

---

# Lectures 9

## Advanced Operating Systems

### Fundamental Security

Computer Systems Administration  
TE2003



# Lecture overview

- At the end of lecture 9 students can identify, describe and discuss:
  - Main factors while selecting an OS
  - OS optimization
  - Advances OS preventive maintenance and troubleshooting
  - Computer Security
  - Security threats
  - Security: prevention and troubleshooting

# Advanced Operating Systems

# Review – OS purpose

## 1. Communicate with hardware

- RAM, HD, CPU, keyboard, mouse, ...
- Drivers

## 2. User interface

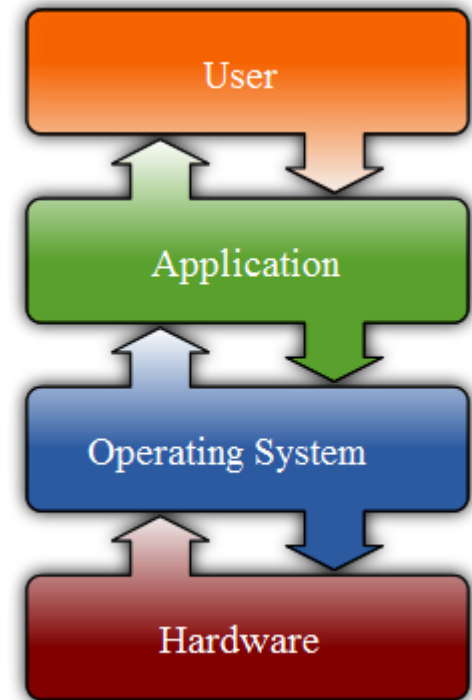
- Visual representation of the computer (GUI and CLI)

## 3. Platform for applications

- Run, use, and shutdown programs

## 4. Organizing and manipulating Programs and Data

- Add, move, and delete files and folders



# Review – OS types

- Single-tasking vs. Multi-tasking
- Single-user vs. Multi-user
- Multithreading
- Embedded
- 32-bit vs. 64-bit
- Desktop OS vs. Network OS
- Multi-processing
  - Refers to HW

*Factors to consider while selecting an OS*

# OS – Other features

- Remote Desktop
- Network Sharing
- Scalable CPU Support
- Encrypted File System (EFS)
- Enhanced Security
- Network Operating Systems (NOS)
  - A server enables clients to share resources
  - Increased functionalities and management
    - Network protocols
      - HTTP, FTP, POP3, DHCP, ...

*Factors to consider while selecting an OS*

# OS

## Windows directory structure

- You might need to know the location of data
  - Manual clean out
- Structure can differ between OS versions
  - XP: c:\Documents and Settings\User\_name\My\_Documents\
    - W7: c:\Users\User\_name\Documents\
      - XP: c:\Windows\Temp\
        - W7: c:\Users\User\_name\AppData\Local\Temp\
          - Specific purpose
            - User File Location
            - System File Location
            - Temporary Files
            - Program Files

# OS

## Installation

- **Default**
  - Requires user attention
- **Custom**
  - Allow users to automate certain activities
  - **Unattended**
  - **Image-based installation**
  - **Remote installation (RIS)**



# OS

## Installation

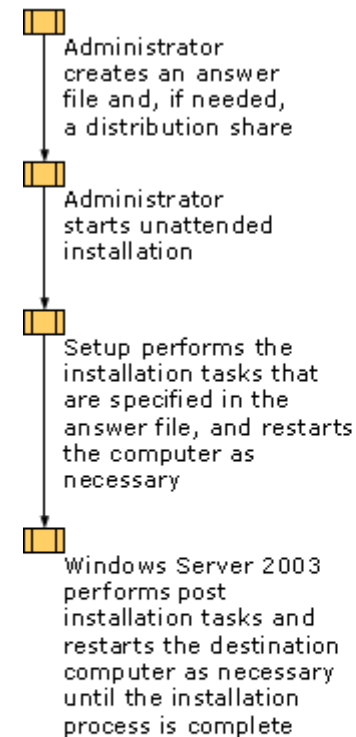
- **Custom**
  - **Unattended**
    - Administrators create an answer file that instructs the Windows Setup about how to install and configure the OS
  - **Image-based installation**
    - Copying preconfigured OS and SW applications to computers
  - **Remote installation (RIS)**
    - Computers without an OS start up and connect to a remote RIS server, which installs the OS

Windows  
System  
Image  
Manager  
(SIM)

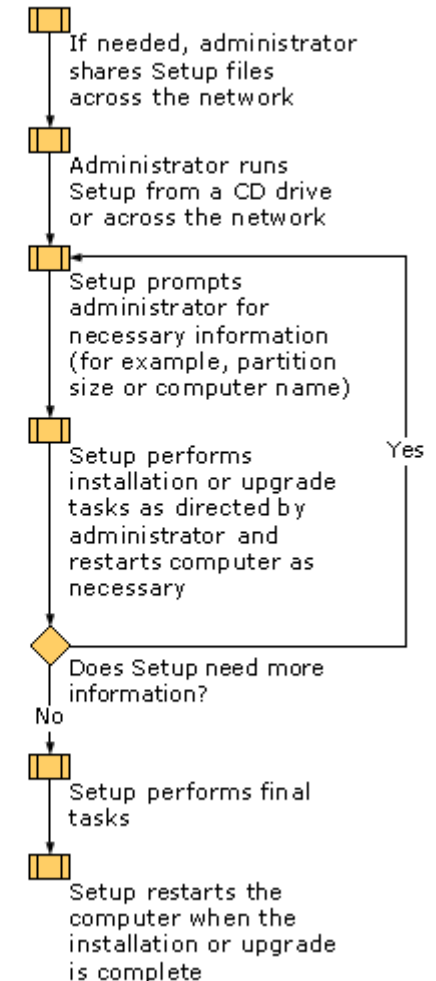
Sysprep

Preboot  
eXecution  
Environment  
(PXE)

### Unattended Installation



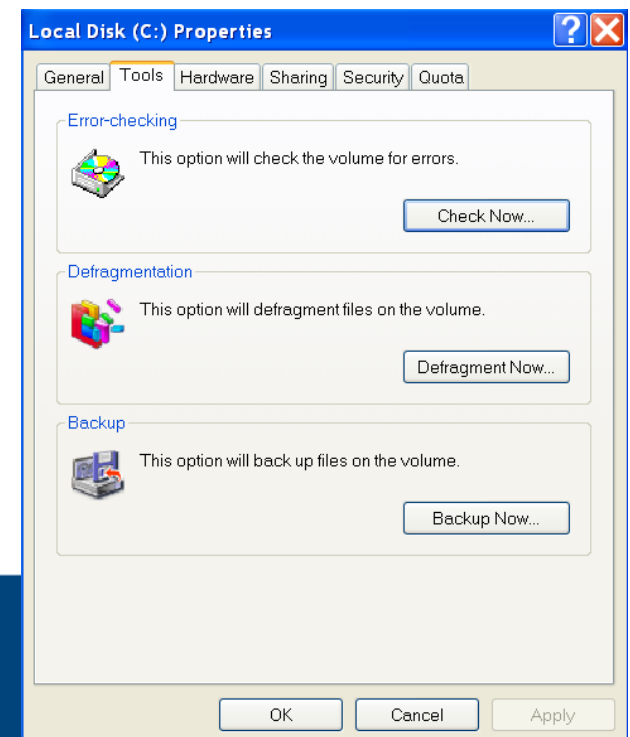
### Interactive Setup



# OS – Optimization

## System and Administrative Tools

- **Disk management**
  - Disk management utility
  - Disk defragmenter
  - Complete analysis of disk partition
  - Disk partitioning tool
- **Device Manager**
- **Task Manager**
- **Services**
- **Virtual Memory**



# OS – Optimization

## System and Administrative Tools

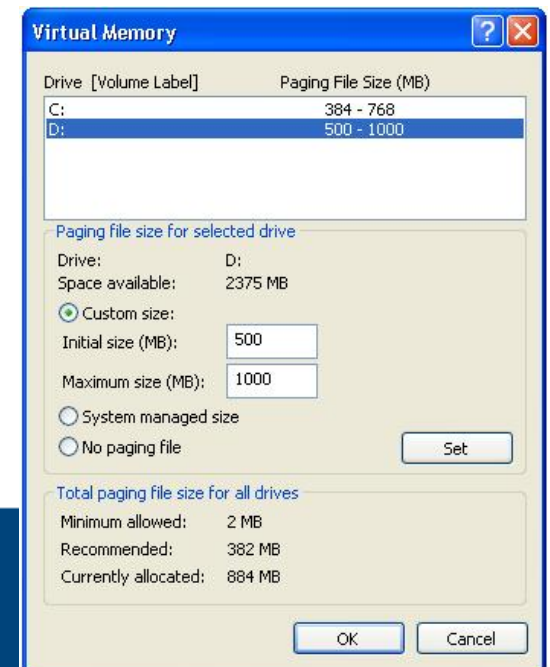
- **Services**

- Applications that runs in the background and waits for requests
- Services may be started, if need, and stopped, for example, for troubleshooting purposes
- Startup mode
  - **Automatic, Manual, Disabled**
- Status
  - **Started or Stopped**
- DHCP, Automatic update, ...

# OS – Optimization

## System and Administrative Tools

- Virtual Memory
  - Optimize the performance of operating systems
  - Uses the hard drive to temporarily store segments of an application or data
  - The OS uses the swap file to mimic RAM
  - Requires administrative privileges to change the size of the swap file
  - Typically, you should let Windows manage the size of the swap file



# OS – Optimization

## Software applications

- Web browsers
  - Cookies
  - Temporary files
  - History
  - Passwords
  - Caching
- Email clients

# OS – Command Line Interface

- DOS
  - CLI or text-based OS
- How to access the CLI on windows?
- Commands and switches?
- How to change directories?
- How to display the contents of directories?
- How to edit a file?
- How to copy files from one location to another? What about copying a entire folder and its contents?
- How to create and remove a directory?
- How to navigate to a different directory?

# OS – Preventive maintenance

- Schedule Automatic Tasks and Updates
  - Task Scheduler
    - GUI: Taskschd.msc
    - CLI: at command
  - Windows Automatic Update
- Restore points
  - Problems happen
  - System Restore
    - Takes "snapshots" of critical system and program files, as well as registry settings, and stores this information as restore points

# Fundamental Security

# Computer and Network Security

- What is it?
- Why is it important?

# Computer and Network Security

- What is it?
  - Prevention and detection of unauthorized access and use of equipment and data
  - Data and equipment protection against disasters or hazards
- Why is it important?
  - Damage or loss of equipment can mean a loss of productivity
  - Repairing and replacing equipment can cost the company time and money
  - Unauthorized use of a network can expose confidential information and reduce network resources
  - Network attacks can lead to all the problems listed above

# Security Threats

- Physical Threats vs. Data Threats
- Internal Threats vs. External Threats
  - Internal Threats
    - Accidental threats vs. Malicious threats
  - External Threats
    - Unstructured attacks vs. Structured attacks
- Threats
  - Viruses, Worms, Trojans
  - Adware, Spyware, Grayware
  - DoS
  - Spam and Popup windows
  - Social Engineering
  - TCP/IP attacks
  - Data Wiping, Hard Drive Destruction, Recycling

# Viruses, Worms, and Trojan Horses

## **Virus**

- Program created by an attacker
- Collect, alter or destroy information

## **Worm**

- Self-replicating program that uses the network to duplicate its code to the hosts on the network
- Worms consume bandwidth in a network

## **Trojan horse**

- Program designed to look like one program (game or utility) that does something else

# Web Security

- Tools used to install a program on a computer
  - ActiveX
    - Controls interactivity on web pages
  - Java
    - Allows applets to run within a browser
  - JavaScript
    - Interacts with HTML source code to allow interactive web sites

# Adware, Spyware, Grayware

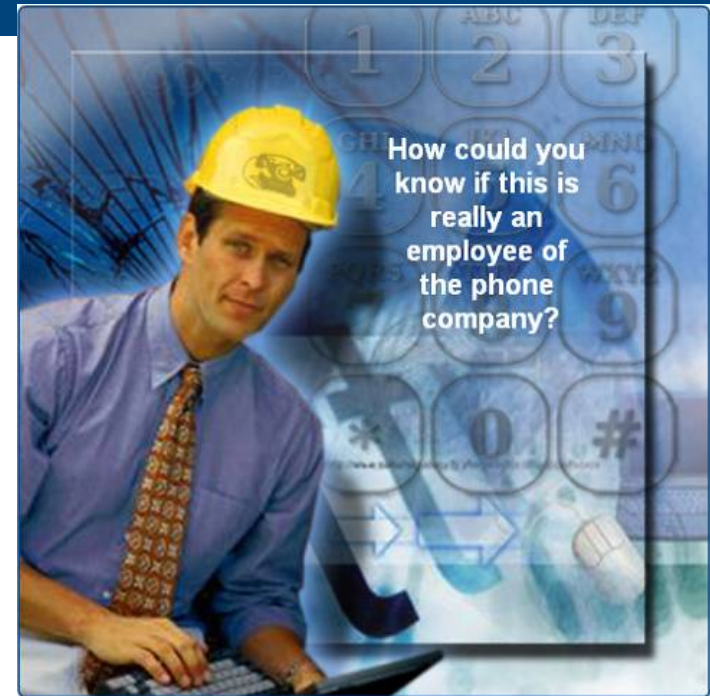
- Without the user's consent
  - Collect stored information
  - Change the computer configuration
  - Open extra windows
- Adware
  - Displays advertising, usually in a popup window.
- Grayware or malware
  - Many grayware attacks are phishing attacks
    - Phishing is a form of social engineering
    - Persuade the users to provide personal information.
- Spyware
  - Monitors computer activity then sends the information back to a remote machine

# Denial of Service (DoS)

- Form of attack that prevents users from accessing normal services
- Sends enough requests to overload a resource or even stopping its operation
- Ping of Death
  - Series of repeated pings intended to crash the receiving computer
- E-mail Bomb
  - Large quantity of bulk e-mail that overwhelms the e-mail server
- Distributed DoS
  - Uses many infected computers, called zombies, to launch an attack

# Other threats

- Spams or Junk email
- Popup windows
- Social Engineering
- TCP/IP attacks
  - SYN , DoS, Replay, ....
- Data Wiping
- Hard Drive Destruction
- Recycling



# Security Procedures

- Basic Local Security Policy
- Physical Equipment Protection
- Data Protection
  - Data Encryption
  - Software Firewall
  - Data Backup
  - File System Security
- Wireless Security
  - Service Set Identifier (SSID)
  - MAC address filtering
  - Encryption and authentication

# Security – Prevention

- Anti-virus
  - Designed to detect, disable, and remove viruses, worms, and Trojan horses
  - Use anti-virus software, options in e-mail software, popup blockers, and common indications of spam to combat spans.
- Browsers have settings that force the computer user to authorize the downloading or use of ActiveX, Java, or JavaScript
- Develop and maintain a security plan to protect both data and physical equipment from loss.
- Keep operating systems and applications up to date and secure with patches and service packs

