RISC-V arch test
Module: Privileged spec
Task 6

Test Description:

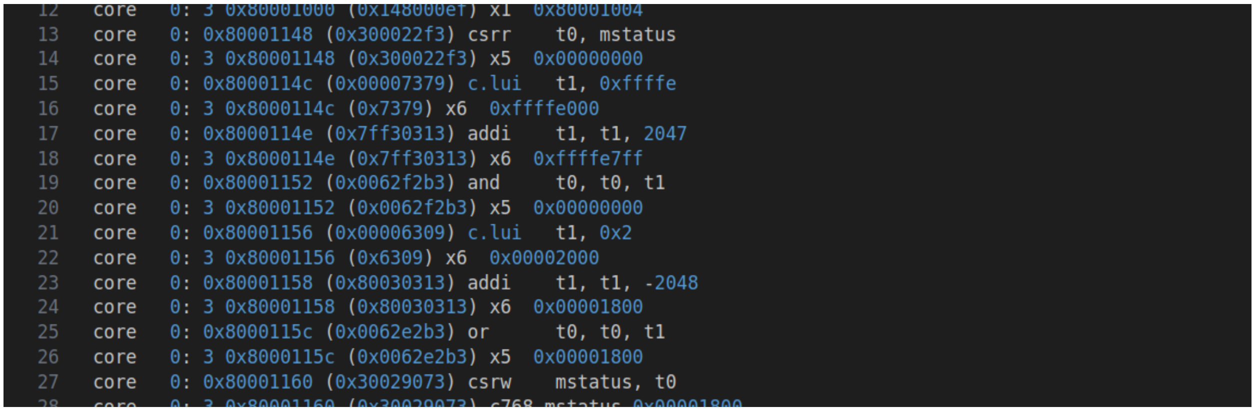
This test has changed the permissions of the locked RWX pmp region to read only using mseccfg (machine security configuration) extension. So, in this test I have configured two PMP regions one is TOR (Top of range) and the second one is NAPOT (Naturally aligned power of two) and. The first region is configured as a locked region with R/W/X permissions and this is the region whose permission I can change from RWX to R only. The second region is locked with execute permissions only and this is the region for the .text segment of the program.

I assigned the previously mentioned permissions to the region using the pmpcfg0 register. After assigning the permissions I did read and write from the first one TOR region. The read and write from this region succeeded because it has the read/write/execute permissions.

After that I set the MML (Machine Mode Lockdown) bit in mseccfg register to change the R/W/X permissions to Read-only.

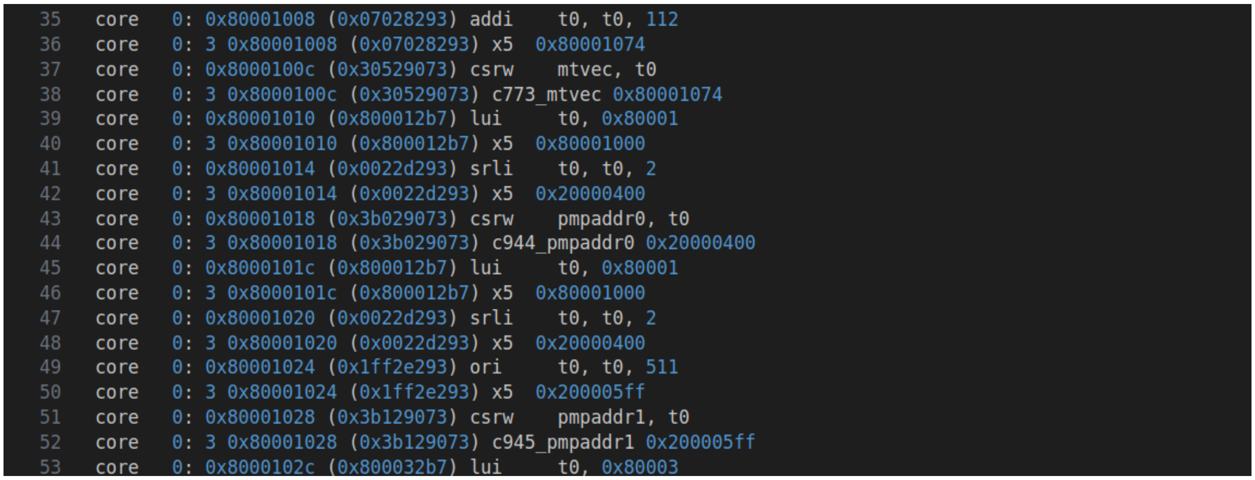
Then again I did read and write from the first one TOR region and now the read operation succeeded but write has failed because the permissions are changed from RWX to R only now. The change of permissions can be seen from the picture below with row having R W X permissions and the last two columns having mseccfg.MLL=1 and pmpcfg.L=1.

Snapshots:



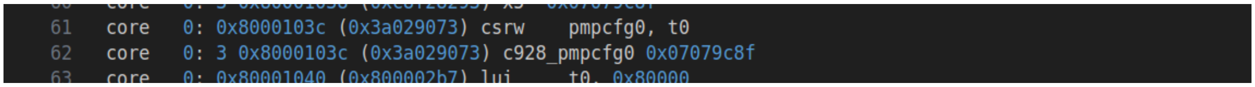
```
core   0: 3 0x80001000 (0x148000ef) x1  0x80001004
core   0: 0x80001148 (0x300022f3) csrr    t0, mstatus
core   0: 3 0x80001148 (0x300022f3) x5  0x00000000
core   0: 0x8000114c (0x00007379) c.lui   t1, 0xffffe
core   0: 3 0x8000114c (0x7379) x6  0xffffe000
core   0: 0x8000114e (0x7ff30313) addi    t1, t1, 2047
core   0: 3 0x8000114e (0x7ff30313) x6  0xffffe7ff
core   0: 0x80001152 (0x0062f2b3) and     t0, t0, t1
core   0: 3 0x80001152 (0x0062f2b3) x5  0x00000000
core   0: 0x80001156 (0x00006309) c.lui   t1, 0x2
core   0: 3 0x80001156 (0x6309) x6  0x00002000
core   0: 0x80001158 (0x80030313) addi    t1, t1, -2048
core   0: 3 0x80001158 (0x80030313) x6  0x00001800
core   0: 0x8000115c (0x0062e2b3) or      t0, t0, t1
core   0: 3 0x8000115c (0x0062e2b3) x5  0x00001800
core   0: 0x80001160 (0x30029073) csrw    mstatus, t0
core   0: 3 0x80001160 (0x30029073) c768_mstatus 0x00001800
```

Switch to machine mode



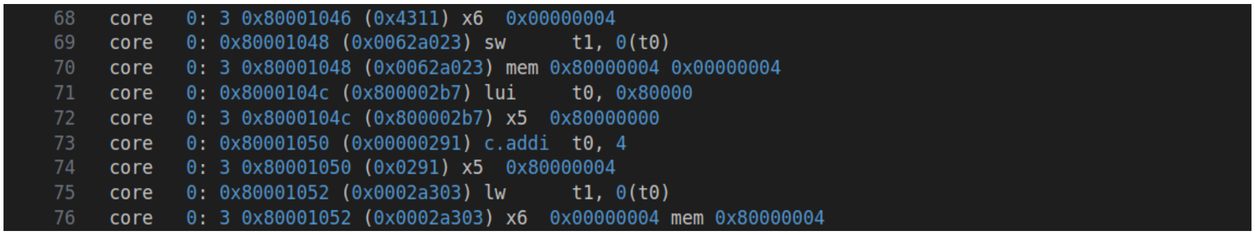
```
core   0: 0x80001008 (0x07028293) addi    t0, t0, 112
core   0: 3 0x80001008 (0x07028293) x5  0x80001074
core   0: 0x8000100c (0x30529073) csrw    mtvec, t0
core   0: 3 0x8000100c (0x30529073) c773_mtvec 0x80001074
core   0: 0x80001010 (0x800012b7) lui     t0, 0x80001
core   0: 3 0x80001010 (0x800012b7) x5  0x80001000
core   0: 0x80001014 (0x0022d293) srli    t0, t0, 2
core   0: 3 0x80001014 (0x0022d293) x5  0x20000400
core   0: 0x80001018 (0x3b029073) csrw    pmpaddr0, t0
core   0: 3 0x80001018 (0x3b029073) c944_pmpaddr0 0x20000400
core   0: 0x8000101c (0x800012b7) lui     t0, 0x80001
core   0: 3 0x8000101c (0x800012b7) x5  0x80001000
core   0: 0x80001020 (0x0022d293) srli    t0, t0, 2
core   0: 3 0x80001020 (0x0022d293) x5  0x20000400
core   0: 0x80001024 (0x1ff2e293) ori     t0, t0, 511
core   0: 3 0x80001024 (0x1ff2e293) x5  0x200005ff
core   0: 0x80001028 (0x3b129073) csrw    pmpaddr1, t0
core   0: 3 0x80001028 (0x3b129073) c945_pmpaddr1 0x200005ff
core   0: 0x8000102c (0x800032b7) lui     t0, 0x80003
```

Select pmpaddr for region 1 and 2



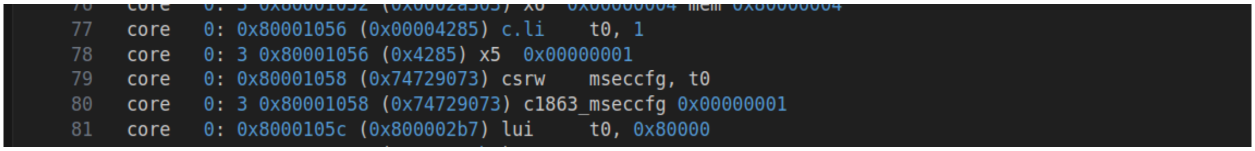
```
core   0: 0x8000103c (0x3a029073) csrw    pmpcfg0, t0
core   0: 3 0x8000103c (0x3a029073) c928_pmpcfg0 0x07079c8f
core   0: 0x80001040 (0x800002b7) lui     t0, 0x80000
```

Configure locked regions using pmpcfg



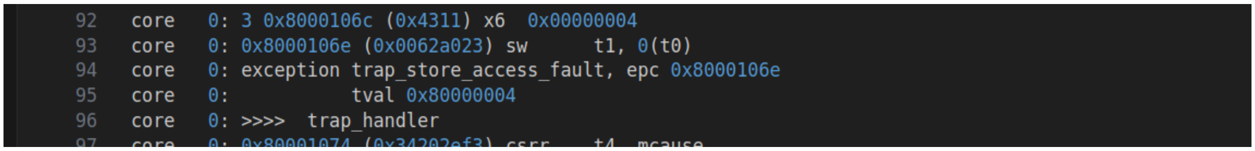
```
core   0: 3 0x80001046 (0x4311) x6  0x00000004
core   0: 0x80001048 (0x0062a023) sw      t1, 0(t0)
core   0: 3 0x80001048 (0x0062a023) mem 0x80000004 0x00000004
core   0: 0x8000104c (0x800002b7) lui     t0, 0x80000
core   0: 3 0x8000104c (0x800002b7) x5  0x80000000
core   0: 0x80001050 (0x00000291) c.addi  t0, 4
core   0: 3 0x80001050 (0x0291) x5  0x80000004
core   0: 0x80001052 (0x0002a303) lw      t1, 0(t0)
core   0: 3 0x80001052 (0x0002a303) x6  0x00000004 mem 0x80000004
```

no load store faults



```
core   0: 0x80001056 (0x00004285) c.li    t0, 1
core   0: 3 0x80001056 (0x4285) x5  0x00000001
core   0: 0x80001058 (0x74729073) csrw    mseccfg, t0
core   0: 3 0x80001058 (0x74729073) c1863_mseccfg 0x00000001
core   0: 0x8000105c (0x800002b7) lui     t0, 0x80000
```

update region to read only



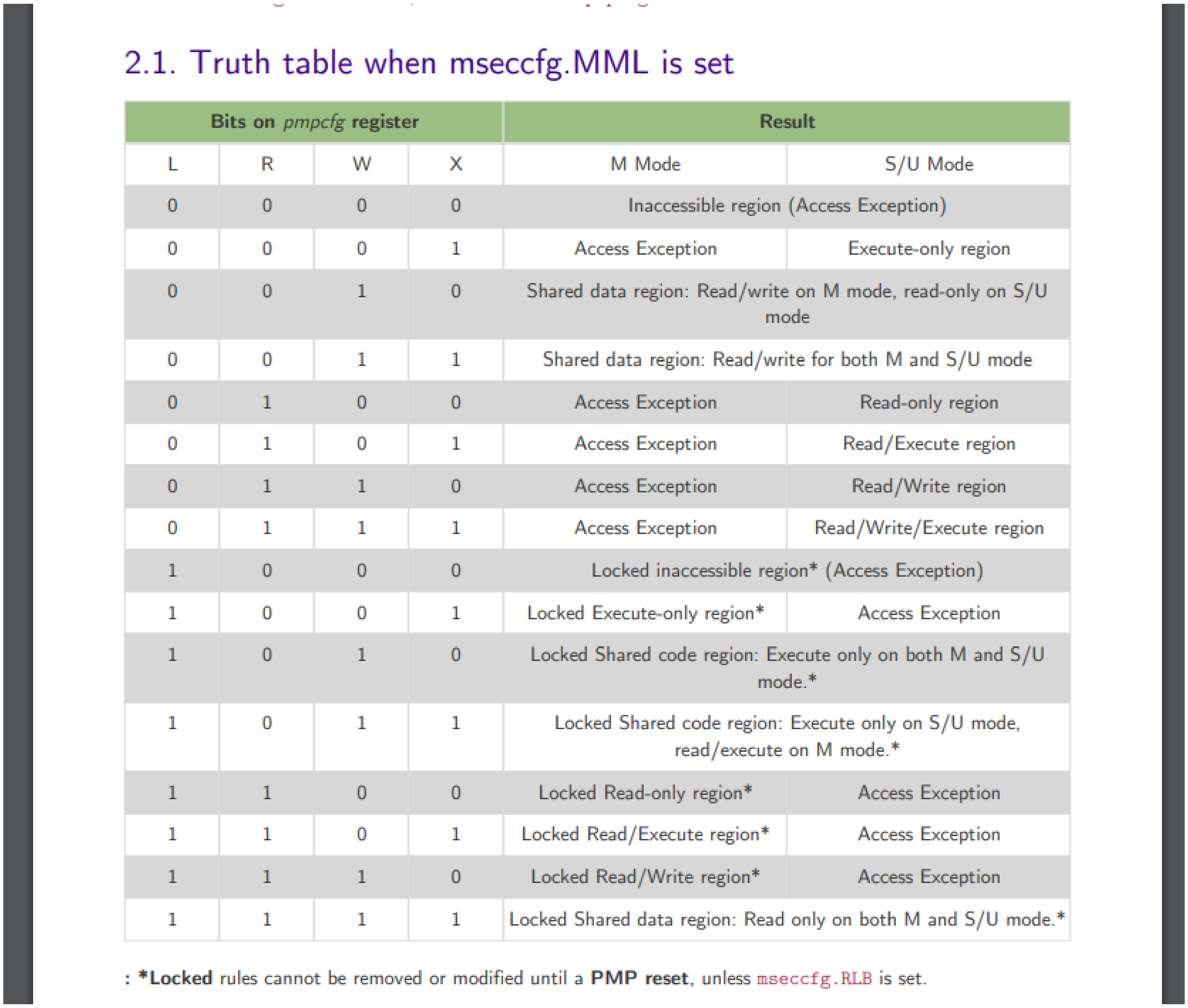
```
core   0: 3 0x8000106c (0x4311) x6  0x00000004
core   0: 0x8000106e (0x0062a023) sw      t1, 0(t0)
core   0: exception trap_store_access_fault, epc 0x8000106e
core   0:           tval 0x80000004
core   0: >>>>  trap_handler
core   0: 0x80001074 (0x34202ef3) csrr    t4, mcause
```

Store access fault after changing permission

What two things happen when you configure a locked pmp region??
When configured a locked pmp region,Pmp specified permissions defined in pmpcfg0 register are enforced on all privileged modes. Pmp entry get locked that write to the configuration register and modify theaddress registers are ignored and when trying to modify it will cause illegal instruction exceptions.

Try to change permissions of that region to only read from read,write and execute. How it can be achieved using smepmp extension.
This can be achieved by setting the mseccfg.MML bit in mseccfg register. This behavior is defined in the smepmp specification.

Reference:



2.1. Truth table when mseccfg.MML is set

Bits on *pmpcfg* register				**Result**	
L	R	W	X	M Mode	S/U Mode
0	0	0	0	Inaccessible region (Access Exception)	
0	0	0	1	Access Exception	Execute-only region
0	0	1	0	Shared data region: Read/write on M mode, read-only on S/U mode	
0	0	1	1	Shared data region: Read/write for both M and S/U mode	
0	1	0	0	Access Exception	Read-only region
0	1	0	1	Access Exception	Read/Execute region
0	1	1	0	Access Exception	Read/Write region
0	1	1	1	Access Exception	Read/Write/Execute region
1	0	0	0	Locked inaccessible region* (Access Exception)	
1	0	0	1	Locked Execute-only region*	Access Exception
1	0	1	0	Locked Shared code region: Execute only on both M and S/U mode.*	
1	0	1	1	Locked Shared code region: Execute only on S/U mode, read/execute on M mode.*	
1	1	0	0	Locked Read-only region*	Access Exception
1	1	0	1	Locked Read/Execute region*	Access Exception
1	1	1	0	Locked Read/Write region*	Access Exception
1	1	1	1	Locked Shared data region: Read only on both M and S/U mode.*	

: ***Locked** rules cannot be removed or modified until a **PMP reset**, unless `mseccfg.RLB` is set.