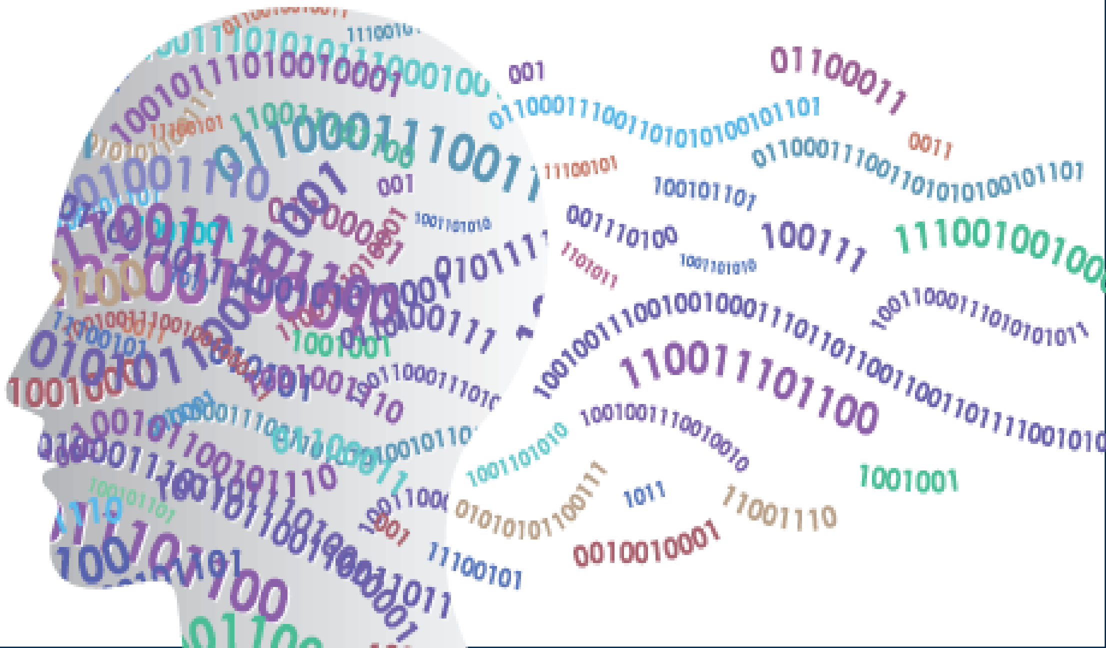
Storage Sanitization – Recent Evolution

SNIA COMPUTE, MEMORY, AND STORAGE SUMMIT

Solutions, Architectures, and Community

VIRTUAL EVENT, MAY 21-22, 2024



Presented by Paul Suhler

Principal Engineer, SSD Standards, KIOXIA

Chair, IEEE Security in Storage Working Group

Abstract

The need to eradicate recorded data on storage devices and media is well understood, but the technologies and methodologies to do it correctly can be elusive.

New standards are being developed that build upon the ISO/IEC 27040 (Storage security) and IEEE 2883™-2022 (Standard for Storage Sanitization) international standards. These provide more clarity for organizations as well as enhanced expectations of what is meant by reasonable security.

Standards organizations are improving the coordination of their work, which will provide a more coherent set of standards.

This session describes the framework of standards and highlights new capabilities and ongoing developments.

Learning objectives

Understand …

- … new developments in data sanitization and related standards,
- … which standards are of use to the listener's organization, and
- … which standards bodies are addressing different aspects of sanitization.

Outline

- Vocabulary
- New capabilities
- Work in progress
- The standards environment
- Summary
- Call to action

Sanitization – vocabulary

- Sanitization methods (from IEEE 2883™-2022):
  - **Clear**: User data cannot be read from the device.
  - **Purge**: User data cannot be recovered from media – even if the device is disassembled and the media read at a low level.
  - **Destruct**: Device is destroyed and data cannot be recovered from the remains of the media.
- Purge: All user data in the storage device is eradicated:
  - Including caches, controller memory buffer, persistent memory region, etc.
  - Techniques: cryptographic erase, block erase, or overwriting.
  - Device cannot be read or written until sanitization succeeds.
  - If sanitization fails, then the organization may require destruction, e.g., shredding.
- Documentation of sanitization is (or should be) required.
- Encryption methods:
  - Overwrite: Replace user data with a specified pattern. Applies mainly to HDDs.
  - Block Erase: Atomic erasure of each portion of the media. Applies to SSDs.
  - Cryptographic Erase: User data is written encrypted; erase is done by eradicating the key. Applies to all devices.

Sanitization – new capabilities

- Key Per I/O: Encryption at a fine granularity
  - Goal: Purge data pertaining to one person out of many people whose data is on the device.
  - Solution: A file pertaining to one person is encrypted using a unique media encryption key.
    - Each Write command can encrypt its data with a different key.
    - Keys are kept in a key management appliance.
    - Keys are ephemeral in the device, i.e., forgotten on power cycle.
    - If the device owner is ordered to forget that person’s data, then that person’s key is deleted from the appliance.
    - The encrypted data can no longer be recovered from any storage device.
  - Standards:
    - NVM Express TP4055, Key Per I/O, which allows each I/O command to encrypt/decrypt with a different key.
    - Trusted Computing Group (TCG) Key Per I/O Security Subsystem Class describes provisioning a storage device with keys.
  - Further details:
    - How to prove that all copies of that key have been purged?
    - If the entire device is to be sanitized, it must be built with (for example) a second-level key that can be changed, purging *all* data on the device.

Sanitization – new capabilities

- Verification of sanitization
  - Goal: Read the device to show that it no longer contains the original user data.
    - Crypto erase or block erase can invalidate media ECC. Attempts to read will fail, so verification cannot be performed.
  - NVM Express TP4152 Post-Sanitize Media Verification was recently ratified.
    - After successful sanitization, the device enters the Media Verification state.
    - The Read command in the NVM Command Set (logical block namespaces) allows returning data despite ECC errors.
    - To avoid repeated raw reads exposing proprietary media reliability characteristics, different data may be returned with each read of the same piece of media.
    - All media is deallocated upon exiting the media verification state.

Sanitization – work in progress

- Sanitization of subcomponents, e.g., NVMe namespaces.
  - One storage device may be shared by multiple VMs (users), each of which has a different namespace in the same device.
  - Swapping a user out requires that their namespace must be sanitized.
  - Other namespaces continue to be written and read.
  - Some other parts of the storage device must not be sanitized.
    - E.g., a controller memory buffer (CMB) may contain a data buffer used for I/Os to other namespaces.
  - The Crypto erase method eradicates the encrypted data of one namespace, even when it is intermixed with data of other namespaces.

Sanitization – work in progress

- IEEE P2883.1 Recommended Practice for Use of Storage Sanitization Methods
  - Organizations need guidance on using and implementing sanitization.
  - What sanitization methods are appropriate?
  - What are the risks, feasibility, effectiveness, economics, and environmental consequences?
  - Will enter public review later this year.
- Updating IEEE 1619 Cryptographic Protection of Data on Block-Oriented Storage Devices
  - Defines the XTS-AES block cipher.
  - A new revision will tighten key-use requirements to improve security.
  - Will enter public review this summer.
  - NIST will update SP800-38E to refer to this new revision of 1619.

Sanitization – work in progress

- More guidance on using and implementing sanitization.
  - IEEE P2883.2 Recommended Practice for Virtualized and Cloud Storage Sanitization
    - How to implement sanitization for virtualized and cloud storage systems.
    - Will address the concerns for storage at scale.
  - IEEE P3406 Purge and Destruct Sanitization Framework
    - Provides requirements for defining new sanitization commands.
    - What parts of a storage device must be sanitized?
    - What sanitization methods are appropriate for the device?
    - What means of verifying sanitization are appropriate for the device?

Sanitization – work in progress

- Customers must trust sanitization
  - Liability for a data breach can be tens of millions of dollars.
  - Without confidence that a storage device was sanitized, the customer may decide to destroy the device.
- Compliance testing
  - Confirm that device performs sanitization correctly.
  - IEEE SISWG is exploring establishing a media sanitization certification program.
- Circularity and reuse
  - Goal: Avoid discarding devices and polluting landfills with destroyed devices.
  - Purge user data and reuse the device, or …
  - Destroy the device by disassembling it and recycling its components.

The standards environment

- IEEE Security in Storage Working Group (SISWG)
  - IEEE Std 2883™-2022 (IEEE Standard for Sanitizing Storage)
  - P2883.1 (Recommended Practice for Use of Storage Sanitization Methods)
  - P2883.2 (Recommended Practice for Virtualized and Cloud Storage Sanitization)
  - P3406 (Purge and Destruct Sanitization Framework)
- ISO/IEC 27040 – Storage security
  - 2nd Edition published in early 2024.
  - Includes requirements and guidance for storage security technologies and practices.
  - Specifies requirements for both logical and media-based sanitization.
  - Defers to IEEE 2883 on specific techniques for media sanitization.

The standards environment

- NIST – National Institute of Science and Technology
  - Cryptographic Module Verification Program (FIPS 140-3)
    - Certified testing labs perform certification.
  - Special Publications – various aspects of cryptography and security
    - SP800-38E, and many others.
    - FIPS 203, 204, and 205 define algorithms resistant to attacks by quantum computers. Support will be mandatory for devices sold to US government (post-CNSA 2.0).
- Regulation (EU) 2019/424 (Lot 9):
  - Refers to appropriate “secure data deletion” standards; 27040 and 2883 together would be in this category.

Summary

- Sanitizing portions of a storage device.
- Verifying sanitization.
- Guidance for users and implementers.
- Coordination of standards for sanitization.
- Building customer confidence in sanitization.

Call to action

- Understand your organization’s needs and sanitize accordingly.
- Consider using the new capabilities in your products.
- Participate in groups that define aspects of sanitization:
  - NVM Express
  - INCITS SCSI (T10)
  - Storage Work Group of the Trusted Computing Group
  - IEEE Security in Storage Working Group (SISWG).

Please take a moment to rate this session.

Your feedback is important to us.

SNIA COMPUTE, MEMORY, AND STORAGE SUMMIT

Solutions, Architectures, and Community

VIRTUAL EVENT, MAY 21-22, 2024