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

PCI Express Security

Let MindShare Bring "PCI Express Security" to Life for You

The threat model for PC systems has changed dramatically over the years. Inserting a card (e.g., AGP, PCI, PCI-X, PCIe) was an action that required physical access to the system board, and the system could be protected with a case lock and intrusion alarms. It was regarded that a plug-in card that the user chose to install in their system should therefore be trusted. There have been many changes to this simple picture that result in a very different threat model today, for example:

- External connectors that are DMA capable, such as Thunderbolt and the USB-C connector, which makes internal data accessible without needing to open the case.
- The ability of devices to hide their purpose, such as a device that appears to be a USB-C charger, but that has malicious capability hidden such as wireless networking capability (a Trojan).
- Downloadable firmware that is used to implement devices (known as soft devices) that used to be hard-coded.
- Counterfeit devices and components 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.

The simple attack over PCIe has moved from being

- a simple DMA read/write of system memory, or
- an errant interrupt causing execution of unintended code,

to being a question of the inability to trust the PCIe fabric itself. For example, has an attacker been able to switch on the debug facilities in a firmware-implemented PCIe switch, and use the switch as a malicious TLP generator? (The answer is Yes).

This PCIe focused security course starts by looking at some of the simpler forms of attacks such as DMA, and some of the defenses again those attacks (IOMMU), and also some of the holes in these defense mechanisms. We then move onto looking at some of the additional features added to help protect the fabric (such as source validation in Access Control Services), and then onto the newest features for evaluating trust, link encryption, and point-to-point encryption. We also look at the supported for a TEE (Trusted Execution Environment) VM.

This is not a platform security course as there are many other topics of relevance to security that we will not discuss, such as UEFI, hypervisors, operating systems, processor security features, etc.

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

This class looks at potential attacks on “legacy” PCIe and some of the mitigations (ACS, IOMMU, etc), and then explores the newer features (CMA, IDE, SPDM, TDISP, etc). This class is based on the ECNs to PCIe 4.0 and 5.0, and also covers the changes from PCIe 6.0 and 6.1.

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.
- DMA attacks.
- Using the IOMMU to prevent DMA attacks, and the potential security holes with an IOMMU.
- Other DMA attack mitigations such as encrypted memory.
- 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 attacks.
- 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.

Course Length: 3 Days

Course Outline:

- Early systems. The necessity for the proliferation of DMA engines. The necessity for interrupts.
- Address spaces, such that memory may be readable/writeable memory, or may be I/O space.
- DMA attacks, copying or modifying memory.
- Malicious hardware entering the supply chain.
- Mutable versus immutable, and the surprises.
- Impersonation (where a device pretends to be something else).
- Convergence and convenience (USB-C for charging but also for attacking).
- Use of an IOMMU to prevent DMA attacks.
- IOMMU issues at boot time versus runtime, setup and configuration of the IOMMU, and the ACPI tables.
- PCIe defined ATC as a bypass for the IOMMU.
- PCIe defined ACS as a mitigation for the ATC.
- Error reporting from devices.
- Congestion based attacks.
- Interrupt based attacks, with the interrupt remapping as mitigation.
- NMI and SMI bypass to the interrupt remapping.
- Fabric based attacks (watching links, changing packets, injecting packets) from the switch.
- Fabric based attacks from retimers.
- The need for
    - Establishing trust (host knowing the device, device knowing the host).

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

  - Key exchange.
  - Encrypted links.
- Keys, certificates and encryption background
  - public and private keys
  - encryption standards
  - certificates
  - X.509 trust model
  - AES-GCM
- 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
- 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)

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

  - 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)
  - manageability 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
- TDISP (TEE Device Interface Security Protocol)
- Summary, putting it all together

Recommended Prerequisites:

The MindShare PCIe 5.0 / 6.0 class or equivalent knowledge is recommended.
Basic knowledge of processor (Intel/AMD/ARM) and computer architecture

Course Material:

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