SSD Evidence Acquisition and Crypto Containers

As demonstrated in recent researches (e.g. [7] How SSD Drives Self-Destroy Court Evidence and What We Can Do About It published by Belkasoft), SSD drives have the capacity to destroy evidence on their own, even if they are disconnected from the original computer and connected through a write blocker. However, to much surprise, evidence self-destruction may not apply to information stored in crypto containers – even if they are stored on SSD drives. In this article we'll analyze three popular crypto containers: BitLocker, TrueCrypt and PGP Disk, in order to see how they handle information stored on SSD volumes.

www.elcomsoft.com

Table of Contents

Background

Every year, more and more computers examined by forensic specialists carry a solid-state drive (SSD) instead of (or in addition to) traditional magnetic storage media. SSDs show clear advantages in terms of absolute performance and, in the absence of any moving mechanical parts, greatly increased shock resistance and overall reliability compared to spinning-disk media.

Whole-disk encryption and encrypted volumes stored on SSD drives are always a compromise in terms of data security and disk performance and reliability. This article makes two strong points in regards to encrypted volumes stored on SSD media.

> **Due to the various compromises and tradeoffs in the implementation of encrypted volumes stored on SSD drives, attacking such volumes may be faster and easier than breaking into the content of similar containers stored on magnetic media.**
>
> **Somewhat counter-intuitively, attacking encrypted volumes located on an SSD drive may even result in recovering more evidence than would be available by acquiring an unencrypted SSD drive.**

Solid-state disks store information in a very different manner compared to traditional media, imposing certain restrictions on how a crypto container may use the available space on an SSD drive. SSD-specific storage methods, when implemented by the manufacturers of crypto containers, can dramatically increase the performance of the encrypted volume, but may lead to certain security tradeoffs.

Acquiring Computers with SSDs and Encrypted Containers

The acquisition of PCs equipped with SSD drives, especially if the use of a crypto container is suspected, requires a different approach compared to acquiring a PC equipped with magnetic storage media.

Traditionally, suspect’s computers were acquired by shutting down the PC (by cutting off power) as soon as possible in order to prevent possible evidence destruction in progress. While this made sense for magnetic storage media where irreversible data destruction takes significant time, recent researches [3][7][9] demonstrate that “solid-state drives (SSDs) have the capacity to destroy evidence catastrophically under their own volition, in the absence of specific instructions to do so from a computer.” [3] Moreover, with the introduction of the Secure Erase command and self-encrypting SSDs, **the entire content of the SSD drive can be destroyed instantly**. The question of how many SSD users will know how to use the command, or will actually use it, remains open.

Indeed, the operation of garbage collector and the effect of the TRIM command will cause the disk to wipe evidence clear even if the disk is detached from the PC it was originally connected to, even if the disk is re-connected via a write blocker. In addition, certain models such as Intel's 320 and 520 series drives as well as SSD drives using SandForce controllers (such as the Vertex 2), encrypt the complete contents of the drive. According to [9], "At the moment, the encryption feature is only useful for a **quick secure erase** of the drive." Indeed, according to Intel, "Executing a SECURE ERASE function, such as that found in the Intel® SSD Toolbox, will cause the Intel SSD 320 Series drives to generate a new internal encryption key." [8] This will instantly render unusable all encrypted information stored on devices featuring hardware-level full-disk encryption. [10]

Prior Art

Very little information is available about the issue of using encrypted volumes on solid-state drives. Any official information available from most manufacturers of SSD drives and crypto containers is scarce and incomplete. When researching the issue, the information had to be collected from a variety of sources including bits semi-official information such as the postings of Symantec employees on their corporate forum (re: PGP Disk). At this time, official representatives are using rhetoric such as "…can neither confirm nor deny", "it's not something I've received a complaint about", "I'll ask the product manager". It seems there's very little certainty about this issue among the very players who should have known more about it than anybody else.

Encrypted Volumes on SSD Drives: Tradeoffs

By creating an encrypted volume on an SSD drive, the user will inevitably has to choose a tradeoff between effective life of the disk, performance, and security. Various settings, parameters and the very type of encrypted volume being created will affect the ability of the SSD controller to perform wear leveling and garbage collection.

Access Speed

Today's high-performance solid-state drives can deliver read and write speeds beyond imaginable just a few years ago. Current CPUs, even when equipped with AES-NI instruction set to accelerate the performance of the AES encryption algorithm, can't keep up with the speed of SSD drives. As mentioned by a PGP user [1], "…even with the AES acceleration, PGP's 10.1 engine is nowhere near unencrypted speeds". This led manufacturers to introduce the ability to opt for less secure encryption by using a shorter encryption key version of the AES algorithm (e.g. AES-128 instead of AES-256 in PGP Disk implementation). The shorter encryption key provides for increased performance at the obvious expense of reduced security.

Whole Disk Encryption Affects SSD Wear Leveling

Multiple sources reference that whole disk encryption (WDE) drastically reduced the ability of an SSD controller to perform wear leveling [2]. Good news is that most SSDs have some 10 to 50 per cent more physical storage capacity compared to their advertised nominal capacity. This hidden extra storage capacity is used to perform wear leveling on full or nearly full disks.

Depending on exact model of an SSD drive, more or less hidden capacity may be available. The additional blocks are not software-addressable, and can be only used by the SSD controller for the purpose of garbage collection and wear leveling. This hidden capacity alone, however, may not be enough to ensure reasonable longevity and write-performance of the SSD drive.

This was exactly the reason why some WDE manufacturers introduced the ability to leave unused parts of the encrypted volume well alone. If the disk is encrypted using such an option, the crypto container will not encrypt unoccupied sectors. This allows SSD wear leveling and garbage collection to work, but presents a major security concern by exposing exactly how much data the encrypted volume contains.

SSD Wear Leveling Affects Security in Crypto Containers

Whole-disk encryption affects the operation of SSD wear leveling. However, wear leveling has adverse effects on security of any encrypted volumes stored on any media utilizing wear leveling algorithms. Due to the way wear leveling operates (data replication), chunks of unencrypted information may remain in the flash chips during initial encryption. According to [5], “If […] you intend to use in-place encryption on a drive that utilizes wear-leveling mechanisms, make sure the partition/drive does not contain any sensitive data before you fully encrypt it (TrueCrypt cannot reliably perform secure in-place encryption of existing data on such a drive; however, after the partition/drive has been fully encrypted, any new data that will be saved to it will be reliably encrypted on the fly).”

In addition, TrueCrypt developers advise against using encrypted containers on part of a device or file system that utilizes a wear-leveling mechanism if plausible deniability is required.

The Issue of Data Replication

Data replication is used by SSD controllers to evenly distribute wear among the entire content of the SSD drive. The wear leveling operation provides increased attack surface via replicated sectors holding chunks of information discarded by the crypto container. This fact also negatively impacts the security of encrypted containers stored on SSD drives. In particular, encrypted volume headers that are typically overwritten when the user changes the password may have multiple replicas in accessible and non-accessible areas of the flash memory. Non-accessible areas, in turn, can be read with inexpensive FPGA or controller-based hardware [3], providing an attacker the ability to try one of the previously used passwords to derive decryption keys.

Disk Encryption and TRIM

Solid-state drives use TRIM operation to improve writing performance by pre-emptively erasing blocks that are no longer used to hold data. TRIM releases unused sectors to built-in garbage collector when a file is deleted or if disk space becomes available in a different way (e.g. the disk is formatted).

Different crypto containers will treat TRIM and SSD garbage collection operations differently. In certain configurations they won't trigger the TRIM operations; in other setups they will. Both approaches are tradeoffs between SSD write performance and effective security of the data stored in an encrypted container. It is essential for a forensic specialist to be aware of the different configurations in order to perform the most effective recovery of information stored in the encrypted container.

If TRIM is not allowed on an encrypted volume, all disk space occupied by an encrypted volume is considered in-use. This in turn will greatly slow down further writes, causing the much longer long read-erase-modify-write cycle to write blocks of data instead of the much simpler (and faster) single write operation. As TRIM is a major let-down in forensic data recovery of any deleted information, by acquiring the PC with an SSD drive holding an encrypted volume opens the way to access all information stored in the container including deleted files (provided that a decryption key is known or obtained with a tool such as Elcomsoft Forensic Disk Decryptor).

If, however, TRIM is allowed to operate on an encrypted container, affected empty sectors will contain unencrypted zeroes even if they are located within a part of the encrypted volume. This in turn allows an attacker to see exactly which blocks on the disk are used to hold encrypted information, and which are not. In particular, this reveals how much data is actually stored on the encrypted disk. Either way, it does compromise security.

PGP Disk

According to a post of a Symantec employee on Symantec's official customer support forum, PGP Disk recognizes specific issues pertinent to SSD drives. Several measures are taken to accommodate the increased speed as well as the many reliability and performance issues of solid-state drives. The following information comes from Bryan Gillson, Symantec Sr. Director, Product Management, Encryption [1]:

1. AES-128 support was introduced to speed up encryption/decryption operations in order to keep up with the much increased throughput of SSD drives. Weaker 128-bit encryption is less secure compared to traditionally used AES-256.
2. "WDE [Whole Disk Encryption] encrypts an entire disk, even unused sectors. This improves security, since an attacker can't tell an empty drive from a full drive. However, this writes to every sector of an SSD and makes every future write a re-write - which are significantly slower on SSDs." [1]
3. [continued] "To combat this, we introduced a command line option: --fast. If you encrypt using this option, it doesn't encrypt blank sectors. Due to security considerations, this is an advanced option only available on the command line.

   If two drives are encrypted with --fast, it's easy to tell which has more data (and therefore which to attack). A fundamental premise of encryption is to obscure the value of the content, so a blank document and a document full of text should be indistinguishable (see Wikipedia's entry on block cipher modes of operation for an

> interesting example of what happens when this goes awry). Using --fast leaks information that could be useful to an attacker, so (as security people), we don't like it." [1]

TrueCrypt

Here's an excerpt from TrueCrypt documentation [4][6]:

> *"TrueCrypt does not block the trim operation on partitions that are within the key scope of system encryption (unless a hidden operating system is running) and under Linux on all volumes that use the Linux native kernel cryptographic services. In those cases, the adversary will be able to tell which sectors contain free space (and may be able to use this information for further analysis and attacks) and plausible deniability may be negatively affected. If you want to avoid those issues, do not use system encryption on drives that use the trim operation and, under Linux, either configure TrueCrypt not to use the Linux native kernel cryptographic services or make sure TrueCrypt volumes are not located on drives that use the trim operation."*

According to this information, the TRIM operation will only be engaged if the entire system partition is encrypted. On dedicated fixed-size volumes (the most popular type of encrypted volumes used by home users), TRIM will not be engaged. As such, forensic specialists may be able to extract all evidence, including deleted files from such volumes.

BitLocker

According to Microsoft, "When Bitlocker is first configured on a partition, the entire partition is read, encrypted and written back out. As this is done, the NTFS file system will issue Trim commands to help the SSD optimize its behavior." [11]

The TRIM operation will be enabled on BitLocker-protected NTFS SSD volumes. This will expose the empty areas of protected volumes. The single paragraph published in [11] was the only bit of official information coming from Microsoft with regards to the specifics of SSD drives encrypted with BitLocker.

Sophos SafeGuard

In [2], Sophos admits that no detailed information about the operation of garbage collection and the TRIM command is available to the company. Security wise, SafeGuard offers users the option to perform regular initial encryption, touching and writing most pages of an SSD except the hidden capacity (hence the issue of having remnants of unencrypted data stored in the extra capacity of the SSD drive that can be read back with an inexpensive FPGA-based device [3]). Initializing the disk with fast initial encryption only encrypts sectors that will actually be written, leaving the rest of the disk unencrypted and susceptible to the operation of garbage collection and the TRIM command.

However, the company does not mention SafeGuard releasing any sectors emptied within the encrypted domain back to the SSD drive. This means that any files deleted within an encrypted volume will be available for forensic recovery providing the volume decryption key or the original plain-text password is known.

Conclusion

Different manufacturers pursue different strategies in working with SSD drives. Regardless of how they implement their encryption, the overall security of encrypted containers stored on SSD drives will inevitably suffer, one way or another, compared to the same crypto container used on a traditional magnetic hard drive. This works in favor of forensic specialists, who may either gain the ability to recover more evidence than would otherwise be available from an unencrypted SSD drive or make use of the lower encryption and protection standards pertinent to specific operation of SSD drives as a storage system with added redundancy via hidden storage capacity, data replication, wear leveling and garbage collection mechanisms.

References

[1] PGP and SSD Wear Leveling
http://www.symantec.com/connect/forums/pgp-and-ssd-wear-leveling

[2] How to protect data on a solid-state drive (SSD) with SafeGuard Device Encryption
http://www.sophos.com/en-us/support/knowledgebase/113334.aspx

[3] Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery? Graeme B. Bell, Richard Boddington
http://www.jdfsl.org/subscriptions/JDFSL-V5N3-Bell.pdf

[4] TrueCrypt Documentation
http://www.truecrypt.org/docs/

[5] TrueCrypt and Wear Leveling
http://www.truecrypt.org/docs/wear-leveling

[6] TrueCrypt TRIM Operation
http://www.truecrypt.org/docs/trim-operation

[7] How SSD Drives Self-Destroy Court Evidence and What We Can Do About It
http://forensic.belkasoft.com/en/why-ssd-destroy-court-evidence

[8] Intel 320-series SSD and FDE(Full Disk Encryption) questions
http://communities.intel.com/thread/20537?start=0&tstart=0

[9] Performance and SSD Wear
http://superuser.com/questions/358122/using-truecrypt-software-encryption-with-an-ssd

[10] SSD's and the Importance of Encryption
http://www.infosecisland.com/blogview/13722-SSDs-and-the-Importance-of-Encryption.html

[11] Full Drive Encryption with Samsung Solid State Drives
http://www.samsung.com/global/business/semiconductor/file/product/ssd/SamsungSSD_Encryption_Benchmarks_201011.pdf

[12] Support and Q&A for Solid-State Drives
http://blogs.msdn.com/b/e7/archive/2009/05/05/support-and-q-a-for-solid-state-drives-and.aspx