云主机安全可信关键技术及实现

演讲人：蔡一兵　博士

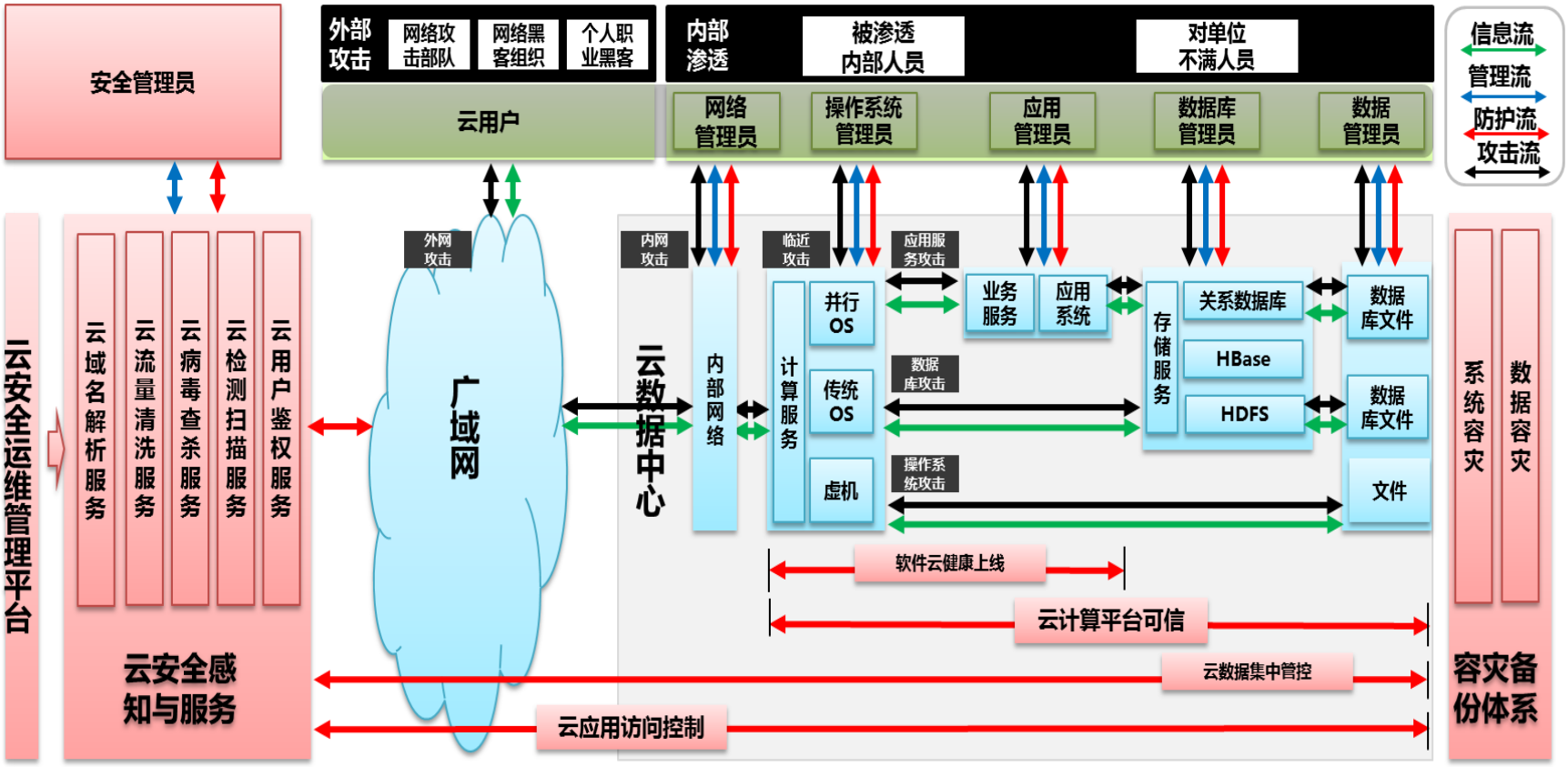
职　务：浪潮信息安全事业部 副总经理

日　期：2014年9月24日

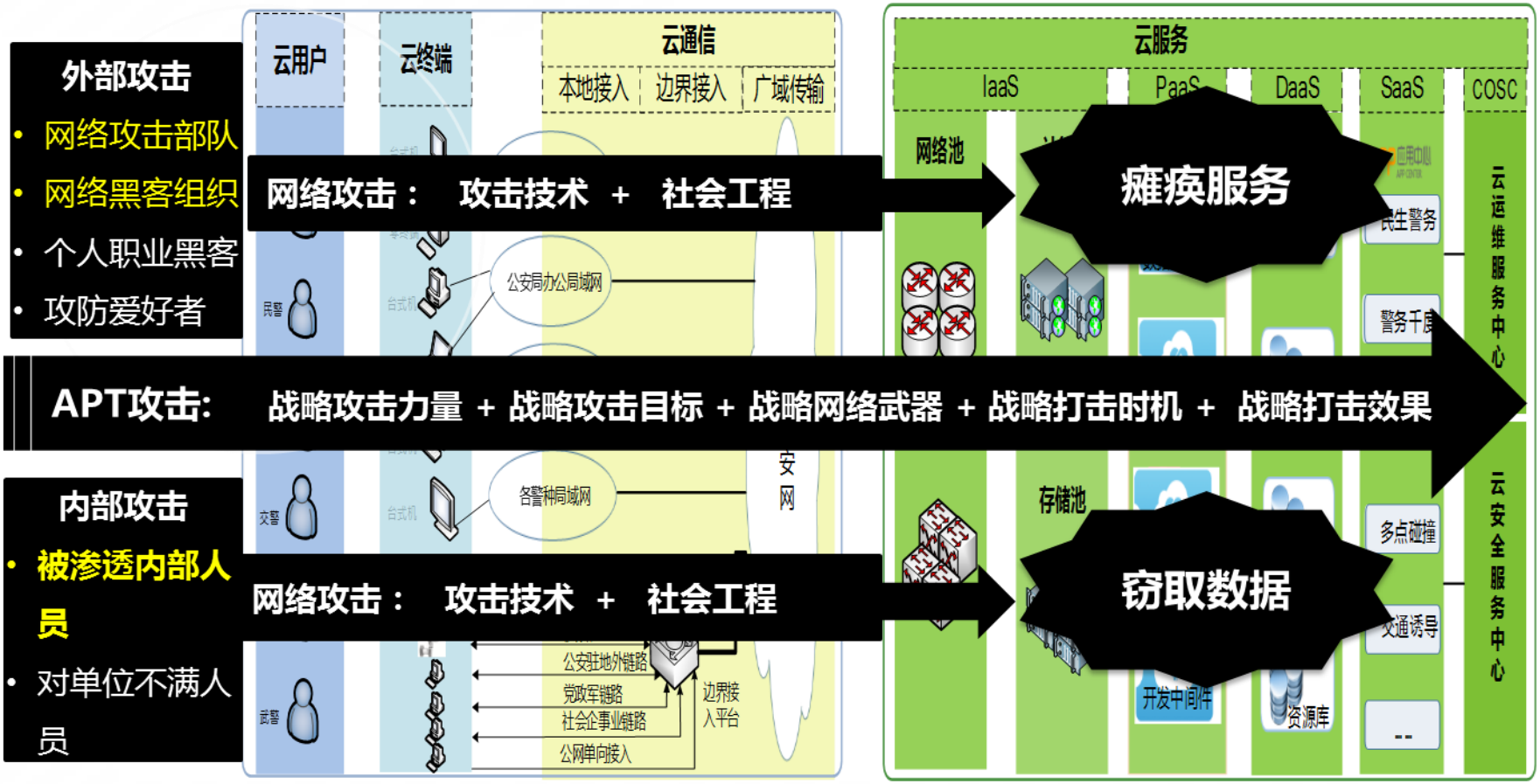
提纲

1. 云主机面临的安全威胁
2. 云主机安全可信关键技术
3. 云主机安全产品实践

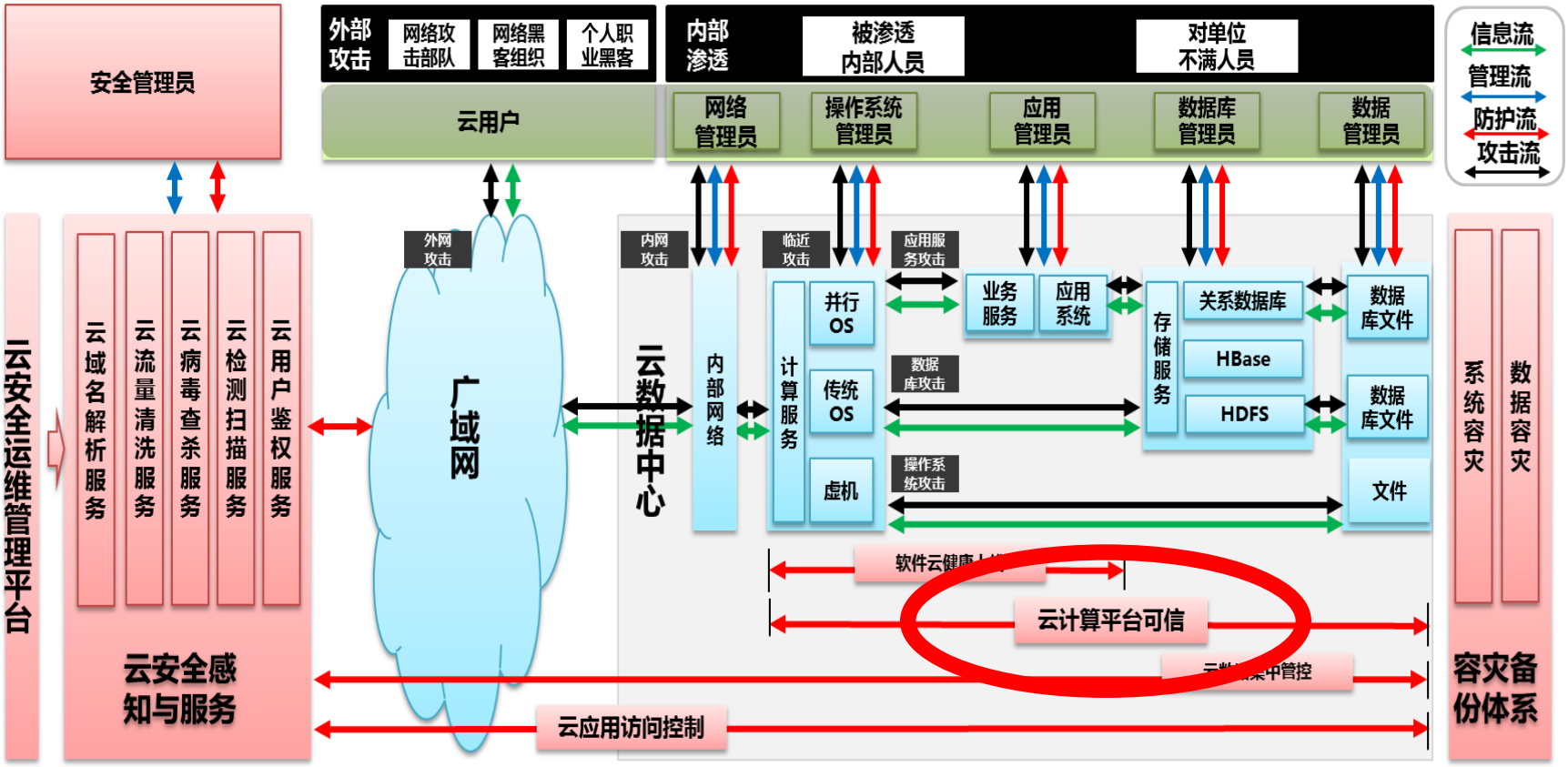
云数据中心防御体系视图



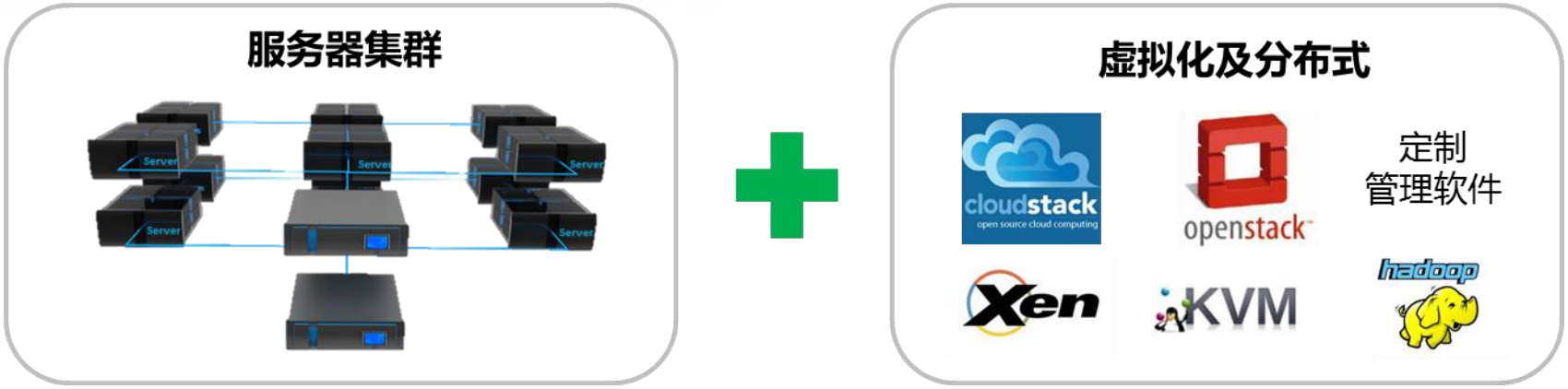
云数据中心威胁视图


外部攻击
网络攻击部队
网络黑客组织
个人职业黑客
攻防爱好者
网络攻击： 攻击技术 + 社会工程
瘫痪服务
APT攻击: 战略攻击力量 + 战略攻击目标 + 战略网络武器 + 战略打击时机 + 战略打击效果
内部攻击
被渗透内部人员
对单位不满人员
网络攻击： 攻击技术 + 社会工程
窃取数据
云用户
云终端
云通信
本地接入
边界接入
广域传输
公安局办公局域网
各警种局域网
公安驻地外链路
党政军链路
社会企事业链路
公网单向接入
边界接入平台
云服务
IaaS
PaaS
DaaS
SaaS
COSC
网络池
存储池
开发中间件
资源库
多点碰撞
交通诱导
云运维服务中心
云安全服务中心

云计算平台可信

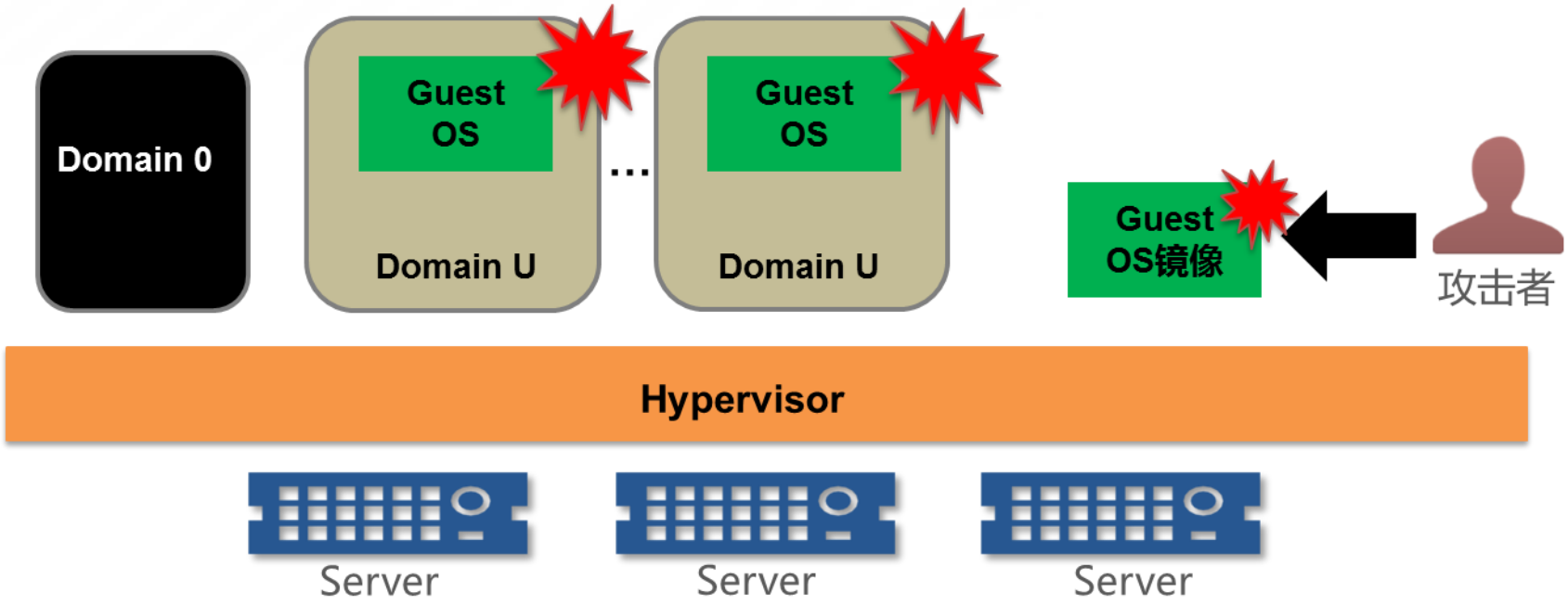

安全管理员
外部攻击
网络攻击部队
网络黑客组织
个人职业黑客
内部渗透
被渗透内部人员
对单位不满人员
信息流
管理流
防护流
攻击流
云用户
网络管理员
操作系统管理员
应用管理员
数据库管理员
数据管理员
云安全运维管理平台
云域名解析服务
云流量清洗服务
云病毒查杀服务
云检测扫描服务
云用户鉴权服务
外网攻击
广域网
内网攻击
云数据中心
内部网络
临近攻击
应用服务攻击
计算服务
并行OS
传统OS
虚机
业务服务
应用系统
存储服务
关系数据库
HBase
HDFS
数据库文件
数据库文件
文件
数据库攻击
操作系统攻击
软件云健康
云计算平台可信
云安全感知与服务
云应用访问控制
系统容灾
数据容灾
容灾备份体系

什么是云主机



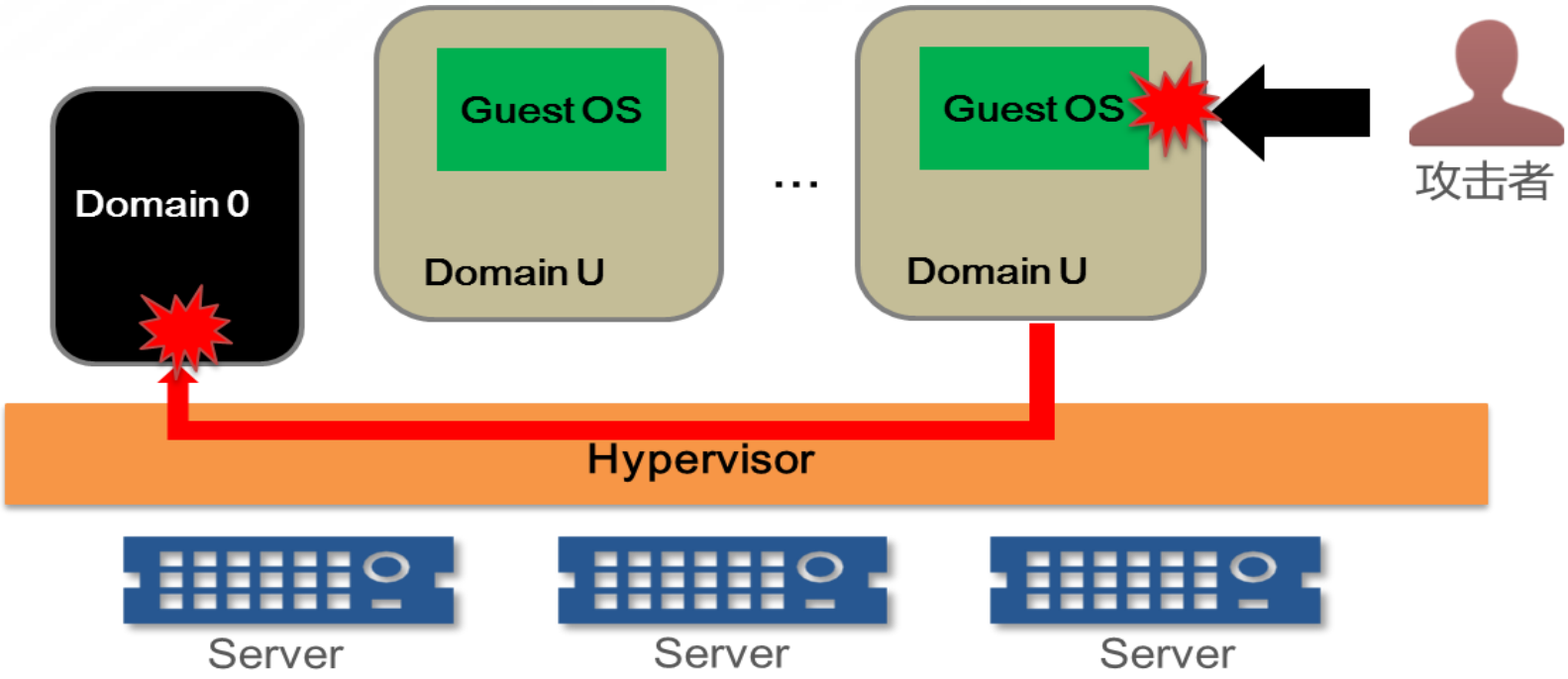
云主机是整合了计算、存储与网络资源，为提供基于云计算模式的**按需使用**和**按需付费**能力的服务器租用服务。云主机租用服务旨在有效降低客户获得计算能力的成本，简化主机管理过程。

云主机安全风险—Guest OS镜像污染



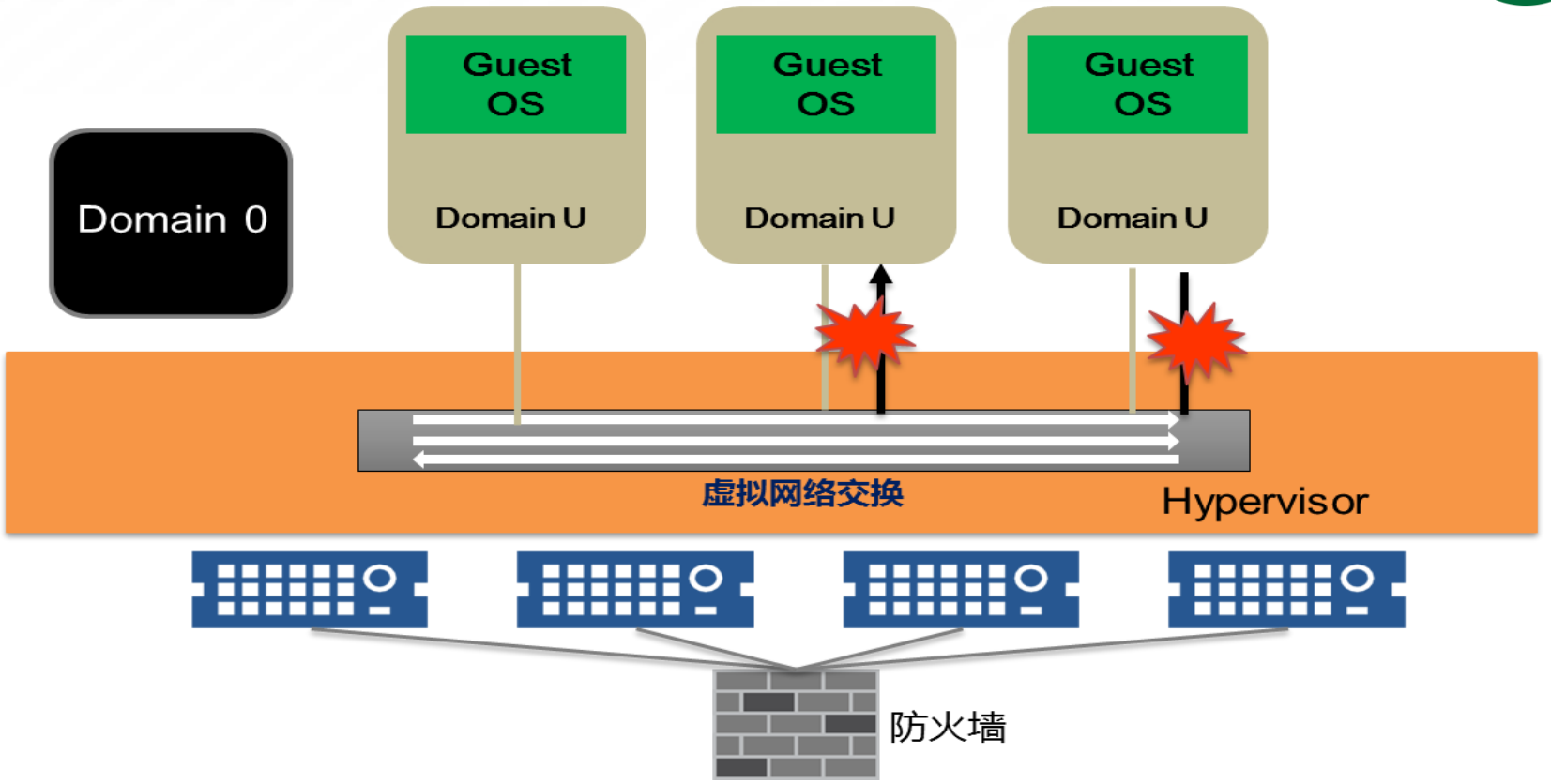
Guest OS本身存在安全漏洞，由于管理不善和安全防护措施不到位，黑客很可能利用漏洞攻击Gest OS的镜像，危害将从单个物理主机扩散到计算池、存储池，甚至整个云数据中心。

云主机安全风险——虚拟机逃逸



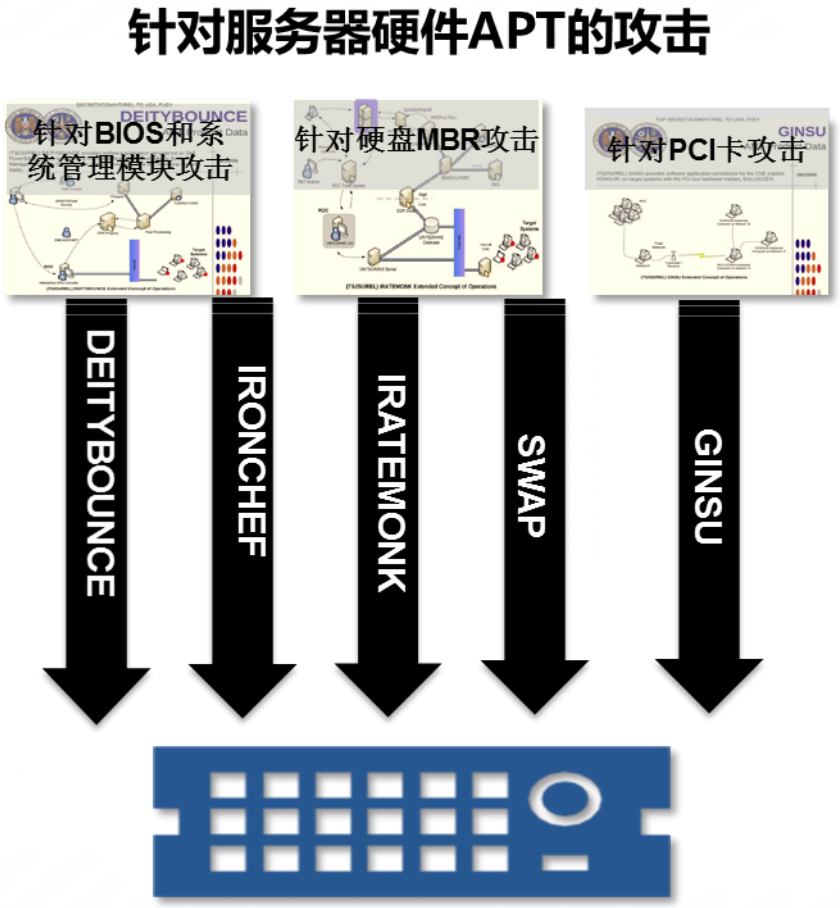
十年前windows操作系统存在大量安全漏洞状态类同，目前XEN、KVM等存在大量未知漏洞，通过Guest OS漏洞攻击Domain0，获取管理员权限，可以攻hypervisor层或者攻击其他主机。

云主机安全风险——虚拟环境下网络 报文难以捕捉



虚拟机内部流量在物理机内部或者同一个安全域内传输，对外不可见、东西向流量安全无法保障。

云主机安全风险——硬件层面APT攻击



- **DECITYBOUNE**：针对BIOS和系统管理模块的漏洞来获得执行OS的权限
- **GINSU**：在PCI卡中植入恶意代码，在系统重启时启动
- **IRATEMONK**：硬盘MBR区植入恶意代码，操作系统无法清除
- **IRONCHEF**：通过BIOS和系统管理模块漏洞，植入恶意代码
- **SWAP**：在BIOS和硬盘受保护区植入恶意代码

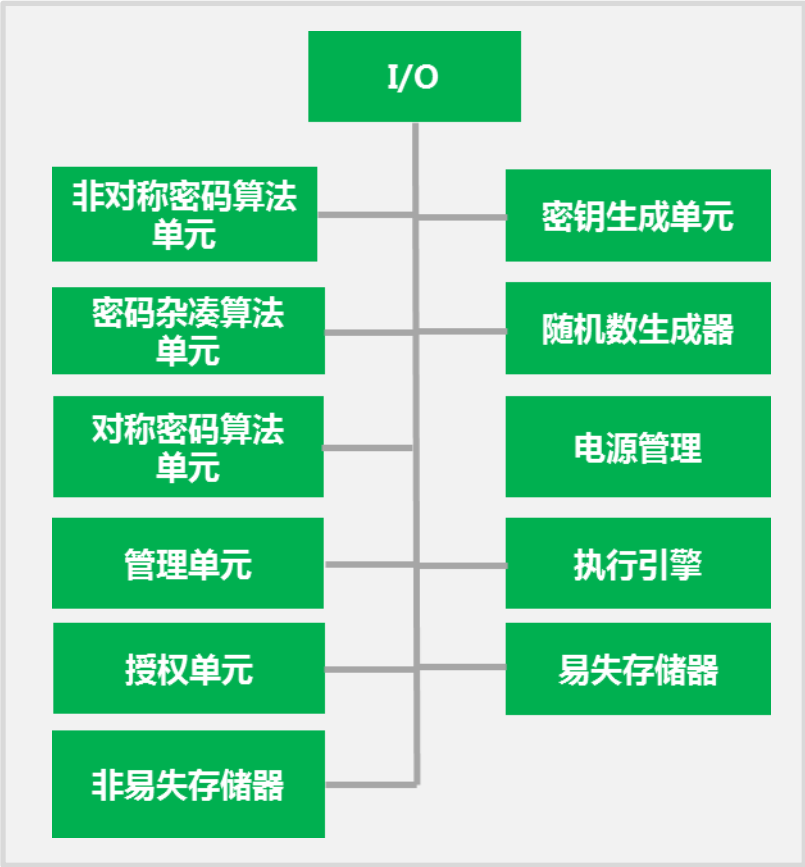
提纲

1. 云主机面临的安全威胁
2. 云主机安全可信关键技术
3. 云主机安全产品实践

云主机安全可信技术思路

云主机安全可信技术，将融合可信计算、操作系统加固、虚拟计算安全等技术，以可信芯片为根，构建链接固件、VMM、Guest OS和上层应用的信任链，应对云主机威胁。

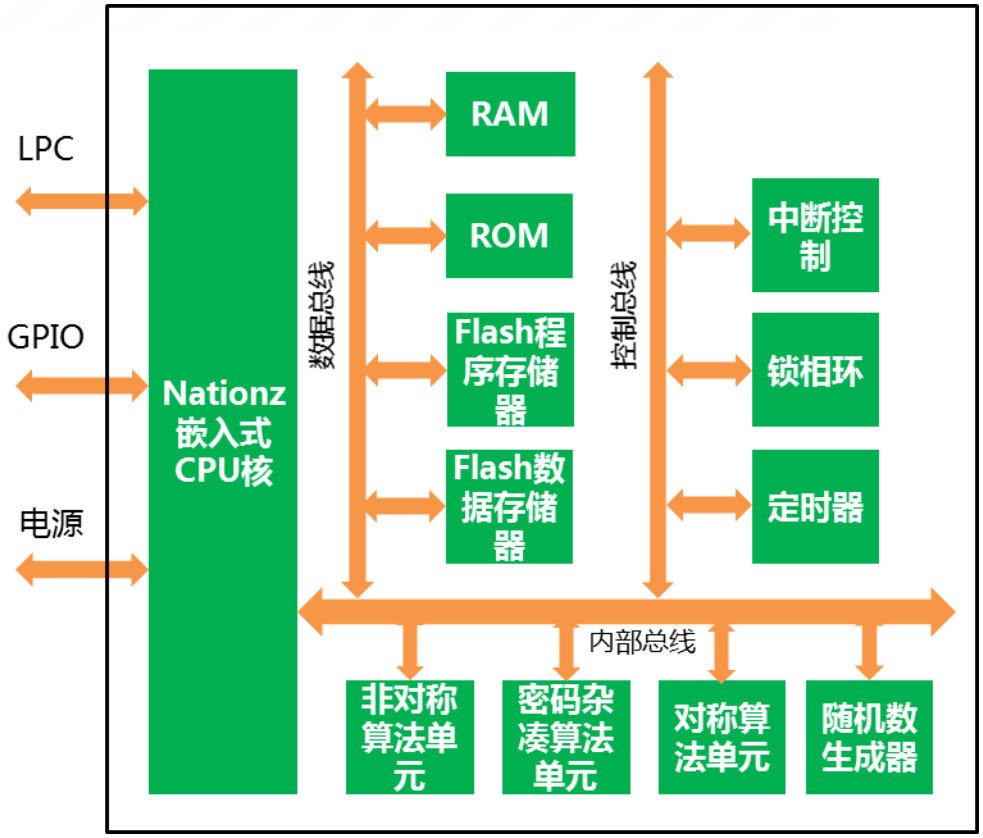
可信芯片——TPM2.0



TCG TPM2.0架构

- **TPM2.0规范是TCG（可信计算组织）于2014年正式发布**
- **TPM2.0与TPM1.2相比的特性：**
  - 支持中国商用密码算法（SM2、SM4）
  - 增加了对称密码算法
  - 改变了原有密钥结构树，适应VMM中的VM迁移
  - 支持多种PCR Bank，根据扩展PCR时所用的Hash算法而决定使用哪一个Bank

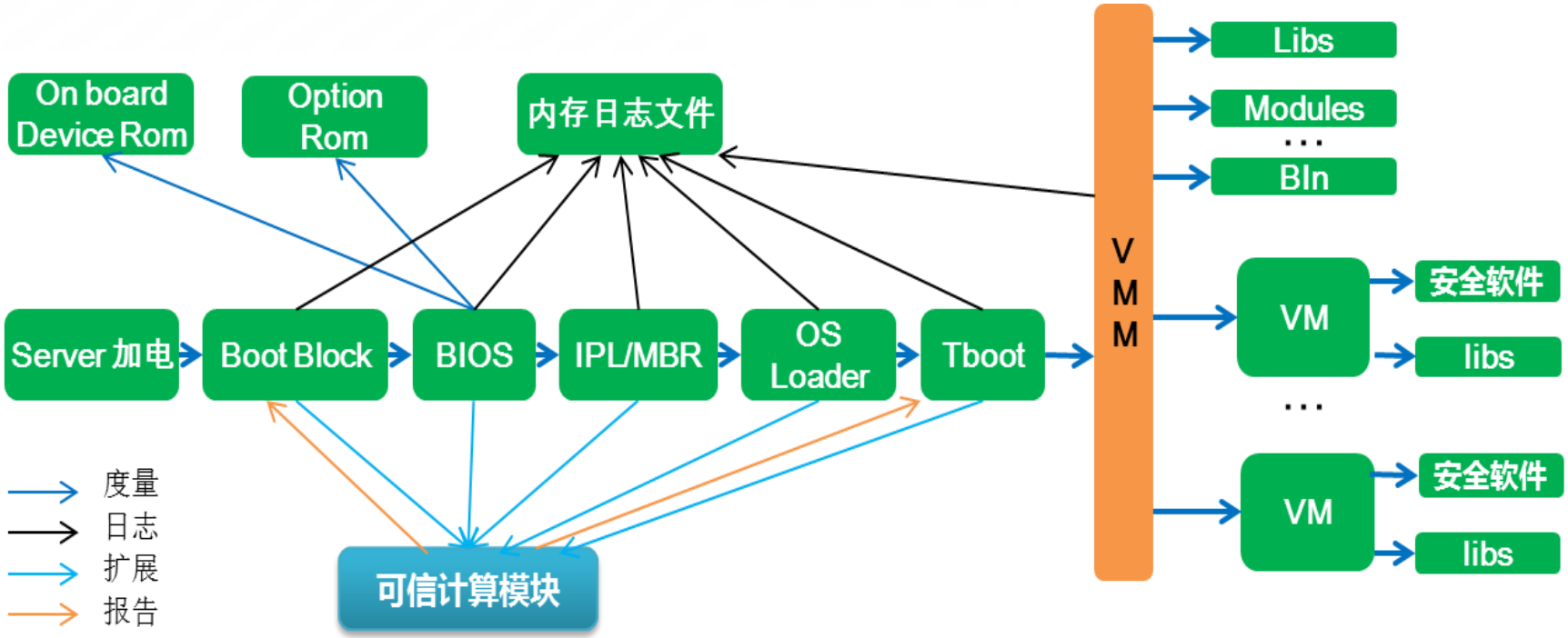
可信芯片——Z32H320TC芯片架构



国民技术Z32H320TC芯片架构

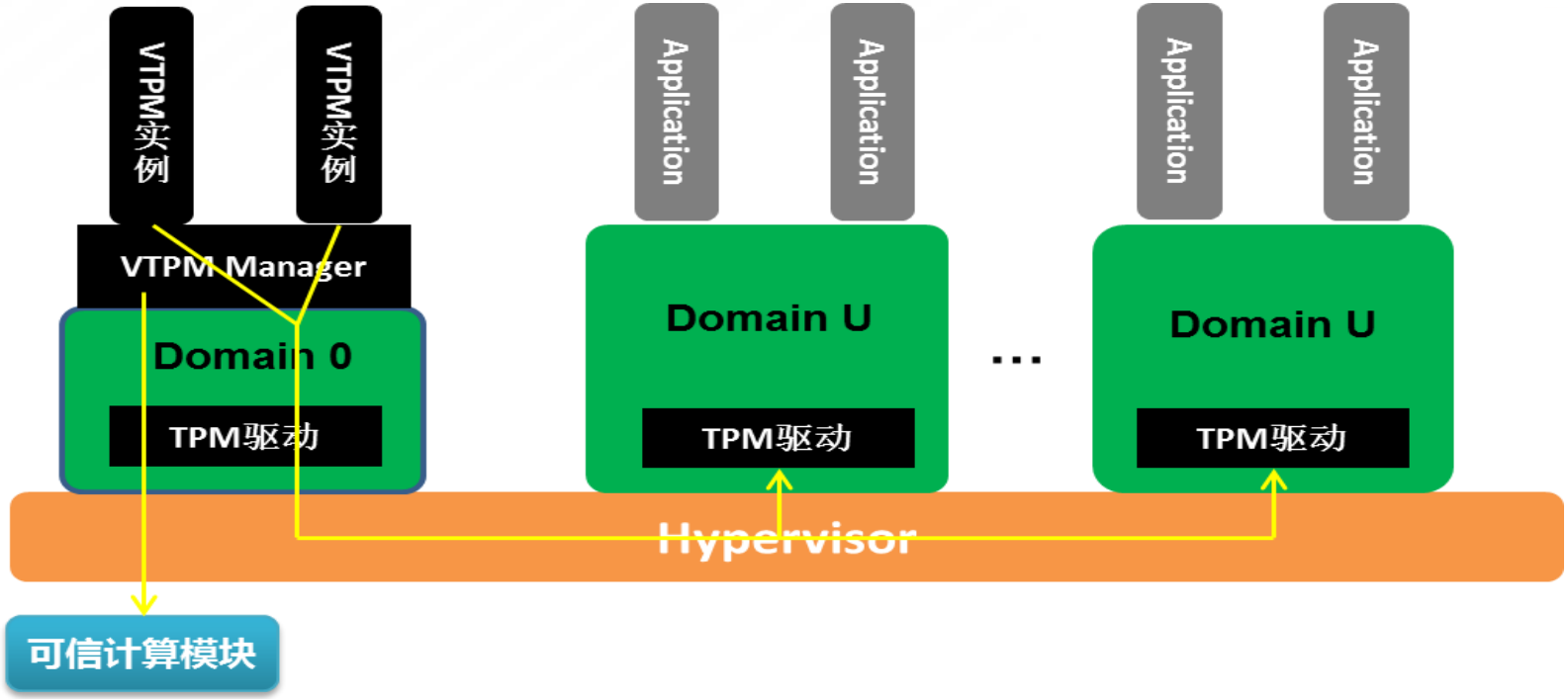
- **通过了保密局型号认证（编号：SXH2014022），批准型号SSX1401安全芯片**
- **国民技术嵌入式CPU核，提供平台身份证明，完整性度量、存储和报告服务及数据加密、访问授权等密码学服务**
- **密码算法性能**
  - SM4对称算法，速率>2Mbps
  - SHA-256、SM3密码杂凑算法，速率>1Mbps
  - SM2公钥算法，256位ECC签名时间<350ms

虚拟化可信——虚拟化环境下信任链的建立



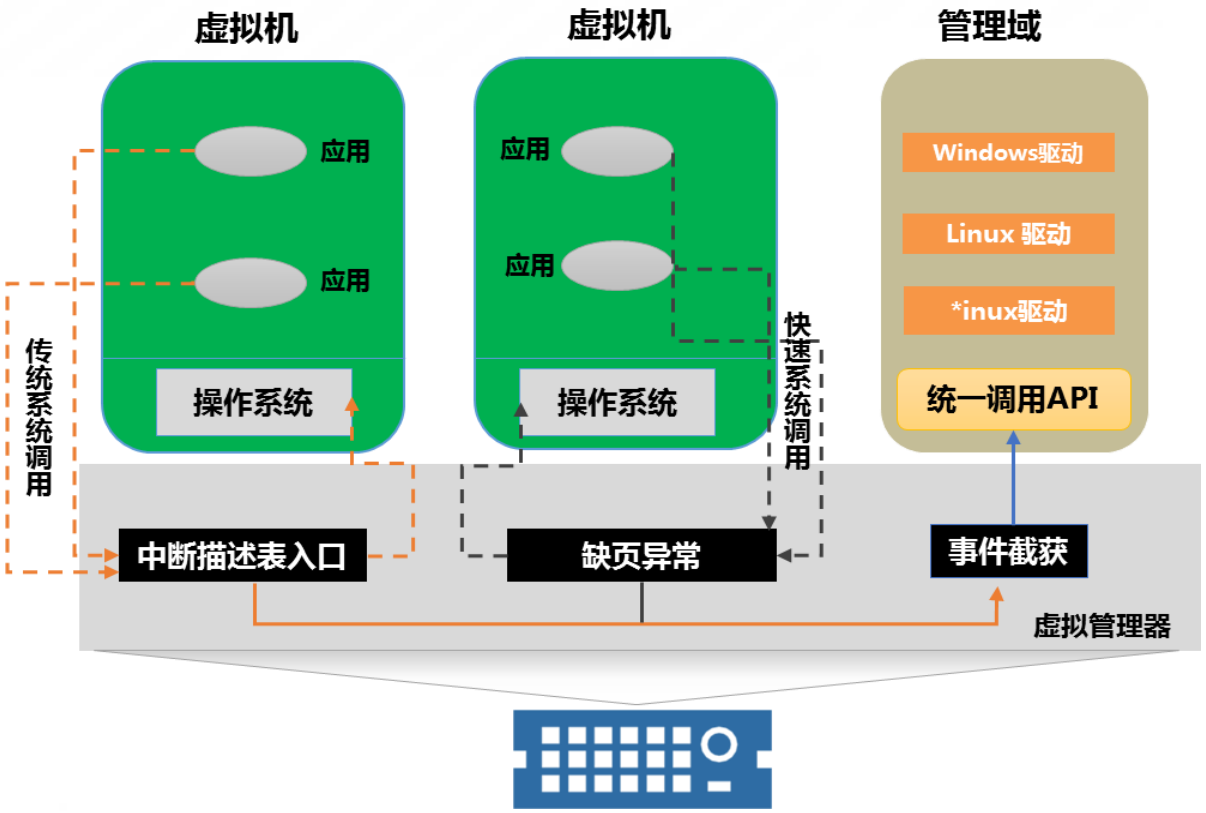
- 在进入到VMM之后的信任链构建则仅仅的使用可信计算芯片完成信任链扩展。
- 虚拟化环境下可信链如何扩展到vm？虚拟机迁移时如何应对信任链的变化？这两个问题较好的解决办法是使用vTPM

虚拟化可信——VTPM



- vTPM是由vTPM manager创建生成的，提供给 VM使用
- 需要可信计算能力的VM 与一个独立的vTPM实例相关联
- 通过Domain0的TPM 驱动给每条TPM 命令包上添加4bit 的vTPM 实例标识的手段使得用户VM 与vTPM 一一对应，这样客户VM 无法通过伪造命令包来与vTPM 进行通信

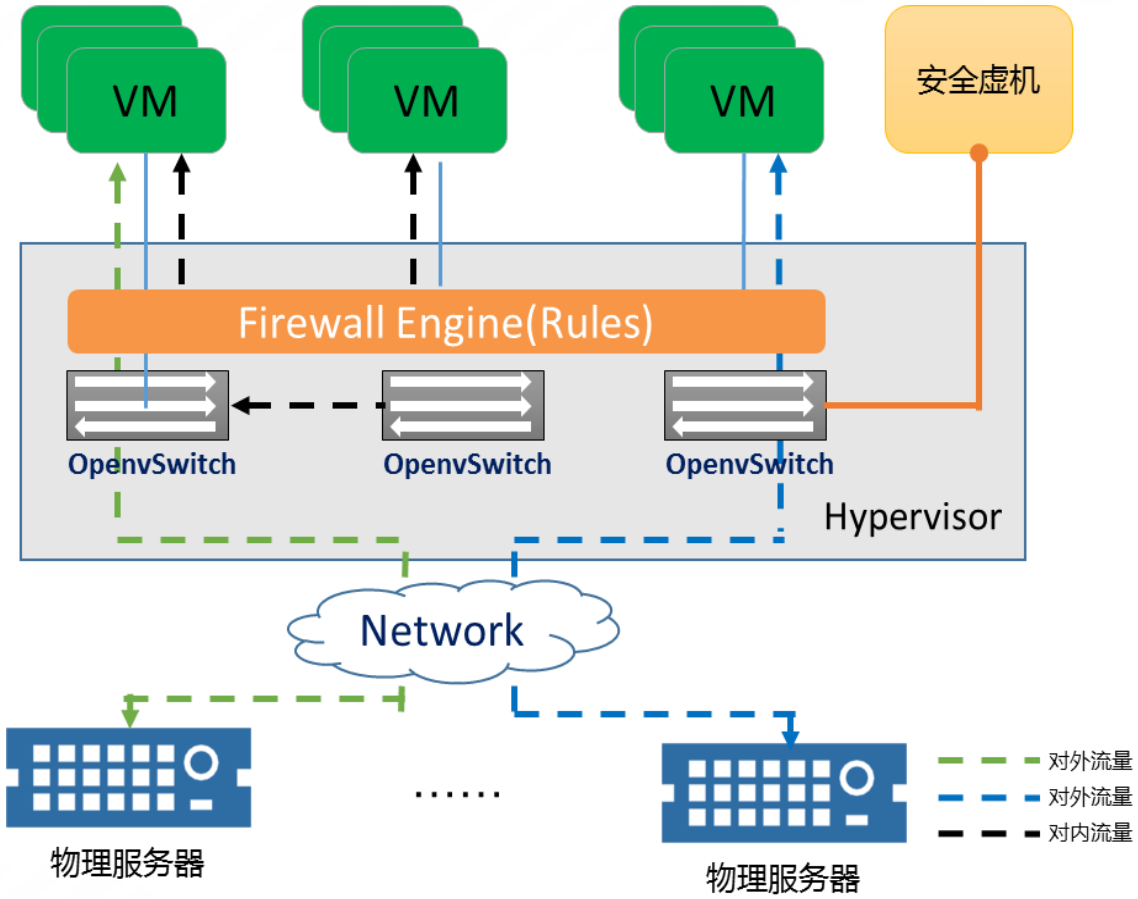
虚拟化安全——基于VMM的虚拟机监控



相对于传统系统调用，快速系统调用是不能进行直接拦截的，但是可以利用3个寄存器的特性来进行转化：SYSENTER_CS_MSR、SYSENTER_EIP_MSR、SYSENTER_ESP_MSR

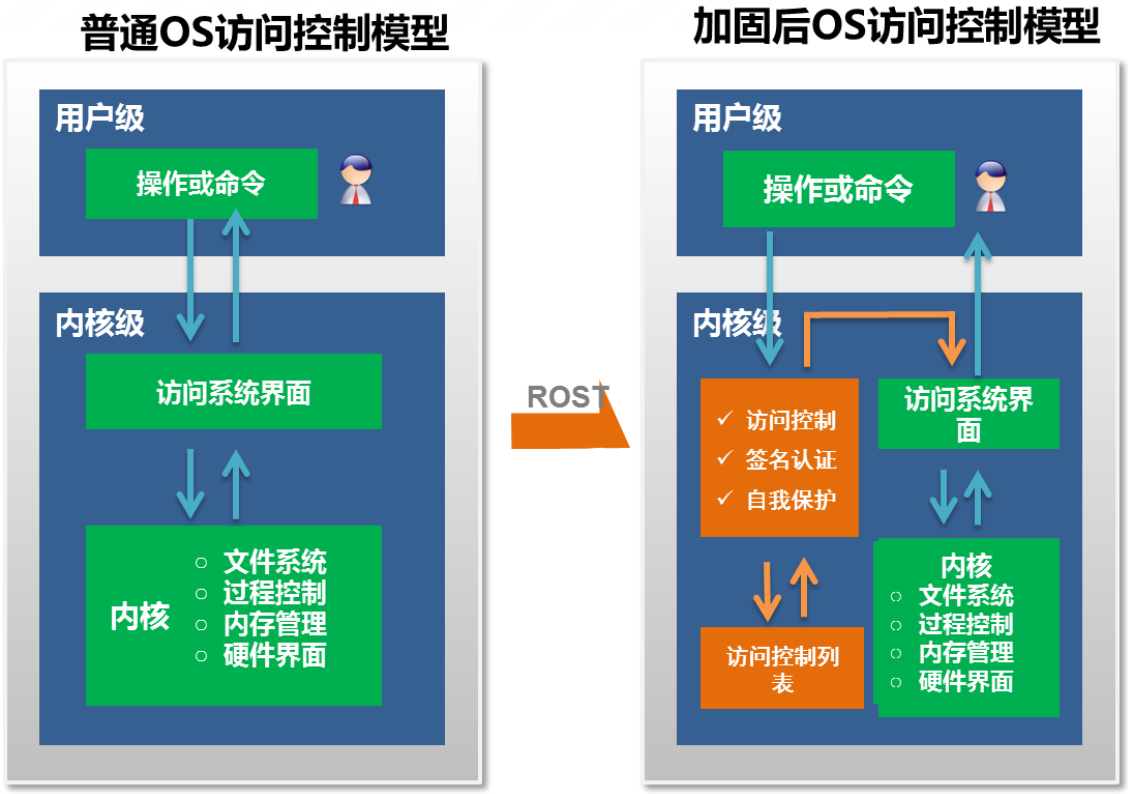
- **一次性部署在VMM中，供多个虚拟机同时使用，减轻部署和管理的复杂度，同时提高安全监控的性能**
- **可有效检测基于内核的Rootkit攻击，以及从VMM层检测Guest OS的恶意操作行为**

虚拟化安全——虚拟网络安全



- 虚拟安全引擎安装在虚拟平台的虚拟交换机之前，通过安全引擎实现各VM的安全策略的执行和管理，实现南北向和东西向的流量控制
- 安全虚机是针对安全引擎的管理、OpenvSwitch的Vlan、QoS的划分，同时也提供相应的日志和事件的展示，为提高产品的扩展性，也对第三方开发相应的API接口

Gest OS安全——内核加固技术

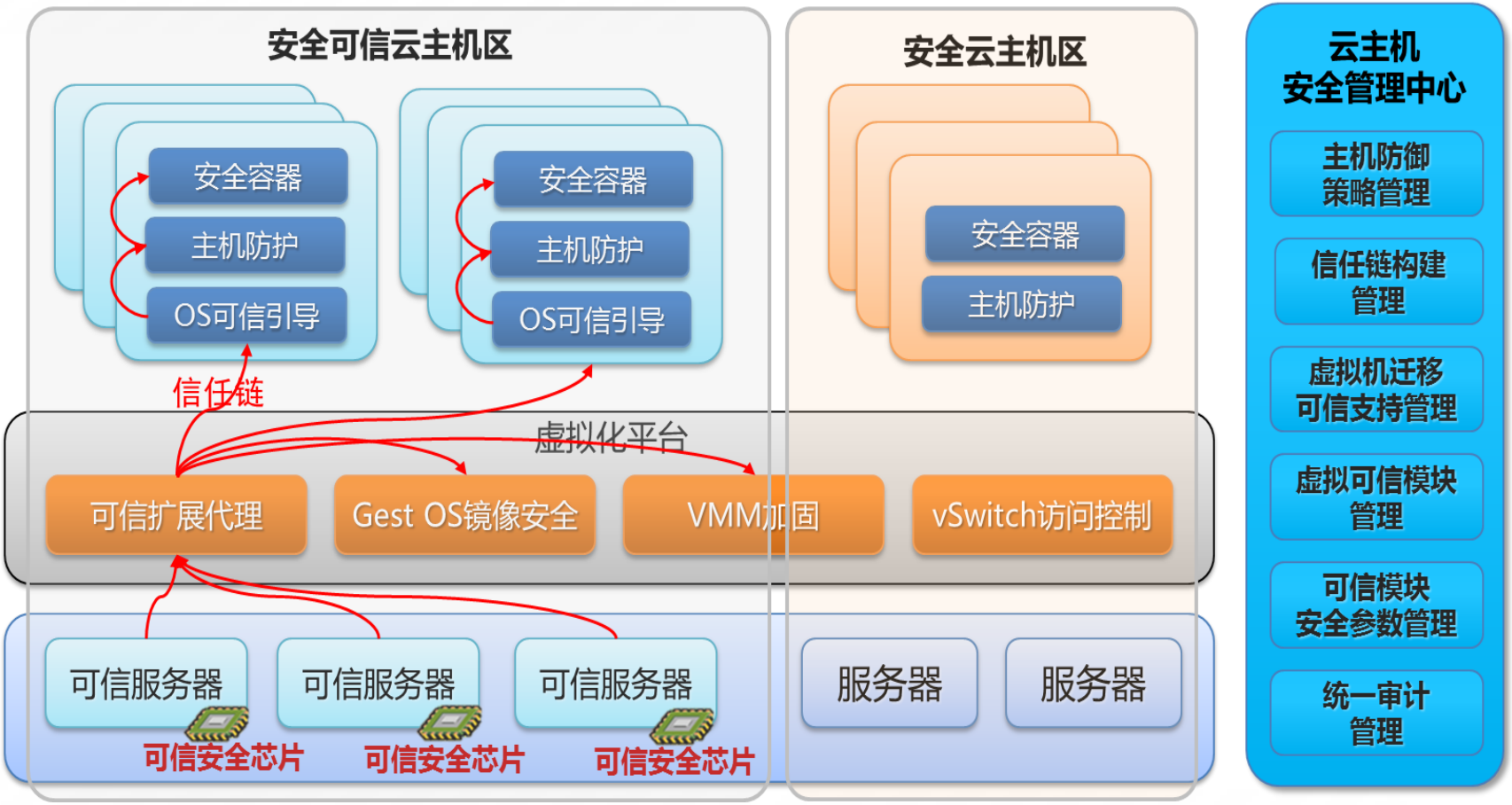


- Gest OS内核加固技术可实现操作系统三权分立、安全标记、强制访问控制等
- 可实现对大部分商用操作系统进行安全加固
- 免疫病毒、木马、未知恶意代码的攻击

提纲

1. 云主机面临的安全威胁
2. 云主机安全可信关键技术
3. 云主机安全产品实践

浪潮云主机安全可信产品架构



浪潮商用2路可信服务器

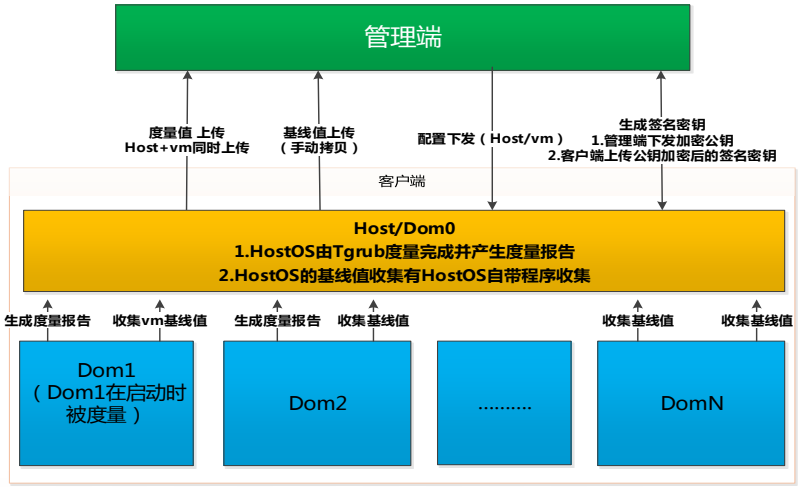
商用可信服务器是一款基于服务器可信安全模块和浪潮最新平台技术的安全服务器产品。该产品采用可信安全模块、安全主板、安全BIOS和安全软件等技术为用户打造的具有高安全性、高性能、高可靠性的安全服务器平台，适用于金融、能源、交通等行业数据中心建设。

- 符合国家管理规定，助您建设关键应用
- 完整的信任链建立，免疫恶意代码的攻击
- 以可信服务器为基础的软硬一体化可信解决方案
- 出色的性能和扩展性，满足用户多种需求

浪潮可信虚拟化套件

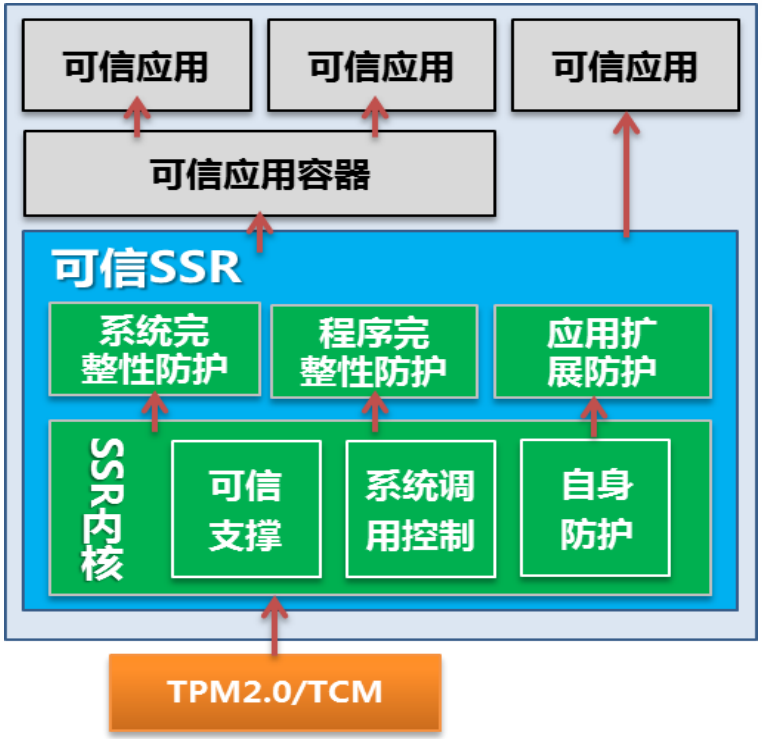
浪潮可信虚拟化套件可以帮助客户建立基于Xen虚拟化平台的可信计算支持。可实现度量VMM、VM镜像和VM镜像内的文件（如OS Kernel、重要应用程序），如果度量文件被篡改，可识别并进行可信报告，同时可选择是否阻止VMM或VM启动。

管理平台



套件技术架构

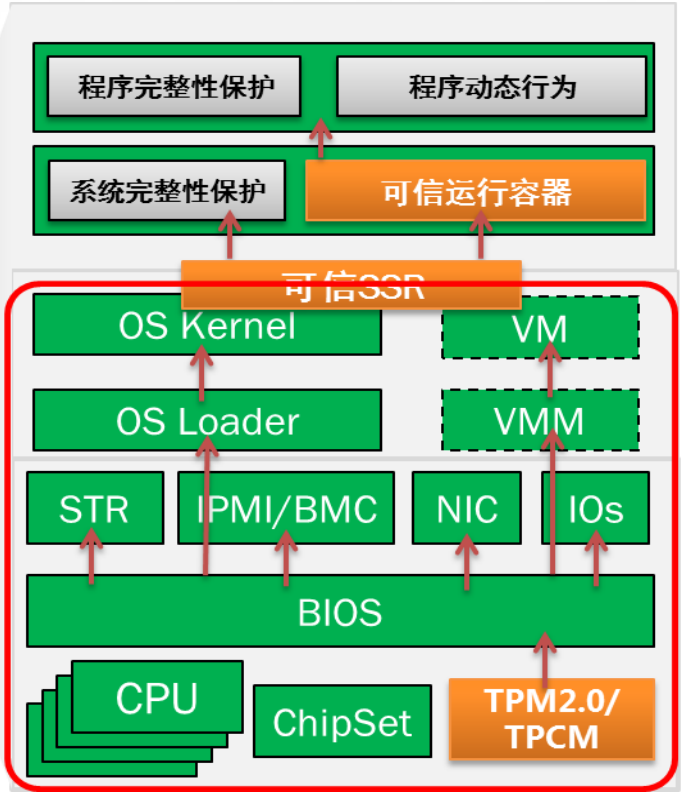
浪潮SSR可信支持

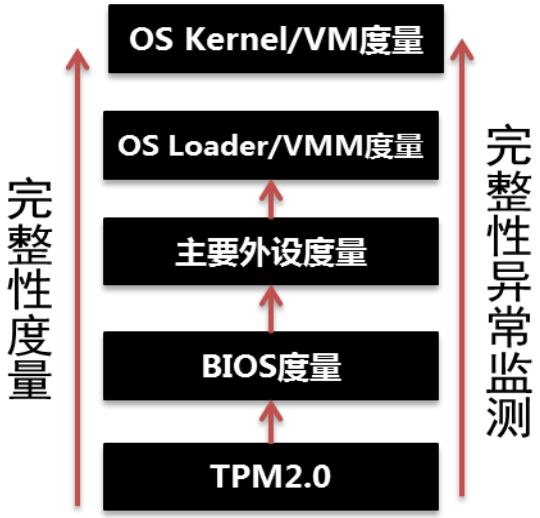


- SSR是一款运行于主流商业操作系统中的内核级安全软件
- 通过来自硬件层的信任链对其进行完整性度量和保护
- 可为应用提供完整的可信支撑及应用运行环境保护，防止恶意代码入侵及黑客攻击
- 可对系统和程序完整性提供支撑，从而保证信任链可传递到应用程序
- 可拦截程序对OS Kernel的调用，可监测到应用程序运行的所有行为，可发现程序的异常行为

以可信芯片为起点平台信任链的建立

可信服务器

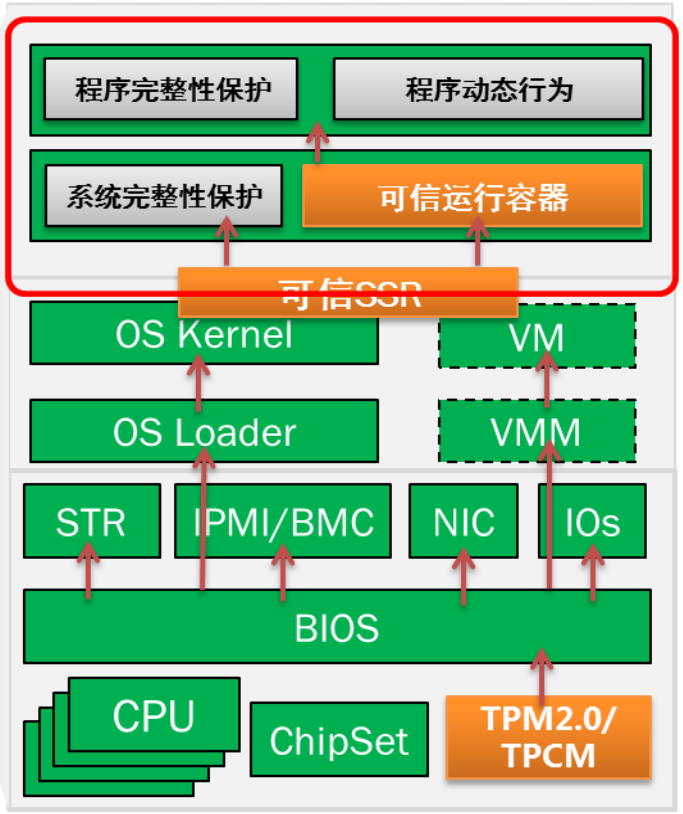


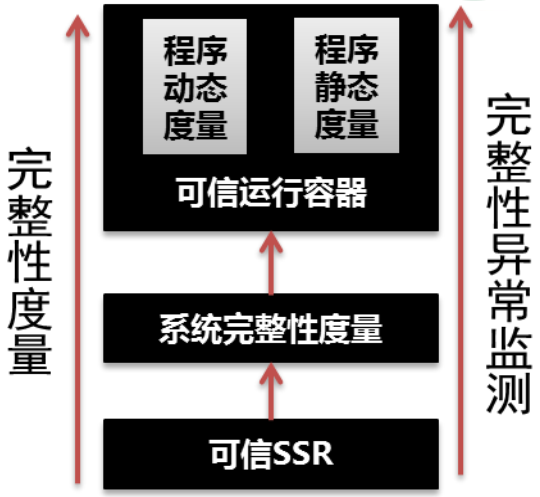


- 通过对BIOS及主要外设的完整性度量，防止固件层敌对势力恶意代码植入
- 通过平台完整性异常监测，及时发现平台存在的安全问题

以可信SSR为起点程序信任链的建立

可信服务器





- 通过系统及程序完整性度量、保护和监测，及时发现软件层的恶意代码植入及黑客入侵
- SSR处于OS内核层，通过可信平台的完整性度量和保护，构造可信的SSR
- 通过可信的SSR，为OS重要配置及软件提供完整性度量和保护，防止敌对入侵

浪潮云主机安全可信价值

ISC 2014

敌对势力			应对之道	
黑客组织 个人职业黑客	商业机密窃取 网络破坏	可信应用程序	防应用恶意代码植入 软件可控/异常发现	可信应用程序 安全运行容器
网络攻击部队 黑客组织	APT攻击 网络情报窃取	可信OS/可信VMM	防OS恶意代码植入 OS运行异常发现	可信基础软件 操作系统安全
网络攻击部队	APT攻击 网络情报窃取	可信服务器硬件平台	防固件恶意代码植入 硬件/固件异常发现	可信计算芯片 服务器国产化

ISC 2014

Thanks!