



Are USB Flash Drives a Security Threat to the Enterprise?

By John Bumgarner

these micro drives bypass all established security mechanisms such as firewalls, intrusion detection systems and antivirus applications. Unknowingly users can unleash viruses, worms and Trojans into the corporate network. Mischievous employees can smuggle in hacking tools, which may be blocked if an organization is using Internet filtering applications. Disgruntled employees can upload valuable data to these devices in seconds before they are fired. Even corporate spies could use these devices to steal data, which could be used to give your competitor an advantage in the market.

Identifying these devices prior to use is nearly impossible, since most are miniaturized. These devices can be camouflaged to resemble a car key fob or an LCD flashlight. They can even be hidden in common objects like the bottom of a coffee cup or a large belt buckle.

Detecting Device Usage

Most of the current USB devices require no external driver installations, because Microsoft provides native support for these Universal Serial Bus Mass Storage devices in Windows 2000, Windows XP and Windows Server 2003 operating systems, as well as Windows Millennium Edition (Windows Me). The devices are also supported in MAC OS 9 and Linux 2.4.17 and beyond.

The driver used to control these drives in Windows operating systems is the `usbstor.sys`, which is the USB storage port driver. When a USB mass storage device is detected, the driver is loaded automatically using the Plug and Play (PnP) hardware identifiers (HWID) or a compatible identifier matched in the file `usbstor.inf`. Common users can install the driver without Administrator or Power User privileges.

The easiest method to determine if a USB mass storage device has been used on a computer running a Windows operating system is to verify the existence of the `usbstor.sys` driver. If a USB mass storage device has been installed on the system the driver will be located in `\winnt\system32\drivers` or `\windows\system32\drivers`.

If the file is present you can verify who has permission to use the driver by right clicking on the file and selecting Properties, which will display the properties window. Select the Security tab to view the users who have access to the driver. By default in Windows 2000 the following groups and users have access to the driver: Administrator Group, Power Users Group, Users Group and the System Account. In Windows XP, the default is the Everyone Group.

In the 2003 movie *The Recruit*, an agent for the Central Intelligence Agency downloaded sensitive information onto a Universal Serial Bus (USB) Flash drive as part of a security test. The drive was then smuggled out in the false bottom of a travel coffee cup, which the agent filled with liquid. This simple technique allowed the agent to bypass the security systems that scanned packages as personnel exited.

Could this happen in the real world? Of course it could, especially since most of us do not work in ultra secure organizations like the CIA.

Throughout history, proprietary information has been downloaded onto magnetic media (floppies, CDs, ZIP disks, etc.) and carried out in briefcases, in purses and even strapped to the human body. Over the years these forms of media have been replaced with various types of USB drives.

The type of USB drive that poses the biggest security threat to enterprises is commonly referred to as a Flash drive. Several manufacturers market the devices under other names, which include USB drive, key drives and pen drives.

All USB Flash drives consist of a compact flash card, which is encased in plastic and plugs into a computer's USB port. Once enabled, the device resembles an additional hard drive where files can be stored. These portable drives come in a variety of sizes, which range from 16MBs to 2GBs and beyond. The average sizes most commonly purchased are 64MBs, 128MBs and 256MBs. Some vendors have even started giving away the 16MB ones with their company logo embossed on the cover at trade shows.

Security Threat Posed

Any USB Flash device introduced into a networked environment poses a grave risk to an organization's overall security posture. In most organizations,

Restricting USB Storage Device Usage

Restricting access to all USB devices is possible within most computer BIOS files. The problem with restricting all USB devices is that many hardware vendors (keyboard, mouse, etc.) use only USB ports and not legacy ones. If this measure is used to restrict access, a BIOS password should be established to prevent unauthorized users from modifying the parameters.

It has been suggested that manually setting the registry key `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\AllocateDASD` (DASD is an old mainframe term that stands for a direct access storage device—a hard drive) or setting *Local Policies > Security Options > Allowed to eject removable NTFS media* will restrict access to USB drives. By setting these values, a user can still install a USB mass storage device, but cannot format the drive or eject the drives through the operating system automated process.

If your business object is to prevent the common user from installing USB mass storage devices using the Windows built-in driver, the following security permissions should be established at the minimum. These security settings are per-workstation or -server and require administrative privileges to perform.

Prior to modifying any security permissions, the administrator needs to remove all installed USB drives and uninstall the USB Mass Storage driver. To remove any installed USB drives, open *Control Panel > Administrative Tools > Computer Management > System Tools > Device Manager > Disk Drives* and remove any unauthorized storage devices. To remove any installed USB drives, open *Control Panel > Administrative Tools > Computer Management > System Tools > Device Manager > Universal Serial Bus Controller* and uninstall the USB Mass Storage Device listed.

The first modification is to deny all access to the driver `usbstor.sys` for each user individually or in a group (DenyUSBAccess). The second is to set the same security permissions on the files `usbstor.inf` and `usbstor.pnf` located in the `\winnt\inf` or `\windows\inf` directory. The third is to remove the Administrator Group, Power User Groups and System Account from the security permission.

These modified security permissions will prevent all common users from installing a USB storage device. It also prevents the System Account from being spoofed to install a USB storage device. Remember anyone in the Administrator Group can bypass these settings if they desire. Anyone that is listed in the deny group that attempts to install a USB Mass Storage Device will receive a warning that only an administrator is authorized to perform the install.

Caution should be exercised when restricting access to these files, because other USB devices (keyboard, mouse, scanner) may use the same driver. Deleting the file `usbstor.sys` is not an option, because it will be automatically replaced within seconds by the operating system with the same file.

Another method of restricting access to USB mass storage devices is setting the same security permissions discussed above on the registry key `HKEY_LOCAL_MACHINE\SYSTEM\Microsoft\CurrentControlSet\Enum\Usbstor`, which is created when a device is installed.

To allow authorized users permissions to install the devices on systems, add the users individually or in a group (AllowUSBAccess) to the files `usbstor.sys`, `usbstor.inf` and `usbstor.pnf`.

Establishing Guidelines

All organizations need to establish an Acceptable Use Policy concerning the use of USB devices within their networks. These guidelines should

cover all USB devices that can be used to store information. Devices like digital cameras, which accommodate Compact Flash, Memory Stick and Secure Digital cards, need to be included in the policy. Personal Digital Assistants (PDAs) can also use the same forms of media that a digital camera can, so they need to be controlled, too. Even MP3 players can be connected to systems via a USB port and they also have the capability to store items other than music files. And of course all forms of USB Mass Storage devices need to be included, especially Flash drives.

The policy should mandate that all users who require USB devices obtain some form of authorization prior to using a device within the network. The policy needs to outline audit requirements, which can be used to identify unauthorized USB devices.

Guidelines need to be established which cover the removal of these devices from the corporation premises. Since all USB Flash drives are portable, the likelihood of them being misplaced or stolen is high. To counter the potential loss of sensitive information stored on the drives, the policy should dictate a minimum level of encryption (Advance Encryption Standard) to protect data. The policy could also require that only drives with embedded biometric readers be authorized within the corporation, especially if they are company issued.


The policy should required all USB Flash drives to contain a file with a contact phone number and P.O. Box which can be used to return a misplaced device. A legal disclaimer file should also be included which indicates that information on the drive is confidential and protected by law.

The policy should require that all removal drives be scanned for viruses when used with a corporate computer. When the devices are no longer needed, the policy should require the drives be wiped using an approved application.

When developing the policy, your legal department should be consulted as to the legalities of searching and seizing unauthorized devices. Human Resources and the legal department need to provide guidance on the type of punishment a person can receive for using a USB Flash drive without prior approval.

An overview about the security risks posed by these devices should be included in any employee awareness programs. Physical security personnel should also receive training about these devices and the potential threat they present to the organization from unauthorized use.

Conclusion

All organizations need to embrace flash drives, since they are growing in popularity and will continue to do so as they replace the traditional floppy drive. The security risks from these devices are increasing, but can be reduced through two measures. The first is to establish policies and procedures that provide guidelines for these devices within the corporation. The second is to establish an awareness campaign about the security threats these devices pose to the organization. 

John Bumgarner, M.A., CISSP, GCIH, IAM, SSCP, is the founder and president of Cyber Watch Inc., which offers strategic, operational and tactical security consulting to a variety of clients. Previously John worked with several U.S. government agencies, including the United States Special Operation Command, Central Intelligence Agency, National Security Agency, Defense Intelligence Agency, and others. He has written articles for Security Management Magazine and has spoken at several conferences on information security topics. John recently developed a product called PassGuard™ used to protect passwords and sensitive accounts from hackers.