基于证书的信任管理研究

耿秀华 著

知识产权出版社
全国百佳图书出版单位

基于证书的信任管理研究

耿秀华 著

知识产权出版社
全国百佳图书出版单位

内容提要

信息技术的迅猛发展，使网络环境已经从早期相对静态的、面向特定组织和用户群体的封闭网络，发展为可公共访问的、面向大量用户的开放动态网络。网络的开放性和实体的动态性，决定了大部分网络应用以陌生主体为参与主体，这使得传统的基于用户身份的访问控制机制无法适应新的安全需求，在这种背景下，信任管理理论应运而生。本文紧紧围绕基于证书的信任管理模型，主要分析和研究了其中的安全性问题和策略问题，并提出了增强系统安全性和可控性的具体方案。

责任编辑：杜丽丽

图书在版编目(CIP)数据

基于证书的信任管理研究/耿秀华著. —北京：知识产权出版社，2011.6

ISBN 978-7-5130-0561-6

Ⅰ.①基… Ⅱ.①耿… Ⅲ.①计算机网络—安全技术—研究

Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字(2011)第 089306 号

基于证书的信任管理研究

JIYU ZHENGSHU DE XINREN GUANLIYANJIU

耿秀华 著

出版发行：知识产权出版社

社　　址：北京市海淀区马甸南村 1 号		**邮　　编**：100088	
网　　址：http://www.ipph.cn		**邮　　箱**：bjb@cnipr.com	
发行电话：010-82000893 82000860 转 8101		**传　　真**：010-82000893	
责编电话：010-82000860 转 8180		**责编邮箱**：dulili@cnipr.com	
印　　刷：知识产权出版社电子制印中心		**经　　销**：新华书店及相关销售网点	
开　　本：787 mm×1092 mm　1/16		**印　　张**：10	
版　　次：2011 年 7 月第 1 版		**印　　次**：2011 年 7 月第 1 次印刷	
字　　数：150 千字		**定　　价**：36.00 元	

ISBN 978-7-5130-0561-6/TP·005(3470)

前　言

如今，信息技术迅猛发展，网络环境已经从早期相对静态的、面向特定组织和用户群体的封闭网络，发展为可公共访问的、面向大量用户的开放动态网络，网络的开放性和实体的动态性，决定了大部分网络应用以陌生主体为参与主体，这使得传统的基于用户身份的访问控制机制无法适应新的安全需求，在这种背景下，信任管理理论应运而生。信任管理的思想最早由 M. Blaze、J. Feigenbaum 和 J. Lacy 提出，它独立于所有的应用或服务，是一种统一地说明和解释安全策略、证书和信任关系的方法，和传统的访问控制机制不同的是：后者是根据请求者的身份来做出授权判断的，而前者是根据证书来做出判定的，它用来回答这样一个问题："访问请求者所提供的证书集合能够证明访问请求与本地安全策略相一致吗？"

1999 年，D. Povery 对信任管理给出了一个更通俗的定义：信任管理是信任意向的获取、评估和实施。此后，对信任管理模型的研究基本上分为两大类：基于证书的信任管理模型和基于经验的信任管理模型，在基于证书的信任管理模型中，实体之间的信任关系通过证书来建立，在基于经验的信任管理模型中实体之间的信任关系依据过去的交互经验来建立。本书紧紧围绕基于证书的信任管理模型，主要分析和研究了其中的安全性问题和策略问题，并提出了增强系统安全性和可控性的具体方案，内容如下：

1. 一致性验证是信任管理的核心问题，提出了一种新的 SPKI/SDSI2.0 证书在分布式环境中的存储策略及相应的证书链搜索算法，存储策略是对象方完全可追溯的，且所有证书只在一处存放，这样不仅可以节约存储空间，还可以避免由于多处存放而产生的不一致性；搜索算法是面向目标的，算法自

动在分布式环境中搜索与访问请求相关的证书,它从公钥出发,边查找公钥的名字证书,边搜索对这些名字的授权,利用堆栈解决了复杂扩展名的查找和授权问题,算法还实现了对委托深度的细粒度控制。

2. 在基于证书的信任管理模型中,系统中的每个主体都可以发放证书,在一个特定的系统状态中,系统管理员需要知道关于系统的一些"特性",如某一主体是否有权访问被保护资源,一个本地名有哪些成员等,这就是策略分析。本书提出了一种高效的、基于逻辑的 SPKI/SDSI2.0 策略分析算法,算法用标准的 Datalog 程序表示 SPKI/SDSI2.0 的系统状态,以 Datalog 程序的最小 Herbrand 模型作为它的语义,证明了该语义的可靠性。利用该算法不仅可以分析 SPKI/SDSI2.0 的授权问题及名字问题,还可以将这两类问题结合起来对系统策略进行综合的分析查询。

3. 利用基于逻辑的方法,定义了信任管理系统 SPKI/SDSI2.0 的安全分析模型,制定了相应的限制规则,在此基础上对 SPKI/SDSI2.0 的权限泄露问题进行了全面的分析,证明了该问题是在多项式时间内可判定的;证明了系统的安全依赖且仅依赖于可信主体集合。提出了在 SPKI/SDSI2.0 系统的一致性验证过程中增加约束检查的方法,通过约束,服务提供者可以自主地表达并实现自己的安全策略,很好地保证了 SPKI/SDSI2.0 系统的安全性,使服务提供者加大了对访问权限的控制力度,减少了委托机制所带来的负面影响。

4. 将可信计算平台应用于信任管理系统,提出了一种搭建在可信计算平台之上的基于角色的信任管理系统,从证书、安全策略、一致性验证等方面具体阐述了如何将基于角色的信任管理框架与可信计算平台有机地结合起来,从根本上提高信任管理系统的可信性、自主性和安全性,最后通过实例对系统的使用进行了具体说明。

关键词:信任管理;证书;SPKI/SDSI2.0;证书链;安全性;约束;一致性验证;基于角色的信任管理框架;可信计算平台

分类号:TP309

ABSTRACT

With the rapid development of information technology, internet environment has evolved from static, particular organization – oriented closed network to dynamic, public–accessed, mass user–oriented open network. Hence, various services are required to make authorization judgments in the environment. As a typical large – scale distributed network, internet has more entities than the previous centralized network. Those entities don't understand each other before, and there is not a unified authority which all of the entities can trust. Therefore, many traditional systems that support security in network application, such as X. 509 and PGP, can't satisfy the requirement. Presented by M. Blaze, J. Feignbaum and J. Lacy in 1997, trust management is independent of any particular application or service. Policies, credentials and trust relationships are expressed and explained by the same way. Unlike other access control mechanisms, trust management makes decisions based on credentials rather than the requestor's identity.

The models of trust management can be classified into two categories, credential–based and evidence–based. Trust relationship is mainly achieved by credentials in the former, whereas it is evaluated according to the interactive experience of the past in the latter. This dissertation focuses on credential–based trust management, and the main contributions are as follows.

1. Compliance – checking is a core problem in trust management. A reasonable distributed credentials storage scheme is proposed in this dissertation. Each credential is stored in one place and all the credentials are subject–traces–

all. Based on this scheme, distributed credential chain discovery in SPKI/SDSI2.0 is put forward. Unlike other algorithms, it needn't reduce credentials and compute the name-reduction closure of a set of credentials. The algorithm searches all the name credentials for one entity, and looks for subsequently the authorization credentials to all those name credentials. Finally, the algorithm uses depth-first search to determine whether there exists a chain from Self to the requestor. The algorithm is goal-directed, and it could automatically gather relevant name and authorization credentials which are needed. Moreover, it could resolve the problem of delegation depth elegantly.

2. SPKI/SDSI2.0 is a popular trust management system at present, and each entity in it can issue policy statements. A set of SPKI/SDSI2.0 credentials forms a state of system. In a given state, many important properties need to be known and analyzed, for example, to a specific right, who are granted in the system. When the number of credentials becomes huge, a special algorithm is required to answer those questions. However, previous algorithms only investigate the problems about authorization and neglect the policy analysis involved names. Moreover, the efficiency of those algorithms is not high. In this dissertation, an efficient policy analysis algorithm for SPKI/SDSI2.0 is presented. Expanding the area of policy analysis essentially, it can analyze not only properties about authorization and name but also about the integrated properties. We get logic programs based on translating each policy statement into some Datalog clauses. The minimal Herbrand model of Datalog program is used as the program's semantics and it can be evaluated in polynomial time. In addition, the soundness of the semantics is proved.

3. The safety analysis model for SPKI/SDSI2.0 is defined, which is based on logic method. Through synthetically analyzing the security properties in SPKI/SDSI2.0, We conclude that simple safety can be decidable in polynomial time and the safety of SPKI/SDSI2.0 only relies on trusted entities. Specifically, a

compliance-checking mechanism of SPKI/SDSI2. 0 with constraint checking is presented to enhance the degree of control over the resource for the owner. This mechanism, which is simple, flexible and easy to implement, can greatly improve the security property of the distributed access control.

4. In role - based trust management framework (*RT*) entities may be authorized according to their properties, so it is an effective way to build trust relationships dynamically for the unfamiliar in large open distributed environment. However, when making authorization decision *RT* only considers the properties of entities while ignores the states of platforms on which entities are operating. An "irresponsible" platform may pose threat to the system security obviously. To address the problem, this dissertation presents a role-based trust management system on the trusted computing platform. The credentials, security policy and compliance-checking are discussed, and the usage of the system is illustrated through a typical example.

KEYWORDS: trust management; cridential; SPKI/SDSI2. 0; credentials chain; security; constraint; compliance-checking; role-based trust management framework; trusted computing platform

CLASSNO: TP309

1 绪论

信任管理主要研究如何在开放动态的网络中,为相互陌生的实体间建立信任关系的问题,本章首先介绍了它的研究背景、研究现状及存在的主要问题,最后对本书的研究内容及主要贡献做了概要性的介绍。

1.1 研究背景

21 世纪是信息时代,信息已成为社会发展的重要战略资源,社会的信息化已是当今世界发展的潮流和核心,因为 Internet 的巨大潜力,社会各个领域的应用越来越多地基于 Internet 的实现和拓展,人们也越来越依赖于所身处的信息世界,Internet 是一个没有中心的自主式的开放组织,它所提供的广泛的连通性不仅为资源共享奠定了基础,而且使得计算能力能够实现整合,通过网络可以将空闲的计算资源组织起来,共同完成一个计算任务。但是,人们在享受网络所带来的信息便利的同时,也不得不承受着越来越严重的信息安全威胁,目前,网络与信息安全问题及其对经济发展、国家安全和社会稳定的重大影响,正日益突出地显现出来,受到越来越多的关注。

近年来,随着计算机技术和通讯技术的迅猛发展,网络中聚合了大量的计算资源、数据资源、软件资源以及服务资源等各种可以利用的资源,为了有效地满足面向互联网的复杂应用对大规模计算能力、海量数据处理和信息服

务的需求,出现了许多基于大规模分布式系统的应用,如普适计算[①],网格计算[②③]、对等网络[④]、Ad Hoc 网络[⑤⑥⑦]等,应用系统表现为由多个软件服务组成的动态协作系统,这使得软件系统所面临的环境由早期的相对静态的、面向特定组织和用户群体的封闭网络逐步走向了现在的可公共访问的、面向大量动态用户的开放网络,这种分布模式的开放网络呈现出以下特点:

(1) 去中心化,即没有中心化的管理权威可以依赖。

(2) 开放性,打破了时空界限,不受时区界限和地理位置的影响,任何实体都可以自由接入,网络具有良好的伸缩性。

(3) 动态性,实体可以动态出入,网络边界也随之动态变化。

(4) 自治性,网络中的各实体具有高度的自治性,均有权决定属于自己的安全策略。

(5) 参与实体数量庞大,各实体之间大部分事先并不认识,彼此之间不可能事先获得关于对方的与安全相关的完整信息。

这使得一些基于传统软件系统形态的安全技术和手段,尤其是安全授权机制,无法适应新的安全需求,因此,为了实现各主体间的信息共享和协作计算,需要一种有效的机制为大规模分布模式中相互陌生、数目庞大、动态分散的主体间建立可靠的信任关系,要求该机制具备下列特点:

(1) 为应用所涉及的各实体之间建立跨安全域的、有效的安全机制,对安全策略、证书及信任关系进行统一处理。

---

① M. Weiser. The computer for the 21st century[J]. Scientific American, 1991, 265(3): 94-101.

② I. Foster, C. Kesselman and S. Tuecke. The anatomy of the grid: enable scalable virtual organizations[J], Supercomputer Application, 2001, 15(3): 200-222.

③ I. Foster, C. Kesselman and S. Tuecke. The grid: blueprint for a new computing infrastructure[M], San Fransisco: Morgan Kanfmann, USA, 1999.

④ F. Geoffrey. Peer-to-peer networks[J]. Computing in Science&Engineering, 2001(6): 75-77.

⑤ H. M. Deng, W. Li, D. P. Agrawal. Routing security in wireless ad hoc networks [J]. IEEE Communications Magazine, 2002, 40(10): 70-75.

⑥ The Internet Engineering Task Force[EB/OL]. Mobile Ad Hoc networks charter. http://www.ietf.org/html.charters/manetcharter.html, 1999.

⑦ D. B. Johnson. Routing in ad hoc networks of mobile hosts[M]. IEEE Workshop Mobile Computing Systems and Applications. New York: IEEE Press, 1994.

(2) 有足够的表达能力来表达网络中复杂多变的信任关系。分布式系统中会不断出现各种不同的条件和限制,以适应不同的应用,因此其使用的安全机制必须能够处理可能出现的新条件。

(3) 支持策略的本地化。网络中的各实体具有高度的自治性,一个实体从小的方面说可以是人或进程,从大的方面说可以是一个管理域或一个组织,每个实体既可以是网络服务的提供者(Provider,简称提供者),也可以是网络服务的请求者(Requestor,简称请求者),均有权制定、实施属于自己的安全策略和安全机制,决定什么样的实体在什么条件下有权享受它所提供的服务。

(4) 与应用相独立。将安全性验证机制与应用或者服务本身的语义分开,其所做的授权决策只依赖于应用或服务所提供的输入,当信任关系发生改变或添加新的信任关系时,不需要更改应用程序,只需改变本地安全策略,这样就可以使安全机制更灵活、更具有广泛性。

传统的安全手段中,访问控制矩阵模型是最基本的表示方法,也是最常用的描述保护状态的模型,它准确地描述了一个实体相对于系统中其他实体的权限,常用于操作系统和数据库中。但是,访问控制矩阵不能用于如今的分布式访问控制,这是因为:

(1) 无法实现跨安全域主体身份的识别,传统的安全认证机制,由于参与系统的个体数量有限,访问之前都经过注册,因此访问是基于用户身份的,根据身份来决定实体的权限,但是在大规模、开放的分布式系统中,参与实体的数量规模大、加上运行环境的异构性、活动目标的动态性以及自主性等特点,系统要熟识每一个用户显然不大可能。

(2) 其安全策略和应用是相关的,若安全策略有所改变,则应用程序也要相应地进行重新配置甚至重写。

(3) 没有足够的表达能力和可扩展能力,不足以处理在分布式系统中出现的各种访问控制条件和限制。

(4) 缺乏委托机制,无法为陌生实体间动态地建立信任关系,在分布式系统中,通过委托机制可以实现灵活和可伸缩的跨域授权机制,使管理任务

分散化。现有的分布式安全机制一般会直接委托一个“可信实体”,这使得只有在委托链的最底端才能体现出策略,通常是一个 ACL 表,所以,这种机制的缺点是高层管理者不能直接控制整个策略①。

(5) 管理域单一,在互联网中,各实体往往隶属于不同的权威管理机构,使得资源访问往往要跨越多个管理域,但本地安全策略不能跨越管理域。

(6) 传统的安全机制是由服务器来实现访问控制,不仅加重了服务器本身的负担,而且系统的安全性完全依赖于服务器,一旦服务器的安全失效,则系统的访问控制策略将全部失效。

此外,在 Web 安全中常见的还有一种非此即彼的二元授权模型,它依据 CA 颁发的证书做出授权判定,但这种访问控制方式要么“全部允许”,要么“全部拒绝”,仅适合于比较单一的授权机制,缺乏灵活性和可扩展性。

在基于公钥证书的分布式安全解决方案中,需要获取实体自身的公钥,这样才能保证加密的信息被真实的实体解密,并且使得验证者能够有效地验证实体的数字签名,现今广为人知的证书系统如 PGP 及 X.509,它们中的安全验证通常由应用本身来完成,所依据的是由可信第三方颁发的公钥证书,但是公钥证书只是将实体 ID 和公钥绑定在一起,A 对 B 的公钥信息签名并不意味着 A 相信 B 是“诚实的”,所以由可信第三方证明的仅仅是实体的身份,而不是它的“可信度”。R. Khare 等人对层次式证书体系应用于跨域访问的不足作了如下总结②:

(1) CA 只能认证实体身份,不能对其品质做出承诺。

(2) 完全依靠可信第三方的认证,忽略了系统中实体彼此之间的信任。而过多地依赖大范围内的 CA,则会导致实体间的利益互相冲突。

(3) 证书撤销列表难以集中维护,可能会造成证书的滥用。

P. Zimmermann 将基于身份的公钥证书与 ACL 结合起来形成分布式访问控制系统,这种系统在使用时需要回答两个问题:其一:谁提出了服务申

① P. Zimmermann. PGP User' Guide[M], Cambridge: MIT Press, 1994.

② R. Khare, A. Rifkin. Trust management on World Wide Web. World Wide Web Journal[J], 1997, 2(3): 77-112.

请？即谁是公钥的拥有者？其二：服务请求者有资格享受该项服务吗？但是，这种方法并不适用于动态的 Internet 网络，因为网络上的实体数量庞大、流动性强，每个实体均可能提出服务申请，彼此在交互之间可能并不熟识，这样，即使第一个认证问题得到了可靠解答，如果服务提供者第一次接触服务请求者，那么，服务提供者仍然无法做出授权决定[①]，为了保证资源的机密性、完整性和可用性不被破坏，服务提供者更关心的是服务请求者的品质、责任心等相关信息，况且，这种分两步走的验证方法使系统更容易遭受攻击。

有人试图修改现有的授权机制以适应自己的安全模型，或反过来修改自己的安全模型以适应授权机制，但由于配置不当，或各组件之间的不协调致使一系列安全漏洞的产生，从而使用户逐渐失去对现有授权机制安全性的信任。

因此，迫切需要一种新的授权机制来解决开放分布式系统所面临的安全问题，提高 Internet 的安全性是保证 Internet 不断发展的关键，如何在开放的 Internet 环境中建立有效的安全保障体系，如何有效地建立和管理个体之间的信任网络，是保障和激励合作交互、使 Internet 应用向着有序性发展的关键[②]。在这种前提下，信任管理理论应运而生，其基本思想是承认开放系统中安全信息的不完整性，系统的安全决策需要依靠可信任第三方提供附加的安全信息。信任管理的意义在于提供了一个适合 Web 应用系统开放、分布和动态特性的安全决策框架。

1.2 研究现状及存在的主要问题

1.2.1 信任及信任管理

在以网络技术为核心的今天，进行安全信息交流的基础是信任，信任是

① M. Blaze, J. Feigenbaum, J. Ioannidis, et al. The role of trust management in distributed systems security. In: Secure Internet Programming: Issues for Mobile and Distributed Objects. Berlin: Springer-Verlag, 1999, 185-210.

② 黄辰林. 动态信任关系建模和管理技术研究[D]. 长沙. 国防科学技术大学, 2005.