 DOI: https://doi.org/10.12345/gcjsygl.v5i24.9842

Discussion on the Application of Virtual Machine Technology in the Field of Information Security

Kun Deng

Xuzhou Xinzhi Technology Co., Ltd., Xuzhou, Jiangsu, 221006, China

Abstract

The maturity and application of a series of advanced technologies such as computer, Internet and cloud computing have brought great convenience to people's learning and work, but it has also caused many security problems. Based on this background, this paper uses the investigation and literature methods to explore the specific application of the virtual machine technology in the field of information security, hoping to bring some help to the relevant work.

Keywords

information security; virtual machine; specific application

信息安全领域虚拟机技术应用探讨

邓昆

徐州信智科技有限公司，中国·江苏 徐州 221006

摘　要

计算机、互联网、云计算等一系列先进的技术的成熟与应用给人们的学习、工作带来了极大便利，但是也引发了许多安全问题。论文基于这一背景，运用调查法、文献法对虚拟机技术展开探讨，并对虚拟机技术在信息安全领域的具体应用进行探究，希望能为相关工作带来些许帮助。

关键词

信息安全；虚拟机；具体应用

1 引言

21 世纪，计算机网络飞速发展，大数据、云计算、互联网等已经渗透社会各行各业，给现代社会的生产生活带来巨大变革。正如网络是把双刃剑一般，计算机网络、云计算等先进技术在方便人们生活的同时也引发了许多新的问题，如企业、个人的信息安全开始遭受各种威胁，企业信息被篡改、个人信息被盗取等事件层出不穷。针对这些信息安全问题，中国提出使用可信 3.0 自主可控的可信计算技术、虚拟化技术来提升信息的安全性，有效解决当前的信息安全危机。经过研究与实践证明，虚拟化技术、可信计算技术有利于构建起一个安全可靠的云环境，让用户信息安全得到保证。但与此同时，虚拟化技术、虚拟机在信息安全领域发挥着积极作用的同时，虚拟机自身也面临着许多安全威胁。下面结合实际首先对虚拟机面临的安全威胁做具体分析。

2 信息安全领域虚拟机面临安全威胁分析

在信息安全领域，虚拟机主要面临来自以下几方面的安全威胁。

2.1 外部安全威胁

虚拟机在运行过程中容易受到来自外部的恶意攻击。一些人员会为利用系统漏洞攻击虚拟机，并获得虚拟机的控制权，最终给虚拟机用户带来不便。此外还有一些恶意攻击者会利用木马病毒攻击虚拟机系统，于虚拟机系统中植入恶意软件破坏系统的架构，降低系统的安全性与可靠性。部分恶意攻击者会通过模仿合法用户对虚拟机的配置或运行数据进行修改，从而达到破坏云环境虚拟机数据机密性、完整性与可用性的目的[1]。

2.2 内部安全威胁

除了一些外部的攻击、入侵外，虚拟机系统内部的管理人员也有可能影响虚拟机的安全稳定运行，给虚拟机内部信息数据安全带来威胁。这是因为，目前内部管理人员对云环境下的用户数据拥有着绝对的管理权、控制权。在权限范围过大的情况下，一些不怀好意的管理员就会滥用自身权力侵犯他人隐私，对用户数据进行窃取或篡改，使用户遭受巨大损失。除此之外，一些管理员也有可能会因为一时的疏忽大意而在系统中安装或植入恶意软件、病毒软件，造成虚拟机的安全性大大下降。一些内部管理人员甚至会恶意破坏虚

【作者简介】邓昆（1978–），男，中国安徽庐江人，硕士，副高级工程师，从事信息安全管理研究。

拟机的运行，如他们会通过内部管理接口修改虚拟机镜像文件，最终实现对虚拟机的控制 [2]。

来自内外部的攻击、入侵、篡改等都会让虚拟机的运行受到很大影响，会让用户数据的完整性、机密性受到严重破坏，因此必须采取有效措施增强虚拟机的安全防护性能，保障用户数据安全。

3 信息安全领域虚拟机技术应用

随着云计算规模的不断扩大，人们对于构建安全可信的云环境的需求愈发强烈，而保证虚拟机的可信启动过程则能够为构建可信云环境筑起第一道安全防线 [3]。因此，论文重点探讨基于计算机与虚拟化技术的虚拟机可信启动总体框架，通过该框架对虚拟机可信启动过程进行监测、控制，让虚拟机足够安全可靠。

3.1 虚拟机启动分析

在云计算以及信息安全领域，虚拟化技术是一项最基层也是最核心的技术，虚拟化技术需要向云用户提供隔离性与安全性保证。然而随着攻击手段的不断发展以及入侵技术的日益成熟，虚拟技术开始很难全面保证用户数据信息的安全性与可靠性。具体如在攻击技术、攻击工具不断发展的情况下，一台虚拟机有可能在启动初期就受到攻击或被恶意控制。那么在此情况下，该虚拟机就已经处于不可控的状态，用户不管在哪一时段使用虚拟机，其私密数据、存储的资源等都有可能受到篡改、窃取或破坏 [4]。

虚拟机在云环境中是作为进程运行于宿主机操作系统上，操作系统通过虚拟机的监视器监视、调度及使用宿主机硬件资源（具备 CPU 虚拟化功能）。在虚拟机监视器的管理下，虚拟机的启动流程为：用户（位于 QEMU 层）发出虚拟机启动命令；启动命令通过执行 Ioctl 系统调用命令进入 KVM 内核层；启动命令进入到内核层后获取到 KVM 句柄，然后映射虚拟机内存；启动命令于内存中映射虚拟机镜像；创建 VCPU，完成 VCPU 内存空间分布；虚拟机在 KVM-RUN 的命令下开始运行。

通过对虚拟机启动流程的分析可知，要想在云环境下实现虚拟机的可信启动，那么就需要为虚拟机配置虚拟可信保障，同时还要根据实际情况，运用相应的监测控制机制对虚拟机启动过程进行监测，必要时进行控制，使虚拟机在启动过程中能更有力防御或应对来自内外部的各类威胁，实现安全启动，同时也为用户提供可信、安全保证。

3.2 虚拟机可信启动框架

云环境下用户使用的计算与存储资源与传统硬件计算机实体中的资源有很大不同。云环境下用户使用的计算与存储资源都是由云服务提供商提供，这意味着，云服务提供商的权限大于云用户，云用户的数据安全、资源安全等有可能遭受来自云服务提供商的威胁。针对此，就需要建构一个科学完善且合理可靠的虚拟机可信启动框架（如图 1 所示），利用该框架有效改善用户信息不安全的现状，为用户信息安全提供保证。

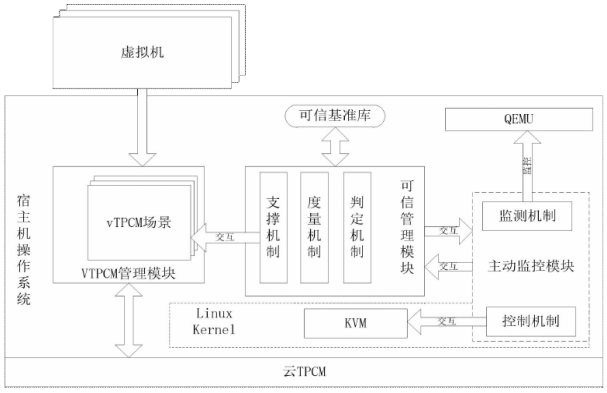

图 1 虚拟机可信启动框架

虚拟机可信启动框架由以下部分构成：可信管理模块、vTPCM 管理模块、主动监控模块以及可信基准库。其中可信管理模块又包含以下三种机制：判定机制、度量机制以及支撑机制。可信管理模块中判定机制的主要作用是：对来自度量机制的度量结果进行接收，同时对度量结果进行校验（依据可信基准库中的基准值）。在校验完成的基础上根据相应的可信判定策略调用主动监控莫开的控制机制，对虚拟机启动过程做主动可信控制。度量机制在可信管理模块中主要有以下作用：格式化存储相关的可执行实体信息（该部分信息主要由主动监控模块发送）；同时对虚拟可信根 vTPCM 进行可信度量，得到度量结果后将其发送给判定机制，由判定机制对度量结果进行判定。实时更新基准库的基准值数据，确保虚拟机在可信启动过程中的灵活、安全以及可靠。需注意的是，该更新行为需要在后台策略的管控下进行。可信管理模块中的支撑机制主要是作为一种媒介而存在（主动监控模块中监测机制与可信管理模块中度量机制与 vTPCM 管理器交互的媒介）[5]。

3.3 虚拟机可信启动框架运用

在云环境下虚拟可信根需要结合相关的控制系统对虚拟机进行主动监控，所以虚拟机所对应的虚拟可信根要先于虚拟机完成初始化。在完成初始化后，随着虚拟机启动，监测机制（位于主动监控模块）就能及时监测虚拟机命令并根据检测结果向 vTPCM 管理模块发出通知，要求 vTPCM 管理模块开始对 vTPCM 的初始化动作。在各条件都正常的情况下，操作人员此时就能通过宿主机的目录看到虚拟可信根设备的初始化进程以及已经成功完成初始化的提示。为了更好地监测、控制虚拟机启动过程，还可在内核层部署钩子函数，通过这一措施对内核层 KVM 虚拟机的行为进行监测、控制，防止各种意外状况的发生。在部署钩子函数的基础上，通过相应的接口函数将虚拟机在启动过程中产生的各项数据、信息收集与整理起来，对各数据与信息进行度量与判定，判断虚拟机的启动是否正常。这样一套程序与机制就能很好

地控制虚拟机启动过程，保证虚拟机的可信启动能够实现。

4 结语

综上所述，在云环境中，虚拟机是最小的服务单元，虚拟机的可信启动对云可信体系的构建非常重要，优化虚拟机启动流程，有利于完善整个云可信体系，有助于保护用户私密数据、宝贵资源不被窃取或破坏。因此，在当前背景下应高度重视对虚拟机的研究与优化，让虚拟机技术在信息安全领域发挥出更大的作用。

参考文献

[1] 曹勇,魏国珩,朱婷婷.虚拟化技术在信息安全领域的应用[J].电子技术与软件工程,2017(13):209.

[2] 邓志杰.虚拟化技术在信息安全领域的应用[J].电子技术与软件工程,2017(2):226.

[3] 刘婧欢.浅谈虚拟化技术在信息安全领域的应用[J].赤子(上中旬),2017(1):149.

[4] 胡志锋.虚拟化技术在信息安全技术专业中的应用[J].电子制作,2016(24):72.

[5] 金剑,张明.浅谈虚拟化技术在信息安全领域的应用[C].《智能城市》杂志社,美中期刊学术交流协会,旭日华夏(北京)国际科学技术研究院,2016.

（上接第 134 页）

溶剂中分离出来。纳滤也被称为低压逆渗透。纳滤和逆渗透差不多的特性，都能很好地把水中的有机物与离子清除出去，不过，纳滤对二价离子的清除比一价离子的清除率高得多。由于纳滤具有的特有属性，人们会合理地利用其特有属性，实现价值最大化[3]。

微滤实则就是一种精密过滤，也叫微孔过滤。主要是在微米级和纳米级范围内过滤掉微粒和细菌。这么精细的技术定会运用于纯水处理中的最后一道程序。由于现在，发电厂对纯水颗粒状物没有很高的要求，致使其没有被广泛地引用。当然，微滤有着筛分、滤饼层过滤及其深层过滤的三种原理良好的分离性能，依然能为电厂水处理中很多地方引用推广。

5 结语

膜技术作为一种新型技术，如果能广泛地应用的在电厂水处理中的，那么必然会带动中国水处理技术更深层次的钻研与提高，并且会多方面、多个角度上引领钻研人员在技术能力方面继续挖掘潜力，寻求更大突破口。对其他学科的技术也能起到借鉴的作用。深化膜技术在电厂水处理中的应用，促使中国整体电厂水行业的发展与进步。

参考文献

[1] 宋荣杰.膜技术在电厂环冷却排污水处理中的应用[J].中国电机工学会第十届青年学术会议,2017(7):2923.

[2] 卞卫华.膜技术在电厂水处理中的应用[J].能源工程,2005(3):56-58.

[3] 陈建花.关于电厂化学水处理中反渗透膜技术的应用探讨[J].当代化工研究,2021(14):119-120.