USB FLASH DRIVES - SECURITY RISKS AND PROTECTION

Dimitar Bogatinov, Slavko Angelevski
University "Goce Delcev" – Stip, Military Academy "General Mihailo Apostolski " - Skopje
dimitar.bogatinov@ugd.edu.mk, slavko.angelevski@ugd.edu.mk,

Abstract:

Information has great importance for organizations in general, especially for the security organizations, and should be adequately protected. Information exists in various forms: paper, electronic information transmitted by telegraph, telephone, shown on film, etc.. No matter in what form the information occur, it should be adequately protected in every moment because information's that are well protected minimize the damage that may occur.

Physical security is considered an integral part of information systems security. The idea that small devices pose a security threat for enterprises is well established. On the other hand, consented and supervised access to USB ports via USB flash drives is sometimes allowed. The large storage capacity of USB flash drives relative to their small size and low cost means that using them for data storage without adequate operational and logical controls can pose a serious threat to information confidentiality, integrity, and availability.

Using USB flash drives can increase the risk of data loss (when a physical device is lost), data exposure (when sensitive data is exposed to the public or a third party without consent), and increased exposure to network-based attacks to and from any system the device is connected to (both directly and via networks over the internet).

In the past years, 70% of businesses have traced the loss of sensitive or confidential information to USB flash memory sticks. While such losses can obviously occur when the devices get lost or stolen, 55% of those incidents are likely related to malware-infected devices that introduced malicious code onto corporate networks.

This paper will highlight the security risks associated with the use of USB flash drives. It will briefly explain some common types of attacks, and common necessary measures to mitigate or at least reduced. As existing products evolve and new ones enter the market, you must use them with caution, always considering their security features, possible vulnerabilities, and ways they could be targeted by malicious attackers.

Key words: USB device, crime, risks, protection, security

1. INTRODUCTION

After nearly 15 years of development, USB storage devices come in just about every conceivable shape and size, from 1 gigabyte (GB) thumb drives up to standard external drives with capacities up to 6 terabytes (TB). Once a mere novelty peripheral, these devices are now as common as the mouse and keyboard. Analysts say that in 2010 the market have shipped over 2.8 billion USB-enabled devices.

Unfortunately, even as USB devices have evolved into useful storage media, they've also turned into a security nightmare for organizations. The development of USB technology has always been about ease of use, connectivity, low cost and performance – with little if any thought to security. It is not only corporate users who enjoy the benefits of today's USB devices. Cyber-criminals and data thieves are increasingly using removable media to introduce malware and steal information from computers. One only need read the news regularly to see that USB devices are involved time and time again in today's highest profile data breaches, either through the loading of breach-causing malware into the backend corporate network, by facilitating intentional covert removal of copied data, or simply by enabling data loss through the misplacement of an unencrypted device. (According to University of Maryland Department of Criminology and Criminal Justice Fall, 2004)

Computer information systems are vulnerable to physical attacks, electronic hacking, and natural disasters. With computer information systems serving as the vital life blood of many organizations, managers must be aware of the both the risks and the opportunities to minimize the risks to information systems. Discussion is divided into types of computer crime, information systems and technology vulnerabilities, and ways to manage the risks.
(According to Computer Crime, Vulnerabilities of Information Systems, and Managing Risks of Technology Vulnerabilities and Portable Panic, The Evolution of USB Insecurity)

2. TYPES OF COMPUTER CRIME

Typically, computer crime can be categorized by the type of activity which occurs. Four basic categories are utilized in describing computer crime.
These are: theft, fraud, copyright infringement, and attacks.

2.1. Theft

Theft in computer crime may refer to either unauthorized removal of physical items such as hardware or unauthorized removal or copying of data or information. It is well known that laptop computers are targeted at airports and restaurants. The prize garnered with theft of a laptop is

usually the data or information such as passwords for corporate systems contained on the laptops rather than the hardware.

For example, in the UK, a laptop with data of some 2 000 people with individual savings accounts (ISAs) was stolen from a HM Revenue & Customs employee; HM Revenue & Customs lost personal details of 6 500 private pension holders; nine NHS trusts lost patient records kept on disk; details of 1 500 students were lost in the post; details of three million British learner drivers were lost in the United States, a USB drive was stolen with names, grades and social security numbers of 6 500 former students, USB flash drives with US Army classified military information were upfor sale at a bazaar outside Bagram, Afghanistan. (Accordinig to The Times. (February 2008). , John Swarts. (June 2006). Watson, Los Angeles Times. (April 2006)).

2.2. Fraud

Fraud on the Internet may run the gamut from credit card offers which are utilized only to capture personal information, to investor postings which promote a stock or investment offer to encourage investment which will benefit the person posting the information, to medical and pharmaceutical -related sites which purport to provide correct medical advice or sell altered medications.

2.3. Copyright infringement

The Internet has provided a unique opportunity and environment for copyright infringement. This type of computer crime encompasses use of software, music, etc which is not appropriately acquired (purchased). Software piracy occurs more easily with the ability to post files for downloading all over the world. However, another more costly copyright infringement occurs when trademarks and logos of corporations are posted on non-authorized web sites. Some criminals utilize the trademarks and logos to appear to be a legitimate site to perpetrate fraud. Many corporations have employees or consulting contractors who constantly crawl the web to sniff out illegal usage of trademarks and logos.

2.4. **Attacks on organizations and individuals**

Attacks on organizational information systems may be either physical or logical. There are several instances of web sites, products, and individuals being libeled or attacked by individuals or groups. One of the classic examples was the attack on Propter and Gamble as an occult organization, AOL and other ISPs cooperate fully with criminal justice systems to reveal identities of those deploying web sites of question.

Denial of Service Attacks (DoS) target specific web sites and associated servers. Some of the newsworthy examples of DoS during 2000 - 2001 have occurred at Microsoft.com, eBay.com, and Amazon.com. Web servers and connections can only handle so much traffic so Denial of Service (DoS) usually takes the form of one of two ways:

- Coordinated attack (typically from unsuspecting desktops) to a particular IP address or URL requesting a page - overwhelms server and DoS occurs
- Attack sends incomplete packets so that traffic gets jammed with requests for re-send. (According to University of Maryland Department of Criminology and Criminal Justice Fall, 2004)

3. USE RISKS - USB FLASH DRIVES

Let's examine three of the top risks, and some of the hacker tools and techniques that factor into these risks.

3.1 Malware Propagation

Security companies are reporting an increase in malware that propagates via USB devices and other removable media. In fact, it was just such a worm outbreak that led the US Army to ban the use of USB devices in late-2008. Malware, such as the SillyFDC worm that plagued the Army, copy themselves to all drives connected to infected machines. Any USB device connected to an infected machine would then become infected and later when it is connected to yet another machine, that machine too also begins infecting other USB devices plugged into it. This "worm like" malware propagation method copies itself to all available drives, shares, removable media and peer-to-peer software application file folders. The most popular methods currently in use are:

- **Simple file copy method**

  Relies on social engineering to entice the user to click on an application icon to launch the application which then copies itself to all available drives.

- **AutoRun.inf modification method**

  Modifies or creates an AutoRun.inf file on all available drives, shares and removable media. When an infected USB drive is later inserted into another computer, the malicious software automatically executes with no user intervention.

3.2. Data Loss

The widespread use of USB devices within an organization can open it up to data loss on two major fronts: data stolen by copying onto a device, and data stolen by copying from a device.

In the former case, Pod-Slurp was one of the first programs to highlight the insecurity issues of USB devices. Simply plugging a USB device loaded with Slurp into a victim's computer would automatically start the scripts copying each and every document from the host PC's My Documents directory on to the USB stick. One could modify the script to target spreadsheets, PowerPoint files or any specific file type of one's choice. Further, it could easily be modified to send files via email or FTP instead of copying them to the USB device.

As for the second scenario, this can be particularly dangerous if a user has innocently loaded sensitive material onto a USB drive and decides to use it on public, unsecured computers, such as systems at airport business centers, Kinko's locations, hotels and libraries.

In a 2005 demonstration at a closed security conference, the author demonstrated a program he wrote called "USB-Puke" that simply silently created a "dd" image (bit-bit copy) of any USB drive that was inserted into the author's laptop. The use of "dd" allowed the author to not only capture copies of all existing files on the users USB drive but to also recover unallocated space containing previously deleted files on the users USB key that remained as remnants on the drive's unallocated space. The demonstration was eye-opening to attendees and was seen as a good tool for raising awareness. However, because of abuse considerations the author never released program publicly. Since then, innumerable other tools have cropped up in the wild with similar attributes and even more advanced features.

For example, HTTP RAT automatically opens a back channel over HTTP to the Public Internet that allows a remote person to simply connect to a compromised PC via Firefox. The remote user can then browse through all connected or available network drives to pick and choose which files to steal remotely over the HTTP connection. And USB Switch Blade extracts all password hashes using pwdump from the target machine for later use in password cracking. Simply walk up to the victim's machine, plug in the USB device for only 60 seconds or less, and walk away with all password hashes. Other variations include the ability to also grab browser history for later mining of user financial site credentials, MSN messenger user credentials and more.

3.3. Hacking

An extremely useful feature of USB drives is their ability to act as a "PC on a stick" through the use of certain platform and virtualization utilities such as BartPE/PeToUSB, UBCD4, UNetBootin and Mo -joPac. It also makes it possible for malicious users to replicate their entire Windows hacking lab with a USB device and run it on virtually any PC with an available USB port. When the malicious user is done, she simply removes the USB device and leaves without a trace.

Similarly, terrorist organizations have adopted the use of encrypted communications software on a USB stick. A terrorist can anonymously walk into any cyber cafe, plug in a USB device containing software such as Mujahedeen Secrets 2, send email, files or have chat communications using military-grade encryption, and then simply unplug the device - leaving no trace of its use on the cyber cafe PC. (According to Lomas, N. 2006. The A to Z of Security, and Portable Panic, The Evolution of USB Insecurity,

4. BEST PRACTICES FOR USB SECURITY

Secure USB drives are the best way to stop the proliferation of data security breaches that have plagued corporations and government agencies ever since unsecured flash drives became available. Some vendors implement security by encrypting data behind passwords. Some provide security by including a biometric fingerprint scanner on the device. Some vendors manufacture both types.

4.1. Seven steps to secure personal storage drives

Every organization can take the seven steps to secure personal storage drives**,** to optimally secure personal storage drives, both on and off the network.

1. Always define and publicize your organization's policy for personal storage devices;
2. Institute the use of company-issued personal storage devices;
3. Make sure devices are fully encrypted;
4. Make sure users cannot circumvent security measures;
5. Maintain an audit trail of data stored on devices;
6. Be able to recover data residing on personal storage devices;
7. Make sure your enterprise solution comprehensively provides the ability to control the use of all removable devices, inside and out-side the corporate environment, and to centrally manage com pan issued USB drives

The value of portable storage devices in today's business environment is clear. Equally clear is the initiative organizations must take to integrate these devices with their storage and security policies. Today's enterprises can take steps to secure and monitor their data with technological solutions, develop robust policies to comply with regulations, and ensure the use of enterprise-ready personal storage devices. (According to Nimrod Reichenberg. Seven Steps to Secure USB Drives)

4.2. USB security solution attributes:

Centralized and policy-based – automated rules that dictate the state of a USB port depending on the user's location and role within the organization – should be the cornerstone of an effective USB security solution. Once granular policies are established, they can be centrally managed and pushed out to individual endpoint devices. A centralized, policy-based approach relies on automation to apply different rules to different users and devices, freeing IT staff to focus on possible breaches rather than administration.

Location-aware – A policy-based solution should allow different rules to be applied to USB ports depending on location. When a laptop or other computing device is in a riskier environment like an airport, polices can be set to restrict all USB connections. When the device is inside the company's walls, read-write access might be permitted. In other locations, like the user's home, read-only access might be applied.

Self-defending – The solution should make it impossible for the end user to defeat the security policy by turning off the policy-enforcement engine. Avoid systems that use prompts to allow users to assign security on their own endpoint devices.

File-system-level operations – Ideally, the removable storage-device security solution should operate at the file-system level to ensure control of all devices (external hard drives, CD/DVD-ROM, other forms of removable storage, etc.) that act as a file system. Meanwhile, the solution should not disable devices like a USB mouse that do not pose a threat.

Auditable and track able – The USB security solution should keep track of policy enforcement actions as well as attempted USB activities and suspected attacks. This kind of tracking is critical for not only tightening up defenses but also complying with data-control and privacy provisions contained in regulations like Sarbanes-Oxley and HIPAA (Healthcare Insurance Portability and Accountability Act). Audit information – such as who transferred information to removable media, how much data was transferred, what files were transferred and what types of devices the information was transferred to – should be accessible to the administrator.

5. COMMONLY USED COUNTERMEASURES

5.1.Disable USB Flash Drives (BIOS)

It is easy to lock or disable USB Flash Drives in the bios. Many times when you try to disable USB – it disables it entirely. This can be a real pain on newer laptops or systems that don't even have a PS2 interface for the mouse or keyboard.

There is a simple registry change that will keep the USB storage drivers from starting when the system boots. Keeps people from walking up to a PC and copying data off with a USB key, but allows you to keep your scanner, keyboard, and mouse working.

As always – back your system up before messing around in the registry.

Just open regedit and browse to this key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor

Notice the value 'Start'

Switch this value to 4, and USB storage devices are disabled.

Switch this value to 3, and USB storage devices are enabled. (Steve Wiseman, April 2006)

5.2. Block writing to USB Removable Disks

To block your computer's ability to use USB Removable Disks follow these steps:

1. Open Registry Editor.
2. In Registry Editor, navigate to the following registry key:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicie

   Create the following value (DWORD):

   WriteProtect and give it a value of 1.

Note: As always, before making changes to your registry you should always make sure you have a valid backup. In cases where you're supposed to delete or modify keys or values from the registry it is possible to first export that key or value(s) to a .REG file before performing the changes.

Close Registry Editor. You do not need to reboot the computer for changes to apply.

Users trying to write to any USB Removable Disk will now get an Access Denied message.

To return to the default configuration and enable your computer's ability to use USB Removable Disks follow these steps:

1. Go to the registry path found above.
1. Locate the following value:

WriteProtect and give it a value of 0. (Senforce Technologies, January 2007).

5.3. Enable / Disable Autorun for a Drive (using Registry)

There are two registry values that can be used to persistently disable AutoRun: NoDriveAutoRun and NoDriveTypeAutoRun. The first value disables AutoRun for specified drive letters and the second disables AutoRun for a class of drives. If either of these values is set to disable AutoRun for a particular device, it will be disabled.

The NoDriveAutoRun value disables AutoRun for specified drive letters. It is a REG_DWORD data value, found under the following key:

HKEY_CURRENT_USER

Software

Microsoft

Windows

CurrentVersion

Policies

Explorer

The first bit of the value corresponds to drive A:, the second to B:, and so on. To disable AutoRun for one or more drive letters, set the corresponding bits. For example, to disable the A: and C: drives, set NoDriveAutoRun to 0x00000005.

The NoDriveTypeAutoRun value disables AutoRun for a class of drives. It is a REG_DWORD or 4-byte REG_BINARY data value, found under the same key.

HKEY_CURRENT_USER

Software

Microsoft

Windows

CurrentVersion

Policies

Explorer

By setting the bits of this value's first byte, different drives can be excluded from working with AutoRun. ***Windows must be restarted before the changes take effect.*** (According to Petri IT Knowledgebase, 2009).

5.4. Password protect USB Drive without using software

There are many third party software's to password protect your USB Drive but here i am going to show how to password protect USB without using any software's.

Many people like to protect their USB Drive from others that is they won't like to share their personal files and data to others. For this they will protect their USB Drive by using some third party software's to password protect their USB Drive. Although this software's are available free they require money to use full version of the software so if you are using windows you no need any software's to protect your USB Drive you just follow this simple ways listed below.

Steps on how to password protect USB Drive without using software's:

- First Insert your USB Drive into the Computer
- Click Start –> Control panel –> System and Security –> Bit locker Drive Encryption
- Click " Bit locker Drive Encryption" now the application will be launchedbitlocker2
- Then search your "USB Drive" and Click "Turn on Bit locker"
- Now Windows will ask you to "set the password"bitlocker3
- Set your password in combination of special characters and symbols
- After Setting up your Password click "Next"
- Now a window will appear asks you to "store the recovery key"
- Click "Save the recovery key to a file" and save the file to your desired location
- Then Click "Next" –> "Start Encrypting"
- The Encryption process may took some time depending on size of your USB Drive
- Done…! From now your USB Drive is protected by password. If someone wants to assess your USB Drive the Windows asks you to enter the "password"

For Removing the Password just follow this steps:

Follow first-3 steps

- On third step Click "Turn off Bit locker"
- Now The USB Drive will be Decrypted

Done..! From now the windows will never asks you to enter the password (According to Techmirchi, 2013)..

5.5. Manually save files with a password

As mentioned above, you can't safely password protect your entire USB stick without using encryption. However, if you shy away from the time consuming encryption process of entire folders and need a really quick way to only protect a few selected files, maybe you can simply save those with a USB password.

Many programs, including Word and Excel, allow you to save files with a password. For example in Word, while the document is open, go to > *Tools* > *Options* and switch to the *Security* tab. Now enter a *Password to open*, click OK, re-enter the password when asked, and finally save your document and don't forget the password.

6. CONCLUSION

The purpose of this paper is to raise awareness of the risks posed by the use of USB flash devices, and thus show a few easy ways to protected from this kind of crime.

The creators of malicious scripts always look to do maximum damage with minimal effort, this USB devices are a primary target for abuse.

Although there is increasing awareness of the risks and costs related to the insecure usage of USB flash drives, there is still a significant amount of work to do. It is therefore crucial that IT asset managers prepare themselves and their organisations to regulate, manage and audit the use of USB flash drives as ensuring the ability to secure information on the network and the opportunity to manage data which enter and leave the company environment is key for any organisation regardless of its size and maturity.

REFERENCES

1. Computer Crime, Vulnerabilities of Information Systems, and Managing Risks of Technology Vulnerabilities, Retrieved from http://www.profhelp.com/crime/computercrime.pdf
2. John Swarts. (June 2006). Small drives cause big problems', USA Today, 16.
3. Lomas, N.(2006).The A to Z of Security, Retrieved from http://software.silicon.com/security/0,39024655,39164025-22,00.htm?r=1;
4. Nimrod Reichenberg. Seven Steps to Secure USB Drives, Retrieved from http://www.brevard.k12.fl.us/infosec/documents/SevenStepstoSecureUSBDrives.pdf
5. Petri IT Knowledgebase.(2009). Retrieved from http://www.petri.co.il/disable_writing_to_usb_disks_in_xp_sp2.htm;
6. Portable Panic, The Evolution of USB Insecurity, Retrieved from http://www.preventia.co.uk/resources/white_papers/lumension/the-Evolution-of-USB-Insecurity.pdf
7. Senforce Technologies. (January 2007). Best Practices for Managing and Enforcing USB Security:*Five Questions You Should Ask About Universal Serial Bus (USB) Security*, Retrieved from http://www.pcsltd.com/pdf/012007-USBWhitepaper.pdf
8. Steve Wiseman. (April 2006). Retrieved from http://www.intelliadmin.com/index.php/2006/04/disable-usb-drives/
9. Techmirchi. (2013).Retrieved from http://techmirchi.com/how-to-password-protect-usb-drive-without-using-software/

10. The Times. (February 2008). ‘Timetable of missing data blunders’, ‘Disc listing foreign criminals lost for year’,
11. University of Maryland Department of Criminology and Criminal Justice Fall. (2004). Computer Crime and Computer Fraud,Retrieved from http://www6.montgomerycountymd.gov/content/cjcc/pdf/computer_crime_study.pdf
12. Watson, Los Angeles Times. (April 2006). ‘US military secrets for sale at Afghanistan bazaar’.