Technical white paper

Storage Device Sanitization Methods and Applications

Table of contents

Overview

Today, one of the top concerns of governments, professionals and IT experts is that of data security. Part of these concerns center around the best practices associated with sanitizing storage devices to prevent unauthorized access to sensitive user data. Once devices are removed from the computing or storage subsystem, any user data left on the device creates a data security vulnerability. The recent, dramatic upturn of data theft has increased the awareness of securing data both during use and when repurposing or disposing of storage devices. Navigating the confusing array of solutions and levels of sanitization can be a challenging and complicated ordeal. This white paper will attempt to address the concerns and developments in the sanitization of user data.

The "Myth" of DoD 5520.22-M

The Department of Defense 5520.22-M standard, which details the process for erasure or "wiping" of data from a storage device, became prevalent when data security first started to be a concern. DoD 5520.22-M was never approved by the Department of Defense for civilian media sanitization. More importantly, the DoD never expected this standard to apply to *classified* data. The DoD does not "certify" data sanitization or destruction standards and does not have the capability to oversee the implementation of any applied standards. For internal classified data, the DoD relies on a combination of wiping, degaussing and/or physical destruction. The U.S. Department of Defense no longer references DoD 5520.22-M as a method to securely erase storage devices. Additionally, DoD 5520.22-M specifies a process by which the storage device is overwritten, multiple times, with random patterns of ones and zeroes. Independent sanitization verification studies have proven that multiple overwrite passes are no more effective than a single overwrite pass in modern devices. And, there is a significant time burden associated with multiple overwrites; overwriting large-capacity hard drives, even once, can take almost an entire day. Busy IT departments simply do not have this kind of time and short cuts are likely to be taken. In summary, DoD 5520.22-M is no longer an accepted methodology for sanitizing modern storage devices.

The Solution: NIST SP800-88 Revision 1

Since 2006, the National Institute for Standards and Technology (NIST), has been working on a specification to fill the void that exists in data sanitization. NIST, a branch of the U.S. Department of Commerce, is chartered with assisting U.S. citizens and business with information security. Through special publications in the 800-series, NIST applies standardization and guidelines for information security. While the full details of all 800-series NIST publications is beyond the scope of this paper, one publication, NIST Special Publication 800-88 Revision 1 "Guidelines for Media Sanitization" is of particular interest. NIST SP 800-88 defines preferred methodologies for sanitizing storage devices. These methods include both overwriting and performing Secure Erase operations. This document has replaced DoD 5520.22-M in terms of standardization and certification practices.

The intent of the NIST SP800-88 document is to provide meaningful and actionable guidelines for sanitizing storage devices (including rotational Hard Disk Drives (HDDs), Solid State Drives (SSDs) and many other types of storage devices). In its most recent 2014 release, NIST has also included guidelines for new NVMe PCIe SSDs.

NIST SP800-88 defines three distinct levels of sanitization and then provides acceptable device functions to achieve that level. The following flow diagram, provided in SP800-88 Revision 1, is included to help guide the reader in making a decision as to the method of sanitization required/desired. The full SP800-88 Revision 1 document can be downloaded, for free, from: http://dx.doi.org/10.6028/NIST.SP.800-88r1.

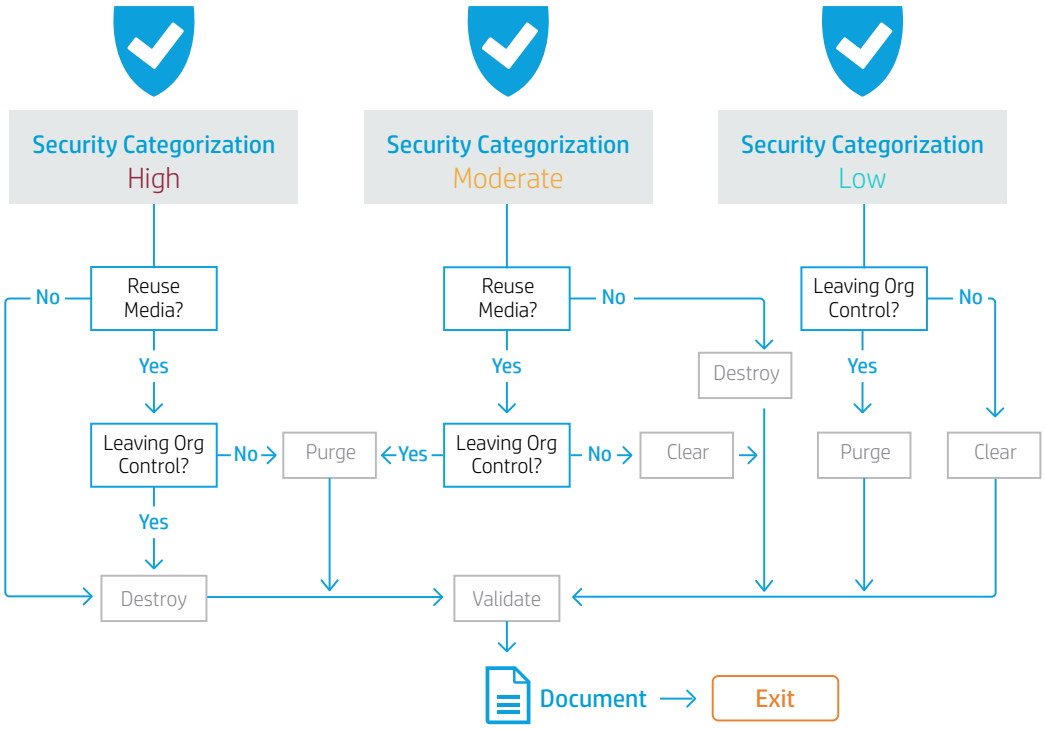

Figure 1. Sanitization Method Flowchart

When deciding which method of sanitization is appropriate, the reader is encouraged to take cost, environmental impact, time, data sensitivity and risk mitigation into account. In the following sections, each of these SP800-88 sanitization methods (Clear, Purge and Destroy) will be explored, in detail.

Clear

The Clear method uses software or hardware products to overwrite the user-addressable storage space on the device with non-sensitive data. Utilizing the device's native read and write commands, this process effectively replaces the user's data with a fixed data pattern. This method is best utilized for devices that are to be re-purposed within an organization. For example, if an employee leaves the company, the IT department would use the Clear method to remove any of the old user's data and re-purpose the drive for a new employee. The device will never physically leave the premises and risk of data theft is low (especially if any encryption policy is implemented). Typically, Clear will not overwrite any spare sector pools or re-allocated sectors on the device.

This method is normally applied to devices using the ATA SECURITY ERASE UNIT command (more commonly called 'Secure Erase'). Secure erase is recognized by NIST SP800-88 as an effective and secure way to meet requirements for data sanitization against attacks up to laboratory level and on data up to Confidential level. So, data involving medical or credit card records, for example, would be effectively cleared from the device. Again, this method is meant to be used only on devices that are to be re-purposed *within* an organization.

Purge

The Purge method takes the functionality of the Clear method one or more steps further. It can utilize a device's built-in read and write functionality but also will involve the use of dedicated sanitization features and commands that apply media-specific techniques to bypass the abstraction of typical read and write commands. Additionally, methods in the Purge category properly deal with any spare or re-allocated sectors/blocks that are not dealt with in the Clear method. All of these differences, above and beyond the Clear method, provide a more robust sanitization operation. Some of the device operations that fall into this method are Enhanced Secure Erase, Overwrite, Block Erase and Cryptographic Erase.

Enhanced Secure Erase, which also uses the ATA SECURITY ERASE UNIT command described in the Clear section above, differs from Normal Secure Erase in two important ways. Enhanced Secure Erase will write a Vendor-Unique, non-repeating data pattern to the media (instead of the Normal Secure Erase fixed pattern of ones or zeroes) and it will include all spare and re-allocated sectors along with all user data areas. This ensures that any user data, whether it resides in the user data area or not, is purged. By either clearing the Erase Mode bit (Normal Secure Erase) or setting the Erase Mode bit to one (Enhanced Secure Erase), the appropriate Secure Erase type is selected in the command. All HP SATA storage devices are required to support both the Normal and Enhanced Secure Erase functionality.

Overwrite is a function in storage devices that only applies to rotational Hard Disk Drives (HDDs). The Overwrite command is not supported on Solid State Drives (SSDs). It is executed using the ATA OVERWRITE EXT command in SATA devices. Overwrite applies a more complex multi-byte data pattern to the device's media. It also has provisions for optional multiple-passes and to enable an option to invert the data pattern between multiple overwrites. While using this multiple overwrite function, alone, may not be beneficial, paring it with other functions can create a powerful and robust (although slow) combination. NIST SP800-88 specifies the use of Overwrite in combination with other Sanitize Device feature set operations.

Block Erase is a function enabled only in SSDs. Rotational HDDs do not support it. Block Erase is executed on an SSD using the ATA command BLOCK ERASE EXT. Block Erase will instruct the SSDs controller to apply an erase voltage to all NAND cells of the device (including any cells which form blocks that have been retired, re-allocated, involved in garbage collection or over-provisioning or are part of a reserved pool of spare blocks). This functionality provides a very fast, complete and robust erasure of the solid state device. NIST SP800-88 actually specifies Block Erase be performed after other functions (like a Cryptographic Erase) as an added assurance that all data on the device is purged (the "belt and suspenders" approach!).

Cryptographic Erase is a command in the Sanitize Feature Set that is only supported in Self-Encrypting Drives (SEDs). Using the ATA command CRYPTO SCRAMBLE EXT, this function removes the encryption key effectively making it impossible to reconstruct any of the data on the storage device. Crypto Scramble is implemented on both HDD and SSD SED devices. As mentioned above, compliant devices that follow NIST SP800-88 are applying either a Block Erase function following Crypto Scramble (on SSDs) or an Overwrite function following Crypto Scramble (on HDDs). Use of ATA Sanitize Device feature set commands is always preferred over the use of normal ATA Security feature set commands provided the device will support it.

All of these methods are recognized by NIST SP800-88 as an effective and secure way to meet requirements for data sanitization against attacks up to advanced laboratory level and on data at the Classified level. The Purge method is most effective on devices which are planned to leave the control of the organization which originally applied data to them. For example, Purge would be beneficial to a company that is replacing 4-year old laptops and sending the laptops in for recycling. The IT department would apply a Purge method to the storage devices in these laptops to prevent the retrieval of any sensitive data from them once they leave the company's premises.

Destroy

The Destroy method means the actual physical destruction of the storage device. Some techniques may render the user data infeasible for retrieval through the device's interface. According to NIST SP800-88, a device is not considered to be destroyed unless all user data is irretrievable even using state of the art forensic laboratory techniques. There are many ways to destroy a storage device including physical shredding, disintegration, pulverization or incineration. And, destruction may be the only option for non-working storage devices where Purge methods cannot be applied because the device is not operational. Since most destructive techniques involve specialized methods and equipment to execute, outsourced third-party firms are often employed to perform these duties. An overall security assessment should be performed to ensure the security of the devices between the pickup point and the destruction facility. Since devices are leaving one organization and, based on the relative sensitivity of the data, a Purge method may need to be applied to the devices (if working) to ensure data security throughout the destruction process. NIST also stipulates the Destroy method for those devices that have failed Clear or Purge verification.

Destruction is recommended for all devices storing data sensitive enough to fall into Secret, Top Secret or Restricted classifications where the storage devices are not repurposed, internally, and are carefully monitored during verification stages.

What Methods Not to Use

Of the many methods available to remove data from a storage device, there are several methods that are *not* recommended. Most of these methods are not recommended because they either have been proven to be ineffective or they are too difficult or too unreliable to implement.

The first method that is not recommended is the simple file delete (also known as 'Weak Erase'). This method is usually applied from the operating system interface by means of the user deleting individual files or entire folders/directories. This method is not effective at all since it merely removes the reference to the data in the file system structure. The actual data is still located on the storage device and the data is easily recovered from the user's trash folder. Even if the trash folder is emptied, the data is still persistent on the storage device.

The second method that is not recommended is the simple device format. By default, some operating systems enable a 'Quick Format'. This merely establishes a new master boot record and flags all existing files to allow them to be overwritten. They are still there and can be accessed with common data recovery tools and little effort. Formatting does not mean you have sanitized a storage device. Eventually, as the device is used, the previous files will all get overwritten. But, this could take quite a while and the previous data is vulnerable until it all gets overwritten.

Another method that is not recommended is the execution of a Block Erase operation through external software. When a Block Erase or Overwrite is executed from a software application, the potential for that application to be compromised by viruses and malware is very high. As an alternative, HP recommends allowing the storage device to execute its own, built-in function initiated by sending the appropriate command to the device.

Finally, HP does not recommend degaussing as a means of clearing user data. NIST SP800-88 has provisions which allow degaussing to satisfy either Purge or Destroy requirements (depending upon the media used). In order for degaussing to be effective, the strength of the degausser needs to be carefully matched to the hard drive's coercivity. Coercivity is a measure of a magnetic material's ability to withstand an external magnetic field without becoming demagnetized. The information on this property of the magnetic materials applied to a hard drive's platters is neither readily available on device labels nor eagerly divulged by device manufacturers. And, there are no convenient means to verify that data has been effectively erased. If work has been done to carefully match the device to the degaussing mechanism, this function can be effective. For mainstream device sanitization, it is not recommended for most users. Degaussing is only effective on HDDs and SSHDs that have platters coated with a magnetically sensitive material. Solid State devices (SSDs) are largely immune to all but the most extreme magnetic fields.

Resources for Carrying out NIST SP800-88

Now that we have clarified the transition from DoD 5520.22-M to NIST SP800-88 and have defined the different sanitization methods specified by SP800-88, what resources are available to carry out these different methods?

The first place to turn to is the HP platform BIOS F10 setup screen. Many platforms are already enabled with Normal Secure Erase functionality to help HP customers carry out Clear activities. Support in other platforms is being added all the time and HP is currently working to also enable Enhanced Secure Erase.

Another place to look is in specialized "tool box" software applications which are written by the storage supplier. These applications are written specifically for the manufacturer's hardware and so often times have increased functionality over off-the-shelf applications which may not be aware of individual drive feature sets or capabilities.

Finally, there are quite a few third-party disk utilities that can execute Secure Erase functionality, at a minimum. Often times, these third-party tools also contain many helpful applications that can assist with tasks such as backup, copy and performance testing, to name a few.

The table, below, is provided as a rough guide to help choose the best operation which aligns with NIST SP800-88. This table should not be considered as a standard, but merely as a guide. It is encouraged to review the entire NIST publication and to consider all of the factors (data risk, sensitivity, ultimate device disposition, the costs and time involved) and any other mitigating circumstances that could affect the choice of a particular method.

NIST SP800-88 Media Sanitize Method	Device Function to Perform
Clear	Normal SECURE ERASE UNIT
Purge	Enhanced SECURE ERASE UNIT
	CRYPTO SCRAMBLE EXT (SED)
	OVERWRITE EXT (HDD) / BLOCK ERASE EXT (SSD)
Destroy	Shred, Disintegrate, Pulverize or Incinerate

Table 1. Sanitization Guide

A Special Note about NVMe Devices

NVMe is a new protocol that operates over the PCIe bus. NVMe does not follow conventional ATA feature sets. As a result, NVMe devices implement sanitization functions a bit differently. NVMe devices support a sanitization function, inside their FORMAT NVM command structure. So, by setting some specific bits in this command structure, a function similar to Secure Erase can be carried out. Current desktop Workstation BIOS implementations support this methodology, just like Secure Erase, in the F10 BIOS setup screens. NIST SP800-88 has a section dedicated to NVMe devices. Devices that support the AHCI protocol over the PCIe interface support normal ATA commands.

Conclusion

As data security threats increase, the need for more robust and effective storage device sanitization measures is increasing as well. More stringent requirements, which protect user data from unauthorized or malicious use, are driving rapid changes in the storage sanitization landscape.

HP is moving away from DoD 5520.22-M in favor of NIST SP800-88 for media erasure guidelines in storage devices and computing platforms. NIST SP800-88 defines three levels of media sanitization: Clear, Purge and Destroy.

The choice of which method to use depends mainly upon the sensitivity of the data and the ultimate disposition of the storage device (e.g. reuse vs. recycle, etc.). There are some methods that are not recommended and should not be used as reliable or easily implemented sanitization methods.

There are many resources available to help execute these sanitization methods. From internal platform-supported functionality to drive supplier and/or third party application, an appropriate method should be available to everyone.

HP Workstation Storage Engineering works closely with HP Security teams and industry storage leaders to ensure we provide the best and most secure storage components possible. So, regardless if you are storing important data or sanitizing your storage devices, you can rest assured that HP storage solutions will exceed your expectations.

To read more about SSD technology for HP Workstations, go to hp.com/V2/GetPDF.aspx/4AA3-8500ENW.pdf

4AA6-6273ENW, March 2017