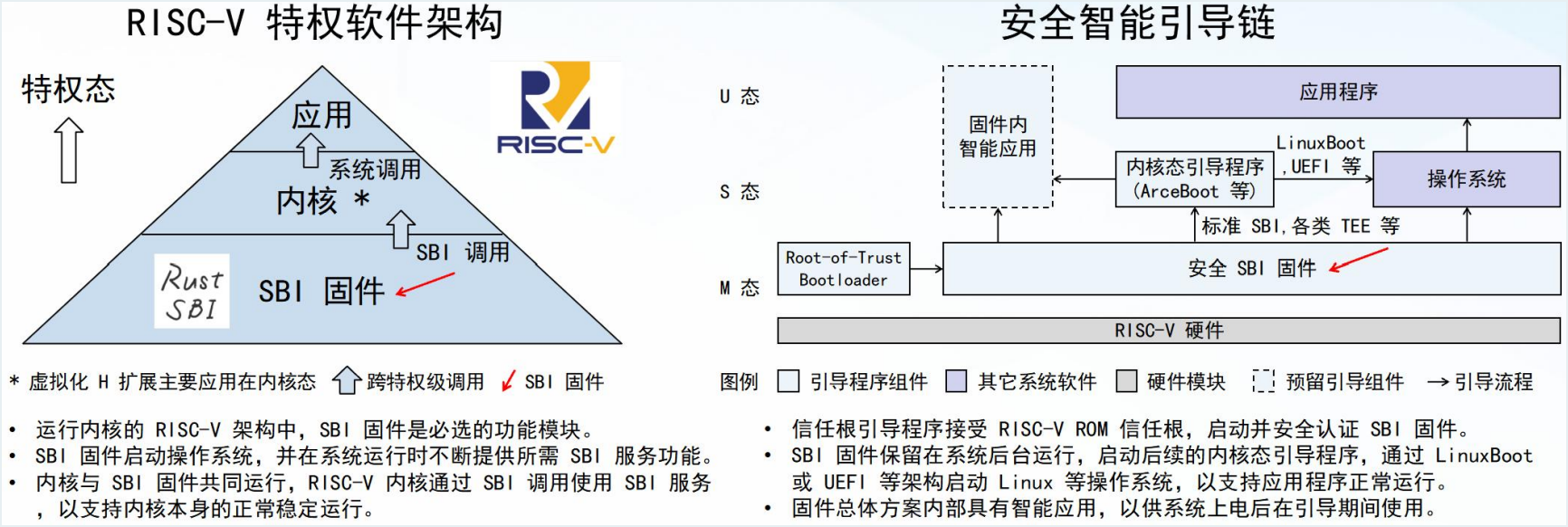
RustSBI 开源安全固件速报（2026）

蒋周奇（洛佳）
中国科学院软件研究所
2026/11/20

中国科学院大学
University of Chinese Academy of Sciences

RustSBI 是什么？

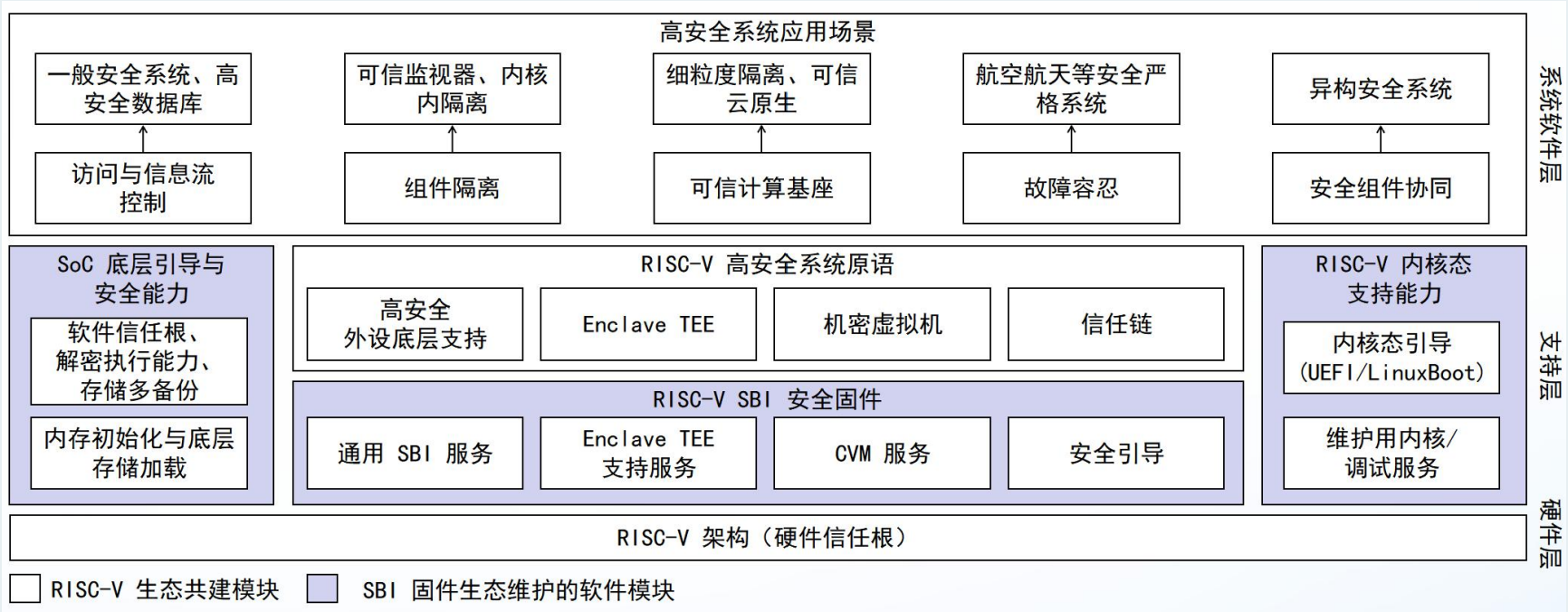


- 运行内核的 RISC-V 架构中，SBI 固件是必选的功能模块。
- SBI 固件启动操作系统，并在系统运行时不断提供所需 SBI 服务功能。
- 内核与 SBI 固件共同运行，RISC-V 内核通过 SBI 调用使用 SBI 服务，以支持内核本身的正常稳定运行。

- 信任根引导程序接受 RISC-V ROM 信任根，启动并安全认证 SBI 固件。
- SBI 固件保留在系统后台运行，启动后续的内核态引导程序，通过 LinuxBoot 或 UEFI 等架构启动 Linux 等操作系统，以支持应用程序正常运行。
- 固件总体方案内部具有智能应用，以供系统上电后在引导期间使用。

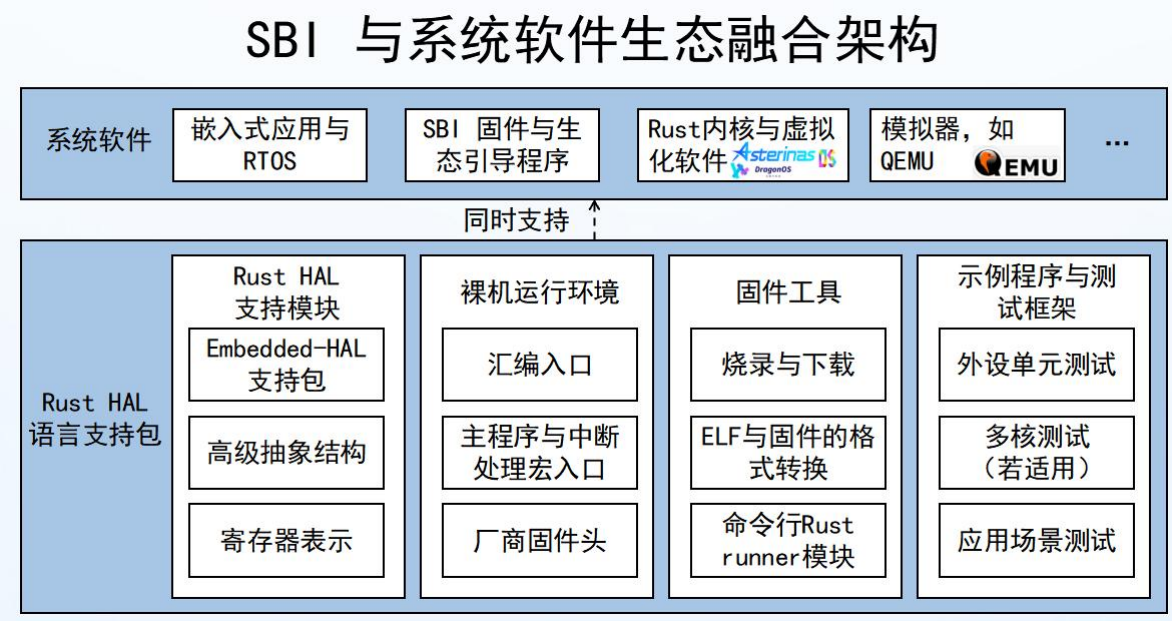
https://github.com/rustsbi/rustsbi

RustSBI 安全固件生态



上层系统软件支持现状

- 支持约 30 款操作系统引导启动
- 支持 U-Boot, EDK II, LinuxBoot 和裸的 SBI 引导途径
- 支持多款硬件平台，含 QEMU 等模拟器和 Miralis 等固件虚拟化设施
- NuttX, AROS, Asterinas 等系统上游支持
- 我们正在建设：全自动板卡 CI 等



lssbi：一条命令诊断您的 SBI 固件

lssbi



`lssbi` lists information about the active RISC-V SBI environment.

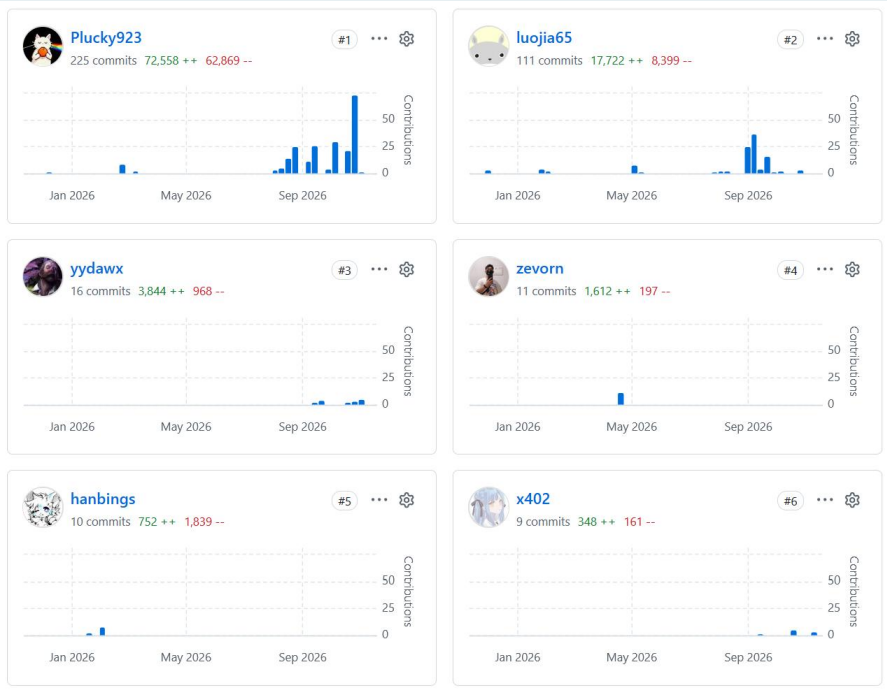
crates.io v0.0.1 | docs failing | license MIT OR MulanPSL-2.0

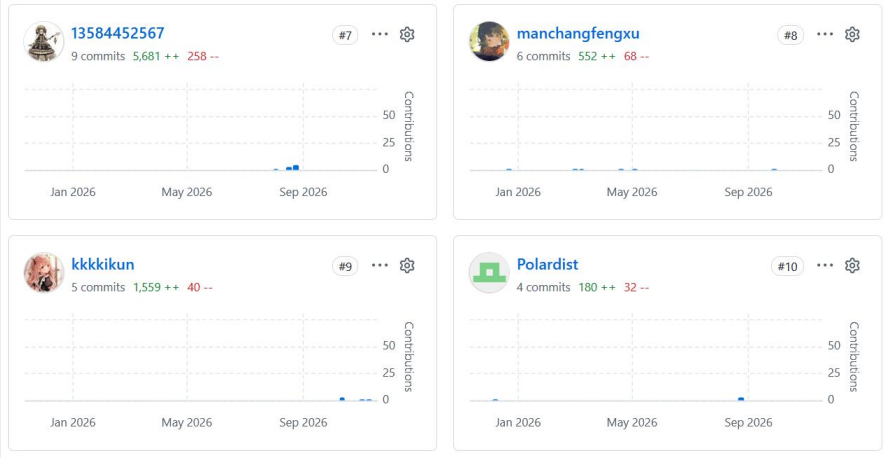
The current backend reads values exported by the `lssbi_probe` DKMS module. The command itself is unprivileged and never loads or unloads kernel modules.

```
luojia@i3-spacemitk3picoitx:~$ lssbi
SBI 规范版本：v2.0（原始值 0x2000000）
SBI 实现：OpenSBI（标识 0x1）
SBI 实现版本：v1.6（原始值 0x10006）
机器厂商标识：SpacemiT (Hangzhou)Technology Co Ltd（原始值 0x710）
机器架构标识：0x8000000058000002
机器实现标识：0x33d8a600
SBI 扩展：
  基础：                          支持
  定时器：                        支持
  处理器间中断：                  支持
  远程栅栏：                      支持
  硬件线程状态管理：              支持
  系统复位：                      支持
  性能监控单元：                  支持
  调试控制台：                    支持
  系统挂起：                      支持
  协作式处理器性能控制：          不支持
  嵌套加速：                      不支持
  窃取时间统计：                  不支持
  监管者态软件事件：              支持
  固件特性：                      支持
  调试触发器：                    支持
  消息代理：                      支持
漏洞：
  PMU2 崩溃 (CVE-2025-63913):     受影响
固件特性（Linux 处理器 #0，SBI 硬件线程 #0）：
  非对齐异常委托：                不支持
  着陆点：                        不支持
  影子栈：                        不支持
  双重陷阱：                      不支持
  PTE A/D 位硬件更新：            不支持
  指针掩码 PMLEN:                 不支持
```

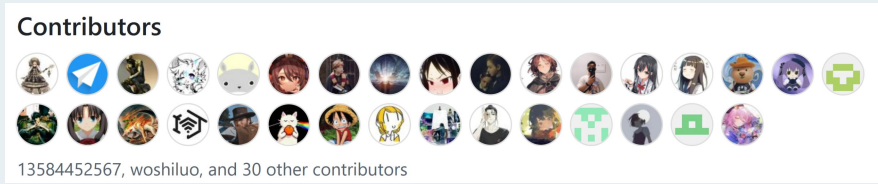
https://github.com/rustsbi/lssbi

今年以来的整体贡献情况





- 发布 0.4.1 版本（5月）
- 感谢所有的开源贡献者！



* 除以上贡献，还有 HAL 支持包的工作

我们的开源之夏项目

已发布申请项目 共 3 个

项目编号：2603c0064

RustSBI Prototyper 固件内特权分离架构设计与实现

进阶 中文

项目热度

￥5000

中选学生：姚礼兴

项目导师：王振辰

导师联系方式：plucky@rustsbi.com

项目编号：2603c0065

RISC-V 架构固件漏洞挖掘与修复

进阶 中文

项目热度

￥5000

中选学生：王诺贤

项目导师：刘通

导师联系方式：liutong@iscas.ac.cn

项目编号：2603c0077

面向 RustSBI 的 Agent Infra

基础/Basic 中文&English

项目热度

￥3500

中选学生：徐阳

项目导师：泽文

导师联系方式：chao.liu@yeah.net

https://summer.ospp.ac.cn/org/orgdetail/03c26314-96aa-44b6-acf2-8e717aaee807?lang=zh



THANKS

中国科学院大学
University of Chinese Academy of Sciences