WHITEPAPER

BLOCKMASTER®

SECURITY THROUGH INNOVATION

www.blockmastersecurity.com

Why Software-Encrypted USB Flash Drives Give a False Sense of Security

Software encryption is not a good match for USB flash drives, as it leaves them open to password cracking. This paper examines the weaknesses of software encryption and makes a strong case for hardware encryption.

BLOCKMASTER®

EXECUTIVE SUMMARY

USB flash drives are essential for saving and transporting digital information, but they can leave data vulnerable. While new Windows 7 includes enhanced security features, software encryption is not sufficient in securing data. Only hardware encryption is robust enough to properly protect critical data.

USB FLASH DRIVES HAVE BECOME HUGELY POPULAR

- They are the most convenient way to transfer large amounts of data.
- They use little power and are long-lasting and reusable.
- They work with any USB-equipped computer.

THERE IS A DOWNSIDE – "THE USB PROBLEM"

- Tens of millions are lost yearly.
- When a flash drive is lost, valuable data is exposed.
- Loss of confidential data can have a devastating effect on an organization.

SOFTWARE ENCRYPTION DOES NOT SOLVE "THE USB PROBLEM"

- Complex passwords can be cracked in mere minutes with a brute-force-attack.
- Simple password-cracking software is easily available on the Internet, often for free.
- Software encryption wears down and breaks USB flash drives, or it exposes data.
- Software encryption can be corrupted by viruses.

WINDOWS 7 DOES NOT SOLVE "THE USB PROBLEM"

- Even Microsoft admits that software encryption can be cracked.
- BitLocker is available only in the high end editions, Windows 7 Ultimate and Windows 7 Enterprise.
- Few people have deployed Windows 7.

HARDWARE ENCRYPTION IS THE ONLY SOLUTION

- Hardware encryption resists both brute-force and dictionary attacks.
- It cannot be removed or altered by malware or a virus.
- It cannot be accidentally or deliberately uninstalled by the user.
- It is transparent and easy to use.
- It is always on and requires no drivers or setup.

BENEFITS AND FUTURE OF USB FLASH DRIVES

USB flash drives are an integral part of our working lives. Alongside laptops and BlackBerrys, USB flash drives play an absolutely crucial role in enabling remote and flexible working patterns. Even more important, USB flash devices give us mobile access to all those files too sensitive or too large to be downloaded over a public network.

USB flash drives are ideal for sharing and transferring large quantities of data – on time and on budget – for the following reasons:

- All modern PCs, Macs and laptops have USB ports.
- Flash drives are resilient and robust, as they do not contain any fragile moving parts and are not sensitive to scratches or dust.
- They make transporting data from place to place a simple and speedy task.
- Their small size (and large memory) makes them incredibly convenient.
- They use little power.
- One drive can replace hundreds of CDs or DVDs.
- They invariably have a long life span and deliver reusable storage.

"Software encryption has taken a significant leap forward in very much the same way that hardware-encrypted USB flash drives did. But this does not mean that software encryption can make a second successful leap from PC to portable device."

But there is a security downside, prompting the rise of "The USB problem". The vast majority of USB drives have gone and continue to go unsecured. Users value the devices for their ability to transfer data between computers. While a lost USB stick can be inconvenient for the user, it has the potential to prompt a major security threat to many organizations. Not many users realize the consequences and gravity of losing a USB drive.

DISAPPEARING DRIVES

Apathetic attitudes have contributed to massive numbers of drives being lost or misplaced. Indeed, last year, more than 20 million sticks around the world were lost, while Centennial[1] estimates that up to 66 percent of USB drives are lost.

It's certainly inconvenient to lose a stick containing your family photographs, but it's a major security breach if sensitive business or customer data is held on these disappearing drives.

These statistics and the onerous impact of data loss have prompted many IT departments and security professionals to push "The USB problem" up their priority list. As reported in the respected IT publication *eWeek*, "The USB problem" is now regarded as the greatest challenge facing IT departments.[2] And this is understandable. Losing intellectual property contained on an open, unsecured USB flash drive could be disastrous for any organization. To ensure shareholder value, public confidence and internal productivity, trade secrets, aggregated data and other sensitive material should be carefully protected.

THE CASE FOR ENCRYPTION

To counter the potential fallout from unsecure USB flash drives, hardware-encrypted flash drives have become available. Not only do such devices offer password protection, but they also offer management capabilities that allow organizations to "control and kill" drives that fall off the radar.

Software offerings that use more traditional software encryption technologies on standard unsecure USB flash drives also are available. Organizations must be cautious, as relying on software encryption of USB flash drives can be dangerous. As this paper highlights, encrypting a drive with traditional software security is a flawed approach and a terrible misuse of a proven technology. There's a mismatch here in terms of a lack of hardware protection, an inability to ensure the integrity of the drive and pure storage technology. While software encryption has its place, this paper asserts it has no place protecting USB flash drives.

SOFTWARE ENCRYPTION BASICS

On a fundamental level, software encryption relies on a desktop computer program to execute an algorithm that encrypts and decrypts files on that computer. The technology has been popularized as a means of fully encrypting hard drives of laptop and desktop computers by open source offerings such as Truecrypt[3], and commercial products such as Microsoft's BitLocker. In this PC environment, software encryption provides an efficient solution. It is a proven and valuable technology that safeguards millions of computers the world over. Thanks to the addition of Trust Platform Modules (TPMs)[4], software encryption has taken a significant leap forward in very much the same way that hardware-encrypted USB flash drives did. But this does not mean that software encryption can make a second successful leap from PC to portable device.

THE SHORT VERSION OF SOFTWARE CONS AND HARDWARE PROS

- With software encryption of USB flash drives, you trust the computer you are using with the security of your data and the performance.
- Software encryption, a form of self-encrypted container, is executed on unknown machines and relies on the security of the host to keep the encryption master keys and the software itself safe. The encryption can be copied off the unsecure device to perform what is called "parallel offline attacks", without the user being aware of the intrusion.
- Software encryption speed depends on the host computer. Files must be unencrypted onto the hard disk, even on unknown machines, in order to be edited. This sets a dangerous precedent.
- Contrary to popular belief, software encryption cannot be used on all current USB flash drives. The encryption may be a bad match for the unsecure drive and begin to degrade its memory, causing a loss of data.

Hardware encryption uses the onboard security chip of the secure USB flash drive to perform all encryption/decryption, key generation and key handling, resulting in a significant leap forward in terms of security and usability. Following are ways in which hardware encryption provides a more secure method of data storage:

- Hardware-encrypted devices are a million times more secure than are software-encrypted USB flash drives, a fact that we explore further in this paper.
- Hardware encryption can enable data transfer speeds up to 10 times faster than those offered by software-encrypted devices. Even more important, it ensures a perfect match between encryption and storage, thus eliminating the problem of disappearing data due to corruption.
- Hardware drives offer a more consistent user experience, which is critical when organizations are seeking mass employee adoption.
- Some hardware-encrypted drives can lower I costs, as they make software portable, thus leavin laptops out of the equation.

SOFTWARE ENCRYPTION WILL CRACK

As already highlighted, software encryption will crack on a USB flash drive. In its MS Windows 7 overview[5], Microsoft itself said that "passwords are secure only until they're cracked, and cracking a password is more a matter of when than if, assuming an attacker is sufficiently dedicated". Software encryption on a USB flash drive relies solely on the user password for security of the encryption master key. Simply put, the user password encrypts the stronger master key, which in turn encrypts the data. When the password is cracked, all stored data is laid bare. As we explain below, it is impossible to limit the number of password attempts, as nothing with assured integrity can count the attempts.

SOFTWARE ENCRYPTION WITHOUT INTEGRITY

By placing the software and data in the hands of the unknown machine on which it is executed, software encryption allows the host computer and the intruder to decide how a password counter performs, meaning that the intruder has unlimited passwordcracking attempts. A seemingly secure password (e.g., 4Bentxc) takes less than an hour to

crack using a very basic brute-force attack.[6]

The business of password cracking or password recovery has a legitimate business purpose in some cases, as it can be used as a means of getting data back that otherwise would be lost. But the allowance of innumerable password attempts puts softwareencrypted data at risk to attacks by malicious intruders. What is truly worrying is that password cracking has turned into a point-and-click procedure, thanks to software available for free on the Internet or for a very low cost. Some of the myriad programs available online include Cain and Abel, John the Ripper, Hydra, ElcomSoft and LastBit.

HARDWARE-ENCRYPTED SECURE APPROACH

Contrast this with the hardware approach, in which the encryption master key is generated in the hardware at setup, using the full strength of the encryption. This is comparable to a random 43-character-long password for AES256. For example:

qU#aGAwPt*MntYAbr(nAroBemAp=loOOklE?Avde FEq[7]

A trusted hardware brute-force protection counter limits the number of password attempts, and the counter has complete integrity and cannot be changed, because it is held on the secure USB flash drive, not on the machine itself.

SOFTWARE ENCRYPTION PASSWORD-CRACKING BASICS

Password cracking is possible because of the endless password attempts that encryption software always can be forced to allow. Often the self-encrypted container is copied off the unsecure USB flash drive without the owner even noticing it – this is called a parallel offline attack. A parallel offline attack is much harder to perform on fully encrypted computers as opposed to partially encrypted ones, as the files are harder to access. Because USB flash drives are easy to use, even intruders without much technical knowledge can crack into them. Once an attack has been successful, the intruder can periodically steal information from the user's unsecure drive, as the intruder now has the master key and cannot be stopped by a changed password.

PASSWORD AND ENCRYPTION MATH

The U.S. government's National Institute of Standards and Technology (NIST) hypothesizes that it would take 149 trillion years to decrypt AES128 with a full-length key[8], given that you can access the encrypted data. If we take the assessment from NIST and run the figures with a key using only an eight-mixed-character password (48 possibilities) instead of the full power of AES128 (2^{128}), the following math reveals itself:

$$149*10^{18}/2^{80}(365*24)$$

which equals approximately one hour – one hour compared to 149 trillion years. Within one hour you can access the data using a brute-force attack.
It should be noted that the way encryption works means that AES256 is not double the security of AES128 but rather the square of the security, simply $(AES128)^2$. Our universe it thought to be around 20 billion years old, which means AES256 leaves ample room for processing power improvement.

SECURITY AND "THE CLOUD"

Software encryption has remained a decent deterrent on the desktop, as it requires greater processing power to break longer passwords. This is all changing, however, with the advent of cloud computing making it possible to create and rent (by the hour) a supercomputer cluster. For example, Sun's Network.com offers integration APIs[9] and access to almost endless processing power. These clusters are a very positive development and a true equalizer that puts processing power in the hands of "the man on the street". Unfortunately, that "man on the street" may very well want to break your software encryption and steal your data – which he can very easily do, thanks to the processing power at his fingertips. Similarly, as criminals adopt the cloud computing concept, password-cracking farms are likely to emerge. When individuals use legitimate cracking software against us, they can also take advantage of commercially available password recovery-software that, according to their manufacturers, accelerate the recovery over 10'000 workstations, with zero scalability overhead.[10]

EASIER PASSWORD ATTACKS ON SOFTWARE ENCRYPTION

As stated before, the password "4Bentxc" takes less than an hour to crack using basic brute-force attack methods, which tend to be an intruder's last resort. An easier, quicker and more common method is a guessing attack or a dictionary attack. Guessing attacks are just what they sound like; if you know one of the user's passwords and had 1'000 attempts to guess, there's a good chance that you get lucky. Dictionary attacks use highly optimized, precompiled lists of common passwords, words, rules and phrases to gain access to the user's data.

THE INFECTED SOFTWARE ENCRYPTION ENGINE

Since software encryption has to trust the host machine, there is a significant risk that the software could be altered by an infected host. There is also the risk that what seems like encryption software will become malware itself instead. This risk is unavoidable since there is no write protection on unsecure USB flash drives. For improved usability, the software encryption autostarts, making the log-in screen hard to miss. The file that handles the autostart, autorun.inf, can also easily be altered or replaced, which is one of the issues that enabled Conficker[11] to infect corporate networks worldwide.

"Since software encryption has to trust the host machine, there is a significant risk that the software could be altered by an infected host. "

SOFTWARE ENCRYPTION AND FLASH STORAGE ARE A TECHNOLOGY MISMATCH

Contrary to popular belief, software encryption cannot be used on all current USB flash drives. Flash, specifically NAND flash, is a technology that has a certain number of read/write cycles in its life span. To improve this life span almost all USB flash drives use what is called "wear leveling"[12] which spreads the tare of the flash cells so that no cell is used more often than any other to store data. A drive without wear leveling will break down quickly. Unfortunately, this has security consequences when using software encryption. Simply put, the software has no way of knowing where the data is actually stored on the unsecure drive with wear leveling, as it is spread around. As stated on the Truecrypt Web page: *"For instance, when you change a volume password/keyfile(s), the volume header is, under normal conditions, overwritten with a reencrypted version of the header. However, when the volume resides on a device that utilizes a wearleveling mechanism, TrueCrypt cannot ensure that the older header is really overwritten… Due to security reasons, we recommend that TrueCrypt volumes are not created/stored on devices (or in file systems) that utilize a wearleveling mechanism (and that TrueCrypt is not used to encrypt any portions of such devices or filesystems)."*[13]

This is a weakness to which all software-encryption solutions likely are susceptible. This is a "damned if you do, damned if you don't" situation, and there is no way to make it work fully and securely. In contrast, hardware encryption can make use of wear leveling without lowering the security, as the chip that performs encryption or works in conjunction with it also performs the wear-leveling operations.

SOFTWARE ENCRYPTION WILL CAUSE DATA CORRUPTION

The BitLocker To Go wizard states that one should "pause encryption before removing the drive or files on the drive could be damaged"[14]. In times of increased stress, this could be very easy for users to forget, and it could cause all data to become irreparably corrupted and beyond practical salvation.

SOFTWARE ENCRYPTION SPREADS SENSITIVE DATA ALL AROUND

Staff members with, USB flash drives are at risk of spreading data around. If an unsecure USB flash drive is fully softwareencrypted, there will be no room available on the actual drive to store the decrypted files. These files must then by copied to the unknown host before being displayed to the

user. Many software-encryption solutions try to repair this data breach by overwriting data that has been left on the unknown machine, but this requires that the encryption software continue running.

SOFTWARE ENCRYPTION PROBLEM

When the user is outside the organization, there is a risk that the software encryption will be erased from the unsecure USB flash drive, either with or without malicious intent. It is practically impossible to enforce a policy that states that all USB flash drives should be encrypted as it in the end of day with software encryption is a user choice. Depending on a user's knowledge level, he or she might not know whether the encryption is activated. These are risks that can be avoided altogether by using a hardware-encrypted USB flash drive.

THE WEAK ECONOMY OF SOFTWARE ENCRYPTION

SOFTWARE ENCRYPTION IS SLOW AND TIME-CONSUMING

The nature of technology necessitates that properly implemented software encryption take a long time to set up. Full-drive encryption, which aims to transform the unsecure USB flash drive into an encrypted volume, requires that each block of data is encrypted at setup. Depending on the storage size of the drive, setup can take anywhere from 20 minutes for 2GB to hours for larger drives, as even BitLocker evangelists report that the process can be extremely timeconsuming[15].

If full-drive encryption with software is instant, you can be sure that no encryption has taken place. In comparison, hardware-encrypted drives take as little as eight seconds to set up; the files are encrypted/decrypted on the fly at the authenticated user's command. Once the hurdle of a painfully slow setup has been jumped, the software encryption will transfer data very slowly. If the drive is inserted into an unknown, poorly performing machine, the results can be mindnumbingly sluggish. Hardware encryption relies on the onboard chip for performance and will perform at a high level over all systems.

THE USER CAUGHT IN THE MIDDLE OF SOFTWARE-ENCRYPTION CONFUSION

Operating encryption software can be both timeconsuming and confusing. The confusion arises because these solutions seldom operate consistently on home and foreign systems. On the home desktop or where appropriate drivers have been installed (which requires administrative privileges), users have the opportunity to simulate the operation of a true hardware-encrypted secure USB flash drive and enable drag-and-drop operations. When operating encryption software on foreign systems, users are often sent back to rely on some form of volume browser or file-by-file encryption, which presents a totally different mode of operation.

With Truecrypt Traveler disks, administrative rights are required on all systems on which the disks will operate.[16] But this still supersedes BitLocker To Go, which offers read-only operation (copy data off) on any system that is not Windows 7 Ultimate or Enterprise. This means that user training is needed in order to limit wasted time from the use of software encryption. Hardware encryption is always true drag-and-drop-based and should not require specific user training programs. As the frustrated user struggles through the setup and operation of the software-encrypted unsecure USB flash drive, he or she must be concerned about the risk of data corruption. If there is one moment of weakness and the user unplugs the drive in the middle of encryption, there is an overwhelming risk that the container or file that is being encrypted at that very moment will break and become corrupted. Hardware-encrypted drives, however, make sure that files stay intact and uncorrupted even in the case of accidental unplugging. Correctly implemented hardware-encrypted USB flash drives simply offer much more robust data transfer operations.

One countermeasure to reduce the risk of data corruption is to back up data continuously. This is not a simple measure to take with software encryption; the full container needs to be backed up every time, as it would be very hard to set up a backup that works on the file level instead of of the container level.

SOFTWARE ENCRYPTION PUNISHES THE FORGETFUL AND STRESSED USER

In a perfect world, no user would ever forget a password. In this imperfect and real world, users forget their passwords at the worst possible moments. The ability to perform a quick and secure remote password reset is essential.

BitLocker To Go offers a password reset scheme that leaves a lot to be desired when it comes to security and productivity. At unlock, the master key is accessible and can be printed or saved as a text file. The end user handles the encryption master keys, a practice seldom seen in larger organizations. The full key is accessible every time the drive unlocks, and it can be used to decrypt the data at any point in the future. This leaves the solution open to social engineering attacks, as an unguarded and unlocked drive can easily be attacked. Because software encryption and its related processes are so timeconsuming, the user puts data at risk by leaving his or her computer during these processes.

If at any point the user forgets the password, the master key is entered and all data must be decrypted onto the present machine, which takes another 20 minutes or multiple hours to complete. Once all stored data has been copied onto a possibly unknown machine, the user needs to go through the BitLocker To Go installation again, if this is possible to do on that computer (only Windows 7 Ultimate and Enterprise presently offer this capability). Encrypting the drive anew will take a minimum of another 20 minutes.

There is limited documentation of administrators holding master certificates on their user accounts to access software-encrypted containers, but we know that this will not affect how long it takes to encrypt/decrypt data with software encryption, and it likely presents its own security issues.

SOFTWARE ENCRYPTION LEAVES OUT THE BENEFITS OF USB FLASH DRIVES

Software Encryption of USB flash drives excludes the possibility of getting a productivity boost at a low cost, with offerings of portable full engines or application virtualization engines like VMware ACE, MokaFive, MojoPac and Ceedo. There is also a range of portable software such as Firefox Web browsers, TeamViewer[17] remote help, trusted e-mail clients and word-processing tools[18]. In a larger organization, encryption solutions most often need to be deployed centrally and managed by the administrator – not the user – something that no software-encryption solution presently offers.

HARDWARE ENCRYPTION IS THE SOLUTION

Hardware encryption is the most cost-efficient way of ensuring the security of USB flash drives and managing them centrally and granularly, providing a multitude of benefits to an organization. BlockMaster offers SafeStick, the secure USB flash drive, and SafeConsole, the central management server with the fullest range of security and productivity benefits on the market, including the following:

- SafeStick instantly secures portable data with always-on automatic hardware AES 256 CBC encryption, far superior to ECB block cipher mode. Uses transparent encryption that won't disturb the user when handling files.
- True brute-force protection, with a password attempt counter built into the hardware.
- The epoxy-sealed, tamperproof single SafeStick controller handles all security features, making it superior and more reliable than multiple chip solutions and software attempts.
- SafeStick is ready to be unlocked in as little as one second after plugging it in. The configuration startup time on first use is optimized, and no other secure USB flash drive is as fast or simple to set up. SafeStick's responsiveness and speed are two of the most important features contributing to a positive user experience. Users who have positive experiences are more likely to accept the enforced and elevated security that SafeStick and SafeConsole provide.
- SafeStick does not require drivers or administrative privileges.

- The SafeStick Authorized Autorun feature ensures that Conficker or Conficker mutants cannot infect the device.
- Conduct remote password resets anytime in seconds over any channel or with trusted local self-service.
- SafeStick alerts the user when faulty unlock attempts are made, ensuring that social engineering hacks will not succeed.
- SafeStick locks down if left behind. At some point users are likely to forget to remove their drives. When that happens, SafeStick takes measures to prevent loss and to ensure integrity and confidentiality by locking down automatically.
- EasyShare lets you share data between SafeStick drives, without sharing your password.
- SafeStick boosts your productivity by enabling secure automatic unlock of SafeStick on trusted machines with ZoneBuilder.
- SafeStick displays a "return to owner" message on lost drives. Recovered SafeStick drives that are inserted into the correct user account are automatically "found," thus lowering administrative costs.
- SafeStick offers next-generation application and content delivery with the Publisher feature in SafeConsole.
- SafeConsole optionally integrates toward and reflects the Active Directory which makes the implementation quick. Administrator groups can be set up in the Active Directory. SafeConsole avoids creating a new identity silo, which saves time and money.

EXPERIENCE **SafeStick®**
Request your free evaluation SafeStick today at www.getsafestick.com.

DOWNLOAD A FREE TRIAL OF **SafeConsole®** SERVER SOFTWARE
for complete visibility and control of your portfolio of secure USB drives.

SOURCES

1) http://cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-506224.html

2) http://www.centennial-software.com/company/press/?id=136

3) http://sourceforge.net/projects/truecrypt/

4) http://www.trustedcomputinggroup.org/

5) http://tech.msn.com/security/articlepcw.aspx?cp-documentid=22327267

6) http://www.lockdown.co.uk/?pg=combi

7) http://www.randpass.com

8) http://www.nist.gov/public_affairs/releases/aesq&a.htm

9) http://www.sun.com/solutions/cloudcomputing/index.jsp

10) http://www.elcomsoft.com/edpr.html

11) http://en.wikipedia.org/wiki/Conficker

12) http://en.wikipedia.org/wiki/Wear_levelling

13) http://www.truecrypt.org/docs/?s=wear-leveling

14) http://www.brighthub.com/computing/smb-security/articles/35534.aspx#ixzz0WNhdYBdh

15) http://www.winsupersite.com/win7/ff_bltg.asp

16) http://www.truecrypt.org/docs/?s=truecrypt-portable

17) http://www.teamviewer.com/download/portable.aspx

18) http://portableapps.com/

www.safeconsole.com

UNITED KINGDOM
+44 (0)2033 554 188
sales@blockmastersecurity.com

UNITED STATES
1 - 888 - 432 - 4957
sales@blockmastersecurity.com

MAIN OFFICE (SWEDEN)
+46 (0)46 - 276 51 00
sales@blockmastersecurity.com

To find your local Reseller please visit
www.blockmastersecurity.com
for more information.