2026 | 第一届CCF网络与系统安全大会
安全为基，智算未来 The 1st CCF Network and System Security Conference

NACRE: RISC-V原生机密容器

宋林轲*†，王文浩*†✉，刘维杰‡，侯锐*†
*中国科学院信息工程研究所网络空间安全防御全国重点实验室，†中国科学院大学网络空间安全学院，
‡南开大学密码与网络空间安全学院

引言

现有机密容器通常将工作负载置于Enclave、CVM或额外保护上下文中。由于保护单元并非容器本身，容器被封装进其他安全抽象，失去了原生性。NACRE 让容器本身成为硬件识别的保护与生命周期单元，实现原生机密容器。

方案	保护单元	资源管理方	可信中介	原生Linux路径	服务调用的上下文切换
基于 Enclave	Enclave / 地址空间	Host OS + 运行时	Enclave 运行时	×	Enclave 切换
基于 CVM	VM / Realm	Guest OS + VMM	Guest OS / TEE	×	VM 切换
BlackBox	容器内存上下文	Host OS	CSM	部分	嵌套页表切换
ConMonitor	容器 EPT	Host OS	Guardian	部分	EPT 上下文切换
RContainer	容器 + Shim-GPT	Host OS	mini-OS + Monitor	部分	GPT / mini-OS 切换
Fasco	容器 Realm	Host OS	系统 Realm	部分	Realm 切换
NACRE	容器身份（CID）	Host OS	可信代理 + Monitor	✓	无保护上下文切换

表1. 现有机密容器方案对比

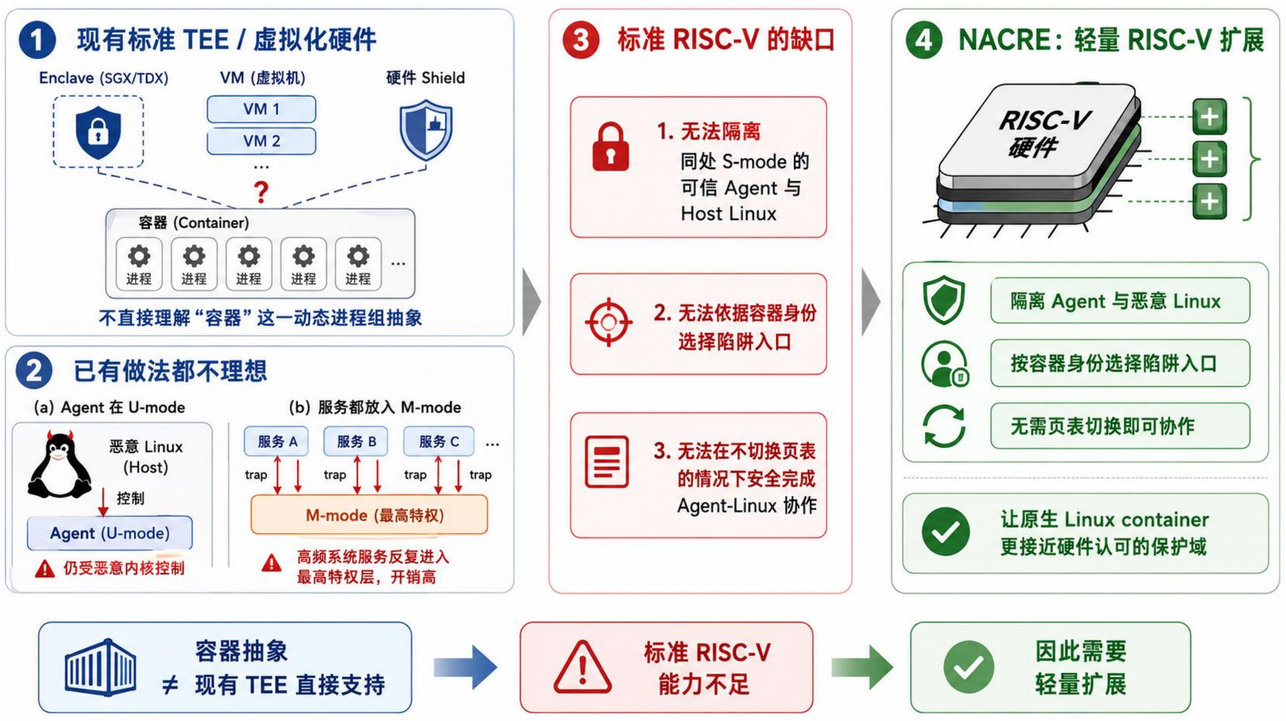


图1. 设计取舍与目标

设计目标

- 容器原生保护： 以动态容器进程组作为统一的保护与生命周期单元；
- 原生资源管理： 保留 Linux 对调度、内存分配与回收的直接管理，以及 fork、COW、exec 和 exit 等原生语义；
- 透明兼容： 尽量复用现有应用与 OCI 镜像，同时不影响普通进程和非机密容器的执行路径。

设计方案

为此，NACRE 将三类职责解耦：Host Linux 执行资源服务，可信 Agent 介导容器交互，Monitor仅授权并提交安全关键状态。

图2. 原生机密容器NACRE架构设计图

内存隔离

- 利用RISCV的PMP保护机密容器进程页表页与机密元数据
- 设置硬件bitmap防护分配的用户叶子页
- 添加Base & Bound寄存器组防护Agent内存区域

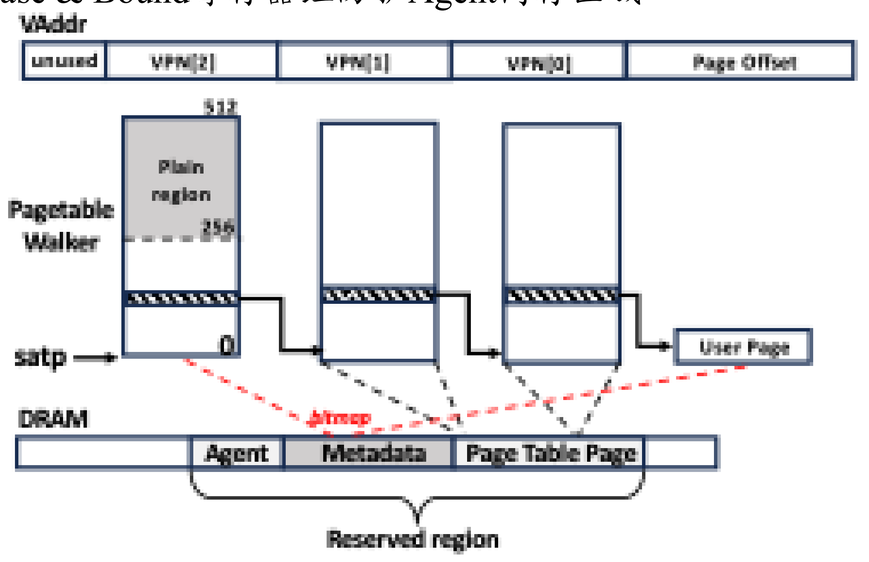


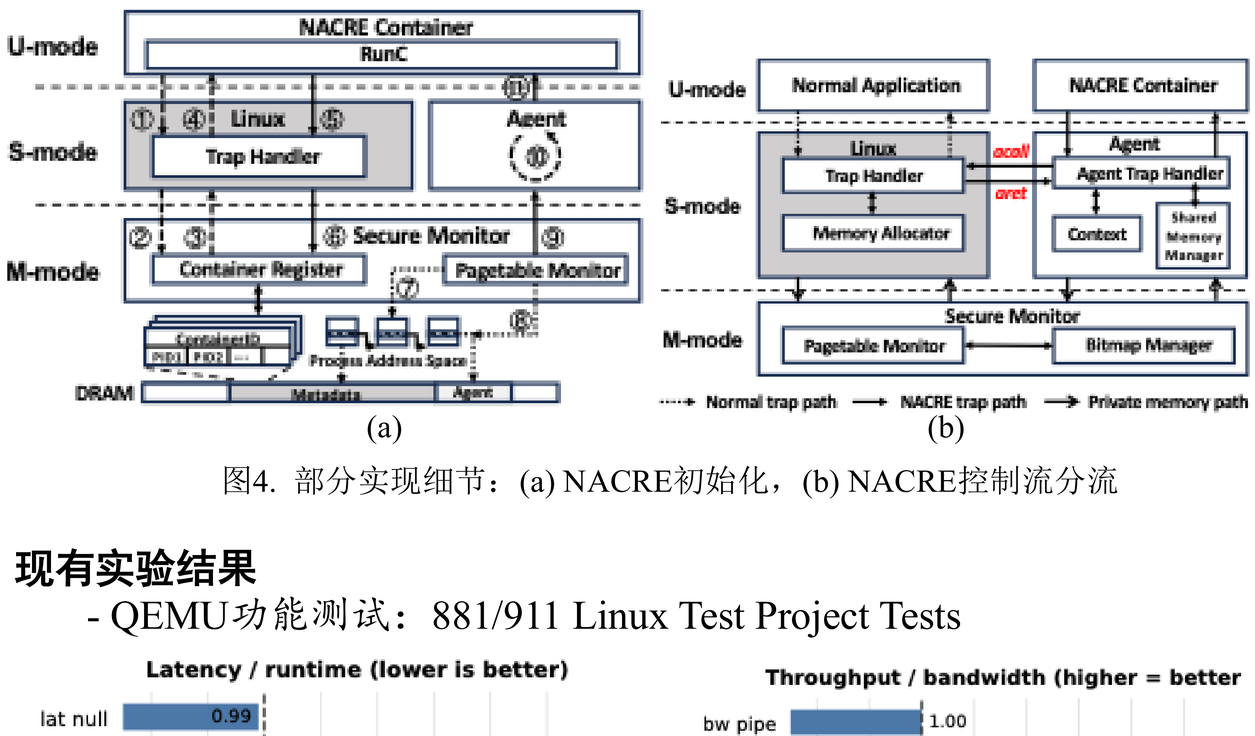
图3. NACRE机密容器进程内存隔离机制

初始化

- linux启动前加载
- RunC通过系统调用初始化Agent
- NACRE容器针对ContainerID和ProcessID进行注册

控制流分流

- NACRE进程不干扰常规进程，利用新指令代理执行
- 支持SysV共享内存，全权由Agent自行负责处理
- Fork共享时由Agent开设Fork处理窗口

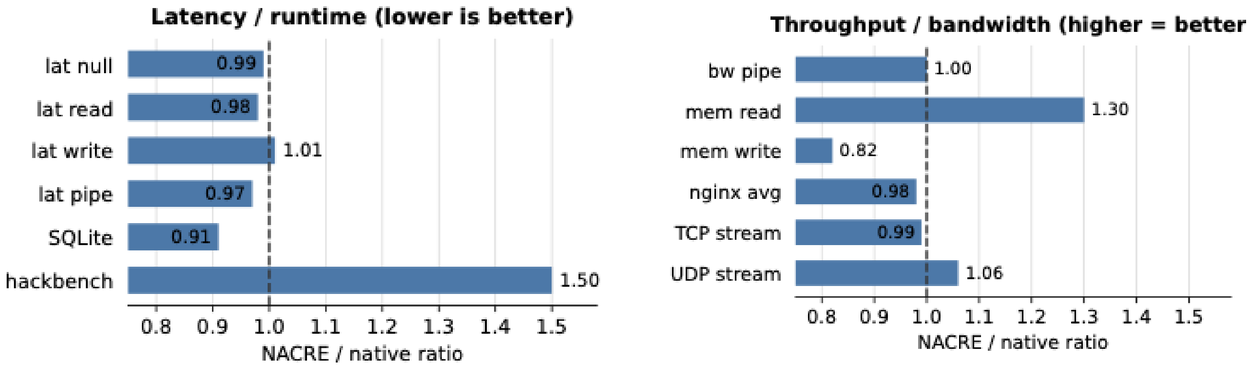


(a) (b)

图4. 部分实现细节：(a) NACRE初始化，(b) NACRE控制流分流

现有实验结果

- QEMU功能测试：881/911 Linux Test Project Tests



(a) (b)

图5. 部分性能测试：(a) 延时测试，(b)吞吐与访存测试

当前工作与进展

正在迁移至XS-GEM5平台与香山平台，后续希望探索面向机密同时安全的面向AI Agent的容器的软硬件协同设计

联系方式：+86 18511165662

电子邮箱：songlinke@iie.ac.cn