Flash Memory Summit

SECURELY REDUCING ON-CHIP RAM REQUIREMENTS FOR CXL™ MEMORY CONTROLLERS

MICROCHIP

A Leading Provider of Smart, Connected and Secure Embedded Control Solutions

SMART | CONNECTED | SECURE

Ariel Sibley, Sr. Technical Staff Engineer

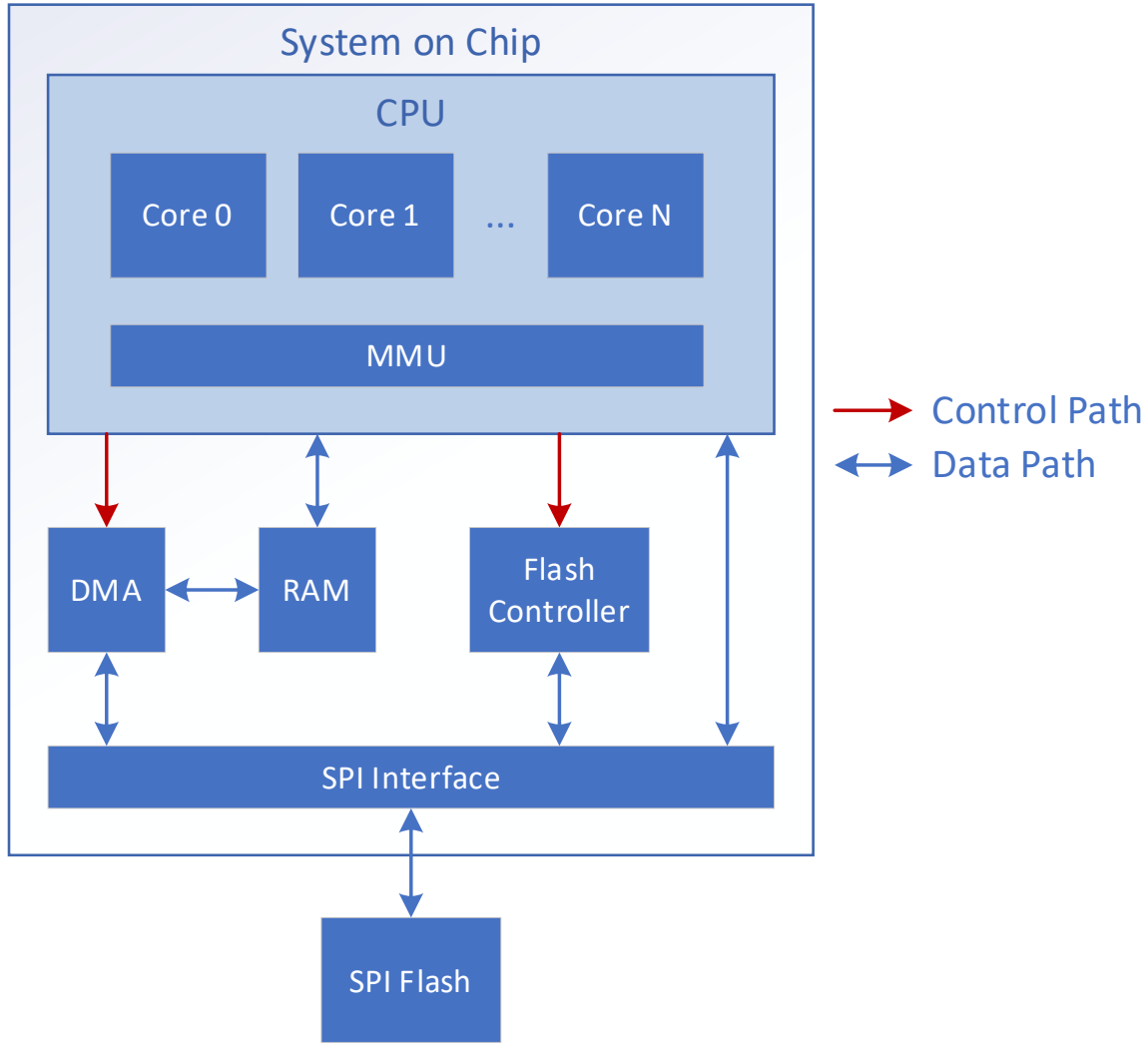
August 10, 2023

Overview

- Problem statement
- Conventional paged execution
- Secured paging
- System considerations

Problem Statement

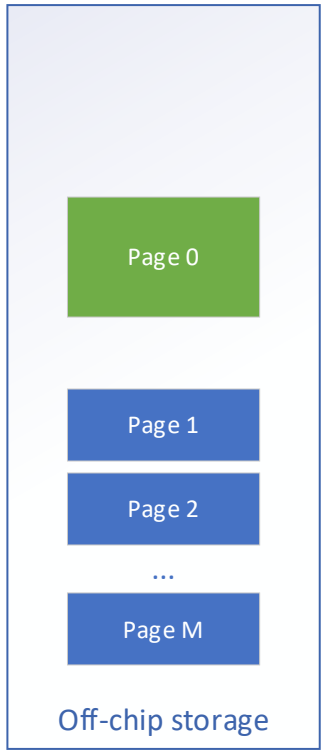
- **System on Chip (SoC) devices such as CXL™ memory controllers contain a CPU executing code from on-chip RAM**
- **On-chip RAM consumes die area and power**
- **Application requires more on-chip RAM than practical**
- **Application is also stored in off-chip storage for persistence**
- **Could execute from off-chip storage, but:**
  - Off-chip storage is slow, especially for random access of small blocks
  - Off-chip storage is not trustable



MICROCHIP

Conventional Paged Execution

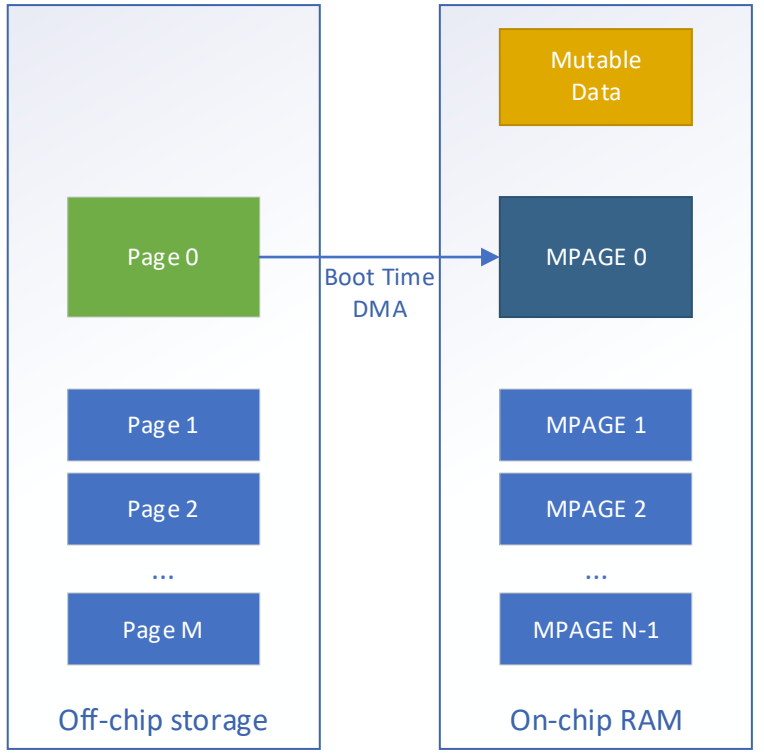
- **Instructions and static data in off-chip storage are divided into pages**
  - Page 0 contains init code and any other unpageable code
  - Page 1 to Page M contains pageable code



MICROCHIP

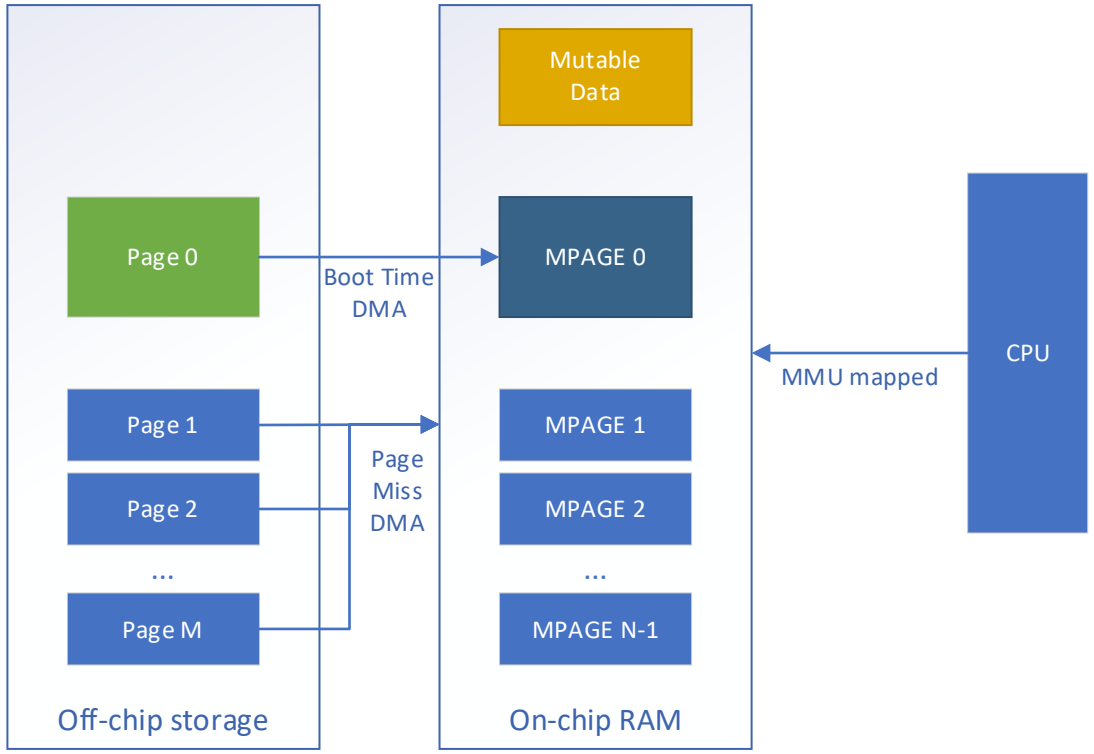
Conventional Paged Execution

- **A portion of on-chip RAM is divided into N pages**
  - MPAGE 0 reflects Page 0, and is DMA'd to on-chip RAM by Boot ROM
- **Typically, M >> N**



Conventional Paged Execution

- **CPU executes from a virtual address space mapped through MMU**
- **If address to be accessed misses in MMU, it triggers a page miss**
- **Page miss handler**
  - DMAs required page from off-chip storage to on-chip RAM
  - Configures MMU to map virtual address of Page X to MPAGE Y



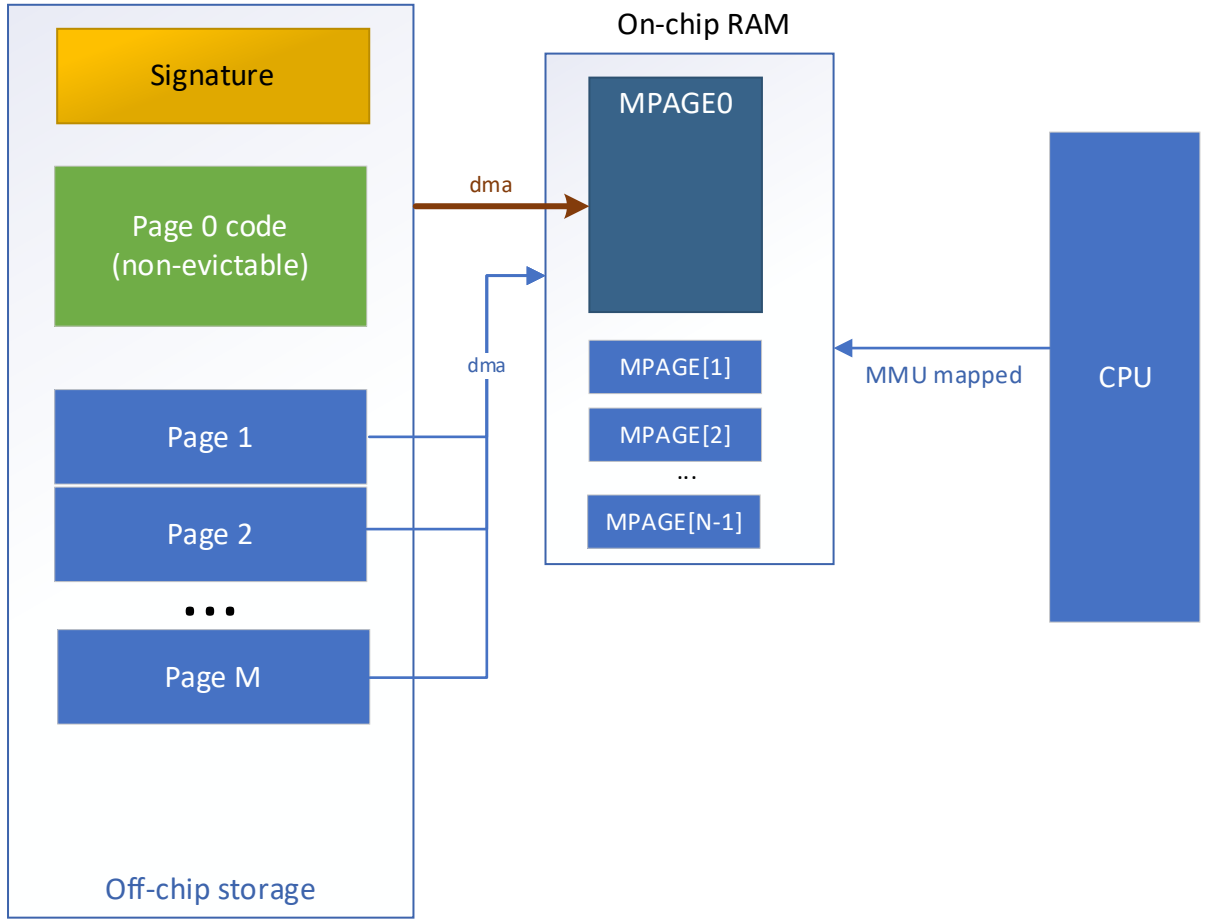
☑ Supports applications larger than on-chip RAM

☑ Data is transferred in large chunks (efficient)

☒ Not secure! Off-chip storage could be modified

Conventional Paged Execution + Secure Boot

- Page 0 code is signed at build time
- Signature is stored in the FW image binary in off-chip storage
- At boot time, ROM code DMAs Page 0 to MPAGE0 in on-chip RAM and authenticates it before allowing it to run



☑ Unauthorized modification to Page 0 detected

☒ Unauthorized modification to Pages 1-M not detected

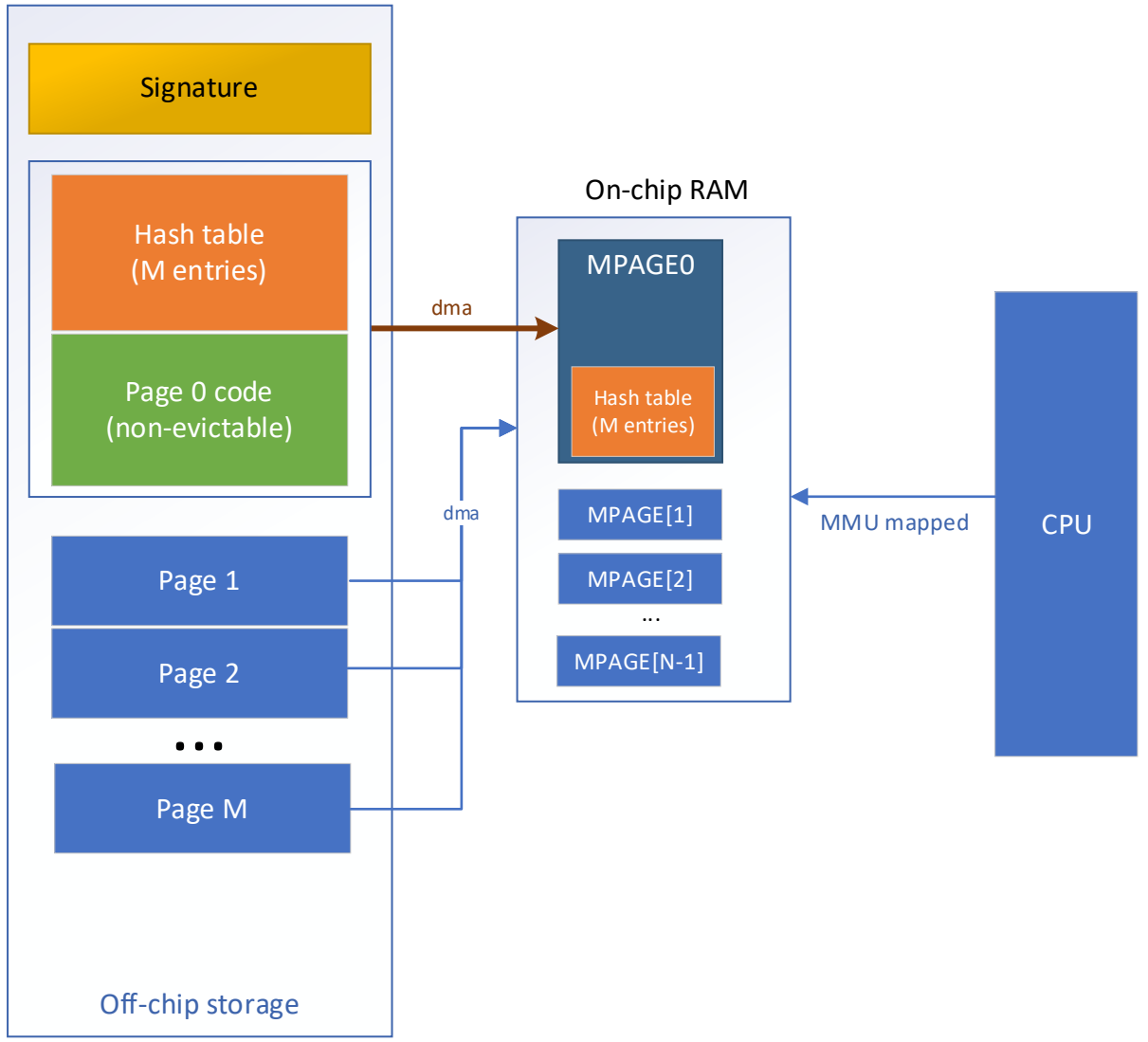
Secured Paging

On boot

- Same as previous secure boot case, plus hash table is also DMA'd to MPAGE0 and authenticated

On page miss of page x

- CPU selects a page p from MPAGE[1:N-1]
- CPU does memcpy/dma of page x from off-chip storage to MPAGE[p]
- CPU measures hash of MPAGE[p] and verifies measurement against hash table entry
- If hash fails, CPU may take corrective action or halt



System Considerations

Paging Latency

- Off-chip storage is much slower than on-chip RAM
- Page misses incur a latency impact

Possible boot time reduction

- Only startup code (Page 0) needs to be authenticated at boot

Eviction Policy

- Various options such as least accessed, least recently accessed or random eviction

Questions?