文本复制检测报告单(全文对照)

№:ADBD2018R_2018013011075920180313133052802134806605　　检测时间:2018-03-13 13:30:52

检测文献:　6_齐能_具有瀑布特征的可信虚拟平台信任链模型

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

学术论文联合比对库

个人比对库

时间范围:　1900-01-01至2018-03-13

检测结果

总文字复制比：21.6%　　跨语言检测结果：0%

去除引用文献复制比：18.7%　　去除本人已发表文献复制比：21.6%

单篇最大文字复制比：10.3%（基于扩展LS~2的可信虚拟平台信任链分析）

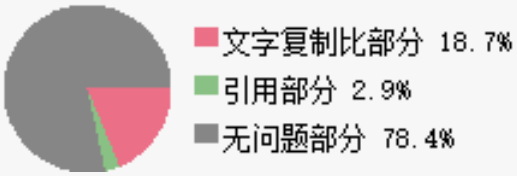
重复字数：[11592]　　总段落数：[5]

总字数：[53634]　　疑似段落数：[5]

单篇最大重复字数：[5519]　　前部重合字数：[500]

疑似段落最大重合字数：[4369]　　后部重合字数：[11092]

疑似段落最小重合字数：[500]



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

4.5%（500）　6_齐能_具有瀑布特征的可信虚拟平台信任链模型_第1部分（总11073字）

29.7%（2632）　6_齐能_具有瀑布特征的可信虚拟平台信任链模型_第2部分（总8867字）

15.4%（1585）　6_齐能_具有瀑布特征的可信虚拟平台信任链模型_第3部分（总10300字）

21.1%（2506）　6_齐能_具有瀑布特征的可信虚拟平台信任链模型_第4部分（总11850字）

37.8%（4369）　6_齐能_具有瀑布特征的可信虚拟平台信任链模型_第5部分（总11544字）

（注释：无问题部分　文字复制比部分　引用部分）

疑似剽窃观点　(1)

6_齐能_具有瀑布特征的可信虚拟平台信任链模型_第2部分

1. 由此可见，启动序列中的任意序列受到破坏都会对整个系统的运行安全产生影响，因此，必须有一种强有力的信任机制来评估系统启动过程是否已经被攻击者所篡改。

1. 6_齐能_具有瀑布特征的可信虚拟平台信任链模型_第1部分　　总字数：11073

相似文献列表　文字复制比：4.5%(500)　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	3.6%（400）

	常德显;冯登国;秦宇;张倩颖; -《通信学报》- 2013-05-25	是否引证：否
2	资本助力 电子政务催生千亿市场	0.4%（39）
	高振刚; -《中国战略新兴产业》- 2018-01-18	是否引证：否
3	风起“云”涌 4300亿市场“蛋糕”待分享	0.3%（38）
	本报记者 刘艳 -《科技日报》- 2017-05-03	是否引证：否
4	莞企腾“云” 技术升级一身轻	0.3%（37）
	本报记者 肖剑雄 -《东莞日报》- 2017-04-17	是否引证：否
5	2019年产业规模力争达到4300亿元	0.3%（35）
	记者 孙冉冉 -《中国政府采购报》- 2017-04-18	是否引证：否
6	工信部布局未来三年云计算发展路径	0.3%（35）
	MEB记者 何珺 -《机电商报》- 2017-04-17	是否引证：否
7	2019年云计算产业规模达4300亿元	0.3%（34）
	记者 刘瑾 -《经济日报》- 2017-04-11	是否引证：否

原文内容	相似内容来源
1 此处有 40 字相似 均每年增长率为21.7%。2016年我国的云计算市场达到514.9亿元，增速为35.9%，处于全球国家云计算发展的前列。 2017年，工业和信息化部发布的《云计算发展三年行动计划（2017 - 2019年）》[]提到，我国云计算的发展目标“到2019年，我国云计算产业规模达到4300亿元”，该行动计划为我国云计算和云计算安全	资本助力 电子政务催生千亿市场 高振刚; -《中国战略新兴产业》- 2018-01-18（是否引证：否） 1.13626亿元的高点,投资前景十分广阔。政务云进入随着云计算市场的不断发展,政务云已成为政府数字化转型的有力支撑。2017年4月,工信部编制《云计算发展三年行动计划(2017-2019年)》,明确提出以工业云、政务云等重点行业领域应用为切入点,加快信息系统向云平台的迁移,到2019年,我国云计算产业规模达到43 2019年云计算产业规模达4300亿元 记者 刘瑾 -《经济日报》- 2017-04-11（是否引证：否） 1.本报北京4月10日讯 记者刘瑾报道：工业和信息化部近日印发的《云计算发展三年行动计划（2017-2019年）》提出，到2019年，我国云计算产业规模达到4300亿元，突破一批核心关键技术，云计算服务能力达到国际先进水平，对新一代信息产业
2 此处有 48 字相似 于全球国家云计算发展的前列。2017年，工业和信息化部发布的《云计算发展三年行动计划（2017 - 2019年）》[]提到，我国云计算的发展目标“到2019年，我国云计算产业规模达到4300亿元”，该行动计划为我国云计算和云计算安全技术创新和产业发展指明了方向，提供了政策保障和法律依托。并且，根据著名安全公司McAfee发布的“2017年	风起“云”涌 4300亿市场“蛋糕”待分享 本报记者 刘艳 -《科技日报》- 2017-05-03（是否引证：否） 1.商也早就粉墨登场。$$近日工业和信息化部（下称工信部）印发的《云计算发展三年行动计划》（下称《行动计划》）提出，“到2019年，我国云计算产业规模达到4300亿元”。借助云计算这个经济发展新动能的助燃剂，为大数据、物联网、人工智能等新兴领域和传统行业的转型发展提供基础支撑。$$云服务商迎 莞企腾“云” 技术升级一身轻 本报记者 肖剑雄 -《东莞日报》- 2017-04-17（是否引证：否） 1.业和信息化部4月10日印发《云计算发展三年行动计划（2017-2019年）》（以下简称《行动计划》）。《行动计划》提出，到2019年，我国云计算产业规模达到4300亿元；支持云计算企业进入资本市场融资，开展并购、拓展市场，加快做大做强步伐。$$记者采访中了解到，近年来在政策的助推和企业的布局 工信部布局未来三年云计算发展路径 MEB记者 何珺 -《机电商报》- 2017-04-17（是否引证：否） 1.促进行动、安全保障行动和环境优化行动五项重点任务。$$定未来三年发展目标$$《行动计划》明确指出未来三年我国云计算发展的发展目标——“到2019年，我国云计算产业规模达到4300亿元，突破一批核心关键技

		术，云计算服务能力达到国际先进水平，对新一代信息产业发展的带动效应显著增强”。$$具体目标还包 2019年产业规模力争达到4300亿元 记者 孙冉冉 -《中国政府采购报》- 2017-04-18（是否引证：否） 1.动计划(2017-2019年)》(以下简称《计划》)，旨在释放市场需求，解决低水平重复建设等问题。$$《计划》为我国云计算未来三年的发展确立了目标。到2019年，我国云计算产业规模达到4300亿元，突破一批核心关键技术，云计算服务能力达到国际先进水平；云计算在制造、政务等领域的应用水平显著提升；云计算数据中心布局得到
3	此处有 51 字相似 信任链技术[]是可信计算的关键技术，针对可信计算技术与云计算技术结合的可信虚拟平台的信任链构建更是十分有必要的。利用 虚拟可信平台模块（Virtualization of Trusted Platform Module, vTPM）[]在云计算环境中构建安全可靠的可信虚拟平台，并且利用可信计算中的关键技术——信任链技术对整个云计算平台进行	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.台的需求,Stefan Berger[2]等人首先提出虚拟信任根(vRT,virtual root of trust)、虚拟可信平台模块(vTPM,virtual trusted platform module)的思想,通过为每个虚拟机提供独立的虚拟信任根来构建实现虚拟化可信平台的原型系统。HP和IBM的研究人员在虚拟信任根的基础上,分别
4	此处有 88 字相似 用以及抽象和统一的TVP概念取得了很多较好的研究成果，并且达成了一些基本的共识。目前，研究此方面的学者绝大多数都认为，在 物理上，TVP作为一个可以支持虚拟化技术的可信主机，并且与一般的可信计算平台的主要区别有两方面，一是拥有在物理硬件可信平台模块（Trusted Platform Module, TPM）构建起来的虚拟可信信任根；而是可以并发的为在可信虚拟平台之上的多个用户虚拟机（Virtual Machine,	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.提出并构建了相应的TVP[2~4],但这些研究主要侧重于具体应用场景的功能实现,缺乏一种抽象、通用的TVP定义。TVP在物理上体现为一个支持虚拟化技术的可信主机,它与普通可信计算平台的区别主要在于:1)拥有构建于硬件可信芯片可信平台模块(TPM,trusted platform module)基础上的虚拟信任根;2)并发地为多个客户应用虚拟机提供信任环境。基于已有研究方案,本文给出如图1所示的TVP基本
5	此处有 69 字相似 以并发的为在可信虚拟平台之上的多个用户虚拟机（Virtual Machine, VM）提供可信虚拟信任环境。这种TVP的 运行架构如图1.1所示。从功能上看，TVP架构主要分为4个层次。第一层为硬件信任根TVP，作为整个架构的最底层，是整个平台信任的物理保证。 第二层主要包括虚拟机监视器（Virtual Machine Monitor, VMM），及构建与VMM之上的管理域（主要	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.ule)基础上的虚拟信任根;2)并发地为多个客户应用虚拟机提供信任环境。基于已有研究方案,本文给出如图1所示的TVP基本运行架构。从功能上看,TVP主要分为4个层次,硬件信任根TPM作为最底层,是平台信任的物理保障。第二层主要包括VMM及管理域(主要是其内核及相关域管理工具,简记为admindomker),它们通常被认为是TVP的可信
6	此处有 63 字相似 的物理保证。第二层主要包括虚拟机监视器（Virtual Machine Monitor, VMM），及构建与VMM之上的 管理域（主要是其内核及相关域管理工具），它们通常被认为是 TVP 的可信计算基（Trusted Computing Base,	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.本运行架构。从功能上看,TVP主要分为4个层次,硬件信任根TPM作为最底层,是平台信任的物理保障。第二层主要包括VMM及管理域(主要是其内核及相关域管理工具,简记为admindomker),它们通常被认为是TVP的可

	TCB）。第三层是虚拟信任根（Virtual Root of Trust, vRT），由于实现方案不同，其加载过程可能	信计算基(TCB,trusted computingbase)。第三层是vRT,由于实现方案不同(如图1中a、b所示),其加载过程可能是传统信任链的一部分,或直接利用动态加载机制如动态
7	此处有 141 字相似 Base, TCB）。第三层是虚拟信任根（Virtual Root of Trust, vRT），由于实现方案不同，其 加载过程可能是传统信任链的一部分，或直接利用动态加载机制如动态度量信任根（Dynamic Root of Trusted Measurement, DRTM）机制启动，这使得它或者成为TCB 的一部分，或者作为应用进程单独存在。最上层是用户虚拟机，是与用户应用密切相关的部分。 图1.1 TVP基本运行架构 根据文献[24]的vRT等概念，HP、IBM等研究机构分别提出并构建了相应的TVP[30	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.计算基(TCB,trusted computingbase)。第三层是vRT,由于实现方案不同(如图1中a、b所示),其加载过程可能是传统信任链的一部分,或直接利用动态加载机制如动态度量信任根(DRTM,dynamic root of trusted measurement)机制启动,这使得它或者成为TCB的一部分,或者作为应用进程单独存在。最上层是用户虚拟机,是与用户应用密切相关的部分。基于上述分析,本文从功能角度给出以下TVP的抽象定义。图1 TVP基本运行架构定义1 TVP是具有可信功能的虚拟化计算平

指　标

疑似剽窃文字表述

1. 运行架构如图1.1所示。从功能上看，TVP架构主要分为4个层次。第一层为硬件信任根TVP，作为整个架构的最底层，是整个平台信任的物理保证。

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. 6_齐能_具有瀑布特征的可信虚拟平台信任链模型_第2部分

总字数：8867

相似文献列表　文字复制比：29.7%(2632)　疑似剽窃观点：(0)

1	王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2015-10-08	15.5%（1370） 是否引证：否
2	201603301253463317_王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2016-03-30	15.5%（1370） 是否引证：否
3	王星魁博士学位论文 -《学术论文联合比对库》- 2015-10-09	14.4%（1280） 是否引证：否
4	王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2015-10-04	14.4%（1276） 是否引证：否
5	201610071545221628_王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2016-10-07	13.3%（1176） 是否引证：否
6	10112_081203_b20090055_LW 王星魁 -《学术论文联合比对库》- 2016-03-31	13.3%（1176） 是否引证：否
7	基于无干扰理论的信任链传递模型 陈亮;曾荣仁;李峰;杨伟铭; -《计算机科学》- 2016-10-15	5.9%（524） 是否引证：否
8	信息郝瑞 -《学术论文联合比对库》- 2014-12-08	5.8%（510） 是否引证：否
9	201610072245292357_王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2016-10-07	4.8%（427） 是否引证：否
10	数据安全交换若干关键技术研究 陈亮(导师：陈性元) -《解放军信息工程大学硕士论文》- 2015-04-20	2.8%（246） 是否引证：否
11	TPM功能介绍 - Sunshine -《网络（http://blog.csdn.net）》- 2017	2.8%（245） 是否引证：否
12	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	1.7%（147） 是否引证：否
13	一个基于进程保护的可信终端模型 陈菊;谭良; -《计算机科学》- 2011-04-15	1.5%（129） 是否引证：是
14	基于可信计算的远程证明的研究 黄秀文; -《武汉纺织大学学报》- 2015-12-15	1.3%（118） 是否引证：否
15	虚拟化模型 - tengyft的专栏 - CSDN博客 -《网络（http://blog.csdn.net）》- 2017	1.3%（117） 是否引证：否
16	CentOS7下安装KVM - z936689039的博客 - CSDN博客 -《网络（http://blog.csdn.net）》- 2017	1.3%（116） 是否引证：否

17	KVM 介绍（1）：简介及安装 - 张某人ER的技术博客 ==学习&分享== - CSDN博客 - 《网络（http://blog.csdn.net）》- 2017	1.3%（116） 是否引证：否
18	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	0.9%（84） 是否引证：是
19	网络技术在新媒体发展中的应用分析 曾鹏;冯明明; - 《西部广播电视》- 2018-01-05	0.3%（30） 是否引证：否
20	基于共享内存的域间通信优化方法研究 吴鸿远(导师：万健) - 《杭州电子科技大学硕士论文》- 2015-05-01	0.3%（30） 是否引证：否
21	基于动态污点分析的二进制程序脆弱性检测技术研究 董国良(导师：臧洌) - 《南京航空航天大学硕士论文》- 2017-03-01	0.3%（29） 是否引证：否
22	基于可信计算的云计算安全若干关键问题研究 罗东俊(导师：唐韶华) - 《华南理工大学博士论文》- 2014-03-31	0.3%（29） 是否引证：否

原文内容		相似内容来源
1	此处有 116 字相似 对于确保平台信任可验证的信任链形式化建模与分析的方法，目前的研究大部分是基于传统的可信计算平台，并且国内研究较多。其中， 陈书义[]等人利用一阶逻辑对可信计算平台启动过程进行建模以分析其信任传递过程，并提出长度受限的信任链模型。张兴[]等人基于无干扰模型对信任链进行了建模分析，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。 上述方法主要针对普通可信计算平台，并不能直接适用于云计算环境下信任链形式化分析。虽然Zhang[26]等人利用无干扰理论	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） 1.6]。可信平台需要提供其信任证明,为此,需要对构建平台信任的基石——信任链进行形式化建模与分析,以确保平台信任的可验证。陈书义等人利用一阶逻辑对可信计算平台启动过程进行建模以分析其信任传递过程[7],并提出长度受限的信任链模型。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,Tr 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.有安全策略限制,讨论信任链传递是没有意义的.然后借鉴Trent的PRI MA方案,基于无干扰模型,用形式化的方法论述了当系统满足非传递无干扰的安全策略时,信任链的建立不受系统中其它安全无关组件与行为的干扰,信任才能有效地传递下去,系统能够建立完整的信任链,实现可信目标.并据此提出了无干
2	此处有 35 字相似 连续的可信云计算信任链模型上，不能够对可信云计算环境进行正确的形式化验证。 针对于无干扰理论的研究，目前大部分的研究是基于信息流的无干扰模型从动作和运行结果的角度建立系统安全策略模型[]。 其中，国外研究方向主要集中在系统外部和软件可信性上，Kai E[]把无干扰利用扩展到非确定性系统，通过系统外部通道共享信	基于无干扰理论的信任链传递模型 陈亮;曾荣仁;李峰;杨伟铭; -《计算机科学》- 2016-10-15（是否引证：否） 1.态的信任链。由于系统平台上应用的多样性及无序性,静态信任链的构建并不适用于操作系统到应用程序及终端到网络之间的可信传递。基于信息流的无干扰模型从动作和运行结果的角度建立系统安全策略模型,从而确保计算机系统的安全性和完整性。文献[2,3]在Rushby的无干扰理论[4]的基础上将系统安全域集实体化为进程集,
3	此处有 73 字相似 立了多级安全域的无干扰理论。 国内的针对无干扰理论的研究主要是将无干扰中的关键定义进行细分，比如，张兴[]、赵佳[]等 在Rushby的无干扰理论的基础上将系统安全域集实体化为进程集，给出了进程运行的可信条件，推导出系统运行可信定理，保证了终端的安全，但是其模型中的	基于无干扰理论的信任链传递模型 陈亮;曾荣仁;李峰;杨伟铭; -《计算机科学》- 2016-10-15（是否引证：否） 1.递。基于信息流的无干扰模型从动作和运行结果的角度建立系统安全策略模型,从而确保计算机系统的安全性和完整性。文献[2,3]在Rushby的无干扰理论[4]的基础上将系统安全域集实体化为进程集,给出了进程运行的可信条件,推导出系统运行可信定理,保证了终端的安全。但是其模型中的可信传递函数check()和clear()有待进一

	没有针对动作的详细定义，不适合验证可信云环境信任链。刘鹏威[]等提出了基于非传递的无干扰理念的二元多级安全模型，在Rus	步证明,并且缺乏对进程的动态保护。文献[5]提出了基于非传递的无干扰理 数据安全交换若干关键技术研究 陈亮 -《解放军信息工程大学硕士论文》- 2015-04-20（是否引证：否） 1.全属性检查函数,保证接入安全网络终端节点的可信性;无干扰理论模型从系统运行的角度,将系统抽象进程、动态、状态和输出,利用进程运行可信,推导出系统运行可信定理,保证了终端的安全性;CDSE模型从定制数据安全交换的整体出发,形式化描述了定制数据安全交换所涉及的元素及操作,并定义了行为约束规则,能够比较
4	此处有 390 字相似 推导出系统运行可信定理，保证了终端的安全，但是其模型中的没有针对动作的详细定义，不适合验证可信云环境信任链。刘鹏威[]等 提出了基于非传递的无干扰理念的二元多级安全模型，在Rushby无干扰理论的基础上重新定义了清除函数，将传递的无干扰理论过渡到非传递的无干扰理论，并依据BLP和Biba模型保护了信息的机密性和完整性，然而同样存在赵佳中的问题。陈菊[]等从进程数据和代码完整性检测出发，利用无干扰理论保证进程之间的操作合法，试图在不安全的操作系统中建立安全的应用支撑。徐甫[]等扩展了非传递无干扰理论，并试图通过重新定义静态干扰和动态干扰，使其支持进程自身代码的修改，但是其静态干扰和动态干扰的定义过于抽象，难以和实际的终端系统相对应，因此并不能在实际上完成其所描述的支持自身代码修改的功能。秦晰[]等提出了一种容忍非信任组件的可信终端模型，该模型利用可信组件对非信任组件的输出进行封装，保证了非信任组件在终端上的存在不会造成严重的安全威胁，实现了域间隔离和无干扰，保证了结果的可预测性和可控性，但是 并没有针对安全域进行详细的描述。 上述对无干扰理论的研究，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	基于无干扰理论的信任链传递模型 陈亮;曾荣仁;李峰;杨伟铭; -《计算机科学》- 2016-10-15（是否引证：否） 1.终端的安全。但是其模型中的可信传递函数check()和clear()有待进一步证明,并且缺乏对进程的动态保护。文献[5]提出了基于非传递的无干扰理念的二元多级安全模型,在Rushby无干扰理论的基础上重新定义了清除函数,将传递的无干扰理论过渡到非传递的无干扰理论,并依据BLP和Biba模型保护了信息的机密性和完整性,然而同样存在文献[2]中的问题。文献[6]从进程数据和代码完整性检测出发,利用无干扰理论保证进程之间的操作合法,试图在不安全的操作系统中建立安全的应用支撑。文献[7]扩展了非传递无干扰理论,并试图通过重新定义静态干扰和动态干扰,使其支持进程自身代码的修改,但是其静态干扰和动态干扰的定义过于抽象,难以和实际的终端系统相对应,因此并不能在实际上完成其所描述的支持自身代码修改的功能。文献[8]提出了一种容忍非信任组件的可信终端模型,该模型利用可信组件对非信任组件的输出进行封装,保证了非信任组件在终端上的存在不会造成严重的安全威胁,实现了域间隔离和无干扰,保证了结果的可预测性和可控性。此外,上述模型都只是从终端系统的角度构建安全模型,并未给出信任链从终端到网络上的扩展。本文在分析上述研究的基础上,将系统 数据安全交换若干关键技术研究 陈亮 -《解放军信息工程大学硕士论文》- 2015-04-20（是否引证：否） 1.0]则对进程在运行过程中产生的中间代码及数据的完整性分析入手,证明了进程在运行过程中的进程交互过程的合法性。文献[11]扩展了非传递无干扰理论,试图通过重新定义静态干扰和动态干扰,使其支持进程自身代码的修改,但是其静态干扰和动态干扰的定义过于抽象,难以和实际的终端系统相对应,因此并不能在实际上完成其所描述的支持自身代码修改的功能。文献[12]提出了一种容忍非信任组件的可信终端模型,该模型利用可信组件对非信任组件的输出进行封装,使得存在于终端上的非信任组件不会造成严重的安全威胁,从而实现了域间隔离和无干扰,保证了结果的可预测性和可控性。然而,上述研究都只是从终端系统的角度构建安全模型,并未考虑到信任链从终端到网络上的扩展,只能为数据安全交换模型的建立提供一定程 一个基于进程保护的可信终端模型 陈菊;谭良; -《计算机科学》- 2011-04-15（是否引证：是） 1.eck()、clear()有待进一步证明;基于非传递的无干扰理

		论的二元多级安全模型研究[9],所利用的非传递无干扰理论是在Rushby的基础上修改了清除函数,从而将Rushby传递的无干扰理论过渡到非传递性的无干扰理论。并且该模型分别依据BLP和Biba模型的思想保护信息的机密性和完整性,对模型进行了严格的形式化描述,证明了其安全性,但是它同样存在文献[7]的问题;文献[10]是对基于无干扰原理的终端安全模 2.递函数(check()、clear()函数)还有待进一步证明。结束语本文提出了一个新的基于无干扰理论的可信终端模型,它从进程数据和代码完整性检测出发,利用无干扰理论保证进程之间的操作都是合法的。该系统可以在不安全的操作系统中建立安全的应用支撑,排除病毒和木马对关键应用程序的破坏。相对文献[7-9]的无干扰模型,本文的可信模型更容易与现实终端系统相对应,实现起来更 信息郝瑞 -《学术论文联合比对库》- 2014-12-08（是否引证：否）
		1.改进方式，但是并没有给出具体的实现方案。Bryan Parno在应用中说明如何进行封装存储[37]。XU Mingdi等提出一种基于TPM的数据保护模型，该模型使用非对称密码算法将受保护数据与特定的可信计算环境相绑定[38]。陆建新等提出一种基于属性的封装方案，该方案将敏感数据与平台属
5	此处有 33 字相似 物理平台、可信衔接点等进行了形式化分析。 （2）基于扩展无干扰理论的可信虚拟平台信任链分析方法 目前大部分的研究是 基于信息流的无干扰模型从动作和运行结果的角度建立系统安全策略模型， 本文按照云计算环境运行特征，拟对原有无干扰理论中的安全域、动作等定义进行扩充，并将动作主体和动作对安全域以及系统状态的影	基于无干扰理论的信任链传递模型 陈亮;曾荣仁;李峰;杨伟铭; -《计算机科学》- 2016-10-15（是否引证：否） 1.态的信任链。由于系统平台上应用的多样性及无序性,静态信任链的构建并不适用于操作系统到应用程序及终端到网络之间的可信传递。基于信息流的无干扰模型从动作和运行结果的角度建立系统安全策略模型,从而确保计算机系统的安全性和完整性。文献[2,3]在Rushby的无干扰理论[4]的基础上将系统安全域集实体化为进程集,
6	此处有 54 字相似 应用此扩展的无干扰理论来分析可信云环境信任链传递模型，用形式化的方法证明当符合非传递无干扰安全策略时，云环境安全域之间的 信息流受到安全策略限制，隔离了域之间的干扰，满足此条件时用完整性度量方法所建立的云环境信任链才是可信的、有效 的。 1.4 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	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.整性验证实现的信任链传递是否有效无法进行验证.只有当系统具有特定的安全机制,满足一定的安全策略,组成系统的各安全域之间的信息流动受到一定安全策略限制,使得组件的运行不受干扰,这时,用完整性度量方法所建立的信任链才是有效的.进一步用图3表示非传递无干扰关系,其中粗箭头连线表示信任传递关系,细箭头连线表示干扰关系.可以看出,信任链有两条,分别是
7	此处有 49 字相似 间的信息流受到安全策略限制，隔离了域之间的干扰，满足此条件时用完整性度量方法所建立的云环境信任	王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2015-10-04（是否引证：否） 1.的同时，保证了存储数据的安全。通过安全性分析

	链才是可信的、有效的。 1.4 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	，不仅提高了网络存储中数据的安全性，而且达到了惰性重加密的效果。1.6 论文结构安排本文共分六章，安排如下：第1章主要介绍论文研究背景及意义，国内外研究现状，以及数据泄漏防护技术面临的问题和解决的新思路。最后介绍了本文主要研究的目标及内容。第2章主要介绍了可 王星魁_虚拟可信平台及数据泄漏防护研究_王星魁-《学术论文联合比对库》- 2015-10-08（是否引证：否） 1.的同时，保证了存储数据的安全。通过安全性分析，不仅提高了网络存储中数据的安全性，而且达到了惰性重加密的效果。1.6 论文结构安排本文共分六章，安排如下：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 王星魁博士学位论文 -《学术论文联合比对库》- 2015-10-09（是否引证：否） 1.时，保证了存储数据的安全。通过安全性分析，不仅提高了网络存储中数据的安全性，而且达到了惰性重加密的效果。1.6 论文结构安排本文共分六章，安排如下：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。太原 201603301253463317_王星魁_虚拟可信平台及数据泄漏防护研究_王星魁-《学术论文联合比对库》- 2016-03-30（是否引证：否） 1.的同时，保证了存储数据的安全。通过安全性分析，不仅提高了网络存储中数据的安全性，而且达到了惰性重加密的效果。1.6 论文结构安排本文共分六章，安排如下：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 201610071545221628_王星魁_虚拟可信平台及数据泄漏防护研究_王星魁-《学术论文联合比对库》- 2016-10-07（是否引证：否） 1.时，保证了存储数据的安全。通过安全性分析，不仅提高了网络存储中数据的安全性，而且达到了惰性重加密的效果。1.6 论文结构安排本文共分六章，安排如下：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 201610072245292357_王星魁_虚拟可信平台及数据泄漏防护研究_王星魁-《学术论文联合比对库》- 2016-10-07（是否引证：否） 1.时，保证了存储数据的安全。通过安全性分析，不仅提高了网络存储中数据的安全性，而且达到了惰性重加密的效果。1.6 论文结构安排本文共分六章，安排如下：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

8	此处有 57 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章主要介绍了云计算中的关键技术——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	王星魁_虚拟可信平台及数据泄漏防护研究_王星魁 -《学术论文联合比对库》- 2015-10-08（是否引证：否） 1.文共分六章，安排如下：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拟机的结构。并重点分析了信任链的构建及完整 201603301253463317_王星魁_虚拟可信平台及数据泄漏防护研究_王星魁 -《学术论文联合比对库》- 2016-03-30（是否引证：否） 1.文共分六章，安排如下：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拟机的结构。并重点分析了信任链的构建及完整 10112_081203_b20090055_LW_王星魁 -《学术论文联合比对库》- 2016-03-31（是否引证：否） 1.位论文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拟机的结构。并重点分析了信任链的构建及 201610071545221628_王星魁_虚拟可信平台及数据泄漏防护研究_王星魁 -《学术论文联合比对库》- 2016-10-07（是否引证：否） 1.如下：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拟机的结构。并重点分析了信任链的构建及 201610072245292357_王星魁_虚拟可信平台及数据泄漏防护研究_王星魁 -《学术论文联合比对库》- 2016-10-07（是否引证：否） 1.如下：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拟机的结构。并重点分析了信任链的构建及 王星魁博士学位论文 -《学术论文联合比对库》- 2015-10-09（是否引证：否） 1.章，安排如下：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。太原理工大学博士研究生学位论文17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 王星魁_虚拟可信平台及数据泄漏防护研究_王星魁-《学术论文联合比对库》- 2015-10-04（是否引证：否） 1.六章，安排如下：第1章主要介绍论文研究背景及意义，国内外研究现状，以及数据泄漏防护技术面临的问题和解决的新思路。最后介绍了本文主要研究的目标及内容。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
9	此处有 32 字相似 第2章主要介绍了云计算中的关键技术——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	王星魁_虚拟可信平台及数据泄漏防护研究_王星魁-《学术论文联合比对库》- 2015-10-04（是否引证：否） 1.强了可信环境动态性和可扩展性。可以说，虚拟化技术弥补了可信计算技术体系中存在的一些不足。2.4 本章小结本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。并重点分析了信任链的构建及完整性 王星魁_虚拟可信平台及数据泄漏防护研究_王星魁-《学术论文联合比对库》- 2015-10-08（是否引证：否） 1.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拟机的结构。并重点分析了信任链的构建及完整性 王星魁博士学位论文 -《学术论文联合比对库》- 2015-10-09（是否引证：否） 1.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。太原理工大学博士研究生学位论文17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。并重点分析了信任链的构建及完 201603301253463317_王星魁_虚拟可信平台及数据泄漏防护研究_王星魁-《学术论文联合比对库》- 2016-03-30（是否引证：否） 1.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拟机的结构。并重点分析了信任链的构建及完整性 10112_081203_b20090055_LW_王星魁-《学术论文联合比对库》- 2016-03-31（是否引证：否） 1.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拟机的结构。并重点分析了信任链的构建及完 201610071545221628_王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2016-10-07（是否引证：否） 1.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拟机的结构。并重点分析了信任链的构建及完 201610072245292357_王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2016-10-07（是否引证：否） 1.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拟机的结构。并重点分析了信任链的构建及完
10	此处有 30 字相似 吗，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。 2 相关技术与理论 2.1 虚拟化技术 虚拟化技术是将实际的物理计算机服务器、内存、	基于动态污点分析的二进制程序脆弱性检测技术研究 董国良 -《南京航空航天大学硕士论文》- 2017-03-01（是否引证：否） 1.析方法的覆盖率进行实验对比，验证了路径自动生成方法能有效提高污点分析的执行效率。第五章：总结与展望。对本文的主要工作及研究成果进行了总结，指出了本文研究的不足之处，并给出了未来研究工作的思路。 南京航空航天大学硕士学位论文9第二章 软件脆弱性检测与分析相关技术2
11	此处有 30 字相似 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。 2 相关技术与理论 2.1 虚拟化技术 虚拟化技术 是将实际的物理计算机服务器、内存、硬盘存储等实体资源进行抽象 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管理方式；主要用来解决当前物理计算机资源利用率低的问题，从而最大化的利	网络技术在新媒体发展中的应用分析 曾鹏;冯明明; -《西部广播电视》- 2018-01-05（是否引证：否） 1.3.2常用的新媒体技术3.2.1虚拟化与云计算技术在计算机中,虚拟化(Virtualization)是一种资源管理技术,是将计算机的各种物理资源,如服务器、网络、内存及存储等,予以抽象、转换后呈现出来,使物理资源变得可切割,使用户以比原本的组态更好的方式来共享这些资源。物理资源经虚拟后变成可以自由分配的逻
12	此处有 29 字相似 统中向外部提供服务。 2.1.1 虚拟化技术分类 为了满足当前云计算提供商需要提供不同功能的功能和需求，在实现层次和	基于可信计算的云计算安全若干关键问题研究 罗东俊 -《华南理工大学博士论文》- 2014-03-31（是否引证：否） 1.服务的一种重要技术手段，但同时它也带来了其本身的安全问题以及虚拟机的安全和管理问题。典型的云计算平台，其资源是通过虚拟化方式租用给不同用户，不

	虚拟方式上都产生了不同类别的虚拟化解决方案，使得不同的虚拟 化系统不仅具有最基本的虚拟化技术，也呈现了各自独特的个性[][]。 下面本文从实现层次和实现方式对虚拟化技术的分类进行介	同用户的虚拟资源可能被绑定到相同的物理资源上，这样不同虚拟机就可能会访问相同的物理设备。如果虚拟化基础软件不能将两个虚拟机有效
13	此处有 57 字相似 ，也呈现了各自独特的个性[][]。 下面本文从实现层次和实现方式对虚拟化技术的分类进行介绍。 (1) 不同实现层次 指令集虚拟化，指的是指令集架构级（Instruction Set Architecture, ISA）虚拟化技术。 该方式的虚拟化技术能够将操作系统在运行中指令集以软件模拟的方式进行实现，将虚拟机中运行过程中产生的指令转化为本地的指令集	王星魁_虚拟可信平台及数据泄漏防护研究_王星魁 -《学术论文联合比对库》- 2015-10-04（是否引证：否） 1.象层次，因而这些虚拟化系统呈现出不同的特性[85-87]。（1）根据虚拟化技术的实现层次分类指令级虚拟化：也称为指令集架构级（Instruction Set Architecture，ISA）虚拟化，通过存软件方法，模拟出与实际运行的应用程序（或操作系统）不同的指令集去执行，这种方法构造的虚拟机成为模拟器。模拟器可以将 王星魁_虚拟可信平台及数据泄漏防护研究_王星魁 -《学术论文联合比对库》- 2015-10-08（是否引证：否） 1.有效的保护系统中数据的安全。2.2.1 虚拟化技术分类（1）根据虚拟化技术的实现层次分类指令级虚拟化：也称为指令集架构级（Instruction Set Architecture，ISA）虚拟化，即以软件模拟出实际运行的操作系统的指令集来实现的方式。模拟器可以将用户虚拟机所产生的指令进行转化从而形成一种本地的指令集 王星魁博士学位论文 -《学术论文联合比对库》- 2015-10-09（是否引证：否） 1.次，因而这些虚拟化系统呈现出不同的特性[85-87]。（1）根据虚拟化技术的实现层次分类指令级虚拟化：也称为指令集架构级（Instruction Set Architecture，ISA）虚拟化，即以软件模拟出实际运行的操作系统的指令集来实现的方式。模拟器可以将用户虚拟机所产生的指令进行转化从而形成一种本地的指令集 201603301253463317_王星魁_虚拟可信平台及数据泄漏防护研究_王星魁 -《学术论文联合比对库》- 2016-03-30（是否引证：否） 1.有效的保护系统中数据的安全。2.2.1 虚拟化技术分类（1）根据虚拟化技术的实现层次分类指令级虚拟化：也称为指令集架构级（Instruction Set Architecture，ISA）虚拟化，即以软件模拟出实际运行的操作系统的指令集来实现的方式。模拟器可以将用户虚拟机所产生的指令进行转化从而形成一种本地的指令集 10112_081203_b20090055_LW_王星魁 -《学术论文联合比对库》- 2016-03-31（是否引证：否） 1.，因而这些虚拟化系统呈现出不同的特性[85-87]。(1) 根据虚拟化技术的实现层次分类指令级虚拟化：也称为指令集架构级（Instruction Set Architecture，ISA）虚拟化，即以软件模拟出实际运行的操作系统的指令集来实现的方式。模拟器可以将用户虚拟机所产生的指令进行转化从而形成一种本地的指令集

		201610071545221628_王星魁_虚拟可信平台及数据泄漏防护研究_王星魁-《学术论文联合比对库》- 2016-10-07（是否引证：否）
		1.而这些虚拟化系统呈现出不同的特性[85-87]。(1) 根据虚拟化技术的实现层次分类指令级虚拟化：也称为指令集架构级（Instruction Set Architecture，ISA）虚拟化，即以软件模拟出实际运行的操作系统的指令集来实现的方式。模拟器可以将用户虚拟机所产生的指令进行转化从而形成一种本地的指令集
		201610072245292357_王星魁_虚拟可信平台及数据泄漏防护研究_王星魁-《学术论文联合比对库》- 2016-10-07（是否引证：否）
		1.拟化系统呈现出不同的特性[85-87]。(1) 根据虚拟化技术的实现层次分类32指令级虚拟化：也称为指令集架构级（Instruction Set Architecture，ISA）虚拟化，即以软件模拟出实际运行的操作系统的指令集来实现的方式。模拟器可以将用户虚拟机所产生的指令进行转化从而形成一种本地的指令集
14	此处有 43 字相似 方式进行实现，将虚拟机中运行过程中产生的指令转化为本地的指令集，然后在本地及其中执行这些被转换的指令集。目前，比较流行的 指令集架构级的虚拟化系统主要由Qemu系统和Bochs系统。 硬件级虚拟化，这种虚拟 化技术主要用来虚拟化具体的计算机主机，使得用户在操作计算机资源时，与真实的计算机具有相同的指令集，可以在用户指令可以直接	王星魁_虚拟可信平台及数据泄漏防护研究_王星魁-《学术论文联合比对库》- 2015-10-08（是否引证：否）
		1.式。模拟器可以将用户虚拟机所产生的指令进行转化从而形成一种本地的指令集，随后将这种本地指令集在计算机上真实的硬件上执行。指令级虚拟化系统主要有Bochs系统和QEMU系统。硬件级虚拟化：这种虚拟化与前面所讲述的指令集架构虚拟化存在相似之处，他们之间存在的差别在于这种虚拟化仅仅是对少数的特殊情况进行考虑，这种情况下
		王星魁博士学位论文_-《学术论文联合比对库》- 2015-10-09（是否引证：否）
		1.式。模拟器可以将用户虚拟机所产生的指令进行转化从而形成一种本地的指令集，随后将这种本地指令集在计算机上真实的硬件上执行。指令级虚拟化系统主要有Bochs 系统和 QEMU 系统。硬件级虚拟化：这种虚拟化与前面所讲述的指令集架构虚拟化存在相似之处，他们之间存在的差别在于这种虚拟化仅仅是对少数的特殊情况进行考虑，这种情况下
		201603301253463317_王星魁_虚拟可信平台及数据泄漏防护研究_王星魁-《学术论文联合比对库》- 2016-03-30（是否引证：否）
		1.式。模拟器可以将用户虚拟机所产生的指令进行转化从而形成一种本地的指令集，随后将这种本地指令集在计算机上真实的硬件上执行。指令级虚拟化系统主要有Bochs系统和QEMU系统。硬件级虚拟化：这种虚拟化与前面所讲述的指令集架构虚拟化存在相似之处，他们之间存在的差别在于这种虚拟化仅仅是对少数的特殊情况进行考虑，这种情况下
		10112_081203_b20090055_LW_王星魁-《学术论文联合比对库》- 2016-03-31（是否引证：否）
		1.式。模拟器可以将用户虚拟机所产生的指令进行转化从而形成一种本地的指令集，随后将这种本地指令集在计算机上真实的硬件上执行。指令级虚拟化系统主要有

		Bochs 系统和 QEMU 系统。硬件级虚拟化：这种虚拟化与前面所讲述的指令集架构虚拟化存在相似之处，他们之间存在的差别在于这种虚拟化仅仅是对少数的特殊情况进行考虑，这种情况下 201610071545221628_王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2016-10-07（是否引证：否） 1.式。模拟器可以将用户虚拟机所产生的指令进行转化从而形成一种本地的指令集，随后将这种本地指令集在计算机上真实的硬件上执行。指令级虚拟化系统主要有Bochs 系统和 QEMU 系统。硬件级虚拟化：这种虚拟化与前面所讲述的指令集架构虚拟化存在相似之处，他们之间存在的差别在于这种虚拟化仅仅是对少数的特殊情况进行考虑，这种情况下 201610072245292357_王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2016-10-07（是否引证：否） 1.式。模拟器可以将用户虚拟机所产生的指令进行转化从而形成一种本地的指令集，随后将这种本地指令集在计算机上真实的硬件上执行。指令级虚拟化系统主要有Bochs 系统和 QEMU 系统。硬件级虚拟化：这种虚拟化与前面所讲述的指令集架构虚拟化存在相似之处，他们之间存在的差别在于这种虚拟化仅仅是对少数的特殊情况进行考虑，这种情况下 王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2015-10-04（是否引证：否） 1.集去执行，这种方法构造的虚拟机成为模拟器。模拟器可以将用户虚拟机发出的所有指令翻译成本地指令集，然后在真实的硬件上执行。指令级虚拟化系统有Bochs和QEMU。硬件级虚拟化：硬件抽象层(Hardware Abstraction Lover，HAL)虚拟化实际上与指令集架构级虚拟化非常相似，
15	此处有 107 字相似 统和Bochs系统。 硬件级虚拟化，这种虚拟化技术主要用来虚拟化具体的计算机主机，使得用户在操作计算机资源时，与真实的计算机具有相同的指令集，可以在用户指令可以直接在计算机主机上进行运行，为用户操作虚拟的计算机提供了遍历，提高了指令运行的效率和速度。基于硬件级虚拟化技术，用户可以方便的使用被映射为物理资源的虚拟机资源，是目前云计算 虚拟化技术中被重点研究的方向。目前基于硬件级的虚拟化技术有EMC公司的VMWare，以及由英国剑桥大学发起的开源框架Xe	王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2015-10-08（是否引证：否） 1.指令集架构虚拟化存在相似之处，他们之间存在的差别在于这种虚拟化仅仅是对少数的特殊情况进行考虑，这种情况下用户的使用环境与计算机具有相同的指令集，这就为绝大多数的用户指令直接在主机上进行操作提供了便利，提高了指令的运行的速度。这种技术还能够实现虚拟资源的物理化转变，当映射为物理资源以后就可以在虚拟环境下使用计算机的本地硬件。这种虚拟化是当前在计 王星魁博士学位论文 -《学术论文联合比对库》- 2015-10-09（是否引证：否） 1.指令集架构虚拟化存在相似之处，他们之间存在的差别在于这种虚拟化仅仅是对少数的特殊情况进行考虑，这种情况下用户的使用环境与计算机具有相同的指令集，这就为绝大多数的用户指令直接在主机上进行操作提供了便利，提高了指令的运行的速度。这种技术还能够实现虚拟资源的物理化转变，当映射为物理资源以后就可以在虚拟环境下使用计算机的本地硬件。这种虚拟

		化是当前 201603301253463317_王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2016-03-30（是否引证：否） 1.指令集架构虚拟化存在相似之处，他们之间存在的差别在于这种虚拟化仅仅是对少数的特殊情况进行考虑，这种情况下用户的使用环境与计算机具有相同的指令集，这就为绝大多数的用户指令直接在主机上进行操作提供了便利，提高了指令的运行的速度。这种技术还能够实现虚拟资源的物理化转变，当映射为物理资源以后就可以在虚拟环境下使用计算机的本地硬件。这种虚拟化是当前在计 10112_081203_b20090055_LW 王星魁 -《学术论文联合比对库》- 2016-03-31（是否引证：否） 1.指令集架构虚拟化存在相似之处，他们之间存在的差别在于这种虚拟化仅仅是对少数的特殊情况进行考虑，这种情况下用户的使用环境与计算机具有相同的指令集，这就为绝大多数的用户指令直接在主机上进行操作提供了便利，提高了指令的运行的速度。这种技术还能够实现虚拟资源的物理化转变，当映射为物理资源以后就可以在虚拟环境下使用计算机的本地硬件。这种虚拟化是当前 201610071545221628_王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2016-10-07（是否引证：否） 1.指令集架构虚拟化存在相似之处，他们之间存在的差别在于这种虚拟化仅仅是对少数的特殊情况进行考虑，这种情况下用户的使用环境与计算机具有相同的指令集，这就为绝大多数的用户指令直接在主机上进行操作提供了便利，提高了指令的运行的速度。这种技术还能够实现虚拟资源的物理化转变，当映射为物理资源以后就可以在虚拟环境下使用计算机的本地硬件。这种虚拟化是当前 201610072245292357_王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2016-10-07（是否引证：否） 1.指令集架构虚拟化存在相似之处，他们之间存在的差别在于这种虚拟化仅仅是对少数的特殊情况进行考虑，这种情况下用户的使用环境与计算机具有相同的指令集，这就为绝大多数的用户指令直接在主机上进行操作提供了便利，提高了指令的运行的速度。这种技术还能够实现虚拟资源的物理化转变，当映射为物理资源以后就可以在虚拟环境下使用计算机的本地硬件。这种虚拟化是当前 王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2015-10-04（是否引证：否） 1.化所考虑的是一种特殊情况：用户执行环境和主机具有相同指令集，并利用这一特点，让绝大多数用户指令在主机上直接执行，从而大大提高执行的速度。该虚拟化技术可以将虚拟资源映射到物理资源并在虚拟机计算中使用本地硬件。硬件级虚拟化是目前研究最广泛的虚拟化技术，相应的虚拟化系统也较多。其中，最具影响

		力的VMware和Xen
16	此处有 33 字相似 向。目前基于硬件级的虚拟化技术有EMC公司的VMWare，以及由英国剑桥大学发起的开源框架Xen，都十分具有影响力。 操作系统级虚拟化，在传统的操作系统运行时，相同计算机的多用户的进程 都是运行同一操作系统下，如果操作系统的内核或进程管理出现缺陷或漏洞，不同用户之间相同类别的进程有可能产生影响。而针对操作	王星魁_虚拟可信平台及数据泄漏防护研究_王星魁 -《学术论文联合比对库》- 2015-10-04（是否引证：否） 1.拟化是目前研究最广泛的虚拟化技术，相应的虚拟化系统也较多。其中，最具影响力的VMware和Xen都属于硬件级虚拟化。操作系统级虚拟化：在传统操作系统中，所有用户的进程本质上是在同一个操作系统的实例中运行，因此内核或应用程序的缺陷可能影响到其它进程。操作系统级虚拟化是一种在服务器操作系统 王星魁_虚拟可信平台及数据泄漏防护研究_王星魁 -《学术论文联合比对库》- 2015-10-08（是否引证：否） 1.领域研究较多的内容，也是虚拟化技术研究中的核心。在虚拟化研究中出现了VMware和Xen等具有影响力的硬件级虚拟化。操作系统级虚拟化：在传统的计算机操作系统中每一位计算机用户的进程本质上是在同一个操作系统的实例中运行，所以操作系统的内核缺陷或者是在程序设计上存在问题都可能会对其他进程产生影响。而对操 王星魁博士学位论文 -《学术论文联合比对库》- 2015-10-09（是否引证：否） 1.内容，也是虚拟化技术研究中的核心。在虚拟化研究中出现了VMware 和 Xen 等具有影响力的硬件级虚拟化系统。操作系统级虚拟化：在传统的计算机操作系统中每一位计算机用户的进程本质上是在同一个操作系统的实例中运行，所以操作系统的内核缺陷或者是在程序设计上存在问题都可能会对其他进程产生影响。而对操 201603301253463317_王星魁_虚拟可信平台及数据泄漏防护研究_王星魁 -《学术论文联合比对库》- 2016-03-30（是否引证：否） 1.领域研究较多的内容，也是虚拟化技术研究中的核心。在虚拟化研究中出现了VMware和Xen等具有影响力的硬件级虚拟化。操作系统级虚拟化：在传统的计算机操作系统中每一位计算机用户的进程本质上是在同一个操作系统的实例中运行，所以操作系统的内核缺陷或者是在程序设计上存在问题都可能会对其他进程产生影响。而对操 10112_081203_b20090055_LW_王星魁 -《学术论文联合比对库》- 2016-03-31（是否引证：否） 1.内容，也是虚拟化技术研究中的核心。在虚拟化研究中出现了VMware 和 Xen 等具有影响力的硬件级虚拟化系统。操作系统级虚拟化：在传统的计算机操作系统中每一位计算机用户的进程本质上是在同一个操作系统的实例中运行，所以操作系统的内核缺陷或者是在程序设计上存在问题都可能会对其他进程产生影响。而对操 201610071545221628_王星魁_虚拟可信平台及数据泄漏防护研究_王星魁 -《学术论文联合比对库》- 2016-10-07（是否引证：否） 1.多的内容，也是虚拟化技术研究中的核心。在虚拟化研究中出现了VMware 和 Xen 等具有影响力的硬件级虚拟化系统。操作系统级虚拟化：在传统的计算机操作系统中每一位计算机用户的进程本质上是在同一个操作系

		统的实例中运行，所以操作系统的内核缺陷或者是在程序设计上存在问题都可能会对其他进程产生影响。而对操 201610072245292357_王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2016-10-07（是否引证：否） 1.多的内容，也是虚拟化技术研究中的核心。在虚拟化研究中出现了VMware 和 Xen 等具有影响力的硬件级虚拟化系统。操作系统级虚拟化：在传统的计算机操作系统中每一位计算机用户的进程本质上是在同一个操作系统的实例中运行，所以操作系统的内核缺陷或者是在程序设计上存在问题都可能会对其他进程产生影响。而对操
17	此处有 40 字相似 行时，相同计算机的多用户的进程都是运行同一操作系统下，如果操作系统的内核或进程管理出现缺陷或漏洞，不同用户之间相同类别的 进程有可能产生影响。而针对操作系统的虚拟化可以有效的解决上述问题。目前最为流行的 操作系统级虚拟化技术当属火热的容器技术[]，其利用Linux的LXC技术，通过设定不同类别的namespace提供给不同	王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2015-10-08（是否引证：否） 1.一位计算机用户的进程本质上是在同一个操作系统的实例中运行，所以操作系统的内核缺陷或者是在程序设计上存在问题都可能会对其他进程产生影响。而对操作系统进行虚拟化则是一种有效解决上述问题的办法，这是一种轻量级的虚拟化技术，在这一技术下可以创建多个虚拟化的操作系统提供给不同的用户，这样每个用户就可以在相对独立的环境 王星魁博士学位论文 -《学术论文联合比对库》- 2015-10-09（是否引证：否） 1.一位计算机用户的进程本质上是在同一个操作系统的实例中运行，所以操作系统的内核缺陷或者是在程序设计上存在问题都可能会对其他进程产生影响。而对操作系统进行虚拟化则是一种有效解决上述问题的办法，这是一种轻量级的虚拟化技术，在这一技术下可以创建多个虚拟化的操作系统提供给不同的用户，这样每个用户就可以在相对独立的环境 201603301253463317_王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2016-03-30（是否引证：否） 1.一位计算机用户的进程本质上是在同一个操作系统的实例中运行，所以操作系统的内核缺陷或者是在程序设计上存在问题都可能会对其他进程产生影响。而对操作系统进行虚拟化则是一种有效解决上述问题的办法，这是一种轻量级的虚拟化技术，在这一技术下可以创建多个虚拟化的操作系统提供给不同的用户，这样每个用户就可以在相对独立的环境 10112_081203_b20090055_LW 王星魁 -《学术论文联合比对库》- 2016-03-31（是否引证：否） 1.一位计算机用户的进程本质上是在同一个操作系统的实例中运行，所以操作系统的内核缺陷或者是在程序设计上存在问题都可能会对其他进程产生影响。而对操作系统进行虚拟化则是一种有效解决上述问题的办法，这是一种轻量级的虚拟化技术，在这一技术下可以创建多个虚拟化的操作系统提供给不同的用户，这样每个用户就可以在相对独立的环境

		201610071545221628_王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2016-10-07（是否引证：否）
		1.一位计算机用户的进程本质上是在同一个操作系统的实例中运行，所以操作系统的内核缺陷或者是在程序设计上存在问题都可能会对其他进程产生影响。而对操作系统进行虚拟化则是一种有效解决上述问题的办法，这是一种轻量级的虚拟化技术，在这一技术下可以创建多个虚拟化的操作系统提供给不同的用户，这样每个用户就可以在相对独立的环境
		201610072245292357_王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2016-10-07（是否引证：否）
		1.一位计算机用户的进程本质上是在同一个操作系统的实例中运行，所以操作系统的内核缺陷或者是在程序设计上存在问题都可能会对其他进程产生影响。而对操作系统进行虚拟化则是一种有效解决上述问题的办法，这是一种轻量级的虚拟化技术，在这一技术下可以创建多个虚拟化的操作系统提供给不同的用户，这样每个用户就可以在相对独立的环境
18	此处有 90 字相似 实的操作系统。使得每个用户都可以在独立的用户空间进行活动，相互之间的进程、网络、文件等都通过namespace进行隔离。 当前典型的操作系统级虚拟化系统有 Linux-VSerser、Solaris Container，以及Docker等容器技术。 （2）不同实现方式 使用二进制翻译的全虚拟化， 针对在全虚拟化技术运行的虚拟机可以单独的使用一个被虚拟的硬件资源。该虚拟的硬件环境能够在不需要修改当前虚拟机的操作系统内	王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2015-10-08（是否引证：否）
		1.立的环境下进行操作，从而避免了同一个系统中的各个进程的相互影响，从而导致系统的整体运行效率下降以及出现相互的影响的状况。当前典型的系统有Linux-VSerser、OpenVZ、Solaris Container，FreeBSD Jail等。（2）根据实现方式不同分类全虚拟化：在全虚拟化的环境下计算机的虚拟机监视器能够虚拟出如同真实硬件环境一样的虚拟硬件环境。因此，每一个虚拟机都可以使用一个
		王星魁博士学位论文 -《学术论文联合比对库》- 2015-10-09（是否引证：否）
		1.学博士研究生学位论文32一个系统中的各个进程的相互影响，从而导致系统的整体运行效率下降以及出现相互的影响的状况。当前典型的系统有 Linux-VSerser、OpenVZ、Solaris Container，FreeBSD Jail 等。（2）根据实现方式不同分类全虚拟化：在全虚拟化的环境下计算机的虚拟机监视器能够虚拟出如同真实硬件环境一样的虚拟硬件环境。因此，每一个虚拟机都可以使用一个
		201603301253463317_王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2016-03-30（是否引证：否）
		1.立的环境下进行操作，从而避免了同一个系统中的各个进程的相互影响，从而导致系统的整体运行效率下降以及出现相互的影响的状况。当前典型的系统有Linux-VSerser、OpenVZ、Solaris Container，FreeBSD Jail等。（2）根据实现方式不同分类全虚拟化：在全虚拟化的环境下计算机的虚拟机监视器能够虚拟出如同真实硬件环境一样的虚拟硬件环境。因此，每一个虚拟机都可以使用一个
		王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术

		论文联合比对库》- 2015-10-04（是否引证：否）
		1.量级的虚拟化技术，内核通过创建多个虚拟的操作系统实例（内核和库）来隔离不同的进程，不同实例中的进程完全不了解对方的存在。典型的操作系统级虚拟化系统有Linux-VSerser、OpenVZ、Solaris Container，FreeBSD Jail等。（2）根据实现方式不同分类全虚拟化：在全虚拟化下，虚拟机监视器（Virtual Machine Monitor，VMM。也称为Hyperxisor）可以
		10112_081203_b20090055_LW 王星魁-《学术论文联合比对库》- 2016-03-31（是否引证：否）
		1.学博士研究生学位论文32一个系统中的各个进程的相互影响，从而导致系统的整体运行效率下降以及出现相互的影响的状况。当前典型的系统有 Linux-VSerser、OpenVZ、Solaris Container，FreeBSD Jail等。(2) 根据实现方式不同分类全虚拟化：在全虚拟化的环境下计算机的虚拟机监视器能够虚拟
		201610071545221628_王星魁_虚拟可信平台及数据泄漏防护研究 王星魁-《学术论文联合比对库》- 2016-10-07（是否引证：否）
		1.行操作，从而避免了同32一个系统中的各个进程的相互影响，从而导致系统的整体运行效率下降以及出现相互的影响的状况。当前典型的系统有 Linux-VSerser、OpenVZ、Solaris Container，FreeBSD Jail等。(2) 根据实现方式不同分类全虚拟化：在全虚拟化的环境下计算机的虚拟机监视器能够
		201610072245292357_王星魁_虚拟可信平台及数据泄漏防护研究 王星魁-《学术论文联合比对库》- 2016-10-07（是否引证：否）
		1.立的环境下进行操作，从而避免了同一个系统中的各个进程的相互影响，从而导致系统的整体运行效率下降以及出现相互的影响的状况。当前典型的系统有 Linux-VSerser、OpenVZ、Solaris Container，FreeBSD Jail等。(2) 根据实现方式不同分类332.2.2 虚拟机与虚拟机监视器虚拟机（
19	此处有 49 字相似 aris Container，以及Docker等容器技术。 （2）不同实现方式 使用二进制翻译的全虚拟化，针对在全 虚拟化技术运行的虚拟机可以单独的使用一个被虚拟的硬件资源。该虚拟的硬件环境能够在不需要修改当前虚拟 机的操作系统内核便可以提供如同真实硬件环境提供的服务，虚拟机内核中也无法感知当前运行的硬件环境是否是在虚拟化环境下。目前	王星魁_虚拟可信平台及数据泄漏防护研究 王星魁-《学术论文联合比对库》- 2015-10-08（是否引证：否）
		1.式不同分类全虚拟化：在全虚拟化的环境下计算机的虚拟机监视器能够虚拟出如同真实硬件环境一样的虚拟硬件环境。因此，每一个虚拟机都可以使用一个虚拟的硬件环境，这个虚拟硬件环境能够提供如同真实的硬件环境相同的支持服务；而在这个支持服务提供中系统不需要真实的硬件或者是操作系统来协助，因此不
		王星魁博士学位论文 -《学术论文联合比对库》- 2015-10-09（是否引证：否）
		1.现方式不同分类全虚拟化：在全虚拟化的环境下计算机的虚拟机监视器能够虚拟出如同真实硬件环境一样的虚拟硬件环境。因此，每一个虚拟机都可以使用一个虚拟的硬件环境，这个虚拟硬件环境能够提供如同真实的硬件环境相同的支持服务；而在这个支持服务提供中系统不需要真实的硬件或者是操作系统来协助，因此不
		201603301253463317_王星魁_虚拟可信平台及数据泄漏

		防护研究_王星魁 -《学术论文联合比对库》- 2016-03-30（是否引证：否） 1.式不同分类全虚拟化：在全虚拟化的环境下计算机的虚拟机监视器能够虚拟出如同真实硬件环境一样的虚拟硬件环境。因此，每一个虚拟机都可以使用一个虚拟的硬件环境，这个虚拟硬件环境能够提供如同真实的硬件环境相同的支持服务；而在这个支持服务提供中系统不需要真实的硬件或者是操作系统来协助，因此不 10112_081203_b20090055_LW_王星魁 -《学术论文联合比对库》- 2016-03-31（是否引证：否） 1.现方式不同分类全虚拟化：在全虚拟化的环境下计算机的虚拟机监视器能够虚拟出如同真实硬件环境一样的虚拟硬件环境。因此，每一个虚拟机都可以使用一个虚拟的硬件环境，这个虚拟硬件环境能够提供如同真实的硬件环境相同的支持服务；而在这个支持服务提供中系统不需要真实的硬件或者是操作系统来协助，因此不 201610071545221628_王星魁_虚拟可信平台及数据泄漏防护研究_王星魁 -《学术论文联合比对库》- 2016-10-07（是否引证：否） 1.式不同分类全虚拟化：在全虚拟化的环境下计算机的虚拟机监视器能够虚拟出如同真实硬件环境一样的虚拟硬件环境。因此，每一个虚拟机都可以使用一个虚拟的硬件环境，这个虚拟硬件环境能够提供如同真实的硬件环境相同的支持服务；而在这个支持服务提供中系统不需要真实的硬件或者是操作系统来协助，因此不
20	此处有 46 字相似 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，以便完成特权指令的虚拟化。 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等都可以提供半虚拟化的虚拟机。 硬件辅助	王星魁_虚拟可信平台及数据泄漏防护研究_王星魁 -《学术论文联合比对库》- 2015-10-08（是否引证：否） 1.产生任何的修改，该内核也无法感知到系统中是否发生了虚拟化。半虚拟化：这是一种与全虚拟化相辅助的一种虚拟化技术，这种虚拟化技术需要借助操作系统的协助才能完成对特权指令的虚拟化，所以会对客户操作系统的内核进行修改，以便操作系统能够发现有问题的指令进行更改。硬件辅助虚拟化：硬件辅助处理敏感指令以 王星魁博士学位论文 -《学术论文联合比对库》- 2015-10-09（是否引证：否） 1.核产生任何的修改，该内核也无法感知到系统中是否发生了虚拟化。半虚拟化：这是一种与全虚拟化相辅助的一种虚拟化技术，这种虚拟化技术需要借助操作系统的协助才能完成对特权指令的虚拟化，所以会对客户操作系统的内核进行修改，以便操作系统能够发现有问题的指令进行更改。硬件辅助虚拟化：硬件辅助处理敏感指令以 201603301253463317_王星魁_虚拟可信平台及数据泄漏防护研究_王星魁 -《学术论文联合比对库》- 2016-03-30（是否引证：否） 1.产生任何的修改，该内核也无法感知到系统中是否发生了虚拟化。半虚拟化：这是一种与全虚拟化相辅助的一种虚拟化技术，这种虚拟化技术需要借助操作系统的协助才能完成对特权指令的虚拟化，所以会对客户操作系统的内核进行修改，以便操作系统能够发现有问题的指令进行更改。硬件辅助虚拟化：硬件辅助处理敏感指

		令以 10112_081203_b20090055_LW 王星魁 -《学术论文联合比对库》- 2016-03-31（是否引证：否） 1.核产生任何的修改，该内核也无法感知到系统中是否发生了虚拟化。半虚拟化：这是一种与全虚拟化相辅助的一种虚拟化技术，这种虚拟化技术需要借助操作系统的协助才能完成对特权指令的虚拟化，所以会对客户操作系统的内核进行修改，以便操作系统能够发现有问题的指令进行更改。硬件辅助虚拟化：硬件辅助处理敏感指令以 201610071545221628_王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2016-10-07（是否引证：否） 1.核产生任何的修改，该内核也无法感知到系统中是否发生了虚拟化。半虚拟化：这是一种与全虚拟化相辅助的一种虚拟化技术，这种虚拟化技术需要借助操作系统的协助才能完成对特权指令的虚拟化，所以会对客户操作系统的内核进行修改，以便操作系统能够发现有问题的指令进行更改。硬件辅助虚拟化：硬件辅助处理敏感指令以 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 王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2015-10-04（是否引证：否） 1.操作系统的实例中运行，因此内核或应用程序的缺陷可能影响到其它进程。操作系统级虚拟化是一种在服务器操作系统中使用的轻量级的虚拟化技术，内核通过创建多个虚拟的操作系统实例（内核和库）来隔离不同的进程，不同实例中的进程完全不了解对方的存在。典型的操作系统级虚拟化系统有Linux-VSerser、O
21	此处有 35 字相似 下运行，并且虚拟出与甚至硬件资源的虚拟硬件环境，实现了多个虚拟机运行在一个物理平台上，提高了计算机硬件的使用率。实际上， VMM的作用不仅仅是提高了一个多任务的管理任务，也是一种十分安全可靠的 虚拟化系统方案。 2.1.3 Xen与KVM （1）Xen Xen是由英国剑桥大学开发的开源虚拟机监视器，Xen必	王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2015-10-08（是否引证：否） 1.理平台上，降低了系统的管理复杂程度，提高了管理的效率和节约了管理成本，并降低了对计算机的空间资源的占用。研究人员普遍认为VMM的作用不只是多任务的管理作用，也是一种更加安全和更加可靠的系统问题解决方案。根据VMM所处的物理系统中的位置将其分为独立监控模式、宿主模式和混合模式三种类型，结构如图2-9所示。 王星魁博士学位论文 -《学术论文联合比对库》- 2015-10-09（是否引证：否） 1.理平台上，降低了系统的管理复杂程度，提高了管理的效率和节约了管理成本，并降低了对计算机的空间资源的占用。研究人员普遍认为VMM的作用不只是多任务的管理作用，也是一种更加安全和更加可靠的系统问题

		解决方案。根据VMM所处的物理系统中的位置将其分为独立监控模式、宿主模式和混合模式三种类型，结构如图2-9所示。 201603301253463317_王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2016-03-30（是否引证：否） 1.理平台上，降低了系统的管理复杂程度，提高了管理的效率和节约了管理成本，并降低了对计算机的空间资源的占用。研究人员普遍认为VMM的作用不只是多任务的管理作用，也是一种更加安全和更加可靠的系统问题解决方案。根据VMM所处的物理系统中的位置将其分为独立监控模式、宿主模式和混合模式三种类型，结构如图2-9所示。 10112_081203_b20090055_LW 王星魁 -《学术论文联合比对库》- 2016-03-31（是否引证：否） 1.理平台上，降低了系统的管理复杂程度，提高了管理的效率和节约了管理成本，并降低了对计算机的空间资源的占用。研究人员普遍认为VMM的作用不只是多任务的管理作用，也是一种更加安全和更加可靠的系统问题解决方案。根据VMM所处的物理系统中的位置将其分为独立监控模式、宿主模式和混合模式三种类型，结构如图2-9所示。 201610071545221628_王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2016-10-07（是否引证：否） 1.理平台上，降低了系统的管理复杂程度，提高了管理的效率和节约了管理成本，并降低了对计算机的空间资源的占用。研究人员普遍认为VMM的作用不只是多任务的管理作用，也是一种更加安全和更加可靠的系统问题解决方案。根据VMM所处的物理系统中的位置将其分为独立监控模式、宿主模式和混合模式三种类型，结构如图2-9所
22	此处有 119 字相似 n，KVM的核心源码很少，已经成为学术界和产业界主流的VMM。KVM需要硬件辅助才可以进行虚拟化，是一种全虚拟化的技术。 KVM 内核模块在运行时按需加载进入内核空间运行。KVM 本身不执行任何设备模拟，需要 QEMU 通过 /dev/kvm 接口设置一个 GUEST OS 的地址空间，向它提供模拟的 I/O 设备，并将它的视频显示映射回宿主机的显示屏。 2.2 可信计算 可信计算技术是一种保障信息系统安全的新技术，可信计算的思想是来源于人类社会，把人类社会成功的基于信任	CentOS7下安装KVM - z936689039的博客 - CSDN博客 -《网络（http://blog.csdn.net）》- （是否引证：否） 1.依赖的虚拟设备、虚机运行时的用户环境和交互，以及一些虚机的特定技术比如动态迁移，都是 QEMU 自己实现的。 KVM： KVM 内核模块在运行时按需加载进入内核空间运行。KVM 本身不执行任何设备模拟，需要 QEMU 通过 /dev/kvm 接口设置一个 GUEST OS 的地址空间，向它提供模拟的 I/O 设备，并将它的视频显示映射回宿主机的显示屏。它是KVM 虚机的核心部分，其主要功能是初始化 CPU 硬件，打开虚拟化模式，然后将虚拟客户机运行在虚拟机模式下，并对虚 KVM 介绍（1）：简介及安装 - 张某人ER的技术博客 ==学习&分享== - CSDN博客 -《网络（http://blog.csdn.net）》- （是否引证：否） 1.依赖的虚拟设备、虚机运行时的用户环境和交互，以及一些虚机的特定技术比如动态迁移，都是 QEMU 自己实现的。 KVM： KVM 内核模块在运行时按需加载进入内核空间运行。KVM 本身不执行任何设备模拟，需要 QEMU 通过 /dev/kvm 接口设置一个 GUEST OS 的地址空间，向它提供模拟的 I/O 设备，并将它的视频显

		示映射回宿主机的显示屏。它是KVM 虚机的核心部分，其主要功能是初始化 CPU 硬件，打开虚拟化模式，然后将虚拟客户机运行在虚拟机模式下，并对虚 虚拟化模型 - tengyft的专栏 - CSDN博客 -《网络（http://blog.csdn.net）》-（是否引证：否） 1.图是KVM架构： 如图所示，左侧部分是一个标准的Linux操作系统，可以是RHEL、Fedora、Ubuntu等。KVM内核模块在运行时按需加载进入内核空间运行。KVM本身不执行任何设备模拟，需要用户空间程序QEMU通过/dev/kvm接口设置一个虚拟客户机的地址空间，向它提供模拟的I/O设备，并将它的视频显示映射回宿主机的显示屏。
23	此处有 33 字相似 O 设备，并将它的视频显示映射回宿主机的显示屏。 2.2 可信计算 可信计算技术是一种保障信息系统安全的新技术，可信计算的思想是来源于人类社会，把人类社会成功的基于信任的管理经验用于 保障计算机系统安全。可信计算的基本思想是： 首先在计算机系统建立一个可以有物理系统安全技术进行保障的信任根；然后以该信	基于可信计算的远程证明的研究 黄秀文; -《武汉纺织大学学报》- 2015-12-15（是否引证：否） 1.期,能够实现预定的目标。可信计算是一种信息系统安全新技术,包括可信硬件、可信软件、可信网络和可信计算应用等诸多方面。可信计算的思想源于人类社会,是把人类社会成功的管理经验用于计算机信息系统和网络空间,以确保计算机信息系统和网络空间的安全可信。TCG认为,可信计算的总体目标是提高计算机系统的安全
24	此处有 33 字相似 于保障计算机系统安全。可信计算的基本思想是： 首先在计算机系统建立一个可以有物理系统安全技术进行保障的信任根；然后以该 信任根为信任基础建立一条从硬件平台到操作系统应用程序启动的信任链， 一级度量一级，直到平台所有组件启动。 可信计算技术中最重要的技术是可信计算模块，旨在通过硬件安全模型采用软件和硬件相结	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.虚拟化平台提供服务可信的保障,用户在使用虚拟化平台提供的资源和服务时,亟需确认该服务平台是否可信任。可信计算技术基于硬件信任根,能够为平台构建从底层硬件到上层应用程序的信任链,并结合度量与远程证明机制为外部提供可信证明[1],从而为平台提供可信运行环境保障,因此,利用可信计算技术构建可信虚拟平台
25	此处有 38 字相似 台的安全性和数据完整性。并且可以提供给第三方进行远程验证计算平台的远程证明方式来达到保护本地和远程终端的安全和可靠。 2.2.1 可信平台模块 可信平台模块是可信计算平台的信任基础和核心技术。 首先，TPM作为可信计算技术实现数据加密、完整性度量的关键模块，必须严格保障自身的安全，并且保障可信计算功能的有效执行，	王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2015-10-08（是否引证：否） 1.章是全文研究工作的基础，本文的其它所有研究环境都是建立在本章论述的虚拟可信平台基础之上。2.1 可信计算技术2.2.1 可信平台模块在可信计算平台中可信平台模块是信任基础。第一，可平台模块自身必须是安全的，这是可信平台模块有效工作的基础。可信平台模块应为存储和计算资源提供可靠的安全保护，应保 201603301253463317_王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2016-03-30（是否引证：否） 1.章是全文研究工作的基础，本文的其它所有研究环境都是建立在本章论述的虚拟可信平台基础之上。2.1 可信计算技术2.2.1 可信平台模块在可信计算平台中可信平台模块是信任基础。第一，可平台模块自身必须是安全的，这是可信平台模块有效工作的基础。可信平台模块应为存储和计算资源提供可靠的安全保护，应保

26	此处有 35 字相似 了很多信息系统安全保障技术，比如访问控制、入侵检测灯光。但是这些技术都是以在计算机启动之后给系统安装针对恶意代码的补丁的 方式来增强系统安全，并没有彻底解决系统安全问题。可信计算中的信任链技术 能够对系统启动过程以及运行中的组件进行完整性度量和信任传递，从源头解决计算机系统的安全问题。 可信计算组织TCG通过嵌	王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2015-10-04（是否引证：否） 1.多种保障系统安全的技术，比如防病毒体系、入侵检测技术和系统访问控制等。这些技术虽然能够增强系统安全，但仍然是类似打补丁的方式，没有彻底解决系统安全问题。可信计算中的信任链构建技术通过度量运行的组件和信任传递保障整个系统运行的代码都是可信的，从源头上解决计算机系统的安全问题。可信计算利用嵌入在计 王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2015-10-08（是否引证：否） 1.了多种保护系统安全的技术，例如入侵检测、病毒防护体系和系统访问控制等。这些技术虽然能够增强系统安全，但仍然是类似打补丁的方式，没有彻底解决系统安全问题。可信计算中的信任链构建技术通过度量运行的组件和信任传递保障整个系统运行的代码都是可信的，从源头上解决计算机系统的安全问题。可信计算利用嵌入在计 王星魁博士学位论文 -《学术论文联合比对库》- 2015-10-09（是否引证：否） 1.了多种保护系统安全的技术，例如入侵检测、病毒防护体系和系统访问控制等。这些技术虽然能够增强系统安全，但仍然是类似打补丁的方式，没有彻底解决系统安全问题。可信计算中的信任链构建技术通过度量运行的组件和信任传递保障整个系统运行的代码都是可信的，从源头上解决计算机系统的安全问题。可信计算利用嵌入在计 201603301253463317_王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2016-03-30（是否引证：否） 1.了多种保护系统安全的技术，例如入侵检测、病毒防护体系和系统访问控制等。这些技术虽然能够增强系统安全，但仍然是类似打补丁的方式，没有彻底解决系统安全问题。可信计算中的信任链构建技术通过度量运行的组件和信任传递保障整个系统运行的代码都是可信的，从源头上解决计算机系统的安全问题。可信计算利用嵌入在计 10112_081203_b20090055_LW 王星魁 -《学术论文联合比对库》- 2016-03-31（是否引证：否） 1.了多种保护系统安全的技术，例如入侵检测、病毒防护体系和系统访问控制等。这些技术虽然能够增强系统安全，但仍然是类似打补丁的方式，没有彻底解决系统安全问题。可信计算中的信任链构建技术通过度量运行的组件和信任传递保障整个系统运行的代码都是可信的，从源头上解决计算机系统的安全问题。可信计算利用嵌入在计 201610071545221628_王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2016-10-07（是否引证：否） 1.了多种保护系统安全的技术，例如入侵检测、病毒防护体系和系统访问控制等。这些技术虽然能够增强系统安全，但仍然是类似打补丁的方式，没有彻底解决系统

		安全问题。可信计算中的信任链构建技术通过度量运行的组件和信任传递保障整个系统运行的代码都是可信的，从源头上解决计算机系统的安全问题。可信计算利用嵌入在计 20161007224529235 7_王星魁_虚拟可信平台及数据泄漏防护研究_王星魁 -《学术论文联合比对库》- 2016-10-07（是否引证：否） 1.了多种保护系统安全的技术，例如入侵检测、病毒防护体系和系统访问控制等。这些技术虽然能够增强系统安全，但仍然是类似打补丁的方式，没有彻底解决系统安全问题。可信计算中的信任链构建技术通过度量运行的组件和信任传递保障整个系统运行的代码都是可信的，从源头上解决计算机系统的安全问题。SRK存储密
27	此处有 78 字相似 系统安全，并没有彻底解决系统安全问题。可信计算中的信任链技术能够对系统启动过程以及运行中的组件进行完整性度量和信任传递， 从源头解决计算机系统的安全问题。 可信计算组织TCG通过嵌入在计算机系统的可信度量根TPM芯片，提出了一种链式信任链度量方式，其从信任根开始一层度量一层， 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，将信任从最底层的信任根扩展到整个计算机系统，建立整	王星魁_虚拟可信平台及数据泄漏防护研究_王星魁 -《学术论文联合比对库》- 2015-10-04（是否引证：否） 1.式，没有彻底解决系统安全问题。可信计算中的信任链构建技术通过度量运行的组件和信任传递保障整个系统运行的代码都是可信的，从源头上解决计算机系统的安全问题。可信计算利用嵌入在计算机系统的可信度量根，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。在早期的度量系统中，具有代表性的是马里兰大学的 王星魁_虚拟可信平台及数据泄漏防护研究_王星魁 -《学术论文联合比对库》- 2015-10-08（是否引证：否） 1.式，没有彻底解决系统安全问题。可信计算中的信任链构建技术通过度量运行的组件和信任传递保障整个系统运行的代码都是可信的，从源头上解决计算机系统的安全问题。可信计算利用嵌入在计算机系统的可信度量根，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。1. 平台状态寄存器平台状态寄存器是T 20160330125346331 7_王星魁_虚拟可信平台及数据泄漏防护研究_王星魁 -《学术论文联合比对库》- 2016-03-30（是否引证：否） 1.式，没有彻底解决系统安全问题。可信计算中的信任链构建技术通过度量运行的组件和信任传递保障整个系统运行的代码都是可信的，从源头上解决计算机系统的安全问题。可信计算利用嵌入在计算机系统的可信度量根，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。1. 平台状态寄存器平台状态寄存器是T 20161007224529235 7_王星魁_虚拟可信平台及数据泄漏防护研究_王星魁 -《学术论文联合比对库》- 2016-10-07（是否引证：否） 1.保护对象体系Fig.2-5 The key store protection system of TPM26可信计算利用嵌入在计算机系统的可信度量根，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 王星魁博士学位论文 -《学术论文联合比对库》- 2015-10-09（是否引证：否） 1.式，没有彻底解决系统安全问题。可信计算中的信任链构建技术通过度量运行的组件和信任传递保障整个系统运行的代码都是可信的，从源头上解决计算机系统的安全问题。可信计算利用嵌入在计算机系统的可信度量根，提出了一种建立平台信任的信任链SRK存储密钥身份密钥存储密钥加密密钥签名密钥加密密钥签名密钥图2-5 TPM 密钥存储保护对象体系 10112_081203_b20090055_LW 王星魁 -《学术论文联合比对库》- 2016-03-31（是否引证：否） 1.式，没有彻底解决系统安全问题。可信计算中的信任链构建技术通过度量运行的组件和信任传递保障整个系统运行的代码都是可信的，从源头上解决计算机系统的安全问题。可信计算利用嵌入在计算机系统的可信度量根，提出了一种建立平台信任的信任链SRK存储密钥身份密钥存储密钥加密密钥签名密钥加密密钥签名密钥图2-5 TPM 密钥存储保护对象体系 201610071545221628_王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2016-10-07（是否引证：否） 1.式，没有彻底解决系统安全问题。可信计算中的信任链构建技术通过度量运行的组件和信任传递保障整个系统运行的代码都是可信的，从源头上解决计算机系统的安全问题。可信计算利用嵌入在计算机系统的可信度量根，提出了一种建立平台信任的信任链SRK存储密钥身份密钥存储密钥加密密钥签名密钥加密密钥签名密钥图2-5 TPM 密钥存储保护对象体系
28	此处有 36 字相似 链式信任链度量方式，其从信任根开始一层度量一层，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 信任从最底层的信任根扩展到整个计算机系统，建立整个平台的可信和可靠。 如图2.2所示： 图2.2 TCG信任链模型 下面本文对PCR和完整性度量机制进行简要的介绍。 （1）PCR 平	信息郝瑞 -《学术论文联合比对库》- 2014-12-08（是否引证：否） 1.开始，到硬件平台，到操作系统，再到应用软件和网络，在信任根的支持下逐层进行度量和验证，从而实现信任的逐层传递，建立起一条信任链，使信任扩展到整个计算机系统。TCG构建可信计算环境的基本思想源于人类社会学中的信任关系，信任根是可信计算环境的可信基点，是可信系统的核心。TCG为可信平台定义了三 王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2015-10-04（是否引证：否） 1.于这个要求实现实际可用的完整性度量系统，仍然有不少问题需要深入研究。信任链是信任度量模型的实施技术方案，通过信任链把信任关系从信任根扩展到整个计算机系统。在TCG的可信PC技术规范中，具体给出了可信PC中的信任链，如图3-1所示。从图3-1可以看出：这种信任链较好地体现了TCG的度量存储 王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2015-10-08（是否引证：否） 1.于这个要求实现实际可用的完整性度量系统，仍然有不少问题需要深入研究。信任链是信任度量模型的实施

		技术方案，通过信任链把信任关系从信任根扩展到整个计算机系统。在TCG的可信PC技术规范中，具体给出了可信PC中的信任链，如图3-1所示。从图3-1可以看出：这种信任链较好地体现了TCG的度量存储 王星魁博士学位论文 -《学术论文联合比对库》- 2015-10-09（是否引证：否） 1.于这个要求实现实际可用的完整性度量系统，仍然有不少问题需要深入研究。信任链是信任度量模型的实施技术方案，通过信任链把信任关系从信任根扩展到整个计算机系统。在 TCG 的可信 PC 技术规范中，具体给出了可信 PC 中的信任链，如图3-1 所示。从图 3-1 可以看出：这种信任链较好地体现了 201603301253463317_王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2016-03-30（是否引证：否） 1.于这个要求实现实际可用的完整性度量系统，仍然有不少问题需要深入研究。信任链是信任度量模型的实施技术方案，通过信任链把信任关系从信任根扩展到整个计算机系统。在TCG的可信PC技术规范中，具体给出了可信PC中的信任链，如图3-1所示。从图3-1可以看出：这种信任链较好地体现了TCG的度量存储 10112_081203_b20090055_LW 王星魁 -《学术论文联合比对库》- 2016-03-31（是否引证：否） 1.于这个要求实现实际可用的完整性度量系统，仍然有不少问题需要深入研究。信任链是信任度量模型的实施技术方案，通过信任链把信任关系从信任根扩展到整个计算机系统。在 TCG 的可信 PC 技术规范中，具体给出了可信 PC 中的信任链，如图3-1 所示。从图 3-1 可以看出：这种信任链较好地体现了 201610071545221628_王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2016-10-07（是否引证：否） 1.于这个要求实现实际可用的完整性度量系统，仍然有不少问题需要深入研究。信任链是信任度量模型的实施技术方案，通过信任链把信任关系从信任根扩展到整个计算机系统。在 TCG 的可信 PC 技术规范中，具体给出了可信 PC 中的信任链，如图3-1 所示。从图 3-1 可以看出：这种信任链较好地体现了 201610072245292357_王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2016-10-07（是否引证：否） 1.实现实际可用的完整性度量系统，仍然有不少问题需要深入研究。信任链是信任度量模型的有效的实施技术方案，通过信任链可以把信任关系从信任根一直扩展到整个计算机系统。在 TCG 的可信 PC 技术规范中，具体给出了可信 PC 中的信任链，如图 3-1 所示。从图 3-1 可以看出：这种信任链较好地体现
29	此处有 86 字相似 如图2.2所示： 图2.2 TCG信任链模型 下面本文对PCR和完整性度量机制进行简要的介绍。	王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2015-10-04（是否引证：否） 1.量启动过程中的硬件、操作系统和应用程序的方法，以此建立通用终端平台的信任。1. 平台状态寄存器在

	（1）PCR 平台状态寄存器（Platform Configuration Register, PCR），可以记录计算机系统在运行时的各种状态，比如系统的内核镜像、系统进程的信息列表等。 但是TPM芯片由于储存的信息有限，所有在PCR中存放的往往是通过SHA-1算法得到的运行状态的哈希值。 SHA-1作为一种	TPM内部有一个平台状态寄存器（Platform Configuration Register，PCR），是用来记录系统运行状态的寄存器。平台的运行状态包括内核镜像、进程信息列表和应用的二进制可执行程序等大量的信息，但是TPM芯片能够存储的信息量有限，只能存储状态的摘要，因此PCR中存放的是使用S
30	此处有 88 字相似 tion Register, PCR），可以记录计算机系统在运行时的各种状态，比如系统的内核镜像、系统进程的信息列表等。 但是TPM芯片由于储存的信息有限，所有在PCR中存放的往往是通过SHA-1算法得到的运行状态的哈希值。 SHA-1作为一种密码学散列函数，对于任何长度的输入消息都可以生产固定长度 的哈希值，一旦输入消息有1bit的差别，就会得出不同的哈希值。因此从PCR中记录的计算机软硬件配置信息是非常容易看到系统	王星魁_虚拟可信平台及数据泄漏防护研究_王星魁-《学术论文联合比对库》- 2015-10-04（是否引证：否） 1.PCR），是用来记录系统运行状态的寄存器。平台的运行状态包括内核镜像、进程信息列表和应用的二进制可执行程序等大量的信息，但是TPM芯片能够存储的信息量有限，只能存储状态的摘要，因此PCR中存放的是使用SHA-1算法得到的哈希值。SHA-1是TCG选用的密码学散列函数，对于任何长度的输入消息都生成一个固定长度（160bit）的输出结果（散列值）。只要输入消息有1bit的差别，得出的散列值就会有明显的不同。而且，散列函数是单向函 王星魁_虚拟可信平台及数据泄漏防护研究_王星魁-《学术论文联合比对库》- 2015-10-08（是否引证：否） 1.TPM内部对系统运行状态进行记录的寄存器。平台的运行状态包括内核镜像、进程信息列表和应用的二进制可执行程序等大量的信息，但是TPM芯片能够存储的信息量有限，只能存储状态的摘要，因此PCR中存放的是使用SHA-1算法得到的哈希值。SHA-1是TCG选用的密码学散列函数，对于任何长度的输入消息都生成一个固定长度（160bit）的输出结果（散列值）。只要输入消息有1bit的差别，得出的散列值就会有明显的不同。而且，散列函数是单向函 王星魁博士学位论文 -《学术论文联合比对库》- 2015-10-09（是否引证：否） 1.M内部对系统运行状态进行记录的寄存器。平台的运行状态包括内核镜像、进程信息列表和应用的二进制可执行程序等大量的信息，但是TPM芯片能够存储的信息量有限，只能存储状态的摘要，因此PCR中存放的是使用SHA-1算法得到的哈希值。SHA-1是TCG选用的密码学散列函数，对于任何长度的输入消息都生成一个固定长度（160bit）的输出结果（散列值）。只要输入消息有1bit的差别，得出的散列值就会有明显的不同。而且，散列函数是单向函 201603301253463317_王星魁_虚拟可信平台及数据泄漏防护研究_王星魁-《学术论文联合比对库》- 2016-03-30（是否引证：否） 1.TPM内部对系统运行状态进行记录的寄存器。平台的运行状态包括内核镜像、进程信息列表和应用的二进制可执行程序等大量的信息，但是TPM芯片能够存储的信息量有限，只能存储状态的摘要，因此PCR中存放的是使用SHA-1算法得到的哈希值。SHA-1是TCG选用的密码学散列函数，对于任何长度的输入消息都生成一个固定长度（160bit）的输出结果（散列值）。只要输入消

		息有1bit的差别，得出的散列值就会有明显的不同。而且，散列函数是单向函 10112_081203_b20090055_LW 王星魁 -《学术论文联合比对库》- 2016-03-31（是否引证：否） 1.M内部对系统运行状态进行记录的寄存器。平台的运行状态包括内核镜像、进程信息列表和应用的二进制可执行程序等大量的信息，但是TPM芯片能够存储的信息量有限，只能存储状态的摘要，因此PCR中存放的是使用SHA-1算法得到的哈希值。SHA-1是TCG选用的密码学散列函数，对于任何长度的输入消息都生成一个固定长度（160bit）的输出结果（散列值）。只要输入消息有1bit的差别，得出的散列值就会有明显的不同。而且，散列函数是单向函 201610071545221628_王星魁_虚拟可信平台及数据泄漏防护研究 王星魁 -《学术论文联合比对库》- 2016-10-07（是否引证：否） 1.M内部对系统运行状态进行记录的寄存器。平台的运行状态包括内核镜像、进程信息列表和应用的二进制可执行程序等大量的信息，但是TPM芯片能够存储的信息量有限，只能存储状态的摘要，因此PCR中存放的是使用SHA-1算法得到的哈希值。SHA-1是TCG选用的密码学散列函数，对于任何长度的输入消息都生成一个固定长度（160bit）的输出结果（散列值）。只要输入消息有1bit的差别，得出的散列值就会有明显的不同。而且，散列函数是单
31	此处有 658 字相似 会得出不同的哈希值。因此从PCR中记录的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 系统在启动过程中，计算机的控制权在BIOS、启动装载程序(Bootloader)、操作系统内核、操作系统外围程序和应用程序之间依次传递。如果恶意代码能够在这个启动序列中的某一个环节上截取控制权，那么它就能够任意篡改和控制之后的启动序列。例如一个恶意的启动装载程序(如恶意的Grub)可以在用户不能察觉的情况下装载一个被篡改过的Linux内核镜像。这个恶意的Linux内核镜像在启动之后，可能提供给攻击者控制整个平台的权限，破坏所有应用的完整性和机密性，敏感数据可能被攻击者所窃取。由此可见，启动序列中的任意序列受到破坏都会对整个系统的运行安全产生影响，因此，必须有一种强有力的信任机制来评估系统启动过程是否已经被攻击者所篡改。TPM硬件中的完整性度量机制就是解决这一问题的重要方法。 信任链机制是TPM对启动序列信任评估的核心。信任链是在信任当前某一环节的前提下，由该环节去评估下一个环节的安全性，确定下一环节可信之后再将控制权转交给下一环节，然后依次向后推进。在信任链中，控制权依次在受信任的客体之间传递。为了保证启动序列的每一环节都是安全可信的，那就必须能够在每一步控制权移交之前对下一个环节进行量化的判断，判断下一环节的客体是否受到了篡改。判断是否被篡改就是通过度	王星魁博士学位论文 -《学术论文联合比对库》- 2015-10-09（是否引证：否） 1.量的软件的完整性。如果这个扩展序列中的某一个度量值被改变了，之后的度量序列都会受到影响。2. 信任链产生与完整性度量系统在启动过程中，计算机的控制权在 BIOS、启动装载程序（Bootloader）、操作系统内核、操作系统外围程序和应用程序之间依次传递。如果恶意代码能够在这个启动序列中的某一个环节上截取控制权，那么它就能够任意篡改和控制之后的启动序列。例如一个恶意的启动装载程序(如恶意的 Grub)可以在用户不能察觉的情况下装载一个被篡改过的 Linux 内核镜像。这个恶意的 Linux 内核镜像在启动之后，可能提供给攻击者控制整个平台的权限，破坏所有应用的完整性和机密性，敏感数据可能被攻击者所窃取。由此可见，启动序列中的任意序列受到破坏都会对整个系统的运行安全产生影响，因此，必须有一种强有力的信任机制来评估系统启动过程是否已经被攻击者所篡改。TPM 硬件中的完整性度量机制就是解决这一问题的重要方法。信任链机制是 TPM 对启动序列信任评估的核心。信任链是在信任当前某一环节的前提下，由该环节去评估下一个环节的安全性，确定下一环节可信之后再将控制权转交给下一环节，然后依次向后推进。在信任链中，控制权依次在受信任的客体之间传递。为了保证启动序列的每一环节都是安全可信的，那就必须能够在每一步控制权移交之前对下一个环节进行量化的判断，判断下一环节的客体是否受到了篡改。判断是否被篡改就是通过度量来完成的，即将客体二进制镜像进行哈希度量

量来完成的，即将客体二进制镜像进行哈希度量，并将所得的度量值扩展到PCR中去。整个启动序列都遵循“先度量，再执行”的原则。当前阶段的代码负责度量下一阶段即将要执行的代码，然后再将度量值扩展PCR中。这样循环往复，就构成了信任链。

2.2.3

可信计算模块虚拟化

TPM虚拟化，就是在虚拟计算平台中将I/O设备虚拟化技术应用于TPM，使得该平台中的每一个虚拟机，

，并将所得的度量值扩展到PCR 中去。整个启动序列都遵循“先度量，再执行”的原则。当前阶段的代码负责度量太原理工大学博士研究生学位论文28下一阶段即将要执行的代码，然后再将度量值扩展 PCR 中。这样循环往复，就构成

2.CR 中去。整个启动序列都遵循“先度量，再执行”的原则。当前阶段的代码负责度量太原理工大学博士研究生学位论文28下一阶段即将要执行的代码，然后再将度量值扩展 PCR 中。这样循环往复，就构成了信任链。信任链的建立过程如图 2-6 所示。计算机在开始启动时，BIOS 启动模块作为信任链的源头，把通电自检 BIOS 的

1.的软件的完整性。如果这个扩展序列中的某一个度量值被改变了，之后的度量序列都会受到影响。(2) 信任链产生与完整性度量系统在启动过程中，计算机的控制权在 BIOS、启动装载程序（Bootloader）、操作系统内核、操作系统外围程序和应用程序之间依次传递。如果恶意代码能够在这个启动序列中的某一个环节上截取控制权，那么它就能够任意篡改和控制之后的启动序列。例如一个恶意的启动装载程序(如恶意的 Grub)可以在用户不能察觉的情况下装载一个被篡改过的 Linux 内核镜像。这个恶意的 Linux 内核镜像在启动之后，可能提供给攻击者控制整个平台的权限，破坏所有应用的完整性和机密性，敏感数据可能被攻击者所窃取。由此可见，启动序列中的任意序列受到破坏都会对整个系统的运行安全产生影响，因此，必须有一种强有力的信任机制来评估系统启动过程是否已经被攻击者所篡改。TPM 硬件中的完整性度量机制就是解决这一问题的重要方法。信任链机制是 TPM 对启动序列信任评估的核心。信任链是在信任当前某一环节的前提下，由该环节去评估下一个环节的安全性，确定下一环节可信之后再将控制权转交给下一环节，然后依次向后推进。在信任链中，控制权依次在受信任的客体之间传递。为了保证启动序列的每一环节都是安全可信的，那就必须能够在每一步控制权移交之前对下一个环节进行量化的判断，判断下一环节的客体是否受到了篡改。判断是否被篡改就是通过度量来完成的，即将客体二进制镜像进行哈希度量，并将所得的度量值扩展到PCR 中去。整个启动序列都遵循“先度量，再执行”的原则。当前阶段的代码负责度量太原理工大学博士研究生学位论文28下一阶段即将要执行的代码，然后再将度量值扩展 PCR 中。这样循环往复，就构成

2.CR 中去。整个启动序列都遵循“先度量，再执行”的原则。当前阶段的代码负责度量太原理工大学博士研究生学位论文28下一阶段即将要执行的代码，然后再将度量值扩展 PCR 中。这样循环往复，就构成了信任链。信任链的建立过程如图 2-6 所示。计算机在开始启动时，BIOS 启动模块作为信任链的源头，把通电自检 BIOS

的

201610071545221628_王星魁_虚拟可信平台及数据泄漏防护研究_王星魁 -《学术论文联合比对库》- 2016-10-07（是否引证：否）

1.件的完整性。如果这个扩展序列中的某一个度量值被改变了，之后的度量序列都会受到影响。(2) 信任链产生与完整性度量系统在启动过程中，计算机的控制权在BIOS、启动装载程序（Bootloader）、操作系统内核、操作系统外围程序和应用程序之间依次传递。如果恶意代码能够在这个启动序列中的某一个环节上截取控制权，那么它就能够任意篡改和控制之后的启动序列。例如一个恶意的启动装载程序(如恶意的 Grub)可以在用户不能察觉的情况下装载一个被篡改过的 Linux 内核镜像。这个恶意的 Linux 内核镜像在启动之后，可能提供给攻击者控制整个平台的权限，破坏所有应用的完整性和机密性，敏感数据可能被攻击者所窃取。由此可见，启动序列中的任意序列受到破坏都会对整个系统的运行安全产生影响，因此，必须有一种强有力的信任机制来评估系统启动过程是否已经被攻击者所篡改。TPM 硬件中的完整性度量机制就是解决这一问题的重要方法。信任链机制是 TPM 对启动序列信任评估的核心。信任链是在信任当前某一环节的前提下，由该环节去评估下一个环节的安全性，确定下一环节可信之后再将控制权转交给下一环节，然后依次向后推进。在信任链中，控制权依次在受信任的客体之间传递。为了保证启动序列的每一环节都是安全可信的，那就必须能够在每一步控制权移交之前对下一个环节进行量化的判断，判断下一环节的客体是否受到了篡改。判断是否被篡改就是通过度量来完成的，即将客体二进制镜像进行哈希度量，并将所得的度量值扩展到PCR 中去。整个启动序列都遵循“先度量，再执行”的原则。当前阶段的代码负责度量28下一阶段即将要执行的代码，然后再将度量值扩展 PCR 中。这样循环往复，就构成了信任链。信任链的建立过程如图 2-6 所示。计算机在开始启动时，BIOS 启动模块作为信任链的源头，把通电自检 BIOS 的

王星魁_虚拟可信平台及数据泄漏防护研究_王星魁 -《学术论文联合比对库》- 2015-10-04（是否引证：否）

1.软件的完整性。如果这个扩展序列中的某一个度量值被改变了，之后的度量序列都会受到影响。2. 信任链产生与完整性度量系统在启动过程中,计算机的控制权在BIOS、启动装载程序（Bootloader）、操作系统内核、操作系统外围程序和应用程序之间依次传递。如果恶意代码能够在这个启动序列中的某一个环节上截取控制权，那么它就能够任意篡改和控制之后的启动序列。例如一个恶意的启动装载程序(如恶意的Grub)可以在用户不能察觉的情况下装载一个被篡改过的Linux内核镜像。这个恶意的Linux内核镜像在启动之后，可能提供给攻击者控制整个平台的权限，破坏所有应用的完整性和机密性，敏感数据可能被攻击者所窃取。由此可见，启动序列中的任意一个环节被破坏，都会完全或部分地危及平台上所有安全应用。所以，必须有一种强有力的信任机制来评估系统启动过程是否已经被攻击

2.有应用的完整性和机密性，敏感数据可能被攻击者所窃取。由此可见，启动序列中的任意一个环节被破坏，都会完全或部分地危及平台上所有安全应用。所以，必须有一种强有力的信任机制来评估系统启动过程是否已经被攻击者所篡改。TPM硬件提供的完整性度量机制能够为启动过程提供可信评估，让设备使用者能够在系统被篡改后能对此作出正确的判断。TPM对启动序列进行评估的核心是信任

3.篡改。TPM硬件提供的完整性度量机制能够为启动过程提供可信评估，让设备使用者能够在系统被篡改后能对此作出正确的判断。TPM对启动序列进行评估的核心是信任链机制。信任链是在信任当前某一环节的前提下，由该环节去评估下一个环节的安全性，确定下一环节可信之后再将控制权转交给下一环节，然后依次向后推进。在信任链中，控制权依次在受信任的客体之间传递。为了保证启动序列的每一环节都是安全可信的，那就必须能够在每一步控制权移交之前对下一个环节进行量化的判断，判断下一环节的客体是否受到了篡改。判断是否被篡改就是通过度量来完成的，即将客体二进制镜像进行哈希度量，并将所得的度量值扩展到PCR中去。整个启动序列都遵循“先度量，再执行”的原则。当前阶段的代码负责度量下一阶段即将要执行的代码，然后再将度量值扩展PCR中。这样循环往复，就构成了信任链。信任链的建立过程如图2-6所示。计算机在开始启动时，BIOS启动模块作为信任链的源头，把通电自检BIOS的配置信息写

王星魁_虚拟可信平台及数据泄漏防护研究_王星魁 -《学术论文联合比对库》- 2015-10-08（是否引证：否）

1.软件的完整性。如果这个扩展序列中的某一个度量值被改变了，之后的度量序列都会受到影响。2. 信任链产生与完整性度量系统在启动过程中，计算机的控制权在BIOS、启动装载程序（Bootloader）、操作系统内核、操作系统外围程序和应用程序之间依次传递。。如果恶意代码能够在这个启动序列中的某一个环节上截取控制权，那么它就能够任意篡改和控制之后的启动序列。例如一个恶意的启动装载程序(如恶意的Grub)可以在用户不能察觉的情况下装载一个被篡改过的Linux内核镜像。这个恶意的Linux内核镜像在启动之后，可能提供给攻击者控制整个平台的权限，破坏所有应用的完整性和机密性，敏感数据可能被攻击者所窃取。由此可见，启动序列中的任意序列受到破坏都会对整个系统的运行安全产生影响，因此，必须有一种强有力的信任机制来评估系统启动过程是否已经被攻击者所篡改。TPM硬件中的完整性度量机制就是解决这一问题的重要方法。信任链机制是TPM对启动序列信任评估的核心。信任链是在信任当前某一环节的前提下，由该环节去评估下一个环节的安全性，确定下一环节可信之后再将控制权转交给下一环节，然后依次向后推进。在信任链中，控制权依次在受信任的客体之间传递。为了保证启动序列的每一环节都是安全可信的，那就必须能够在每一步控制权移

		交之前对下一个环节进行量化的判断，判断下一环节的客体是否受到了篡改。判断是否被篡改到PCR中去。整个启动序列都遵循“先度量，再执行”的原则。当前阶段的代码负责度量下一阶段即将要执行的代码，然后再将度量值 2.的，那就必须能够在每一步控制权移交之前对下一个环节进行量化的判断，判断下一环节的客体是否受到了篡改。判断是否被篡改到PCR中去。整个启动序列都遵循“先度量，再执行”的原则。当前阶段的代码负责度量下一阶段即将要执行的代码，然后再将度量值扩展PCR中。这样循环往复，就构成了信任链。信任链的建立过程如图2-6所示。计算机在开始启动时，BIOS启动模块作为信任链的源头，把通电自检BIOS的配置信息写
		201603301253463317_王星魁_虚拟可信平台及数据泄漏防护研究_王星魁 -《学术论文联合比对库》- 2016-03-30（是否引证：否）
		1.软件的完整性。如果这个扩展序列中的某一个度量值被改变了，之后的度量序列都会受到影响。2. 信任链产生与完整性度量系统在启动过程中，计算机的控制权在BIOS、启动装载程序（Bootloader）、操作系统内核、操作系统外围程序和应用程序之间依次传递。。如果恶意代码能够在这个启动序列中的某一个环节上截取控制权，那么它就能够任意篡改和控制之后的启动序列。例如一个恶意的启动装载程序(如恶意的Grub)可以在用户不能察觉的情况下装载一个被篡改过的Linux内核镜像。这个恶意的Linux内核镜像在启动之后，可能提供给攻击者控制整个平台的权限，破坏所有应用的完整性和机密性，敏感数据可能被攻击者所窃取。由此可见，启动序列中的任意序列受到破坏都会对整个系统的运行安全产生影响，因此，必须有一种强有力的信任机制来评估系统启动过程是否已经被攻击者所篡改。TPM硬件中的完整性度量机制就是解决这一问题的重要方法。信任链机制是TPM对启动序列信任评估的核心。信任链是在信任当前某一环节的前提下，由该环节去评估下一个环节的安全性，确定下一环节可信之后再将控制权转交给下一环节，然后依次向后推进。在信任链中，控制权依次在受信任的客体之间传递。为了保证启动序列的每一环节都是安全可信的，那就必须能够在每一步控制权移交之前对下一个环节进行量化的判断，判断下一环节的客体是否受到了篡改。判断是否被篡改到PCR中去。整个启动序列都遵循“先度量，再执行”的原则。当前阶段的代码负责度量下一阶段即将要执行的代码，然后再将度量值 2.的，那就必须能够在每一步控制权移交之前对下一个环节进行量化的判断，判断下一环节的客体是否受到了篡改。判断是否被篡改到PCR中去。整个启动序列都遵循“先度量，再执行”的原则。当前阶段的代码负责度量下一阶段即将要执行的代码，然后再将度量值扩展PCR中。这样循环往复，就构成了信任链。信任链的建立过程如图2-6所示。计算机在开始启动时，BIOS启动

模块作为信任链的源头，把通电自检BIOS的配置信息写

信息郝瑞 -《学术论文联合比对库》- 2014-12-08（是否引证：否）

1.PM的物理攻击，只能通过扩展操作来改变PCR的值。TPM的一个最典型的应用就是安全度量机制，记录了系统的启动序列。系统在启动过程中，系统的控制权在BIOS Boot Block，BIOS,启动装载程序（Bootloader）、操作系统内核以及应用程序之间依次传递。如果攻击者能够在启动序

2.，记录了系统的启动序列。系统在启动过程中，系统的控制权在BIOS Boot Block，BIOS,启动装载程序（Bootloader）、操作系统内核以及应用程序之间依次传递。如果攻击者能够在启动序列中的某一个环节上截取系统的控制权，那么它就能够任意篡改控制之后的启动序列。例如一个恶意启动装载程序加载了一个被篡改过的Linux内核镜像。这个恶意的Linux内核镜像启动之后，可以提供给攻击者控制整个平台的权限。因此启

3.者能够在启动序列中的某一个环节上截取系统的控制权，那么它就能够任意篡改控制之后的启动序列。例如一个恶意启动装载程序加载了一个被篡改过的Linux内核镜像。这个恶意的Linux内核镜像启动之后，可以提供给攻击者控制整个平台的权限。因此启动序列中的任意一个环节遭到破坏之后，整个平台的安全无法得到保障。TPM提供的完整性度量机制是一种强有力的信任机制能

4.为系统启动过程提供可信评估，能够评估系统是否已经被攻击者所篡改，在系统被篡改后能够让系统使用者对此作出正确的判断。TPM对启动序列进行评估的核心是通过信任链来实现的。是在信任当前某一环节的基础上，由该环节去评估下一个环节的完整性，确定这一环节可信之后再将系统的控制权转交给下一环节，依次类推，构建了一条信任链。在信任链中，系统控制权依次在受信任的客体之间传递。为了保证启动序列的每一环节都是可信的，就必须能够在系

5.评估下一个环节的完整性，确定这一环节可信之后再将系统的控制权转交给下一环节，依次类推，构建了一条信任链。在信任链中，系统控制权依次在受信任的客体之间传递。为了保证启动序列的每一环节都是可信的，就必须能够在系统控制权移交之前对下一个环节进行量化判断，判断下一环节客体的完整性。判断客体的完整性是通过度量来完成的，即将客体的二进制代码进行Hash运算，并将所得的Hash值扩展至PCR中。当前阶段的代码负责度量下一阶段将要执行的代码，然后再将度量值扩展到PCR中。整个启动序列都是遵循“先度量，再执行”的原则

6.的完整性。判断客体的完整性是通过度量来完成的

，即将客体的二进制代码进行Hash运算，并将所得的Hash值扩展至PCR中。当前阶段的代码负责度量下一阶段将要执行的代码，然后再将度量值扩展到PCR中。整个启动序列都是遵循“先度量，再执行”的原则。在信任链中，信任根在启动过程中没有被度量，即存在一个假设信任根是可信

TPM功能介绍 - Sunshine - 《网络（http://blog.csdn.net）》-（是否引证：否）

1.记录整个平台的状态，但PCR并不只用于校验度量日志，因此在启动过程中用到了多个PCR。 2.2 信任链产生与完整性度量 恶意代码能够在这个启动序列中的某一个环节上截取控制权，那么它就能够任意篡改和控制之后的启动序列。必须有一种强有力的信任机制来评估系统启动过程是否已经被攻击者所篡改，TPM硬件提供的完整性度量机制能够为启动过程提供可信

2.信任链产生与完整性度量 恶意代码能够在这个启动序列中的某一个环节上截取控制权，那么它就能够任意篡改和控制之后的启动序列。必须有一种强有力的信任机制来评估系统启动过程是否已经被攻击者所篡改，TPM硬件提供的完整性度量机制能够为启动过程提供可信评估，让机器使用者能够在系统被篡改后能够对此作出正确判断。 信任传递机制：在信任当前某一环节的前提

3.件提供的完整性度量机制能够为启动过程提供可信评估，让机器使用者能够在系统被篡改后能够对此作出正确判断。 信任传递机制：在信任当前某一环节的前提下，由该环节去评估下一个环节的安全性，确定下一环节可信之后再将控制权转交给下一环节，然后依次向后推进。整个启动序列中都遵循“先度量，再执行”的原则，当前阶段的代码负责度量下一阶段即将要执行的代码，然后再将度量扩展到PCR寄

4.当前某一环节的前提下，由该环节去评估下一个环节的安全性，确定下一环节可信之后再将控制权转交给下一环节，然后依次向后推进。整个启动序列中都遵循“先度量，再执行”的原则，当前阶段的代码负责度量下一阶段即将要执行的代码，然后再将度量扩展到PCR寄存器中，这样循环往复，这就构成了信任链。 源头（BIOS启动模块）在启动过程中是没有受到度量，即存在一个假设—这个源头是安全可信的。大多数PC系统使用的是可刷写的

基于可信计算的远程证明的研究 黄秀文; -《武汉纺织大学学报》- 2015-12-15（是否引证：否）

1..1.1可信度量平台可信度量是指通过一定的方法按步骤度量并报告平台的状态。从系统加电启动,一直到最后应用程序每一步都需要度量,整个启动序列都遵循“先度量,再执行”的原则。当前阶段的代码负责度量下一阶段即将要执行的代码,然后再将度量值扩展到PCR中,这样一级信任一级,以此保证平台的可信,保证环境的安全。当然任何信任关系中总是存在某种基础性的假设,必然存

		在默认环节的信任关系的基石。在一个

指　标

疑似剽窃观点

---

1. 由此可见，启动序列中的任意序列受到破坏都会对整个系统的运行安全产生影响，因此，必须有一种强有力的信任机制来评估系统启动过程是否已经被攻击者所篡改。

疑似剽窃文字表述

---

1. 1.4 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，
2. 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章主要介绍了云计算中的关键技术——虚拟化技术，
3. 指令集架构级的虚拟化系统主要由Qemu系统和Bochs系统。
   硬件级虚拟化，这种虚拟
4. 计算机具有相同的指令集，可以在用户指令可以直接在计算机主机上进行运行，为用户操作虚拟的计算机提供了遍历，提高了指令运行的效率和速度。基于硬件级虚拟化技术，用户可以方便的使用被映射为物理资源的虚拟机资源，是目前云计算
5. 当前典型的操作系统级虚拟化系统有 Linux-VSerser、Solaris Container，以及Docker等容器技术。
6. 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，以便完成特权指令的虚拟化。
7. KVM 内核模块在运行时按需加载进入内核空间运行。KVM 本身不执行任何设备模拟，需要 QEMU 通过 /dev/kvm 接口设置一个 GUEST OS 的地址空间，向它提供模拟的 I/O 设备，并将它的视频显示映射回宿主机的显示屏。
8. 从源头解决计算机系统的安全问题。
   可信计算组织TCG通过嵌入在计算机系统的可信度量根TPM芯片，提出了一种链式信任链度量方式，其从信任根开始一层度量一层，
9. 但是TPM芯片由于储存的信息有限，所有在PCR中存放的往往是通过SHA-1算法得到的运行状态的哈希值。SHA-1作为一种密码学散列函数，对于任何长度的输入消息都可以生产固定长度
10. 如果恶意代码能够在这个启动序列中的某一个环节上截取控制权，那么它就能够任意篡改和控制之后的启动序列。
11. 这个恶意的Linux内核镜像在启动之后，可能提供给攻击者控制整个平台的权限，破坏所有应用的完整性和机密性，敏感数据可能被攻击者所窃取。
12. TPM硬件中的完整性度量机制就是解决这一问题的重要方法。
    信任链机制是TPM对启动序列信任评估的核心。信任链是在信任当前某一环节的前提下，由该环节去评估下一个环节的安全性，确定下一环节可信之后再将控制权转交给下一环节，然后依次向后推进。在信任链中，控制权依次在受信任的客体之间传递。为了保证启动序列的每一环节都是安全可信的，那就必须能够在每一步控制权移交之前对下一个环节进行量化的判断，判断下一环节的客体是否受到了篡改。判断是否被篡改就是通过度量来完成的，即将客体二进制镜像进行哈希度量，并将所得的度量值扩展到PCR中去。整个启动序列都遵循“先度量，再执行”的原则。当前阶段的代码负责度量下一阶段即将要执行的代码，然后再将度量值扩展PCR中。这样循环往复，就构成了信任链。
    2.2.3

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. 6_齐能_具有瀑布特征的可信虚拟平台信任链模型_第3部分

总字数：10300

相似文献列表　文字复制比：15.4%(1585)　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	14.0%（1439） 是否引证：否
2	陈志远_基于模态逻辑的模型检测技术研究 陈志远 -《学术论文联合比对库》- 2013-12-22	1.1%（113） 是否引证：否
3	面向计时攻击的形式化分析 王寅龙;赵强;林克成;李志祥;王希武;邓高明; -《计算机科学》- 2011-10-15	0.8%（79） 是否引证：否
4	CTCS-4级安全通信协议的形式化建模和验证 陈慧丽(导师：石广田) -《兰州交通大学硕士论文》- 2013-06-01	0.8%（79） 是否引证：否
5	复旦MSE复习资料-软件工程部分(SE01 概论2011) - 豆丁网 -《互联网文档资源（http://www.docin.com）》- 2015	0.8%（79） 是否引证：否
6	基于UML模型规约的程序切片技术研究--优秀毕业论文 - 豆丁网 -《互联网文档资源（http://www.docin.com）》- 2016	0.8%（79） 是否引证：否
7	复杂系统需求获取形式化的研究 - 豆丁网 -《互联网文档资源（http://www.docin.com）》- 2016	0.8%（79） 是否引证：否
8	0210822陈慧丽 陈慧丽 -《学术论文联合比对库》- 2013-04-16	0.8%（79） 是否引证：否
9	0210828寻璐 -《学术论文联合比对库》- 2013-04-16	0.8%（79） 是否引证：否
10	匹配版352368583 -《学术论文联合比对库》- 2014-03-14	0.8%（79） 是否引证：否
11	20109130221486 -《学术论文联合比对库》- 2013-03-13	0.8%（79） 是否引证：否
12	20109130226459 -《学术论文联合比对库》- 2013-03-25	0.8%（79） 是否引证：否
13	基于混合层次关系的扩展角色图模型研究 黎湘运(导师：封孝生) -《国防科学技术大学硕士论文》- 2010-11-01	0.8%（79） 是否引证：否
14	智能高速列车无线闭塞中心交接形式化描述与验证 寻璐(导师：胡晓辉) -《兰州交通大学硕士论文》- 2013-06-01	0.8%（79） 是否引证：否
15	基于场景和形式化方法的软件需求建模研究 程勇(导师：袁兆山) -《合肥工业大学硕士论文》- 2002-06-03	0.8%（79） 是否引证：否
16	形式语言B与OOZS的比较 沈洁; -《经济研究导刊》- 2011-01-05	0.7%（76） 是否引证：否
17	形式语言B与RSL的比较 张宏;邹盛荣; -《电脑知识与技术》- 2008-11-25	0.7%（76） 是否引证：否
18	基于MWB的BPEL到π演算自动转换工具的研究与实现 程锋涛(导师：侯红) -《西北大学硕士论文》- 2010-06-30	0.4%（46） 是否引证：否
19	基于CPS的实时系统的面向方面的形式化方法 邓建波(导师：张立臣) -《广东工业大学硕士论文》- 2011-05-01	0.4%（46） 是否引证：否
20	威胁评估发展刍议 吴文龙;黄文斌;刘剑; -《电光与控制》- 2012-12-01	0.3%（34） 是否引证：否
21	基于PVS对SCADE开发轨交控制系统的形式化建模与验证 周佳铭(导师：郭建) -《华东师范大学硕士论文》- 2011-05-01	0.3%（32） 是否引证：否

	原文内容	相似内容来源
1	此处有 32 字相似 对TPM虚拟化必须满足这两方面的安全要求。方便性	陈志远_基于模态逻辑的模型检测技术研究 陈志远 -《学术论文联合比对库》- 2013-12-22（是否引证：否）

	，是指在TPM虚拟化完成之后，方便对其进行维护、升级和迁移。 2.3 形式化分析方法 在计算机科学和软件工程的学科领域中，形式化方法是适合针对软件系统和硬件系统的描述、开发以及验证的基于数学逻辑的特种技术。形式化分析方法的目的是期望软件和硬件设计过程中	1.行结合，得到时态道义逻辑系统。现在对道义逻辑与时态逻辑组合起来进行研究仍然是一个研究热点[][][]。 1.2.2 形式化方法在计算机科学和软件工程领域，形式化方法[][]（Formal methods）广泛应用于软件和硬件系统的描述、开发和验证。其本质是基于数学的方法来描述目标软件
2	此处有 83 字相似 重安全性和可靠性的高度整合的系统。形式化方法通常有一套十分严谨的定义和概念，比如一致性和完整性，以及拥有严谨的证明规范。 其本质是基于良好的数学逻辑方法来描述软件系统拥有安全属性的一直技术。不同的形式化方法的数学基础是不同的，有的以集合论和一阶谓词演算为基础，有的则以时态逻辑为基础。 2.3.1 无干扰理论 1982年，Goguen和Meseguer[]最早提出基于信息流的无干扰理论，但是目前使用的无	基于场景和形式化方法的软件需求建模研究 程勇 -《合肥工业大学硕士论文》- 2002-06-03（是否引证：否） 1.如：一致性和完整性，以及定义规约，实现和正确性。 形式化方法的本质是基于数学的方法来描述目标软件系统属性的一种技术。不同形式化方法的数学基础是不同的，有的以集合论和一阶谓词演算为基础侧Z和VDM，有的则以时态逻辑为基础。形式化方法通常还需要形式规约说明语言的支持。形式规约说明语言由语法、语义和一组关系组成p”肥· 形式语言B与RSL的比较 张宏;邹盛荣; -《电脑知识与技术》- 2008-11-25（是否引证：否） 1.型地以形式化规约语言给出。这个基础提供一系列精确定义的概念,如:一致性和完整性,以及定义规范的实现和正确性。形式化方法的本质是基于数学的方法来描述目标软件系统属性的一种技术。不同的形式化方法的数学基础是不同的,有些方法是基于集合论和一阶谓词演算。有些是基于时态逻辑。RSL和B都是是基于集合论和一阶谓词演算。2.3逻辑基础B建立在Zermelo-Frankel集合理论基础上,B抽象机符 基于混合层次关系的扩展角色图模型研究 黎湘运 -《国防科学技术大学硕士论文》- 2010-11-01（是否引证：否） 1.模工具；数学特别适合于表示状态，也就是表示“做什么”，数学比自然语言更适于描述详细的需求。 形式化方法的本质是基于数学的方法来描述目标软件系统属性的一种技术。不同的形式化方法的数学基础是不同的，有的以集合论和一阶谓词演算为基础（如Z 和VDM），有的则以时态逻辑为基础。形式化方法需要形式化规约说明语言的支持。 基于模型的形式化方法通过明确定义状态和操作来建立一个系统模型（ 形式语言B与OOZS的比较 沈洁; -《经济研究导刊》- 2011-01-05（是否引证：否） 1.型地以形式化规约语言给出。这个基础提供一系列精确定义的概念,如:一致性和完整性,以及定义规范的实现和正确性。形式化方法的本质是基于数学的方法来描述目标软件系统属性的一种技术。不同的形式化方法的数学基础是不同的,有些方法是基于集合论和一阶谓词演算。有些是基于时态逻辑。OOZS和B就是采用一阶谓词逻辑和集合论作为其形式语义基础,把映射、函数等数学概念用到规格说明中来,简明直观,易于阅读提 面向计时攻击的形式化分析 王寅龙;赵强;林克成;李志祥;王希武;邓高明; -《计算机科学》- 2011-10-15（是否引证：否）

		1.型地以形式化规约语言给出。这个基础提供了一系列精确定义的概念,如一致性和完整性,以及定义规范的实现和正确性。形式化方法的本质是基于数学的方法来描述目标软件系统属性的一种技术。不同的形式化方法的数学基础是不同的,有的以集合论和一阶谓词演算为基础,有的则以时态逻辑为基础。形式化方法需要形式化规约说明语言的支持[8]。2.1等价关系与划分集合S上的等价关系是一个二元关系RS×S,它是自反、 20109130221486 -《学术论文联合比对库》- 2013-03-13（是否引证：否） 1.型地以形式化规约语言给出。这个基础提供一系列精确定义的概念，如：一致性和完整性，以及定义规范的实现和正确性。形式化方法的本质是基于数学的方法来描述目标软件系统属性的一种技术。不同的形式化方法的数学基础是不同的，有的以集合论和一阶谓词演算为基础，有的则以时态逻辑为基础。形式化方法需要形式化规约说明语言的支持。3.1.2 形式化方法的分类按照形式化方法的说明目标软件系统对其进行 20109130226459 -《学术论文联合比对库》- 2013-03-25（是否引证：否） 1.型地以形式化规约语言给出。这个基础提供一系列精确定义的概念，如：一致性和完整性，以及定义规范的实现和正确性。形式化方法的本质是基于数学的方法来描述目标软件系统属性的一种技术。不同的形式化方法的数学基础是不同的，有的以集合论和一阶谓词演算为基础，有的则以时态逻辑为基础。形式化方法需要形式化规约说明语言的支持。形式化方法的主要优势是可以做到不用运行系统也可以模拟证明其具有的功能。形式 0210822陈慧丽 陈慧丽 -《学术论文联合比对库》- 2013-04-16（是否引证：否） 1.型地以形式化规约语言给出。这个基础提供一系列精确定义的概念，如：一致性和完整性，以及定义规范的实现和正确性。形式化方法的本质是基于数学的方法来描述目标软件系统属性的一种技术。不同的形式化方法的数学基础是不同的，有的以集合论和一阶谓词演算为基础，有的则以时态逻辑为基础。形式化方法需要形式化规约说明语言的支持。形式化方法的主要优势是可以做到不用运行系统也可以模拟证明其具有的功能。形式 0210828寻璐 -《学术论文联合比对库》- 2013-04-16（是否引证：否） 1.么它就是形式化的，典型地以形式化规约语言给出。这个基础提供一系列精确定义的概念，以及定义规范的实现和正确性。形式化方法的本质是基于数学的方法来描述目标软件系统属性的一种技术。不同的形式化方法的数学基础是不同的，有的以集合论和一阶谓词演算为基础，有的则以时态逻辑为基础。形式化方法需要形式化规约说明语言的支持。采用形式化的方法对软件系统建立的模型，有利于发现软件系统的是否一致性和不完整性等 智能高速列车无线闭塞中心交接形式化描述与验证 寻璐 -《兰州交通大学硕士论文》- 2013-06-01（是否引证：否）

1.好的结构性、更优的可维护性、较高的可信度，可以更好的满足用户对软件质量的需求[13][14][15]。形式化方法的本质是基于数学的方法来描述目标软件系统属性的一种技术。不同的形式化方法的数学基础是不同的，有的以集合论和一阶谓词演算为基础，有的则以时态逻辑为基础。形式化方法需要形式化规约说明语言的支持。3.1.2 形式化方法的分类按照形式化方法的说明目标软件系统对其进行

CTCS-4级安全通信协议的形式化建模和验证 陈慧丽 -《兰州交通大学硕士论文》- 2013-06-01（是否引证：否）

1.形式化规约语言给出。这个基础提供一系列精确定义的概念，如一：致性和完整性，以及定义规范的实现和正确性。形式化方法的本质是基于数学的方法来描述目标软件系统属性的一种技术。不同的形式化方法的数学基础是不同的，有的以集合论和一阶谓词演算为基础，有的则以时态逻辑为基础。形式化方法需要形式化规约说明语言的支持。形式化方法的主要优势是可以做到不用运行系统也可以模拟证明其具有的功能

陈志远_基于模态逻辑的模型检测技术研究 陈志远 -《学术论文联合比对库》- 2013-12-22（是否引证：否）

1.算机科学和软件工程领域，形式化方法[][]（Formal methods）广泛应用于软件和硬件系统的描述、开发和验证。其本质是基于数学的方法来描述目标软件系统性质的一种技术。不同的形式化方法的数学基础是不同的，有的以集合论和一阶谓词演算为基础，有的则以时态逻辑为基础。将形式化方法应用于软件系统和硬件设计中，是期望能够像其它工程学科一样，通过适当的数学分析以提高系统设计的可靠性和鲁棒性。

匹配版352368583 -《学术论文联合比对库》- 2014-03-14（是否引证：否）

1.型地以形式化规约语言给出。这个基础提供一系列精确定义的概念，如：一致性和完整性，以及定义规范的实现和正确性。形式化方法的本质是基于数学的方法来描述目标软件系统属性的一种技术。不同的形式化方法的数学基础是不同的，有的以集合论和一阶谓词演算为基础，有的则以时态逻辑为基础。形式化方法需要形式化规约说明语言的支持。形式化方法的主要优势能够做到通过描述系统自身的行为和功能，不通过运行系统来

复旦MSE复习资料-软件工程部分(SE01 概论2011) - 豆丁网 -《互联网文档资源（http://www.docin.com）》- 2015-9-13 2:20:28（是否引证：否）

1.型地以形式化规约语言给出。这个基础提供一系列精确定义的概念,如,一致性和完整性,以及定义规范的实现和正确性。形式化方法的本质是基于数学的方法来描述目标软件系统属性的一种技术。不同的形式化方法的数学基础是不同的,有的以集合论和一阶谓词演算为基础,如Z和VDM,有的则以时态逻辑为基础。形式化方法需要形式化规约说明语言的支持53 ?根据说明目标软件系统的方式,形式化方法可以分为两类?1,面向模型的形式化方

基于UML模型规约的程序切片技术研究--优秀毕业论文 - 豆丁网 -《互联网文档资源（http://www.docin.com）》- 2016-5-23 8:07:39（是否引证：否）

1.的以形式化规约语言给出。这个基础提供一系列精确定义的概念,如,一致性和完整行,以及定义规范的实现和正确性。 形式化方法的本质是用基于数学的方法来描述目标软件系统属性的一种技术。不同的形式化方法的数学基础是不同的,有的以集合论和一阶谓词演算为基础,如Z和VDM,有的则以时态逻辑为基础[40]。形式化方法需要形式化规约说明语言的支持。 基于UML模型规约的程序切片技术研究 - 24 - 4.1.2 形式化方法的研

复杂系统需求获取形式化的研究 - 豆丁网 -《互联网文档资源（http://www.docin.com）》- 2016-6-19 15:48:23（是否引证：否）

1.型地以形式化规约语言给出。这个基础提供一系列精确定义的概念,如,一致性和完整性,以及定义规范的实现和正确性。形式化方法的本质是基于数学的方法来描述目标软件系统属性的一种技术。不同的形式化方法的数学基础是不同的,有的以集合论和一阶谓词演算为基础,如,和,有的则以时态逻辑为基础。形式化方法需要形式化规约说明语言的支持。,扬州大学硕士学位论文形式化方法的本质是基于数学的方法来描述目标软件系统属性的一

基于MWB的BPEL到π演算自动转换工具的研究与实现 程锋涛 -《西北大学硕士论文》- 2010-06-30（是否引证：否）

1.式刻划、开发和验证系统。形式化方法有良好的数学基础，它是以典型地以形式化规约语言给出的数学方法。不同的形式化方法的数学基础是不同的，有的以集合论和一阶谓词演算为基础，有的则以时态逻辑为基础。形式化方法主要分为形式验证方法和形式规范方法两大类。其中形式化验证方法是指通过结果来判定与之前需

基于CPS的实时系统的面向方面的形式化方法 邓建波 -《广东工业大学硕士论文》- 2011-05-01（是否引证：否）

1.语言给出。这个基础提供一系列一致性和完整性的精确定义的概念，以及定义规范的实现和正确性。形式化方法的本质是基于数学方法来描述目标软件系统属性的一种技术，不同形式化方法的数学基础不同，但形式化方法需要形式化规约说明语言支持。 形式化方法的一个重要研究内容是形式规约(F ormal Spe

威胁评估发展刍议 吴文龙;黄文斌;刘剑; -《电光与控制》- 2012-12-01（是否引证：否）

1.态势和威胁事件进行推理。5形式化方法表述为便于威胁评估的计算机实现,有必要对其进行形式化方法的表述,其实质是基于数学方法描述目标系统属性。不同形式化方法的数学基础不同,文中主要基于集合论和谓词演算进行说明。对用于描述和推理关联、态势和威胁等的形式概念进行定义,应明确关联不仅仅是一个多目标

基于PVS对SCADE开发轨交控制系统的形式化建模与验证 周佳铭 -《华东师范大学硕士论文》- 2011-05-01（是否引证：否）

		1.又寸SCADE SLlite进行形式化转换的意义。2.1形式化方法理论 形式化方法的本质是用基于数学的方法来描述目标设计系统属性的一种技术，它是对程序“做什么”的数学描述l’“!，用具有精确语义的形式语言书写的程序功能描述，它也是设计和编写程序的出发
3	此处有 58 字相似 QT架构及信任链模型进行详细的描述。本文主要针对TVP-QT及信任链模型，而针对虚拟化平台固有的安全性机制，比如VMM的 特权域操作、VM之间的隔离性等安全性机制，可参考Gilles Barthe[52]等学者给出的形式化描述与分析[]。 本文在本节对TVP-QT的功能组件以及TVP-QT信任链信任属性进行定义，本文在第4章将利用文献[27]提出的安全系统逻	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.分析,因此不考虑虚拟化平台自身的固有安全机制,比如虚拟机监控器(VMM,virtual machinemonitor)的特权操作、虚拟机之间的隔离及内存操作控制等,可参考Gilles Barthe等给出的形式化描述与分析[14]。2.1 TVP信任模型HP、IBM等研究机构都针对虚拟化环境提出并构建了相应的TVP[2~4],但这些研究主要侧重于具体
4	此处有 262 字相似 Loader、VMOS、应用程序（APP）等相关组件。基于上述对TVP-QT的分析，本文从功能角度给出TVP-QT的抽象 定义。 定义3.1 TVP-QT是具有可信功能的虚拟化计算平台，主要包括2类功能组件：TVP-QT:={M, RT}，M表示虚拟化平台所有主机类型集合，包括构成虚拟化平台的基本组件VMM、管理域内核、可信衔接点及用户虚拟机等，它们是利用虚拟化技术为用户提供资源与服务的主体；信任根（Root of Trust, RT）是构建TVP信任环境的基础，也是TVP的核心组件，对虚拟化平台来说，它包括硬件TPM、可信衔接点TJP和vTPM。 对于TVP的主机M，根据其类型进一步细化为M:={m, vm}，其中，m:={VMM, Dom0 Kernel, TJP}，特指底层的VMM、Dom0 Kernel和可信衔接点TJP，它们是 TVP 的TC	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.是用户虚拟机,是与用户应用密切相关的部分。基于上述分析,本文从功能角度给出以下TVP的抽象定义。图1 TVP基本运行架构定义1 TVP是具有可信功能的虚拟化计算平台,它主要包含2类功能组件:TVP:={M,RT},其中,M表示虚拟化平台所有主机类型集合,包括构成虚拟化平台的基本组件VMM、管理域及用户虚拟机等,它们是利用虚拟化技术为用户提供资源与服务的主体;信任根(RT,root of trust)是构建TVP信任环境的基础,也是TVP的核心组件,对虚拟化平台来说,它包括硬件可信芯片TPM和vRT。对于TVP的主机M,根据其类型进一步细化为M:={m,vm},其中,m:={vmm,admindomker},特指底层的VMM及admindomker,它们是TVP的TCB的主要组成部分。vm:={vm1
5	此处有 113 字相似 om0 Kernel, TJP}，特指底层的VMM、Dom0 Kernel和可信衔接点TJP，它们是 TVP 的TCB。 vm:={vm1, …，vmn}，表示虚拟化平台上层的用户虚拟机vm 集合。 相似地，TVP的信任根也进一步分类为RT:={TPM, vRT}={TPM, (TJP, vTPM)}，其中，TPM 是底层的硬件信任根，主要 通过可信计算技术为物理平台提供信任保障，它拥有可信平台的非易失存储、密钥存储等固有特性；vRT包含可信衔接点TJP和vT	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:={vmm,admindomker},特指底层的VMM及admindomker,它们是TVP的TCB的主要组成部分。vm:={vm1,…,vmn},表示虚拟化平台上层的用户虚拟机vm集合*。相似地,TVP的信任根也进一步分类为RT:={TPM,vRT},其中,TPM是硬件信任根,主要用于为物理平台提供信任保障,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
6	此处有 82 字相似 计算技术为物理平台提供信任保障，它拥有可信平台的非易失存储、密钥存储等固有特性；vRT包含可信衔接点TJP和vTPM，在	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.PM,vRT},其中,TPM是硬件信任根,主要用于为物理平台提供信任保障,它拥有非易失存储及密钥存储等固有特

	功能实现上可表现为主机m中内核组件或部分独立的可信组件，本文将vRT抽象为一个独立的可信功能组件，通过特定的映射关系与硬件信任根TPM关联，以确保其vRT的可信性。 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的可信依赖于物理TPM，用来衔接底层的虚	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TVP:={(m
7	此处有 35 字相似 nel, TJP)), ((TJP, vTPM1), vm1), …,((TJP, vTPMn), vmn) } 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	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.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
8	此处有 74 字相似 此，TVP-QT更符合TCG的链式度量标准。另一方面，TVP-QT增加了TJP，从逻辑上比已有的TVP更加合理。 3. 2 TVP-QT信任链及属性 TCG 组织从实体行为预期性角度给出可信的定义，并采用装载前度量的方案，给出了信任链传递和控制权转移的过程[19]。 并且，TVP的信任链与普通可信计算平台相似，也需要保证可信平台能够基于信任根，通过逐级的信任传递，对可信虚拟化平台环境进	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.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TCG组织从实体行为预期性角度给出可信的定义,并采用装载前度量的方案,给出了信任链传递和控制权转移的过程。与普通可信计算平台类似,TVP的信任链同样需要保障平台能够基于信任根,通过逐级的信任传递,构建虚拟化平台的可信运行环境。
9	此处有 117 字相似 定义，并采用装载前度量的方案，给出了信任链传递和控制权转移的过程[19]。并且，TVP的信任链与普通可信计算平台相似，也 需要保证可信平台能够基于信任根，通过逐级的信任传递，对可信虚拟化平台环境进行构建。但是，虚拟化平台可以同时执行多个用户虚拟机实例，使得构建在其至上的信任链传递会出现不同的信任链分支，这与可信计算最初构建信任环境的思想并不一致[19]。 尽管如此，只要虚拟化平台能够确保信任链构建过程的唯一性、正确性，以及能对任意的外部实体R证明确实构建了对应的信任链，那么	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.度给出可信的定义,并采用装载前度量的方案,给出了信任链传递和控制权转移的过程。与普通可信计算平台类似,TVP的信任链同样需要保障平台能够基于信任根,通过逐级的信任传递,构建虚拟化平台的可信运行环境。由于虚拟化平台自身的特殊性,它要求并发地执行多个用户虚拟机实例,因此,其信任链与普通可信平台的信任链存在不同(如图1所示 2.一层到第二层的信任传递(主机m),还要增加之后的第三层vRT与第四层用户虚拟机的信任传递,而且第四层中的用户虚拟机还需要多个实例并发执行,使得信任传递会出现多个不同分支,这与可信计算最初构建信任环境的思想并不一致。为了确保这种信任传递的正确性,需要对TVP信任链进行形式化验证,证明在程序控制权传递过程中,各个进程的确能够按照预期执行
10	此处有 62 字相似 示，从外部实体来看，虚拟化平台仍然满足TCG最初建	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)

	立信任环境的思想。 图3.2 虚拟化平台可信环境信任链构建与验证 为了确保这种信任传递的正确性，需要对 TVP-QT信任链进行验证，证明在程序控制权传递过程中，各个进程的确能够按照预期执行， 而且能够对外证明上述属性。本文将上述验证目标抽象为信任链的信任属性（Trusted Property, TP），其抽象定	1.第四层中的用户虚拟机还需要多个实例并发执行,使得信任传递会出现多个不同分支,这与可信计算最初构建信任环境的思想并不一致。为了确保这种信任传递的正确性,需要对TVP信任链进行形式化验证,证明在程序控制权传递过程中,各个进程的确能够按照预期执行,整个过程不存在信任缺失(比如存在其他程序执行、加载等情况),而且能够对外证明上述属性。本文将上述验证目标抽象为信任链的信
11	此处有 51 字相似 确保这种信任传递的正确性，需要对 TVP-QT信任链进行验证，证明在程序控制权传递过程中，各个进程的确能够按照预期执行， 而且能够对外证明上述属性。本文将上述验证目标抽象为信任链的信任属性（Trusted Property, TP），其抽象定义如下。 定义3.2 （TVP-QT信任链模型的信任属性TPTVP-QT）根据上文对TVP-QT信任	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.,证明在程序控制权传递过程中,各个进程的确能够按照预期执行,整个过程不存在信任缺失(比如存在其他程序执行、加载等情况),而且能够对外证明上述属性。本文将上述验证目标抽象为信任链的信任属性(TP,trustedproperty),这种信任属性的验证包括2个方面,一方面是信任链在本地平台构建过程中的唯一性、正确性验证,另一方面是平台向外部实体R证明自
12	此处有 39 字相似 信任属性的描述，TVP-QT的信任属性应该定义为一个二元组TPTVP-QT:={TCTVP-QT,VerTVP-QT}， 其中TCTVP-QT表示TVP-QT信任链模型构建时所包含的可信组件传递序列， 即上文对TVP-QT信任链模型具体构建过程的描述的各个组件序列。VerTVP-QT表示为对TVP-QT信任链模型执行序列	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.。定义2(TVP信任链的信任属性TPTVP)TVP的信任属性定义为一个二元组TPTVP:={TCTVP,VerTVP},其中,TCTVP表示TVP信任链构建时所包含的可信程序传递序列,VerTVP表示对该信任链执行序列的远程验证。按照2.1节中对TVP中相应功能组件的定义,该信任属性可以进一步细化为TP
13	此处有 82 字相似 链模型构建时所包含的可信组件传递序列，即上文对TVP-QT信任链模型具体构建过程的描述的各个组件序列。VerTVP-QT 表示为对TVP-QT信任链模型执行序列的远程认证。 按照3.1节对TVP-QT中相应功能组件的定义，该TVP-QT信任属性可以进一步细分为： TPTVP-QT: ={TCTVP-QT,VerTVP-QT} ={(TCm,TCvRT,,TCvm),(Verm, VervRT,, 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.TPTVP:={TCTVP,VerTVP},其中,TCTVP表示TVP信任链构建时所包含的可信程序传递序列,VerTVP表示对该信任链执行序列的远程验证。按照2.1节中对TVP中相应功能组件的定义,该信任属性可以进一步细化为TPTVP:={(TCm,TCvRT,TCvm),(Verm,VervRT,Vervm)}。可见,该信任属性根据组件类型可分为3类:
14	此处有 77 字相似 T，以及用户虚拟机的信任属性TCvm。其中TCvRT包含TCTJP 和TCvTPM两个属性。下面对TVP-QT三类组件的 信任属性分别进行阐述。 （1）主机m的信任属性表示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 第一层硬件TPM的CRTM到Dom0 Kernel的可信启动过程：(CRTM→BIOS→OSLoader→VMM→Dom	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.,Vervm)}。可见,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)到上层用户应用的可信启动过程

15	此处有 175 字相似 OSLoader→VMM→Dom0 Kernel)TPM_Static，此部分信任链可基于硬件可信芯片TPM的可信度量， 且在TVP-QT信任链传递过程中不存在除TVP-QT信任链组件之外的程序代码加载。Verm:=Verify(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R相信TVP-QT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。由定义3.1对vRT以及定义3.2对TVP-QT信任属性的定义，可对TPvRT进行进一步细分： TPvRT:={(TC	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.of trust for measurement)到上层用户应用的可信启动过程:(CRTM BL OS App)TPM,且在信任传递过程中不存在其他程序代码加载。Verm:=Verify(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
16	此处有 85 字相似 VP-QT的可信衔接点拥有这样的信任链属性TCTJP；TCvTPM表示基于硬件信任根构建的用户虚拟机信任根vTPM，值得 注意的是，vTPM的信任属性与其实现方式密切相关，它可能实现为一个微内核系统或一个应用进程，而且需要建立vTPM与TPM之间的强依赖关系，以硬件信任根保障vTPM的可信。 TJP到vTPM的信任传递，既可以采用静态度量，也可以采用动态度量，其信任传递的过程为：(TJP→vTPM)TPM_St	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.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,而且需要建立vRT与硬件信任根之间的强依赖关系,以硬件信任根保障软件vRT的可信。 3)vm的信任属性与上述主机m的信任属性类似,表示为TPvm:={TCvm,Vervm},其中,TCvm:=(INIT
17	此处有 64 字相似 _Staic或(TJP→vTPM)TPM_Dynamic。 VervTPM:=Verify(vTPM, VervTPM) 表示对外验证vTPM所声称的信任属性TCvTPM，使远程验证者R相信TVP-QT的vTPM拥有这样的信任链属性TCvTPM； （3）用户虚拟机vm的信任属性类似主机m的信任属性类似，表示为TPvm:={TCvm, Vervm}，其中TCvm表示	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.(CRTM BL OS App)TPM,且在信任传递过程中不存在其他程序代码加载。Verm:=Verify(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,
18	此处有 40 字相似 PM所声称的信任属性TCvTPM，使远程验证者R相信TVP-QT的vTPM拥有这样的信任链属性TCvTPM； （3） 用户虚拟机vm的信任属性类似主机m的信任属性类似，表示为TPvm:={TCvm, Vervm}，其中TCvm表示基于vTPM构建的信任链，在创建vm时需采用动态度量方式对TJP进行度量，vm从初始化到	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.VervRT,Vervm)}。可见,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 roo
19	此处有 54 字相似	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

	例域，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。 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，因此本文采用对vTPM实例 域采用静态度量方式。VM Builder完成对vTPM实例域的度量后，把控制权交给vTPM实例域，vTPM实例域获得控制	) 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之后加载的第一个应用进程。这种实

指　标

疑似剽窃文字表述

---

1. 其本质是基于良好的数学逻辑方法来描述软件系统拥有安全属性的一直技术。不同的形式化方法的数学基础是不同的，有的以集合论和一阶谓词演算为基础，有的则以时态逻辑为基础。
2. 对于TVP的主机M，根据其类型进一步细化为M:={m, vm}，其中，m:={VMM,
3. vm:={vm1, … , vmn}，表示虚拟化平台上层的用户虚拟机vm 集合。
4. 需要保证可信平台能够基于信任根，通过逐级的信任传递，对可信虚拟化平台环境进行构建。
5. 为了确保这种信任传递的正确性，需要对 TVP-QT信任链进行验证，证明在程序控制权传递过程中，各个进程的确能够按照预期执行，而且能够对外证明上述属性。
6. 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，因此本文采用对vTPM实例

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. [] GILLES B, GUSTAVO B, JUAN D C, et al. Formally verifying isolation and availability in an idealized model of virtualization[A]. Proc of the 17th International Conference on Formal Methods[C]. Berlin, Springer, 2011.231-245..
4. [56] 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..
5. [57] 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..

4. 6_齐能_具有瀑布特征的可信虚拟平台信任链模型_第4部分

总字数：11850

相似文献列表　文字复制比：21.1%(2506)　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	17.7%（2097） 是否引证：否
2	王小亮_105796_面向云计算环境的信任链研究 王小亮 -《学术论文联合比对库》- 2013-01-14	1.2%（137） 是否引证：否
3	BH20099252103_刘彬 刘彬 -《学术论文联合比对库》- 2012-12-25	1.2%（137） 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	1.1%（136） 是否引证：否
5	面向云计算环境的信任链研究 王小亮(导师：王春露) -《北京邮电大学硕士论文》- 2012-12-17	1.1%（127） 是否引证：否
6	1852131086 -《学术论文联合比对库》- 2014-04-27	1.0%（117） 是否引证：否
7	虚拟可信平台及数据泄漏防护研究 王星魁(导师：彭新光) -《太原理工大学博士论文》- 2016-09-01	0.7%（79） 是否引证：否

	原文内容	相似内容来源
1	此处有 80 字相似 次的构建模块、功能组件或文件进行哈希值存储。按照TCG标准，采用迭代计算Hash值的方法对PCR进行扩	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.在物理机器通电以后，如果没有针对 TPM 的物理攻击，那么就通过扩展操作来改变 PCR 的内容。即将

	展操作，将PCR的 现值与新值相连，计算Hash值作为新的完整性度量值存储到PCR中，描述如下： New PCRi=Hash(Old PCRi||New Value)， 其中， Hash 函数选用SHA-1，||表示连接符号。在实验中成功运行虚拟机UbuntuTest1。按照下表的顺序对PCR进行	PCR 的现值与新值连接，再计算 Hash 值并作为新的完整性度量值存储到 PCR 中：New PCRi=Hash（Old PCRi ||New Value）其中：Old PCRi是扩展之前的PCR值；New PCRi是扩展之后的PCR值；New Value是完整性度量值； Has
2	此处有 48 字相似 img等组件) PCR[15] VM中的应用程序 按照TVP-QT信任链顺序存储的信任链信息结果如图3.7所示。 只要程序或者文件不发生任何变化，即使反复执行或者查看，信任链中不会重复记录程序或者文件的哈希值，哈希值也不会发生变化。而一旦程序或者文件内容发生变化，下次执行该程序或者打开该文件时，就不可避免的在信任链中留下痕迹，用	面向云计算环境的信任链研究_王小亮 -《北京邮电大学硕士论文》- 2012-12-17（是否引证：否） 1.的内容已经被篡改。如果不对hellow做任何修改，反复运行或者查看其内容，信任链中都不会有更多关于helloword的记录。实验证明只要程序或者文件不发生任何变化，即使反复执行或者查看，信任链中也不会重复记录程序或者文件的哈希值。因此信任链不会随着平台长时间运行而无限增大。而一旦程序或者文件内容发生变化，下次执行该 BH20099252103_刘彬_刘彬 -《学术论文联合比对库》- 2012-12-25（是否引证：否） 1.llow 做任何修改，反复运行或者查看其内容，信任链中都不会有更多关于 helloword 的记录。实验证明只要程序或者文件不发生任何变化，即使反复执行或者查看，信任链中也不会重复记录程序或者文件的哈希值。因此信任链不会随着平台长时间运行而无限增大。而一旦程序或者文件内容发生变化，下次执行该程序或者打开该文件时， 王小亮_105796_面向云计算环境的信任链研究_王小亮 -《学术论文联合比对库》- 2013-01-14（是否引证：否） 1.llow 做任何修改，反复运行或者查看其内容，信任链中都不会有更多关于 helloword 的记录。实验证明只要程序或者文件不发生任何变化，即使反复执行或者查看，信任链中也不会重复记录程序或者文件的哈希值。因此信任链不会随着平台长时间运行而无限增大。而一旦程序或者文件内容发生变化，下次执行该程序或者打开该文件时， 1852131086 -《学术论文联合比对库》- 2014-04-27（是否引证：否） 1.helloworld程序后重新进行编译。结果如图6-4所示。图6-4 某程序发生变化时信任链显示情况实验证明只要程序或者文件不发生任何变化,即使反复执行或者查看,信任链中也不会重复记录程序或者文件的哈希值。因此信任链不会随着平台长时间运行而无限增大。而一旦程序或者文件内容发生变化,下次执行该程序或者打开该文件时,就不可避免的
3	此处有 90 字相似 只要程序或者文件不发生任何变化，即使反复执行或者查看，信任链中不会重复记录程序或者文件的哈希值，哈希值也不会发生变化。而 一旦程序或者文件内容发生变化，下次执行该程序或者打开该文件时，就不可避免的在信任链中留下痕迹，用	BH20099252103_刘彬_刘彬 -《学术论文联合比对库》- 2012-12-25（是否引证：否） 1.反复执行或者查看，信任链中也不会重复记录程序或者文件的哈希值。因此信任链不会随着平台长时间运行而无限增大。而一旦程序或者文件内容发生变化，下次执行该程序或者打开该文件时，就不可避免的在信任链中留下痕迹，可信第三方就可以据此判断平台状态是否

	户虚拟机使用者就可以据此判断平台状态是否可信。 图3.7 信任链PCR信息 本文 在实验中人为的对虚拟机启动的配置文件添加一些无用的注释，实验结果如下，由图看出，针对于可信衔接点的PCR信息已经发生改变	可信。6.3.2 信任链的验证本文主要使用 Logtamper v1.0 和 Mood-nt 2.3 两个恶意程序来检验 T-YUN验证物理节点可信 王小亮_105796_面向云计算环境的信任链研究_王小亮 -《学术论文联合比对库》- 2013-01-14（是否引证：否） 1.反复执行或者查看，信任链中也不会重复记录程序或者文件的哈希值。因此信任链不会随着平台长时间运行而无限增大。而一旦程序或者文件内容发生变化，下次执行该程序或者打开该文件时，就不可避免的在信任链中留下痕迹，可信第三方就可以据此判断平台状态是否可信。6.3.2 信任链的验证本文主要使用Logtamper 1.0和Mood-nt 2.3两个恶意程序来检验信任链验证机制的有效性。顾名思义，Lo 面向云计算环境的信任链研究_王小亮 -《北京邮电大学硕士论文》- 2012-12-17（是否引证：否） 1.或者文件不发生任何变化，即使反复执行或者查看，信任链中也不会重复记录程序或者文件的哈希值。因此信任链不会随着平台长时间运行而无限增大。而一旦程序或者文件内容发生变化，下次执行该程序或者打开该文件时，就不可避免的在信任链中留下痕迹，可信第三方就可以据此判断平台状态是否可信。6.3.2信任链的验证本文主要使用Logtamper 1.0和Mood-nt 2.3两个恶意程序来检 1852131086 -《学术论文联合比对库》- 2014-04-27（是否引证：否） 1.何变化,即使反复执行或者查看,信任链中也不会重复记录程序或者文件的哈希值。因此信任链不会随着平台长时间运行而无限增大。而一旦程序或者文件内容发生变化,下次执行该程序或者打开该文件时,就不可避免的在信任链中留下痕迹,可信第三方就可以据此判断平台状态是否可信。2.1.20 5.3.2 信任链验证本文主要使用Logtamper 1.0和Mood-nt 2.3两个恶意程序来检
4	此处有 42 字相似 大学，感谢为大学建设付出努力的领导们。大学的图书馆资源、校园环境、实验室、研究生宿舍，丰富多彩的学术活动、知识讲座，都为 我的科研和生活增添了独特的色彩，使我能够把更多的学习精力放在科研上。 感谢在研究生 期间对我进行过指导的计算机科学学院的老师们，感谢李晓宁老师、黎静辅导员，感谢在研究生期间的任课老师，是你们的用心指导和辛	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.大学，我在这里完成了我的研究生生涯，学校为我们提供了良好的学习环境和资源，图书馆，教室，实验室，食堂，宿舍构成了我的每天的生活轨迹，使我能够心无旁骛的沉浸在科研活动中。感谢在研究生阶段教导过我的老师们，感谢辅导员对我帮助，感谢任课老师教给了我实用的专业技能，你们的辛勤付出使我能更加从容地面对
5	此处有 34 字相似 文同舟共济的向未来前行。 感谢在百忙中抽出时间对我的论文进行审阅的各位老师。 再此感谢所有人，在以后的生活中，我会用 更多的时间去帮助其他需要帮助的人。 硕士期间科研成果和项目	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.培育基金的支持，在此表示感谢。最后，再次感谢所有的人，在今后的人生道路上，我会继续努力，用自己的能力帮助更多需要帮助的人。50就读硕士期间发表的论文和参与的科研项目发表学术论文情况：[1] 王闪,谭良. Web 大数据环境下相似重复数据清理[J].

	论文 录用情况： [1]. 齐能,谭良. 具有瀑布特征的可信虚拟平台信任链模型[J]. 计算机应用, 2018,38(2)	
6	此处有 60 字相似 (2): 327-336. [2]. 齐能,谭良. 一种具有瀑布特征的可信虚拟平台信任链模型. CTCIS2017 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]. 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.]等。下面本文分别	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.申请专利情况：[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.
7	此处有 37 字相似 系统逻辑（Logic of Secure System, LS2）”对TVP-QT信任链模型进行形式化分析。 4.1 基本假定 在对TVP-QT信任链属性进行形式化分析前，本文假定以下条件是 成立的： （1）TVP 中各个层次的系统镜像文件（包括主机m以及用户虚拟机层次上的各个用户虚拟机VM）的完整性未受破坏	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.,必须对上述扩展的LS2证明系统(规则)提供严格的正确性、有效性证明,其详细证明过程参见附录。4 TVP信任链分析4.1基本假定在对TVP信任链属性分析之前本文假定以下条件是满足的:1)TVP中涉及到的所有系统镜像文件(包括主机m及各个用户虚拟机)的完整性未受破坏,且用户虚拟机已预先植入所需的可信度量
8	此处有 196 字相似 4.1 基本假定 在对TVP-QT信任链属性进行形式化分析前，本文假定以下条件是成立的： （1）TVP 中各个层次的 系统镜像文件（包括主机m以及用户虚拟机层次上的各个用户虚拟机VM）的完整性未受破坏，并且各个用户虚拟机都预先植入所需要的可信度量和证明代理功能组件；（2）主机m支持动态加载动态度量根 DRTM技术，能够为TJP和vTPM提供动态的可信运行环境；（3）vTPM的平台身份密钥（Attestation Identity Key，AIK）已得到可信第三方的认证并颁发证书，这里不考虑其具体实现方案； （4）远程验证方案基于 TCG 组织给出的完整性报告协议，且在远程挑战者 R 与本地 TVP 之间已经建立了安全信道[2	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.见附录。4 TVP信任链分析4.1基本假定在对TVP信任链属性分析之前本文假定以下条件是满足的:1)TVP中涉及到的所有系统镜像文件(包括主机m及各个用户虚拟机)的完整性未受破坏,且用户虚拟机已预先植入所需的可信度量及证明代理;2)主机m支持动态加载DRTM技术,能够为vRT提供动态的可信运行环境;3)vRT的平台身份密钥(AIK,attestation identity key)已得到可信第三方的认证并颁发证书,这里不考虑其具体实现方案(参见vTPM[2]及TrustVisor[11]等);4)远程验证方案基于TCG组织给出的完整性报告协议,且在远程挑战
9	此处有 127 字相似 testation Identity Key，AIK）已得到可信第三方的认证	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）

	并颁发证书，这里不考虑其具体实现方案；（4） 远程验证方案基于 TCG 组织给出的完整性报告协议，且在远程挑战者 R 与本地 TVP 之间已经建立了安全信道[26]。 从3.2的分析可知，本文对TVP-QT 信任链的信任属性分析验证主要包括3 部分： （1）m信任链构建的验证及该信任链的远程验证（含TJP）； （2）TJP动态度量验证及远程验证； （3）利用vTPM构建的vm信任链验证及远程证明； 在这3部	1.)已得到可信第三方的认证并颁发证书,这里不考虑其具体实现方案(参见vTPM[2]及TrustVisor[11]等);4)远程验证方案基于TCG组织给出的完整性报告协议,且在远程挑战者R与本地TVP之间已经建立了安全信道。根据定义1和定义2,本文对TVP信任链的信任属性分析验证主要包括2部分:本地信任链构建的验证及该信任链的远程验证,如图3所示。其中,对主机m和vRT(将其作为一个单独的软件组件扩展信任传递)的信任属性证明可参考Anupam Datta
10	此处有 115 字相似 her_APP(m) ≡ ... 图4.1 TVP-QT中 m 信任链传递 程序执行流程：m首先从CRTM启动执行， 它从主机内存地址m.bios_loc中读取BIOS的代码b，将其扩展到一个PCR中（其中，m.pcr.s表示该主机在这里存储所有相关度量值，且该主机的度量值存储于静态度量的PCR中），之后执行指令Jump b；然后CRTM将控制权 传递给m的BIOS，它从主机内存地址m.os_loader_loc中读取的OS_Loader代码o，将其扩展到一个PC	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. TVP中vm信任链传递程序执行流程:首先确保vRT的正确加载并运行;然后vRT将控制权传递给初始程序INIT(vm),它从虚拟机内存地址vm.bl_loc中读取Bootloader中的代码b,将其扩展到一个虚拟PCR中(其中,m.vpcr.vm表示该虚拟机在这里存储所有相关度量值,且该虚拟机的度量值存储于主机m而不是vm);之后执行指令Jump b将控制权交给Bootloader;Bootloader继续按序从内存vm.os_loc读取OS的代码o,将其扩展到m.vpcr.
11	此处有 87 字相似 m的BIOS，它从主机内存地址m.os_loader_loc 中读取的OS_Loader代码o，将其扩展到一个PCR中， 之后执行指令Jump o，将控制权交给OSLoader；OSLoader继续按序从内存m.vmm_loc读取VMM的代码v，将其扩展到m.pcr.s，然后转换控制权给VMM， VMM、Dom0 Kernel执行相似流程，直到可信衔接点TJP的加载。 4.2.2 本地可信属性描述 由上文描述的	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.虚拟PCR中(其中,m.vpcr.vm表示该虚拟机在这里存储所有相关度量值,且该虚拟机的度量值存储于主机m而不是vm);之后执行指令Jump b将控制权交给Bootloader;Bootloader继续按序从内存vm.os_loc读取OS的代码o,将其扩展到m.vpcr.vm,然后转换控制权给OS;OS执行相似的过程将控制权交给虚拟机的应用代码a。在此过程中,要求TVP的用户虚拟机必须在vRT成功加载之后启动,否则会
12	此处有 169 字相似 执行相似流程，直到可信衔接点TJP的加载。 4.2.2 本地可信属性描述 由上文描述的信任链传递所涉及的程序执行过程 可知，体现主机m信任链的是主机进行可信度量后的PCR值，它与执行程序之间存在着唯一确定的映射关系。因此，基于定义3.2及上述映射关系，可将m的本地信任传递属性归纳为：如果可信度量后的PCR中度量值序列是正确的值，那么在该虚拟机上信任链所加载的程序顺序就是正确的。即m的本地信任传递属性就是要求所有相应启动程序如BIOS、OSLoader、 VMM、Dom0 Kernel、vTPM Builder、vTPM-VM Binding、VM Builder等都能按确	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.h(m)动态加载机制确保其可信执行,即JDRTM成立[15]。2)本地可信属性描述及证明根据上述信任链传递中程序执行过程可知,最终体现vm信任链的是虚拟平台的vPCR值,它与执行程序之间存在唯一性、确定性映射。因此,基于定义2及上述映射关系,可将vm的本地信任传递属性归纳为:如果最终的vPCR中度量值序列是正确的值,那么在该虚拟机上信任链所加载的程序顺序就是正确的。即vm的本地信任传递属性就是要求所有相应启动程序如Bootloader、OS、APP等都能按确定的先后顺序加载。以扩展LS2将这种顺序形式化表示为SRTMMeasuredBoot(vm,)..

13	此处有 50 字相似 ader、VMM、Dom0 Kernel、vTPM Builder、vTPM-VM Binding、VM Builder 等都能按确定的先后顺序加载。以LS2将这种顺序形式化表示为 MeasuredBootSRTM(m, t)= (Reset(m,J)@tS)(Jump(J,BIOS(m)) @tb) (Jump(J,OSLoader(	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.上信任链所加载的程序顺序就是正确的。即vm的本地信任传递属性就是要求所有相应启动程序如Bootloader、OS、APP等都能按确定的先后顺序加载。以扩展LS2将这种顺序形式化表示为SRTMMeasuredBoot(vm,)....vm.()(Reset(vRT,)(,])(Reset(vm,)@)(Jump(,BL(vm)@))(Jump
14	此处有 55 字相似 , tvv))(┐Jump(J)on(tvv, tvvb)) (┐Jump(J)on(tvvb, to_app)) 上述公式表示：如果TVP的m基于信任链构建了本地信任环境，则其启动过程一定是从BIOS跳转到OSLoader， 从OSLoader到VMM，从VMM到Dom0_Kernel，然后Dom0_ Kernel到TJP，而在此期间不会有其他	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.t t t J t t t tl on t t J tJ t J tJ on t t J on t t tJ on t t)上述公式表示:如果TVP的vm基于信任链构建了本地信任环境,则其启动过程一定是从BL(Bootloader)跳转到OS,而在此期间不会有其他程序执行。这就需要证明上述程序启动序列与vPCR值之间的一一映射关系。基于前文的假
15	此处有 80 字相似 到OSLoader，从OSLoader到VMM，从VMM到Dom0_Kernel，然后Dom0_ Kernel到TJP， 而在此期间不会有其他程序执行。这就需要证明上述程序启动序列与PCR值之间的一一映射关系。基于前文的假定前提，要证明的信任链本地信任属性如下。 定理4.1 如果 m从CRTM启动运行，且与该m启动过程对应的PCR值为 seq(BIOS(m),OSLoader(m),VMM(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.上述公式表示:如果TVP的vm基于信任链构建了本地信任环境,则其启动过程一定是从BL(Bootloader)跳转到OS,而在此期间不会有其他程序执行。这就需要证明上述程序启动序列与vPCR值之间的一一映射关系。基于前文的假定前提,要证明的信任链本地信任属性如下。定理1如果vRT加载(即JDRTM)成功,而且与该vm启动过程对应的vPCR值为seq(INIT(vm),BL(vm),OS(vm
16	此处有 37 字相似 l(m), vTPM Builder(m), vTPM-VM Binding(m), VM Builder(m))， 那么该m的本地信任链传递过程就是唯一的、正确的，即确定地从BIOS(m)到 OSLoader(m)再VMM(m)、Dom0 Kernel(m)、vTPM Builder(m) 、 vTPM-VM	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)成功,而且与该vm启动过程对应的vPCR值为seq(INIT(vm),BL(vm),OS(vm),APP(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
17	此处有 47 字相似 nel(m),vTPM Builder(m), vTPM-VM Binding(m), VM Builder(m)) 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.pcr. s中，即： tS,t1,t2,t3,t4, t5,t6,J.(tSt1<t2<t3<t4 <t5 <t6<t) (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.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),BL(vm),OS(v

18	此处有 69 字相似 S(m))@t1)Reset(m,J)@tS (┐Reset(m)on(tS,t) (1) 接下对图4.1中信任链的 执行过程进行说明，最先执行的操作是以CRTM为起点启动m，即Reset(m,J)，然后m执行第一个信任程序BIOS(m)。利用LS2规则， 在某个时间tB，程序会跳转到b,且其他时间不会有程序跳转，内存位置（即PCR值）被该线程锁定，即有以下属性(2)成立。	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.vpcr≤1m)))@)(Reset(vm,)@)(Reset(vm)on(,])TTtJ tt t接下来考虑图4中程序执行过程,最先执行的操作是启动vm,即Reset(vm,J),然后vm利用vRT执行第一个信任程序INIT(vm)。利用图2中规则Resetvm,建立并证明程序INIT(vm)的不变量INIT(vm)b,eA t t:在某个时间tB,程序会跳转到b且在其他时间不会有
19	此处有 60 字相似 先执行的操作是以CRTM为起点启动m，即Reset(m,J)，然后m执行第一个信任程序BIOS(m)。利用LS2规则，在 某个时间tB，程序会跳转到b,且其他时间不会有程序跳转，内存位置（即PCR值）被该线程锁定，即有以下属性(2)成立。 (((Mem(m.pcr.s,seq(BIOS,b,o))@t') (< t'< t))((< < t) (Jump(	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.NIT(vm)。利用图2中规则Resetvm,建立并证明程序INIT(vm)的不变量INIT(vm)b,eA t t:在某个时间tB,程序会跳转到b且在其他时间不会有程序跳转,内存位置(即vPCR值)被该线程锁定。即有以下属性(1)成立 INIT(vm)(,)',,.(((Mem(m..vm,seq(,,))@')).((')(Jump(,)@)))(
20	此处有 41 字相似 间to、tv、td、tvb、tvv、tvmb、to_app，程序会跳转到o、v、d、vb、vv、vmb、o_app、,且 其他时间不会有程序跳转，相应的内存位置（即PCR值）被该线程锁定，即有属性(3)、 （4）、（5）、（6）、（7）、（8）、（9）成立，鉴于篇幅，这些属性略。 根据式（2）—（9）可知，如果前提条件满足	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.esetvm,建立并证明程序INIT(vm)的不变量INIT(vm)b,eA t t:在某个时间tB,程序会跳转到b且在其他时间不会有程序跳转,内存位置(即vPCR值)被该线程锁定。即有以下属性(1)成立 INIT(vm)(,)',,.(((Mem(m..vm,seq(,,))@')).((')(Jump(,)
21	此处有 35 字相似 锁定，即有属性(3)、（4）、（5）、（6）、（7）、（8）、（9）成立，鉴于篇幅，这些属性略。 根据式（2）—（9） 可知，如果前提条件满足，那么m上执行程序的顺序一定是从BIOS(m)到 OSLoader(m)再到VMM(m)、Dom0 Kernel(m)、TJP(m)。 (┐Reset(m,l)on (	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.a vpcrinit b o a t t t tt t t t J o tJ on t t≤(2)根据式(1)、式(2)可知,如果前提条件满足,那么vm上执行程序的顺序一定是从INIT(vm)到BL(vm)再到 OS(vm),,,.()(Reset(vm,)(,])(Reset(vm,)@)(Jump(,BL(vm
22	此处有 158 字相似)@ to_app) (┐Jump(J, VM Builder(m) on(tvmb, to_app)) (10) 定理4.1即得证。 虽然上述证明过程未显式地描述攻击者的存在，但已经蕴含着攻击场景。比如，在BIOS(m)之后跳转到o的过程中，由于o是从内存m.osloader_loc读取的，而该位置	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. T Bo B Ot t t J t t t tI on t t J tJ t J on t tJ t J on t t定理1得证。虽然上述证明过程未显式地描述攻击者的存在,但已经蕴含着攻击场景。比如,在INIT(vm)之后跳转到b的过程中,由于b是从内存vm.bl_loc读取的,而该位置可能在之前已被攻击者线程写入其他程序,但可信计算技术

	可能在之前已被攻击者线程写入其他程序，但可信计算技术提供的度量扩展机制使得能够推理只有得到正确的内存值时才能继续运行下一个程序。 后面的以此类推。 4.2.3 信任链远程验证 TVP-QT的m需要向外部挑战者证明自己所声称信任属性，即其信任链传递	提供的度量扩展机制使得能够推理只有得到正确的内存值时才能继续运行下一个程序。同样的,需要证明从b跳转到o的正确性。利用LS2提供的Resetvm规则和Jumpvm规则,证明TVP上本地信任链传递的
23	此处有 202 字相似 可信计算技术提供的度量扩展机制使得能够推理只有得到正确的内存值时才能继续运行下一个程序。后面的以此类推。 4.2.3 信任链远程验证 TVP-QT的m需要向外部挑战者证明自己所声称信任属性，即其信任链传递过程中所执行程序的确定序列，使外部挑战者相信它的确按上述信任链构建了可信执行环境，需要证明MeasuredBootSRTM(m,t)成立。 （1）远程验证程序执行 首先，根据 TCG 远程证明协议规范及在虚拟化平台中的实现，给出m 信任传递的远程验证过程中涉及到的程序，如图4.2所示。 TPMSRTM(m) ≡ w = read m.pcr.s; r = sign(PCR(s),w),AIK-1(m); send r 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.o的正确性。利用LS2提供的Resetvm规则和Jumpvm规则,证明TVP上本地信任链传递的唯一性、正确性成立。4.3信任链的远程验证TVP的vm需要向外部挑战者证明自己所声称信任属性,即其信任链传递过程中所执行程序的确定序列,使外部挑战者相信它的确按上述信任链构建了可信执行环境,需要证明MeasuredBootSRTM(vm,t)成立。1)远程验证程序执行首先,根据TCG远程证明协议规范及在虚拟化平台中的实现[16,17],给出vm信任传递的远程验证过程中涉及到的程序,如图5所示。SRTM1vmvmvRT(vm)read m..vm;sign((vm),),(vm);sendw vpcrr vPCR w A
24	此处有 111 字相似 M Binding(m), VM Builder(m)) 图4.2 TVP-QT中m信任传递的远程验证程序 首先，m 读取本地存储的PCR值，用自己的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PCR值是匹配的，则表明该m拥有所声称的可信属性，否则验证失败。在此过程 中远程验证者与m应是不同实体，以保证该验证过程的有效性。 这些前提条件形式化表示为 SRTM = {AIK(m),H	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。将这些前提条件形式
25	此处有 48 字相似 ，并用预期的度量值序列与收到的值进行对比，如果PCR值是匹配的，则表明该m拥有所声称的可信属性，否则验证失败。在此过程中 远程验证者与m应是不同实体，以保证该验证过程的有效性。 这些前提条件形式化表示为 SRTM	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.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。将这些前提条件形式化表示为SRTMDRTM SRTM{Honest((vm)),(TPM(m)(vm)),(vm)}ΓAIKvRT V

	= {AIK(m),Honest(AIK(m),{ TPM SRTM(m),TPM DRTM(m))}} (11) （	AIK 2)信任链属性的远程
26	此处有 111 字相似 {AIK(m),Honest(AIK(m),{ TPM SRTM(m),TPM DRTM(m))}} (11) （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 4.2 如果远程验证者确认m提供的度量值是唯一的、正确的，那么该m对应的PCR值一定是如下的确定序列 seq(BIOS(m), OSLoader(m),VMM(m),Dom0_Kernel(m),vTPM Builder(m), 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),BL(vm),OS(vm),APP(vm)),因为根据定理1可知,该序列表明该虚拟机的确执行了相应的信
27	此处有 100 字相似 el(m),vTPM Builder(m), vTPM-VM Binding(m), VM Builder(m))， 因为根据定理4.1可知，该序列表明m的确执行了相应的信任链传递过程。 形式化表示为： SRTM├ [Verifier(m)]t.(t<te) (Mem(m.pcr.s, seq(BIOS(m), OSLoader(m),VMM(m), Dom0_Kernel(m),vTPM Builder(m), vTPM-VM	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.的,那么该vm对应的PCR值一定是如下的确定序列 seq(INIT(vm),BL(vm),OS(vm),APP(vm)),因为根据定理1可知,该序列表明该虚拟机的确执行了相应的信任链传递过程。形式化表示为 ,SRTM[Verifier(vm)].()(Mem(..vm,seq(INIT(vm),BL(vm),OS(vm),APP(vm))@)tb teV eΓt t tm pcrt(3)SRTM
28	此处有 122 字相似 ctedSRTM(m)├ [Verifier(m)]t.(t<te) MeasureBootSRTM(m,t) (13) 这两个属性有递进关系，即如果属性(12)成立，则属性(13)可以利用定理1的结论直接证明。因此，下面对属性(12)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： [Verifier(m)]tf, e,I.(tf<te)= (m)Contain(e,SIGAIK(m)-1) {|PCR(s), seq(BIOS(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.cted(vm)[Verifier(vm)].()(vm,)tb teV eΓt t tMeasuredBoot 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 I t t I AIK(vm)1(vm)Contain(,{|()
29	此处有 34 字相似 VM Builder(m)))|})(Sent(I,e)@ tf) I.(Write(I,I,e)@ tf)) 根据图4.2中的远程验证程序，建立并证明以下程序不变量：对于程序前缀 QIS(CRTMSRTM(m))，有以下属性成立： [Q](I,e,t.(ttb,te]) Write(J,I,e)@	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.|})((Sent(,)@).(Write(,,)@))AIKS Se SIG PCR sI e t I I I e t根据图5中的远程验证程序,建立并证明以下程序不变量:对于程序前缀Q IS vRTS RTM vm,有以下属性成立。[],(,,.((,])Write(,,)@)(','.((('(,])Se

30	此处有 61 字相似 (Read(l,m.pcr.s,e'') @tR)e'=SIGAIK(m)-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读取了值e''，且e'是一个签名值。	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.vm,'')@)'{|(),''|}))R R RAIKe t t t I vpcr e te SIG 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

指　标

疑似剽窃文字表述

---

1. 只要程序或者文件不发生任何变化，即使反复执行或者查看，信任链中不会重复记录程序或者文件的哈希值，
2. 一旦程序或者文件内容发生变化，下次执行该程序或者打开该文件时，就不可避免的在信任链中留下痕迹，用户虚拟机使用者就可以据此判断平台状态是否可信。
   图3.7 信任链PCR信息
   本文
3. 我的科研和生活增添了独特的色彩，使我能够把更多的学习精力放在科研上。
   感谢在研究生
4. 可知，体现主机m信任链的是主机进行可信度量后的PCR值，它与执行程序之间存在着唯一确定的映射关系。因此，基于定义3.2及上述映射关系，可将m的本地信任传递属性归纳为：如果可信度量后的PCR中度量值序列是正确的值，那么在该虚拟机上信任链所加载的程序顺序就是正确的。即m的本地信任传递属性就是要求所有相应启动程序如BIOS、OSLoader、
5. 这就需要证明上述程序启动序列与PCR值之间的一一映射关系。基于前文的假定前提，要证明的信任链本地信任属性如下。
6. 虽然上述证明过程未显式地描述攻击者的存在，但已经蕴含着攻击场景。比如，在BIOS(m)之后跳转到o的过程中，由于o是从内存m.osloader_loc读取的，而该位置可能在之前已被攻击者线程写入其他程序，但可信计算技术提供的度量扩展机制使得能够推理只有得到正确的内存值时才能继续运行下一个程序。
7. 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PCR值是匹配的，则表明该m拥有所声称的可信属性，否则验证失败。在此过程

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.

5. 6_齐能_具有瀑布特征的可信虚拟平台信任链模型_第5部分

总字数：11544

相似文献列表　文字复制比：37.8%(4369)　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	12.4%（1436） 是否引证：否
2	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	12.4%（1426） 是否引证：否
3	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	11.3%（1299） 是否引证：是
4	罗东俊_200710102074_基于可信计算的云计算安全若干关键技术研究 罗东俊 -《学术论文联合比对库》- 2013-10-08	3.3%（378） 是否引证：否
5	云计算中信任链的动态性研究 朱洁(导师：林果园) -《中国矿业大学硕士论文》- 2017-05-01	2.2%（255） 是否引证：否
6	可信计算平台信任链理论与技术研究 司丽敏(导师：蔡勉) -《北京工业大学硕士论文》- 2011-06-01	2.1%（244） 是否引证：否
7	王红新-80211004-新兴电子商务环境下的柔性支付模型研究 王红新 -《学术论文联合比对库》- 2013-02-26	1.4%（162） 是否引证：否
8	可信系统保护模型研究与设计 邱罡(导师：周利华) -《西安电子科技大学博士论文》- 2010-09-01	1.4%（159） 是否引证：否

9	支持进程代码修改的非传递无干扰可信模型	1.0%（110）
	徐甫; -《计算机工程》- 2013-11-15	是否引证：否
10	信任链传递研究进展	0.9%（100）
	左双勇; -《桂林电子科技大学学报》- 2010-08-25	是否引证：否
11	基于云模型和信任链的信任评价模型研究	0.9%（100）
	陈建钧;张仕斌; -《计算机应用研究》- 2014-08-27 1	是否引证：否
12	无干扰可信模型及可信平台体系结构实现研究	0.6%（69）
	张兴(导师：沈昌祥) -《解放军信息工程大学博士论文》- 2009-04-20	是否引证：否
13	罗东俊_200710102074_基于可信计算的云计算安全若干关键技术研究	0.3%（31）
	罗东俊 -《学术论文联合比对库》- 2013-11-12	是否引证：否

	原文内容	相似内容来源
1	此处有 59 字相似 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(m)]tR, e,l.(tR<te)= (m) Contain(e,SIGAIK(m)-1){|PCR(s), seq(BIOS(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.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 l t t l AIK(vm)11(vm)(vm)Con
2	此处有 63 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), vTPM-VM	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
3	此处有 163 字相似 , vTPM Builder(m), vTPM-VM Binding(m), VM Builder(m))@tR) 即 定理4.2属性式(12)得证。利用属性式(12)结论及定义3.1，可直接证明属性式(13)成立。 根据上述证明可知，在TVP-QT信任链构建过程中，能够有条件地保持其信任属性，即构建信任链所需要执行的不同程序在跳转过程中，不会被其他恶意代码所控制或插入，从而不存在信任缺失的情况，且这种信任属性能够向远程验证者提供证明。 4.3 可信衔接点TJP的本地验证及远程证明 本节根据4.2对TVP-QT中的相关定义和说明，对可信衔接点TJP的动态	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.seq(INIT(vm),BL(vm),OS(vm),APP(vm))@)tb teV R R eRt t tpcrt即定理2属性式(3)得证。利用属性式(4)结论及定义1,可直接证明属性式(4)成立。根据上述证明可知,在TVP信任链构建过程中,能够有条件地保持其信任属性,即构建信任链所需要执行的不同程序在跳转过程中,不会被其他恶意代码所控制或插入,从而不存在信任缺失的情况,且这种信任属性能够向远程验证者提供证明。5实例系统分析与讨论上述分析验证过程是针对第2节提出的TVP抽象模型进行的,为了在实际系统中应用本文的分析方法,选择课题
4	此处有 40 字相似 。 4.3.1 本地程序执行 根据4.2节对TVP-QT中TJP信任属性TPTJP定义以及TPvRT中对TCTJP的	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.信任环境。图3 TVP的信任传递证明4.2信任链的本地验证1)本地程序执行根据2.2节中TVP用户虚拟机信任属性TPvm定义,其信任链本地执行过程中涉及到的程序如

	定义，其信任链本地执行过程中涉及到的程序如图4.3所示。 Latelaunch DTRM(vTPM-Builder)≡vtb=read m.vTPM-Builder_loc; Extend m.dp	图4所示。Latelaunch()vRT read m.;extend m..,vRT;Jump vRT;m SLBdpcr k...INIT(vm)read v
5	此处有 115 字相似 。将其表示为 Honest(TPMSRTM (m)TJPDRTM(m)TJPDRTM(m)vTPMSRTM/DRTM (vm))。 此外，TVP在启动m时，相应的线程K对必须能够对当前m对应的PCR值有锁控制，这种控制对潜在的攻击者也成立，表示为 ProtectedSRTM(m)=t,K.(Reset(m,K)@t)(IsLocked((m. pcr.s,m.pcr.d),K)@)t 由于TJP 的vTPM Builder被抽象为一个单独的应用程序（无论其实现	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.之后启动,否则会导致在vRT启动之前的vm无法使用该vRT,将其表示为DRTM SRTMHonest(TPM(m)vRT(vm))。此外,TVP在启动vm时,相应的线程J对必须能够对当前vm对应的虚拟PCR值有锁控制,这种控制对潜在的攻击者也成立,表示为 ProtectedSRTM(vm),.(Reset(vm,)@)(IsLocked(m..vm,)@)t J J tvpcr J t由于vRT被抽象为一个单独的软件程序(无论其实现形式是独立的轻量级可信执行环境
6	此处有 120 字相似 K)@t)(IsLocked((m.pcr.s,m.pcr.d),K)@)t 由于TJP 的vTPM Builder被 抽象为一个单独的应用程序（无论其实现形式是独立的轻量级可信执行环境或仅是提供可信功能的应用进程），利用Latelaunch(vTPM Builder)动态加载机制确保其可信执行，即KDRTM成立[27]。 4.3.2 本地可信属性描述 基于定义3.2及TJP度量后的PCR和其中的每个组件存在的唯一性、确定性映射关系，可将TJP的本地信任传递属性归纳为：如	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(vm),.(Reset(vm,)@)(IsLocked(m..vm,)@)t J J tvpcr J t由于vRT被抽象为一个单独的软件程序(无论其实现形式是独立的轻量级可信执行环境或仅是提供可信功能的应用进程),利用Latelaunch(m)动态加载机制确保其可信执行,即JDRTM成立[15]。2)本地可信属性描述及证明根据上述信任链传递中程序执行过程可知,最终体现vm信任链的是虚拟平台的vPCR值,它与执行程序之间存在唯一性、确定
7	此处有 102 字相似 27]。 4.3.2 本地可信属性描述 基于定义3.2及TJP度量后的PCR和其中的每个组件存在的唯一性、确定性映射 关系，可将TJP的本地信任传递属性归纳为：如果最终的PCR中度量值序列是正确的值，那么TJP信任链所加载的程序顺序就是正确的。即TJP的本地信任传递属性就是要求所有相应启动程序如vTPM Builder、 vTPM-VM Binding、VM Builder等都能按确定的先后顺序加载。以LS2将这种顺序形式化表示为 Mea	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.过程可知,最终体现vm信任链的是虚拟平台的vPCR值,它与执行程序之间存在唯一性、确定性映射。因此,基于定义2及上述映射关系,可将vm的本地信任传递属性归纳为:如果最终的vPCR中度量值序列是正确的值,那么在该虚拟机上信任链所加载的程序顺序就是正确的。即vm的本地信任传递属性就是要求所有相应启动程序如Bootloader、OS、APP等都能按确定的先后顺序加载。以扩展LS2将这种顺序形式化表示为 SRTMMeasuredBoot(vm,)..
8	此处有 43 字相似 本地信任传递属性就是要求所有相应启动程序如vTPM Builder、vTPM-VM Binding、VM Builder 等都能按确定的先后顺序加载。以LS2将这种顺序形式	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.上信任链所加载的程序顺序就是正确的。即vm的本地信任传递属性就是要求所有相应启动程序如

	化表示为 MeasuredBoot DRTM(TJP,t)= (Jump(K,vTPM Builder(TJP)))@tvtb) (Jump(K,vTP	Bootloader、OS、APP等都能按确定的先后顺序加载。以扩展LS2将这种顺序形式化表示为 SRTMMeasuredBoot(vm,)....vm.()(Reset(vRT,)(,])(Reset(vm,)@)(Jump(,BL(vm)@))(Jump
9	此处有 42 字相似 tvvb)) (┐Jump(K)on(tvvb,tvvmb))(┐Jump(K)on(tvvmb,tvtpmb)) 上述公式表示：如果TVP基于信任链构建TJP信任环境，则其启动过程一定是从vTPM Builder跳转到vTPM-VM Binding，然后到VM Builder，而在此期间不会有其他程序执行。这就需要证	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.t t t J t t t tl on t t J tJ t J tJ on t t J on t t J on t t)上述公式表示:如果TVP的vm基于信任链构建了本地信任环境,则其启动过程一定是从BL(Bootloader)跳转到OS,而在此期间不会有其他程序执行。这就需要证明上述程序启动序列与vPCR值之间的一一
10	此处有 115 字相似 信任环境，则其启动过程一定是从vTPM Builder跳转到vTPM-VM Binding，然后到VM Builder， 而在此期间不会有其他程序执行。这就需要证明上述程序启动序列与PCR值之间的一一映射关系。基于前文的假定前提，要证明的信任链本地信任属性如下。 定理4.3 如果TJP加载成功，且与该TJP加载过程对应的PCR值为seq(vTPM Builder(TJP),vTPM-VM Binding(TJP),VM Builder(TJP))，那么该TJP的本地	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.上述公式表示:如果TVP的vm基于信任链构建了本地信任环境,则其启动过程一定是从BL(Bootloader)跳转到OS,而在此期间不会有其他程序执行。这就需要证明上述程序启动序列与vPCR值之间的一一映射关系。基于前文的假定前提,要证明的信任链本地信任属性如下。定理1如果vRT加载(即JDRTM)成功,而且与该vm启动过程对应的vPCR值为 seq(INIT(vm),BL(vm),OS(vm),APP(vm)),那么该vm的本地信任链传递过程就是唯一的、正确的,即
11	此处有 36 字相似 seq(vTPM Builder(TJP),vTPM-VM Binding(TJP),VM Builder(TJP))， 那么该TJP的本地信任链传递过程就是唯一的、正确的，即确定地从vTPM Builder(TJP)到vTPM-VM Binding(TJP)再到VM Builder(TJP)。该信任属性形式化表	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.M)成功,而且与该vm启动过程对应的vPCR值为seq(INIT(vm),BL(vm),OS(vm),APP(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)
12	此处有 179 字相似 t) 证明过程类似m的信任链本地可信属性的证明，在此不再叙述。 4.3.3 信任链远程验证 TVP-QT的TJP 需要向外部挑战者证明自己所声称的信任属性，即其信任链传递过程中所执行程序的确定序列，使外部挑战者相信它的确按上述信任链构建了可信执行环境，需要证明MeasuredBootDRTM(TJP,t)成立。 （1）远程验证程序执行 首先，根据 TCG 远程证明协议规范及在虚拟化平台中的实现，给出TJP 信任传递的远程验证过程中涉及到的程序，如图4.4所示。 TPMDRTM(TJP) ≡ w = read m.pcr.d;	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.Resetvm规则和Jumpvm规则,证明TVP上本地信任链传递的唯一性、正确性成立。4.3信任链的远程验证 TVP的vm需要向外部挑战者证明自己所声称信任属性,即其信任链传递过程中所执行程序的确定序列,使外部挑战者相信它的确按上述信任链构建了可信执行环境,需要证明MeasuredBootSRTM(vm,t)成立。1)远程验证程序执行首先,根据TCG远程证明协议规范及在虚拟化平台中的实现[16,17],给出vm信任传递的远程验证过程中涉及到的程序,如图5所示。SRTM1vmvmvRT(vm)read m..vm;sign((vm),),(vm);sendw vpcrr vPCR

	r = sign(PCR(s),w),AIK-1(m	
13	此处有 109 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。在此过程 中远程验证者与TJP所属的主机m应是不同实体，以保证该验证过程的有效性。 这些前提条件形式化表示为 DRTM = {	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。将这些前提条件形式
14	此处有 66 字相似 ，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。在此过程中 远程验证者与TJP所属的主机m应是不同实体，以保证该验证过程的有效性。 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 根据远程证明协议执行流程，给出以下信任传递属性的远程证	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.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。将这些前提条件形式化表示为SRTMDRTM 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
15	此处有 110 字相似 证过程的有效性。 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 4.4如果远程验证者确认TJP提供的度量值是唯一的、正确的，那么该TJP对应的PCR值一定是如下的确定序列seq(vTPM Builder(TJP),vTPM-VM Binding(TJP),VM Builder(TJP))，因为根据定理4.3	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（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),BL(vm),OS(vm),APP(vm)),因为根据定理1可知,该序列表明该虚拟机的确执行了相应的信
16	此处有 84 字相似 seq(vTPM Builder(TJP),vTPM-VM Binding(TJP),VM Builder(TJP))， 因为根据定理4.3可知，该序列表明该虚拟机的确执行了相应的信任链传递过程。 形式化表示为：	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.的,那么该vm对应的PCR值一定是如下的确定序列seq(INIT(vm),BL(vm),OS(vm),APP(vm)),因为根据定理1可知,该序列表明该虚拟机的确执行了相应的信任链传递过程。形式化表示为

	DRTM├ [Verifier(m)]t.(t<te) (Mem(m. pcr.d,seq(vTPM Builder(TJP), vTPM-VMBinding(TJP),VM Builder	,SRTM[Verifier(vm)].()(Mem(..vm,seq(INIT(vm),BL(vm) ,OS(vm),APP(vm))@)tb teV eΓt t tm pcrt
17	此处有 46 字相似 形式化分析。首先，介绍了主机m信任链构建本地执行的形式化表示，从程序执行的角度证明了主机m信任链模型的有效性；并且介绍了 本地可信属性，如果PCR中度量值序列是正确的值，那么主机m信任链所加载的程序顺序就是正确的， 并对其进行证明；然后结合远程验证，证明了从外部实体的角度上看，主机m的执行顺序也是可以信任的。然后用相同方法介绍了可信衔	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.现vm信任链的是虚拟平台的vPCR值,它与执行程序之间存在唯一性、确定性映射。因此,基于定义2及上述映射关系,可将vm的本地信任传递属性归纳为:如果最终的vPCR中度量值序列是正确的值,那么在该虚拟机上信任链所加载的程序顺序就是正确的。即vm的本地信任传递属性就是要求所有相应启动程序如Bootloader、OS、APP等都能按确定的先后顺序加载。以扩展L
18	此处有 64 字相似 中，给出无干扰的基本定义如下。 定义5.1 系统M由如下要素构成： （1）一个包含唯一初始状态的状态集。约定使用等表示系统状态； （2）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； （3）一个由系统中所有发出原子动作的 动作主体集，每一个主体可能发出不同的动作，相同的动作也可能由不同的主体发出。即每一个属于中的动作都有一个包含于中的主体集	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：否） 1.gacy/SP/nistspecialpublication800-146.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 ，
19	此处有 173 字相似 主体集，每一个主体可能发出不同的动作，相同的动作也可能由不同的主体发出。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； （5）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； （6）每一个原子动作以及原子动作的主体都有自身所属的并且不可再分的Min安全域，这些安全域构成的集合称为Min安全域集； 安全域中的主体向系统发出操作动作与系统进行交互，并且能够观察到相应的结果。安全域的划分可以限制系统中的信息流动。并且根据	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：否） 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
20	此处有 53 字相似 每一个原子动作以及原子动作的主体都有自身所属的并且不可再分的Min安全域，这些安全域构成的集合称为Min安全域集；安全域 中的主体向系统发出操作动作与系统进行交互，并且能	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.s0∈S.O为系统输出集合.A为系统操作动作集合,指系统自身发出的控制动作以及输入性质的动作.D为系统隔离域集合,隔离域中的主体向系统发出操作动作与系统进行交互,并且能够观察到相应的结果.隔离域的划分可以

	够观察到相应的结果。安全域的划分可以限制系统中的信息流动。 并且根据云计算环境运行机制，安全域集的某一子集也可能单独成为运行的一个组合安全域，这些由子集组成的组合安全域称为，且中任	限制系统中的信息流动.单步状态转换函数step:S×A→S,step(s,a)表示系统发生了内部操作a之后的状态.输出函数output:S×A 可信计算平台信任链理论与技术研究 司丽敏 -《北京工业大学硕士论文》- 2011-06-01（是否引证：否） 1. A 为系统操作动作集合，指系统自身发出的控制动作以及输入性质的动作 。D 为系统隔离域集合，隔离域中的主体向系统发出操作动作与系统进行交互，并且能够观察到相应的结果。隔离域的划分可以限制系统中的信息流动。 O 为系统输出集合。 单步状态转换函数 step:S ×A →S ，step (s , a 云计算中信任链的动态性研究 朱洁 -《中国矿业大学硕士论文》- 2017-05-01（是否引证：否） 1.其中：（1）D 为系统隔离域集合，其中元素记为 Dom N，代表某一隔离域，在Xen 中即为虚拟机，隔离域中的主体向系统发出操作动作与系统进行交互，并且能够观察到相应的结果，通过隔离域的概念限制系统中的信息流。（2）S 系统的状态集合，表示为1 2{s ,s ,(43)}。某一时刻的系统状态可以用一组客体对象及其取值来表示 支持进程代码修改的非传递无干扰可信模型 徐甫; -《计算机工程》- 2013-11-15（是否引证：否） 1.为系统输出集合;A为系统操作动作集合,指系统自身发出的控制动作以及系统中运行着的进程发出的动作;P为系统进程集合,进程向系统发出操作动作与系统进行交互,并且能够观察到相应的结果。进程间的干扰关系由系统策略决定。单步状态转换函数step:S A S。t step(s,a)表示发生操作动作a后,系统状
21	此处有 105 字相似 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） 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； （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	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：否） 1.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 ：
22	此处有 52 字相似 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	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：否） 1.，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

	动作所观察到的行为执行结果。 （12）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 ： 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	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式做过多探讨。这
23	此处有 111 字相似 定义为行为，也就是原子动作的连接序列。本文遵从原有的无干扰理论，对系统进行描述。 定义5 .2 系统视图。 系统视图 对应于实际机器M，其关注于存储单元(内外存单元、芯片存储单元等)及其取值，以及可观察存储单元、可修改存储单元等内涵。 （1）存储单元集。机器的每一个存储单元都有一个名字。所有存储单元名字的集合构成存储单元集，又叫做名字 集。 （2）系统视图值集。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	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：否） 1.定义 2 是完备的。接下来，给出结构化机器的定义，以便与实际的云系统（机器）结合起来。定义 3. 结构化机器。结构化机器对应于实际机器 M，其关注于存储单元(内外存单元、芯片存储单元等)及其取值，以及可观察存储单元、可修改存储单元等内涵。（1）存储单元集 。机器的每一个存储单元都有一个名字。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
24	此处有 81 字相似 内涵。 （1）存储单元集。机器的每一个存储单元都有一个名字。所有存储单元名字的集合构成存储单元集，又叫做名字集。 （2）系统视图值集。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）系统视图内容函数。 定义5.3 域视图。 域视图对应于M中的安全域，是M视图的子集。 对应于系统状态等相关内容函数，域视图有以下表示：	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：否） 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
25	此处有 151 字相似 图。 域视图对应于M中的安全域，是M视图的子集。 对应于系统状态等相关内容函数，域视图有以下表示： （1）域视图 值集。安全域中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域视图内容函数计算。所有取值的集合构成值集。 （2）域视图内容函数。 （3）域视图观察函数和域视图修改函数。观察函数和	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：否） 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

	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5.4 主体视图。 （1）在整个系统M中，域中有很多可以发出动作的主体，即 。 亦有。 仅次于安全域的单位为动作主体，	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
26	此处有 94 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。具体的取值可以由下面的主体视图内容函数计算。 （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 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	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：否） 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 。观察函数和修改函数分别给出了特定的安全域 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
27	此处有 72 字相似 可以由下面的主体视图内容函数计算。 （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 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：。 在系统视图上：。 并且由可得域视图的输出一致性： 。 （2）（弱）单步一致性： 对于传递安全策略，需满足单步一	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：否） 1.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
28	此处有 195 字相似 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：。 在系统视图上：。 并且由可得域视图的 输出一致性： 。	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：否） 1.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。

	（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“单步一致性”。注意：本文中遵从Rushby的符号表达，约定使用表达蕴含关系。 定义5.6 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	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“单步一致性”。注意：本文中遵从文献[37]的符号表达，约定使用 表达蕴含关系。定义5. 引用监视器假设 RMA(ReferenceMonitor Assumption)。引用监视器对
29	此处有 46 字相似 干扰关系之外，还要考虑间接干扰关系上的“单步一致性”。注意：本文中遵从Rushby的符号表达，约定使用表达蕴含关系。 定义5.6 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1当中的干扰关系称作是“直接干扰关系”，则可以定义“间接干扰关系”如下:	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：否） 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 当中的干扰关系 称作是“直接干扰关系
30	此处有 164 字相似 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1当中的干扰关系称作是“直接干扰关系”，则可以定义“间接干扰关系”如下: 定义5.7 干扰源集。 干扰源集的递归定义如下: ，且 ，且。其中，。 干扰源集的含义是:抽取所有对安全域有直接或间接干扰关系的安全域形成集合。 定义5.8 弱预期函数。 ，且 。 其中，， 。 弱预期函数的含义是，“将所有 对安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。	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：否） 1.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 当中的干扰关系 称作是“直接干扰关系”，则可以定义“间接干扰关系” 如下:定义 7. 干扰源集 。干扰源集的递归定义如下:，且。其中，，。干扰源集的含义是:抽取所有对安全域 有直接或间接干扰关系的安全域形成集合。定义 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
31	此处有 91 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-

	集合。 定义5.8 弱预期函数。 ，且 。 其中，， 。 弱预期函数的含义是，“将所有对安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5.9 域集等价关系:。 并且Rushby定义了系统满足非传递性无干扰策略的判定定理。 定理5.1 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的～	28 12:54（是否引证：否） 1.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 非传递无干扰行为可信性判定等式与判定定理定义 11.非传递安全策略
32	此处有 103 字相似 干扰安全策略控制下的预期行为。 定义5.9 域集等价关系:。 并且Rushby定义了系统满足非传递性无干扰策略的判定 定理。 定理5.1 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。 5.2 TVP-QT信任链传递形式化描述 本文基于扩展后的无干扰理论，对TVP-QT信任链模型进行形式化描述。由于扩展	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.在无干扰模型中,干扰关系分为传递性和非传递性.传递的无干扰模型给出了系统M对由关系~>表达的信息流策略安全的条件,一般表 可信计算平台信任链理论与技术研究 司丽敏 -《北京工业大学硕士论文》- 2011-06-01（是否引证：否） 1.出动作之前状态的系统视图。 基于上述定义，文献[32]给出了下面的展开定理（unwinding）。 定理 4-1 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。 在无干扰模型中，干扰关系分为传递性和非传递性。传递的无干扰模型给出了系统M 对由关系~? 表达的信 云计算中信任链的动态性研究 朱洁 -《中国矿业大学硕士论文》- 2017-05-01（是否引证：否） 1.,α)，则称 s 是系统可达状态。当且仅当系统的操作序列α 满足无干扰完整性时，系统状态s是可达的可信状态。定理 3.1 系统满足非传递性无干扰完整性的判定定理设 NC 是一个视图隔离的云节点，有一个具有非传递性的 (25)? 策略，并且 NC满足：输出一致性、弱单步一致性和局部干扰性，则 NC 满足非传递性无干扰策略[45]。输出一致性：若对于系统中任意的域 u∈U ，状态集合 S 中存在一个等价关系u~ ，该等价关系满足如下 支持进程代码修改的非传递无干扰可信模型 徐甫; -《计算机工程》- 2013-11-15（是否引证：否） 1.,)(,)psources pstep s a t(8)由式(5)及归纳假设,可得结论(2)。得证。定理2(进程运行可信定理)设M是一个视图

		隔离的系统,具有非传递性的~和~策略,并且M满足输出一致性、动态弱单步一致性、静态弱单步一致性、局部干扰性和干扰互斥性,则M中运行的所有进程是运行可信的。证明:令0s t s,由引理3可得:p P:
33	此处有 38 字相似 为可信虚拟平台的可信度量根：即图3.1中TPM下的CRTM。 按照组合安全域的信任链传递方式，可以表示为以下公式： 基于可信计算技术的装载前度量技术实现的可信链可以这样形式化地描述： ； 表示如果由安全域通过摘要运算获得的摘要值与预期值相等,则安全域信任组件,信任关系将由传递至系统控制权也转移到其中dige	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.信度量根核心CRTM,表示信任链由CRTM开始,注意AiAk不一定为空,这是由计算平台组件之间复杂的依赖关系所决定的.基于可信计算技术的装载前度量技术实现的可信链可以这样形式化地描述:digest(Ai,Ak)=expect(Ak)Ai→Ak.如果由组件Ai通过摘要运算获得的Ak摘要值与预期值expec
34	此处有 110 字相似 域的信任链传递方式，可以表示为以下公式： 基于可信计算技术的装载前度量技术实现的可信链可以这样形式化地描述： ； 表示如果由安全域通过摘要运算获得的摘要值与预期值相等,则安全域信任组件,信任关系将由传递至系统控制权也转移到其中digest(A,B)表示安全域A对安全域B进行摘要运算的结果，expect(A)表示组件A的完整性预期值 ， 表示控制权从A转移到B。 同理对应组合域有： 。 5.3 扩展无干扰信任传递判定定理 单纯的通过完整性验证实现的	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.信计算技术的装载前度量技术实现的可信链可以这样形式化地描述:digest(Ai,Ak)=expect(Ak)Ai→Ak.如果由组件Ai通过摘要运算获得的Ak摘要值与预期值expect(Ak)相等,则组件Ai信任组件Ak,信任关系将由Ai传递至Ak,系统控制权也转移到Ak.其中digest(A,B)表示组件A对组件B进行摘要运算的结果,expect(A)表示组件A的完整性预期值.下面论述a,b,c∈S,如果干扰关系~>是传递性的,则信任链不成立.若Ai→Ak,a,b∈Ai,且c∈Ak,则由a~>b 罗东俊_200710102074_基于可信计算的云计算安全若干关键技术研究 罗东俊 -《学术论文联合比对库》- 2013-10-08（是否引证：否） 1.TM开始。注意不一定为空，这是由系统组件之间复杂的依赖关系所决定的。于是，TCG信任链构建方法可表示为：上式表示如果组件通过摘要算法获得组件的摘要值与预期值相等，则组件信任组件，系统控制权也转移到。但这种方法构建的信任链存在的问题是，对，如果干扰关系是传递性的，则信任链不成立。下面进行论述。设，，，且，则：
35	此处有 298 字相似 表示组件A的完整性预期值，表示控制权从A转移到B。 同理对应组合域有： 。 5.3 扩展无干扰信任传递判定定理 单纯的通过完整性验证实现的信任链传递是否有效无法进行验证。只有当系统具有特定的安全机制，满足一定的安全策略，组成系统的各安全域之间的信息流动受到一定安全策略限制，使得组件的运行不受干扰，这时，用完整性度量方法所建立的信任链才是有效的。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。信任	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.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否有效无法进行验证.只有当系统具有特定的安全机制,满足一定的安全策略,组成系统的各安全域之间的信息流动受到一定安全策略限制,使得组件的运行不受干扰,这时,用完整性度量方法所建立的信任链才是有效的.进一步用图3表示非传递无干扰关系,其中粗箭头连线表示信任传递关系,细箭头连线表示干扰关系.可以看出,信任链有两条,分别是

链传递模型关键之处是验证系统中是否满足非传递无干扰关系，但从非传递无干扰关系的定义出发很难进行验证，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。

下面本文分别从系统、安全域（和）、动作主体三个角度对本文提出的信任链模型应该满足的安全策略进行描述和分析验证。其中，从系

2.ub~>c a/~>c,则系统将不存在非预期的干扰,称满足以上关系的D×D上二元关系为非传递无干扰关系,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否有效无法进

3.运行时若满足非传递无干扰关系,则信任链能够建立,信任关系能够传递,达到平台可信目标.4.2无干扰信任传递判定定理上述信任链传递模型关键之处是验证系统中是否满足非传递无干扰关系,但从非传递无干扰关系的定义出发很难进行验证,于是,基于定理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

王红新-80211004-新兴电子商务环境下的柔性支付模型研究_王红新-《学术论文联合比对库》- 2013-02-26（是否引证：否）

1.性及运行时的动态性[133]。文[174]围绕满足什么条件时，信任链的建立和传递才是有效的这一问题开展讨论，指出：只有当系统本身满足一定的安全策略时，组成系统的各安全域之间的信息流动受到一定安全策略限制，使得组件的运行不受干扰，达到可信目标，这样，用完整性度量方法所建立的信任链才是有效的。④信任传递过程中线下信任与线上信任的关联提倡实名制的SNS网络所建立起来的社区有向真实世界回归的趋势，在虚拟社区内，物理世界

可信系统保护模型研究与设计_邱罡-《西安电子科技大学博士论文》- 2010-09-01（是否引证：否）

1.行可信;否则安全域之间可能会产生非预期的信息流动，即使通过了信任链的度量，也不能达到系统运行可信的目标。只有当系统具有特定的安全机制，满足一定的安全策略，组成系统的各安全域之间的信息流动受到一定安全策略限制，使得组件的运行不受干扰，这时，用完整性度量方法所建立的信任链才是有效的。Bibal98]模型是实现了多级安全(MLS)思想的完整性模型。它规定在任何情况下不可信的输入都是与可信

罗东俊_200710102074_基于可信计算的云计算安全若干关键技术研究_罗东俊-《学术论文联合比对库》- 2013-10-08（是否引证：否）

1.一般表示为，如果，，则。非传递的无干扰模型给出了系统对由无干扰关系表达的信息流策略安全的条件，一般表示为，如果，，但。非传递的无干扰模型描述了一种隔离性要求比较严格的通道控制安全策略，它要求安全域之间只能有直接干扰关系，而不能存在间接造成的干扰关系。本节给出非传递无干扰策略下系统行为可信性判定方法。

		2.息从流向，组件的输出必然受到影响，原有关系被破坏。这时尽管有，但非预期干扰导致。而如果干扰关系是非传递性的，由于非传递无干扰关系只允许系统组件之间有直接干扰关系，不允许存在间接造成的干扰关系，即对，，则由以上推导过程可知组件和间将不存在非预期干扰，记作，这时，信任链将不被破坏。于是得到下面具有条件约束的 信任链传递研究进展_左双勇; -《桂林电子科技大学学报》- 2010-08-25（是否引证：否） 1.体,直至系统启动完成。文献[9]给出了一种分析和判定可信计算平台信任链传递的方法,用形式化的方法证明了当符合非传递无干扰安全策略时,组件之间的信息流受到安全策略的限制,隔离了组件之间的干扰,使得信任链的建立不受其它安全无关组件与行为的干扰,从而为系统建立了完整的信任链。信息在组件间的传递 罗东俊_200710102074_基于可信计算的云计算安全若干关键技术研究_罗东俊 -《学术论文联合比对库》- 2013-11-12（是否引证：否） 1.中，干扰关系可分为传递性和非传递性。传递性无干扰策略一般表示为：如果，，则。非传递性无干扰策略一般表示为：如果，，但。非传递的无干扰策略描述了一种隔离性要求比较严格的通道控制安全策略，它要求安全域之间只能有直接干扰关系，而不能存在间接造成的干扰关系。本节给出非传递无干扰策略下系统行为可信性判定方法。为了 基于云模型和信任链的信任评价模型研究_陈建钧;张仕斌; -《计算机应用研究》- 2014-08-27 1（是否引证：否） 1.信任链上实体的信任度。文献[8]提出了一种分析和判定可信计算平台信任链传递的方法,用形式化的方法证明了当符合非传递无干扰安全策略时,组件之间的信息流受到安全策略的限制,隔离了组件之间的干扰。文献[9]提出基于角色的信任证覆盖网络(RBCON)生成、维护等算法,在此基础上给出信任链搜索方案
36	此处有 79 字相似 则需要对安全域的输入和系统状态的论述。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。 且满足一下条件： （2）相对于（1），系统的动作主体满足输出一致性。即一个安全域内的操作动作造成的输出影响只依赖于发	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.于定理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作的域的上一状态系统视图相关联.即 sdo~m(a)t∧(con 云计算中信任链的动态性研究_朱洁 -《中国矿业大学硕士论文》- 2017-05-01（是否引证：否） 1.于此模型的虚拟机的运行满足是无干扰可信的，只要证明此模型满足定理 3.1 中的 3 个无干扰展开式。1. 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。在 DTM 模型的信任链动态维护流程中，dom(a)i x(s ~ s ∧b=a)=true 时，判

		罗东俊_200710102074_基于可信计算的云计算安全若干关键技术研究 罗东俊 -《学术论文联合比对库》- 2013-10-08（是否引证：否）
		1.全域是等价的话，则在这样两个状态下，执行中相同的动作将产生相同的输出结果。用系统视图的概念，输出一致性可以表示成：系统的一个内部动作造成的输出影响只依赖于发出动作的安全域的系统视图。定义4-9：弱单步一致性（weakly step consistent）。系统具有弱单步一致性当且仅当：。弱
		支持进程代码修改的非传递无干扰可信模型 徐甫; -《计算机工程》- 2013-11-15（是否引证：否）
		1.)(,)proc as t output s a output t a,s,t S,a A输出一致性还可以描述为:系统的一个内部操作a对输出造成的影响只依赖于proc(a)的系统视图。定义13如果下式成立,则称系统M具有局部干扰性。()~()~~(,)pproc a p proc a p s step
37	此处有 105 字相似 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。且满足一下条件： （2）相对于（1）， 系统的动作主体满足输出一致性。即一个安全域内的操作动作造成的输出影响只依赖于发出动作动作主体的系统视图。 ； （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。 ； （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.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)∨contents(ste
		罗东俊_200710102074_基于可信计算的云计算安全若干关键技术研究 罗东俊 -《学术论文联合比对库》- 2013-10-08（是否引证：否）
		1.全域是等价的话，则在这样两个状态下，执行中相同的动作将产生相同的输出结果。用系统视图的概念，输出一致性可以表示成：系统的一个内部动作造成的输出影响只依赖于发出动作的安全域的系统视图。定义4-9：弱单步一致性（weakly step consistent）。系统具有弱单步一致性当且仅当：。弱 2.ence Monitor Assumptions，RMA）：假设1：等价关系在引用监视器下的解释为：假设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安全域的上一个状态系统视图相关联。即假设3：系统中如果一个动作改变了一个存储单元的值，则发出该动作的安全域一定可以写访问该存储单元。即定义4-
		可信计算平台信任链理论与技术研究 司丽敏 -《北京工业大学硕士论文》- 2011-06-01（是否引证：否）
		1.的系统视图指它能够观察到的系统状态的组成部分。用系统视图的概念，输出一致性还可以表示成：系统的一个内部操作动作造成的输出影响只依赖于发出动作的域的系统视图。 定义4-7 如果下式成立则称为系统M具有局部干扰性（locally respects ~>）：() 2. 一个域的系统视图指它能够观察到的系统状态的组成部分。用系统视图的概念，输出一致性还可以表示成

		：系统的一个内部操作动作造成的输出影响只依赖于发出动作的域的系统视图。 定义4-7 如果下式成立则称为系统M具有局部干扰性（ locally respects ~>
		云计算中信任链的动态性研究_朱洁 -《中国矿业大学硕士论文》- 2017-05-01（是否引证：否）
		1.于此模型的虚拟机的运行满足是无干扰可信的，只要证明此模型满足定理 3.1 中的 3 个无干扰展开式。1. 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。在 DTM 模型的信任链动态维护流程中，dom(a)i x(s ~ s ∧b=a)=true 时，判
38	此处有 94 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。 ； （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、访问该动作所在的域的系统状态。 ； （6）系统内对系统内的系统状态的操作有以下关系。	罗东俊_200710102074_基于可信计算的云计算安全若干关键技术研究_罗东俊 -《学术论文联合比对库》- 2013-10-08（是否引证：否）
		1.ence Monitor Assumptions，RMA）：假设1：等价关系在引用监视器下的解释为：假设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安全域的上一个状态系统视图相关联。即假设3：系统中如果一个动作改变了一个存储单元的值，则发出该动作的安全域一定可以写访问该存储单元。即定义4-8：输出一致性（ output consistent ）。系统具有输出一致当且仅当：。
		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 2.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.，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 2.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
		可信计算平台信任链理论与技术研究_司丽敏 -《北京工业大学硕士论文》- 2011-06-01（是否引证：否）

		1. 一个域的系统视图指它能够观察到的系统状态的组成部分。用系统视图的概念，输出一致性还可以表示成：系统的一个内部操作动作造成的输出影响只依赖于发出动作的域的系统视图。 定义4-7 如果下式成立则称为系统M具有局部干扰性（ locally respects ~> ）
39	此处有 70 字相似 得成立。 5.4 基于扩展无干扰的TVP-QT验证 本文基于开源的系统Xen，结合本文第3章介绍的TVP-QT架构， 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。 并在此系统下，验证了TVP-QT信任链是符合非传递无干扰判定定理。 如图3.1所示，从TVP-QT第一层到系统最上层存	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.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系统上的设备驱动模型由运行于虚拟机上的前端驱动(虚拟设备)和运行于虚拟机监视器上的后端驱动(实际驱动程
40	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。 依据定理5.3，该系统中的I/O设备驱动程序满足如下要求： 由输出一致性的定义可知，该虚拟机使用的虚拟资源可以由VMM	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/
41	此处有 54 字相似 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。 依据定理5.3，该系统中的I/O设备驱动程序满足如下要求： 由输出一致性的定义可知，该虚拟机使用的虚拟资源 可以由VMM进行分配，并且不存在其他虚拟机无干扰的动作存在。由局部干扰性定义可知，VMM系统中，虚拟I/O设备除其所在的	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.O设备的交互满足非传递无干扰关系,则通过启动阶段针对各虚拟机整体作为文件的完整性验证后,VMM系统建立的信任链是有效的.依据定理2,该VMM系统的I/O设备驱动程序需满足如下要求:(1)由输出一致性的定义可知,VMM维护的虚拟资源必须具有其属于哪个虚拟机的属性标识.(2)由局部干扰性定义可知,VMM系统中,虚拟I/O设备除其所在的虚拟机外其它虚拟机
42	此处有 120 字相似 下要求： 由输出一致性的定义可知，该虚拟机使用的虚拟资源可以由VMM进行分配，并且不存在其他虚拟机无干扰的动作存在。由 局部干扰性定义可知，VMM系统中，虚拟I/O设备除其所在的虚拟机外其它虚拟机不能改变它的运行状态，I/O设备驱动与虚拟设备间所传输的数据对其它虚拟机是不可见和不可修改的。该VMM系统的隔离机制确保虚	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.备驱动程序需满足如下要求:(1)由输出一致性的定义可知,VMM维护的虚拟资源必须具有其属于哪个虚拟机的属性标识.(2)由局部干扰性定义可知,VMM系统中,虚拟I/O设备除其所在的虚拟机外其它虚拟机不能改变它的运行状态,I/O设备驱动与虚拟设备间所传输的数据对其它虚拟机是不可见和不可修改的.该VMM系统的隔离机制确保虚拟机必须采用虚拟设备接口访问后端驱动程序.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

	拟机必须采用虚拟设备接口访问后端驱动程序。 由弱单步一致性可知，该虚拟机在运行过程中的动作只会对此系统进行状态的改变。 （2）存在多个用户虚拟机 该情况下，在存	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
43	此处有 39 字相似 一个用户虚拟机下增加了虚拟机之间的信息流的无干扰情况。因此本文对多个虚拟机在系统中共享资源的同时进行无干扰的验证。 由 输出一致性的定义可知，VMM维护的虚拟资源必须具有其属于哪个虚拟机的属性标识。 可以保证系统中的输出信息可以定位到某一个虚拟机，此虚拟机的不同状态下产生的操作不干扰其他虚拟机的运行。由局部干扰性定义可	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.文件的完整性验证后,VMM系统建立的信任链是有效的.依据定理2,该VMM系统的I/O设备驱动程序需满足如下要求:(1)由输出一致性的定义可知,VMM维护的虚拟资源必须具有其属于哪个虚拟机的属性标识.(2)由局部干扰性定义可知,VMM系统中,虚拟I/O设备除其所在的虚拟机外其它虚拟机不能改变它的运行状态,I/O设备驱动
44	此处有 83 字相似 拟机，此虚拟机的不同状态下产生的操作不干扰其他虚拟机的运行。由局部干扰性定义可知，VMM系统中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。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。 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。 5.5 本章小结 本章按照云计算环境	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.机是不可见和不可修改的.该VMM系统的隔离机制确保虚拟机必须采用虚拟设备接口访问后端驱动程序.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 罗东俊_200710102074_基于可信计算的云计算安全若干关键技术研究 罗东俊 -《学术论文联合比对库》- 2013-10-08（是否引证：否） 1.出一致性的定义可知，可信通道的输出只由其输入决定，即只决定于可信通道本身，任何其他安全域无法干扰其运算，或者篡改；（2）由弱单步一致性定义可知，对于若干安全域共享的客体对象，可信通道必须具有同步保护机制防止不同安全域对该资源的竞争；（3）由局部遵从的定义可知，可信通道必须保证安全域所传输的数据对那些与其无干扰关系的安全域是不可见和不可修改的。据此，在
45	此处有 104 字相似 全域、动作等定义进行扩充，并将动作主体和动作对安全域以及系统状态的影响等扩展到无干扰理论中；最后应用此扩展的无干扰理论来 分析可信云环境信任链传递模型，用形式化的方法证明当符合非传递无干扰安全策略时，云环境安全域之间的信息流受到安全策略限制，隔离了域之间的干扰，满足此条件时用完整性度量方法所建立的云环境信任链才是可信的、有效的。 最后利用无干扰理论对该信任链模型进行了分析和验证，证明了扩展后的无干扰理论验证信任链模型的有效性。 6 总结与展望	可信系统保护模型研究与设计 邱罡 -《西安电子科技大学博士论文》- 2010-09-01（是否引证：否） 1.任链的度量，也不能达到系统运行可信的目标。只有当系统具有特定的安全机制，满足一定的安全策略，组成系统的各安全域之间的信息流动受到一定安全策略限制，使得组件的运行不受干扰，这时，用完整性度量方法所建立的信任链才是有效的。 Bibal98]模型是实现了多级安全(MLS)思想的完整性模型。它规定在任何情况下不可信的输入都是与可信 王红新-80211004-新兴电子商务环境下的柔性支付模型研究 王红新 -《学术论文联合比对库》- 2013-02-26（是否引证：否） 1.围绕满足什么条件时，信任链的建立和传递才是有效

		的这一问题开展讨论，指出：只有当系统本身满足一定的安全策略时，组成系统的各安全域之间的信息流动受到一定安全策略限制，使得组件的运行不受干扰，达到可信目标，这样，用完整性度量方法所建立的信任链才是有效的。④信任传递过程中线下信任与线上信任的关联提倡实名制的SNS网络所建立起来的社区有向真实世界回归的趋势，在虚拟社区内 信任链传递研究进展 左双勇; -《桂林电子科技大学学报》- 2010-08-25（是否引证：否） 1.完整性度量,如果匹配,则判定该实体可信,系统的控制权将发生转移,再度量下一个实体,直至系统启动完成。文献[9]给出了一种分析和判定可信计算平台信任链传递的方法,用形式化的方法证明了当符合非传递无干扰安全策略时,组件之间的信息流受到安全策略的限制,隔离了组件之间的干扰,使得信任链的建立不受其它安全无关组件与行为的干扰,从而为系统建立了完整的信任链。信息在组件间的传递[10]如图4所示。图 基于云模型和信任链的信任评价模型研究 陈建钧;张仕斌; -《计算机应用研究》- 2014-08-27 1（是否引证：否） 1.一种基于模糊理论的可信计算信任评估方法,把模糊推理与信任传递相结合,全面地评估信任链上实体的信任度。文献[8]提出了一种分析和判定可信计算平台信任链传递的方法,用形式化的方法证明了当符合非传递无干扰安全策略时,组件之间的信息流受到安全策略的限制,隔离了组件之间的干扰。文献[9]提出基于角色的信任证覆盖网络(RBCON)生成、维护等算法,在此基础上给出信任链搜索方案。上述信任模型或信任评 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.整性验证实现的信任链传递是否有效无法进行验证.只有当系统具有特定的安全机制,满足一定的安全策略,组成系统的各安全域之间的信息流动受到一定安全策略限制,使得组件的运行不受干扰,这时,用完整性度量方法所建立的信任链才是有效的.进一步用图3表示非传递无干扰关系,其中粗箭头连线表示信任传递关系,细箭头连线表示干扰关系.可以看出,信任链有两条,分别是
46	此处有 29 字相似 链模型进行了分析和验证，证明了扩展后的无干扰理论验证信任链模型的有效性。 6 总结与展望 6.1 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
47	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	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-

	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	28 12:54（是否引证：否） 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
48	此处有 32 字相似 的云计算出现了很多新型虚拟化技术，比如：容器技术、Unikernel等新型的虚拟化技术。如何针对这些新型的虚拟化技术进行 可信平台构建也是下一步的研究方向。 并且本文在信任链构建过程中 也是针对单个或少数虚拟机同时启动的情况下，没有对云计算环境中存在很多虚拟机的情况进行信任链构建进行分析；并且没有对在信任	云计算中信任链的动态性研究 朱洁 -《中国矿业大学硕士论文》- 2017-05-01（是否引证：否） 1.系统[37]。因此具有密钥管理，加解密、数字签名，数据安全存储等功能。在此基础上，它可以完成作为可信存储根和可信报告根的职能。为了存储信任链建立过程中组件的完整性度量值，TPM 中设计了一个关键部件配置寄存器 PCR（Platform Configuration

指　标

疑似剽窃文字表述

1. 利用属性式(12)结论及定义3.1，可直接证明属性式(13)成立。
   根据上述证明可知，在TVP-QT信任链构建过程中，能够有条件地保持其信任属性，即构建信任链所需要执行的不同程序在跳转过程中，不会被其他恶意代码所控制或插入，从而不存在信任缺失的情况，且这种信任属性能够向远程验证者提供证明。
2. 关系，可将TJP的本地信任传递属性归纳为：如果最终的PCR中度量值序列是正确的值，那么TJP信任链所加载的程序顺序就是正确的。即TJP的本地信任传递属性就是要求所有相应启动程序如vTPM Builder、
3. 这就需要证明上述程序启动序列与PCR值之间的一一映射关系。基于前文的假定前提，要证明的信任链本地信任属性如下。
4. 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。在此过程
5. 本地可信属性，如果PCR中度量值序列是正确的值，那么主机m信任链所加载的程序顺序就是正确的，
6. 机器的每一个存储单元都有一个名字。所有存储单元名字的集合构成存储单元集，又叫做名字
7. 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。
8. 安全域中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域视图内容函数计算。所有取值的集合构成值集。
9. 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5.4
10. 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。具体的取值可以由下面的主体视图内容函数计算。
11. 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“单步一致性”。注意：本文中遵从Rushby的符号表达，约定使用表达蕴含关系。
    定义5.6 间接干扰关系。
12. 若将定义1当中的干扰关系称作是“直接干扰关系”，则可以定义“间接干扰关系”如下:
    定义5.7 干扰源集。
    干扰源集的递归定义如下:
    ，且

，且。其中，。
干扰源集的含义是:抽取所有对安全域有直接或间接干扰关系的安全域形成集合。
定义5.8 弱预期函数。
，且
。
其中，，
。
弱预期函数的含义是，“将所有
13. 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5.9 域集等价关系:。
并且Rushby定义了系统满足非传递性无干扰策略
14. 分析可信云环境信任链传递模型，用形式化的方法证明当符合非传递无干扰安全策略时，云环境安全域之间的