动态完整性度量系统

冯伟 李为 秦宇

冯伟 18810678038 fengwei2009@iscas.ac.cn

具体内容介绍

1. 系统简介

完整性度量主要是对系统中关键组件、重要配置与数据等进行检查，确保它们的完整性没有被破坏，从而提升系统的安全防护能力；传统可信计算度量技术主要侧重静态度量，在动态度量与监控方面是缺乏的，容易遭受运行时攻击、TOCTOU攻击等。动态完整性度量系统通过深入研究平台动态度量、LKIM内核数据完整性度量、ebpf动态安全监控等关键技术，实现了进程动态度量、内核不变量监控、用户态敏感信息采集、内核事件安全监测等度量模块，并结合度量信息通信与管理模型，形成一套动态完整性安全解决方案。

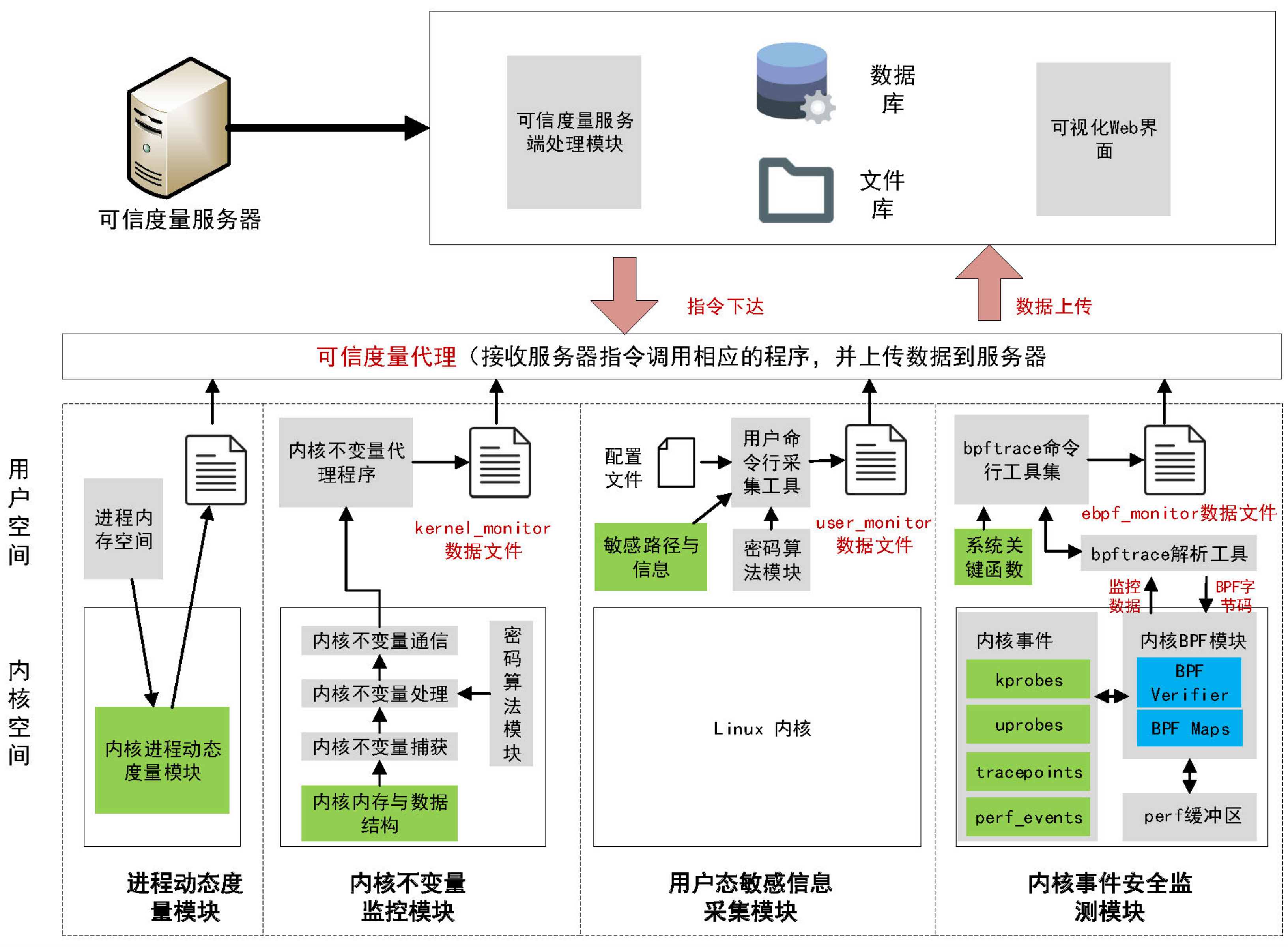


图1 系统架构

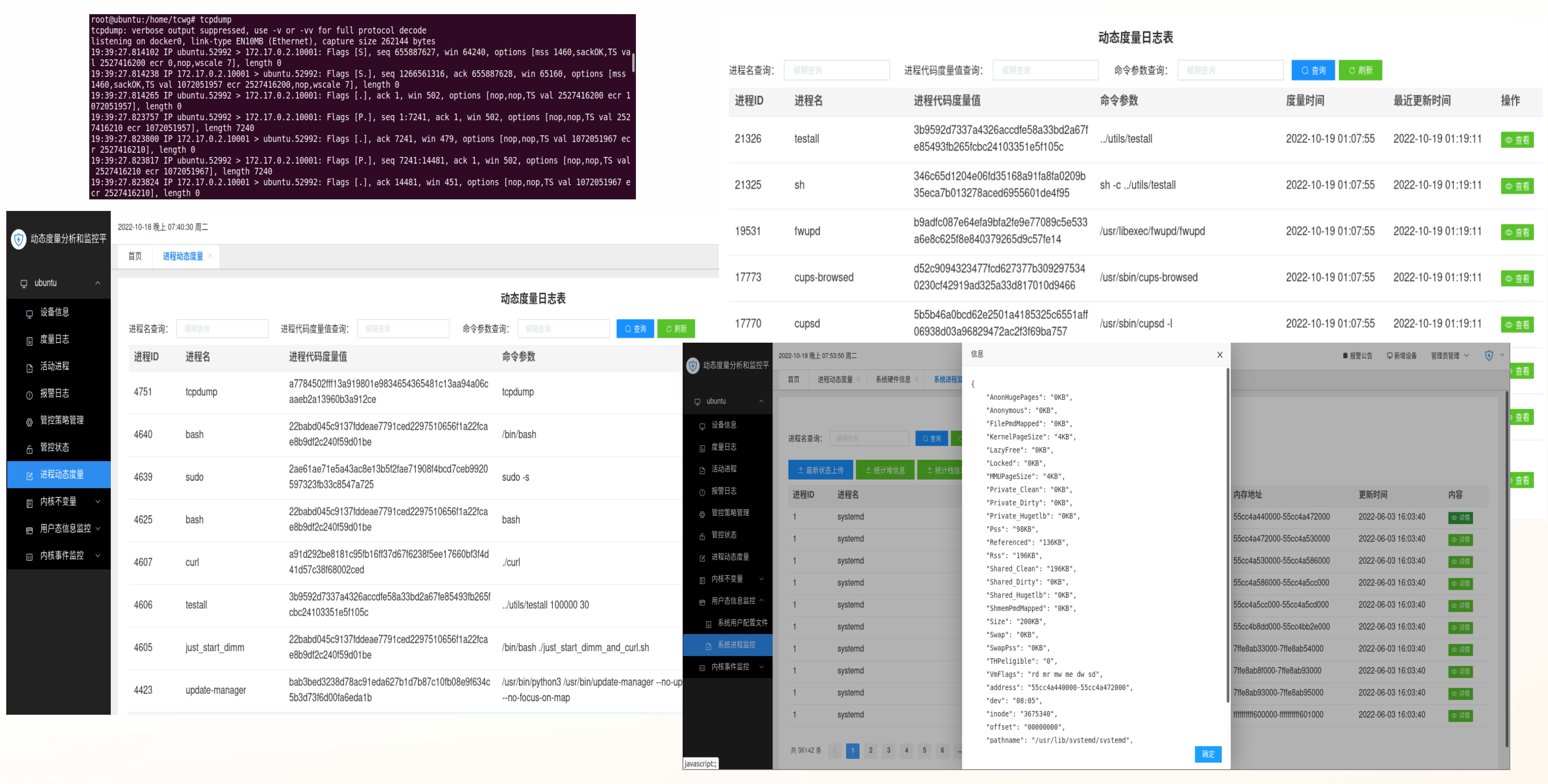
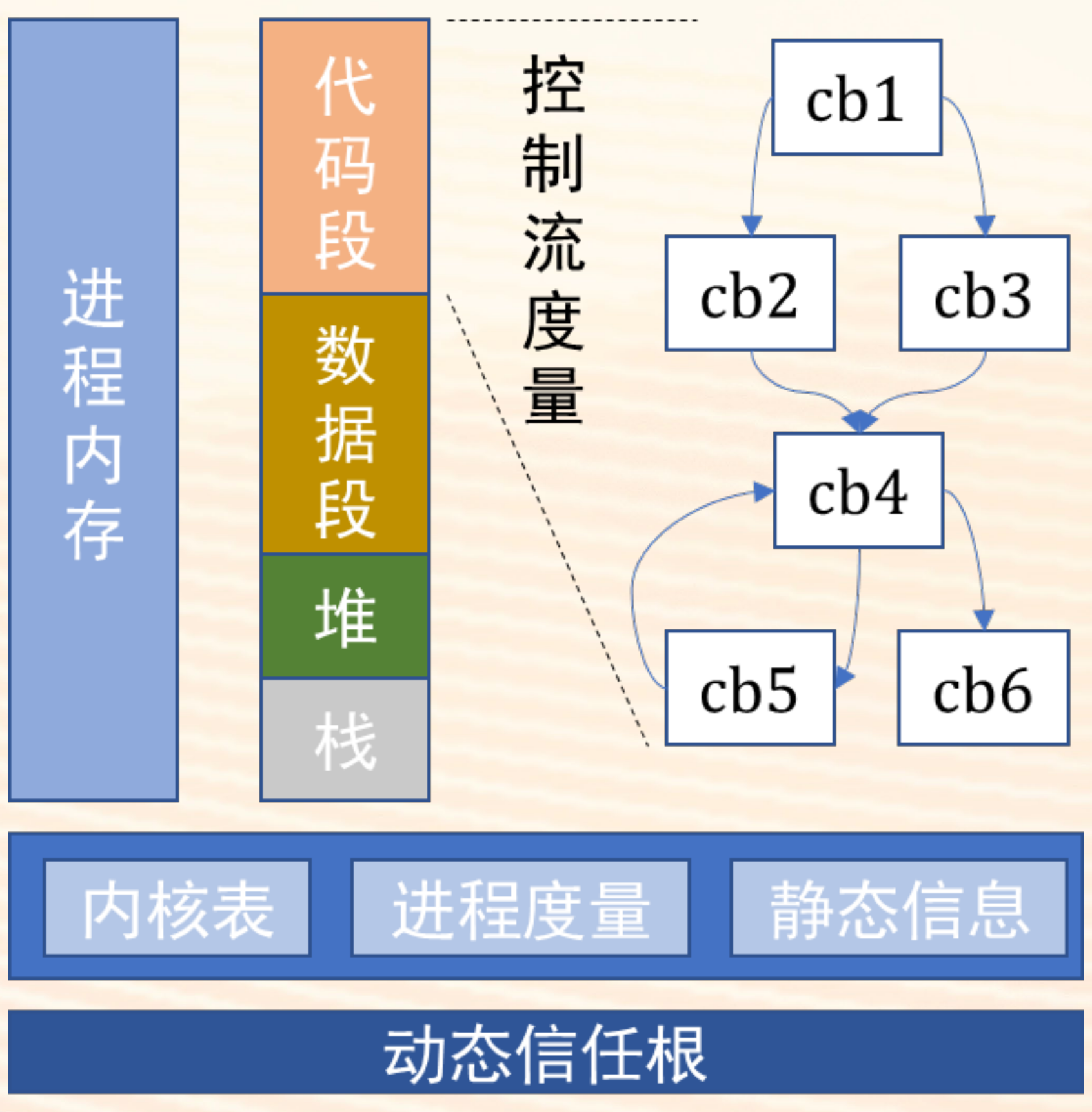
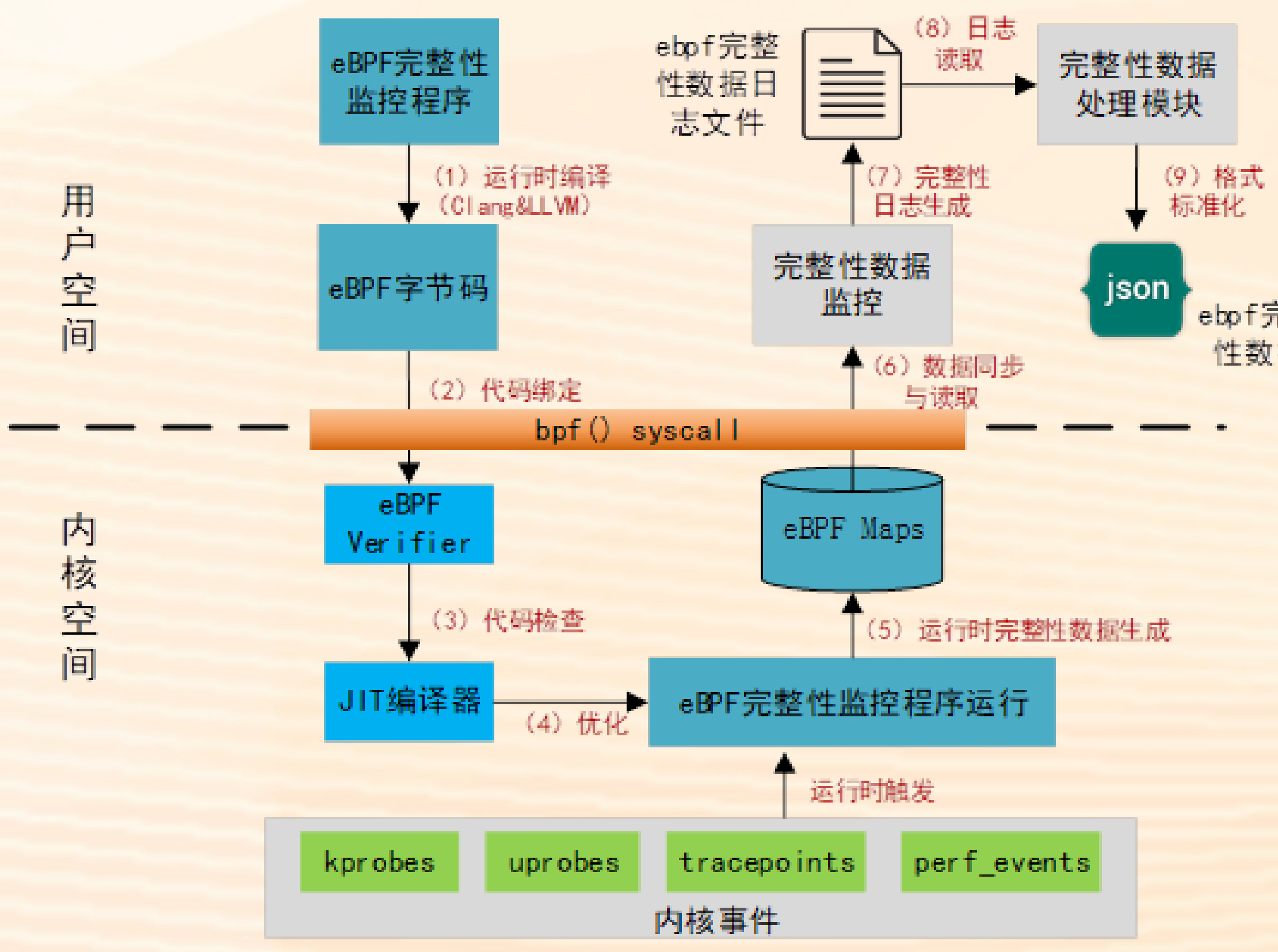


图2 系统运行界面

2. 技术思路

- **度量对象**：程序代码段、关键数据、环境变量、系统脚本、堆、栈、内核数据结构、关键系统调用、进程创建、可执行文件加载、内核模块加载、文件操作、内核权限等
- **度量流程**：确定度量基准；运行时完整性度量；度量代理统一管理度量模块；可信度量服务器进行判断、策略指定、度量数据存储与管理、控制命令下发
- **度量技术**：进程动态度量、LKIM内核度量、ebpf动态监控





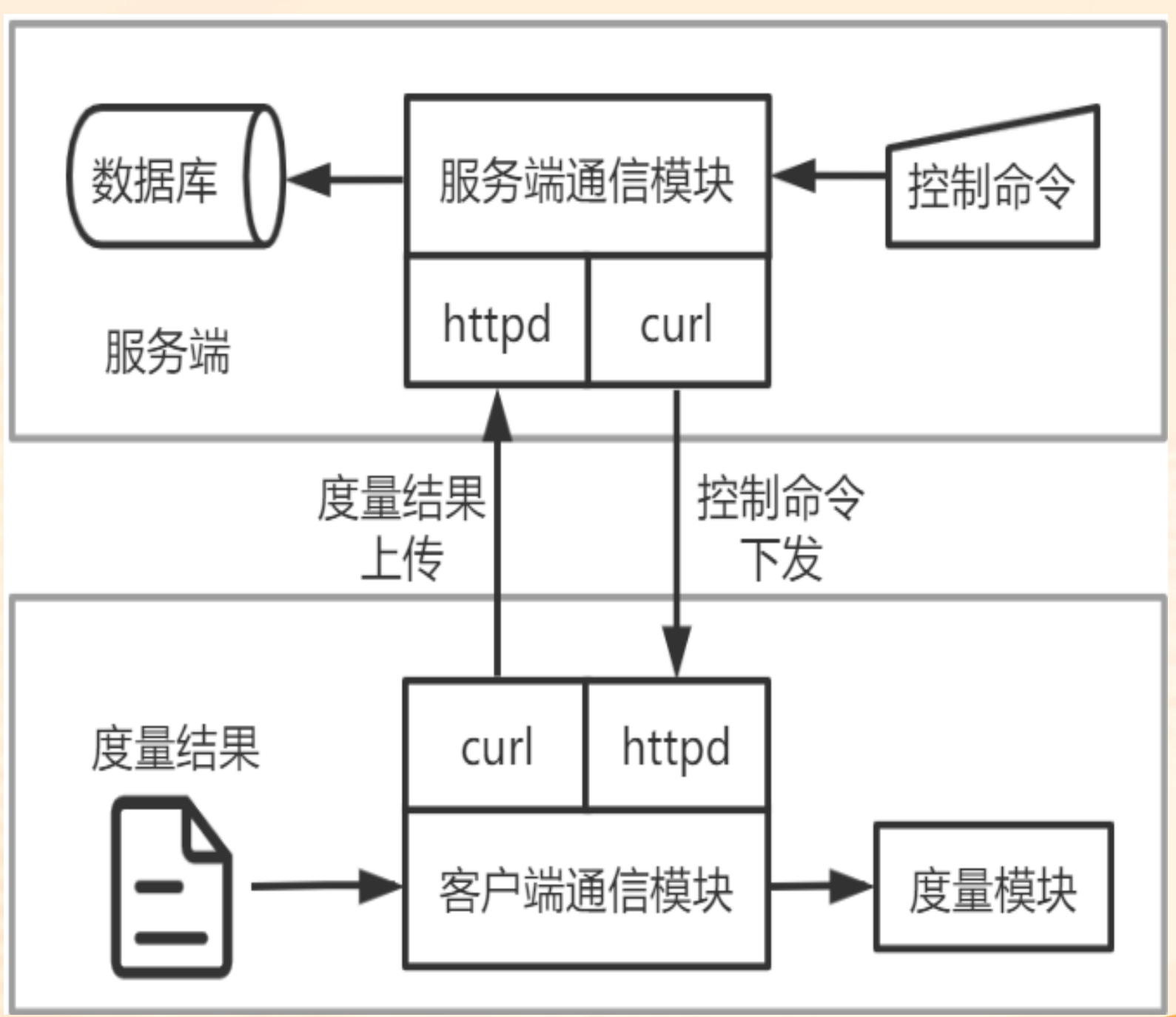


图3 进程动态度量　图4 ebpf动态监控　图5 度量通信与管理