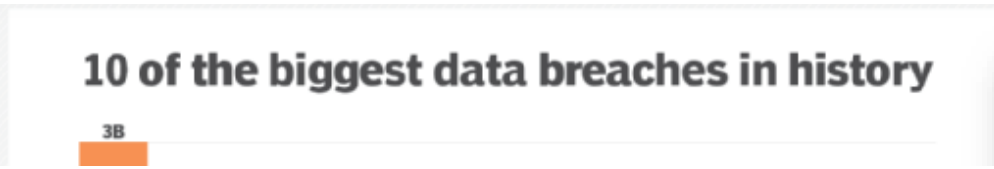
Securing Computational Storage for the AI Era

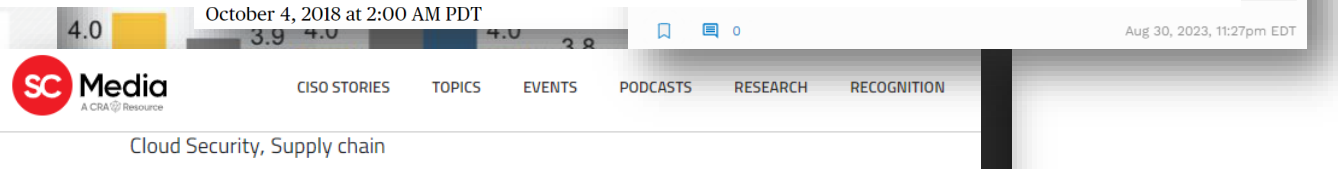
Jason Molgaard
Principal Storage Solutions Architect
SOLIDIGM

Technical Council Co-Chair
SNIA®

FMS the Future of Memory and Storage

Security is a HUGE Concern



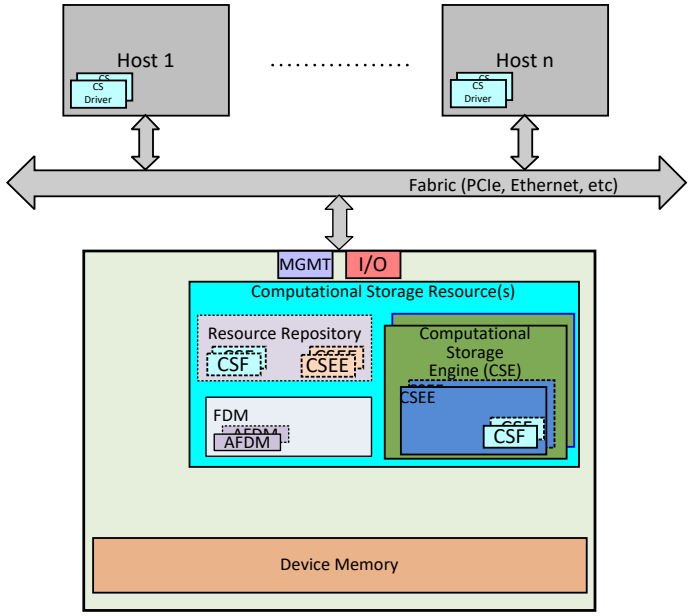


For many industries (e.g. eCommerce, financial services, and others) ***encryption at rest*** *and* ***in flight*** *are no longer advanced capabilities, but* ***table stakes*** *for any cloud storage supplier. –* ***StorageNewsletter.com, 1/3/2024***

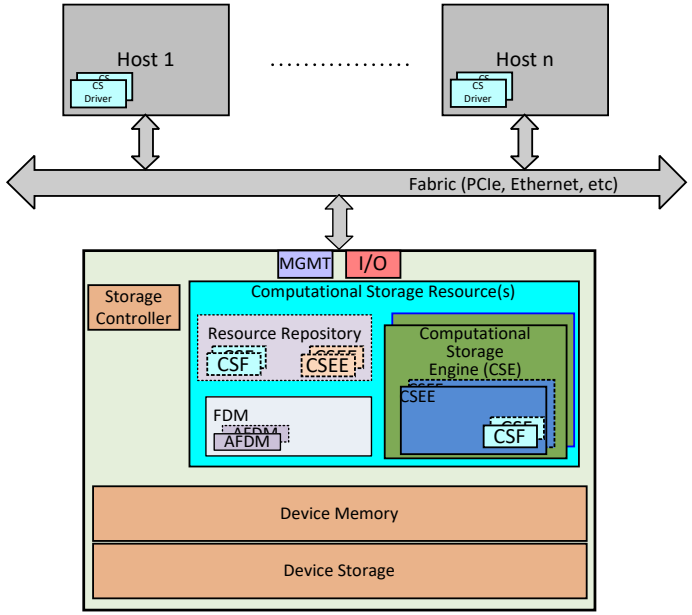
What about security for Computational Storage?

Key SNIA CS Security Concepts

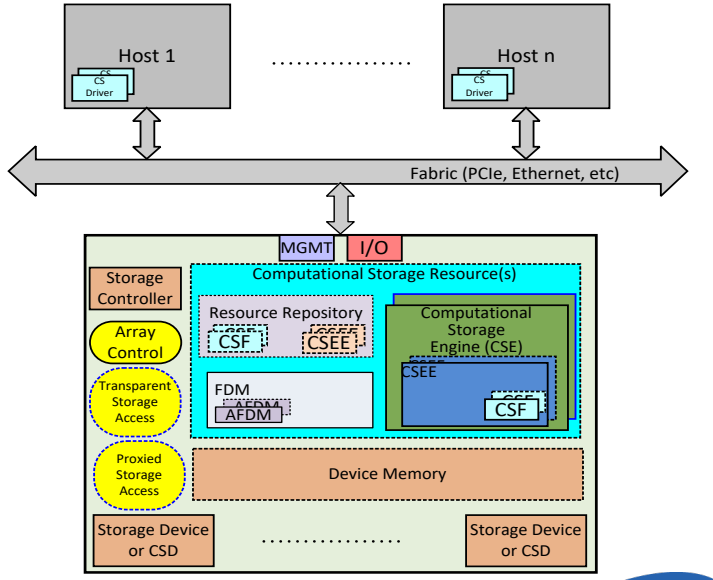
- SNIA Architecture outlines security Recommendations
- SNIA Security Assumptions
  - The environment consists of multiple physical or virtual hosts with one or more CSxes
  - CSx security requirements are comparable to the security requirements common to SSDs/HDDs in multi-tenant environment



Computational Storage Processor (CSP)



Computational Storage Drive (CSD)



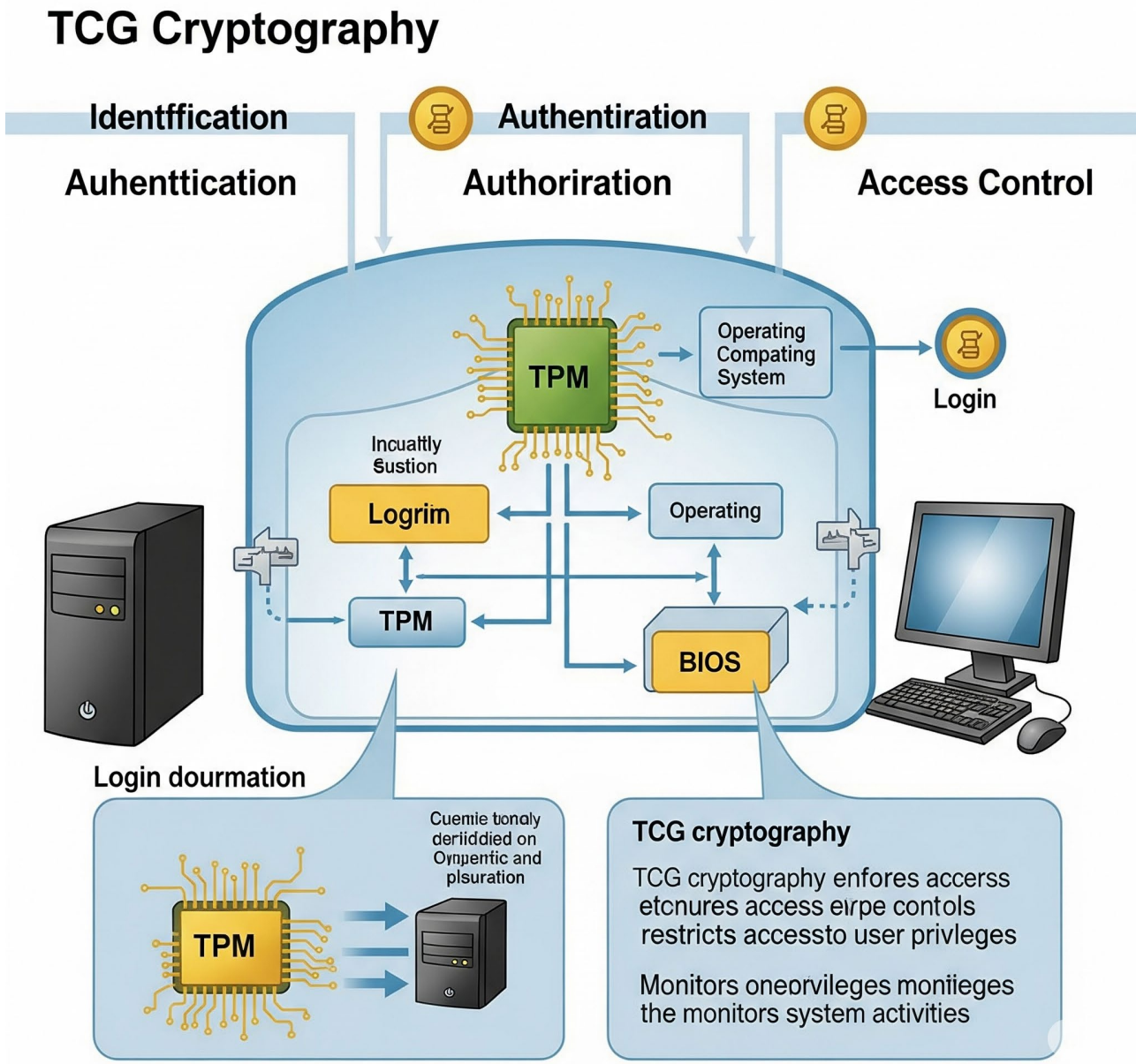
Computational Storage Array (CSA)

Analyzing SNIA CS Security Recommendations

- Security requirements for CSxes are comparable to the security requirements of traditional SSDs and HDDs in a multi-tenant environment
  - Yes, the attack surface may be different, but security needs are unchanged
  - Computational Storage must address the added attack surfaces
- Leverage existing SSD and HDD security techniques and methodologies

Realizing the SNIA CS Security Recommendations

- Establish a Trust Relationship with the CSD resources (CSF, CSEE, CSE)
  - Leverage public key cryptography, as specified by TCG, to perform:
    - Identification
    - Authentication
    - Authorization
    - Access Control



Extending Beyond the SNIA CS Security Recommendations

CSD Software or Firmware	• Validate the download in the same manner as traditional drive firmware updates • Verification of the digital signature of the download
Downloadable CSFs	• Validate the download in the same manner as drive firmware updates • Verification of the digital signature of the download
Pre-Installed CSFs	• CSD Firmware may want to perform attestation of the CSF to ensure it is valid

Additional Considerations

Separation

- Should CSFs be isolated from normal drive functions?
  - Consider dedicated and separate compute resources
  - Consider leveraging CPU privilege levels

CSF Source

- Should CSFs be internally developed only (closed market)?
- Should there be a “CSF Store” similar to the iOS/Android stores?

Call to Action

- **CSx security is imperative**
- The SNIA CS Architecture lays the groundwork for security
  - Defines trust relationships
- Existing methodologies can be applied to augment the SNIA CS Architecture security recommendations
  - Validation of downloads (firmware/software/CSFs)
  - Attestation of pre-installed CSFs
- Implement security solutions in your CSx developments
- Discuss the “CSF Store”

JOIN THE EFFORTS WITHIN SNIA