Understanding Whole Disk Encryption

Understanding Whole Disk Encryption

- Companies are more concern about loss of **Personal identity information (PII)** and **trade secrets**
  - **Company PII** - might consist of employees' full names, home addresses, and Social Security numbers
    - With this information, criminals could easily apply for credit card accounts
  - **Trade secrets** are any information a business keeps confidential because it provides a competitive edge over other companies

Understanding Whole Disk Encryption

- Of particular concern is the theft of laptop computers and other handheld devices
  - If data on these devices isn't secured properly, the owners could be liable for any damages incurred, such as stolen identities, credit card fraud, or loss of business caused by the release of trade secrets to the competition
- Many states have enacted laws requiring any person or business to notify potential victims of the loss as soon as possible
- To help prevent loss of information, software vendors now provide whole disk encryption

Understanding Whole Disk Encryption

- Current whole disk encryption tools offer the following features:
  - Preboot authentication - single sign-on password, fingerprint scan, or token
  - Full or partial disk encryption with secure hibernation
  - Advanced encryption algorithms
  - Key management function
  - A **Trusted Platform Module (TPM)** microchip to generate encryption keys and authenticate logins

Understanding Whole Disk Encryption

- Whole disk encryption tools encrypt each sector of a drive separately
- Many of these tools encrypt the drive's boot sector

- To examine an encrypted drive, decrypt it first
  - Run a vendor-specific program to decrypt the drive

Examining Microsoft BitLocker

- Microsoft's utility for protecting drive data is called BitLocker
- Available only with Vista/Win 7 Enterprise and Ultimate editions
- Hardware and software requirements
  - A computer capable of running Windows Vista/7
  - The TPM microchip, version 1.2 or newer
  - A computer BIOS compliant with Trusted Computing Group (TCG)
  - Two NTFS partitions for the OS and an active system volume with 1.5 GB available space
  - The BIOS configured so that the hard drive boots first before checking other bootable peripherals

Examining Third-Party Disk Encryption Tools

- Several vendors offer third-party WDE utilities that often have more features than BitLocker
- BitLocker can encrypt only NTFS drives and not FAT drive

Examining Third-Party Disk Encryption Tools

- Some available third-party WDE utilities:
  - PGP Whole Disk Encryption
  - Voltage SecureDisk
  - Utimaco SafeGuard Easy
  - Jetico BestCrypt Volume Encryption
  - SoftWinter Sentry 2020 for Windows XP
- Some available open-source encryption tools:
  - TrueCrypt
  - CrossCrypt
  - FreeOTFE

Understanding the Windows Registry

Understanding the Windows Registry

- **Registry**
  - A database that stores hardware and software configuration information, network connections, user preferences, and setup information
- For investigative purposes, the Registry can contain valuable evidence
- To view the Registry, you can use:
  - Regedit (Registry Editor) program for Windows 9x systems
  - Regedt32 for Windows 2000 and XP

Exploring the Organization of the Windows Registry

- Registry terminology:
  - Registry
  - Registry Editor
  - HKEY
  - Key
  - Subkey
  - Branch
  - Value
  - Default value
  - Hives

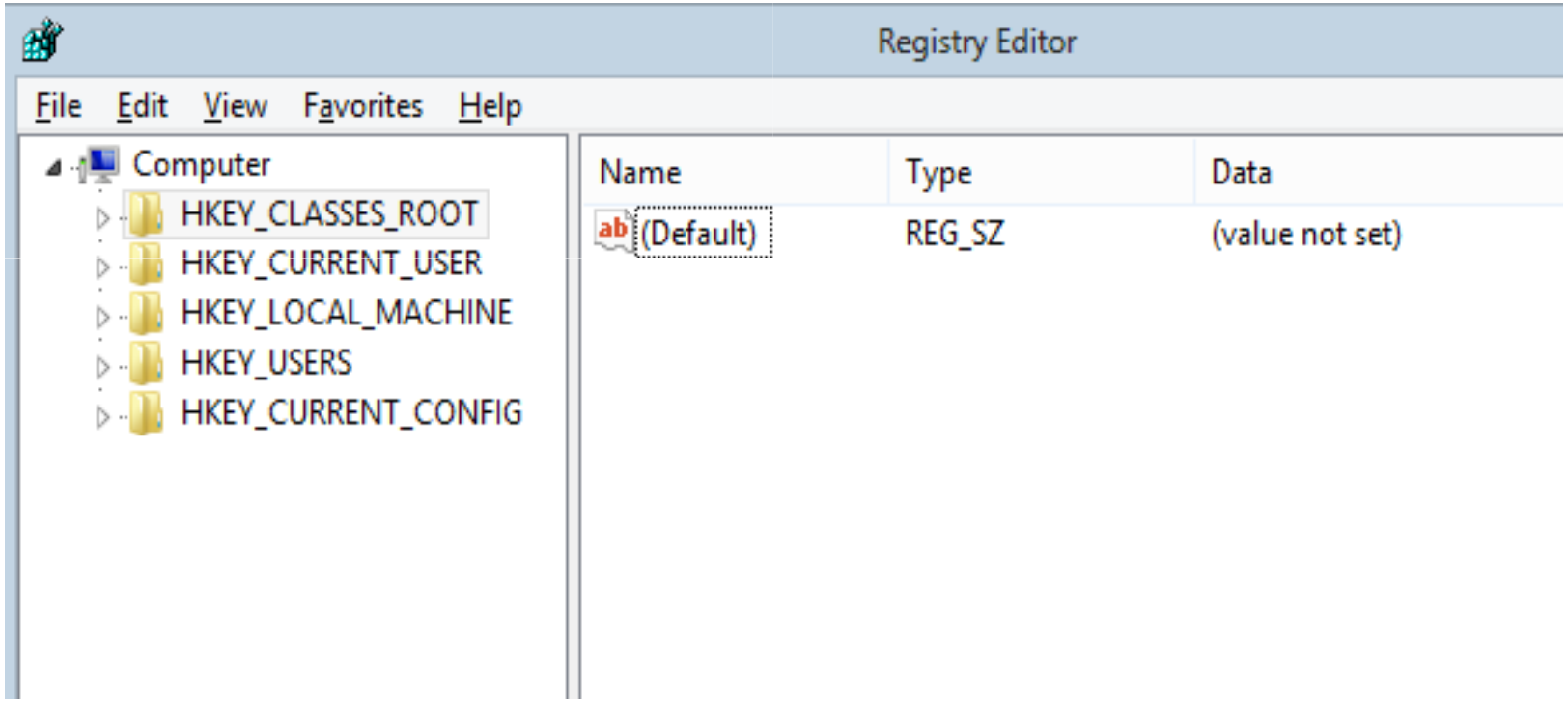
Exploring the Organization of the Windows Registry

Table 6-6 Registry file locations and purposes

Filename and location	Purpose of file
Windows 9x/Me	
Windows\System.dat	User-protected storage area; contains installed program settings, usernames and passwords associated with installed programs, and system settings
Windows\User.dat Windows\profile\user-account	Contains the most recently used (MRU) files list and desktop configuration settings; every user account created on the system has its own user data file
Windows NT, 2000, XP, and Vista	
Documents and Settings\ user-account\Ntuser.dat	User-protected storage area; contains the MRU files list and desktop configuration settings
Winnt\system32\config\Default	Contains the computer's system settings
Winnt\system32\config\SAM	Contains user account management and security settings
Winnt\system32\config\Security	Contains the computer's security settings
Winnt\system32\config\Software	Contains installed programs settings and associated usernames and passwords
Winnt\system32\config\System	Contains additional computer system settings

Exploring the Organization of the Windows Registry

- **Start**, and then click **Run**
- Type **Regedit**, and then click **OK**



Exploring the Organization of the Windows Registry

Table 6-7 Registry HKEYs and their functions

HKEY	Function
HKEY_CLASS_ROOT	A symbolic link to HKEY_LOCAL_MACHINE\SOFTWARE\Classes; provides file type and file extension information, URL protocol prefixes, and so forth
HKEY_CURRENT_USER	A symbolic link to HKEY_USERS; stores settings for the currently logged-on user
HKEY_LOCAL_MACHINE	Contains information about installed hardware and software
HKEY_USERS	Stores information for the currently logged-on user; only one key in this HKEY is linked to HKEY_CURRENT_USER
HKEY_CURRENT_CONFIG	A symbolic link to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profile*xxxx* (with *xxxx* representing the current hardware profile); contains hardware configuration settings
HKEY_DYN_DATA	Used only in Windows 9x/Me systems; stores hardware configuration settings

Understanding Microsoft Startup Tasks

Understanding Microsoft Startup Tasks

- Learn what files are accessed when Windows starts
- This information helps you determine when a suspect’s computer was last accessed
  - Important with computers that might have been used after an incident was reported

Startup in Windows NT and Later

- All Windows NT computers perform the following steps when the computer is turned on:
  - Power-on self test (POST)
  - Initial startup
  - Boot loader
  - Hardware detection and configuration
  - Kernel loading
  - User logon

Startup Process for Windows Vista

- Uses the new Extensible Firmware Interface (EFI) as well as the older BIOS sys-tem.
- NT Loader (NTLDR) has been replaced by three boot utilities
  - Bootmgr.exe—displays list of operating systems
  - Winload.exe—loads kernel, HAL, and drivers
  - Winresume.exe—restarts Vista after hibernation

Startup Files for Windows XP

- **NT Loader (NTLDR)** - loads the OS
- **Boot.ini** - displays a boot menu
- **BootSect.dos** - boot sector location
- **NTDetect.com** - queries the system for device and configuration data
- **NTBootdd.sys** - device driver
- **Ntoskrnl.exe** - Windows XP OS kernel
- **Hal.dll -** llows the OS kernel to communicate with the computer’s hardware
- **Pagefile.sys –** optimize the amount of physical RAM available
- **Device drivers** - contain instructions for hardware devices

Startup in Windows NT and Later

- Windows XP System Files

Table 6-8 Windows XP system files

Filename	Description
Ntoskrnl.exe	The XP executable and kernel
Ntkrnlpa.exe	The physical address support program for accessing more than 4 GB of physical RAM
Hal.dll	The Hardware Abstraction Layer (described earlier)
Win32k.sys	The kernel-mode portion of the Win32subsystem
Ntdll.dll	System service dispatch stubs to executable functions and internal support functions
Kernel32.dll	Core Win32 subsystem DLL file
Advapi32.dll	Core Win32 subsystem DLL file
User32.dll	Core Win32 subsystem DLL file
Gdi32.dll	Core Win32 subsystem DLL file

Startup in Windows NT and Later

- Contamination Concerns with Windows XP
  - When you start a Windows XP NTFS workstation, several files are accessed immediately
    - The last access date and time stamp for the files change to the current date and time
  - Destroys any potential evidence
    - That shows when a Windows XP workstation was last used

Startup in Windows 9x/Me

- System files in Windows 9x/Me containing valuable information can be altered easily during startup
- Windows 9x and Windows Me have similar boot processes
  - With Windows Me you can’t boot to a true MS-DOS mode
- Windows 9x OSs have two modes:
  - **DOS protected-mode interface (DPMI)**
  - **Protected-mode GUI**

Startup in Windows 9x/Me

- The system files used by Windows 9x have their origin in MS-DOS 6.22
  - **Io.sys** communicates between a computer's BIOS, the hardware, and the OS kernel
    - If F8 is pressed during startup, Io.sys loads the Windows Startup menu
  - **Msdos.sys** is a hidden text file containing startup options for Windows 9x
  - **Command.com** provides a command prompt when booting to MS-DOS mode (DPMI)

Understanding MS-DOS Startup Tasks

Understanding MS-DOS Startup Tasks

- Two files are used to configure MS-DOS at startup:
  - **Config.sys**
    - A text file containing commands that typically run only at system startup
  - **Autoexec.bat**
    - A batch file containing customized settings

Understanding MS-DOS Startup Tasks

- **Io.sys** is the first file loaded after the ROM bootstrap loader finds the disk drive – loads OS
- **Msdos.sys** is the second program to load into RAM immediately after Io.sys
  - It looks for the Config.sys file to configure device drivers and other settings
- **Command.com -** loads Autoexec.bat

Other Disk Operating Systems

- Control Program for Microprocessors (CP/M)
- Digital Research Disk Operating System (DR-DOS)
- Personal Computer Disk Operating System (PC-DOS)

Understanding Virtual Machines

Understanding Virtual Machines

Virtual machine

Allows you to create a representation of another computer on an existing physical computer

A virtual machine is just a few files on your hard drive

Must allocate space to it

A virtual machine recognizes components of the physical machine it's loaded on

Virtual OS is limited by the physical machine's OS

Understanding Virtual Machines

In computer forensics

- Virtual machines make it possible to restore a suspect drive on your virtual machine
  - And run nonstandard software the suspect might have loaded

From a network forensics standpoint, you need to be aware of some potential issues, such as:

- A virtual machine used to attack another system or network

Creating a Virtual Machine

Two popular applications for creating virtual machines

VMware and Microsoft Virtual PC

Using Virtual PC

You must download and install Virtual PC first

Creating a Virtual Machine

You need an ISO image of an OS

Because no OSs are provided with Virtual PC

Virtual PC creates two files for each virtual machine:

A .vhd file, which is the actual virtual hard disk

A .vmc file, which keeps track of configurations you make to that disk

See what type of physical machine your virtual machine thinks it's running

Open the Virtual PC Console, and click Settings