学号_____姓名_____专业_____级_____学院_____（密）……（封）……（线）……

四川师范大学

科学硕士研究生学期作业（论文）专用封面

所修课程名称：_____学术培养

作业（论文）题目：文献资料分类索引

读书报告

文献综述

文献阅读及学术交流

修课程时间：2015 年 9 月至 2017 年 9 月

完成作业（论文）日期：2017 年 9 月

任课教师打分：

任课教师评阅意见：

任课教师签名：　　年　　月　　日

目　录

一、文献资料分类索引

1、题目：《云计算安全:架构、机制与模型评价》

作者：林闯，苏文博，孟坤，刘渠，刘卫东

摘要：随着云计算服务的广泛使用，租户对云计算的安全性提出了越来越高的要求，云计算环境的动态性、随机性、复杂性和开放性使得原有安全方案难以适用，这也阻碍了云计算的进一步发展与应用。文中在分析云计算服务模式特点以及安全挑战的基础上，针对云计算安全架构、机制以及模型评价三个方面展开研究与综述。文中指出云计算的安全架构不仅需要可信根、可信链路以及上层可信服务的安全保证，还需要实现可管、可控的动态安全管理与可度量的安全评价优化过程。文中对已有云计算安全机制和模型评价方法进行了比较分析，最后提出了基于多队列多服务器的云计算安全建模与分析思路。

2、题目：《云计算环境安全综述》

作者：张玉清，王晓菲，刘雪峰，刘玲

摘要：伴随云计算技术的飞速发展，其所面临的安全问题日益凸显，在工业界和学术界引起了广泛的关注。传统的云基础架构中存在较高安全风险，攻击者对虚拟机的非法入侵破坏了云服务或资源的可用性，不可信的云存储环境增大了用户共享、检索私有数据的难度，各类外包计算和云应用需求带来了隐私泄露的风险。从云计算环境下安全与隐私保护技术的角度出发，通过介绍云虚拟化安全、云数据安全以及云应用安全的相关研究进展，分析并对比典型方案的特点、适用范围及其在安全防御和隐私保护方面的不同效用，讨论已有工作的局限性，进而指出未来发展趋势和后续研究方向。

3、题目：《可信计算的研究与发展》

作者：沈昌祥，张焕国，王怀民，王戟，赵波

摘要：可信计算是一种信息系统安全新技术，它已经成为国际信息安全领域的一个新热潮，并且取得了令人鼓舞的成绩。我国在可信计算领域起步不晚、水平不低、成果可喜。我国已经站在国际可信计算的前列。文中综合论述近年来可信计算理论与技术的一些新发展，特别是介绍我国可信计算的一些新发展，并对目前可信计算领域存在的一些问题和今后发展提出了自己的看法和观点。

4、题目：《虚拟可信平台模块动态信任扩展方法》

作者：余发江，陈列，张焕国

摘要：将可信计算技术应用到虚拟计算系统中，可以在云计算、网络功能虚拟化(network function virtualization，简称 NFV)等场景下，提供基于硬件的可信保护功能。软件实现的虚拟可信平台模块(virtual trused platform module，简称 v TPM)基于一个物理 TPM(physical TPM，简称 p TPM)，可让每个虚拟机拥有自己专属的 TPM，但需要将对 p TPM 的信任扩展到 v TPM 上。现有方法主要采用证书链来进行扩展，但在虚拟机及其 v TPM 被迁移后，需要重新申请 v TPM 的身份密钥证书，可能会存在大量的短命证书，成本较高，且不能及时撤销旧 p TPM 对 v TPM 的信任扩展，也不能提供前向安全保证。提出了一种 v TPM 动态信任扩展(dynamic trust extension，简称 DTE)方法，以满足虚拟机频繁迁移的需求。DTE 将 v TPM 看作是 p TPM 的一个代理，v TPM 每次进行远程证明时，需从一个认证服务器(authenticaiton server，简称 AS)处获得一个有效的时间令牌。DTE 在 v TPM 和 p TPM 之间建立了紧密的安全绑定关系，同时又能明显区分两种不同安全强度的 TPM。在 DTE 里，v TPM 被迁移后，无需重新获取身份秘钥证书，

旧 p TPM 可及时撤销对 v TPM 的信任扩展，而且 DTE 可提供前向安全性。从原型系统及其性能测试与分析来看，DTE 是可行的。

5、题目：《一种可信虚拟机迁移模型构建方法》

作者：石源，张焕国，吴福生

摘要：虚拟机的安全迁移是保障云环境安全可信的重要需求之一。对于包含虚拟可信平台模块(virtual TPM，vTPM)的可信虚拟机，还需要考虑 vTPM 的安全迁移问题。目前，已有一些针对可信虚拟机的安全迁移的研究，但是由于研究可信虚拟机的模型不统一，导致迁移模型解决问题的方案不能适用所有的迁移方案，存在一定的局限性。针对可信虚拟机的迁移缺乏统一的安全模型及测试方法的问题，参考虚拟机迁移中普遍存在的安全问题以及可信计算和云的相关规范，从整体系统层面对可信虚拟机的迁移进行安全需求分析;提出一种可信虚拟机迁移框架，将可信迁移的参与组件进行了抽象并描述了迁移协议中的关键步骤和状态;以标号迁移系统 LTS 为操作语义描述工具对可信迁移系统进行进一步的描述，以系统中迁移进程组件的建模为基础构建出动态的迁移系统状态迁移树;分析了 LTS 模型可以用于可信迁移协议的一致性测试，并通过与其他相关工作的比较说明了模型在考虑安全属性方面的完备性。

6、题目：《基于无干扰的云计算环境行为可信性分析》

作者：张帆，张聪，陈伟，胡方宁，徐明迪

摘要：云安全是目前云计算研究的热点之一。作为云安全基础的可信计算，目前仍存在一些关键问题有待解决，这使得云安全事实上是有缺陷的。针对可信计算中的动态行为可信度量问题，提出了一种基于无干扰的云环境行为可信性分析方法:首先，基于可信计算组织 TCG(Trusted Computing Group)和学术界对于“可信”的定义，给出了行为可信的判定等式。进一步地，建立了基于状态递归等价的行为可信的充要条件，解决了目前尚没有有效的行为可信性验证方法的问题，就我们尽可能的调研而言，目前没有见到类似结论。最后，给出了实验示例，证明了方法是有效的。

7、题目：《基于扩展 LS~2 的可信虚拟平台信任链分析》

作者：常德显，冯登国，秦宇，张倩颖

摘要：针对可信虚拟平台信任链的形式化分析问题，建立了包括虚拟机和虚拟信任根在内的可信虚拟平台完整的信任链模型，并详细定义其应满足的信任属性，通过扩展 LS2，验证了可信虚拟平台信任链模型能够有条件地满足其正确性、唯一性。对实例系统分析表明本文所建立信任链模型的通用性及基于扩展 LS2 分析方法的有效性。

8、题目：《一种可信虚拟平台构建方法的研究和改进》

作者：李海威，范博，李文锋

摘要：为了减小虚拟环境下虚拟可信平台模块(v TPM)实例及系统软件可信计算基(TCB)的大小，同时进一步保护 v TPM 组件的机密性、完整性和安全性，解决传统虚拟可信计算平台下可信边界难以界定的问题，文章提出了一种新的构建可信虚拟平台的方法和模型。首先，将 Xen 特权域 Domain 0 用户空间中弱安全性的域管理工具、v TPM 相关组件等放置于可信域 Domain T 中，以防止来自 Domain 0 中恶意软件的攻击及内存嗅探，同时作为 Xen 虚拟层上面的安全服务实施框架，Domain T 可以给 v TPM 的相关组件提供更高级别的安全保护。其次，通过重构 Domain 0 中拥有特权的管理和控制应用软件，将特权域的用户空间从可信计算基中分离出来，进而减小虚拟可信平台可信计算基的大小。最后，设计

并实现了新的基于可信虚拟平台的可信链构建模型。通过与传统可信虚拟平台比较，该系统可以有效实现将虚拟化技术和可信计算技术相融合，并实现在一个物理平台上同时运行多个不同可信级别的操作系统，且保证每个操作系统仍然拥有可信认证等功能。

9、题目：《基于信任扩展的可信虚拟执行环境构建方法研究》

作者：王丽娜，高汉军，余荣威，任正伟，董永峰

摘要：为保护虚拟机运行环境及上层服务软件的完整性、安全性，提出了一种基于信任扩展的可信虚拟执行环境的构建方法。首先，建立物理平台配置寄存器(PCR，platform configuration register)与虚拟 PCR 的映射关系，以此实现虚拟可信平台模块(vTPM)与底层可信计算基的绑定;其次，利用本地 vTPM 管理器签发证书，完成可信证书链在虚拟机中的延伸。通过物理平台至虚拟平台的信任扩展，虚拟机可以有效地利用 TPM 提供的相关功能(如远程证明、密封存储等)，完成平台环境的证明及私密信息的安全存储，从而构建了可信虚拟执行环境。最后，实现了原型系统并进行了测试，测试结果证明本系统可以有效地实现虚拟平台的密封存储和远程证明等功能。

10、题目：《基于无干扰理论的信任链传递模型》

作者：陈亮，曾荣仁，李峰，杨伟铭

摘要：针对现有的信任链传递模型可用性不强、缺乏将信任链扩展到网络环境的缺点，提出了一种新的基于无干扰理论的信任链传递模型。该模型将系统抽象为进程、动作和执行，从可信根出发，通过度量程序及其动态库完整性来保证进程静态可信;分析交互进程之间的关系，利用无干扰理论判定其合法性;通过对接入终端的可信度量，将信任链扩展到整个网络系统。最后给出了相应的形式化定义及安全性证明。

11、题目：《基于无干扰理论的云服务行为可信模型》

作者：谢洪安，刘大福，苏旸，张英男

摘要：为解决云服务环境下存在的资源共享及特权安全威胁，将传统的无干扰理论引入云服务环境中，提出一种基于无干扰理论的云服务可信模型(NICTM)。该模型将云服务中域、动作、状态、输出等进行抽象，形式化地定义了云服务环境中域的可信;然后证明了用户域行为可信定理，符合定理的用户域可以被证明是可信的;最后在 Xen 虚拟化平台上实现了基于模型的原型系统，并通过实验验证了模型的可行性。

12、题目：《一种基于无干扰模型的信任链传递分析方法》

作者：张兴，黄强，沈昌祥

摘要：基于可信计算组织(TCG)的完整性度量只能保证组件没有被篡改，但不一定能保证系统运行可信性。其问题在于，当组件运行时，受其它组件的干扰，出现非预期的信息流，破坏了信任链传递的有效性。文章在分析可信计算平台的信任模型基础上，基于无干扰理论模型，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，这样用完整性度量方法所建立的信任链才是有效的。

13、题目：《云计算:从云安全到可信云》

作者：吴吉义，沈千里，章剑林，沈忠华，平玲娣

摘要：虽然云计算产业具有激动人心的市场前景，但对于使用云服务的用户而言，云计算存在着多方面的潜在风险和各种安全问题。在客观分析了当前云计

算领域发展中面临的安全挑战问题基础上，总结了云安全领域的最新研究进展，最后还指出了云安全领域的主要研究方向。云计算与可信计算技术的融合研究将成为云安全领域的重要趋势。

14、题目：《一种可信终端运行环境远程证明方案》

作者：谭良，陈菊

摘要：可信终端的远程证明无论是基于二进制的证明方案还是基于属性的证明方案，针对的均是终端的静态环境，反映的是终端的软件配置结构，并不能证明终端运行环境的真正可信。针对这一问题，提出了一种终端可信环境远程证明方案。针对静态环境，该方案考虑了满足可信平台规范的信任链以及相关软件配置的可信属性证明;针对动态环境，该方案考虑了终端行为的可信属性证明。并分别给出了信任链、平台软件配置和终端行为等属性证明的可信性判定策略和算法，以及终端运行环境远程证明的综合性判定策略和算法。另外，在 Windows 平台上，设计和实现了该方案中的两个核心实体:证明代理和验证代理，并设计了证明代理和验证代理之间的通信协议。最后，介绍了该方案在 Windows 平台上的一个典型应用案例以及证明代理在该应用实例中的性能开销。应用实例验证了该方案的可行性。

二、读书报告

研究生生涯这几年，我阅读了大量与研究方向相关的学术论文，使我受益匪浅。并且阅读的参考文献不仅仅有可信计算、云计算、云计算安全等方面，也涵盖了相关的计算机领域的学科，比如大数据，密码学等。现在我将这几年来对所阅读文献总结如下，并提出自己的一些观点，主要针对研究方向及其相关领域的文献进行总结。

将虚拟化技术与可信计算相结合构建的可信虚拟平台及其信任链模型是目前的一个研究热点。目前大部分的研究成果是采用在虚拟平台上扩展传统信任链的构建方法，不仅模型过粗且逻辑不完全合理，而且还存在底层虚拟化平台和顶层用户虚拟机两条分离的信任链问题。并且目前的无干扰理论形式化方法只定义了动作所属域，没有针对云环境下系统动作的主体等进行定义，不能完全适用于云计算环境下的信任链传递模型。

根据 NIST 定义，云计算是可以使用户按照使用量付费并且获得高效的、快捷的网络服务的新型资源共享模式，其主要目的是在提高网络、服务器、硬盘存储、软件等共享资源利用率的同时，使云租户不再关注硬件资源的管理和维护，云租户只需要在硬件资源上投入很少的管理维护工作就可以得到很高的资源回报。云计算的高效的资源处理能力也带动了大数据、人工智能等相关领域的发展。目前的云计算提供商，比如国外的 Intel、IBM、微软，以及国内的腾讯、阿里巴巴都拥有非常成熟的云计算技术和应用服务提供技术。云计算的快速发展同时也给云计算带来了除传统信息安全、网络安全之外的安全问题，其中，如何向云租户证明云计算底层平台的安全性、虚拟机(Virtual Machine, VM)的安全性是一个非常重要的问题。而可信计算是保障信息系统安全最为重要的技术手段之一，它通过提供数据保护、身份认证、远程证明以及完整性度量等特性提高包括底层物理资源、应用软件等在内的计算平台的可信性和可靠性。因此，将可信计算技术应用在提高云计算环境的安全性是工业界和产业界必须重视的地方。

根据中国信息通信研究院 2017 年 7 月发布的《云计算关键行业应用报告》，近几年，云计算的发展十分迅速，并产生了以云主机为主要服务的云计算市场。其中，2016 年，全球云计算市场的经济整体规模已经达到了 654.6 亿美元，较 2015 年增长 25.4%，并且预计在 2020 年云计算市场规模将达到 1453.3 亿美元，平均每年增长率为 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，工信部在官方网站发布通知《云计算发展三年行动计划（2017－2019 年）》中提到，我国云计算的发展目标到 2019 年我国的云计算规模预计达到 4300 亿元，该项内容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 年全球云计算安全报告”显示，在 2016 下半年到 2017 年，在参与调查的公司中，为把更多的精力投入到提高客户体验中，IT 预算中有超过 80%的预算被用来使用云服务及其解决方案。但是，仅有 23%的企业完全信任云计算提供商。

目前的大部分云租户不能完全信任云提供商提供的云计算服务的原因，主要是由于云租户在使用云提供商提供的虚拟机时，并不能确认云计算平台上的物理主机是云提供商按照各自操作系统官方文件进行启动的，以及租户请求的虚拟机是按照预期的配置和要求进行启动的。因为云计算环境下的虚拟机存在着包括传统信息系统安全以及新型网络安全等威胁，比如：虚拟机恶意代码攻击、虚拟机

逃逸等，这些都会导致虚拟机在重新启动时的组件被篡改，在云租户对虚拟机进行重新启动时，可能无法判断虚拟机的操作系统、数据是否被篡改。而可信虚拟平台的构建可以利用可信平台模块（Trusted Computing Platform, TPM）中的可信度量、可信报告等技术向用户发送关于云计算平台的可信度量结果，并且证明自身的安全性。一方面，云计算架构中独特的虚拟机监视器（Virtual Machine Monitor, VMM）的隔离机制、安全机制、监控机制，为在物理服务器操作系统和应用服务建立可信计算环境提供了保障，也可以有效的防止外界对可信计算环境的侵扰和破坏；另一方面，可信计算技术为虚拟化技术中的虚拟机提供了完整性度量和信任链扩展的思路，为虚拟机对云租户提供云服务提供了保障。

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（Virtu-alization 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信任链构建，建立从云计算平台底层物理服务器到提供服务的可信虚拟机的信任链，可以给目前的云计算安全问题提供一个新的解决思路，为构建安全的云计算环境提供更好的安全保障。

并且，针对信任链传递模型的形式化分析方法一直是可信计算研究领域中重点关注的问题，从安全系统的整体构建角度上来看，一个安全可靠的系统不仅仅在功能上是安全的，也必须利用形式化分析中的数学模型描述其组件和安全属性，并用语义明确的定义和安全定理证明其安全性。在针对信任链形式化分析方法中的众多理论中，无干扰理论一直是备受研究者关注的形式化分析方法。无干扰理论基于有限状态机描述系统的行为和动作，并从传递无干扰和非传递无干扰给出系统的安全定理。但是目前的针对信任链传递模型的形式化分析方法还不能完全适用于云计算环境下的可信虚拟平台，其缺点主要表现在其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，比如，系统的发出动作在整体上是属于某一域，但是实际上也存在发出该动作的主体。

可信计算技术与虚拟化技术的结合的可信虚拟平台（Trusted Virtualization Platform, TVP）一直以来都受到国内外学者的广泛关注。Intel 的 Stefan Berger 等人最先提出 vTPM 的概念，随后产生了很多关于 TVP 及其信任链构建的研究成果，其中，开源的虚拟机架构 Xen 是最早支持 vTPM 的 VMM，为学术界和产业界提供非常便捷的实验平台；2015 年，云计算公司 EMC 宣布在 VMware vSphere 6.0 中支持 vTPM；2016 年，微软宣布在 win10 中加入可信计算，并提供 Hyper-V 技术。总之，学术界和产业界都已开始重视可信计算技术与虚拟化技术的结合。为更好的对本文研究内容的国内外研究现状进行阐释，本文将从可信虚拟平台架构、可信虚拟平台信任链模型、无干扰理论形式化分析方法三部分进行描述。

国外研究者针对可信计算解决虚拟系统安全问题的研究比较早，在 2000 年后都被研究者用来解决虚拟系统平台安全的问题，这些平台包括 Terra，Perseus 等，这些平台的主要思想是把底层计算平台分为两部分，可信区域和不可信区域，其中可信区域上运行着高安全性需求的虚拟机，而存在着安全威胁的虚拟机被放在不可信区域。这些方案为可信虚拟平台的研究提供很好的理论基础。

TVP 的概念首先由 Stefan Berger 等人提出，随后文献等学者针对如何构建具体应用场景的 TVP 功能应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 是一个可以支持可信计算虚拟化技术的物理主机，并且其与一般的带有 TPM 的可信主机的主要区别在于，一是拥有在物理硬件可信平台模块构建起来的虚拟可信信任根；二是可以并发的为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。并且 TVP 架构可以被分为 4 个具有不同功能的层次。第一层为硬件信任根 TPM，为整个可信虚拟平台提供物理保障。第二层主要包括虚拟机监视器 VMM，以及建立在 VMM 上，包括内核和 VMM 管理工具的管理域，并且被当做 TVP 的可信计算基来启动。第三层是作为虚拟机启动的虚拟可信根（Virtual Root of Trust, vRT），并且虚拟可信根的加载方式以两种不同的实现方案来实现，一种是当做传统信任链的一部分进行静态加载，另一部分是利用动态度量机制（Dynamic Root of Trusted Measurement, DRTM）实现动态加载。所以虚拟可信根可以作为 TCB 的一部分，也可以当做 TVP 上的单独进程。第四层是与用户关系最为密切的用户虚拟机。

HP、IBM 等研究机构分别提出并构建了相应的 TVP，其 TVP 架构可根据不同应用需求建立用户可定制的 TVP，在很大程度上推动了 TVP 的发展。随后，Krautheim 等学者基于云计算环境建立了 TVP，使其可以保护云计算环境下的虚拟机运行，以及保护虚拟机运行时上层服务软件的完整性、安全性。Zhang Lei 等提出一种具有可信域层次的 TVP，通过可信云平台和可信虚拟机进行分离的 TVP 构建机制，并实现了对可信云平台以及可信虚拟机的安全保障。国内的研究中，王丽娜给出了基于信任链扩展的 TVP 架构，常德显等根据 TVP 的功能层次给出了包括虚拟机和虚拟可信根的 TVP 定义，并细分为 VMM、Dom0、TPM、vRT 等组件总结起来，目前针对 TVP 模型的研究尽管取得了很多成果并达成了基本共识，即 TVP 模型都包含基本组件 vRT、vTPM 等，但绝大多数已有的研究成果把 TVP 的 VMM 和管理域都作为 TCB，一起作为虚拟机的 vRT，这样的设计粒度明显过粗且逻辑上不完全合理的，因为管理域包含 OS 及大量的应用程序，不能采用链式度量所有的应用程序并存储其 PCR 值。

为更好的对信任链模型的研究现状进行更好的阐述，本文将从目前信任链模型三个不同类别的研究现状进行描述。

（1）通过对 TCG 链式信任链模型的扩展，实现 TVP 下可信度量以及信任传递。Scarlata 等提出在构建 TVP 时，通过可信测量构建从 CRTM 可信根到每个客户虚拟机的信任链，就可以证明每个客户虚拟机是可信的，显然这种信任链模型是不完善的，无法适应比较复杂的 TVP 环境。John 对信任链扩展上提出了“Transitive Trust Chain”信任链模型，并且简要的指出了信任链传递过程为 TPM→VMM→TVEM manager→TVEM→VM OS→应用程序，但是此种信任链模型没有详细的描述特权域操作系统以及虚拟机操作系统的可信度量。Shen]等根据 TCG 动态度量方法提出了一种基于 Xen 的可信虚拟机在 DRTM 下的信任链构建，其具体的构建过程为：CPU→可信代码→Xen VMM→Dom0（→vTPM Manager→Domain Builder）→Guest 0S→Guest Application，此种信任链模型也存在 John 中的问题。

（2）通过研究可信云平台和可信虚拟机两部分的信任链，构建 TVP 下的信任链模型。常德显等提出 TVP 信任链包括按照 TVP 的功能层次从硬件 TPM 层→TCB 层→vRT 层→用户虚拟机层的信任链模型，此信任链模型对 vRT 及层次间的连接定义比较模糊。Zhang Lei 等提出一种基于无干扰的可信域层次信任链模型，并且指出分别度量物理主机和 VM 的方式，即首先度量从物理的 TPM 到

物理主机的应用程序，然后度量 VM 的 vTPM 和应用程序，显然此种信任链模型无法有效的对 TVP 下构建完整的链式信任链模型，不能向用户虚拟机呈现一条完整的信任链模型。

（3）树形或者星形的信任链模型。一部分学者认为 TCG 的链式信任链可信度量方式在虚拟化环境下是难以有效构建的。朱智强提出了一种安全可扩展的星型信任度量结构，在信任度量时只需要信任根（RT）对管理域节点（Management Domain, MDn）进行度量即可，但是此信任链模型的关键节点 RT 需要对所有的管理节点进行度量，RT 的负担重，无法高效的完成 TVP 下的可信度量以及信任传递。曲文涛[[]]等提出了一种解决 RT 负担的改进方案，带链式结构的星型信任链模型，设计了 MDn 节点分担了 RT 的部分度量负担，但是此种信任链模型也存在负担重的 MDn 节点。总结起来，目前针对 TVP 的信任链模型的共同问题是信任链模型过粗且逻辑上不合理的问题，与具体云环境中虚拟化平台也不完全相符合，且目前研究内容中的可信虚拟平台信任链与虚拟机信任链是两条不同的信任链，这两条信任链在度量层次和度量时间上均是分离的，不能向虚拟机用户展示一条从 TPM 到虚拟机应用的完整信任链。但是目前的信任模型存在以下问题：

（1）现有的 TVP 模型把整个第三层都作为 TVP 的 TCB 并作为虚拟机的 vRT，是不精细的且逻辑上也不完全合理的。第三层包括 VMM 以及 DOM 管理域，信任链为 CRTM→BIOS→BootLoader→VMM→DOM OS→Apps，DOM 管理域包含 OS 及大量的应用程序，不能采用链式度量所有的应用程序并存储其 PCR（Platform Configuration Module, PCR）值。

（2）虚拟平台信任链与虚拟机信任链是两条不同的信任链，即在整个 TVP 以及客户虚拟机启动过程中存在两条完全分隔的信任链，一条是可信虚拟平台在启动时的信任链，另一条是客户虚拟机在启动时的信任链，这两条信任链在度量层次和度量时间上均是分离的。如何向虚拟机用户展示一条从 TPM 到虚拟机应用的完整信任链，即这两条信任链存在如何衔接的问题。

目前针对于信任链形式化建模与分析的方法有很多研究方向，其中最为热门的当属无干扰理论，本文在此对无干扰理论的研究现状进行阐述。针对于无干扰理论的研究，目前大部分的研究是基于有限状态机从系统内部域产生的动作和行为以及其运行结果的角度上建立了系统安全属性和定理。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息量。Baldan 等对无干扰中存在干扰的信息流添加了因果关系，建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、赵佳等在由 Rushby 提出的有限状态机的无干扰理论的基础上针对系统安全域进行了实例化，使其具体成为进程集合，然后给出了进程集合运行的可信条件和满足终端安全的可信定理，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。刘鹏威等重新定义了清除函数，增加了非传递的无干扰安全定理，然而同样存在赵佳中的问题。陈菊等利用无干扰理论构建了从进程和代码完整性之间的安全操作。徐甫等在动态干扰和静态干扰对无干扰理论进行了扩展，但是文章中的动态和静态的定义都是十分抽象的，无法与实际的操作进行匹配。秦晰等从信任组件处理非信任组件的角度对非信任组件的输出进行了域间隔离和干扰，但是并没有针对安全域进行详细的描述。

针对可信计算平台，张兴等利用无干扰理论对传统可信计算平台信任链进行了建模分析，并且指出只有满足传递无干扰安全策略才可以构建安全的信任链。

虽然 Zhang 等人利用无干扰理论对可信云计算环境信任链进行了形式化分析和验证，但是此种信任链分析方法是建立在不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。

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全域和系统状态的影响进行详细的说明，比如针对于安全域，动作可能属于不同的主体，不同的主体也可发出不同的动作。

阅读过文献后，我们要学习别人是怎么发现问题的。知道对这个问题的一些看法，分歧等。然后，在此基础上扩展开来，根据兴趣和研究的目的，知道，在研究的领域，那些文献最有启发性，去图书馆查找相关的论文，逐步扩展自己的视野，构建个人的专业知识结构和看法。在我们看过文献，结合自己的专业知识，有一定的基础之后，对于繁杂的文献，我们要有个人的判断，将自己置于研究之中，就像你自己是实验的主导，你应该怎么多，这样才会有自己的看法，提出不同的观点。追踪某个专题，某个专家的研究进展，比较对于同一专题的论点的发展，掌握其新的方法或新的结论，或注意作者观点的改变，探究其原因，培养个人的学术修养，对于高质量高水平的期刊，定期浏览，从面上了节学术进展和热点，根据个人的兴趣和工作进展，逐篇仔细阅读。

三、文献综述

vTPM 体系架构研究进展

摘要：云计算与可信计算相结合是构建可信云环境的重要方法，对可信平台模块的虚拟化成为解决云计算安全问题的一个重要的研究方向。介绍了虚拟可信模块基本知识，分析总结了目前虚拟可信模块的典型架构分类及研究进展，包括松耦合型，紧密耦合型，半紧密耦合型三种 vTPM 结构，并重点分析了当前主要的松耦合型 vTPM 架构，在传统和新型松耦合型架构上进行了比较和总结。基于松耦合型 vTPM 架构，给出了目前松耦合型 vTPM 架构亟待解决问题，并展望了未来 vTPM 架构的发展方向。

关键字：vTPM 架构，云计算，可信计算，虚拟可信模块

1. 引言

云计算技术的兴起，带来了一种新的服务方式，云计算技术通过对计算机资源进行虚拟化，然后将虚拟化资源提供给云租户，可以说虚拟化技术是云计算技术得以发展和实施的关键。而将可信计算与云计算技术相结合是保证云计算安全一个重要的途径。可信平台模块 TPM（TrustedPlatformModule）是可信计算平台的信任根，是整个平台可信的基点，是可信计算技术的关键技术之一[1]。TPM 可以为云计算虚拟化环境提供密码运算、安全存储和可信报告等基础安全功能，并且可以实现对计算平台自身、计算平台的使用者、计算平台的软硬件配置以及应用程序的完整性和合法性的可信认证。并且随着可信计算技术规范的制定与更新[2]，如可信 PC、可信平台模块(TPM)、可信软件栈(TSS)、可信网络连接(TNC)等，以及可信计算相关理论的愈见成熟，如信任链技术、远程证明等，可见通过对可信计算技术中的可信平台模块的虚拟化是保证云计算安全重要的研究方向之一。

云计算复杂的运行环境，使得当上层云服务需要向外提供较为充分的可信证明安全功能服务时，对 TPM 资源的使用竞争矛盾就会凸显而来。针对虚拟化平台多用户操作系统实例，即多个虚拟机（VM, virtual machine）并发运行于同一物理平台的需求，Stefan Berger[3]等人首先提出虚拟可信平台模块（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（vRT, virtual root of trust）来构建实现虚拟化可信平台的原型系统，并且通过模拟硬件 TPM 的接口和功能，使每个虚拟机拥有自己独立的 vTPM，保护敏感信息、存储虚拟环境度量值、提供远程证明等，从而实现多个虚拟机共享复用 TPM 硬件资源。

鉴于 vTPM 对云计算虚拟化环境安全的重要性，在工业界和学术界的共同研究下，在虚拟化平台上实现的 vTPM 架构也在不断的发展和改善中。本文结合国内外对可信计算技术的虚拟化以及 vTPM 架构的研究，按照 vTPM 与客户虚拟机和 TPM 绑定的紧密程度，将 vTPM 的架构分为三类，松耦合型 vTPM、紧密耦合型 vTPM、半紧密耦合型 vTPM。并且随着 TPM2.0 规范已经在 2015 年成为了国际执行标准[4]，并且更好的适应云计算平台的发展，能更好的与松耦合型 vTPM 体系架构相结合，能确保 vTPM 与虚拟机的完整性度量、存储、迁移等相关操作更加灵活。在对松耦合型架构的研究上，IBM 的 Berger 等首先对松耦合型 vTPM 进行描述，随后可信计算组织 TCG 的虚拟平台工作小组 VPWG 对 vTPM 架构的进行了规范的设计和描述[5]，松耦合型 vTPM 被越来越多的研究者关注。TPM2.0 规范以其更加灵活的特性，使得松耦合型 vTPM 架构是未来发展的一个

重要的趋势。总结来说，松耦合型 vTPM 架构的演变趋势可以概括为从虚拟机通过相应的驱动使用 TPM 功能，发展到目前 vTPM 实例和 vTPM 管理器在云计算虚拟化平台中作为一个分离的轻量级域被使用[]，这种变化可以减轻可信云平台特权域的工作负担，更加保证虚拟机对 TPM 功能使用的灵活性，以及对虚拟机安全的保障。

综合近些年 vTPM 体系架构的发展，本文对 TPM 及 vTPM、TPM 规范进行了相关的描述，分析总结了目前虚拟可信模块的典型架构分类及研究进展，包括松耦合型，紧密耦合型，半紧密耦合型三种 vTPM 结构，并重点分析了当前主要的松耦合型 vTPM 架构，在传统松耦合型架构和新型松耦合型架构上进行了比较和总结。并基于松耦合型 vTPM 架构，给出目前 vTPM 架构存在的问题以及未来 vTPM 架构的发展方向，力求对 vTPM 体系架构理论与技术的研究发展进行客观和全面的介绍。

2. 基本概念介绍

2.1 TPM 与 vTPM

可信平台模块（Trusted Platform Module， TPM）是一种硬件组件，目前已成为专业个人计算机主板的一部分，它是整个平台可信的基点，是可信计算的关键技术之一。TPM 安全地存储着敏感的加密密钥，加密密钥中的部分密钥从来不会离开 TPM。可信平台模块 TPM 是可信计算平台的信任根，是可信计算的关键技术之一。TCG 定义可信计算平台的信任根包括 3 个根，它们是可信测量根 RTM、可信存储根 RTS 和可信报告根 RTR.其中可信测量根 RTM 是一个软件模块，可信存储根 RTS 由可信平台模块 TPM 芯片和存储根密钥 SRK 组成，可信报告根 RTR 由可信平台模块 TPM 芯片和根密钥 EK 组成。可信计算平台以可信度量根核（CRTM）为起点，以信任链的方式来度量整个平台资源的完整性，将完整性的度量值存储在 TPM 中的平台寄存器 PCR 中，并通过 TPM 向询问平台可信状态的实体提供报告，供访问者判定该平台是否可信。这种工作机制被称为可信的度量、存储、报告机制，是可信计算机与普通计算机在安全机制上的最大区别。如图是 TCG TPM 基本架构[1]：

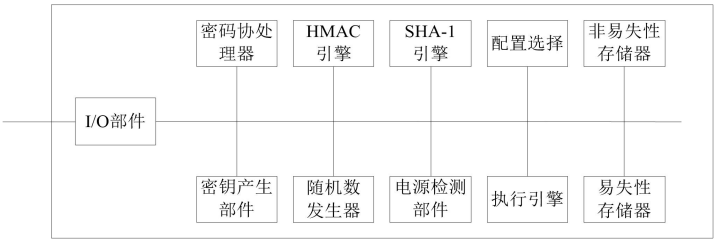


图 1 TCG 的 TPM 组成结构

从传统意义上讲，TCG 规定 TPM 负责保证平台的可信性和安全性，但是它只能为一台机器提供保护并阻止多个实体同一时间的非法访问。为了使 TPM 和虚拟化很好的结合，IBM 和 Intel 提出在 Xen 中实现 vTPM 的概念[3]，该方法可以为每台 VM 提供一个虚拟的 TPM，使它们觉得自己拥有独立的 TPM 一样，在后文将会介绍该架构。这就需要创建多个虚拟 TPM 实例来实现，并且每个实例都如实模仿硬件 TPM 的功能。另外，开源软件比如 Qemu[6]，还有一些专利产品像 VMWareWorkstation[7]，已经成功模拟了个人计算机。它们为时钟、中断控制器、PCI 总线和相关设备提供了透明的模仿机制。并且通过模拟硬件 TPM 的接口和功能，使每个虚拟机拥有独立的 vTPM，可以对自身进行保护敏感信息、存储虚拟环境度量值、提供远程证明等，从而实现多个虚拟机共享复用 TPM 硬件

资源。vTPM 的出现可以使可信计算的重要技术如 TPM、信任链等用来保护云计算虚拟化平台，例如对虚拟化平台上的实体进行安全保证，结合信任链技术，对整个虚拟化平台进行完整性度量等。

2.2 vTPM 基本原理

虚拟化技术是实现 vTPM 的一个关键的技术。虚拟化在计算机方面通常是指计算机元件在虚拟的基础上而不是真实的基础上运行，即使用某些程序对计算机资源进行逻辑表示，使之不受物理环境的限制。虚拟化的目的是最大化地利用计算能力和数据储存等计算机资源，用户访问和使用这些虚拟化的资源不再受制于现有资源的架设方式、地域或物理组态，实现比原本组态更好方式的存取。并且根据对虚拟化的程度又可分为全虚拟化和半虚拟化，全虚拟化是几乎整个系统的所有硬件都是虚拟的，操作系统或者其他软件不需要修改就可以运行在这个虚拟环境下。半虚拟化不对所有硬件进行虚拟化，需要对软件做一些修改才能运行在虚拟环境下。半虚拟化没有虚拟硬件环境，而是将客户程序运行在一个单独的隔离域中，就像是运行在一个单独系统。

结合对虚拟化技术的简单论述，从实现结构来看，vTPM 一般也包括两种: 全虚拟化和半虚拟化结构。全虚拟化以软件的形式提供非常接近硬件 TPM 的函数功能和接口。半虚拟化方式则需要修改 vTPM 到 TPM 的访问接口或直接修改底层 TPM 硬件功能来完成,如文献。全虚拟化也存在两种方式，一种是对硬件 TPM 的虚拟化，另一种是使用开源项目对 TPM 功能进行仿真。通过虚拟 TPM 管理工具(vTPMManager)为每一个虚拟域提供单独的仿真 TPM 程序"这样既可以提高运算效率,又可以使得不同的虚拟域之间彼此隔离,进行各自独立的可信计算"但是需要注意的是必须保证仿真 TPM 程序的安全。硬件 TPM 的虚拟化，是通过虚拟化技术对物理 TPM 虚拟成多个 TPM，根据虚拟机对 TPM 的需求分配给不同的虚拟机。而另使用开源项目对 TPM 仿真则是完全在可信虚拟平台上使用软件模拟的 TPM 功能，比如 TPM_Emulator，这种方式不需要硬件 TPM 的支持，在使用上比较灵活，但是缺乏了硬件 TPM 的保护执行，必需有严格的保护机制来保障这种全虚拟化 vTPM 的运行。全虚拟化和半虚拟化在向平台上的虚拟机提供 TPM 功能时都存在各自的优点和不足，比如针对 TPM 功能的密钥管理方面, 全虚拟化方式为了提高 vTPM 密钥生成效率采用软件方式，但这种密钥层次得不到硬件 TPM 的保护执行，半虚拟化的方式能解决这个问题，但需要修改硬件 TPM, 比如增加特权级别。如何合理的衡量全虚拟化和半虚拟化结构的优点和不足来实现 vTPM 是研究者应该重视的一个问题。

2.3 vTPM 基本要求

TCG 的 TPM 设计在总体上是很成功的。它体现了 TCG 以硬件芯片增强计算平台安全的基本思想，为可信计算平台提供了信任根。TPM 以密码技术支持了 TCG 的可信度量、存储!步及告功能，为用户提供确保平台系统资源完整性、数据安全存储和平台远程证明。TPM 作为可信平台的信任根，有丰富的计算资源和密码资源，TPM 在设计时应该满足一下要求[8][9]：

1 完整性度量，保证使用该芯片的机器，从启动开始的每个操作都具有完整的验证机制，防止黑客或者病毒篡改系统信息；

2 敏感数据加密存储与封装，将敏感数据存储在芯片中的屏蔽区，用户数据通过硬件级加密存储到外部设备，防止数据被窃取；

3 身份认证功能，硬件级的用户身份标识，秘钥和硬件的绑定实现身份确认，防止伪装攻击的发生；

4 内部资源授权访问，通过 TPM 的授权协议能够方便地实现用户对其资源设置访问权限，在保证安全性的情况下实现资源的便捷共享；

5 数据加密传输，能够在与外界进行通信时，加密通信链路上的数据，防止监听、篡改或者窃取。

而基于 TPM 进行设计的 vTPM 在安全性、可靠性等要求方面都应该保证最基本的 TPM 安全要求。vTPM 应该满足 TPM 的一些基本要求，区别在于 TPM 针对于可信物理平台，而 vTPM 则是针对于虚拟化环境中的用户虚拟机。vTPM 还应该针对独特的虚拟化环境拥有自身的安全性、可靠性等要求。并且虚拟 TPM 必须可使平台上的每个虚拟机都可利用其功能，让每个需要 TPM 功能的虚拟机都感觉是在访问自己私有的 TPM 一样。一般来说，一个平台只有一个硬件 TPM，而虚拟机的 TPM 的个数远远多于系统里的物理 TPM 个数，因此这就须要创建多个虚拟 TPM 实例，每一个都要如实地仿效硬件 TPM 的功能。vTPM 要为每一个在 VMM 上运行的虚拟机提供 TPM 服务[10][11]。

作为云环境中提供可信功能的重要部件，vTPM 架构必须适应云服务的需求，充分保证云计算环境的可信。鉴于虚拟化的特性，vTPM 的设计不仅实现物理 TPM 在虚拟化环境中的功能体现，更重要的是实现物理 TPM 在虚拟化中的属性体现，即安全存储属性、可信身份属性、信任传递属性。特别地，在虚拟化环境中，由于虚拟机的可迁移性，vTPM 在迁移时的这些安全属性必须依然能够保持，并在目标平台重新建立信任链。结合可信计算组织 TCG 的对最新 TPM 的相关定义，在设计 vTPM 架构时，解决在安全属性和迁移过程变化后出现的问题，也应该保证以下几个要求：

首先针对平台使用者[1]：

1 平台适用性。在设计 vTPM 架构时，应该适用于不同的操作系统平台，使 vTPM 架构可以保证不同种类操作系统的安全。

2 方便用户使用。在云计算环境的虚拟机主机的使用者可以方便的使用 vTPM 的相应功能。

3 方便开发者维护。vTPM 架构设计应该考虑开源代码的要求，是开发者在使用 vTPM 进行功能使用时，可以自由高效的选择 vTPM 的部署方式。

并且在向虚拟机提供 TPM 功能上 vTPM 应该有以下基本的功能要求：

1 一个 vTPM 必须为在虚拟机上运行的操作系统提供使用模型和 TPM 命令集，就像硬件 TPM 为其上操作系统提供的同样的模型和命令集；

2 虚拟机和它的 vTPM 之间的联系，必须在虚拟机的整个生命周期中都保持着，这包括虚拟机连同与之关联的 vTPM 一并从一个物理机转移到另一个机器的情况，最重要的是保证虚拟机与 vTPM 实例一一对应的关系，并且在虚拟机运行过程中只能被允许访问自身的 vTPM 实例；

3 vTPM 和它下面的可信计算基（Trusted Computing Base）之间必须保持紧密联系，并且与硬件 TPM 清晰可分。

在针对与保护系统安全方面，结合文献[KVM][11]等学者给出的 vTPM 设计的要求，可以包括一下几个方面：

1 从数据安全存储而言，vTPM 的密钥及非易失性数据受物理 TPM 保护存储，不可被未授权实体访问；

2 从虚拟机可信身份而言，vTPM 的身份证书提供虚拟机的真实身份证明，建立从物理平台到虚拟机的信任链；

3 在虚拟机的远程证明方面，vTPM 基于 2 为虚拟机的完整性提供远程证明，

根据验证
方的需要可通过映射物理 PCR 到 vPCR 从而提供深度远程证明；

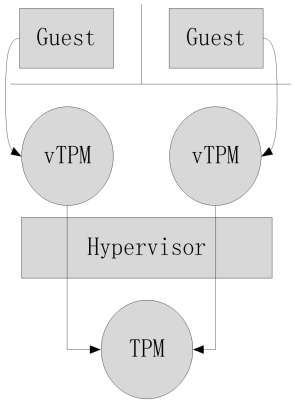
4 从 vTPM 迁移而言，合理迁移 vTPM 中的密钥，降低密钥重新生成的开销，保证迁移过程中 vTPM 的机密性和完整性，并保证迁移后密钥和非易失性数据的可用性；

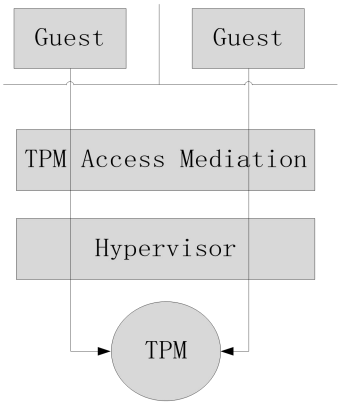
5 可以从物理 TPM 实现对虚拟机的信任链扩展，利用信任链技术保证虚拟机的完整性度量；

6 保证虚拟机的操作系统状态受到 TPM 的保护，防止操作系统被修改；并且保证虚拟机中软件的安装、卸载、运行等需要得到用户授权；监控 Dom0 和管理员对虚拟机的内存访问，防止虚拟机内存数据被获取。

3. vTPM 体系架构研究进展

本文对于 vTPM 体系结构，国内外学者研究都较多。目前大部分研究成果均来自于开源的 VMM——Xen[12][13][14]。按照 vTPM 与客户虚拟机和 TPM 绑定的紧密程度，本文将 vTPM 归纳为三类：其一是“松耦合型 vTPM”，即客户虚拟机与 vTPM 和 TPM 之间采用 Split I/O 技术[15]进行绑定。其模型如图 2。其二是“紧密耦合型 vTPM”，即客户虚拟机与 vTPM 和 TPM 之间采用 Direct I/O 技术[16][17]进行绑定。这类 vTPM 只是 TPM 逻辑上的概念，即各个客户虚拟机 I/O 通过直接陷入 VMM 并通过物理驱动共享 TPM，逻辑上的 vTPM 实际上就是 TPM。其模型如图 3 所示。其三是“半紧密耦合型 vTPM”, 即客户虚拟机与 vTPM 和 TPM 之间可采用 Direct I/O 技术或 Passthrough I/O 技术[18]进行绑定，并在 TPM 内部构建出多个 vTPM，使其能提供对多客户虚拟机的支持，每个虚拟机执行时使用各自的 guestTPM 上下文，该上下文随虚拟机的切换而切换。其模型图 4 如所示。





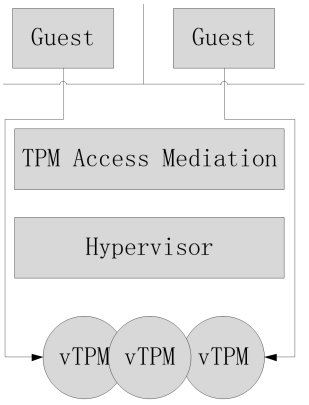


图 2 松耦合 vTPM　图 3 紧密耦合 vTPM　图 4 半紧密耦合 vTPM

3.1 松耦合型 vTPM

本文对于松耦合型 vTPM，其典型代表是文献[18]在 Xen 平台上提出的 vTPM。如图 5 右所示。从图 5 右可以看出，一方面，vTPM 借助于 Xen 的 Xenbus 和设备 I/O 环机制[14]，通过前端虚拟驱动（安装在客户虚拟机）和后端虚拟驱动（安装在管理域 Dom0）与客户虚拟机绑定。另一方面，vTPM 借助于 Xen 的安全硬件接口，通过 vTPM Manager 和设备驱动程序与 TPM 绑定。这种松耦合型 vTPM 方案的优点是：①对 Xen 的修改小。vTPM 与 TPM 和客户虚拟机之间通信仅仅依靠 Xen 现有的消息传递机制，不需要增加额外的代价。②vTPM 与 TPM 之间的是松耦合关系，方便迁移。vTPM 与 TPM 之间仅存在 PCR 映射、证书链传递等关系，而 vTPM 的状态、密钥层次结构以及 vTPM 与应用程序之间的 Session

状态等均与 TPM 无关；③可以用全软件方式实现，灵活地向用户提供接口或服务。但主要缺点是：① vTPM 是一个软件，无法具有硬件 TPM 一样的抗攻击能力；①vTPM 根实例的权限太大，它不仅产生 vTPM 子实例，而且还负责产生不对称密钥、加密、解密以及非对称密钥在 vTPM 之间的迁移；①vTPM 位于管理域中，因此各个 vTPM 的敏感数据均在管理域中，但管理域并不是绝对安全的，这些敏感数据也有可能泄漏；④ 管理域会成为性能的瓶颈，而且多个 vTPM 实例之间可能还会发生相互影响; ⑤信任链较长。其完整的信任链为 TPM→BIOS→VMM→管理域→vTPM 根实例→vTPM 实例→前端虚拟驱动→后端虚拟驱动→……。信任链越长，信任损失可能越严重；⑥vTPM 迁移只支持同构 VMM 平台，对于异构 VMM 平台之间的迁移，目前还没有相关的研究工作。

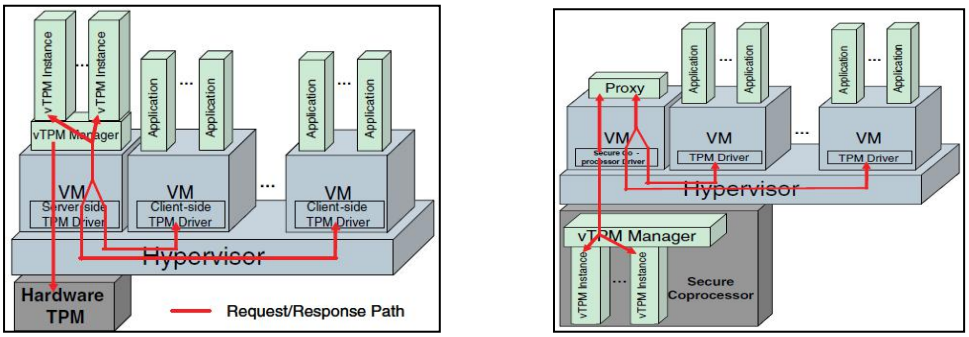


图 5　Xen 上的松耦合型 vTPM 架构

为了解决松耦合型 vTPM 面对的安全和性能问题，文献[18]还提出了该方案的一种变种，如图 4 左所示，其中 vTPM 的功能由一个外部安全协处理器插件提供，它能够在一个容易受攻击的环境中为敏感数据（如私钥）提供最大的安全。文献[19][20]提出了松耦合型 vTPM 单隔离域方案，即 vTPM 运行在一个单独的隔离域，vTPM 的管理程序仍然运行在 Dom0，这种方案可以减轻管理域的性能负担；而文献[21]在 Xen 上实现了双隔离域方案，如图 6 所示，即 vTPM 运行在 DomU-vTPM 域，vTPM 管理程序运行在 DomB 域。这种方案的优点是进一步将原来运行在 Dom0 中的 vTPM 管理器从 Dom0 中分出，进一步减轻管理域的性能负担，降低安全风险，而只需在 Dom0 中的 libxc 库中增加了对 DomB 的管理接口。

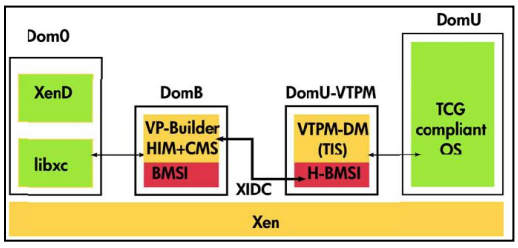


图 6 运行在隔离域的 vTPM 架构

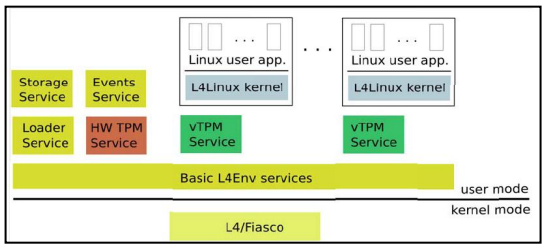


图 7 L4/Fiasco 和 L4Env 环境下的 vTPM

另外，文献[21]还在 L4/Fiasco 和 L4Env 环境下实现了松耦合型 vTPM，其架构如图 6 所示。该方案包括如下组件：HW TPM Service 组件是一个访问硬件 TPM 的服务，vTPM Service 组件是一个基于 TPM emulator 的一个虚拟 TPM 服务，L4 Linux kernel 组件是一个 L4 Linux 虚拟机，Loader Service 组件是一个管理和加载虚拟机和 vTPM 的服务，Storage Service 组件是加载和存储 vTPM 数据的服务。在该方案中，vTPM 实际上是一个构建于 TPM 模拟器上的服务，它作为 L4 的本地任务，其内存与虚拟机内核和 Linux 应用相互隔离。每一个客户虚拟机通过加载 vTPM 驱动程序与 vTPM 绑定。另外，文献[22]提出的 vTPM 架构

与此类似，不同的是 VMM 不同，文献[22]基于 Xen。

3.2 紧密耦合型 vTPM

本文对于“紧密耦合型 vTPM”，其典型代表是文献[23]在 Xen 平台上提出的 TPM 共享方案。逻辑上的 vTPM 实际上就是 TPM。如图 7 所示，在 VMM 中提供了一个能处理客户虚拟机可信请求的中间件平台以及 TPM 的驱动程序。紧密耦合型 vTPM 的主要优点是：①安全性高。该方案 vTPM 的安全性就是 TPM 的安全性；②信任链短。由于该方案的 vTPM 是一个逻辑实体，因此，不会增加额外的长度；③管理域负担轻。管理域除了管理各个 vTPM 的生命周期以外，没有其它额外的开销。这个方案的主要缺点是：①TPM 的负担重。各个客户虚拟机的可信请求最终均由 TPM 处理，大大加重了 TPM 的负担；②对 Xen 的修改大，需要在 VMM 增加中间件平台和 TPM 的驱动程序，使得 VMM 存在漏洞的可能性增加，VMM 的安全性降低；③即使是同种 VMM 之间的迁移也非常困难。由于不同的客户虚拟机分时共享 TPM，每一个客户虚拟机在使用 TPM 功能时涉及的 TPM 内部状态数据、密钥树结构、Session 状态不容易实时跟踪收集。

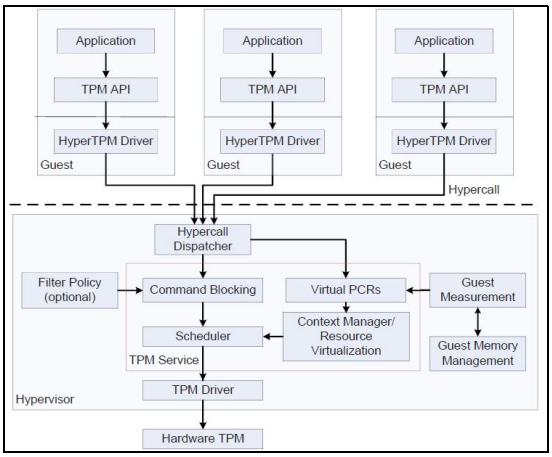


图 7　Xen 上的紧密耦合型 vTPM 架构

3.3 半紧密耦合型 vTPM

本文对于“半紧密耦合型 vTPM”，目前这方面的研究工作并不多，只有文献[24]在相关的命令中进行了简单讨论，但并不具体详细。除此以外，还没有见到相关的研究成果。另外，TCG 组织在 2007 年 8 月正式成立的虚拟平台工作组 TCG VPWG（Virtualized Platform Work Group）的部分工作也涉及到如何在 TPM 内部构建多个 vTPM 使其支持虚拟化的问题，但没有公开相关的解决方案[25]。IT 设备厂商目前只制定了 PCI 设备的设备虚拟化规范[21]，统一了 PCI 设备虚拟化的接口，其中 SR-IOV(Single Root IO Virtualization) [22]即是 PCI 设备虚拟化规范之一，即凡是具有 SR- IOV 功能的设备都能够将一个物理设备虚拟成多个虚拟设备，并能够将每个虚拟设备分给不同的虚拟机使用。但 TPM 不是 PCI 设备，而是一个 LPC 设备，因此，已有的 PCI 设备虚拟化规范不能应用于 TPM 设备的虚拟化。目前，尽管半紧密耦合型 vTPM 到实用还有很多工作要做，但此类 vTPM 与松耦合型 TPM 相比，其优点是：①更安全，所有的状态数据和敏感数据均在硬件 TPM 中，均受 TPM 的保护；②信任链短；不需要前后端的虚拟驱动。与紧密耦合型 vTPM 相比，优点是：①挂起、恢复和迁移方面比较容易；②对 VMM 的改动相对较小。半紧密耦合型 vTPM 的主要缺点是硬件的扩展需要增加额外的成本。

4. 松耦合型 vTPM 体系架构演变

从本文 3 节对三种不同类型 vTPM 架构目前的研究描述来看，松耦合型 vTPM 架构比较适合目前的云计算平台，本文针对云计算虚拟化平台的松耦合型 vTPM 架构，总结了松耦合型 vTPM 架构主要有以下优点：

高扩展：松耦合型 vTPM 架构适应不同的主流虚拟化架构，比如 Xen，KVM 等，云平台提供者可以根部虚拟化架构的不同特点对松耦合型 vTPM 进行改进和设计，虚拟机实体通过调用相应的 vTPM 驱动，对自身进行进行完整性和安全保证；

高便捷：根据松耦合型 vTPM 架构设计的可信云计算环境可以有效的保证虚拟机实体的安全完整性度量。虚拟机实体通过向 vTPM 管理器进行 vTPM 实例使用请求，然后进行 vTPM 实例的使用。这个过程只需要由 vTPM 管理器进行 vTPM 实例的创建和后端驱动的管理，虚拟机实体就可以对 vTPM 的相应功能进行使用，不需要加载太多的模块；

低成本：松耦合型 vTPM 架构对 VMM 修改较小，可以通过较其他两种架构较少的开发成本以及对硬件的扩展。

总体来说，松耦合型 vTPM 架构能更好的保证云计算环境。结合本文 3 节对松耦合型 vTPM 架构的研究来看，目前松耦合型 vTPM 架构在主体架构方向发生了两个主要的变化：一是传统的 vTPM 架构，主要是由 IBM 的 Berger 在文献[2]首先提出，随后的松耦合型 vTPM 架构主要是在此基础上进行功能的扩展。二是对在传统 vTPM 架构的基础结合 TPM2.0 规范发展的一种新型架构，此 vTPM 架构在传统的 vTPM 架构中对 vTPM 管理器和 vTPM 进行分离。

4.1 传统松耦合型 vTPM 架构

结合目前主流虚拟化架构之一的 Xen VMM，并根据经典文献[2]，本文对传统的松耦合型 vTPM 架构的主要运行机制进行描述。在 Xen 中，vTPM 作为一个可选组件为虚拟机实体提供如同物理 TPM 一样的功能服务，并且 vTPM 管理器在特权域 Domain0 中与物理 TPM 直接通信，获取可信计算资源。vTPM 是通过运行在 Domain0 的 TPM 仿真器（TPM_emulator）产生，并且由 vTPM 管理域负责管理每个 vTPM 实例的创建、删除、恢复等操作，并负责建立 vTPM 实例整个生命周期中与虚拟机实体的惟一对应关系。基于 Xen 的可信虚拟平台的设计是以 Xen 虚拟设备的分离驱动机制作为基础，每一个 vTPM 实例都包含一个前端驱动和后端驱动，虚拟机实体通过自身 vTPM 实例前段驱动进行与位于 Domain0 中的后段驱动进行通信。

传统松耦合型 vTPM 架构在 Xen 中具体实现过程分为两个步骤：

第一步：在虚拟机实体启动时，VMM 根据配置信息和 vTPM 相关信息进行 vTPM 的配置工作。具体过程如下：

VMM 通过脚本文件分配新的 vTPM 设备的编号，将其存储在 XenStore 中，并通过管道文件向 vTPM 管理器发送 vTPM 实例的创建指令；

vTPM 的守护进程收到改指令后调用 vTPM 设备软件运行，并将该程序实例与该虚拟域板顶起来，从而成功初始化了该 vTPM 设备。

第二步：vTPM 设备初始化完成后，虚拟机实体可以访问 vTPM 设备。具体过程如下：

当虚拟机需要访问 TPM 设备时，TPM 前段驱动通过事件通道将 TPM 指令发送给 TPM 后端驱动，TPM 后端驱动通过事件通道编号找到相对应的 vTPM 设备标识号，填写请求包，发送给 vTPM 管理器；

vTPM 的 vTPM 后端监听守护进程读取 vTPM 后端驱动传来的指令头部，获得 vTPM 设备标识号，随后读取指令的其他部分并通过与 vTPM 设备标识号对应的管道传递给相应的 vTPM 设备软件；

vTPM 设备从管道文件中读取 TPM 指令信息，解析并处理后，将处理结果中的内容与标识号关联后通过所有 vTPM 设备软件共用的管道软件传回给 vTPM 管理器；

vTPM 管理器将收到的执行结果通过后端和前端驱动返回给虚拟域，实现一次完整的 TPM 操作。

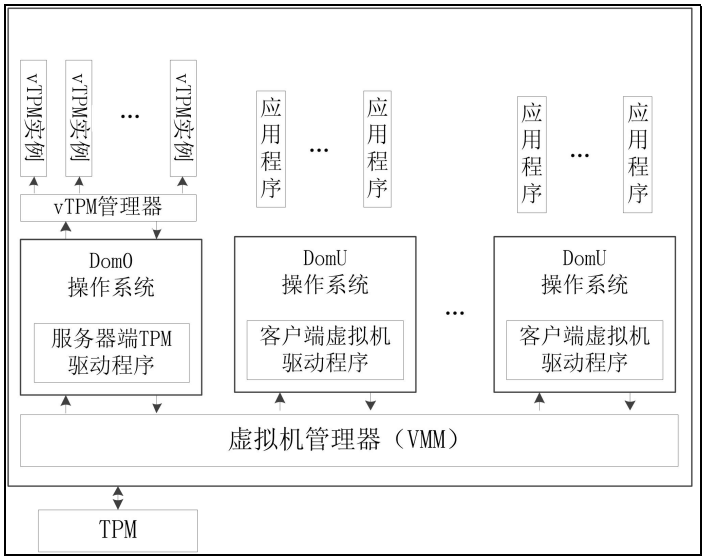


图 8　传统松耦合型 vTPM 架构

4.2 新型松耦合型 vTPM 架构

云计算的不断发展，基于虚拟化平台的 vTPM 会更加方便管理和使用，vTPM 架构会朝着松耦合型方向发展。在 Xen4.6 对基于 TPM2.0 的 vTPM 架构中，vTPM 管理器作为一个单独的域运行在 VMM 之上，在 vTPM 实例创建机制上与传统松耦合型 vTPM 架构创建 vTPM 实例的过程相似，但是此时的 vTPM 实例也被单独生成一个域。这种新型的 vTPM 架构可以减轻虚拟化平台管理域对 vTPM 的管理，把对 vTPM 管理的工作分给独立的 vTPM 管理域，使整个虚拟化平台的完整性和安全性更加得到保证。并且在虚拟机和 vTPM 迁移上，此 vTPM 架构通过 VMM 的迁移机制对 vTPM 实例和对应的虚拟机实现迁移。

新型松耦合型 vTPM 架构在 Xen 的具体实现过程如下三个步骤：

第一步：vTPM 管理域的配置以及启动；

vTPM 管理域可以通过配置文件由 VMM 进行启动，其仅仅使用部分较少的空间和内存。vTPM 管理域管理 vTPM 实例的创建、销毁等，但是虚拟化平台运行期间，只能有一个 vTPM 管理域。并且运行在 VMM 之上的 vTPM 管理域通过调用 TPM2.0 设备驱动接口，对 vTPM 实例域 TPM 功能的请求进行回复。

第二步：vTPM 管理与启动之后，对虚拟机 vTPM 的请求进行监听并创建相应的 vTPM 实例域；

在虚拟机进行请求 vTPM 请求后，vTPM 管理域通过设备标识号进行 vTPM 实例域的重启或者创建，然后提供相应的后端驱动，由虚拟机连接 vTPM 实例域。

第三步：虚拟机进行 vTPM 实例的使用；

虚拟机通过 VMM 提供的 vTPM 前段驱动向 vTPM 域发起功能使用请求。vTPM 实例域通过 vTPM 管理域对 TPM 功能进行使用实现一次完整的 TPM 操作。

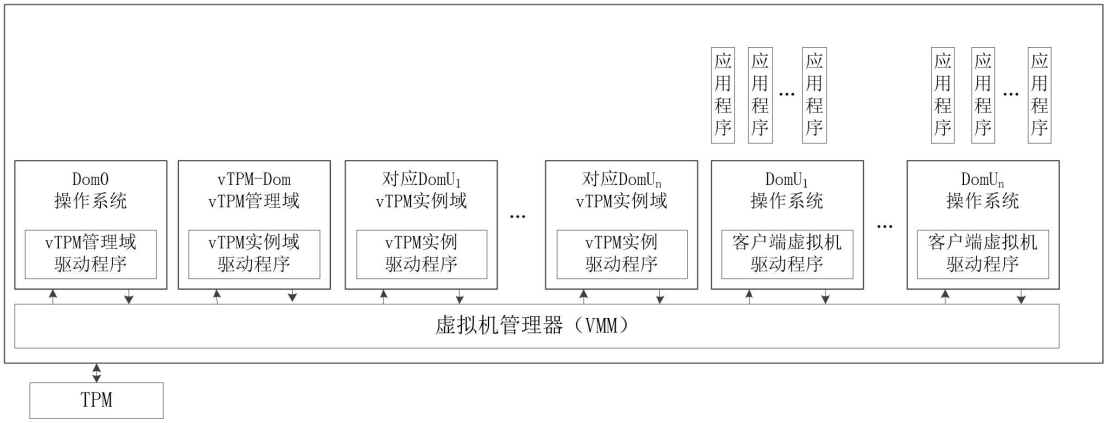


图 9　新型松耦合型 vTPM 架构

5. 问题与挑战

目前的 vTPM 架构研究对解决云计算环境安全是一个重要方向，对于目前的 vTPM 架构，无论是松耦合型 vTPM、紧密松耦合型 vTPM 还是半紧密耦合型 vTPM，均存在不同的优点和缺点。但安全和效率始终是一个很难解决的两难问题；松耦合型 vTPM 效率高但安全性差，紧密松耦合型 vTPM 安全性高但效率差，只有半紧密耦合型 vTPM 安全性高效率也相对较高，但这方面的工作还没有开始。对于目前的云计算环境的发展来看松耦合型 vTPM 架构会在可信计算云计算技术结合的虚拟化平台上有很大的发展空间。目前对松耦合型 vTPM 架构研究的主要方向主要表现在以下方面：

信任链技术是 TPM 一个重要的技术，在 vTPM 架构设计时，如何在保证松耦合性的同时保证对虚拟化平台的完整性度量模型进行设计；

解决 TPM2.0 驱动端口与虚拟化监视器端口的统一；

目前的 vTPM 管理域只能保证一个 vTPM 实例域进行连接，如何使 vTPM 管理域可以连接多个 vTPM 实例的同时并且能保证 TPM 功能使用的完整性和高效率；

解决 vTPM 管理域备份和恢复的问题，目前的新型松耦合型 vTPM 架构规定了只有一个 vTPM 管理域存在虚拟化平台的活动期，一旦 vTPM 管理域出现故障，对 vTPM 实例域以及虚拟机的 TPM 相关功能都会产生影响。

6. 结束语

可信计算与云计算技术的结合可以在一定程度上保证云计算环境的结合，可信平台模块作为可信计算中最为重要的一个模块，它的虚拟化将成为云计算安全领域重要的方向之一，对虚拟可信平台模块架构的研究是十分必要。本文在对目前对 vTPM 架构的研究进行分类和分析，并且对松耦合型 vTPM 架构进行了详细的分析和总结，阐述了在未来对松耦合型 vTPM 架构的研究方向。随着以后对 vTPM 架构的研究的不断深入，可信计算技术与云计算相结合势必会成为云安全研究的一个重要方向。

参考文献

[1]Trusted Computing Group.TCG .https://www.trustedeomputinggroup.org

[2]Trusted Computing Group.TCG 规范列 表.https://www.trustedeomputinggroup.org/specs/

[3]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.

[4]http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=66510

[5]https://www.trustedcomputinggroup.org/work-groups/virtualized-platform/

[6]www.qemu.org

[7]www.vmware.com

[8] Yap J Y,Tomlinson A. Para- virtualizing the trusted plat-form module: An enterprise framework based on version2.0 specification[C]//5th International Conference，IN-TRUST 2013.Berlin: Springer- Verlag， 2013:1- 16.

[9]杨永娇，严飞，毛军鹏，张焕国.Ng- vTPM: 新一代 TPM 虚拟化框架设计[J].武汉大学学报（理学报）.2015:61(2),103-111

[10] Sadeghi A，Stuble C，Winandy M． Property- based TPMvirtualization［C］/ /Proceedings of the 11th International Conference on Information Security，ISC’ 08． Berlin :Springer-Verlag ， 2008:1- 16．

[11] Zhang F，Chen J，Chen H，et al． Cloudvisor: Retrofit-ting protection of virtual machines in multi- tenant cloud with nested virtualization［ C］/ /Proceedings of the Twenty Third ACM Press Symposium on Operating Systems Principles． New York: ACM， 2011: 203- 216

[12]University of Cambridge: "Xen v3.0 - Interface Manual" (2007)

[13] University of Cambrdige: "Xen v3.0 - User's Manual" (2007)

[14]Xensource.Xen Open-Source Hypervisor. http://www.xensource.com/products/downloads[EB/OL], 2012

[15]Paul Barham,Boris Dragovic,Keir Fraser.Xen and the art of virtualization[J]. ACM Press,164-177,2003

[16] D Abramson,J Jackson，S Muthrasanallur,and et a1．Intel Vtmmfization Technology for Directed I/O[J]．1ntell Technology Journal,10(3):87-93,2006

[17] J Sugerman,G.Venkitachalam,and B.-H.Lim.Virtualizing I/O devices on VMware workstation’s hosted virtual machine monitor[C].In Proceedings of the USENIX Annual Technical Conference,88-97,2007

[18] J.Liu,W.Huang,B.Abali,and D.Panda.High performance vmm-bypass i/o in virtual machines[C].In Proceedings of the USENIX Annual Technical Conference, 136-144,2006

[19] Berger, Stefan and Caceres, Ramon and Goldman, Kenneth A. and Perez, Ronald and Sailer, Reiner and van Doorn, Leendert, "vTPM: virtualizing the trusted platform module"[C], in USENIX-SS'06: Proceedings of the 15th conference on USENIX Security Symposium,231-242, 2006

[20] Anderson, Melvin J. and Moffie, Micha and Dalton, Chris I.: " Towards Trustworthy Virtualization Environments: Xen Library OS Security Service Infrast

ructure"[R] , Hewlett-Packard Laboratories, 43-51,l2007
[21] D. Plaquin and M. Nicholes, "Providing trust for management of utility c omputing services"[R], in HP TechCon 2005, April 2005
[22] David Plaquin, Serdar Cabuk, Chris Dalton, Dirk Kuhlmann, Philipp Grete, Carsten Weinhold, Alexander Böttcher,Derek Murray, Theodore Hong,Marcel Wi nandy, TPM Virtualisation Architecture document[R],Open Trusted Computing,20 09
[23] Scarlata, Vincent and Rozas, Carlos and Wiseman, Monty and Grawrock, David and Vishik, Claire: " TPM Virtualization: Building a General Framework "[C] , Trusted Computing(2007), 43-56,2007
[24] Paul England,Jork Loeser,Para-Virtualized TPM Sharing[C],TRUST 2008, 4 968:119-132, 2008
[25]Goldman, K.A., Berger, S.: TPM Main Part 3- IBM Commands,http://domin o.research.ibm.com/[EB/OL],2009
[26]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.
[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, 86(2-3):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]陈亮, 曾荣仁, 李峰,等. 基于无干扰理论的信任链传递模型[J]. 计算机科学, 2016, 43(10):141-144.
[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.
[36]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,2011:07-31.
[37]曲文涛. 虚拟机系统的可信检测与度量[D].上海交通大学,2010:90-117.
[38]CHEN S Y, WEN Y Y,ZHAO H. Formal analysis of secure bootstrap in trusted computing[C]// Proc of the 4th International Conference on Autonomic and Trusted Computing Berlin, Springer, 2007:352-360.
[39]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.
[40]Rushby J. Noninterference, transitivity, and channel-control security policies[M]//

SRI International, Computer Science Laboratory, 1992:01-50.
[41]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.
[42]Paolo Baldan, Alessandro Beggiato. Multilevel Transitive and Intransitive Non-interference, Causally[J]. Theoretical Computer Science, 2018, 706:54-82.
[43]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.
[44]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, 2008, 45(6):974-980.
[45]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[J]. 通信学报, 2009, 30(2):52-58.
[46]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.
[47]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.
[48]秦晰, 常朝稳, 沈昌样, 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.
[49]Smith J, Nair R. Virtual Machines: Versatile Platforms for Systems and Processes (The Morgan Kaufmann Series in Computer Architecture and Design)[M]. Morgan Kaufmann Publishers Inc. 2005.
[50]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.

四、文献阅读及学术交流

阅读文献目录	编 号	文 献 名	著 者 名	源自何处
	1	基于 Xen 的虚拟化访问控制研究综述	柯文浚，董碧丹，高洋	计算机科学
	2	基于 SGX 的虚拟机动态迁移安全增强方法	石源，张焕国，赵波	通信学报
	3	云计算安全: 架构、机制与模型评价	林闯，苏文博，孟坤	计算机学报
	4	云安全研究进展综述	俞能海，郝卓，徐甲甲	电子学报
	5	Security in cloud computing :opportunities and challenges	Ali M, Khan S U, Vasilakos A V.	Information Science
	6	可信 3.0 战略: 可信计算的革命性演变	沈昌祥，张大伟，刘吉强	中国工程科学
	7	虚拟可信平台模块动态信任扩展方法	余发江，陈列，张焕国	软件学报
	8	中国信通院-研究成果-权威发布-专题报告	中国信息通信研究院	中国信息通信研究院
	9	2017 年全球云计算安全报告	McAfee	McAfee
	10	可信系统信任链研究综述	徐明迪，张焕国，张帆，杨连嘉	电子学报
	11	基于信任扩展的可信虚拟执行环境构建方法研究	王丽娜，高汉军，余荣威	通信学报
	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
	13	混合云服务安全若干理论与关键技术研究	朱智强	武汉大学
	14	虚拟机系统的可信检测与度量	曲文涛	上海交通大学
	15	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

听参取加学学术术报会告议记汇录报	编 号	会议或报告名称	举办地和主讲人	见 证 人
	1	Spark 技术及案例及经验分享	成龙校区第一实验楼西 204、李勤	黎静
	2	前端开发新技术	成龙校区第一实验楼西 204、朱洲森 教授	黎静
	3	基于模型的系统工程(Model-Based Systems Engineering)	成龙校区第一实验楼西 204、雷勇	黎静
	4	虚拟化与云计算环境下的互联网系统架构	成龙校区第一实验楼西 204、朱珠	黎静
	5	研究生学术资源信息获取方法	校史馆学术报告厅、赖朝新	黎静
	6	Web 应用安全风险及应对方案	成龙校区第一实验楼西 204、李小俊	黎静
	7	Scrum 敏捷开发技术	成龙校区第一实验楼西 204、李林	黎静
	8	企业系统架构模式设计	成龙校区第一实验楼西 204、杨川	黎静
	9	面向海量数据存储的编码研究	成龙校区第一实验楼西 204、唐小虎教授	黎静
	10	New Computational Methods for Criminal and Victim Identification and Forensic Investigation	成龙校区第一实验楼西 204、Kong Wai Kin Adams	黎静

主讲学术报告记录	在本栏逐一列举本人所主讲学术报告名称、主要内容、报告地、听众范围等。 1、《一种具有瀑布特征的可信虚拟平台信任链模型及分析方法》； 主要内容为向计算机专业以及相关专业学生和导师对硕士期间的工作进行报告，及云计算技术、云计算安全、可信计算技术、当前可信虚拟平台模型（TVP）及信任链模型、TVP 及信任链模型相关研究工作、目前 TVP 及信任链模型的不足之处；论文的创新点以及所作的主要研究工作；.具有瀑布特征的可信虚拟平台（TVP-QT）及其信任链模型、TVP-QT 优点；.TVP-QT/TVP-MCSD 实例系统、实验结果、实验分析；云计算环境下可信虚拟平台的研究结论及展望。 报告地：第一实验楼西 204； 听众范围：计算机科学学院计算机方向研究生以及其他相关方向本科生、研究生。 2、《云计算环境下可信虚拟平台模型》； 主要内容为：云计算技术、云计算安全、可信计算技术、当前可信虚拟平台模型（TVP）及信任链模型、TVP 及信任链模型相关研究工作、目前 TVP 及信任链模型的不足之处；论文的创新点以及所作的主要研究工作；.具有瀑布特征的可信虚拟平台（TVP-QT）及其信任链模型、TVP-QT 优点；.TVP-QT/TVP-MCSD 实例系统、实验结果、实验分析；云计算环境下可信虚拟平台的研究结论及展望。 报告地：第一实验楼西 204； 听众范围：计算机科学学院计算机方向研究生以及其他相关方向本科生、研究生。