分布式系统中综合的信任管理模型研究

祝胜林1,2, 杨　波1, 张明武1

(1华南农业大学信息学院，广东广州 510642；2中山大学

广东省信息安全技术重点实验室，广东广州 510275)

摘要：信任问题是分布式系统中的核心问题，包括授权委托，主观信任评估等方面．针对该问题的研究可以分为基于凭证的和基于证据的信任管理模型．为了提高信任管理问题的处理效率和灵活性，本文基于开放的思想，提出了综合凭证与证据的信任管理模型．

关键词：信任管理；基于凭证的；基于证据的；信任管理模型

中图分类号： TP309　　**文献标识码：** A　　**文章编号：** 1001-411X(2007)02-0113-03

Research on a Comprehensive Trust Management Model in Distributed Systems

ZHU Sheng-lin1,2, YANG Bo1, ZHANG Ming-wu1

(1 College of hrformatics, South China Agric. Univ., Guangzhou 510642, China;

2 Guangdong Province Key Lab of Information Security, Sun Yat-Sen University,Guangzhou 510275, China)

Abstract: Trust management is the core problem in distributed systems, including authorization delegating, subject trust evaluating and so on. Research on trust management model may be credential-based or evidence-based. A comprehensive trust management model into which credential-based and evidence-based components were integrated was proposed in this paper to improve efficiency and adaptability.

Key words: trust management ; credential-based ; evidence-based ; trust management model

传统的系统是面向封闭的、熟识用户群体和相对静态的，而分布式系统中，譬如：Internet，实体之间大部分相互并不了解，是面向开放的、公共可访问和高度动态的，没有一个全部实体可以信赖的权威中心．因此，许多基于传统软件系统形式的安全技术和手段，譬如：访问控制列表(access control list)和一些传统的公钥证书体系(X.509，PGP)等不再能够满足分布式系统的安全需要．在分布式系统中，不熟识的参与者之间建立并维护信任关系以保证分布式应用的安全运转就成为了一个基础性的问题．1996年，Blaze等[1]提出“信任管理”(*trust management*)的思想，它是一种以密钥为中心的授权机制，即把公钥作为主体，可以直接对公钥进行授权．将授权转化为回答一个一致性证明(proof of compliance)问题：“凭证集合**C**是否证明了请求r符合本地安全策略P?”．为了使信任管理能够独立于特定的应用，Blaze等还提出了一个基于信任管理引擎(trust management engine，TME)的信任管理模型，也被研究者称为基于凭证的信任管理模型[2]．第1代信任管理系统是Blaze等[1]提出的PolicyMaker，它所采用的一致性证明算法得到了详细的推理和证明[3]．第2代信任管理系统是Blaze等[4]实现的KeyNote，它沿用了PolicyMaker的大部分思想和原则，但KeyNote要求它的策略和凭证必须使用某种特定的断言语言书写，现在它已

收稿日期：2006-09-15

作者简介：祝胜林(1969—)，男，副教授，在职博士研究生；通讯作者：杨　波(1963—)，男，教授，E-mail：byang@scau.edu.cn

基金项目：国家自然科学基金(60573043)，广东省信息安全技术重点实验室开放基金(H06002)

经成为了 IETF 的 RFC 文档. 其他信任管理系统相继被提出,譬如:REFEREE[5]和 DL[6]等. Povey[7]在 Blaze 等提出的信任管理思想的基础上,结合 Adul-Rahman 等[8]提出的主观信任模型思想,给出了一个更具一般性的信任管理定义:信任管理是信任意向(trust intention)的获取、评估和实施. 授权委托和安全凭证是一种信任意向的具体表现,而主观信任模型则主要从信任的定义出发,使用数学的方法来描述信任意向的获取和评估. 主观信任模型认为,信任是主体对客体特定行为的主观可能性预测,取决于经验(过去交互成功和失败的次数)并且随着客体行为的结果变化而不断修正. 同样地,为了使主观信任能够独立于特定的应用,不少研究者也提出了基于信任度的评估模型,这种模型也被称为基于证据的信任管理模型[2]. Beth 信任度评估模型引入了经验的概念来表述和度量信任关系,并给出了由经验推荐所引出的信任推导和综合计算公式[9]. Jøsang 等[10]引入了事实空间(evidence space)和观念空间(opinion space)的概念来描述和度量信任关系,并提供了一套主观逻辑(subjective logic)运算子用于信任度的推导和综合计算[10]. 但在这 2 个模型中由于无法有效地消除恶意推荐带来的影响,所以其他研究者将奖惩机制引入模型. 在分布式系统中,基于凭证的授权机制和基于证据的协作机制相互融合,便以实现对信任的高效管理,本文研究融合 2 种机制的综合信任管理模型.

1 综合的信任管理模型

基于凭证的信任管理模型的关键是证书链的发现[11],即在由凭证集的元素生成的证书图中,是否存在一条从授权源(source of authority)到请求者(requester)的一条证书链(certificate chain),如果存在则找到它. 基于证据的信任管理的关键是信任的表示、度量以及信任度的推导[2]. 为了提高信任管理问题的处理效率和灵活性,遵循信任管理的一般性含义,本文基于开放的思想,提出了综合凭证与证据的信任管理模型.

1.1 模型设计

在不同的证书存储策略下,证书链的发现算法(credential chain discovery algorithm, CCDA)可能不同;而由于对信任的表述、度量和推理的方法不同,对信任度的评估算法(trust degree evaluation algorithm, TDEA)也会不同,因此信任管理引擎模型需要采用开放的形式,通过安全外挂算法模块实现正确的决策. 模型体系如图 1 所示. 其中①是请求的提交入口;②是动作输出口.

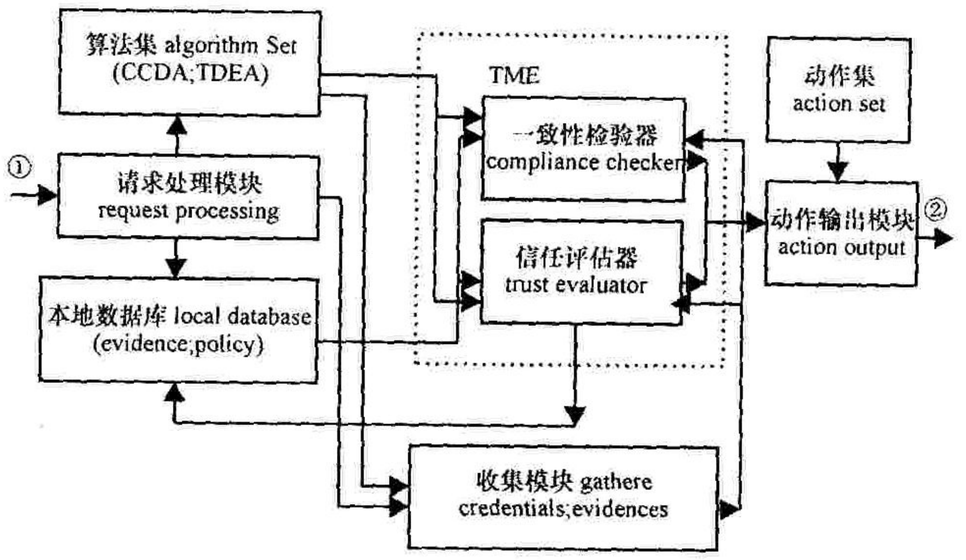

图 1 模型体系结构

Fig. 1 Model architecture

1.2 功能模块

在图 1 所示的模型体系结构中,通过 3 个外挂的资源集实现系统的开放性,它们分别是算法集(algorithm set)、本地数据库(local database)、动作集(action set). 算法集提供一致性检验或信任评估的算法;本地数据库包括记录情况,譬如:交易次数、成功交易次数,本地策略或条件;动作集是为了适应不同的应用程序有不同的动作. 信任管理引擎(TME)包括一致性检验器(compliance checker)和信任评估器(trust evaluator). 3 大功能模块分别是请求处理模块(request processing)、收集器模块(gatherer)和动作输出模块(action output). 下面对这 3 个功能模块进行简介.

1.2.1 请求处理模块 请求处理模块的主要功能是对请求进行分析,确定请求是授权请求还是主观信任请求:(1)授权请求是指需要授权访问相关资源的请求,对这种请求的处理是基于凭证的信任管理. 处理步骤:凭证的收集、本地策略和证书链发现算法的加载、一致性检验. (2)主观信任请求是指需要对参与协作方进行信任度评估的请求,对这种请求的处理是基于证据的信任管理. 处理步骤:证据的收集(间接证据)、本地证据(直接证据)和信任度评估算法的加载、信任评估.

1.2.2 收集器模块 收集器的功能是根据请求处理模块的分析处理结果确定是进行凭证的收集,还是进行间接证据的收集. (1)凭证收集:在证书类型系统中[11],良型证书的存放是有一定规则的,根据这

些规则可以快速定位相关的凭证.(2)间接证据:它是指推荐方与被评估方之间进行过的交互.在分布式系统中,由于没有完全可信任的中心,间接证据可以通过一定的协议完成相关信息的交换,譬如:递归方式的搜索、广播方式.收集器收集到的凭证或证据送到信任管理引擎,信任评估的结果可以作为新的证据存入本地数据库.

1.2.3　动作输出模块　由于信任管理引擎输出的结果是实数值,譬如:[-1,1],对于不同的数值表示的意义需要通过动作集进行相应的定义.因此动作输出模块的功能是依据信任引擎的输出和动作集两方面确定动作的输出.由于应用系统的不同,能够完成的动作可以不同,通过对动作集外部定义保证了信任引擎的灵活性.

2　模型的分析

图1所示的模型,从信任的全局出发,综合了授权委托问题和主观信任问题的2个方面,从对请求的分析,启动凭证或证据的收集,通过对外挂资源集中的资源加载完成一致性证明或信任评估.通过模型分析,信任管理的有效性实现还需要解决如下问题:

(1)收集凭证和证据的有效性问题:凭证和证据的存储是分布的,有效地定位凭证和证据需要一定的策略保证,譬如:证书类型系统,DHT(dynamic hash table);另外还需要相应的协议来实施,譬如:通过广播获取与被评估方有过交互的主机集合,或者代理机制.

(2)资源集的安全问题:由于资源集中的数据对信任管理引擎正常工作和动作的输出有特别重要的作用,需要确保其中的数据不被篡改、替换.

(3)模型的应用接口问题:本模型虽然综合了基于凭证和基于证据2个方面,具有更高的有效性和灵活性,但要能够更好地被应用需要解决好接口问题.接口问题不仅解决用户维护资源集中数据的方便,还要解决与应用系统对接的方便.

3　小结

信任管理问题是分布式系统中的一个基础问题,对这个问题的研究包括基于凭证的和基于证据的方向,本文提出综合的信任管理模型就是要统一这2个方向,使得两者相辅相承,提高信任管理的处理效率和灵活性.在今后的研究中,准备采用J2EE体系来实现该模型.

参考文献:

[1] BLAZE M, FREIGENBAUM J, LACY J. Decentralized trust management[C]//Proceedings of the 17th Symposium on Security and Privacy. [S. L.]: IEEE Computer Society Press, 1996: 164-173.

[2] 袁时金. 信任管理关键技术研究[D]. 上海:复旦大学, 2004: 10.

[3] BLAZE M, FEIGENBAUM J, STRAUSS M. Compliance checking in policymaker trust management system[C]// Proceedings of the Financial Cryptography'98, Lecture Notes in Computer Science 1465, London: Springer-Verlag, 1998: 254-274.

[4] BLAZE M, FEIGENBAUM J, IOANNIDIS J, et al. The keynote trust management system version 2 [S]. IETF RFC 2704, http://www.ietf.org/rfc/rfc2704.txt, 1999-09-18.

[5] CHU Y H, FEIGENBAUM J, LAMACCHIA B, et al. REFEREE: Trust management for web applications[J]. World Wide Web Journal, 1997, 2(2): 127-139.

[6] NINGHUI LI, BENJAMIN N, GROSOF, FEIGENBAUM J. Delegation logic: A logic-based approach to distributed authorization [J]. ACM Transactions on Information and Syetem Security, 2003, 6(1): 128-171.

[7] POVEY D. Developing electronic trust policies using a risk management model[C]//Proceedings of the International Exhibition and Congress on Secure Networking-CQRE (Secure)'99, Lecture Notes In Computer Science. London: Spring-Verlag, 1999: 1-16.

[8] ABDUAL-RAHMAN A, HAILES S. A distributed trust model[C]//Proceedings of the 1997 New Security Paradigms Workshop. Cumbria: ACM Press, 1998: 48-60.

[9] BETH T, BORCHERDING M, KLEIN B. Valuation of trust in open network[C]//GOLLMANN D. Proceedings of the european symposium on research in security (ESORICS). London: Springer-Verlag, 1994: 3-18.

[10] JØSANG A. A model for trust in security systems[C]// Proceedings of the 2nd Nordic Workshop on Secure Computer Systems. Philadelphia: ACM Press, 1997.

[11] LI Ning-hui, WINSBOROUGH H, MITCHELL J C. Distributed Credential Chain Discovery in Trust Management [C]//Proceeding of the 8th ACM Conference on Computer and Communication Security. Philadelphia: ACM Press, 2001:156-165.

【责任编辑　周志红】