ISC 2016

2016 中国互联网安全大会 China Internet Security Conference

协同联动 共建安全+命运共同体

基于硬件的云计算平台安全架构

上海交通大学

夏虞斌

上海交通大学・讲师

上海瓶钵科技・创始人

瓶钵

目录

基于硬件的云计算平台安全架构

· 安全：云计算的最大挑战

· 基于硬件虚拟化的安全云架构

· 基于INTEL SGX的云安全能力增强

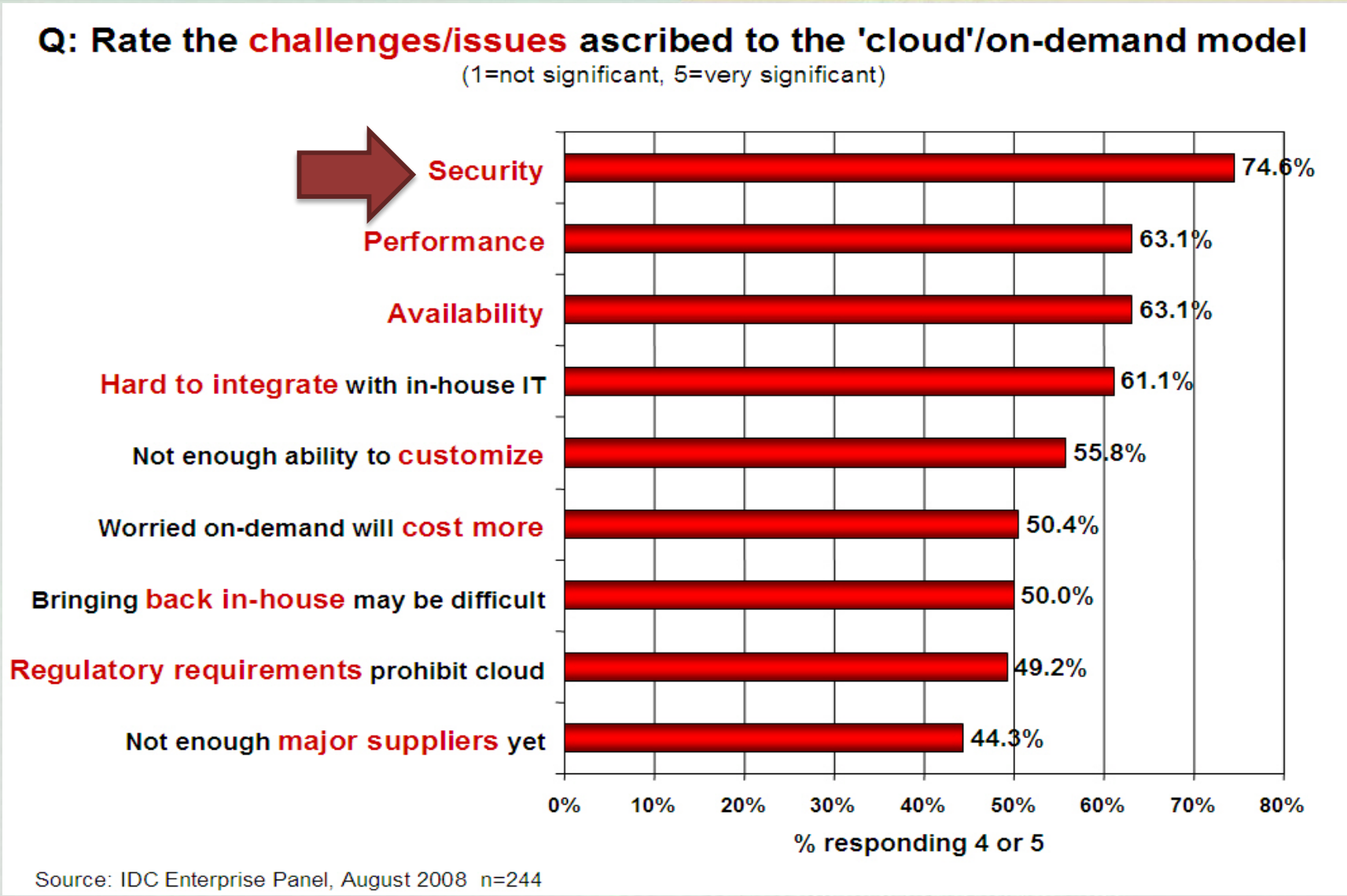
· 基于ARM TRUSTZONE的可信计算环境

上海瓶钵信息科技 上海交通大学 ISC 2016 中国互联网安全大会 360互联网安全中心

安全：云计算最大挑战

“用云不信云” 需要从设计保证安全

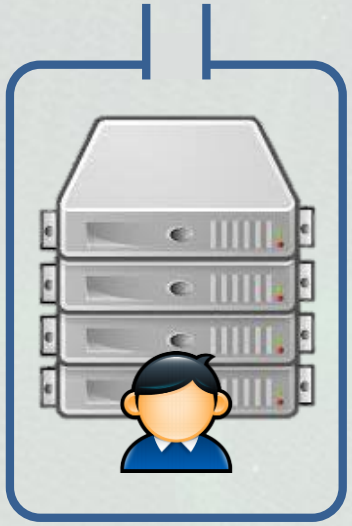
安全是云计算面临的最大挑战[IDC 2008]



云计算引入了新的安全威胁

传统网络服务

黑客攻击
路径单一

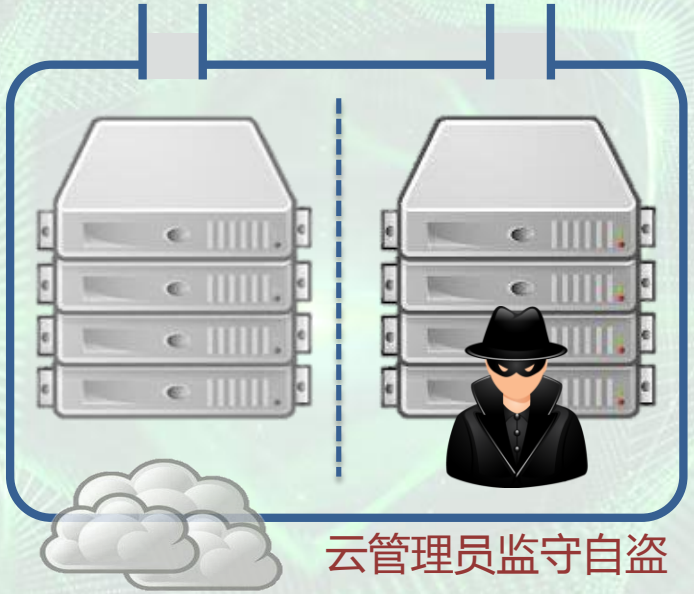


用户掌控所有数据

基于云平台的网络服务

通过其他云租户
间接进行攻击

用户失去
对数据的
掌控权



其他不可控
因素

云管理员监守自盗

云计算面临的7大威胁 [Gartner 2008]

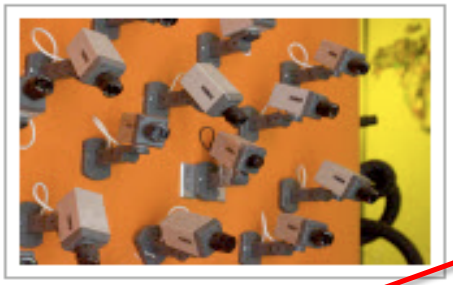
- Privileged operator access
- Regulatory compliance
- Data location
- Data segregation
- Recovery
- Investigative support
- Long-term viability

特权管理员访问

安全威胁实例：不想作恶的大公司

Google Fires Employee Accused Of Spying On Kids

By Phil Villarreal on September 16, 2010 9:15 AM



(RAWRZ!)

For a Google engineer who was fired in July, it apparently wasn't enough just to Google people in order to stalk them. Instead, he allegedly abused his access and violated the company's privacy policies to snoop on users.

Valleywag reports the man spied on four teenagers, peeking in on emails, chats and Google Talk call logs for several months before the company discovered what was going on.

…，偷窥用户隐私数据，如email、聊天记录、拨打电话记录达数月之久…

云计算的安全等级

安全等级	篡改内容	窃取数据	记录用户活动
最高	不允许	不允许	不允许
高	不允许	不允许	允许
中	不允许	允许	允许
低（现状）	允许	允许	允许

篡改内容：例如，修改用户的算法，使其得出不正确的结果

窃取数据：例如，偷取用户的信用卡账号，银行密码等

记录活动：例如，记录用户什么时候和谁打过电话，但不知道具体通话内容

上海瓶钵信息科技 上海交通大学 ISC 2016 中国互联网安全大会 360互联网安全中心

基于硬件虚拟化的安全云架构

如何防御来自堡垒内部的攻击？

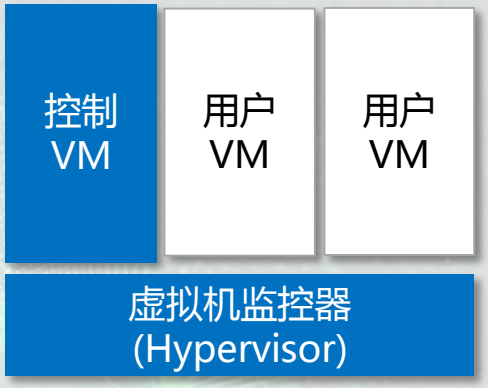
为什么云服务商需要用户的数据明文？

- **不需要明文的例子**
  - 云存储：Dropbox、各种网盘等
  - 用户可将加密后的数据发送至云服务商保存

- **需要明文的例子**
  - Amazon云虚拟机、大数据分析等
  - 对数据进行运算时，必须在内存中解密数据

恶意管理员如何窃取用户明文数据？

- **背景介绍：Virtual Machine**
  - 多个用户共享物理主机
  - 用户VM间通过虚拟机监控器隔离
  - 控制VM和虚拟机监控器有最高权限



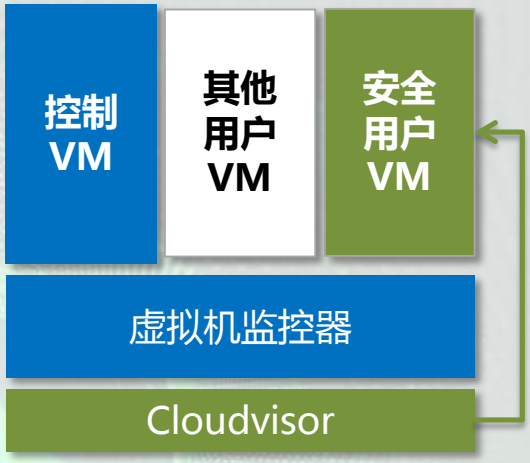
- **恶意管理员攻击方式-1**
  - 管理员通过控制VM来启动、关闭、重启迁移用户VM
  - 副作用：管理员也可通过控制VM直接读取用户内存

解决方案：Cloudvisor by IPADS

- **设计：解耦VM管理和VM安全**
  - 管理员仍可启动、关闭、迁移用户VM
  - 管理员无法读取用户VM的内存
- **实现：嵌套虚拟化**
  - 在Hypervisor底下插入安全层Cloudvisor
  - 通过安全硬件保证Cloudvisor的安全

Cloudvisor具体架构

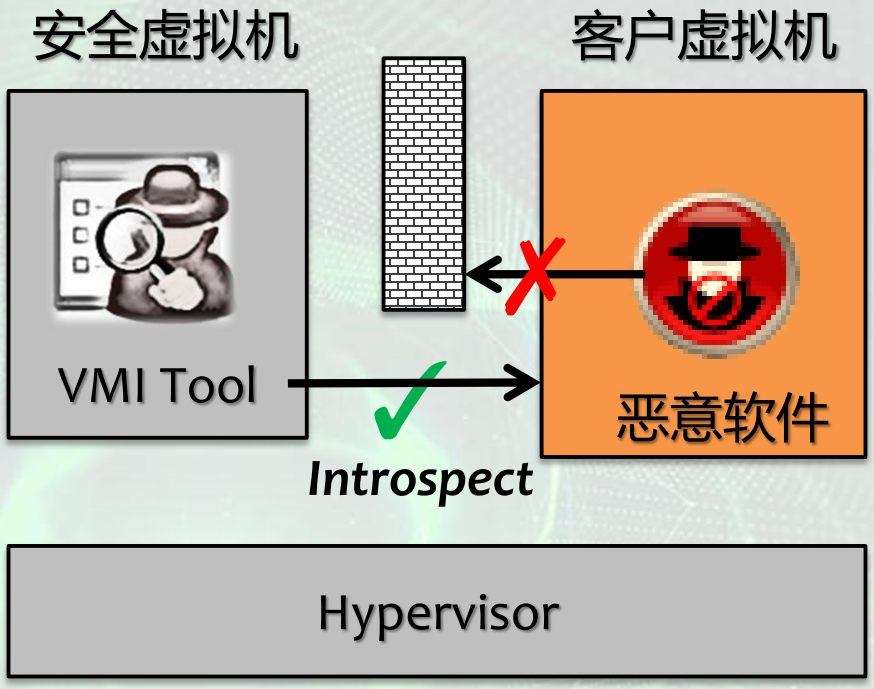
- **不相信控制VM和虚拟机监控器**
  - 代码多：百万行代码，可能存在大量漏洞
  - 人员多：大量管理员都可操作
- **只相信CloudVisor**
  - 代码少：5000行代码，出现漏洞的概率低
  - 人员少：有权限接触CloudVisor的人非常少
  - 权限高：一旦启动，无法被关闭或绕过



Cloudvisor: retrofitting protection of virtual machines in multi-tenant cloud with nested virtualization, SOSP'11.

虚拟机自省技术：VM Introspection

- **VMI的优势**
  - 不用修改客户虚拟机
  - 保证杀毒软件自身的安全
  - 新的恶意软件检测技术
  - 性能损失小
  - 在学术界已有十多年积累
  - 已集成在VMware套件中



- **恶意管理员攻击方式-2：硬件攻击**
  - 直接在服务器上接入恶意硬件
  - 利用物理手段，直接读取内存中所有数据
  - 绕过所有软件防御
- **攻击者**
  - 管理员，或伪装成数据中心的维护人员
  - 政府要求获得数据

上海瓶钵信息科技 上海交通大学 ISC 2016 中国互联网安全大会 360互联网安全中心

基于 INTEL SGX 的云安全能力增强

最小化可信基

解决方案：HyperCoffer, by IPADS

- **设计：采用加密处理器**
  - 所有数据在内存中为加密状态
  - 仅当数据从内存进入处理器时才解密
  - 前提：攻击者无法直接读取处理器内部数据
- **实现：可部署性**
  - 用户将虚拟机镜像加密后上传到云服务器运行
  - 用户虚拟机本身不需要修改，只需要加密

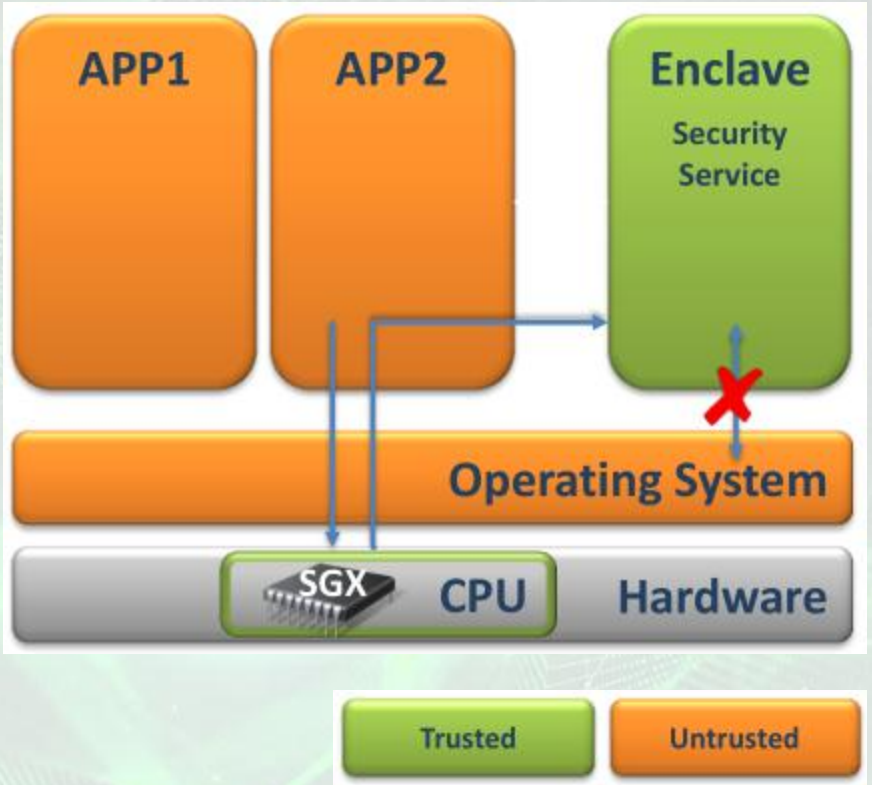
HyperCoffer具体架构

- **不相信内存、硬盘等设备**
  - 攻击者可物理攻击获取明文
- **只相信安全处理器**
  - 无法对处理器进行物理攻击
- **云服务商完全没有明文**
  - 依然能管理：如开机、关机、迁移等

Architecture Support for Guest-Transparent VM Protection from Untrusted Hypervisor and Physical Attacks, HPCA'13

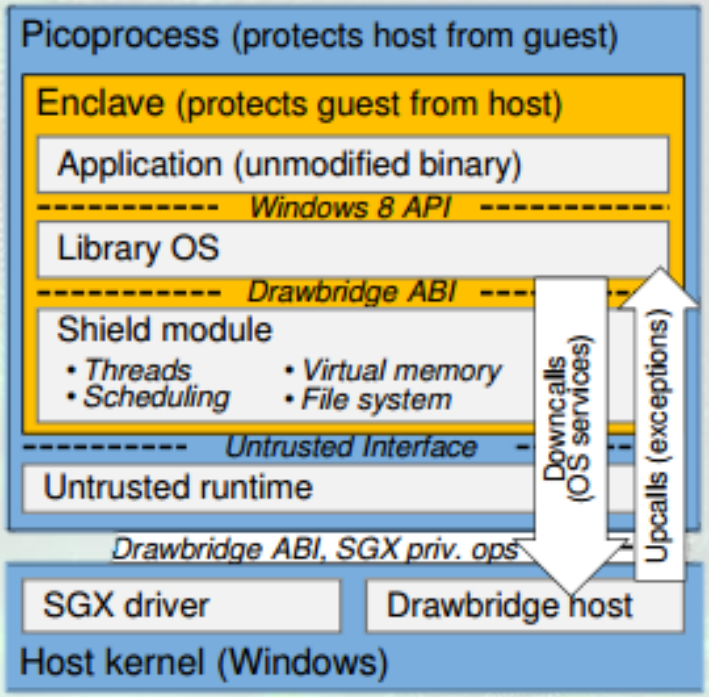
Intel SGX 技术

- **基于SGX的硬件隔离**
  - 代码运行在Enclave中
  - 支持多线程并发，可被中断
- **只信任CPU**
  - 完全透明的内存加密
  - 18条新指令
- **Enclave本身没有特权**
  - 只能运行在用户态
  - 内存保护机制



Haven：在SGX中运行原生应用

- **使用libOS对应用进行封装**
  - 使用libOS提供系统服务
  - 重定向本地系统调用
- **基于Windows实现**
  - 使用了DrawBridge内核
  - 可直接运行SQL Server



Shielding applications from an untrusted cloud with haven, OSDI'14.

上海瓶钵信息科技 上海交通大学 ISC 2016 中国互联网安全大会 360互联网安全中心

基于 ARM TRUSTZONE 技术的可信执行环境

从移动设备到服务器的延伸

ARM TrustZone提供的芯片级隔离

- **TrustZone提供了与外界完全隔离的运行环境**
  - 即使外部OS完全被攻破，攻击者也无法读取或篡改安全OS
  - 安全世界与外部完全独立，运行自有操作系统和应用生态
  - 适合用来保存关键的数据
- **不需要额外的硬件支持**
  - 利用ARM TrustZone技术，目前主流芯片均已支持
  - 通过分时复用，用1个CPU实现2个CPU的功能
  - 相比2个CPU：**成本更少，功耗更低，性能更好**

基于ARM64的服务器产品

HP ProLiant
(Applied Micro, TI)

Softiron 64-0800
(AMD)

Gigabyte R120-P30
(Applied Micro)

Wiwynn LN1148-10SL
(Marvell)

Gigabyte MT70-HD0
(Cavium)

Cirrascale RM1905D
(Applied Micro)

Mitac Datun
(Applied Micro)

Gigabyte D120-S3G
(Annapurna)

什么是TEE？

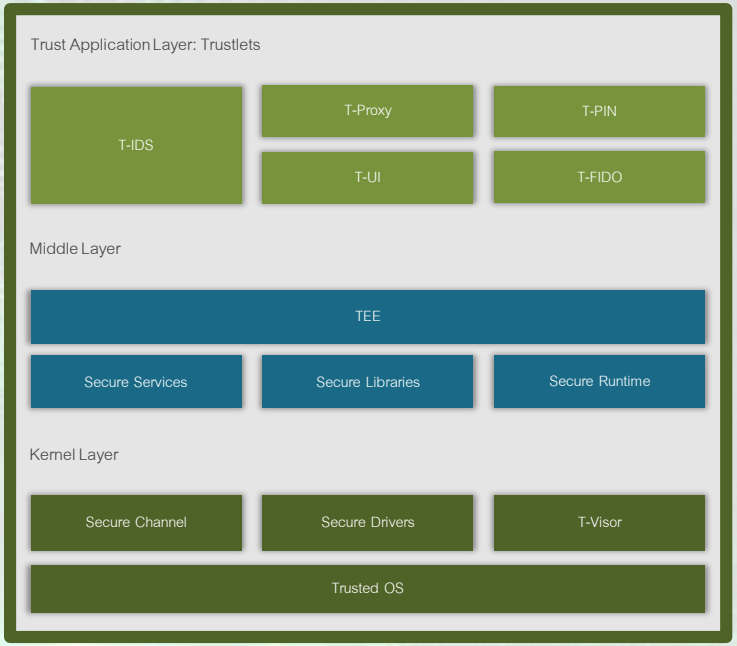
- **TEE (Trusted Execution Environment)**
  - GlobalPlatform在2013年提出
  - 与REE (Rich Execution Environment) 对应
- **TEE通常用于运行关键的操作**
  - 移动支付：指纹验证、PIN码输入等
  - 机密数据：私钥、证书等的安全存储
  - 内容保护：DRM（数字版权保护）
  - …

我们身边的TEE

- **移动终端领域，TEE已经成为指纹手机的标配**
  - 使用TEE来隔离指纹的采集、存储、验证等过程
  - 即使手机被越狱或Root，攻击者也无法获取指纹数据

TEE内部架构

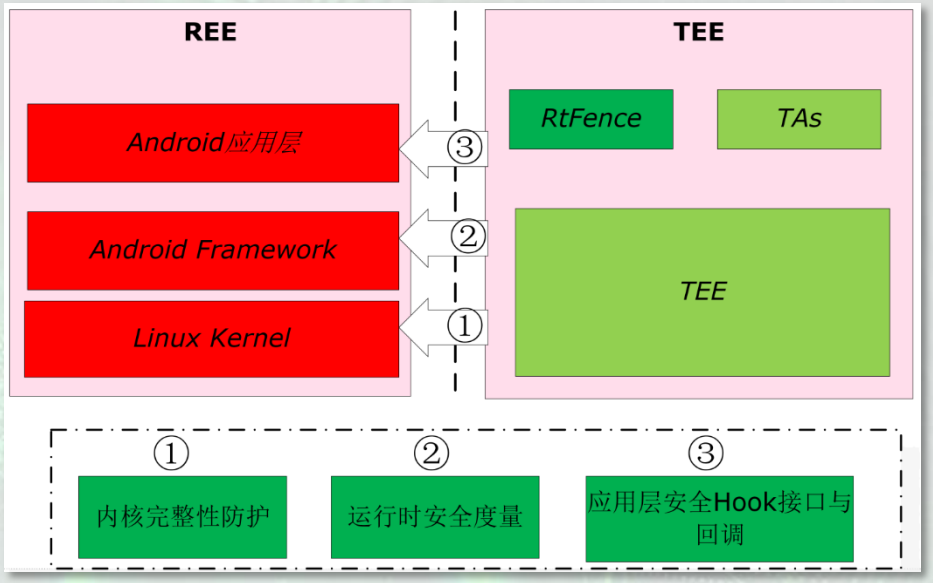
- **TEE内部运行一个完整的操作系统**
  - 与REE操作系统无关，也无需适配
  - TEE与REE通过共享内存进行交互
- **TEE内部也分内核态与用户态**
  - TEE的用户态可以运行多个不同的安全应用（TA）
  - 安全应用可支持动态下载和动态更新
- **TEE内部结构**
  - **Secure OS + 中间件 + 安全应用 + 外部交互**



TEE运行环境

RTFence：实时增强REE的系统安全

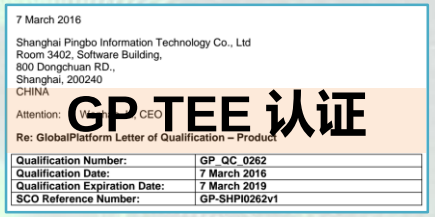
- **内核完整性监控**
  - 保证内核的完整性
- **运行时度量**
  - 确保关键数据完整性
- **安全服务Hook与回调**
  - 为上层安全软件提供防护接口
- **检测效果**
  - 能检测与防御大部分1-day与0-day内核漏洞攻击



关于我们：上海瓶钵

上海瓶钵信息科技 上海交通大学 中国互联网安全大会 360互联网安全中心

- **专注于移动安全的核心技术研发**
  - 来自上海交大，2012年开始研发，2015年初市场化
  - 由知名安全研究人员和业内具有影响力的专业人员组成
- **获得国内外知名企业的认可**
  - 与国内外知名企业/机构合作，成为**华为官方供应商**
- **产品通过国内外专业机构的检测与认证**
  - 获2015年挑战杯**全国特等奖**
  - 通过GP、工信部TAF、公安部三所等安全认证



TrustKernel

谢　谢