Chapter 16

Managing and Supporting Windows XP
Security Using Windows NT/2000/XP

Goals

Secure system resources – including hardware and software – from improper use

Secure users’ data from improper access

Concept of user accounts is key to understanding Windows XP
User Accounts

Define a user to Windows

Record information about the user (user name, password, groups the account belongs to, rights and permissions assigned to the account)

Types

  Global

  Local

  Built-in
User Profiles

Created by system after administrator creates local user account and user logs for first time

Types

Roaming

Mandatory

Group
Administering Local User Accounts: Password Guidelines

Usernames: up to 15 characters

Passwords: up to 127 characters

Do not use a password that is easy to guess

Use combination of letters, numbers, and non-alphanumeric characters
Administering Local User Accounts: Password Guidelines (continued)

Set a password for Administrator account

Passwords can be controlled by administrator; generally users should be able to change their own

Create a forgotten password floppy disk
Creating a User Account

Figure 16-2  Create a user account using either Computer Management or the User Account applets in Control Panel
Options for Controlling How a User Logs On

Welcome screen (default)

User must press Ctrl-Alt-Del to get to logon window

Fast User Switching
User Groups

Types

- Administrators
- Backup Operators
- Power Users
- Limited Users
- Guests

Local policies can be assigned to a user group, affecting all users in the group.
Group Policy

Normally intended for use on a domain;

   Can also be used on a standalone or computer in a workgroup

Can be applied to the computer or can be applied to each user who logs on
Disk Quotas

Limit how much disk space user has access to. Does not specify location of files, just total space allowed. Can be set only if you are using NTFS.
EFS (Encrypted File System)

Process of putting readable data into code that must be translated before it can be accessed (usually done using a key)

Applies only to Windows 2000/XP NTFS file system
How to Use Encryption

Can be implemented at either the folder or file level

Folder level is encouraged and considered a “best practice” strategy
The Windows NT/2000/XP Registry

Hierarchical database containing information about all hardware, software, device drivers, network protocols, and user configuration needed by the OS and applications

Logical organization

   Upside-down tree structure (keys, subkeys, values)

Physical organization

   Stored in five files, called hives
Components That Use the Registry

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setup programs for devices and applications</td>
<td>Setup programs can record configuration information in the registry and query the registry for information needed to install drivers and applications.</td>
</tr>
<tr>
<td>User profiles maintained and used by the OS</td>
<td>Windows maintains a profile for each user that determines the user’s environment. User profiles are kept in files, but, when a user logs on, the profile information is written to the registry, where changes are recorded, and then later written back to the user profile file. The OS uses this profile to control user settings and other configuration information specific to this user.</td>
</tr>
<tr>
<td>Files active when Ntldr is loading the OS</td>
<td>During the boot process, NTDetect.com surveys present hardware devices and records that information in the registry. Ntldr loads and initializes device drivers using information from the registry, including the order in which to load them.</td>
</tr>
</tbody>
</table>
## Components That Use the Registry (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device drivers</td>
<td>Device drivers read and write configuration information from and to the registry each time they load. The drivers write hardware configuration information to the registry and read it to determine the proper way to load.</td>
</tr>
<tr>
<td>Hardware profiles</td>
<td>Windows can maintain more than one set of hardware configuration information (called a <strong>hardware profile</strong>) for one PC. The data is kept in the registry. An example of a computer that has more than one hardware profile is a notebook that has a docking station. Two hardware profiles describe the notebook, one docked and the other undocked. This information is kept in the registry.</td>
</tr>
<tr>
<td>Application programs</td>
<td>Many application programs read the registry for information about the location of files the program uses and various other parameters that were stored in .ini files under Windows 9x.</td>
</tr>
</tbody>
</table>

**Table 16-1** Components that use the Windows NT/2000/XP registry
Logical Organization of the Registry

Figure 16-11  The Windows NT/2000/XP registry is logically organized in an upside-down tree structure of keys, subkeys, and values.
## Five Subtrees of the Registry

<table>
<thead>
<tr>
<th>Subtree (Main Keys)</th>
<th>Primary Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKEY_CURRENT_USER</td>
<td>Contains information about the currently logged-on user</td>
</tr>
<tr>
<td>HKEY_CLASSES_ROOT</td>
<td>Contains information about software and the way software is configured. This key points to data stored in HKEY_LOCAL_MACHINE.</td>
</tr>
<tr>
<td>HKEY_CURRENT_CONFIG</td>
<td>Contains information about the active hardware configuration, which is extracted from the data stored in the HKEY_LOCAL_MACHINE subkeys called SOFTWARE and SYSTEM.</td>
</tr>
<tr>
<td>HKEY_USERS</td>
<td>Contains information used to build the logon screen and the ID of the currently logged-on user</td>
</tr>
<tr>
<td>HKEY_LOCAL_MACHINE</td>
<td>Contains all configuration data about the computer, including information about device drivers and devices used at startup. The information in this key does not change when different users log on.</td>
</tr>
</tbody>
</table>

Table 16-2  The five subtrees of the Windows NT/2000/XP registry
Editing the Registry

Modified automatically when you make a change (in Control Panel or Device Manager)
Rare occasions require a manual edit
Backup system state first;
   Changes take effect immediately and are permanent

Registry editors
   Regedt.32.exe (Windows NT/2000)
   Regedit.exe (Windows NT/2000/XP)
## Windows XP Maintenance and Troubleshooting Tools (continued)

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Information (Systeminfo.exe)</td>
<td>A version of System Information to be used from a command-prompt window</td>
</tr>
<tr>
<td>System Restore</td>
<td>Restores system to previously working condition; restores registry, some system and application files</td>
</tr>
<tr>
<td>Task Killing Utility (Tskill.exe)</td>
<td>Stops a process or program currently running</td>
</tr>
<tr>
<td>Task Lister (Tasklist.exe)</td>
<td>Lists currently running processes</td>
</tr>
<tr>
<td>Task Manager (Taskman.exe)</td>
<td>Lists and stops currently running processes</td>
</tr>
</tbody>
</table>
Windows Update

Figure 16-17  Windows Update process found updates appropriate to this computer
Troubleshooting the Boot Process (Hierarchical List)

Last Known Good Configuration (and sometimes Driver Rollback)
Safe Mode on Advanced Options menu
System Restore (new)
Windows 2000/XP Boot disk
Recovery Console
Automated System Recovery (new)
Reinstall Windows XP using Windows XP CD
# Advanced Options Menu

<table>
<thead>
<tr>
<th>Windows Advanced Options Menu</th>
<th>Please select an option:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safe Mode</td>
<td></td>
</tr>
<tr>
<td>Safe Mode with Networking</td>
<td></td>
</tr>
<tr>
<td>Safe Mode with Command Prompt</td>
<td></td>
</tr>
<tr>
<td>Enable Boot Logging</td>
<td></td>
</tr>
<tr>
<td>Enable VGA Mode</td>
<td></td>
</tr>
<tr>
<td>Last Known Good Configuration</td>
<td>(your most recent settings that worked)</td>
</tr>
<tr>
<td>Directory Services Restore Mode</td>
<td>(Windows domain controllers only)</td>
</tr>
<tr>
<td>Debugging Mode</td>
<td></td>
</tr>
<tr>
<td>Start Windows Normally</td>
<td></td>
</tr>
<tr>
<td>Reboot</td>
<td></td>
</tr>
<tr>
<td>Return to OS Choices Menu</td>
<td></td>
</tr>
</tbody>
</table>

Use the up and down arrow keys to move the highlight to your choice.

*Figure 16-18*  Windows XP Advanced Options menu
System Restore

Similar to ScanReg, but cannot be executed from command prompt

Restores system state using a restore point (snapshot of system settings and configuration)

Does not affect user data on hard drive but can affect installed software and hardware, user settings, and OS configuration settings

Cannot help recover from a virus or worm infection
Automated System Recovery

Restores system partition to its state when the backup was made

Changes made since last backup are lost

Periodically make fresh copies of ASR disk set