Flash Memory Summit

OakGate TECHNOLOGY

Memory Fencing for Detection of DMA Memory Address Violations

Presented by:

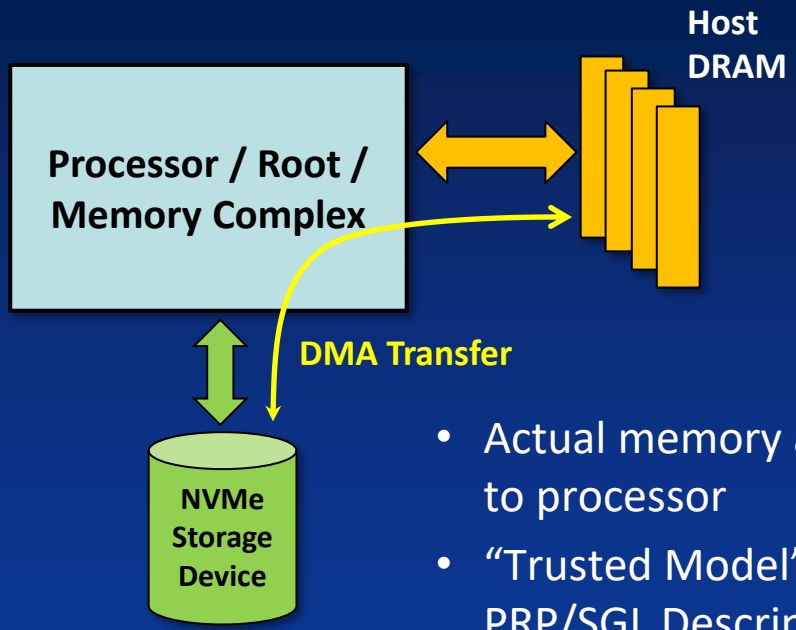
Bob Weisickle, CTO and Co-Founder

OakGate Technology

Santa Clara, CA

August 2019

Problem Statement



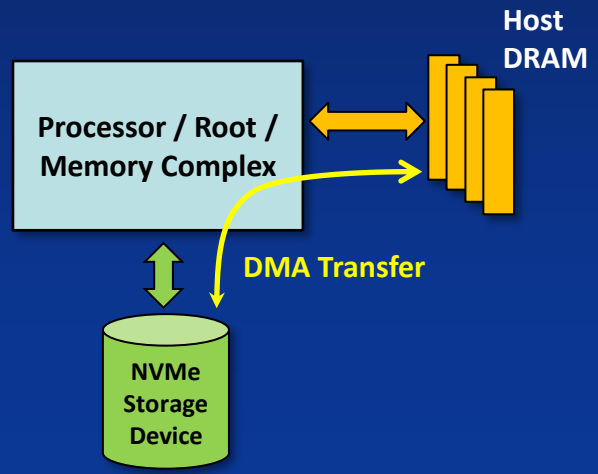
IMPACT

- Data Corruption
- System Stability
- Security Exposure

- Actual memory accessed by SSD is transparent to processor
- "Trusted Model" – SSD is expected to honor the PRP/SGL Descriptors
- Processor "expects" device to be PCIe/NVMe spec compliant

Solution

Enable the host to detect functional errors that occur when a device with a Direct Memory Access (DMA) engine accesses memory space outside of the area specified by the device driver



Drive Validation and Qualification Benefits

Detect functional errors caused by memory incursions

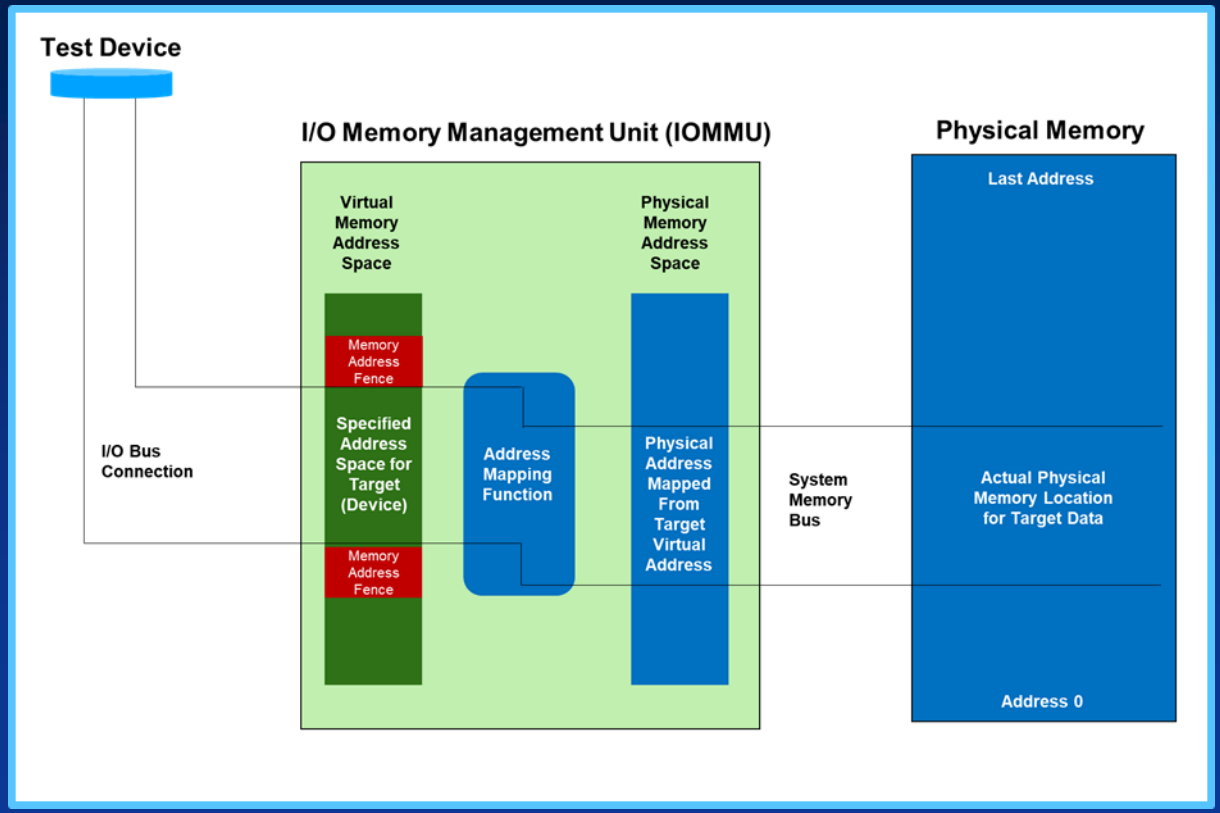
Exercise the complete 48-bit DMA address range

Detect system hacking, unauthorized memory access, malware

How Memory Fencing Works

Description:

- Highlights mapping and fencing of virtual memory to physical memory over a PCIe bus and system memory bus
- If the Target accesses a memory address that is outside the "Memory Address Fence," an error will be generated and the test engineer will receive a notification from and the error will be logged



Memory Fencing Examples

- SSD Device Reading/Writing beyond the buffer
- DIF/DIX Meta Data Access Errors
- DMA Buffer continuing to be accessed too long after reset was acknowledged
- Full exercise of the complete 48-bit DMA address space

Wrap Up

- Memory fencing technology is being successfully used today to detect functional errors that occur when a DMA engine accesses memory space outside of the area specified by the device driver
- Reduced the time to “root cause” Data Validation Errors and System Instability caused by invalid DMA accesses
- Closed a Drive Test Escape by ensuring that all DMA address bits can be verified

Flash Memory Summit

OakGate TECHNOLOGY

Audience Q&A