一种应用于对等网络的可信片上 Agent 模型

徐小龙,程春玲,陈丹伟,熊婧夷
(南京邮电大学 计算机学院,江苏 南京 210003)

摘 要:提出一种可信片上 Agent 模型(T-AoC),它用于开放的、不安全的、面向网络边缘节点的对等网络环境中。为了有效保护应用 Agent 计算的系统中的 Agent 不被恶意 Agent 执行环境及 Peer 主机对 Agent 的攻击,T-AoC 模型采用集成芯片作为硬件基础为 Agent 提供安全、可靠的执行环境。该芯片可安装在各需要运行 Agent 及其应用系统的对等网络节点主机上。基于信任关系转移的思想,增强对等网络节点之间的可信性,更有效地构建各种安全、可靠的基于 Agent 的 P2P 应用系统。具体描述了 T-AoC 模型的层次架构、工作原理和运行流程,以及 T-AoC 在 P2P 网络信息搜索系统的应用示范,分析了 T-AoC 的性能特点。

关键词:对等网络; Agent; 芯片; 片上系统; 安全
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2010)09-0140-05

Research on Model of Trusted Agent-on-Chip for P2P Networks

XU Xiao-long, CHENG Chun-ling, CHEN Dan-wei, XIONG Jing-yi
(College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: A Trusted Agent-on-Chip model (T-AoC) is presented in this paper, which could be used in open, insecure Peer-to-Peer network computing environment make up of edge nodes of Internet. In order to effectively protect Agents in the Agent application systems from attacks of malicious Agent execution environments and hosts, T-AoC model adopts the integrated chip as the hardware foundation to provide a safe and reliable execution environment for Agent. The chip can be installed in the host of peers needing to run Agent-based systems. Based on the idea of trust relation transfer, the credibility of peer is enhanced, and it is more efficient to build a variety of safe and reliable Agent-based P2P applications. This paper describes the architecture, working principle and operation process of T-AoC model in detail, as well as how to deploy T-AoC in the P2P network information search system demo. The performance analysis of T-AoC is presented at the end of this paper.

Key words: peer-to-peer networks; Agent; chip; system-on-chip; security

0 引 言

对等计算技术[1-4](Peer-to-Peer computing,简称 P2P)的思想改变 Internet 原来的 C/S 计算(Client/Server Computing,客户/服务器计算)或是 B/S 计算(Brower/Server Computing,浏览器/服务器计算)这样不对称的计算模式,重点关注基于 Internet 的边缘节点;网络中对等节点(Peer)地位对等,可以同时成为服务的使用者和提供者,这为大规模的信息共享、直接通信和协同工作提供了灵活的、可扩展的计算平台。

Agent(智能主体)技术[5-8]是适用于软件、硬件或是软硬件环境的新型计算技术,最常见的是用于网络计算系统的软件平台的构建。应用 Agent 技术可以使系统更具有智能性、灵活性、鲁棒性,网络系统中的计算节点的通信能力、交互能力和协作能力也可以得到有效的增强。

Agent 技术和 P2P 网络技术相结合,利用 P2P 的网络自组织等能力允许数量庞大的机器之间相互连接从而形成一个大规模的分布式系统,利用 Agent 来封装对等网络每个节点上的"应用层"软件系统,使系统具有 Agent 的优良特征,从而有效地构建各种新型的大规模分布式网络软件系统。驻留在不同对等节点上的 Agent 可以协作、迁移。对等节点在协同工作的时候,所有与协调、协作和协商的工作全部由 Agent 完

收稿日期:2010-01-02;**修回日期**:2010-04-07
基金项目:教育部博士点基金(20093223120001);江苏省科技支撑计划(BE2009158);江苏省高校自然科学研究项目(09KJB520010);教育部专项研究课题(2009117)
作者简介:徐小龙(1977-),男,副教授,博士,研究方向为计算机软件、分布式计算、Agent 技术和信息安全等。

成。P2P 网络系统应用层所包含的功能组件可以由移动 Agent 按需动态携带、迁移并部署到目的节点上。功能组件可由任务的发起者来制作和发行,以切实达到任务的发起者所要求的效果和目标。

在开放的、不安全的、由难以控制的网络边缘节点构成的 P2P 网络[9,10]中应用 Agent 技术会导致以下的安全问题[11~14]:传输过程中的 Agent 受到恶意 Peer 的攻击;恶意 Agent 执行环境及 Peer 主机攻击迁移到本地的 Agent;恶意的移动 Agent 攻击 Peer 的主机系统。其中,现有的用于保护网络中传输的数据和代码的信息安全技术已经比较成熟,可以有效地包含传输中的 Agent 的代码和数据;包含病毒防御系统在内的本地计算机主机系统实时保护的软件系统所采用的身份认证、访问控制也可以有效地包含 Peer 的主机系统,此外,sandbox(沙盒)技术和安全证明码等新技术也可以进一步增强对恶意 Agent 中的有害代码的防御能力。

而这样的系统的安全危险在于恶意的 Peer 节点可能会攻击 Agent 的代码和数据,这样的问题是比较难以解决的。Peer 节点在接受异地迁移来的 Agent 时,将有可能完全控制 Agent 的执行,Agent 在 Peer 系统里面被执行时,恶意的 Peer 将会窥探和获取 Agent 的代码和数据。针对这一情况,文中的核心重点就是要避免恶意 Peer 攻击移动 Agent。

文中提供一种可信片上 Agent 模型(Trusted Agent-on-Chip, T-AoC)。T-AoC 汲取了 SoC(System-on-a-chip,片上系统)的思想,利用单个微电子集成芯片作为系统的硬件基础平台。P2P 网络中的每个 Peer 都配备 T-AoC 芯片,作为 Agent 的运行空间,在开放的、不安全的 P2P 网络计算环境中构建一个安全、可靠的 Agent 执行环境,从而为基于 T-AoC 的网络应用系统提供一个基础的软、硬件平台。

1　恶意 Peer 攻击分析

在 P2P 网络中,Agent 从一个 Peer 迁移到另一个 Peer 节点上运行时,Agent 的程序将不得不暴露在 Peer 的主机系统中。如果该 Peer 是恶意节点的,就会窥探并截获该 Agent 的程序,并进行一系列恶意的行为,包括[11~14]:

(1)恶意 Peer 对该 Agent 实施拒绝服务攻击(DoS,Denial of Service),甚至可以破坏 Agent 的完整性;

(2)移动 Agent 所携带的私密信息或是迁移过程中获得数据信息在迁移到恶意 Peer 时被窃取;

(3)移动 Agent 包含的数据信息被恶意 Peer 篡改,其完整性被破坏;

(4)恶意 Peer 截获 Agent 程序后,将其修改成恶意 Agent,其代码在 Agent 迁移到其他 Peer 或是返回源 Peer 时将会实施一些具有相当破坏力的行为。

Peer 必须访问 Agent 代码和数据在其主机系统中执行它,因此很难完全防御上述的恶意行为,即异地全面地保护 Agent 进的程序或数据。目前的解决措施还是沿用传统的网络信息安全的技术、机制、模型和方案来负责保护 Agent 的私密性、完整性,并在 Peer 被篡改时能够及时发现恶意行为,并实施后续的相关措施。但是显然,对于移动 Agent 这种新型网络计算技术而言,这种做法是不够的,其安全性能难以达到可信计算系统的要求。

2　可信片上 Agent 模型 T-AoC

2.1　T-AoC 模型层次结构

T-AoC 模型的核心思想是采用高安全性、高性价比的软、硬件平台对移动 Agent 的安全运行进行有效的保护。文中提出的做法是在每一个 Peer 节点上安装 T-AoC 芯片,该芯片是移动 Agent 的可信硬件执行环境。

T-AoC 芯片内设有 Agent 执行环境,移动 Agent 可以在该平台上运行,并完成需要完成的任务。T-AoC 芯片事实上起到了一举两得的效果,既可以保护主机,又可以保护迁移到该节点的 Agent。首先,在保护迁移到该节点的 Agent 方面,改变了 Agent 的运行地点,T-AoC 芯片成为 Agent 的新的、安全的运行环境。Peer 主机通过专用或通用的标准化接口和设备与 T-AoC 芯片连接通信,T-AoC 芯片内的程序、数据和运行情况是无法被 Peer 的主机系统获得的。Peer 主机不必一定设置 Agent 的服务设施,即 T-AoC 芯片可以成为唯一的 Agent 环境。当然,T-AoC 芯片仍然需要与 Peer 主机进行通信,如传递消息等。可见,T-AoC 芯片可以有效地保障 Agent 的安全。

文中采用 T-AoC 作为 Agent 安全、可信赖的软、硬件运行平台,即在 T-AoC 上实现全部的 Agent 及其服务设施。如图 1 所示,T-AoC 系统的整体软、硬件体系架构基于分层的思想从上至下包括 Agent 和 Agent 服务设施等 5 个层次:

(1)T-AoC 最上层是 Agent 及 Agent 服务设施,Peer 节点在收到迁移到本地的 Agent 时,立即通过标准通信接口将 Agent 传输到 T-AoC 中,并在 Agent 服务设施中运行。如果 Agent 采用了加密和数字签名等安全技术,Agent 服务设施还需提供相应的加解密和验证等服务,同时保证运行于同一 Agent 服务设施中

的多个 Agent 在自己的空间内的相互独立的运行。

(2)编程功能类库提供实现各种任务的基于 Agent 的应用系统所需的功能类,类库中的类根据需要添加、修改和升级。

(3)嵌入式操作系统运行在 T-AoC 芯片的硬件平台上,可选择采用和按需裁剪嵌入式 Linux 等片上操作系统,本方案中采用嵌入式 Linux 系统,来控制 Agent 和系统的运行和管理 T-AoC 的软、硬件资源。

(4)底层是包含处理器、存储设备、接口部件、通信模块和周边电路的半导体芯片,实现了最基础的计算、存储和通信功能。

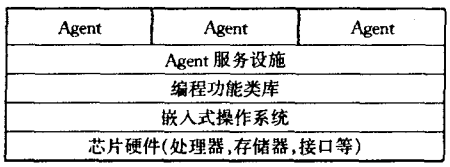

图 1 T-AoC 技术的层次架构图

2.2 基于 T-AoC 的 Agent 保护原理

如图 2 所示,在应用 Agent 的基于集中式或半分布式网络拓扑 P2P 网络系统中,每个 Peer 既充当 Agent 接收节点(Agent Receiver,AR)又是 Agent 的发送节点(Agent Sender,AS),可在其所属的 Super Peer(超级节点)充当的 Proxy 注册主机名称和网络地址、安全需求和 T-AoC 的制造商(T-AoC Manufacturer,T-AoCM)颁发的数字证书。

这些信息用于为 AS 定位 AR。T 是一个设备制造商,它生产 T-AoC 设备。T-AoCM 证书里包含下列信息:

(T-AoC 制造商,T-AoC 类型、T-AoC 提供的安全策略,T-AoC 公钥)

Peer 主机利用拥有的 T-AoCM 公钥副本来验证 T-AoCM 颁发的数字证书。T-AoC 利用负责加密的协处理器来产生密钥以保证私钥不被任何人窥探。

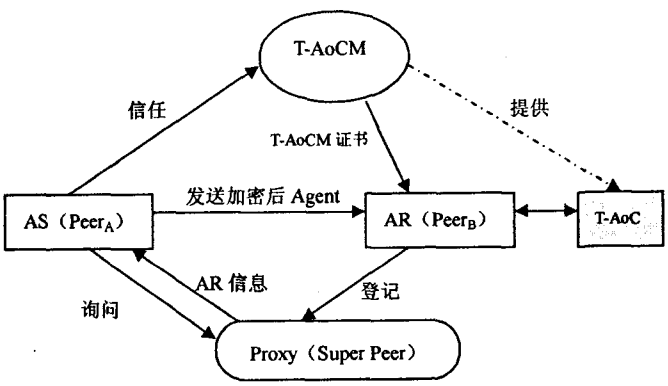

图 2 基于 T-AoC 技术的 Agent 保护原理图

如果 T-AoCM 拥有获得广泛认可的好的信誉,并获得 P2P 网络中 Peer 的信任,即 Peer 相信 T-AoCM 会正确地设计生产此类设备,Peer 的所有者购买 T-AoC 并获得相应的数字证书。Peer 就可以派 Agent 前往其它拥有 T-AoC 设备的 Peer[14]。

基于 T-AoC 设备制造商被广大的 Peer 所有者信任,获得 T-AoC 的 Peer 构成了安全、可信的 P2P 网络,在这样的网络中,所有拥有 T-AoC 的 Peer 进行基于 Agent 的合作,即用 Peer 对 T-AoCM 的信任取代了 Peer 之间的信任关系[14],T-AoCM 可以实现完备的 T-AoC 安全解决方案,易于管理、信誉良好(可由权威机构监管或是专家监控),与 T-AoC 设备购买者利益独立。

2.3 T-AoC 工作流程

T-AoC 按照以下的流程[14]来运作:

(1)作为 Agent 发送者(Agent Sender, AS)向代理(Proxy)提交 Agent 接收者(Agent Receiver, AR)的标识等信息,获得 T-AoCM 证书等必需信息;

(2)Agent 发送者用证书副本公钥验证数字证书,若成功,则进行下一步;否则就不会将 Agent 发送给该接收者;

(3)Agent 发送者需要验证该 Agent 接收者的安全策略是否符合其需求,若不符合,就不会将 Agent 发送给该接收者;若符合,用 Agent 接收者的 T-AoC 的证书公钥,通过加密和消息摘要等技术来保证 Agent 不被 Agent 接收者窥探,完整性也不被破坏;

(4)Agent 接收者接受到达的 Agent,将它输入 T-AoC;

(5)Agent 接收者拥有的 T-AoC 系统首先检验 Agent 是否被篡改或破坏,若是则丢弃不执行,否则解密此 Agent;

(6)运行完成后,T-AoC 采用同上方法获取后续 Agent 接收者的数字证书,并加密 Agent 的代码、数据及执行结果;

(7)T-AoC 将加密后的 Agent 传给 Agent 接收者,Agent 接收者将 Agent 迁移至后续 Agent 接收者或返回至 Agent 源节点。

完整的 T-AoC 工作、部署原理即运行流程如图 3 所示。

2.4 T-AoC 应用示范

下面介绍 T-AoC 在 P2P 网络信息搜索系统的应用示范,网络架构模型如图 4 所示。P2P 网络信息搜索系统允许 Peer 向其它 Peer 查询其所需要的信息,信息分为两种,一种是免费共享的信息,一种是需要付费购买的信息,下面的示范仅限于假设 Peer 都希望获益,即提供需要付费购买的信息,付费的方式采用虚拟的网络电子货币的方式。

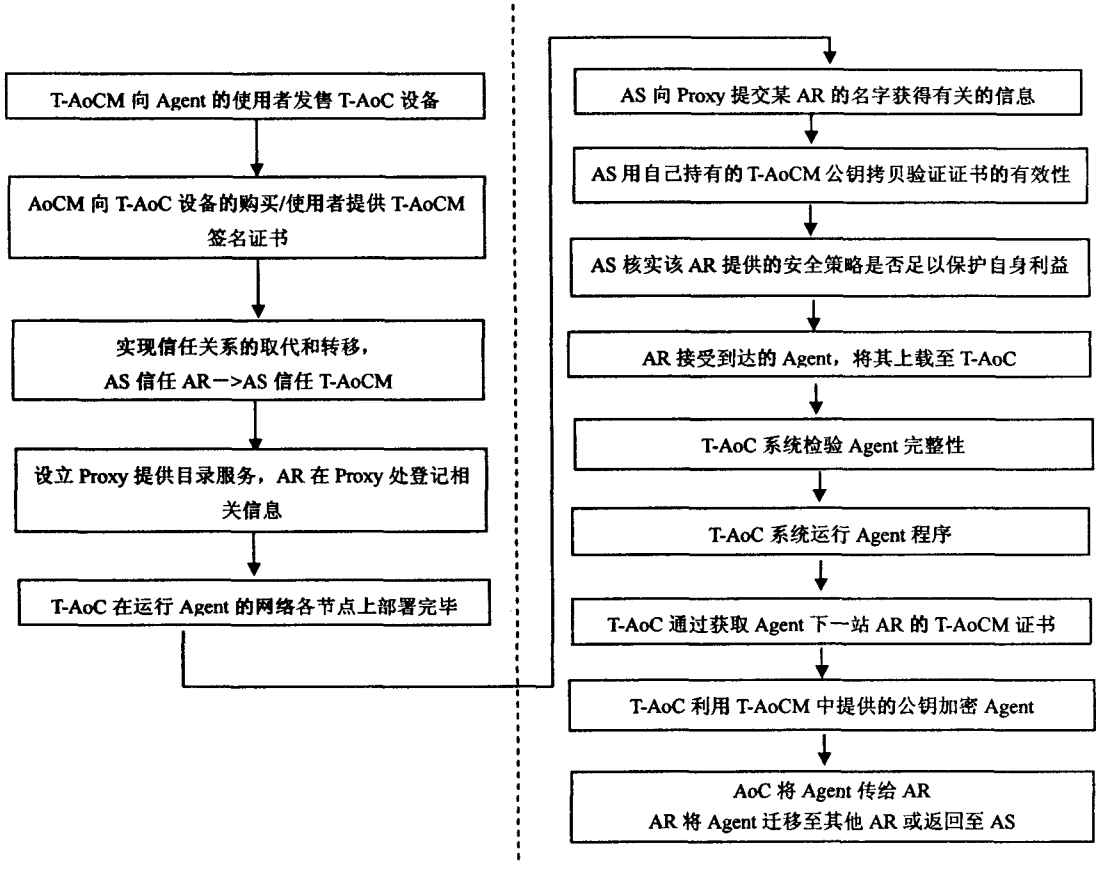

图 3　T－AoC 工作、部署原理即运行流程图

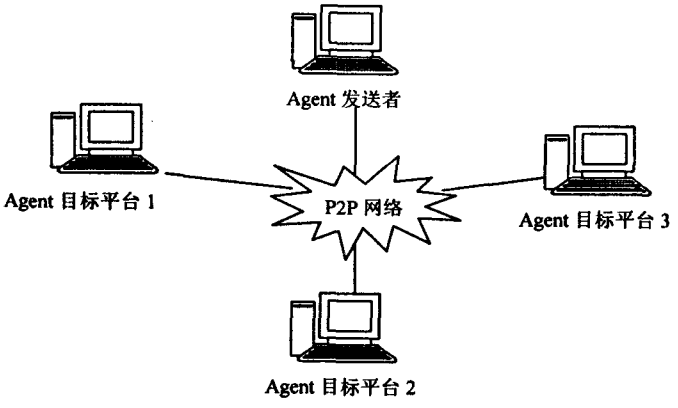

图 4　示范系统的网络架构

网络环境中设置有四个 Peer,均运行两个 Agent 执行环境,一个为主机 Agent 执行环境,一个为 T－AoC 执行环境。其中一个 Peer 为 Agent 发起端,并根据用户关于信息的请求,定制和派遣 Agent。另三个 Peer 的主机 Agent 执行环境为异地迁移来的 Agent 的首要"落脚点"。

作为 Agent 发送者的 Peer 派遣的 Agent 到达其它 Peer 后,查询符合 Agent 发送者请求的信息。如果用户的请求服务类型为"查询是否拥有信息以及获取该信息支付的费用多少",交易成功的话,携带查询结果迁移到后续的节点继续搜寻;如果用户的目的是购买,则还需进行相应的支付行为,并将信息资料提取并发送给 Agent 发送者。如果没有符合条件的信息,Agent 根据自己路由机制,迁移到下一 Peer。其中,涉及到用户的信用卡帐户等私密信息的购买 Agent 必须用 T－AoC 公钥加密对之进行加密,并将之送入 T－AoC 执行。

3　T－AoC 性能分析

下面从 5 个方面对 T－AoC 的性能特点进行分析:

(1)安全可靠性。

T－AoC 是一个封闭的系统,主机对 T－AoC 的攻击是困难的,在 T－AoC 运行的 Agent 的安全性因此也得以有效的保障。

(2)平台独立性。

Agent 运行在 T－AoC 中,Peer 主机采用的硬件平台(如采用 Wintel 架构的计算机和苹果电脑等)、操作系统可以是异构的,与 T－AoC 提供的 Agent 的服务设施无关。另外底层芯片种类可以一样也可以不同,Agent 的服务设施也独立于底层的硬件基础。

(3)功能多样性。

Agent 可包含实现多种多样功能的程序和数据,

因此 T－AoC 的功能也得以扩展。通过将迁移到本地的各种不同功能 Agent 输入到 T－AoC，意味着增强了 T－AoC 的功能，响应不断变化的需求，同时实现系统升级。

(4)通用兼容性。

T－AoC 技术应遵循本技术领域通行的国际标准，这样归属于不同开发商和所有者的 Agent 和 T－AoC 系统可以互相兼容，实现顺畅的交互与交易，从而具有广泛适用性。

4 结束语

目前新的网络应用需求和应用模式不断涌现，呈现出更加多样和灵活的特征，P2P 网络计算技术和 Agent 技术的融合正符合了这种需求和趋势。然而 P2P 网络计算环境的动态性、异构性、自治性、分布性、开放性以及去中心化等特征使得由来自于不同自治管理域的节点构成的网络本身存在严重的可信性(Creditability)隐患，为 Agent 在 P2P 网络中的应用带来了严重的障碍。恶意节点行为对计算环境的可信性和正常运行构成严重威胁，Agent 容易受到恶意节点主机的攻击，文中针对这种情况提出了 T－AoC 模型，基于信任关系转移的思想来构建可信的 Agent 运行环境。T－AoC 模型与技术对于其它开放的、跨组织和管理域的无中心网络计算环境(如网格计算等)的软件系统的构造和运行也具有良好的参考价值和应用前景。

参考文献：

[1] 陈贵海.对等网络:结构、应用与设计[M].北京：清华大学出版社，2007.

[2] Ripeanu M,Foster I,Iamnitchi A. Mapping the Gnutella network: properties of large－scale Peer－to－Peer Systems and implications for system design[J]. IEEE Internet Computing, 2002,6(1):50－57.

[3] 黄新力. 基于复杂网络理论的对等计算系统关键技术研究[D].上海:上海交通大学,2006.

[4] Chang F, Dean J, Ghemawat S,et al. Bigtable: A distributed storage system for structured data[C]//In: Proc. of the 7th USENIX Symp. on Operating Systems Design and Implementation. Berkeley: USENIX Association,2006:205－218.

[5] FIPA. FIPA abstract architecture specification [EB/OL]. 2008. http://www. fipa. org/specs/fipa00001/SC00001L. html.

[6] 史忠植.智能主体及其应用[M].北京:科学出版社，2000.

[7] 张云勇,刘锦德.移动 Agent 技术[M].北京：清华大学出版社，2003.

[8] 王汝传,徐小龙,黄海平.智能 Agent 技术及其在现代信息网络技术中的应用[M].北京:北京邮电大学出版社，2006.

[9] 窦　文,王怀民,贾　焰,等.构造基于推荐的 Peer－to－Peer 环境下的 Trust 模型[J]. 软件学报，2004,15(4):571－583.

[10] 余一娇,金　海.对等网络中的搭便车行为分析与抑制机制综述[J].计算机学报,2008,31(1):1－15.

[11] Hohl F. Time limited blackbox security : Protecting mobile agents from malicious hosts[C]//In: Vigna, Giovanni. Mobile Agents and Security, LNCS 1419. [s. l.]:Springer－Verlag, 1998.

[12] Sander T, Tschudin C F. Protecting Mobile Agents Against Malicious Hosts. Mobile agents and security, Lecture Notes in Computer Science[M]. New York: Springer－Verlag,1998: 44－60.

[13] 王汝传,徐小龙, 郑晓燕,等.移动代理安全机制的研究[J].计算机学报,2002,25(12): 1294－1301.

[14] 王汝传,孙开翠,张登银,等.基于 JavaCard 的移动代理保护的研究[J].计算机学报，2004,27(4):492－499.

(上接第 139 页)

参考文献：

[1] Information Technology. Open Systems Interconnection: Security Frameworks for Open Systems: Access Control Framework[S]. ITU－T Recommendation X.812|ISO/IEC 10181－3,1995.

[2] 徐晓春,陆松年,杨松年,等.基于 XACML 的 Web 服务访问控制模型[J].计算机工程,2004,30(5):75－92.

[3] Extensible access control markup language[EB/OL]. 2005. http://www.oasis－open.org/commit－tees/xacml.

[4] 邓　凯,裴　浩.基于 XACML 和 SAML 的 Shibboleth 隐私保护方法的探索分析[J]. 计算机应用与软件 ,2009,26(1):267－269.

[5] 李鹏飞.多媒体应用安全分析与设计[D]. 西安:西安电子科技大学,2009.

[6] 邓柳军,张文博,李　洋.基于 XACML 安全策略 J2EE 应用服务器安全授权框架[J].计算机工程与设计,2009,30(5):1041－1044.

[7] Chen X F. Receipt free electronic voting based on semi－trusted model[J]. Chinese Journal of Computers, 2003, 26(5):557－562.

[8] 郑起莹,沈建京.基于 XACML 的 Web 服务安全访问控制模型[J].计算机工程与设计,2007,28(16):3832－3836.

[9] 张晓波.基于 XACML 的角色访问控制机制的研究与实现[D].长春:吉林大学，2008.

[10] 陈维烨.多媒体信息的安全传输与管理[D].上海:上海交通大学 2009.

[11] Mbanaso U M, Cooper G S, Chadwick D W, et al. Privacy Preserving Trust Authorization Framework Using XACML [C]//Wowmom. [s. l.]:[s. n.],2006:673－678.