



SNIA[®] STORAGE
SECURITY SUMMIT
Wednesday, May 11, 2022 • Virtual

Computational Storage: Security Call to Arms and Opportunities

Bill Martin
Jason Molgaard



A SNIA[®] Event

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
 - Any slide or slides used must be reproduced in their entirety without modification
 - The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

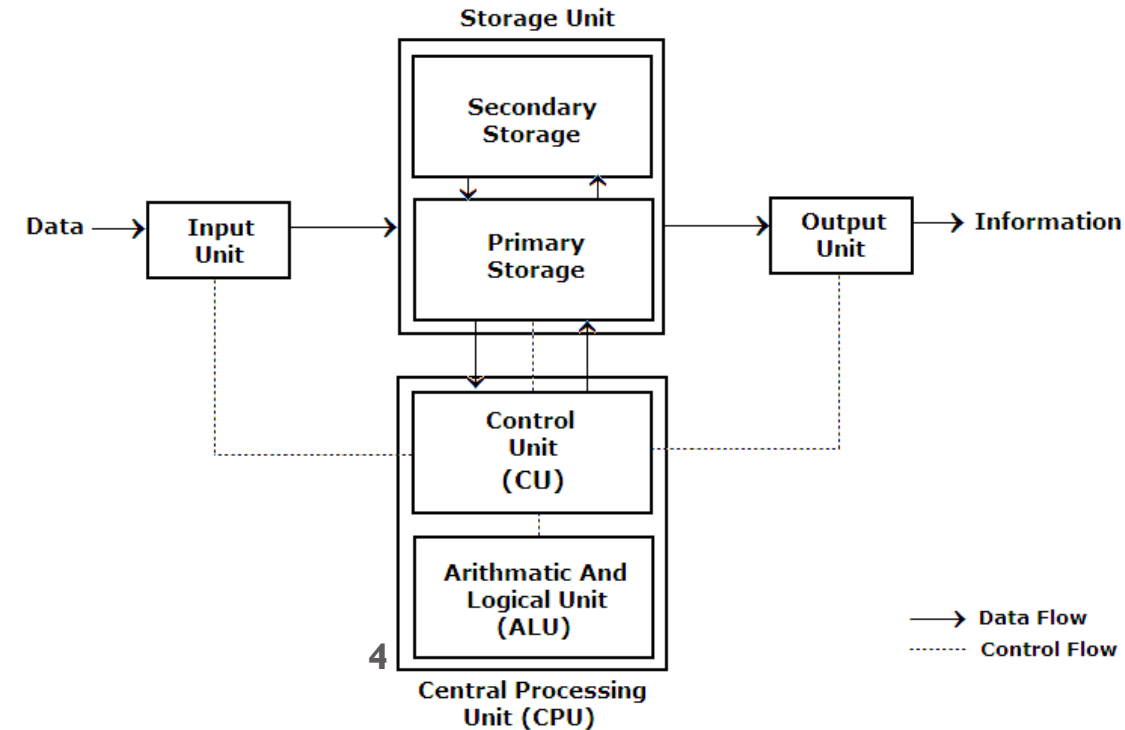
NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.



What is Computational Storage

Compute, Meet Data

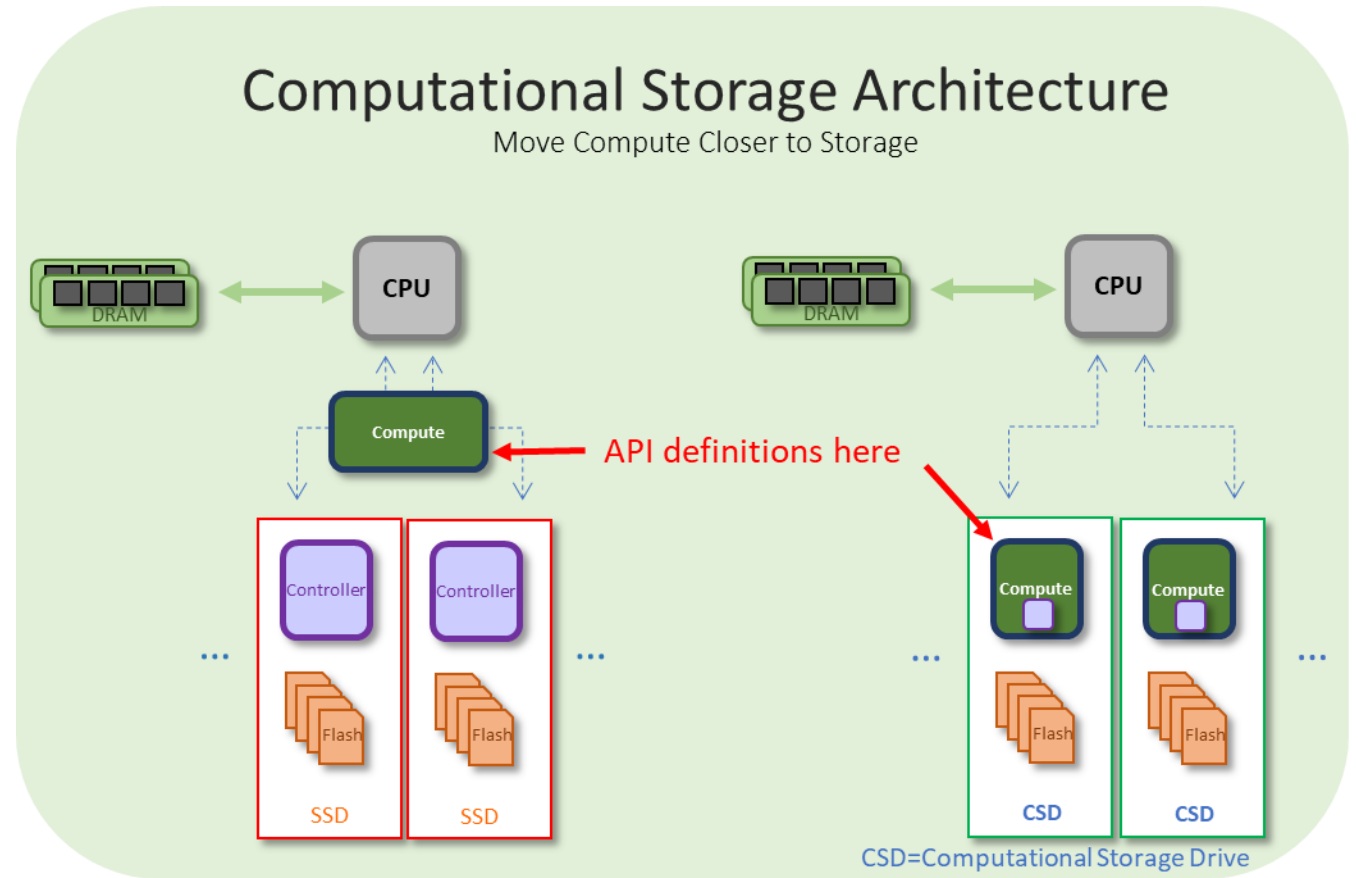
- Based on the premise that storage capacity is growing, but **storage architecture has remained mostly unchanged** dating back to pre-tape and floppy...



Introducing Computational Storage

Computational Storage:

Architectures that provide Computational Storage Functions coupled to storage, offloading host processing or reducing data movement.



Speaking the Same Language

- Foundational Constructs

- Computational Storage Devices (CSx)

- Computational Storage Processor (CSP)


- Component that contains one or more CSEs for an associated storage system without providing persistent data storage

- Computational Storage Drive (CSD)

- Storage element that contains one or more CSEs and persistent data storage

- Computational Storage Array (CSA)

- Storage array that contains one or more CSEs

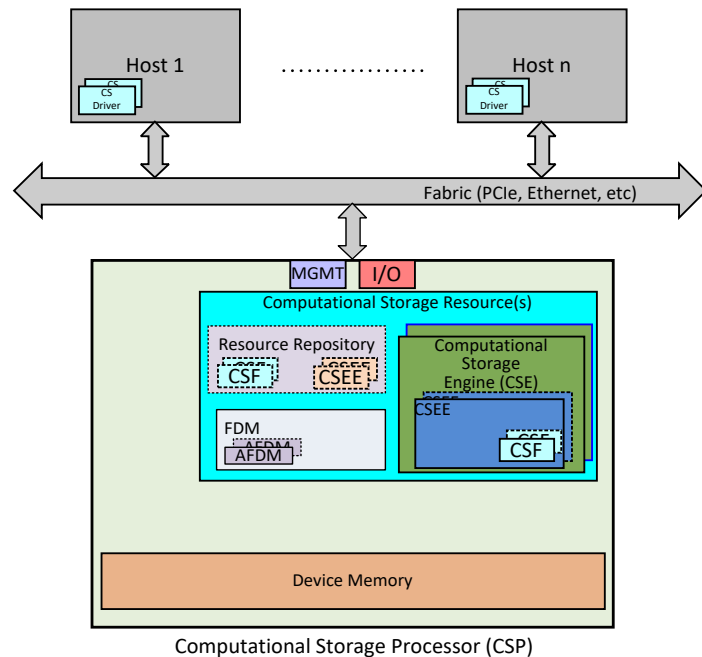


“NO,
(USAGE)
def.i-ni-tion /,c
that says exactly
definition in a
with a satisfac
nition if some
nition, it must
type have it: A
definition, not
thing such a
nition The

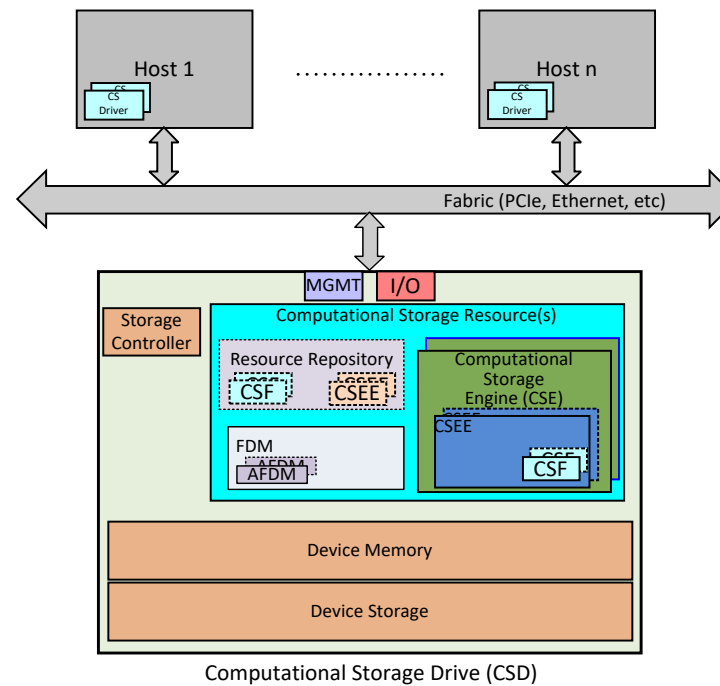
Computational Storage Architecture

Architecture Overview

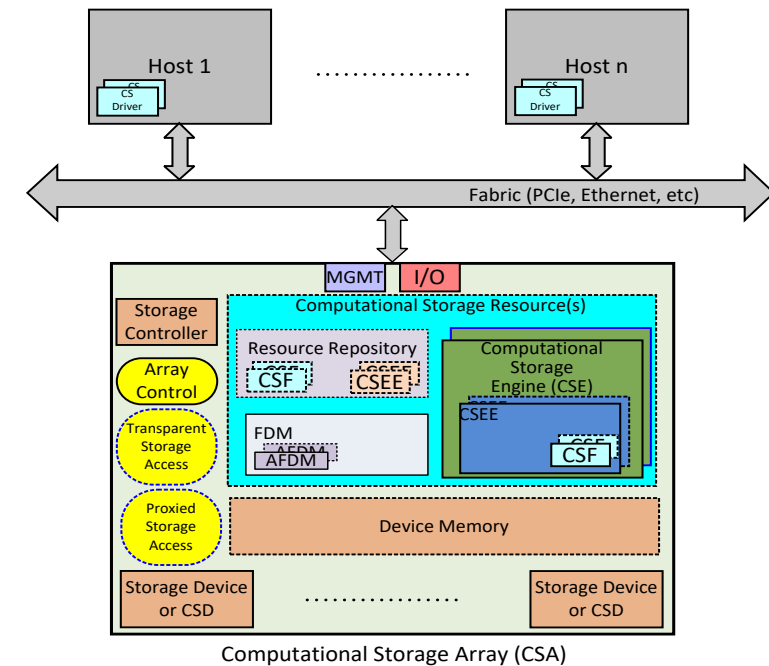
Computational Storage Processor



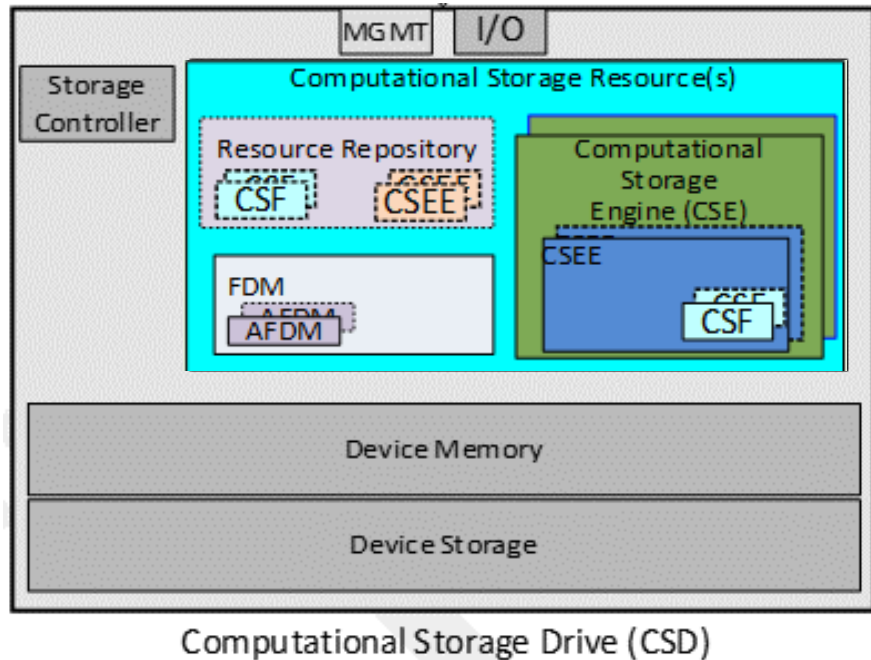
Computational Storage Drive



Computational Storage Array



A Deeper Dive of the CSx Architecture



CSR - Computational Storage Resources are the resources available in a CSx necessary for that CSx to store and execute a CSF.

CSE - Computational Storage Engine is a CSR that is able to be programmed to provide one or more specific operation(s).

CSEE - A Computational Storage Engine Environment is an operating environment space for the CSE.

CSF - A Computational Storage Function is a set of specific operations that may be configured and executed by a CSE.

FDM - Function Data Memory is device memory that is available for CSFs to use for data that is used or generated as part of the operation of the CSF.

AFDM - Allocated Function Data Memory is a portion of FDM that is allocated for one or more specific instances of a CSF operation

Computational Storage Drive Model – Host Loaded CSEEs with CSF

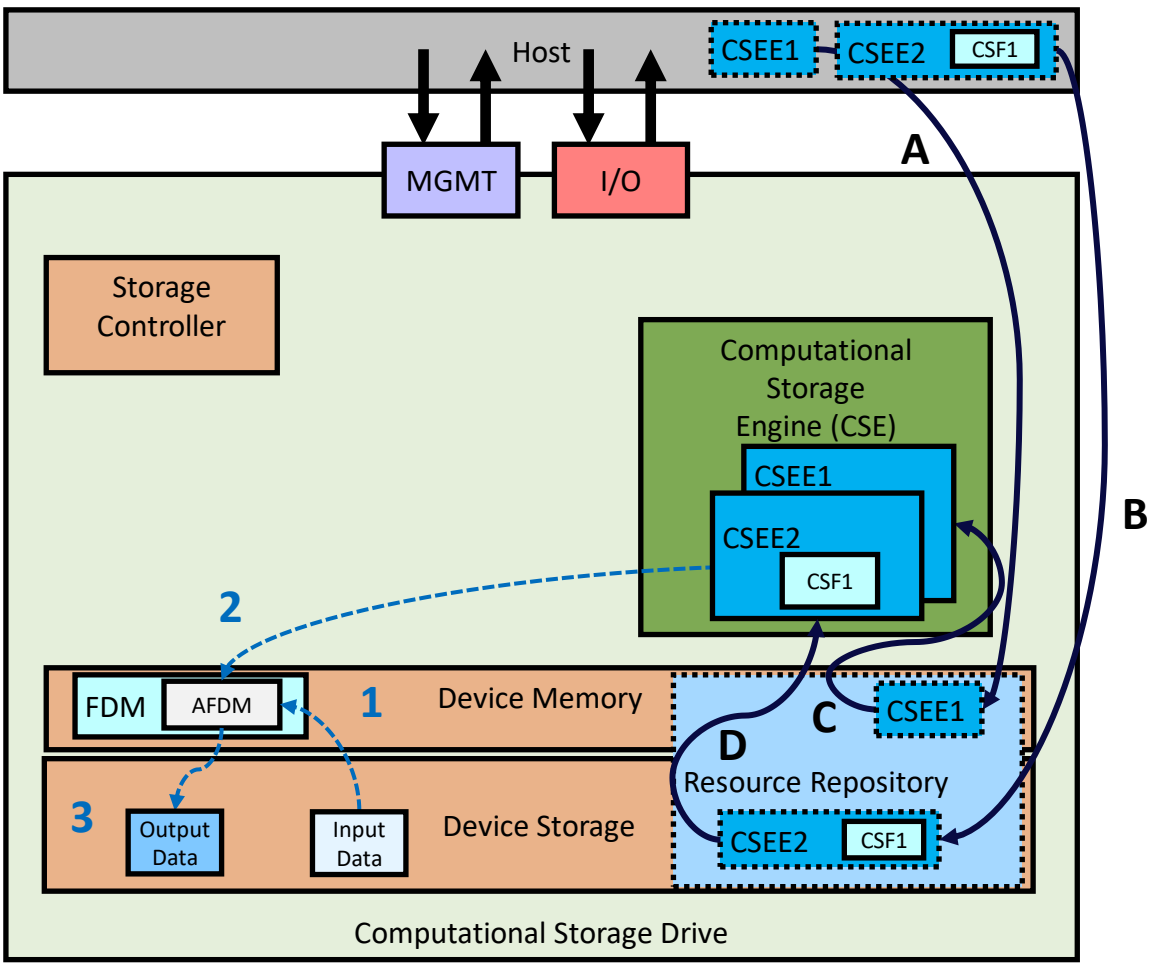
Example for ‘Host Downloaded’ CSEE (memory and storage) and CSF

Configuring to use CSF

- A – Download CSEE1 from Host to Memory
 - B – Download CSEE2 from Host to Storage with CSF1
 - C – Load and Activate CSEE1 from Memory
 - D – Load and Activate CSEE2 from Storage
- Execute CSF1 within the configured CSEE2

Memory Usage Steps

- 1 – AFDM within FDM is loaded from storage by CSF
- 2 – CSF executes the function on data in AFDM
- 3 – CSF returns data to storage after function completes





Possible areas of Security Concerns that Computational Storage raises



Possible areas of Security Concerns that Computational Storage raises

Near Term

Fully Constrained System

- The environment consists of a single physical host or virtual host with one or more CSxes
- That host is responsible for the security of the ecosystem that the CSxes operate within
- Physically secure attachment between host and CSx
- CSx-security requirements are comparable to the security requirements common to SSDs/HDDs and are managed under current SSD security paradigm (e.g., TCG Opal drive)
- This system relies on the host and existing SSD security paradigms to provide security



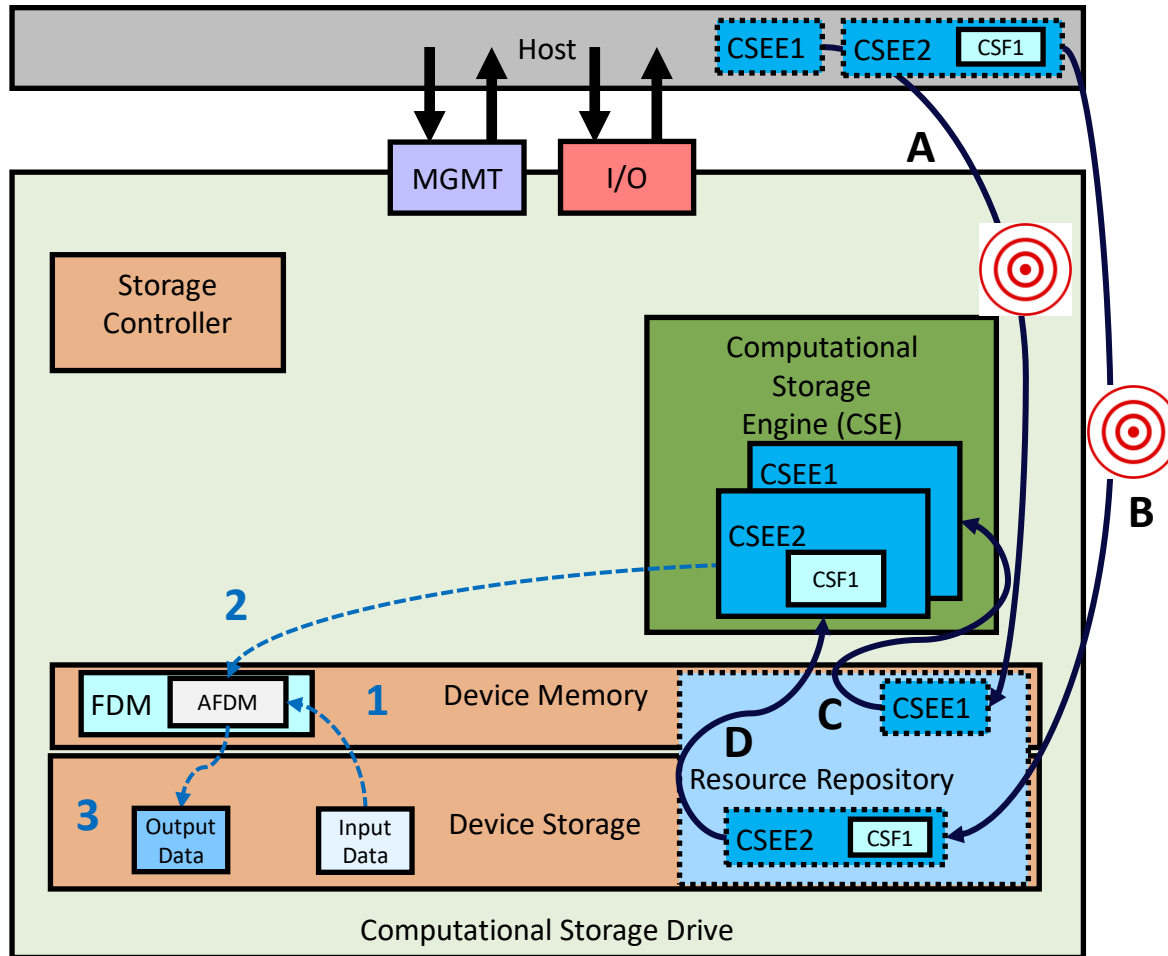
Possible areas of Security Concerns that Computational Storage raises

Intermediate Term

Partially Constrained System

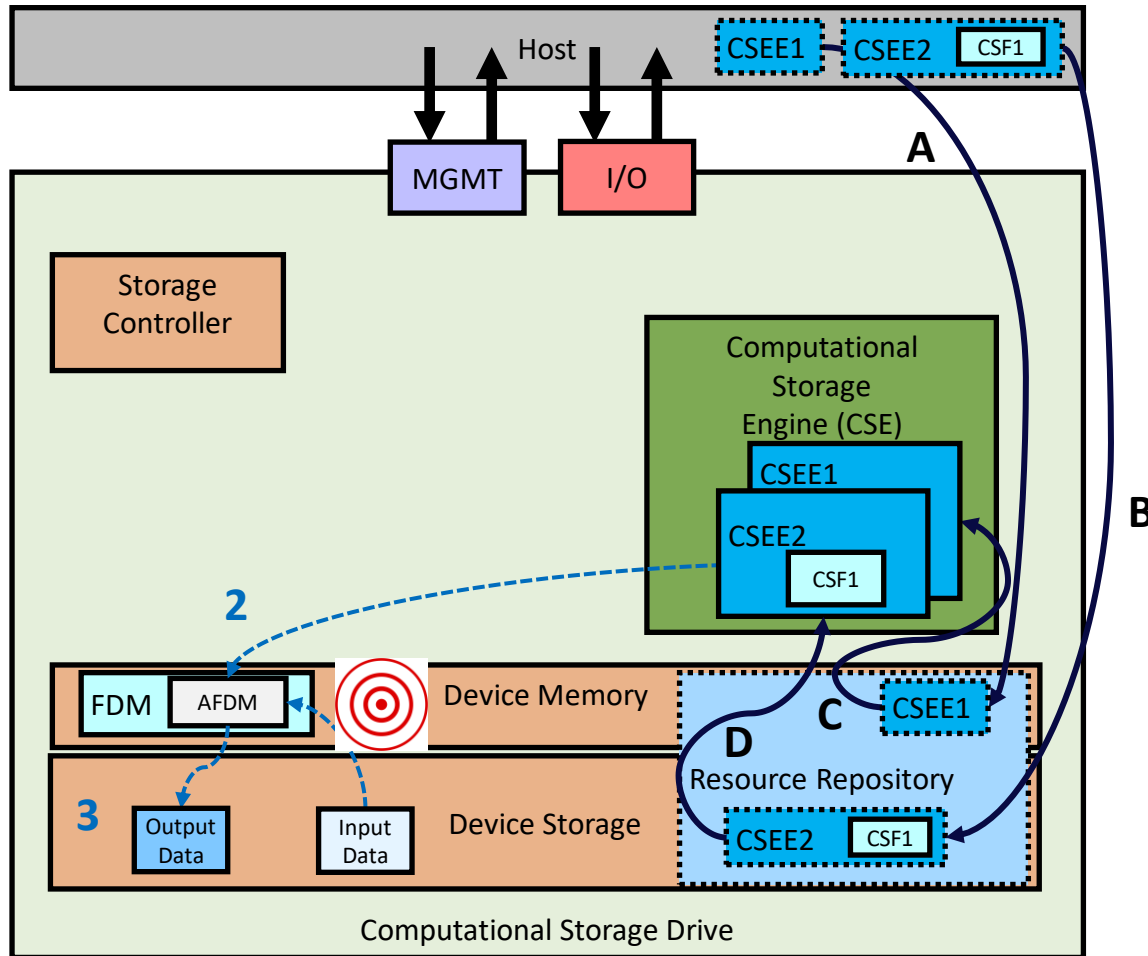
- The environment consists of a single physical host with two or more virtual hosts
- Physically secure attachment between host and CSx

Possible area of security concern: downloaded program



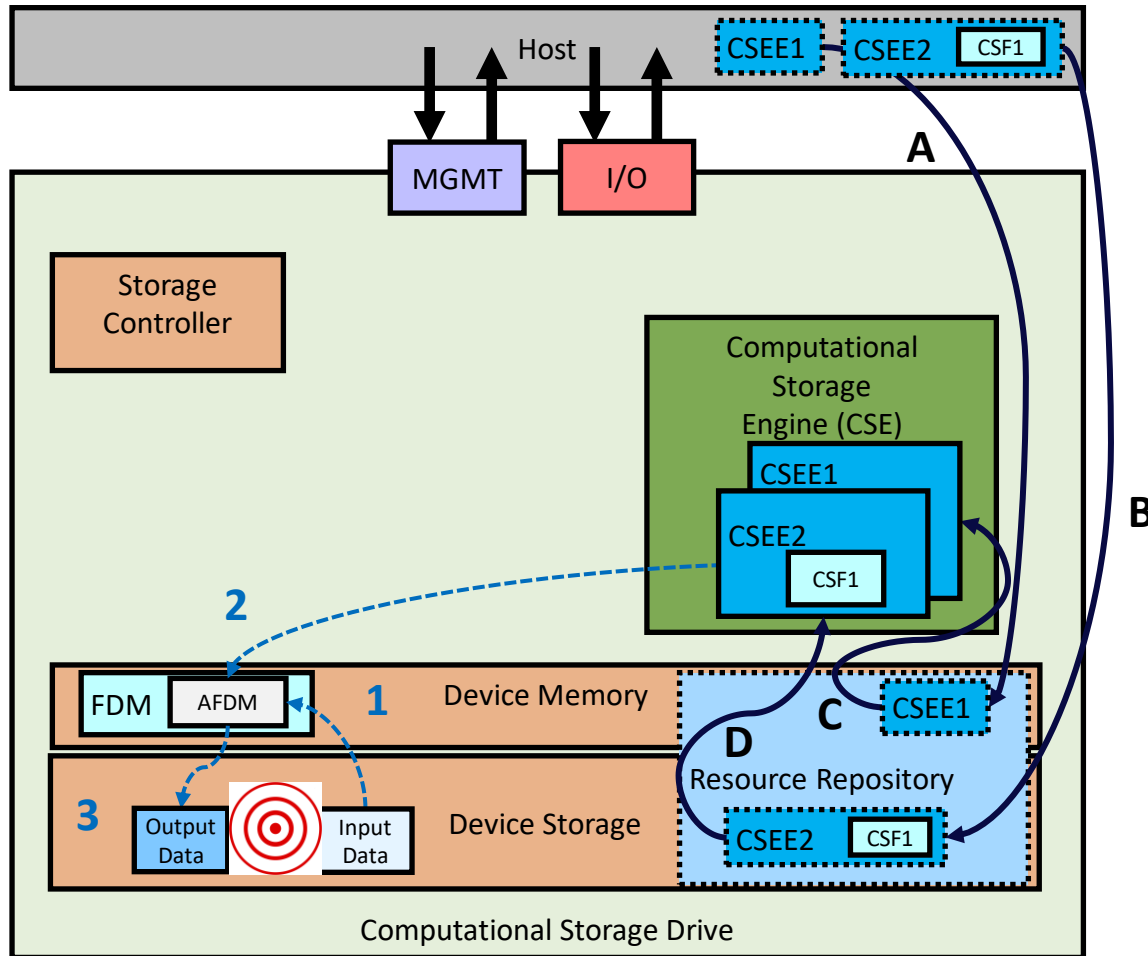
- Rogue Program
- Broken Program
- Corrupted download
- Verification required for downloaded code
- OS running on drive with vulnerability

Possible area of security concern: shared memory



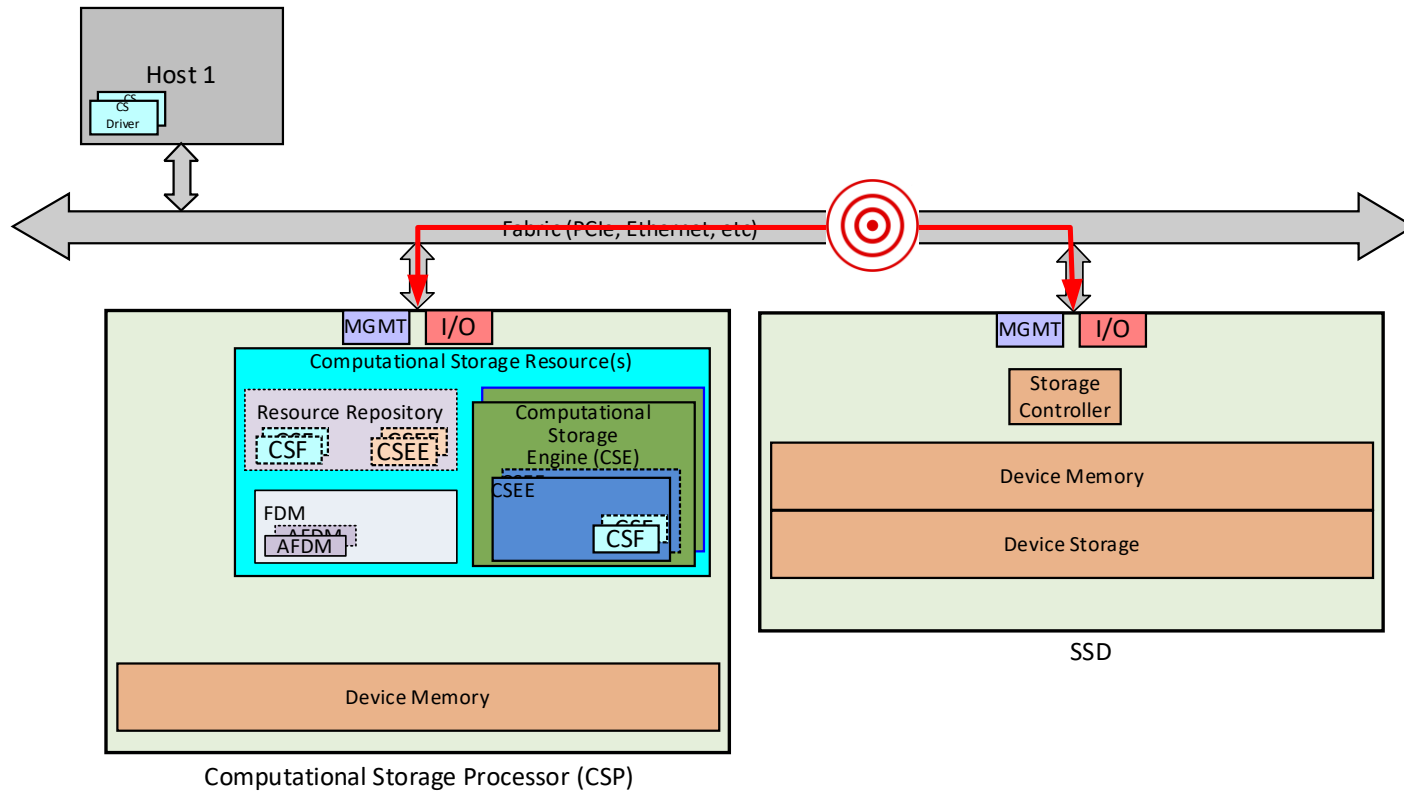
- **Leakage from one CSF to another**
- **Data remains after CSF is deactivated**
- **Corruption of memory by CSF**
- **Denial of service by CSF consuming all memory**
- **Sanitization of memory**
- **Key storage in memory**

Possible area of Security concern: Device Storage



- **Encrypted data?**
 - Secure key distribution
- **Rogue CSF**
intercepting key
- **CSF corrupting of data**
on media

Possible area of Security concern: CSP <-> SSD



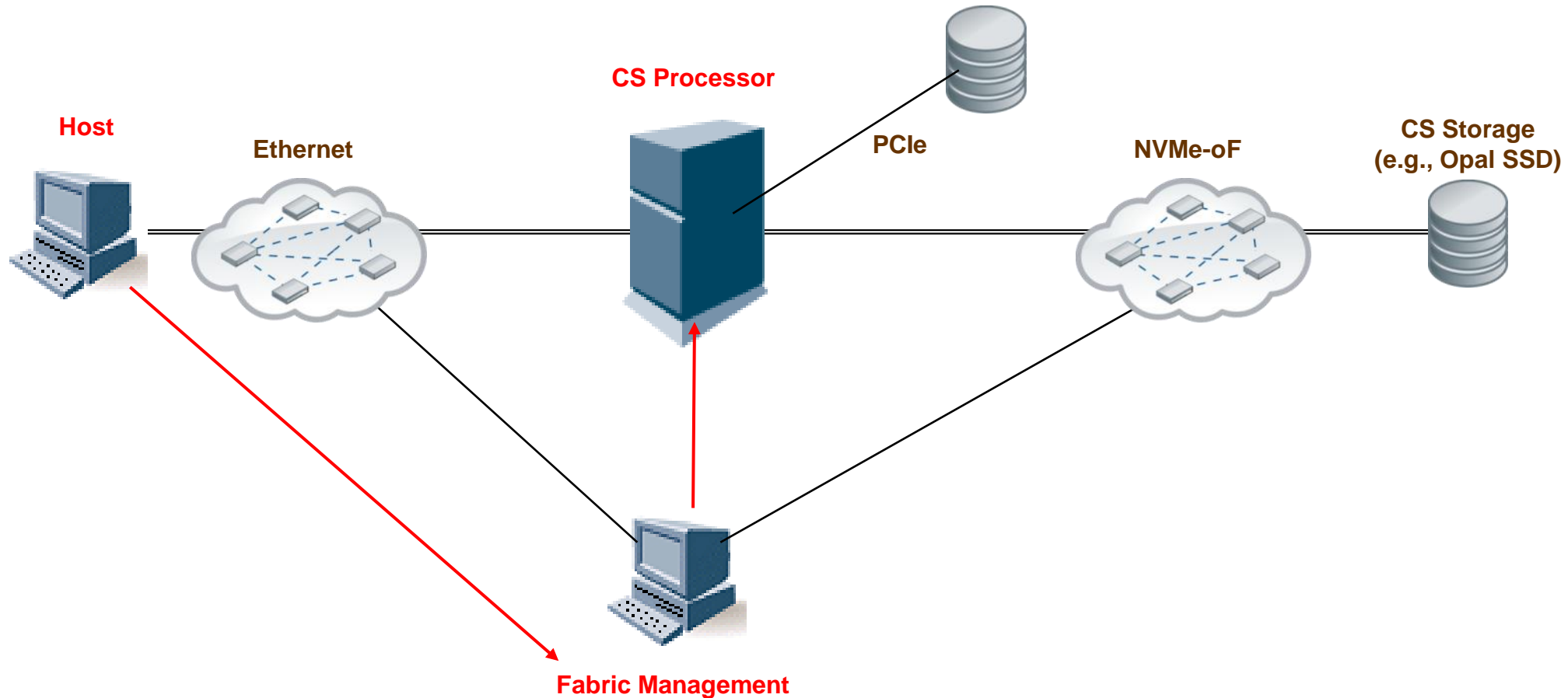
- **CSP manages SSD as Opal drive?**
 - Management of credentials on CSP
 - Security of credentials on CSP
- **Communication between CSP and SSD has to be secured**
- **If the CSP is shared between hosts, then that allows an SSD to be accessed by multiple hosts**



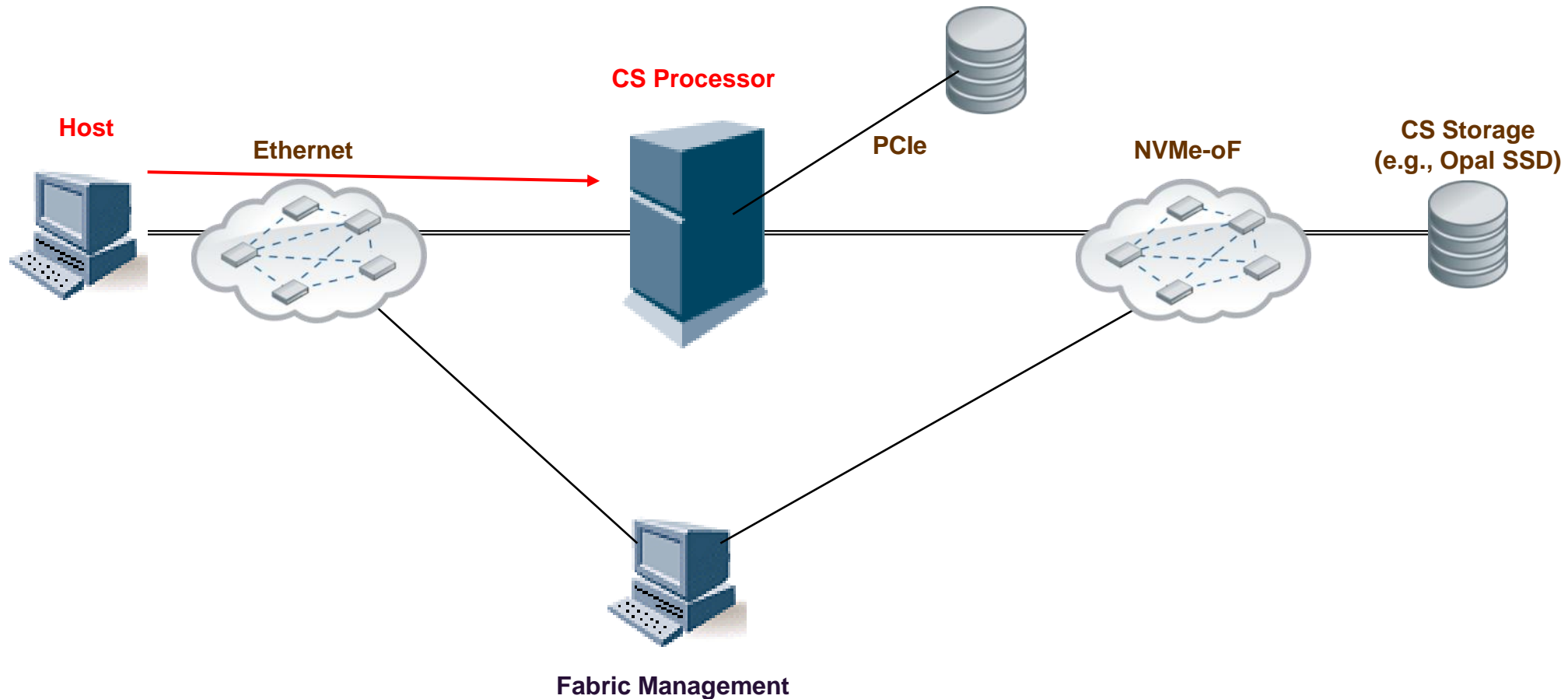
Possible areas of Security Concerns that Computational Storage raises

Long Term

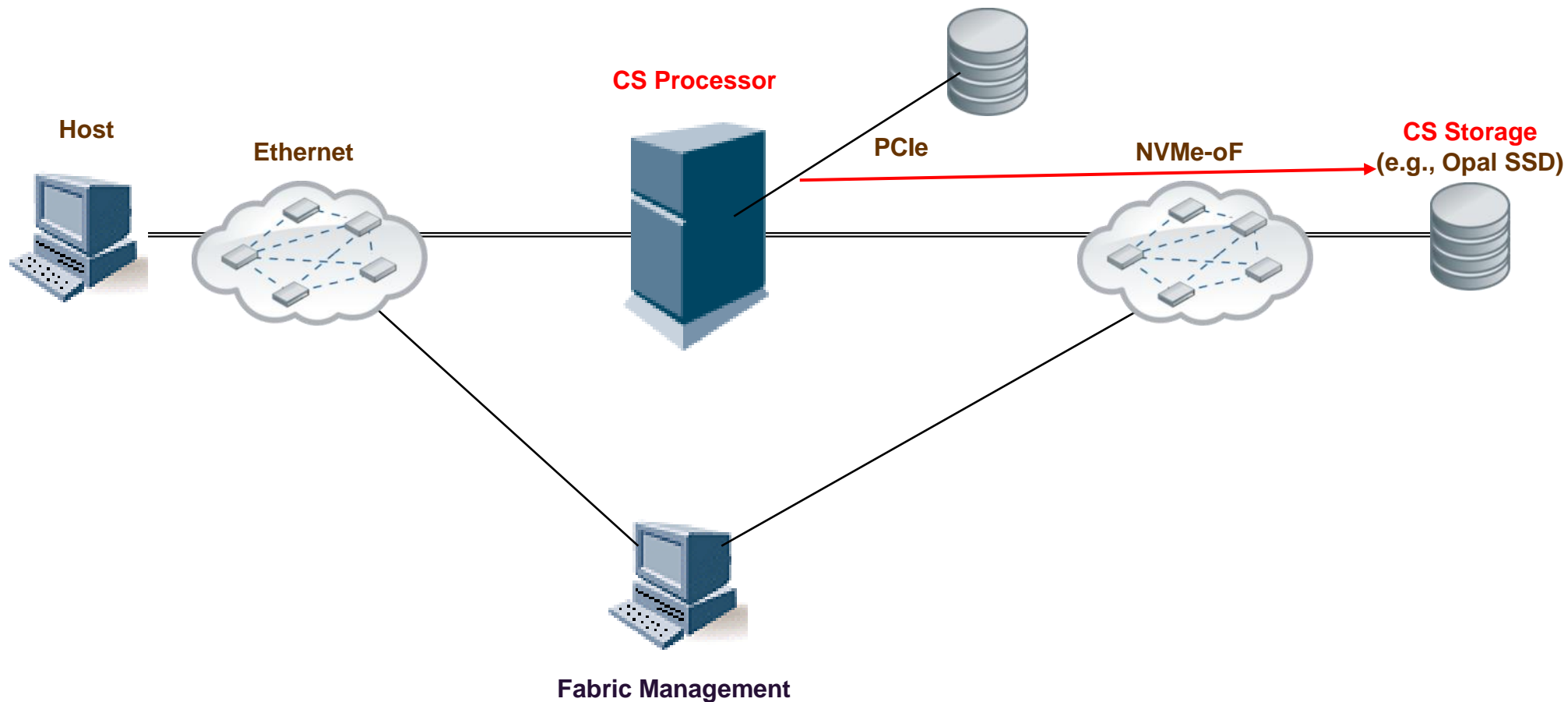
Hypothetical Configuration – Management Security #1



Hypothetical Configuration – Management Security #2



Hypothetical Configuration – Management Security #3





Security call to arms

For Computational Storage

Summary

- Storage producers call to arms
 - Computational Storage implementations that ignore security do so to their peril
- Security community call to arms
 - New attack surfaces are opened by Computational Storage
 - Come join the SNIA Computational Storage activities
- Opportunities do exist to manage CSx security
- Computational Storage may present opportunities to facilitate device security



Please take a moment to rate this session.

Your feedback is important to us.