Chapter 20

Security and Administration Transparencies

Chapter 20 - 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.**

Chapter 20 - Objectives

- 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.**

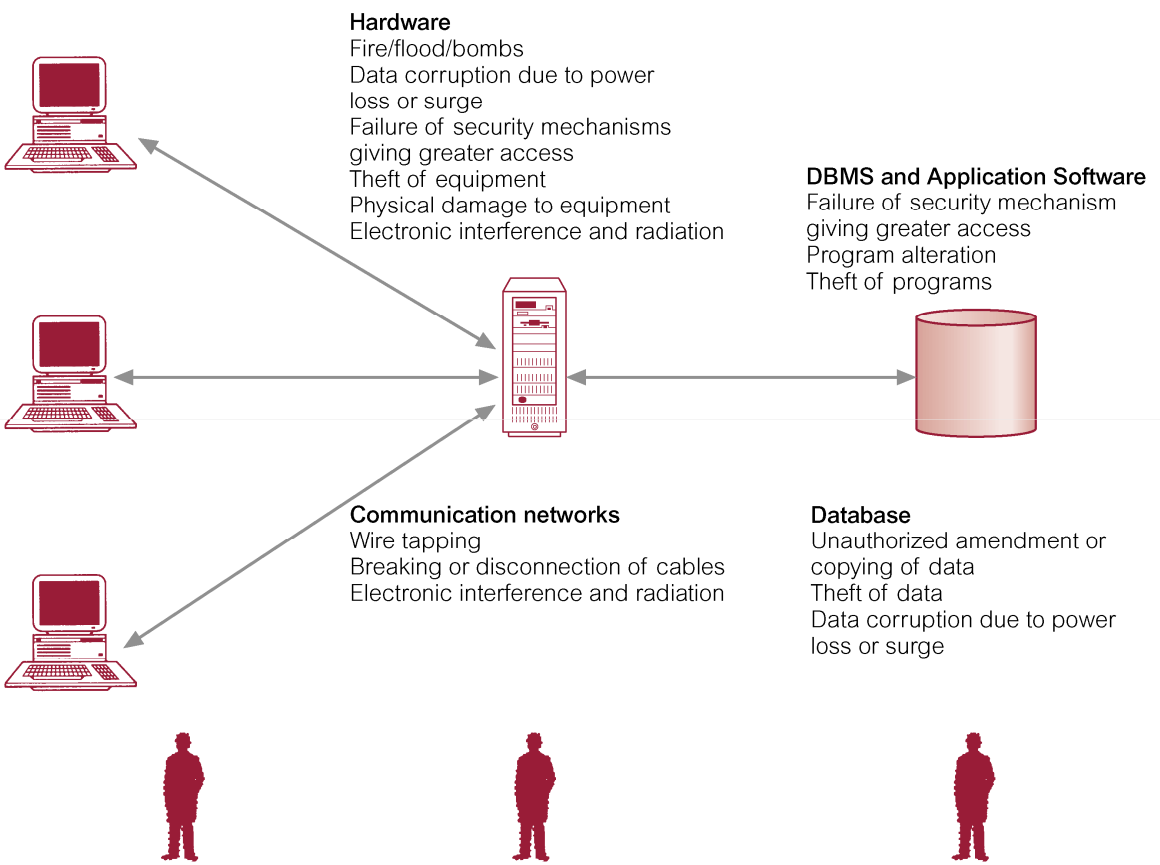
Database Security

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

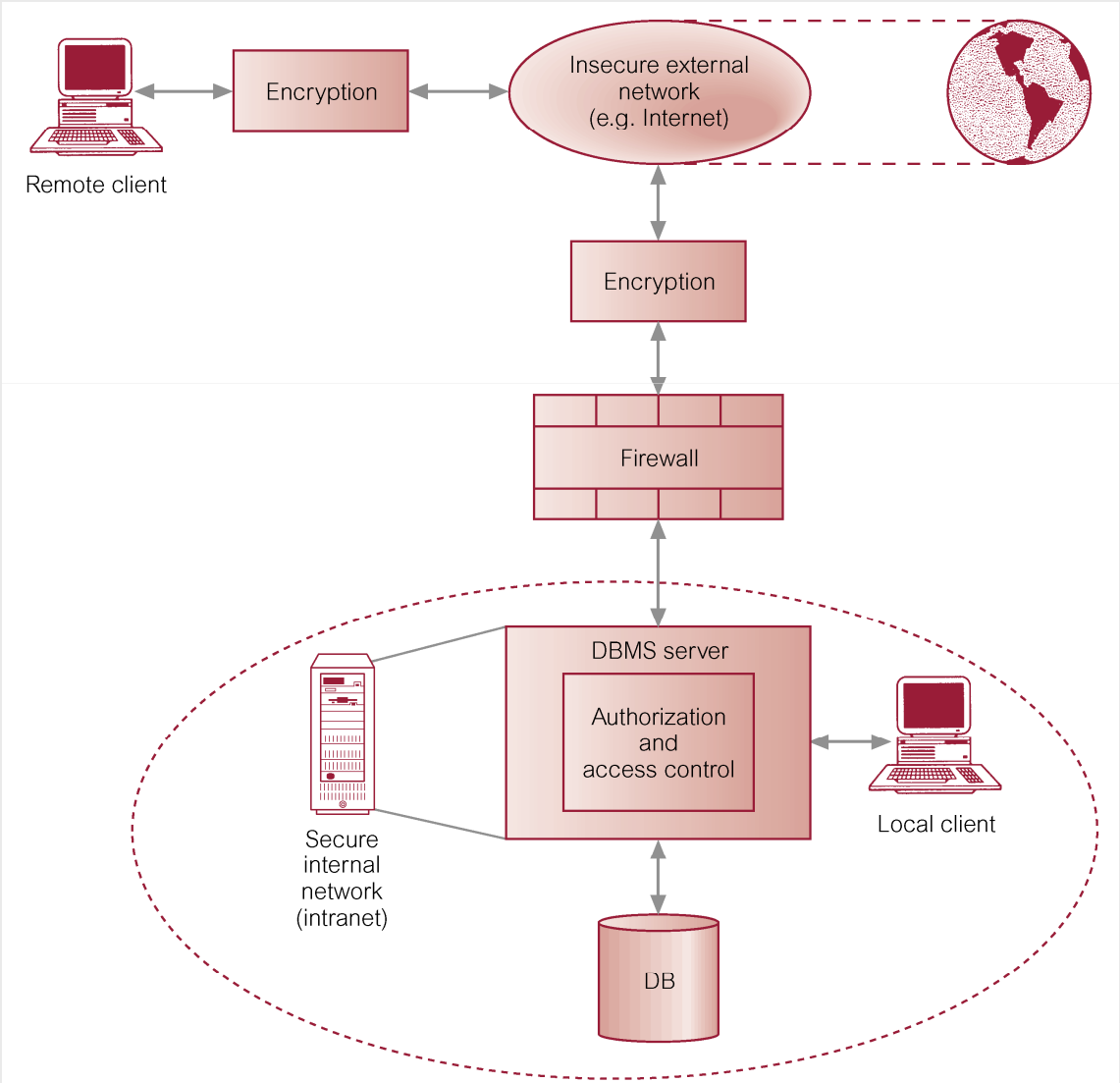
Database Security

- **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



Typical Multi-user Computer Environment



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.**

Popular Model for MAC called Bell-LaPudula

- **Insert Figure 20.3(a)**

Popular Model for MAC called Bell-LaPudula

clientNo	fName	lName	telNo	prefType	maxRent	securityClass
CR76	John	Kay	0207-774-5632	Flat	425	*C*
CR56	Aline	Stewart	0141-848-1825	Flat	350	*C*
CR74	Mike	Ritchie	01475-392178	House	750	*S*
CR62	Mary	Tregar	01224-196720	Flat	600	*S*

clientNo	fName	lName	telNo	prefType	maxRent	securityClass
CR76	John	Kay	0207-774-5632	Flat	425	*C*
CR56	Aline	Stewart	0141-848-1825	Flat	350	*C*
CR74	Mike	Ritchie	01475-392178	House	750	*S*
CR62	Mary	Tregar	01224-196720	Flat	600	*S*
CR74	David	Sinclaire				*C*

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

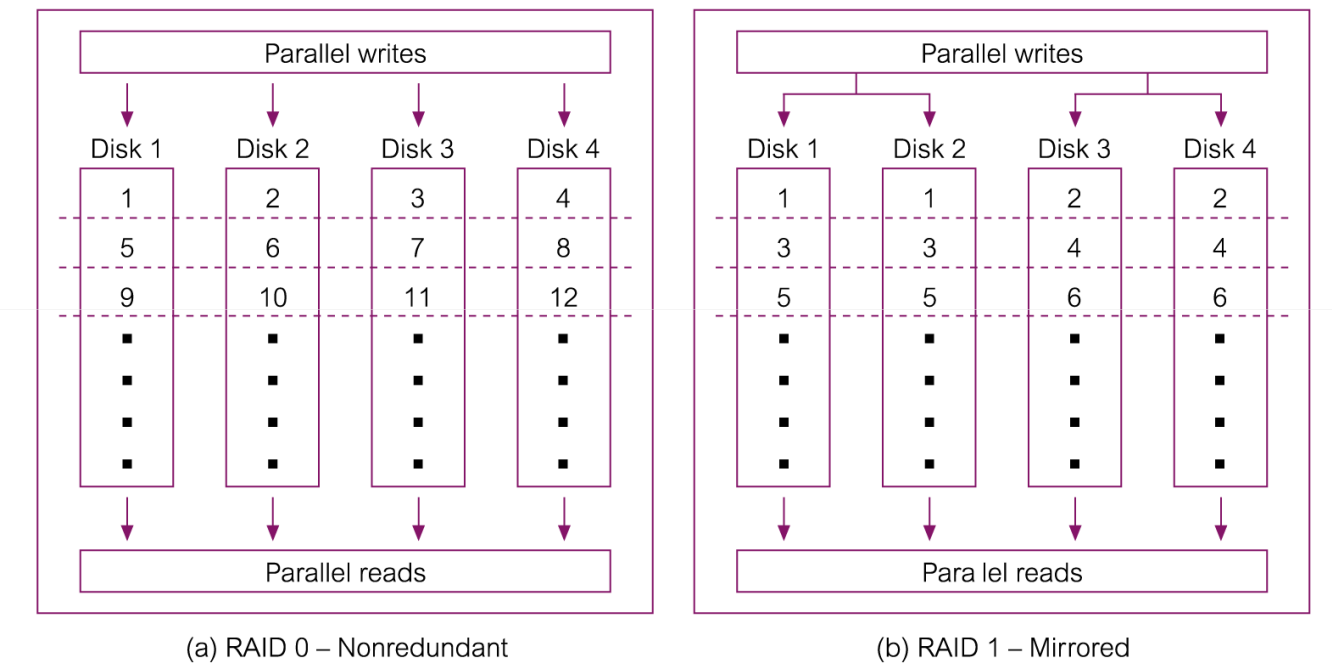
- **Performance is increased through *data striping*: the data is segmented into equal-size partitions (the *striping unit*), which are transparently distributed across multiple disks.**

- **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

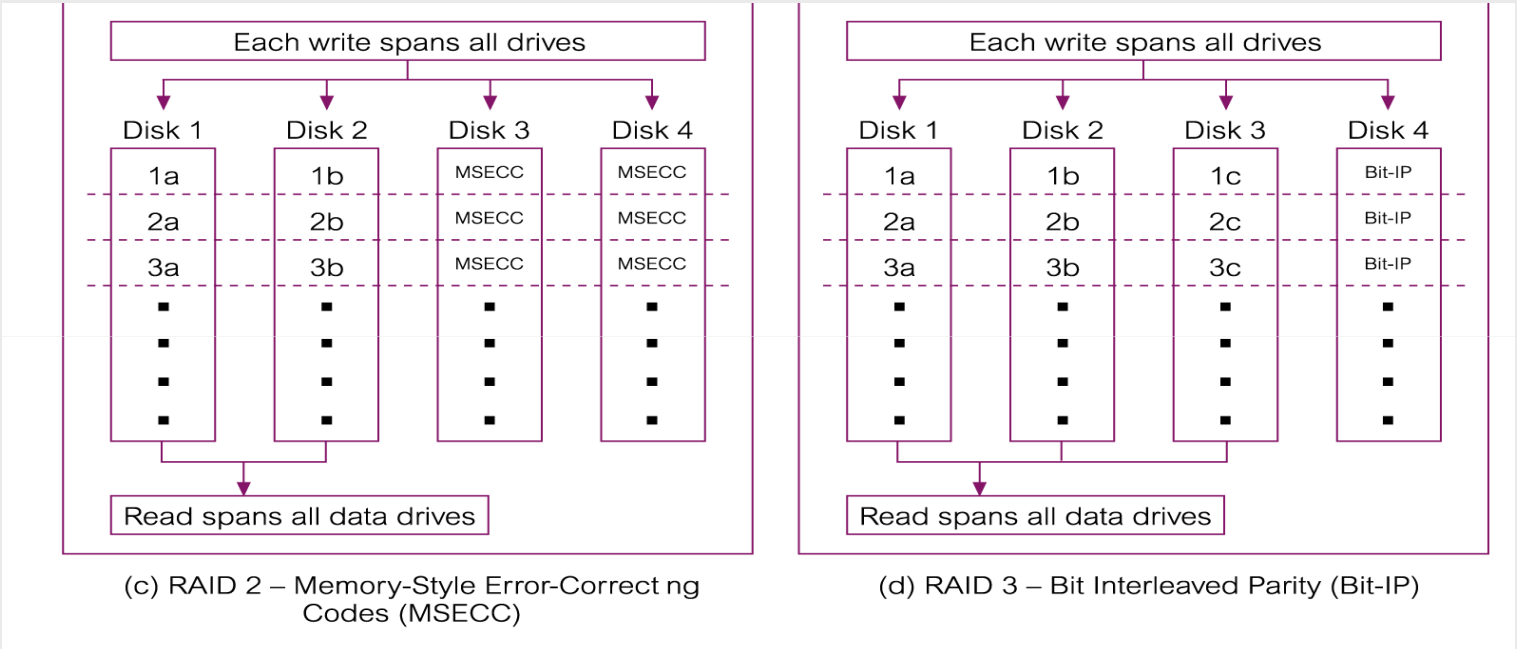
RAID 0 and RAID 1



(a) RAID 0 – Nonredundant

(b) RAID 1 – Mirrored

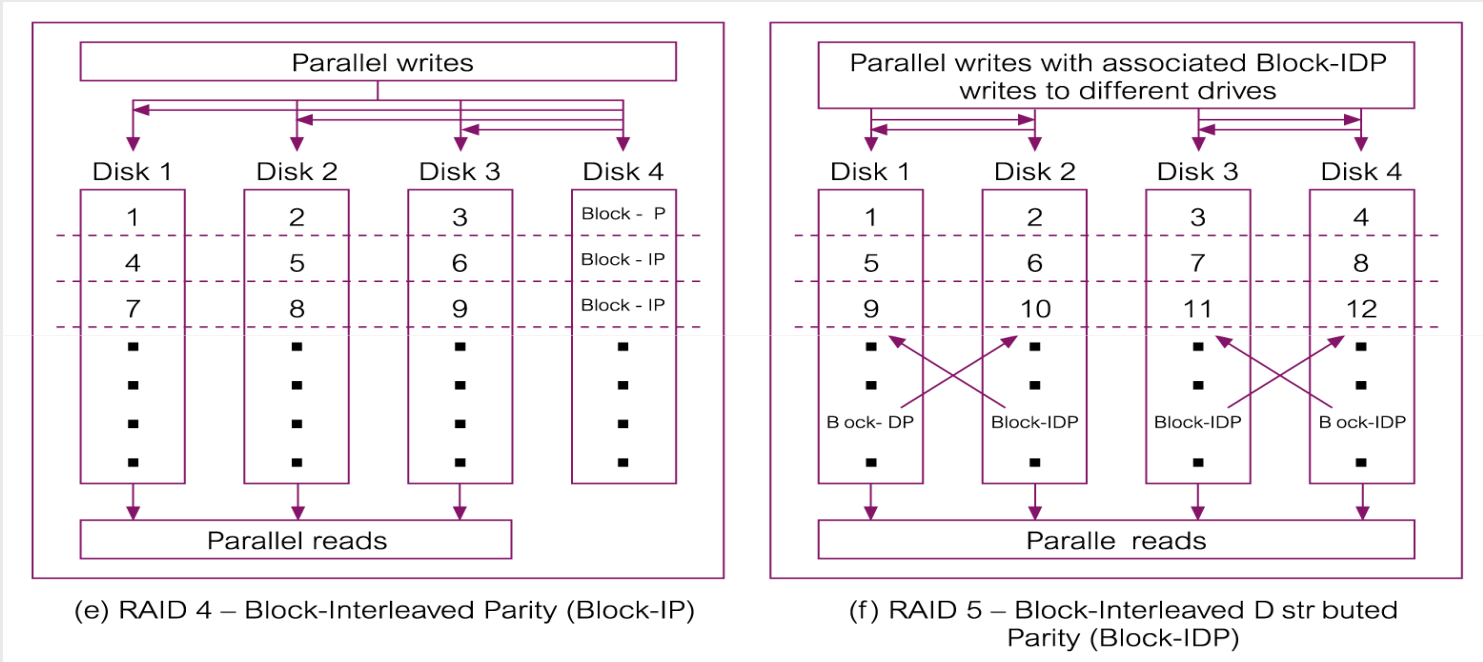
RAID 2 and RAID 3



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

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

RAID 4 and RAID 5



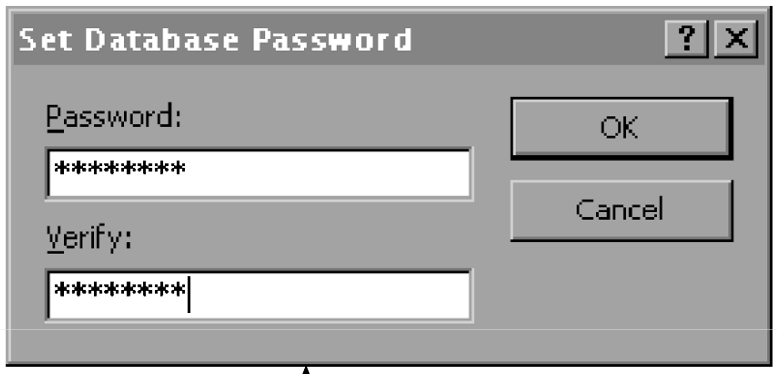
(e) RAID 4 – Block-Interleaved Parity (Block-IP)

(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



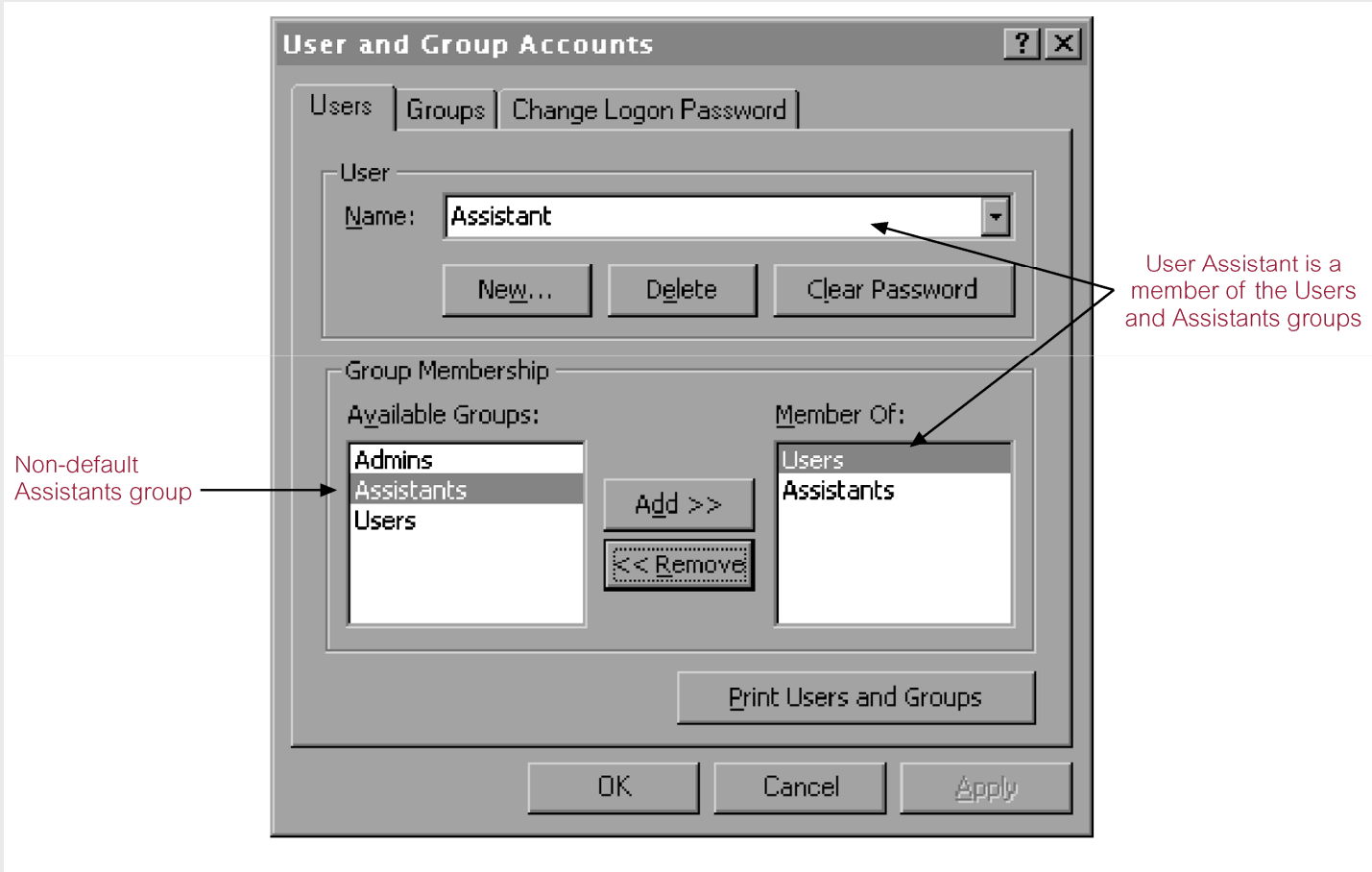
Dialog box to set a password to control access to the database (password not echoed on the screen)

(a)

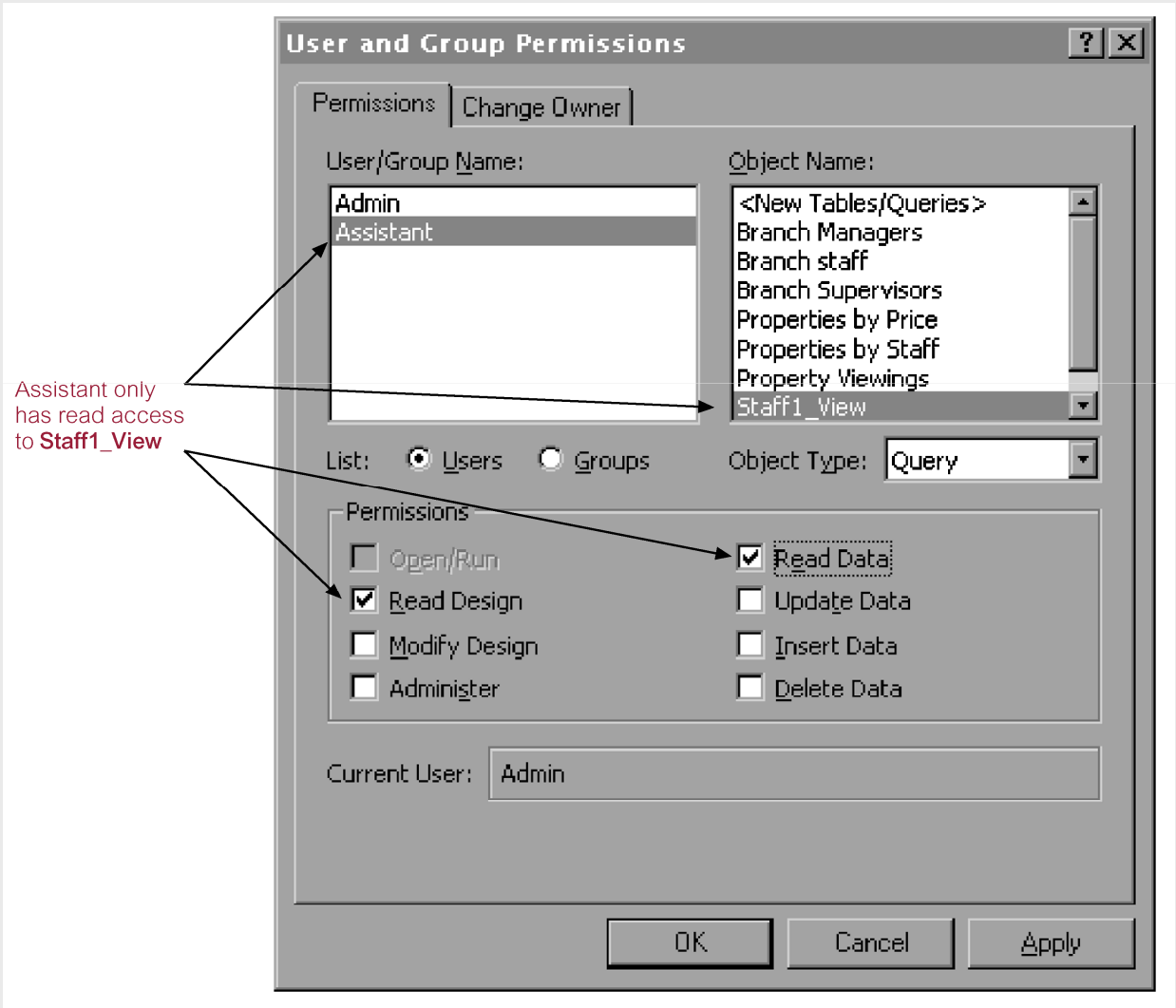
Dialog box displayed each time database is open to obtain required password

(b)

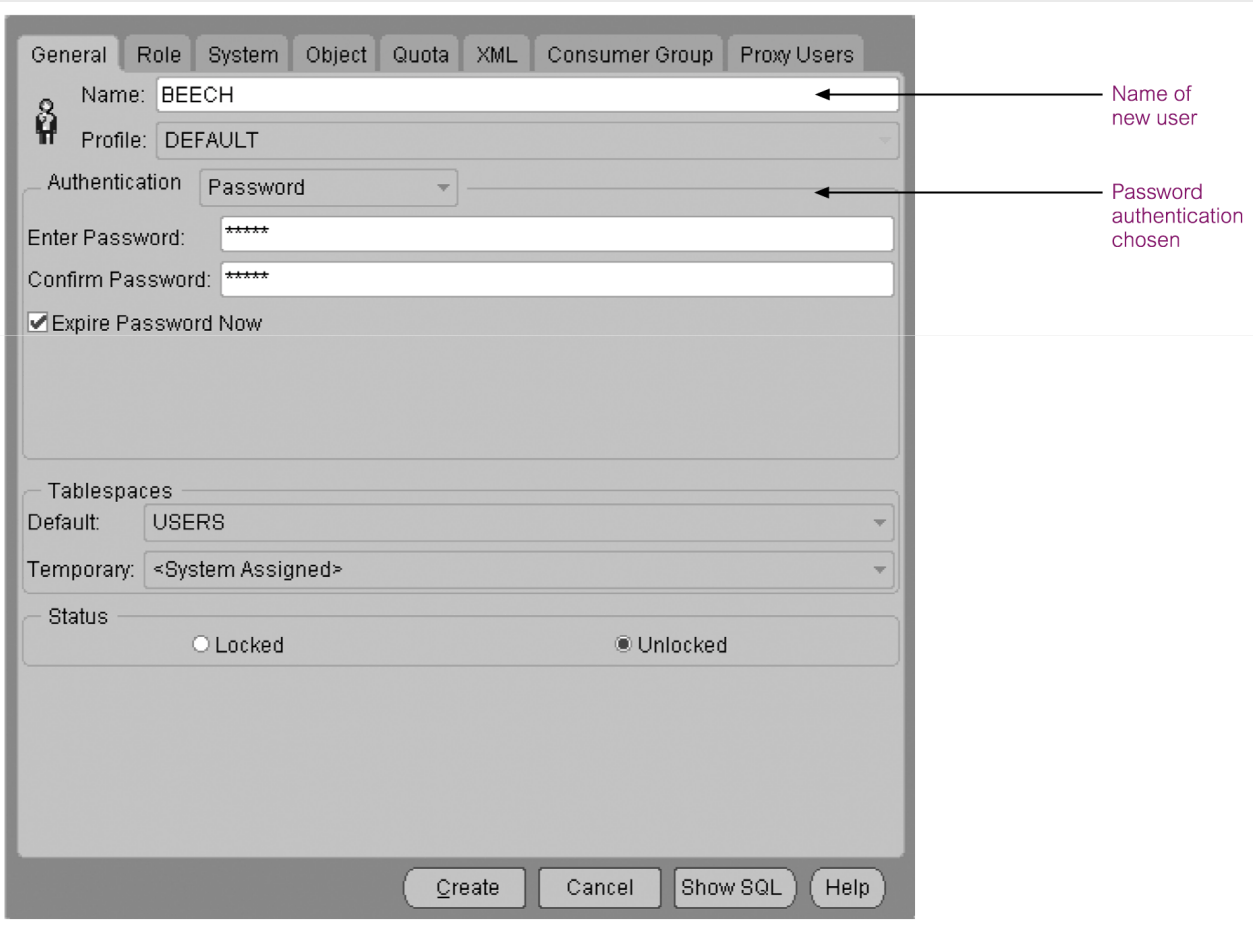
User and Group Accounts dialog box for the *DreamHome* database



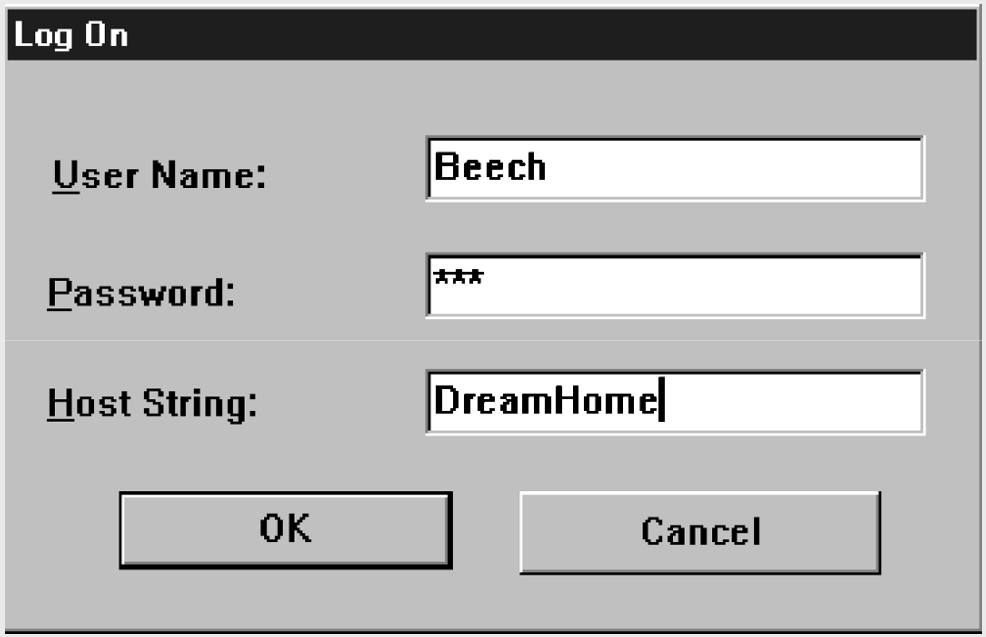
User and Group Permissions dialog box



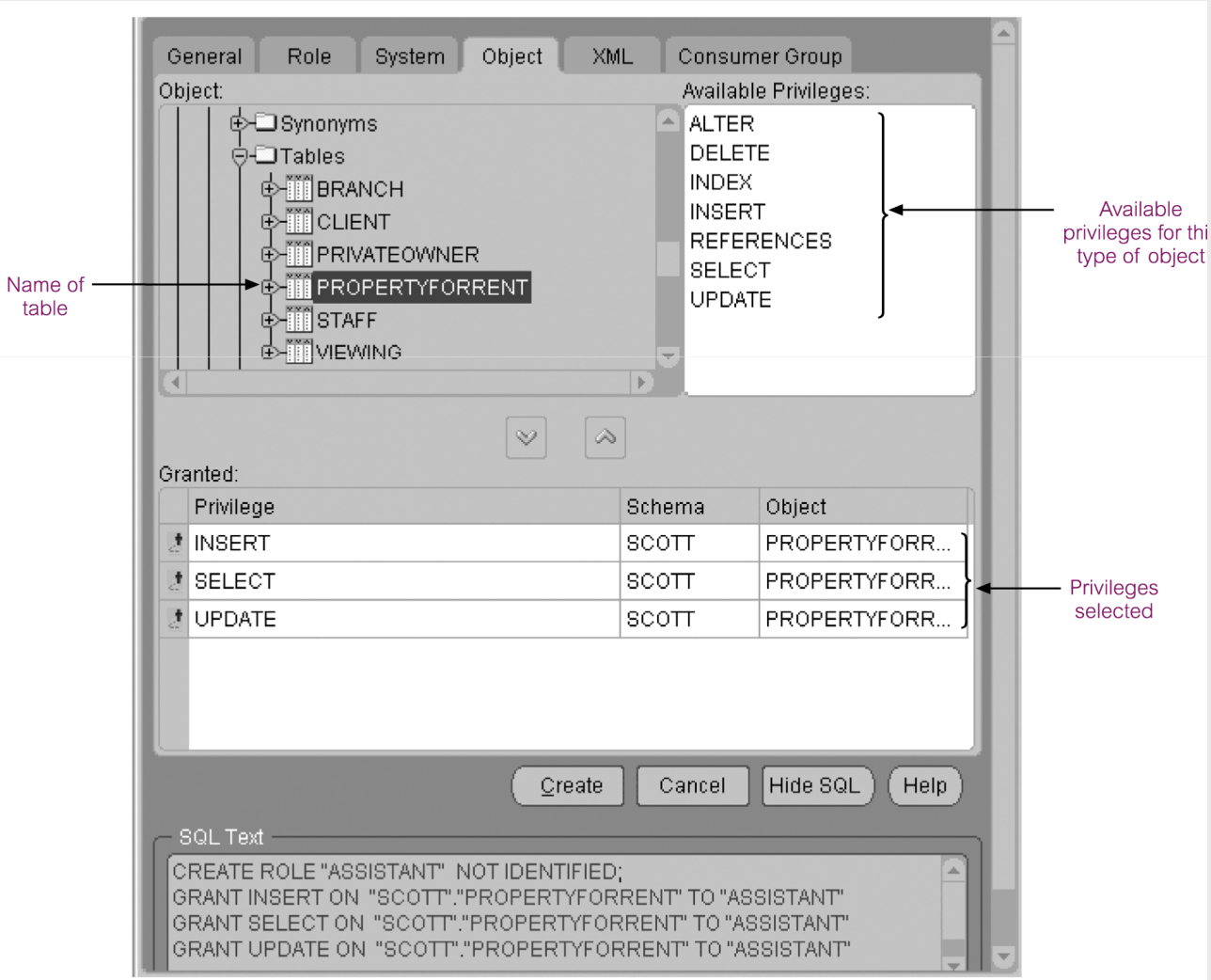
Creation of a new user with password authentication set



Log on dialog box



Setting the Insert, Select, and Update privileges



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**
  - **Kerberos**
  - **Secure sockets layer (SSL) and Secure HTTP (S-HTTP)**
  - **Secure Electronic Transactions (SET) and Secure Transaction Technology (SST)**
  - **Java security**
  - **ActiveX security**

How Secure Electronic Transactions (SET) Works