

面向第三方的云平台可信性在线评测及分析技术

赵波^{1,2}, 李想^{1,2,3}, 严飞^{1,2}, 张立强^{1,2}, 张焕国^{1,2}

(1. 武汉大学国家网络安全学院空天信息安全与可信计算教育部重点实验室, 湖北 武汉 430072;

2. 湖北省网络空间安全研究中心, 湖北 武汉 430072;

3. 鹏城实验室网络空间安全研究中心, 广东 深圳 518000)

摘要: 云计算的服务模式对用户数据安全产生的严重威胁, 必须通过第三方对云计算是否可信进行评测, 才能保障云计算产业的健康发展。由此, 总结了国家高技术研究发展计划课题“面向第三方的云平台可信性在线评测及分析技术”的研究内容与成果, 描述了从云平台可信评测模型与体系结构、可信性动态评测技术、可信证据收集及可信测试机制、可信性的多维量化评估方法、评测原型系统与工具集5个方面的研究工作, 并对云平台的可信性进行评测。

关键词: 云平台; 可信计算; 评测模型; 第三方

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2019054

Trusted platform for third-party cloud computing online evaluation and analysis technology

ZHAO Bo^{1,2}, LI Xiang^{1,2,3}, YAN Fei^{1,2}, ZHANG Liqiang^{1,2}, ZHANG Huanguo^{1,2}

1. Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education,
School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China

2. Cyberspace Security Research Center of Hubei Province, Wuhan 430072, China

3. Cyberspace Security Research Center, Peng Cheng Laboratory, Shenzhen 518000, China

Abstract: The service model of cloud computing creates a serious threat to user data security, the trustworthiness of cloud computing through third parties, must be evaluated then the healthy development of the cloud computing industry can be guaranteed. The research of the National High Technology Research and Development Program of

收稿日期: 2019-01-04; 修回日期: 2019-02-14

通信作者: 李想, lixiang950629@whu.edu.cn

基金项目: 国家高技术研究发展基金资金项目 (“863” 计划) (No.2015AA016002); 广东省鹏城实验室资助项目 (PCL2018KP004)

Foundation Items: The National High Technology Research and Development Program of China (863 Program) (No.2015AA016002), Peng Cheng Laboratory Project of Guangdong Province (PCL2018KP004)

论文引用格式: 赵波, 李想, 严飞, 等. 面向第三方的云平台可信性在线评测及分析技术[J]. 网络与信息安全学报, 2019, 5(5): 90-104.

ZHAO B, LI X, YAN F, et al. Trusted platform for third-party cloud computing online evaluation and analysis technology[J]. Chinese Journal of Network and Information Security, 2019, 5(5): 90-104.

China, “trusted platform for third-party cloud computing online evaluation and analysis technology” were summarized. The trusted evaluation model and architecture were described from the cloud platform, the dynamic evaluation technology, the credible evidence collection and the trusted test mechanism, the credibility of the quantitative evaluation method, and the prototype system integrated by tools, to evaluate the credibility of cloud platform.

Key words: cloud platform, trusted computing, evaluation model, third party

1 引言

具有巨大市场增长前景的云计算在提供方便易用与低成本特性的同时也带来了较传统模式更严重的安全威胁。2011年3月,作为最早提出云计算服务的谷歌公司,爆发了重大安全事件,约有15万Gmail用户的数据被泄露,邮箱和聊天记录被删除,部分用户则表示其账号被重置。2013年3月,跨平台云笔记Evernote遭到攻击者非法入侵,为保证其个人信息不被攻击者获取,重置了约5000万用户的密码。2013年6月,美国国家安全局和联邦调查局“棱镜门”项目被暴露,该项目通过进入Microsoft、Google、Apple、Yahoo等九大网络巨头公司的中心服务器挖掘个人数据,监控美国公民的行为,用户数据遭到严重泄露,引发了极为恶劣的国际影响。云计算面临极大的安全与隐私挑战,云用户在享受云服务带来便利的同时,更加担心自身数据被泄露的风险。

为提高云平台的信任度,本文开展面向第三方的云平台可信评测技术研究及其原型系统研究,增强我国在云计算高速发展新形势下的科技竞争力,占领信息科学基础研究的制高点,保护我国云计算产业稳定快速发展。

2 相关工作

与云平台可信评测相关的工作包括云计算安全标准制定、可信证据收集与测试、远程验证与云平台审计、云平台量化评估等方面。

在云计算安全标准制定方面,云安全联盟(CSA, Cloud Security Alliance)联合英国标准协

会(BSI, British Standards Institution)推出了STAR认证项目,采用中立性认证技术对云服务供应商安全性开展第三方独立评估,评估依据主要是ISO/IEC 27001:2005管理体系标准以及CSA云控制矩阵文档;全国信息安全标准化技术委员会TC260已完成《云计算安全及标准研究报告》《信息安全技术云计算服务安全指南》《信息安全技术云计算服务安全能力要求》等标准的制定^[1-3]。开展云平台的评测工作是云计算发展的一个必然趋势,目前的工作主要偏重于云服务商资质、服务质量等方面的离线评测,如何进行面向第三方的在线监测评估是云计算发展所面临的一个挑战。

在可信证据收集方面,Chen等^[4]在云平台软件和硬件之间设计了一个独立的可信监控者,向用户提供虚拟机运行时证据和证明报告;描述了主要构件安全性测试方法有基于错误注入及动态监测的构件安全性测试方法^[6-7]、构件安全性测试错误注入模型、基于动态错误树的构件安全性测试策略^[8]、基于接口错误注入的构件安全性测试方法^[9]。目前的可信测试工作主要集中在对软件的测试,云平台具有动态伸缩、多租户、泛在访问、虚拟化以及资源边界模糊等特征,如何对云平台进行可信测试,需在测试技术、方法上有重大突破。

在远程验证审计方面,基于密码学技术的方法主要是对外包到云上之前的数据进行预处理,如属性加密等,同时保持数据的部分可计算性,如保留部分检索能力^[10-11],但普遍需要消耗较多计算或存储资源或仅针对特殊应用,目前还未达到大规模实用阶段;辛思远等^[12]提出一种基于属

性的远程验证方式, 云节点的可信信息由可信平台模块 (TPM, trusted platform module) 保存, 由云计算管理中心集中处理验证请求、由云平台验证代理对基础设施即服务 (IaaS, infrastructure-as-a-service) 进行动态实时、保护隐私的属性证明。目前云平台审计的研究工作处于初期发展阶段, 云审计还面临没有明确的审计目的、权威审计标准等诸多挑战。

在云平台量化评估方面, Al-Kuwaiti^[13]等对 Dependability、Fault-tolerance、Reliability、Security 和 Survivability 这 5 个关于可信的概念进行了深入阐述, 介绍了每个概念的属性及概念间的关系, 揭示了如何对这些概念进行度量, 哪些概念的属性是可度量, 哪些是不可度量, 这对云服务安全性评估及属性选择具有非常重要的参考意义。现有面向云平台的量化评估研究大多数仍处于探索阶段, 面临着评测指标不细致、评测手段缺乏足够量化方法支撑、局限于部分属性等问题, 缺乏系统的、合理的、面向可信云平台的量化评估体系。

3 面向第三方的云平台可信性在线评测及分析

本文的研究内容从云平台可信评测模型与体系结构、云平台可信性动态评测技术、云平台可

信证据收集及可信测试机制、云平台可信性的多为量化评估方法、云平台评测原型系统与工具集 5 个方面展开, 实现了云计算平台的可信评测、恶意行为检测、安全追责管控、数据隐私保护、可信服务提供等关键技术, 形成了云计算平台安全技术体系, 并进行了云计算安全示范应用及验证, 解决了如何判定云计算可信性的难题。

3.1 云平台可信评测模型与体系结构

本文在云服务提供商与用户之外, 引入一个对云平台提供测评服务的可信第三方, 研究面向第三方的云平台可信评测模型与体系结构, 提出基于可信第三方的主动、持续监控的可信评测思路, 为用户提供有针对性的可信性查询服务。

在结构设计方面, 基于可信思想建立云平台可信评测体系结构, 形成与原有云平台并立的双体系架构, 达到同时保护评测证据和评测机制的目的; 在可信第三方的设计方面, 研究可信第三方的模块构成和工具部署; 在可信第三方与云平台网络连接方面, 采用可信连接架构 (TCA, trusted connect architecture) 思想, 为用户和云服务提供商提供中立、双向的测评服务, 保护双方隐私。面向第三方的云平台可信评测体系结构如图 1 所示。

云平台可信评测体系结构主要由可信第三方

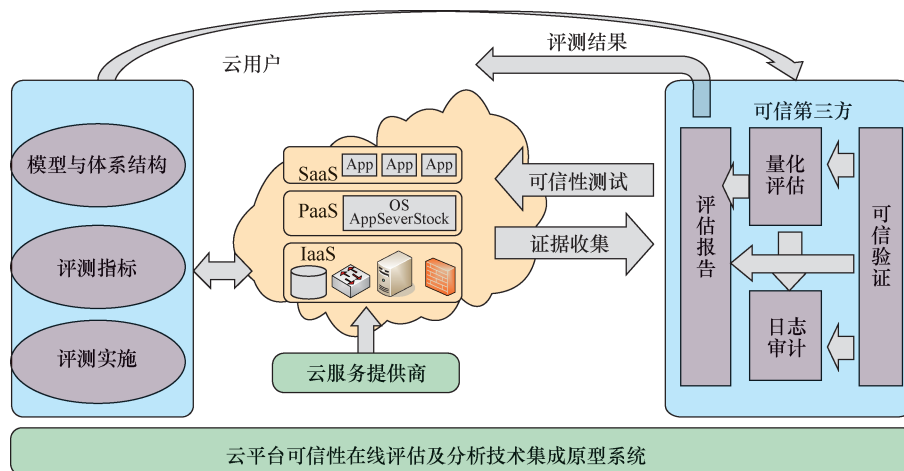


图 1 云平台可信评测体系结构

和可信证据收集代理构成。可信第三方执行云平台评测的主体过程，可信证据收集代理部署在目标云内部，用于目标云服务、环境、资源等信息的搜集。

3.2 云平台可信性动态评测技术

针对现有云测评缺乏动态评测手段的问题，本文引入了云平台可信动态评测体系与关键技术，从 IaaS、平台即服务（PaaS，platform-as-a-service）、软件即服务（SaaS，software-as-a-service）3 个层面提出了可信性动态评测及分析技术，为云平台评测及分析提供了技术支持，在测试技术和方法上有重大突破。

3.2.1 IaaS 层可信性动态评测及分析技术

云平台的可信性离不开 IaaS 层基础设施的支持，而 IaaS 层的硬件可能存在安全漏洞和潜在的侧信道，一旦它们被攻击者利用，就会破坏云平台安全。本文针对这种问题提出了 IaaS 层固件漏洞挖掘方法和云平台硬件侧信道数据泄露检测方法。

1) 本文提出一种基于漏洞特征信息流跟踪、关键过程重构的 IaaS 层固件安全性测试方法，主要由 3 个部分构成，分别是设备固件获取、设备固件初步分析以及关键代码反汇编。充分利用了集成固件映像解析、目标文件平台识别、嵌入式文件系统逆向解析以及嵌入式操作系统逆向识别等功能的 Binwalk 等开源自动化工具提取固件；针对整个系统进行分析并跟踪系统的启动流程，观察其启动的关键服务，定位和分析系统中存在的配置文件、初始化脚本、数据库等重要文件的分布，判断和搜集设备相关的各类重要信息（包括权限管理、设备性能、用户接口、缺省设置等），初步检测出可能隐藏在脚本中的安全漏洞和缺省配置中的隐藏后门；对关键服务程序以及对外接口程序进行反汇编，对固件进行逆向分析并发现漏洞。

2) 本文提出了基于侧信道分析的云平台数据泄露检测技术，从侧信道的角度检测云平台硬件基础设施是否会泄露用户数据^[14]。该技术的具体流程为：发射机利用硬件组件或数字设备的有意和无意发射，通过使用变体二进制频移键控调制泄露数据，并且发射的信号可以通过基于软件的虚拟示波器这种隐蔽信道来捕获和解码。为了检索接收到的信息，首先提取并计算信号的尖峰，然后对原始数据进行平滑处理，最后将平滑的数据检查并解调为真实的有效载荷数据。传输数据的接收由以下方式完成：预处理捕获开关电源（SMPS，switching mode power supply）发射的信号并对其进行归一化；执行小波变换和尖峰计算；原始数据处理将计算的峰值间隔转换为基于频率的信号并执行低通滤波器平滑，估计并应用阈值，然后计算脉冲宽度并提取原始数据位；报头检测和调制过程搜索比特帧报头并解调帧的有效载荷。

该检测技术可为数据泄露检测提供了证明依据，可用于判断云平台硬件基础设施层是否有通过侧信道泄露数据的风险。基于侧信道分析的数据泄露检测原理如图 2 所示。

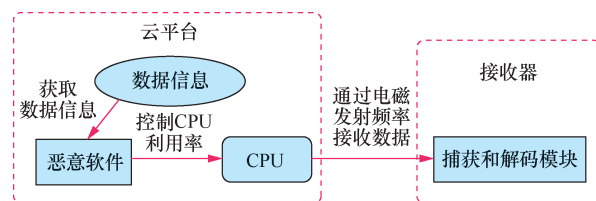


图2 基于侧信道分析的数据泄露检测原理

3.2.2 PaaS 层可信性动态评测及分析技术

在云平台 PaaS 层部署的测试程序代理，经常发生虚拟机迁移的过程，若测试程序代理 agent 被破坏，则整个测试过程将不可信。本文针对这种问题提出了云平台测试程序代理 agent 的保护机制和虚拟机迁移过程可信判定方法。

1) 在基于假设一个抗篡改的 CPU 芯片可信

是合理的情况下,本文提出一种适用于云平台可信性测试环境的 agent 保护机制 (APM, agent protection mechanism),通过 agent 内核态保护模块 (APKM, agent protection kernel module) 完整性保护方法、Agent 完整性与命令正确性验证方法以及 APM 有效性验证方法,在无须额外硬件支持的同时保证 Agent 的完整性以及命令执行的正确性^[15]。具体方案为:由 X86 计算机架构所形成的内存锁机制保护 APKM 的完整性,再由 APKM 对 Agent 实施保护,内存锁机制的安全性则由云节点控制寄存器 (CR, control register) 中写保护位 (WP, write protect) 状态的正确性来保障,通过这种信任链方式将信任关系从 WP 的置位正确性延伸到 APKM,再到 Agent,从而保

证 Agent 从云上获取的测试数据的完整性,保障了整个云平台测试过程的可信;在运行过程中,云服务提供商 (CPP, cloud service provider) 与可信第三方 (TTP, trusted third party) 随机对云节点控制寄存器 CR0 中的 WP 状态进行质询,APKM 对 Agent 进行完整性验证并检查其执行命令的正确性,质询和验证的结果都将发送给 TTP 作为判断测试数据是否可信的依据。Agent 保护机制的架构如图 3 所示。

2) 本文提出了一种可信虚拟机迁移模型的构建方法,该方案抽象了可信迁移的参与组件,并描述了迁移协议中的关键步骤和状态;以标号迁移系统 (LTS, labeled transition system) 为操作语义描述工具对可信迁移系统进行描述,以在

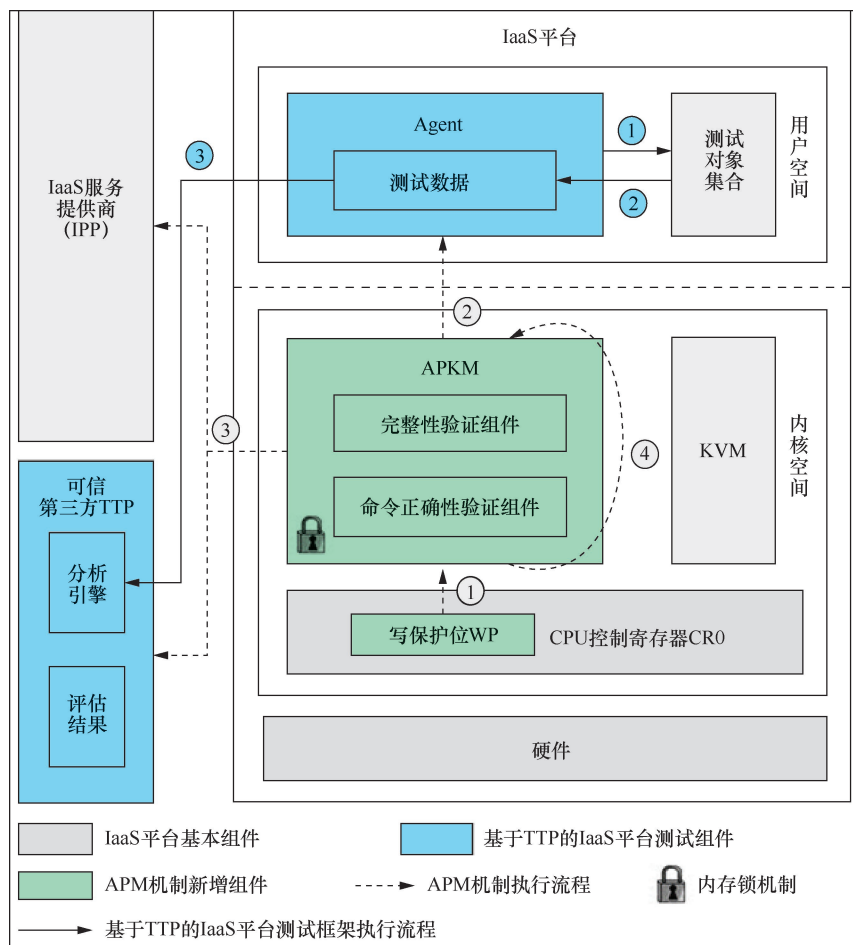


图3 Agent 保护机制的架构

系统中构建迁移过程组件，并基于该模型构建动态迁移系统状态迁移树；分析在可信迁移协议中采用 LTS 模型的一致性测试，即对平台的可信虚拟机迁移进行可信性评测^[16]。本文方法基于 LTS 为可信迁移系统的行为建模，然后以建立的模型为基础构建出动态的迁移系统状态迁移树，为了提高测试效率，笔者根据相关规则对其进行约减。最后通过分析此模型在协议一致性测试工作场景中的效果，证明了其有效性。本文方案的可信迁移模型如图 4 所示。

3.2.3 SaaS 层可信性动态评测及分析技术

云平台 SaaS 层直接向云用户提供具体的计算服务，所以该层中服务程序的可信性以及数据传输过程的安全性必须得到有效评测。本文针对这种问题提出了云平台服务程序抗攻击能力的检测方法和数据传输过程安全性评估方法。

1) 针对面向返回的编程 (ROP, return-oriented programming) 能够绕过数据执行保护，并结合内存泄露和暴力破解突破地址空间布局随机化 (ASLR, address space layout randomization) 等现有系统防御机制的问题，本文基于 ROP shellcode 不满足时间和空间局部性原理，利用硬件性能计数器的功能提出了一种云平台抗 ROP 攻击检测方法。该方法分为离线预处理和动态监控两个阶段：在离线预处理阶段收集并存储所有函数正常的性能事件值；在动态监控阶段监测程

序执行，在调用敏感系统函数前检测同一函数相同性能事件值是否异常变化^[17]。本文方法以函数为单位来收集数据，对同一函数相同性能事件中可能存在的异常使用 k -中心点聚类算法进行分析，能够准确检测 ROP 攻击。云平台抗 ROP 攻击能力的测试架构如图 5 所示。

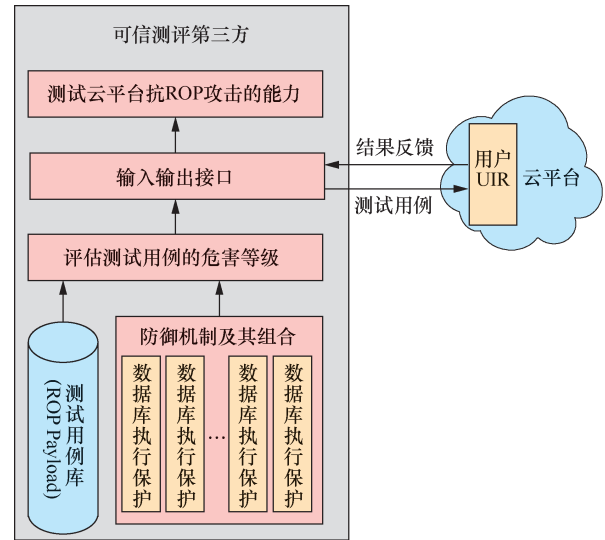


图5 云平台抗 ROP 攻击能力的测试架构

2) 针对云用户本身无法验证云服务提供商是否对数据进行了有效的加密保护，以及云平台密码算法识别分析技术识别率低、分析策略单一等缺点导致的无法有效识别程序变量的问题，本文开展了云平台密码机制测评工作，提出了一种通用密码机制测评方法。该方法捕获的原始网络数据分组，根据数据分组的协议结构提取包含的数据字段，整合

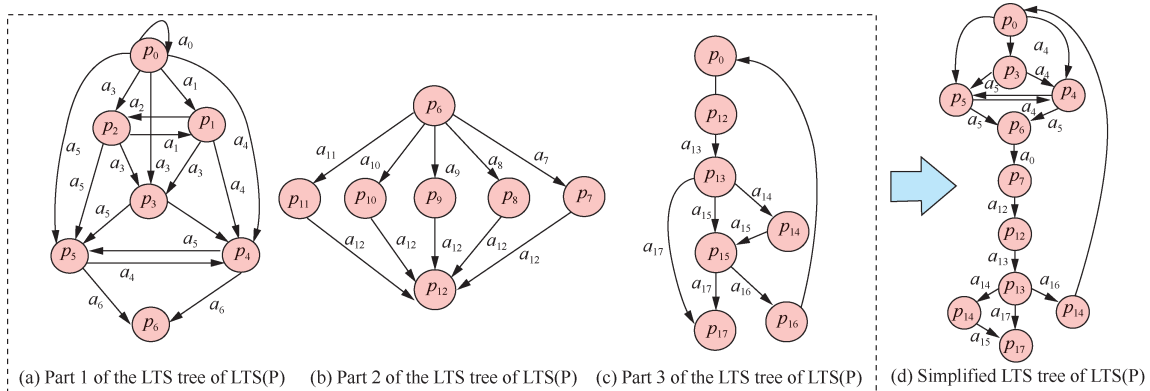


图4 可信迁移系统的 LTS 模型

形成载荷数据流, 载荷数据流经过压缩数据还原和信息熵计算两个步骤判断是否已加密, 并使用字节为数据单位的数据流的最大熵值, 载荷数据流的熵值与最大熵值越接近, 表示数据流已被加密的概率越高, 即云传输加密支持强度越高。

3.3 云平台可信证据收集及可信测试机制

针对用户与云平台之间的信任问题, 本文提出了面向第三方的云平台可信证据收集、验证、防护架构、测试体系和方法, 完成了云平台可信证据的收集、验证及证据收集机制的保护工作。

3.3.1 云平台可信证据测试体系

本文开展了基于等级保护安全技术的云计算安全防护框架及测试体系相关的工作, 进行了云计算安全测试体系研究, 同时也开展了对云基础设施、云网络、云外包服务的可信测试进行具体证据体系研究, 并研究面向第三方的云安全测试证据互操作方法, 建立面向第三方的云计算安全检测证据互操作架构。本文提出了面向第三方的云平台可信证据体系和面向互操作的云计算安全检测证据统一采集, 基于等级保护安全技术设计要求, 针对云计算环境, 按照各级系统安全保护环境和定级系统互联的技术要求 (即测试目标和要求), 建立测试体系。其中, 安全区域边界、安

全计算环境、安全管理中心和安全通信网络共同组成了安全计算环境, 定级系统互联由安全互操作部件和跨定级系统安全管理中心组成。本文基于上述云计算安全防护技术框架、云计算安全测试体系的研究、云环境下的检测证据互操作方法, 设计统一采集接口, 以达到证据互操作、公正评测的目的。基于等级保护安全技术的云计算安全防护框架及测试体系如图6所示。

3.3.2 云平台可信证据收集和验证方法

本文通过对云安全风险的分析, 得到影响云平台可信性测评的关键因素, 这些关键因素包括基础设施安全、多租户网络安全和外包服务安全等^[18], 随着云平台证据收集代理连续运行, 必然会产生海量、庞杂的安全数据, 对该类数据的泄露或非法访问将对相应的信息系统造成严重的隐私泄露威胁。针对上述影响云平台可信性测评的关键因素, 云平台上的服务模式分层特点, 提出相应的可信证据采集与验证方法, 采用了属性泛化和转换方法防止敏感信息的泄露, 采用面向第三方的基于多层次可信证据收集代理 (CPTECA, cloud platform trusted evidence collection agent) 进行云平台证据实时采集, 根据证据使用场景、服务类型等特点进行证据自动化收集和验证方法研

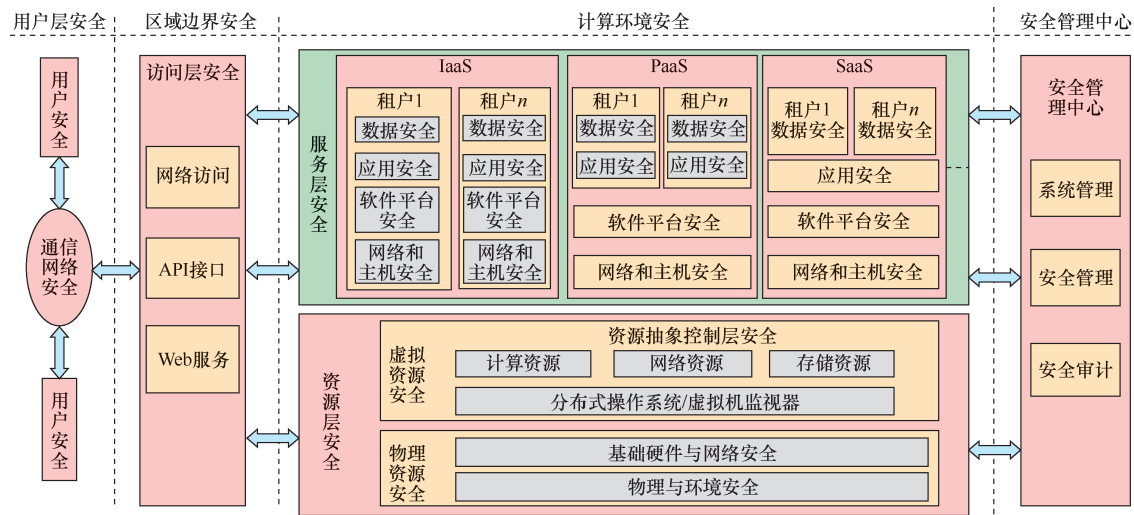


图6 网络安全等级保护云计算安全防护技术框架

究。其中，重点针对云基础设施平台上的程序行为可信性、多租户网络隔离性和外包应用行为安全性进行动态和在线收集和验证研究。

3.3.3 云平台可信证据收集保护方法

针对云计算节点证据收集系统的完整性会被篡改的问题，开展了基于静态加载度量的云计算节点证据收集系统保护的相关工作，提出在传统服务器平台上已有的静态加载度量技术能够实现物理平台上的静态可信链，从而保护平台上的固件、操作系统和应用在加载前的完整性不被篡改，加载度量实现了对将要加载的从硬件到应用的可执行对象的完整性保护，使信任从物理平台上的硬件传递到了应用^[19-20]。本文方案主要说明了计算节点中的证据收集系统保护方法。面向虚拟化平台（KVM，Kernel-based virtual machine）提出基于静态加载度量的云计算节点证据收集系统保护架构如图7所示。

3.4 云平台可信性的多维量化评估方法

本文提出了对可信属性量化和度量的树形结构，以及用于对可信性进行评估的3级、100多个评

测指标，并将所有评测指标的量化方法予以确定。

3.4.1 基于度量算子知识库与可信树的证据量化方法

本文提出一种基于度量算子知识库与可信树相结合的证据统一量化机制，度量算子知识库包含常规的各类直接量化指标以及间接量化机制，解决单一证据量化问题，可信属性树用于表达复杂证据关系，解决复杂证据量化问题，可信度量树解决系统可信性汇聚问题。基于度量算子知识库和可信树的量化机制如图8所示。度量算子内置可信性评测所需各类指标的量化方法、量化机制，直接量化指标提供计算依据描述/提供计算方法调用接口和返回值，间接量化指标提供间接测量方法描述/提供定性结果的定量转换方法以及默认值^[21]。可信属性树全面覆盖1至3级指标，提供单个指标的多重证据支持，可信度量树提供系统层数值汇聚方法，提供异构指标的归一化机制。

本文基于提出的云平台可信性量化指标体系中的3级100多个评测指标，根据每个指标给出了量化方法和量化依据，通过抽象不同指

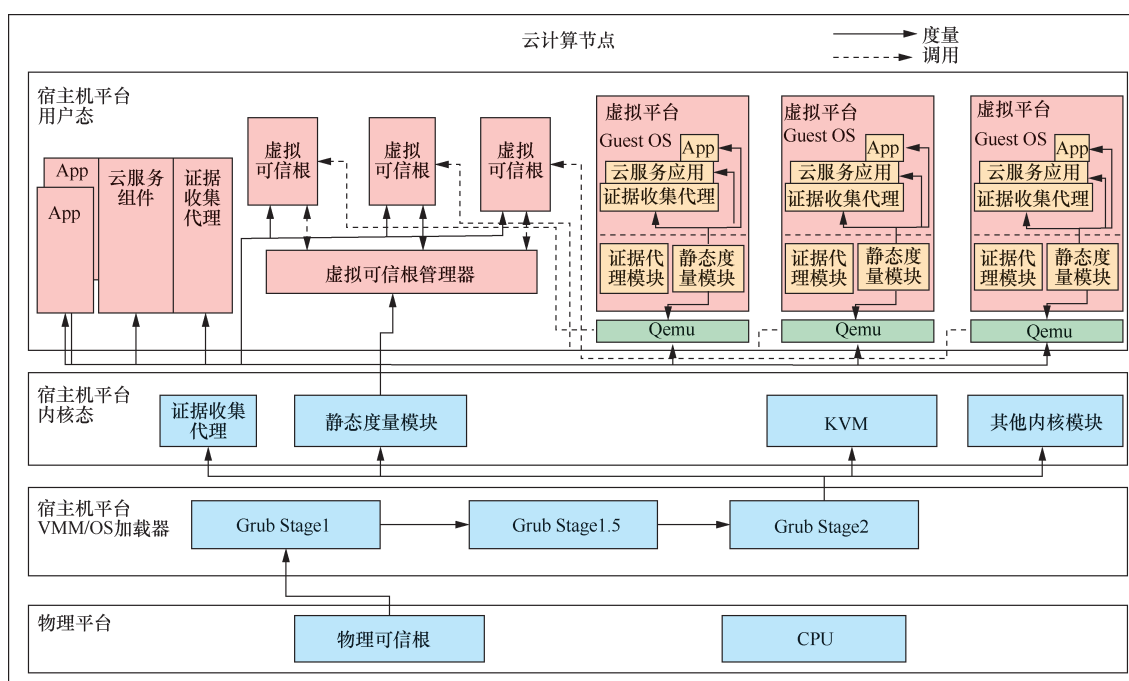


图7 基于静态加载度量的云计算节点证据收集系统保护架构

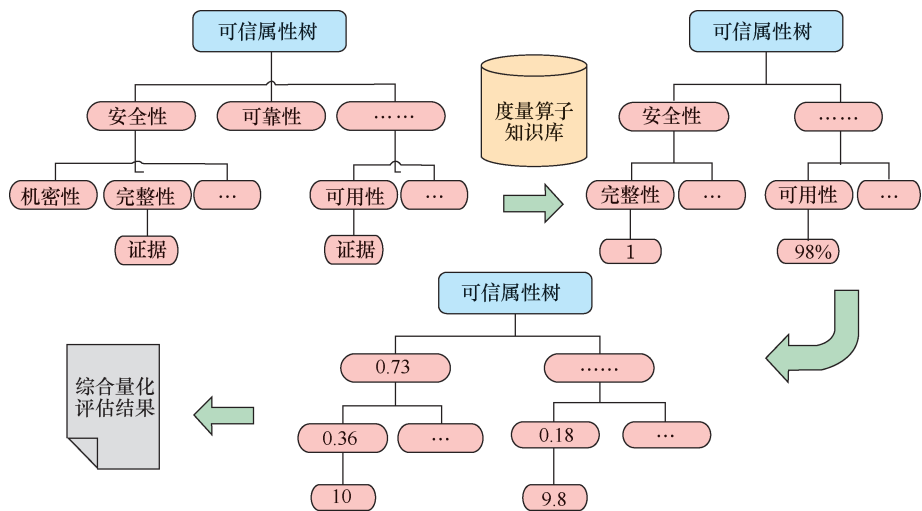


图 8 基于度量算子知识库和可信树的量化机制

标算子建立度量算子知识库。利用证据树、度量树和可信树多种机制实现对证据的度量和量化值的汇聚。

3.4.2 基于攻击平面的 SaaS 应用全度量分析方法

本文基于攻击面度量方法的核心思量，结合 SaaS 应用的自身特点，提出了面向 SaaS 应用的安全性量化分析框架 ASB-Metric，设计了面向 SaaS 应用安全性度量的核心指标，使用一个有带权参数的实向量空间来构建攻击面指标，并根据用户安全需求使用层次分析法对攻击指标进行赋值。依据攻击平面的思想设计并实现了一套面向 SaaS 应用的安全性量化分析方法。攻击平面是一种系统安全性分析方法，它抽象了系统与外部环境之间的数据交换方式，通过函数调用方法+交互机制+交互数据的方式对系统潜在攻击范围进行建模分析，通过资源重要程度和攻击者努力程度进行定量比较。

4 实验与评估

本文基于上述动态评测技术、可信证据收集机制、多维量化评估方法，研制了 10 款评测工具，工具成果支持了面向第三方的云平台可信评测原型系统的形成。本节针对该原型系统进行功能性

测试，并对测试结果进行分析，根据实验情况，该原型系统具有较好的应用效果。

4.1 实验环境

本文将技术点形成的 10 款测试工具进行功能上的合并，形成并集成了共 7 款云平台可信性评测工具：虚拟机隐私风险检测工具、基于区块链的测试数据安全存储工具、云平台程序行为可信性证据收集验证工具、多租户网络可信证据收集验证工具、云数据服务可信证据收集验证工具、云平台分布式压力测试工具、云平台漏洞扫描工具。原型系统效果如图 9 所示。

该原型系统部署在中国软件评测中心（北京），本实验可通过远程登录访问面向第三方的云平台可信评测原型系统，对华为可信云 FusionSphere 进行可信性评测与分析。

4.2 实验结果与分析

本实验是使用部署在中国软件评测中心（北京）的面向第三方的云平台可信评测原型系统，对华为可信云 FusionSphere 的可信性进行评测，以验证原型系统中各项测试功能的有效性。FusionSphere 是华为技术有限公司拥有自主知识产权的可信云平台，其针对安全性和可靠性等方面做了丰富的企业级增强，具有非常好的商用性，

络系统进行实践性的扫描，为其生成全面的安全扫描报告，安全报告中包括云平台网络中的弱点和漏洞信息以及相应可采用的修补方法和安全策略，实现对云平台网络安全性的增强。测试结果如图 11 所示，显示扫描出了一个名为“McAfee Common Management Agent 版本获取”的漏洞。

虚拟机隐私风险检测工具从隐私安全角度评测云平台可信性，从用户虚拟机角度进行检测。包含 3 项功能：虚拟机系统安全审计、隐私文件异常访问检测和网络端口安全性检测，通过工具执行过程中的各种输出信息和结果报告做进一步分析。被测结果如图 12 所示，被测云虚拟机存在系统登录失败次数 25 次、安全套接层（SSL, secure sockets layer）证书过期、缺少文件完整性工具等，表明该虚拟机存在一定的隐私风险。

基于区块链的测试数据安全存储工具保证测试数据与测试结果的强完整性安全需求，同时允许多个验证方并发访问。在保证测试数据安全存储的同时，保证其可公开性和验证方的可控性。

包含 3 个程序：程序 1 模拟控制端，用于发起数据保存的打包计算，接收另外两个计算机的运行结果并综合展示；程序 2 模拟计算机 c1 端的执行情况；程序 3 模拟计算机 c2 端的执行情况。该工具为每一组测试数据计算抗篡改的元数据，如示例文件夹中打开的任一文件所示，在 CurrentBlockHeaderStrSHA256 段内找出符合 difficulty 目标的区块头散列值。测试数据的安全存储如图 13 所示，在打开的 show/Mchain.文件夹下，发现新生成的元数据列表和 masterrecords.txt 中给出计算每个自己的区块链的耗时长。由可信第三方构建 Mchain，专用于测试数据的保存、共享发布和验证。

4.2.2 可信证据收集测试与多维量化评估

云数据服务可信证据收集验证工具保证能获得云数据服务应用的可信证据，同时能验证云数据服务应用是否可信，并且支持审计日志的读取。支持对测试数据服务完整性验证与测试 MapReduce 程序行为可信验证时的结果展示，支持对测试用户云应用数据隐私保护的结果展示，

标记	主机	漏洞名称	危险级别	简要描述	返回信息	漏洞ID
	49.4.13.180	McAfee Common Management Agent 版本获取	信息	发现远程主机正在运行McAfee Common Management Agent服务。	McAfee Common Management Agent version:	0012015D

图 11 云平台漏洞扫描结果

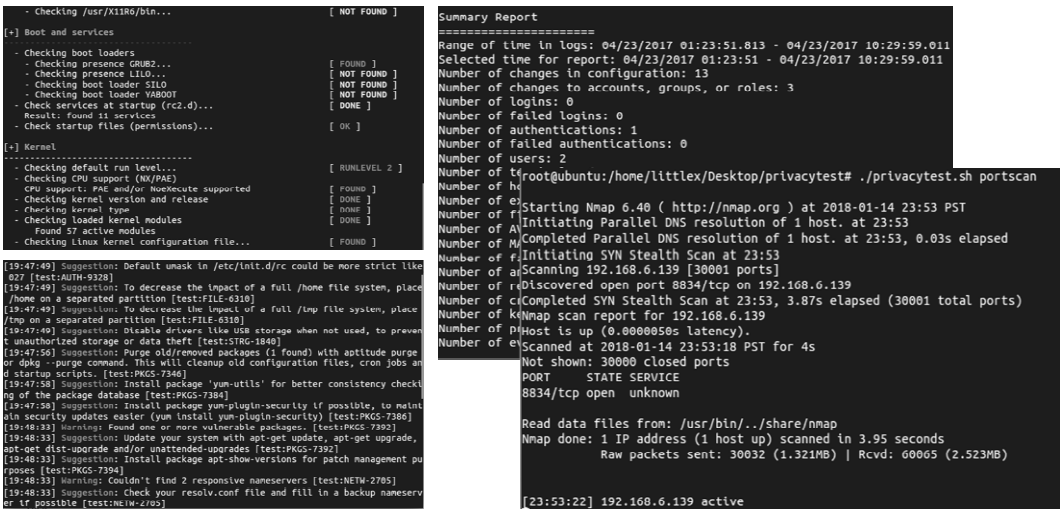


图 12 虚拟机隐私风险检测结果

提供完整性指数与隐私指数对测试结果进行量化。本工具支持对云数据服务的静态文件和动态行为的度量，同时保证度量过程中的隐私。测试结果如图 14 所示，被测云服务实际执行行为均符合用户预期行为，行为可信性指数为 1。

云平台程序行为可信性证据收集验证工具既

能收集云平台的程序配置证据，又能与云平台配置程序内核保护白名单进行比较，以发现不属于云平台程序配置的未知程序并验证其是否为恶意代码。测试结果如图 15 所示，被检测出的未知程序为恶意代码，并且检测到一个行为特征，该特征表示此未知代码会篡改子系统配置文件。其云

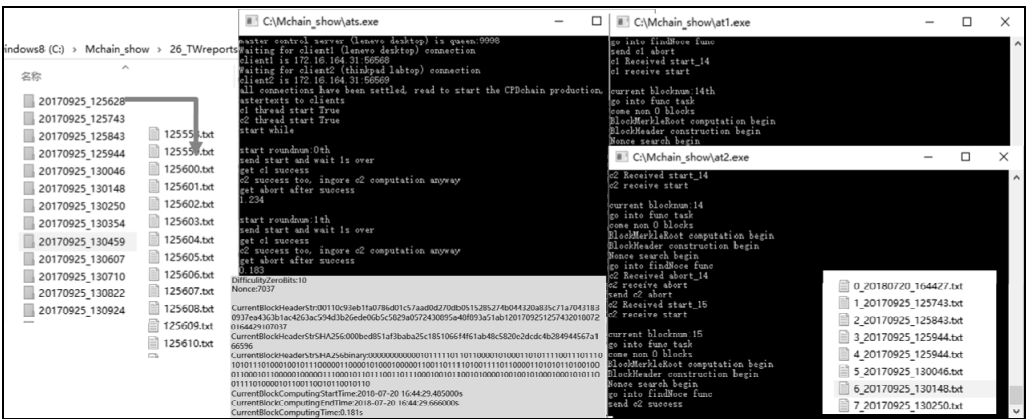


图 13 测试数据安全存储

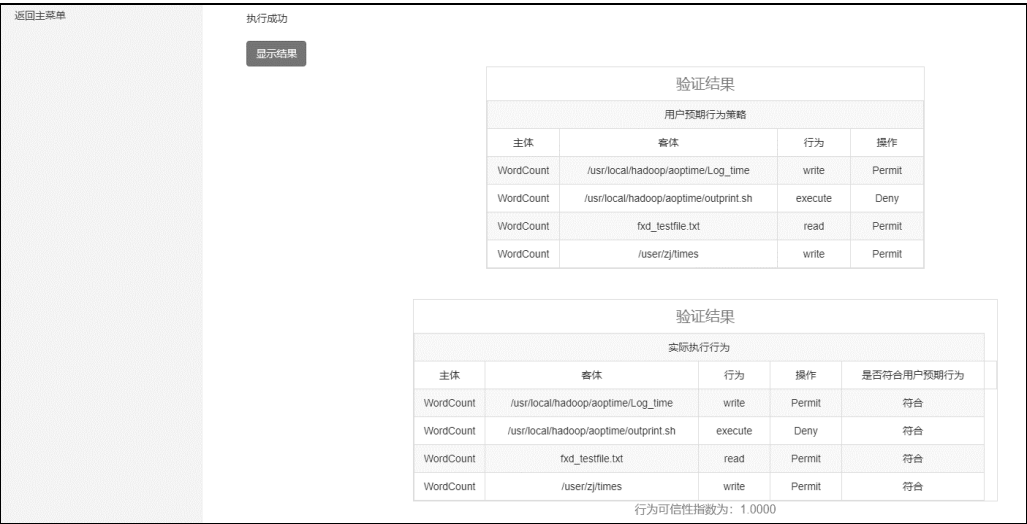


图 14 云数据服务测试结果



图 15 云应用行为可信性测试结果

平台程序可信指数为 0.075, 表明其不可信。

多租户网络可信证据收集验证工具考虑了来自云平台内部工作人员的威胁, 在云平台内网存在恶意虚拟机时, 进行检测与识别。该工具验证预期和实际的云平台租户网络拓扑是否一致, 并显示相应结果 (在界面中呈现实际云平台拓扑图以及预测云平台拓扑图)。测试结果如图 16 所示, 被测云平台多租户网络隔离指数为 0, 预期和实际的云平台租户网络拓扑完全一致。

4.3 系统实施效果

本文的原型系统还与北京因特信安软件科技有限公司针对因特信安可信服务器进行安全性测试分析。该公司是从事可信计算、可信云计算和信息安全技术与产品的研发、生产和销售的专业公司。本文研究人员针对因特信安可信服务器的所有可信功能进行测试分析, 包括 TPM 功能、可信启动、可信度量、可信内核、可信应用, 采用功能性测试和安全性测试结合的方法, 以黑盒测试为主, 性能测试+压力测试为辅, 对专用测试环境进行了有针对性的可信性检测。测试结果显示, 可信服务器具备比较完备的可信功能, 能检测出 90% 以上的篡改攻击, 相对传统服务器而言, 在安全性、可靠性与可信性方面具有较大优势。

5 结束语

本文总结了国家高技术研究发展计划课题“面向第三方的云平台可信性在线评测及分析技术”的研究结果, 并简要描述了研究内容与方案。

本文的研究工作主要分为以下 5 个方面。

1) 以云平台可信评测模型与体系结构为目标, 提出了面向第三方的统一可扩展的云平台可信性评测指标体系。

2) 以云平台可信动态评测技术为目标, 研究了云平台 IaaS 层、PaaS 层、SaaS 层的可信性动态评测及分析技术。

3) 以云平台可信性评测为目标, 建立了云平台可信证据测试体系和面向互操作的证据采集方法, 针对证据收集验证过程中涉及的隐私保护问题研究了相关保护方法; 研究了基于可信度量、动态过程控制、远程证明、共享内存摆渡等多种技术的证据收集过程保护方法。

4) 以云平台可信评测工具集成与聚合为目标, 覆盖了安全性、可靠性、可用性和可维护性这 4 个指标体系, 建立了支持隐私保护的云平台可信属性远程验证方法与协议, 研究了相关分析方法, 并研制了相应工具集, 实现了云平台可信

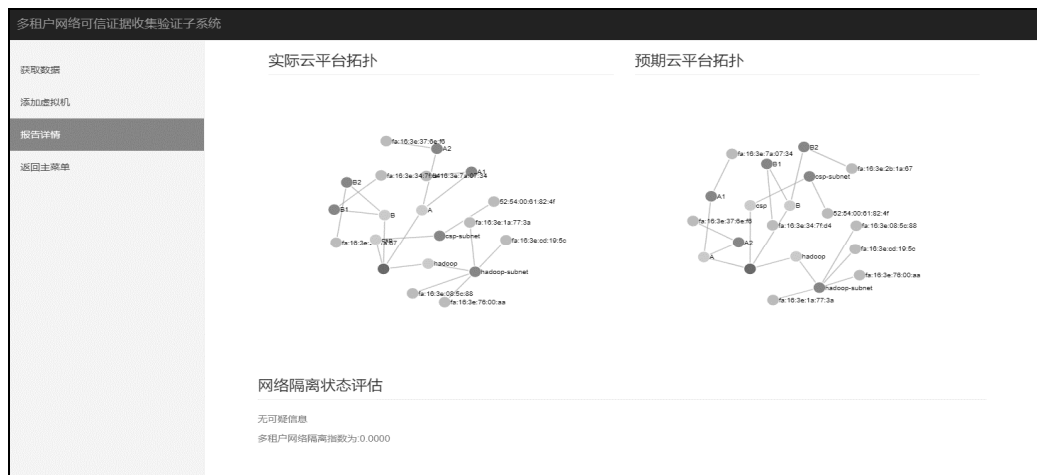


图 16 多租户隔离性测试结果

评测原型系统。

5) 以商用可信云平台单元测试环境构建与集成测试保障为目标, 支持了安全性、可靠性、可用性和可维护性这4个指标, 在单元测试的基础上支持了政务云、教育云等典型示范应用的集成可信测试, 包含可信证据的采集、验证与分析评估, 以及自研测试工具的集成。

本文研发的云平台可信证据收集验证工具集原型系统通过了第三方测试机构功能、安全性及性能测试, 能够为面向第三方的云安全评测提供有力支持, 具有较好的应用前景和价值。

参考文献:

- [1] 中国电子技术标准化研究所. 云计算标准研究报告[R]. 2010.
China Electronics Standardization Institute. Cloud computing standards research report[R]. 2010.
- [2] 王惠莅, 杨晨, 杨建军. 云计算安全和标准研究[J]. 信息技术与标准化, 2012(5): 16-19.
WANG H L, YANG C, YANG J J. Information security and standard of cloud computing[J]. Information Technology & Standardization, 2012(5): 16-19.
- [3] 王惠莅, 罗锋盈, 杨建军, 等. 云计算服务安全关键标准研究[J]. 信息技术与标准化, 2013.
WANG H L, LUO F Y, YANG J J. Research on key standards for the security of cloud computing services[J]. Information Technology & Standardization, 2013.
- [4] CHEN C, MANIATIS P, PERRIG A. Towards verifiable resource accounting for outsourced computation[J]. ACM Sigplan Notices, 2013, 48(7): 167.
- [5] 邵政斌. 流量伪装技术及其成本分析[D]. 长沙: 湖南大学, 2007.
SHAO Z B. Traffic camouflaging technology and its cost analysis[D]. Changsha: Hunan University, 2007.
- [6] LIU D X, CHI C H, LI M. Normalizing traffic pattern with anonymity for mission critical applications[C]// 37th Annual Simulation Symposium. 2004: 293-299.
- [7] 胡文心. 网络流量规范化的流量伪装模型的研究[D]. 上海: 华东师范大学, 2006.
HU W X. The model and implementation of normalizing network traffic pattern with anonymity for mission critical applications[D]. Shanghai: East China Normal University, 2006.
- [8] FU X W, GRAHAM B, BETTATI R, et al. On effectiveness of link padding for statistical traffic analysis attacks[C]//23rd International Conference on Distributed Computing Systems. 2003: 45-52.
- [9] 胡文心, 蔡建华, 俞琨. 网络流量规范化的流量伪装方法, CN101383831A[P]. 2009.
HU W X, CAI J H, YU K. Network traffic normalized traffic masquerading method, CN101383831A[P]. 2009.
- [10] CAO N, WANG C, LI M, et al. Privacy-preserving multi-keyword ranked search over encrypted cloud data[C]//IEEE Infocom 2011. 2011: 10-15.
- [11] LI J, WANG Q, WANG C, et al. Fuzzy keyword search over encrypted data in cloud computing[C]//Infocom, Mini-Conference. 2010.
- [12] XIN S, ZHAO Y, LI Y. Property-based remote attestation oriented to cloud computing[C]//2011 Seventh International Conference on Computational Intelligence and Security. 2011: 1028-1032.
- [13] KUWAITI M, KYRIAKOPOULOS N, HUSSEIN S. A comparative analysis of network dependability, fault-tolerance, reliability, security, and survivability[J]. Commun Surveys Tuts, 2009, (4): 106-124.
- [14] ZHAO B, NI M T, FAN P R. Powermitter: data exfiltration from air-gapped computer through switching power supply[J]. China Communications, 2018, 15(2):170-189.
- [15] 樊佩茹, 赵波, 倪明涛, 等. APM:适用于 IaaS 平台的 agent 保护机制[J]. 通信学报, 39(4): 176-188.
FAN P R, ZHAO B, NI M T, et al. APM:agent protection mechanism applied for IaaS platform[J]. Journal on Communications, 2018, 39(4): 176-188.
- [16] 石源, 张焕国, 吴福生. 一种可信虚拟机迁移模型构建方法[J]. 计算机研究与发展, 2017, 54(10):2284-2295.
SHI Y, ZHANG H G, WU F S. A method of constructing the model of trusted virtual machine migration[J]. Journal of Computer Research and Development, 2017, 54(10): 2284-2295.
- [17] 严飞, 彭慧容, 何凡, 等. HBROP:基于硬件性能计数器的函数级 ROP 检测[J]. 武汉大学学报(理学版), 2017, 63(2):109-116.
YAN F, PENG H R, HE F, et al. HBROP: HPC-based function-level approach to detect ROP attack[J]. Journal of Wuhan University, 2017.
- [18] ZHAN J, FAN X D, CAI L, et al. TPTVer: A trusted third party based trusted verifier for multi-layered outsourced big data system in cloud environment[J]. China Communications, 2018, 15(2): 122-137.
- [19] 詹静, 杨静. 基于远程证明的可信 Modbus/TCP 协议研究[J]. 工程科学与技术, 2017, 49(1).
ZHAN J, YANG J. Research on remote attestation-based trusted modbus/TCP protocol[J]. Advanced Engineering Sciences, 2017, 49(1).
- [20] 詹静, 杨静, 马俊明, 等. 一种基于共享内存摆渡的 Modbus/TCP 安全通信方法[J]. 中国科技论文, 2017, 12(2): 135-140.

ZHAN J, YANG J, MA J M, et al. Modbus/TCP secure communication method based on shared memory ferry[J]. China Sciencepaper, 2017, 12(2):135-140.

- [21] ZHANG L Q, YAN F, ZHAO B, et al. Dependence-induced risk: security metrics and their measurement framework[J]. China Communications, 2016, 13(11): 119-128.

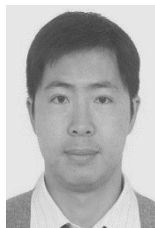
[作者简介]



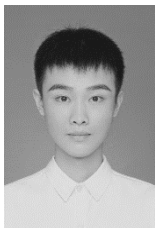
赵波 (1972—)，男，山东青岛人，博士，武汉大学教授、博士生导师，主要研究方向为信息系统安全、可信计算、嵌入式安全、人工智能及大数据安全隐私保护。



严飞 (1980—)，男，湖北武汉人，博士，武汉大学副教授，主要研究方向为信息安全、可信计算、系统安全。



张立强 (1979—)，男，黑龙江呼兰人，博士，武汉大学讲师，主要研究方向为信息安全、云安全、安全测评。



李想 (1995—)，男，湖北武汉人，武汉大学硕士生，主要研究方向为系统安全、云计算安全。



张焕国 (1945—)，男，河北元氏人，武汉大学教授、博士生导师，主要研究方向为密码学、信息安全。