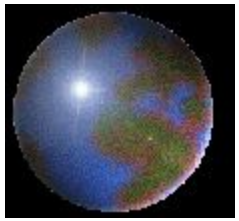
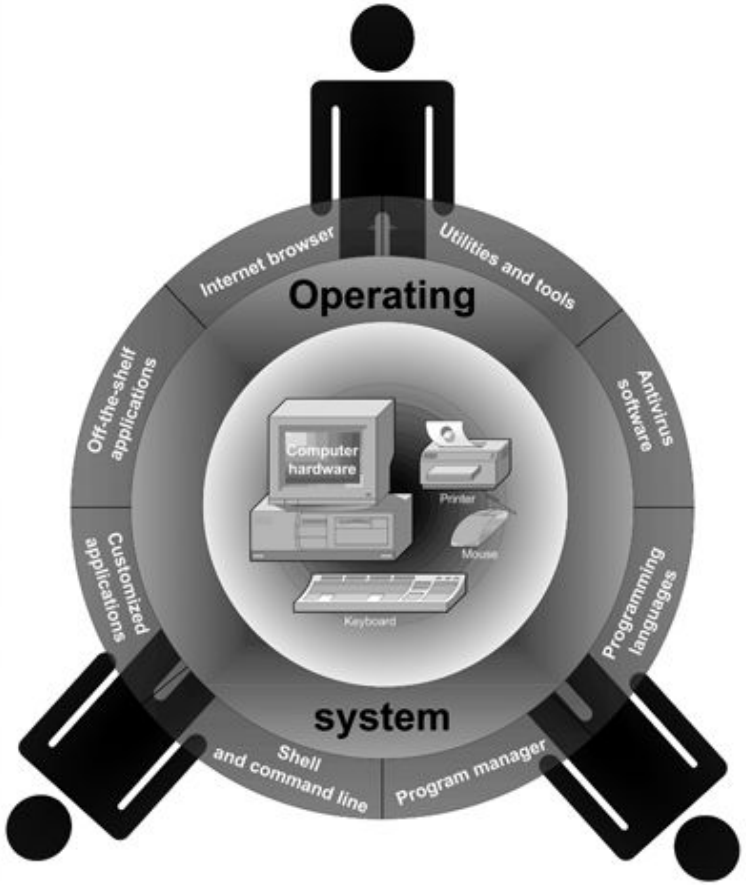


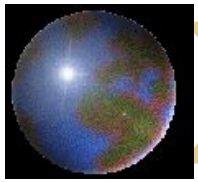
Database Security and Auditing: Protecting Data Integrity and Accessibility

Chapter 2
Operating System Security Fundamentals

Operating System Overview

- Operating system: collection of programs that allows user to operate computer hardware
- Three layers:
  - Inner layer, computer hardware
  - Middle layer, operating system
  - Outer layer, different software



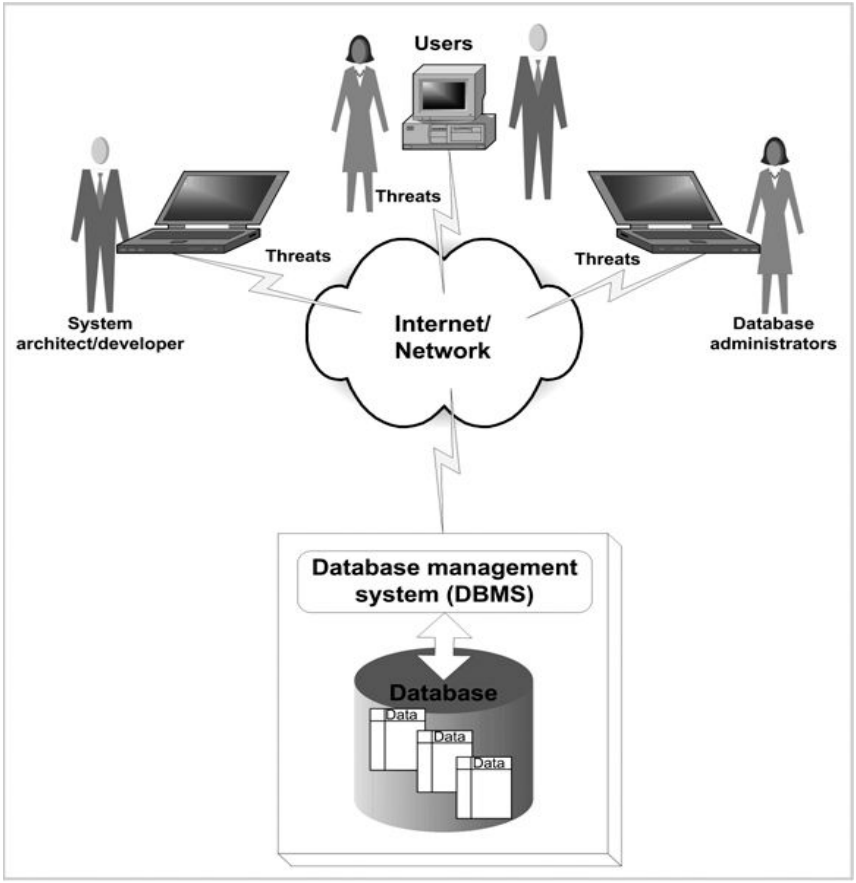


Operating System Overview

- Key functions of an operating system:
  - Multitasking, multisharing
  - Computer resource management
  - Controls the flow of activities
  - Provides a user interface
  - Administers user actions and accounts
  - Runs software utilities and programs
  - Enforce security measures
  - Schedule jobs
  - Provide tools to configure the operating system and hardware

The OS Security Environment

- A compromised OS can compromise a database environment
- Physically protect the computer running the OS (padlocks, chain locks, guards, cameras)
- Model:
  - Bank building (operating system)
  - Safe (database)
  - Money (data)



The Components of an OS Security Environment

- Used as access points to the database
- Three components:
  - Services
  - Files
  - Memory

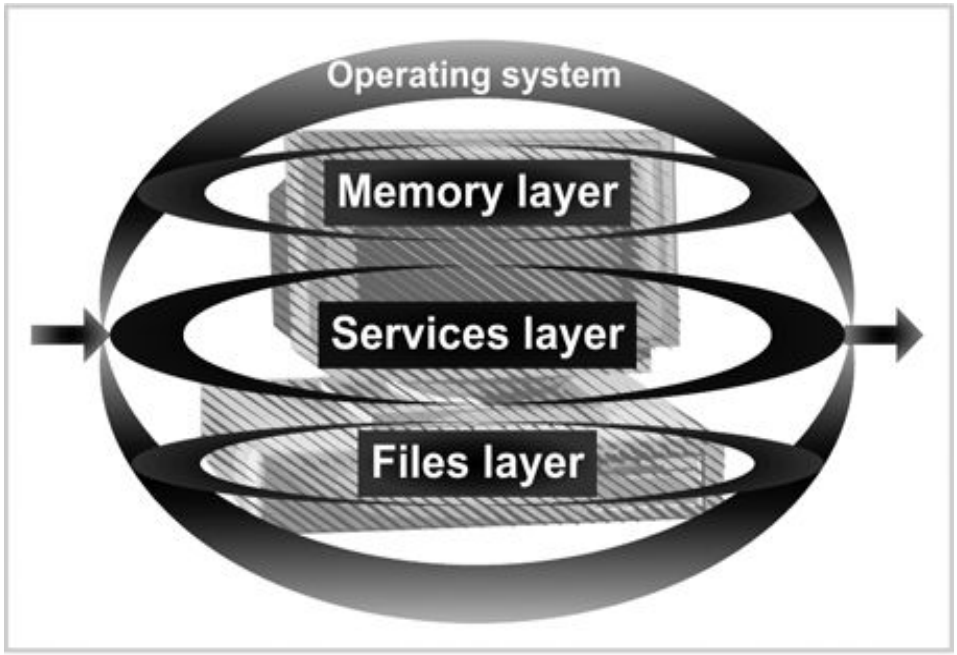
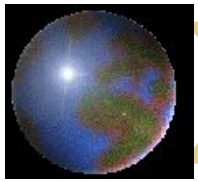
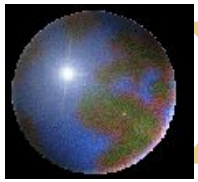


FIGURE 2-3 Operating system security environment



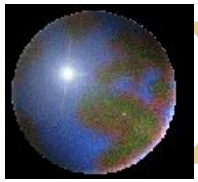
Services

- Main component of operating system security environment
- Used to gain access to the OS and its features
- Include
  - User authentication
  - Remote access
  - Administration tasks
  - Password policies



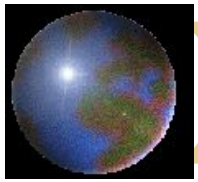
Files

- Common threats:
  - File permission
  - File sharing
- Files must be protected from unauthorized reading and writing actions
- Data resides in files; protecting files protects data



File Permissions

- Read, write, and execute privileges
- In Windows:
  - Change permission on the Security tab on a file's Properties dialog box
  - Allow indicates grant; Deny indicates revoke



File Permissions (continued)

- In UNIX/Linux
  - Three permission settings: owner; group to which owner belongs; all other users
  - Each setting consist of rwx
    - r for reading, w for writing, and x for executing
  - CHMOD command used to change file permissions

File Permissions (continued)

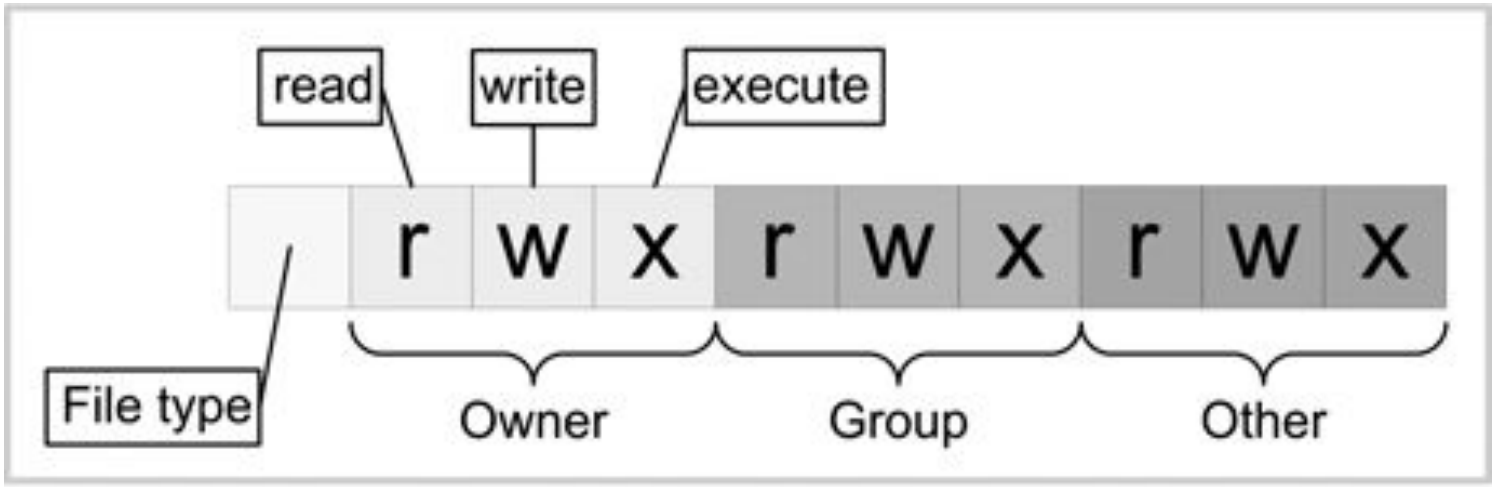
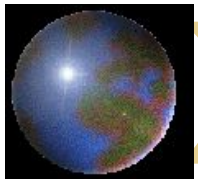


FIGURE 2-5 UNIX file permissions

```
$ chmod  644  mail_list
```

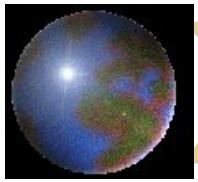


File Transfer

- FTP (File Transfer Protocol):
  - Internet service for transferring files from one computer to another
  - Transmits usernames and passwords in plaintext
  - Root account cannot be used with FTP
  - Anonymous FTP: ability to log on to the FTP server without being authenticated

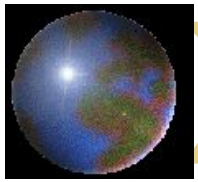
File Transfer (continued)

- Best practices:
  - Use Secure FTP utility if possible
  - Make two FTP directories:
    - One for uploads with write permissions only
    - One for downloads with read permissions only
  - Use specific accounts with limited permissions
  - Log and scan FTP activities
  - Allow only authorized operations



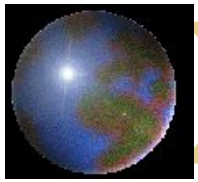
Sharing Files

- Naturally leads to security risks and threats
- Peer-to-peer programs: allow users to share files over the Internet
- Reasons for blocking file sharing:
  - Malicious code
  - Adware and spyware
  - Privacy and confidentiality
  - Pornography
  - Copyright issues



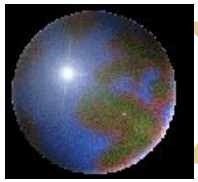
Memory

- Hardware memory available on the system can be corrupted by badly written software
- Can harm data integrity
- Two options:
  - Stop using the program
  - Apply a patch (service pack) to fix it



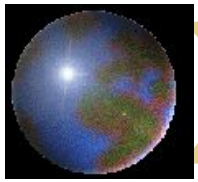
Authentication Methods

- Authentication:
  - Verifies user identity
  - Permits access to the operating system
- Physical authentication:
  - Allows physical entrance to company property
  - Magnetic cards and biometric measures
- Digital authentication: verifies user identity by digital means



Authentication Methods (continued)

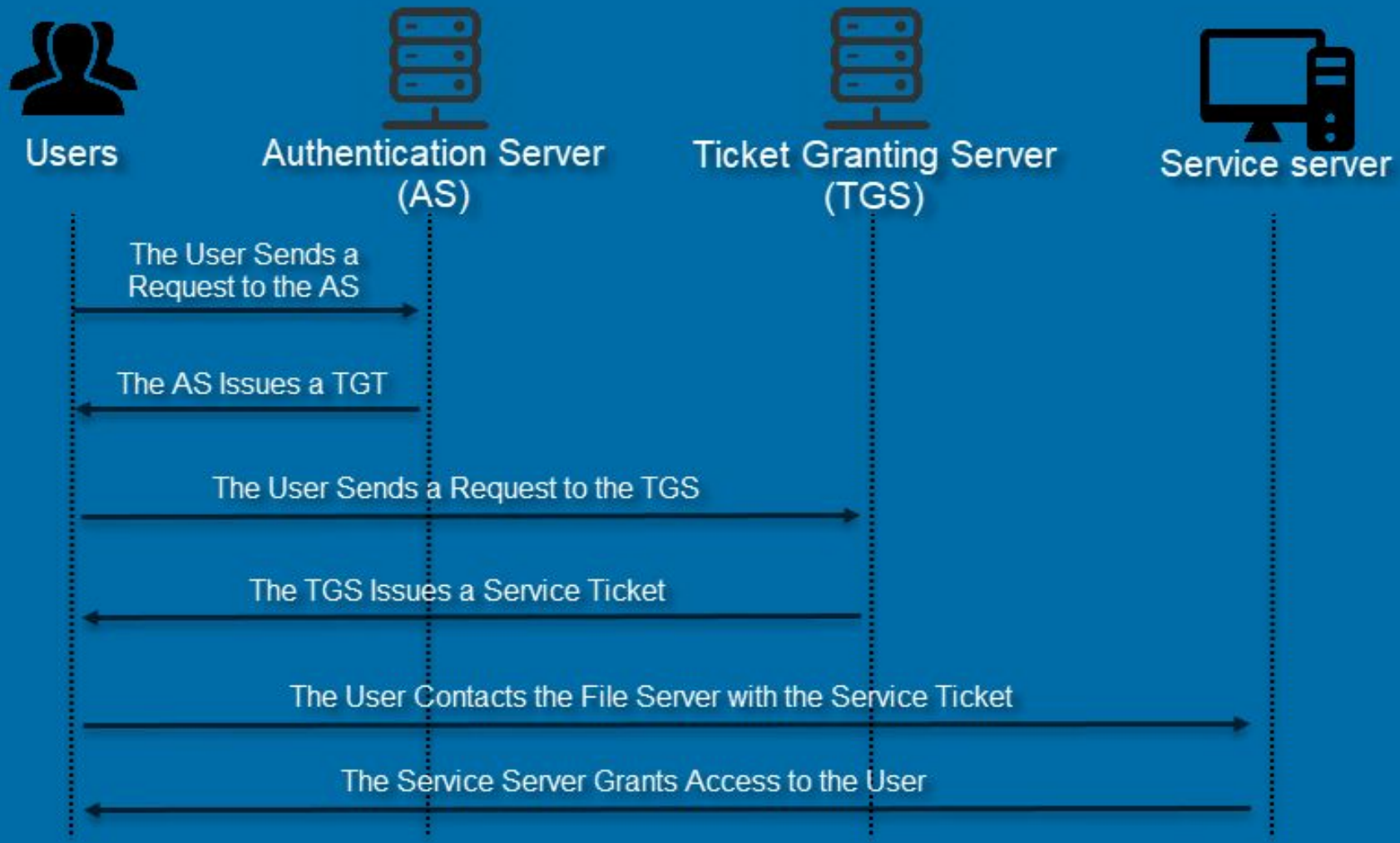
- Digital certificates: digital passport that identifies and verifies holder of certificate
- Digital token (security token):
  - Small electronic device
  - Displays a number unique to the token holder; used with the holder's PIN as a password
  - Uses a different password each time

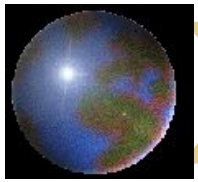


Authentication Methods (continued)

- Digital card:
  - Also known as a security card or smart card
  - Similar to a credit card; uses an electronic circuit instead of a magnetic strip
  - Stores user identification information
- Kerberos:
  - Developed by MIT
  - Uses tickets for authentication purposes

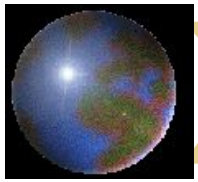
How Kerberos Grants Access to Users





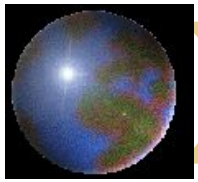
Authentication Methods (continued)

- Lightweight Directory Access Protocol (LDAP):
  - Developed by the University of Michigan
  - A centralized directory database stores:
    - Users (user name and user ID)
    - Passwords
    - Internal telephone directory
    - Security keys
  - Efficient for reading but not suited for frequently changing information



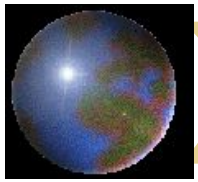
Authentication Methods (continued)

- NT LAN Manager (NTLM):
  - Developed and used by Microsoft
  - Employs a challenge/response authentication protocol
- Public Key Infrastructures (PKI):
  - User keeps a private key
  - Authentication firm holds a public key
  - Encrypt and decrypt data using both keys



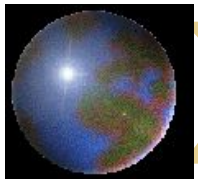
Authentication Methods (continued)

- RADIUS: used by network devices to provide a centralized authentication mechanism
- Secure Socket Layer (SSL): authentication information is transmitted over the network in an encrypted form
- Secure Remote Password (SRP):
  - Password is not stored locally
  - Invulnerable to brute force or dictionary attacks



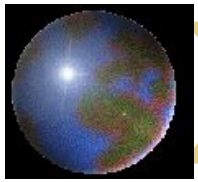
Authorization

- Process that decides whether users are permitted to perform the functions they request
- Authorization is not performed until the user is authenticated
- Deals with privileges and rights



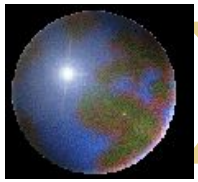
User Administration

- Create user accounts
- Set password policies
- Grant privileges to users
- Best practices:
  - Use a consistent naming convention
  - Always provide a password to an account and force the user to change it at the first logon
  - Protect passwords
  - Do not use default passwords



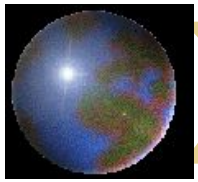
User Administration (continued)

- Best practices (continued):
  - Create a specific file system for users
  - Educate users on how to select a password
  - Lock non-used accounts
  - Grant privileges on a per host basis
  - Do not grant privileges to all machines
  - Use ssh, scp, and Secure FTP
  - Isolate a system after a compromise
  - Perform random auditing procedures



Password Policies

- First line of defense
- Dictionary attack: permutation of words in dictionary
- Make hard for hackers entering your systems
- Best password policy:
  - Matches your company missions
  - Enforced at all level of the organization



Password Policies (continued)

- Best practices:
  - Password aging
  - Password reuse
  - Password history
  - Password encryption
  - Password storage and protection
  - Password complexity
  - Logon retries
  - Single sign-on enables a user to log in once and gain access to the resources of multiple software systems without being prompted to log in again

Vulnerabilities of OS

- Top vulnerabilities to Windows systems:
  - Internet Information Services (IIS)
  - Microsoft SQL Server (MSSQL)
  - Windows Authentication
  - Internet Explorer (IE)
  - Windows Remote Access Services
  - Microsoft Data Access Components (MDAC)
  - Windows Scripting Host (WSH)
  - Microsoft Outlook and Outlook Express
  - Windows Peer-to-Peer File Sharing (P2P)
  - Simple Network Management Protocol (SNMP)

National Vulnerability Database:

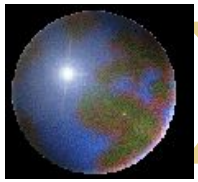
http://nvd.nist.gov/

Vulnerabilities of OS

National Vulnerability Database:

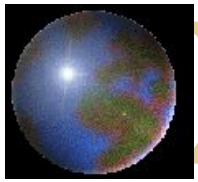
http://nvd.nist.gov/

- Top vulnerabilities to UNIX systems:
  - BIND Domain Name System
  - Remote Procedure Calls (RPC)
  - Apache Web Server
  - General UNIX authentication accounts with no passwords or weak passwords
  - Clear text services
  - Sendmail
  - Simple Network Management Protocol (SNMP)
  - Secure Shell (SSH)
  - Misconfiguration of Enterprise Services NIS/NFS
  - Open Secure Sockets Layer (SSL)



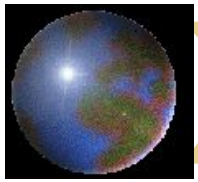
E-mail Security

- Tool must widely used by public
- May be the tool must frequently used by hackers:
  - Viruses
  - Worms
  - Spam
  - Others
- Used to send private and confidential data as well as offensive material



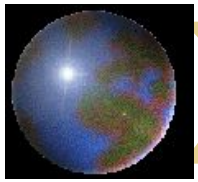
E-mail Security (continued)

- Used by employees to communicate with:
  - Clients
  - Colleagues
  - Friends
- Recommendations:
  - Do not configure e-mail server on the same machine where sensitive data resides
  - Do not disclose technical details about the e-mail server



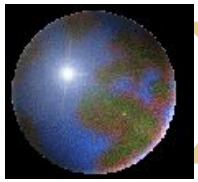
Summary

- Operating system:
  - Collection of programs that allows programs and users to interact with the computer resources
  - Main access point to the DBMS
- Authentication:
  - Validates the identity of the user
  - Physical authentication
  - Digital authentication



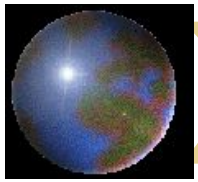
Summary (continued)

- Authorization:
  - Determines whether the user is permitted to perform the function he or she requests
  - Is not performed until the user is authenticated
  - Deals with privileges and rights that have been granted to the user



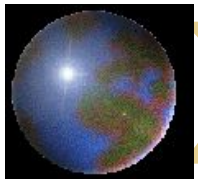
Summary (continued)

- Password policy:
  - First line of defense
  - Must match your company missions
  - Must be enforced at all levels of the organization
- Security problems with files:
  - File permissions
  - File transfer and sharing
- E-mail security



Quick Quiz

- A(n) _____ is a collection of programs that allows the user to operate the computer hardware.
  A. information system
  B. database
  C. DBA
  D. operating system
- The components that make up the operating system security environment are used as _____ to the database.

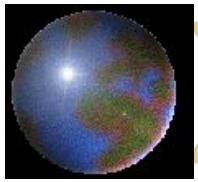


Quick Quiz

- The main component of the operating system security environment is _____.

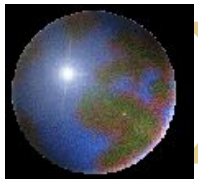
A. services
B. file transfer
C. memory
D. file sharing

- The _____ method is the process of verifying the identity of the user by means of a digital mechanism or software.



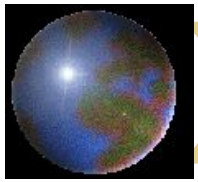
Quick Quiz

- _____ is a process that decides whether users are permitted to perform the functions they request.
  A. Identification
  B. Authentication
  C. Authorization
  D. Verification
- _____ allows you to sign on once to a server (host machine) and then not have to sign on again if you go to another server where you have an account.
  A. Password history
  B. Password reuse
  C. Logon retries
  D. Single sign-on



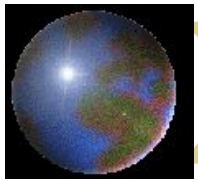
Lab 2 – Part I
Hardening OS

- Suppose you are the security manger for a small high-tech company. Outline security measures that you would implement to protect the operating system containing code for a new product innovation.
- Everyone research on this topic and prepare a 5-minute presentation with 10-page slides in the next meeting.



More on Hardening OS

- Hardening Linux
  - Hardening Linux by John Terpstra, et al
  - Hardening Linux by James Turnbull
- Hardening Windows
  - Hardening Windows Systems by Roberta Bragg
  - Hardening Windows by Jonathan Hasell
- Hardening Solaris
  - http://www.boran.com/security/sp/Solaris_hardening.html



Lab 2 – Part II(for practice)
Password Crackers

- Top 10 password crackers:
  http://sectools.org/crackers.html

  - Cain & Abel is a password recovery tool:
    http://www.oxid.it/cain.html
  - John the Ripper password cracker:
    http://www.openwall.com/john/doc/
  - Crack by Alec Muffett:
    http://lib.ru/SECURITY/crackfaq.txt
  - Ophcrack: http://ophcrack.sourceforge.net/

Lab 2:

- Report your findings about how to harden one of the selected OS.
- Download and report one of the password cracker software