一种新的操作系统入侵检测框架

腾讯 杨亚军

Tencent 腾讯 APD 架构平台部

个人&团队简介

- 个人简介：2011年中科院博士毕业后加入腾讯操作系统团队，从事操作系统和底层虚拟化平台的研发工作

- 腾讯操作系统研发团队
  - linux服务器操作系统：tlinux，内部使用量接近百万
  - 底层虚拟化平台：tlinux-xen，tlinux-kvm，用户囊括内部云和腾讯云
  - 协议栈优化技术研发
  - 操作系统安全增强技术研发
  - 容器虚拟化技术研发

安全防护形势不容乐观

- 你之所以生活在光明之中，是因为有人阻挡了黑暗
  - 国内黑客逾10W，年攻击次数逾10亿次
- 安全核心领域
  - 网络攻防
  - 入侵检测
  - 漏洞检测与防护

入侵检测面临挑战

- 海量数据的实时获取
  - 问题：全面无死角
  - 问题：性能开销
  - 问题：如何适应业务环境的复杂性

操作系统层面的入侵监控信息获取框架

- 海量数据的实时分析

新的入侵检测框架

- 操作系统层面的入侵信息获取支持
  - Hook&信息获取&信息传送
    - 全面无死角
    - 操作系统层面支持，业务环境适应性好

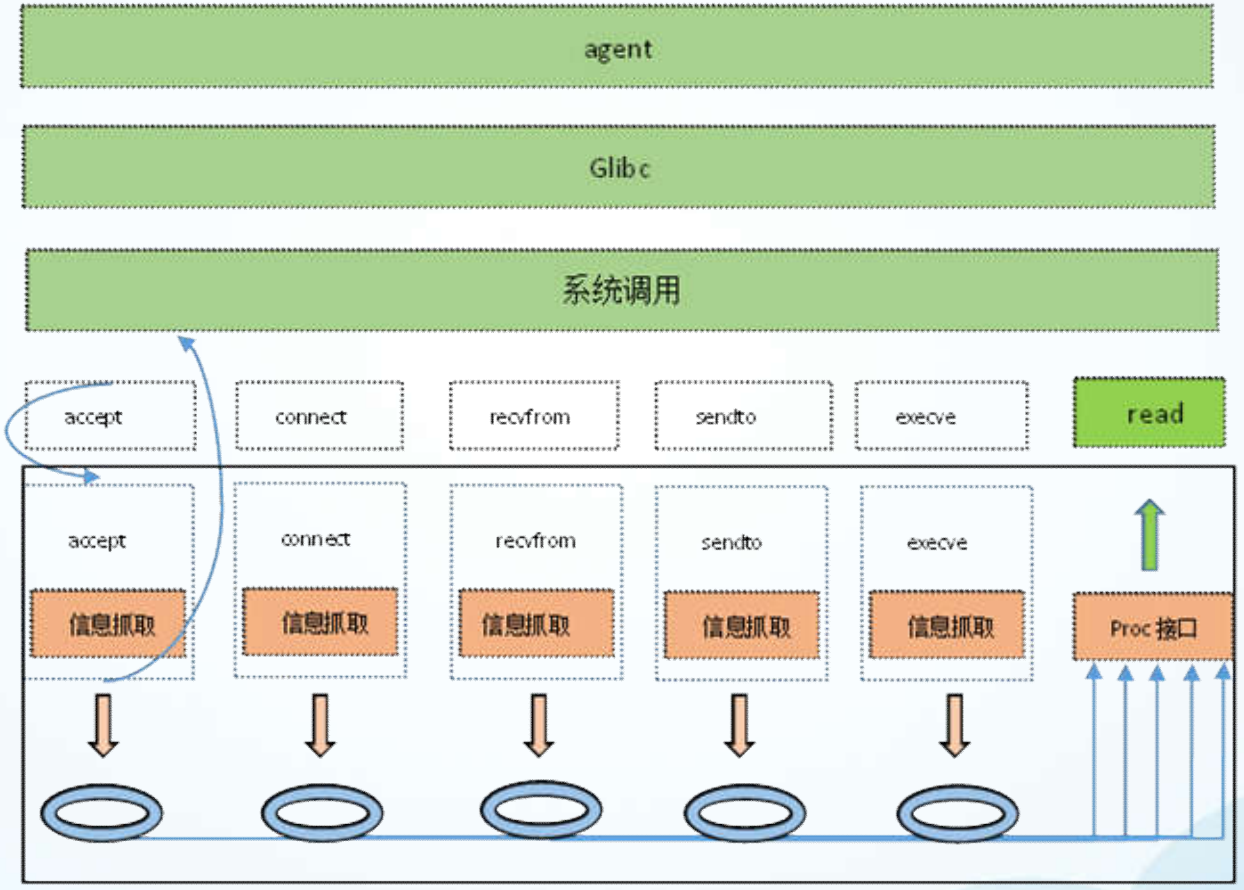
- 面临挑战
  - 性能开销
  - 海量现网业务支持
    - 部分开放内核模块支持
    - 部分不开放内核模块支持

技术路线

- 内核热补丁
  - 针对有内核模块支持系统
- C库劫持&进程热补丁
  - 针对无内核模块支持系统

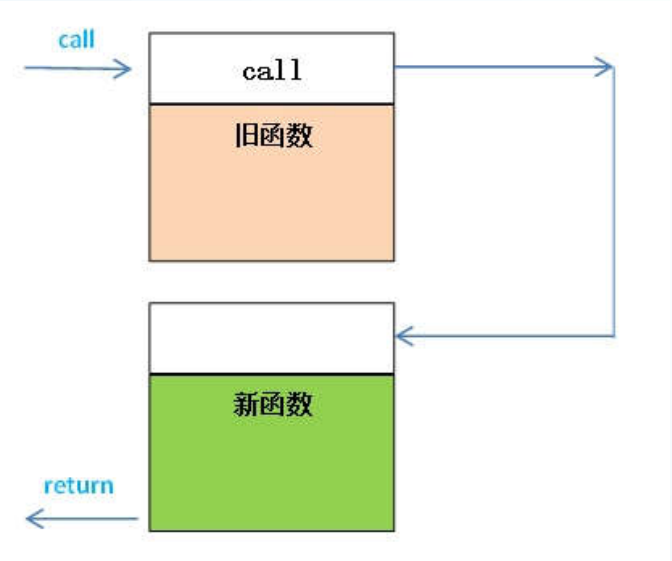
技术路线一：内核&内核热补丁（1）

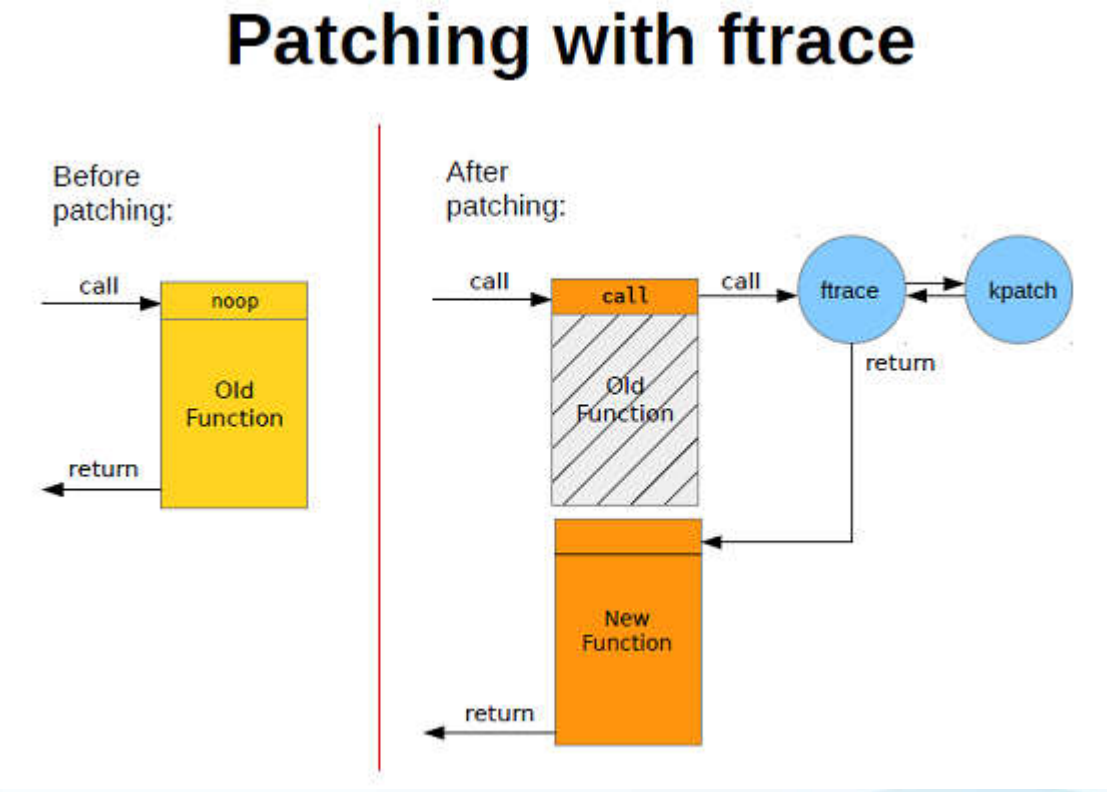
- 整体架构



技术路线一：内核&内核热补丁（2）

- 内核热补丁
  - ftrace&kpatch
    - 性能开销大
  - tpatch



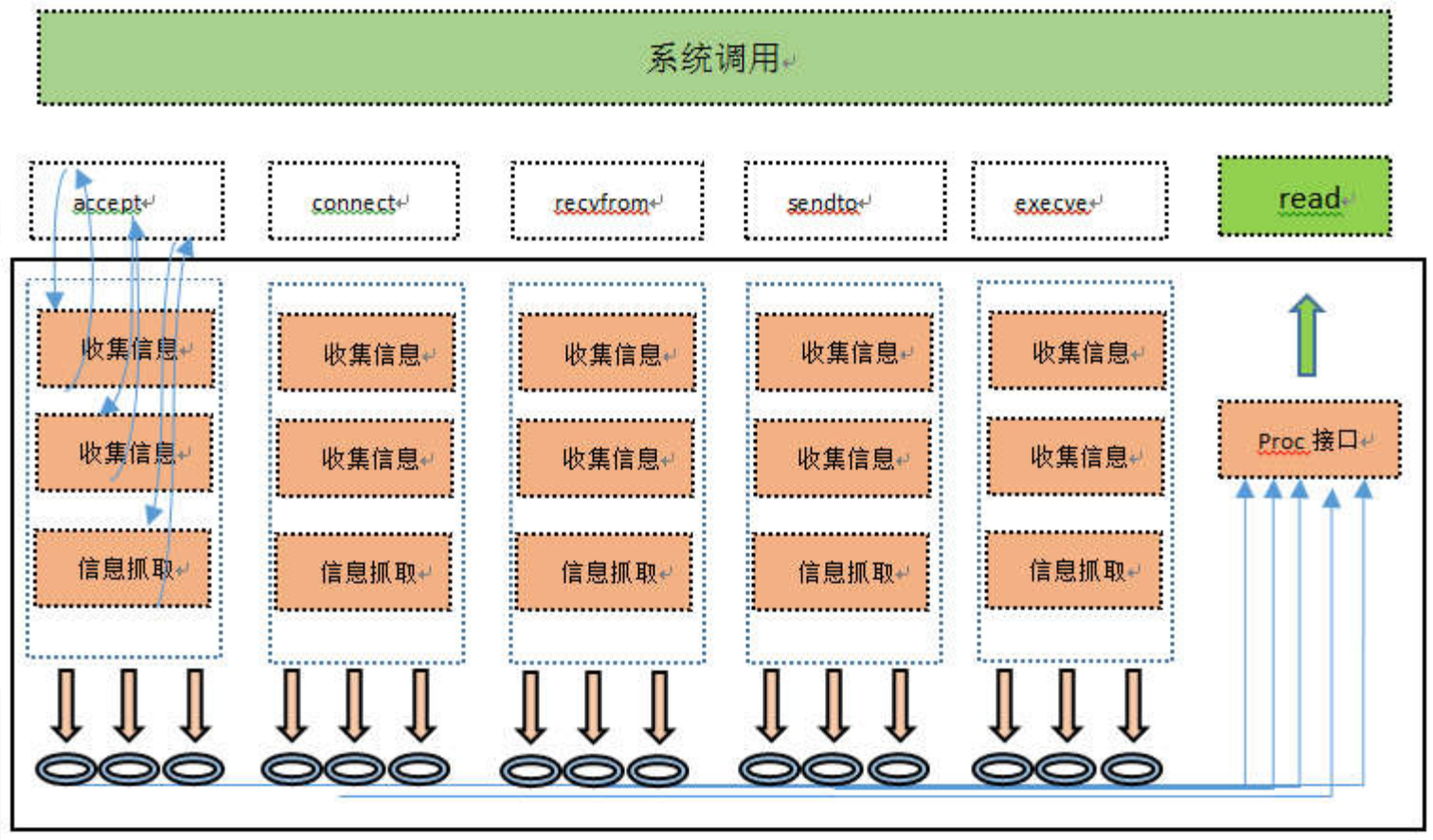


技术路线一：内核&内核热补丁（3）

- 性能优化
  - 数据传送：无锁缓冲区
    - ringbuffer
    - per-cpu化

技术路线一：内核&内核热补丁（4）

- 热补丁性能优化

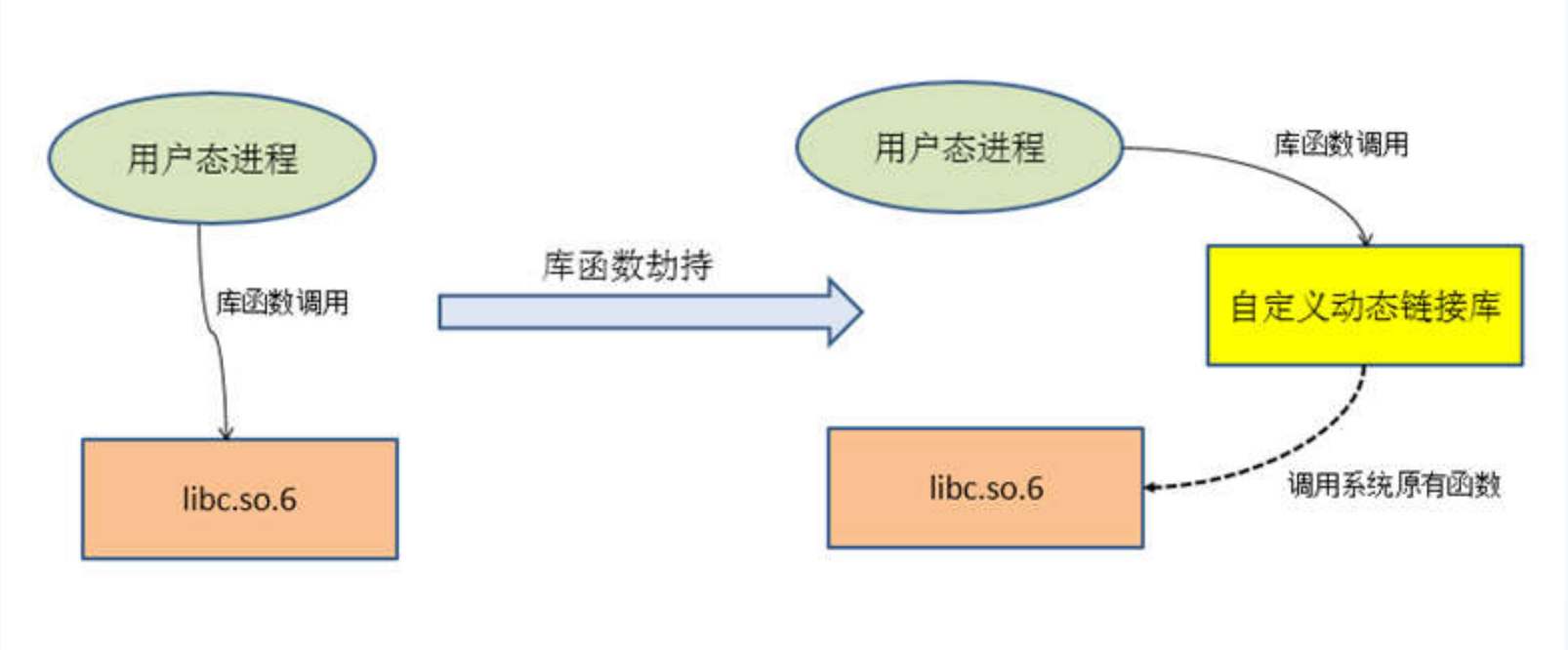


技术路线一：内核&内核热补丁（5）

- 性能开销优化
  - 引用计数优化：开销降低3%
  - 代码优化：开销降低2%

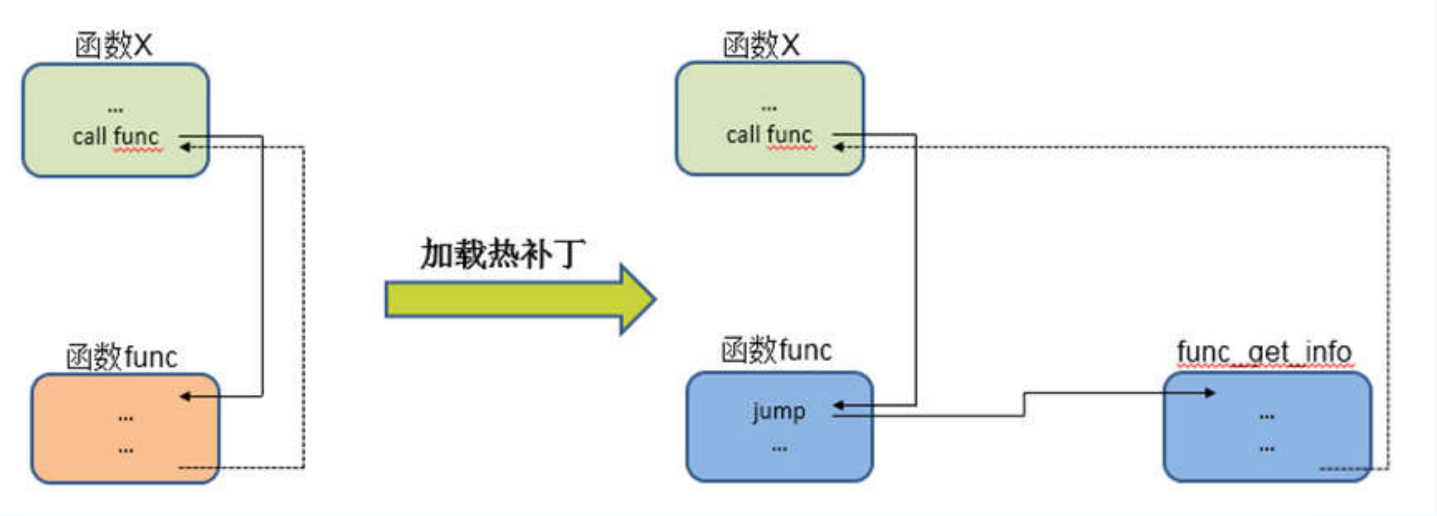
技术路线二：C库劫持&进程热补丁（1）

- C库劫持



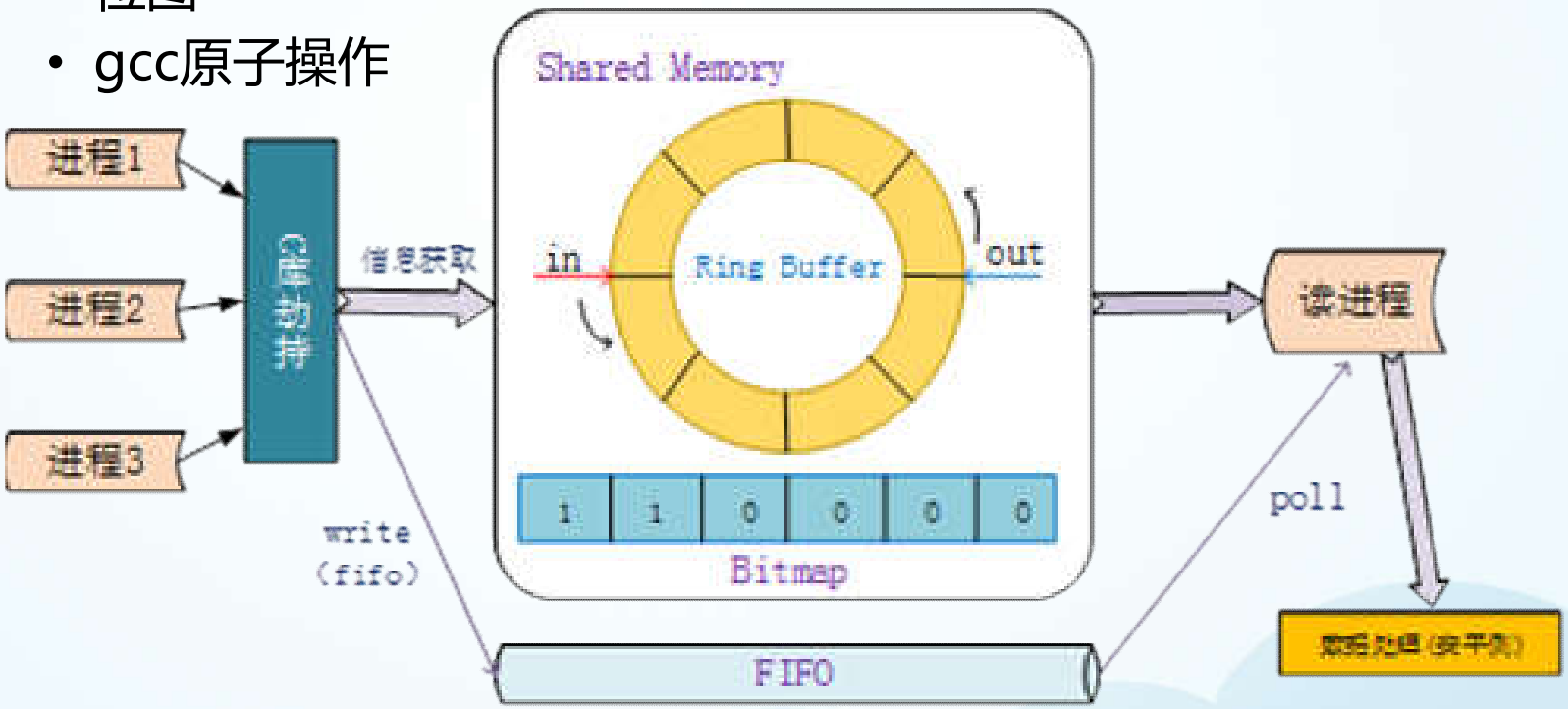
技术路线二：C库劫持&进程热补丁（2）

- 进程热补丁



技术路线二：C库劫持&进程热补丁（3）

- 性能优化
  - 信息传送：无锁缓冲区
    - ringbuffer
    - 位图
    - gcc原子操作

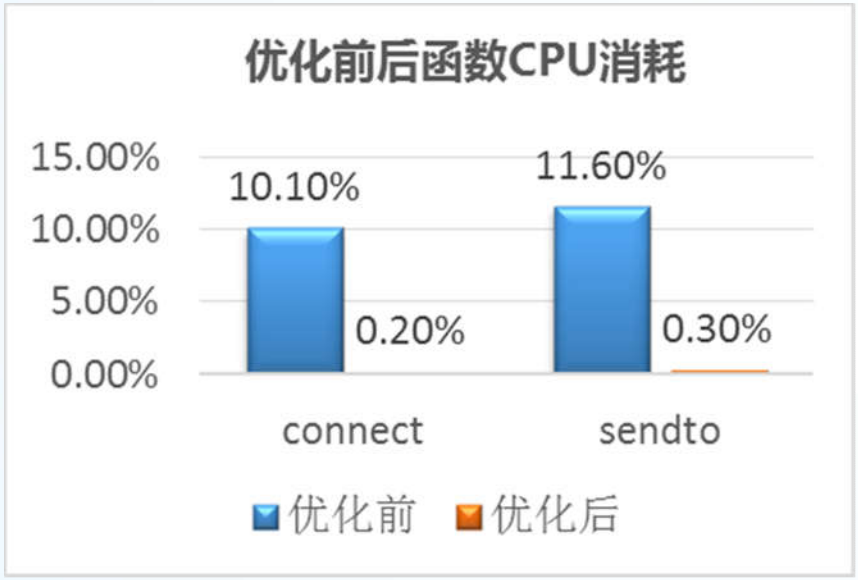


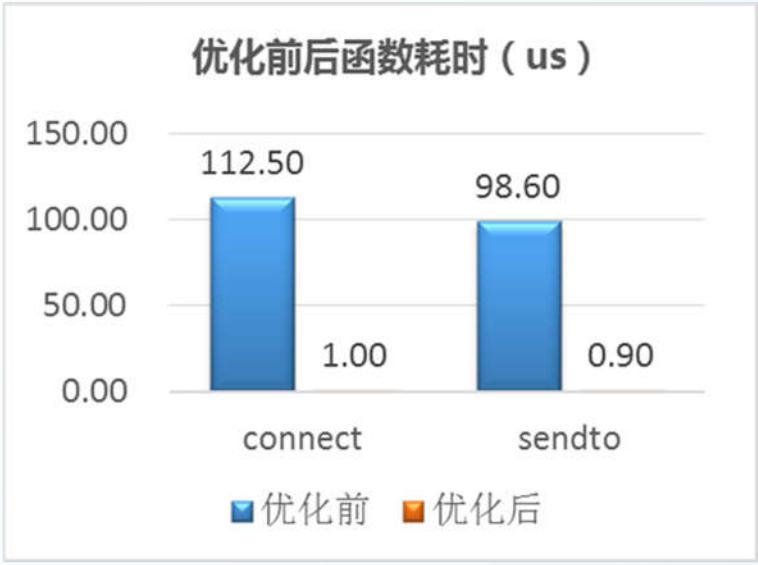
技术路线二：C库劫持&进程热补丁（4）

- 性能优化
  - 信息获取
    - 取消proc下的信息获取
  - 信息过滤
    - 固定时间段内的相同信息不传递
    - 高负载网络传输场景有效
  - 时间信息获取开销
    - Gettimeofday + TSC

效果总结

- 性能开销优化效果





回顾

- 操作系统入侵检测框架
  - 全面无死角
  - 基本无额外性能开销，对业务服务性能无影响
  - 业务场景适应面广

操作系统安全增强未来展望

- 身份认证
  - 内核签名
  - 模块签名
  - 进程签名
- 访问控制
  - 取消root的完全权限
  - 权限细分
  - 关键数据访问受限
- 密钥管理
  - 密钥分发和管理框架与操作系统紧密结合，密钥由内核管理并据此进行相关认证，应用层接触不到私钥

Q&A