GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Thumb Drive Threats and Countermeasures in a Microsoft Windows Environment

GIAC Practical Assignment 1.4b Option 1
Mark Baggett
August 2004

© SANS Institute 2004, Author retains full rights.

TABLE OF CONTENTS

1.0 INTRODUCTION 3
2.0 THE TECHNOLOGY 3
2.1 Market Penetration 4
2.2 Exploring the Benefits 4
2.3 Innovations in the Thumb Drive Market 5
3.0 EXPLORING THE THREATS 5
3.1 Virus Infections 6
3.2 Stealth USB Drives 7
4.0 THREAT COUNTERMEASURES 7
4.1 Managing USB Thumb Drives in a Windows Environment 7
4.2 Limited Effectiveness of NTFS DACLS 8
4.3 Disabling Autorun on USB Devices 8
4.4 Digital Rights Management 9
4.5 Protecting the Confidentiality of Data Using Encrypting File System (EFS) 10
4.5.1 Encrypting Files/Directories with the GUI 10
4.5.2 Encrypting Files/Directories with CIPHER 11
4.5.3 Identifying EFS Encryption Keys 11
4.6 Disabling USB Usage in a Managed Windows Environment 11
4.6.1 Group Policy Management 12
4.6.2 Importing the USBDisable.adm Template 13
4.6.3 Using the Administrative Template 14
5.0 DATA FORENSICS AND DISPOSAL 15
6.0 CONCLUSION 16
7.0 REFERENCES 16

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

ABSTRACT

USB Flash drives or thumb drives are small, fast, removable media devices, which offer large amounts of storage space and cross platform compatibility. They are a much-needed replacement for the all but obsolete floppy disk. However, they also have given rebirth to many of the threats associated with the use of floppy disks. As security professionals, we must recognize these threats and determine what countermeasures are appropriate for our environment. This paper will examine USB drives growing presence in our work place and the benefits and threats that they now present. This paper will examine different countermeasures that are available to you in a managed Microsoft Windows environment to reduce your exposure to viruses and loss of intellectual property. This paper will also show how to completely disable the use of USB drives if you decide that the threats far out weigh the benefits.

1.0 INTRODUCTION

USB (Universal Serial Bus) Flash Disks are solid-state memory devices, that plug into a USB 1.2 or 2.0 slot on a computer. These devices can hold in excess of 1 GB of data. The portability, ease of use, speed, and storage capacity make these devices a much-needed replacement for the all but obsolete floppy disk. Along with any new technology comes a new set of risks that must be understood and properly mitigated. This paper explores some of the risks posed by USB devices in the work environment, and offers a few techniques for the mitigation of these risks.

2.0 THE TECHNOLOGY

USB Flash Drives are also referred to as Thumb Drives, Pen Drives, or Keychain Drives. These small devices are inexpensive, portable, fast, and can store large amounts of data. USB drives are based on Compact Flash technology. Compact Flash technology was first introduced in 1994 by SanDisk Company and is an outgrowth of EEPROM technology[1] The first USB drives held only a few megabytes of data and were much slower than today's drives. Those drives plugged in to a USB 1.0 or 1.1 interfaces and could transfer data at only 1 or 12 Megabits per second. The duration of time that data can be stored on a USB device varies based on usage. However, some manufacturers estimate their products life span to be about ten years.[2]

Today USB Thumb Drives can also use USB 2.0 and transfer data at speeds up to 480-Megabits per second. USB Thumb Drives are now capable of storing anything from a few megabytes to gigabytes of data. Most of today's Operating Systems have support for USB drives preinstalled. Operating these devices is as simple as plugging the device

[1] Science Daily, "Flash Memory", URL:http://www.sciencedaily.com/encyclopedia/flash_memory (July 2004)

[2] Dan Costa, "Flash Forward, Part 1", URL:http://www.cpuplanet.com/features/article.php/2179171 (June 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

into an available USB slot and using the storage in the same manner as any other drive on a computer. The devices now have small microprocessors, adding functionality to the drives. These microprocessors enable USB drives to add services such as encryption, biometric authentication, and a wide range of other security related services. The thumb drive is quickly evolving from a simple storage unit to powerful "Micro-server".[3]

2.1 Market Penetration

The USB Flash Drive Alliance expects 49 to 55 million of these devices to be sold in 2004. Over the next four years, the number is expected to grow between 98.2 and 242 million units. Over that same period, the average storage capacity is expected to reach between 1.1 and 1.7 GB. If these estimates are correct, the USB Flash Drive will become the most widely used removable solid-state storage format.[4] There is little doubt that these devices are quickly becoming the modern day reincarnation of floppy disks.

2.2 Exploring the Benefits

One significant advantage that the USB drive has over CDs and floppy disks is durability. USB drives are not as prone to scratches, dirt, and fingerprints as CDs. Since there are no moving parts, the likelihood is a USB drive will outlast floppy disks, CDs, and DVDs by several years. In fact, according to Lexar Media, the mean time between failures for a floppy disk is 30,000 hours. This is considerably less than then estimated mean time between failure for USB drives which is around 300,000 hours. [3]

USB drives can last as long as their solid-state holds up, which is dependent upon the usage of the device. According to Peter Gutmann, "EEPROM/flash cells can typically endure 1M or more write/erase cycles, the presence of slight defects in the tunneling oxide (leading to leakage and eventual breakdown during the tunneling process), reduces the effective life of the entire collection of cells to 10-100K write/erase cycles".[5]

USB drives are also faster than other removable media solutions. Floppy disks transfer data at speeds of 1 MB per second and CDs at 16.6 MB per second.[6] USB drives on a USB 2.0 interface are capable of transferring data at 480 Mbps.[7]

---

[3] Nathan Obr, USB Storage A focus on UFDs", Microsoft Corporation, URL:http://download.microsoft.com/download/c/f/1/cf1806ad-5a4f-4f7d-a5b2-07fdb59a7adb/WH03_TPA60.exe (June 2004)

[4] USB Alliance, "USB Flash Drive Worldwide Forecast: Revenues, Units and Capacity 2004-2008", URL:http://www.usbflashdrive.org/usbfd_marketoutlook.html (June 2004)

[5] Peter Gutmann, "Data Remanence in Semiconductor Devices", IBM T.J.Watson Research Center, URL:http://www.securityfocus.com/library/3636 (June 2004)

[6] The PC Guide, "Floppy Disk Controller Speed", http://www.pcguide.com/ref/fdd/confSpeed-c.html (June 2004)

[7] PCSTATS, "USB 2.0 – Working at 480 Mbps", URL:http://www.pcstats.com/articleview.cfm?articleID=885# (June 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

USB Thumb Drives are supported natively by most modern computers. Windows XP, Windows 2000 SP4, MAC OS X, and Linux can read a USB drive without the installation of additional drives.

In summary, USB drives are fast, removable, and portable, have more storage capacity, and are more durable than most other forms of media supported natively by modern operating systems.

2.3 Innovations in the Thumb Drive Market

There are several new USB security related products, which may be beneficial to security professionals and hackers alike. For example, LinuxMobile can turn a USB Thumb Drive into a bootable Linux OS, which can be used for forensics, and data recovery. A bootable USB Thumb Drive can also be used for more nefarious tasks such as grabbing the SAM Account database from the host OS for offline password cracking. Fireball Keypoint can help to mitigate some of the risks associated with mobile users on untrusted computers. Keypoint USB Micro-servers provide storage-like traditional USB drives, but also scan the hosts for keyloggers, Trojans, spyware, viruses, and other malicious software to insure the integrity of the data on the storage unit. The X-Key Exchange Micro-server has similar malware detection abilities. It also runs an email client, which will communicate with the Microsoft Exchange server over https and keep email in an AES encrypted database. These devices can help mitigate the risk associated with corporate users plugging their USB drives in to untrusted machines.[8] Some USB drives have write protection switches, preventing unauthorized writing to the drive. These switches work the same way the write protection tab did on floppy drives. When the switch is in the write-protect position, data can be read from, but cannot be written to the USB drive. Used properly this simple feature can go a long way in preventing virus infection on the USB drive. Some USB drive manufacturers are adding authentication mechanisms to their thumb drive product line. Using biometrics, password authentication, or a combination of the two, users are required to authenticate before accessing data on the drive. Combined with encryption to protect the data, this can help mitigate the risks associated with viruses and accidental data loss from misplaced keychain drives.

3.0 EXPLORING THE THREATS

The risks associated with USB drives are very similar to those associated with floppy disks. If an organization has decided to eliminate the use of floppy disks, eliminating the use of USB drives should also be considered. All the threats created by floppy disks are now revisited with USB drives. These threats can now propagate more quickly and are not constrained by the limited capacity of floppy disks.

[8] Toni Kistner, “Personal servers simplify remote work”, URL:http://www.networkworldfusion.com/net.worker/news/2004/0524netlead.html?page=1 (June 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Although I did not have direct access to the original, I have read summaries of a report released in July of 2004 by the Gartner group stating USBs represent a significant risk to corporate enterprises. According to an article posted on The Register in the same report, Gartner advises, "Firms should think about disabling universal plug and play functions after installing desired drivers, to restrict their use to authorized devices…"[9]

With a USB drive, a user can walk out the door with one gigabyte of intellectual property in their pocket. Users can also walk in the door with a gigabyte of unlicensed unauthorized software for installation on corporate systems. Misplacing a gigabyte of confidential information is as simple as misplacing a set of keys. Most companies recognize the loss of a laptop containing confidential data as a security threat. USB drives can hold a significant amount of data, and the data loss can be as significant as the loss of a laptop. The confidential data on your USB drives should be treated with the same respect as that data sitting on your laptop hard drive.

Many USB drives are large enough to hold the SAM database for a large domain. An intruder with physical access to a Windows Domain Controller and a bootable CD can easily walk away with a complete copy of all your logins and passwords in their pocket. A bootable Linux distribution such as Knoppix (www.knoppix.com) contains USB drivers, can mount NTFS partitions and has all the tools needed to access, dump and crack your domain passwords. Be sure to use a properly managed SYSKEY to maintain the confidentiality of your database. Refer to http://www.windowsecurity.com/articles/Securing_Server_2003_Domain_Controllers.html and http://support.microsoft.com/default.aspx?kbid=310105 for more information on SYSKEY.

3.1 Virus Infections

Additional capacity and speed make the USB drive an excellent medium for the spread of viruses. A USB drive attached to a users key chain can go everywhere the user goes and can be plugged into most computers the user encounters. The ability to quickly share files between computers means USB drives are plugged into many computers. Have you been in a room where a USB drive containing a presentation or important file was passed around to everyone in the room? I have. The result is that the USB drives present multiple opportunities for spreading viruses.

In a Windows environment, a USB drive can infect a host immediately after insertion to the computer. If the virus places a malicious autoexec.inf on the removable media, it can use the autorun feature to automatically execute itself upon insertion of the USB drive of a Windows machine. According to Microsoft, the autorun feature can be used on any device whether it is static or removable as long as the media is marked as removable.[10] Floppy disk viruses required the user to open an infected file or boot a computer with the infected bootable floppy in the drive to infect the host. USB drives

[9] John Leyden, 'iPods are the latest security risk",
URL:http://www.theregister.co.uk/2004/07/07/ipod_security_risks/ (August 2004)
[10] Microsoft Corporation, "USB Storage - FAQ for Driver and Hardware Developers",
URL:http://www.microsoft.com/whdc/device/storage/usbfaq.mspx (June 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

viruses can infect the host in exactly the same way or use the auto execution features. By using the auto execution feature these viruses can infect its host using methods that require less action on the part of the victim.

3.2 Stealth USB Drives

USB drives are starting to come in all shapes and sizes. Many MP3 players have USB interfaces that can be used to store files. Peripheral manufacturers such as Diskgo! are putting USB drives into a variety of devices. An employee may walk out of the office with a customer database on the USB drive in their pocket; but that database could just as easily be on their wrist or in a pen. USB drives now come in the shape of wristwatches and executive ballpoint pens. (Figure 1 Stealth USB Devices) As these devices get smaller, they can go just about anywhere.[11]


[11]

Figure 1 Stealth USB Devices

4.0 THREAT COUNTERMEASURES

Some third-party software providers have introduced products to provide countermeasures for some of these threats. GFI sells a product called GFILanGuard Portable Storage Control, giving the Administrator Granular Control over all the removable media on the workstations in the domain. Other products in this market space include SecureWave's SecureNT and Smartline's DeviceLock. Alternatively, some of Windows built in management tools such as registry entries and Group policies can be used to maintain control of USB Devices in your environment and mitigate some of the risk.

4.1 Managing USB Thumb Drives in a Windows Environment

By default, most USB drives are formatted in a FAT32 format. To utilize some of Windows extended security features, it will be necessary to convert your USB to NTFS. Microsoft has chosen not to make formatting the USB with NTFS an option via the Explorer interface. So turning a USB to a NTFS device is a two-step process. If the USB drive is not already formatted, use Explorer to format it as a FAT32 partition. Next go to the CMD.EXE prompt and type "CONVERT <DRIVE>: /FS:NTFS /V" where <DRIVE> is the drive letter of the USB device. For example "Convert E: /FS:NTFS /V" would

[11] Diskgo!, "Peripheral EDGE DiskGO! USB Watch", URL:http://www.edgetechcorp.com/products/diskgo/ (August 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

convert the E: drive to NTFS. Once the conversion process is completed you now have an NTFS formatted USB drive and can benefit from the extended security features of NTFS. For example, you can now use NTFS DACLS to limit access to the files stored on the thumb drive. However, the portability of USB drives limits the effectiveness of DACLS in restricting access to protected files.

4.2 Limited Effectiveness of NTFS DACLS

DACLS are not effective if a user has administrative privileges to their own computer. Once a USB drive is added to a machine, it is a device on that machine and is under the full control of any administrators of that machine. As administrator, you always have the option to take ownership of a file, and modify its permissions. As a result, NTFS DACLS can be modified by anyone who can find a machine on which they have administrative privileges and a USB port. This seriously limits the effectiveness of DACLS on USB Thumb Drives. In an environment where no one has administrative privileges on their computer, this may provide a minimum amount of security. However, DACLS should not be relied on to protect the confidentiality of information, and should only be used as part of a defense in depth strategy.

4.3 Disabling Autorun on USB Devices

Another way to manage the risk associated with USB drives would be to disable autorun on all USB drives. Disabling the autorun feature on all USB drives is an effective countermeasure against the automatic spreading of viruses from the USB to workstations upon insertion in the USB slot. There are two ways to accomplish disabling autorun on the USB drive. Disable autorun based on a drive letter or based on a drive type. To disable the media based on the drive type, set the following registry key.

\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

Set the key named NoDriveTypeAutoRun to an integer representing where the Autorun is to be disabled.

Start with 0 (zero).
Do you want autorun disabled on all Removable media? Yes , add 4
Do you want autorun disabled on all Hard drives and other fixed drives? Yes, add 8
Do you want autorun disabled on all Network Drives? Yes, add 10
Do you want autorun disabled on all CD-ROM Drives? Yes, add 20
Do you want autorun disabled on all RAM Drives? Yes, add 40

Therefore, to disable autorun on all drive types you set the registry key to 82. To disable autorun on only removable media set the registry key to 4. To disable autorun on CDs and Removable Media (including USB drives) set the registry to 24.

Autorun can also be disabled using a specific drive letter. To manage autorun based on the drive letter, modify a different key under \HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Set the registry key named NoDriveAutorun to an integer representing the drives on which you wish to prevent the use of autorun. To disable it on a set of drives add the numbers next to the letters below of the drive letters you wish to disable.

1	a
2	b
4	c
8	d
16	e
32	f
64	g
128	h
256	i
512	j
1024	k
2048	l
4096	m
8192	n
16384	o
32768	p
65536	q
131072	r
262144	s
524288	t
1048576	u
2097152	v
4194304	w
8388608	x
16777216	y
33554432	z

To disable autorun on just the "E:" drive set the registry key to 16. To disable autorun on "A:" and "E:" set the registry key to 17 (16 + 1). To disable it on all drives except the D: drive set the registry key to 67108863.[12]

4.4 Digital Rights Management

The loss of intellectual property can have serious consequences and poses a serious threat to many organizations. However, this threat, all be it serious, is not a new one. Although USB drives are large and fast, CD-Rs, floppy disks and copy machines have been around for a long time. If the desire is to protect intellectual property, then disabling USB drives is only one small piece of a much larger puzzle. Digital Rights Management product suites will allow control over when, how, where, and by whom, a document can be copied. Any DRM suite worth its salt will prevent the unauthorized

[12] Microsoft Developers Network, “Enabling and Disabling Autoplay”, Microsoft Corporation, URL:http://msdn.microsoft.com/library/default.asp?url=/library/en-us/shellcc/platform/Shell/programmersguide/shell_basics/shell_basics_extending/autorun/autoplay_reg.asp (June 2004)

© SANS Institute 2004, Author retains full rights.

copying of data to any removable media. These tools are the way to go for any organization truly concerned with the protection of intellectual property.

4.5 Protecting the Confidentiality of Data Using Encrypting File System (EFS)

Windows EFS can be used to encrypt confidential data on a USB Thumb Drive and protect its confidentiality. EFS can be an effective countermeasure against the exposure of confidential data resulting from the loss of a thumb drive. To protect the data on a thumb drive using EFS, the thumb drive must first be formatted as a NTFS partition as described in section 4.1 above.

4.5.1 Encrypting Files with EFS

Once the USB drive is formatted with NTFS, use EFS to encrypt data. EFS is the Microsoft Encrypted Files System. This security subsystem is built into Microsoft Windows 2000 or better. EFS will encrypt the data while it is stored at rest on the disk. Data is decrypted automatically when it is read into the computer memory or copies across the network. Using EFS to encrypt a file and/or directory on a USB drive will insure that the data is encrypted while it is stored in the encrypted location. The data can only be accessed by a machine, containing the keys with which the drive was encrypted. To encrypt a folder on a USB drive using Explorer, right click the folder to encrypt and select PROPERTIES. (Figure 2 Encrypting Using EFS)The file folder properties box will appear. Select the Advanced button to bring up the advanced attributes dialog. Click “Encrypt contents to secure data” to encrypt your directory.

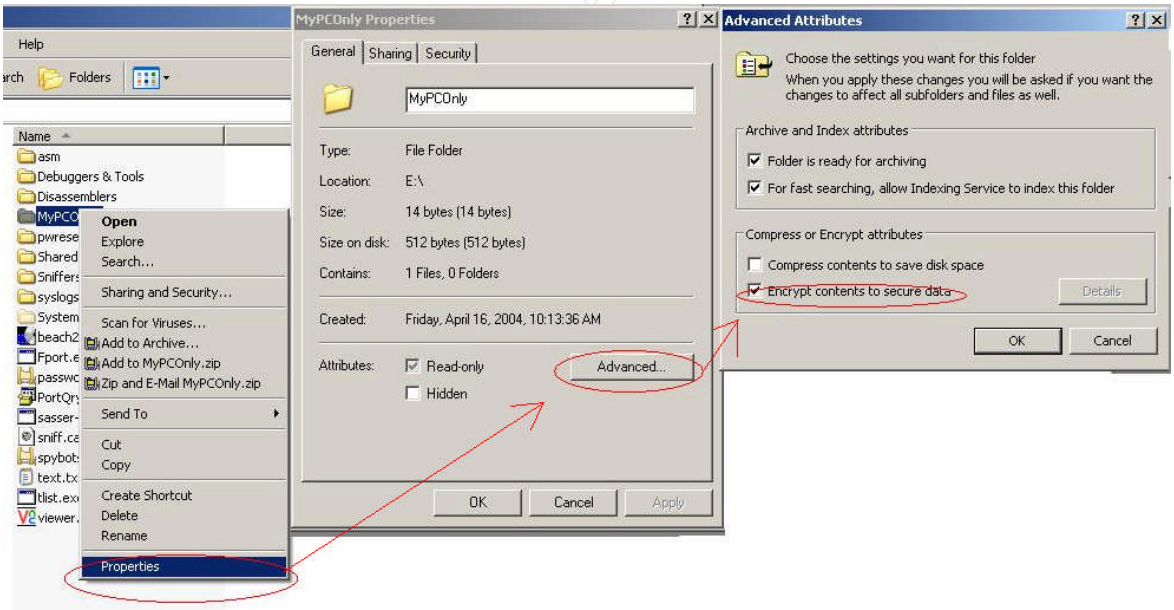


Figure 2 Encrypting Using EFS

If you are encrypting the root of a USB drive, the usability of that drive across multiple machines will be limited. Only the machine that encrypted the USB drive root will be able to access any of the directories on the USB drive. To benefit from the added security of EFS, but still use the USB drive to transfer data between machines, encrypt a subdirectory of the USB drive with EFS rather than the root. For example, you may

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

create a \MyComputerOnly directory that contains the data that can only be read by the X.509 certificate installed on your computer.

4.5.2 Encrypting a Directory with CIPHER

You can also encrypt a directory from the command line using CIPHER.EXE. The syntax to encrypt your directory and all files in that directory is “CIPHER /E /A <DRIVE:DIRECTORY TO ENCRYPT>”. For example, “CIPHER /E /A E:\encryptme” will encrypt the encryptme directory on the E:\ drive along with any files that currently exist in that directory.

This directory will only be readable by those machines that have the appropriate EFS keys installed. Proper management of Cryptographic keys is beyond the scope of this paper. Familiarize yourself with the use of EFS recovery keys and with protecting private keys. You may wish to archive a copy of the certificates that were used to encrypt the directory.

4.5.3 Identifying EFS Keys

To identify what keys need to be exported from your system for recovery purposes, use EFSINFO.EXE. EFSINFO /C <DRIVE:DIRECTORY> to display the Thumbnail of the Certificate that had encrypted that directory. Compare the Thumbnail from EFSINFO to those on the certificates in the “CERTIFICATES” MMC Snap-in. Use the Certificate Snap in to export the Keys. WARNING: If the Private Key is compromised, then so is the data that was encrypted by it. Treat all keys with the proper respect.

4.6 Disabling USB Usage in a Managed Windows Environment

If you decide the use of USB drives present to much risk to your organization, there are steps that can be taken in a managed windows environment to help lessen the risks. If you determine it is necessary, you can prevent the use of USB drives.

If a USB drive has never been used on a machine, prevent the USB from ever being used by restricting the NTFS DACLS on <SYSTEMROOT>\inf\usbstor.inf and <SYSTEMROOT>\inf\usbstor.pnf. Example:c:\windows\inf\usbstor.inf
(Figure 3 Restricting USBSTOR.PNF)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

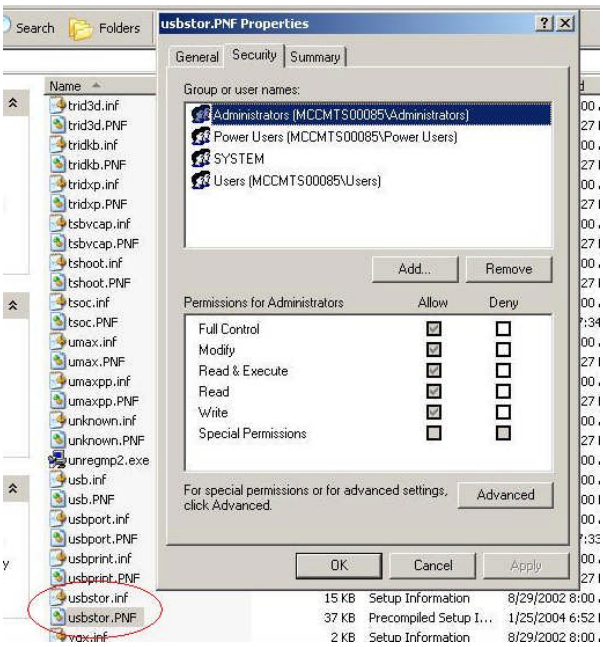


Figure 3 Restricting USBSTOR.PNF

It is best to deny Full Permissions to the built-in group “Everyone”. Restricting access to the files only prevents the installation of the USB drivers. Restricting permissions to "Everyone" prevents an Administrator from inadvertently installing the drivers. This is important because once the drivers are installed, the USB drives will be available to all users on the machine.

To restrict the use of USB drives after the installation of the drivers, a registry modification is necessary. You can automate this process by importing the registry changes or applying the change via group policy. Disabling the USB drives requires the following registry change:

In the registry key
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR
Modify the “Startup” value. Set it to a value of 4 to Disable USB drives.

If these registry keys do not exist then the USB drivers have not been installed and restricting permissions as described above will prevent the use of USB drives.[13]

4.6.1 Group Policy Management

If using Active Directory, a custom administrative template can be created which will allow administrative control over the use of USB drives on a domain. The ‘DisableUSB.ADM’ template below can be imported in to the group policy to disable USB drives on the machines in your domain.

[13] Microsoft Knowledge Base, “HOW TO: Disable the Use of USB Storage Devices in Windows XP”, Microsoft Corporation, URL:http://support.microsoft.com/?kbid=823732 (August 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Template DisableUSB.ADM

```
CLASS MACHINE
CATEGORY !!categoryname
 POLICY !!policyname
  KEYNAME "SYSTEM\CurrentControlSet\Services\USBSTOR"
  EXPLAIN !!explaintext
    PART !!labeltext DROPDOWNLIST REQUIRED
      VALUENAME "Start"
      ITEMLIST
       NAME !!Disabled VALUE NUMERIC 3 DEFAULT
       NAME !!Enabled VALUE NUMERIC 4
      END ITEMLIST
    END PART
  END POLICY
END CATEGORY

[strings]
categoryname="Restrict USB Drives Usage"
policyname="Disable USB"
explaintext="Disables the computers USB Drives completely"
labeltext="Disable USB"
Enabled="Enabled"
Disabled="Disabled"
```

4.6.2 Importing the USBDisable.adm Template

(Figure 4 Importing USBDisable.adm)

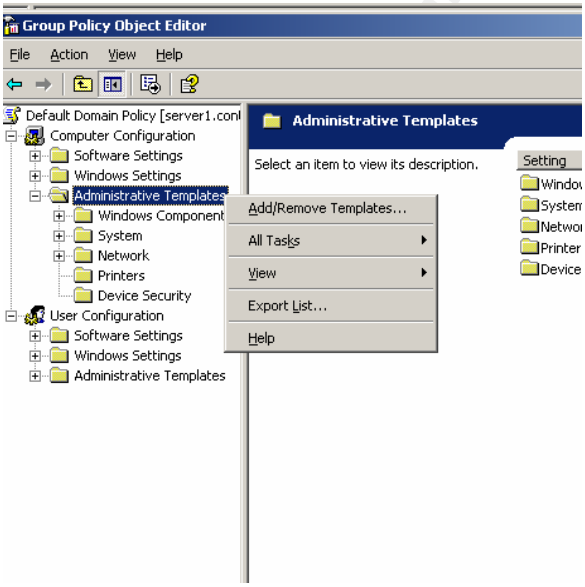


Figure 4 Importing USBDisable.adm

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

To use the “DisableUSB template” above, first, open the Windows Group Policy Management tool. Next, expand the group policy objects branch and locate the policy in which you wish to disable USB drives. Right-click on the policy and select EDIT from the menu. The GROUP POLICY OBJECT EDITOR will appear. Next, under the COMPUTER CONFIGURATION section right-click on ADMINISTRATIVE TEMPLATES, and select Add/Remove Templates. Once this is done The Add/Remove Templates dialog will appear (Figure 5 Add/Remove Templates). Select ADD, browse to DisableUSB.ADM, and click OK.

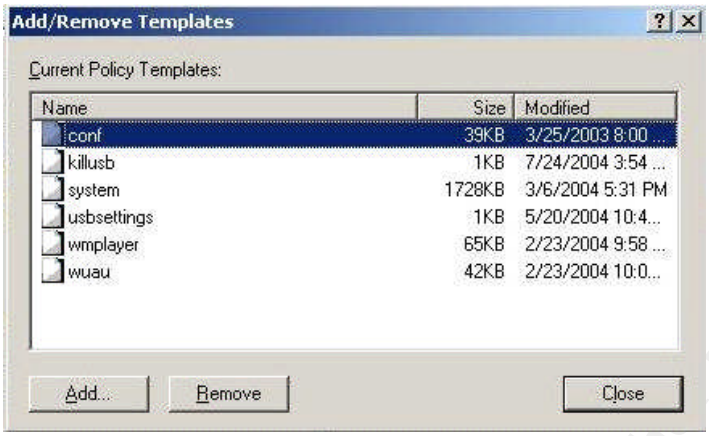


Figure 5 Add/Remove Templates

4.6.3 Using the Administrative Template

The Administrative Template is a registry-based policy and is not considered to be “fully managed”. When the Group policy is removed, the settings in the policy persist on the workstation. It is functionally equivalent to a direct registry modification. It also means that the settings within the policy are not visible under the default filter settings. To configure the USB settings, it will be necessary to change the Group policy display filter. First, right-click the Administrative Templates, select VIEW, followed by “Filtering…”. (Figure 6 Policy Filtering)

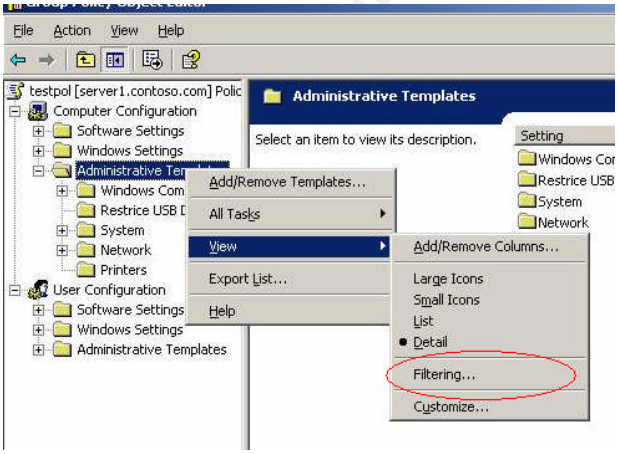
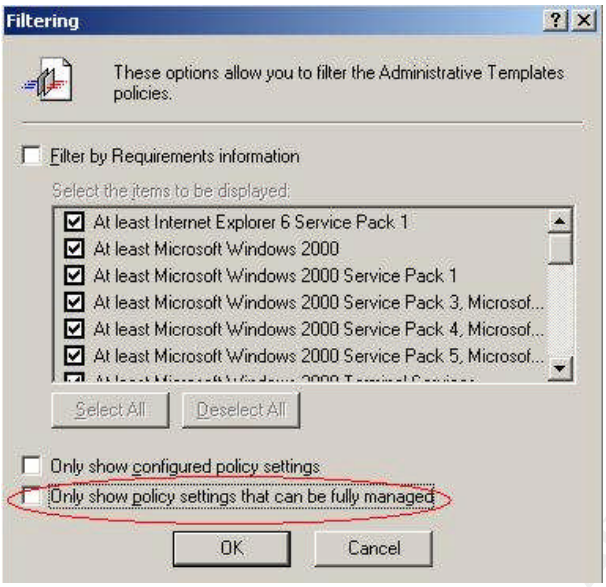


Figure 6 Policy Filtering

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Figure 7 Filter Details

After selecting the Filtering, the following Dialog box will appear. Uncheck “Only show policies that can be fully managed”. (Figure 7 Filter Details) After unchecking this box, you can use the group policy editor to control the use of USB drives. Select ENABLE or DISABLE from the group policy to manage USB drives.



5.0 DATA FORENSICS AND DISPOSAL

Similar to platter-based disk drives, data stored on USB Flash Drives are recoverable even after having been deleted. Data leaves behind a signature even after it has been overwritten. It is likely that specialized hardware could examine those signatures and recover data from USB drives after it has been erased and overwritten. To dispose of the data, USB thumb drives should be physically destroyed. Whacking it with a hammer several times should do the job. In the technical whitepaper “Data Remanence in Semiconductor Devices” by Peter Gutmann of IBM's T. J. Watson Research Center, Mr. Gutmann gives several recommendations for preventing the retrieval of data from residual images. Among them are:

- Cycle EEPROM/flash cells 10-100 times with random data before writing anything sensitive to them to eliminate any noticeable effects arising from the use of fresh cells (but see also the point further down about over-intelligent non-volatile storage systems).
- Remember that some non-volatile memory devices are a little too intelligent, and may leave copies of sensitive data in mapped-out memory blocks after the active copy has been erased. Devices and/or file systems, which implement wear-leveling techniques, are also problematic since there is no way to know where your data is really going unless you can access the device at a very low level. [5]

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

6.0 CONCLUSION

USB drives, like any other technology can be a blessing or a curse. These small devices make it very easy to transfer files from one machine to another, or to back up information to a very durable, fast medium. They can also be used to spread viruses or steal confidential data. It is necessary to examine the threats and apply the appropriate countermeasures to manage the risk at a level acceptable to your corporate environment.

7.0 REFERENCES

1. Science Daily, “Flash Memory”, Science Daily, URL:http://www.sciencedaily.com/encyclopedia/flash_memory (July 2004)

2. Dan Costa, “Flash Forward, Part 1”, CPU Planet, URL:http://www.cpuplanet.com/features/article.php/2179171 (June 2004)

3. Nathan Obr, USB Storage A focus on UFDs", Microsoft Corporation, URL:http://download.microsoft.com/download/c/f/1/cf1806ad-5a4f-4f7d-a5b2-07fdb59a7adb/WH03_TPA60.exe) June 2004

4. USB Alliance, “USB Flash Drive Worldwide Forecast: Revenues, Units and Capacity 2004-2008”, URL:http://www.usbflashdrive.org/usbfd_marketoutlook.html (June 2004)

5. Peter Gutmann, “Data Remanence in Semiconductor Devices”, IBM T.J.Watson Research Center, URL:http://www.securityfocus.com/library/3636 (June 2004)

6. The PC Guide, “Floppy Disk Controller Speed”, The PC Guide, URL:http://www.pcguide.com/ref/fdd/confSpeed-c.html (June 2004)

7. PCSTATS, “USB 2.0 – Working at 480 Mbps”, URL:http://www.pcstats.com/articleview.cfm?articleID=885# (June 2004)

8. Toni Kistner, “Personal servers simplify remote work”, URL:http://www.networkworldfusion.com/net.worker/news/2004/0524netlead.html?page=1 (June 2004)

9. John Leyden, ":iPods are the latest security risk", The Register, URL:http://www.theregister.co.uk/2004/07/07/ipod_security_risks/ (August 2004)

10. Microsoft Website, “USB Storage - FAQ for Driver and Hardware Developers“, Microsoft Corporation, URL:http://www.microsoft.com/whdc/device/storage/usbfaq.mspx (June 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

11. Diskgo!, “Peripheral EDGE DiskGO! USB Watch“, URL:http://www.edgetechcorp.com/products/diskgo/ (August 2004)

12. Microsoft Developers Network, “Enabling and Disabling Autoplay”, Microsoft Corporation, URL:http://msdn.microsoft.com/library/default.asp?url=/library/en-us/shellcc/platform/Shell/programmersguide/shell_basics/shell_basics_extending/autorun/autoplay_reg.asp (June 2004)

13. Microsoft Knowledge Base, “HOW TO: Disable the Use of USB Storage Devices in Windows XP” , Microsoft Corporation, URL:http://support.microsoft.com/?kbid=823732 (August 2004)

14. Microsoft Help Files, “Managing Certificates”, Microsoft Corporation, Absolute Path: ms-its:C:\WINDOWS\Help\encrypt.chm::/encrypt_concepts_certmgt.htm (XP Professional SP2)

15. Linux Mobile System, Sourceforge.net, URL:http://linuxmobile.sourceforge.net/ (June 2004)

16. Christopher Elliot, “Got the World on a Keychain”, URL:http://www.elliott.org/vault/pt/2002/keychain.htm (June 2004)

17. Microsoft Website, “Device Driver Tools and Settings”, Microsoft Corporation, URL:http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/techref/en-us/Default.asp?url=/resources/documentation/windowsServ/2003/all/techref/en-us/w2k3tr_drvr_tools.asp (June 2004)

18. Microsoft Technet, “Implementing Registry-Based Group Policy for Applications”, Microsoft Corporation, URL:http://www.microsoft.com/technet/prodtechnol/windows2000serv/deploy/confeat/regappgp.mspx (June 2004)

19. Microsoft Knowledge Base, “HOW TO: Create Custom Administrative Templates in Windows 2000”, Microsoft Corporation, URL:http://support.microsoft.com/default.aspx?scid=kb;en-us;323639 (June 2004)

20. Microsoft Knowledge Base, “HOW TO: Disable the Use of USB Storage Devices in Windows XP”, Microsoft Corporation, URL:http://support.microsoft.com/?kbid=823732 (August 2004)

21. Peter Gutmann, “Secure Deletion of Data from Magnetic and Solid-State Memory”, Department of Computer Science University of Auckland, URL:http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html (June 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.