

Assessing the Security of Hardware-Based vs. Software-Based Encryption on USB Flash Drives

White Paper
June 2008

80-11-01583 Revision 1.0

Table of Contents

Scope	3
Evaluating Access Control and Encryption	3
Fending Off Common Attacks	3
<i>Brute Force Attack</i>	3
<i>Parallel Attack</i>	4
<i>Cold Boot Attack</i>	4
<i>Malicious Code</i>	4
Choosing the Right Security	5
<i>Activation</i>	5
<i>Dependence on Security of Operating System</i>	5
<i>Designed for Usability</i>	5
Comparing Performance	5
Summing Up the Differences	6
SanDisk® Cruzer® Enterprise USB Flash Drives	7

Scope

USB flash drives are favorites of “road warriors,” “day extenders,” and employees who occasionally work at home, at a customer’s site or even in a cafe. These compact devices enable users to store and transfer data with confidence and ease.

But these user benefits have intensified the concerns of IT departments charged with securing confidential corporate data against theft and/or loss. In their search for adequate security, they are faced with many options, most of which encrypt the data stored on employee USB flash drives. The choice of IT professionals is further complicated by two factors: the many different levels of data encryption being offered; the existence of both hardware-based and software-based security solutions.

How do various types of hardware encryption measure up against software encryption in terms of critical factors such as:

- Password access control and encryption
- Protection against common attacks
- USB flash drive and related security implementation
- Performance
- Usability

This paper discusses these issues, and concludes with a close-up of the security mechanisms used in the SanDisk® Cruzer® line of enterprise-grade USB flash drives.

Evaluating Access Control and Encryption

Two major elements are essential in securing data on USB flash drives:

- Access control, whereby access is granted to decrypt data only to users who have been authenticated as authorized users.
- Encryption, performed either by software or hardware means, whereby data is altered in order to make it inaccessible without the proper key to decrypt the data.

Access control is measured by the strength of authentication. At a minimum, a complex password, typically consisting of an 8-character combination of letters and digits, is used to prevent attempts to guess the password.

Encryption is measured by the strength of the algorithm that is used to encrypt the data, and by the ability of the software or hardware-based system to generate a truly random encryption key. The AES encryption algorithm is typically implemented in both software- and hardware-based security solutions. The fact that many governments approve the AES algorithm is testimony to its validity. The strength of the AES algorithm depends on its bit length. Currently, a 256-bit AES algorithm is the highest level that is commercially available both for software-based and hardware-based encryption. In USB flash drive solutions, encryption keys are generally either 128-bit or 256-bit in length. In software implementations, these keys are generated by the host computer or input from an external system. In hardware implementations, they can also be generated by a true random number generator that is part of a dedicated, cryptographic processor. The major advantage of hardware-based encryption keys is that they never leave the USB flash drive, unlike software-based keys which can be temporarily stored in the host’s random access memory (RAM) or on its hard disk drive.

Fending Off Common Attacks

It is widely acknowledged that hardware-based encryption implementations can help prevent a range of common attacks more effectively than software-based encryption. But not all hardware-based encryption implementations are equal in strength.

Brute Force Attack

Brute force attacks guess the password or the encryption key. An attacker who illegally gets a hold of a USB flash drive can plug it into a computer and use a program designed to guess hundreds of passwords or the encryption key every second, based on algorithms specifically designed for this purpose.

These attacks are thwarted both by enforcing the use of complex passwords and by counting and thereby limiting the number of login or decryption attempts. Software implementations cannot thwart these attacks efficiently since they must use the host's memory to store intermediate results, including the number of login/decryption attempts counter. This implies that a modestly knowledgeable hacker can locate and then reset the counter without too much effort until the password is discovered.

In hardware-based security solutions, access control, encryption and decryption are implemented by a dedicated crypto module located inside the USB flash drive. When hackers run a brute force program on the host computer, the crypto module counts the number of attempts and locks down the USB flash drive, rendering information stored on it inaccessible after a predefined limit is reached. Some systems also destroy the data and the encryption keys on the USB flash drive as an extra precautionary measure.

Unlike with software-based solutions, hackers cannot run analysis utilities to locate and reset the counter since the USB flash drive does not allow any external program to run on it and access its memory.

Parallel Attack

A parallel attack is a brute force attack variant in which the attacker copies the encrypted data from the stolen USB flash drive, shares the data with as many computers as possible that are under his/her control, and then puts them to work in parallel to guess the password offline and unlock the encrypted data. By nature and design, software implementations cannot prevent the attacker from easily copying the encrypted file from the USB flash drive and initiating a parallel offline attack.

In contrast, hardware-based implementations prevent the mapping of storage from the USB flash drive to the OS file system until the user enters a correct password. As a result, the attacker cannot copy the USB flash drive contents without first knowing the password.

Cold Boot Attack

Very recent research by a team at the highly respected Princeton¹ University points to how a little known characteristic of DRAM memory can serve as a window of opportunity for a cold boot attack.

DRAM memory is used to store data while the system is running. After power is removed, all content is deleted in a gradual process that can take anywhere between a few seconds and up to a few minutes. If the chip is cooled by artificial means, the content can be retained for as long as 10 minutes.

This characteristic of DRAM memory enables a hacker to read the memory content by cutting power and then performing a cold boot with a malicious operating system. This is deadly for disk encryption products that rely on software means to store encryption keys. An attacker can cut power to the computer, then power it back up and boot a malicious operating system that copies the memory content. The attacker can then search through the captured memory content, find the master decryption keys and use them to start decrypting hard disk contents. To retain the content for a longer interval, the hacker can simply chill the DRAM chip before cutting power.

A hardware-based encryption system is not vulnerable to a cold boot attack since it does not use the host RAM to store the keys.

Malicious Code

Malicious code can run on a PC into which a USB flash drive is inserted. This could alter the software-based encryption, including the software itself or the drivers, to disable the encryption. Malicious code can also copy data from the USB flash drive after it has been authenticated, or it can copy the user password and use it after the user logs out of the drive.

Hardware-based encryption is not affected by malicious code because it uses a security mechanism that is independent of the PC and its operating system.

¹ Center for Information Technology Policy, Princeton University, "Lest We Remember: Cold Boot Attacks on Encryption Keys", J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten, Feb 21, 2008

Choosing the Right Security

Activation

Software-based encryption can be implemented on all types of media used by the organization. Hardware-based encryption is tied to a specific device; however, this means that it is “always on” as part of the device specifications. This of course makes security a given, requiring no user intervention. In contrast, software-based encryption can be disabled by the user/attacker, or the user can unintentionally forget to enable it, causing data to be stored with no protection.

Dependence on Security of Operating System

An application’s security depends on the security level of the operating system. A flaw in the operating system is likely to lead to the subsequent vulnerability of the application running on top of it.

For instance, a security problem involving the operating system can cause security problems with the cryptographic module implementation. Examples of this phenomenon include operating systems that leak memory contents through swap files, and flaws in the memory management and protection schemes of operating systems.

Software-based encryption, by nature, depends on high-level operating system services. Hardware-based encryption does not, and is therefore not dependent on the secure implementation of these services to ensure its own level of security.

Designed for Usability

The level and type of security provided by software-based encryption typically requires driver installation onto the PC operating system to enable the USB flash drive to function properly. When the USB flash drive is used on a foreign PC, it also requires driver installation with the associated risks of incompatible drivers and malicious code transfer.

Some hardware-based encryption solutions also require installation of a driver on the host PC, making the driver susceptible to attacks and making the drive more cumbersome to install.

More robust hardware-based encryption does not require driver installation, nor any other type of software installation on the host PC. This keeps the encryption independent of the PC while not leaving behind software footprints.

Application Code Integrity

Application code is stored in memory and is executed on demand or according to prior instructions. If this code is stored in a common memory space which is not necessarily protected as required (as explained in the section on “Brute Force Attack”), an adversary can modify it, causing the USB flash drive to either malfunction or leak critical information.

Software-based encryption is much less effective at maintaining application code integrity than hardware-based encryption, which uses a fully contained memory space. In some hardware-based encryption systems, the code is digitally signed against the hardware, verifying software integrity each time the USB flash drive is inserted in the PC to provide an extremely high level of code integrity.

Comparing Performance

It is generally recognized that hardware-based encryption solutions are superior in terms of throughput capacity and speed as compared with software encryption, with the added benefit of not degrading the performance of other programs or processes that are running. This is because dedicated hardware inside the USB flash drive is used for the encryption/decryption process, rather than latching onto existing processing capacity as in the case of software-based encryption.

Of course, not all types of hardware-based encryption deliver equivalent throughput and speed on USB flash drives. The experience of a given company with flash memory management and the type of flash technology used are key factors in evaluating the USB flash drive and its encryption.

Summing Up the Differences

Table 1 summarizes the various types of attacks that can be used to retrieve data, encrypted keys and passwords, and the differences between hardware-based and software-based encryption in preventing these attacks. It also summarizes a few major issues that should be taken into account before making a decision on the type of encryption to implement.

Table 1: Hardware-Based vs. Software-Based Encryption Comparison

	Hardware-Based	Software-Based
Brute force attacks (including parallel attacks)	Prevented by access control and device lockdown Prevented by blocking copying of data in its encrypted form from the device to the host memory.	Difficult to prevent
Cold boot attack	Prevented by not using RAM or other common memory space to store encryption keys, and by the fact that the keys never leave the USB flash drive	Can be prevented if secure memory is available on the PC
Malicious code	Prevented by using a security system independent of the PC and its OS	No way to prevent if the PC and its OS are infected
Activation	Tied to a single device, security activation is automatic as part of the device specs	Can be implemented on all types of media, security activation is dependent on the user
Dependence on OS security	Independent	Dependent
Designed for usability	No drivers required	Driver installation on the host PC required, potentially a security risk
Application code integrity	Strong, uses fully contained memory space on the USB flash drive	Weak, uses common memory
Performance	Fast, since dedicated hardware is used for encryption processes	Slower, since existing processing capacity is used

SanDisk® Cruzer® Enterprise USB Flash Drives

SanDisk, a leading global brand for USB flash drives, offers an extensive portfolio of security solutions to the enterprise market. SanDisk Cruzer Enterprise USB flash drive (Figure 1) and central management and control (CMC) software keep confidential data secure both inside and outside the office by the application of both 256-bit AES hardware encryption and strong password protection. This combination of security means that SanDisk Cruzer Enterprise:

- Offers superior security by using a separate, cryptographic processor core that secures encrypted data in a secured memory space on the USB flash drive to protect against brute force, counter, parallel offline, cold boot and malicious code attacks
- Implements mandatory access control that automatically encrypts all data written to the drive
- Functions independently of the level of security offered by the operating system
- Requires no drivers for installation
- Delivers an exceedingly high level of application code integrity by digitally signing and verifying the signature against the hardware every time the USB flash drive is inserted into a PC
- Achieves very fast transfer speeds of up to 24MB/s Read, 20MB/s Write
- Optionally offers a central management and control (CMC) system to administer password recovery and renewal, enable remote termination of lost Cruzer Enterprise USB flash drives, centrally back up and restore data, and track USB flash drive usage for auditing purposes.

SanDisk is vertically integrated, from flash manufacture to final, secure products, and is a strong leader in technological innovation. This technology is deployed globally in millions of enterprise-grade USB flash drives in corporate, financial and healthcare environments.



Figure 1: SanDisk Cruzer Enterprise, a secure USB flash drive with up to 8GB² memory

² 1 megabyte (MB) = 1 million bytes. 1gigabyte (GB) = 1 billion bytes. Some capacity not available for data storage.

For more information please visit www.sandisk.com/enterprise or e-mail enterprise@sandisk.com.

SanDisk®

SanDisk Corporate Headquarters
601 McCarthy Boulevard
Milpitas, California 95035-7932
Corporate Phone: (408) 801-1000
Corporate Fax: (408) 801-8657
www.sandisk.com

SanDisk, the SanDisk logo and Cruzer are trademarks of SanDisk Corporation, registered in the United States and other countries. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s).

© 2008 SanDisk Corporation. 80-11-01583 Revision 1.0, June 2008