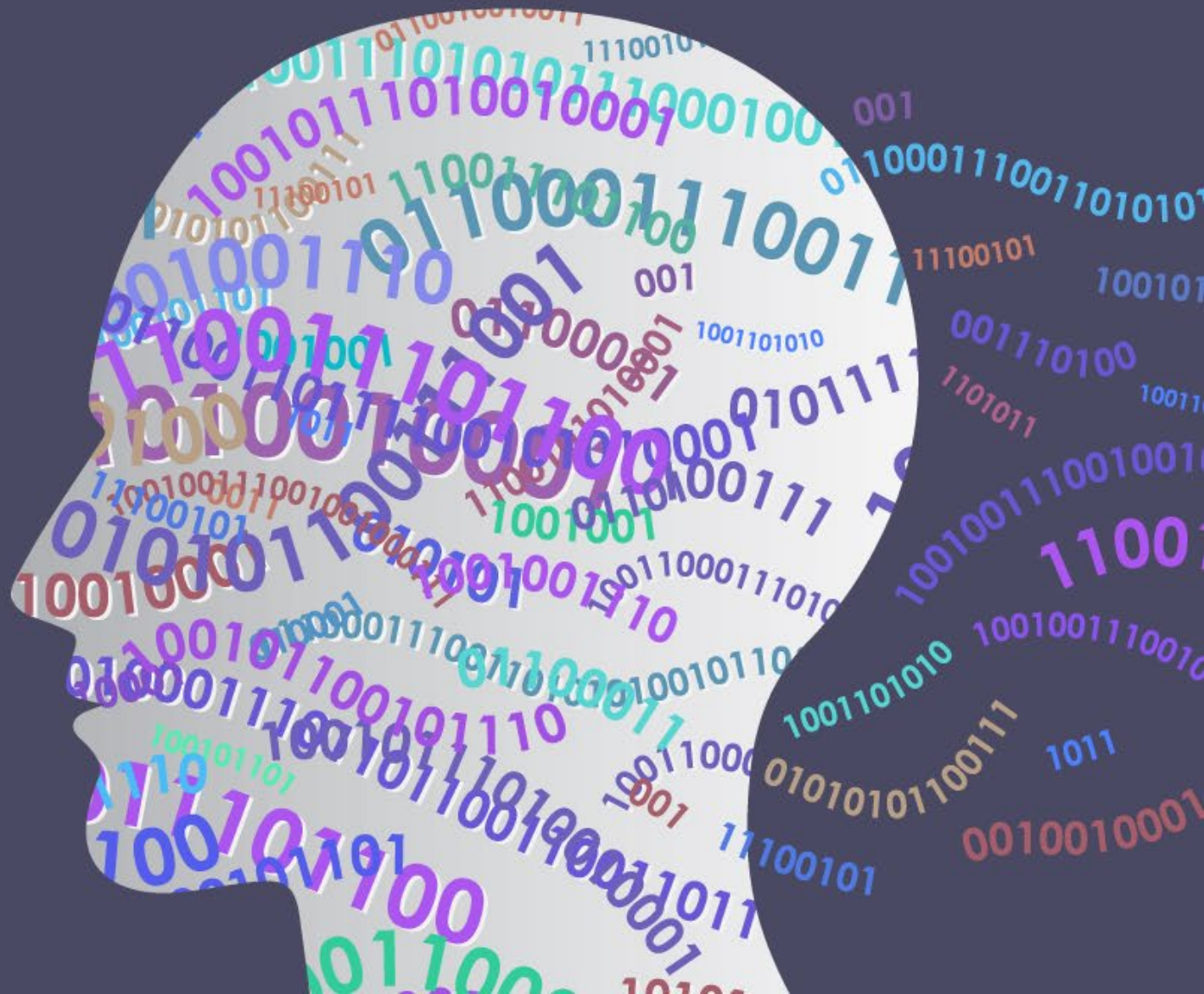
SNIA COMPUTE + MEMORY + STORAGE SUMMIT

Architectures, Solutions, and Community
VIRTUAL EVENT, APRIL 11-12, 2023

Storage Sanitization – The Next Chapter



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. With the publication of the new ISO/IEC 27040 (Storage security) and IEEE 2883™-2022 (Standard for Storage Sanitization) international standards, there is some clarity for organizations as well as enhanced expectations of what is meant by reasonable security.

However, many issues remain to be addressed. This session highlights these new standards as well as exploring some of the remaining issues, including initiatives that are underway to deal with some of the gaps.

Learning Objectives

Understand …

- … the need for certifying sanitization that is performed by storage devices and the limits of certification,
- … the aspects of data storage sanitization that are not addressed by existing standards, and
- … which standards bodies are addressing different aspects of sanitization.

Outline

- Sanitization of storage devices
- New directions for sanitization
- Compliance testing and certification
- Customer concerns
- Circularity and reuse
- The standards environment
- Summary of new directions
- Call to action

Sanitization of storage devices – existing operations

- 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.
- The entire storage device is sanitized:
  - 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.

Sanitization of storage devices – new directions

- Sanitization of subcomponents, e.g., NVMe namespaces.
  - One device may be shared by multiple VMs (customers), each of which has a different namespace in the same storage device.
  - Swapping a customer 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.

Sanitization of storage devices – new directions

- Encryption at a fine granularity
  - Example: A file pertaining to one person is encrypted using a unique key.
    - The file requires only a small part of a namespace.
    - The file may be duplicated across multiple storage devices.
  - Goal: Purge only that one file.
  - NVMe Key Per I/O allows each Write command to encrypt 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 purged from the appliance.
  - The encrypted data can no longer be recovered.
  - But …
    - 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 of storage devices – new directions

- Support for verification of sanitization.
  - Read the device to prove 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.
  - So, existing command sets need to be extended to support those reads.
  - Repeated raw reads can expose proprietary media reliability characteristics. Verification must allow returning different data with each read of the same piece of media.

Sanitization of storage devices – new directions

- Organizations need guidance on using and implementing sanitization.
  - What sanitization methods are appropriate?
  - What are the risks, feasibility, effectiveness, economics, and environmental consequences?
- New standards are under development in IEEE SISWG:
  - IEEE P2883.1 Recommended Practice for Use of Storage Sanitization Methods
    - How to use sanitization to meet your organization's needs.
  - 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.

Compliance testing and certification

- Private testing companies typically work for customers who buy devices.
  - Most testing includes directly reading media, e.g., HDD spin stand or NAND raw interface.
  - The device vendor may or may not be involved, e.g., showing where to look for user data.
- Will vendors pay for certifying that their products sanitize correctly?
  - Cost must be passed to customers.
  - Will this result in a higher price to customers?
  - NIST FIPS140-3 compliance testing has been paid for by vendors.
- IEEE SISWG is exploring possible use of the IEEE Conformity Assessment Program to establish a media sanitization certification program.

Customer concerns

- Liability for a data breach can be tens of millions of dollars.
- Liability can exist in perpetuity.
  - Will someone someday invent an algorithm or computer that can crack encrypted data?
- Is the storage device sanitization firmware buggy?
- Has the firmware been compromised?
- With each new device hardware or even firmware, the questions return.
  - Re-certification is required.
- Is the sanitization software tool buggy?
- Is the software tool compromised?
- Did the technician use the sanitization software correctly?

- Without confidence that a storage device was sanitized, the customer may decide to destroy the device.

Circularity and reuse – a new goal

- Destruction of devices is wasteful and potentially polluting, producing a pile of hazardous materials that should not end up in landfills.

- Better to purge the user data from the device and reuse the device.
  - But, the customer must be certain that the user data cannot be recovered.
- If the device must be destroyed, then disassemble it first.
  - This facilitates recycling materials into different streams.
  - New standards will provide guidance.

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)
- ISO/IEC 27040 – Storage security
  - Publication of 2nd Edition anticipated in mid-2023.
  - 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
    - A new area is algorithms to provide security in the face of attacks by quantum computers.
- Regulation (EU) 2019/424 (Lot 9):
  - Refers to appropriate “secure data deletion” standards; 27040 and 2883 together would be in this category.

Summary of new directions

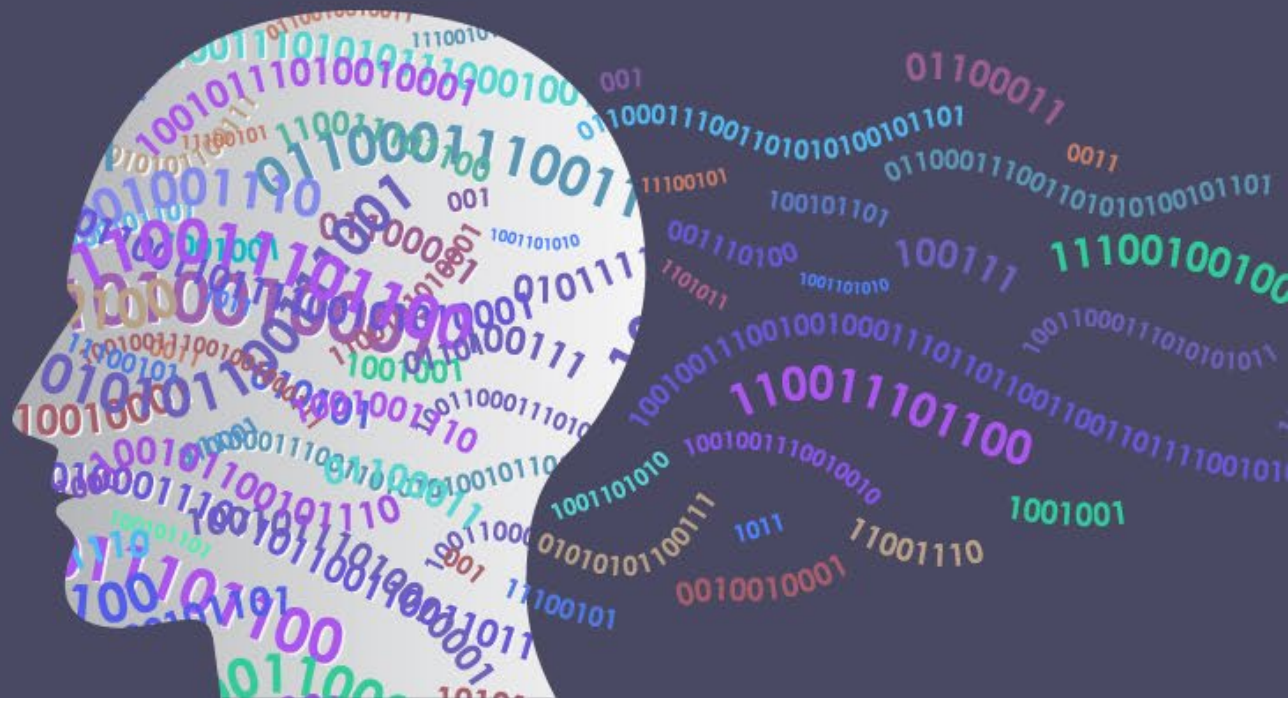
- Sanitizing portions of a storage device.
- Adding storage device support for verification of sanitization.
- Guidance for users and implementers.
- Establishing certification programs for sanitization.
- Coordination of standards for sanitization.
- Building customer confidence in sanitization.

Call to Action

- Understand your organization's needs.
- Read the upcoming SNIA white paper on encryption key management.
- Participate in groups that define sanitization-related commands – NVM Express, INCITS SCSI (T10), INCITS ATA Storage Interfaces (T13).
- Participate in the IEEE Security in Storage Working Group (SISWG).

SNIA COMPUTE + MEMORY + STORAGE SUMMIT

Architectures, Solutions, and Community
VIRTUAL EVENT, APRIL 11-12, 2023



Please take a moment to rate this session.

Your feedback is important to us.

