Protego: A Low-Overhead Open-Source I/O Physical Memory Protection Unit for RISC-V

SSH-SoC 2023, July 9th, 2023

Integrated Systems Laboratory (ETH Zürich)

Nils Wistoff  nwistoff@iis.ee.ethz.ch
Andreas Kuster  mail@andreaskuster.ch
Michael Rogenmoser  micaero@iis.ee.ethz.ch
Robert Balas  balasr@iis.ee.ethz.ch
Moritz Schneider  moritz.schneider@inf.ethz.ch
Luca Benini  lbenini@iis.ee.ethz.ch

PULP Platform
Open Source Hardware, the way it should be!
Hardware shared by sensitive & untrusted workloads
Threat Model

- **User Mode**
  - App
  - ... (multiple applications)
  - App

- **Supervisor Mode**
  - Operating System

- **Machine Mode**
  - Firmware

- **Hardware Mode**
  - Trusted SoC

---

nwistoff@iis.ee.ethz.ch - SSH-SoC - July 9th, 2023
Threat Model

User Mode

Supervisor Mode

Operating System

Machine Mode

Firmware

Hardware Mode

Trusted SoC

Untrusted!
Threat Model

Untrusted

User Mode
App

Supervisor Mode
Operating System

Machine Mode
Secure Monitor (SM)

Hardware Mode
Trusted SoC

Enclave

App

Runtime

SSH - SoC

nwistoff@iis.ee.ethz.ch - SSH-SoC - July 9th, 2023
Threat Model

Untrusted

Enclave

User Mode

Untrusted

Enclave

Risk Model

Operating System

Isolation using Physical Memory Protection (PMP)

Hardware Mode

Secure Monitor (SM)

App

App

Runtime

Trusted SoC
Physical Memory Protection (PMP)

Set of control and status registers (CSRs) define permitted memory ranges.

Check each memory access against PMP configuration.

- RISC-V CPU
- PMPs
- Interconnect
- Main Memory
- Peripherals

access fault!
PMP in Heterogeneous Systems

- RISC-V CPU
- Heterogeneous CPU
- Accelerator (e.g. DMA)
- Off-Chip Interface

Interconnect

- Main Memory
- Peripherals
PMP in Heterogeneous Systems

- RISC-V CPU
- Heterogeneous CPU
- Accelerator (e.g. DMA)
- Off-Chip Interface

PMPs

Interconnect

Main Memory

Peripherals

RISC-V CPU

Heterogeneous CPU

Accelerator (e.g. DMA)

Off-Chip Interface

Main Memory

Peripherals
I/O Physical Memory Protection (IOPMP)

- RISC-V CPU
- Heterogeneous CPU
- Accelerator (e.g. DMA)
- Off-Chip Interface

- PMPs
- Protego
- Protego
- Protego

- Interconnect
- Main Memory
- Peripherals

IOPMP unit
Protego Architecture

Contains **memory ranges** and corresponding **permissions**
Protego Architecture

Protego

- PMP W
- PMP R
- Bound Check
- AXI Demux
- Error Slave

Access permitted?

 CFG

AR
AW
AXI req

Burst within 4K region?
Protego Architecture

Protego

PMP Config

PMP W

PMP R

Bound Check

AXI Demux

Error Slave

AR

AW

AXI req

CFG

nristoff@iis.ee.ethz.ch - SSH-SoC - July 9th, 2023
Case Study: DMA Attack

**PMP** denies access to protected memory region

![Diagram showing the components of an RISC-V CPU, PMPs, DMA, Interconnect, Main Memory, and Peripherals. The PMP is shown denying access to a protected memory region.]
Case Study: DMA Attack

DMA can be programmed to access protected memory instead, bypassing PMP.
Case Study: DMA Attack

Protego extends PMP to heterogeneous system masters
Area vs. Timing

Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AXI4 address width</td>
<td>64 bits</td>
</tr>
<tr>
<td>AXI4 data width</td>
<td>64 bits</td>
</tr>
<tr>
<td>AXI4 ID width</td>
<td>4 bits</td>
</tr>
<tr>
<td>AXI4 user width</td>
<td>1 bit</td>
</tr>
<tr>
<td>Inflight transactions</td>
<td>4</td>
</tr>
<tr>
<td>Number of IOPMP entries</td>
<td>16</td>
</tr>
<tr>
<td>IOPMP granularity</td>
<td>4 KiB</td>
</tr>
</tbody>
</table>

GF22FDX, 0.8V, 25°C

- Reaches up to **2 GHz**
- Low area overhead
Area Breakdown

Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AXI4 address width</td>
<td>64 bits</td>
</tr>
<tr>
<td>AXI4 data width</td>
<td>64 bits</td>
</tr>
<tr>
<td>AXI4 ID width</td>
<td>4 bits</td>
</tr>
<tr>
<td>AXI4 user width</td>
<td>1 bit</td>
</tr>
<tr>
<td>Inflight transactions</td>
<td>4</td>
</tr>
<tr>
<td>Number of IOPMP entries</td>
<td>16</td>
</tr>
<tr>
<td>IOPMP granularity</td>
<td>4 KiB</td>
</tr>
</tbody>
</table>

PMP logic consumes most area

GF22FDX, 0.8V, 25° C, 1.4 GHz
Existing IOPMP Work

- RISC-V draft specification [1]
- Few recent implementations exist
  - DITES [2]
    - 3889 LUTs, 1211 Registers
  - IOPMP [3]
    - 6 cycles, 1GHz, ca. 380 kGE
- To the best of our knowlegde, **first open-source implementation**

---


Conclusion

- **Protego**: configurable IOPMP for RISC-V
- Allows for physical memory protection in heterogeneous systems
- Ultra-low hardware overhead of ca. **40 kGE**, running at up to **2 GHz**
- Available **open source**

Thank you!
IOPMP Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AXI4 address width</td>
<td>64 bits</td>
</tr>
<tr>
<td>AXI4 data width</td>
<td>64 bits</td>
</tr>
<tr>
<td>AXI4 ID width</td>
<td>4 bits</td>
</tr>
<tr>
<td>AXI4 user width</td>
<td>1 bit</td>
</tr>
<tr>
<td>Inflight transactions</td>
<td>4</td>
</tr>
<tr>
<td>Number of IOPMP entries</td>
<td>16</td>
</tr>
<tr>
<td>IOPMP granularity</td>
<td>4 KiB</td>
</tr>
</tbody>
</table>

At compile-time

At run-time

- `iopmp_addrx`:
  - `addr[54:2]`

- `iopmpCfgx`:
  - `L reserved Mode X W R`
  - 1 2 2 1 1 1