Self-Encrypting Drive (SED) standardization proposal for NVDIMM-N devices

Vault ‘19

Frederick Knight – Principal Standards Technologist, NetApp, Inc.,
Sridhar Balasubramanian – Principal Security Architect, NetApp, Inc.,
February 2019
Agenda Slide

1) Evolution of storage technology

2) NVDIMM
   - Backgrounder
   - Technology Overview
   - Operational context

3) NVDIMM-N as SED

4) NVDIMM-N Encryption Standardization Proposal
Evolution of Storage Technology

Some things have changed…

- Is it compute or is it storage?

```
2001
Compute
- CPU
- DRAM
Storage
- SSD
- HDD
- Tape

2019
Compute & Storage
- CPU
- DRAM
- NVDIMM
- SSD (high performance)
- PCIe, SAS
- SSD (mainstream)
- SATA
- HDD
- Tape
```
NVDIMM - Backgrounder
DRAM Memory Speed with Storage Persistence

HDD → IOPS (even if random...) → FLASH → Latency (even under load...) → NVDIMM

- DRAM Memory Speed
- NAND Storage Persistency

Lower Latency
Higher IOPS = Improved System Performance

Reference: In-memory computing Summit 2016
NVDIMM Taxonomy

**NVDIMM-N**
- Memory mapped DRAM.
- Flash is not system mapped
- Access Methods -> byte- or block-oriented access to DRAM
- Capacity = DRAM DIMM (1’s - 10’s GB)
- Latency = DRAM (10’s of nanoseconds)
- Energy source for backup
- DIMM interface (HW & SW) defined by JEDEC

**NVDIMM-P**
- Memory-mapped Flash and memory-mapped DRAM
- Two access mechanisms: persistent DRAM (−N) and block-oriented drive access (−F)
- Extends DDR protocol to enable transactional access
- Capacity = NVM (100’s GB-1’s TB)
- Latency = NVM (100’s of nanoseconds)

**NVDIMM-F**
- Memory mapped Flash. DRAM is not system mapped.
- Access Method -> block-oriented access to NAND through a shared command buffer (i.e. a mounted drive)
- Capacity = NAND (100’s GB-1’s TB)
- Latency = NAND (10’s of microseconds)
NVDIMM Use cases

- In-memory Database
  - Journaling, reduced recovery time, tables

- Traditional Database
  - Log acceleration by write combining and caching

- Enterprise Storage
  - Tiering, caching, write buffering and metadata storage

- High-Performance Computing
  - Checkpoint acceleration

Reference: SNIA Flash Memory Summit 2018
NVDIMM - Technology Overview

- A non-volatile DIMM (NVDIMM) is a Dual In-line Memory Module (DIMM) that maintains the contents of Synchronous Dynamic Random Access Memory (SDRAM) during power loss.
- An NVDIMM-N class of device can be integrated into a standard compute or storage platforms to provide non-volatility of the data in DIMM.
- NVDIMM-N relies on byte addressable energy backed function to preserve the data in case of power failure.
- A Byte Address Energy Backed Function is backed by a combination of SDRAM and non-volatile memory (e.g., NAND flash) on the NVDIMM-N.
- JESD245C Byte-Addressable Energy Backed Interface (BAEBI) defines the configuration specifics for interoperating with NVDIMM-N class of devices.
NVDIMM-N – Block Diagram

- System provides 12V to the NVDIMM-N from power supply during normal operation
- Options for emergency power source during the Catastrophic Save operation
  - System switches the 12V power source from power supply to a system-wide battery/supercap
  - The NVDIMM-N switches its power source from the system to an alternate battery/supercap
    - charged with power from the 12V pin

from Micron DDR4 SDRAM NVRDIMM datasheet

© 2019 NetApp, Inc.
NVDIMM-N – Device Operational Context

Application Persistent Data Layer

- **PMEM Tier**
  - Persistent
  - Byte level access
  - Memory speed latencies

- **SSD Tier**
  - Persistent
  - Block level access
  - Lower latencies

- **Hard Drive Tier**
  - Persistent, long-term archive
  - Block level access
  - Higher latencies

© 2019 NetApp, Inc.
NVDIMM-N as Self-Encrypting Device (SED) type

- An NVDIMM-N device may be a self-encrypting device (SED) type that protects data at rest. This means the NVDIMM-N controller:
  - encrypts data during a Catastrophic Save operation
  - decrypts data during a Restore operation

- and the data is:
  - plaintext while sitting in SDRAM
  - ciphertext while sitting in NVM (e.g., flash memory)

- Unlock the device with a password
  - TCG Storage Protocol
  - SSC based on opalite
Data At Rest Encryption Standardization Proposal for NVDIMM-N

- The NVDIMM-N encryption standardization proposal amounts to the following:
  - Extensions to BAEBI specification to accommodate security protocol definitions in consequence with encryption capability in NVDIMM-N devices
  - Extensions to TCG Storage Interface Specifications defining the Security Protocol Typed Block for handling interactions with NVDIMM-N devices.
  - Adapting a TCG SSC standard for accommodating NVDIMM-N class devices
- With industry sponsorship from HPE, NetApp, and others
Cryptographic Components within NVDIMM-N SED

- The NVDIMM-N uses these engines:
  - encrypt and decrypt
    - encrypt/decrypt data using AES
    - XEX with Tweak and ciphertext Stealing (XTS)
      - a block cipher mode is appropriate for the usage model
  - random bit generator (RBG)
    - hardware entropy source seeding a NIST-approved DRBG
    - generates data encryption keys
    - generates salt for PBKDF
  - password-based key derivation function (PBKDF)
    - adds salt from RBG to strengthen the password
    - includes an integrity check value for verifying password
  - key wrap and unwrap
    - wrap/unwrap the DEK using the key derived via PBKDF2
    - Key wrap engine using AES encryption scheme
Standardization Approach
Adding Encryption to the Standards / Specifications

JEDEC BAEBI changes

- Model based on:
  - SCSI Security Protocol IN / OUT commands
  - SATA Trusted Send / Trusted Receive commands
  - NVMe Security Send / Security Receive commands

- Allows maximum knowledge reuse and maximum code reuse

- Uses Registers on the I2C bus for Security related status
  - Existing registers – add new error bits (SECURITY ERROR)
  - New registers – with additional error bits (SECURITY ERROR)
  - New registers for Security Protocol type and Security Protocol Specific field

- New Typed Block Data for Security Protocol data (type 4)
  - Uses existing Typed Block Data transfer protocol
  - 32 Byte Granular buffer lengths
Initializing the NVDIMM
Authenticate via I2C control path; allows DDR data path to be used
NVDIMM Save operation

Power loss triggers encryption and save operations
NVDIMM Unlock and Restore operation

Host re-authenticates and triggers decryption and restore

[Diagram of NVDIMM Unlock and Restore operation]

- NVDIMM controller
- Decrypt
- Hardware AES engine
- Key Derivation Function
- Wrapped DEK
- KEK
- DEK
- Power control
- DDR data path
- I2C
- Data
- Auth Key (AK)
- Typed Block data (4)
- Other cmd/ctl
- Energy Source
- Host (Motherboard)
Adding Encryption to the Standards / Specifications

Trusted Computing Group (TCG)

- Add new Section to TCG Storage Interface Interactions Specification (SIIS)
- Define the mapping of the TCG IF-SEND function to the BAEBI Security Typed Block Data (type 4)
  - Write data to the BAEBI TYPED_BLOCK_DATA_BYTE0 through TYPED_BLOCK_DATA_BYTE31 registers
- Define the mapping of the TCG IF-RECEIVE function to the BAEBI Security Type Block Data (type 4)
  - Read data from the BAEBI TYPED_BLOCK_DATA_BYTE0 through TYPED_BLOCK_DATA_BYTE31 registers
- Discovery
- Error cases (locked vs. unlocked)
Adding Encryption to the Standards / Specifications

Trusted Computing Group (TCG)

- Opal / Ruby / Something else?
- How many ranges? One to start; consider allowing a small number
- 32 Byte password minimum
- One Admin Authority / One or two User Authorities?
- Small DataStore (maybe 128KiB; NOT MiB or GiB – slow access over I2C)
- NO MBR Shadowing
Adding NVDIMM Encryption to Systems

System usage considerations

- You can’t just pull the plug (power off) to force a reset
- You must run code to execute the Security Protocol to cause decryption of the memory contents before you have memory.
- Interleaved DIMMs add additional complexity
- Secure Firmware Update considerations
  - BIOS must have additional awareness beyond just normal SEDs
  - You have to think about these devices a little differently than traditional SEDs.
As evidenced by recent workload trends relating to in-memory databases, AI, and cache acceleration in enterprise storage, which all require large amount of data to be staged in memory.

Data retention during power cycle is an important consideration against which NVDIMM-N class is an appropriate fit.

Data staged in NVDIMM-N devices requires same level of protection as that of SED’s.

We hope encryption standardization for NVDIMM-N devices will enable its wider adoption across PMEM-aware workloads.
Thank You