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

Jim Lairmore – GSEC practical assignment version 1.4b

Are USB Flash Drives a harmless tool, or a security threat?

Summary

The days of the floppy disk are finally over. I know what you're thinking. You've heard this all before. For years we have been reading reports of its imminent demise. First it was the super floppy, then the Zip drive, then the CD-R. Unfortunately, none of these solutions has offered the ease of use and simplistic operation necessary to really catch on. But I think we can now safely say with certainty that the day we see the 3.5" disk go the way of the 5 ¼" is close at hand. What is the reason for this death knell? What is it that will finally spell the end of the venerable floppy disk? The USB flash drive. The low cost, ease of use, flexibility, durability, and portability of these devices is seeing their use proliferate exponentially both at home and in the workplace with no apparent end in sight.

This paper will take a look at these devices and examine their capabilities, uses, and benefits. We will then look at some of the risks these devices may bring to your environment. Finally, we will find that, much like Instant Messaging, it may be more practical to manage the use of this new technology than try ban it and will look at some steps to take in order to minimize the risks posed by their use.

What is it?

Known by nearly as many names as there are manufacturers (pen drives, flash disks, USB drive, key drive, etc), USB flash drives are basically compact flash cards that plug into the USB port on your computer and act as an additional drive. Most of these pocket sized storage devices are just slightly larger than a cigarette lighter and can hold anywhere from 8MB - 1GB of data. And because USB utilizes Plug and Play technology, flash drives are platform and manufacturer independent which makes them perfect for sharing data between PC's with different operating systems. USB is natively supported on PC's running Windows ME/2000/XP (Windows 98 SE is also supported but requires a driver installation), Mac OS 9-10X, and Linux 2.4.17 and above. Just plug the Flash Drive into an available USB port and your computer will see it as an additional drive. Being a solid state memory device, flash drives have no moving parts, perform well even in dusty environments, and have data transfer rates of up to 6MB/sec. Flash Drives also do not require a separate power source or batteries and draw very little power from the computer through the USB connection, making them ideal for laptops. Most devices claim a data retention time of ten years and a useful life of one million read/write operations. At least one model is even waterproof. It can be dropped into a glass of water and have its contents retrieved undamaged.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

As memory prices have continued to fall in recent years, so too has the price of these devices. Businesses are already popping up that will print your company logo on the side of a Flash Drive for as little as a penny per drive. The day they replace the T-shirt and the pen as a promotional giveaway is clearly on the horizon. And while larger drives with more storage and features can go for a pricey $500 or more, some of the 64MB basic models can already be found for as little as $10. In fact, market research firm In-Stat/MDR is projecting growth of the flash memory market to climb from $7.6 Billion in 2001 to $16.2 Billion in 2006[1]. No doubt Flash Drives will play a key role in this increase.

On the PC side, Dell Computer is leading the charge in this revolution as it has already dropped the floppy as standard equipment from some of its Inspiron notebooks. They also announced earlier this year that they will stop including it in some of its Dimension desktops as part of a wider move away from this previously vital component in favor of its own USB Memory Key storage device[2]. Short of a consumer uprising protesting this trend, expect other manufacturers to quickly follow suit.

USB flash drives currently come in two types: With an integrated CPU, and without an integrated CPU. Combining a CPU with a Flash memory chip gives flash drives the ability to run applications directly from the disk. This has allowed imaginative device manufacturers to incorporate a wide variety of interesting capabilities into their products including several security features (more on this later). It also, of course, allows the device to be bootable. As you can probably guess, this raises a few security concerns that we will be taking a look at a little later on.

The Good

USB Flash drives have a virtually limitless number of uses. You may be sitting there already thinking of ways to use one of these handy devices yourself. The obvious one is the ability to transport large files to or from a remote workstation without having to worry about computer compatibility issues or slow network connection speeds. It is far more convenient to transport data around on a device the size of a pen and weighing only a few ounces than it is to carry around an external hard drive or continually burn CD's. It also gives employees the option of taking work home or going on business trips without having to carry around a heavy laptop. Another benefit to not traveling with your laptop is avoiding the potential for damage to your machine. The pounding a unit can take from crowded overhead compartments, taxicab trunks, and hotel bellhops can really take their toll. The Assurant Group reported accidental damage to laptops as the number 1 cause of loss in 2001[3] with nearly 1.4 million claims. Showing a measurable ROI (return on investment) to upper management is always a challenge in the security business, but eliminating airline surcharges and

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

reducing repair and replacement costs are two line items every business can identify in an age of strained IT budgets. These slim plastic devices also fit right into a shirt pocket or purse and will not be found by metal detectors, speeding you through the security screening process.

Flash drives also offer some distinct advantages over CD-R's and CD-RW's. First, you can edit the document or data stored on the drive as many times as you like without burning another disk. Second, you won't waste an entire 700MB disc to hold only a few MB of data. Third, data transfer rates are comparable, if not faster. Fourth, Flash Drives are far more durable and can't be scratched like CD-ROMs. Imagine security administrators or forensic investigators being able to use a Flash Drive as a portable toolkit that could include security patches, recovery tools, penetration testing tools, or even Snort. You could simply plug in a Flash Drive carrying Snort, load and configure it, then examine network traffic without having to worry about bringing a laptop, remembering a crossover cable, or finding an available span port. Or how secure would your system become if you could just carry your OS around on a bootable unit with you and use your PC's hard drive only to store programs and data. Without the OS, no one could get into your system.

Manufacturers have already begun to build devices around specific uses, most notably as MP3 players. The ease of transferring files to and from the device makes them ideal for this purpose. These players typically come with headphones and neck straps and can even be found with equalizers, bass boosters, and LCD screens. While some of these units work on a Lithium-ion rechargeable battery (charged by plugging it into the USB port and drawing its power from the PC), others require one AAA battery for use while away from the connection (giving it as much as 12 hours of playing time). Other manufacturers also include the ability to use the device as a complete POP3/SMTP e-mail client that will allow you to read and compose text based and HTML mail from any PC without adding any files or altering any registry settings on the host machine. Some even let you import your current Windows address book or Outlook Express settings. Other features being offered include ID3 tagging of MP3 files, FM radios, and digital voice recorders, making them the ideal digital notepad.

Flash drives are also being made with expansion slots built into the unit to accommodate Memory Stick, Compact Flash, and Secure Digital cards. This means flash drives with this capability are upgradeable to the highest capacity card available on the market and allows you to expand the storage space of the system even further. Interoperability of media also allows you to share cards between other types of devices such as PDA's, digital cameras, and MP3 players. Lexar Media's JumpDrive Trio[4] actually features a three-in-one card slot, making it possible to send data off to the recipient on the flash card of their choice.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

And speaking of sending, because of their size, flash drives are also easy to ship. Just drop them into a small box or padded envelope and send them off. Sure, you can always email the file, but there may be instances when a client or customer, for security reasons, isn't comfortable with sending data over the Internet and would still like a hard copy. Shipping off one of these handy units is cheaper and faster than printing out 64MB of information.

Security features have also begun to be incorporated into many of these products. Like the old floppies, many of them are coming with a write protect switch that can prevent the data from being erased either accidentally or on purpose. Others use passwords to access the data. Some of these systems will actually allow you to partition your disk into protected and unprotected areas. When accessing the protected area you are prompted to enter your password, otherwise, only the unprotected areas are visible. Still others will password protect the entire drive and require software to be installed on each PC that will be utilizing the security features. This can be a bit cumbersome, but since the security software can travel with you on the drive, it is available whenever you need it installed.

By far the coolest of the devices that have incorporated security thus far is the ThumbDrive Touch from Trek 2000[5].The ThumbDrive Touch is a fingerprint secure USB drive that incorporates a biometric reader sensor onto the device itself. This device performs user authentication each time the drive is inserted into the USB port of the PC. Only when the user has been positively identified does the data stored on the ThumbDrive become accessible. This device boasts a false acceptance rate of approximately 1 in 10000 and a false rejection rate of approximately 1 in 1000. If you are worried that you may not be able to access your data at a critical juncture due to false rejection, the unit also allows you to set up a password as a failsafe. If you have trouble remembering passwords, however, this device can solve that problem for you. With 16MB drives starting as low as $80, they are certainly a viable solution to securely transporting sensitive data.



Other helpful things to look for that are being offered on various units when shopping for a drive are the ability to clip it to a pocket, attach it to a key chain, or loop it through a neck strap in order to keep from losing them. Additionally, an indicator light showing data transfers in progress and a USB cable that can run from the back of the PC to the front so you don't have to fumble around behind a dusty computer can also be useful.

The Bad

Unfortunately, these devices don't come without their drawbacks. As noted previously, prices for the larger drives, especially with some type of

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

security feature, are still a little steep. To transport something like Windows 2000 SP3, you would need at least a 512MB drive. With some type of security, those devices could run $150 or more. This may keep them from gaining widespread acceptance.

Another obvious negative is one of the things that make them so appealing. The small size and portability of these devices allows them to be easily misplaced or stolen. If you happen to lose or misplace a Flash Drive with no security features, anyone who picks up the device can easily gain access to your data. Worldwide, 591,000 notebooks were reported stolen in 2001[3]. No statistics were available for PDA's, but imagine the potential for loss and theft of a device no larger than the size of a pen. This certainly points out the necessity for choosing a device with some sort of security features incorporated. At the very least, securing your device (say to a pocket or key chain) will help to keep from walking off and leaving it behind and should be a priority.

Currently, the majority of these devices lack any type of security features or password protection that would protect the data they are storing. Additionally, most users are not security conscious or do not want to be bothered with configuring software or entering passwords when accessing data, therefore, they are unlikely to enable these features even if they are available. One other drawback to keep in mind when searching for a drive with some sort of security features is the fact that most of the software will only work with the Windows operating system. This is an obvious oversight and one that I am sure the manufacturers will rectify as the market matures since security is certainly a concern across all OS's.

Another annoyance is the fact that currently USB ports are to be found only on the backs of most computers or laptops (see the need for a USB cable in the previous section). Again, as this technology matures, I'm sure that more and more manufacturers will move one or more USB ports to the front or sides of the machine for easier access (something that is already being seen on newer model laptops). This can easily be accomplished by moving the USB, firewire, and/or other data access ports from the back and into the space used by the current (and obsolete) floppy drive.

The Ugly

As with any useful tool, it seems, comes its eventual corruption to a use in a manner for which it was not originally intended. And so it goes with the Flash Drive. The very things that make it so appealing, its small size, ease of use, and portability, also make it a potentially dangerous tool. Consider these points:

1) You don't need any specialized computer knowledge or have administrator privileges to install or use one.
2) You can't manage USB devices via Group Policy.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

3) They can easily be carried past security guards or metal detectors.
4) At 1MB/sec, a user can transfer a 120MB file to a flash drive in 2 minutes.
5) The BIOS on most new PC's can be set to boot to the USB drive first.

Viruses are high on anybody's security priority list, but certainly the risks posed by Flash Drives are a cause for additional concern. Not since the 80's, when floppies were about the only way to share data, has there been an easier way for infected files to be transferred by bypassing normal antivirus scanning methods. Most employers don't cover the cost of installing antivirus software on a user's home machine or want to be liable for administrative support by requiring it. If employees do not have software installed, or more likely, don't keep definitions up to date if they do, virus transport from home to work is likely to increase. Another more disturbing scenario would involve a virus writer leaving a Flash Drive lying around a corporate environment in the hopes that someone will pick it up and open the infected file ("Hey, Bob. Today's my lucky day. Look what I found in the lobby on the way in"). Since most antivirus software is based on signatures of known threats, an unknown virus introduced in this fashion could slip right by current scans and infect an entire network. This is already a threat through the Internet or email, but Flash Drives certainly add another front to the antivirus wars that will need to be addressed.

Malicious software is another concern high on the priority list. While it is true that CD-R's may have already made this type of transfer a moot point, this does provide another (easier) avenue for those with malicious intent to bring these types of programs into the corporate environment. It is certainly more convenient since the transport medium does not constantly have to be replaced, but simply overwritten.

Data theft is another area ripe for the exploiting by these devices. Due to its sensitive nature and potential for negative publicity, corporate espionage is a problem that goes largely unreported. Rest assured, however, that hackers, corporate spies, and disgruntled employees steal data from networks everyday. Anyone with access to things like credit card databases, social security numbers, or personal HR information can download it in just a few minutes and walk right out the front door with no one being the wiser.

The ability to boot to these devices makes them especially dangerous in the wrong hands. A quick change in the system BIOS to boot to USB first and anybody can boot into a program such as LinNT or ERD Commander and change the administrator password on a system. They could then create their own accounts, install spyware, or leave backdoors for later use. They would even be able to cover their tracks making it nearly impossible to know they were there or what changes were made.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

One problem that often goes unnoticed or ignored in the corporate environment is the practice of employees using the company's T1 connection to the Internet to download their favorite MP3's, shareware programs, MPEG's, or porn on company time. Such abuse of company assets not only takes up valuable bandwidth and should be considered stealing, but slows the network and cuts employee productivity. Websense Inc. reported in November of 2002 that employee Internet misuse cost American corporations more than $85 Billion per year in lost productivity[6]. If you don't think that this type of activity is happening at your site, consider this alarming statistic. NetRatings Inc reported in September of 2002 that Internet usage from work has continued to rise year over year with 46 million people logging on in August of that year between the hours of 8AM and 4PM[7]. While this misuse has been occurring for several years now, the ability of employees to transfer large amounts of data to a home PC with ease can only see this type of activity increase.

Additionally, most companies keep any software programs used in the environment on a network server. This makes sense from a convenience standpoint. Programs can easily be installed on new machines, or reinstalled on machines with problems, all without having to search through shelves of software, or carry around CD's, or move PC's to a central location. These files also usually include a small text file with the CD-Key so installation can be made with a minimum of hassles. With the introduction of an easy transport method like Flash Drives, however, it also means that anyone with access to those shares can make illegal copies of those programs for their own use. Now you can simply wait for your office to buy the latest copy of Microsoft Office and then take it home without needing a CD Burner. In large environments, there can be as many as 100 IT staff members and in smaller offices, it could be the entire staff, all with access to your software. Any one of these people may want to make a copy to take home or to share on a P2P network. With the recording industry going after companies like Napster, it's not a stretch to think that manufacturers like Microsoft would like to shut down illegal software swapping. Litigation in these areas is breaking new ground everyday and companies have already been successfully sued for failing to keep employees from swapping music files at work. If an employee is making illegal copies of your software and it can be traced back to you, it is conceivable that you could be held liable. Open shares and an easy transport method makes this scenario a realistic possibility.

Reducing the Risk

By now you may be pushing the panic button and ordering the IT department to remove the USB ports on all of your PC's. While this may be the only real way to completely stop the use of these devices, it may not be a very practical one. Instead, we will look at some things we can do to manage the risks posed by their use to an acceptable level.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

A defense in depth approach to securing your environment is a necessity in today's computing enterprise in the fight against hackers and applies equally as well to viruses. If your antivirus software is only installed and configured to scan network drives and email, you are exposing yourself to virus risks. The desktop is the last chance to stop a virus before it penetrates your defenses and infects your network. Be sure to install antivirus software on all machines and keep the signatures up to date. Also, be sure that they are set up to scan all attached drives and removable media (like the floppy drive). This will help to insure that users cannot bypass your network-based scanning methods and that any virus brought in from home will be caught if transferred from a Flash Drive. To be sure your current antivirus software will catch such a transfer, conduct a test. I conducted a test in our lab environment running Symantec antivirus CE 8.0 and a Flash Drive infected with the Eicar test virus (Eicar is not really a virus, but an ASCII file that emulates virus behavior for the purposes of testing antivirus software. You can download the Eicar file at Eicar.org). When transferred from the Flash Drive, Norton did catch and delete the virus. Also, be sure to update any antivirus policy you have to include the scanning of all drives and removable media. Users will also need to be trained to scan files before opening them. Many users are aware that they should not open email attachments from unknown sources, but they may need to be reminded that this is a danger that applies to all files from any source.

You may also want to have a company policy detailing the use of Flash Drives. Some companies already have policies outlining the use PDA's, CD-R's, and wireless cards. Why not add Flash Drives? You should get upper management's approval before implementing any such policy, but be sure it includes guidelines on taking data out of the office or bringing files in from home. Of course, just writing the policy isn't enough. It needs to get into the hands of those it is intended for and they need to be educated on what is expected. Educating users on the risks that such devices can present will be one of your most important tools in fighting their misuse.

Limit access to shares containing software programs used in your environment. Certainly those in charge of setting up new PC's or troubleshooting problems may need access, but network engineers and even data security personnel do not need to be able to get into these folders. You may even want to store the CD-Key text file separately or encrypt it in order to make installing pirated software more difficult.

Internet content filtering is one way to keep employees from surfing the Internet at will. There are many third party solutions out there that can block access to Internet sites. Even if your company wants to keep the employees happy and let them surf, access to porn, gambling, hate, and other inappropriate sites should still be blocked. Not only are these sites far more likely to transmit viruses, but it also makes sense from a liability standpoint.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

If physical security was not a priority before, it should certainly be now. Be sure that access to critical servers is restricted to only those users that have a need to directly log on to the machine. Do not let unauthorized personnel wander in and out of an unlocked or unmonitored server room, and don't allow unknown people to access these rooms unchallenged. Additionally, place a BIOS password on servers so that they are not easily reconfigured. Remember that it only takes a few minutes to download megabytes of critical data.

If the use of Flash drives is to be allowed by your company, be sure to use only secure devices. Specify the type of security the devices will be required to employ and have the passwords adhere to the same standards as other passwords on your network. Be sure your users know how to install and enable these security features and enforce their use.

Losing a Flash Drive full of valuable information can be devastating. In this case Labmice.net makes the following suggestion:

> In the event your Flash Drive is lost or misplaced, including a small readable text file that includes return information could help you get it back. You may want to consider NOT including your company name in the file, and simply refer to a phone number or P.O. Box. You may also want to include a legal disclaimer that clearly identifies the information on the drive as confidential and protected by law.[9]

The Bottom Line

Flash Drives are an exciting and seemingly harmless new technology, but, as we have seen, are not without significant risks. As they increase in popularity, they will be next to impossible to ban and eliminate from any environment. Education and awareness will be the keys to reducing your exposure. Be sure to raise the awareness level of administrators and users in your environment or you could be exposing yourself to additional security problems.

References:

[1] InStat/MDR "Flash Memory Market Regaining its Luster." 11 October 2002. URL: http://www.instat.com/newmk.asp?id=361

[2] Spooner, John G. "Dell to Drive Floppy Out." 07 February 2003. URL: http://www.zdnet.com.au/reviews/computers/peripherals/story/0,2000023513,20271863,00.htm

[3] Assurant Group press release. 27 February 2002. URL: http://www.assurant.com/AG_Press%20Releases/PR-02-27-02.htm

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

[4] Lexar Media.
URL: http://store.digitalfilm.com/index.cfm?category=15&productid=JDT-231&details=Yes

[5] Trek 2000.
URL: http://www.trekstorusa.com/thumbdrive_touch.htm#tdt_features

[6] Websense Inc. URL:
http://www.websense.com/company/news/pr/02/111202.cfm

[7] NetRatings Inc. URL: http://www.nielsen-netratings.com/pr/pr_020912.pdf

[8] SecureWave. URL: http://www.securewave.com/products/securent/index.html

[9] "USB Flash Drives: Useful Device or Security Threat?" 31 March 2003.
URL: http://www.labmice.net/articles/usbflashdrives.htm.

[10] Reichard, Kevin. "USB Flash Drives: A Little Goes A Long Way." 19 March 2003. URL: http://www.smallbusinesscomputing.com/testdrive/print.php/2115681

[11] Lyon, Jack. "Mini Megabytes: USB Flash Drives." 13 August 2002.
URL: http://computers.cnet.com/hardware/0-1092-8-20256442-1.html

[12] Elliot, Christopher. "Got the World on a Keychain." 27 September 2002.
URL: http://www.elliott.org/vault/pt/2002/keychain.htm

© SANS Institute 2003, Author retains full rights.