A **Tabernus** Whitepaper

Advances in SSD Erasure Solutions: A Risk Based Approach

By Joe Mount, Daniel Dyer, David Dykes, Tabernus

Whitepaper provided courtesy of:

WE DO ITAD RIGHT

Lifespan

IT Asset Disposition Services for Enterprises

www.lifespantechnology.com

888.720.0900

CONTENTS

INTRODUCTION

Effectively erasing data from storage devices is a critical function of data security management. While the approach for erasing hard drives is widely understood, solid state disks (SSD) require different techniques to achieve sufficient data security. Because Solid State Disk (SSD) storage technology is inherently unique in the way data is stored, the assumption that the erasure techniques that work for traditional hard drives will also work for SSDs is problematic.

There are some advances in SSD erasure solutions and their corresponding effectiveness based on recent testing. Utilizing a risk based approach to data security, the appropriate erasure method or can be applied to SSD to defeat its corresponding threat.

What are Solid State Disks (SSD)?

A solid-state drive (SSD), sometimes called a solid-state disk or electronic disk, is a data storage device that uses NAND-based flash memory chips to store data.

Unlike traditional hard disk drives (HDDs), which are electromechanical devices containing spinning disks and movable read/write heads, SSDs do not employ any moving mechanical components.

Most advantages of solid-state disks over traditional hard drives come from the characteristic of data being accessed completely electronically instead of electro-mechanically. This makes SSD a very durable and reliable solution.

However, the reality is that SSD do not last forever. Flash memory can only be programmed and erased a finite number of times. The SSD manufacturers can effectively predict how long SSD can last with a lot of accuracy and they have particular functions to extend the longevity of SSDs.

What is the Data Erasure Challenge?

Traditional hard drives store their data in a linear, ordered manner.

Due to the nature of flash memory's operation, data cannot be directly overwritten as it can in a hard disk drive.

SSDs spend a great amount of effort on rearranging pieces of data and cataloging their new locations. The main reason for this is uniform wear leveling of the SSD. This puts a big responsibility on the flash memory controller and its firmware to maintain data integrity.

The controller on the SSD manages the flash memory and interfaces with the host system. The controller uses a logical to physical mapping system known as logical block addressing (LBA) and that is part of the controller’s flash translation layer (FTL).

The flash translation layer (FTL) acts as a traffic cop managing the mapping between logical block addresses (LBAs) that are visible to the user via the ATA or SCSI interface and the inaccessible, physical pages of flash memory.

When new data comes in replacing older data already written, the SSD controller will write the new data in a new location and update the logical mapping to point to the new physical location. The old location is no longer holding valid data, but it will eventually need to be erased before it can be written again. As a result, the old version of the data remains in digital form in the flash memory. This leftover data is referred to as digital remnants.

Since in-place overwriting is not possible in SSDs, the overwrite-based erasure techniques that work for hard drives may not work properly for SSDs. Those techniques assume that over writing a portion of the LBA space results in overwriting the same physical media that stored the original data. Overwriting data on an SSD results in logical sanitization where the data is irretrievable via the host interface. But overwriting does not necessary result in complete digital sanitization in *all areas* of the SSD.

Data Erasure Options

There are three methods to be considered for data protection for SSD:

1. Cryptographic Erase
2. Secure Erase
3. Traditional Overwriting

Although not a method of data removal, cryptographic erase is where the encryption key on the SSD is deleted or destroyed so that the information on the SSD is no longer decipherable. The benefit of this method is that it is a quick action taking only minutes to complete and the data on the SSD, while present on the drive, is undecipherable without the original encryption key. This is an effective means of protecting data. For instance, the Apple iPad erases user settings and information by removing the encryption key that protects the data. This process takes just a few minutes. The disadvantages of cryptographic erase as a method is that not all SSD drives employ hardware encryption, so it cannot be uniformly utilized in all cases. Furthermore, technically the data is still present on the storage drive. So, although there is wide spread belief the data cannot be deciphered and retrieved after this process, there is conjecture of what future developments in technology would be able to do to encrypted devices.

Secure erase is a built in command that exists in a SSD drive firmware that erases all areas of the storage device. This is considered the best method of dealing with SSD data removal because the SSD manufacturer wrote this firmware feature and is in the best position to address all storage areas of the drive and the drives inner workings. Additionally, the SSD manufacturer has the ability to utilize vendor unique commands unknown to outside third parties. If secure erase worked flawlessly in all cases for all drives, then this method would be the solution of choice. Unfortunately, there have been some well-documented studies regarding the implementation of secure erase in drives and the results are that secure erase does not execute consistently in every case.

Finally, traditional overwriting is a method where multiple passes of blank data are written to the drive over and over. An example of a traditional overwriting method is US Department of Defense – 3 pass overwrite. This method of data removal will clear the logical data locations that are user viewable through your computer. However, this method will not effectively clear all digital locations in the SSD that reside beneath the firmware or flash transition layer. But, due to the characteristics of the SSD firmware, a multiple overwrite solution will populate this blank data to the digital spaces below the firmware level at the discretion of the SSD firmware code.

Risk Based Approach

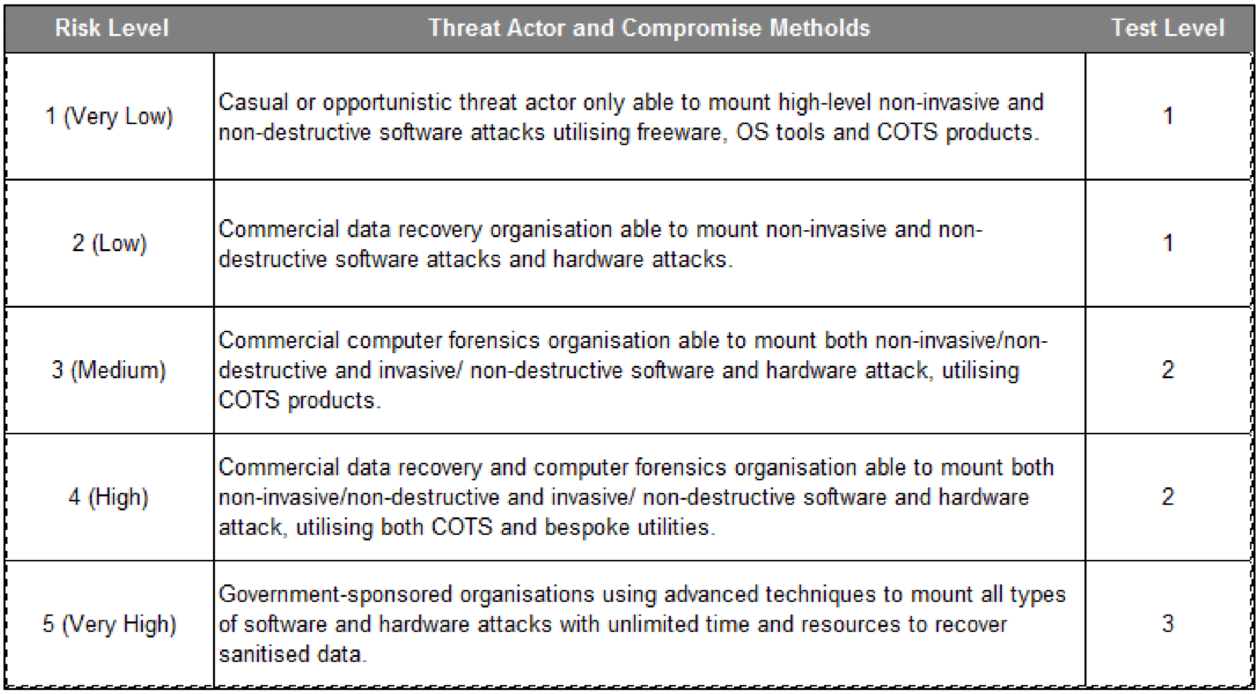
There are options for data removal for SSD, but none of the options appear to be perfect. So, what's the best way to approach the problem?

The correct choice of sanitization level or method for a particular application really depends on the sensitivity of the data that is being erased and the means and expertise of the expected threat. This approach is called a *risk based* approach.

Each method or combination of data removal methods can be tested for its effectiveness based on a defined threat. In kind, forensic testing can be set up to represent the defined threat capability and to qualify the data removal solution

See the *Threat Capability Matrix* in Table 1 provided by Asset Disposal and Information Security Alliance (ADISA). There are five (5) levels of risk from low to high where 1 is the lowest level of threat and 5 is the highest.

Once the risk level is defined then the data removal method needs to hold up against a corresponding test level that mimics the risk or threat.



Risk Level	Threat Actor and Compromise Metholds	Test Level
1 (Very Low)	Casual or opportunistic threat actor only able to mount high-level non-invasive and non-destructive software attacks utilising freeware, OS tools and COTS products.	1
2 (Low)	Commercial data recovery organisation able to mount non-invasive and non-destructive software attacks and hardware attacks.	1
3 (Medium)	Commercial computer forensics organisation able to mount both non-invasive/non-destructive and invasive/ non-destructive software and hardware attack, utilising COTS products.	2
4 (High)	Commercial data recovery and computer forensics organisation able to mount both non-invasive/non-destructive and invasive/ non-destructive software and hardware attack, utilising both COTS and bespoke utilities.	2
5 (Very High)	Government-sponsored organisations using advanced techniques to mount all types of software and hardware attacks with unlimited time and resources to recover sanitised data.	3

Table 1. Threat Matrix Provided by ADISA

This risk based approach allows risk management and security professionals to select data removal solutions that have been qualified (lab tested) against a categorized threat.

Currently, many selections for data removal or sanitization are made very subjectively in a *one-size fits all* policy. This one size fits all may drive unnecessary cost or risk into a data sanitization event or companywide policy.

Take the earlier example of Apple's iPad use of cryptographic erasure. This method of data removal may not be suitable for *top secret* government risk levels, but cryptographic erase may be very appropriate to apply to Apple consumers and their data.

Mitigating Risk for SSD

When looking at a risk based approach for solid state storage, consider the following when formulating your data sanitization policy:

1. Profile your threat.
2. Identify the product type that you are displacing.
3. Understand your tolerance to risk.
4. Place SSD into a managed and controlled asset disposal stream.
5. Have prescriptive means of sanitization.

SUMMARY

Solid State Drives (SSD) and flash storage are unique and complex devices that provide high value to users. As such, SSD will see a rapid and increased adoption in the marketplace. Moving forward, the mind set of data removal from the traditional hard drive is changing in how information is accessed and dealt with on a digital level.

While current government data erase standards do not uniformly agree on how to sanitize SSD, the experts can agree on the effectiveness of certain solutions or combination of solutions based on testing methodology.

Ultimately moving to a risk based approach will marry the appropriate data removal solution to the corresponding threat level. Solutions that have been tested appropriately and qualified against defined threat levels should be utilized over one-size fits all solutions.

Government and industry standards on how to uniformly deal with SSD are still evolving; however, the ability to securely erase a SSD device is becoming a solvable problem.

This whitepaper was created by Tabernus, LifeSpan's partner for secure data erasure.

WE DO ITAD RIGHT
Lifespan

www.LifeSpantechnology.com

888.720.0900

Contributions to this whitepaper provided by Steve Mellings, founder of Asset Disposal and Information Security Alliance (ADISA). *www.**adisa**.org.uk*