RISC-V S-mode Physical Memory Protection for Hypervisor

Editor - Dong Du and Sandro Pinto

Version 0.1, 11/2023: This document is in development. Assume everything can change. See http://riscv.org/spec-state for details.

Table of Contents

Preamble

This document is in the Development state

Assume everything can change. This draft specification will change before being accepted as standard, so implementations made to this draft specification will likely not conform to the future standard.

Copyright and license information

Contributors

The proposed specifications (non-ratified, under discussion) has been contributed to directly or indirectly by:

- Dong Du, Editor <dd_nirvana@sjtu.edu.cn>
- Sandro Pinto, Editor <sandro.pinto@dei.uminho.pt>
- Bicheng Yang
- Jose Martins

Chapter 1. Introduction

RISC-V S-mode Physical Memory Protection (SPMP) is an extension to provide isolation when MMU is unavailable or disabled. This specification introduces the extension to support SPMP and hypervisor extension.

Chapter 2. Specification

There are some changes (besides sspmp) to support both SPMP and hypervisor extension.

2.1. vSPMP extension

This extension describes how SPMP is used in a guest VM.

1. A set of vSPMP CSRs for the VS-mode are required, including 64 vSPMP address registers and 16 configuration registers. When V=1, vSPMP CSR substitutes for the usual SPMP CSR, so instructions that normally read or modify SPMP CSR access vSPMP CSR instead. This is consistent with the paging in VS-mode (i.e., vsatp).
2. For HLV, HLVX, and HSV instructions, the hardware should check vSPMP before G-stage address translation (or hgPMP protection when hgatp.BARE is set to zero).
3. The vSPMP checking is performed in the guest physical addresses before G-stage address translation (or hgPMP protection when hgatp.BARE is set to zero).

2.2. hgPMP extension

This extension describes how SPMP protects a hypervisor from guests (only enabled when hgatp.BARE is set to zero).

1. When hgPMP is enabled, all guest memory accesses will be checked by hgPMP; while hypervisor (in HS mode) and HU mode applications will not be affected.
2. A set of hgPMP CSRs for the HS-mode are required, including 64 hgPMPaddr address registers and 16 hgPMPcfg configuration registers. When V=1, and hgatp.MODE=Bare, hgPMP provides isolation between the hypervisor and guest VMs.
3. XLEN-bit read/write hgpmpswitch0 and hgpmpswitch1 CSRs are also provided in hgPMP, which are identical to spmpswitch0 and spmpswitch1 shown in Figure 7. Only hgpmpswitch0 is used for RV64. During the context switch, the hypervisor can simply store and restore hgpmpswitch (we use hgpmpswitch to represent either hgpmpswitch0 or hgpmpswitch1) as part of the context. An hgPMP entry is activated only when both corresponding bits in hgpmpswitch and A field of hgpmpicfg are set. (i.e., hgpmpswitch[i] & hgpmpicfg.A)
4. The hgPMP checking is performed after the guest address translation (or vSPMP checking), before PMP checking.

As hgPMP does not apply to the hypervisor, the encodings of configuration registers are simplified in the following table.

The encodings of hgpmpcfg are shown in the table:

Bits on *hgpmpcfg* register				**Result**
S	R	W	X	V Mode (VS + VU)
0	0	0	0	Inaccessible region (Access Exception)

Bits on *hgpmpcfg* register				Result
0	0	0	1	Execute-only region
0	1	0	0	Read-only region
0	1	0	1	Read/Execute region
0	1	1	0	Read/Write region
0	1	1	1	Read/Write/Execute region
Others				Reserved