基于 RISC-V 的 Type-1 hypervisor 的设计与实现

毕业设计答辩报告

齐呈祥

指导老师：李罡

2023 年 6 月 6 日

Background

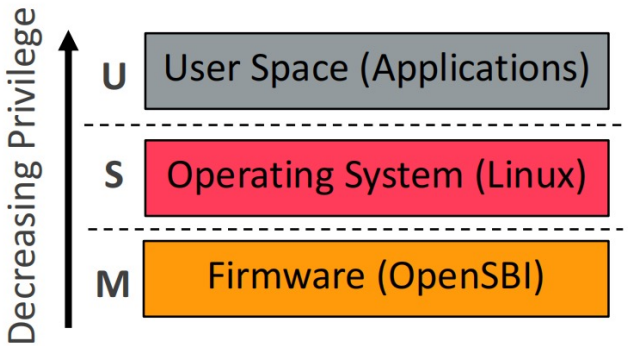
- 为什么需要虚拟化？
  - 数据中心的数量越来越庞大，需要使用虚拟化技术实现数据中心统一管理。
  - 物联网技术的发展，需要虚拟化技术来对物联网系统做安全保障。
- 为什么要在 RISC-V ISA 上做虚拟化？
  - RISC-V 目前是最流行的开源 ISA，在不到十年时间里全世界芯片出货量超过 100 亿颗。
  - RISC-V 为国内突破卡脖子技术的关键技术，国内学术界和工业界都在积极构建基于 RISC-V 架构的产品与社区。

RISC-V: the ISA

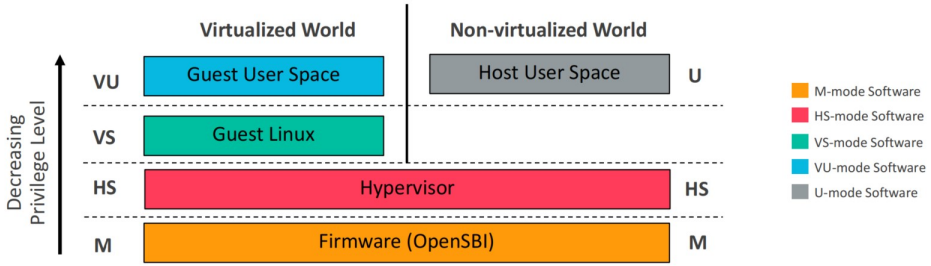
- RISC-V 是一个开放标准 ISA
  - 在 2010 年首次被伯克利开发
  - 与商业/私有标准相区别：x86/ARM
- RISC-V 传统特权级
  - M(Machine)/S(Supervisor)/U(User)
- RISC-V 虚拟化扩展
  - 在 2021 年 11 月正式被批准
  - S(Supervisor) -> HS(Hypervisor Supervisor)/VS(Virtual Supervisor)

RISC-V: the ISA

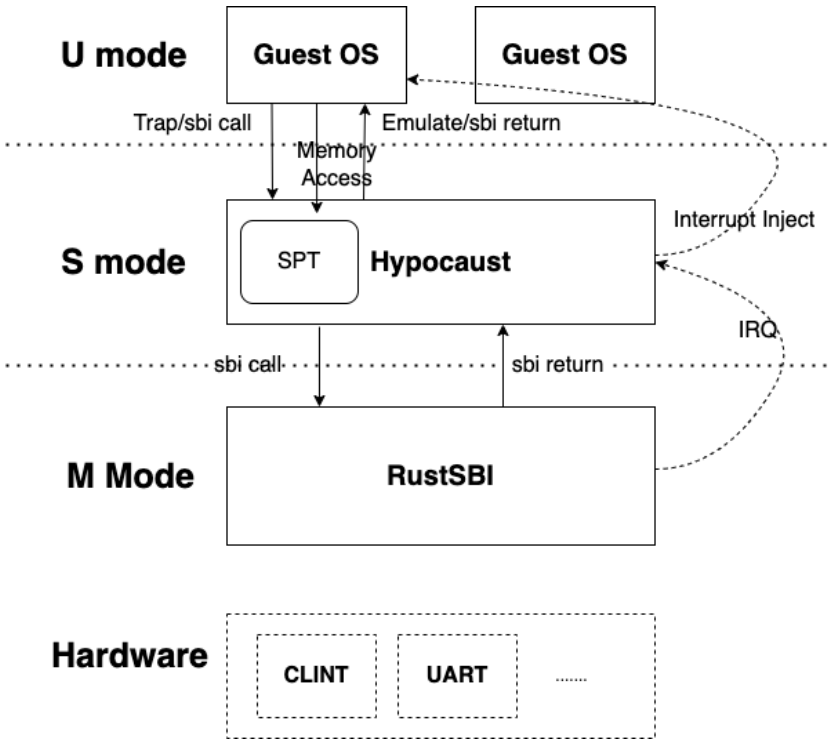
RISC-V 传统特权级



RISC-V Hypervisor Extension 特权级

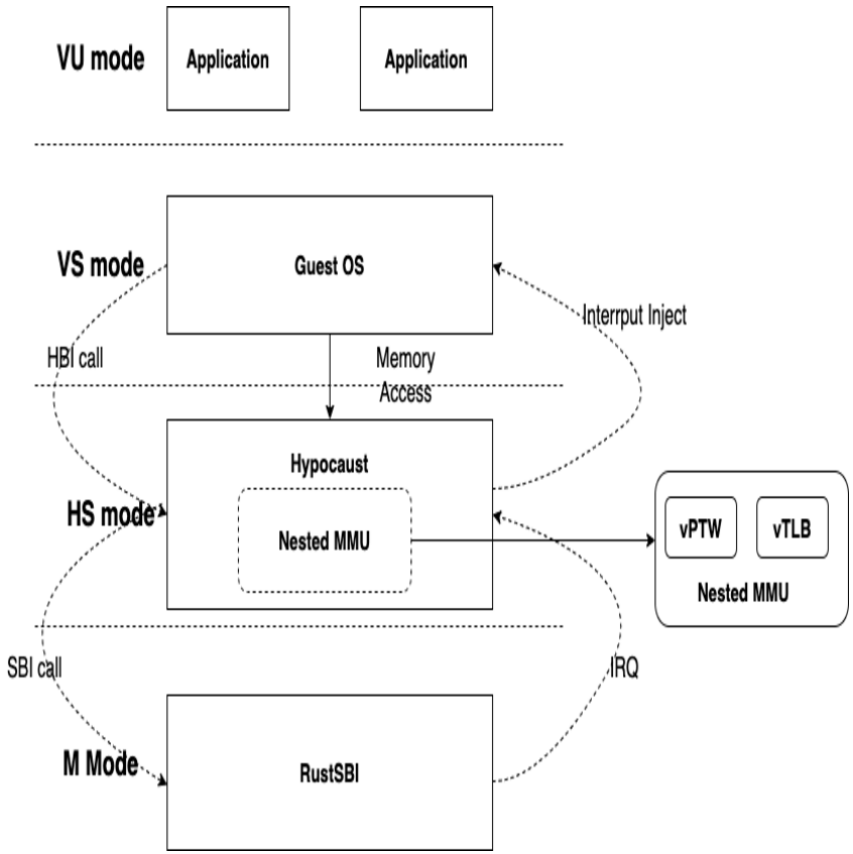


Hypocaust: Design



- CPU 虚拟化：S mode 陷入与模拟
- 内存虚拟化：影子页表技术
- 中断虚拟化：PLIC 模拟与中断转发
- IO 虚拟化：设备透传
- 系统运行：minikernel

Hypocaust-2: Design



- 基于设备树的配置
- RISC-V Hypervisor Extension 辅助虚拟化
- 两阶段页表翻译
- 异常代理与中断转发（PLIC 模拟）
- 设备透传
- 可运行 rCore-Tutorial-v3，RT-Thread 以及 Linux mainline

Capable of booting system

hypocaust-2 启动 RT-Thread

```
[rustsbi] RustSBI version 0.3.1, adapting to RISC-V SBI v1.0.0
[rustsbi] Implementation     : RustSBI-QEMU Version 0.2.0-alpha.2
[rustsbi] Platform Name      : riscv-virtio,qemu
[rustsbi] Platform SMP       : 1
[rustsbi] Platform Memory    : 0x80000000..0x140000000
[rustsbi] Boot HART          : 0
[rustsbi] Device Tree Region : 0xbfe00000..0xbfe00f85
[rustsbi] Firmware Address   : 0x80000000
[rustsbi] Supervisor Address : 0x80200000
[rustsbi] pmp01: 0x00000000..0x80000000 (-wr)
[rustsbi] pmp02: 0x80000000..0x80200000 (---)
[rustsbi] pmp03: 0x80200000..0x140000000 (xwr)
[rustsbi] pmp04: 0x140000000..0x00000000 (-wr)
[Hypervisor] Hello Hypocaust-2!
[Hypervisor] hart id: 0, dtb: 0xbfe00000
[Hypervisor] Hypocaust-2 > running with hardware RISC-V H ISA acceration!
[Hypervisor] Heap initialize finished!
[Hypervisor] test addr: 0x100000, size: 0x1000
[Hypervisor] UART addr: 0x10000000, size: 0x100
[Hypervisor] CLINT addr: 0x2000000, size: 0x10000
[Hypervisor] PLIC addr: 0xc000000, size: 0x600000
[Hypervisor] Initialize hypervisor environment
[Hypervisor] Guest root page table: 0x8082c
[Hypervisor] va: [0x80200000: 0x802829d0)
[Hypervisor] guest va -> [0x80200000: 0x88200000), guest pa -> [0x88200000: 0x90200000)
[Hypervisor] Hypervisor enable paging!
[Hypervisor] remap test passed!
[Hypervisor] allocated hstack: [0xfffffffffffa000: 0xffffffffffffe000)
[Hypervisor] Switch to guest......
[Tracking] write PLIC threshold reg, addr: 0xc201000, value: 0x0
[Tracking] write PLIC threshold reg, addr: 0xc201000, value: 0x0
heap: [0x802829d0 - 0x842829d0]

 \ | /
- RT -     Thread Operating System
 / | \     5.0.0 build Mar  4 2023 15:19:41
 2006 - 2022 Copyright by RT-Thread team
lwIP-2.0.3 initialized!
[I/sal.skt] Socket Abstraction Layer initialize success.
[I/utest] utest is initialize success.
[I/utest] total utest testcase num: (0)
Hello RISC-V
msh />
```

hypocaust-2 启动主线 Linux

```
[    0.460370] remote fence extension is not available in SBI v1.0
[    0.460518] remote fence extension is not available in SBI v1.0
[    0.460631] remote fence extension is not available in SBI v1.0
[    0.460739] remote fence extension is not available in SBI v1.0
[    0.460848] remote fence extension is not available in SBI v1.0
[    0.460958] remote fence extension is not available in SBI v1.0
[    0.461067] remote fence extension is not available in SBI v1.0
[    0.461175] remote fence extension is not available in SBI v1.0
[    0.461283] remote fence extension is not available in SBI v1.0
[    0.461391] remote fence extension is not available in SBI v1.0
[    0.461499] remote fence extension is not available in SBI v1.0
[    0.461607] remote fence extension is not available in SBI v1.0
[    0.461714] remote fence extension is not available in SBI v1.0
[    0.461822] remote fence extension is not available in SBI v1.0
[    0.461929] remote fence extension is not available in SBI v1.0

Please press Enter to activate this console.
~ # ls
[    4.164373] remote fence extension is not available in SBI v1.0
[    4.164625] remote fence extension is not available in SBI v1.0
[    4.167375] remote fence extension is not available in SBI v1.0
[    4.167555] remote fence extension is not available in SBI v1.0
[    4.167715] remote fence extension is not available in SBI v1.0
[    4.167872] remote fence extension is not available in SBI v1.0
[    4.168029] remote fence extension is not available in SBI v1.0
[    4.168186] remote fence extension is not available in SBI v1.0
[    4.168342] remote fence extension is not available in SBI v1.0
[    4.168497] remote fence extension is not available in SBI v1.0
[    4.168651] remote fence extension is not available in SBI v1.0
[    4.168805] remote fence extension is not available in SBI v1.0
[    4.168962] remote fence extension is not available in SBI v1.0
[    4.169119] remote fence extension is not available in SBI v1.0
[    4.169277] remote fence extension is not available in SBI v1.0
[    4.169432] remote fence extension is not available in SBI v1.0
bin         etc         lost+found  sbin        test
dev         linuxrc     proc        sys         usr
~ # echo  Hello World
Hello World
~ #
```

Status&Future Works

项目进程

- 基于 hypocaust/hypocasut-2 的经验，开发了 hypercraft(https://github.com/KuangjuX/hypercraft)，一个 VMM 库，目前适配了由清华大学开发的 ArceOS 并可以类似 KVM 作为 Type-2 hypervisor 启动
- 搭建了一个基于 rocket-chip 带 H Extension 的软核 RISC-V SoC，并正在尝试将 hypocasut-2/hypercraft 跑在 FPGA 上。

未来展望

- 扩展为多核/多 guest
- 实现 RISC-V AIA/IOMMU 驱动以提高性能和安全性
- 等待真实支持硬件虚拟化的 RISC-V 的芯片并移植

Q&A

Q&A

Thanks!