



Why Software Encrypted USB Flash Drives give a False Sense of Security

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



EXECUTIVE SUMMARY

USB flash drives are an essential tool, but they can leave data exposed. While new Windows 7 includes enhanced security features, software encryption is not sufficient. Only hardware encryption is robust enough to properly protect critical data.

USB FLASH DRIVES HAVE BECOME HUGE POPULAR

- They are the most convenient way to transfer large amounts of data.
- They use little power, 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.
- Dictionary attacks can do it even faster.
- Simple password cracking software is easily available on the internet, often free.
- 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 only available in the high end editions, Windows 7 *Ultimate* and Windows 7 *Enterprise*.
- Few people have yet deployed Windows 7.

HARDWARE ENCRYPTION IS THE ONLY SOLUTION

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



BENEFITS AND FUTURE OF USB FLASH DRIVES

USB flash drives are an integral part of our working lives. Alongside the connected Laptop and Blackberry, these devices now play an absolutely crucial role in enabling remote and flexible working patterns. But more, USB Flash devices give us mobile access to all those files too sensitive or too large to be downloaded over the public network.

USB flash drives are ideal for sharing and transferring large quantities of data - on time and on budget - because:

- all modern PC, Macs and laptops have USB ports
- Flash drives are resilient and robust - have no fragile moving parts and are not sensitive to scratches or dust
- they make transporting data from place to place a simply and speedy task
- their small size (and large memory) makes them incredibly convenient
- they use little power and one drive can replace hundreds of CDs or DVDs
- Flash drives invariably have a long lifespan and deliver reusable storage.

But there is a security downside, prompting the rise of the “USB problem”. Historically, the vast majority of USB drives were (and still are) unsecured. And while users value the devices for their ability to transfer data between computers, losing a USB stick is often more an inconvenience than a major security threat to the business.

DISAPPEARING DRIVES

This rather apathetic attitude has contributed to a massive numbers of drives being lost or misplaced. Indeed, last year, over 20 million sticks were lost across the world, while IT giant Cisco¹ estimates that up to 66% of USB drives are lost.

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

It is these figures, and the onerous impact of data loss, that has prompted many IT departments and security professionals to push the “USB problem” up

their priority list. Indeed, as reported in respected IT publication, eWeek, the “USB problem” is now regarded as the largest challenge for IT departments.²

And this is understandable. Losing intellectual property on an open, unsecured USB flash drive could be disastrous for any organization. There are clear reasons to protect trade secrets, aggregated data or other sensitive records, as doing so ensures shareholder value, public confidence, and internal productivity.

THE CASE FOR ENCRYPTION

To counter this threat from unsecure USB flash drives, hardware encrypted flash drives have become available. Not only do such devices offer password protection, but they offer management capabilities that allow organizations to “control and kill” drives that fall off the reservation.

Software offerings are also available – utilizing more traditional software encryption technologies to encrypt standard unsecure USB flash drives.

But organizations beware - relying on software encryption of USB flash drives is a dangerous move. As this paper will highlight, 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 to encrypt and decrypt 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 Truecrypt³, and commercial products such as Microsoft's BitLocker to name but a few.

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. Indeed, by adding hardware with TPM⁴ (Trust Platform Modules), software encryption has been able to take a significant leap forward in the development of hardware encryption chips for the USB flash drive environment.

But this does not mean 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 visiting with the security of your data and the performance.

- The 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. It can always be copied off the unsecure device to perform what is then called "parallel offline attacks" without the user being aware of the intrusion.

“software encryption has been able to take a significant leap forward in the development of hardware encryption chips for the USB flash drive environment. But this does not mean software encryption can make a second successful leap from PC to portable device.”

- The software encryption speed depends on the host computer and files must be unencrypted onto disk even on unknown machines to be edited – 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.

With Hardware Encryption you trust the onboard security chip of the secure USB flash drive to perform all encryption/decryption, key generation and key handling. This results in a significant leap forward in terms if security and usability:

- Hardware encrypted devices are a million times more secure than software encrypted USB flash drives, a fact that we explore further in this paper.
- Hardware drives enable data transfer speeds up to 10 times than those offered by software encrypted devices. Critically, it also assures a perfect match to eliminate the disappearing data problem.
- Hardware drives also offer a more consistent user experience, critical when organizations are seeking mass employee adoption.
- Some hardware encrypted drives can lower IT costs as they fill the need of making data portable and thus act as a laptop replacement.

SOFTWARE ENCRYPTION WILL CRACK

As already highlighted, software encryption will crack on a USB flash drive. In Microsoft's own words (in its MS Windows 7 overview⁵), "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 is utilized to encrypt the stronger master key - which in turn encrypts the data. When the password is cracked, all stored data is laid bare. It is not feasible to limit the number of password attempts. Indeed, as we see below, it is a physical impossibility 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 any password counter performs. This means that the intruder will always have unlimited password attempts and opens the way for unlimited password cracking attacks. For example, an apparently secure password - 4Bentxc - takes less than an hour to crack using a very basic brute-force attack⁶.

The business of password cracking or password recovery has in some cases a legitimate business purpose as it may be used as a means of getting data back that else would be lost in criminal investigation for example. But the allowance of endless password attempts also makes software encryption open to attacks by malicious intruders.

“an apparently secure password - 4Bentxc - takes less than an hour to crack using a very basic brute-force attack.”

What is truly worrying is that password cracking has turned into a point and click procedure with software that is available for free or at a very low cost. There is a myriad of programs available for download, including Cain and Abel, John the Ripper, Hydra, ElcomSoft and LastBit to name just the more popular choices.

HARDWARE ENCRYPTED SECURE APPROACH

Contrast this with the hardware approach. The encryption master key is generated in the hardware on 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=loOOKIE?Av deFEq⁷

A trusted hardware brute-force protection counter limits the number of password attempts to access data. Properly implemented, this counter has complete integrity and cannot be changed because it

is held on the secure USB flash drive, and 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 to perform a parallel offline attack. A parallel offline attack is much harder to perform on fully encrypted computers as the files are harder to access. The USB flash drive with its ease of use means that an intruder assistant needs little technical knowledge. Once the attack has been successful the intruder can periodically steal the users’ unsecure drive since the intruder now has the master key and will not be stopped by the user changing passwords according to policy.

PASSWORD AND ENCRYPTION MATH

The US governments National Institute of Standards and Technology (NIST) has made the hypothesis that it would take 149 trillion years to decrypt AES128 with a full length key⁸ given that you can get access to the encrypted data.

If we take the assessment from NIST and run the figures with a key using only a 8 mixed character password (48 possibilities) instead of the full power of AES128 (2^{128}) the following math reveals itself: $149 \cdot 10^{18} / 2^{80} (365 \cdot 24)$ which equals approximately one hour. So it is one hour compared to 149 trillion years. Within one hour it is assessed that 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 the square of the security, simply $(AES128)^2$. And given that the universe it thought to be 20 billion years AES256 leaves ample room for processing power improvement.

SECURITY AND “THE CLOUD”

Software encryption has remained a decent deterrent



on the desktop because of the processing power required to break the long, random passwords that are possible on these devices. This is all changing however, with the advent of cloud computing. It is now entirely possible to create and rent (by the hour) a super computer cluster. One example of such a service is Sun's Network.com – offering integration APIs⁹ and access to almost endless processing power. These clusters are a very positive development and a true equalizer that puts true processing power in the hands of “the man on the street”.

Unfortunately, that “man on the street” could very well want to break into your computer and steal your data – now entirely possible thanks to the processing power at his fingertips. Similarly, as criminals adopt the cloud computing concept, password cracking farms are likely to emerge. And, continuing to use legitimate software against us, such individuals can also take advantage of commercially-available password recovery software that, according to the manufacturer, accelerate the recovery over 10,000 workstations with zero scalability overhead.¹⁰

“Software Encryption cannot, as the popular assumption is, be used on all current USB flash drives.”

EASIER PASSWORD ATTACKS ON SOFTWARE ENCRYPTION

As stated before the password “4Bentxc” takes less than an hour to crack using basic attack methods. But an easier and quicker method is often of a guessing or dictionary attack. Brute-force attacks are often the intruder's last resort. More common methods are guessing attacks and dictionary attacks. Guessing attacks are simply what they sound like. If you know one of the users passwords and you had a 1000 attempt to guess you might be lucky, maybe even highly likely to be lucky. Dictionary attacks use highly optimized pre-compiled 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 it could be altered by an infected host – and in effect become a piece of malware. There is also the risk that, what to the user seems to be the encryption software becomes a 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 login 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 Conficker¹¹ to infect corporate networks worldwide.

SOFTWARE ENCRYPTION AND FLASH STORAGE IS A TECHNOLOGY MISMATCH

Software Encryption cannot, as the popular assumption is, be used on all current USB flash drives. Flash or specifically NAND flash is a technology that has certain number of read/write cycles lifespan. To improve this lifespan almost all USB flash drives uses what is called wear leveling¹². The wear leveling spreads the tare of the flash cells so that no cell is used more 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 actually is 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 re-encrypted version of the header. However, when the volume resides on a device that utilizes a wear-leveling 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 wear-leveling mechanism (and that TrueCrypt is not used to encrypt any portions of such devices or filesystems).”¹³



This is a weakness that all Software Encryption solutions likely are susceptible to. And this is damned if you do, damned if you don't. There is no option of making it work fully and securely. Hardware encryption can make use of wear leveling without lowering the security as all operations are performed by the chip that performs the wear leveling or works in conjunction with it.

SOFTWARE ENCRYPTION WILL CAUSE DATA CORRUPTION

Besides the risk of data corruption from the lack of wear leveling it is stated in the BitLocker To Go wizard that one should "pause encryption before removing the drive or files on the drive could be damaged"¹⁴. This of course something that in the heat of the moment the user one day will forget. And this can cause all data to become irreparably corrupted and beyond practical salvation.

SOFTWARE ENCRYPTION SPREADS SENSITIVE DATA ALL AROUND

There is a major risk that staff with USB flash drives that are software encrypted will spread data around.

If an unsecure USB flash drive is fully software encrypted there will be no storage available on the actual drive to store the decrypted files. These must then be copied to the unknown host before being displayed to the user. Many Software Encryption solutions try to repair this data breach by over-writing data that has been left on the unknown machine, but this requires the encryption software to be still running.

"Once the hurdle of a painfully slow setup has been jumped the software encryption will perform at low speeds when it comes to data transfers."

SOFTWARE ENCRYPTION ON OR OFF PROBLEM

When the user is outside the organization there is a risk data the software encryption is erased from the unsecure USB flash drive 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. Dependent on the user knowledge a staff might believe that the encryption is activate when it in fact was deleted long ago. These are risks that are not present with hardware encrypted USB flash drives.

THE WEAK ECONOMY OF SOFTWARE ENCRYPTION

SOFTWARE ENCRYPTION IS SLOW AND TIME CONSUMING

Due to the nature of technology a properly implemented Software Encryption will take time to setup. If it is full drive encryption which aims at transforming the unsecure USB flash drive into an encrypted volume each block of data needs to be encrypted at setup. Dependent on the storage size this is procedure that can take anywhere from 20 minutes for 2GB to hours for larger drives, as even BitLocker evangelist report *the process can be extremely time consuming*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 low as 8 seconds to setup; the files are encrypted/decrypted on-the-fly at the authenticated users command.

Once the hurdle of a painfully slow setup has been jumped the software encryption will perform at low speeds when it comes to data transfers. If the drive is inserted into an unknown machine with a weak performance the results can be mind numbing 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 time consuming and confusing. The confusion arises since these solutions seldom operate consistently on home and foreign systems. At the home desktop or where appropriate drivers have been installed (requires administrative privileges) there is the opportunity to simulate the operation of a true hardware encrypted secure USB flash drive and enable drag-and-drop operations and make it look real. On the foreign systems the user is often sent back to rely on some form of volume browser or file-by-file encryption which presents a totally different mode of operation.

“Correctly implemented hardware encrypted USB flash drives simply offer much more robust data transfer operations.”

With Truecrypt Traveler disks administrative right are required on all system it is to operate on¹⁶. But this still supersedes BitLocker To Go that only offers read-only operation (copy data off) on any system that is not Windows 7 Ultimate or Enterprise. This means that user training will be needed to limit time waste 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 a major threats looms with the risk of data corruption. If there is one moment of weakness and the user plugs out the drive in the middle of encryption there is an overwhelming risk that the container or file that is currently being encrypted will break and become corrupted. Hardware encrypted drives makes sure that files stay intact. In the case of an unfortunate plug out this scarcely causes data corruption. Correctly implemented hardware encrypted USB flash drives simply offer much more robust data transfer operations.

The possible counter measure to limit the havoc of data corruption would be to backup data

continuously. This is not a simple measure to take with software encryption as the full container would need to be backed up each time as it in theory would be very hard to setup a backup that works on file level instead of container level.

SOFTWARE ENCRYPTION PUNISHES THE FORGETFUL AND STRESSED USER

In a perfect world no user would ever forget a password. The world apparently lacking perfection users forget their passwords in the least appropriate situations. The ability to perform a quick and secure remote password reset is essential.

As an example of Software Encryption practices BitLocker To Go offers a password reset scheme that leaves much to improve security and productivity wise. At unlock the master key is accessible to be printed or saved as a text file. The end user thereby handles the encryption master keys, something seldom seen in larger organizations. The full key is accessible each time the drive unlocks and can be used to decrypt the data at any point in time from there on. This leaves the solution open to social engineering attacks, an unguarded unlocked drive can easily be attacked – as the processes surrounding software encryption are time consuming there is a risk of the user leaving the machine to work on its own.

If the user at any point forgets the password the master key is entered and all data must be decrypted onto the present machine which again takes 20 minutes up to hours of time. All stored data has now been copied onto a possibly unknown machine. Then the user needs to go through the BitLocker To Go installation again, if this is possible at the present machine (only Windows 7 Ultimate and Enterprise presently offers this capability). Encrypting the drive a new will take yet another 20 minutes at a minimum.

There is limited documentation of using a DRA scheme with administrators holding master certificates on their user accounts to access software encrypted containers but this will not affect the time it takes to encrypt/decrypt data with software encryption and likely holds its own security issues.



SOFTWARE ENCRYPTION LEAVES OUT THE BENEFITS OF USB FLASH DRIVES

Software Encryption of USB flash drives locks out even the possibilities of getting a productivity boost at a low cost with offerings of portable full or application virtualization engines like VMware ACE, MokaFive, MojoPac or Ceedo. There is also a range of portable software such as Firefox web browsers, Teamviewer¹⁷ remote help, trusted email clients or word processing tools¹⁸. In a larger organization these solution most often needs to be deployed centrally and managed by the administrator and not the user, something that no software encryption solution presently offers.



HARDWARE ENCRYPTION IS THE SOLUTION

There is a more cost efficient way of handling USB flash drive security. It is the way hardware encrypted secure USB flash drives can be centrally and granularly managed. This means that a multitude of benefits become available through out the 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.

- Instantly secure 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.

“hardware encrypted secure USB flash drives can be centrally and granularly managed. This means that a multitude of benefits become available through out the organization.”

- True brute-force protection with password attempt counter built into the hardware.
- The epoxy sealed tamper proof single SafeStick microprocessor chip handles all security features making it superior and more reliant than multiple chip solutions and software attempts.
- You are ready to unlock SafeStick 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 setup. The responsiveness and speed of SafeStick is one

of the most important features for a positive user experience. A positive experience will achieve user acceptance of the enforced and elevated security that SafeStick and SafeConsole provides.

- Does not require drivers or administrative privileges.
- SafeStick Authorized Autorun feature ensures that Conficker or Conficker mutants cannot infect the device.
- Remote Password Resets anytime in seconds over any Channel or with Trusted Local Self-Service
- Social Engineering Protection, faulty unlock attempts are alerted to the user to make sure that social engineered hacks will not succeed.
- Locks down if left behind. At some point users are likely to forget their drives. When that happens, the SafeStick takes measures to prevent loss and to assure integrity and confidentiality by locking secure information down automatically.
- The SafeStick feature EasyShare lets you share data and not your password.
- Boost productivity by enabling secure automatic unlock of SafeStick on trusted machines with ZoneBuilder.
- A “return to owner” display message on lost SafeStick drives; recovered SafeStick drives that are inserted into the correct user account are automatically “found,” thus lowering administrative costs.
- Next Generation Application and Content Delivery with the Publisher feature in SafeConsole.
- SafeConsole integrates towards and reflects the Active Directory which makes the implementation quick. Administrator groups can be setup in the Active Directory. SafeConsole avoids creating a new identity silo. Time and money is saved.

EXPERIENCE SafeStick©

Request your free trial SafeStick today at www.getsafestick.com

DOWNLOAD SafeConsole© SERVER SOFTWARE

for complete visibility & control of your SafeStick portfolio





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_leveling
- 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/>

UNITED KINGDOM

+44 (0)20 33 55 41 88

sales@blockmastersecurity.com

UNITED STATES

+1 - 888 - 432 - 4957

sales@blockmastersecurity.com

MAIN OFFICE (SWEDEN)

+46 (0)46 - 276 51 00

sales@blockmaster.se

