文本复制检测报告单(全文对照)

№:ADBD2018R_2018032815205120180328152219100281213215 5 检测时间:2018-03-28 15:22:19

检测文献: 齐能_20151304001_信息安全
作者: 齐能
检测范围: 中国学术期刊网络出版总库
中国博士学位论文全文数据库/中国优秀硕士学位论文全文数据库
中国重要会议论文全文数据库
中国重要报纸全文数据库
中国专利全文数据库
互联网资源(包含贴吧等论坛资源)
英文数据库(涵盖期刊、博硕、会议的英文数据以及德国Springer、英国Taylor&Francis 期刊数据库等)
港澳台学术文献库
优先出版文献库
互联网文档资源
图书资源
CNKI大成编客-原创作品库
时间范围: 1900-01-01至2018-03-28

检测结果

总文字复制比：4.5% 跨语言检测结果：0%
去除引用文献复制比：2.3% 去除本人已发表文献复制比：4.5%
单篇最大文字复制比：1.4%（基于无干扰的云计算环境行为可信性分析）

重复字数：	[2431]	总段落数：	[5]
总字数：	[53471]	疑似段落数：	[5]
单篇最大重复字数：	[775]	前部重合字数：	[84]
疑似段落最大重合字数：	[1447]	后部重合字数：	[2347]
疑似段落最小重合字数：	[84]		

指 标：☐疑似剽窃观点 ☑疑似剽窃文字表述 ☐疑似自我剽窃 ☐疑似整体剽窃 ☐过度引用

表格：0 脚注与尾注：60

0.8%（84） 齐能_20151304001_信息安全.doc_第1部分（总11184字）
4.1%（360） 齐能_20151304001_信息安全.doc_第2部分（总8871字）
2.1%（215） 齐能_20151304001_信息安全.doc_第3部分（总10066字）
2.7%（325） 齐能_20151304001_信息安全.doc_第4部分（总12170字）
12.9%（1447） 齐能_20151304001_信息安全.doc_第5部分（总11180字）

（注释：无问题部分 文字复制比部分 引用部分）

1. 齐能_20151304001_信息安全.doc_第1部分

总字数：11184

相似文献列表 文字复制比：0.8%(84) 疑似剽窃观点：(0)

1	博士论文规范-百度文库 -《互联网文档资源（http://wenku.baidu.c）》- 2012	0.7%（82） 是否引证：否
2	四川师范大学博士硕士学位论文撰写打印要求及格式范本_图文 -《互联网文档资源（http://wenku.baidu.c）》- 2016	0.7%（82） 是否引证：否
3	四川师范大学博士硕士学位论文撰写打印要求及格式范本--2013.2 -《互联网文档资源（http://wenku.baidu.c）》- 2016	0.7%（82） 是否引证：否

	原文内容	相似内容来源
1	此处有 44 字相似	博士论文规范-百度文库 -《互联网文档资源

	分类号： (按中国图书分类法) 单位代码： 10636 密级： （注明密级与保密期限） 学号： 20151304001 硕士学位论文 中文论文题目：具有瀑布特征的可信虚拟平台信任链模型及其分析方法 英文	（http://wenku.baidu.c）》- 2012-11-19 21:48:27（是否引证：否） 1. .3.4 作者简历：包括教育经历、工作经历、攻读学位期间发表的论文和完成的工作等 起 5 示例 1：学位论文封面格式 分类号： 密 (按中国图书分类法) 单位代码： 10636 学 号： 级： （注明密级与保密期限） 四川师范大学 博 士 学 位 论 文 中文论文题目 ： 英文论文题目 ： 英文论文题目：（小二号仿宋体加黑）（16pt 四川师范大学博士硕士学位论文撰写打印要求及格式范本_图文 -《互联网文档资源（http://wenku.baidu.c）》- 2016/9/26 21:06:03（是否引证：否） 1. 月 日 论文答辩日期： 年 月 日 7 附件1.3：专业学位硕士论文封面格式（浅黄色A4皮纹纸装订，打印时此行取消） 分类号： (按中国图书分类法) 单位代码： 10636 密 级：（注明密级与保密期限） 学 号： 专业学位硕士论文 中文论文题目 ：（小二号仿宋体加黑）英文论文题目：（16pt Time New Rom 四川师范大学博士硕士学位论文撰写打印要求及格式范本--2013.2 -《互联网文档资源（http://wenku.baidu.c）》- 2016-12-28 6:14:32（是否引证：否） 1. 年 月 日 论文答辩日期： 年 月 日 附件1.3：专业学位硕士论文封面格式（浅黄色A4皮纹纸装订，打印时此行取消） 分类号： (按中国图书分类法) 单位代码： 10636 7 密 级：（注明密级与保密期限） 学 号： 专业学位硕士论文 中文论文题目 ：（小二号仿宋体加黑）英文论文题目：（16pt Time New Rom
2	此处有 40 字相似 ods Based on the Trusted Virtualization Platform 论文作者： 齐能 指导教师： 谭良 专业名称： 信息安全 研究方向： 可信计算 所在学院： 计算机科学学院 论文提交日期： 年月日 论文答辩日期： 年月日 具有瀑布特征的可信虚拟平台信任链模型及其分析方法	四川师范大学博士硕士学位论文撰写打印要求及格式范本_图文 -《互联网文档资源（http://wenku.baidu.c）》- 2016/9/26 21:06:03（是否引证：否） 1.（小二号仿宋体加黑）英文论文题目：（16pt Time New Roman，Bold）论文作者：（四号仿宋） 指导教师： 专业名称： 研究方向： 所在学院： 论文提交日期 ： 年 月 日 论文答辩日期： 年 月 日 7 附件1.3：专业学位硕士论文封面格式（浅黄色A4皮纹纸装订， 四川师范大学博士硕士学位论文撰写打印要求及格式范本--2013.2 -《互联网文档资源（http://wenku.baidu.c）》- 2016-12-28 6:14:32（是否引证：否） 1.（小二号仿宋体加黑）英文论文题目：（16pt Time New Roman，Bold）论文作者：（四号仿宋） 指导教师： 专业名称： 研究方向： 所在学院： 论文提交日期 ： 年 月 日 论文答辩日期： 年 月 日 附件1.3：专业学位硕士论文封面格式（浅黄色A4皮纹纸装订，打印 博士论文规范-百度文库 -《互联网文档资源（http://wenku.baidu.c）》- 2012-11-19 21:48:27（是否引证：否） 1.： 英文论文题目：（小二号仿宋体加黑）（16pt Time New Roman，Bold） 作者： 指导教师： 合作导师： 专业名称： 研究方向： 所在学院： 论文提交日期 6 示例 2： 四川师范大学博士学位论文独创性声明 本人声明所呈交的学位论文是本人在导师指导下进行的研究工

脚注和尾注

1. National Institute of Standards and Technology | NIST [EB/OL]. NIST. [2018-03-10].https://www.nist.gov/.
2. 柯文浚, 董碧丹, 高洋. 基于Xen的虚拟化访问控制研究综述[J]. 计算机科学, 2017, 44(s1):24-28..
3. 石源, 张焕国, 赵波,等. 基于SGX的虚拟机动态迁移安全增强方法[J]. 通信学报, 2017, 38(9)..
4. 林闯,苏文博,孟坤,刘渠,刘卫东.云计算安全:架构、机制与模型评价[J].计算机学报,2013,09:1765-1784..
5. 俞能海,郝卓,徐甲甲,张卫明,张驰.云安全研究进展综述[J]. 电子学报,2013,02:371-381..
6. Ali M,Khan S U,Vasilakos A V.Security in cloud computing :opportunities and challenges[J].Information Science,2015,305:357-383..
7. Zhao D, Mohamed M, Ludwig H. Locality-aware Scheduling for Containers in Cloud Computing[J]. IEEE Transactions on Cloud Computing, 2018, PP(99):1-1..
8. Kumar P R, Raj P H, Jelciana P. Exploring Data Security Issues and Solutions in Cloud Computing[J]. Procedia Computer Science, 2018, 125:691-697..
9. 胡俊, 沈昌祥, 公备. 可信计算3.0 工程初步[J]. 网络与信息安全学报, 2017(8)..
10. 余发江, 陈列, 张焕国. 虚拟可信平台模块动态信任扩展方法[J]. 软件学报, 2017, 28(10):2782-2796..
11. 谭良,徐志伟. 基于可信计算平台的信任链传递研究进展[J]. 计算机科学,2008,10:15-18..
12. 中国信通院-研究成果-权威发布-专题报告[EB/OL]. [2017-07-10].中国信息通信研究院. http://www.caict.ac.cn/kxyj/qwfb/ztbg/201709/t20170919_2208939.htm.
13. 工业和信息化部关于印发《云计算发展三年行动计划（2017-2019年）》的通知[EB/OL].[2017-04-10]. 中华人民共和国工业和信息化部 http://www.miit.gov.cn/n1146295/n1146592/n3917132/n4062056/c5570298/content.html.
14. McAfee：2017年全球云计算安全报告[EB/OL]. [2017].http://www.chinacloud.cn/show.aspx?id=25993&cid=29.
15. 徐明迪,张焕国,张帆,杨连嘉. 可信系统信任链研究综述[J]. 电子学报,2014,10:2024-2031.
16. BERGER S, CACERES R, GOLDMAN K A, et al. VTPM: virtualiz-ing the trusted platform module[A]. Proc of the 15th USENIX Security Symposium[C]. Berkeley, USA, 2006. 305-320..
17. Xensource, Xen Open-Source Hypervisor[EB/OL]. https://www.citrix.com/downloads/xenserver/,2017..
18. Data Storage, Converged, Cloud Computing, Data Protection | Dell EMC US[2018-03-10] ?Dell Inc. .https://www.dellemc.com/en-us/index.htm.
19. Microsoft - Official Home Page [EB/OL].[2018-03-10]. Microsoft 2018. https://www.microsoft.com/zh-cn/.
20. Garfinkel T, Pfaff B, Chow J, et al. Terra: a virtual machine-based platform for trusted computing[C]// Nineteenth ACM Symposium on Operating Systems Principles. ACM, 2003:193-206..
21. B. PFITZMANN, J. RIORDAN, C. STUBLE,et al. "The PERSEUS system architecture", Technical Report RZ 3335 (#93381), IBM Research Division, Zurich Laboratory, 2001..
22. CHRIS I D, DAVID P, WOLFGANG W, et al. Trusted virtual platforms: a key enabler for converged client devices[A]. Proc of the ACM SIGOPS Operating Systems Review[C]. New York, USA, 2009. 36-43..
23. BERGER S, RAMON C, DIMITRIOS P, et al. TVDc:managing security in the trusted virtual datacenter[A]. Proc of ACM SIGOPS Operating Systems Review[C]. New York, USA, 2008. 40-47..
24. KRAUTHEIM F J, DHANANJAV S P, ALAN T S. Introducing the trusted virtual environment module: a new mechanism for rooting trust in cloud computing[A]. Proc of the 3rd International Conference on Trust and Trustworthy Computing[C]. 2010.211-227..
25. 王丽娜,高汉军,余荣威等.基于信任扩展的可信虚拟执行环境构建方法研究[J].通信学报, 2011, 32(9):1-8..
26. Zhang Lei , Chen Xingshu, Liu Liang , Jin Xin.Trusted domain hierarchical model based on noninterference theory[J].The Journal of China Universities of Posts and Telecommunications .August 2015, 22(4): 7-16..
27. 常德显,冯登国,秦宇,张倩颖.基于扩展LS2的可信虚拟平台信任链分析[J].通信学报,2013,34(5):31-41..
28. Yu, Z., Zhang, W. & Dai, H. J A Trusted Architecture for Virtual Machines on Cloud Servers with Trusted Platform Module and Certificate Authority[J].Journal of Signal Processing Systems, 2017, Vol.86 (2-3), pp.327-336.
29. 池亚平,李欣,王艳,王慧丽. 基于KVM的可信虚拟化平台设计与实现[J]. 计算机工程与设计,2016,(06):1451-1455..
30. 李海威,范博,李文锋. 一种可信虚拟平台构建方法的研究和改进[J]. 信息网络安全,2015,(01):1-5..
31. 蔡谊,左晓栋. 面向虚拟化技术的可信计算平台研究[J]. 信息安全与通信保密,2013,(06):77-79..
32. 徐天琦,刘淑芬,韩璐. 基于KVM的可信虚拟化架构模型[J]. 吉林大学学报(理学版),2014,(03):531-534..
33. 杨丽芳,刘琳. 基于虚拟机的可信计算安全平台架构设计[J]. 煤炭技术,2014,(02):170-172..
34. 蔡谊,左晓栋. 面向虚拟化技术的可信计算平台研究[J]. 信息安全与通信保密,2013,(06):77-79..
35. F. John Krautheim*, Dhananjay S. Phatak, and Alan T. Sherman,Introducing the Trusted Virtual Environment Module:A New Mechanism for Rooting Trust in Cloud Computing[C],TRUST 2010, LNCS 6101, 2010:211–227..

2. 齐能_20151304001_信息安全.doc_第2部分

总字数：8871

相似文献列表　文字复制比：4.1%(360)　疑似剽窃观点：(0)

1	虚拟可信平台及数据泄漏防护研究	1.6%（138）
		是否引证：否

	王星魁(导师：彭新光) -《太原理工大学博士论文》- 2016-09-01	
2	虚拟机性能干扰预测模型及其调度策略研究	1.1%（98）
	孟凡欣(导师：贺红) -《山东大学硕士论文》- 2014-05-10	是否引证：否
3	车载自组织网络中RSU部署和控制方案的研究	0.6%（55）
	朱利旻(导师：陶军) -《东南大学硕士论文》- 2015-04-01	是否引证：否
4	信息检索中的查询扩展算法研究	0.6%（54）
	李大高(导师：程显毅) -《江苏大学硕士论文》- 2008-06-01	是否引证：否
5	基于ASP．NET和WebGIS的校园信息 - 豆丁网	0.6%（53）
	-《互联网文档资源（http://www.docin.com）》- 2012	是否引证：否
6	基于TomEE的某海关JAVA EE应用服务器的研究与应用	0.5%（43）
	苑桐(导师：赵亚伟;孙浩) -《中国科学院大学(工程管理与信息技术学院)硕士论文》- 2013-09-01	是否引证：否
7	基于BI技术的证券公司客户分析模型的研究及实现	0.5%（43）
	原雷(导师：赵亚伟;杨绍军) -《中国科学院大学（工程管理与信息技术学院）硕士论文》- 2014-03-01	是否引证：否
8	基于改进粒子群算法的云任务调度方案研究	0.4%（34）
	苗冬云(导师：陈涛) -《安徽财经大学硕士论文》- 2015-12-01	是否引证：否
9	DTI三维重建和MRS多体素重建在阿尔茨海默病中的应用	0.4%（32）
	张月(导师：万遂人;孙钰) -《东南大学硕士论文》- 2016-05-28	是否引证：否
10	基于共享内存的域间通信优化方法研究	0.3%（30）
	吴鸿远(导师：万健) -《杭州电子科技大学硕士论文》- 2015-05-01	是否引证：否

	原文内容	相似内容来源
1	此处有 67 字相似 任链的传递才是安全可靠的。最后，基于本文建立的可信虚拟平台架构对扩展无干扰理论进行了分析和验证，证明了扩展后的无干扰理论 验证信任链模型的有效性。 论文组织结构 本文共分为六章，每章的安排如下： 第1章主要介绍了论文的研究背景及意义，主要从目前国内外 云计算的发展及云计算安全的发展；然后介绍了国内外的研究现状，主要从可信虚拟平台，信任链模型，形式化分析方法三个方面进行介	车载自组织网络中RSU部署和控制方案的研究 朱利旻 -《东南大学硕士论文》- 2015-04-01（是否引证：否） 1.分发路由，依据数据大小采用不同的分发手段来降低数据分发的延迟，并分别从理论角度和仿真角度对机制的有效性进行分析与验证。1.4论文组织结构本文共分为六章，各章的主要内容具体如下：第一章阐述了论文课题的研究背景、研究目标与研巧内容，W及论文组织结构。第二章介绍了车辆自组织网络技术，分析了现有的车辆自组织网络中路边单元的部署 基于ASP．NET和WebGIS的校园信息 - 豆丁网 -《互联网文档资源（http://www.docin.com）》- 2012-12-22 3:08:27（是否引证：否） 1.询系统、网络地理信息系统的开发等。系统的研究路线如图,所示,图,系统的研究路线,基于,和,的校园信息管理系统开发及应用,论文的组织结构本文分为五章,基本结构如下,第一章绪论。主要介绍了论文的研究背景及意义,国内外研究现状,论文的主要研究内容,技术路线和论文的组织结构。第二章主要介绍了论文用到的相关技术和系统开发的平台,详细介绍了, 基于BI技术的证券公司客户分析模型的研究及实现 原雷 -《中国科学院大学（工程管理与信息技术学院）硕士论文》- 2014-03-01（是否引证：否） 1.析处理（OLAP)、J2EE等技术，最终形成多角度、多手段、多渠道、功能全面的客户分析系统。1.4本文组织结构论文共分为六章。第一章绪论。该章主要是介绍本论文的研究意义和背景，国内外商业智能特别是客户分析方面的研究现状，以及本论文的研究目的和研究内容。第二章客户分析模型关键技术研究。本章简 基于TomEE的某海关JAVA EE应用服务器的研究与应用 苑桐 -《中国科学院大学(工程管理与信息技术学院)硕士论文》- 2013-09-01（是否引证：否） 1.监视服务，应用更新等，进行了逐一的应用案例的效果验证，满足某海关二期项目的需求，达到了最初的目

		的。1.4本文组织结构论文共分为六章。第一章绪论。该章主要是介绍本论文的研究意义和背景，基于某海关二期项目中的企业级JAVA EE应用服务器构建面临的问题，与国内外开源和商用JAVA EE应用服务
2	此处有 39 字相似 ，主要从目前国内外云计算的发展及云计算安全的发展；然后介绍了国内外的研究现状，主要从可信虚拟平台，信任链模型，形式化分析 方法三个方面进行介绍；最后介绍了本论文的研究方向和研究内容。 第2章主要介绍 了对本文研究提供思路的相关理论和技术。首先介绍了云计算中的关键技术和虚拟化技术，以及虚拟机和虚拟机监视器，目前最流行的V	虚拟可信平台及数据泄漏防护研究 王星魁 -《太原理工大学博士论文》- 2016-09-01（是否引证：否） 1.17第 1 章主要介绍论文研究背景及意义，国内外研究现状，以及数据泄漏防护措施暴露出来的不足及解决的新方法。并在最后介绍了本论文的研究方向和研究内容。第 2 章主要介绍了可信计算中的关键技术和虚拟化技术的基本原理，深入分析和研究了可信平台模块的硬件结构及功能，虚拟化技术的分类和虚
3	此处有 36 字相似 信虚拟平台，信任链模型，形式化分析方法三个方面进行介绍；最后介绍了本论文的研究方向和研究内容。 第2章主要介绍了对本文 研究提供思路的相关理论和技术。首先介绍了云计算中的关键技术和虚拟化技术， 以及虚拟机和虚拟机监视器，目前最流行的VMM结构Xen和KVM；其次介绍了可信计算中的关键技术，主要介绍了虚拟可信平台模	虚拟机性能干扰预测模型及其调度策略研究 孟凡欣 -《山东大学硕士论文》- 2014-05-10（是否引证：否） 1.的研究背景、意义、现状、目标、5山东大学硕士学位论文 ,内容以及论文的组织结构安排。第二章，相关研究和技术。首先介绍了云计算的关键技术一虚拟化技术，包括虚拟化技术的基本概念.，虚拟化技术的特点，以及对xen虚拟机的介绍。第二节阐述了虚拟机性能干扰预测模型在国内外
4	此处有 32 字相似 论和技术。首先介绍了云计算中的关键技术和虚拟化技术，以及虚拟机和虚拟机监视器，目前最流行的VMM结构Xen和KVM；其次 介绍了可信计算中的关键技术，主要介绍了虚拟可信平台模块，信任链的 构建和完整性度量技术，以及虚拟可信平台模块的分类和目前信任链技术的不足；最后介绍了形式化方法，并简要的介绍了安全系统逻辑	虚拟可信平台及数据泄漏防护研究 王星魁 -《太原理工大学博士论文》- 2016-09-01（是否引证：否） 1.及数据泄漏防护措施暴露出来的不足及解决的新方法。并在最后介绍了本论文的研究方向和研究内容。第 2 章主要介绍了可信计算中的关键技术和虚拟化技术的基本原理，深入分析和研究了可信平台模块的硬件结构及功能，虚拟化技术的分类和虚拟机的结构。并重点分析了信任
5	此处有 54 字相似 系统需要满足的性质，然后介绍了非传递无干扰安全策略，其中本文提出的扩展无干扰理论方法可以适用于目前的可信虚拟平台信任链的 分析。 第6章主要是对本文的研究内容进行概括分析，并指出了论文的不足之处，对未来的研究方向进行了展望。 相关技术与理论 虚拟化技术 虚拟化技术是将实际的实体资源进行抽象，使单一的计算机资源可以被用来提供多个同类资源的资源	信息检索中的查询扩展算法研究 李大高 -《江苏大学硕士论文》- 2008-06-01（是否引证：否） 1.提出的三种查询扩展算法(AwAROE算法、KQE算法、ACQE算法)进行了实验，并对它们的性能进行了比较与分析。 第6章:对全文工作进行总结，并对未来研究方向进行了展望。江苏大学硕士学位论文第2章信息检索与查询扩展综述2.1基本概念2.1 .1什么是信息 基于改进粒子群算法的云任务调度方案研究 苗冬云 -《安徽财经大学硕士论文》- 2015-12-01（是否引证：否） 1.的环境配置和算法仿真流程;最后对论文提出的改进的离散粒子群算法进行了仿真实验结果的分析。第五章:总结与展望。对全文的研巧内容和工作进行了总结,指出了论文研究中的不足,并对未来的研究方向进行了展望。 2是环境下任务调度相关研究2.1是计算巧述2.1.1云计

		It的定义一直レッ来,将计算作为一种物品进斤交易是计算机领域一直 DTI三维重建和MRS多体素重建在阿尔茨海默病中的应用 张月 -《东南大学硕士论文》- 2016-05-28（是否引证：否） 1.即自动纤维量化方法，比较纤维束上100个采样点的弥散张量成像参数变化情况。第五章为总结与展望，对全文工作进行总结，指出本研究的创新点和不足之处，并对未来的研究方向进行展望。4 第二章磁共振波谱和弥散张量成像原理第二章磁共振波谱和弥散张量成像原理2.1磁共振物理学原理脚
6	此处有 65 字相似 被开放源码，无法进行内核修改，因此只能选择全虚拟化方式。当前可以提供全虚拟化的架构有Xen、VMware、KVM等。 操作系统辅助虚拟化的半虚拟化。和全虚拟化技术中不对内核进行修改的虚拟化方式不同，半虚拟化技术需要通过对虚拟机操作系统进行内核修改， 才可以完成对操作系统的虚拟化。通过半虚拟化技术提供的虚拟机可以通过操作系统下的命令查看到虚拟机的架构。Xen等都可以提供	虚拟机性能干扰预测模型及其调度策略研究 孟凡欣 -《山东大学硕士论文》- 2014-05-10（是否引证：否） 1.技术按照执行软件指令方式的不同可分为三类[25]:全虚拟化、半虚拟化、硬件辅助虚拟化，全虚拟化技术不需要修改虚拟机操作系统内核，而半虚拟化技术需要修改虚拟机操作系统内核，硬件辅助虚拟化技术则是随着多核技术的发展和硬件资源的不断优化，而衍生出来的新的虚拟化技术。下面详细介绍一下这 基于共享内存的域间通信优化方法研究 吴鸿远 -《杭州电子科技大学硕士论文》- 2015-05-01（是否引证：否） 1.相比,运行速度和几乎相当,性能损失最差不会超过10%。与其它虚拟化解决方案相比,Xen最初只是被定义为基于半虚拟化技术的虚拟机系统,半虚拟化技术的实现需要对客户操作系统的内核代码进行一定的修改,替换掉不能虚拟化的敏感指令并重新规划内核地址空间的使用,Hypervisor也提供API接口来满足其
7	此处有 31 字相似 到系统应用启动完成的链式信任链，完成可信计算平台的信任度量。经过计算机物理硬件、系统引导、操作系统以及启动后的应用程序的 逐级认证，将信任从硬件底层的静态信任根扩展到整个可信计算平台， 保障其安全可靠。 TCG的链式信任链模型如图2.2所示： 图2.2 TCG信任链模型 下面本文对PCR和完整性度量	虚拟可信平台及数据泄漏防护研究 王星魁 -《太原理工大学博士论文》- 2016-09-01（是否引证：否） 1.系统的可信度量根，提出了一种建立平台信任的信任链实现方法[84]，其从信任根开始一层度量一层，并逐级认证，将信任从最底层的信任根传递到整个系统，保证系统执行环境的可信。TCG 提出以 TPM 为信任根，逐级度量启动过程中的硬件、操作系统和应用程序的方法，以
8	此处有 36 字相似 计算机软硬件配置信息是非常容易看到系统完整性的改变。 （2）完整性度量机制 在实际的机器进行启动时，往往都是从系统的 BIOS开始，经过设备检查、系统引导、操作系统初始化、操作系统内核加载等 主要的过程，直到应用程序加载，才会完成整个系统的启动。如果中间任一环节被恶意篡改导致系统的控制权被恶意的转向不同的过程，	虚拟可信平台及数据泄漏防护研究 王星魁 -《太原理工大学博士论文》- 2016-09-01（是否引证：否） 1.量对象对的 PCR值如图 3-17 所示。(3) 性能测试在系统启动过程中，TPM 会依次度量 BIOS、引导扇区、操作系统内核、系统配置文件等信息的完整性，并建立信任链。在加载下一个环节之前，先度量其完整性，当某个环节的完整性遭到破坏时，系统无法启动。这

指　标
疑似剽窃文字表述

1. 验证信任链模型的有效性。
   论文组织结构
   本文共分为六章，每章的安排如下：
   第1章主要介绍了论文的研究背景及意义，主要从目前国内外
2. 分析。
   第6章主要是对本文的研究内容进行概括分析，并指出了论文的不足之处，对未来的研究方向进行了展望。
3. 操作系统辅助虚拟化的半虚拟化。和全虚拟化技术中不对内核进行修改的虚拟化方式不同，半虚拟化技术需要通过对虚拟机操作系统进行内核修改，

脚注和尾注

1. 朱智强. 混合云服务安全若干理论与关键技术研究[D].武汉大学,2011..
2. 曲文涛. 虚拟机系统的可信检测与度量[D].上海交通大学,2010..
3. CHEN S Y, WEN Y Y,ZHAO H. Formal analysis of secure bootstrap in trusted computing[A]. Proc of the 4th International Conference on Autonomic and Trusted Computing[C]. Berlin, Springer, 2007. 352-360..
4. 张兴, 黄强, 沈昌祥.一种基于无干扰模型的信任链传递分析方法[J].计算机学报,2010,33(1):74-81..
5. Rushby J. Noninterference , transitivity , and channel-control security policies[M]. SRI International , Computer Science Laboratory , 1992.
6. Kai E, Meyden R V D, Zhang C. Intransitive noninterference in nondeterministic systems[C]// ACM Conference on Computer and Communications Security. ACM, 2012:869-880..
7. Paolo Baldan, Alessandro Beggiato. Multilevel Transitive and Intransitive Non-interference, Causally[J]. Theoretical Computer Science, 2018, 706:54-82..
8. 张兴，陈幼雷，沈昌祥.基于进程的无干扰可信模型[J]..通信学报，2009，30(3):6-11.
9. 赵佳，沈昌祥，刘吉强，等.基于无干扰理论的可信链模型[J].计算机研究与发展，200845(6):974-980.
10. 刘威鹏，张兴.基于非传递元干扰理论的二元多级安全模型研究[JJ.通信学报，2009，30(2):52-58.
11. 陈菊，谭良.一个基于进程保护的可信终端模型[J].计算机科学，2011，38(4):115-117.
12. 徐甫.支持进程代码修改的非传递元干扰可信模型[J].计算机工程，2013，39(11):150-153，168.
13. 秦晰，常朝稳，沈昌祥，等.容忍非信任组件的可信终端模型研究[J]..电子学报，2011，39(4):934-939.
14. Smith, Jim, Nair, et al. Virtual Machines: Versatile Platforms for Systems and Processes (The Morgan Kaufmann Series in Computer Architecture and Design)[J]. 2005..
15. Adams K, Agesen O. A comparison of software and hardware techniques for x86 virtualization[J]. Acm Sigops Operating Systems Review, 2006, 40(5):2-13..
16. Get Docker | Docker [EB/OL].[2018-03-10].https://www.docker.com/get-docker.
17. KVM project[EB/OL], http://www.linux-kvm.org/, 2017.

3. 齐能_20151304001_信息安全.doc_第3部分

总字数：10066

相似文献列表　文字复制比：2.1%(215)　疑似剽窃观点：(0)

1	基于扩展LS~2的可信虚拟平台信任链分析 常德显;冯登国;秦宇;张倩颖; -《通信学报》- 2013-05-25	2.1%（215） 是否引证：否

	原文内容	相似内容来源
1	此处有 31 字相似 本文，vRT主要包括可信衔接点TJP和vTPM，根据目前最新的vTPM实现方式和本文的TJP，vRT作为可信虚拟平台上的 独立的应用程序或者组件，并且通过软件的方式与硬件TPM进行关联 ，由TPM确保vRT的安全可信。其中vTPM是软件形式的TPM，具有TPM的安全功能；TJP是可信衔接点，TJP的可信依	基于扩展LS~2的可信虚拟平台信任链分析　常德显;冯登国;秦宇;张倩颖; -《通信学报》- 2013-05-25（是否引证：否） 1.任保障,它拥有非易失存储及密钥存储等固有特性;vRT在功能实现上可表现为m中内核组件或独立的可信组件,这里将其抽象为一个独立功能组件,通过特定的映射关系与硬件信任根TPM关联以确保其可信性,即vRT依赖于TPM,它以软件形式体现,用于为上层用户虚拟机提供信任保障。因此,TVP从功能角度可定义为
2	此处有 35 字相似 nel, TJP)), ((TJP, vTPM1), vm1), …,((TJP, vTPMn), vmn) }	基于扩展LS~2的可信虚拟平台信任链分析　常德显;冯登国;秦宇;张倩颖; -《通信学报》- 2013-05-25（是否引证：否）

	其中，m必须使用TPM 来构建信任，而虚拟机vm则是利用TJP和其相应 的vTPM来构建信任。 特别地，可信衔接点TJP可以划分为TJP:= { vTPM Builder, vTPM-VM	1.供信任保障。因此,TVP从功能角度可定义为TVP:={(m,TPM),(vm1,vRT1),…,(vmn,vRTn)},其中,m必须使用TPM来构建信任,而虚拟机vm则是利用其相应的vRT来构建信任。*如无特别说明,本文所使用的vm均泛指任意用户i的虚拟机vmi。2.2 TVP信任链及其信任属性TC
3	此处有 57 字相似 TJP 和TCvTPM两个属性。本文将按照主机、虚拟信任根、虚拟机三个方面对TVP-QT的信任属性进行描述。（1） 主机的信任属性TPm可以表示为TPm:={TCm,Verm}。其中，TCm表示表示以底层TPM为硬件信任根进行信任链构建的本地信任属性，在该部分信任链传递过程中不存在除信任链之外的其他组件的加载，即主机m正确的可信启动过程应该完整的表	基于扩展LS~2的可信虚拟平台信任链分析 常德显;冯登国;秦宇;张倩颖; -《通信学报》- 2013-05-25（是否引证：否） 1.,该信任属性根据组件类型可分为3类:主机m的信任属性TPm、vRT信任属性TPvRT及用户虚拟机的信任属性TPvm。1)主机m的信任属性表示为TPm:={TCm,Verm},其中,TCm表示基于硬件信任根构建的信任链,即主机m在本地正确地完成从可信度量根(CRTM,core root of trust for measurement)到
4	此处有 54 字相似 程验证过程中向外部实体R证明m应该拥有的信任属性TCm，即Verm:=Verify(m, TCm)。 同理，虚拟可信根 vRT的信任属性表示为TPvRT:= {TCvRT, VervRT}，TCvRT表示为vRT的本地可信加载的信任属性，VervRT表示对外部实体证明的信任属性。并且，由定义3.1对vRT以及定义3.2对TVP-QT信任属性的定义	基于扩展LS~2的可信虚拟平台信任链分析 常德显;冯登国;秦宇;张倩颖; -《通信学报》- 2013-05-25（是否引证：否） 1.(m,TCm)表示对外验证主机m所声称的信任属性TCm,使远程验证者确信TVP平台主机m拥有这样的信任链属性TCm。2)vRT的信任属性为TPvRT:={TCvRT,VervRT},表示vRT的本地可信加载及其对外的证明。需要注意的是,vRT的信任属性与其实现方式密切相关(图1中的a、b),它可能实现为一个微内核系统或一个应用进程,而且需要
5	此处有 38 字相似 ，包括vTPM实例域的配置文件(.cfg)以及启动文件(.img)和Mini OS、tpm instance等组件。但是 由于目前的DRTM机制在实现过程中会存在很多限制，比如要求进行动态度量的代码 需要不依赖与其他组件，对本文的vTPM实例不太适用，因此本文采用静态度量方式实现对vTPM实例的完整性度量。VM Bui	基于扩展LS~2的可信虚拟平台信任链分析 常德显;冯登国;秦宇;张倩颖; -《通信学报》- 2013-05-25（是否引证：否） 1.任链与第2节中定义一致。图6基于XEN的TVP实例系统本文建立的通用抽象模型不关注具体系统实现细节,以上述实例系统为例,由于目前较新的DRTM机制对其保护的应用有诸多限制,比如要求受保护的代码自包含等,因此上述实例系统在实现时并未采用DRTM机制保障TSD的安全,而是将TSD作为admindomker之后加载的

指　标

疑似剽窃文字表述

---

1. vRT的信任属性表示为TPvRT:= {TCvRT, VervRT}，TCvRT表示为vRT的本地可信加载的

脚注和尾注

1. Goguen J A, Meseguer J. Security Policies and Security Models.[C]// IEEE Symposium on Security & Privacy. DBLP, 1982:11-20..
2. Datta A, Franklin J, Garg D, et al. A Logic of Secure Systems and its Application to Trusted Computing[J]. 2009:221-236..
3. WANG Zhi, JIANG Xu- xian. HyperSafe:a lightweight approach to provide lifetime hypervisor control- flow integrity[C]//Proc of IEEE Sym-posium on Security and Privacy. Washington DC:IEEE Computer Society, 2010:380-395..
4. JONATHAN M M, NING Q, LI Y L, et al. TrustVisor: efficient TCB reduction and attestation[A]. Proc of the IEEE Symposium on Security and Privacy[C]. Oakland, USA, 2010. 143-158..

相似文献列表　文字复制比：2.7%(325)　疑似剽窃观点：(0)

1	基于扩展LS~2的可信虚拟平台信任链分析 常德显;冯登国;秦宇;张倩颖; -《通信学报》- 2013-05-25	2.7%（325） 是否引证：否

	原文内容	相似内容来源
1	此处有 53 字相似 l(m)、vTPM Builder(m) 、 vTPM-VM Binding(m)、VM Builder(m)的顺序进行 信任链构建。该信任属性形式化表示为 ProtectedSRTM(m)+ Mem(m.pcr.s,seq (BIOS(m),OSLoader(m),VMM(m),Dom0_Kernel(m),vTPMBuilder(m), v	基于扩展LS~2的可信虚拟平台信任链分析 常德显;冯登国;秦宇;张倩颖; -《通信学报》- 2013-05-25（是否引证：否） 1.vm)),那么该vm的本地信任链传递过程就是唯一的、正确的,即确定地从INIT(vm)到BL(vm)再到OS(vm)。该信任属性形式化表示为 DRTMSRTMProtectedSRTM(vm)Mem(m..vm,seq(INIT(vm),BL(vm),OS(vm),APP(vm)))MeasuredBoot(vm,)Jv pcrt证明首先
2	此处有 43 字相似 0_Kernel(m),vTPM Builder(m), vTPM-VM Binding(m), VM Builder(m)))成立，可以利用LS2的PCR公理可知，上述公式中的所有的子序列都会在时间t之前 被扩展到m.pcr.s中，用形式化表示为： tS,t1,t2,t3,t4, t5,t6,J.(tSt1<t2<t3<t	基于扩展LS~2的可信虚拟平台信任链分析 常德显;冯登国;秦宇;张倩颖; -《通信学报》- 2013-05-25（是否引证：否） 1.据前提条件可知在时间点t有Mem(m.v pcr.vm,seq(INIT(vm),BL(vm),OS(vm),APP(vm)))成立,反复利用PCR公理即可直接得到在该序列中的所有子序列一定在时间t之前就出现在m.vpcr.vm中,即1 2 3 1 2 332,,,,.()(Mem(m..vm,seq(INIT(vm),
3	此处有 43 字相似 信计算中基于实体预期行为的表述可以推理出只有得到正确的预期的PCR值，信任链的构建才可以继续，程序才可以继续被加载。 信任链远程验证 主机m的信任属性不仅仅表现在本地属性的验证上，还需要对远程验证者证明 自己在信任链传递过程中，所有程序的加载都是按照预期顺序进行的，从而建立了安全可靠的可信计算环境。 LS2中对远程验证的属性	基于扩展LS~2的可信虚拟平台信任链分析 常德显;冯登国;秦宇;张倩颖; -《通信学报》- 2013-05-25（是否引证：否） 1.张兴等人基于无干扰模型对信任链进行了建模分析[8],从系统信息流控制角度验证满足传递无干扰安全策略的信息流才能构建有效的信任链。为了验证本地的信任属性,需要利用远程证明协议对远程验证方提供验证。冯登国等[9,10]基于国际可信计算组织(TCG,TrustedComputing Group
4	此处有 59 字相似) MeasureBootSRTM(m,t) (4) 属性（4）可由属性（3）根据定理4.1直接得出，因此本文再次对 属性（3）进行证明： 证明：首先根据前提假设及[Verifier(m)]，利用公理VER可得到： [Verifie r(m)]tf,e,l.(tf<te)= (m)Contain(e,SIGAIK(m)-1) {|PCR(s), se	基于扩展LS~2的可信虚拟平台信任链分析 常德显;冯登国;秦宇;张倩颖; -《通信学报》- 2013-05-25（是否引证：否） 1.Boot t(4)这两个属性有递进关系,即如果属性(3)证明成立,则属性(3)利用定理1的结论直接可证。因此,这里需要明属性(4)。证明首先根据前提假定及,[Verifier(vm)]Vtb te,利用公理VER可直接得到,[Verifier(vm)]Vt b te S,,.(S e)t e l t t l AIK(vm)1(vm)Contain(,{|()
5	此处有 72 字相似 程验证过程中如果程序没有执行相关内存写入的操作，则数据e'，e"的顺序一点是先读取了e"然后才能进行数据e'的发送，并且 e'是一个经过签名的值。	基于扩展LS~2的可信虚拟平台信任链分析 常德显;冯登国;秦宇;张倩颖; -《通信学报》- 2013-05-25（是否引证：否） 1.PCR s e该属性表明在验证过程中如果本地没有写入内存的操作且发送了数据e',则在之前的某时刻本地一定

	本文将利用推理规则SEQ和公理Act1证明上述不变量成立。利用诚实规则并进行简化后可得[26]： [Verifie r(m)]tR,e,I.(tR<te)= (m) Contain(e,SIGAIK(m)-1){|PCR(s), se	读取了值e",且e'是一个签名值。利用推理规则SEQ和公理Act1证明上述不变量成立。利用诚实规则并进行简化后可得,[Verifier(vm)]Vt b te R,,",.(R e)t e e I t t I AIK(vm)11(vm)(vm)Con
6	此处有 55 字相似) 根据公理PCRC： ├(Mem(m.pcr.s,e'')@t) Contains(e,SIGK{|e'|}) 以及Mem(m.pcr.s,e'')存在的事实，可知式(14)中第2种可能不成立，故只有 e''= seq(BIOS(m),OSLoader(m),VMM(m), Dom0_Kernel(m), vTPM Builder(m),	基于扩展LS~2的可信虚拟平台信任链分析 常德显;冯登国;秦宇;张倩颖; -《通信学报》- 2013-05-25 (是否引证：否) 1.s(6)根据公理 PCRC(Mem(m..vm,")@)Contains(,K{|'|})vpcr e t e SIG e以及Mem(m.v pcr.vm,e")存在的事实,可知式(6)中第2种可能不成立,故只有 e"seq(INIT(vm),BL(vm),OS(vm),APP(vm))成立。利用等值公理Eq对式(5)进行变换可得,[Verif

指　标

疑似剽窃文字表述

---

1. 信任链远程验证
   主机m的信任属性不仅仅表现在本地属性的验证上，还需要对远程验证者证明

脚注和尾注

1. Mozilla Firefox Ltd.[EB/OL] http://www.firefox.com.cn/download/.2017.
2. CodeWeavers Inc.[EB/OL]https://www.winehq.org/.2017.
3. Kingsoft Office Corporation.[EB/OL]http://linux.wps.cn/.2017.
4. The Eclipse Foundation.[EB/OL]https://www.eclipse.org/downloads/..

5. 齐能_20151304001_信息安全.doc_第5部分

总字数：11180

相似文献列表　文字复制比：12.9%(1447)　疑似剽窃观点：(0)

1	基于无干扰的云计算环境行为可信性分析 张帆;张聪;陈伟;胡方宁;徐明迪; -《计算机学报（优先出版）》- 2017-07-28 12:54	6.9%（775） 是否引证：是
2	一种基于无干扰模型的信任链传递分析方法 张兴;黄强;沈昌祥; -《计算机学报》- 2010-01-15	3.6%（402） 是否引证：是
3	基于扩展LS~2的可信虚拟平台信任链分析 常德显;冯登国;秦宇;张倩颖; -《通信学报》- 2013-05-25	1.4%（154） 是否引证：否
4	可信云环境下软件仿真型vTPM密钥保护的研究 王闪(导师：谭良) -《四川师范大学硕士论文》- 2017-03-30	0.9%（98） 是否引证：否
5	无干扰可信模型及可信平台体系结构实现研究 张兴(导师：沈昌祥) -《解放军信息工程大学博士论文》- 2009-04-20	0.6%（69） 是否引证：否

原文内容		相似内容来源
1	此处有 105 字相似 inding(TJP),VM Builder(TJP)) 图4.4 TVP-QT中m信任传递的远程验证程序 首先，m 读取本地TJP的PCR值，用AIK签名（AIK-1(m)）并将其发送给挑战者。然后，挑战者验证该签名，并用预期的度量值序列与收到的值进行对比，如果匹配，则表明该主机m的TJP拥有所声称的可信属性，否则验证失败。 同样的，为防止远程验证的合理性，外部实体和TJP也应是不同的实体。	基于扩展LS~2的可信虚拟平台信任链分析 常德显;冯登国;秦宇;张倩颖; -《通信学报》- 2013-05-25 (是否引证：否) 1.OS(vm),APP(vm)))sigv sig AIKv vPCR图5 TVP中虚拟机信任传递的远程验证程序首先,vm读取本地虚拟PCR值,用自己的AIK签名(1AIK(vm))并将其发送给挑战者。然后,挑战者验证该签名,并用预期的度量值序列与收到的值进行对比,如果匹配,则表明该vm拥有所声称的可信属性,否则验证失败。在此过程中,vRT必须先于vm启动以确保vm信任链建立,且远程验证者与vm应是不同实体,以保证该验证过程的有效性。将这些

	这些前提条件形式化表示为 DRTM = {Hon	
2	此处有 52 字相似 也应是不同的实体。 这些前提条件形式化表示为 DRTM = {Honest(AIK(m)),AIK(m)} （2） 信任链属性的远程验证 根据相应的远程验证的执行流程，TJP远程证明的信任属性的验证目标可表示为定理4. 4。 定理 4.4 如果PCR中存储TJP度量值得序列是 seq(vTPM Builder(TJP),vTPM-VM B	基于扩展LS~2的可信虚拟平台信任链分析 常德显;冯登国;秦宇;张倩颖; -《通信学报》- 2013-05-25（是否引证：否） 1.RTMDRTM SRTM{Honest((vm)),(TPM(m)(vm)),(vm)}ΓAIKvRT V AIK 2)信任链属性的远程验证根据远程证明协议执行流程,给出以下信任传递属性的远程证明目标。定理2如果远程验证者确认vm提供的度量值是唯一的、正确的,那么该vm对应的PCR值一定是如下的确定序列 seq(INIT(vm
3	此处有 32 字相似 动作执行后）； （2）一个由系统中可能对系统状态产生影响的所有不可再分的原子动作集合A，并且约定用a, b, c... 表示单独的原子动作； （3）一个由系统中所有可以进行动作执行的 动作所属的主体集合O，主体和动作之间并不是一一映射的关系，因为相同的动作可能由不同的动作主体发出，而一个特定的主体可以发	基于无干扰的云计算环境行为可信性分析 张帆;张聪;陈伟;胡方宁;徐明迪; -《计算机学报（优先出版）》- 2017-07-28 12:54（是否引证：是） 1.46.pdf4 计 算 机 学 报 2017 年等表示系统状态；（6）一个由系统中所有原子动作组成的动作集 ，约定用 等表示原子动作；（7）一个由系统中所有行为构成的行为集 。其中，行为表达为原子动作序列的形式 ，约定用希腊字母 等表示行为。一个行为的示例是,其中 是连接符；（8）一个输出集 ，
4	此处有 35 字相似 相同的动作可能由不同的动作主体发出，而一个特定的主体可以发出不同的动作。即每一个属于中的动作都有一个包含于中的主体集。即 动作的主体集； （4）一个由系统中所有由特定动作集组成的行为序列集。 行为一般表示为几个动作的组成，行为类似于程序的存在，可以包含不同的进程。在本文中约定用希腊字母等表示行为。一个行为可以表	基于无干扰的云计算环境行为可信性分析 张帆;张聪;陈伟;胡方宁;徐明迪; -《计算机学报（优先出版）》- 2017-07-28 12:54（是否引证：是） 1.df4 计 算 机 学 报 2017 年等表示系统状态；（6）一个由系统中所有原子动作组成的动作集 ，约定用 等表示原子动作；（7）一个由系统中所有行为构成的行为集 。其中，行为表达为原子动作序列的形式，约定用希腊字母 等表示行为。一个行为的示例是,其中 是连接符；（8）一个输出集 ，其
5	此处有 33 字相似 系统中所有由特定动作集组成的行为序列集。行为一般表示为几个动作的组成，行为类似于程序的存在，可以包含不同的进程。在本文中 约定用希腊字母等表示行为。一个行为可以表示为：，其中是连接符； （5）系统经过动作之后观察到的系统的输出集合()； （6）系统发出的每一个原子动作，都在当前状态下可以找到自身所属的	基于无干扰的云计算环境行为可信性分析 张帆;张聪;陈伟;胡方宁;徐明迪; -《计算机学报（优先出版）》- 2017-07-28 12:54（是否引证：是） 1.作组成的动作集 ，约定用 等表示原子动作；（7）一个由系统中所有行为构成的行为集 。其中，行为表达为原子动作序列的形式，约定用希腊字母 等表示行为。一个行为的示例是,其中 是连接符；（8）一个输出集 ，其中包含了使用动作 进行观察时所看到的结果 ；（9）每一个原子动作都有自身所属的安全域，这些安全域构成
6	此处有 32 字相似	基于无干扰的云计算环境行为可信性分析 张帆;张聪;陈伟;胡方宁;徐明迪; -《计算机学报（优先出版）》- 2017-07-

	能存在交集。即对于，有。且对应与系统状态，域也有相应的状态，用表示域状态集合，约定使用分别表示安全域的状态在系统状态为本 安全域状态，显然有； （7）系统安全策略和。安全域相互之间可以 存在特定的干扰信息流，具有无干扰关系的信息量彼此之间不能影响。和分别称为信息流的干扰和无干扰关系，一旦两个信息流存在干扰	28 12:54（是否引证：是） 1.输出集，其中包含了使用动作 进行观察时所看到的结果；（9）每一个原子动作都有自身所属的安全域，这些安全域构成的集合称为安全域集。；（10）安全策略 和 。安全域集之间可以有信息流动，信息是否能够在特定域间流动由安全策略 和 决定， 和 分别称为干扰和无干扰关系，两者互为补集；（11）安全域
7	此处有 36 字相似 扰关系的信息量彼此之间不能影响。和分别称为信息流的干扰和无干扰关系，一旦两个信息流存在干扰关系，则无干扰就不复存在； （8）动作主体到动作的映射函数：。返回一个特点动作所属的动作主体； （ 9）安全域到动作的映射函数：。返回一个特定动作所属的Min安全域，并且必然，使得。 （10）单步系统状态函数：。.单步	基于无干扰的云计算环境行为可信性分析 张帆;张聪;陈伟;胡方宁;徐明迪; -《计算机学报（优先出版）》- 2017-07-28 12:54（是否引证：是） 1.信息流动，信息是否能够在特定域间流动由安全策略 和 决定， 和 分别称为干扰和无干扰关系，两者互为补集；（11）安全域到动作的映射函数： 。 返回一个特定动作 所属的安全域 ；（12）单步函数: .单步函数描述的是机器从前一个状态，执行某个动作之后，应该到达的后一个状态。（13）行为结果函 数 ：
8	此处有 72 字相似 信息流存在干扰关系，则无干扰就不复存在； （8）动作主体到动作的映射函数：。返回一个特点动作所属的动作主体； （9） 安全域到动作的映射函数：。返回一个特定动作所属的Min安全域，并且必然，使得。 （10）单步系统状态函数：。.单步函数描述的是系从前一个状态， 由某一安全域某一动作主体执行某个动作之后，应该到达的后一个状态；在系统存在安全域中的主体，执行动作之后，对系统的改变为。	基于无干扰的云计算环境行为可信性分析 张帆;张聪;陈伟;胡方宁;徐明迪; -《计算机学报（优先出版）》- 2017-07-28 12:54（是否引证：是） 1.间可以有信息流动，信息是否能够在特定域间流动由安全策略 和 决定， 和 分别称为干扰和无干扰关系，两者互为补集；（11）安全域到动作的映射函数： 。 返回一个特定动作 所属的安全域 ；（12）单步函数: .单步函数描述的是机器从前一个状态，执行某个动作之后，应该到达的后一个状态。（13）行为结果函 数 ： 。行 为 结 果 函 数给出了：在状态使用特定的动
9	此处有 57 字相似 下的主体，执行动作之后，对安全域改变为； 且单步状态函数满足以下条件： 。 （11）行为结果函数：。行为结果函数： 给出了：在状态使用特定的动作所观察到的系统的输出集合； （12）行为执行函数：。如果用表示空动作序列，则可以表示 为： 对于系统状态： 对于安全域状态： 需要强调的是，无干扰模型将输入定义为行为，也就是原子动作的连接序列。本文遵	基于无干扰的云计算环境行为可信性分析 张帆;张聪;陈伟;胡方宁;徐明迪; -《计算机学报（优先出版）》- 2017-07-28 12:54（是否引证：是） 1.描述的是机器从前一个状态，执行某个动作之后，应该到达的后一个状态。（13）行为结果函 数 ： 。 行 为 结 果 函 数给出了：在状态使用特定的动作 所观察到的行为执行结果。（14）行为执行函数： 。如果用表示空动作序列，则 可以表示为右递归的形式: 。需要强调的是，无干扰模型[37]将输入（即原子动作的连接序列）定义为行为。本文遵从该定义而不对行为形
10	此处有 37 字相似	基于无干扰的云计算环境行为可信性分析 张帆;张聪;陈伟;胡方宁;徐明迪; -《计算机学报（优先出版）》- 2017-07-

	修改等操作单元对其进行修改。 （1）系统的存储单元集合N，该存储单元集合及其取值构成了系统在特定时刻下的系统状态； （2）系统的视图值集V。集合N中的每一个存储单元在系统的状态都会有一个特定 的可以表示系统目前状态的值。本文定义内容观察等函数表示目前状态的值； （3）系统视图观察函数。 定义5.3 域视图。	28 12:54（是否引证：是） 1.名字。所有存储单元名字的集合构成存储单元集 ，又叫做名字集 。显然，对于云计算系统 M，其存储单元集 由的名字构成： 。（2）值集 。每一个存储单元 在特定的状态 都会有一个特定的值 。具体的取值可以由下面的内容函数计算。所有取值的集合构成值集 。 （3）内容函数 。（4）观察函数 和修改函数 。观察
11	此处有 47 字相似 全域视图集合DS和对弈的视图值集合。安全域u中的存储单元在安全域的特定状态都会有一个特定的视图值集合； （2）域视图 内容函数。 （3）域视图观察函数和域视图修改函数。域视图的观察函数和修改函数分别给出了安全 域自身所拥有的存储单元的集合和可以进行修改操作的存储单元值的集合。 定义5.4 主体视图。 （1）在整个系统M中，域	基于无干扰的云计算环境行为可信性分析 张帆;张聪;陈伟;胡方宁;徐明迪; -《计算机学报（优先出版）》- 2017-07-28 12:54（是否引证：是） 1.一个存储单元 在特定的状态 都会有一个特定的值 。具体的取值可以由下面的内容函数计算。所有取值的集合构成值集 。（3）内容函数 。（4）观察函数 和修改函数 。观察函数和修改函数分别给出了特定的安全域所能观察和修改的存储单元的集合，其中 是幂集计算。定义 4. 关系 称为是等价关系，当且仅当同时满足输出一致性和（弱）单
12	此处有 31 字相似 仅次于安全域的单位为动作主体，动作主体对应系统中的存储单元在域不同状态下，由动作发出后，其存储单元也会改变。 主体视图 值集。动作主体每一个存储单元在特定的状态下都会有一个特定的值， 其中有。、 （2）主体视图内容函数。 （3）主体视图观察函数和主体视图函数。不同的主体能观察和修改的存储单元的集合不	基于无干扰的云计算环境行为可信性分析 张帆;张聪;陈伟;胡方宁;徐明迪; -《计算机学报（优先出版）》- 2017-07-28 12:54（是否引证：是） 1.有存储单元名字的集合构成存储单元集 ，又叫做名字集 。显然，对于云计算系统 M，其存储单元集 由的名字构成： 。（2）值集 。每一个存储单元 在特定的状态 都会有一个特定的值 。具体的取值可以由下面的内容函数计算。所有取值的集合构成值集 。（3）内容函数 。（4）观察函数 和修改函数 。观察
13	此处有 37 字相似 存储单元也会改变。 主体视图值集。动作主体每一个存储单元在特定的状态下都会有一个特定的值，其中有。、 （2）主体视图 内容函数。 （3）主体视图观察函数和主体视图函数。不同的主体能观察和修改 的存储单元的集合不同。 定义5.5 如果存在等价关系则系统必须同时满足输出一致性和单步一致性，只有这样在系统运行时才会	基于无干扰的云计算环境行为可信性分析 张帆;张聪;陈伟;胡方宁;徐明迪; -《计算机学报（优先出版）》- 2017-07-28 12:54（是否引证：是） 1.一个存储单元 在特定的状态 都会有一个特定的值 。具体的取值可以由下面的内容函数计算。所有取值的集合构成值集 。（3）内容函数 。（4）观察函数 和修改函数 。观察函数和修改函数分别给出了特定的安全域所能观察和修改的存储单元的集合，其中 是幂集计算。定义 4. 关系 称为是等价关系，当且仅当
14	此处有 167 字相似 5 如果存在等价关系则系统必须同时满足输出一致性和	基于无干扰的云计算环境行为可信性分析 张帆;张聪;陈伟;胡方宁;徐明迪; -《计算机学报（优先出版）》- 2017-07-28 12:54（是否引证：是）

	单步一致性，只有这样在系统运行时才会两个不同的域或者主体是等价的。 （1）输出一致性： 在系统视图上：。 并且由可得域视图的输出一致性： 。 （2）系统单步一致性和弱单步一致性： 对于云计算环境下的传递安全策略，必须满足以下描述的单步一致性： 。 而对于非传递安全策略，则需要满足以下的弱单步一致性： 。 从单步一致性和弱单步一致性可看出，其实弱单步一致性仅仅增加了一个很重要的条件。 因为，弱单步一致性是在满足单步一致性的前提下的安全策略。 定义5.6 云计算环境下的间接干扰关系。 对于云计算环境下	1.修改的存储单元的集合，其中 是幂集计算。定义 4. 关系 称为是等价关系，当且仅当同时满足输出一致性和（弱）单步一致性。（1）输出一致性：。（2）（弱）单步一致性：对于传递安全策略，需满足单步一致性：。对于非传递安全策略，需满足弱单步一致性：。与单步一致性相比，弱单步一致性增加了条件，这个条件很重要。这是因为：弱单步一致性对应的是非传递无干扰，因此其除了要考虑直接干扰 关系之外，还要考虑间接干扰关系上的
15	此处有 53 字相似 步一致性可看出，其实弱单步一致性仅仅增加了一个很重要的条件。因为，弱单步一致性是在满足单步一致性的前提下的安全策略。 定义5.6 云计算环境下的间接干扰关系。 对于云计算环境下的非传递安全策略而言，系统中的安全域u虽然不能 直对w产生干扰，，但是，仍然可以间接对进行干扰(因为)。因此本文在定义5.1中的可以被当做直接干扰关系的基础上对间接干扰	基于无干扰的云计算环境行为可信性分析 张帆;张聪;陈伟;胡方宁;徐明迪; -《计算机学报（优先出版）》- 2017-07-28 12:54（是否引证：是） 1.的安全域 必须具有对该存储单元修改授权，即:由于传递无干扰是非传递无干扰的一个特例，下面继续给出非传递无干扰的相关定义。定义 6. 间接干扰关系 。对于非传递安全策略 而言，安全域 虽然不能直接干扰安全域（因为），但是，仍然可以间接对进行干扰(因为)。若将定义 2 当中的干
16	此处有 71 字相似 义如下: ，且 。其中，。 定义5.8 弱预期函数。 云计算环境下的弱预期函数可以被表述为：对安全域中无论是存在 直接干扰关系还是间接干扰关系的动作都进行保留，并将不存在干扰关系的动作进行剔除，从而可以判断出在非传递无干扰安全策略下的系统的整体的预期行为。 由于信任链的构建从链式构建的角度上看，前后进行度量的组件才会存在干扰关系，所以弱预期函数可以从信任链的构建机制上进行验证	基于无干扰的云计算环境行为可信性分析 张帆;张聪;陈伟;胡方宁;徐明迪; -《计算机学报（优先出版）》- 2017-07-28 12:54（是否引证：是） 1.义 8. 弱预期函数 。，且。其中，，。弱预期函数 的含义是，“将所有对安6 计 算 机 学 报 2017 年全域 有直接或间接的干扰关系的动作保留，并将除此以外的所有动作删除”，从而得到在非传递无干扰安全策略控制下的预期行为。定义 9. 域集等价关系：。定义 10. 非传递安全策略下局部无干扰属性。。3 云系统下行为可信性分析3.1 非传递
17	此处有 54 字相似 以弱预期函数可以从信任链的构建机制上进行验证[58]。 ，且 。	一种基于无干扰模型的信任链传递分析方法 张兴;黄强;沈昌祥; -《计算机学报》- 2010-01-15（是否引证：是） 1.一状态和发出该动作的域在发出动作之前状态的系统视图.基于上述定义,文献[5]给出了下面的展开定理(unwinding).定理1.系统满足非传递性无干扰策略的判定定理.设M是一个视图隔离的系统,有一个具有非传递性

	其中，， 。 定义5.9 域集等价关系。 定理5.1 云计算环境下系统需要满足的非传递无干扰策略的判定定理。 存在一个在视图角度上存在隔离的系统M， 如果M的安全域之间存在非传递的干扰关系，并且同时满足系统弱单步一致性、局部干扰性、输出一致性时，则该系统满足非传递无干扰	的~>策略,并且M满足:输出一致性、弱单步一致性和局部干扰性,则M满足非传递性无干扰策略.在无干扰模型
18	此处有 38 字相似 统状态的论述。同理，从安全域角度描述安全策略，则需要对动作主体的输入和对系统状态的进行论述。 定理5.2 TVP-QT 系统需要满足非传递无干扰关系的判定定理。 （1）系统的域满足输出一致性。 某个系统域的系统视图的改变只能因为内部的动作和行为执行，不能因为由其他域的动作或行为引起。且满足以下条件： （2）相	一种基于无干扰模型的信任链传递分析方法 张兴;黄强;沈昌祥; -《计算机学报》- 2010-01-15（是否引证：是） 1.,本文给出无干扰信任传递判定定理,用于判定可观测的系统状态和输出在满足什么条件时,信任链的建立和传递才是有效的.定理2.系统满足非传递无干扰关系的判定定理:(1)系统的域满足输出一致性.即一个内部操作动作造成的输出影响只依赖于发出动作域的系统视图.(2)系统中发生的一个动作造成的对系统状态影响只与发出该动
19	此处有 48 字相似 足输出一致性。动作主体的系统视图的改变只能依赖于该主体的内部所属动作，不同主体的动作是不能产生影响的。 ； （3） 系统中发生的一个动作造成的对系统状态影响只与发出该动作的域的上一状态系统视图相关联[58]。 （4）相对于（3），系统中发生的一个动作造成的对安全域状态影响只与发出该动作的动作主体的上一状态系统视图相关联。 （	一种基于无干扰模型的信任链传递分析方法 张兴;黄强;沈昌祥; -《计算机学报》- 2010-01-15（是否引证：是） 1.无干扰关系的判定定理:(1)系统的域满足输出一致性.即一个内部操作动作造成的输出影响只依赖于发出动作域的系统视图.(2)系统中发生的一个动作造成的对系统状态影响只与发出该动作的域的上一状态系统视图相关联.即 sdo~m(a)t∧(contents(step(s,a),n)≠contents(s,n)vcontents(ste
20	此处有 48 字相似 系统中发生的一个动作造成的对系统状态影响只与发出该动作的域的上一状态系统视图相关联[58]。 （4）相对于（3）， 系统中发生的一个动作造成的对安全域状态影响只与发出该动作的动作主体的上一状态系统视图相关联。 （5）系统中，如果一个动作改变了其动作主体的值，则发出该动作的主体一定可以写、访问该主体的系统视图，并且可以写、访问该	一种基于无干扰模型的信任链传递分析方法 张兴;黄强;沈昌祥; -《计算机学报》- 2010-01-15（是否引证：是） 1.无干扰关系的判定定理:(1)系统的域满足输出一致性.即一个内部操作动作造成的输出影响只依赖于发出动作域的系统视图.(2)系统中发生的一个动作造成的对系统状态影响只与发出该动作的域的上一状态系统视图相关联.即 sdo~m(a)t∧(contents(step(s,a),n)≠contents(s,n)vcontents(ste 无干扰可信模型及可信平台体系结构实现研究 张兴 -《解放军信息工程大学博士论文》- 2009-04-20（是否引证：否） 1.，a为域u发出的一个动作，满足:s一t峥ou加ut(s，a)=ou加ut(t，a)2.可信管道中发生的一个动作造成的对系统状态影响只与发出该动作的域的上一状.S~tA (contents(steP(s，a)，n)护contents(s，n)v

		contents
21	此处有 39 字相似 相对于（3），系统中发生的一个动作造成的对安全域状态影响只与发出该动作的动作主体的上一状态系统视图相关联。 （5） 系统中，如果一个动作改变了其动作主体的值，则发出该动作的主体一定可以写、访问该 主体的系统视图，并且可以写、访问该动作所在的域的系统状态。 系统内对系统内的系统状态的操作有以下关系。 （6）系统	一种基于无干扰模型的信任链传递分析方法 张兴;黄强;沈昌祥; -《计算机学报》- 2010-01-15（是否引证：是） 1.ntents(t,n))→contents(step(s,a),n)=contents(step(t,a),n).(3)系统中,如果一个动作改变了一个客体对象的值,则发出该动作的域一定可以写访问该客体对象.即contents(step(s,a),n)≠contents(s,n)→n∈alter(dom(a),s). 无干扰可信模型及可信平台体系结构实现研究 张兴 -《解放军信息工程大学博士论文》- 2009-04-20（是否引证：否） 1.steP(t，a)，n)态系统视图相关联。a为域u发出的一个动作，即: 3.可信管道域中，如果一个动作改变了一个客体对象的值，则发出该动作的域一定可以写访问该客体对象。即 contents(steP(s，a)，n)护contents(s，n)一n〔。打er(面
22	此处有 29 字相似 统进行了仿真，具体的仿真实验可以结合本文第三章的第3节和第4节的基于Xen的实例系统和仿真实验，在此不再重复叙述。此实例 系统利用虚拟机监视提供的资源隔离机制实现了满足扩展无干扰的 安全系统。在该系统中，运行的安全域必须通过VMM才可以进行信息交流，所以每个安全域彼此之间是不能直接进行信息交流的。	一种基于无干扰模型的信任链传递分析方法 张兴;黄强;沈昌祥; -《计算机学报》- 2010-01-15（是否引证：是） 1.定性和可预期性,能够确保信任链的建立不受系统中组件间干扰行为的影响.5原型实现与验证我们基于开源的虚拟机监视器(VMM)系统Xen[4,7],利用虚拟隔离实现了一个满足非传递无干扰的系统.它将应用完全隔离,各应用之间不能直接共享信息,所有隔离域之间的信息交换均通过虚拟机监视器进行.如图4所示,VMM系统上的
23	此处有 35 字相似 上的前端驱动和运行于VMM之上的后端驱动组成，实现对硬件功能的使用。该用户虚拟机在运行过程中产生的信息流可以从图中的顺序 进行传递。若使该虚拟机信任链有效，必须确保系统中存在非预期的干扰。 根据定理5.2，基于Xen的TVP-QT系统的I/O设备是满足定理5.1的要求的；验证描述如下： 由输出一致性的定义可	一种基于无干扰模型的信任链传递分析方法 张兴;黄强;沈昌祥; -《计算机学报》- 2010-01-15（是否引证：是） 1.安全等级的应用系统,VMM系统上的信任链由图左侧的和②两步建立(先由硬件平台验证基础软件层VMM,再由VMM对虚拟机整体进行验证).但若使信任链有效,必须确保系统中不存在非预期的干扰,即图4非传递无干扰关系示意图VMM系统中运行于VMM之上的虚拟机可以对应于无干扰模型的安全域,各个域之间的交互只通过I/
24	此处有 31 字相似 VMM而进行资源的访问，这是有VMM的资源隔离特性所决定的。因此虚拟机彼此之间是无法直接产生干扰关系的，所以虚拟机内部的 组件进行构建时，只有内部存在直接干扰关系的动作，而间接干扰关系 可以通过VMM进行隔离，保证了单个虚拟机组件的信任传递。由弱单步一致性定义可知，对于若干虚拟机共享的客体对象，VMM系统	一种基于无干扰模型的信任链传递分析方法 张兴;黄强;沈昌祥; -《计算机学报》- 2010-01-15（是否引证：是） 1.递无干扰关系,记作AINB.非传递无干扰关系描述的是一种隔离性要求比较严格的通道控制安全策略,具有非传递无干扰关系的系统组件之间只有直接干扰关系,不存在间接造成的干扰关系.4无干扰信任传递判定定理4.1非传递无干扰模型与信任链传递的关系基于以上分析可知,单纯的通过完整性验证实现的信任链传递是
25	此处有 69 字相似 的组件进行构建时，只有内部存在直接干扰关系的动作，而间接干扰关系可以通过VMM进行隔离，保证了单个	一种基于无干扰模型的信任链传递分析方法 张兴;黄强;沈昌祥; -《计算机学报》- 2010-01-15（是否引证：是） 1.机制确保虚拟机必须采用虚拟设备接口访问后端驱动

	虚拟机组件的信任传递。 由弱单步一致性定义可知，对于若干虚拟机共享的客体对象，VMM系统必须具有同步保护机制以防止不同虚拟机对该资源的竞争[58]。 综上，依据 本文给出的TVP-QT信任传递模型，经过完整性验证，系统运行能够达到可信目标。 本章小结 本章按照云计算环境运行特征	程序.每个虚拟机能够访问的I/O寄存器被限制,能够禁止未授权的访问.(3)由弱单步一致性定义可知,对于若干虚拟机共享的客体对象,VMM系统必须具有同步保护机制以防止不同虚拟机对该资源的竞争.该系统依据非传递无干扰策略模型对传统VMM的虚拟I/O设备体系进行了改造,只要根据应用程序需求,合理划分安全域,各应用安全域的运行
26	此处有 29 字相似 Xen的TVP-QT的分析和验证证明了，TVP-QT是满足扩展无干扰安全判定定理的。 总结与展望 工作总结 本文对 具有瀑布特征的可信虚拟平台及其信任链模型、信任链形式化分析 方法进行研究。针对目前可信虚拟平台逻辑不合理、设计粒度过粗的问题，提出了一种具有瀑布特征的可信虚拟平台架构，该可信虚拟平	一种基于无干扰模型的信任链传递分析方法 张兴;黄强;沈昌祥; -《计算机学报》- 2010-01-15（是否引证：是） 1.干扰的存在导致了系统运行可信,提出了可信计算平台的信任链传递模型;第4节分析了非传递无干扰模型与信任链传递的关系,提出了具有干扰关系的可信计算平台的信任链传递模型,分析了组件干扰与平台信任传递的关系,指出系统域间无干扰也就意味着系统输出的确定性和可预期性,依据无干扰理论给出了一种判定可信
27	此处有 45 字相似 前可信虚拟平台逻辑不合理、设计粒度过粗的问题，提出了一种具有瀑布特征的可信虚拟平台架构，该可信虚拟平台架构在层次上添加了 可信衔接点层次，主要由虚拟机构建模块、虚拟可信平台模块构建模块、虚拟机和其虚拟可信平台模块 绑定模块组成。当可信虚拟平台启动时，不仅可以以静态度量方式参与底层虚拟化平台的启动，也可以和虚拟可信模块共同作为虚拟机启	可信云环境下软件仿真型vTPM密钥保护的研究 王闪 -《四川师范大学硕士论文》- 2017-03-30（是否引证：否） 1.ement，DRTM）[47]实现信任链的多次完整性度量，这就是动态可信度量根技术。122.3 可信计算虚拟化 2.3.1 虚拟可信平台模块的概念虚拟可信平台模块（virtual Trusted Platform Module，v TPM）[14],它通过模拟硬件 TPM
28	此处有 32 字相似 个运行过程是安全可信的，基于安全系统逻辑形式化方法进行该信任链进行形式化分析，证明了该信任链的安全性。 此外基于扩展的 无干扰理论形式化方法进行信任链形式化分析，针对目前的非传递无干扰 理论均没有考虑到云计算运行中时的安全域、动作所属主体以及动作对安全域和系统状态的影响进行详细的说明，对无干扰理论在安全域	基于无干扰的云计算环境行为可信性分析 张帆;张聪;陈伟;胡方宁;徐明迪; -《计算机学报（优先出版）》- 2017-07-28 12:54（是否引证：是） 1.一致的，因而云系统一定是安全的。基于定义 12 的形式，目前尚没有有效的属性验证方法（仅仅文献[35]给出了多项式实践的无干扰属性验证方法，然而其所针对的非传递无干扰属性并非 Rushby 的原始定义，而是其一种变体）。接下来，本文将基于两个状态机寻求定义 12 的验证理论。定义 13
29	此处有 53 字相似 能,谭良. 一种具有瀑布特征的可信虚拟平台信任链模型[C]// CTCIS2017.长沙.（会议论文） 参与的科研项目 ： [1]. 国家自然科学基金项目：可信平台模块虚拟化问题	可信云环境下软件仿真型vTPM密钥保护的研究 王闪 -《四川师范大学硕士论文》- 2017-03-30（是否引证：否） 1.[1] 发明专利“数据处理装置及方法”, 201510615762.7, 谭良,王闪.参与的科研项目：[1] 国家自然科学基金项目：可信平台模块虚拟化问题研究. 编号：61373162.[2] 王闪. 四川师范大学研究生优秀论文培育基金. 编号：校研字[2016]4 -19.

	研究. 编号：61373162. [2]. 国家自然科学基金项目：低碰撞区跳频序列在高动态无线通信网络中的应用 研究. 编号：61701331.	

指　标

疑似剽窃文字表述

---

1. 然后，挑战者验证该签名，并用预期的度量值序列与收到的值进行对比，如果匹配，则表明该主机m的TJP拥有所声称的可信属性，否则验证失败。
2. 可信衔接点层次，主要由虚拟机构建模块、虚拟可信平台模块构建模块、虚拟机和其虚拟可信平台模块

说明：1.总文字复制比：被检测论文总重合字数在总字数中所占的比例

2.去除引用文献复制比：去除系统识别为引用的文献后，计算出来的重合字数在总字数中所占的比例

3.去除本人已发表文献复制比：去除作者本人已发表文献后，计算出来的重合字数在总字数中所占的比例

4.单篇最大文字复制比：被检测文献与所有相似文献比对后，重合字数占总字数的比例最大的那一篇文献的文字复制比

5.指标是由系统根据《学术论文不端行为的界定标准》自动生成的

6.红色文字表示文字复制部分;绿色文字表示引用部分

7.本报告单仅对您所选择比对资源范围内检测结果负责

amlc@cnki.net

http://check.cnki.net/

http://e.weibo.com/u/3194559873