TCG Storage Workgroup Status Update

SWG Update

Chandra Nelogal (DELL) and Joseph Chen (ULINK)

Agenda

- Introduction
- Learning Objectives
- Status Update
  - Various standards documents
- Upcoming plans
- Other sessions

Introduction

- We represent the TCG (Trusted Computing Group)
  - TCG Covers many things security
  - Trustedcomputinggroup.org
- Storage Work Group
  - Focuses on security features specific to storage devices and solutions
  - Data at rest security specifications (SSCs)
    - Security Subsystem Classes
    - Enterprise, Opal, Ruby, Pyrite
  - Storage Interface Interactions Specification (SIIS)
  - Feature sets, supplementals to SSCs
    - CNL, CNL SUM, Configurable PINs, Block SID, etc.

Learning Objectives

- Get an overview of the current activities w.r.t. standards
- Get a preview of upcoming standards activities
- Security trends in storage
- Help plan for your security features and capabilities
  - For your organization's products and solutions
- Welcome your participation and input

Core, SSC, and SIIS Specification

Chandra Nelogal

Chandra Nelogal

1. Core and SSCs
    a. Enterprise SSC
    b. Opal 2.02
    c. Pyrite 2.0
    d. Ruby
    e. Key Per I/O
2. SIIS
    a. SIIS 1.10
    b. SIIS 1.11

Status of SSCs

- Core spec – Last updated in 2015
  - No outstanding items being tracked
- Enterprise – Last updated in 2015
  - No outstanding items being tracked
- Opal SSC – 2.02 – just completed public review
  - Main changes from previous version (2.01, released 2015)
  - Changes to LockOnReset, DoneOnReset
    - Allows for hardware reset, in addition to power cycle and programmatic resets
  - Changes – reporting estimated time for data removal mechanisms
    - GenKey, Revert, RevertSP
  - Manufactured-Inactive state is mandatory
  - Block SID support is mandatory
  - Various clean up and updates based on TC comments
- Ruby
  - Published in Jan, 2020
  - No outstanding items being tracked for this SSC
- Pyrite
  - Updated in May, 2020
  - No outstanding items being tracked for this SSC

Under Development

- Key Per I/O
  - Key insertion and management per I/O request
  - Specification under development
  - Please attend/listen to the Key Per I/O focused session for more details

SIIS Updates

- SIIS 1.10 – completed public review
  - Previous version SIIS 1.09 – released in Dec 2020
  - Main changes – touching upon various commands and details
    - A newly defined SIIS feature descriptor – main point is a flag to define write pointer behavior related to zoned namespace commands
    - NVMe MI – subsystem reset
    - NVMe Namespace Write Protection – if an NS is write protected, TCG methods will fail
    - NVMe Compare and Verify commands – will fail if the LBA range is readlocked
    - NVMe Copy command – will fail if the source is read locked and/or the destination is write locked
- SIIS 1.11
  - Some considerations (not final or plan of record)
    - NVDIMM-N
    - Sanitize and Format NVM clean up
    - Interactions with firmware update
    - Reservations
    - Other items as they are brought up

Features and Test

Joseph Chen

Joseph Chen

1. Features
    a. Block SID Authentication
    b. CNL
    c. CNL App Notes
    d. CNL/LUN
    e. CNL and SUM
    f. Shadow MBR for Multiple Namespaces
    g. Configurable PIN Length
2. Test
    a. Test Cases
    b. Test Suite
    c. Certification

Block SID Authentication Updates

- Block SID Authentication v1.00 r1.00 was published in August 2015
- Block SID Authentication v1.01 r1.00 was published in Feb 2021
  - Added Locking SP Freeze Lock Support and State
  - Added new life cycle state called “Manufactured-Frozen”
  - Defined the interaction of Manufactured and Manufactured-Frozen states
- Allow the Locking SP to be frozen to prevent malicious software attack

Configurable Namespace Locking Feature Set Updates

- Configurable Namespace Locking (CNL) v1.00 r1.00 published in Feb 2019
  - Define the initial operation for the CNL, Assign and Deassign and Set methods
  - Define Namespace Global Range Locking Object and Namespace Non-Global Range Locking Object
- CNL Application Note v1.00 r1.00 published in Jan 2020
  - Show CNL examples and use cases
- Configurable Locking for NVMe Namespaces and SCSI LUNs v1.01 r1.00 recently published
  - Added Configurable Locking support for the SCSI LUNs in addition to the NVMe Namespaces
- Configurable Locking for NVMe Namespaces and SCSI LUNs v1.02 r1.xx under internal review
  - Added support for the Single User Mode (SUM) SUM_C and AssignToSUMRange

Configurable Locking for NVMe Namespaces and SCSI LUNs

- NVMe Namespaces
  - Assign/Deassign and Set methods

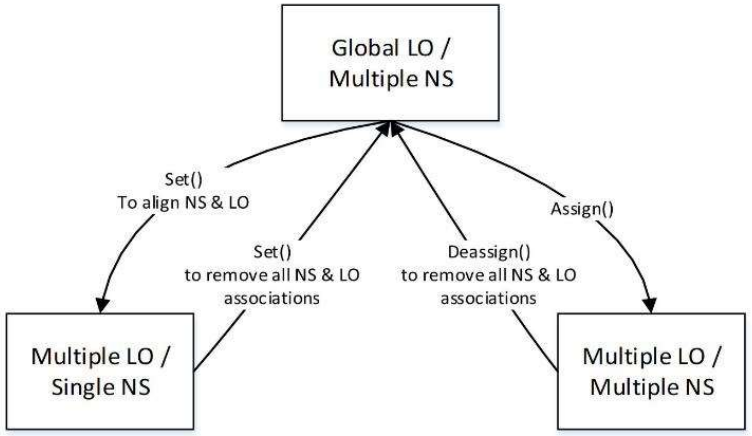


Figure 1 - Locking SP Modes (NVMe)

- SCSI LUNs
  - Assign/Deassign method

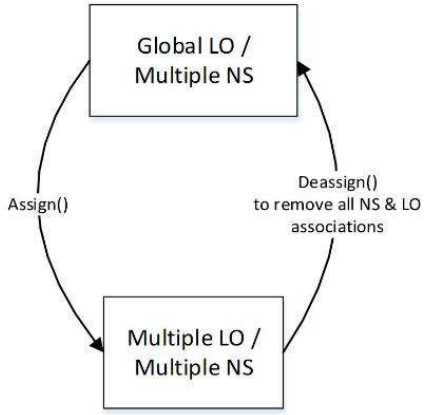


Figure 2 - Locking SP Modes (SCSI)

Configurable Locking Objects

- Global Range Locking object
  - Any namespace or LUN that is not associated with below
- Namespace Global Range Locking object
  - First Locking object to be associated with a Namespace/LUN
- Namespace Non-Global Range Locking object
  - Locking object associated with an LBA range within a namespace/LUN

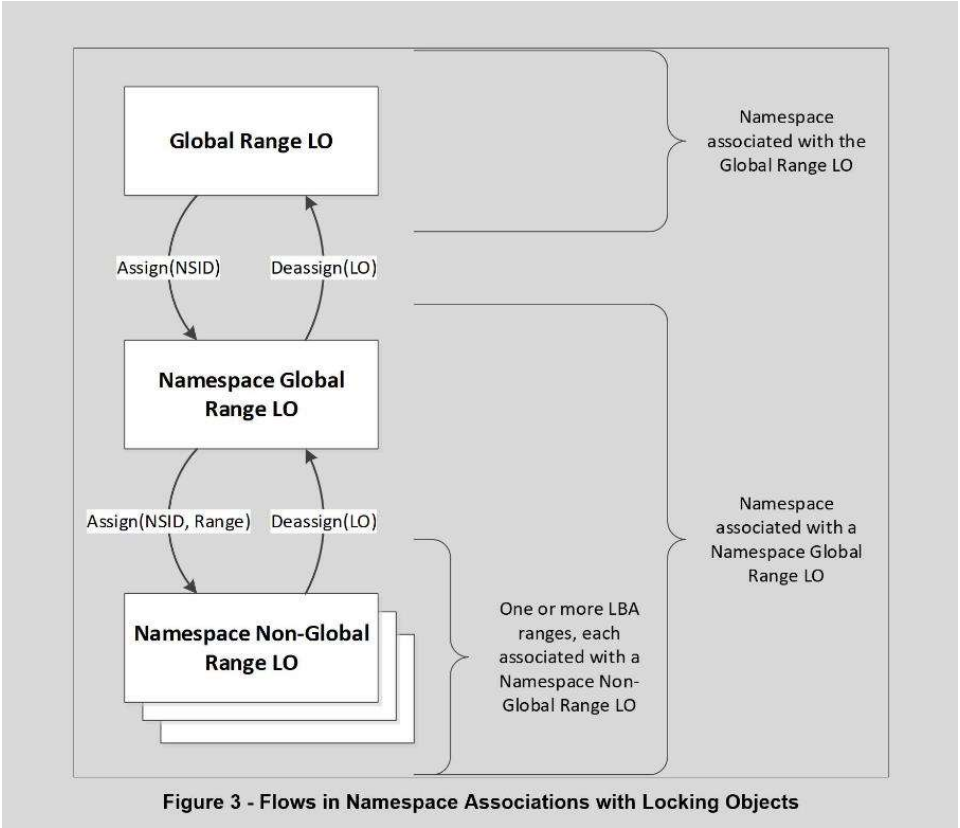
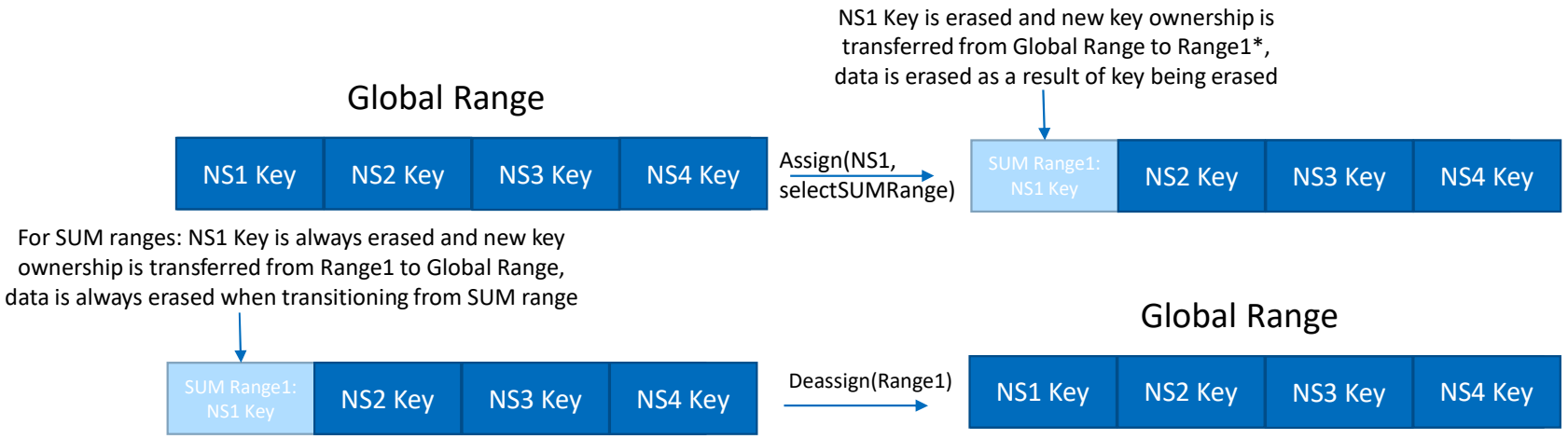


Figure 3 - Flows in Namespace Associations with Locking Objects

SUM & CNL Proposal in v1.02

- Add parameter to Assign to indicate caller wants to associate Namespace with an available SUM range
- Mandate:
  - Assign to SUM Range results in erase of data
  - Deassign from SUM Range results in erase of data
    - KeepNamespaceGlobalRangeKey = True results in failure of Deassign method



Shadow MBR for Multiple Namespace Updates

- Shadow MBR for Multiple Namspaces v1.00 r1.21 published on Oct 2020
- Defines rules for the MBRControl.NSID
  - Default value of MBRControl.NSID shall be 0x0000_0000 or 0xFFFF_FFFF, or existing namespace.
  - When MBRControl.NSID is equal to 0xFFFF_FFFF, the MBR and MBRControl tables in the Locking SP are shared by all namespaces and controllers within the NVM subsystem.
  - When MBRControl.NSID is equal to existing namespace, the MBR and MBRControl tables in the Locking SP are assigned to only the existing namespace; meaning MBR shadowing are applied to single namespace
- Rules of MBRControl.NSID
  - Set method for MBRControl.NSID of non-existing namespace except 0x0000_0000 shall fail
  - Support of Set method for MBRControl.NSID of 0xFFFF_FFFF is optional.
  - If MBRControl.NSID is equal to 0x0000_0000, Set method for MBRControl.Enable of TRUE shall fail
  - If MBRControl.Enable is equal to TRUE, Set method for MBRControl.NSID of non-existing Namespace including 0x0000_0000 shall fail

Other SWG Features Updates

- C_PIN Enhancements Feature (optional feature)
  - Configurable C_PIN TryLImit per Authority
  - Configurable C_PIN Persistence per Authority
  - Min and Max PIN length
- C_PIN Forced PIN Change (optional feature)
  - When enabled, requires the Authority PIN change before the authentication
  - Forced PIN change by allowing only Set method on the PIN column and Random method

Test and Certification Updates

- TCG Storage Workgroup Certification Program
  - TCG Storage Opal Family Test Cases Specification was published in April 2019
    - Test specification covers Opal family product such as Opal, Pyrite, and Ruby SSC
  - Certification Program version 2.0 was published in August 2020
    - Require completion of Compliance Test and Security Evaluation
    - Certification for TCG members
- Test Suites and Test Houses
  - Test Suites and Test Houses were approved in Nov 2020
    - Opal SSC Test Suite 4.0 is the approved Test Suite
    - ULINK is the approved Test House
- Storage Certified Products
  - The storage certified products were published on the TCG webpage

Other Sessions

- Please join the TCG SWG Key Per I/O presentation for the latest development status of the specification

