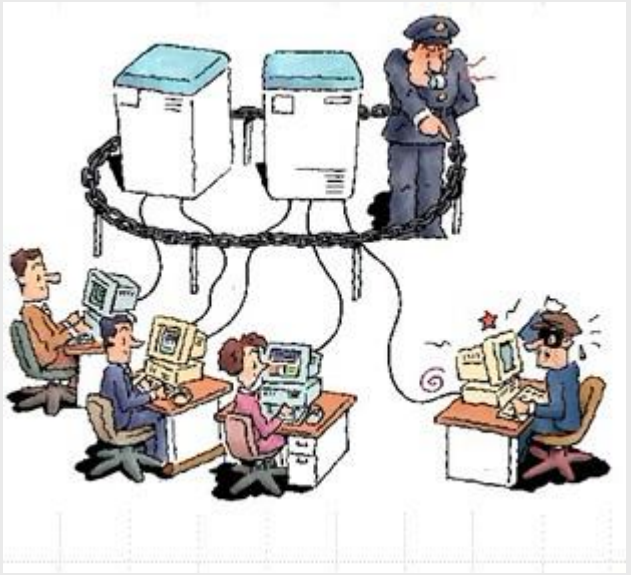


Security

Dr. Xu Yang

Objectives

1. Scope of database security.
2. Why database security is a serious concern for an organization.
3. Type of threats that can affect a database system.
4. How to protect a computer system using computer-based controls.
5. Security measures provided by Oracle DBMSs.
6. Approaches for securing a DBMS on the Web.

Database Security

- database security encompasses hardware, software, people, and data.

- Importance of Data
  - Bank accounts
  - Credit card, Salary, Income tax data
  - University admissions, marks/grades
  - Land records, licenses

Database Security

Database Security

mechanisms that protect the database against intentional or accidental threats.

- Database security aims to minimize losses caused by anticipated events in a cost-effective manner without unduly constraining the users.

Threats

- We consider database security in relation to the following situations:
  - Theft and fraud
  - Loss of confidentiality
  - Loss of privacy
  - Loss of integrity
  - Loss of availability

Threats

- **Threats**

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

  – Tangible losses (hardware, software, data)

  – Intangible losses (credibility, confidentiality)

Examples of threats

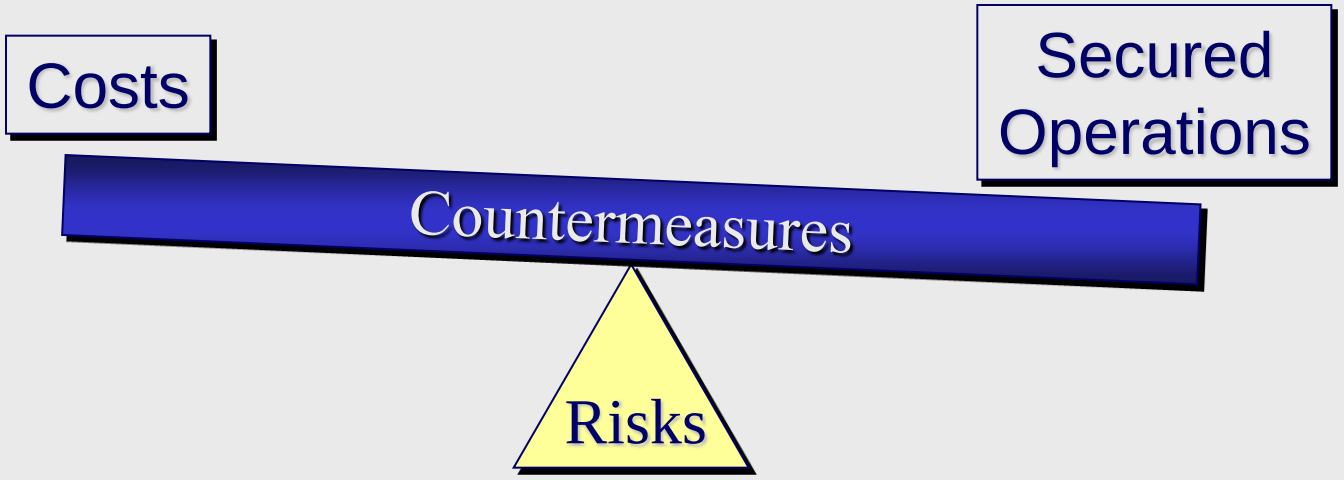
Threat	Theft and fraud	Loss of confidentiality	Loss of privacy	Loss of integrity	Loss of availability
Using another person's means of access	✓	✓	✓		
Unauthorized amendment or copying of data	✓			✓	
Program alteration	✓			✓	✓
Inadequate policies and procedures that allow a mix of confidential and normal output	✓	✓	✓		
Wire tapping	✓	✓	✓		
Illegal entry by hacker	✓	✓	✓		
Blackmail	✓	✓	✓		
Creating 'trapdoor' into system	✓	✓	✓		
Theft of data, programs, and equipment	✓	✓	✓		✓
Failure of security mechanisms, giving greater access than normal		✓	✓	✓	
Staff shortages or strikes				✓	✓
Inadequate staff training		✓	✓	✓	✓
Viewing and disclosing unauthorized data	✓	✓	✓		
Electronic interference and radiation				✓	✓
Data corruption owing to power loss or surge				✓	✓
Fire (electrical fault, lightning strike, arson), flood, bomb				✓	✓
Physical damage to equipment				✓	✓
Breaking cables or disconnection of cables				✓	✓
Introduction of viruses				✓	✓

Threats and Countermeasures

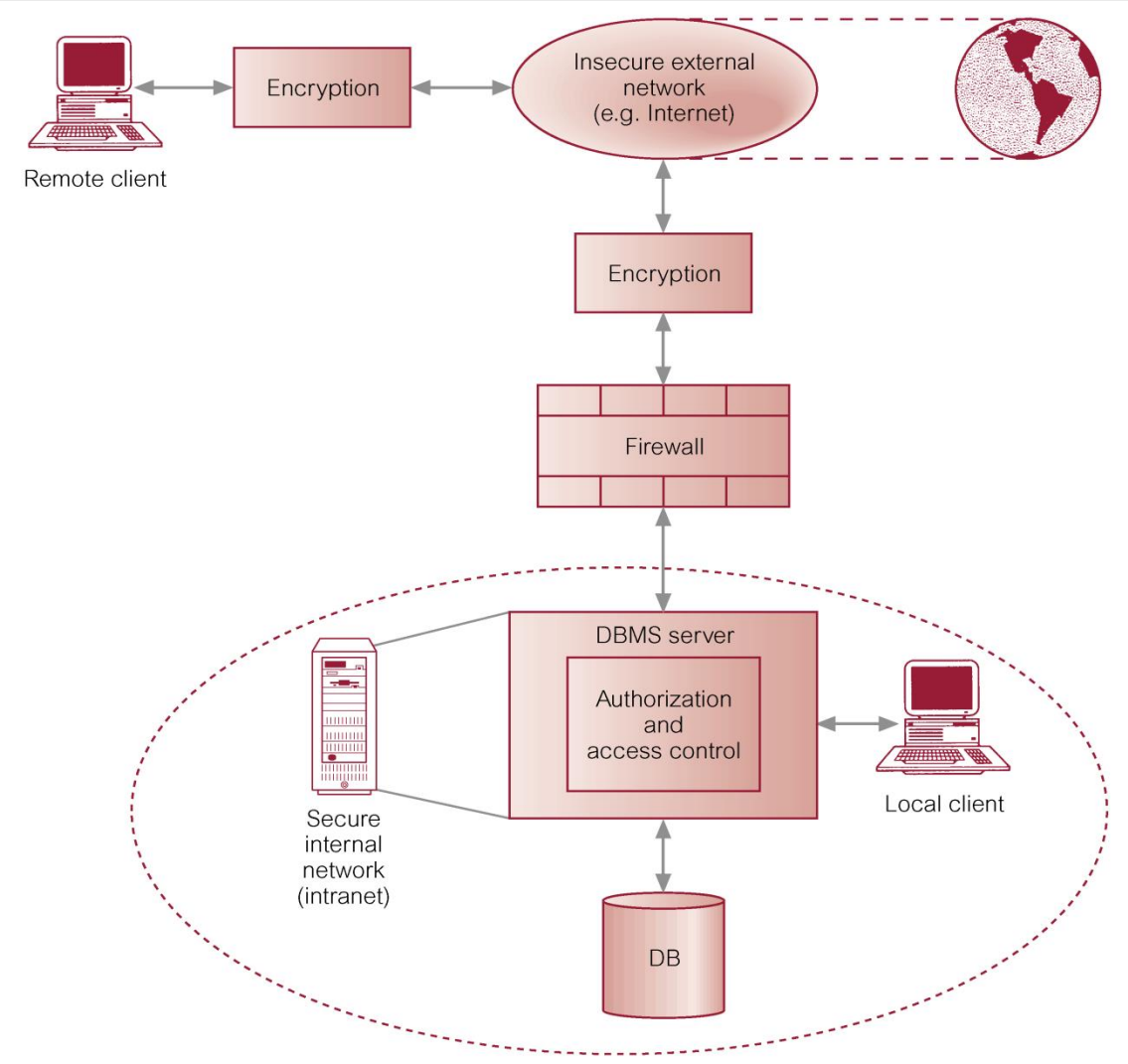
- Initiate countermeasures to overcome threats
  - Consider the types of threat and their impact on the organization
    - » Cost-effectiveness
    - » Frequency
    - » Severity

Threats and Countermeasures

- Objective is to achieve a balance between a reasonable secure operation, which does not unduly hinder users, and the costs of maintaining it.



Typical Multi-User Computer Environment



Countermeasures – Computer-Based Controls

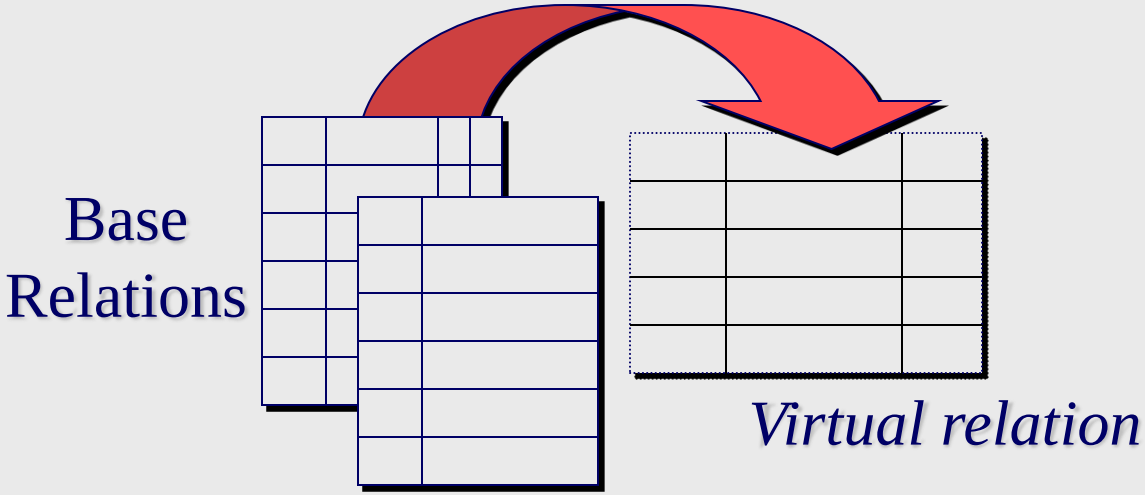
- Concerned with physical controls to administrative procedures and includes:
  - Authorization
  - Views
  - Backup and recovery
  - Integrity
  - Encryption
  - RAID technology

Authorization and Authentication

- Authorization
  - Granting privileges which enables users and applications to legitimately have access to a system or object (table, view, application, procedure, etc.)
    - » Access to database(s)
    - » Manipulation and definition of data
- Authentication
  - Mechanism that determines whether the user is who s/he claims her/himself to be
- The DBA (Database Administrator) is the central authority for managing a DBS.

Countermeasures – Computer-Based Controls

- **View**
  - Dynamic result of one or more relational operations operating on the base relations to produce another relation.
  - 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 Technology

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

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

RAID Technology

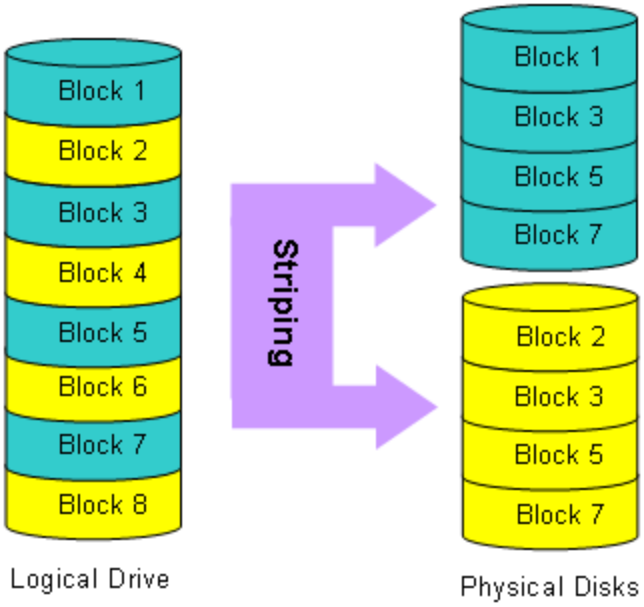
- RAID is used to combine multiple hard drives into a single logical volume. Thus instead your computer seeing several hard drives, it only sees one.

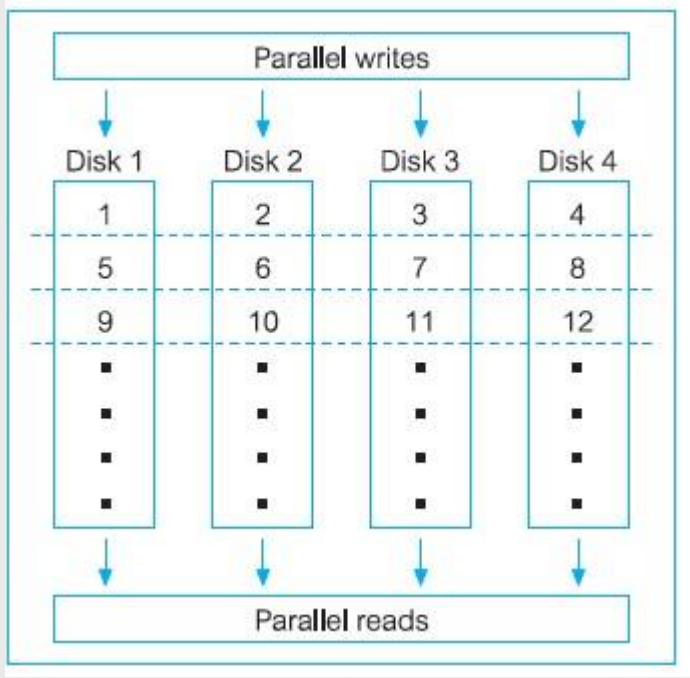
Advantages of this new storage subsystem is increased capacity, data security, and performance,

The tradeoff, however , is increased cost and complexity.

Data Striping

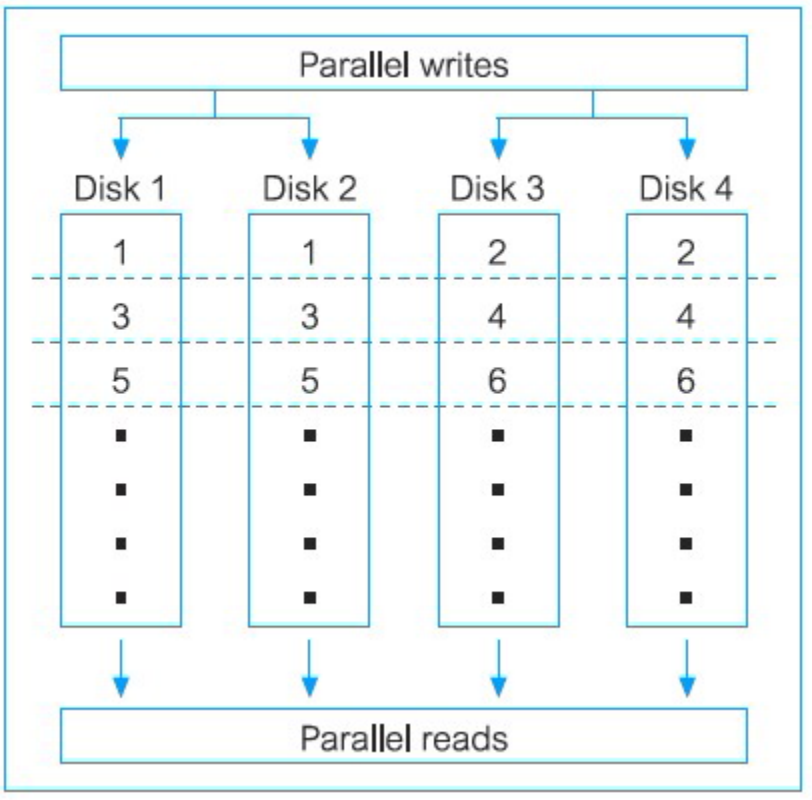
- Performance is increased through ***data striping***: the data is segmented into equal-size partitions (the *striping unit*), which are transparently distributed across multiple disks.





Mirrored

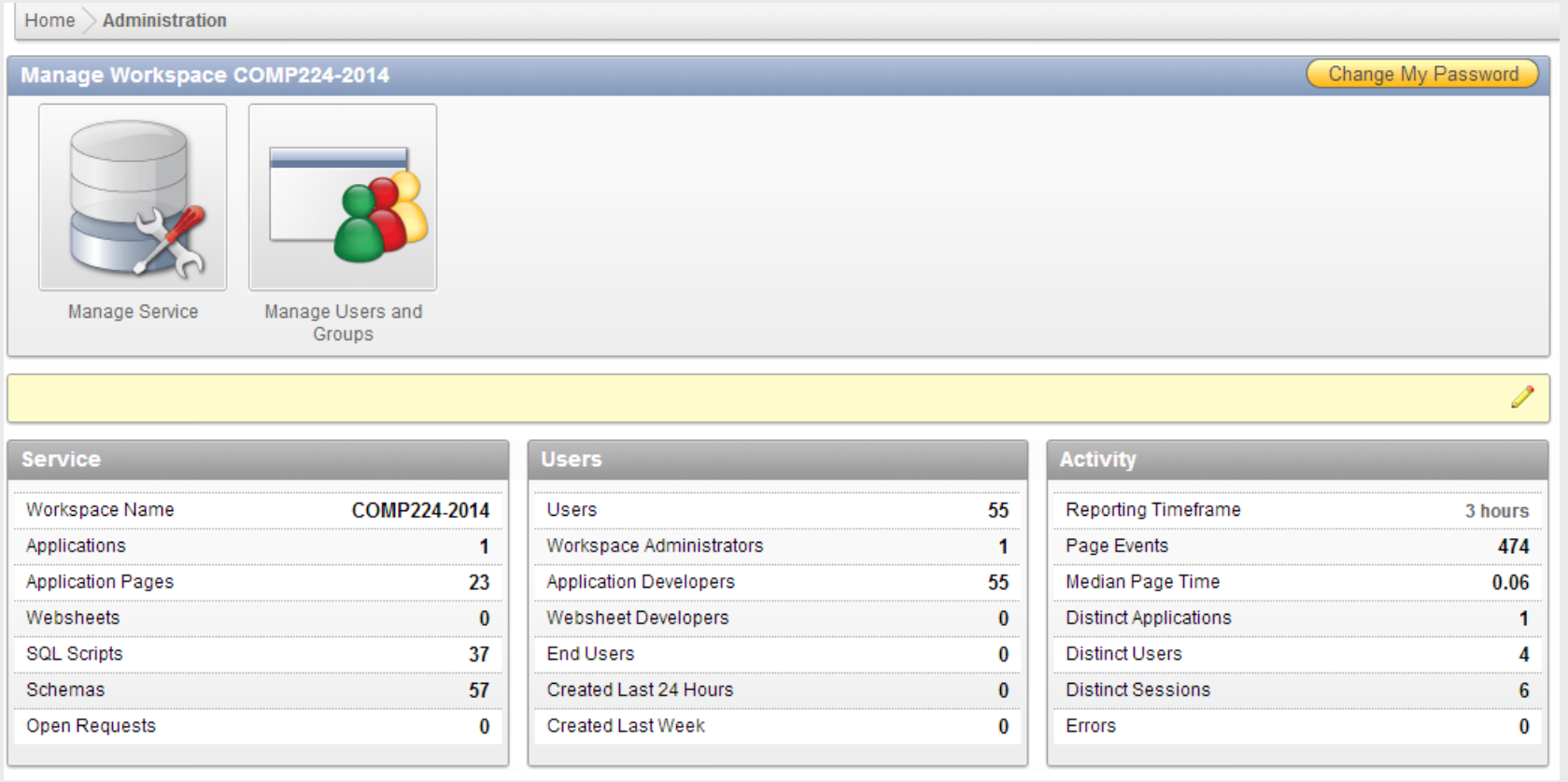
- System maintains (*mirrors*) two identical copies of the data across different disks. To maintain consistency in the presence of disk failure,



Security in Oracle APEX

- **Oracle Application Express** is a rapid Web application development tool for the Oracle database. Using only a Web browser and limited programming experience, you can develop professional applications that are both fast and secure.

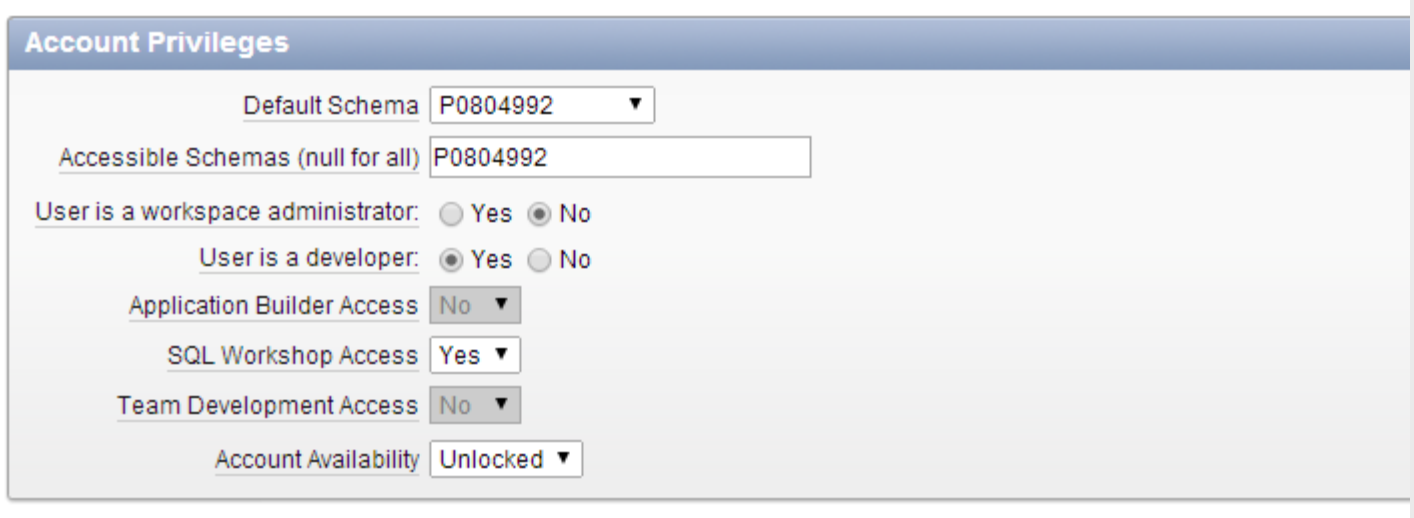
Administration

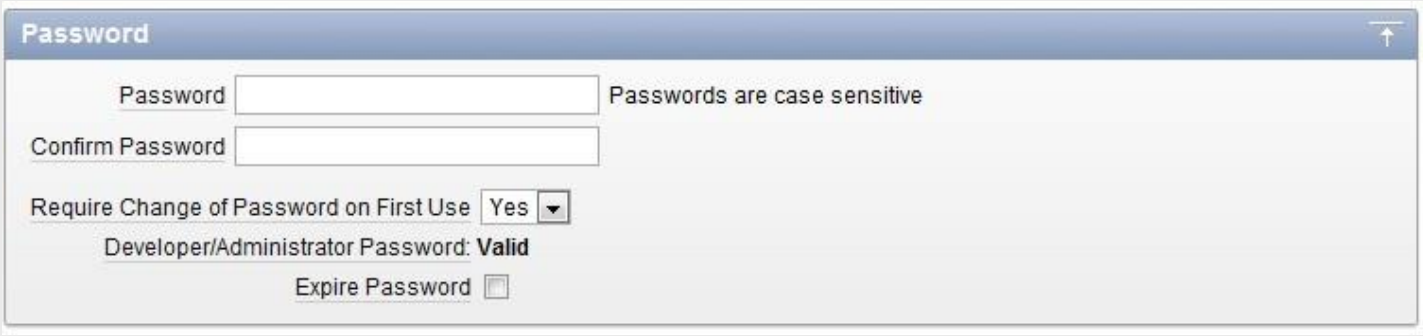


Edit User


Show All
Edit User
Account Privileges
Password
User Groups
Edit User
Workspace: COMP224-2014
* Username
P0804992
* Email Address
P0804992@ipm.edu.mo
First Name
Last Name
Description

Account Privileges and Password





a **privilege** is a right to execute a particular type of SQL statement or to access another user's objects.

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:**
  - Privacy --inaccessible to anyone but sender and receiver;
  - Integrity--not changed during transmission;
  - Authenticity--receiver can be sure it came from sender ;
  - Non-fabrication--sender can be sure receiver is genuine;
  - Non-repudiation--sender cannot deny he or she sent it.
- **Must also protect information once it has reached Web server.**
- **Download may have executable content, which can perform malicious actions, and measures need to be taken to prevent them.**

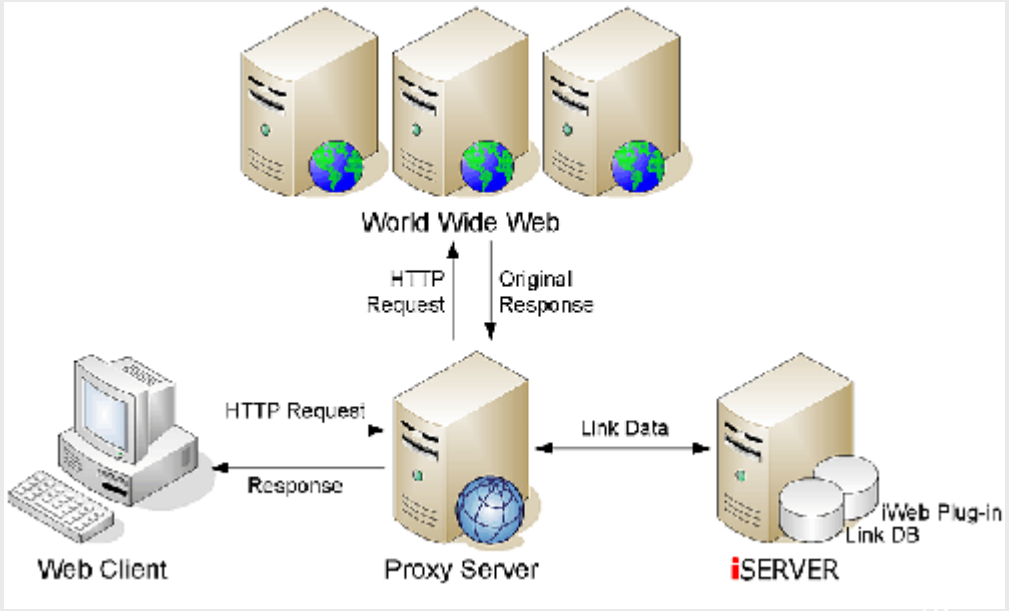
DBMSs and Web Security

- **Issues associated with database security on the public Internet and private intranets:**
  - Proxy servers
  - Firewalls
  - Public key cryptography
  - Message digest algorithms and digital signatures
  - Digital certificates

Proxy Servers

- Proxy server is computer that sits between browser and Web server.
- It intercepts all requests to Web server to try to fulfill requests itself.
- Has two main purposes:
  - improve performance;
  - filter requests.

Problem: proxy server owner can keep a look and there he/she can find many sensitive data like passwords and username, web browsing history.



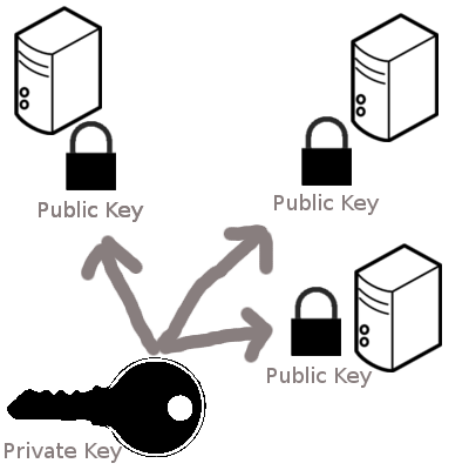
Firewalls

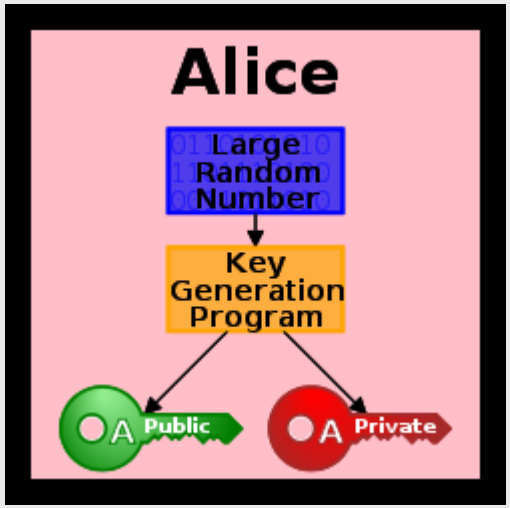
- **A system designed to prevent unauthorized access to/from a private network.**
- Can be implemented in both hardware and software, or a combination of both.
- Several types of firewall techniques: Packet filter, Application gateway, Circuit-level gateway, Proxy server.

Problem: firewalls assume that "bad guys" are on the outside only.

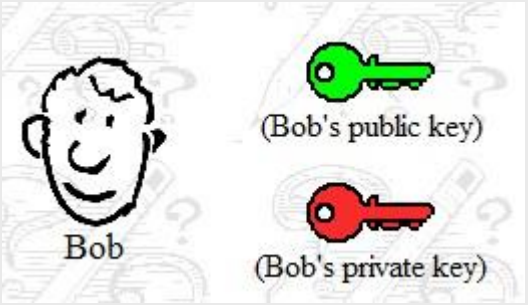
Public key cryptography

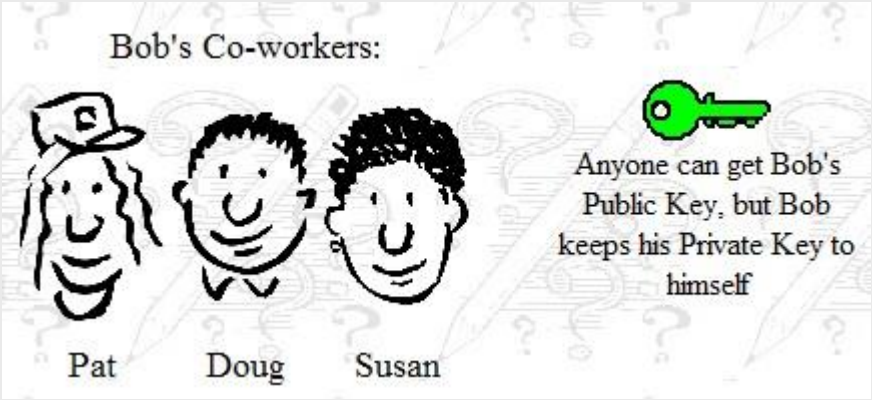
- Two separate keys generated by asymmetric key algorithms:
  - One to lock or encrypt the plaintext, and one to unlock or decrypt the cyphertext.
  - Public key is published, and private key is kept secret. Anyone with a copy of your public key can then encrypt information that only you can read.
  - It is computationally infeasible to deduce the private key from the public key



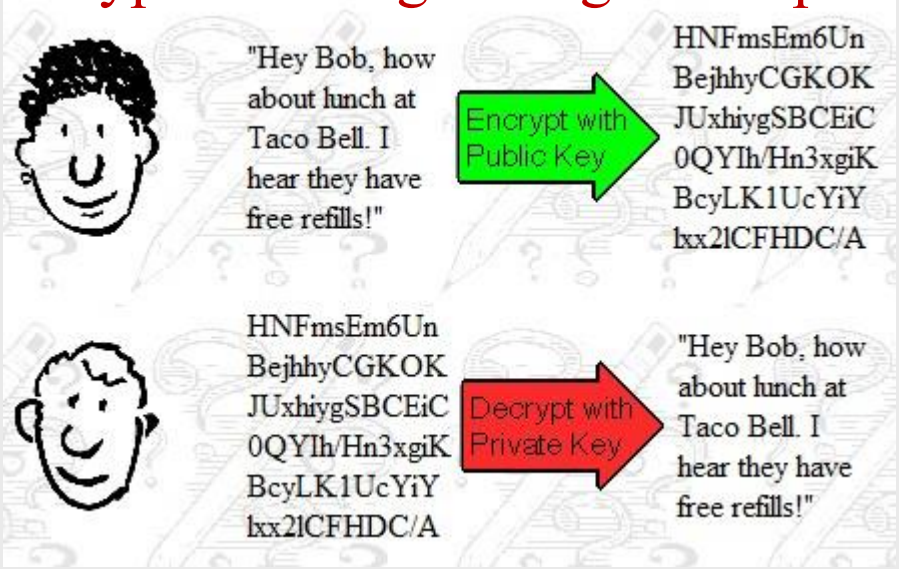


Public Key Cryptography





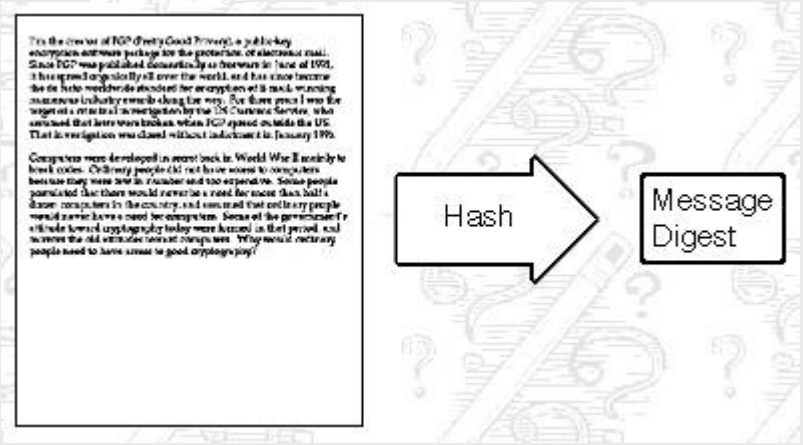
Susan can encrypt a message using Bob's public key



Bob use his private key to decrypt the message

Digital Signature

To sign a document, Bob use a mathematic function to compute a message digest.



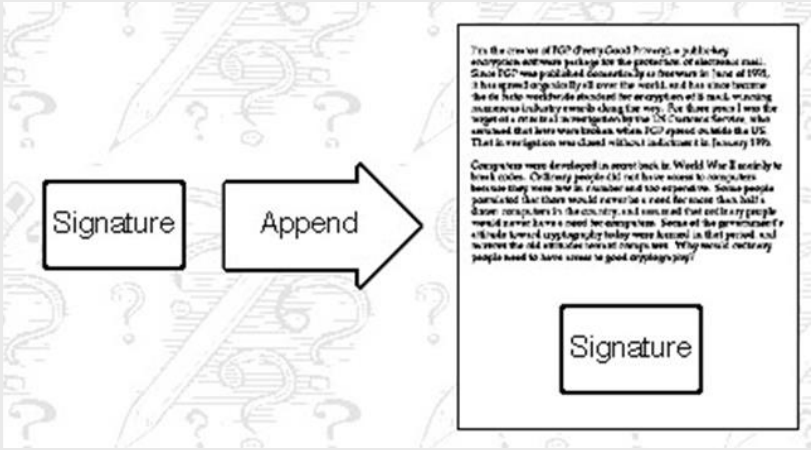
- *A message of any length, even thousands or millions of bits — and produces a fixed-length output; say, 160-bits.*
- *if the information is changed in any way — even by just one bit — an entirely different output value is produced.*

Message digest algorithm (one way hash function) takes an arbitrary-sized string (*message*) and generates fixed-length string (*digest* or *hash*).

Digital Signature

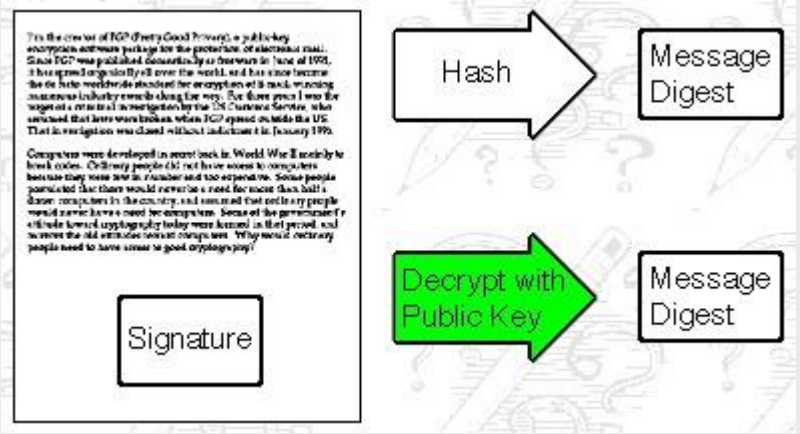
Then encrypt the message digest with **his private key**. This is ***digital signature***

Finally, append the digital signature to document



Digital Signature

Pat receive document from Bob.



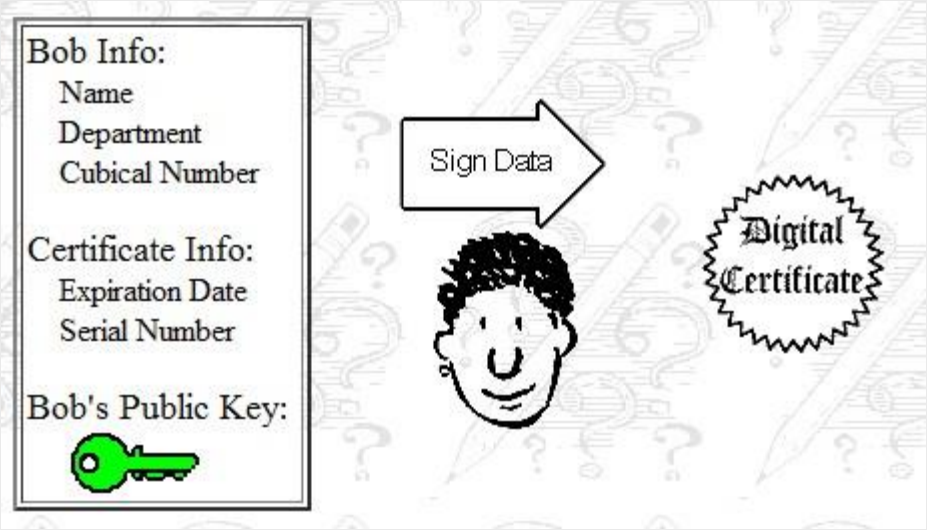
A digital signature is derived by applying a mathematical function to compute the message digest of an electronic message or document, and then encrypt the result of the computation with the signer's private key.

Decrypts the signature(using Bob's public key) changing it back into a message digest--*Bob signed the document*.
If two message digests are same--*the signed data has not been changed.*

Plot Complication…

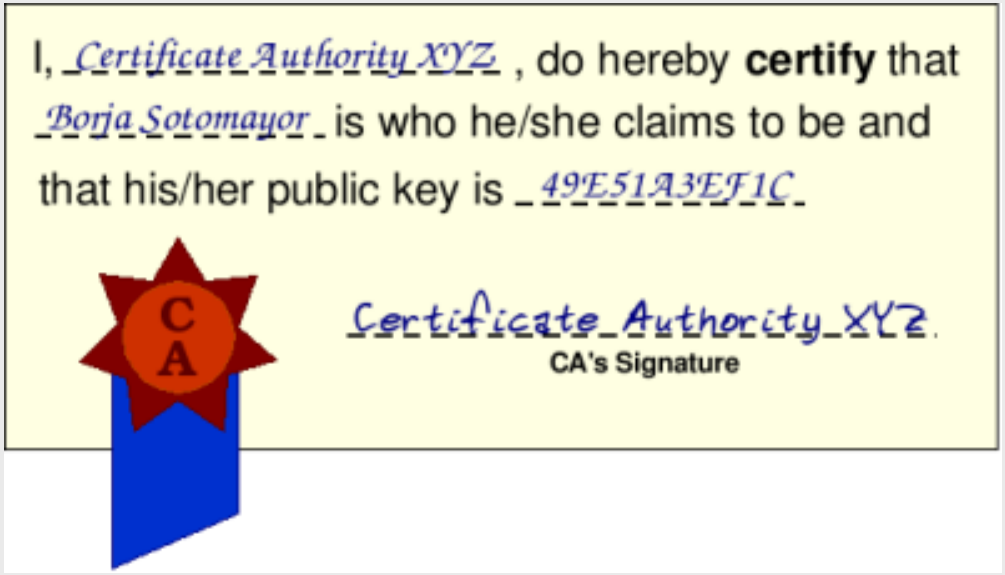
The public key is from  ?

- Susan works at the company's certificate authority center. Susan can create a **digital certificate** for Bob.



Digital Certificates

- A ***digital certificate*** is a digital document that *certifies* that a certain public key is owned by a particular user. This document is signed by a third party called the *certificate authority* (or CA).



Sender applies for certificate from CA.

CA issues encrypted certificate containing applicant's public key and other identification information.

End