Overview

- Organization
- Model
- Components
- CPU Modes
- System processes
- Services processes
- Users processes
- Subsystems processes
- System services
OS Organization

- Access to hardware is not allowed
- Access to hardware is made via system services
OS Model

- Applications access the OS via one defined Application Program Interface (API)
OS Contexts

- Applications
  - CPU runs in user mode
- OS
  - CPU runs in kernel mode
CPU Modes

- Protect critical system data from user applications
  - User mode
  - Kernel mode
CPU Modes - mechanism

- User programs typically run in both modes
- CPU mode switch <> CPU context switch
Essential Windows Kernel Mode Components

CPU Modes - scenarios
TCB

- Context
  - No CPU restriction in kernel
  - No memory restriction in kernel
  - No security check in kernel
- Definition
  - Portions of the system trusted to enforce the security
- Components
  - Most hardware
  - All kernel code
  - Some user code (SeTcbPrivilege)
  - Administrators
Memory Layout

- Each application occupies 4 GB of address space
- All applications share system memory space
Essential Windows Kernel Mode Components

OS Major Components

- System processes
  - Session manager
  - Logon manager
  - Security manager
  - Services manager

- Services processes
  - alerter

- User processes
  - pinball
  - explorer

- Environment processes
  - POSIX
  - Win32

Executive

Hardware Abstraction Layer

Hardware
Environment Subsystems

- Definition
- Role
- Types
Environment Subsystems - interfaces

- Subsystem
  - Process runs in a private address space
- Application
  - Sends messages to subsystem
  - Unaware of messages
  - Implicitely linked with system's interfaces (image = code + metadata)

Diagram:

- application.exe
  - Functions calls
    - Windows API
      - Win32 API
        - Kernel32.dll
        - Gdi32.dll
        - User32.dll
    - Native API
      - Ntdll.dll
Environment Subsystems - strategy
Essential Windows Kernel Mode Components

Environment Subsystems - strategy

- Application
  - Win32 API
  - Subsystem DLLs
    - Native API
    - CPU mode switch
  - Subsystem
    - Executive
Environment Subsystems - strategy
# Environment Subsystems - strategy

<table>
<thead>
<tr>
<th>Service implementation</th>
<th>CPU mode switching</th>
<th>CPU context switching</th>
<th>Message sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>User process</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Executive</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Server</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Win16 Support

- MS-DOS applications
  - One-one relation
- Win16 applications
  - Many-one relation
System processes

- Are started by the system
- Are running on every system
- Cannot be stopped
Session Manager Subsystem

- Definition
- Role
- Particularities
  - Part of the TCB
  - Native user application
Logon Manager

- Definition
- Role
  - Interactive logon request management
  - Authentication User interface management
  - User profile initialization
  - Shell creation
  - TASKMGR management

<table>
<thead>
<tr>
<th>Who you are (identification)</th>
<th>What you know (authentication)</th>
<th>What you are (authentication)</th>
</tr>
</thead>
</table>

www.winitor.com
Local Security Authority Subsystem

- Definition
- Role
Essential Windows Kernel Mode Components

Service Control Manager

- Definition
- Role
User Processes - creation

- System
- SsMs
- Winlogon
- Csrss
- Userinit
- Shell
- Services
- Lsass

Permanent
Volatile (interactive)
Thanks!