A Guide to Managing and Maintaining Your XP PC

Chapter 16

Managing and Supporting Windows XP

All Rights Reserved - שאול קובל מערכות מחשבים

You Will Learn…

- How to use Windows XP features to secure the PC and protect users and their data
- About the Windows NT/2000/XP registry
- About tools for troubleshooting and maintaining Windows XP
- How to troubleshoot the Windows XP boot process

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

Viewing User Profiles

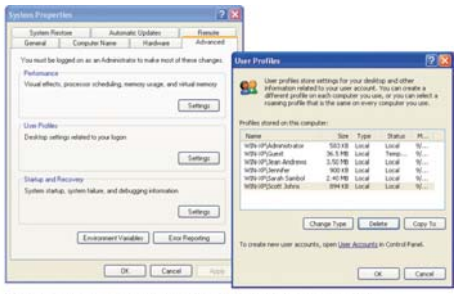

Figure 16-1 View all user profiles stored on this PC using the System Properties window

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

 All Rights Reserved - שאול קובל מערכות מחשבים

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

 All Rights Reserved - שאול קובל מערכות מחשבים

Creating a User Account

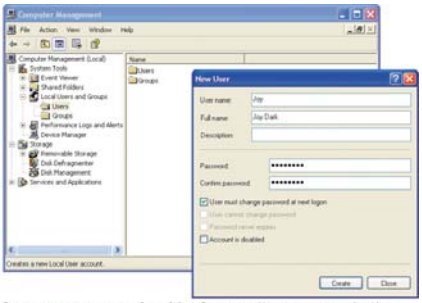

Figure 16-2 Create a user account using either Computer Management or the User Account applets in Control Panel

 All Rights Reserved - שאול קובל מערכות מחשבים

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

 All Rights Reserved - שאול קובל מערכות מחשבים

Controlling How a User Logs On and Off

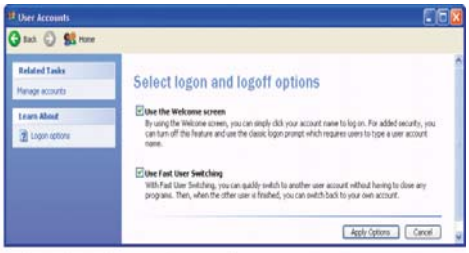

Figure 16-3 Options to change the way users log on or off

 All Rights Reserved - שאול קובל מערכות מחשבים

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

 All Rights Reserved - שאול קובל מערכות מחשבים

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

 All Rights Reserved - שאול קובל מערכות מחשבים

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

 All Rights Reserved - שאול קובל מערכות מחשבים

Setting Disk Quotas

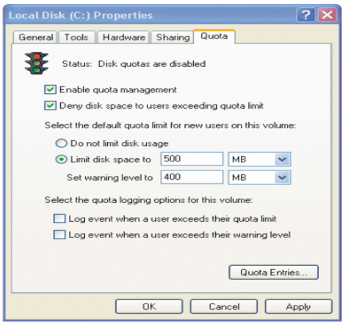

Figure 16-6 Setting disk quotas

 All Rights Reserved - שאול קובל מערכות מחשבים

Setting Disk Quotas (continued)

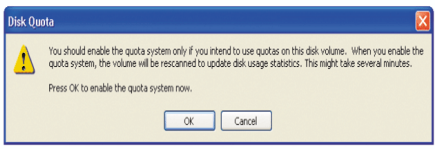

Figure 16-7 The prompt at the end of the quota-setting process gives you information about enabling quotas

 All Rights Reserved - שאול קובל מערכות מחשבים

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

 All Rights Reserved - שאול קובל מערכות מחשבים

How to Use Encryption

- Can be implemented at either the folder or file level
- Folder level is encouraged and considered a "best practice" strategy

 All Rights Reserved - שאול קובל מערכות מחשבים

Encrypting Folder Contents

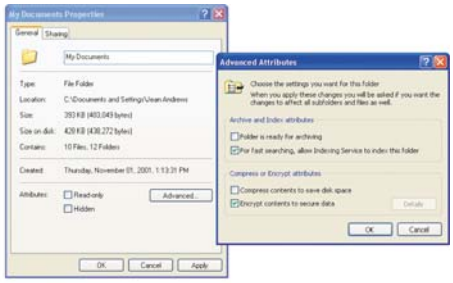

Figure 16-8 Encrypt folder contents

Encrypting Folder Contents

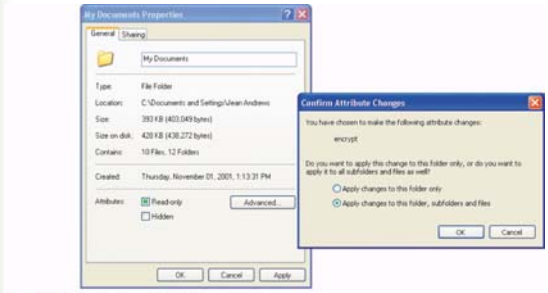

Figure 16-9 Apply changes to all folder contents

The Cipher Command

- Use when encrypting a large number of files or folders from a command prompt or using a batch file
- CIPHER [/E, /D] [/S:dir] [pathname[…]]
  - /E encrypts specified files or folders
  - /D decrypts specified files or folders
  - /S:dir applies action to specified folder and its subfolders
  - Pathname = name of file/folder and its path that is to be encrypted/decrypted

Internet Connection Firewall (ICF)

- Protects a PC from unauthorized access from the Internet when the PC is connected directly to the Internet
- Examines every incoming communication
  - Initiated by the PC (permitted)
  - Initiated by an outside device/computer (refused)
- Do not use on a PC that has Internet from a LAN

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

Component	Description
Setup programs for devices and applications	Setup programs can record configuration information in the registry and query the registry for information needed to install drivers and applications.
User profiles maintained and used by the OS	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.
Files active when Ntldr is loading the OS	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.

Components That Use the Registry (continued)

Component	Description
Device drivers	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.
Hardware profiles	Windows can maintain more than one set of hardware configuration information (called a **hardware profile**) 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.
Application programs	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.

Table 16-1 Components that use the Windows NT/2000/XP registry

All Rights Reserved - שאול קובל מערכות מחשבים

Logical Organization of the Registry

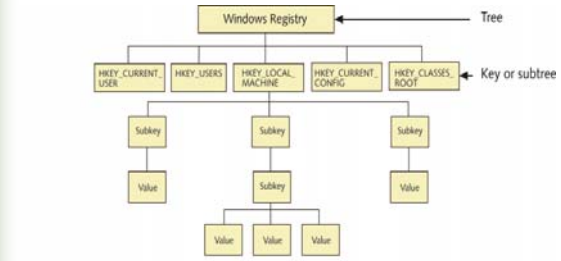

Figure 16-11 The Windows NT/2000/XP registry is logically organized in an upside-down tree structure of keys, subkeys, and values

All Rights Reserved - שאול קובל מערכות מחשבים

Five Subtrees of the Registry

Subtree (Main Keys)	Primary Function
HKEY_CURRENT_USER	Contains information about the currently logged-on user
HKEY_CLASSES_ROOT	Contains information about software and the way software is configured. This key points to data stored in HKEY_LOCAL_MACHINE.
HKEY_CURRENT_CONFIG	Contains information about the active hardware configuration, which is extracted from the data stored in the HKEY_LOCAL_ MACHINE subkeys called SOFTWARE and SYSTEM
HKEY_USERS	Contains information used to build the logon screen and the ID of the currently logged-on user
HKEY_LOCAL_MACHINE	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.

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

All Rights Reserved - שאול קובל מערכות מחשבים

Physical Organization of the Registry

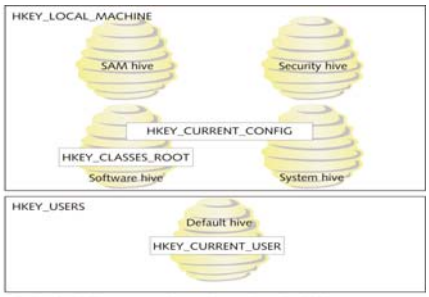

Figure 16-13 The relationship between registry subtrees (keys) and hives

All Rights Reserved - שאול קובל מערכות מחשבים

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.32exe (Windows NT/2000)
  - Regedit.exe (Windows NT/2000/XP)

All Rights Reserved - שאול קובל מערכות מחשבים

Other Maintenance and Troubleshooting Tools

- Executed from a command line (.exe file extension)
- Microsoft Management Console snap-ins (.msc file extension)
- Built-in tools (eg, Safe Mode)

All Rights Reserved - שאול קובל מערכות מחשבים

Windows XP Maintenance and Troubleshooting Tools

Tool	*Description*
Add or Remove Programs	Uninstalls software that is causing a problem
Automated System Recovery (ASR)	Drastically recovers failed system; a last resort (all data and applications written to the drive since last backup are lost)
Backup (Ntbackup.exe)	Backs up and restores data and software
Boot logging	Option on Advanced Options startup menu to log events to Ntbtlog.txt file
Bootcfg (Bootcfg.exe)	Views and edits contents of Boot.ini file used to hold startup settings

All Rights Reserved - שאול קובל מערכות מחשבים

Windows XP Maintenance and Troubleshooting Tools (continued)

Tool	*Description*
Cacls.exe	Changes ACL assigned to a file or group of files to control which users have access to a file and the type of access they have
Chkdsk (Chkdsk.exe)	Checks and repairs errors on logical drive
Cipher.exe	Displays and changes encryptions applied to files and folders using NTFS file system
Compact.exe	Displays and changes compressions applied to files and folders using NTFS file system
Computer Management (Compmgmt.msc)	Console provides access to snap-ins used to manage and troubleshoot a system

All Rights Reserved - שאול קובל מערכות מחשבים

Windows XP Maintenance and Troubleshooting Tools (continued)

Tool	*Description*
Convert.exe	Converts FAT16 or FAT32 logical drive to NTFS
Defrag.exe	Command-line tool to defragment logical drive or floppy disk; similar to Disk Defragmenter
Dependency Walker (Depends.exe)	Provides list of files needed for an application to load
Device Driver Roll Back	Replaces a driver with the one that worked before current driver was installed
Device Manager (Devmgmt.msc)	Displays and changes device drivers and other hardware settings

All Rights Reserved - שאול קובל מערכות מחשבים

Windows XP Maintenance and Troubleshooting Tools (continued)

Tool	*Description*
DirectX Diagnostic Tool (Dxdiag.exe)	Used to troubleshoot problems with DirectX API used by Microsoft
Disk Cleanup (Cleanmgr.exe)	Deletes unused files to make more disk space available
Disk Defragmenter (Dfrg.msc)	Defragments a logical drive or floppy disk
Disk Management (Diskmgmt.msc)	Displays and changes partitions on hard drives and formats drives
DiskPart (Diskpart.exe)	Command-line tool to manage partitions and volumes of a hard drive

All Rights Reserved - שאול קובל מערכות מחשבים

Windows XP Maintenance and Troubleshooting Tools (continued)

Tool	*Description*
Dr. Watson (Drwtsn32.exe)	Records errors and information about those errors when applications fail
Driver Signing and Digital Signatures (Sigverifi.ext)	Verifies that drivers, software, and system files have been approved by Microsoft
Error Reporting	Produces an error report and sends it to Microsoft when error occurs and PC is connected to Internet
Event Viewer (Eventvwr.msc)	Records and displays system problems
Expand.exe	Extracts a file from a cabinet file or compressed file

All Rights Reserved - שאול קובל מערכות מחשבים

Windows XP Maintenance and Troubleshooting Tools (continued)

Tool	*Description*
Fsutil (Fsutil.exe)	Displays information about and does advanced management tasks on drives and file systems
Getmac (Getmac.msc)	Displays the MAC address for the installed network adapter
Group Policy (Gpedit.msc)	Displays and changes policies controlling users and the computer
Group Policy Result (Gpresult.exe)	Displays currently applied group policies
Group Policy Update (Gpupdate.exe)	Immediately puts into effect changes just made to local group policies

All Rights Reserved - שאול קובל מערכות מחשבים

Windows XP Maintenance and Troubleshooting Tools (continued)

Tool	*Description*
Help and Support	Provides information, connects to Windows newsgroups, enables Remote Assistance
Last Known Good Configuration	Startup option used when normal or safe mode do not work
Performance Monitor (Perfmon.msc)	Reports information about performance problems
Program Compatibility Wizard	Looks at legacy software and attempts to resolve issues that prevent software from working
Recovery Console	Provides a command line to perform troubleshooting tasks when desktop will not load

All Rights Reserved - שאול קובל מערכות מחשבים

Windows XP Maintenance and Troubleshooting Tools (continued)

Tool	*Description*
Registry Editor (Regedit.ext)	Displays and changes entries in the registry
Remote Assistance	Allows a user to share computer with a support technician at a remote location
Remote Desktop	Allows a support technician to control a Windows XP computer remotely
Runas.exe	Runs a program using different permissions than those assigned to currently logged-on user
Safe Mode	Loads Windows desktop with minimum configuration; used to troubleshoot problems with problem-causing startup options

All Rights Reserved - שאול קובל מערכות מחשבים

Windows XP Maintenance and Troubleshooting Tools (continued)

Tool	*Description*
SC (Sc.exe)	Communicates commands to Service Controller
Services (Services.msc)	Graphical version of SC
System Configuration Utility (Msconfig.exe)	Controls settings used to troubleshoot a failing system
System File Checker (Sfc.exe)	Verifies version of all system files when Windows loads
System Information (Msinfo32.exe)	Displays information about hardware, applications and Windows; useful when troubleshooting

All Rights Reserved - שאול קובל מערכות מחשבים

Windows XP Maintenance and Troubleshooting Tools (continued)

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

All Rights Reserved - שאול קובל מערכות מחשבים

Windows XP Maintenance and Troubleshooting Tools (continued)

Tool	*Description*
Uninstall Windows XP Professional	Uninstalls Windows XP and reverts back to a previously installed OS
Windows File Protection	Protects system files and restores overwritten system files as needed
Windows Update (Wupdmgr.exe)	Examines the system, compares it to available updates on Microsoft Web site, and recommends updates

All Rights Reserved - שאול קובל מערכות מחשבים

System Information Window

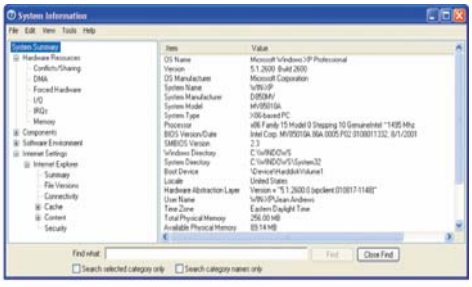

Figure 16-15 The System Information window displays important information about the system's hardware, software, and environment

All Rights Reserved - שאול קובל מערכות מחשבים

Help on the Web

- Windows Update feature
  - Manages the process of downloading updates from the Microsoft Web site
- Windows XP newsgroups

 All Rights Reserved - שאול קובל מערכות מחשבים

Windows Update

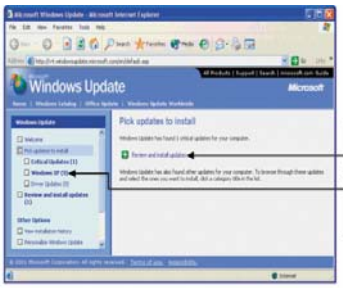

Figure 16-17 Windows Update process found updates appropriate to this computer

 All Rights Reserved - שאול קובל מערכות מחשבים

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

 All Rights Reserved - שאול קובל מערכות מחשבים

Advanced Options Menu

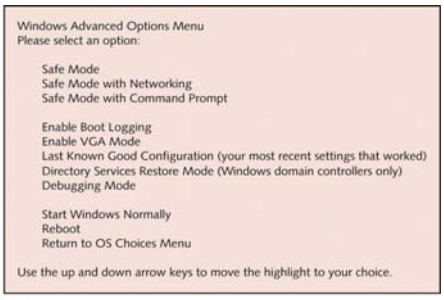

Figure 16-18 Windows XP Advanced Options menu

 All Rights Reserved - שאול קובל מערכות מחשבים

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

 All Rights Reserved - שאול קובל מערכות מחשבים

MS-DOS Startup Disk

- Can be used to boot into MS-DOS mode, giving an A prompt
- Can access the drive and recover data files (if hard drive is not using NTFS file system)
- Cannot launch Windows XP or be used to recover from a failed installation

 All Rights Reserved - שאול קובל מערכות מחשבים

Creating an MS-DOS Startup Disk

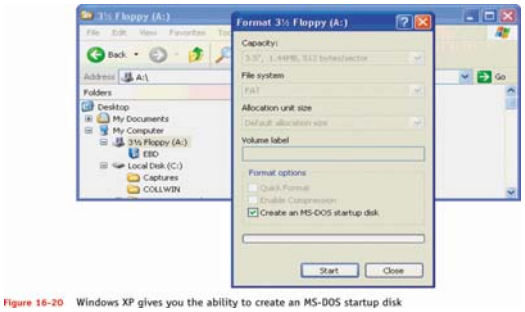

Figure 16-20 Windows XP gives you the ability to create an MS-DOS startup disk

All Rights Reserved - שאול קובל מערכות מחשבים

Windows XP Boot Disk

- Used to troubleshoot a failed boot
- Cannot troubleshoot problems with unstable device drivers or those that occur after the Windows 2000/XP logon screen displays

All Rights Reserved - שאול קובל מערכות מחשבים

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

All Rights Reserved - שאול קובל מערכות מחשבים

ASR Process

Figure 16-22 Automatic System Recovery process must have the ASR floppy disk

All Rights Reserved - שאול קובל מערכות מחשבים

ASR Process (continued)

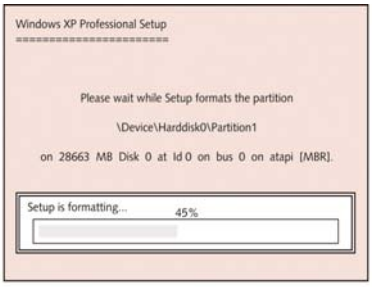

Figure 16-23 As part of the Automatic System Recovery process, Windows XP Setup repartitions and reformats the volume holding Windows XP

All Rights Reserved - שאול קובל מערכות מחשבים

Error Messages

Error Message	What It Means and What to Do About It
Invalid partition table Error loading operating system Missing operating system	The program in the MBR displays these messages when it cannot find the active partition on the hard drive or the boot sector on that partition. Use Fdisk or Diskpart from a command prompt to check the hard drive partition table for errors. Sometimes Fdisk/mbr solves the problem. Third-party recovery software such as PartitionMagic might help. If a setup program came bundled with the hard drive (such as Data Lifeguard from Western Digital or MaxBlast from Maxtor), use it to examine the drive. Check the hard drive manufacturer's Web site for other diagnostic software.
A disk read error occurred NTLDR is missing NTLDR is compressed	A disk is probably in the floppy disk drive. Remove the disk and reboot. When booting from the hard drive, these errors occur if Ntldr has been moved, renamed, or deleted, or is corrupted, if the boot sector on the active partition is corrupted, or you have just tried to install an older version of Windows such as Windows 98 on the hard drive. First try replacing Ntldr. Then check Boot.ini settings.

All Rights Reserved - שאול קובל מערכות מחשבים

Error Messages (continued)

Error Message	What It Means and What to Do About It
A text error message appears on a blue screen and then the system halts. These Windows NT/2000/XP errors are called **stop errors** or **blue screens (BSOD)**. Some stop errors follow.	Stop errors are usually caused by viruses, errors in the file system, a corrupted hard drive, or a hardware problem.
Stop 0x00000024 or NTFS_File_System	The NTFS file system is corrupt. Immediately boot into the Recovery Console, and copy important data files that have not been backed up to another media before attempting to recover the system.
Stop 0x00000050 or Page_Fault_in_Nonpaged_Area	Most likely RAM is defective.
Stop 0x00000077 or Kernel_Stack_Inpage_Error	Bad sectors are on the hard drive, there is a hard drive hardware problem, or RAM is defective. Try running Chkdsk or, for the FAT file system, run Scandisk using a Windows 98 startup disk.
Stop 0x0000007A or Kernel_Data_Inpage_Error	There is a bad sector on the hard drive where the paging file is stored; there is a virus or defective RAM. Try running Chkdsk or Scandisk.

All Rights Reserved - שאול קובל מערכות מחשבים

Error Messages (continued)

Error Message	What It Means and What to Do About It
Stop 0x0000007B or Inaccessible_Boot_Device	There is a boot sector virus or failing hardware. Try Fdisk/mbr or fixmbr.
Black screen with no error messages	This is likely to be a corrupted MBR, partition table, boot sector, or Ntldr file. Boot the PC using a Windows XP boot disk and then try the fixmbr and fixboot commands from the Recovery Console. You might have to reinstall Windows.

Table 16-4 Windows XP error messages and their meanings

All Rights Reserved - שאול קובל מערכות מחשבים

Summary

- Security features that protect Windows XP architecture, its users, and their data
- How the Windows NT/2000/XP registry is organized and how to edit it
- Troubleshooting tools available under Windows XP
- How to troubleshoot the boot process

All Rights Reserved - שאול קובל מערכות מחשבים