云基础设施安全性研究综述

黄 瑛 石文昌
(中国人民大学数据工程与知识工程教育部重点实验室 北京 100872)
(中国人民大学信息学院 北京 100872)

摘 要 云计算是当今全球关注的热点,有可能引起信息技术新的变革,但同时也带来了新的安全问题。从云计算环境最基础的层次入手,对云基础设施的安全性进行研究,考察云基础设施安全性的研究状况,从全局角度分析云基础设施存在的安全问题,结合云基础设施的安全服务技术框架讨论云基础设施安全性的主要关键技术,旨在为云基础设施乃至整个云计算环境的安全问题的解决建立良好的基础。

关键词 云计算,基础设施,安全,隐私,虚拟化
中图法分类号 TP309 **文献标识码** A

Survey of Research on Cloud Infrastructure Security

HUANG Ying SHI Wen-chang
(Key Lab of Data Engineering and Knowledge Engineering of Ministry of Education, Renmin University of China, Beijing 100872, China)
(School of Information, Renmin University of China, Beijing 100872, China)

Abstract Cloud computing is a worldwide hot topic nowadays. It will probably cause a new revolution to information technologies. But meanwhile it induces new security problems as well. Standing on the bottom layer of a cloud computing environment, this paper carried out research on security of cloud infrastructure. It observed the state-of-the-art of cloud infrastructure security, analyzed security problems existing in cloud infrastructure from a wide perspective. In combination with a technical framework of cloud infrastructure security, it discussed principle key techniques of cloud infrastructure security. The motivation of the paper is to lay a solid ground for solving security problems in cloud infrastructure as well as in the whole cloud computing environment.

Keywords Cloud computing, Infrastructure, Security, Privacy, Virtualization

利用有限的资源实现效益的最大化始终是计算机科学技术发展追求的目标之一。从基于集群的计算模式发展到网格计算模式,就是一种计算能力的提高和有效利用有限资源的进步。而当前如火如荼的云计算模式,则可以说更多的是一种服务模式的提升,它以现有的技术和方法为基础,整合利用一系列的服务、应用、信息和基础设施,旨在为用户提供无限制的、可伸缩的、易获得的IT资源服务[1-5]。这种"即需即得,用完即止"的服务模式充分体现"网络就是计算机"的思想[4]。

云计算发展非常迅速,大有向电子政务和电子商务等领域广泛渗透之势,引起了IT业界和相关领域的广泛关注,并受到各国政府的重视与支持。国际、国内很多成功的云计算案例纷纷涌现。国际上,亚马逊(Amazon)的EC2/S3[6]、谷歌的MapReduce/AppEngine[7,8]、Yahoo! 的HDFS[9]、微软的Azure[10]、IBM的蓝云[11]、Salesforce的CRM[12]等都是著名的案例;而国内,无锡的云平台、山东东营的政务云、中化集团的中化云等也逐渐呈现[13],同时,云计算的国家级策略也在不断酝酿[14]。在应用领域,不少银行对云计算发挥着助推作用,例如,著名投资银行Morgan Stanley和法国投资银行等都有相应的举措[15,16]。美国的纽约时报和纳斯达克证券交易所等则已成为亚马逊的大型客户[15,17]。政府方面,美国政府计划在2010至2015年间以40%的综合年增长率资助联邦政府的云计算建设,预计在2015年的投入将超过70亿美元[18],其总务管理局(GSA)还专门为云计算服务设立了门户网站[19]。根据国际IDC的分析,2009年全球云计算服务的市场额约为174亿美元,2013年估计可达442亿美元,欧洲的市场则将从2008年的9.71亿欧元发展到2013年的60.05亿欧元[19]。

云计算服务模式拥有传统服务模式所不具备的很多特性,它融合多种技术以集约化的资源管理方式向用户提供自由、方便和灵活的服务,这种新的服务模式很可能引起历史上又一次重大的产业变革,但同时也带来不少值得深思的新的安全问题。

针对云计算模式带来的新的安全问题,本文首先分析云基础设施提供的安全性的重要意义,然后弄清云基础设施中

到稿日期:2010-08-10 返修日期:2010-11-10 本文受国家自然科学基金项目(61070192,91018008,60873213),国家高技术研究发展计划项目(2007AA01Z414),北京市自然科学基金项目(4082018),上海市智能信息处理重点实验室开放课题(IIPL-09-006)资助。
黄 瑛(1987-),女,硕士生,主要研究方向为信息安全;石文昌(1964-),男,博士,教授,博士生导师,主要研究方向为信息安全、可信计算、系统软件,E-mail:wenchang@ruc.edu.cn(通信作者)。

哪些特性与安全性密切相关，探讨云基础设施存在什么样的安全问题，讨论提升云基础设施安全性的技术架构，最后结合国际上云基础设施安全性研究的状况，阐述解决云基础设施安全问题的关键技术。

1 云基础设施安全性的意义

云计算浪潮已经波及世界各地，但实际应用的局限性显而易见，其中，安全问题是重要的原因之一。就用户而言，在乐意接受云提供商(CP，Cloud Provider)提供的一系列数据、应用或硬件资源等方便服务之前，如何能够放心地享用这些服务是他们踌躇不前的关键。由传统的自己拥有和完全掌控信息资产的格局转变为租用由第三方提供的物理的和虚拟的基础设施资源的方式，用户难免担忧以这种方式租用服务是否会像使用的互联网服务那样，既面临复杂多变、防不胜防的黑客攻击，又不得不忍受网络时而中断或拥塞而不稳定的困扰，这就需要云提供商无论是在政策和管理上还是在技术上都要向用户保证其提供的服务的可信性。正如 EMC 信息安全部 RSA 和欧洲信息安全署 ENISA 等所提出的那样，数据的私密性和安全性以及服务的稳定性已成为用户考虑是否使用云服务和如何选择云提供商的关键衡量指标[19-21]，目前，云服务的应用范围仅能涉及安全要求较低的应用，隐私保护和安全问题是阻碍云计算发展的重要障碍。在实际应用中，典型的云计算服务公司(比如 Amazon，Google 和 Microsoft 等)提供的服务出现安全漏洞的消息时有所闻[22-24]。可见，云安全问题的解决迫在眉睫。

云计算模式的基础是云基础设施，承载服务的应用和平台等均建立在云基础设施之上，确保云计算环境中用户数据和应用安全的基础是要保证服务的底层支撑体系(即云基础设施)的安全和可信，否则，其他的安全的解决途径，比如云提供商的信誉保障、服务合约的规定、政府制定的法律法规、组织或联盟的相关标准、甚至云提供商提供的安全管理基础服务等，恐都难逃治标而不治本的结局。所以，确保云基础设施的安全性对云计算的发展具有深远的意义。

2 云基础设施及其安全相关特性

云计算模式定义了基础设施、平台和软件等 3 个层次的服务方式，云基础设施是指为支撑其中的基础设施服务而构建的软硬件体系，它包含物理基础设施资源和虚拟基础设施资源。虚拟基础设施资源是在物理基础设施资源的基础上利用虚拟化技术构建的虚拟资源，涉及操作系统、存储、网络以及 CPU 等一系列硬件和软件资源。云基础设施栈的结构可以描述为如图 1 所示的形式。其中，位于基础设施底层的是硬件，包括 CPU、GPU 和网络设备等；该层之上的一层是虚拟化的基础，包括虚拟机管理器(Hypervisor)和虚拟网络机制(比如虚拟局域网 VLAN 和虚拟专用网 VPN 等)；再往上分别是虚拟资源和云相关管理软件。虚拟资源可以是多版本的各类操作系统、虚拟化网络以及存储等。云相关管理软件主要包括云管理器组件、云安全管理基础服务组件和计费管理组件等，它们是确保云计算环境的安全和规范不可或缺的成分，因此，我们视其为云特有的基础设施部件。

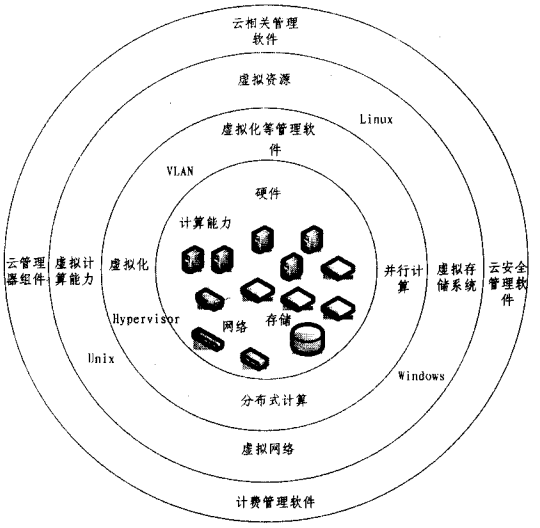

图 1 云基础设施栈结构

云计算模式灵活的动态管理方式和多租户形态给云计算环境的安全性增添了挑战，虚拟化技术的运用则进一步加大了确保云基础设施安全性的难度。为彻底剖析云基础设施存在的安全问题，有必要了解与云基础设施安全性密切相关的云服务特性。我们通过表 1 对传统环境和云计算环境两种不同环境下的服务特性进行对比分析，重点从网络开放程度、平台管理模式、资源共享方式、服务迁移要求和服务灵活程度等角度进行分析。

表 1 云基础设施安全性相关服务特性对比

分析角度	传统环境下的情况	云计算环境下的情况
网络开放程度	网页服务器、邮件服务器等接口暴露在外，设置访问控制、防火墙等防护措施维护安全。	用户部署的系统完全暴露在网络，任何节点可能遭受攻击。
平台管理模式	部署的系统通过内部管理员管理。	利用多样化网络接入设备远程管理，涉及网络通信协议、网页浏览器、SSH 登录等服务。
资源共享方式	一台物理主机对应一个用户。	多个用户同时共享 IT 资源(比如存储资源、物理平台)，用户之间需要有效隔离与通信。
服务迁移要求	不存在服务迁移问题。	单个云提供商提供给用户的服务应该可灵活迁移，以达到负载均衡并有效利用资源。同时，用户希望在多个云提供商间灵活迁移服务和数据。
服务灵活程度	一旦拥有，便一直拥有，容易造成资源浪费。	按需伸缩的服务，保证服务随时可用、可终止、可扩展、可缩减。

3 云基础设施的安全性问题

云安全包含两方面的含意，其一是借助云计算的能力解决传统的安全问题，其二是云计算本身引入了新的安全问题。利用新型的云计算模式重新部署原来在传统架构上实现的安全防护功能可以一定程度上增强安全防卫的效果，比如，可以弥补传统杀毒模式的不足，提高杀毒的实效性[25]，不少杀毒软件公司纷纷推出的杀毒云就是一类实际应用的典型例子。运用作为云计算基础的虚拟化技术也可以在一定程度上增强云数据中心的安全性，比如，可增强虚拟机实例间的隔离，降低拒绝服务(DoS，Denial of Service)攻击发生的可能性[26]，又如，利用虚拟化网络设施可有效缓解云计算的多租户特点引发的安全问题[27]。然而，源于云计算环境下用户数据的隐私

与安全问题和虚拟化环境的资源共享问题，新型服务模式和虚拟化技术的引入不可避免地会带来一系列新的安全问题。下面就讨论由这样的客观因素引起的云基础设施的安全性问题。

3.1 服务的可靠性问题

当前，云提供商提供的云服务的可靠性还难以令用户放心，换言之，云提供商还难以满足用户的特定服务需求。这种状况可能是由非恶意的行为引起的，比如，云提供商因前期估计不足而导致无法向用户提供额外计算能力，云提供商暂时无法满足当前用户提出的要求，缺乏合理的资源分配算法，管理员配置失误或过滤条件设置过于苛刻等；也可能是由恶意的行为导致的，比如，恶意用户通过利用系统的漏洞，人为地拒绝合法用户合理的服务申请，或通过发出大量毫无意义的服务请求以耗费服务器大量的计算能力而造成服务器拒绝合法服务等。由于云计算服务具有迁移特点，使得黑客可能只需专注于对单个服务器进行泛洪攻击就可以妨碍整个数据中心提供正常服务。目前使用最广泛的缓解服务质量问题的方法是借助服务合约，比如，服务级协议(SLA，Service-Level Agreement)。服务级协议作为云提供商为用户提供的利益保障依据，载述了服务未达到预期程度时提供补偿的声明，但并未对云提供商的利益作出规定。在服务合约制定的内容和规范方面，有待于确立一套实用的标准说明。从技术角度上看，若能适时地提出警告或防止拒绝服务攻击的发生，则会在很大程度上提高服务的可靠性。对云计算环境的网络流的有效监控能在一定程度上防御拒绝服务攻击或分布式拒绝服务(DDoS，Distributed Denial of Service)攻击，不幸的是当前的云基础设施还普遍缺乏一套有效的网络监控体系。

3.2 支持服务的技术标准或工具问题

出现在云计算环境中的虚拟机管理器多种多样，不同的虚拟机管理器支持的虚拟机格式不同，不同的云提供商采用的虚拟机管理器可能不同，数据在不同的服务提供商处存储的语义也可能不同。由于缺乏在不同的云提供商之间实现数据和服务移植的支持工具、数据格式标准或服务接口，在不同云的云提供商或自身的IT部门之间迁移数据或服务时，用户面临着高成本而低效率的窘境。因此，在不同的云提供商之间进行数据和服务迁移比较困难，一旦选择云计算架构，用户可能被迫产生对单个云提供商的依赖，这是用户不愿意面对的场景。

云提供商有义务向用户证明其内部操作是否符合服务合约的要求。提高云端的透明度将有利于提高用户对云提供商的信任程度，这属于合规性证明问题。通过开发必要的标准、工具和链接包，用于监视和证明云的物理设施和虚拟设施的运行，可以提高云端的底层透明度。然而，至今为止，在监视硬件、虚拟机管理器或虚拟机器等的运行状态方面，还缺乏行之有效的手段。

用户在使用云服务的过程中，云提供商可向用户反馈云计算环境的相关日志、报告和认证等信息，以便用户依据这些信息判断云提供商是否如实遵守要求。当前能够根据日志记录和报告等信息结合用户的服务要求判断操作合规性的工具还很欠缺。

3.3 特权问题和数据备份与灾难恢复问题

当用户把数据存放在云计算环境中时，数据的隐私和安全始终是他们关心的首要问题，事实上，在复杂的云计算环境中确实存在一定的安全隐患。其中，云提供商内部管理人员所拥有的特权对用户数据的隐私具有严重威胁，这就是典型的特权管理员问题，因此必须提供有效的管理机制来防止特权管理人员利用职权之便窃取用户私密数据或对其造成破坏。通过数据的加密存储可缓解这种潜在的威胁，但数据在云中生存的过程中难免有出现明文的时候，所以被攻击者利用的可能性难以避免。

完善的数据备份与灾难恢复功能在保证数据安全方面发挥了重要的作用。重复数据删除(Deduplication)机制通常用于数据备份过程，以便节约磁盘空间与网络带宽。然而，云计算环境的多租户形态反而使得重复数据删除机制有可能成为泄露用户信息的侧信道[28]。云计算环境中的用户数量非常庞大，备份每个用户的所有数据所需的磁盘空间容量非常惊人，且众多用户的数据在云环境中混合存储和备份，诚然，必须要提供有效的措施和工具，以方便高效地实施数据备份，妥善区分和管理好所有用户的数据，保证用户数据的机密性、完整性和可用性。

3.4 虚拟化和云管理软件的安全问题

虚拟化是构建云计算环境的关键。系统虚拟化管理软件通常称为Hypervisor。对某个Hypervisor的攻击可以波及其所支撑的所有虚拟机，威胁云计算环境的安全。现实中，曾出现过以非管理人员身份利用主流Hypervisor(即VMware虚拟机管理器)的漏洞实施的攻击，VMware安全中心为此发布过补丁更新[29,30]。Hypervisor的管理接口和安全模型的漏洞是黑客常攻击的目标。King等人提出了基于虚拟机的Rootkit概念[31]。针对Hypervisor的典型的攻击有“虚拟机逃离”[32]和“虚拟机跳跃”[19,33,34]等。虚拟机逃离是指虚拟机内的程序可能会逃出到虚拟机以外，危及主机的安全。虚拟机跳跃是指借助与目标虚拟机共享同一个物理硬件的其他虚拟服务器，对目标虚拟机实施攻击。另外，管理员对Hypervisor的配置失误也可能成为安全隐患。

云管理器各组件分布在多个物理服务器上，在提供服务的过程中，各组件之间的数据中转和传输过程的增加会导致云管理器容易被攻击者利用，比如，通过嗅探、中间人攻击和重放攻击等可以容易地实施数据拦截。进一步地，如果云管理器本身遭到攻击者入侵，云环境给用户提供的服务将会面临更加严峻的威胁。

云安全管理基础服务组件本身和计费管理软件等也有可能受到安全威胁，也需要得到保护。云安全管理基础服务主要包括认证、访问控制、授权和审计等，它们从多角度实施对用户数据隐私和安全的保护。在认证和标识管理方面，必须突破传统的用户名/密码认证机制，才能防御账户或服务劫持攻击、凭证或密码重用攻击和网络钓鱼攻击；在访问控制方面，必须灵活融合多类访问控制方法(比如基于属性的方法和基于凭证的方法)，同时，依据不同的隐私保护需求辅以合适的特权原则；在密钥管理方面，必须克服硬件安全模块在虚拟机上应用的不足，研究分布式环境下的密钥管理标准，实施多类密钥的安全管理，保证虚拟化环境密钥生成机制的可信性和公开网络中密钥管理接口的安全。此外，必须注意上述相关服务组件都有可能遭受恶意用户攻击。

3.5 安全的虚拟化环境问题

虚拟化环境本身的特性也会带来新的安全威胁，在云环

境下这些威胁有增无减，这主要体现在虚拟机数量繁多、虚拟化环境的动态性、多样性和资源共享等方面。

特性 1　虚拟机数量繁多。

云环境下虚拟机数量规模之大，导致虚拟机之间感染快速，需要安装的补丁数量繁多，增加安全扫描的繁重程度。

特性 2　动态特性。

动态虚拟化环境引发很多值得深思的问题：虚拟机起始状态不定；虚拟机在同一物理主机上的生命周期可能不完整，传统的系统监视工具难以适用[35]；网络结构变化多端，感染传播迅速，难以确定感染源；虚拟机的 MAC 地址随机分配，计算机名与以太网地址并非始终绑定[36]；虚拟机映像若被窃取可能会造成敏感信息泄露；系统的可回滚特性导致传统认证机制存在漏洞，比如，回滚的时间点恰好在随机数已产生但并未使用之时，随机数就有可能在加解密中被重复利用；启动和管理虚拟机迁移的控制机制容易受到威胁[37]，例如，虚拟机管理器实施到迁移时的通信上的访问控制如果薄弱，可能影响整个迁移过程的正常执行，又如，迁移过程中的数据传输容易因 DNS 投毒或路由劫持等攻击而泄露敏感信息，最后，利用迁移模块本身的漏洞攻击虚拟机管理器可能获得对所有客户机系统的控制能力。

特性 3　多样性。

同一台主机上的虚拟机类型多样，它们的系统类型及配置无法预料，各种平台采用的 Hypervisor 可能不同，有些并不支持可信启动功能，这需要多样化的工具实施监控。

特性 4　资源共享。

资源共享带来的安全问题始终是虚拟化环境安全的核心。虚拟化环境下的资源共享主要体现在存储、内存和路由等层面，比如，云用户可对内部网络的其他用户进行端口扫描或其它测试；云用户可将存储域网络（SAN，Storage Area Network）中同一逻辑单元的另一用户的虚拟硬件设备挂载到自己的系统中并窃取数据。资源隔离的失败可能导致虚拟机跳跃攻击和侧信道攻击等[19]。Hypervisor 虽然能够提供一定的隔离能力，但并无法控制运行中虚拟资源共享的信息流。系统中的数据删除不彻底现象在云环境下更容易造成信息泄漏，因为同一主机上多个不同用户共享虚拟存储设备，使得一个用户未彻底删除的数据易被其他用户恢复并窃取，这就是遗留数据被盗用问题。在网络隔离方面，云环境采用基于“安全组”或“安全域”的虚拟隔离方法代替传统的局域网或外联网所采用的基于物理设备的隔离方法，降低了网络的安全保护能力[38]。由资源共享导致的攻击层出不穷，比如，主机通过监控虚拟机的行为并利用共享剪贴板等机制达到攻击目的[39]；虚拟机与虚拟机之间可互相监控造成网络包嗅探或 ARP 投毒等攻击[39]；还有利用物理资源共享特性躲过 Hypervisor 而实现的跨虚拟机攻击[34]。

另外，虚拟机映像本身受到的安全威胁也非同小可。IBM 研究人员分别从映像发布者、映像使用者和映像管理者等角度探讨了虚拟机映像面临的安全威胁的应对办法[40]。

4　云基础设施安全技术服务框架

支撑云基础设施安全性的技术服务框架可通过图 2 的形式描述，它在基础设施层之上构建一个基础设施安全服务体系层，该体系层主要包括服务合约标准体系、平台网络监控体系、一套支持迁移和合规性审查的技术标准/工具、保证存储数据隐私与安全的方案、虚拟化与云管理相关组件自身的安全保证和安全虚拟化环境保障体系。在该安全保障层之上是云平台更高层的服务，包括云安全管理基础服务（比如安全审计和访问控制等）、计费管理服务、平台层服务和软件层服务。该安全技术服务框架的目标是建立安全、透明的云基础设施环境，图 2 表示借助该安全技术服务框架把左侧没有安全保障的云基础设施构建成右侧有安全保障的云基础设施。

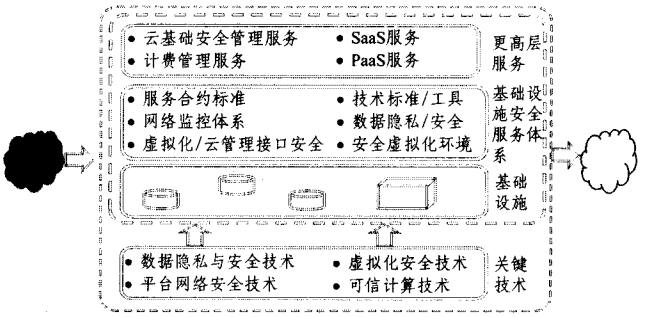

图 2　云基础设施安全技术服务框架

5　云基础设施安全研究状况

2007 年以来云计算的影响越来越广泛[41]，同时，云安全问题受关注的程度也越来越高。T. Mather 等人系统地阐述了云计算的安全与隐私问题[42]。云安全联盟（CSA，Cloud Security Alliance）针对云计算应用中遇到的问题和挑战为用户提出了指导性建议[43]。欧洲网络信息安全署（ENISA，European Network and Information Security Agency）则研究云计算应用中信息安全的利弊与风险[19]。2010 年，CSA 再次发布了关于云计算十大威胁的技术报告[44]。EMC 信息安全事业部 RSA 就云环境中最基本的安全问题云基础设施的安全问题进行了分析[20]。国内同行也纷纷对云计算及其安全性展开了讨论[45,13,46]。至今，云计算安全性很多方面的问题都引起了人们的关注，比如，服务级协议、合规性、访问控制[47,48]、账户管理[42,49-51]、审计[52,53]和授权[54]等，特别地，对云基础设施服务的安全性研究在逐渐增多。

针对云计算环境下的合规性管理方法，I. Brandic 等人提出了利用特定的语言表示根据安全和隐私需求制定的合规性要求[55]。由于服务级协议是目前云提供商向用户提供的唯一合法的服务协议，该协议的标准化有利于增加用户对提供商的信任，由此，Kandukuri 等人对服务级协议的标准化问题进行了研究[56]，S. A. de Chaves 等人则进一步提出了安全服务级协议的概念[57]。

斯坦福大学计算机科学研究团队的 T. Garfinkel 等人自 2003 年以来在虚拟化安全性研究方面取得了不少成果，比如，保护虚拟机内核的 Livewire 系统[58]和保证虚拟机不受特权用户侵害的 Terra 系统[59]等。针对虚拟化环境提出新的映像存储格式对云计算虚拟化环境的安全性具有积极的作用。德国莱比锡马普研究所软件系统协会（MPI-SWS）的 N. Santos 等人 2009 年提出可信云计算平台[60]，以防止云提供商特权管理员对虚拟机的非法访问，但并未实现原型。

IBM 研究部门的 S. Berger 和 J. Trent 等人一直关注服务器端安全性的研究，他们的研究主要集中在两方面：安全 Hypervisor 和虚拟化可信平台。在安全 Hypervisor 方面，研

究 Hypervisor 和虚拟机的完整性检测方法，以保证 Hypervisor 平台、虚拟机及其上运行的应用的安全启动，同时研究对虚拟机使用资源（比如内存、CPU，甚至网络带宽）的计算与控制，提出的安全 Hypervisor 还能提供方便的安全策略管理与分布式审计方法，这对于云计算环境安全基础设施建设无疑起到非常重要的先驱作用。在虚拟化可信平台方面，研究如何能更好地将 TPM 应用于虚拟化环境，继 2005 年和 2006 年相继推出 sHype（Secure Hypervisor，安全虚拟机监控器）和 vTPM（Virtual TPM，虚拟可信平台模块）之后，2008 年通过整合 sHype，vTPM，TPM 和相关管理软件，提出了可信虚拟数据中心的设计[61]。2009 年，进一步研究虚拟机完整性的检测方法，推出完整性验证器，继而在 2010 年，把虚拟机的完整性验证器应用到云计算环境中，借助云验证器（Cloud Verifier）实施对云基础设施的访问控制和完整性的验证[62]。

6 云基础设施安全关键技术

针对前面讨论的云基础设施面临的安全问题，下面探讨实现云基础设施安全性的关键技术，主要涉及用户数据的隐私保护与安全、云计算平台的网络安全、虚拟化安全和可信计算等方面。

6.1 数据隐私与安全技术

云数据中心内部管理员的特权模式对用户数据隐私造成严重威胁，为防止云提供商对用户数据的错误使用，需要采用符合云计算环境的特殊加密和管理方式，比如，C. Centry 等人提出了一种完全同态加密机制[63]；M. Jensen 等人利用基于环和组签名的加密方法实现用户数据的匿名存储[64]；W. Itani 等人提出通过加密协处理器的防篡改能力提供云环境下的安全执行域，从物理和逻辑上防止数据的未授权访问[65]；E. Victor 等人利用基于属性的加密措施设计数据的访问控制方法，以加密形式保存用户数据[66]。针对遗留数据被盗用问题，美国国防部提出清零和特殊处理等指导性建议解决方案[42]。特别地，J. Kirch 等人提出了可利用自加密和完全磁盘加密方法对虚拟机映像及组成映像的文件中的加密数据实行保护[67]。

云环境下多用户的密钥管理是加密存储中必须面对的有其特殊性的问题，它既允许多用户之间的数据共享访问，又要防止数据的非法访问，这就需要合理的密钥管理架构。比如，L. Seitz 等人提出了支持加密数据多方访问的密钥管理架构[68]；J. Huang 等人利用会话 ID 和用户 ID 管理密钥[69]。

6.2 平台网络安全技术

针对云相关管理软件各组件之间可能涉及数据中转或上传或下载等传输情况，可结合数据加密与加密传输协议（比如基于 SSL 的 FTP，HTTPS 或 SCP 等）实现数据机密性与完整性。除了传统的设置防火墙安全策略的方法提高网络的安全性外，可通过监控网络流量防止泛洪等攻击，比如，A. Bakshi 等人提出利用虚拟机器上第三方入侵检测系统对网络状态实行监控以防止 DDoS 攻击[70]；F. Bonnassieux 和 R. Barbera 等人分别提出了网格计算环境网络监控工具 MapCenter[71] 和 NetSaint[72]。

6.3 虚拟化安全技术

虚拟化安全是云计算中核心的安全问题，这方面的研究成果针对的安全控制点主要包括对共享信息流的控制、对内存空间和内核的保护、对虚拟机行为的监控等，可从对 Hypervisor 的改进入手或引进新的监控系统来寻求问题的解决途径。R. Sailer 等人在传统 Hypervisor 架构中添加监控器，监控器通过安全策略定义访问每个虚拟资源的要求和每个分区访问资源的权限集合，通过对比访问要求和欲对资源执行的操作实现对共享信息流的控制，以构建安全的 Hypervisor[73]。D. G. Murray 等人针对具体的 Hypervisor（即 xen）研究通过缩小基于 xen 的虚拟系统的可信计算基（TCB，Trusted Computing Base）的尺寸来提高 xen 环境的安全性[74]。A. Seshadri 等人开发的 SecVisor 系统利用硬件内存保护机制保护内核代码的完整性，属于一个小型的 Hypervisor[75]。T. Garfinkel 等人提出入侵检测系统 Livewire，该系统利用硬件页保护机制监控虚拟机的内核状态[58]。Z. Wang 等人研究基于 Hypervisor 的轻量级系统，即同样利用硬件页保护功能控制对内存空间的访问[76]。B. Payne 和 M. Sharif 等人研究的都是对虚拟机行为的监控，前者是在虚拟机外面实现监控[77]，后者将监控器设计在虚拟机里面，借助硬件虚拟特性直接监控[78]。虚拟化安全方面的很多研究借助于硬件特性，包括传统的页保护机制和硬件虚拟化技术，比如，Intel 的可信任执行技术（TXT）和 AMD 的安全虚拟机技术（SVM，Secure Virtual Machine）等。但是对复杂多变的云环境来说，有些方法并不适用，鉴此，Q. Liu 等人尝试通过摆脱对硬件虚拟特性的依赖而寻求实现监控目的的方法[79]。另外，T. Garfinkel等人提出在 Hypervisor 和虚拟系统之间构建虚拟层，用以实现对虚拟机器的安全管理，包括防火墙的设置、病毒扫描、虚拟机迁移和共享资源的访问控制等[36]。

虚拟化面对的一个重要问题是映像繁多而管理复杂，在云计算环境中尤为明显。D. Reimer 等人提出利用映像文件中的语义信息形成一种新的映像存储格式，对代表映像文件的清单文件执行库控制和映像更新操作，避免直接对映像文件内容进行操作，以求简单快速之效[80]。虚拟磁盘是虚拟化环境主要的存储形式，然而传统虚拟磁盘在共享访问、版本维护和安全保障等方面都不尽人意。B. Pfaff 等人提出考虑使用新的虚拟分布式文件系统存储格式代替传统的虚拟磁盘，以便更好地实现共享访问和版本维护等[81]。G. Ammons 等人针对映像本身的安全管理提出虚拟机映像管理系统 Mirage[40]，通过访问控制机制规范对映像的访问，利用映像过滤器过滤恶意的或不必要的信息，增加跟踪机制和库维护服务以增强映像管理的安全性。

6.4 可信计算技术

可信计算技术的重要应用是保护软件的完整性，可信平台模块 TPM 是可信计算的关键部件，它以密码技术为核心，具有计算与存储功能，支持数据保护、身份证明和完整性度量等，可对软件进行完整性度量并提供度量报告，这在云计算环境中具有重要的应用价值。在如何利用 TPM 建立可信的操作系统环境方面已有不少研究工作和成果[82-86]。在此基础上，为解决 TPM 存在的问题而结合软硬件条件以保证操作系统完整性的研究也不在少数[86,87]。

可信计算技术与虚拟化技术的结合正逐步成为确保云基础设施安全性的研究热点之一。S. Berger 等人研究虚拟可信平台模块的目的就是想把传统的 TPM 功能应用到虚拟化环境中[88]，如果结合云的特点把它应用到云计算环境中，也许

能从云基础设施层面增强虚拟机实例的安全性。J. Kong 等人以虚拟化技术与可信计算技术的结合为基础[89]，通过修改客户虚拟机，强化虚拟机器之间的隔离，增强虚拟机上用户数据的机密性，以期达到纵使云提供商能够控制虚拟机器的可用性，也无法控制虚拟机器的机密性。

结束语 云安全蕴含着云计算环境具有的安全处理能力和云计算环境带来的新的安全问题两重意义。后者已成为云计算发展的障碍，是本文关注的对象。云基础设施是云计算环境的根基，其固有的安全问题就是云计算环境带来的安全问题之源头所在。为了清除妨碍云计算发展的绊脚石，必须解决云基础设施的安全问题。本文的目的就是为解决此类问题建立基础。本文的主要贡献是以全局的视角系统地展示云基础设施的安全问题所在以及国际上解决这些问题的整体技术水平，与此同时，给出了用于解决这些问题的主要关键和热点技术。希望本文的工作能使同行们给予同类研究更多的关注，并为提升云基础设施的安全性发挥积极的推动作用。

参 考 文 献

[1] Armbrust M, Fox A, Griffith R, et al. Above the Clouds: A Berkeley View of Cloud Computing[R]. Berkeley, USA: Electrical Engineering and Computer Sciences University of California at Berkeley, 2009

[2] Buyya R, Yeo C S, Venugopal S. Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities[C]// The 10th IEEE International Conference on High Performance Computing and Communications. Dalian, China, 2008: 5-13

[3] Mell P, Grance T. The NIST Definition of Cloud Computing [R]. National Institute of Standards and Technology, Information Technology Laboratory, 2009

[4] Armbrust M, Fox A, Griffith R, et al. A View of Cloud Computing[J]. Communications of the ACM, 2010, 53(4): 50-58

[5] Grossman R L. The Case for Cloud Computing[J]. IT Professional, 2009, 11(2): 23-27

[6] Amazon Web Services [EB/OL]. http://aws.amazon.com/, 2011

[7] Google MapReduce Code [EB/OL]. http://code.google.com/p/appengine-mapreduce/, 2011

[8] Google AppEngine Code [EB/OL]. http://code.google.com/intl/zh-CN/appengine/, 2011

[9] Wikipedia. Handoop[EB/OL]. http://en.wikipedia.org/wiki/HDFS#Hadoop_Distributed_File_System, 2011

[10] Windows Azure [EB/OL]. http://www.microsoft.com/ windowsazure/, 2011

[11] IBM Cloud Computing [EB/OL]. http://www-935.ibm.com/services/us/cloud/, 2011

[12] Salesforce[EB/OL]. http://www.salesforce.com/cn, 2010

[13] 朱近之，方兴，刘秦豫，等. 智慧的云计算[M]. 北京：电子工业出版社，2010

[14] 中云网[EB/OL]. http://www.china-cloud.com/ index.html, 2011

[15] Staten J. Is Cloud Computing Ready For The Enterprise? [R]. Cambridge, USA: Forrester Research, March 2008

[16] Weblogic Journal. Morgan Stanley is banking on cloud [EB/OL]. http://weblogic.sys-con.com/node/589951, 2011

[17] Gottfrid D. Self-Service, Prorated Supercomputing Fun! [EB/OL]. http://open.blogs.nytimes.com/2007/11/01/self-service-prorated-super-computing-fun/, 2007

[18] Kaufman L M. Data Security in the World of Cloud Computing [J]. IEEE Security & Privacy, 2009, 7(4): 61-64

[19] Catteddu D, Hogben G. Cloud Computing: Benefits, Risks and Recommendations for Information Security[R]. Europe: European Network and Information Security Agency(ENISA), 2009

[20] Curry S, Darbyshire J, Fisher D W, et al. Infrastructure Secutiry: Getting to the Bottom of Compliance in the Cloud[R]. The Security Division of EMC, March 2010

[21] Yildiz M, Abawajy J, Ercan T, et al. A Layered Security Approach for Cloud Computing Infrastructure[C]// The 10th International Symposium on Pervasive Systems, Algorithms, and Networks. Kaohsiung, Taiwan, 2009: 763-767

[22] Amazon Security Bulletins [EB/OL]. http://aws.amazon.com/security/security-bulletins/, 2011

[23] Google. [EB/OL]. http://googledocs.blogspot.com/2009/03/just-to-clarify.html, 2009

[24] Microsoft. [EB/OL]. http://www.microsoft.com/technet/security/, 2010

[25] Muttik I, Barton C. Cloud security technologies[R]. Amsterdam, Netherlands: Elsevier, February 2009

[26] Hwang Kai, Kulkareni S, Hu Yue. Cloud Security with Virtualized Defense and Reputation-Based Trust Mangement[C]// The 8th IEEE International Conference on Dependable, Autonomic and Secure Computing. Chengdu, China, 2009: 717-722

[27] Hao Fang, Lakshman T V, Mukherjee S, et al. Secure cloud computing with a virtualized network infrastructure[C]// The 2nd USENIX conference on Hot topics in cloud computing. Boston, Massachusetts, 2010: 1-7

[28] Harnik D, Pinkas B, Shulman-Peleg A. Side Channels in Cloud Services: Deduplication in Cloud Storage[J]. IEEE Security & Privacy, 2010, 8(6): 40-47

[29] Secunia. [EB/OL]. http://secunia.com/advisories/37081/, 2009

[30] Secunia. [EB/OL]. http://secunia.com/advisories/36389, 2009

[31] King S T, Chen P M, Wang Yi-Min, et al. SubVirt: Implementing malware with virtual machines[C]// the 2006 IEEE Symposium on Security and Privacy. Berkeley, California, USA, May 2006: 314-327

[32] Kortchinsky, Kostya. [EB/OL]. http://www.immunityinc.com/documentation/cloudburst-vista.html, 2011

[33] Tavis O. An Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments[R]. USA: Google, February 2010

[34] Ristenpart T, Tromer E, Shacham H, et al. Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds[C]// The 16th ACM Conference on Computer and Communications Security. Chicago, Illinois, USA, Nov. 2009: 199-212

[35] Christodorescu M, Sailer R, Schales D L, et al. Cloud Security Is Not(Just) Virtualization Security[C]// The 2009 ACM workshop on Cloud computing security. Chicago, November 2009: 97-102

[36] Garfinkel T, Rosenblum M. When Virtual is Harder than Real: Security Chanllenges in Virtual Machine Based Computing Environments[C]// The 10th Workshop on Hot Topics in Operating Systems. Santa Fe, New Mexico, USA, 2005: 12-15

[37] Oberheide J, Cooke E, Jahanian F. Empirical exploitation of live virtual machine migration[C]// The 11th IFIP/IEEE international conference on Symposium on Integrated Network Mana-

gement. Long Island, New York, 2009: 630-637

[38] Kaufman L M. Can Public-Cloud Security Meet Its Unique Challenges? [J]. IEEE Security and Privacy, 2010, 8(4): 55-57

[39] Dawoud W, Takouna I, Meinel C. Infrastructure as a service security: Challenges and solutions [C] // The 7th International Conference on Informatics and Systems. Cairo, Egypt, March 2010: 1-8

[40] Wei Jin-peng, Zhang Xiao-lan, Ammons G, et al. Managing Security of Virtual Machine Images in a Cloud Environment [C] // The ACM workshop on Cloud computing security. Toronto, Canada, November 2009: 91-96

[41] Wikipedia. [EB/OL]. http://en.wikipedia.org/wiki/Cloud_computing, 2011

[42] Mather T, Kumaraswamy S, Latif S. Cloud Security and Privacy [M]. USA: O'Reilly Media, 2009

[43] Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 [R]. The Cloud Security Appliance, December 2009

[44] Cloud Security Alliance. Top Threats to Cloud Computing (V1.0) [R]. The Cloud Security Alliance, Mar. 2010

[45] 王庆波，金萍，何乐，等. 虚拟化与云计算[M]. 北京：电子工业出版社，2010

[46] 李虹，李昊. 可信云安全的关键技术与实现[M]. 北京：人民邮电出版社，2010

[47] Jung Youngmin, Chung Mokdong. Adaptive security management model in the cloud computing environment [C] // The 12th international conference on Advanced communication technology. Korea, February 2010: 1664-1669

[48] Yu Shu-cheng, Wang Cong, Ren Kui, et al. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing [C] // The 29th conference on Information communications. San Diego, USA, 2010: 1-9

[49] Rohit R, Bharat B, Ben O L, et al. Protection of Identity Information in Cloud Computing without Trusted Third Party [C] // The 29th IEEE Symposium on Reliable Distributed Systems. New Delhi, Punjab, India, 2010: 368-372

[50] Pelin A, Bharat B, Rohit R, et al. An Entity-Centric Approach for Privacy and Identity Management in Cloud Computing [C] // The 29th IEEE Symposium on Reliable Distributed Systems. New Delhi, Punjab, India, 2010: 177-183

[51] Angin P, Bhargava B, Ranchal R, et al. A User-Centric Approach for Privacy and Identity Management in Cloud Computing [C] // The 29th IEEE International Symposium on Reliable Distributed Systems. New Delhi, Punjab, India, 2010: 177-183

[52] Wang Cong, Wang Qian, Ren Kui, et al. Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing [C] // The 29th conference on Information communications. San Diego, USA, 2010: 1-9

[53] Schunter M, Probst C W, Pendarakis D, et al. Security audits of multi-tier virtual infrastructures in public infrastructure clouds [C] // The ACM workshop on Cloud computing security workshop. Chicago, Illinois, USA, 2010: 93-102

[54] Calero J M A, Edwards N, Kirschnick J, et al. Toward a Multi-Tenancy Authorization System for Cloud Services [J]. IEEE Security & Privacy, 2010, 8(6): 48-55

[55] Brandic I, Dustdar S, Anstett T, et al. Compliant Cloud Computing (C3): Architecture and Language Support for User-Driven Compliance Management in Clouds [C] // The 3rd International Conference on Cloud Computing. Miami Marriott, USA, 2010: 244-251

[56] Kandukuri B R, Ramakrishna P V, Rakshit A, et al. Cloud Security Issues [C] // The 2009 IEEE International Conference on Services Computing. Bangalore, India, September 2009: 517-520

[57] de Chaves S A, Westphall C B, Lamin F R. SLA Perspective in Security Management for Cloud Computing [C] // The 6th International Conference on Networking and Services. Cancun, Mexico, March 2010: 212-217

[58] Garfinkel T, Rosenblum M. A Virtual Machine Introspection Based Architecture for Intrusion Detection [C] // The 10th Annual Network and Distributed Systems Security Symposium. California, 2003: 253-285

[59] Ben T G, Pfaff B, Chow J, et al. Terra: A Virtual Machine-Based Platform for Trusted Computing [C] // The 19th ACM symposium on Operating systems principles. New York, USA, 2003: 193-206

[60] Santos N, Gummadi K P, Rodrigues R. Towards Trusted Cloud Computing [C] // The 2009 conference on Hot topics in cloud computing. San Diego, California, 2009: 3

[61] Berger S, Cáceres R, Goldman K, et al. Security for the cloud infrastructure: trusted virtual data center implementation [J]. IBM Journal of Research and Development, 2009, 53(4)

[62] Schiffman J, Moyer T, Vijayakumar H, et al. Seeding Clouds with Trust Anchors [C] // The ACM Workshop on Cloud Computing Security. Chicago, USA, October 2010: 43-48

[63] Centry C. A Fully Homorphic Encryption Scheme [D]. Stanford University, California, September 2009

[64] Jensen M, Schäge S, Schwenk J. Towards an Anonymous Access Control and Accountability Scheme for Cloud Computing [C] // The 3rd International Conference on Cloud Computing. Miami, Florida, USA, 2010: 540-541

[65] Itani W, Kayssi A, Chehab A. Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures [C] //The 8th IEEE International Conference on Dependable, Autonomic and Secure Computing. Chengdu, China, 2009: 711-716

[66] Echeverria V, Liebrock L M, Dongwan S. Permission Management System: Permission as a Service in Cloud Computing [C] // The 34th Annual IEEE Computing Software and Applications Conference Workshops. Seoul, South Korea, July 2010: 371-375

[67] Kirch J. Virtual machine security guidelines [R]. The Center for Internet Security, 2007

[68] Seitz L, Pierson J M, Brunie L. Key Management for Encrypted Data Storage in Distributed Systems [C] // The 2th IEEE International Security in Storage Workshop. Washington, DC, 2003: 20-31

[69] Huang Jianzhong, Xie Changsheng, Cai Bin. Research and Implement of an Encrypted File System Used to NAS [C] // The 2th IEEE International Security in Storage Workshop. Washington, DC, 2003: 1-5

[70] Bakshi A, Dujodwala Y B. Securing Cloud from DDOS Attacks Using Intrusion Detection System in Virtual Machine [C] // The 2th International Conference on Communication Software and Networks. Singapore, February 2010: 260-264

[71] Bonnassieux F, Harakaly R, Primet P. MapCenter: An Open Grid Status Visualization Tool [C] // The 15th International Conference on Parallel and Distributed Computing Systems. Shenzhen, China, 2002: 2-3

（下转第 69 页）

因而有

$$Adv_{\Pi,A}^{ind-atk}(k)=p(1)-p(0)=2p(1)-1=p'(1)-p'(0)$$
$$=Adv_{\Pi,A}^{css-atk}(k)$$

当 $Adv_{\Pi,A}^{css-atk}(k)$ 并非可省略函数时，则有 $Adv_{\Pi,A}^{ind-atk}(k)$。

结束语 在基于对照的框架下对语义安全性进行了形式化表示。统一了语义安全性、不可分辨性的定义框架，针对选择明文攻击、非适应选择密文攻击和适应性选择密文攻击，提供了研究不可分辨性和语义安全性关系的简化表示。接着给出了在新条件下对语义安全性和不可分辨性之间对等性的简单证明。与前述证明相比，这种证明更为简洁易懂，无需定义不可分割性等任何中间对象，即可实现定义框架的统一。

参 考 文 献

[1] Bhatt M, Flahive A, Wouters C, et al. Move: a distributed framework for materialized ontology view extraction[J]. Algorithmica, 2006, 45(3): 457-481

[2] Chandrasekaran B, Josephson J R, Benjamins V R. What are ontologies, and why do we need them? [J]. IEEE Intelligent Systems, 1999, 14(1): 20-26

[3] Wouters C, Dillon T, Rahayu W, et al. Ontologies on the move [C] // Database Systems for Advanced Application. LNCS, Springer Verlag, 2004: 812-823

[4] Bhatt M, Flahive A, Wouters C, et al. A distributed approach to sub-ontology extraction [C] // Advanced Information Networking and Applications (AINA'04). IEEE Society, Japan, 2004: 636-641

[5] Flahive A, Apduhan B O, Rahayu W, et al. Simulating the distributed ontology framework in the semantic grid environment with gridSIM[C] // The 2006 International Conference on Parallel and Distributed Processing Techniques and Applications. CSREA Press, Las Vegas, Nevada, USA, 2006: 717-723

[6] De Roure D, Jennings N, Shadbolt N. The semantic grid: a future e-science infrastructure[C] // Berman F, Hey A J, Fox G, eds. Grid Computing, ch 17. Wiley, 2003: 437-470

[7] Taniar D, Rahayu W. Parallel sort-merge object-oriented collection join algorithms[J]. Computer Systems Science and Engineering, 2002, 17(3): 145-158

[8] Flahive A, Apduhan B O, Rahayu J W, et al. Validating the distributed ontology framework for deployment onto the semantic grid environment[C] // The IEEE International Conference on Parallel and Distributed Systems ICPADS. IEEE Computer Society, 2005(2): 684-688

(上接第 30 页)

[72] Barbera R, Re P L, Sava G, et al. Grid monitoring with NetSaint [R]. Italy: Università di Catania and Istituto Nazionale di Fisica Nucleare (INFN), Italy, 2002

[73] Sailer R, Valdez E, Jaeger T, et al. sHyper: Secure Hypervisor Approach to Trusted Virtualized Systems[R]. Yorktown Heights, New York: IBM Thomas J. Watson Research Center, 2005

[74] Murray D G, Milos G, Hand S. Improving Xen Security through Disaggregation[C] // The 4th ACM SIGPLAN/SIGOPS international conference on virtual execution environments. Seattle, Washington, USA, 2008: 151-160

[75] Seshadri A, Luk M, Qu Ning, et al. SecVisor: A Tiny Hypervisor to Provide Lifetime Kernel Code Integrity for Commodity OSes [C] // The 21th ACM SIGOPS Symposium on Operating Systems Principles. Stevenson, WA, USA, 2007: 335-350

[76] Wang Zhi, Jiang Xuxian, Cui Weidong, et al. Countering Kernel Rootkits with Lightweight Hook Protection [C] // The 16th ACM Conference Computer and Communications Security. Chicago, USA, 2009: 545-554

[77] Payne B D, Carbone M, Sharif M, et al. Lares: An Architecture for Secure Active Monitoring Using Virtualization [C] // The IEEE Symposium on Security and Privacy. Oakland, California, USA, 2008: 233-247

[78] Sharif M, Lee Wenke, Cui Weidong, et al. Secure In-VM Monitoring Using Hardware Virtualizaiton[C] // The 16th ACM Conference on Computer and Communications Security. Chicago, IL, USA, 2009: 477-487

[79] Liu Qian, Weng Chu-liang, Li Ming-lu, et al. An In-VM Measuring Framework for Increasing Virtual Machine Security in Clouds[J]. IEEE Security & Privacy, 2010, 8(6): 56-62

[80] Reimer D, Thomas A, Ammous G, et al. Opening black boxes: Using semantic information to combat virtual machine image sprawl[C] // The 2008 ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments. Seattle, Washington, USA, March 2008: 111-120

[81] Pfaff B, Garfinkel T, Rosenblum M. Virtualization Aware File Systems: Getting Beyond the Limitations of Virtual Disks[C] // The 3rd Symposium on Networked Systems Design & Implementation. San Jose, California, USA, 2006: 353-366

[82] Sailer R, Zhang Xiaolan, Jaeger T, et al. Design and implementation of a TCG-based integrity measurement architecture[C] // The 13th conference on USENIX Security Symposium. San Diego, CA, USA, 2004: 16-32

[83] Trusted Computing Group. PC client specific TPM interface specification (TIS) [R]. Version 1.2, Trusted Computing Group, July 2005

[84] Shi E, Perrig A, Doorn L V, et al. BIND: Fine-grained Attestation Service for Secure Distributed Systems [C] // The 2005 IEEE Symposium on Security and Privacy. Oakland, California, USA, 2005: 154-168

[85] Jaeger T, Sailer R, Shankar U. PRIMA: Policy-Reduced Integrity Measurement Architecture[C] // The 11th ACM symposium on access control models and technologies. Tahoe City, CA, USA, 2006: 19-28

[86] Korthaus R, Sadeqhi A R, Stüble C. A Practical Property-based Bootstrap Architecture[C] // The 2009 ACM workshop on Scalable trusted computing. Hyatt Regency Chicago, IL, USA, 2009: 29-38

[87] McCune J M, Parno B J, Perrig A. Flicker: An Execution Infrastructure for TCB Minimization[C] // The 3rd ACM SIGOPS/EuroSys European Conference on Computer Systems. Glasgow, Scotland, UK, 2008: 315-328

[88] Berger S, Cáceres R, Goldman K A, et al. vTPM: virtualizing the trusted platform module[C] // The 15th Conference on USENIX Security Symposium. Vancouver, B. C., Canada, 2006: 305-320

[89] Kong Jinzhu. A Practical Approach to Improve the Data Privacy of Virtual Machines[C] // the 10th International Conference on Computer and Information Technology. Bradford, UK, 2010: 936-941