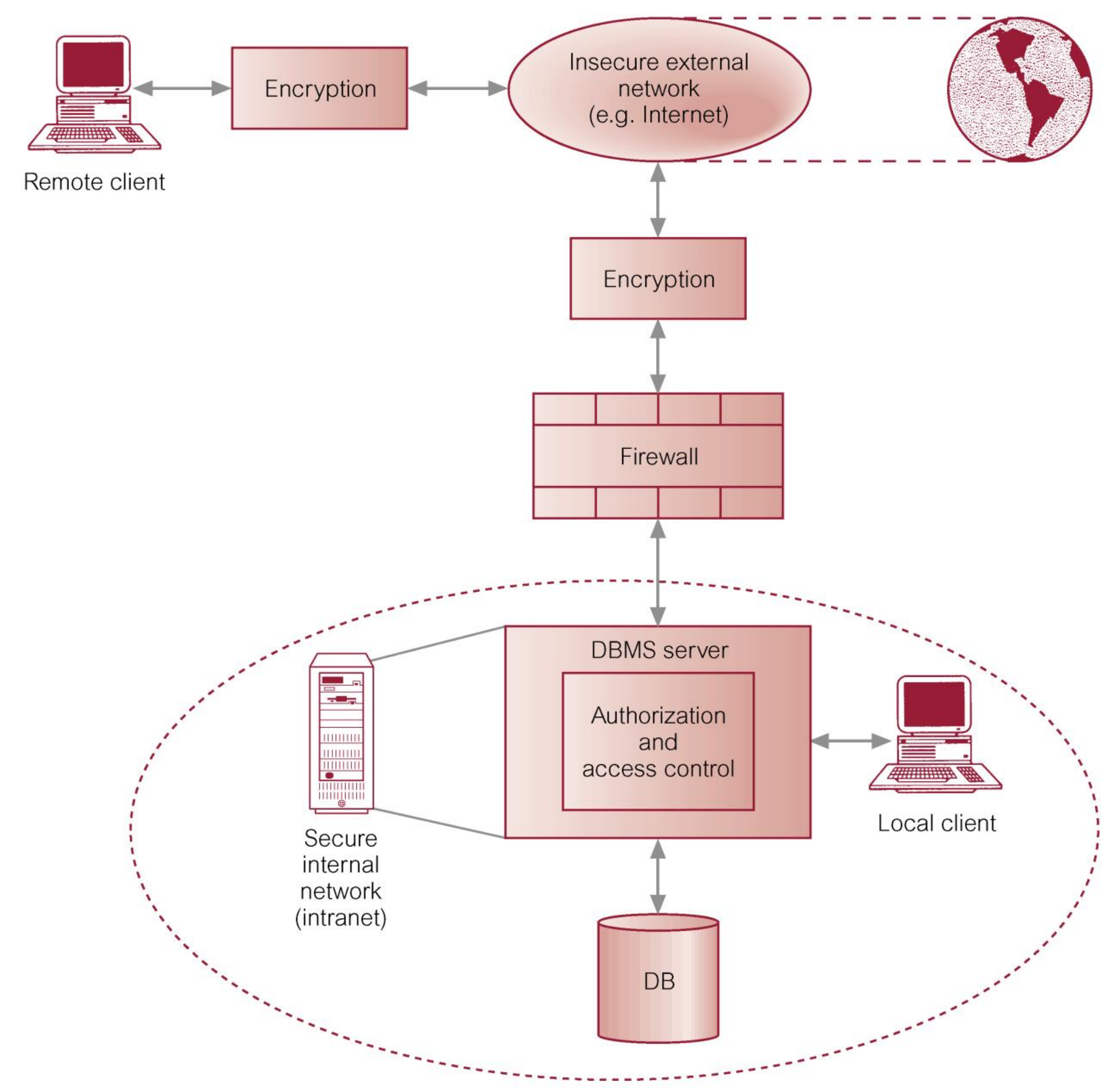
Database
Unauthorized amendment or copying of data
Theft of data
Data corruption due to power loss or surge

Users
Using another person's means of access
Viewing and disclosing unauthorized data
Inadequate Staff training
Illegal entry by hacker
Blackmail
Introduction of viruses

Programers/Operators
Creating trapdoors
Program alteration (such as creating software that is insecure)
Inadequate staff training
Inadequate security policies and procedures
Staff shortages or strikes

Data/Database Administrator
Inadequate security policies and procedures

Typical Multi-user Computer Environment


Remote client
Encryption
Insecure external network (e.g. Internet)
Encryption
Firewall
DBMS server
Authorization and access control
Local client
Secure internal network (intranet)
DB

Countermeasures – Computer-Based Controls

- Concerned with physical controls to administrative procedures and includes:
  - Authorization
  - Access controls
  - Views
  - Backup and recovery
  - Integrity
  - Encryption
  - RAID technology

Countermeasures – Computer-Based Controls

- Authorization
  - The granting of a right or privilege, which enables a subject to legitimately have access to a system or a system’s object.
  - Authorization is a mechanism that determines whether a user is, who he or she claims to be.

Countermeasures – Computer-Based Controls

- Access control
  - Based on the granting and revoking of privileges.
  - A privilege allows a user to create or access (that is read, write, or modify) some database object (such as a relation, view, and index) or to run certain DBMS utilities.
  - Privileges are granted to users to accomplish the tasks required for their jobs.

Countermeasures – Computer-Based Controls

- Most DBMS provide an approach called Discretionary Access Control (DAC).
- SQL standard supports DAC through the GRANT and REVOKE commands.
- The GRANT command gives privileges to users, and the REVOKE command takes away privileges.

Countermeasures – Computer-Based Controls

- DAC while effective has certain weaknesses. In particular an unauthorized user can trick an authorized user into disclosing sensitive data.

- An additional approach is required called Mandatory Access Control (MAC).

Countermeasures – Computer-Based Controls

- DAC based on system-wide policies that cannot be changed by individual users.
- Each database object is assigned a *security class* and each user is assigned a *clearance* for a security class, and *rules* are imposed on reading and writing of database objects by users.

Countermeasures – Computer-Based Controls

- **DAC determines whether a user can read or write an object based on rules that involve the security level of the object and the clearance of the user. These rules ensure that sensitive data can never be 'passed on' to another user without the necessary clearance.**

- **The SQL standard does *not* include support for MAC.**

Mandatory Security Mechanism or **Multi-Level Security (MLS)**

- MLS is used to enforce multi-level security by classifying the data and the users into various security classes.

- The need for Multi-Level Security (MLS) exists for Government, Military and Intelligent Applications, and Industrial and Corporate environments.

- There are specific hardware standards/levels available (A,B,C,D) – the Department of Security requires specific hardware and customer software to enforce this.

Mandatory Security Mechanism or **Multi-Level Security (MLS)**

Typical Security levels

- Top Secret (TS),
- Secret (S),
- Confidential (C)
- Unclassified (U).

TS is the highest priority with **U** being the lowest priority.

Mandatory Security Mechanism or **Multi-Level Security (MLS)**

Bell_LaPadula Model –

- they published paper on multi-level security where they give definition of the typical security levels.

BLM classifieds each **subject** (user, account, and program) and **object** (relation, tuple, attribute, view…) into one of the security classifications (TS,S,C,U).

Classification of subject	class(s)
Classification of object	class(o)

Mandatory Security Mechanism or **Multi-Level Security (MLS)**

Two restrictions apply on data access on the class(s) and class(o).

- **<u>Simple property</u>**: A subject S is not allowed read access to an object O unless class(s) is greater than or equal to (=>) class(o)
- **<u>Star property</u>**: A subject S is not allowed write access to an object O unless class(s) is less than or equal (<=) to class(o).

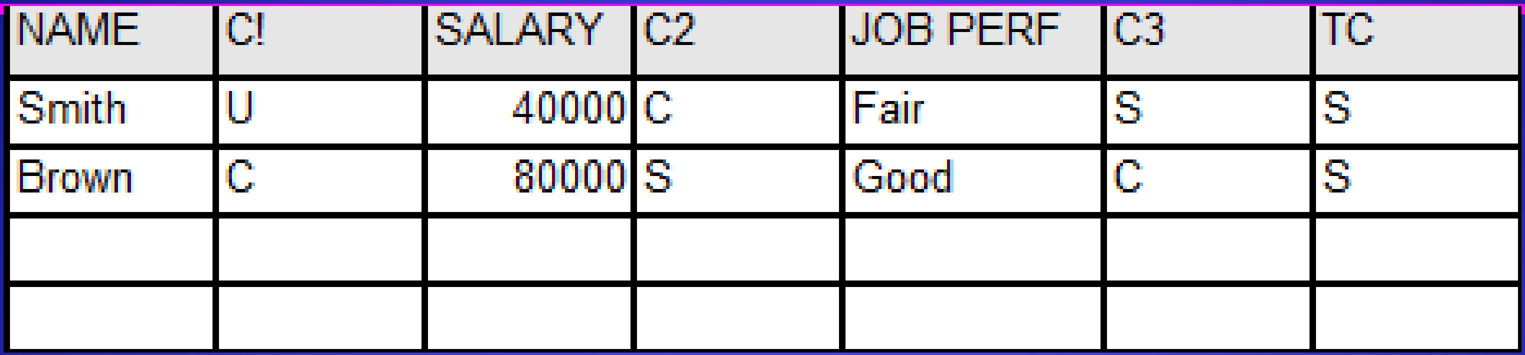
We have to merge classification with relation:

- R(A1(S),A2(c1),A3(c2),CZ(c3)…An, Cn, TC)

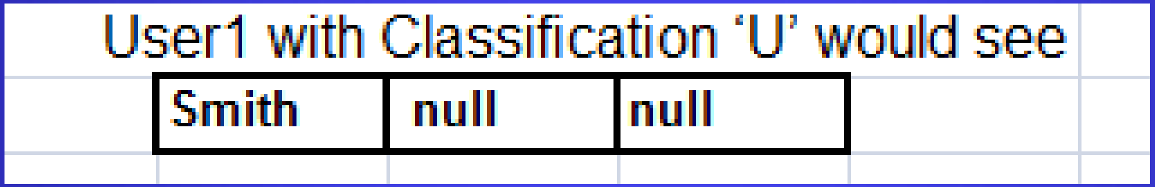
Mandatory Security Mechanism or Multi-Level Security (MLS)

- TC (tuple classification) represents a general classification for the tuple itself. The value of TC should be the highest classification of any attribute within that tuple.
- **Apparent Key**: In multi-level security relation, it is the set of attributes that would be primary key in a single-level table/relation
- **Polyinstantiation**: Where several tuples can have the same apparent key value but have different attribute values for a user at different classification levels

Example of MLS

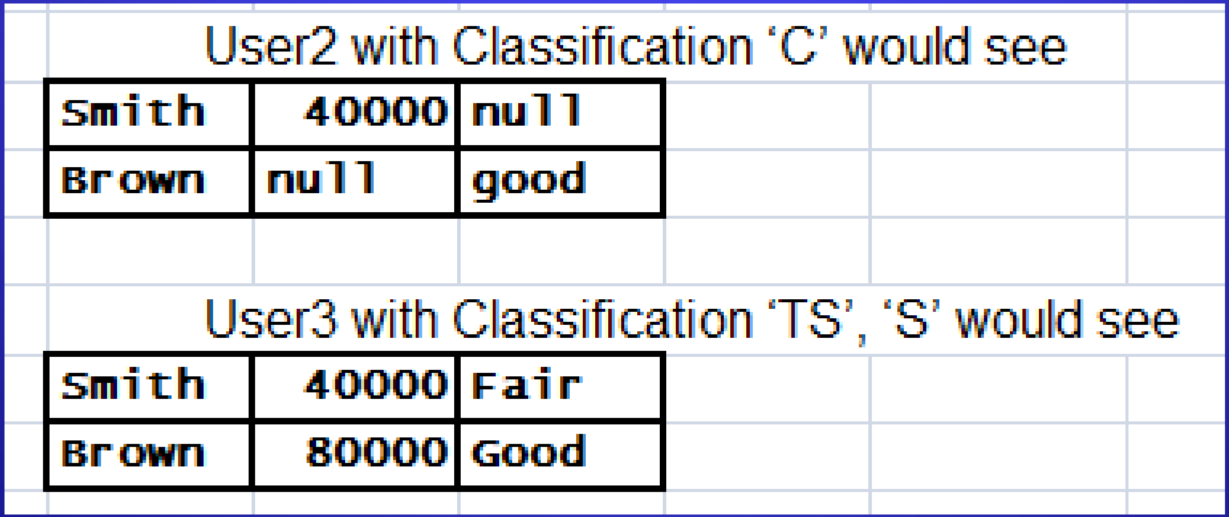


NAME	C!	SALARY	C2	JOB PERF	C3	TC
Smith	U	40000	C	Fair	S	S
Brown	C	80000	S	Good	C	S



User1 with Classification ‘U’ would see

Smith	null	null



User2 with Classification ‘C’ would see

Smith	40000	null
Brown	null	good

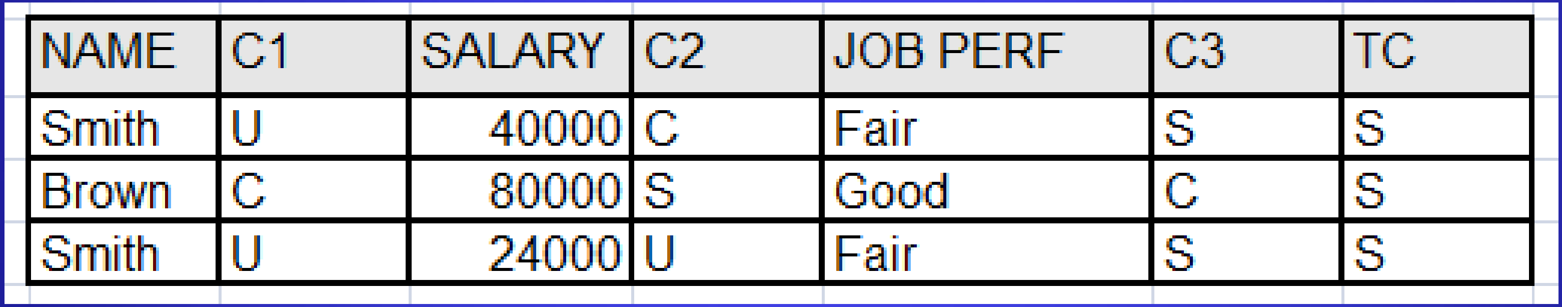
User3 with Classification ‘TS’, ‘S’ would see

Smith	40000	Fair
Brown	80000	Good

Example of MLS

User1 with Classification ‘U’ with discretionary insert, update, delete

- If salary is null Then set it to $24000   Else increase by 10%
- This would result in record of → Smith, 24000, null



NAME	C1	SALARY	C2	JOB PERF	C3	TC
Smith	U	40000	C	Fair	S	S
Brown	C	80000	S	Good	C	S
Smith	U	24000	U	Fair	S	S

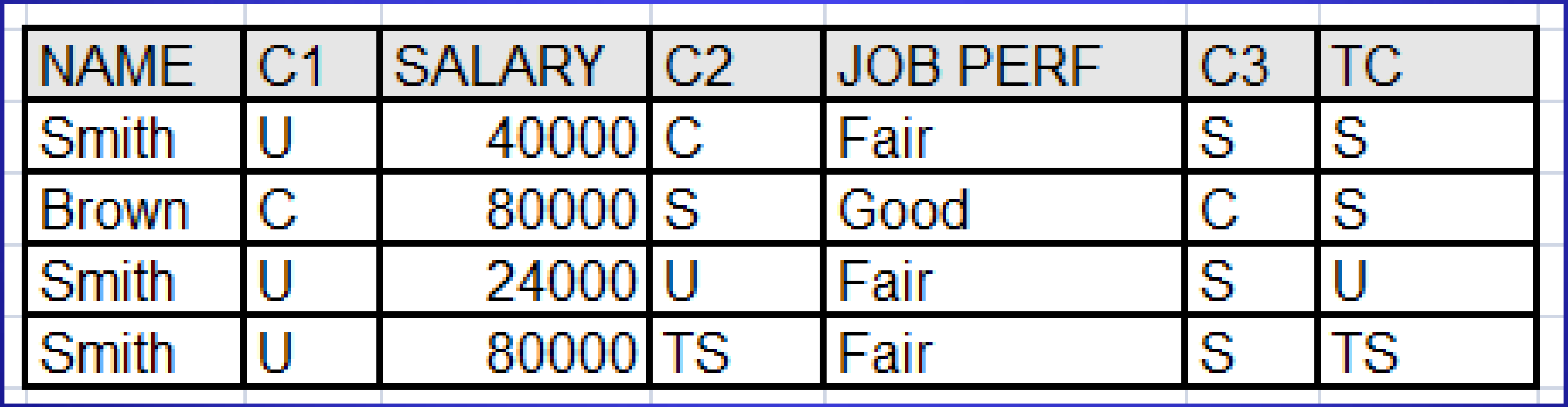
Example of MLS

(Would add second record for Smith – example of polyinstantiation)

User 3 ‘TS’

If salary is null Then set it to 100000 Else increase by 100%

Would result in record: Smith U, 80000 TS, Fair S,



NAME	C1	SALARY	C2	JOB PERF	C3	TC
Smith	U	40000	C	Fair	S	S
Brown	C	80000	S	Good	C	S
Smith	U	24000	U	Fair	S	U
Smith	U	80000	TS	Fair	S	TS

Secure Systems

Department of Defense (DOD) has defined the following specs/matrix on security levels.

Most Secure = highest price

A1 = must provide verifiable (vendor specs) security

B3 = provides security against covert channels

B2 = provides security against covert channels

B1 = provides mandatory access control (MLS minimum)

C2 = must provide discretionary security

C1= must provide discretionary security

D

Least Secure

Countermeasures – Computer-Based Controls

View

- Is the dynamic result of one or more relational operations operating on the base relations to produce another relation.

- A view is a virtual relation that does not actually exist in the database, but is produced upon request by a particular user, at the time of request.

Countermeasures – Computer-Based Controls

- Backup
  - Process of periodically taking a copy of the database and log file (and possibly programs) to offline storage media.

- Journaling
  - Process of keeping and maintaining a log file (or journal) of all changes made to database to enable effective recovery in event of failure.

Countermeasures – Computer-Based Controls

- Integrity
  - Prevents data from becoming invalid, and hence giving misleading or incorrect results.

- Encryption
  - The encoding of the data by a special algorithm that renders the data unreadable by any program without the decryption key.

RAID (Redundant Array of Independent Disks) Technology

- Hardware that the DBMS is running on must be *fault-tolerant*, meaning that the DBMS should continue to operate even if one of the hardware components fails.

- Suggests having redundant components that can be seamlessly integrated into the working system whenever there is one or more component failures.

RAID (Redundant Array of Independent Disks) Technology

- The main hardware components that should be fault-tolerant include disk drives, disk controllers, CPU, power supplies, and cooling fans.

- Disk drives are the most vulnerable components with the shortest times between failure of any of the hardware components.

RAID (Redundant Array of Independent Disks) Technology

- One solution is to provide a large disk array comprising an arrangement of several independent disks that are organized to improve reliability and at the same time increase performance.

RAID (Redundant Array of Independent Disks) Technology

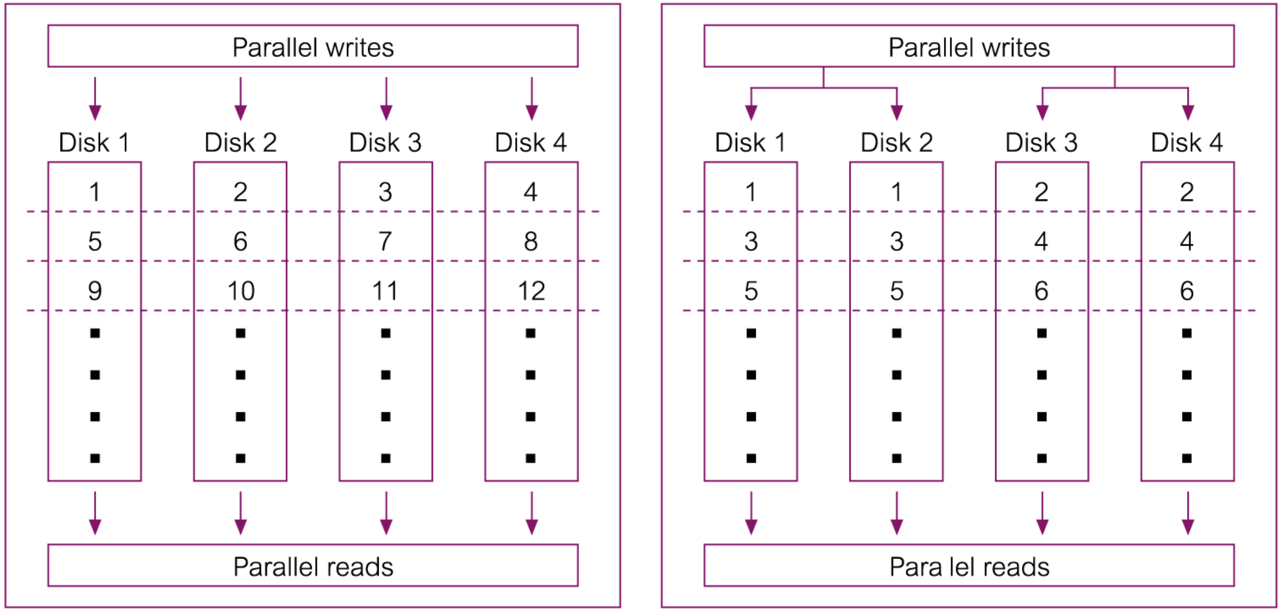
- **Performance is increased through *data striping*: the data is segmented into equal-size partitions (the *striping unit*), which are transparently distributed across multiple disks.**

- **Reliability is improved through storing redundant information across the disks using a *parity* scheme or an *error-correcting* scheme.**

RAID (Redundant Array of Independent Disks) Technology

- There are a number of different disk configurations called RAID levels.
  - RAID 0 Nonredundant
  - RAID 1 Mirrored
  - RAID 0+1 Nonredundant and Mirrored
  - RAID 2 Memory-Style Error-Correcting Codes
  - RAID 3 Bit-Interleaved Parity
  - RAID 4 Block-Interleaved Parity
  - RAID 5 Block-Interleaved Distributed Parity
  - RAID 6 P+Q Redundancy

RAID 0 and RAID 1



Parallel writes

Disk 1	Disk 2	Disk 3	Disk 4
1	2	3	4
5	6	7	8
9	10	11	12
▪	▪	▪	▪
▪	▪	▪	▪
▪	▪	▪	▪
▪	▪	▪	▪

Parallel reads

(a) RAID 0 – Nonredundant

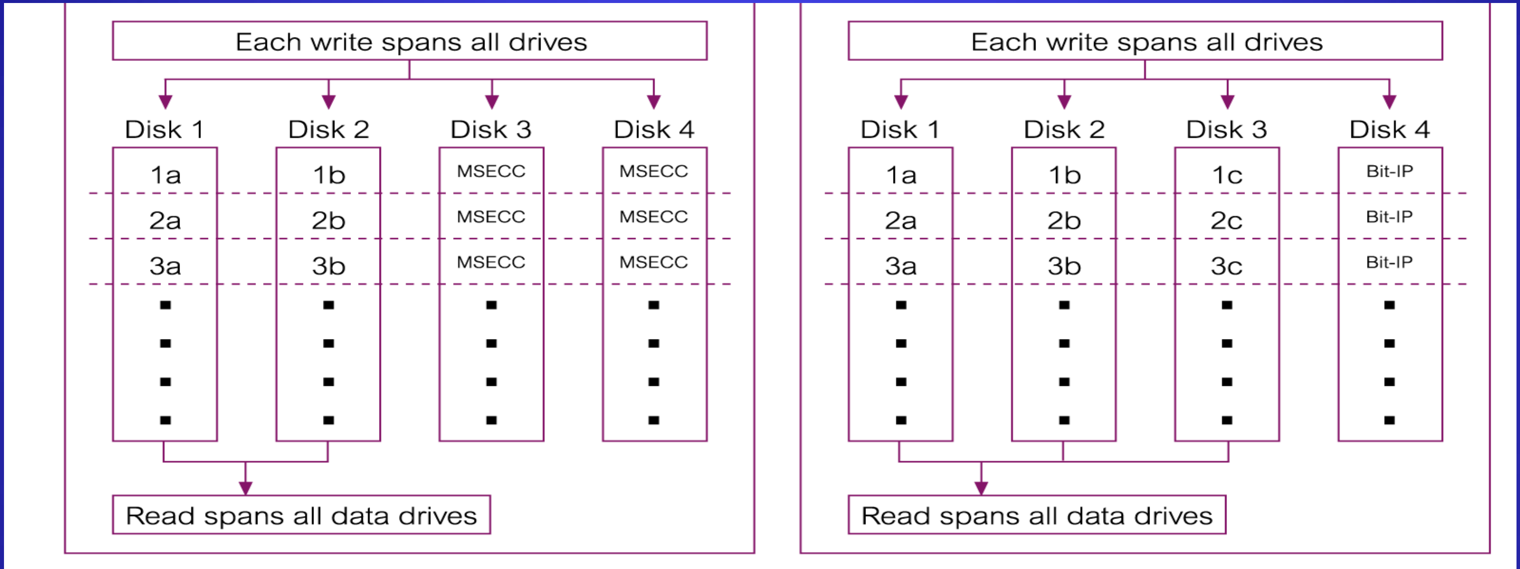
Parallel writes

Disk 1	Disk 2	Disk 3	Disk 4
1	1	2	2
3	3	4	4
5	5	6	6
▪	▪	▪	▪
▪	▪	▪	▪
▪	▪	▪	▪
▪	▪	▪	▪

Para lel reads

(b) RAID 1 – Mirrored

RAID 2 and RAID 3



Each write spans all drives

Disk 1	Disk 2	Disk 3	Disk 4
1a	1b	MSECC	MSECC
2a	2b	MSECC	MSECC
3a	3b	MSECC	MSECC
■	■	■	■
■	■	■	■
■	■	■	■
■	■	■	■

Read spans all data drives

(c) RAID 2 – Memory-Style Error-Correct ng Codes (MSECC)

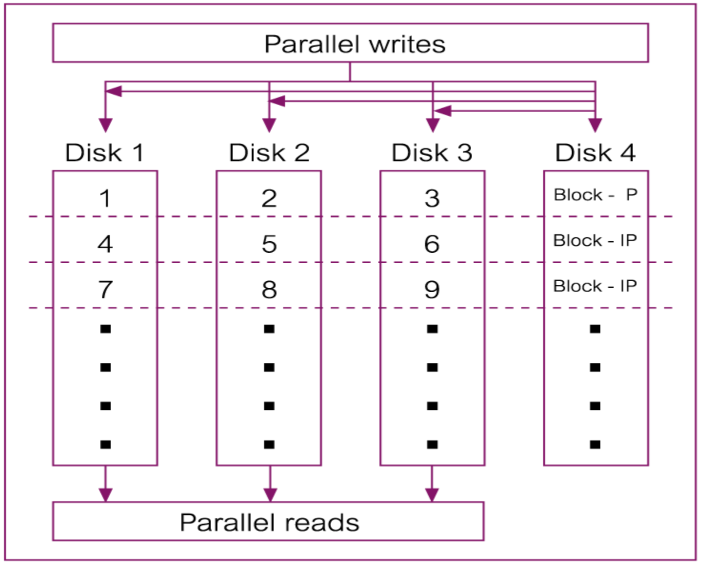
Each write spans all drives

Disk 1	Disk 2	Disk 3	Disk 4
1a	1b	1c	Bit-IP
2a	2b	2c	Bit-IP
3a	3b	3c	Bit-IP
■	■	■	■
■	■	■	■
■	■	■	■
■	■	■	■

Read spans all data drives

(d) RAID 3 – Bit Interleaved Parity (Bit-IP)

RAID 4 and RAID 5

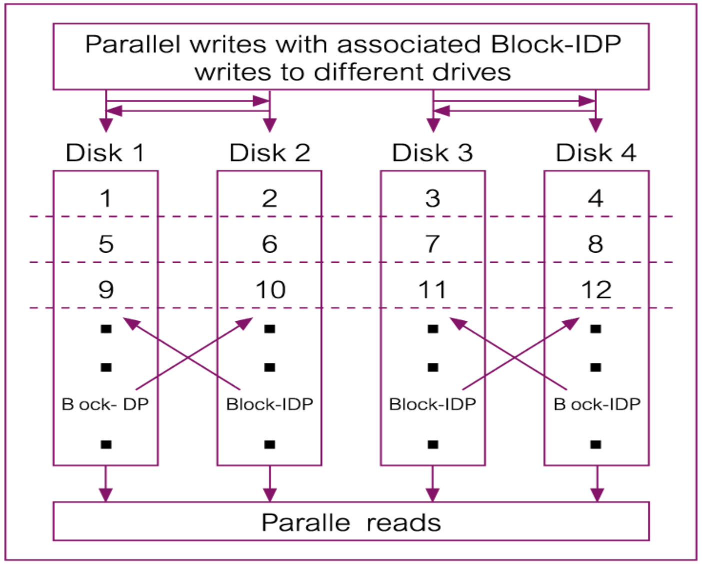


Parallel writes

Disk 1	Disk 2	Disk 3	Disk 4
1	2	3	Block - P
4	5	6	Block - IP
7	8	9	Block - IP
■	■	■	■
■	■	■	■
■	■	■	■
■	■	■	■

Parallel reads

(e) RAID 4 – Block-Interleaved Parity (Block-IP)



Parallel writes with associated Block-IDP writes to different drives

Disk 1	Disk 2	Disk 3	Disk 4
1	2	3	4
5	6	7	8
9	10	11	12
■	■	■	■
■	■	■	■
B ock- DP	Block-IDP	Block-IDP	B ock-IDP
■	■	■	■

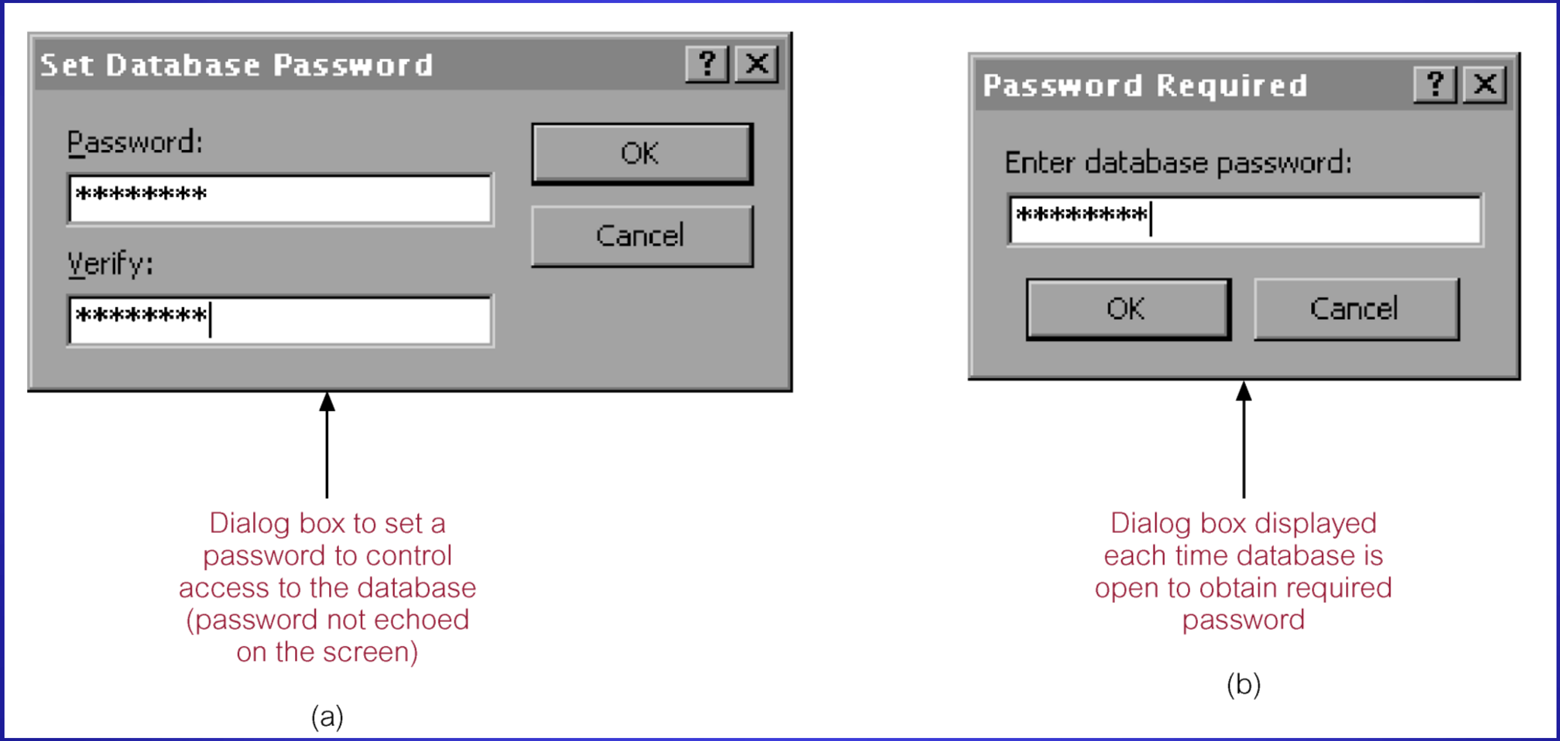
Paralle reads

(f) RAID 5 – Block-Interleaved D str buted Parity (Block-IDP)

Security in Microsoft Office Access DBMS

- Provides two methods for securing a database:
  - setting a password for opening a database (system security);
  - user-level security, which can be used to limit the parts of the database that a user can read or update (data security).

Securing the *DreamHome* database using a password



Password: *********

Verify: *********

Enter database password: *********

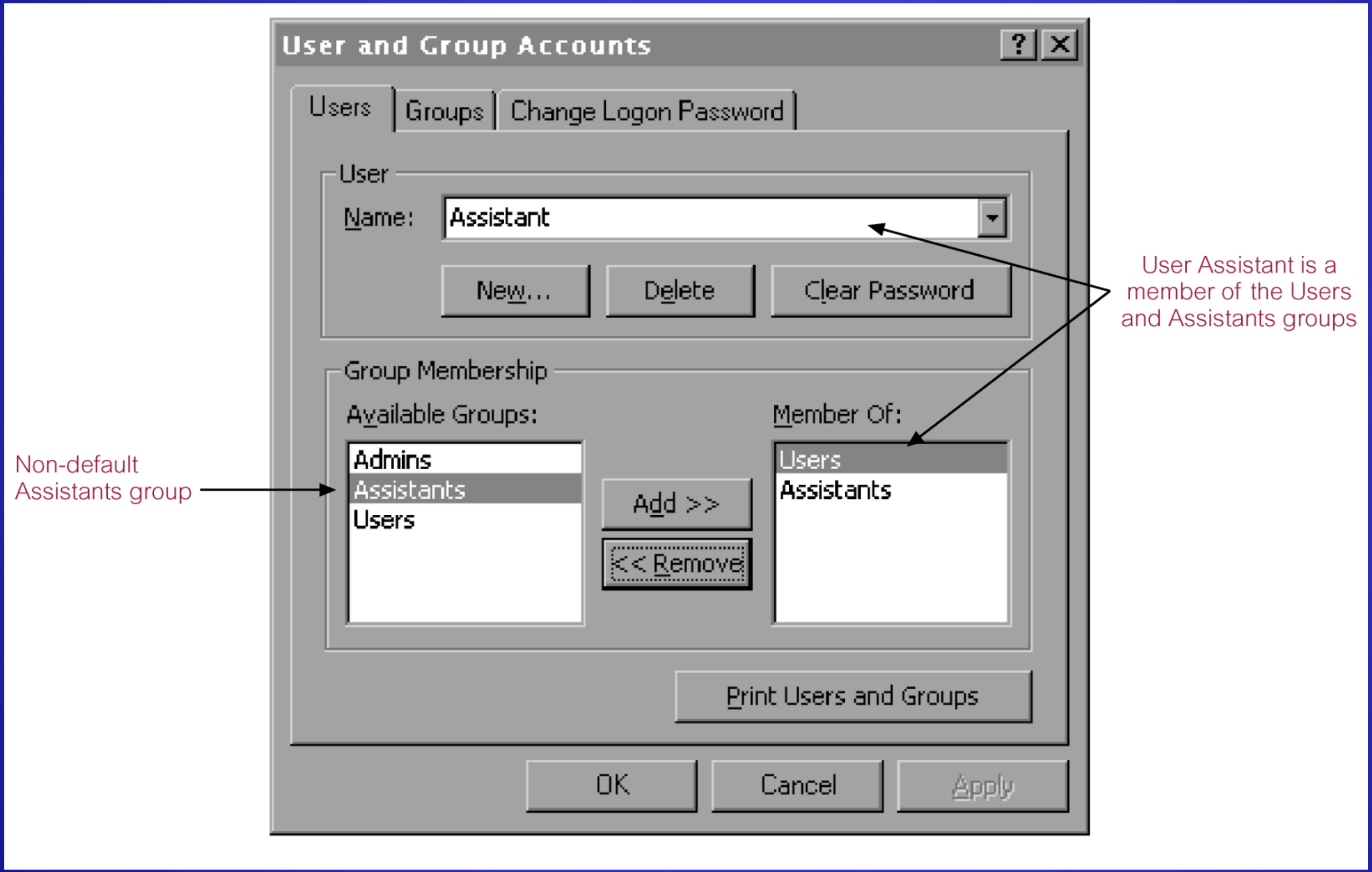
Dialog box to set a password to control access to the database (password not echoed on the screen)

(a)

Dialog box displayed each time database is open to obtain required password

(b)

User and Group Accounts dialog box for the *DreamHome* database



User and Group Accounts

Name: Assistant

Group Membership

Available Groups:

- Admins
- Assistants
- Users

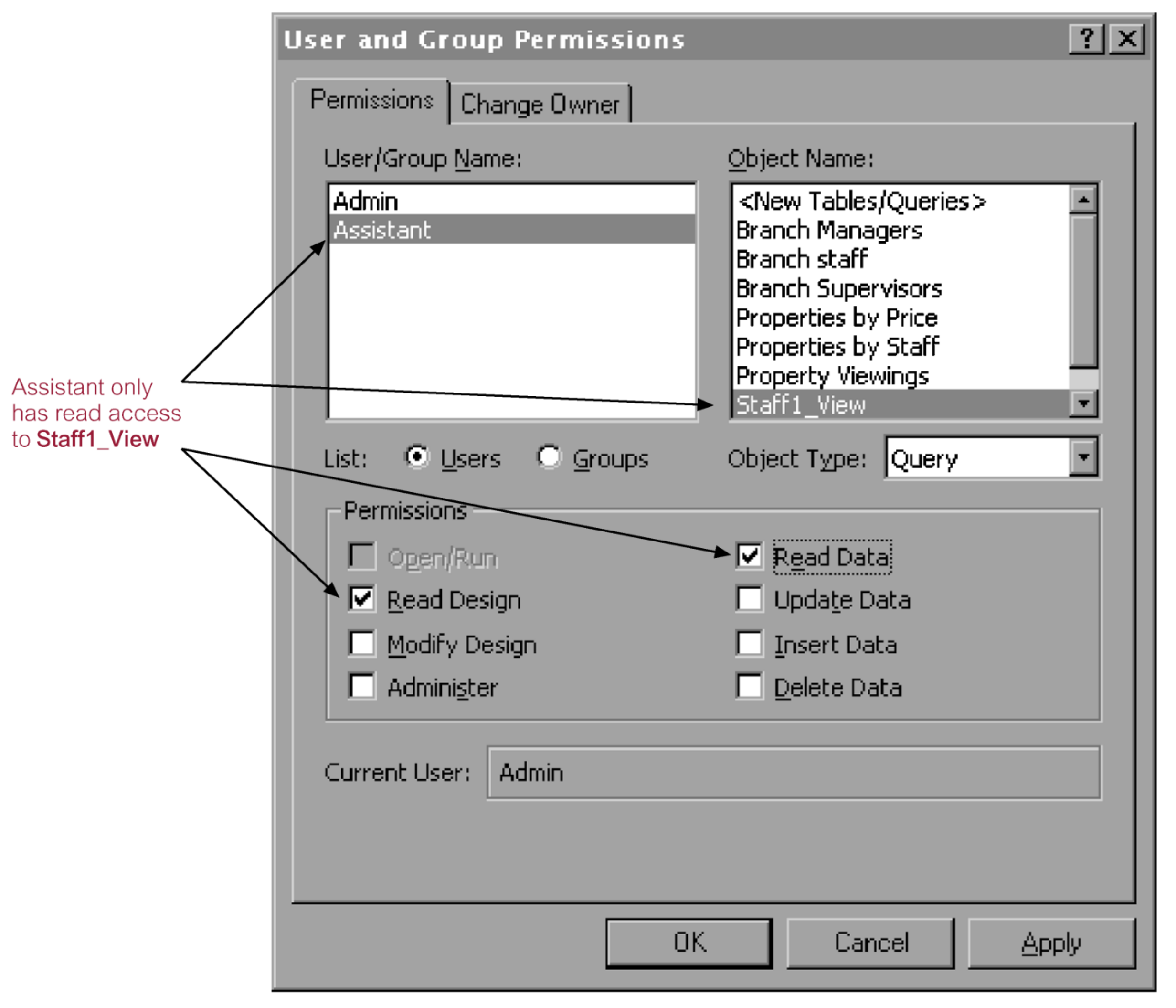
Member Of:

- Users
- Assistants

User Assistant is a member of the Users and Assistants groups

Non-default Assistants group

User and Group Permissions dialog box



User/Group Name:

- Admin
- Assistant

Object Name:

- <New Tables/Queries>
- Branch Managers
- Branch staff
- Branch Supervisors
- Properties by Price
- Properties by Staff
- Property Viewings
- Staff1_View

List: ● Users ○ Groups

Object Type: Query

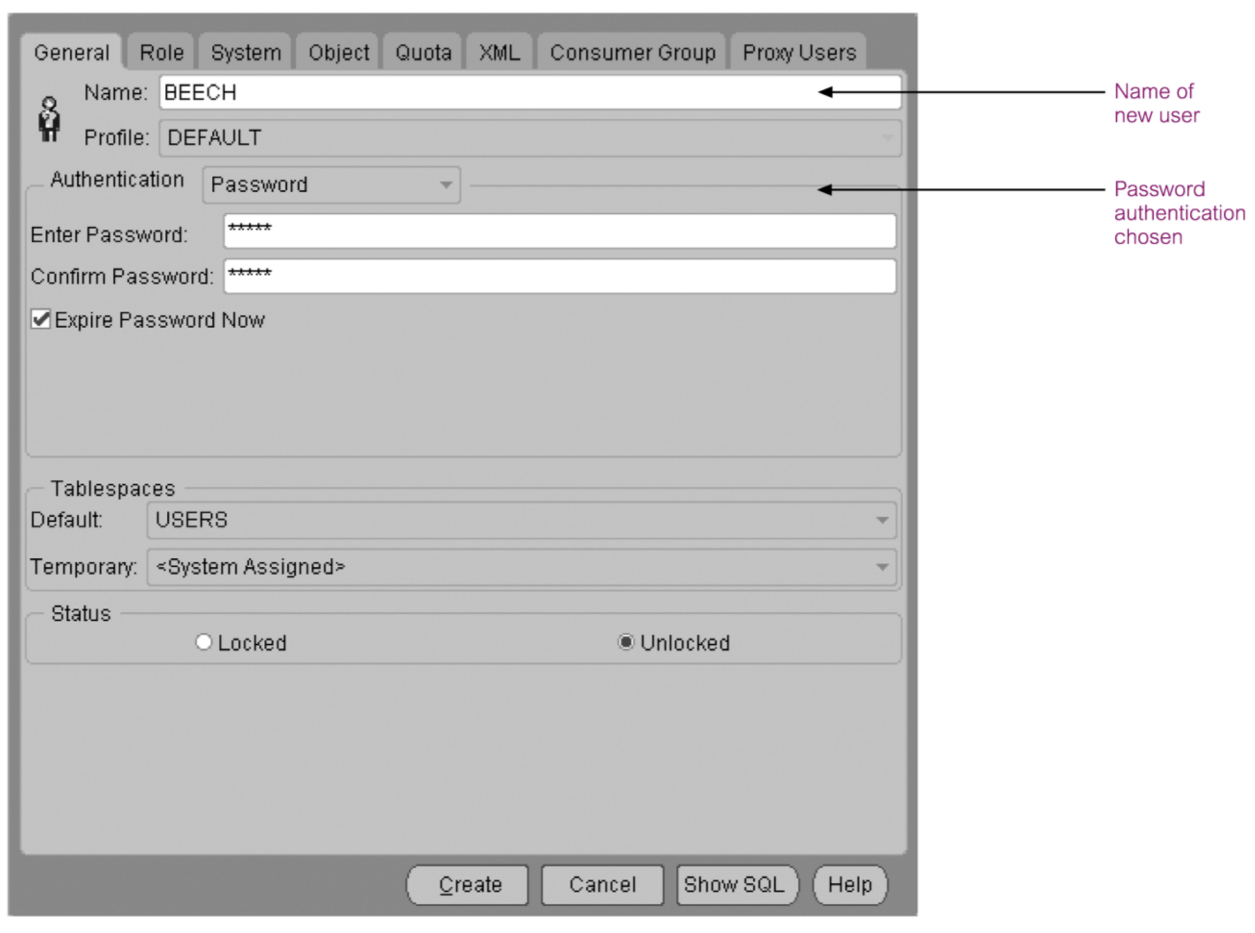
Permissions

□ Open/Run	☑ Read Data
☑ Read Design	□ Update Data
□ Modify Design	□ Insert Data
□ Administer	□ Delete Data

Current User: Admin

Assistant only has read access to **Staff1_View**

Creation of a new user with password authentication set



General | Role | System | Object | Quota | XML | Consumer Group | Proxy Users

Name: BEECH

Profile: DEFAULT

Authentication: Password

Enter Password: *****

Confirm Password: *****

☑ Expire Password Now

Tablespaces

Default: USERS

Temporary: <System Assigned>

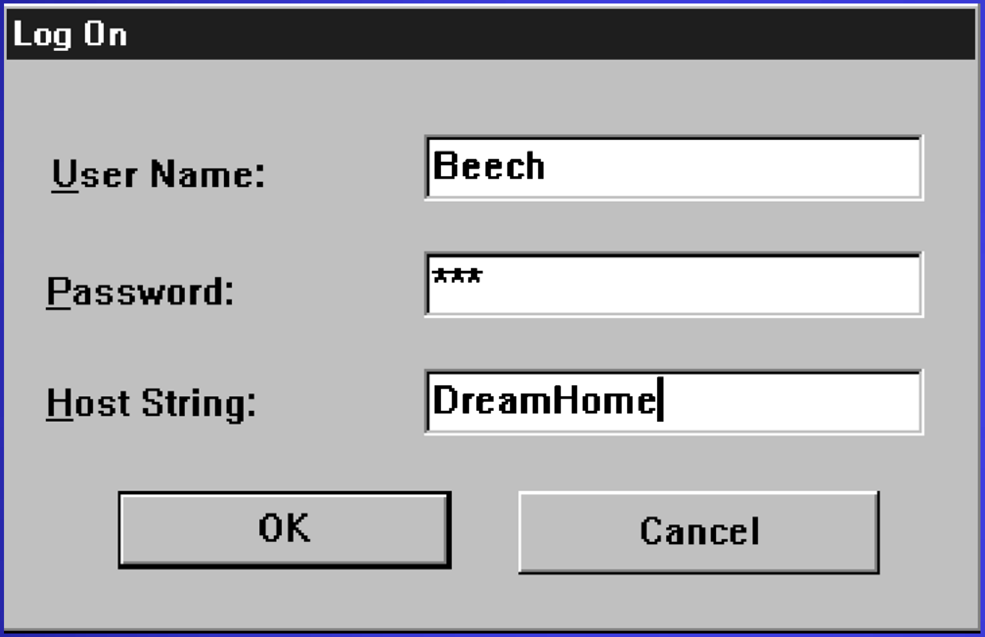
Status

○ Locked ● Unlocked

Name of new user

Password authentication chosen

Log on dialog box

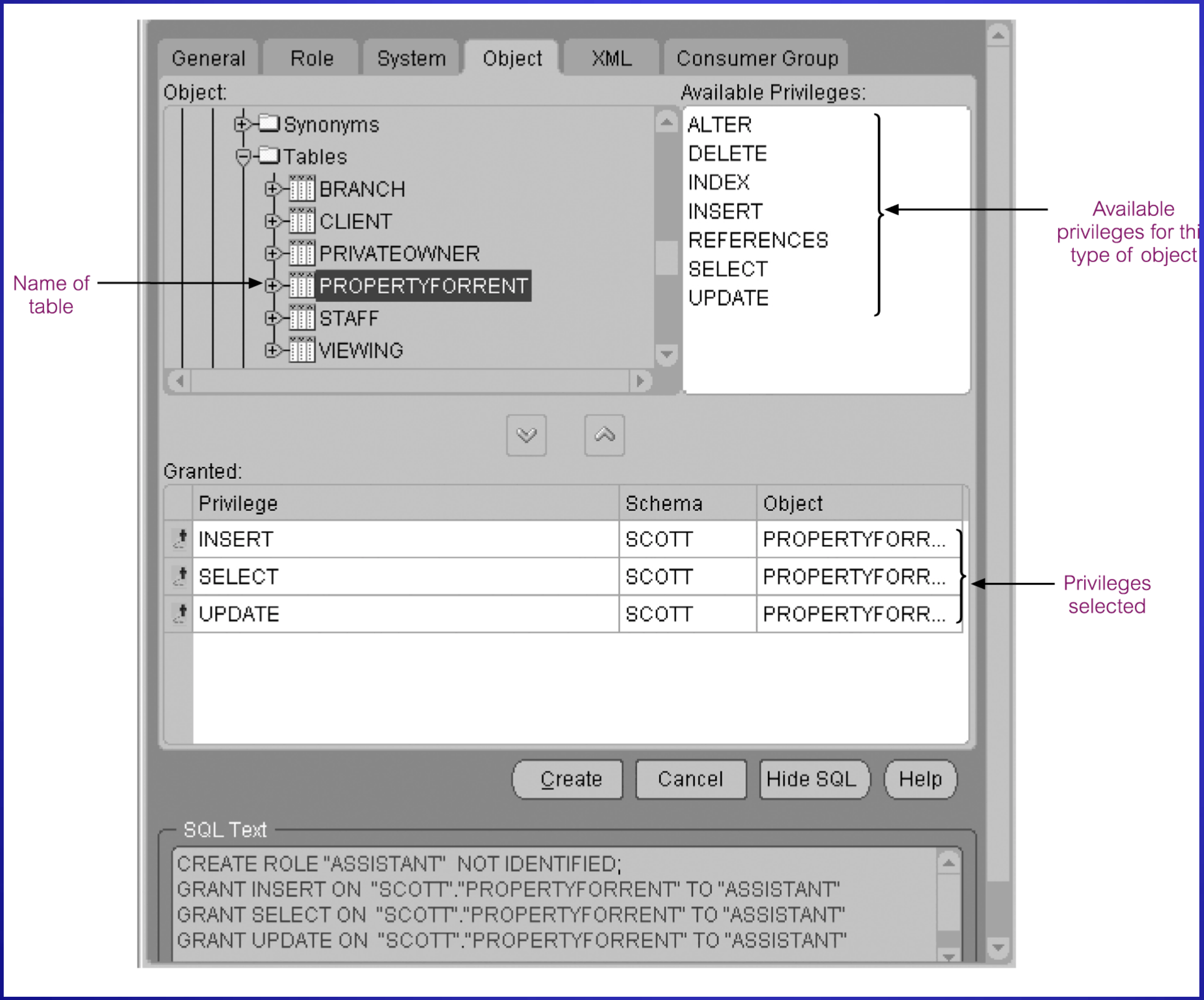


User Name: Beech

Password: ***

Host String: DreamHome

Setting the Insert, Select, and Update privileges



Privilege	Schema	Object
INSERT	SCOTT	PROPERTYFORR...
SELECT	SCOTT	PROPERTYFORR...
UPDATE	SCOTT	PROPERTYFORR...

```
CREATE ROLE "ASSISTANT"  NOT IDENTIFIED;
GRANT INSERT ON  "SCOTT"."PROPERTYFORRENT" TO "ASSISTANT"
GRANT SELECT ON  "SCOTT"."PROPERTYFORRENT" TO "ASSISTANT"
GRANT UPDATE ON  "SCOTT"."PROPERTYFORRENT" TO "ASSISTANT"
```

DBMSs and Web Security

- Internet communication relies on TCP/IP as the underlying protocol. However, TCP/IP and HTTP were not designed with security in mind. Without special software, all Internet traffic travels ‘in the clear’ and anyone who monitors traffic can read it.

DBMSs and Web Security

- Must ensure while transmitting information over the Internet that:
  - inaccessible to anyone but sender and receiver (privacy);
  - not changed during transmission (integrity);
  - receiver can be sure it came from sender (authenticity);
  - sender can be sure receiver is genuine (non-fabrication);
  - sender cannot deny he or she sent it (non-repudiation).

DBMSs and Web Security

- Measures include:
  - Proxy servers
  - Firewalls
  - Message digest algorithms and digital signatures
  - Digital certificates
    - » Is a type of authentication that is widely used in e-commerce. So it is digital passport that identifies and verifies the holder of the certificate
  - Kerberos
    - » Developed by MIT to enable two parties to exchange information over an pen network by assigning a unique key, called ticket to each user. This ticket is used to encrypt communicated messages
  - Secure sockets layer (SSL) and Secure HTTP (S-HTTP)
    - » SSL: is a method in which authentication information is transmitted over the network in an encrypted form. It is used to secure user communication. This protocol was developed by Netscape

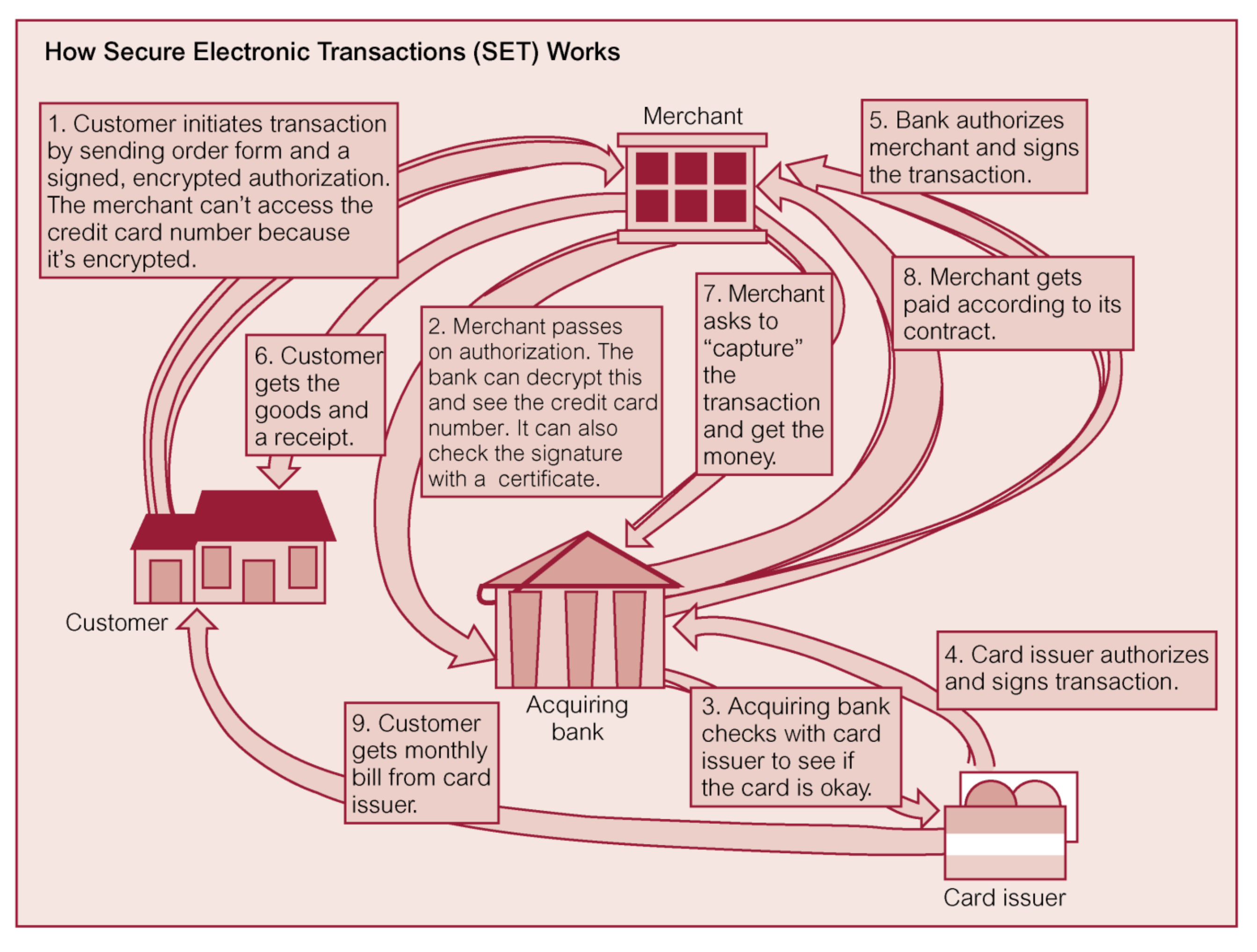
DBMSs and Web Security

- Measures include:
  - LDAP (Lightweight Directory Access Protocol)
    - » LDAP uses a centralized directory database storing information about people, office, and machines in a hierarchical manner. LDAP stores information:
      - Users (name and ID)
      - Passwords
      - Internal telephone directory
      - Security keys
  - PKI (Public Key Infrastructure)
    - » PKI, also known as public key encryption, is an authentication method in which a user keeps a private key and the authentication firm hold the a public key, These two keys are used to encrypt and decrypt communication between the two parties. Private key is usually kept as a digital certificate on the user's system.

DBMSs and Web Security

- Secure Electronic Transactions (SET)
  - SRP was developed by Stanford.
- RADIUS (Remote Authentication Dial-In User Service)
  - RDIUS is commonly used by network devices to provide a centralized authentication mechanism.
  - RADIUS is client /server based , and used a dial-up server, a virtual private network (VPN), or a wireless access point communicating to a RADIS server.
- SRP (Secure Remote Password)
  - SRP was developed by Stanford.
  - It is a protocol in which the password is not stored locally in encrypted or plaintext form.
  - This method in invulnerable to brute force or dictionary attack.

How Secure Electronic Transactions (SET) Works



How Secure Electronic Transactions (SET) Works

1. Customer initiates transaction by sending order form and a signed, encrypted authorization. The merchant can't access the credit card number because it's encrypted.

2. Merchant passes on authorization. The bank can decrypt this and see the credit card number. It can also check the signature with a certificate.

3. Acquiring bank checks with card issuer to see if the card is okay.

4. Card issuer authorizes and signs transaction.

5. Bank authorizes merchant and signs the transaction.

6. Customer gets the goods and a receipt.

7. Merchant asks to "capture" the transaction and get the money.

8. Merchant gets paid according to its contract.

9. Customer gets monthly bill from card issuer.