RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑

可信计算的一个有效应用：
租客自助服务定义管理的云中可信网络

Trusted Computing's Successful Application—
Tenant Self-servicing Defined and Managed Trusted LAN in the Cloud

毛文波

道里云信息技术

RSA CONFERENCE CHINA 2012
RSA信息安全大会2012

专题会议主题：

专题会议分类：

内容提纲

- 多租赁云数据中心的安全问题：如何隔离租客
- 现有方法讨论
- 可信计算与可信虚拟化架构上：虚拟机与LAN的真空包装
- 由租客自助服务定义与管理的云中可信网络（Tenant Self-servicing Defined and Managed Trusted LAN）
- 租客自助可编程性
- 讨论：安全操作系统设计原理的与时俱进
- 结论

多租赁云数据中心的安全问题

云计算数据中心的IT资源是多租赁（multi-tenancy）共享的，如何隔离租客？

传统IT安全的首要方法：用一个大防火墙围住整个数据中心

- 当数据中心 = IT作为资产时，这样做很有意义，攻击者都被挡在防火墙之外
- 当IT作为服务时（云），攻击者完全可以是合法租客（叫做骇租客），已经在防火墙里面了，将骇租客与良租客用防火墙围在一起，有意义吗？
- 主要尚未解决的云安全问题：对云数据中心的LAN做隔离；

  CPUs，存储等的隔离问题都已经解决的远比LAN的情况好

骇租客可以在自己租用的虚拟机里
1. 扫描获得别人的 IP/MAC；
2. 伪造扫描所得 IP/MAC 地址，就坐等收发包吧！（当然等受害者下班关机后更不易被察觉）

现有方法讨论：公有云方法1

公有云（由网络公司领头）——知识共享乃网络公司之头等大事！

什么？信息安全？自己在应用里加密吧！（讨厌，她的数据没法共享了！）

- 问题1：用户从来都不是安全专家，比如毫无管理密钥的能力。
- 问题2：用户自身想要违反安全策略呢，比如企图泄漏组织内部数据？
- 问题3：史上遗留下来的安全操作系统设计问题：让用户（小白级小山羊）和骇客（专家级大灰狼）在虚拟机内部相互PK！

问题3的根源：

史上留传下的OS都只管理本机硬件资源，以前本机资源有限，OS就只好与业务挤在一起，于是羊（用户）与狼（骇客）也在一起（都是业务嘛），猎手（安全OS，如Linux中的SELinux模块）也与狼在一起。猎手与狼PK孰强孰弱，还真不好说！

如今云时代了，OS已经不再是一个管理囿于本（虚拟）机资源的概念了，安全OS的设计当然也要与时俱进。稍后作更详细讨论。

现有方法讨论：公有云方法2

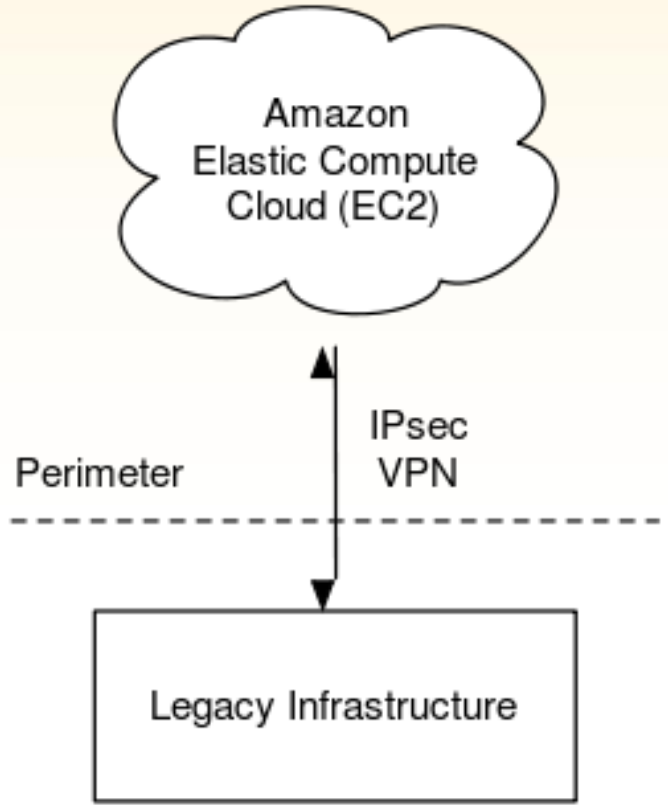
亚马逊 Virtual Private Cloud (VPC)

当租客在自己的办公场所已经配备自有IT资源时（Legacy Infrastructure, 主要是LAN资源）：

应用VPN技术 + CIDR技术，租客可以将租用的云上资源配置成自有LAN的一个子网；

由于子网的对外通信必须走母网的网关，其隔离策略完全由租客自有LAN的隔离策略确定，于是：

- 租客等于没有租用云上的LAN资源，因为云上的所有通信一律绕回家，走租客自有LAN的网关
- 本地自有LAN资源不是按需服务的
- 本地自有LAN是云上租用资源的通信瓶颈
- 租客不是在用纯粹的云服务，更像是云备份
- 仍然属于由租客自己负责安全技术



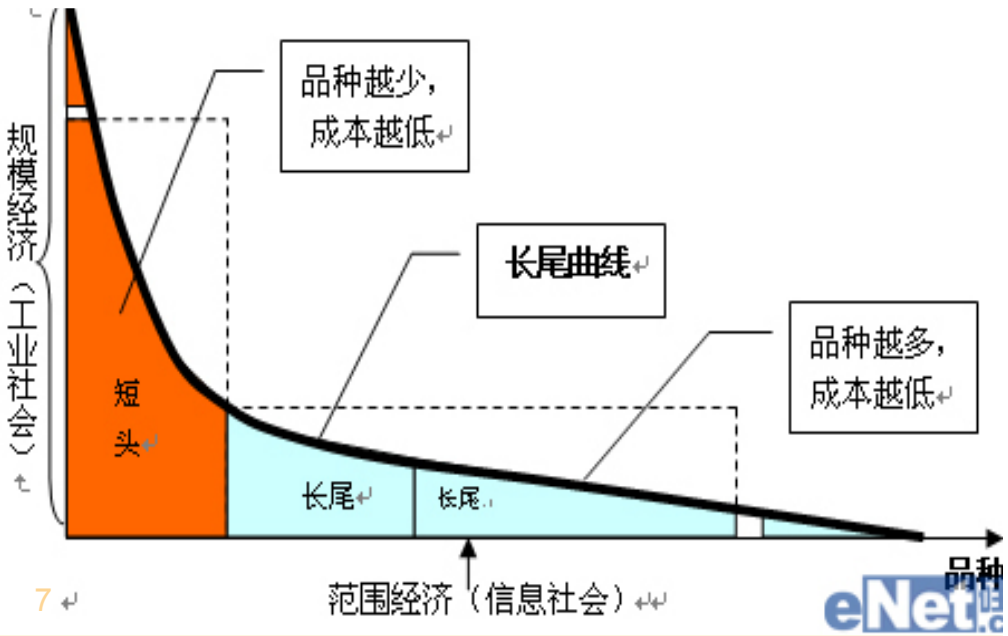
Virtual Private Cloud (VPC)

现有方法讨论：私有云方法

RSA CONFERENCE CHINA 2012

私有云——都说私有云比公有云安全，为什么呢？

- IT公司专家们当然要义不容辞负责用户安全，绝不制作让小山羊去咬大灰狼那样的产品
- 如Cisco的VDC（Virtual Device Contexts），VN-Tag，HP提出的VEPA技术，直至传统的VLAN等技术，都可在数据中心里虚拟出多个相互隔离的逻辑子网群
- 由交换器、路由器、专用服务器等硬件设备组合构成，不属于“软件定义的网络”（Not in Software Defined Network, SDN）
- 无弹性、不易快速动态部署按需变更、不支持租客自助部署私有子网群、网络拓扑受限于单个数据中心、昂贵、大量仅租用少量虚拟机的“长尾”小租客们用不起：为他们隔离小私有网会造成大量网络资源浪费



看来私有“云”确实比公有云安全

- 私有“云”？ 是IT作为服务吗？
- 可怜的小租客们，你们想云，

  但“云”不想你们哦 …

现有方法讨论：软件定义的网络，SDN（Software Defined Networking）

虚拟化数据中心共享许多IT资源：CPU，存储，网络；工业界在CPU与存储虚拟化方面都已经有不俗建树；网络虚拟化呢？目前业界与学术界都在“软件定义的网络”（SDN）方面努力：

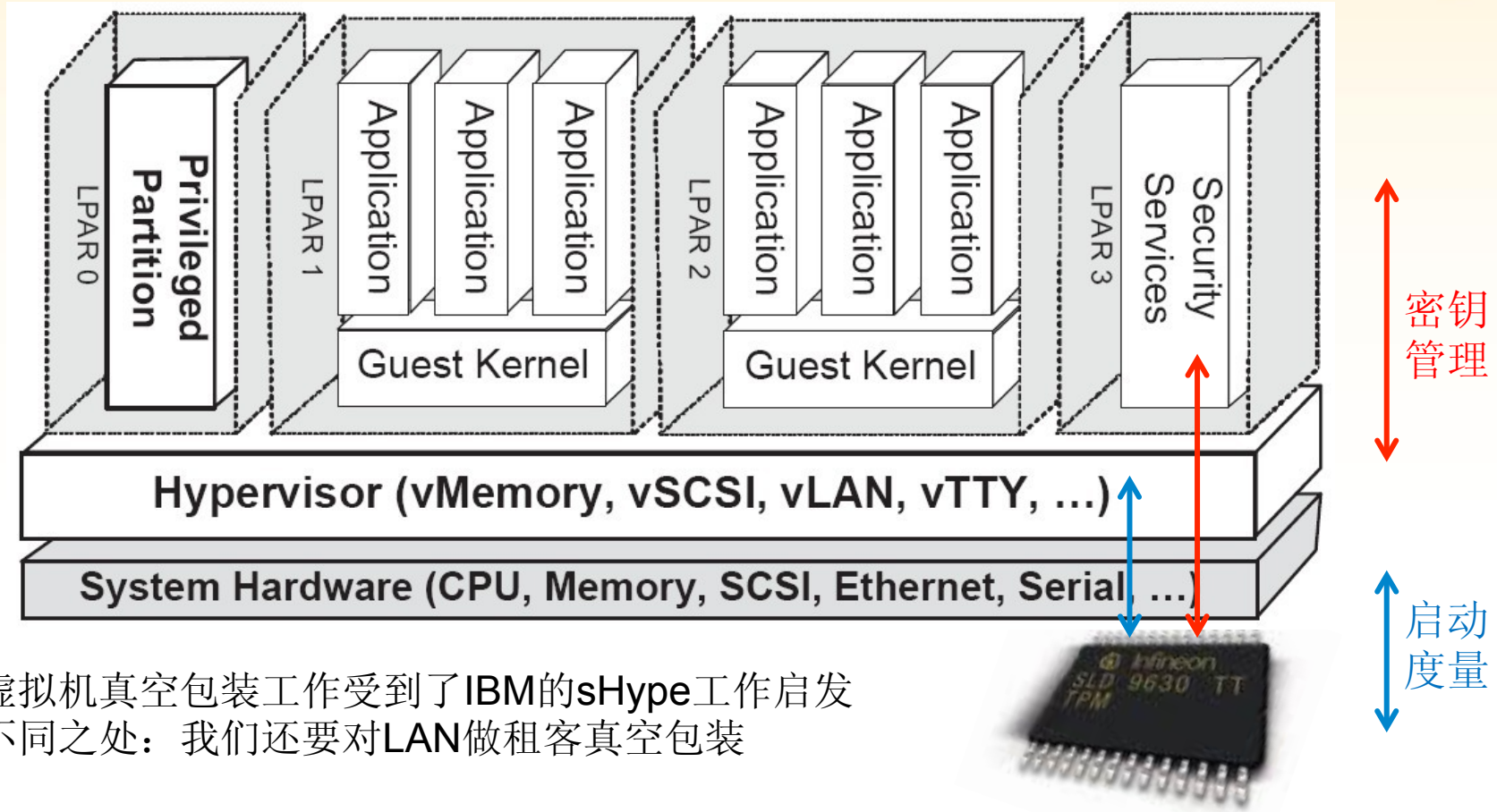
- OpenFlow, OpenvSwitch, VXLAN, NVGRE，以及OpenStack的Quantum项目等，都应用了细化VLAN的技术实现网络隔离：可以使用软件方法配置相互隔离的VLAN，实现租客/业务与租客/业务之间的隔离
- 主要在大规模可扩展自动部署管理层面解决VLAN存在的诸多重要问题：如4K-、L2-、甚至跨数据中心的互联，自动地址学习，等问题
- 技术手段：在IP包的元数据部分打上不同（虚拟子网属性）标记，配合交换器、路由器学习标记获得虚拟子网拓扑信息，让IP包按照不同标记走不同虚拟隧道，形成不同虚拟子网；可以想象用软件方法将许多网线不停地插拔到某些虚拟机上，让它们保持内部互通，并与外部虚拟机不通

如果使用此类SDN技术做租客之间的隔离（尤其考虑小租客，比如租用少于20个虚拟机的一类，大量长尾区小租客是使用公有云服务的主力军）：

- 考虑数据中心的负载均衡需求（此乃数据中心刚性需求！）：在如此小的VLAN内部根本毫无做负载均衡的空间，若在数据中心LAN的范围做负载均衡，每当VLAN越界不通时（即，插拔虚拟机网线造成不通时），需重新配置VLAN拓扑，让路由器、交换器重新学习新拓扑构造；代价太大了！
- 网络拓扑结构单一，不能跨越数据中心，不支持开放云的发展方向

结论：云安全所需的网络隔离仍然需要业界同仁努力创新

基于可信计算的虚拟机真空包装→LAN真空包装

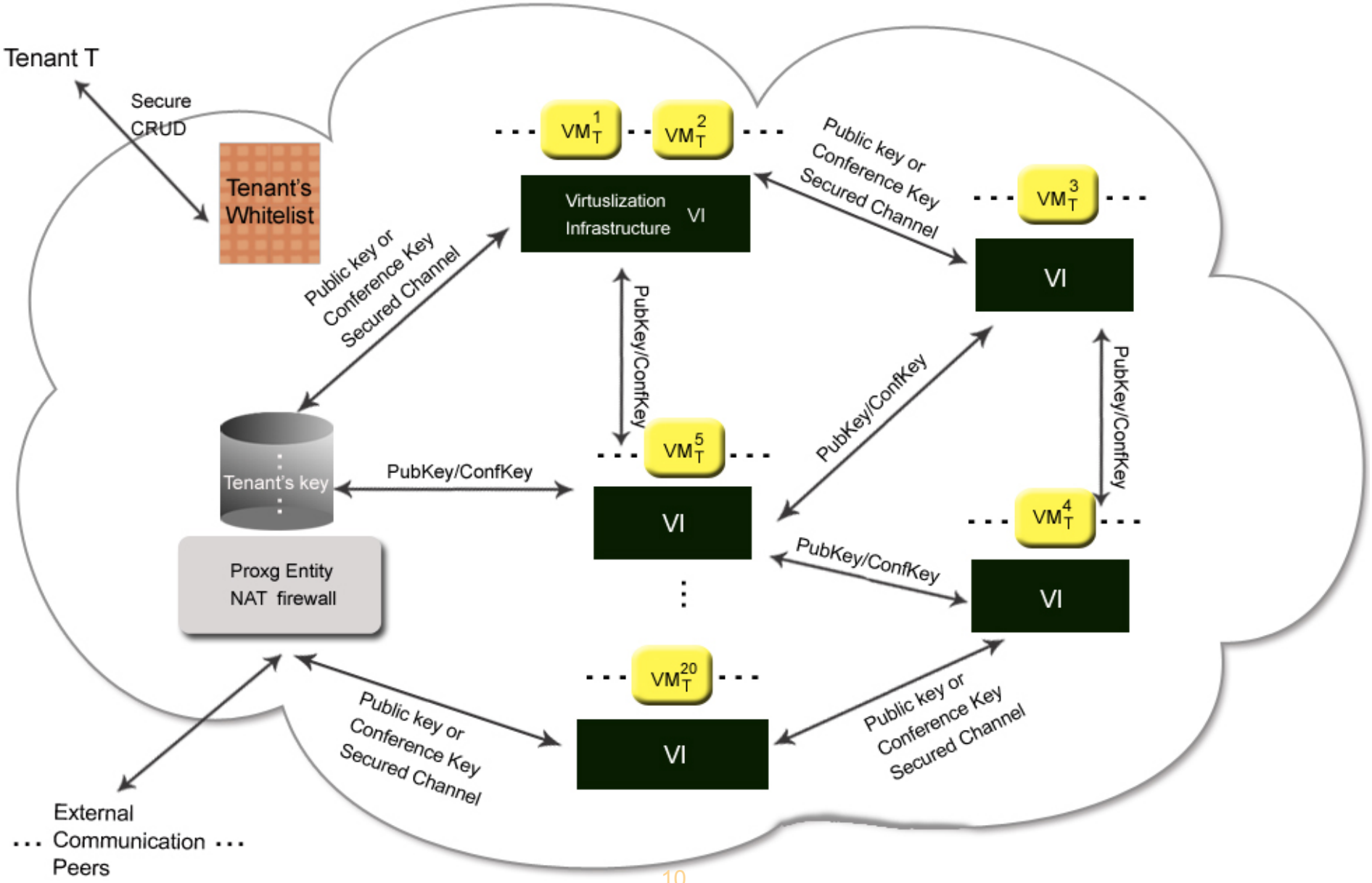


虚拟机真空包装工作受到了IBM的sHype工作启发
不同之处：我们还要对LAN做租客真空包装

IBM的sHype内核技术只管理本机，不跨越服务器，更无法跨越数据中心
云安全所需LAN真空包装不仅要跨越服务器，还要跨越数据中心，非密码学不行

关键技术：可信计算技术支持虚拟化架构上的IPsec，对IP包的payload做密码保护

由租客自助服务定义与管理的可信网络



租客自助可编程性（1）

- 每个虚拟机都有一个全球唯一的公钥证书，证书的crypto credential（即，私钥）由可信虚拟架构管理
- 所有虚拟机都按SDN方法形成互联，不会对负载均衡、瘦提供、动态迁移等造成任何不便
- 租客编制一张白名单：列出所租用虚拟机身份，以及外部通信伙伴身份（比如上页图中情况，一个小租客租用了20个虚拟机）
- 虚拟架构读取租客编制的白名单，对租客所租用虚拟机之间通信的IP包的payload数据做密码学服务：对发数据情况做加密服务，对收数据情况做解密服务
- 另有一个代理Proxy Entity（PE，可以是NAT, gateway, firewall）服务器也读取租客的白名单，为其中所列的租客外部通信伙伴做密码学代理服务，对向外流的数据包做解密服务，对向内流的数据包做加密服务
- 显然，虽然所有虚拟机在网络控制上都是互联的（就像Internet情况），然而在数据上只有那些在租客定义的白名单中的虚拟机及外部通信伙伴才互联
- 如此实现的网络隔离完全由租客自助定义、动态部署、按需管理，可以叫做虚拟私有LAN（Virtual Private LAN，PVL）
- 由于公钥证书的全球唯一分布性，此VPL的网络拓扑结构不必限于单个数据中心，具有向开放云数据中心发展的前景
- **密码处理增加开销： crypto + LAN latency < 1.5x LAN latency without crypto**

租客自助可编程性（2）

租客自定义的VPL白名单还可以含有VPL内部安全通信策略，比如实现组织内部业务隔离：

{vm1, vm3, …, vm19}：研发

{vm2, vm4, …, vm10}：销售

{vm12, vm14}：人力资源

{vm16, vm18}：财务

{vm20}：CXO 办公室

甚至实现更加细化的安全策略，比如Bell-LaPadula（BLP）多层安全策略：BLP-i 可以单向写数据至BLP-j，（i < j），反向不然：

{vm1, vm3, …, vm19}：研发：BLP-1

{vm2, vm4, …, vm10}：销售：BLP-0

{vm12, vm14}人力资源：BLP-0

{vm16, vm18}：财务：BLP-1

{vm20}：CXO 办公室：BLP-2

讨论：安全OS设计原理须与时俱进

史上留传下的OS都只管理本机硬件资源，以前本机资源有限，OS就只好与业务挤在一起，于是猎手（安全OS，如Linux中的SELinux模块）与狼也在一起。猎手与狼PK孰强孰弱，还真不好说！

现在不仅机器都连上了，还可以在一台机器内部做虚拟化分层，于是

- 连上了，浏览器就是OS，资源管理仅限于本机的老黄历要与时俱进：
  - 浏览器虽可跑在（无比弱智的）本机OS上，却可以与连上的机器交互，将强大的后端硬件资源呈现给用户管理与使用，所以云时代的OS不必再囿于管理本机硬件资源
- 虚拟化分层了，安全OS设计中猎手在狼窝里奋战也是老黄历，也要与时俱进：
  - 在同一硬件上还可以做虚拟化分层，让有的（比如业务处理）OS跑在低权限层，有的（比如安全管理）OS跑在高权限层，这样就可以保证位于低权限层的狼斗不过位于高权限层的猎手

注意：由于虚拟化架构的服务器分布性，跑在虚拟化架构层的安全软件天然不易遭受分布式拒绝服务攻击

虚拟机与VPL真空包装技术的设计遵循了与时俱进的OS新概念，成为一个有效的安全OS设计方法学

结论

如何提供可信多租赁云服务（如何让租客以按需自助服务方式在云数据中心里隔离出私有安全的计算、存储、通信环境）？

- 当前主要问题：如何对云数据中心里共享LAN资源进行隔离，这是云安全与通常网络安全最不一样的所在
- 当今公有云：信息安全是用户自己的事！
- 当今私有云：仍然处于IT作为资产的昂贵、不可自助服务、缺乏弹性、不支持按需租用、等状态，无视大量位于“长尾区域”的小租户们对使用安全云服务的期待
- 本报告的技术提出了对虚拟机与LAN做真空包装的新概念：在虚拟化架构层使用密码学方法对数据做保护
- 无需对网络的控制层元数据形成任何干扰，对数据中心的负载均衡及瘦提供要求不形成任何限制
- 对于租户、用户、骇客、业务OS、应用、等，屏蔽它们对于安全策略的可见性
- 用白名单方法实现了由租客自助服务方式定义与管理云中可信网络：Virtual Private LAN，格外适用于小租客使用云计算服务

理论升华：安全OS设计概念的与时俱进，提出了有效的虚拟化架构上安全OS设计方法学，不仅保护者强势于攻击者，而且分布式部署的安全软件天然不易遭受分布式拒绝服务攻击

谢谢

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012