IaaS 云安全研究综述

欧阳雪, 徐彦彦

武汉大学测绘遥感信息工程国家重点实验室 武汉 中国 430079

摘要 目前, 在新一代大规模互联网迅猛发展的背景下, 产生的数据量也随之持续增长, 这就导致用户的本地设备难以满足海量数据的存储和计算需求。与此同时, 云计算作为一种经济高效且灵活的模式, 具有易于使用、随用随付、不受时间和空间限制的优势, 彻底改变了传统 IT 基础设施的提供和支付方式, 可以有效解决无限增长的海量信息存储和计算问题。因此, 在没有昂贵的存储成本和计算资源消耗的情况下, 资源有限的用户可以采用云服务提供商(Cloud Service Provider, CSP)为用户提供所期望的服务。其中, 基础设施即服务(Infrastructure as a Service, IaaS)作为云计算的三种服务类型之一, 将虚拟化、分布式计算和网络存储等技术结合, 可以在互联网上提供和租用计算基础设施资源服务(如计算、存储和网络)。故云计算依靠 IaaS 层提供的计算基础设施资源, 使用户不再需要购买额外设备, 从而大大降低使用成本, 同时也为上层服务奠定基础。然而, 随着云计算服务的不断发展, 基于 IaaS 的安全问题引起人们的关注。为了系统了解 IaaS 的安全研究进展和现状, 本文对 IaaS 的安全问题以及学术界和工业界的解决方案进行了详细调查。首先, 本文介绍 IaaS 的相关理论基础并对分析不同类型的云安全威胁。然后, 从学术界现有研究出发, 分析 IaaS 提供的计算、存储和网络服务中存在的安全威胁, 并调查现有的解决方案。此外, 对工业界中云服务提供商的 IaaS 安全服务进行重点调查, 包括数据安全、网络防护和其他安全服务等方面。最终, 展望未来 IaaS 云安全在学术和工业环境中的发展趋势。

关键词 云计算; 云安全; 虚拟化安全; 计算机系统安全; 数据安全

中图法分类号 TP309.2 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2022.09.04

Survey on IaaS Cloud Security

OUYANG Xue, XU Yanyan

State Key Laboratory of Information Engineering in Surveying, Mapping and Remote Sensing, Wuhan University, Wuhan 430079, China

Abstract At present, a new generation of large-scale Internet is emerging at breakneck speed. The amount of data generated continues to expand, making it difficult for local storage devices of users to keep up with the need for vast data storage and computing. In the meantime, cloud computing offers the advantages of being easy to use, pay-as-you-go, and free from time and space constraints. It has fundamentally changed the way traditional IT infrastructure is provisioned and paid for, and it is capable of effectively resolving the problem of infinite growth in massive data storage and computing. As a result, users with limited resources can employ cloud service providers (CSPs) to provide cloud computing services without incurring high storage costs or computational resource consumption. In particular, Infrastructure as a Service (IaaS), one of three cloud computing service models, enables the provision and rental of computing infrastructure resource services (such as compute, storage, and network) over the Internet by combining technologies such as virtualization, distributed computing, and network storage. Thus, IaaS is dependent on the computing infrastructure resources given by the IaaS layer to eliminate the need for users to purchase additional equipment, significantly reducing the cost of use, while also serving as the basis for higher-layer services. However, as cloud computing services continue to grow, IaaS-based security issues are causing concern. To systematically study the present state of security research in IaaS, this paper provides a detailed survey of security challenges in IaaS and solutions in academia and industry. Firstly, this paper introduces the theoretical foundations of IaaS and analyzes various types of cloud security threats. Then, the current research from academics is then utilized to analyze the security risks in the compute, storage, and network services provided by IaaS and to study the existing solutions. In addition, the IaaS security surveys of cloud service providers in the industry are explored, and finally, the direction of future research is discussed.

Key words cloud computing; cloud security; Infrastructure as a Service; virtualization security; data security

通讯作者: 徐彦彦, 博士, 教授, E-mail: xuyy@whu.edu.cn。

本课题得到国家重点研发计划(No. 2021YFB2501100); 国家自然科学基金资助项目(No. 41571426); 武汉市应用基础研究计划项目(No. 2017010201010114)资助。

收稿日期: 2021-09-13; 修改日期: 2021-12-16; 定稿日期: 2022-07-12

1 介绍

自 2006 年“云计算”(Cloud Computing)的概念首次被提出以来, 就受到研究者的广泛关注[1]。本质上, 云计算是一种基于互联网的服务提供模型[2], 从应用层到基础层可以分为三种服务类型: 软件即服务(Software as a Service, SaaS)提供完整软件应用服务; 平台即服务(Platform as a Service, PaaS)提供应用程序的开发环境和资源等服务; 基础设施即服务(Infrastructure as a Service, IaaS)提供底层硬件基础设施部署等服务。

IaaS 作为云计算的三种服务类型之一, 依靠云服务提供商(Cloud Service Provider, CSP), 并根据现有的虚拟化、分布式计算和网络存储等技术为用户提供通用基础设施服务(如计算、存储和网络), 用户基于这些基础设施资源部署需要的中间件和应用软件等。因此, IaaS 可以提供较为完善的基础设施服务, 并成为云计算服务体系的基石。然而, IaaS 的公有云模式是通过公共网络向多个互不信任的用户提供共享资源服务, 这就导致公共云的多租户特性可能出现资源隔离不足或共享信息泄露等问题。一般来说, 攻击者主要是恶意的 CSP 和使用相同 CSP 的恶意用户, 他们通过攻击或占有用户资源的方式来获取用户的数据或获得额外资源服务, 从而影响用户数据的机密性、完整性、可用性和用户与 CSP 之间的合同安全性[3]。

面对 IaaS 云环境产生的安全挑战, 本文首先介绍 IaaS 的相关基础知识和 IaaS 云安全威胁。然后, 从学术界和工业界的角度出发, 重点对 IaaS 提供的计算、存储和网络等服务中存在的安全问题进行具体分析, 并梳理提供的解决方案。最后对未来研究方向进行总结和展望。

2 IaaS 相关基础知识和安全威胁

2.1 IaaS 相关基础知识

IaaS 架构如图 1 所示。可以看出, 物理层主要为 IaaS 提供底层基础硬件资源, 然后虚拟机监视器(hypervisor)管理和整合基础硬件资源, 并进行重新分配虚拟硬件资源来构建多个虚拟机。最后云管理平台对虚拟化资源进行平台统一的调度和管理, 为用户提供完整的 IaaS 服务。IaaS 主要包括计算、存储和网络服务。

计算服务 用户可根据自身业务的计算需求, 向 CSP 弹性租用 hypervisor、虚拟机或服务器, 并通过网络将工作负载迁移进去, 进而提高用户的工作效率。目前国内外 CSP 都提供 IaaS 计算服务, 例如 Amazon AWS 的弹性计算云 EC2[4]、Google Cloud 的 Compute Engine[5]、Microsoft Azure 虚拟机[6]、阿里云服务器 ECS[7]、华为弹性云服务器[8]和百度的智能云服务器 BCC[9]等。

存储服务 在 IaaS 环境下, CSP 可以根据用户的具体使用场景来提供不同的存储设备。根据数据存储服务的差异, 主要分为对象存储、块存储和文件存储。

网络服务 IaaS 的网络服务可以实现云环境下的虚拟网络功能, 并为每个用户建立独立的网络环境来运行虚拟机。根据用户需求, 网络服务可以提供公网网络和私有网络。

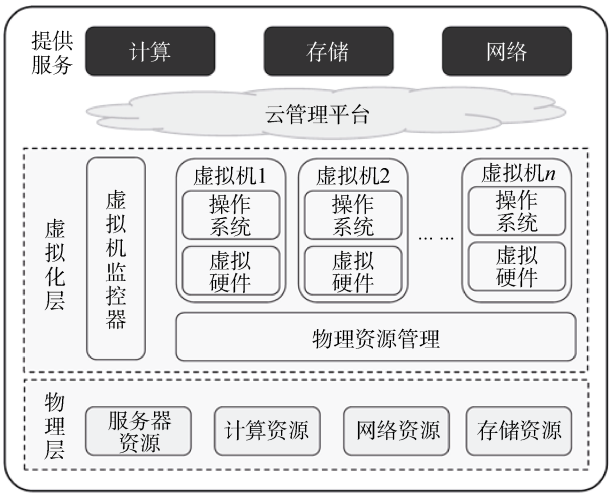

图 1 IaaS 架构
Figure 1 IaaS Architecture

2.2 IaaS 云安全威胁

攻击者针对 IaaS 云平台有两类攻击目标。第一类攻击目标是通过攻击用户的 hypervisor 或虚拟机来获得或破坏用户的资源, 这类攻击者主要是恶意用户或恶意 CSP; 第二类攻击目标是通过攻击 CSP 或用户来获得比服务水平协议(Service Level Agreement, SLA)更多的服务, 这类攻击者主要是恶意用户。其中, 恶意用户指的是租用同一个 CSP 提供设施的用户, 恶意 CSP 包括被攻击者破坏的正常 CSP 和本身具有破坏性的 CSP。

根据以上两类攻击目标, 并以云计算领域的权威机构(CSA[10-11]、ENISA[12]和 NIST[13])的调查为依据, 分析 IaaS 安全威胁, 如表 1 所示, 对安全威胁内容、云安全属性和安全责任进行总结。其中, 这两类攻击的目标都是攻击用户和 CSP 的云安全属性, 即机密性、完整性、可用性和合同安全性[3]。机密性确保 CSP 上使用和存储的用户的数据和数据访问模式

等信息不会被泄露; 完整性确保用户的数据的内容在使用 CSP 后都是一致; 可用性确保用户访问的 CSP 资源是否可以正常使用, 并且如果数据因某种原因而无法访问, 用户可以恢复数据; 合同安全性确保 CSP 按照合同中的服务水平协议诚实而完整地将 IaaS 服务提供给用户。并且, 针对数据层面, 安全威胁包括数据泄露和内部威胁; 针对系统层面, 安全威胁包括缺乏安全架构和策略、不安全的接口和应用程序编程接口(Application Programming Interface, API)以及控制平台薄弱; 针对用户管理层面, 安全威胁有配置错误和变更控制不足和身份信息监控和管理不力; 针对服务层面, 安全威胁有滥用和恶意使用服务和账户劫持。此外, CSP 在 IaaS 云环境中的主要安全责任包括: 1)强制隔离不同用户的虚拟机, 保证不同虚拟机之间的计算过程或内存互相隔离; 2)维护虚拟化基础设施, 保证按时更新和进程保护, 并及时将安全漏洞信息告知用户。同时, 用户在 IaaS 云环境中的主要安全责任包括两个方面[14]: 1)保管自身安全密钥; 2)关注 CSP 的漏洞公告, 及时对存在的安全风险进行处理。

表 1 IaaS 安全威胁总结

(“√”表示云安全属性被破坏或者存在安全责任, 空白则表示尚不具有该项指标)

Table 1 Summary of IaaS security threat

(“√” indicates that the cloud security attributes are compromised, or have safety responsibility, and blank indicates that the indicator is not yet available)

安全层面	安全威胁	威胁内容	云安全属性				安全责任	
			机密性	完整性	可用性	合同安全性	用户	CSP
数据层面	数据泄露	攻击者通过非法访问或恶意攻击等手段获取用户数据	√	√	√		√	√
	内部威胁	内部人员通过内部网络或系统直接访问用户数据	√	√	√	√		√
系统架构层面	缺乏安全架构和策略	攻击者根据 IaaS 的架构和策略的安全漏洞破坏 CSP 并获得用户相关数据	√	√	√			√
	不安全的接口和 API	攻击者根据接口和 API 存在安全漏洞任意调用或篡改用户数据	√	√	√			√
	控制平台薄弱	控制平台包含数据复制、迁移和存储的过程。如果 CSP 管理人员配置错误, 则导致数据泄漏、不可用或损坏	√	√	√			√
用户身份管理层面	配置错误和变更控制不足	用户错误配置 IaaS 环境而导致自身数据被泄露	√	√	√		√	
	身份信息监控和管理不力	如果用户无法妥善管理身份信息, 则攻击者可以轻易获取用户信息	√	√	√	√	√	
服务层面	滥用和恶意使用服务	攻击者向同一租户域的其他用户发动攻击来阻止其正常使用 IaaS 服务	√	√	√			√
	账户劫持	攻击者利用 IaaS 服务窃听用户活动和篡改用户数据	√	√	√		√	√

根据表 1 中不同安全层面的威胁内容可知, IaaS 安全威胁主要针对用户的云安全属性, 所以需要对其安全防御进行重点研究。同时, 合同安全性虽然涉及的安全威胁较少, 但同样需要 CSP 提高并加固 SLA 的可用性和有效性。最后, IaaS 的安全威胁不仅依靠 CSP 关注和保护, 用户也需要提高自身安全意识, 即 CSP 和用户双方都需要共同承担相应责任, 才能有效抵抗攻击者的破坏行为。

3 IaaS 云安全研究

本节首先介绍 IaaS 提供的计算、存储和网络服务中存在的安全威胁, 然后总结学术界提供的解决方案。

3.1 基于计算服务的安全研究

计算服务是 CSP 通过 IaaS 为用户提供计算设备的租用, 主要包括 hypervisor、虚拟机。然而, 攻击者可以利用 IaaS 环境下的多租户特性来影响用户计算服务的正常使用。本节针对以上问题, 对 hypervisor 和虚拟机存在的安全威胁和相应防御手段进行研究。

3.1.1 虚拟机监视器(hypervisor)

虚拟机监视器(hypervisor)主要负责规划、部署和管理虚拟机。然而, 随着 IaaS 的发展, hypervisor 的规模不断扩大, 使其安全性难以得到保证。一旦 hypervisor 出现安全隐患, 则攻击者可以通过 hypervisor 的代码漏洞或破坏其完整性来执行虚拟机逃逸攻击, 从而严重影响 IaaS 的计算服务。例如, 截至 2021 年 1 月, Xen 具有超过 20 万代码行(Lines Of Code, LOC), 而 Xen 所有版本的报告中至少存在 457 处漏洞[15]。面对代码规模日益增大的 hypervisor, 需

要构建新型轻量级 hypervisor 来精简运行操作系统, 从而达到减小 TCB 规模的目的。因此, 针对 hypervisor 的攻击, 典型的防御手段有构建新型轻量级 hypervisor 和保证 hypervisor 的完整性。

针对构建新型轻量级 hypervisor 的研究, 文献[16]基于硬件虚拟化技术新型 hypervisor, 称为 SecVisor。代码上, SecVisor 只包括虚拟化内存管理单元、IO 内存管理单元和物理内存, 而传统的 hypervisor 则包含整个虚拟化系统。同时, 在安全上, SecVisor 确保只有经过用户批准的代码才能执行, 防止攻击者的非法入侵; 文献[17]提出的 TrustVisor 尽管只包含 TrustVisor 和 PAL, 但在实现可信计算的同时保护敏感代码, 使 TrustVisor 成为一种轻量级和高性能的 hypervisor; CloudVisor[18]采用嵌套虚拟化技术将虚拟化的资源管理功能与安全保护功能分开, 使 TCB 的规模大幅下降; 基于微内核的原理, HypSec[19]对现有的 hypervisor 分割成一个小型的可信监视器(称为 corevisor)和一个大型的不可信监视器(称为 hostvisor), 并利用硬件虚拟化技术来隔离和保护 corevisor, 从而保证 HypSec 安全; 此外, 针对数字取证场景, 文献[20]提出的 ForenVisor 删除了与取证场景无关的模块(如设备驱动程序), 从而减小 TCB 的大小。并且 ForenVisor 不使用网络来进行存储, 而是通过本地设备来存储取证数据, 故在保证取证数据完整性的同时也降低了 ForenVisor 被网络攻击的风险。ForenVisor 的研究表明, 在特定的场景下, 通过删减与场景无用的模块来保证 hypervisor 的安全是可行的。表 2 给出了传统 hypervisor(KVM 和 Xen)与文献[16-20]的 TCB 大小比较。

表 2 TCB 大小比较(单位: LOC)

Table 2 TCB size comparison

Hypervisor	LOC	Hypervisor	LOC
KVM	1857575	TrustVisor[17]	7889
Xen	71604	CloudVisor[18]	5500
Xen + Dom0	2054756	HypSec[19]	8566
SecVisor[16]	3526	ForenVisor[20]	1400

针对 hypervisor 完整性的研究, 可以采用防止篡改、探测篡改和完整性度量等手段。为了防止攻击者篡改 hypervisor, HyperSafe[21]采用不可绕过的内存锁定技术来保证 hypervisor 的代码和数据完整; 在探测篡改方面, 文献[22]提出基于硬件辅助的探测篡改框架 HyperCheck 来获取托管虚拟机的完整状态并安全传输到远程服务器。然而, 攻击者可以在获取 hypervisor 的完整状态之前隐藏并清除攻击痕迹, 致使需要一种完整性度量方法来确保被攻击的 hypervisor 无法隐藏攻击痕迹。为了解决这一问题, HyperSentry[23]采用硬件提供的隔离部件来秘密度量 hypervisor 是否完整, 并且 HyperSentry 的秘密性可以确保被攻击 hypervisor 不会隐藏攻击踪迹。此外, 考虑到虚拟机在迁移前需要对迁移 hypervisor 进行完整性度量来判断 hypervisor 是否可信, 文献[24]提出的相邻完整性度量机制来动态监视其相邻 hypervisor 的完整性, 并将度量结果传递给该区域的 TCB 来执行完整性验证。

3.1.2 虚拟机研究

虚拟机是由 hypervisor 创建并运行在客体操作系统的完整计算机系统, 其具有配置快速和维护灵活等特点, 使得用户可以像使用物理计算机一样对虚拟机进行操作。然而, 由于虚拟机的生命周期包括运行(running)、挂起(suspended)、恢复(resume)和关闭(off)等阶段, 这就导致攻击者可以利用虚拟机生命周期的不同阶段的特点来进行攻击, 从而泄露用户信息。因此, 面对虚拟机不同阶段的攻击, 需要研究如何对虚拟机的各个阶段进行安全防护。

1) 运行阶段

在运行状态下, 数据泄漏是虚拟机的主要安全威胁[25], 其中包括针对外部数据泄漏的侧信道攻击(side-channel attacks)和针对内部数据泄漏的隐蔽信道攻击(covert channel attacks)。

侧信道攻击是通过在虚拟机的密码运行进程中产生的与敏感信息相关的侧信道信息来恢复密钥, 这些侧信道信息包括时间、功率消耗和电磁场等暴露在外部的数据。此外, 在侧信道攻击中, 由于在使用相同物理资源的不同用户的虚拟机进程之间频繁交互, 故攻击者采用高速缓存存储器来探测当前运行的目标虚拟机的加密操作和操作执行状态, 从而推断目标虚拟机产生的密钥[26]。针对侧信道攻击, 主要防御手段有加密通信过程、防止攻击者获得虚拟机的进程访问信息、及时检测攻击行为和重新分配信道等。

文献[27]对涉及高速缓存的通信过程进行加密, 保证在高速缓存上运行的数据都以密文形式传输, 从而避免虚拟机在运行阶段产生数据泄漏。为了防止攻击者获得虚拟机进程访问信息, 文献[28]定期向高速缓存信道添加随机噪声, 使攻击者无法读取目标虚拟机的访问信息; 文献[29]提出的 XenPump 方案通过随机延迟的方式混淆高速缓存侧信道中的虚拟机进程访问时间, 使攻击者无法准确获得进程访问信息。为了及时检测高速缓存侧信道攻击行为, 文

献[30]基于“FLUSH+RELOAD”技术来检测高速缓存侧信道攻击, 并在发现攻击后在同一操作系统中清除可疑的虚拟机进程; HomeAlone[31]通过设置自身的虚拟机不会使用某些高速缓存行, 然后测量进程运行期间的高速缓存数据的变化情况。一旦 HomeAlone 发现没有使用的高速缓存行发生变化, 则表明存在恶意虚拟机。此外, 为了防止虚拟机之间无法共用高速缓存行, 文献[32]将互不信任的用户分配到不同的 CPU 或内存, 从而保证用户在不同的信道下的高速缓存不会重叠并防止用户信息泄露; 文献[33]使用 hypervisor 来控制内存映射, 使得无论虚拟机进程访问高速缓存数据的顺序如何变化, 受保护的敏感信息都能可以留在高速缓存行中并无法通过进程变化进行清除。

由于虚拟机内部存在隔离缺陷, 致使存在一种隐蔽信道允许双方进行内部通信。与侧信道攻击不同, 侧信道攻击不需要通信双方合谋, 而隐蔽信道攻击必须由通信双方合谋才能实现数据的传输。在隐蔽信道攻击中, 攻击者首先利用缓冲区溢出和虚拟机镜像污染等手段将合谋者放入到目标虚拟机并获取秘密信息, 然后通过隐蔽信道把目标虚拟机的信息传输给攻击者。因此, 隐蔽信道攻击在传输过程中难以被监视系统(如防火墙、入侵检测系统和网络流量日志等)所察觉, 从而增加抵御攻击的难度。针对隐蔽信道攻击, 主要防御手段有减弱隐蔽信道攻击、检测攻击行为和破坏隐蔽信道中的信息等。

为了减弱隐蔽信道造成的虚拟机数据泄漏, 文献[34]限制 Xen 虚拟机的进程响应时间, 保证目标进程没有运行结束时, 攻击进程得不到调度, 从而减弱基于高速缓存的隐蔽信道攻击。在检测隐蔽攻击方面, 文献[35]假设在 GPU 上同时运行的应用程序中包含攻击应用程序, 并采用提出的 GPUGuard 方法来检测两个应用程序的内核之间是否存在合谋行为。一旦发现合谋行为, 则将可疑内核重新分配到一个独立的安全域中。因此, GPUGuard 可以有效抵御基于 GPU 的隐蔽攻击, 从而保护用户虚拟机的安全; ReplayConfusion[36]用于检测基于高速缓存的隐蔽信道攻击, 即通过记录不同程序运行的高速缓存来确定是否存在攻击行为。如果检测到用户信息泄漏, 就可以有效阻止攻击者的攻击行为。为了破坏隐蔽信道中的信息, 文献[37]针对基于内存共享的隐蔽信道提出随机共享方案。该方案通过随机合并不同虚拟机中的相同内存页, 可以保证即使在隐蔽信道攻击下, 接收方也无法准确知道发送方写入哪些内存页, 使得攻击者无法获取隐蔽信道正在传输的信息, 从而保证用户虚拟机的安全。

2) 挂起和恢复阶段

在挂起和恢复阶段, 攻击者通过虚拟机回滚攻击(VM rollback attack)在用户不知情的情况下恢复快照并运行虚拟机[38], 使用户虚拟机被恶意破坏并泄露用户数据。

虚拟机回滚攻击分为两种攻击方式: 1)攻击者通过穷举攻击猜测目标虚拟机的登录密码。即使目标虚拟机会限制错误输入密码次数, 但攻击者仍然可以在每次输入密码后将虚拟机无限回滚到初始状态来清除虚拟机内的计数器; 2)攻击者通过回滚权限控制模块来撤消用户的更改权限, 从而将目标虚拟机的信息公开给攻击者。针对虚拟机回滚攻击, 主要防御手段有禁用挂起/恢复机制和判断挂起/恢复阶段的安全性等。

文献[39]提出的 HyperWall 机制通过禁用挂起和恢复机制来保障虚拟机的安全, 使攻击者无法通过虚拟机回滚攻击来获得目标虚拟机信息, 但是该方法在禁用的同时也使某些虚拟机常规操作(如快照或虚拟机迁移等)无法正常使用。此外, 为了判断挂起和恢复阶段的安全性, 文献[40]对用户虚拟机所有回滚行为都记录下来, 用户可以根据记录来判断回滚期间是否存在恶意行为; 文献[41]提出通过使用可信 hypervisor 来确保计数器只能是递增状态, 使得攻击者无法通过穷举攻击来获取用户虚拟机的登入密码, 从而有效抵御虚拟机回滚攻击。

3) 关闭阶段

在关闭阶段, 虚拟机执行的迁移操作可以将虚拟机内运行的操作系统和应用程序从一个物理位置迁移到另一个物理位置, 从而实现虚拟机负载平衡、灾难恢复和硬件维护的目的[42]。虚拟机迁移可以分为两种操作类型, 即离线迁移和实时迁移。其中, 离线迁移是在虚拟机完全关闭情况下通过网络进行迁移; 实时迁移与离线迁移的步骤几乎一致, 但在线迁移的迁移过程仅有短暂的虚拟机关闭时间, 以确保在迁移过程中 IaaS 服务仍具有可用性。

然而, 由于迁移策略不完善或者迁移数据未加密, 导致攻击者可以采用拒绝服务(Denial of Service, DoS)攻击和中间人(Man In The Middle, MITM)攻击来破坏迁移虚拟机。在 DoS 攻击中, 攻击者在主机操作系统上创建许多虚拟机, 致使主机操作系统过载并无法再接受任何迁移的虚拟机, 从而降低达到用户服务的可用性并增加攻击者获得额外虚拟资源服务的目的。此外, 由于在虚拟机迁移过程中所有迁移的数据都默认以明文的形式传输, 导致攻击者可

以利用传输网络将自身置于传输信道中, 并使用迁移目标欺骗和 DNS 中毒等手段执行中间人攻击, 从而截获到用户的敏感数据[43]。因此, 为了确保虚拟机迁移期间的安全性, 防止攻击者获取任何敏感信息, 主要防御手段有设定迁移条件和加密迁移期间的数据。

针对虚拟机在迁移过程中的DoS攻击, 文献[44]提出满足以下三个迁移条件才能迁移虚拟机: 根据检测物理主机的网络状态来选择迁移虚拟机、根据设置的迁移时间阈值来选择迁移时间以及根据迁移主机的带宽利用率来选择迁移目的主机。基于以上三个迁移条件, 用户虚拟机可以从被 DoS 攻击的主机上迁移到其他正常的主机上, 从而有效减轻 DoS 攻击的影响; 文献[45]提出虚拟机迁移过程中的安全需求, 即平台间认证、传输数据的保护和虚拟可信根的保护; 文献[46]分析虚拟机实时迁移需要满足安全和性能要求, 其中安全要求包括迁移虚拟机的机密性和完整性得到保证, 并且只有可信实体才能提出迁移请求和接收正确的虚拟机, 性能要求指的是尽可能缩短虚拟机的停机时间和迁移时间以提高服务可用性。此外, 为了加密迁移期间的数据, 文献[47]基于属性认证和可信信道来确保迁移数据以密文的形式进行安全传输, 从而保证传输数据的机密性和完整性; 文献[48]对验证合法的迁移虚拟机使用AES加密对迁移数据进行加密; 文献[49]基于可信平台模块(Trusted Platform Module, TPM)提出一种基于角色的迁移机制, 其中迁移虚拟机采用 TPM 私钥对迁移数据进行加密, 并以密文的形式向目标虚拟机进行身份认证, 如果认证成功则同意迁移。该方法可以有效抵御中间人攻击, 保证虚拟机在迁移过程中的通信安全。

表 3 依据 hypervisor 和虚拟机生命周期的不同阶段, 对攻击实例、攻击效果、抵御攻击原理和抵御方案进行归纳总结。可以看出, 由于 hypervisor 存在大规模代码和和缺乏完整性等问题, 使得攻击者可以利用虚拟机逃逸攻击来窃取非法权限。因此, 可以通过构建新型轻量级 hypervisor 和保证 hypervisor 的完整性手段来实现 hypervisor 的安全。此外, 攻击者为了窃取用户虚拟机的数据或获得额外的 IaaS 服务资源, 可以根据虚拟机生命周期的各个阶段的特点来分别执行相应的攻击, 使其干扰用户虚拟机的正常服务, 并严重影响用户数据的机密性、完整性和可用性。为了解决不同阶段的安全问题, 在未来的研究中需要全面关注虚拟机在整个生命周期的保护以保证用户使用虚拟机的安全性和可靠性。

表 3 基于 hypervisor 和虚拟机生命周期的不同阶段的安全研究

Table 3 Security study based on different phases of hypervisor and virtual machine lifecycle

攻击对象		攻击实例	攻击效果	抵御攻击手段	抵御方案
Hypervisor		虚拟机逃逸攻击	获取或篡改宿主机的数据和在宿主机上的全部虚拟机运行状态	构建新型轻量级 hypervisor	文献[16-20]
				保证 hypervisor 的完整性	文献[21-24]
虚拟机	运行阶段	侧信道攻击、隐蔽信道攻击	泄露用户虚拟机相关数据	加密通信过程、防止攻击者获得虚拟机进程访问信息、及时检测攻击和重新分配信道	文献[27-33]
				减弱隐蔽信道攻击、检测攻击行为和破坏隐蔽信道中的信息	文献[34-37]
	挂起和恢复阶段	虚拟机回滚攻击	破坏用户虚拟机的正常使用和泄露用户数据	禁用挂起和恢复机制、判断挂起和恢复阶段的安全性	文献[38-41]
	关闭阶段	DoS 攻击、中间人攻击	影响虚拟机安全迁移	设定迁移条件	文献[44-46]
				对迁移期间的数据加密	文献[47-49]

3.2 基于存储服务的安全研究

IaaS 的存储服务是由 CSP 所提供, 用户可以通过外包的方式将数据传输到 CSP 的云存储服务器, 并在不同终端上访问数据, 从而实现数据的存储和共享。然而, 存储服务在用户提供便利的同时, 也存在以下的安全问题:

(1) 由于 CSP 具有“诚实但好奇”的特点[50], 导致 CSP 在提供数据存储服务的同时可能也会查看、删除甚至泄露用户数据;

(2) CSP 出现设备故障而导致用户数据丢失;

(3) 恶意攻击者通过攻击 CSP 的云存储服务器来获取用户数据。

为解决因存储服务造成的数据泄露问题, 在技术方面, 用户需要在外包之前对数据进行加密, 但加密在保障数据的安全性同时会对密文检索和共享造成不便[50]。因此, 为保证用户存储在 CSP 上的数据不被泄露, 可以采用代理重加密[51-53]、属性基加密(Attribute-Based Encryption, ABE)[54-56]、可搜索加密(Searchable Encryption, SE)[57-59]和可信平台模块TPM[60-62]等手段实现安全存储。

表 4 针对 IaaS 的安全存储服务进行总结, 其中包括解决方法、实现过程、抵御方案、实现效果以及存在问题。可以看出, 不同的解决方法从软件到硬件都能实现用户在密文域下的高效检索和共享, 但也存在一些问题和限制。针对这些问题和限制, 如何进行改进以实现 IaaS 数据安全性和可用性之间的平衡将是今后研究的重点。

3.3 基于网络服务的安全研究

由于 IaaS 具有“虚拟隔离、物理共存”的特点, 使 IaaS 环境下的攻击行为是在 hypervisor 或虚拟机的内部进行。因此针对外部防御的传统计算机网络安全隔离机制(如物理防火墙等)不适用于 IaaS 环境。因此需要采用新的方式来构建虚拟网络基础设施来保证虚拟机之间的安全通信。

针对 IaaS 环境下虚拟化网络中的安全问题, 主要的防御手段有虚拟防火墙(virtual firewall)[63-65]、入侵检测系统(Intrusion Detection System)[66-69]和设计安全虚拟网络机制或框架[70-72]。表 5 归纳了网络服务存在的安全问题、解决思路、解决方案以及实现效果。可以看出, 虚拟网络服务的安全研究可以通过防御手段以一种新的方式保证虚拟机之间的安全通信, 从而为用户的网络服务提供技术保障。

表 4 存储服务的安全研究

Table 4 Security study of storage services

解决方法	实现过程	抵御方案	实现效果	存在问题
代理重加密	允许第三方代理将发送方的可解密密文转换为接收方的可解密密文, 同时代理不知道任何有关明文的信息	文献[51-53]	允许在不同域之间转换密文	对于不可信的代理会造成密钥和明文信息泄露
属性基加密	加密方无需关注解密方身份, 只定义解密方的属性即可	文献[54-56]	解决解密方变化导致频繁更改密钥的问题	没有提供属性撤销机制; 密钥管理困难
可搜索加密	用户向云服务器提交搜索查询, 服务器可以用相应数据进行响应	文献[57-59]	服务器不知道数据内容, 只需了解搜索结果	关键字猜测攻击
可信平台模块(TPM)	提供加密操作、生成随机数和哈希函数	文献[60-62]	能够抵抗各种软件攻击	成本较高

表 5 虚拟网络服务的安全研究

Table 5 Security study of virtual web services

存在问题	解决思路	解决方案	实现效果
传统的基于计算机网络安全隔离机制不适用于 IaaS 环境	虚拟防火墙	文献[63-65]	为用户提供网络防火墙服务, 即数据包过滤和监视等
	入侵检测系统	文献[66-69]	即时监视网络传输, 并在发现可疑传输时发出警报或采取反应措施
	设计安全虚拟网络机制或框架	文献[70-72]	实现虚拟机安全网络通信

4 工业界的 IaaS 云安全实际解决方案

现有学术研究在探索 IaaS 安全的同时, 工业界在也提供了实际 IaaS 云安全实际解决方案。由于 CSP 不仅需要确保用户使用安全的虚拟机, 而且还要提供相应的安全服务。因此, 本节针对 CSP 厂商在数据安全、网络防护和其他安全服务等方面提供的安全服务进行简要介绍, 包括 Amazon AWS、Google Cloud、Microsoft Azure、阿里云、华为云和百度云。

4.1 计算安全

当前, CSP 提供的计算服务主要是外租虚拟机或云服务器。然而, 如果 CSP 提供的虚拟机或云服务器没有设置相关的安全防护, 则可能受到病毒入侵或外部攻击, 导致数据泄露或丢失, 影响用户的正常使用。

为了防止虚拟机或云服务器免受攻击或病毒入侵, AWS 提供的 EC2 云服务器使用 AWS Nitro 系统, 该系统包含轻量级的 Hypervisor 和安全芯片。通过 Nitro 系统, EC2 云服务器上的虚拟化资源会自动卸载到专用硬件和软件中, 从而最大限度减少攻击面; Google Cloud 提供的 Compute Engine 是在 Google 的数据中心运行的虚拟机, 该虚拟机提供默认使用庇护式虚拟机(Shielded VM)和统一可延伸固件接口(Unified Extensible Firmware Interface, UEFI)使虚拟机具备纵深防御能力, 可以不受恶意攻击者的系统固件、UEFI 扩展和驱动程序攻击, 也能避免虚拟机的数据泄露和重放攻击; Azure 提供的虚拟机使用来

自 Microsoft 和 McAfee 等大型安全性供应商的安全软件来保护虚拟机免受恶意文件、恶意软件和其他威胁的侵害; 阿里云的云服务器 ECS 的安全最佳实践为用户提供账号安全管理和云盘加密等功能, 为云基础设施提供安全保障; 华为云提供的弹性云服务器 ECS 的安全保障是由应用防火墙和漏洞扫描等安全服务提供, 并且 ECS 提供对用户云环境的安全评估, 可以帮助用户快速发现安全弱点和威胁, 从而有效减少恶意攻击带来的损失; 百度云的云服务器 BCC 的防入侵解决方案可以有效抵御黑客攻击, 并及时发现并有效抵御黑客攻击。

4.2 存储数据安全

随着用户数量的增长, CSP 对数据安全的重视程度不断提高。为了保护用户存储在 CSP 上的数据, Amazon AWS 提供一项完全管理的数据安全和数据隐私服务, 称为 Amazon Macie。该服务利用机器学习和模式匹配来发现和保护存储在 AWS 中的敏感数据。用户可以直接在 Macie 中查看敏感数据, 并且可以配合其他服务进行监视和处理, 从而降低数据保护的成本; Google Cloud 提供的 VPC Service Controls 是通过隔离不同租户的 Google Cloud 服务的资源来降低数据泄露的风险, 并确保只有授权的用户才能访问敏感数据; 华为云的专属加密服务是对用户的敏感数据进行加密来确保数据的安全性; 此外, 阿里云提供的敏感数据保护服务是根据用户预先定义的敏感数据来扫描存储在阿里云中的数据, 并通过敏感数据规则对数据进行分级和检测, 从而防止敏感数据被非法访问。

4.3 网络防护

在 IaaS 环境中, CSP 所提供的服务是否可靠直接依赖于网络的安全性, 这就导致单纯依靠身份验证来防止攻击者假冒其他合法用户是远远不够的。因此, 为提供安全的网络服务, CSP 主要在分布式拒绝服务攻击(Distributed Denial of Service attack, DDoS)防护、虚拟防火墙和网络检查等方面提供相应服务。

1) DDoS 防护

在 DDoS 攻击中, 攻击者将网络上多个被攻陷的服务器或虚拟机作为攻击机器, 并同时通过网络向目标用户发动攻击, 从而迫使用户无法使用服务。为了避免用户在使用 IaaS 服务时被 DDoS 攻击勒索, 需要一种持续防护 DDoS 攻击的服务来确保网络的稳定性。例如, AWS 提供 AWS Shield 是一种托管式 DDoS 防护服务, 可以提供网络流量持续监控。AWS Shield 可以检测所有传入到 AWS 服务的流量, 并及时发现恶意流量。此外, 当用户的服务器或虚拟机受到大流量 DDoS 攻击时, 华为云的 DDoS 高防服务可以保证用户的服务仍然可以持续使用。DDoS 高防服务的原理是将用户的服务域名替换成高防 IP, 并让所有访问都经过高防 IP 进行过滤, 从而实现网络的有效检测和过滤恶意流量, 降低 DDoS 攻击风险。

2) 虚拟防火墙

在虚拟防火墙防护方面, Azure 防火墙不仅可以保护 Azure 虚拟网络资源, 为所有可能存在的安全威胁进行筛选, 而且可以提醒用户拒绝恶意 IP 地址; 类似地, AWS 提供的 AWS Network Firewall 为用户 Amazon 虚拟私有云部署必要的网络保护。该服务提供网络筛选, 可以实现停止恶意流量和监控域名的效果, 并且用户可以灵活定义防火墙规则以便对网络流量进行管理和控制。

3) 网络检查

CSP 不仅需要提供相关的网络防护服务, 还要对网络进行有效检查和及时修复来保证用户使用的 IaaS 网络服务的安全性和稳定性。例如, Google Cloud 提供的 Network Telemetry 是一种用户网络监控、取证和安全保障的服务。Network Telemetry 可以实时识别可能具有风险的流量和访问模式, 并为 Google Cloud 网络服务迅速提供响应日志; 同理, 百度云提供的安全检测服务能够检测出多种常见的网络漏洞, 然后快速帮助用户发现网络中存在的问题并及时帮助用户修复漏洞。

4.4 服务安全

CSP 除了保证数据和网络安全, 还需要提供用户使用 IaaS 服务的安全服务, 包括用户密钥保护、用户身份安全、应急响应和地理位置存储安全等。

1) 用户密钥保护

用户密钥包括 API 密钥、密码和加密密钥等。CSP 对用户密钥的管理有以下挑战: (1)用户和 CSP 对密钥所有权的掌握; (2)对密钥管理系统(Key Management System, KMS)和受保护资源所在基础设施的访问控制。为解决以上挑战, Azure 提供的 Key Vault 服务通过控制访问策略对用户的密钥保管库进行身份授权和验证, 从而防止其他人获得相关密钥; AWS 提供的 KMS 服务可以让用户对密钥的生命周期和权限进行集中控制, 使得用户可以随时创建和管理密钥的使用权限, 并定时更换 KMS 的主密钥来防止密钥泄露; 阿里云提供的 KMS 服务则是先将用户保存在 KMS 的密钥进行加密然后进行存储。当用户使用密钥时, 先获取存储在 KMS 的密钥再进行解密使用。因此, 加密操作可以让攻击者难以直接获取到用户密钥, 保证用户密钥的安全性。

2) 用户身份安全

CSP 都会为用户提供密码来识别其身份, 同时使用访问控制进一步实现用户对资源的统一管理。例如, AWS 利用单点登录(Single Sign-On, 简称 SSO)来集中管理多个 AWS 账户和应用程序的访问, 并为用户创建、分配和管理权限; 类似地, 阿里云的访问控制服务采用 SSO 来指定不同的角色进行访问, 并通过集中控制用户的访问权限和存储资源来实现用户身份的管理和授权; 此外, Google Cloud 提供的 Titan 安全密钥是一种硬件芯片, 用于对用户账号实现多重身份验证, 即要求用户通过自己已知的信息(如密码)和拥有的信息(如硬件实体密钥或访问代码)来同时验证其身份。该验证方法可以保证用户的身份信息即使被攻击者窃取也无法访问其账号。

3) 应急响应

当发生黑客入侵和木马病毒等威胁用户安全的事件时, 应急响应能够提供应对和分析事件的服务, 从而降低安全事件所带来的影响与损失。例如, 百度云和阿里云的应急响应服务范围包含网络的非法攻击和病毒入侵等破坏事件, 并及时发现造成破坏的隐患, 从而有效记录和处理事件以及跟踪后续的安全状况; 此外, 华为云提供的态势感知服务能够检测安全风险, 并还原攻击历史、感知攻击现状和预测攻击态势。用户可以通过该服务查询和查看安全态势数据, 并获取安全威胁的处理建议。

4) 地理位置存储安全

由于 CSP 数据中心和用户所在的地理位置有所不同, 导致不同地理位置的用户使用同一个 CSP 服务的带宽也有所差异。因此, 多数 CSP 会在多个地理区域上部署服务区, 保证不同位置的用户可以根据就近原则选择服务区, 从而提高 IaaS 速度。同时, CSP 还可以拦截和阻断指定的国家和地区的来源 IP, 从而避免用户被该地区的恶意骚扰。

表 6 总结了不同 CSP 提供的 IaaS 安全服务。可以看出, CSP 在计算安全、数据安全、安全防护和安全服务方面分别提供不同类型的服务。例如, 在计算安全上, 采用现有系统、软件和解决方案等手段; 在数据保护上, 采用隔离、分类和加密等手段; 在身份安全的保护上, 采用 SSO、多重身份认证和统一身份认证等手段; 此外, 在用户密钥保护、DDoS 防护、虚拟防火墙、网络检查、应急响应和地理存储安全方面, CSP 已达成共识。总而言之, 工业界的 IaaS 安全服务基本达成一致, 并且在此基础上开发出一些额外功能来满足用户的其他需求, 从而保证用户的云安全属性。

表 6 CSP 提供的 IaaS 安全服务总结

Table 6 Summary of IaaS security services by CSP

安全服务 / CSP	计算安全	数据安全		网络防护			服务安全			云安全属性			
		敏感数据保护	用户密钥保护	DDoS 防护	虚拟防火墙	网络检查	身份安全	应急响应	地理位置存储安全	机密性	完整性	可用性	安全合同性
AWS	AWS Nitro 系统	√	√	√	√	√	SSO	√	√	√	√	√	√
Google Cloud	庇护式虚拟机和 UEFI	√	√	√	√	√	SSO	√	√	√	√	√	√
Azure	安全软件	√	√	√	√	√	多重身份验证	√	√	√	√	√	√
阿里云	安全最佳实践	√	√	√	√	√	多重身份验证	√	√	√	√	√	√
华为云	应用防火墙、漏洞扫描和安全评估	√	√	√	√	√	统一身份验证	√	√	√	√	√	√
百度云	防入侵解决方案	√	√	√	√	√	统一身份验证、SSO	√	√	√	√	√	√

5 总结和展望

IaaS 作为云计算的重要服务类型之一, 负责提供较为完善的基础设施服务, 如今已被广泛关注和使用。本文围绕 IaaS 的安全挑战, 旨在从学术界的研究和工业界解决方案两个方面对目前 IaaS 安全研究和实践进行系统的分析。通过分析可知 IaaS 云存在多种安全威胁, 而现有学术研究和工业界尚未完全的解决所有的问题。因此, 结合当前的研究进展, 未来的工作可以关注以下几点。

(1) 需要在 hypervisor 和虚拟机的体系结构中进行标准化设计。由于虚拟化技术的安全缺陷是显而易见的, 例如虚拟机逃逸攻击、虚拟机同驻下的高速缓存侧信道攻击和隐蔽信道攻击、虚拟机回滚攻击

等, 这就导致在实际应用时, 需要采用不同的解决方法来抵御恶意攻击, 使得构建 IaaS 安全环境非常困难。因此, 为了给用户提供安全的 IaaS 云环境, 需要对 hypervisor 和虚拟机进行标准化的安全设计来解决其存在的安全问题, 其中包括: 在确保 hypervisor 完整性的同时, 通过不同用户的具体需求来有效缩减其代码规模, 使 hypervisor 达到轻量级的同时也具备可用性和隐私性。并且为保证虚拟机生命周期的安全, 需要对虚拟机不同阶段的攻击进行全方面防护。

(2) 解决安全加密存储方案存在的缺陷。由于在 CSP 提供的存储服务承载了大量用户的数据, 使得用户的信息泄漏带来诸多威胁。加密技术是实现用户数据隐私保护的主要解决手段。常见的加密方案如代理重加密、属性加密等可以为用户提供安全有效的数据存储和共享, 但这些方案可能存在密钥泄露和用户数据携带恶意信息等问题。因此, 云服务器需要考虑如何安全管理用户密钥以及识别和拦截恶意信息成为研究重点。同时, 为减轻计算资源受限的用户的计算量, 设计轻量级的密文检索加密方案以实现 IaaS 安全存储服务和数据可用性之间的平衡是当前学术研究迫切需求。

(3) 在 IaaS 网络安全设计时需要考虑全面部署防御设施问题。IaaS 云环境中的资源共享、多租户、动态性等特性使传统单纯以物理防火墙等安全网络隔离机制方式失效。因此, 在为 IaaS 环境构建安全的虚拟网络防御体系时, 不仅需要考虑物理和虚拟环境的相互隔离, 还要考虑多租户场景中的动态网络资源分配, 从而全面防止任何非法访问和入侵。

(4) 需要提高 CSP 自身安全机制。尽管用户与 CSP 之间签订的合同可以为用户提供法律和经济保护来免受威胁, 但在工业界中, CSP 会默认其自身内部和提供的服务是安全的, 并且严格遵照 SLA 为用户提供保障, 这就导致 CSP 很少披露其内部安全和提供服务的缺陷。此外, CSP 不会向用户提供任何技术证明, 使用户无法验证或确定 CSP 是否真正和完整地提供满足用户期望的服务。因此, 需要提高 CSP 自身安全机制的透明度来更好的保障其合同安全性, 如漏洞扫描、威胁检测和日志收集等服务。

(5) 学术研究与工业 IaaS 云部署结合。目前, 学术界针对 IaaS 云安全提供大量的解决方案, 但很少实际转移到工业界 IaaS 环境中。因此, 通过工业界产生的实际问题与学术研究提供解决方案结合起来, 可以大力推动 IaaS 云安全的发展。

总之, IaaS 服务的安全不仅需要从技术层面全方位抵御各个攻击, 更需要在法律法规和行业标准化等方面进行严格制定和有效监督, 从而维护 IaaS 服务的健康发展。

参考文献

[1] 中国信息通信研究院. 云计算发展白皮书[R].2019.

[2] Wu J Y, Shen Q L, Zhang J L, et al. Cloud Computing: Cloud Security to Trusted Cloud[J]. *Journal of Computer Research and Development*, 2011, 48(S1): 229-233.
(吴吉义, 沈千里, 章剑林, 等. 云计算: 从云安全到可信云[J]. *计算机研究与发展*, 2011, 48(S1): 229-233.)

[3] Huang W, Ganjali A, Kim B H, et al. The State of Public Infrastructure-As-a-Service Cloud Security[J]. *ACM Computing Surveys*, 2015, 47(4): 1-31.

[4] Amazon. EC2 云服务器/云主机[EB/OL]. https://www. amazonaws.cn/ec2/?nc2=h_ql_prod_cp_ec2.

[5] Google. Google Cloud Compute Engine[EB/OL]. https://cloud.google.com/compute.

[6] Azure. 虚拟机[EB/OL]. https://azure.microsoft.com/zh-cn/ services/virtual-machines/.

[7] 阿里云. 云服务器 ECS[EB/OL]. https://cn.aliyun.com/ product/ecs.

[8] 华为云. 弹性云服务器 ECS[EB/OL]. https://www.huaweicloud.com/product/ecs.html.

[9] 百度智能云. 云服务器 BCC[EB/OL]. https://cloud.baidu.com/product/bcc.html.

[10] 国际云安全联盟. Top Threats to Cloud Computing: Egregious Eleven Deep Dive[R].2020.

[11] 国际云安全联盟. 云计算关键领域安全指南 V4.0[R].2017.

[12] Catteddu D. Cloud Computing: Benefits, Risks and Recommendations for Information Security[C]. *Web Application Security*, 2010: 17.

[13] Mell P M, Grance T. The NIST definition of cloud computing[R]. National Institute of Standards and Technology, 2011.

[14] 中国信息通信研究院云计算与大数据研究所. 云计算安全责任共担白皮书[R].2020.

[15] CVE. Search Results[EB/OL]. http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Xen.

[16] Seshadri A, Luk M, Qu N, et al. SecVisor: A Tiny Hypervisor to Provide Lifetime Kernel Code Integrity for Commodity OSes[C]. *The twenty-first ACM SIGOPS symposium on Operating systems principles - SOSP '07*, 2007: 335-350.

[17] McCune J M, Li Y L, Qu N, et al. TrustVisor: Efficient TCB Reduction and Attestation[C]. *2010 IEEE Symposium on Security and Privacy*, 2010: 143-158.

[18] Zhang F Z, Chen J, Chen H B, et al. CloudVisor: Retrofitting Protection of Virtual Machines in Multi-Tenant Cloud with Nested Virtualization[C]. *The Twenty-Third ACM Symposium on Operating Systems Principles*, 2011: 203-216.

[19] Li S, Koh J S, Nieh J. Protecting Cloud Virtual Machines from Hypervisor and Host Operating System Exploits[C]. *28th USENIX Security Symposium*, 2019: 1357-1374.

[20] Qi Z W, Xiang C C, Ma R H, et al. ForenVisor: A Tool for Acquiring and Preserving Reliable Data in Cloud Live Forensics[J]. *IEEE Transactions on Cloud Computing*, 2017, 5(3): 443-456.

[21] Wang Z, Jiang X X. HyperSafe: A Lightweight Approach to Provide Lifetime Hypervisor Control-Flow Integrity[C]. *2010 IEEE Symposium on Security and Privacy*, 2010: 380-395.

[22] Zhang F W, Wang J, Sun K, et al. HyperCheck: A Hardware-AssistedIntegrity Monitor[J]. *IEEE Transactions on Dependable and Secure Computing*, 2014, 11(4): 332-344.

[23] Azab A M, Ning P, Wang Z, et al. HyperSentry: Enabling Stealthy In-Context Measurement of Hypervisor Integrity[C]. *The 17th ACM conference on Computer and communications security*, 2010: 38-49.

[24] Wu T, Yang Q S, He Y P. A Secure and Rapid Response Architecture for Virtual Machine Migration from an Untrusted Hypervisor to a Trusted one[J]. *Frontiers of Computer Science*, 2017, 11(5): 821-835.

[25] Jin X, Wang Q X, Li X, et al. Cloud Virtual Machine Lifecycle Security Framework Based on Trusted Computing[J]. *Tsinghua Science and Technology*, 2019, 24(5): 520-534.

[26] Younis Y A, Kifayat K, Shi Q, et al. A New Prime and Probe Cache Side-Channel Attack for Cloud Computing[C]. *2015 IEEE International Conference on Computer and Information Technology*; *Ubiquitous Computing and Communications*; *Dependable*, *Autonomic and Secure Computing*; *Pervasive Intelligence and Computing*, 2015: 1718-1724.

[27] Zhang Y T, Gao L, Yang J, et al. SENSS: Security Enhancement to Symmetric Shared Memory Multiprocessors[C]. *11th International Symposium on High-Performance Computer Architecture*, 2005: 352-362.

[28] Liu F, Ren L F, Bai H T. Mitigating Cross-VM Side Channel Attack on Multiple Tenants Cloud Platform[J]. *Journal of Computers*, 2014, 9(4): 1005-1013.

[29] Wu J Z, Ding L P, Lin Y Q, et al. XenPump: A New Method to Mitigate Timing Channel in Cloud Computing[C]. *2012 IEEE Fifth International Conference on Cloud Computing*, 2012: 678-685.

[30] Chiappetta M, Savas E, Yilmaz C. Real Time Detection of Cache-Based Side-Channel Attacks Using Hardware Performance Counters[J]. *Applied Soft Computing*, 2016, 49: 1162-1174.

[31] Zhang Y Q, Juels A, Oprea A, et al. HomeAlone: Co-Residency Detection in the Cloud via Side-Channel Analysis[C]. *2011 IEEE Symposium on Security and Privacy*, 2011: 313-328.

[32] Raj H, Nathuji R, Singh A, et al. Resource Management for Isolation Enhanced Cloud Services[C]. *The 2009 ACM workshop on Cloud computing security - CCSW'09*, 2009: 77-84.

[33] Kim T, Peinado M, Mainar-Ruiz G. StealthMem: System-Level Protection Against Cache-Based Side Channel Attacks in the Cloud[C]. *The USENIX Security Symposium*, 2012: 189-204.

[34] Peng S H, Maitisabier T, Jin Z. Research on Xen Virtual Machine Scheduling Strategy to Mitigate Covert Side Attacks[J]. *Engineering Journal of Wuhan University*, 2018, 51(4): 371-376.
(彭双和, 图尔贡·麦提萨比尔, 金傅. 针对减弱隐蔽信道攻击的 Xen 虚拟机调度策略[J]. *武汉大学学报(工学版)*, 2018, 51(4): 371-376.)

[35] Xu Q M, Naghibijouybari H, Wang S B, et al. GPUGuard: Mitigating Contention Based Side and Covert Channel Attacks on GPUs[C]. *The ACM International Conference on Supercomputing*, 2019: 497-509.

[36] Yan M J, Shalabi Y, Torrellas J. ReplayConfusion: Detecting Cache-Based Covert Channel Attacks Using Record and Replay[C]. *2016 49th Annual IEEE/ACM International Symposium on Microarchitecture*, 2016: 1-14.

[37] Xiao J D, Xu Z, Huang H, et al. Security Implications of Memory Deduplication in a Virtualized Environment[C]. *2013 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 2013: 1-12.

[38] Xia Y B, Liu Y T, Chen H B, et al. Defending Against VM Rollback Attack[C]. *IEEE/IFIP International Conference on Dependable Systems and Networks Workshops*, 2012: 1-5.

[39] Szefer J, Lee R B. Architectural Support for Hypervisor-Secure Virtualization[C]. *The seventeenth international conference on Architectural Support for Programming Languages and Operating Systems - ASPLOS'12*, 2012: 437-450.

[40] Garfinkel T, Pfaff B, Chow J, et al. Terra: A Virtual Machine-Based Platform for Trusted Computing[C]. *The nineteenth ACM symposium on Operating systems principles*, 2003: 193-206.

[41] Matetic S, Ahmed M, Kostiainen K, et al. ROTE: Rollback Protection for Trusted Execution[C]. *USENIX Security Symposium*, 2017: 1289-1306.

[42] Oberheide J, Cooke E, Jahanian F. Empirical Exploitation of Live Virtual Machine Migration[C]. *Proceedings of BlackHat DC convention*, 2008: 1-6.

[43] Choudhary A, Govil M C, Singh G, et al. A Critical Survey of Live Virtual Machine Migration Techniques[J]. *Journal of Cloud Computing*, 2017, 6: 23.

[44] Zhang M, Ji X S, Liu W Y, et al. Defensive Method Against DoS Attack Based on Virtual Machine Migration[J]. *Application Research of Computers*, 2019, 36(7): 2174-2178.
(张淼, 季新生, 刘文彦, 等. 基于虚拟机迁移的 DoS 攻击防御方法[J]. *计算机应用研究*, 2019, 36(7): 2174-2178.)

[45] Zhang J B, Zhu Y X, Hu J, et al. Scheme of Virtual Machine Trusted Migration in Cloud Environment[J]. *Chinese Journal of Network and Information Security*, 2018, 4(1): 6-14.
(张建标, 朱元曦, 胡俊, 等. 面向云环境的虚拟机可信迁移方案[J]. *网络与信息安全学报*, 2018, 4(1): 6-14.)

[46] Zhou H, Wang J, Zhang H G. A Trusted VM-VTPM Live Migration Protocol in Clouds[C]. *The 1st International Workshop on Cloud Computing and Information Security*, 2013: 299-302.

[47] Wan X, Zhang X F, Chen L, et al. An Improved VTPM Migration Protocol Based Trusted Channel[C]. *2012 International Conference on Systems and Informatics*, 2012: 870-875.

[48] Sun D G, Zhang J, Fan W, et al. SPLM: Security Protection of Live Virtual Machine Migration in Cloud Computing[C]. *The 4th ACM International Workshop on Security in Cloud Computing*, 2016: 2-9.

[49] Wang W, Ya Z, Lin B, et al. Secured and Reliable VM Migration in Personal Cloud[C]. *2010 2nd International Conference on Computer Engineering and Technology*, 2010: V1-705.

[50] Xu Y Y, Zhao X, Gong J Y. A Large-Scale Secure Image Retrieval Method in Cloud Environment[J]. *IEEE Access*, 7: 160082-160090.

[51] Ge C P, Liu Z, Xia J Y, et al. Revocable Identity-Based Broadcast Proxy re-Encryption for Data Sharing in Clouds[J]. *IEEE Transactions on Dependable and Secure Computing*, 2021, 18(3): 1214-1226.

[52] Liang K T, Au M H, Liu J K, et al. A DFA-Based Functional Proxy re-Encryption Scheme for Secure Public Cloud Data Sharing[J]. *IEEE Transactions on Information Forensics and Security*, 2014, 9(10): 1667-1680.

[53] Liang K T, Au M H, Liu J K, et al. A Secure and Efficient Ciphertext-Policy Attribute-Based Proxy re-Encryption for Cloud Data Sharing[J]. *Future Generation Computer Systems*, 2015, 52: 95-108.

[54] Huang Q L, Yang Y X, Shen M S. Secure and Efficient Data Col-

laboration with Hierarchical Attribute-Based Encryption in Cloud Computing[J]. *Future Generation Computer Systems*, 2017, 72: 239-249.

[55] Wang S L, Zhou J W, Liu J K, et al. An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing[J]. *IEEE Transactions on Information Forensics and Security*, 2016, 11(6): 1265-1277.

[56] Li H W, Yang Y, Dai Y S, et al. Achieving Secure and Efficient Dynamic Searchable Symmetric Encryption over Medical Cloud Data[J]. *IEEE Transactions on Cloud Computing*, 2020, 8(2): 484-494.

[57] Li M, Yu S C, Ren K, et al. Toward Privacy-Assured and Searchable Cloud Data Storage Services[J]. *IEEE Network*, 2013, 27(4): 56-62.

[58] Tahir S, Ruj S, Rahulamathavan Y, et al. A New Secure and Lightweight Searchable Encryption Scheme over Encrypted Cloud Data[J]. *IEEE Transactions on Emerging Topics in Computing*, 2019, 7(4): 530-544.

[59] Li K, Zhang W M, Yang C, et al. Security Analysis on One-to-many Order Preserving Encryption-Based Cloud Data Search[J]. *IEEE Transactions on Information Forensics and Security*, 2015, 10(9): 1918-1926.

[60] Noman A, Adams C. Hardware-Based DLAS: Achieving Geo-Location Guarantees for Cloud Data Using TPM and Provable Data Possession[C]. *2014 17th International Conference on Computer and Information Technology*, 2014: 280-285.

[61] Talib A M, Atan R, Abdullah R, et al. CloudZone: Towards an Integrity Layer of Cloud Data Storage Based on Multi Agent System Architecture[C]. *2011 IEEE Conference on Open Systems*, 2011: 127-132.

[62] Bertholon B, Varrette S, Bouvry P. Certicloud: A Novel TPM-Based Approach to Ensure Cloud IaaS Security[C]. *2011 IEEE 4th International Conference on Cloud Computing*, 2011: 121-130.

[63] Modi C N, Acha K. Virtualization Layer Security Challenges and Intrusion Detection/Prevention Systems in Cloud Computing: A Comprehensive Review[J]. *The Journal of Supercomputing*, 2017, 73(3): 1192-1234.

[64] Giannakou A, Rilling L, Pazat J L, et al. AL-SAFE: A Secure Self-Adaptable Application-Level Firewall for IaaS Clouds[C]. *2016 IEEE International Conference on Cloud Computing Technology and Science*, 2016: 383-390.

[65] Bagheri S, Shameli-Sendi A. Dynamic Firewall Decomposition and Composition in the Cloud[J]. *IEEE Transactions on Information Forensics and Security*, 2020, 15: 3526-3539.

[66] Mishra P, Pilli E S, Varadharajan V, et al. Intrusion Detection Techniques in Cloud Environment: A Survey[J]. *Journal of Network and Computer Applications*, 2017, 77: 18-47.

[67] Hubballi N, Suryanarayanan V. False Alarm Minimization Techniques in Signature-Based Intrusion Detection Systems: A Survey[J]. *Computer Communications*, 2014, 49: 1-17.

[68] Meng W Z, Li W J, Kwok L F. EFM: Enhancing the Performance of Signature-Based Network Intrusion Detection Systems Using Enhanced Filter Mechanism[J]. *Computers & Security*, 2014, 43: 189-204.

[69] Su M Y, Yu G J, Lin C Y. A Real-Time Network Intrusion Detection System for Large-Scale Attacks Based on an Incremental Mining Approach[J]. *Computers & Security*, 2009, 28(5): 301-309.

[70] Hu L, Chen X S, Chen L, et al. Agentless Communication Encryption Framework for Virtual Machine in IaaS Environment[J]. *Application Research of Computers*, 2016, 33(3): 855-859.
(胡亮, 陈兴蜀, 陈林, 等. IaaS环境下虚拟机无代理通信加密机制[J]. *计算机应用研究*, 2016, 33(3): 855-859.)

[71] Chen L, Chen X S, Jiang J F, et al. Research and Practice of Dynamic Network Security Architecture for IaaS Platforms[J]. *Tsinghua Science and Technology*, 2014, 19(5): 496-507.

[72] Gonzales D, Kaplan J M, Saltzman E, et al. Cloud-Trust—A Security Assessment Model for Infrastructure as a Service (IaaS) Clouds[J]. *IEEE Transactions on Cloud Computing*, 2017, 5(3): 523-536.

欧阳雪 于 2020 年在广西师范大学电子与通信工程专业获得硕士学位。现在武汉大学通信与信息系统专业攻读博士学位。研究领域为云计算安全。Email: ouyangxue602@whu.edu.cn

徐彦彦 于2007年在武汉大学通信与信息系统专业获得博士学位。现在武汉大学测绘遥感信息工程国家重点实验室任教授、博士生导师。研究领域为云计算安全与大数据隐私保护、空间信息传输与处理、多媒体网络通信。Email: xuyy@whu.edu.cn