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

可信云计算的基础设施与环境安全

演讲人姓名：赵 波

演讲人单位：武汉大学

RSA CONFERENCE CHINA 2012

汇报提纲

1. 发展与隐患
2. 国内外研究现状
3. 总体研究方案
   - ① VMM层安全研究
   - ② 云计算环境应用层安全研究
   - ③ 用户可感知的可信评估方案研究
4. 总结

1.1云计算发展及其趋势

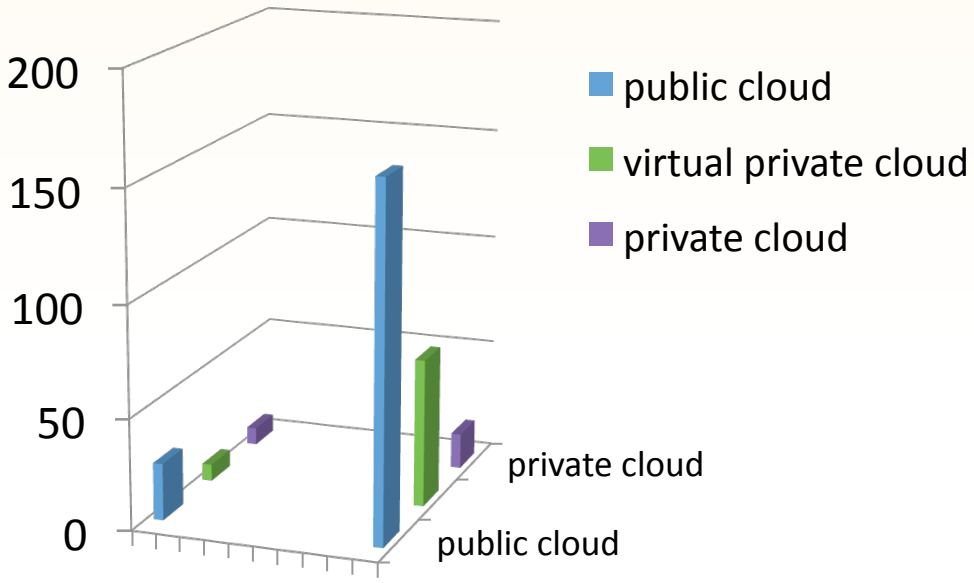
Lauren C. States | **@lauren_states**
VP & CTO, Cloud Computing & Growth Initiatives, IBM

Lauren is responsible at IBM for the technology strategy for the company's growth initiatives, including cloud computing, Smarter Planet, business analytics and emerging markets. Previously she was VP of Cloud Computing for the IBM Software Group. She is also a ***Top 100 Cloud Blogger****.*

1. **Cloud computing will allow everybody to be a service provider.** The infrastructure to do things is no longer a limiting factor. Focus will shift to application and business services.
2. **Employees will be able to use any device** to access, transact and manage their work.
3. **There will be a security breach in 2012** that will force organizations to rethink how they secure their data and applications.
4. **A new class of real time, personalized service providers will emerge** and they will develop partnerships to exploit the advantages of big data, social media and mobility.
5. **In Africa, the convergence of social, mobile and cloud will emerge** as critical tools for governments to deliver services and drive economic growth.

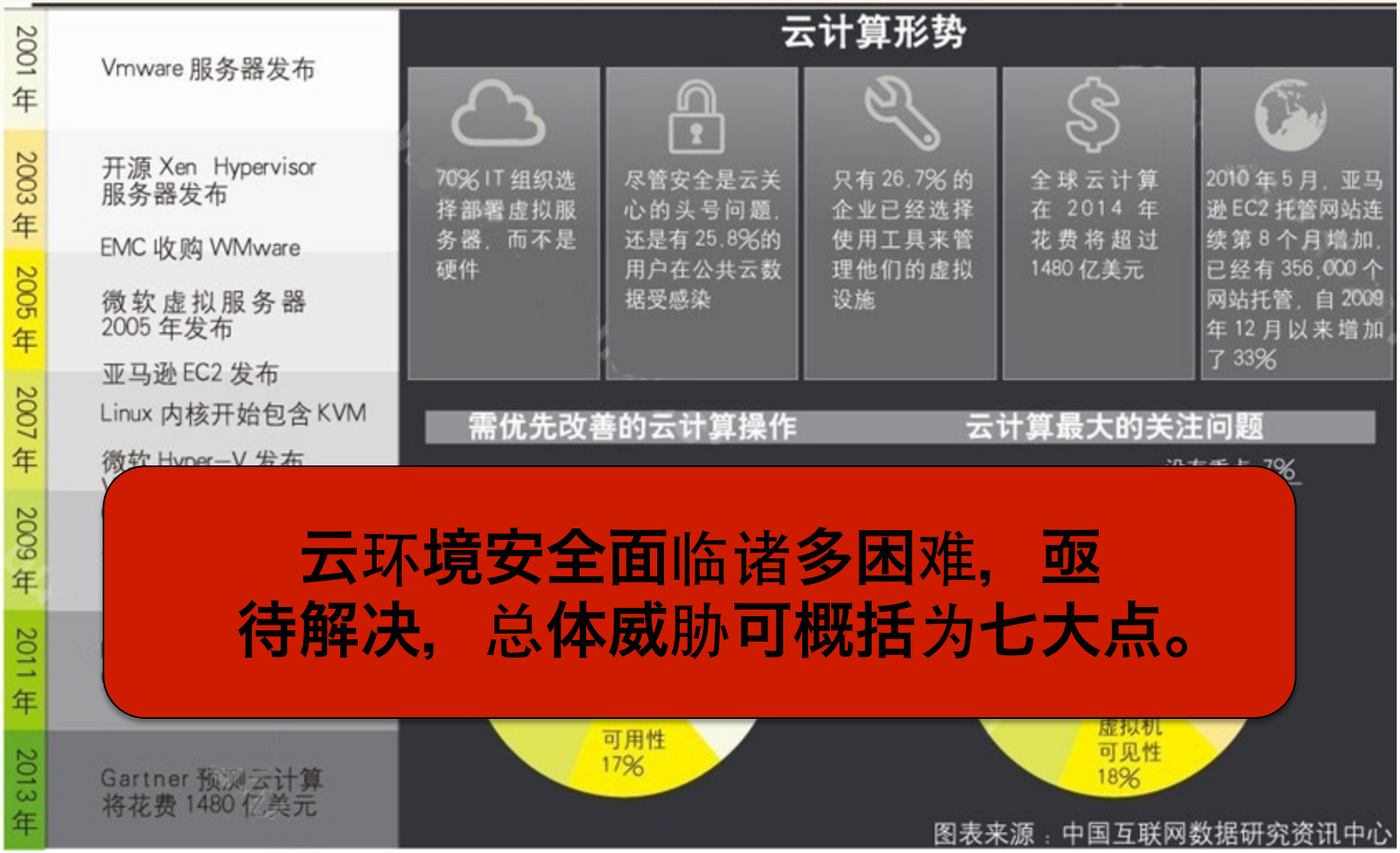
云计算作为新一代信息技术，需要促进其研发和应用。

1.1 云计算发展及其趋势



Gartner预测，在2011年全球IT支出增长幅度为5.6%，达到了3.6万亿美元，以此同比增长，预测2020年IT支出至少达到5.88万亿。云计算所占比重将从1.13%增至4.25%。截止2013年，80%的公司将在云服务方面投放7%~30%的预算。云计算增长迅速，发展空间进一步扩大。

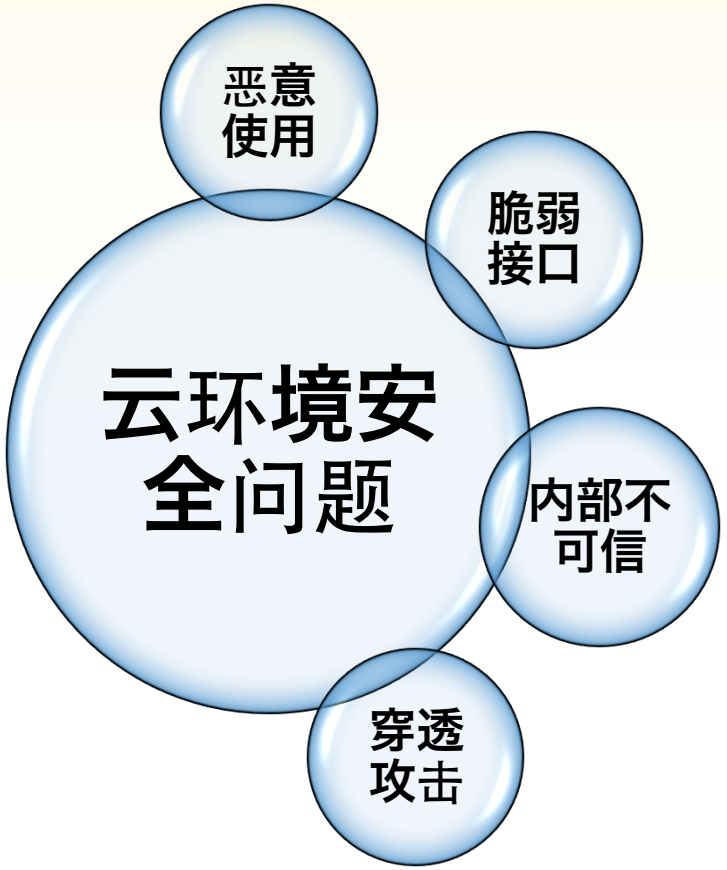
1.2 云计算关注问题汇总



云环境安全面临诸多困难，亟待解决，总体威胁可概括为七大点。

1.3 云计算环境安全威胁

云安全联盟（CSA）于2010年在旧金山举办的RSA会议上提出了以下安全问题：



大部分云端对用户行为限制较低，可运行各种程序，为恶意用户构建僵尸网络等提供了便利。

◆ 威胁2：存在安全风险的程序接口

为方便租户管理和交互云端服务，云服务商通常会提供一些相应的API，脆弱的API设计会影响到用户数据的私密性、可用性以及密码完整性。

3

云端的内部人员通常会被赋予较高的权限，通过使用管理软件，可以轻松地获取用户的私密数据，监控用户行为。

◆ 威胁4：虚拟机穿透攻击

运行在云端的虚拟机监控器存在安全漏洞，不法用户可利用这些安全漏洞获取更高的权限，进而影响到共享同一基础设施上的其他用户。

1.3 云计算环境安全威胁

云安全联盟（CSA）于2010年在旧金山举办的RSA会议上提出了以下安全问题：

◆ 威胁5： 数据丢失及泄漏

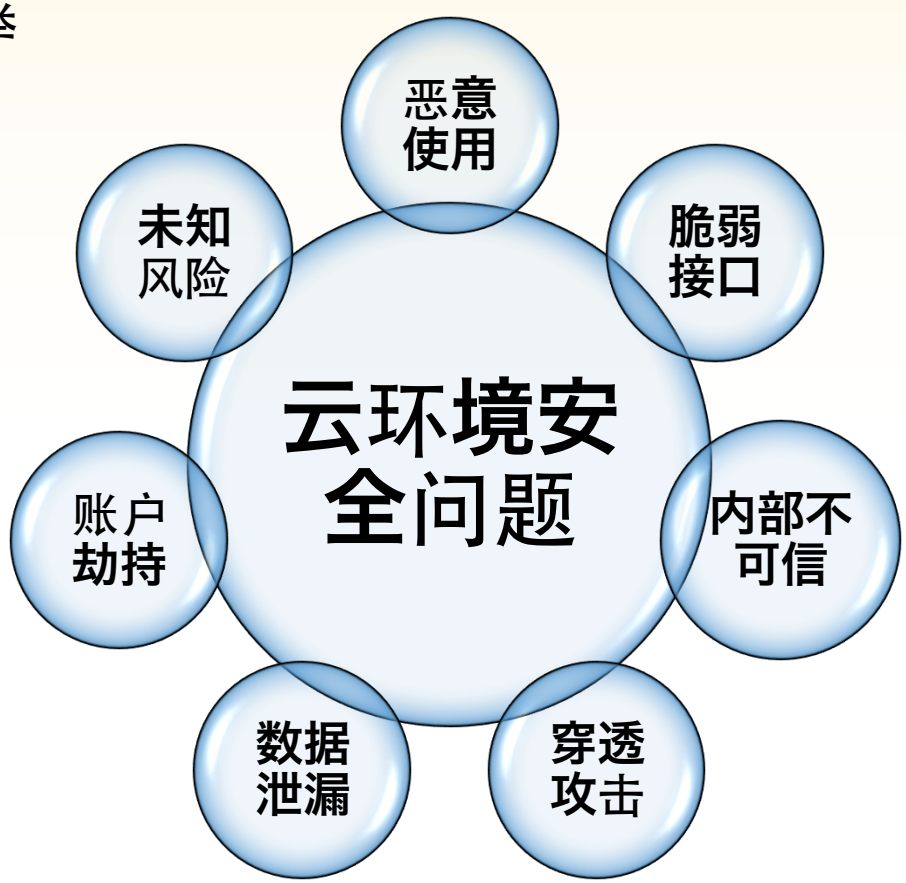
由于云端存在大量潜在的风险， 数据损坏威胁迅速增长。不完善的认证、授权及审计控制， 操作失效和数据中心可信任性问题。

◆ 威胁6：账户和服务劫持攻击

利用钓鱼、欺骗等手段， 以及潜在的软件漏洞， 攻击者可成功实现账户劫持， 篡改数据， 监听用户行为。

◆ 威胁7：未知风险问题

云端软硬件所属权及相关的维护等问题，一定程度上会引起未知的安全威胁。



1.3 云计算环境安全威胁

云环境安全保护

- 威胁1： 针对云计算的恶意使用
- 威胁2：存在安全风险的程序接口
- 威胁3：云端内部不可信
- 威胁4：虚拟机穿透攻击
- 威胁5： 数据丢失及泄漏
- 威胁6：账户和服务劫持攻击

→ 云计算环境基础设施架构安全问题严重

→ 云计算环境可信数据安全问题亟待解决

云环境用户可感知

- 云环境下的可信评估等

→ 用户可感知的可信评估方案研究势在必行

汇报提纲

1. 发展与隐患
2. **国内外研究现状**
3. 总体研究方案
   - ① VMM层安全研究
   - ② 云计算环境应用层安全研究
   - ③ 用户可感知的可信评估方案研究
4. 总结

2.1 云环境安全现状堪忧

安全挑战

随着云计算等新型计算模式的出现，虚拟化凭借其在隔离和自我测量方面具有的极大安全优势，得到了越来越广泛的应用。

然而在提高信息系统安全的同时，虚拟化技术本身面临着前所未有的安全挑战。

- **安全威胁**

目前已经有了相当对虚拟机展开攻击并获得了成功的事例，在Xen中发现77处安全漏洞，在VMware ESX中发现21处。

- **影响**

这些漏洞可以直接被利用于执行恶意程序，从而威胁整个虚拟环境和云环境的安全。产生这些安全漏洞的根本原因在于缺乏对云环境安全特性的理论分析及研究。此外，如何让用户感知云环境的可信，从而能够放心的使用各种云服务也是一个重大的问题。

这些问题将会对依赖虚拟机技术的云计算等目前国家正在大力倡导的科学新技术的推广应用带来威胁。云环境的安全性保护迫在眉睫，用户可感知的可信云环境的形成势在必行。

2.2 国内外研究现状概述

云环境安全问题的根源：

- 缺乏对虚拟机监控器的安全保护,缺少对云环境安全缺陷的形式化分析。
- 缺少有效的多维度软件隔离及数据保护手段。
- 缺少云环境整体可信性评估方案的理论研究与分析，导致用户无法感知云环境的可信性。

2.3 虚拟机监控器保护

使用基于硬件的技术来保护虚拟机监控器：为了克服TCG的链式信任缺陷，CPU厂商Intel、AMD分别提出了DRTM，支持系统在运行状态情况下的延迟加载度量。

确性，例如seL4形式化证明了8700行C代码实现的正确性，并证明了该实现过程与原规范的一致性。

保证虚拟机监控器完整性：HyperGuard和HyperCheck是两种提供了虚拟机监控器完整性测量的架构。

2.3 虚拟机监控器保护

现阶段

国外针对虚拟机监控器本身的保护已逐渐起步。其中最为典型的有HyperSafe和HyperSentry。

HyperSafe概述

HyperSafe能够赋予现有的“Type-I，裸机”虚拟机监控器特有的自我保护能力，从而保护整个生命周期的控制流完整性。目前已经有原型系统，并且在BitBisor和Xen上实验论证了其保护能力和低开销。

HyperSentry概述

通过引入度量代理对运行时的虚拟机监控器进行实时完整性度量。

HyperSentry优势

提供保证隐式的度量触发策略，使得虚拟机监控器在受到完整性度量时无法隐藏攻击路径，有效避免可擦除攻击干扰，具备上下文度量能力。

可行方案引入新问题

HyperSentry虚拟机监控器保护架构可能会引入新的攻击手段。

2.4 云环境下软件和数据安全保护

基于硬件虚拟化的监控技术不仅能够提供软件隔离，而且能够有效的防止内核攻击。现有
基于硬件虚拟化的监控技术不仅能够提供软件隔离，而且能够有效的防止内核攻击。现有
的基于硬件虚拟化的监控模型的
Lares

将整个应用软件从操作系统中隔离出来：这种方法一般
将整个应用软件从操作系统中隔离出来：这种方法一般是使用商用VMM为各个应用程序提供独立运行空间，保护粒度比较大，性能比较高

通过修改应用软件代码为敏感数据提供细粒度的隔
通过修改应用软件代码为敏感数据提供细粒度的隔离保护方案：这种保护方法一般需要修改应用程序
敏感数据提供细粒度的隔离保护方案：这种保护方法一般需要修改应用程序

2.4 云环境下软件和数据安全保护

现阶段

针对云环境软件和数据的隔离方法，国内外有许多相关的研究工作。国内较为著名的是Cherub模型。

Cherub模型概述

基于可信轻量虚拟机监控器的安全架构，由华中科技大学的邹德清教授等人提出，并在使用虚拟机监控器保护应用程序方面作出了突出贡献。

Cherub优势

该模型使用主流CPU的动态可信根和硬件虚拟化扩展，在系统运行时启动一个轻量虚拟机监控器（LVMM），并使用该LVMM作为其他安全应用的平台，提高了虚拟机系统的可管理性和安全性，并且具有较小的整体虚拟化开销。

Cherub硬件基础

Cherub 架构同操作系统无关，但要求处理器支持硬件虚拟化和动态可信根扩展指令。

2.5 用户可感知的可信评估方案

信任模型，为研究云计算环境服务可信性问题提供评价理论基础。

用户可感知的可信评估方案

云计算环境服务可信性综合判定方法研究：由于云环境服务的组合性与多样性，影响云计算环境服务的可信性，每种因素的可信性特征只能反映环境可信状态的一个部分，只有将多种的可信性因素综合起来，才能较为全面地反映云计算环境的实际可信状况。

高可生存性是云计算平台提供高质量服务的前提。

2.6 云环境安全仍存在诸多问题

完整性测量仍有问题

HIMA根据相应安全标准研制开发的专门用于安全保护系统的控制设备，具有完善的测试手段。此外，还有vTPM、SIM等技术，但是，大多代价较大，效果不佳。

国内研究成果

Cherub使用主
态可信根和硬
展，在系统运
个轻量虚拟机监控器，提高了虚拟机系统的可管理性和安全性，具有较小的整体虚拟化开销。但要求处理器支持硬件虚拟化和动态可信根扩展指令。

针对于云环境的安全保护力度有待加强，必须给予更多的关注和重视，从可信的角度找到合适的解决思路。

国外成熟研究方案

HyperSafe目前已经有原型系统，并且在BitBisor和Xen上实验论证了其保

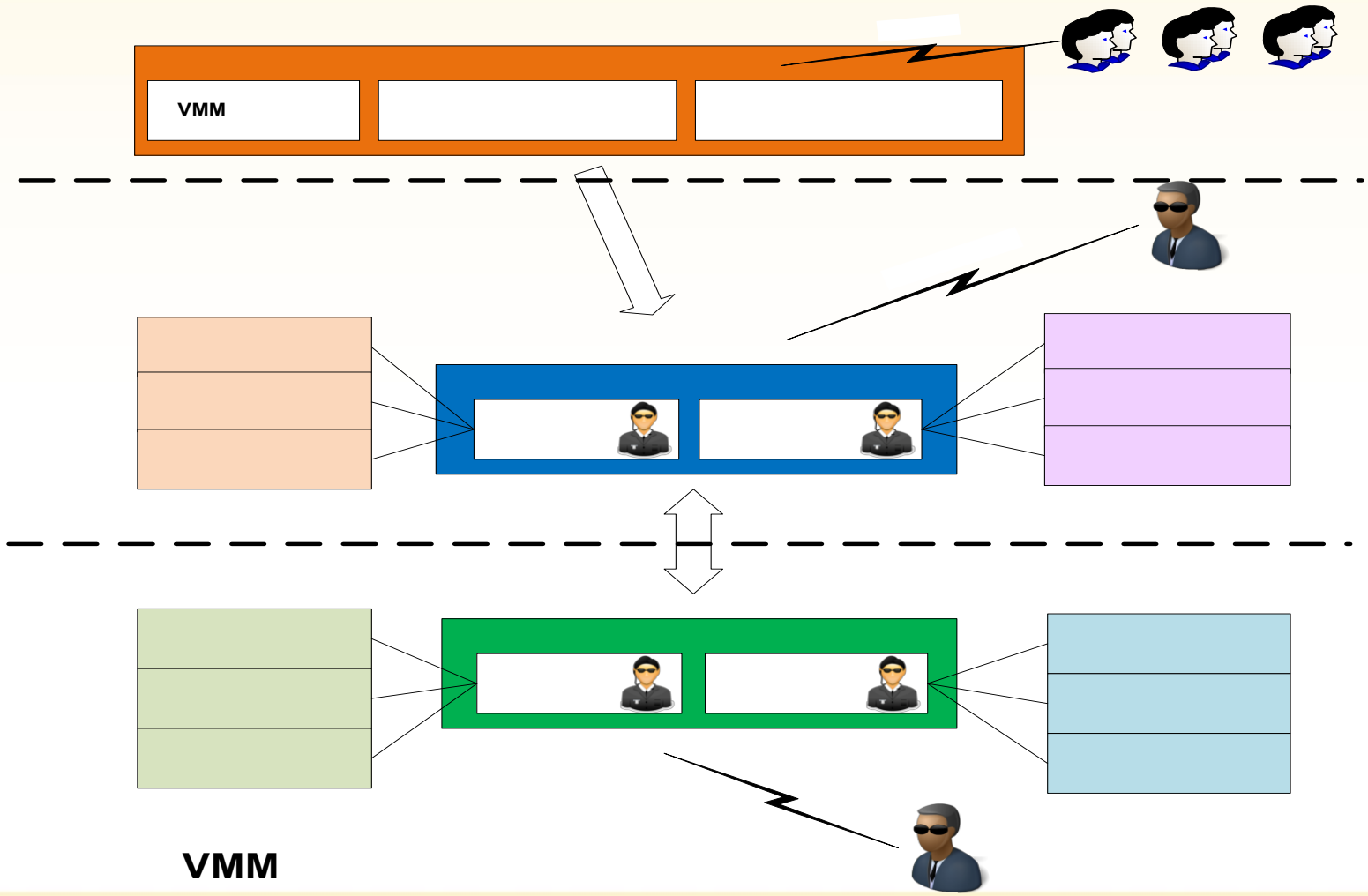
可行方案引入新问题

HyperSentry可以提供保证隐式的度量触发策略，且具备上下文度量能力。但可能引入新的攻击手段。

汇报提纲

1. 发展与隐患
2. 国内外研究现状
3. **总体研究方案**
   - ① VMM层安全研究
   - ② 云计算环境应用层安全研究
   - ③ 用户可感知的可信评估方案研究
4. 总结

3、 基础设施与环境安全的总体研究思路



汇报提纲

1. 发展与隐患
2. 国内外研究现状
3. 总体研究方案
   - ① **VMM层安全研究**
   - ② 云计算环境应用层安全研究
   - ③ 用户可感知的可信评估方案研究
4. 总结

3.1 VMM层

RSA CONFERENCE CHINA 2012

给出目标虚拟化环境的形式化描述

目标虚拟化系统的安全缺陷分析

虚拟机监控器安全性约束规则

保护虚拟化环境的安全的技术方法

从虚拟机监控器到虚拟机内部，提供了一整套虚拟化环境保护方法有效防止来自跨域或同域环境中的恶意软件攻击，确保云环境的隐私性和完整性。

3.1 VMM层--研究方法架构

从理论研究到技术实践

面向安全缺陷的VMM保护方法研究

虚拟机监控器安全初始化 → 虚拟机监控器动态完整性保护 → 虚拟机监控器的安全配置和逻辑设计

为虚拟化环境构建安全隔离的执行环境

VMM安全缺陷的理论分析

VMM的安全缺陷

多层次安全缺陷分析

虚拟化环境的形式化描述

目标虚拟化环境

相关资料

提出一套虚拟机监控器安全性约束规则

对形式化进行全面安全缺陷分析，找出虚拟化环境存在的安全缺陷

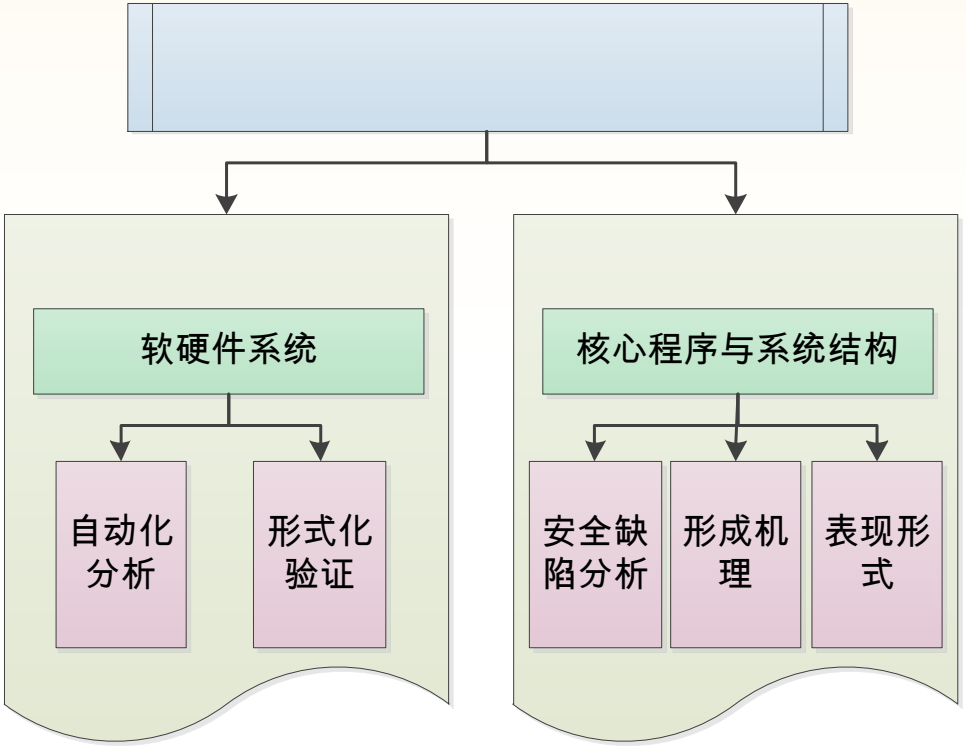
在抽象解释实例化的基础上对虚拟化环境进行形式化描述

以信息系统安全的理论和技术为基础支撑，基于抽象解释理论针对虚拟化环境构造抽象对象域

3.1 VMM层--虚拟化环境安全性缺陷的理论建模研究

RSA CONFERENCE CHINA 2012

问题描述：虚拟机自身安全性是目前亟需解决的信息安全问题之一，研究虚拟化环境的保护问题，首先需要找出其安全缺陷。



关键内容：

◆ 虚拟化环境的形式化描述

对大规模软、硬件系统进行自动化分析与形式化验证，在大型软、硬件系统的形式化验证研究中得到广泛应用。

◆ 多层次安全缺陷分析

从多个层次、多个角度对目标虚拟化环境的核心程序、系统结构进行全面安全缺陷进行分析，找出目标虚拟化环境存在的安全缺陷的形成机理和表现形式。

3.1 VMM层--虚拟化环境安全性缺陷的理论建模

要研究对虚拟化环境的安全性增强方法，首先需要从理论角度对虚拟化环境的安全缺陷进行建模。

针对虚拟化环境的未知缺陷，利用抽象解释给出正确设计静态分析的充分条件

根据被检测安全缺陷设计具体的抽象解释函数和抽象域

综合利用静态分析的主要方法即抽象解释的实例，构建虚拟化环境安全性缺陷模型。

- 类型推断
- 数据流分析
- 约束分析

- 虚拟化环境的形式化描述
- 多层次安全缺陷分析

3.1 VMM层--虚拟化环境安全性缺陷的理论建模

（1）虚拟化环境的形式化描述

基于抽象解释理论对程序的语义进行抽象

对程序的抽象语义再进行抽象

对目标虚拟化环境不同类型的缺陷进行分类

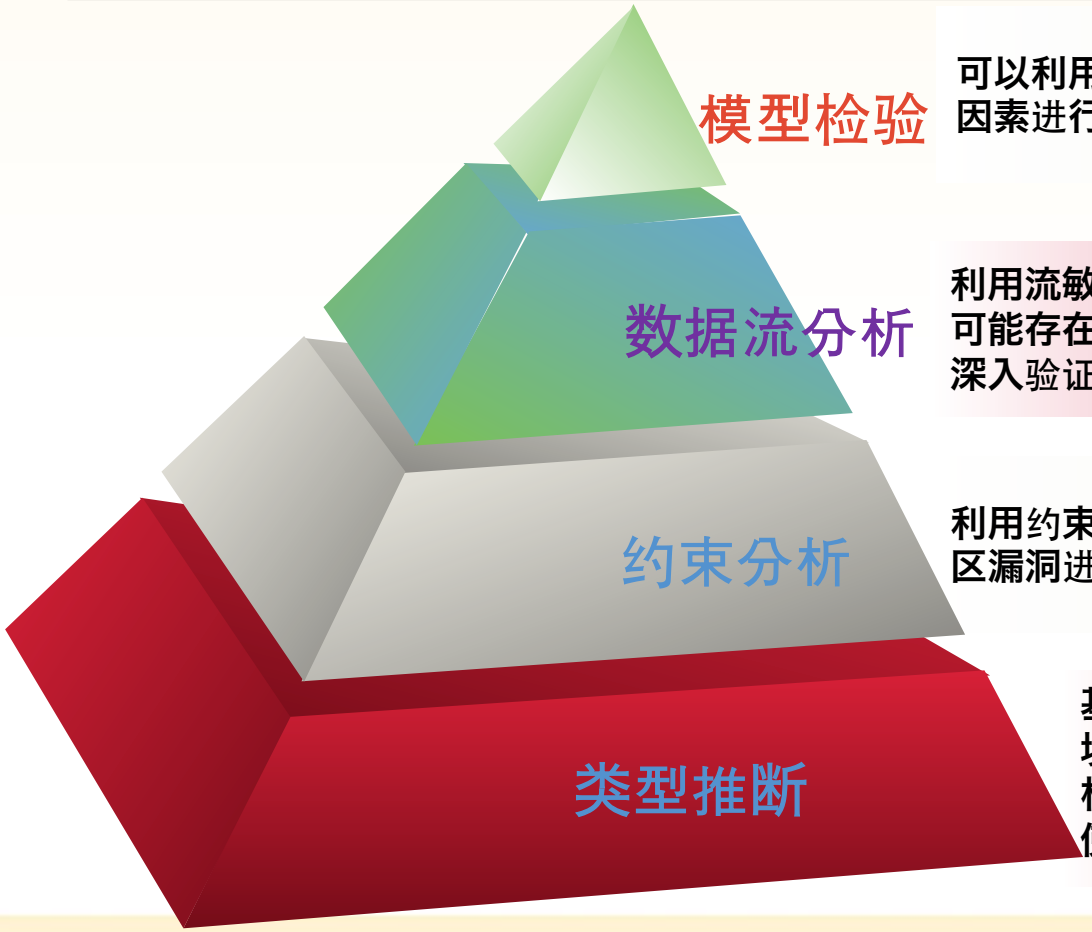
构造不同类型缺陷的抽象域基础上，构造适合的检测语言类

虚拟化系统的核心程序作为对象

3.1 VMM层--虚拟化环境安全性缺陷的理论建模

（2）多层次安全缺陷分析

对虚拟化环境的形式化描述与安全性分析，将得出目标虚拟化环境存在的安全缺陷，从而从理论层面为后续虚拟化环境保护方法的研究提供依据。



可以利用模型检验技术对目标操作系统隐含的不安全因素进行分析。

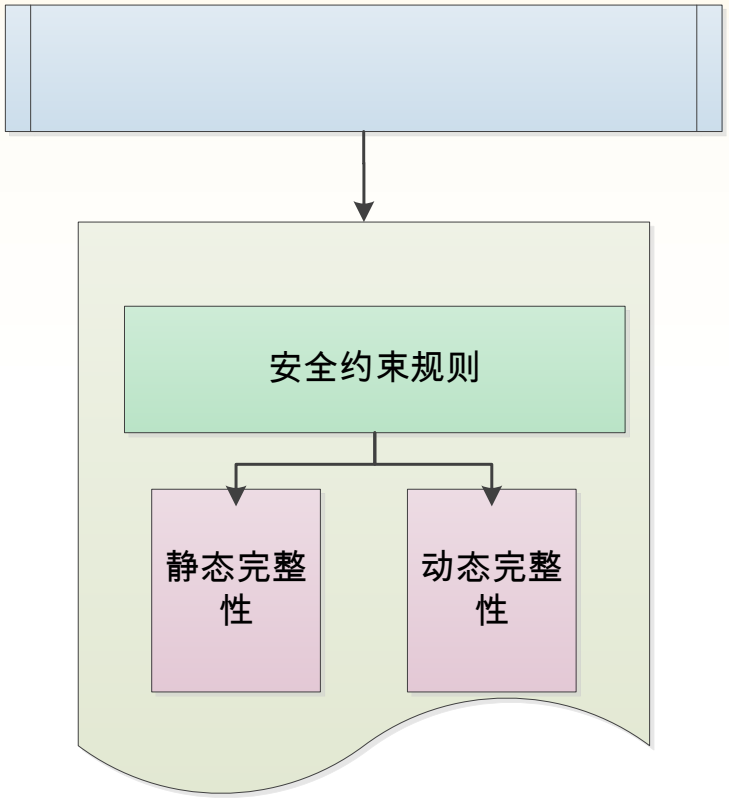
利用流敏感、上下文敏感等约束针对目标虚拟化环境中可能存在的数组越界漏洞，以及程序安全时态属性进行深入验证。

利用约束分析可以针对目标虚拟化环境可能存在的缓冲区漏洞进行深入发掘

基于类型推断的缺陷检测可以针对目标虚拟化环境格式化字符串漏洞、目标虚拟化环境内核中的权限检查，以及目标虚拟化环境中不安全的指针使等进行深入分析。

3.1 VMM层--虚拟化环境保护方法研究

问题描述：虚拟机安全性缺陷建模的研究从理论层面分析了现有虚拟化环境的主要安全缺陷，还需要从技术层面来保证虚拟化环境的安全。



关键研究内容：

◆ 虚拟机监控器保护方法研究

从可信计算和安全约束规则的角度研究虚拟机监控器的保护方法，确保虚拟机监控器在安全初始化状态下启动并且持续运行在未被篡改环境中，保证其静态与动态完整性。

3.1 VMM层--虚拟化环境保护方法研究方案

针对虚拟机监控器脆弱性发起的攻击，会影响运行于其上虚拟域的安全，只有保证虚拟机监控器的静态与动态完整性特征，才能保证整个虚拟化环境的安全。

- 分析虚拟机监控器的特点，为保护虚拟机监控器的安全提供指导
- 针对现有的以及可能遇到的安全威胁，从安全约束规则的角度研究虚拟机监控器的保护方法。
- 从静态、动态、设计的角度对虚拟机监控器进行保护，制定虚拟机监控器开发者和使用者都必须遵循的规则

静态
虚拟机监控器安全初始化规则研究，保证虚拟机监控器加载时的静态完整性。

动态
虚拟机监控器动态完整性保护规则研究。有效避免虚拟机逃逸攻击，保证虚拟机监控器的动态完整性。

设计
通过研究虚拟机监控器的脆弱性评估方法，抽象出虚拟机监控器的安全配置和逻辑设计。

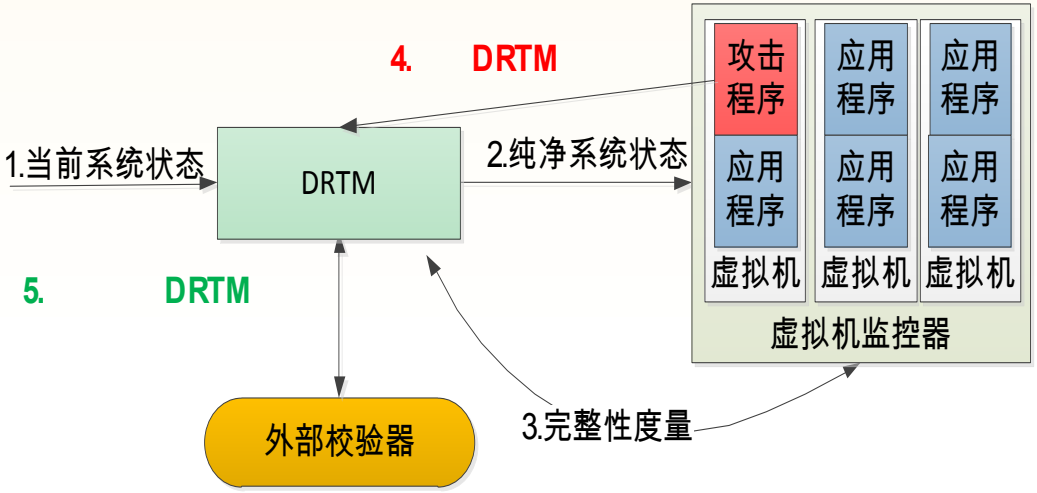
3.1 VMM层--虚拟化环境保护方法研究方案

（1） 虚拟机监控器安全初始化规则研究

RSA CONFERENCE CHINA 2012

技术方法：

- 通过创建DRTM来初始化虚拟机监控器。DRTM的成功创建可以保证虚拟机监控器初始化环境是安全的。
- 在新环境中执行的虚拟机监控器可能已遭受攻击
- 采用一种外部校验器以及与之进行安全通讯的机制，以此来确认DRTM是否被安全创建。



遵循规则：

DRTM机制允许外部校验器在新的执行环境中检测数据或代码存储区完整性。

TPM芯片、AMD和Intel使用可行的DRT机制来执行新环境的完整性度量，对虚拟机监控器初始化完整性保护规则研究提供了基础。

技术实践： 虚拟化环境保护方法研究方案

（2） 虚拟机监控器动态完整性保护规则研究

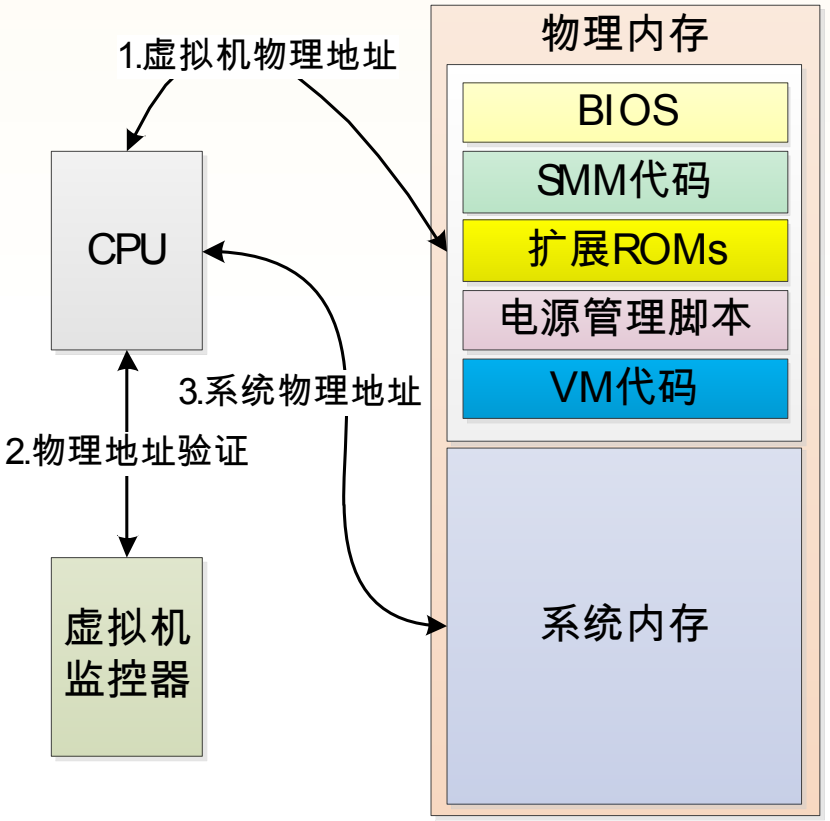
研究基于硬件虚拟化机制的虚拟机监控器运行时保护规则，可以有效避免虚拟机逃逸攻击，保证虚拟机监控器的动态完整性。

技术方法：

- 通过对虚拟机监控器进行完整性保护，可以使得其上层的虚拟机运行任何操作系统及其应用，这样的操作系统可以禁用虚拟内存。
- 通过数据结构来映射和访问虚拟机监控器内存区域，从而直接访问系统物理内存
- 在完整性保护的虚拟机监控器到达内存控制器前，它必须验证来自于虚拟机的物理地址

遵循规则：

一个完整性保护的虚拟机监控器必须在最高特权级执行其内核程序，且使用物理存储虚拟化机制来阻止虚拟机中代码访问其内存区。



3.1 VMM层--虚拟化环境保护方法研究方案

（3） 虚拟机监控器的安全配置和逻辑设计研究

通过研究虚拟机监控器的脆弱性评估方法，抽象出完整性保护的虚拟机监控器的安全配置和逻辑设计理念。

虚拟机监控器的安全配置和逻辑设计研究

- 依据虚拟机监控器的设计，需要根据客户环境来配置运行期间的虚拟机监控器。
- 以支持虚拟机间通讯和虚拟机监控器的客户运行接口（虚拟化设备的驱动加速器），能够直接访问虚拟机监控器数据。
- 一个完整性保护的虚拟机监控器必须保证这些配置和运行时的接口改动尽可能的小。
- 设计者也必须确认虚拟机监控器的内核操作逻辑尽可能简单，在一定限制内的虚拟机监控器代码基能执行手动和分析性审计，用以克服其脆弱性。

虚拟机监控器的安全配置和逻辑设计需要遵循的规则

完整性保护的虚拟机监控器代码必须无脆弱性。

3.1 VMM层--具体的实现思路

安全缺陷分析技术

不同的安全缺陷分析技术的侧重点不同，必须对比各种分析技术的特点，找到每种方法的适应性，才能分析复杂的虚拟化环境，并且从中找出安全缺陷。

虚拟机监控器安全约束规则抽取技术

必须针对其完整性保护制定必要的规则，根据虚拟机监控器的行为抽取出相应的安全约束规则，是保证其行为规范化的前提。

域间安全管理模块的构建技术

域间安全管理模块为域间的信息交互提供安全策略并进行仲裁，该模块的构建技术直接决定了虚拟机域间隔离的强度。

虚拟机内核实时监控技术

通过动态监控虚拟机内核的运行状态，能够有效防止高特权级的恶意进程入侵虚拟机内核，破坏受保护对象的运行环境。

虚拟机监控器内软件保护代理的设计与实现

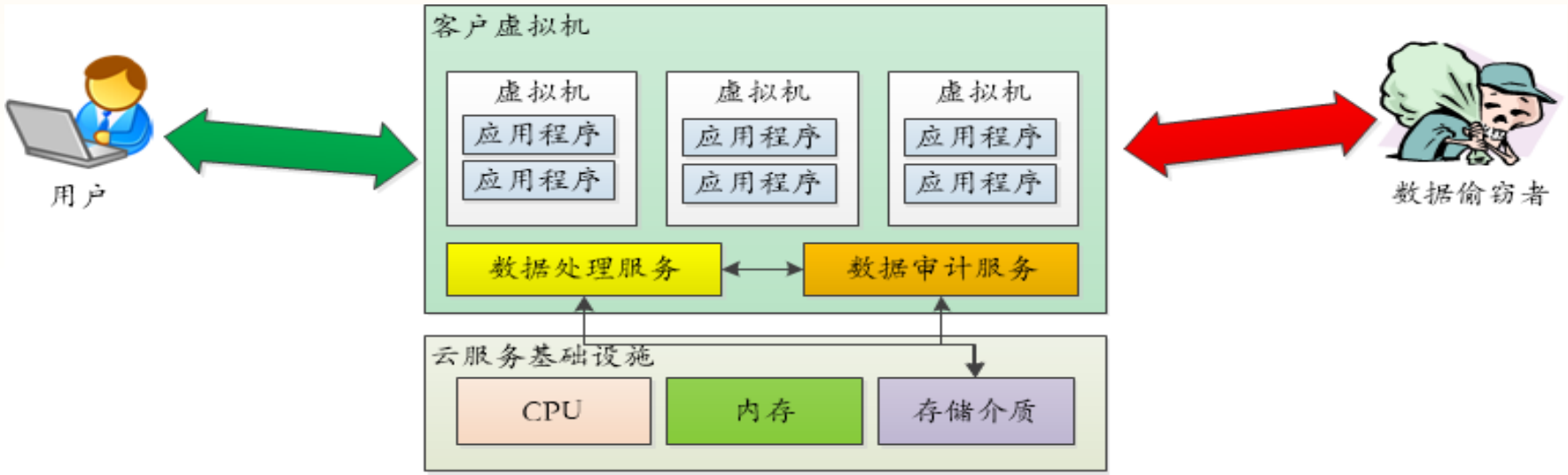
通过在虚拟机监控器内引入软件保护代理，能够实现服务与接口的分离，从而提供高效的数据完整性校验以及远程证明等安全服务。

汇报提纲

1. 发展与隐患
2. 国内外研究现状
3. 总体研究方案
   - ① VMM层安全研究
   - ② **云计算环境应用层安全研究**
   - ③ 用户可感知的可信评估方案研究
4. 总结

3.2云计算环境应用层安全研究

如何保证虚拟域内软件和数据的可信，是可信计算应用到云计算中的一个关键问题。



用户对软件和数据的安全性需求涵盖了软件运行和数据处理的全生命周期，涉及到创建、存储、使用、归档、销毁各个阶段，在不同生命周期，所面临的可信环境不同，所面临的安全风险也不同，只有在整个生命周期里能对用户软件和数据提供可靠的安全防护，才能完全保证软件和数据的安全。

对全生命周期进行保护尚存在诸多问题，因此，应着重考虑针对生命周期内的两个重要阶段-----存储和运行状态进行保护，以达到应用可信的目的。

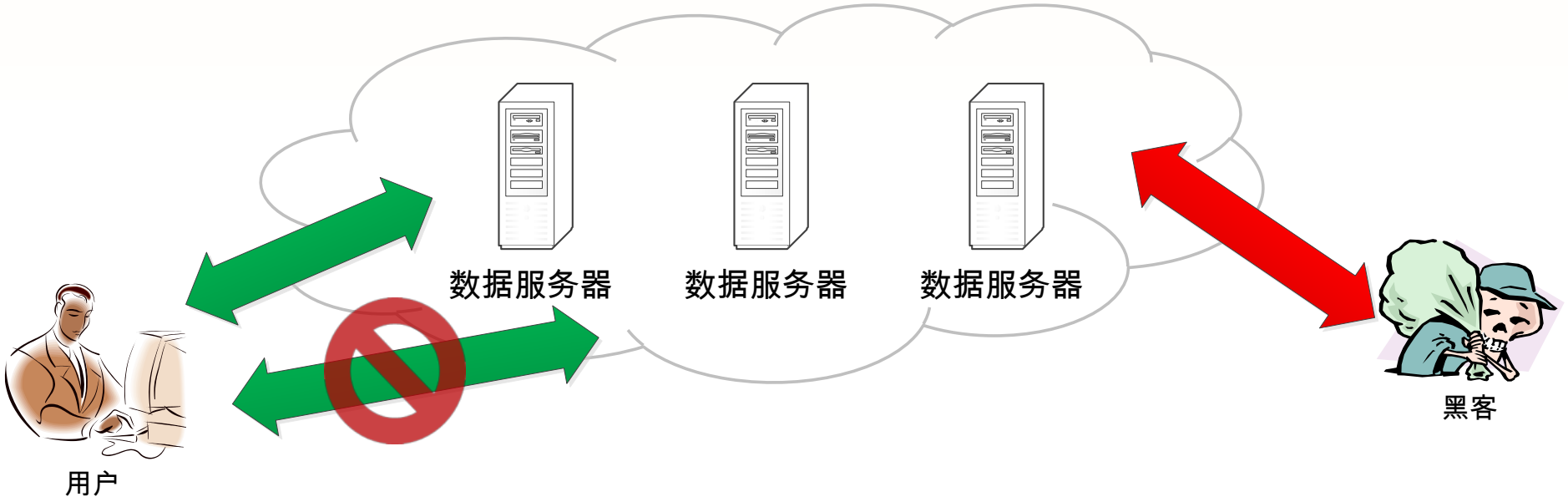
3.2云计算环境应用层安全研究

RSA CONFERENCE CHINA 2012

（1）软件和数据的存储安全

软件和数据在云端的安全可信问题是可信云计算的一个关键问题，也是云计算推广与应用过程中用户最为关注的问题。

用户难以对云计算的安全性产生信任的根本原因在于用户丧失了对自身软件和数据的可感知性与可控性，外包了数据就等于外包了控制权。



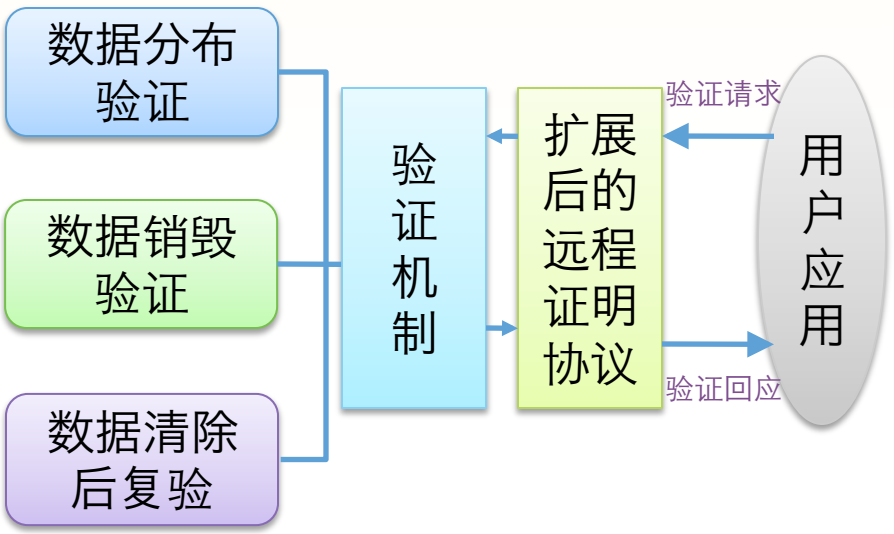
3.2云计算环境应用层安全研究

（1）软件和数据的存储安全

1，安全存储：
在存储方面设计保护隐私的数据映射模型，消除数据的内在关联性，防止信息泄露。

关键研究内容：

- 消除数据的内在关联性，防止信息泄露。
- 利用可信计算技术对数据来源进行辅助标识，增强数据来源定位的准确性。
- 增加数据销毁验证，通过计时分析将到期数据在磁盘、内存中彻底清除。
- 进行数据清除后的复验，满足数据全生命周期安全验证。



3.2云计算环境应用层安全研究

（2）软件和数据的运行安全

从资源隔离的角度构建目标软件的多维多粒度隔离环境，保证高安全需求软件的运行时环境安全，有效防止来自跨域或同域环境中的恶意软件攻击，确保软件的隐私性和完整性。

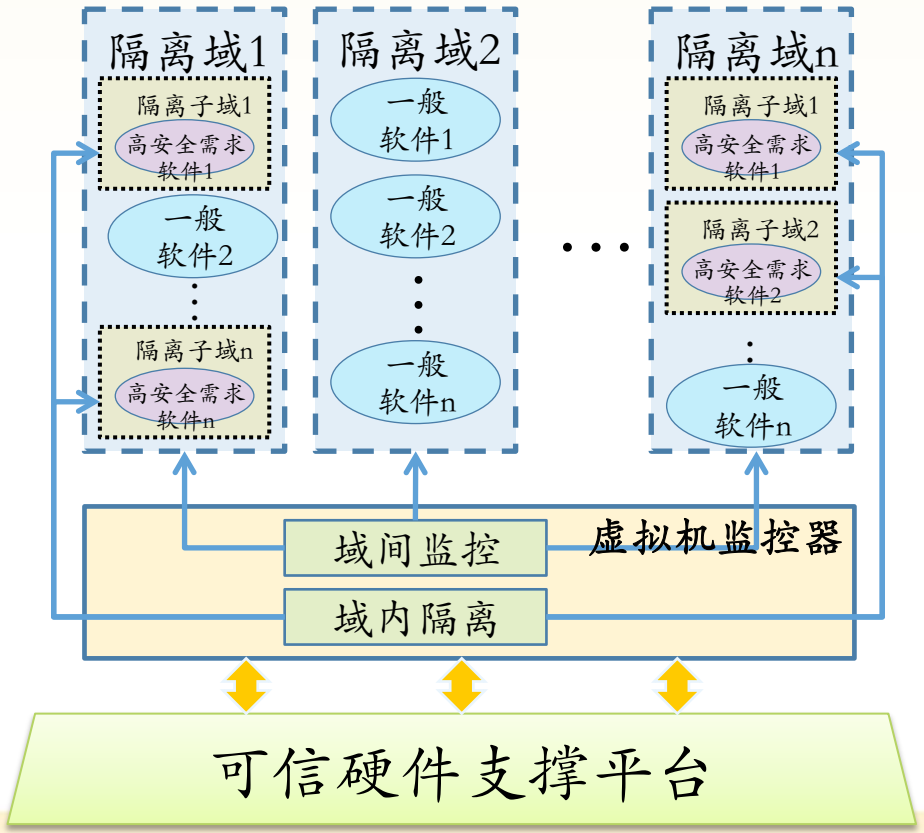
技术方法：

- 建立一种双重多维隔离机制，为多个虚拟域提供带有访问控制功能的强隔离。
- 在目标隔离域中进一步建立隔离子域，为虚拟域内软件提供细粒度的隔离保护。
- 从受保护对象的生命周期角度出发，支持动态隔离策略，最大限度减小虚拟机监控器的负担和系统运行时的开销。

隔离模型包括：

域间高安全需求软件隔离方法

域内高安全需求软件隔离方法

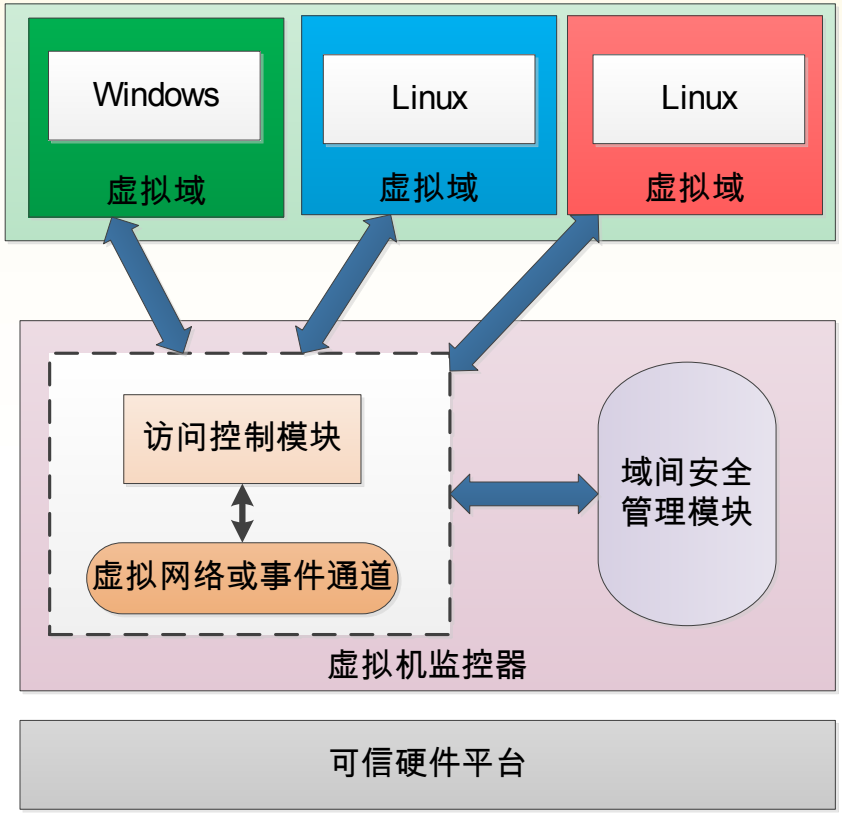


3.2云计算环境应用层安全研究

（2）软件和数据的运行安全-软件域间隔离

技术方法：

- 在虚拟域间数据通信的关键路径上添加访问控制模块。
- 在虚拟机监控器内添加一个域间安全管理模块，提供安全策略及其仲裁等相应的安全服务。
- 在虚拟域创建时，域间安全管理模块收集其安全属性并记录。
- 访问控制模块在虚拟域软件通信时提取相关的安全属性，然后从域间安全管理模块中提取出相应的安全策略进行仲裁。
- 根据仲裁的结果进行访问控制，阻止敏感信息的非法扩散。



基于硬件虚拟化技术的虚拟机监控器为各个虚拟域提供独立运行空间，并通过对虚拟机间软件通信行为进行约束以增强隔离力度

3.2云计算环境应用层安全研究

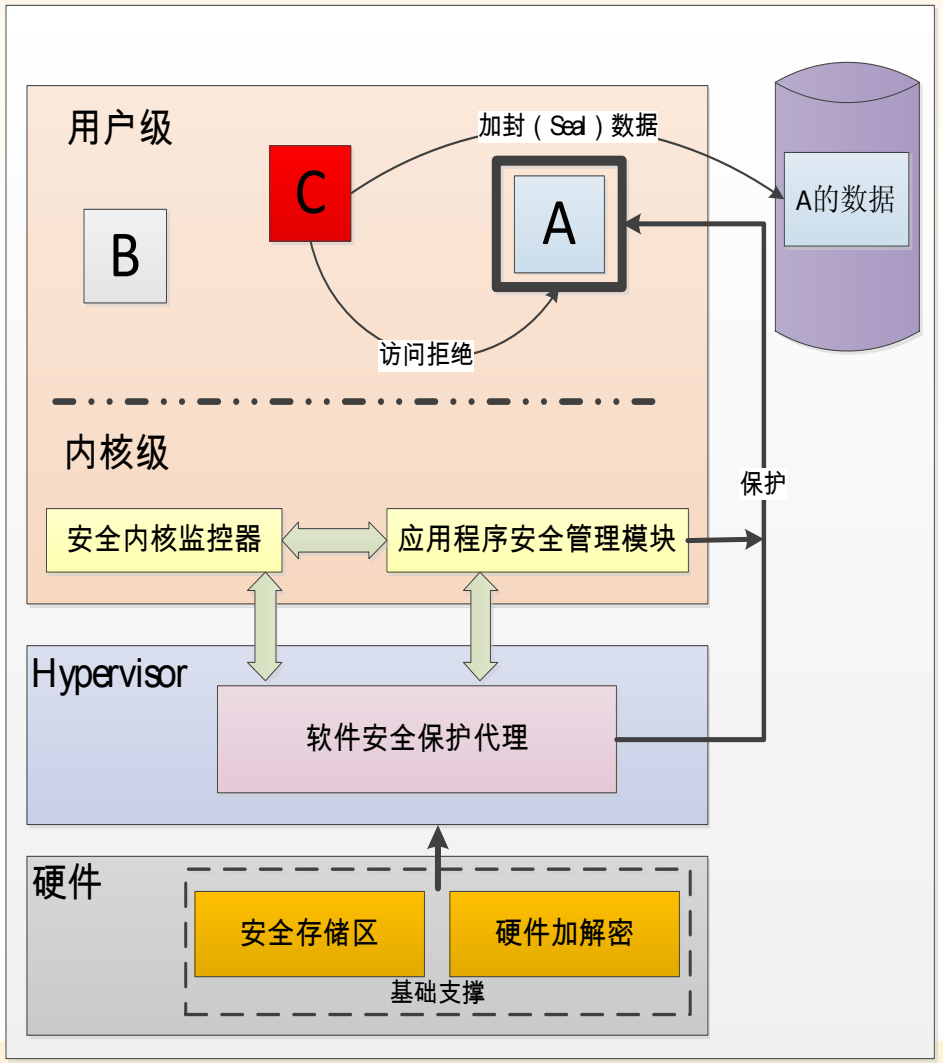
（2）软件和数据的运行安全-软件域内隔离

RSA CONFERENCE CHINA 2012

针对本地存储敏感数据面临的安全威胁
参考vTPM的设计思想，通过位于虚拟机监控器中的软件保护代理(SSPA)以及位于虚拟机内核层的应用程序安全管理模块(ASMM)对虚拟机内敏感数据进行封装、完整性校验以及远程证明。

针对虚拟机内软件运行空间的安全问题
用应用层软件隔离结合内核运行环境监控的方案来进行保护。

- 位于受保护虚拟机监控器中的SSPA，对各个受保护对象的内存进行隔离和保护。
- 安全内核监控器(SIM)可以有效阻止恶意进程针对内核运行环境的攻击，其本身受SSPA的保护。



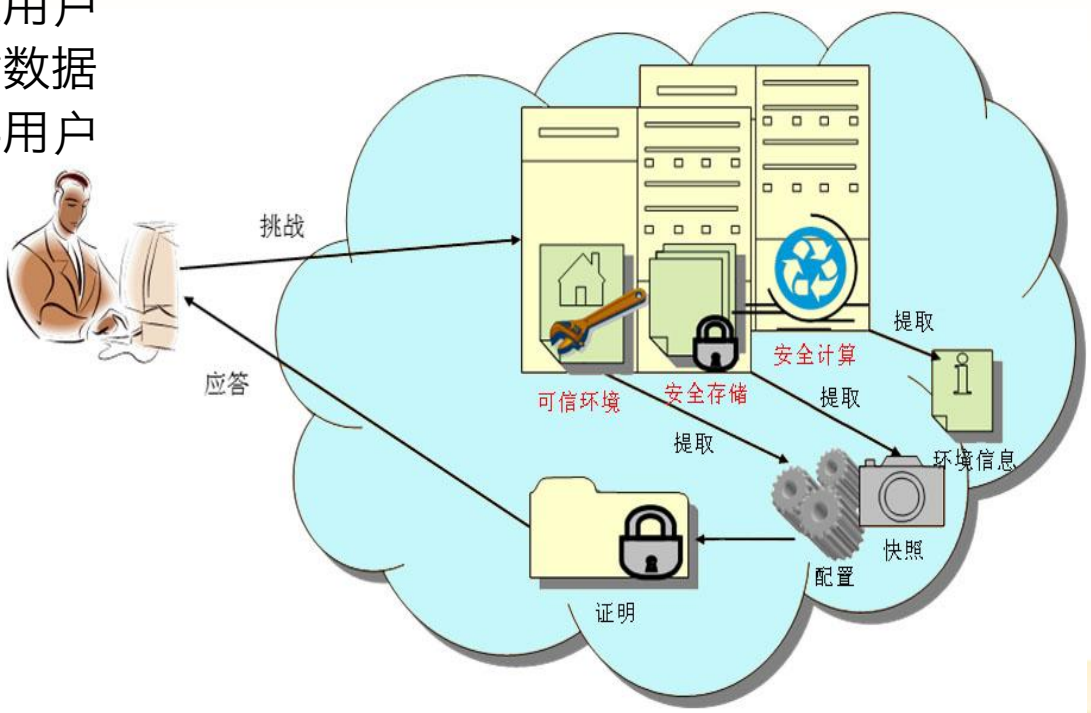
3.2云计算环境应用层安全研究

（2）软件和数据的运行安全-数据安全

RSA CONFERENCE CHINA 2012

数据运行态的安全：
从数据创建，修改、分配到删除整个过程对数据进行保护。

关键研究内容：
以增强用户对云环境安全性的可感知性与可验证性为前提，围绕用户数据处理的整个生命周期，针对数据安全处理环节进行安全性增强与用户反馈。



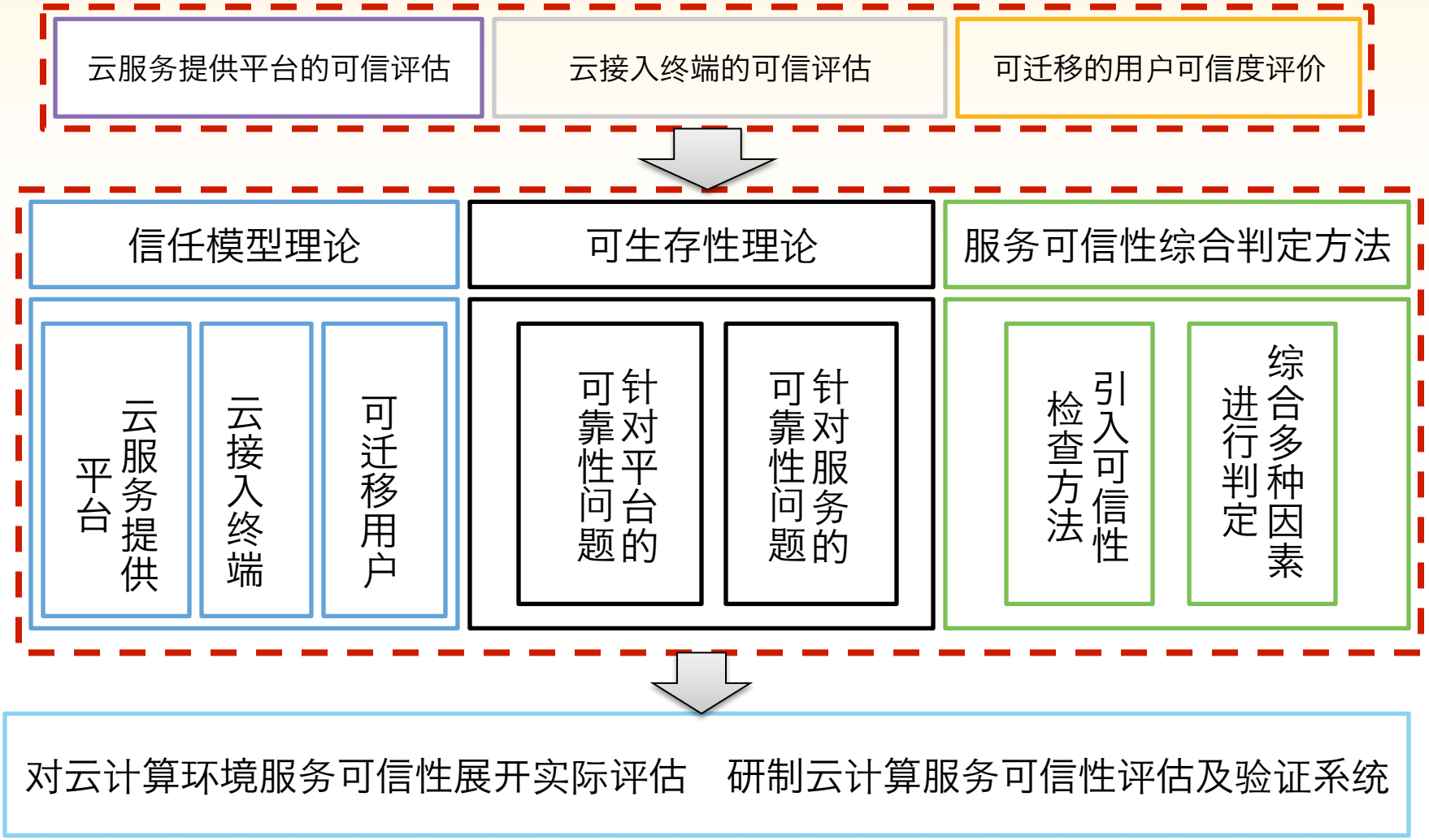
汇报提纲

1. 发展与隐患
2. 国内外研究现状
3. 总体研究方案
   - ① VMM层安全研究
   - ② 云计算环境应用层安全研究
   - ③ **用户可感知的可信评估方案研究**
4. 总结

3.3 用户可感知的可信评估

- 如果云环境的安全可信是可证明的，云环境安全就能被感知
- 用户可感知问题可以转换为云环境可信性评估问题
- 针对云计算的三种典型服务模式（IaaS，PaaS 和SaaS），综合考虑云计算环境中服务可信性的各类信任评估需求
- 从云服务提供平台的可信评估、云接入终端的可信评估，以及可迁移的用户可信度评价管理机制，形成一个多层次综合的可信评估及验证系统

3.3 用户可感知的可信评估



3.3 用户可感知的可信评估

（1）信任模型

研究云计算内部组件间的信任关系

研究服务提供平台对接入终端的信任关系

研究接入终端对云服务提供平台的信任关系

研究可迁移用户对云服务提供平台的信任关系

分析和研究云计算环境中多层次信任关系

构建面向云服务的信任模型

- 形式化描述
- 抽取云环境中安全属的共性与特性
- 研究云环境安全属性的内在关联性
- 借助经典证据理论进行研究

3.3 用户可感知的可信评估

（2）平台可生存性策略

云计算平台由于资源高度集中，比其它计算模式更容易遭受各种形式的攻击，因此云计算平台的高可生存性是其提供高质量服务的前提。

云计算平台可生存性策略研究

针对云服务提供平台的生命周期，研究云服务提供平台生命周期内的可生存性策略，对其同一生命周期内不同时期的平台动作行为进行约束。

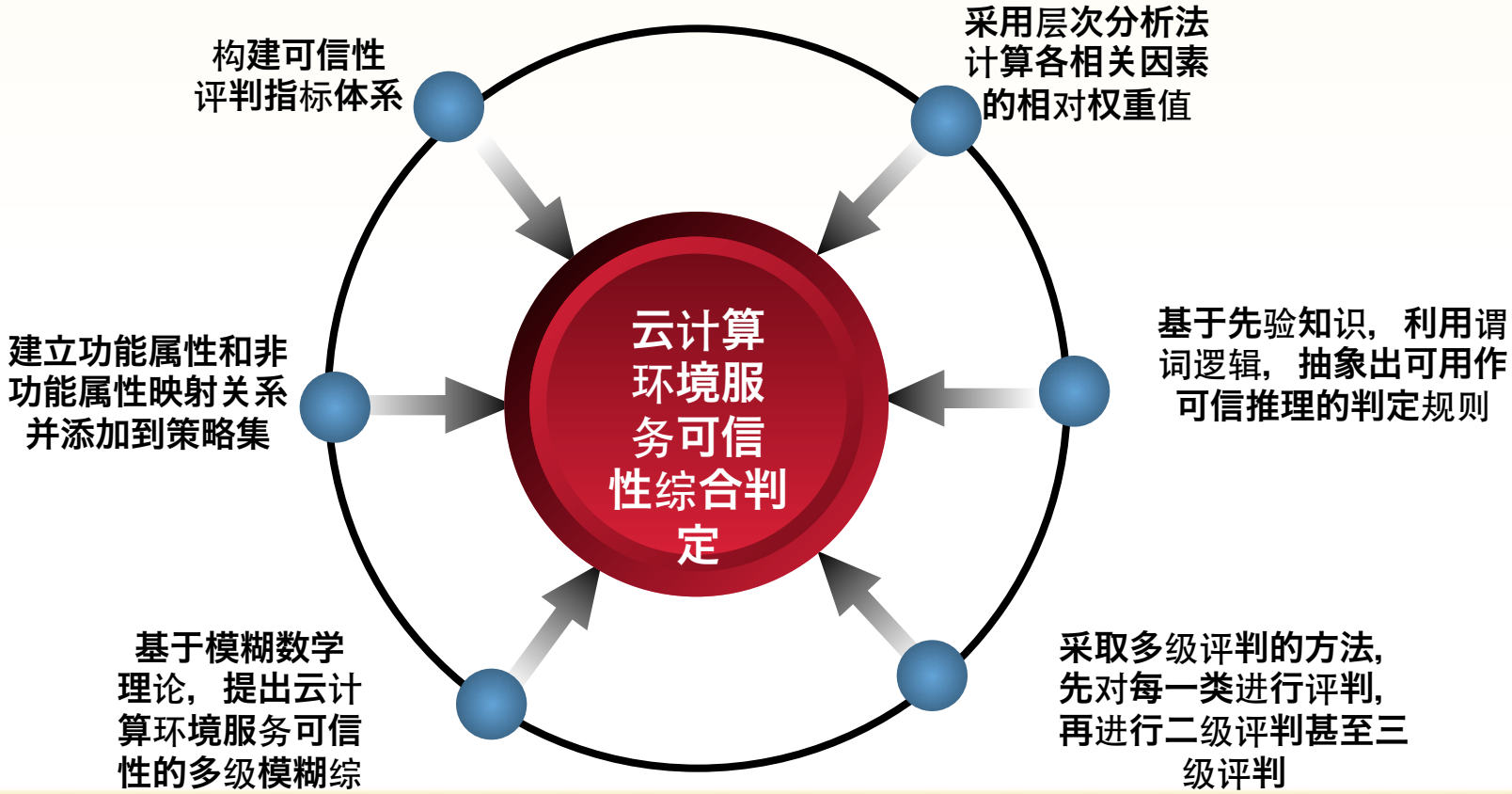
针对云计算环境中多接入终端且接入终端差异化较大的特点。研究其在异构环境下的服务可信性保障策略，据此制定云接入终端的接入约束准则。

针对可迁移用户的复杂性以及对平台的依赖性，研究制定迁移策略，对用户迁移行为准则进行约束。

3.3 用户可感知的可信评估

（3）服务可信性综合判定

已有的研究大都针对某种可信性因素，使用特定的可信性检查方法，但是这些可信性检查方法往往是孤立的，这样的结论存在片面性，不能完全准确反应云计算环境的真实可信状态。



3.3 用户可感知的可信评估

（4）服务可信性评估验证系统

建立云计算服务可信性评估及验证系统

- ◆基于前述的理论研究
- ◆针对云计算环境服务可信性展开实际评估
- ◆通过实验论证的方式

利用面向云计算环境服务可信性评估需求的建模方法，建立可信性因素集，确定影响云环境服务可信性的相关因素及影响因子

利用系统独立组件的评估结果，根据云环境功能性与非功能性属性之间的关联关系，构建可信性判断集，建立综合评判的证据集

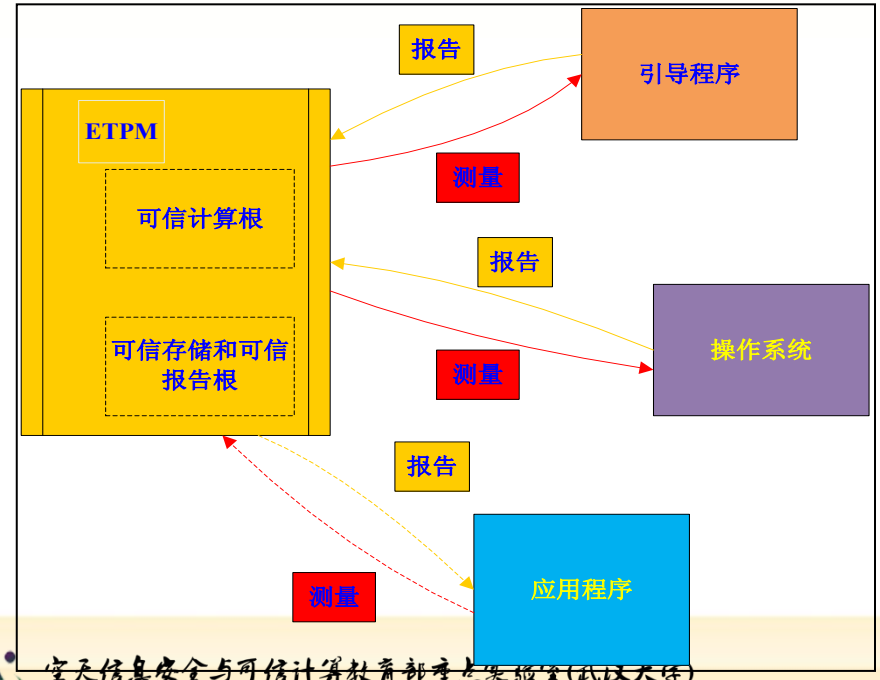
利用多级模糊评判和层次分析法，确定各评判因子的权重关系，给出综合评判模型，并进行数值分析，得到综合性判定结果

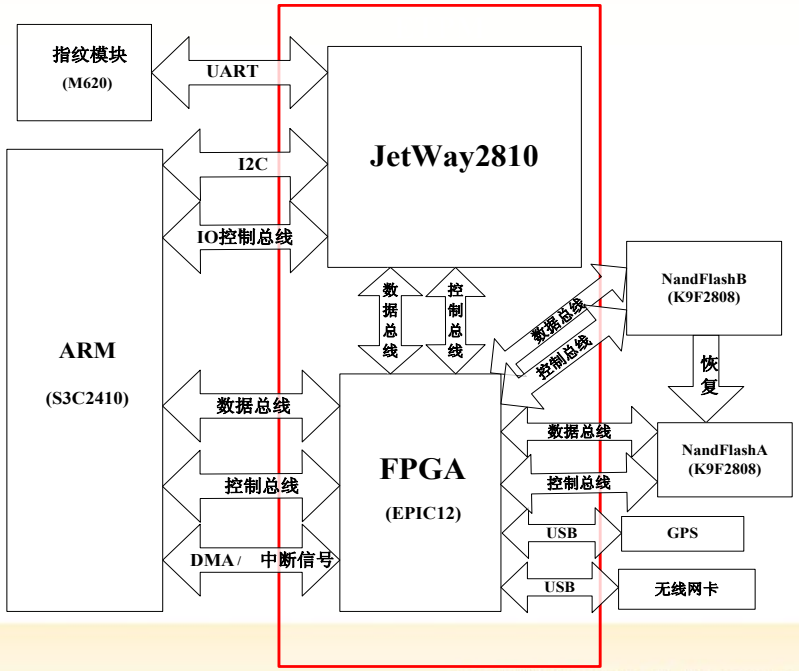
4、工作基础及实践

(1) 一种星型的信任链结构研究

提出 具有系统备份恢复能力的星型信任结构

解决 国外链式信任存在的信任衰减、结构实现复杂的难题，适应云环境中信任的传递和验证。



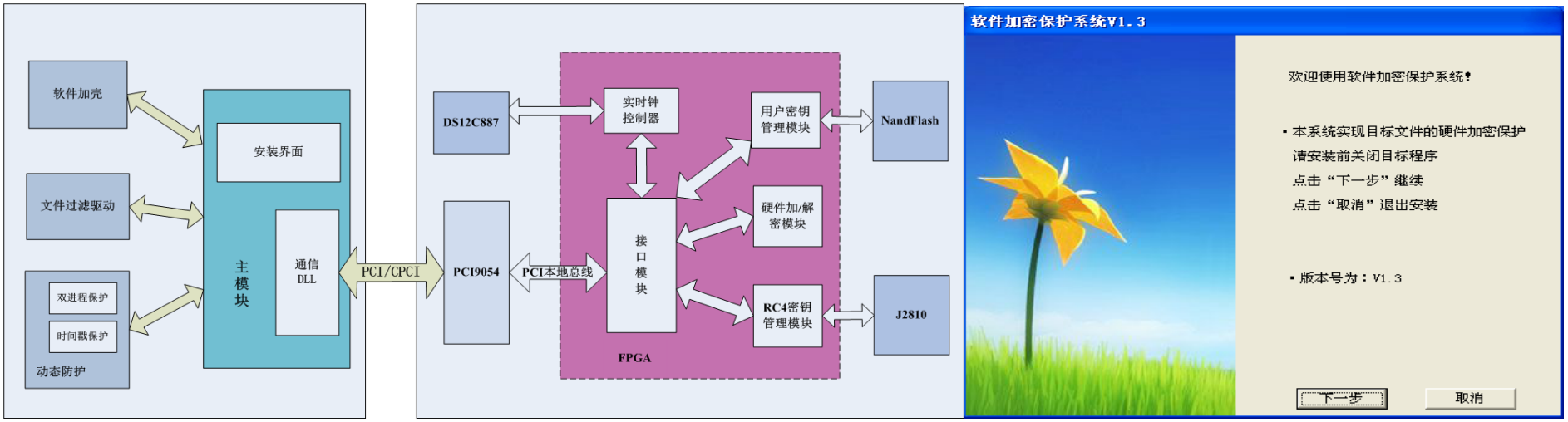


4、工作基础及实践

(2)基于可信平台技术的软件保护与安全分发

提出 基于可信硬件的软件保护与安全分发体系

实现了一套基于可信硬件的软件安全分发与保护系统，给出云环境中的隐私数据及软件保护、内存保护等问题的实现思路

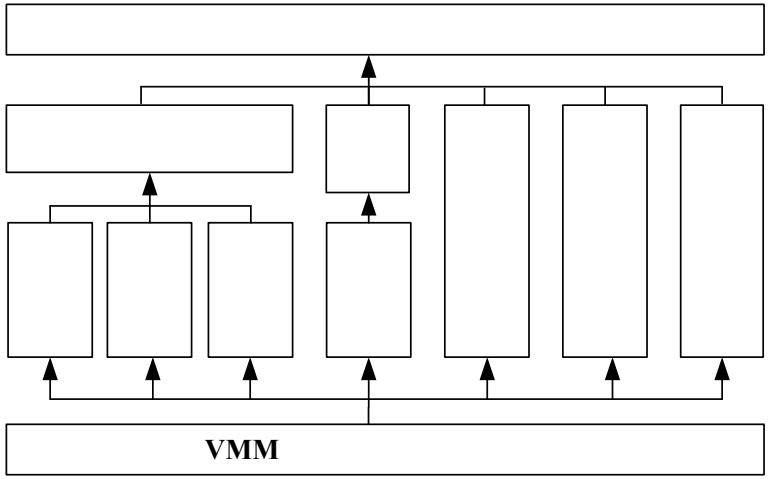


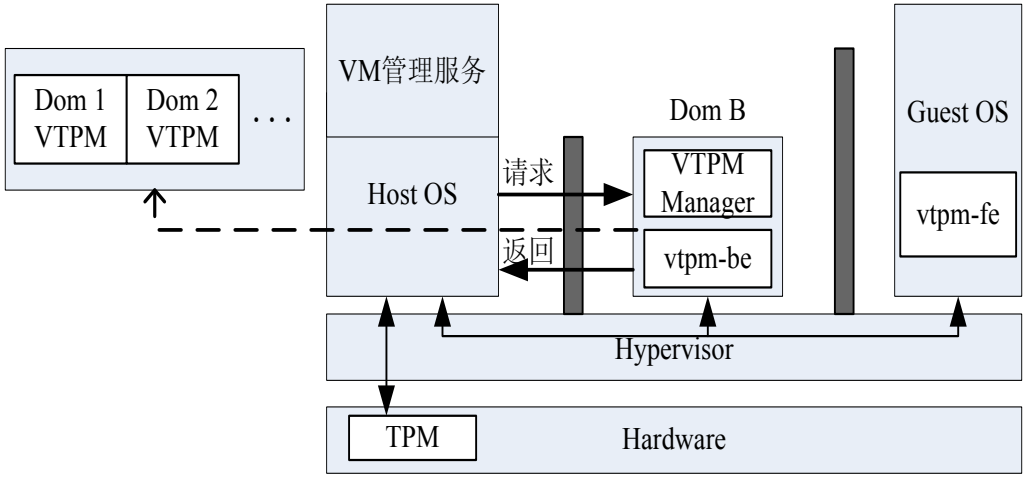
4、工作基础及实践

(3) 基于可信虚拟计算平台的数据防泄漏

提出 基于可信虚拟平台的数据防泄漏理论模型及方法

解决 云计算中可信计算环境的隔离与度量难题



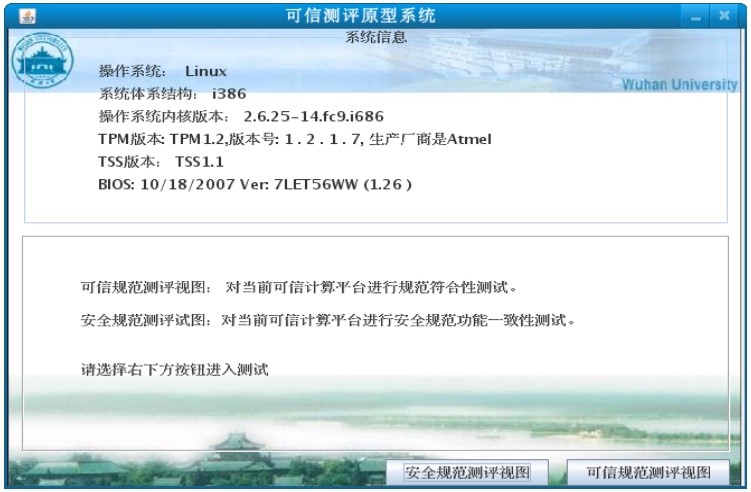


4、工作基础及实践

(4)可信计算环境安全性测评理论与关键技术

提出 一套可信计算环境安全性测试与评估方法

解决 云平台安全性测试与评估方面的空白，证明用户可感知的可信云计算环境



已实施测评对象


Lenovo Thinkpad R61i


HP NC 6230


HP NC 6400


某国产可信计算机


某国产可信计算机

4. 总结

云环境基础设施架构安全研究

从理论角度分析现有虚拟机系统的安全缺陷，对虚拟化环境安全性缺陷进行建模；提出一套虚拟机监控器安全性约束规则，保护虚拟机监控器；从虚拟机监控器到虚拟机内部，提供了一整套虚拟化环境保护方法有效防止来自跨域或同域环境中的恶意软件攻击，确保云环境的隐私性和完整性。

云计算环境可信软件与数据安全研究

以增强用户对云环境安全性的可感知性与可验证性为前提，围绕用户数据处理的整个生命周期，通过论证软件和数据的存储态和运行态两方面的安全可信，达到用户对软件和数据的安全需求。而软件可信及数据本身的保护对于用户而言至关重要，须给予高度重视。

用户可感知的可信评估方案研究

针对云计算的三种典型服务模式，包括IaaS，PaaS 和SaaS，综合考虑云计算环境中服务可信性的各类信任评估需求，包括云服务提供平台、接入终端以及可迁移的用户可信评估，从服务可信属性抽取与描述、服务可信属性量化策略、服务可信性综合判定方法等方面开展研究。

通过以上三个方面的研究，可以得到云环境整体安全性的加强，从而为云计算环境的发展和普及奠定坚实的基础。

谢谢

RSA CONFERENCE
CHINA 2012