Panel Discussion: What Me Worry? Erasure of SSDs – Is It an Issue?

Monty A. Forehand

Security Engineering Director

Seagate Technology

Questions We should be asking?

- What are my life-cycle erase requirements?
  - What is the impact of erase/program cycles consumed ?
- Is it a Self Encrypting Drive (all the data all the time)?
  - Crypto Erase is the only way to fully reach retired locations.
  - Allows for efficient partial device erasure (e.g. TCG Band).
- What happens when I issue an erase command?
  - Block Erase of ALL data flash including over-provision?
  - What conditioning is done to avoid data remnance in the cells?
  - What system data is not erased (SMART, bad block table, etc.)?
  - Is the erase operation atomic across power cycles?
  - Are there vendor mechanisms for recovering erased data?
- Can I erase a portion of the device (say a TCG Band)?
- What commands are supported for Erase?
  - TCG Revert? ATA Security Erase Unit? ATA/SCSI Sanitize Commands?

Backup

SSD/SSHD Full Device Sanitize Options

	Over-write	Block Erase	Block Erase + Pattern Write	Crypto Erase
Time (Relative)	Hour	Minutes	Minutes + Hour	< 1Second
Sanitizes All Retired / Spare Blocks	Not Necessarily (Vendor Specific)	Not Necessarily (Vendor Specific)	Not Necessarily (Vendor Specific)	Yes
Full Array Erase / Program Cycle Consumed	Yes, Likely both (Pre-Erase)	Yes	Yes, Both	Fractional % of the array
Complexity	No defined way to "re-write" flash (Vendor Specific)	Block Erase Permanence (Vendor Specific)	Must Defeat write virtualization entire array (Vendor Specific)	Eradicate the keys only
Attestability	Vendor Specific	Vendor Specific	Vendor Specific	Gov. Certified SED security today (Seagate)
Sanctioning	None known	Government sanction for flash Sanitization*1	Government sanction for flash Sanitization*1	None Yet

- Vendor specific mechanisms are very difficult to reveal / understand / attest to.
- MLC and finer silicon geometries ➔ precious few cycles in the life of the device.

➔ Encryption and Crypto Erase are the most efficient way to attestably sanitize virtualized (flash) storage devices (maybe the only practical way?).

*1 (Examples for Flash Memory, SSD/SSHD not addressed) NIST "SP800-88: Guidelines for Media Sanitization"
NATO "Advanced Data Storage Technology (ADST) Memory Systems Sanitization Guidance", Sept 2009

Speaker Bio

Monty A. Forehand
Security Engineering Director
Seagate Technology

Monty Forehand is Director of Security Engineering at Seagate Technology, leading security products engineering, standards, certifications, and ecosystem development worldwide across all Seagate storage product lines. Monty joined Seagate in June of 1990 and has held various leadership, architecture, technology, design, and development engineering positions in 21 years at Seagate, including the integration of the first flash devices onto hard drives. Monty joined the emerging security products effort at Seagate in 2002 and led the development and deployment of the first fully integrated self encrypting drive (SED) products in the industry. Monty has BS and MS Electrical and Computer Engineering degrees from Oklahoma State University and holds 12 patents and many in-process invention disclosures related to storage and storage security, including the application of security and self encrypting drives on flash-based devices.