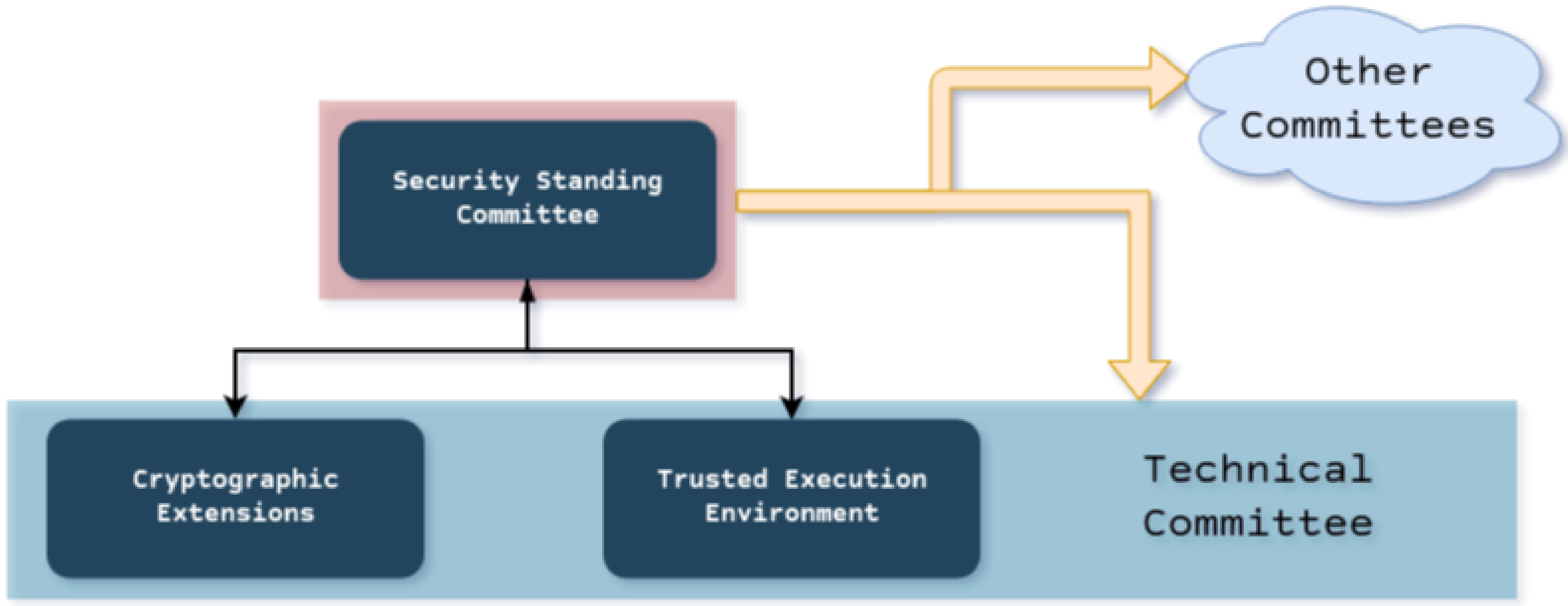
Updates from the RISC-V TEE Group

Nick Kossifidis <mick@ics.forth.gr>

Security-related RISC-V Task Groups



About the TEE Task Group

- **One of the most popular groups (112 registered members)**
- **Regular conference calls / mailing list**
- **Its mission is:**
  - To define an architecture specification for supporting Trusted Execution Environments on RISC-V processors
  - To provide necessary implementation guidelines and/or recomendations in order to assist developers to realize the specification
  - To enable the development of necessary components (hardware and software) to support the specification

Work in progress

- **On the hardware side**
  - Modifications on the Physical Memory Protection (PMP) mechanism
  - Proposal for an I/O Physical Memory Protection (IOPMP) block
  - Proposal for a Control Flow Integrity (CFI) extension
- **On the software side**
  - Secure Monitor architecture
- **TODO**
  - Secure Boot
  - ...

Physical Memory Protection on RISC-V

- Part of the Machine ISA (Privilege Spec)
- Per-hart firewall for physical memory access
- 32bit addresses for RV32, 56bit for RV64
- 4 address matching modes
- R/W/X permission handling

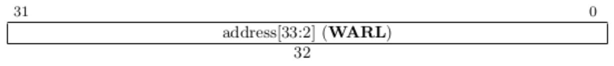


Figure 3.26: PMP address register format, RV32.

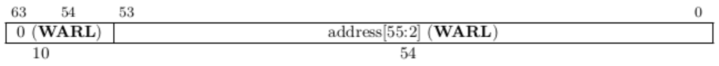


Figure 3.27: PMP address register format, RV64.

A	Name	Description
0	OFF	Null region (disabled)
1	TOR	Top of range
2	NA4	Naturally aligned four-byte region
3	NAPOT	Naturally aligned power-of-two region, ≥8 bytes

Table 3.8: Encoding of A field in PMP configuration registers.

pmpaddr	pmpcfg.A	Match type and size
yyyy...yyyy	NA4	4-byte NAPOT range
yyyy...yyy0	NAPOT	8-byte NAPOT range
yyyy...yy01	NAPOT	16-byte NAPOT range
yyyy...y011	NAPOT	32-byte NAPOT range
...	...	...
yy01...1111	NAPOT	2^{XLEN}-byte NAPOT range
y011...1111	NAPOT	2^{XLEN+1}-byte NAPOT range
0111...1111	NAPOT	2^{XLEN+2}-byte NAPOT range
1111...1111	NAPOT	2^{XLEN+3}-byte NAPOT range

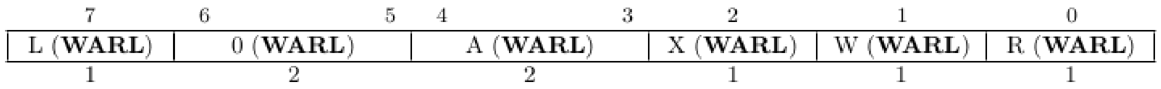
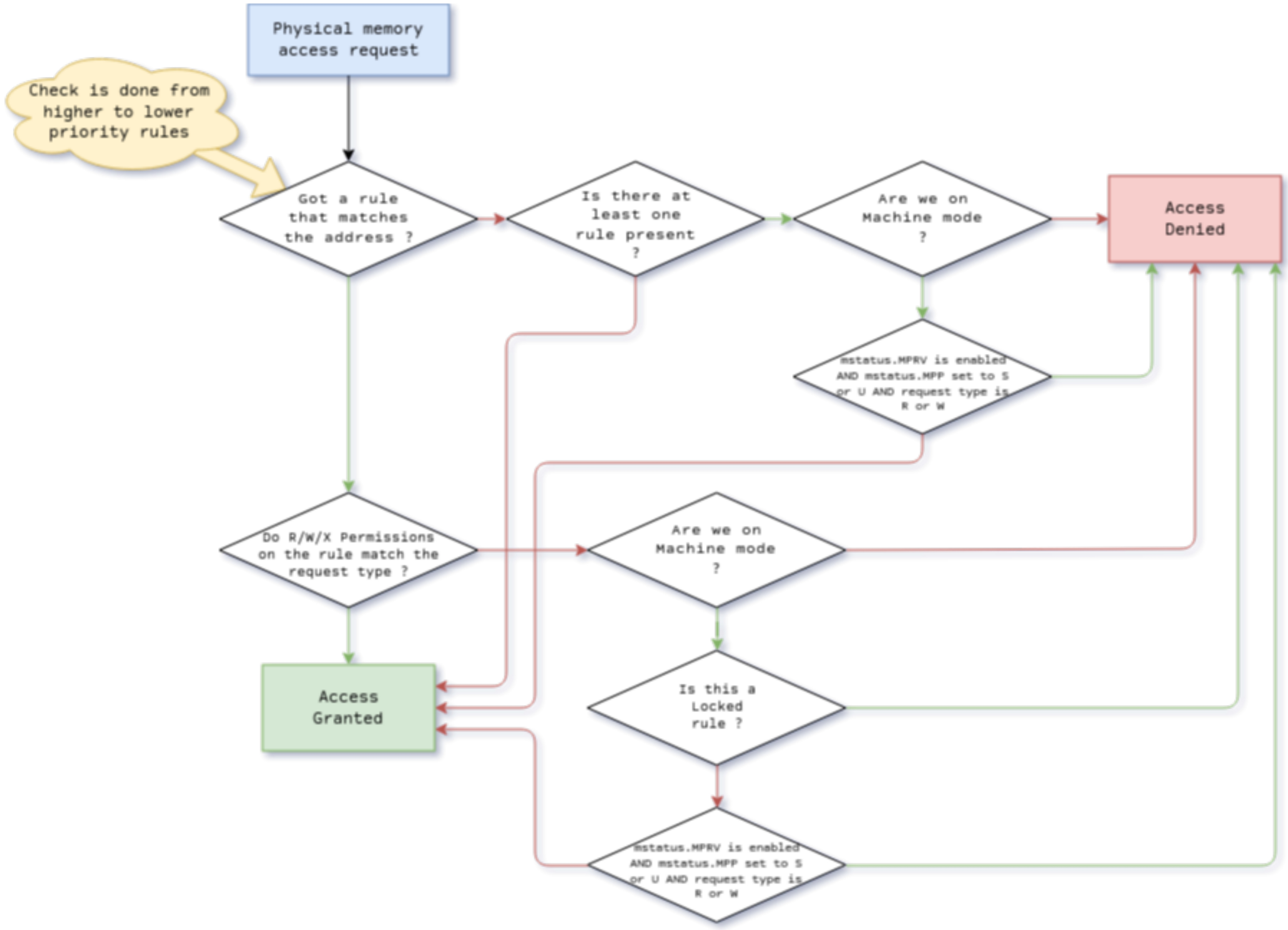


Figure 3.28: PMP configuration register format.

Physical Memory Protection on RISC-V


Physical memory access request
Check is done from higher to lower priority rules
Got a rule that matches the address ?
Is there at least one rule present ?
Are we on Machine mode ?
Access Denied
mstatus.MPRV is enabled AND mstatus.MPP set to S or U AND request type is R or W
Do R/W/X Permissions on the rule match the request type ?
Are we on Machine mode ?
Access Granted
Is this a Locked rule ?
mstatus.MPRV is enabled AND mstatus.MPP set to S or U AND request type is R or W

Virtual memory protection on RISC-V

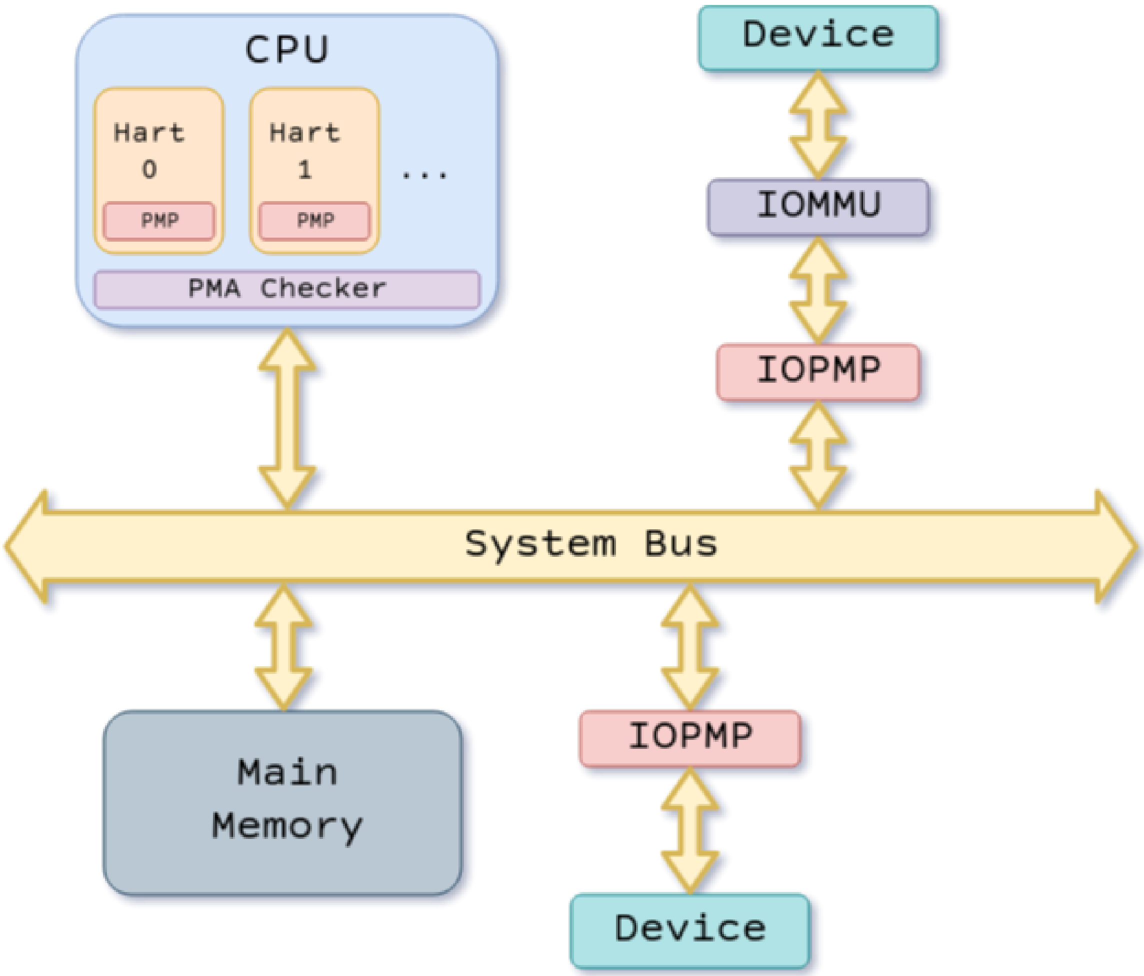
- Part of the Supervisor ISA (Privilege Spec)
- 32bit virtual addresses for RV32, 39/48bit for RV64
- Radix-tree page table, 4KiB pages with support for 4MiB (RV32) and 2MiB (RV64) “megapages”, 1GiB “gigapages” and 512GiB “terapages” (RV64)
- Each table entry handles R/W/X permissions and the U permission that allows access to that entry from U mode (else it’s S mode only)
- The sstatus.SUM bit allows Supervisor to R/W User mode pages (SMAP) (execution of User mode memory from Supervisor is always denied)
- The sstatus.MXR bit allows executable only pages to also be treated as readable

Proposed PMP modifications

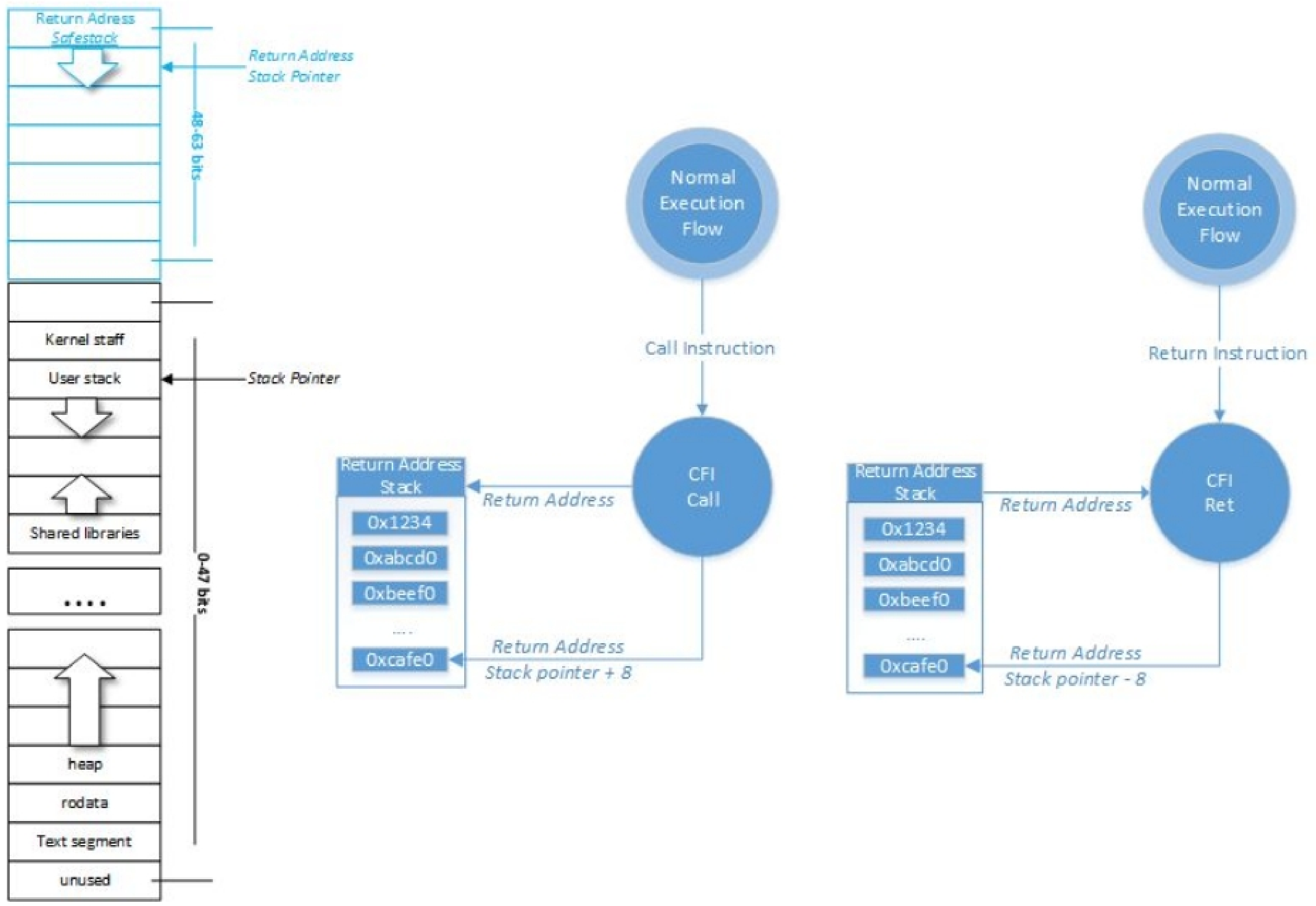
- Currently the only way to limit M mode's access is to use Locked entries, however locked entries are permanent until a hart reset is performed + are also enforced on S/U modes which doesn't make sense since S/U modes can't modify PMP settings anyway (so locking an entry only makes sense for M mode)
- We want to prevent M mode from accessing memory that belongs to S/U modes, to provide the equivalent of S mode's sstatus.SUM bit
- We want to have locked rules that are only enforced on M mode but not on S/U modes (e.g. to allow M mode to only have execute permission, without also allowing S/U to have the same privilege)
- Say hello to Machine Mode Isolation bit on mstatus (mstatus.MMI) !

L bit on pmpcfg	mstatus.MMI	Meaning
0	0	Temporary entry; R/W/X enforced on sub-M modes; M-mode succeeds
0	1	Temporary entry; R/W/X enforced on sub-M modes; M-mode fails
1	0	Locked entry; R/W/X enforced on all modes
1	1	Locked entry; R/W/X enforced on M-mode; sub-M modes fails

I/O PMP Block proposal



Control Flow Integrity extension proposal



Secure Monitor’s architecture

Current implementations from group members

- MultiZone from HexFive (https://hex-five.com/products/)
- Keystone from UC Berkeley (https://keystone-enclave.org/)

A lot of work to be done !

- Define APIs between TEEs and between TEEs and the rest of the world (we need to work together with the upcoming platform specification task group e.g. for the SBI part)
- Define a memory isolation scheme using PMP (there is a draft proposal on that)
- Define a memory isolation scheme for I/O PMP
- Define mechanisms for handling multiple harts
- Define mechanisms for interupt handling / delegation
- Define common format for TEE binaries (e.g. ELF with extras)
- Write code for all of the above and test it
- Provide an SDK
- ...

Questions ?

Thank you !