Security Beyond The SED

Robert Wann

Enova Technology Corporation

rwann@enovatech.com

www.enovatech.com

Santa Clara, CA
August 2016

SED – Self Encrypting Drive

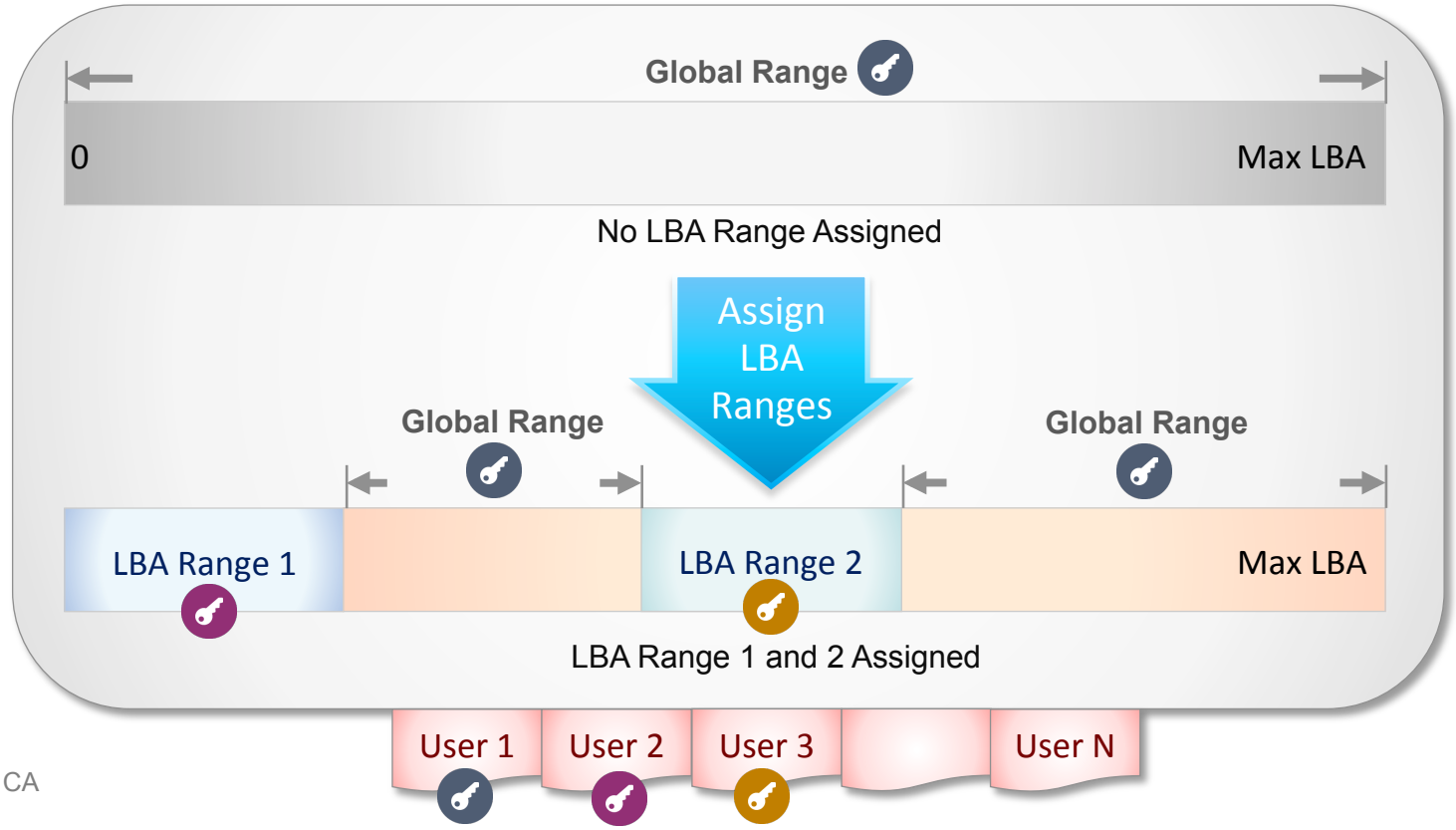
Benefits

- Automatically responds to PIO/DMA read/write data/non-data commands over SATA interface
- Data being written is transparently encrypted whereas data being read is transparently decrypted

Concerns

- Non-unified authentication method and key management
- Workflow that works with multiple vendors and capacities
- Access time to first available data
- Performance degrades when AES CBC/XTS 256-bit is on

What is Opal 2.0?



Can TCG Opal 2.0 Solve These Concerns?

Enhancements over SED

- Strong identity-based authentication method built on top of the SED
- Granular control over disk read/write privilege for any single user of a Locking SP

Presents other issues however

- Opal 2.0 has multiple optional implementations related to security
- Different vendors address Opal 2.0 security features differently – this creates problem for IT staffs that need a unified solution to work with mixed legacy/existing and expansion products
- The authentication method is encoded but not encrypted

What about the eDrive?

An eDrive can be internally a -

- Boot Drive, or
- Data Drive

Alternatively, an eDrive can be a USB3.0/3.1-to-SATA portable drive

An eDrive constitutes three major functions:

- Transparent Hardware Full Disk Encryption or Self Encrypting Drive
- TCG Opal 2.0 Firmware
- IEEE 1667 Firmware

All concerns with SED/Opal 2.0 remain with several enhancements when Microsoft BitLocker (MBAM) engages to manage through 1667 & Opal 2.0 interfaces; BitLocker in this case yields the heavy duty encryption work to the SED.

Vision - Longer Industrial Life For Embedded Appliances

- A hardware controller that manages all aspects of security features ***internally*** to simplify the design of your appliances by enabling:
  - In-line 6Gbps AES XTS/CBC/ECB 256-bit crypto performance
  - Identity-based or role-based authentication method with payload being encrypted and signed
  - RSA or ECC public/private keys generation, verify and sign so as to create a trusted relationship among all computing tiers
  - message digest and signature, challenge and response protocols such as HMAC and CMAC
  - automatically transforming any drive capacities to SED, Opal 2.0 or eDrive so as to facilitate same access point to the mixed legacy/existing and expansion products for timing critical applications

The *X-Wall MX*+ eDrive Controller

- In-line 6Gbps AES XTS/CBC/ECB 256-bit crypto performance
- TCG Opal 2.0 & IEEE 1667 Firmware
- Fast secure erase in less than a millisecond
- RSA 2048, HMAC, CMAC, SHA256, Hash_DRBG RNG