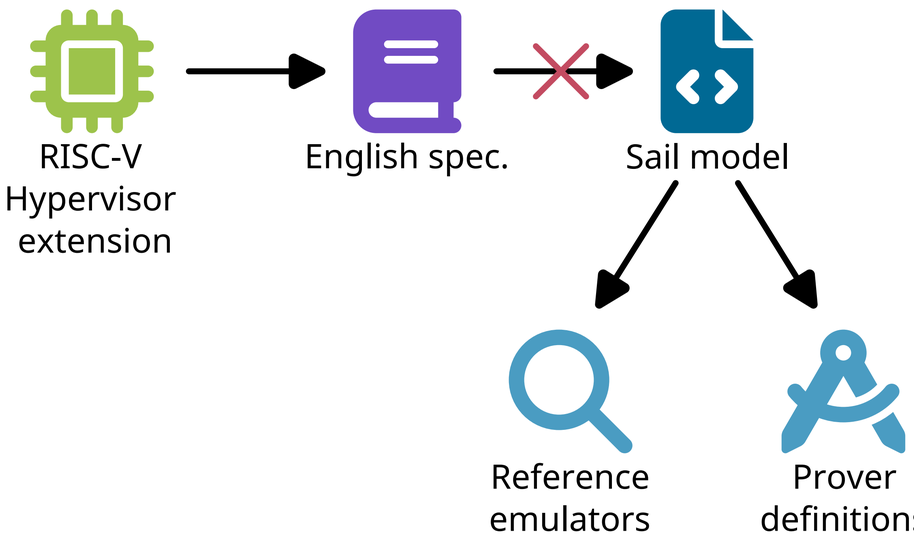
RISC-V Hypervisor extension formalization in Sail

Lowie Deferme[1], Dominique Devriese[1]

[1]DistriNet, KU Leuven, 3001 Leuven, Belgium

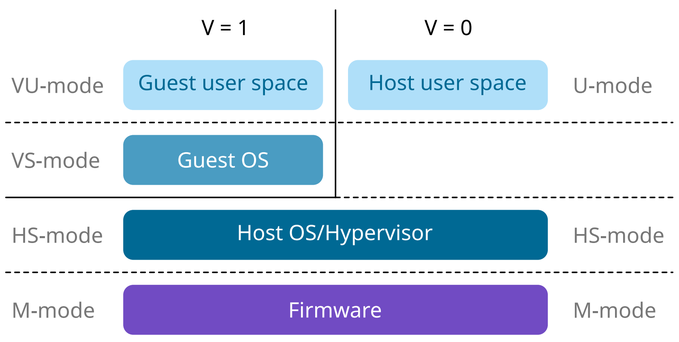
Introduction



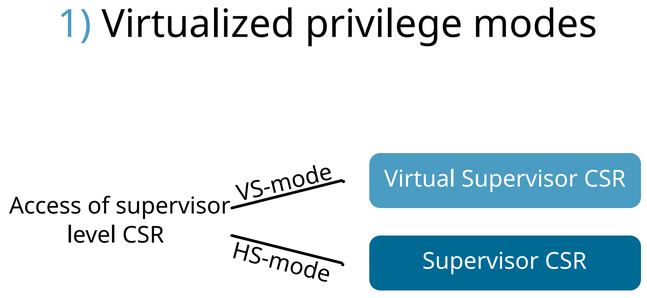
Apart from the prose specification, RISC-V semantics are defined in a domain specific language called Sail. This Sail model is unambiguous and allows to extract functionally correct reference emulators and definitions for theorem provers. Unfortunately, not all ratified extensions are implemented in this model.

One such missing extension is the Hypervisor extension. This extension provides hardware support for virtualization.

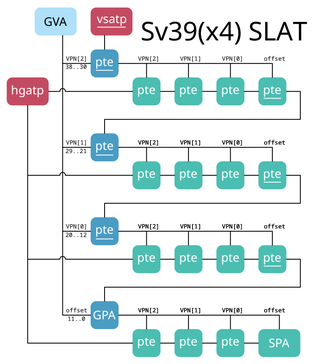
Hypervisor Extension



1) Virtualized privilege modes



2) Supervisor level register banking



3) Second Level Address Translation

Unit tests

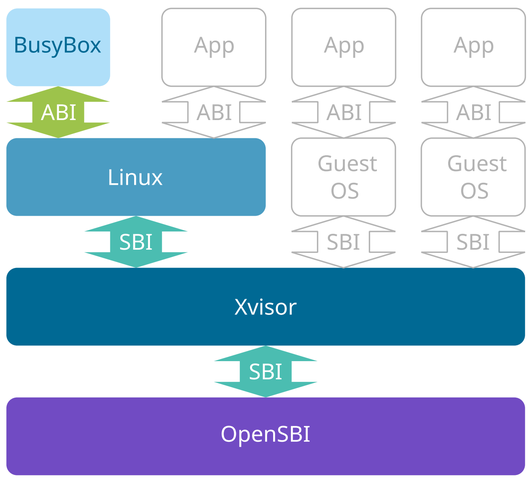
1) Bundled unit tests
   - *Limitation*: Only check for regressions
2) Self-written unit tests
   - *Risk*: same misinterpretation in test and model
   - *Mitigation*: unit tests are validated against other models (Spike)
3) Third-party test suites
   - *Risk*: dependent on other aspects of the ISA that might not be implemented.
   - *Mitigation:* manual inspection of traces of failing tests

Used 3rd party test suites

Real-world hypervisor

1) Emulator
   - Extracted from Sail model
2) OpenSBI
   - "Supervisor Binary Interface"
3) **Xvisor**
   - Type I hypervisor
   - Makes use of H-extension
4) Linux
   - Guest operating system
5) BusyBox
   - User-space application
   - Common UNIX utilities

Pre-built, containerized stack




```
root@1a3a7c7bc7ce:/hyp# echo "autoexec" | ./sim/sail/c_emulator/riscv_sim_RV64 -Vmem -Vplatform -Vreg -Vinstr  \
--enable-dirty-update --enable-pmp --mtval-has-illegal-inst-bits --xtinst-has-transformed-inst --ram-size 1024 \
--device-tree-blob rv64gch_xvisor.dtb opensbi_xvisor_payload.elf
enabling dirty update.
enabling PMP support.
enabling storing illegal instruction bits in mtval.
enabling storing transformed instruction bits in mtinst and htinst.
...
Trying; cpio
Mounted initrd using cpio at /
INIT: bootcmd: vfs run /boot.xscript
ooooooo  ooooo ooooo     oooo ooooo  .ooooo..o   .ooooo.   oooooooo.
 `8888    d8'   `888.     .8'   `888' d8P'    `Y8  d8P'  `Y8b  `888   `Y88.
   Y888..8P      `888.   .8'    888  Y88bo.      888      888  888   .d88'
    `8888'        `888. .8'     888   `"Y88b.    888      888  888ooo88P'
   .8PY888.        `888.8'      888       `Y88b 888      888  888`88b.
  d8'  `888b        `888'       888  oo     .d8P `88b    d88'  888  `88b.
o888o  o888888o      `8'       o888o 8''88888P'   `Y8bood8P'  o888o  o888o
Created default shared memory
guest0: Created
guest0: Parsing /images/riscv/virt64/nor_flash.list
guest0: Loading 0x0000000000000000 with file ./firmware.bin
...
guest0: Kicked
[guest0/uart0] RISC-V SBI specification v2.0 detected
[guest0/uart0] RISC-V SBI implementation ID=0x2 Version=0x3002
[guest0/uart0]
[guest0/uart0] RISC-V Virt64 Basic Firmware
...
[guest0/uart0] [test] Busybox help
[guest0/uart0] BusyBox v1.32.1 (2024-02-28 17:04:07 UTC) multi-call binary.
[guest0/uart0] BusyBox is copyrighted by many authors between 1998-2015.
[guest0/uart0] Licensed under GPLv2. See source distribution for detailed
[guest0/uart0] copyright notices.
...
```

Results

Unit tests

1) Bundled tests
   - All succeed
2) Self written unit tests
   - 81/81 succeed
3) Third-party tests
   - 133/136 succeed
   - 2 non-hypervisor related
   - 1 suspected error in suite

Real-world hypervisor boots guest OS

Reasonable confidence in correctness of Sail model

No significant inconsistencies between:

1) Natural language specification of H-extension
2) Its use by Xvisor
3) Its implementation in Spike
   - *Minor issue was found, reported and fixed*

KU Leuven
Department of Computer Science
Celestijnenlaan 200A box 2402
3001 Leuven, Belgium

Funded by the European Union

European Research Council
Established by the European Commission