Using Self-Encrypting Storage Devices Today and Tomorrow

Tim Markey

Firmware Security Engineer

SandForce

Presentation Overview

- Brief overview of Trusted Computing Group (TCG) Self-Encrypting Drive (SED) architecture
- How can different SED use models address various security requirements
- Possible development of self-encrypting storage in near future

TCG Storage Workgroup

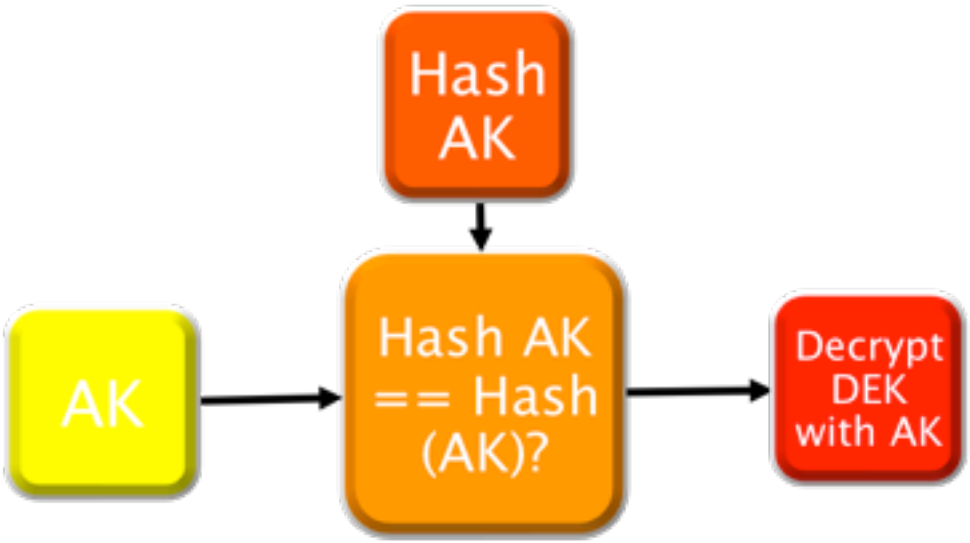
- Subsystem Classes Specifications (SSC).
  - Opal
    - Desktops / Notebooks in Corporate Environment
  - Enterprise
    - Servers / Data Centers

LBA Range Locking

- Multiple LBA Range Locking
- Global Range
- AES Encryption Mode – 128/256
- Read/Write, Lock Enabled/Locked
- Lock on Reset

LBA Ranges + Global Range

Data Encryption Key Binding



AK = Authentication Key
DEK = Data Encryption Key

TCG Opal SSC

- For Laptop / Desktop Systems in Corporate Environment
- Defined Admin / User Roles
- Minimum of 4 ranges + Global (Opal 1.0).
- Shadow MBR (128 MB)
- Crypto-Erase

TCG Enterprise SSC

- Data Center and Server Environment
- Single “Bandmaster” Role
- Minimum 1 range + Global.
- Multiple Initiator Support
- Crypto-Erase

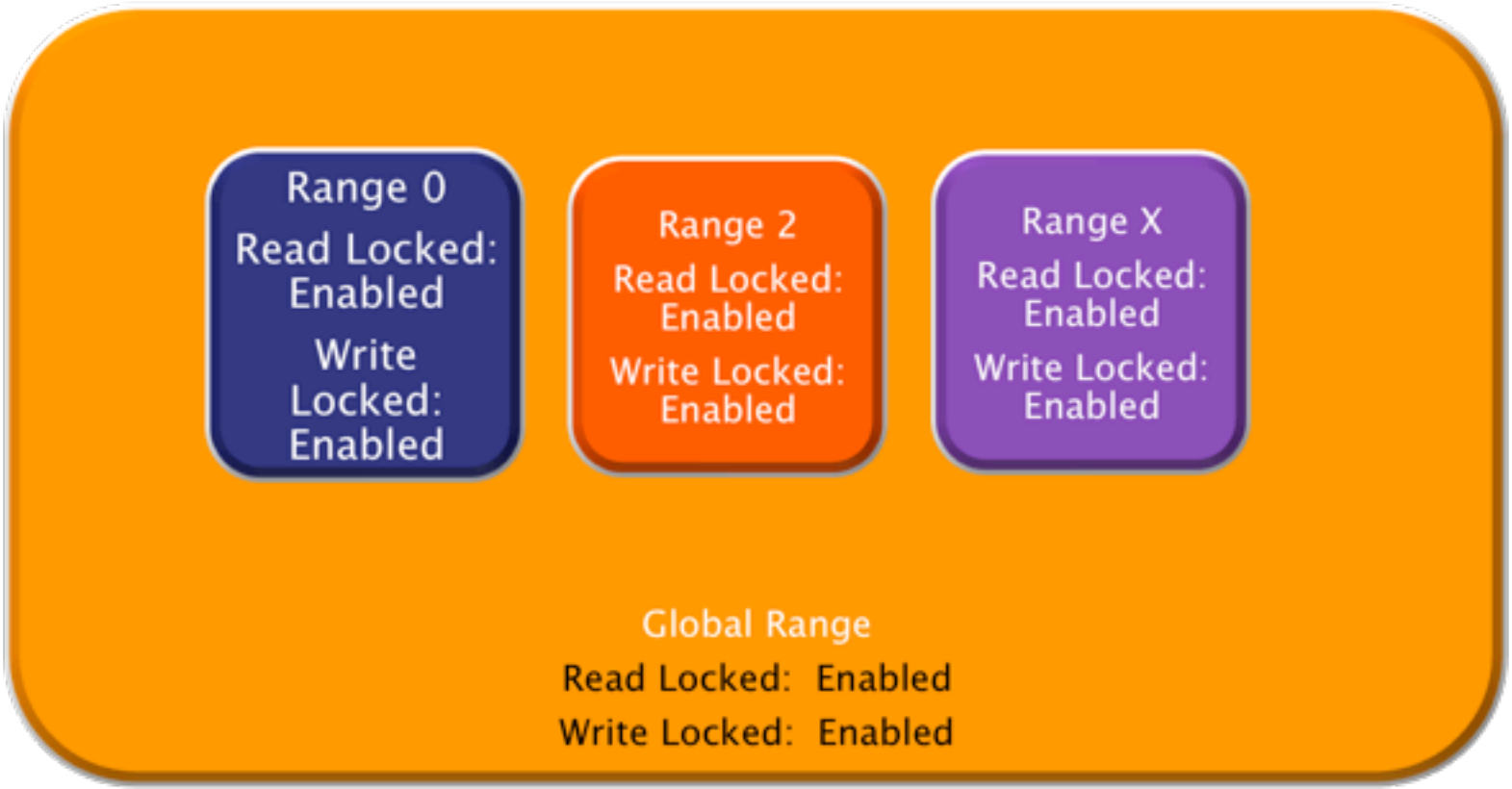
Opal vs. Enterprise

SSC	Min Ranges	Roles	Shadow MBR	Use
Opal	4 + Global	User / Admin	Yes	Corporate Laptop/
Enterprise	1	Bandmaster	No	Enterprise Servers

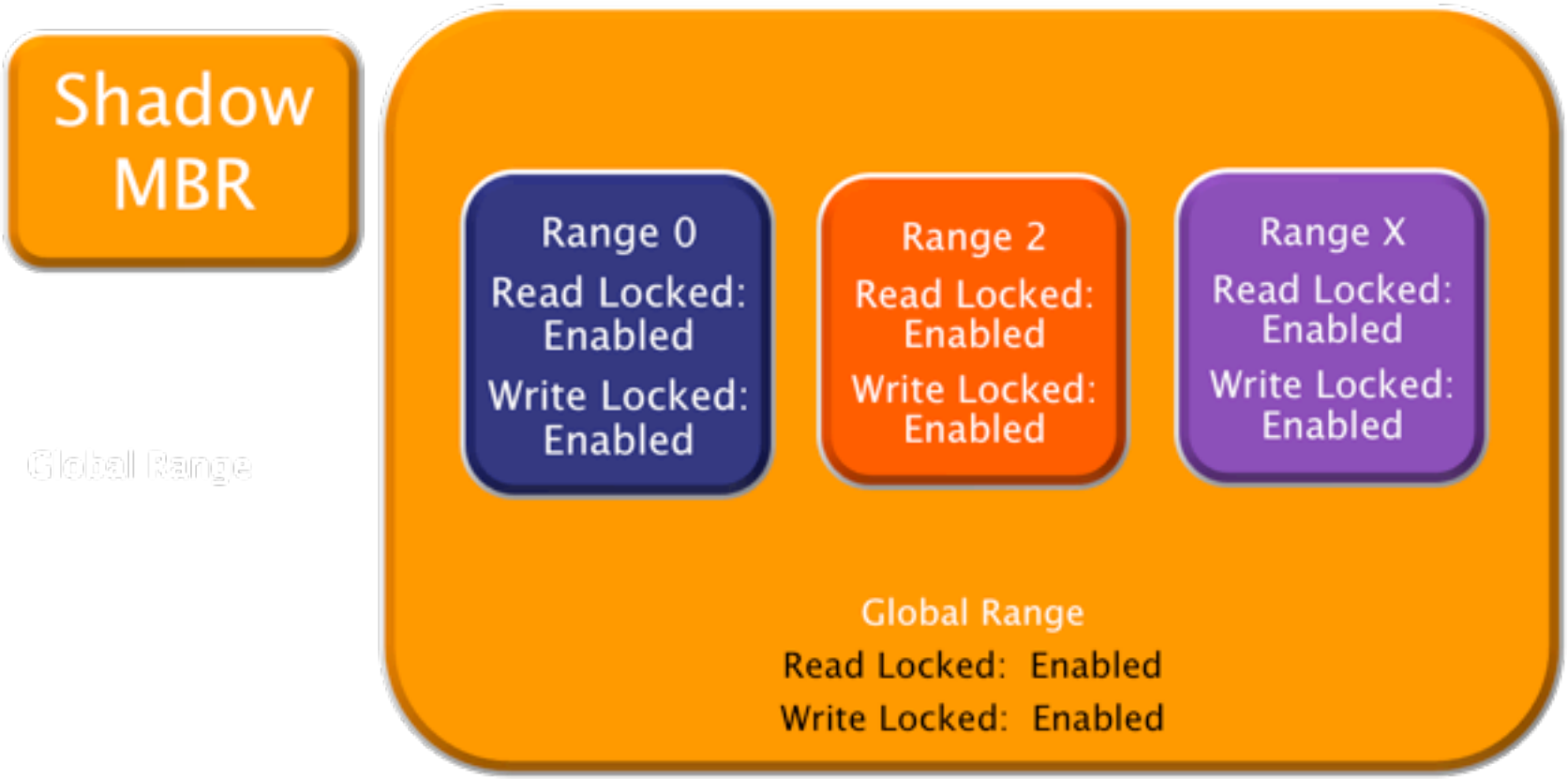
SED Use Models

- Basic protection modes
- Transparent encryption with crypto erase
- Multi user storage
- Open O/S with Secure Partition
- Secure OS example

Use Case #1 – Basic Enterprise



Use Case #1 – Basic Opal



Use Case #2 -Transparent Encryption

- Crypto erase only
- Opal (no MBR) or Enterprise
- 1 unlocked LBA range
- No lock on reset

Range X

ReadLockEnabled: Disabled
WriteLockEnabled: Disabled
Read Locked: Disabled
Write Locked: Disabled

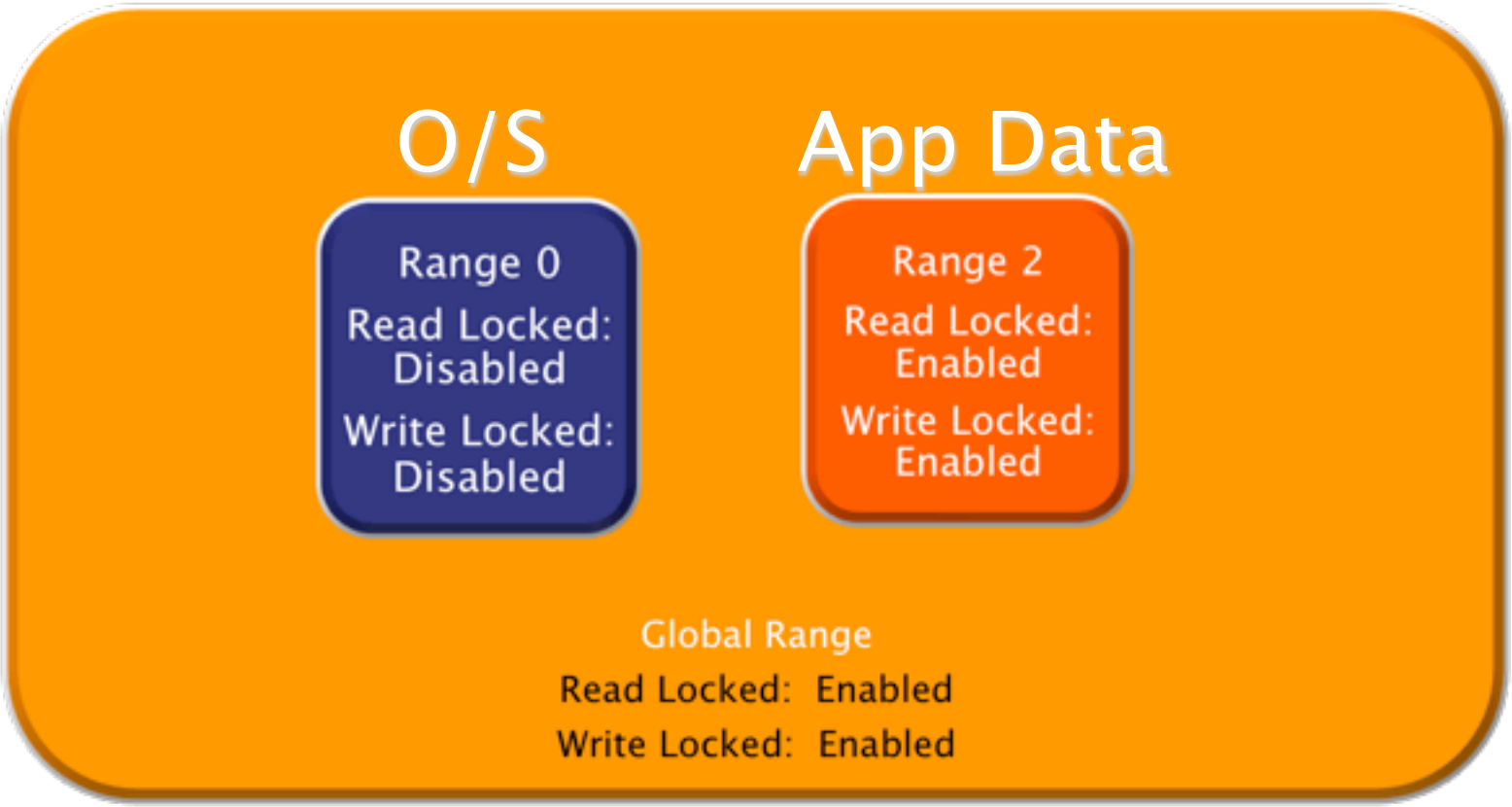
Use Case #2 –Transparent Encryption (Advantages / Disadvantages)

- Advantage:
  - Crypto-Erase without overhead
- Possible Uses
  - Opal – Sending a system back for repair
  - Enterprise – Repurposing the whole drive or a band.
- Disadvantage:
  - No User Authentication. If Drive is lost / stolen, data is compromised
  - Still requires software to Manager the Erase

Use Case #3 – Open O/S w/ Secure Partition

- O/S Boots Unlocked Range or Shadow MBR
- O/S retrieves PIN from locked Blob locked using TPM PCR registers
- O/S unlocks main LBA Range using retrieved PIN
- Advantage: Prevents Boot Viruses
- Disadvantage: No User Authentication

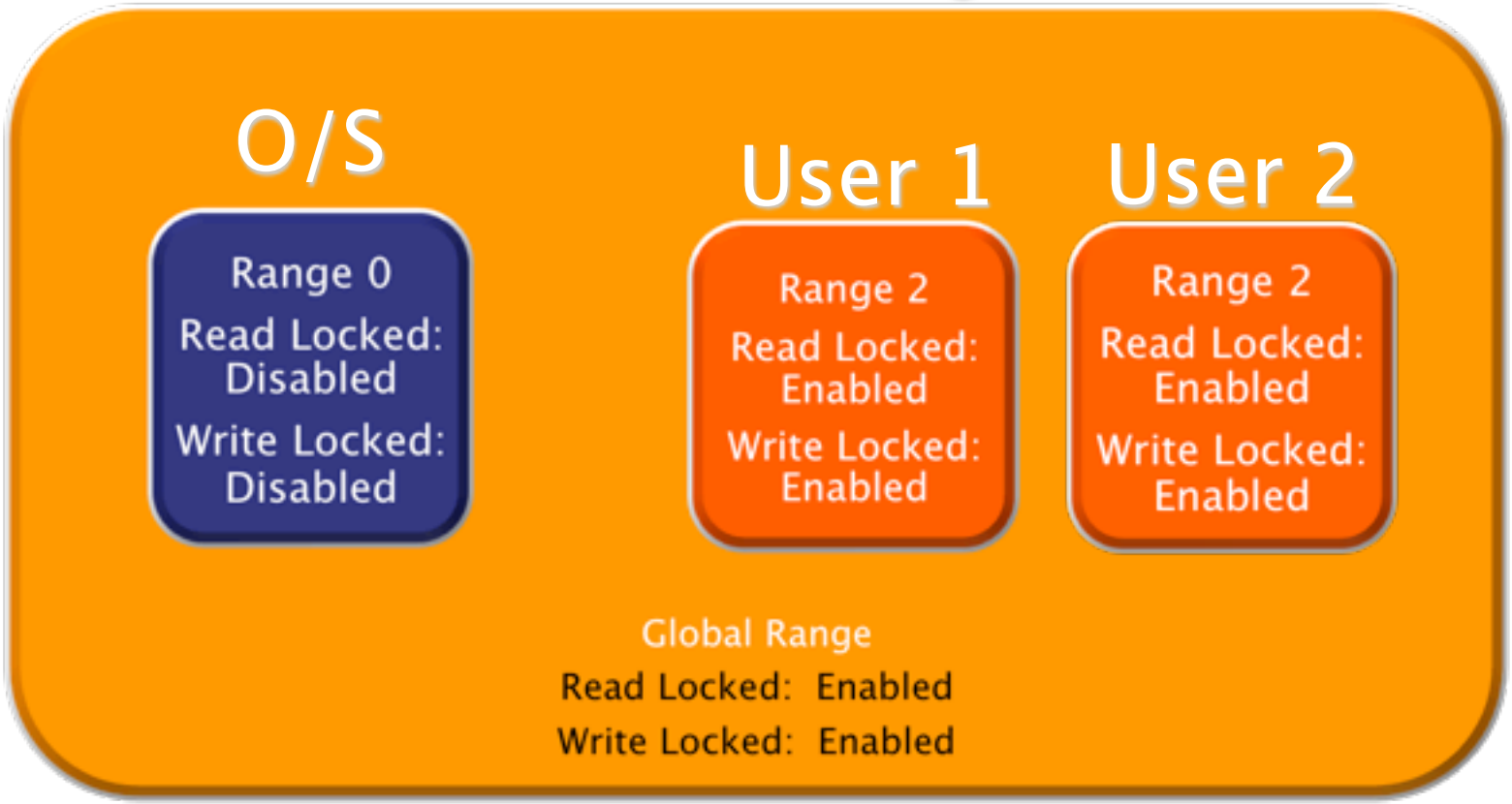
Use Case #3 – Open O/S w/ Secure Partition



Use Case #4 – Multi user storage

- Multi user storage
- Opal or Enterprise
- 1 global range, 1 O/S Range, Multiple User Ranges.
- Lock on reset
- Possible Use: Shared Corporate Computer.
- Advantage: Secure User Space.
- Disadvantage: No User Authentication. If Drive is lost / stolen, data is compromised.

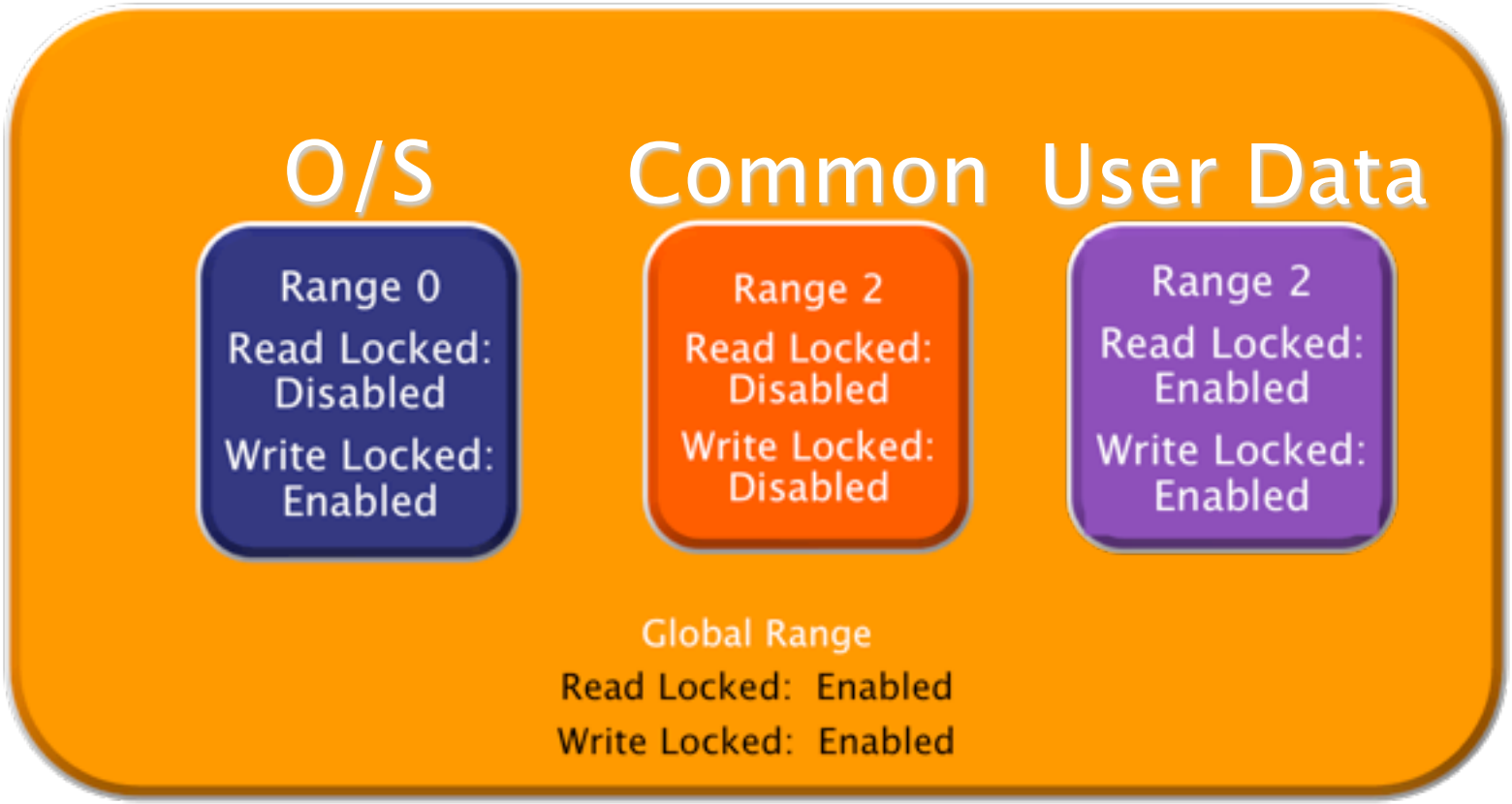
Use Case #4 – Multi-User Storage



Use Case #5 – Secure O/S

- Opal or Enterprise
- 1 global range, 1 read-only bootable O/S Range, 1 Open Range, 1 or more Locked Ranges.
- Lock on reset
- Possible Use: Shared Corporate Computer.
- Advantage: Boot O/S cannot be modified (no boot virus).
- Disadvantage: No User Authentication. If Drive is lost / stolen, data is

Use Case #5 – Secure O/S



Future SED developments

- Tampering sensors
  - Automatic lock on tamper trigger
  - Could be tied to external signal, such as case opening or movement of drive
  - Drive remains locked until Power-Cycle / Re-authentication / Tamper-Condition is removed.

Visit the SandForce Exhibition Booth

World-class reliability, performance, & power efficiency for enterprise, client, and industrial SSD applications

- Visit us at **booth #407** to see our DuraClass™ technology in action with the latest 24nm MLC flash technology and new non-HDD form factors like the JEDEC MO-300

- Stop by to enter our **free drawings** to win one of many different SandForce Driven SSDs from Corsair, Kingspec, Kingston, OCZ, OWC, Patriot Memory & Viking
  - Free drives given away approximately every 30 minutes!

- See other SandForce Driven™ SSDs in our partners' booths

- Visit the many SandForce Trusted™ SSD ecosystem members