Speed is Great, but what about Security?

Monty A. Forehand
Security Engineering Director
Seagate Technology

Data Breaches are Expensive

- Average cost per data breach increasing every year *
  - $6.8 million in ‘09
  - $7.2 million in ‘10

- Data Breeches can occur while a device is in-service or after it is taken out of service.

- Security, Encryption, Self Encrypting Drives, and cryptographic erase can help.

*** Ponemon Institute, *2010 Annual Study: U.S. Cost of a Data Breach,* February, 2009, www.ponemon.org, http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Mar_worldwide_costofdatabreach**

Security and SSD / SSHDs

- SSD / SSHD data virtualization presents new challenges that drive the need for real security, cryptography, and encryption.
- We will explore further in the following slides.

SSD = Solid State Drive

SSHD = Solid State Hybrid Drive

SED = Self Encrypting Drive

What is a Self Encrypting Drive (SED)?

- Encryption of all user data, all the time, at-speed.
  - No performance Loss*. No (p)re-encryption required.
- Strong internal security mechanisms
- Simple to robust standard security management interfaces
  - TCG, T10, T13, IEEE, etc.
- Broad-based security mgmt software support.
- Government (NIST/FIPS) Certified Security.

➔ Attestable and strong protection of data at rest.

➔ Instantaneous and strong Cryptographic Erase for environmentally friendly end-of-life and re-purpose.

➔ Deployed widely on HDDs today.

* http://www.trustedstrategies.com/papers/comparing_hardware_and_software_fde.pdf

Self Encryption on SSDs and SSHDs?

➔ Absolutely! All the benefits apply and then some.

- Software encryption performance and power penalties are potentially more pronounced on “faster” devices.
  - Software FDE = Dramatic performance loss http://anthonyvance.com/blog/security/ssd_encryption/ *
  - Self Encrypting HDD/SSD/SSHD = No performance loss. http://www.samsung.com/global/business/semiconductor/products/SSD/downloads/SamsungSSD_Encryption_Benchmarks_201011.pdf
- Encryption reaches blocks returned for garbage collection for erasure/sanitization.
- Encryption reaches retired blocks for erasure/sanitization.

* Software FDE: “…. it’s clear that the encrypted SSD is much slower than in its unencrypted form (by as much as two thirds, going by the overall Xbench score). By analogy, encumbering the SSD with FDE is like harnessing a champion racehorse to a plow. However, if you are interested in FDE, security is probably more important to you than raw speed anyway.”

SSD/SSHD Full Device Sanitize Options

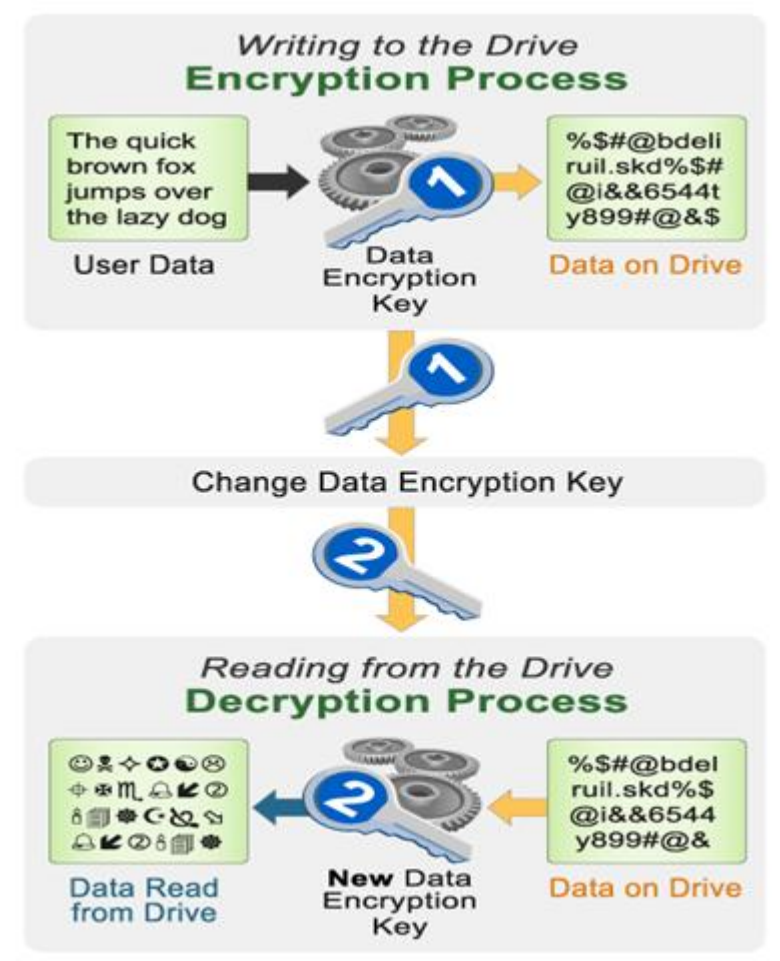
	Over-write	Block Erase	Block Erase + Pattern Write	Crypto Erase
Time (Relative)	Hour	Minutes	Minutes + Hour	< 1Second
Sanitizes All Retired / Spare Blocks	Not Necessarily (Vendor Specific)	Not Necessarily (Vendor Specific)	Not Necessarily (Vendor Specific)	Yes
Full Array Erase / Program Cycle Consumed	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

Cryptographic Erase



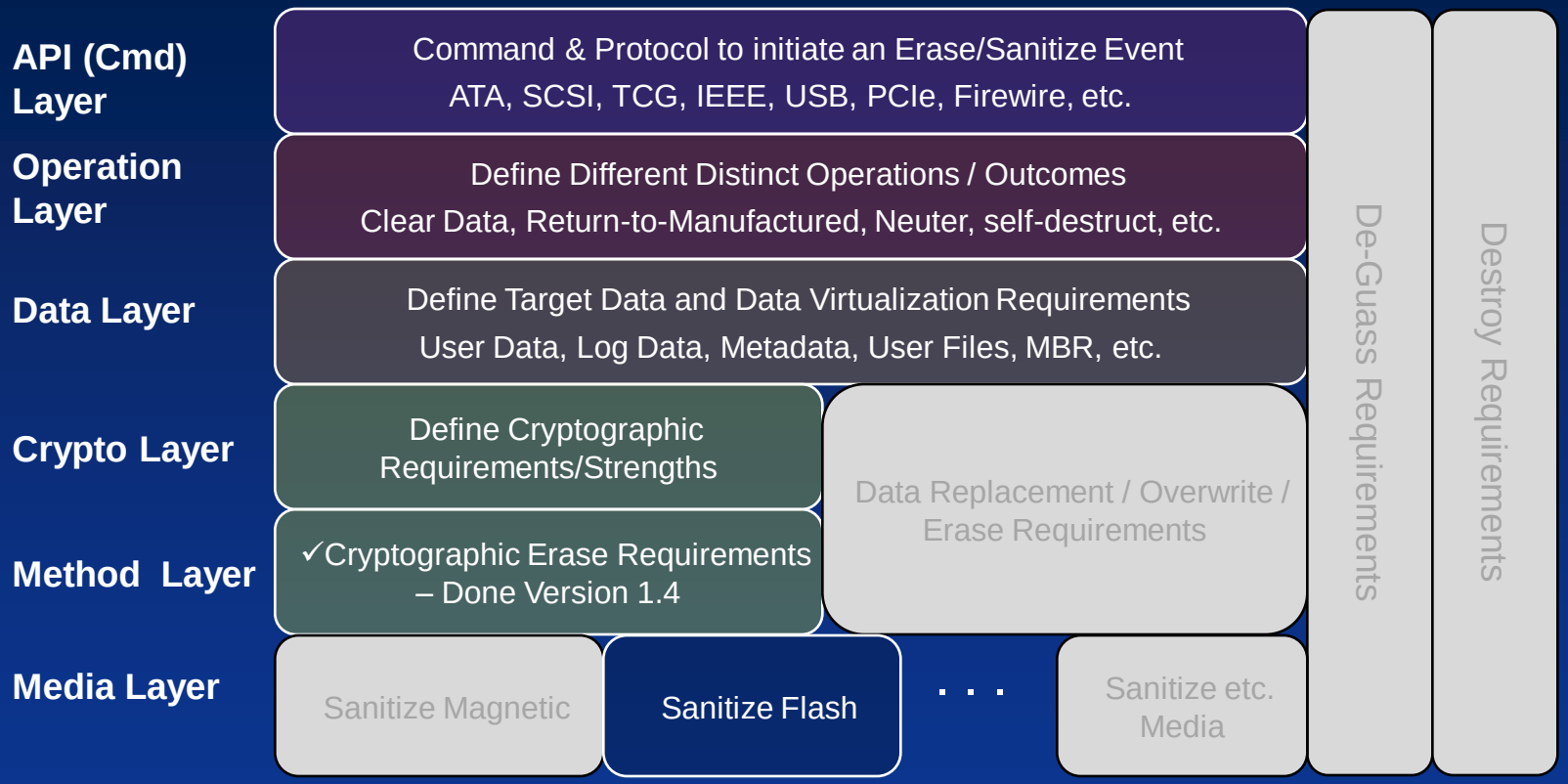
- Eradication of the Data Encryption Key renders old data unintelligible – to the cryptographic certainty of the algorithms and the strength/quality of the keys.

SSD/SSHD Calls to Action

- Need Cryptographic Erase Sanctioning
  - Effort's kicked-off at 2010 Flash Memory Summit
  - Industry & Government consortium functioning.
    - Crypto erase standardization is progressing to plan of a standard.
      - Layers: API, Operational, Data, Crypto, Method, & Media Layers
      - Crypto Erase Method Layer specification complete.
      - Remaining layers in progress.
    - T10/SCSI & T13/SATA have approved "Sanitize-Crypto Erase" command. TCG Ent & Opal SSCs support crypto erase (API Layer).
- More Self Encrypting SSD/SSHD Products
- More Ecosystem / Customer / Industry Partnerships.

Backup

Cryptographic Erase Sanctioning



- Layered Approach to Crypto Erase definition.
- Grayed-out boxes not the focus of this effort.

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.