1-512-256-0197
www.mindshare.com
training@mindshare.com

CXL Security

Let MindShare Bring "CXL Security" to Life for You

The need for security in computer systems has increased dramatically over the years. There are many factors behind this, including:

- Downloadable firmware that is used to implement devices (known as soft devices) that used to be hard-coded.
- Counterfeit devices in the supply chain.
- Malicious actors building back doors into genuine devices.
- Virtualization, where we have multiple operating systems sharing the same platform.
- Greatly increasing complexity opening the door to design errors and implementation bugs.
- Sophisticated attackers with resources to search for the smallest hole.
- Increased rewards for a successful system attack, whether monetary (perhaps from the theft of crypto), or from destructive intent to a target (such as a power grid).
- Increasing connectivity of systems, such that a platform that was isolated and therefore secure, is now online and attackable from the other side of the world.
- Device portability, such that physical access to a system in a secure data center is not required, the target is a laptop or phone class of system.
- Growth of sensitive data on devices, such that the system attacker might be a "good guy" such as law enforcement trying to prevent a terrorist attack.
- An increasing complex world where the definition of "good guy" and "bad guy" are not clear.

CXL, as an interconnect that carries memory and cache traffic, offers a high value target. Consider a system where memory encryption is implemented by the memory controller. In such a system, it may be easier to attack traffic on the interconnect before it reaches the memory controller and is encrypted.

CXL 2.0 added security capabilities, based on the PCIe and DMTF features. This CXL focused security course covers these security topics looking at how such high value traffic is protected, and the enhancements in CXL 3.0 and 3.1.

This course covers CXL 2.0, CXL 3.0 and CXL 3.1.

You Will Learn:

- Threat models.
- STRIDE categories (spoofing, tampering, repudiation, information disclosure, repudiation, denial of service, elevation of privilege).
- CXL overview, highlighting the areas we will discuss with respect to attacks.
- Differences between CXL.io and CXL.mem / CXL.cache in terms of addressing and IOMMU, and the effects on security.
- Using the IOMMU to prevent DMA attacks, and the potential security holes with an IOMMU.
- Other DMA attack mitigations such as encrypted memory and enclaves.
- Interrupt attacks.
- Using Interrupt Remapping to prevent interrupt attacks, and the security holes with interrupt remapping.
- The idea of mutable versus immutable, and why everything needs to be treated as mutable.
- Error reporting attacks.
- Switch based attacks.
- Using the IOMMU to prevent DMA attacks, and the potential security holes with an IOMMU.
- The enhancements to the CXL fabric and to manageability (IDE – Integrity and Data Encryption plus SPDM, MCTP and CMA).

1-512-256-0197
www.mindshare.com
training@mindshare.com

- The boundaries of the protection from the enhancements, and possible paths to attacking such a secured system.
- TSP (TEE (Trusted Execution Environment) Security Protocol)

Course Length: 2-Days, (optional 3rd Day)

Course Outline:

- Fabric based attacks (watching links, changing packets, injecting packets).
- Malicious hardware, counterfeit hardware.
- Impersonation (where a device pretends to be something else).
- The need for
  - Establishing trust (host knowing the device, device knowing the host).
  - Key exchange.
  - Encrypted links.
- Keys, certificates and encryption background
  - symmetric encryption
  - public and private keys
  - TLS (Transport Layer Security) background
  - encryption standards
  - certificates
  - X.509 trust model
  - AES-GCM
- TCG (Trusted Computing Group) background
  - root of trust
  - attestation
  - system startup
- CXL.io protection
  - uses PCIe IDE
  - link security threat model
  - exposures not covered by the threat model
  - stream establishment
  - side channel attacks via unencrypted headers
  - TLPs
  - TLP Encryption
  - TLP Aggregation
  - IDE Extended Capability structure
  - IDE Sub-Streams
  - IDE_KM (Key Management)
  - power management and resets
  - error conditions and error reporting
  - IDE may not be sufficient, what else may be needed
    - key exchange
    - trust
- CXL. memory and CXL.cache protection
  - similar to PCIe IDE, but FLIT based
  - link IDE only, the role of the switch
  - FLITs
  - FLIT Encryption

1-512-256-0197
www.mindshare.com
training@mindshare.com

  - FLIT Aggregation
  - IDE control FLIT
  - MAC handling, truncated MACs, MAC transmission
  - containment mode and skid mode
  - PCRC for crypto engine robustness
  - CXL_IDE_KM, key management for CXL.cachemem
  - Changes for the 256 byte flit
- DMTF Specifications overview
- Security Protocol and Data Model (SPDM)
  - multiple paths to devices (SMbus, I2C)
  - threat model
  - mutable and immutable objects
  - authentication
  - attestation
  - recommended flow
  - handling versions
  - certificates and chains of certificates
  - mutual authentication
  - session key exchange
  - Diffie-Hellman scheme background
  - PSK (pre-shared key)
  - secure session
  - provisioning
  - alias certificates (dynamic certificates)
  - complications of having 2 certificate models
  - open source libspdw, a sample implementation
- CMA (Component Measurement and Authentication)
- MCTP (management Component Transport Protocol)
- DOE (Data Object Exchange)
  - Mailboxes and their use
  - DOE Extended Capability structure
  - DOE Capabilities registers
  - DOE Interrupts
- TSP (TEE Security Protocol)
  - PCIe TDISP background
  - CXL implementation of TSP
- Memory Encryption

Optional content covered in a 3-day class and covered on 1st day

- DMA attacks, copying or modifying memory.
- Use of an IOMMU to prevent DMA attacks.
- IOMMU issues at boot time versus runtime, setup and configuration of the IOMMU, and the ACPI DMAR tables.
- Error reporting from devices.
- Congestion based attacks.
- Interrupt based attacks, with the interrupt remapping as mitigation.

1-512-256-0197
www.mindshare.com
training@mindshare.com

Recommended Prerequisites:

The MindShare CXL 2.0 class or equivalent knowledge is recommended as a pre-requisite.
Basic knowledge of processor (Intel/AMD/ARM) and computer architecture

Course Material:

Downloadable PDF version of the presentation slides.
Recorded eLearning of the course when available.