>> 首页
>> 被收录信息
>> 投 稿 须 知
>> 模 板 下 载
>> 信 息 发 布
>> 常见问题及解答
>> 合 作 单 位
>> 产 品 介 绍
>> 编委会/董事会
>> 关 于 我 们
>> 网 上 订 阅
>> 友 情 链 接

友情链接
>> 中国期刊网
>> 万方数据资源库
>> 台湾中文电子期刊
>> 四川省计算应用研究中心
>> 维普资讯网

基于可信轻量虚拟机监控器的安全架构*

Trusted lightweight VMM based security architecture

中文关键词：轻量级虚拟机监控器 信任链 安全架构 动态加载

英文关键词：lightweight VMM chain of trust security architecture launching on the fly

基金项目：湖南省教育厅资助项目（08C881）

作者	单位
程戈1,2， 邹德清2， 李敏2， 季成2	(1.湘潭大学 数学与计算科学学院， 湖南 湘潭 411105； 2.华中科技大学 计算机科学与技术学院 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， 武汉 430074)

中文摘要：

虚拟化技术越来越多地被用于增强商用操作系统的安全性。现有的解决方案通常将虚拟机管理软件（VMM）作为可信集，利用其作为底层架构的优势来为上层软件提供安全功能。这些方案都是基于通用虚拟机管理软件，因而存在以下问题：a）虚拟化性能上开销大；b）作为可信集相对比较庞大；c）不能提供有效的信任链证明自身可信性。针对上述问题，提出以轻量虚拟机监控器作为可信集的安全架构——Cherub架构，Cherub利用主流处理器的安全扩展指令和硬件辅助虚拟化技术在运行的操作系统中插入轻量级的虚拟机监控器，并利用该虚拟机监控器作为可信集用于实现多种安全目标。实验结果证明了该架构的有效性，并具有代码量小、动态可加载和虚拟化开销小等优点。

英文摘要：

Virtualization technology is more and more popular in enhancing the security of the operating system. The previous solutions usually take the virtual machine moniter (VMM) as the trusted computing base (TCB) and provide a security function by virtualization technology. However, those solutions have the following problems: a)Virtualization brings overhead which requires the users to bear the cost of virtualization when they don't need high security environment. b)The general-purpose VMMs based solution cannot meet the users' (especially the client-side users) demand for the environmental diversity. c)The general-purpose VMMs are relatively large as a trusted computing base (TCB). This paper addressed the challenge to reduce the overhead of virtualization and established a dynamic chain of trust when used VMM to enhance the security of OS. This paper proposed a security architecture named Cherub which took a lightweight virtual machine moniter(LVMM) as the TCB. Cherub utilized the dynamic root of trust for measurement and hardware virtualization to insert a trusted LVMM under the commercial operating system, which could be the TCB to achieve various security goals. Implemented Cherub in Linux and the evaluation demonstrates that Cherub is effective and practical in security and performance perspectives.