STORAGE DEVELOPER CONFERENCE

SDC 23

BY Developers FOR Developers

The IEEE Security in Storage Working Group

Paul Suhler

Chair, IEEE SISWG

KIOXIA Corporation

Abstract

- The IEEE Security In Storage Work Group (SISWG) produces standards that many storage developers, storage vendors, and storage system operators care about, including:
  - A family of standards on sanitization: The IEEE 2883 family.
  - A family of standards on encryption methods for storage components: The IEEE 1619 family.
  - A standard on Discovery, Authentication, and Authentication in Host Attachments of Storage Devices: The IEEE 1667 specification.

Overview

- Organization:
  - IEEE Computer Society
    - Cybersecurity and Privacy Standards Committee (CPSC)
      - Security in Storage Working Group (SISWG)
- Charter is to address any aspect of security as it relates to storage.
- SISWG develops international standards, rather than domestic standards.
- SISWG is an individual membership working group. Members do not formally represent companies or other entities.
  - Typically 15 – 18 individuals participate in the biweekly meetings.

Historical Work

- IEEE Std 1667-2018 (Discovery, Authentication, and Authorization in Host Attachments of Storage Devices)
- IEEE Std 1619-2007 (Cryptographic Protection of Data on Block-Oriented Storage Devices)
  - AES-XTS
- IEEE Std 1619.1-2007 (Authenticated Encryption with Length Expansion for Storage Devices)
  - Various AES modes: CCM, GCM, CBC-HMAC, XTS-HMAC
- IEEE Std 1619.2-2021 (Wide-Block Encryption for Shared Storage Media)
  - EME-2-AES and XCB-AES

Recent Work – Sanitization

- IEEE Std 2883™–2022 (IEEE Standard for Sanitizing Storage)
  - Motivated by the lack of mandatory requirements in some standards.
    - Claims of compliance are meaningless if there are no “shall” requirements.
  - Updated definitions of concepts originally in ISO/IEC 27040.
  - Defined methods (Clear, Purge, Destroy).
  - Defined techniques for Clear and Purge (overwrite, block erase, crypto erase).
  - Defined techniques for Destruct (disintegrate, incinerate, melt).
  - Defined verification of sanitization outcomes (full versus sampling).
  - Updated media-specific sanitization methods.
  - Other standards can now point to 2883 for requirements.

Current Work – Sanitization

- IEEE P2883.1 Recommended Practice for Use of Storage Sanitization Methods
  - How to use sanitization to meet your organization’s needs.
  - Analyze value of data and risks from data breaches.
    - Risk is much worse for disclosure of personal information than for company cafeteria menu.
  - Develop clear procedures for sanitization of devices.

Current Work – 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.

Current Work – Sanitization

- IEEE P3406 (Standard for a Purge and Destruct Sanitization Framework) – pending approval of project.
  - Will provide requirements for standards organizations defining purge and destruct techniques.
  - Especially important for new storage technologies (e.g., DNA or crystal storage).
  - Need to make data recovery “infeasible using state of the art laboratory techniques”.
  - Some techniques will need to be deprecated.
    - E.g., if AES were to be broken, then Crypto Erase implementations that rely on it would be ineffective.

Current Work – Other

- IEEE P1667: Updating 1667-2018.
  - Editorial corrections.
  - Handling of resets in PCIe multi-port and single-port devices.

Current Work – Other Standards Organizations

- Individual members of SISWG work with the editors of documents developed in:
  - ISO/IEC JTC1/SC 27
    - ISO/IEC 27040, to align with IEEE 2883-2022.
  - SNIA Security TWG:
    - Media sanitization white paper.
    - Encryption key management white paper.
  - TCG:
    - Key Per I/O SSC and application note.
  - NIST:
    - SP800-88 Media Sanitization Guidelines (2014).
  - Open Compute Project (OCP)
    - Some OCP documents may be candidates for standardization.

Future Work – Certification

- The IEEE Conformity Assessment Program (ICAP) has the ability to perform certifications.
- Efforts are underway to establish a cybersecurity certification scheme.
- SISWG could become involved with ICAP as part of a certification of data eradication (proof of eradication).

Future Work

- Possible updates to IEEE 2883-2022.
  - NVMe post-sanitize media verification.
  - NVMe namespace purge.
  - eMMC changes.
  - Purge for SD cards.
  - Purge for other technologies, e.g., NVDIMMs, Storage Class Memory (SCM).

SISWG and Other IEEE SA Groups

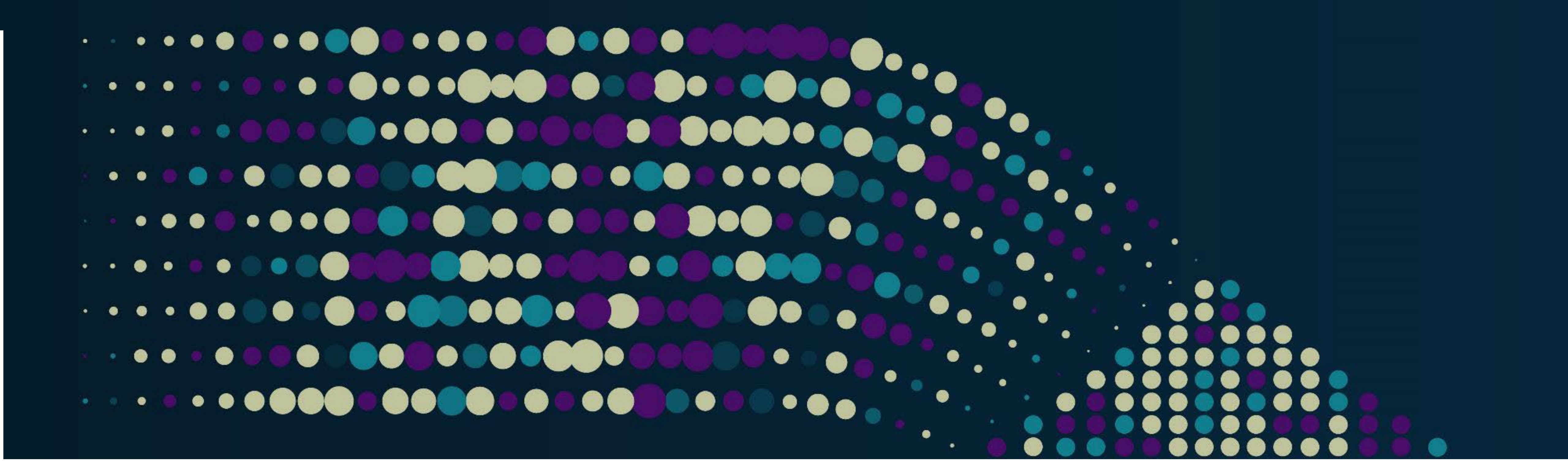
- IEEE work group focusing on post-quantum cryptography (IEEE P3172).
  - A family method that recommends new quantum encryption for various storage types (e.g., block, stream) may be appropriate for SISWG’s IEEE 1619 family.
- IEEE work group focusing on Zero Trust Security (ZTS, IEEE P2887).
  - An application of those principles to storage devices and systems is also within the purview of the IEEE SISWG.

Other IEEE-SA / CPSC Working Groups

- Authentication in a Multi-server Environment WG (C/CPSC/AMSE)
  - P2989 Standard for Authentication in a Multi-server Environment
- Data Leakage Tracing WG (C/CPSC/DLTWG)
  - P3361 Standard for Evaluation Method of Robustness of Digital Watermarking Implementation in Digital Contents
- Interworking Framework for Privacy-Preserving Computation WG (C/CPSC/IFPPC)
  - P3117 Standard for Interworking Framework for Privacy-Preserving Computation
- Quantum Security WG (C/CPSC/QuSEC)
  - P3172 Recommended Practice for Post-Quantum Cryptography Migration

Other IEEE-SA / CPSC Working Groups

- Space System Cybersecurity WG (C/CPSC/S2CY)
  - P3349 Standard for Space System Cybersecurity
- System & Software Runtime Security WG (C/CPSC/S2RS)
  - P3389 Standard for Technical Framework of Runtime Application Self-Protection (RASP)
- Software Supply Chain Security WG (C/CPSC/SSCS-WG)
  - P3390 Standard for Security Management Capability Framework of Open Source Software Supply Chain for Software Providers
- Zero Trust Security WG (C/CPSC/ZTSWG)
  - P2887 Recommended Practice for Zero Trust Security
  - P3409 (Draft) Standard for a Zero Trust Security Framework



Please take a moment to rate this session.

Your feedback is important to us.