Thoughts on Security for CXL 3.x GFAM Clusters with Embedded Compute

11/12/2023

- Craig Warner:
  - Scalable Memory Systems Group

CXL 3.0 Enables Large Multi-Host Clusters

it's real

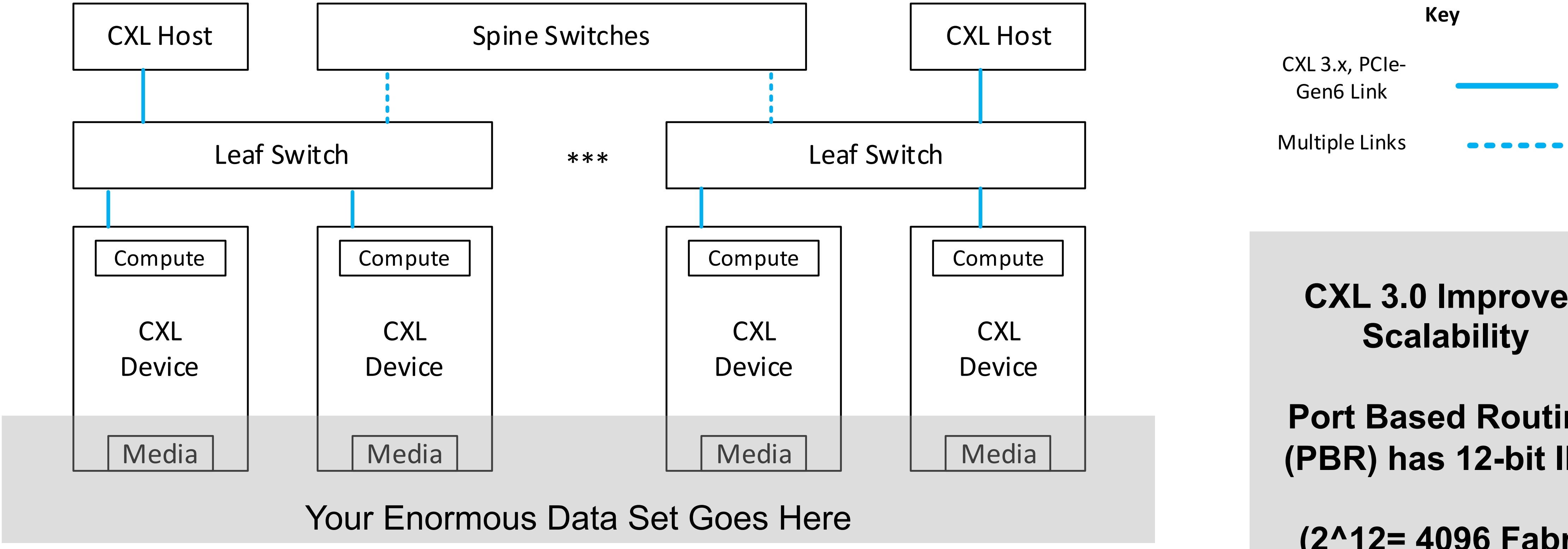
CXL Compute Express Link

- CXL is the first industry standard "memory" fabric supported by both, big x86 SoC vendors
- CXL uses PCIe for it's lower-level protocols

Delivering CZ120 memory expansion module samples based on CXL 2.0 Standards

	CXL 1.1	CXL 2.0	CXL 3.0
Spec Release	2019	2020	2022
Switching (Single-Level)	No	Yes	Yes
Switching (Multi-Level)	No	No	Yes
Multi-Host Memory Sharing	No	No	Yes
Direct Memory Access for Device-to-Device	No	No	Yes

An Example CXL 3.0 Global Fabric Attached Memory (GFAM) Cluster

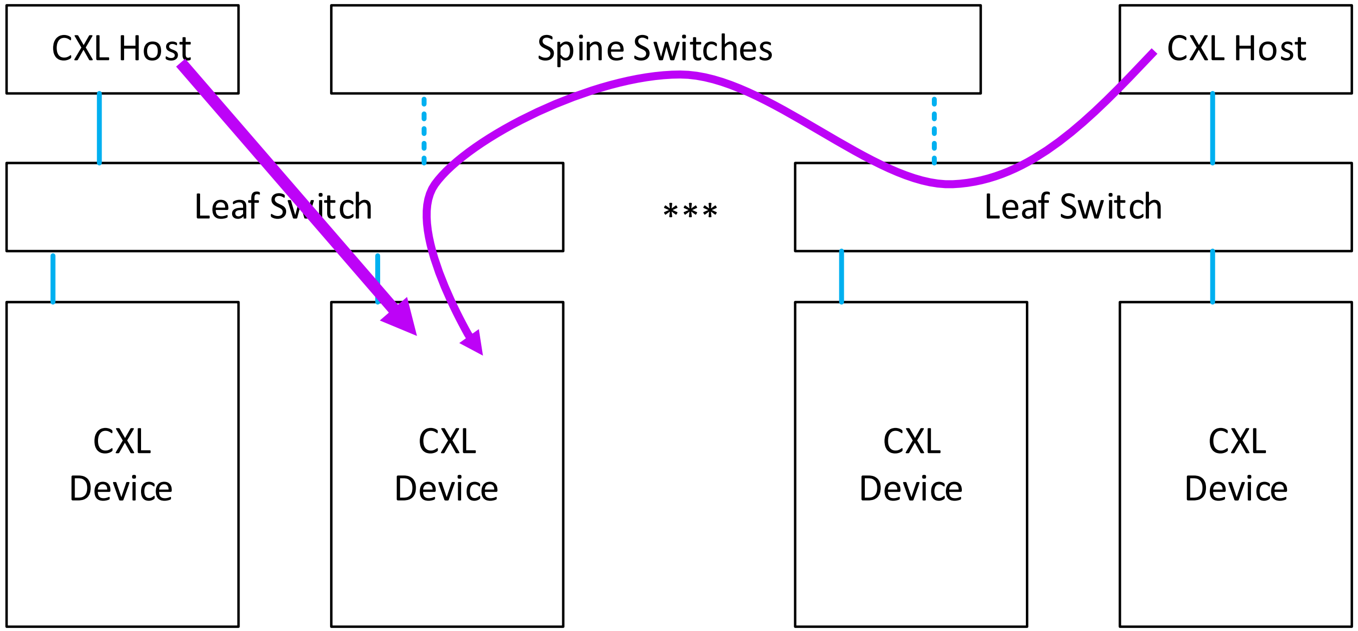


CXL 3.0 Improves Scalability

Port Based Routing (PBR) has 12-bit IDs

(2^12= 4096 Fabric Connections)

What’s a “Memory” Fabric?



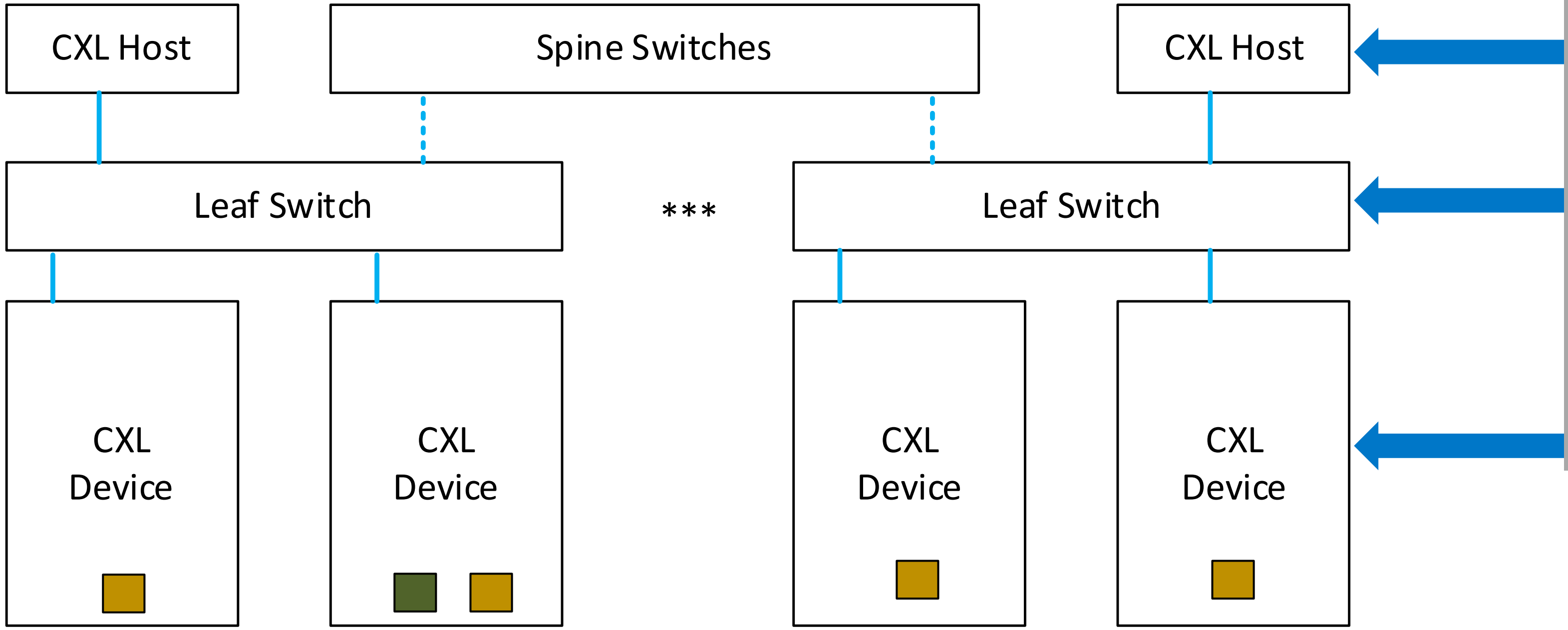
Unique Qualities of a CXL Memory Fabrics

- With CXL hosts can access memory on CXL devices with **“load”** and **“store”** instructions
- The host SoC caches are used for the data fetched from the CXL devices
- For CXL 3.0, the “idle” cache miss latency goal for large GFAM is ~600ns (sometimes called load to use latency)

Basic Security: CXL 3.0 Defines Access Control

Cluster Tenants:

- One tenant can’t see another tenant’s data because of CXL defines access tables set up by cluster Operator



Cluster Operator:

- Controls Configuration for Each Tenant (Cores, Memory)
- Fabric Management Software used to configure switches, devices, and hosts
- Access tables are in the CXL Devices

More Advanced Security Questions

Can the tenant data be snooped with CXL logic analyzers?

- Can these be kept out of the lab?
- What happens when hard to fix problems need more data?

Can a malicious cluster operators snoop at tenant data?

- Switch hardware will likely have data capture hooks
- Switch hardware might have arbitrary packet generation hooks

not

Can tenant data be seen on decommissioned modules?

- More important for persistent memory technologies

CXL Logic Analyzers Exist

(picture courtesy of teledynelecroy.com)

Encrypting data is the fix

Importance of closing attack surfaces depends on the nature of the customer’s work

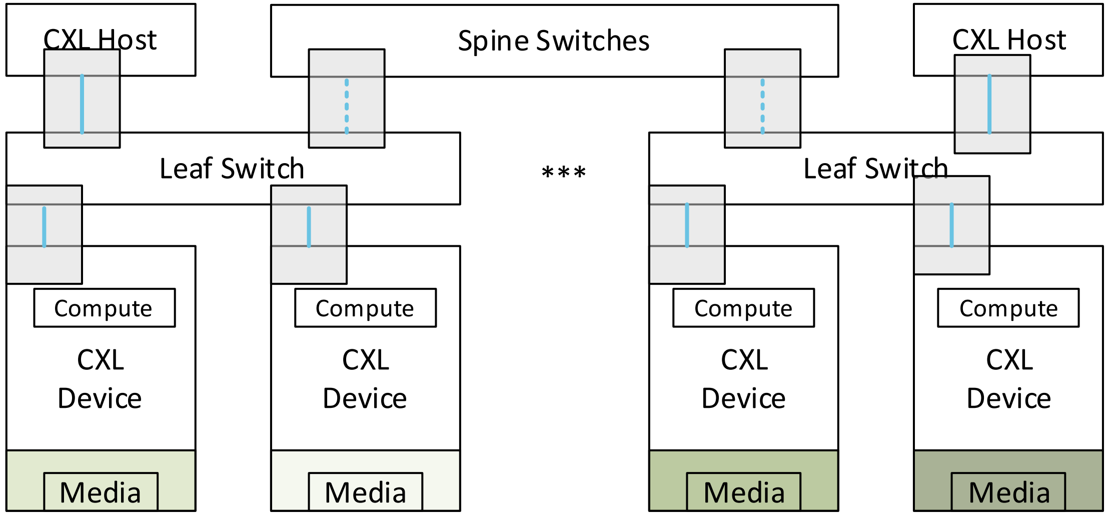
One Approach to Encryption: CXL Link and CXL Media Encryption

Consider one tenant with lots of Near Memory Computing

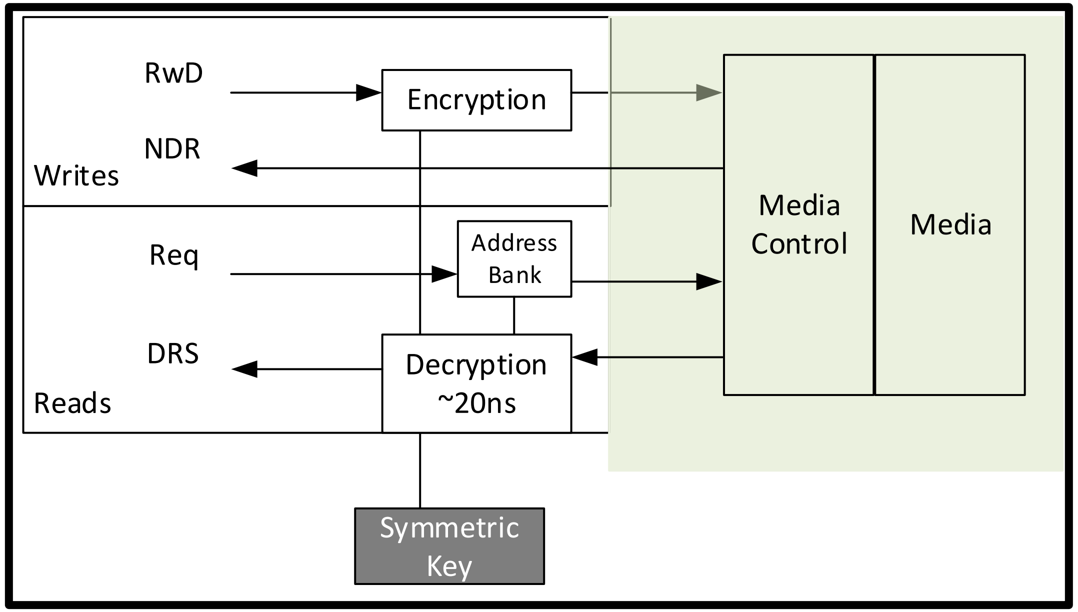
□ Clear-Text

▨ Cypher-Text: CXL links can be made secure with
CXL Integrity and Data Encryption (CXL IDE)

🟩 Cypher-Text: Media can be encrypted with
AES-256-XTS



- CXL IDE encrypts the CXL packet data – not the CXL packet headers
- Media encryption details not defined by CXL
- AES-256-XTS is a proven data at rest scheme
  - Modest size/power consumption
  - Reasonable latency

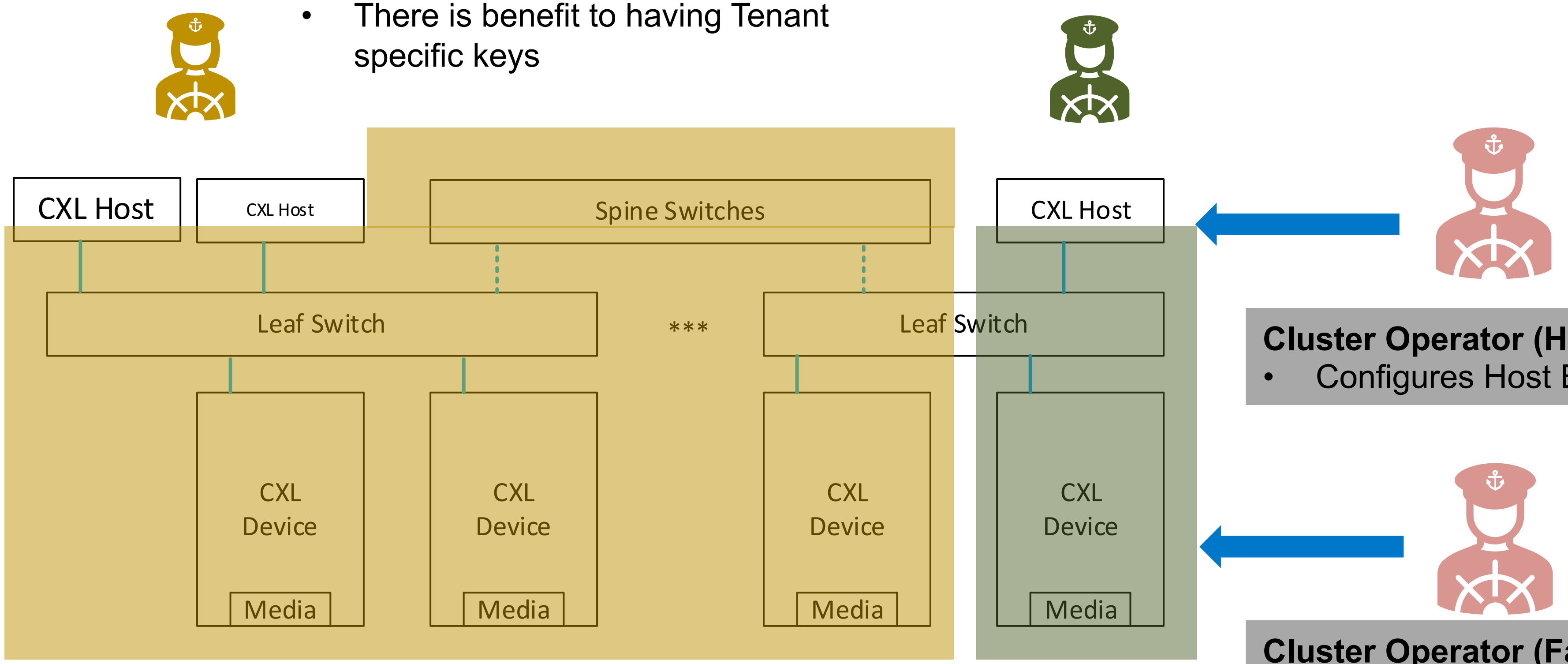


Another Approach to Encryption: Host Side Encryption

- Hosts can implement encryption, so CXL packet data is always encrypted.
- Can be deployed on a cluster with link and media encryption.
- Not every host needs to be a, big x86 server; Hosts can be application specific processors

Cluster Tenants:

- There is benefit to having Tenant specific keys



Cluster Operator (Host Keys):

- Configures Host Encryption

Cluster Operator (Fabric):

- Access Control
- Utilization Monitoring
- Etc.

Encryption Strategy Comparison

	Device Media Encryption & CXL IDE	Host Side Encryption
Clear Text in Fabric Silicon • Fabric manager must be trusted • Switch vendor must be trusted	Yes	No Link Encryption not needed (Latency Advantage)
Encryption Keys	Each CXL Device can have its own keys	Multiple hosts need the same key
Near Memory Compute in CXL module	Enabled	Not possible
Compression in CXL module	Enabled	Encrypted data does not compress well

Micron®