
# 可信计算技术原理与应用



服务计算技术与系统教育部重点实验室　　集群与网格计算湖北省重点实验室

# 提纲


- 基于Turaya的可信平台
- 虚拟化可信计算平台

# 单内核模型


- 单内核：也称宏内核，它是一个很大的进程，内部又可以分为若干模块
- 模块间的通信是通过直接调用其它模块中的函数实现的，而不是消息传递，因此速度很快
  - 采用执行流抽象，通信在内核中直接进行
- 耦合程度高，可扩展性和可维护性差，安全性较差

# 微内核模型

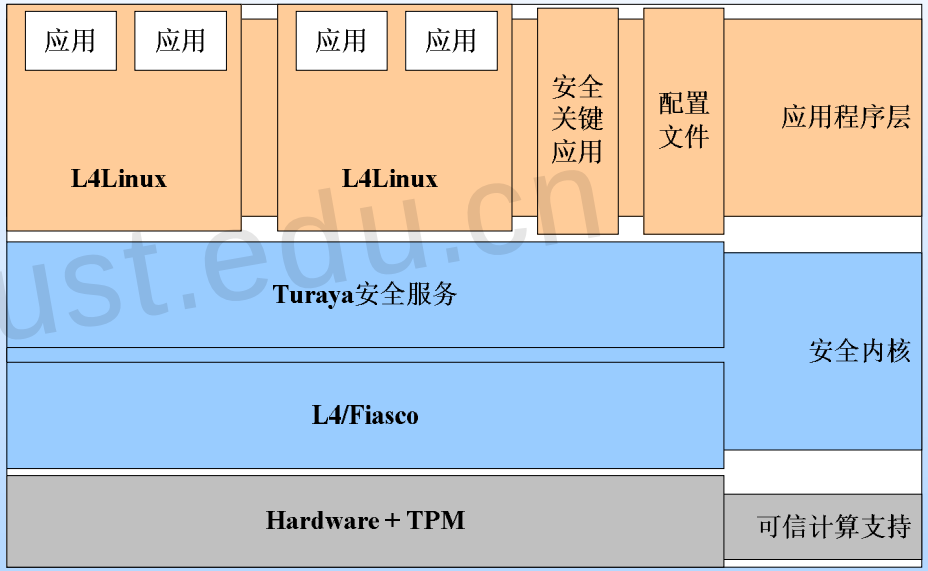

- 与单内核相同，微内核结构也是采取进程/线程模型，但是大部分系统级服务被挪出了内核，作为应用级进程提供
- 大部分内核都作为独立的进程在特权状态下运行，它们通过消息传递进行通信
- 微内核模型只保留了很小的内核部分，用以提供中断/异常管理、IPC管理机制等必要的基础机制
- 微内核部分经常只不过是一个消息转发站：当系统调用模块要给文件系统模块发送消息时，消息直接通过内核转发
  - 这种方式有助于实现模块间的隔离，提高内核的安全性。

# 进程/线程模型优缺点


- **优点：**
  - **扩展性好：隐藏了物理CPU的相关信息，为用户提供了虚拟的、并发的CPU，提供了清晰的编程模型，使得用户开发程序可以不受限于具体的硬件平台**
- **缺点：**
  - **线程间通信的异步性导致信息处理的延时和不确定性，进而影响了系统的效率和实时性；**
  - **线程抽象强行分开了任务之间的本原联系，造成系统额外开销。很多原本同步的任务用线程实现，为了维护这种同步性，在线程间增加同步机制，给系统带来了许多不必要的开销**
  - **模型屏蔽了底层信息，不利于编写高效的程序。**

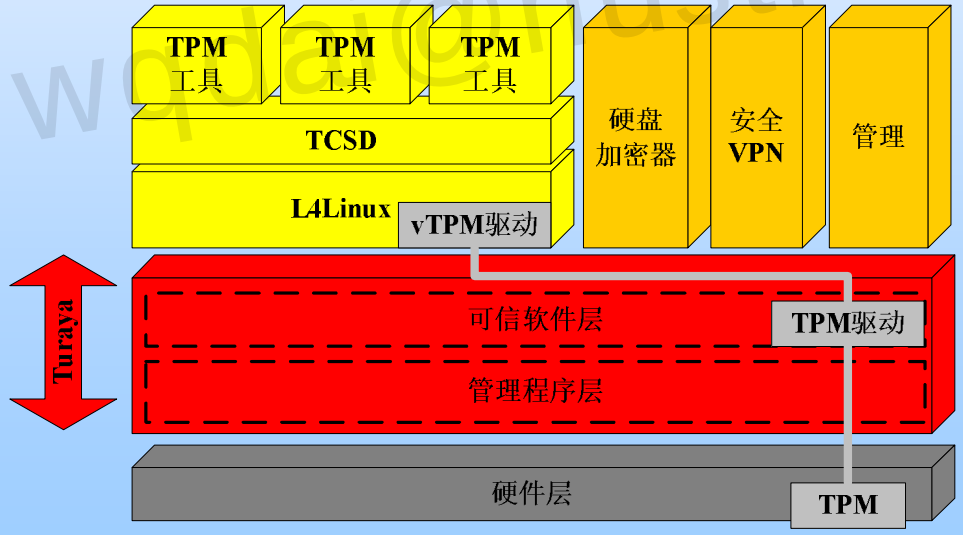
# PERSEUS

- 整个结构被分成了四层：硬件层、资源管理层、可信软件层和应用软件层
- 硬件层中的TPM芯片是整个安全架构的可信根
- 资源管理层：对CPU、内存等资源进行抽象，采用VCPU、虚拟内存等思想对硬件资源进行有效的管理，提供进程识别和隔离功能，提供安全IPC
- 可信软件层：是资源管理层所提供功能扩展的功能模块
  - 可以创建可信存储，建立安全的、完整的报告，通过TPM封装数据。
  - 利用TPM为安全存储提供加密密钥。
  - 通过hypervisor对进程和通道实行隔离，提高他们的安全性。
  - 对大量的存储数据进行加密
- 应用层：包括应用程序，非关键的服务，虚拟机。应用程序中包括安全性要求很高的应用程序
  - 直接运行在可信软件层上
  - 拥有非常小的可信计算基（TCB）
  - 目的单一，为专用程序设计的

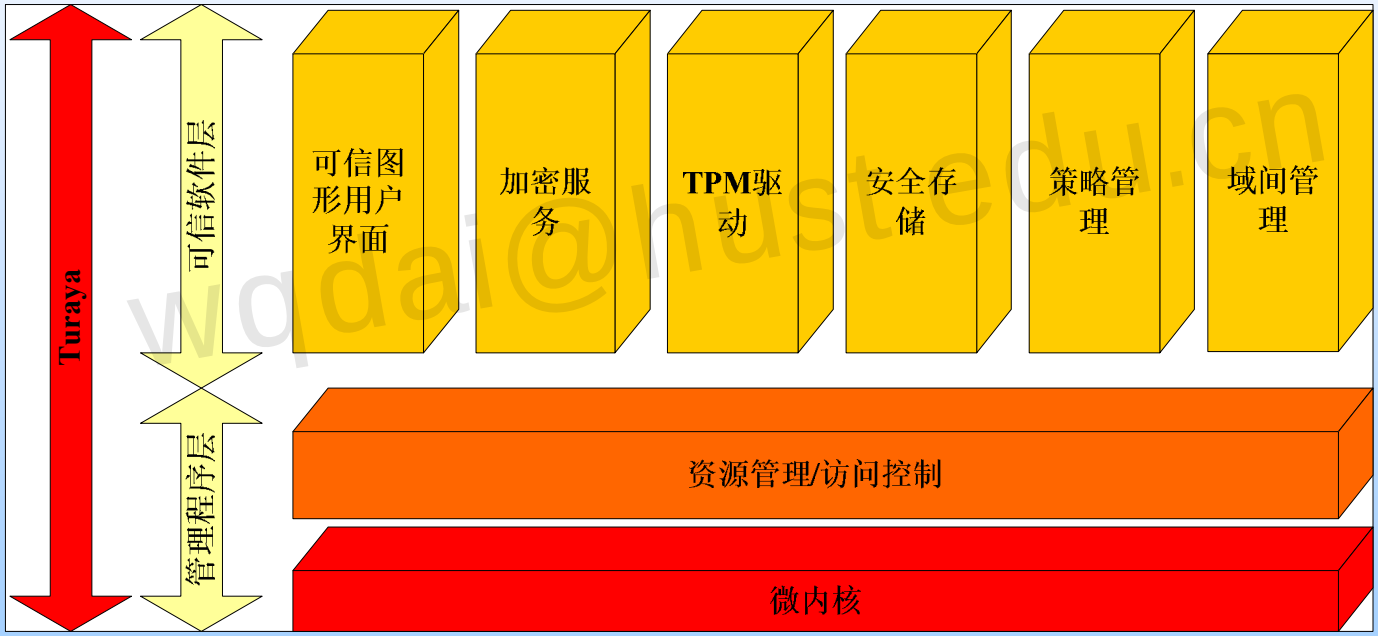


# 基于Turaya 可信计算架构

- Turaya是一个高可信的安全内核，它研究的目的是为实现最高安全标准和在操作系统级别加入可信计算功能
  - 完全的硬盘加密
  - 智能的VPN客户端可以在隔离区和虚拟专用网络之间建立安全连接
  - 通过透明文件加密技术实行全面数据泄漏防护

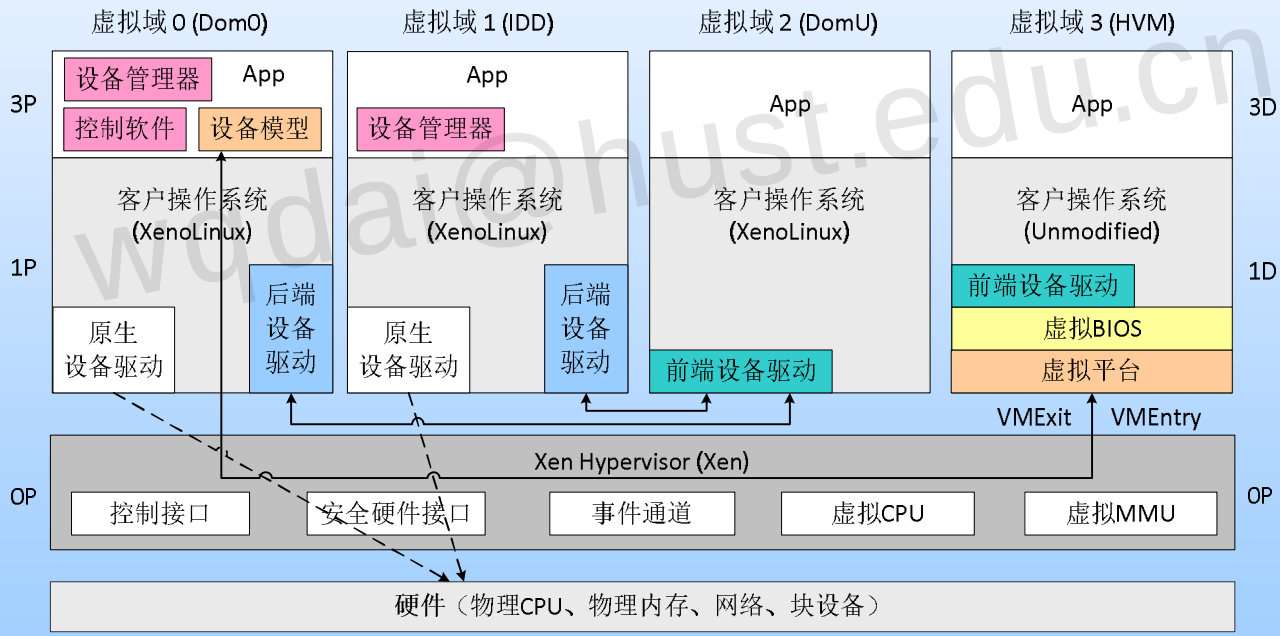


# 基于Turaya 可信计算架构



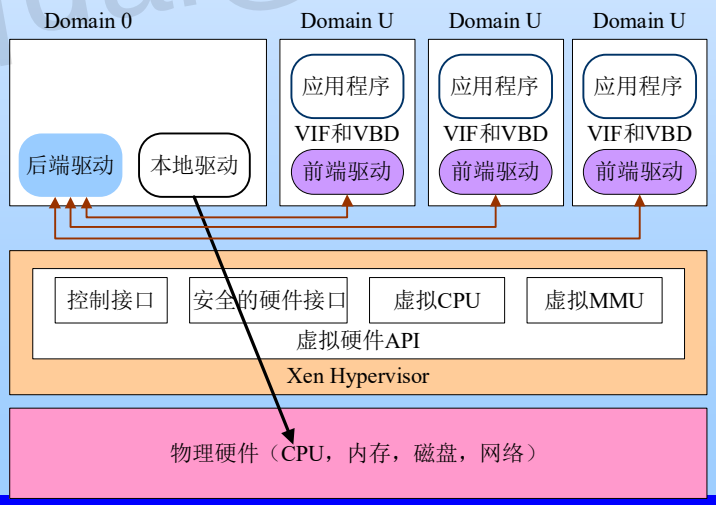
# 虚拟化可信计算平台

## Xen虚拟化架构



# 虚拟化可信计算平台

- **前后端驱动设计**
  - **在Xen中，通过授权表来实现前后端共享内存页面，在Xenstore（位于Dom0中的系统数据库）中存放授权页面的索引（Grant Reference）**
  - **分离设备驱动在共享内存中交换请求和响应，通过事件通道来进行异步通知**
  - **当前端和后端成功地建立连接，前端和后端可以在共享内存中放置请求和响应，然后通过事件通道进行通信**
  - **后端设备驱动在Dom0中，前端设备驱动在DomU中**



# 虚拟化可信计算平台

- vTPM必须为在虚拟机上运行的操作系统提供硬件TPM相同使用模型和TPM命令集
- 虚拟机和它的vTPM实例之间必须保持紧密联系，这种联系在虚拟机的整个生命周期中都需要保持着，包括虚拟机连同与之关联的vTPM一并从一个物理机器转移到另一个机器的特殊情形
- vTPM和真实TPM之间必须保持紧密联系
- vTPM与硬件TPM应该很容易区分，因为两者的安全特性是不同的