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

PCI Express and CXL Security

Let MindShare Bring "PCI Express and 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.

We have moved from a world where a simple I/O device installed in a system was reasonably safe, to a world where literally everything could be used as a possible attack vector. The weak points may come from design limitations, from designs being used outside of the environment that they were intended for, and from implementation defects.

This PCIe and CXL security course looks at the security features added to PCIe and CXL as a defense against attacks via the fabric. These include features for evaluating identity and trust in devices, encrypting traffic on the links (PCIe and CXL), and preventing traffic on the links from being modified (IDE : Integrity and Data Encryption). This course covers PCIe 5.0, 6.0 and 6.1, and CXL 2.0, 3.0 and 3.1.

You Will Learn:

- Threat models.
- STRIDE categories (spoofing, tampering, repudiation, information disclosure, repudiation, denial of service, elevation of privilege).
- System and PCIe overview, highlighting the areas we will discuss with respect to attacks.
- CXL overview, highlighting the areas we will discuss with respect to attacks.
- The idea of mutable versus immutable, and why everything needs to be treated as mutable.
- The enhancements to the PCIe fabric and to manageability (CMA/SPDM/IDE)
- The boundaries of the protection from the enhancements, and possible paths to attacking such a secured system.
- Differences between CXL.io and CXL.mem / CXL.cache in terms of the IDE implementations.
- TLPs and Flits.
- Switch attacks.
- PCIe TDISP and CXL TSP, support for Trusted Execution Environments.

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

Course Length: 4-Days

Course Outline:

- The need for
  - Establishing trust (host knowing the device, device knowing the host).
  - Key exchange.
  - Encrypted links.
- Keys, certificates and encryption background
  - public and private keys
  - encryption standards
  - certificates
  - X.509 trust model
  - AES-GCM
- PCIe IDE (Integrity and Data Encryption)
  - link security threat model
  - Exposures not covered by the threat model
  - Link IDE
  - The switch as an attack vector
  - Selective IDE
  - Mixing Link and Selective IDE
  - Stream establishment
  - Side channel attacks via unencrypted headers
  - IDE TLPs
  - TLP Encryption
  - TLP Aggregation
  - IDE Extended Capability structure
  - IDE Sub-Streams
  - Power management and resets
  - Error conditions and error reporting
  - Partial header encryption with PCIe 6.0
  - Segments with PCIe 6.0
  - Link and selective IDE with Flit Mode (PCIe 6.0)
  - IDE may not be sufficient, what else may be needed
    - key exchange
    - trust
  - TDISP (TEE Device Interface Security Protocol)
- PCI-SIG and DMTF Specifications overview
- TCG (Trusted Computing Group) background
  - root of trust
  - attestation
  - system startup
- CMA/SPDM (Component Measurement and Authentication / Security Protocol and Data Model
  - multiple paths to PCIe devices (SMBus, I2C)
  - threat model
  - mutable and immutable objects
  - authentication
  - TLS (Transport Layer Security) background
  - 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
- IDE_KM (IDE Key Management)
  - Key management messages over SPDM
  - Root port handling
- DOE (Data Object Exchange)
  - Mailboxes and their use
  - DOE Extended Capability structure
  - DOE Capabilities registers
  - DOE Interrupts
- MCTP (Management Component Transport Protocol)
  - managebility traffic and the pre-boot environment
  - transport bindings
  - messages
  - packets
  - endpoints and EIDs (endpoint IDs)
  - the MCTM Bus Manager
  - SPDM over MCTP Binding
  - Secured MCTP Messages over MCTP Binding
- MCTP over SMBus and I^2C
- MCTP over PCIe, and PCIe VDMs
- CXL.io protection
  - uses PCIe IDE
  - differences between PCIe and CXL.io IDE
- CXL. memory and CXL.cache protection
  - similar to PCIe IDE, but FLIT based, with some important differences
  - link IDE only, the role of the switch
  - FLITs
  - FLIT Encryption
  - FLIT Aggregation
  - IDE control FLIT
  - MAC handling, truncated MACs, MAC transmission
  - containment mode and skid mode
  - PCRC for crypto engine robustness
  - Support for 256 byte flits
  - TSP (Trusted Execution Environment Security Protocol)
- CMA for CXL
- CXL_KM_IDE

Recommended Prerequisites:

PCIe/CXL knowledge. 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