Flash Memory Summit

Data Sanitization Developments and Trends

Presenter:

Paul Suhler
Principal Engineer, SSD Standards, KIOXIA America, Inc.
Chair, IEEE Security in Storage Working Group

What is sanitization?

- The removal of all user data from a storage device.
- Sanitization methods (from IEEE 2883™-2022):
  - **Clear**: User data cannot be read from the device through the interface.
  - **Purge**: User data cannot be recovered from media – even if the device is disassembled and the media read at a low level.
  - **Destruct**: User data cannot be recovered from the remains of the media.
- Sanitization techniques:
  - **Cryptographic erase**: User data is encrypted; the decryption key is eradicated.
  - **Block erase**: Media-specific alteration, e.g., flash erase.
  - **Overwrite**: Media contents are rewritten with different data.

Why sanitize?

- Liability for a data breach can be tens of millions of dollars.
- Liability can exist in perpetuity.
- Without confidence that a storage device was sanitized, the customer may decide to destroy the device.

The standards environment

- Guidance for organizations on how to use and implement sanitization.
  - What are the appropriate sanitization methods for each organization?
  - What are the risks, feasibility, effectiveness, economics, and environmental consequences?
- 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)
  - SISWG is exploring use of the IEEE Conformity Assessment Program to establish a media sanitization certification program.
- ISO/IEC 27040 – Storage security
  - Requirements and guidance for storage security technologies and practices.
  - Requirements for both logical and media-based sanitization.
  - Refers to IEEE 2883 for specific techniques for media sanitization.

The standards environment

- NIST – National Institute of Science and Technology
  - Cryptographic Module Verification Program (FIPS 140-3)
  - Special Publications – various aspects of cryptography and security
- Regulation (EU) 2019/424 (Lot 9):
  - Refers to appropriate “secure data deletion” standards; 27040 and 2883 together would be in this category.

Sanitization of storage devices – new directions

- Verifying (or auditing) sanitization
  - Read the device to prove that it no longer contains the original user data.
  - Crypto erase or block erase can invalidate media ECC.
  - Reads will fail, so verification cannot be performed.
  - Existing command sets need to be extended to support those reads.
- Circularity and reuse
  - 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.
  - If the device must be destroyed, then disassemble it first and feed different recycling streams.

Sanitization of storage devices – new directions

- Sanitization of subcomponents, e.g., a single NVMe namespace.
  - Multiple users (e.g., VMs) share a device, with each using a different namespace.
  - When a user out is swapped out, their namespace must be sanitized.
  - It may be necessary to continue reading and writing other namespaces.
  - Crypto erase is probably the only practical technique.
- Encryption at a fine granularity
  - A file pertaining to one person is encrypted using a unique key.
  - Keys are kept in a key management appliance.
  - If the device owner is ordered to forget that person's data, then that person's key is deleted from the appliance.
  - Example: Key Per I/O (commands in NVM Express; key provisioning in TCG).

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.

Questions?