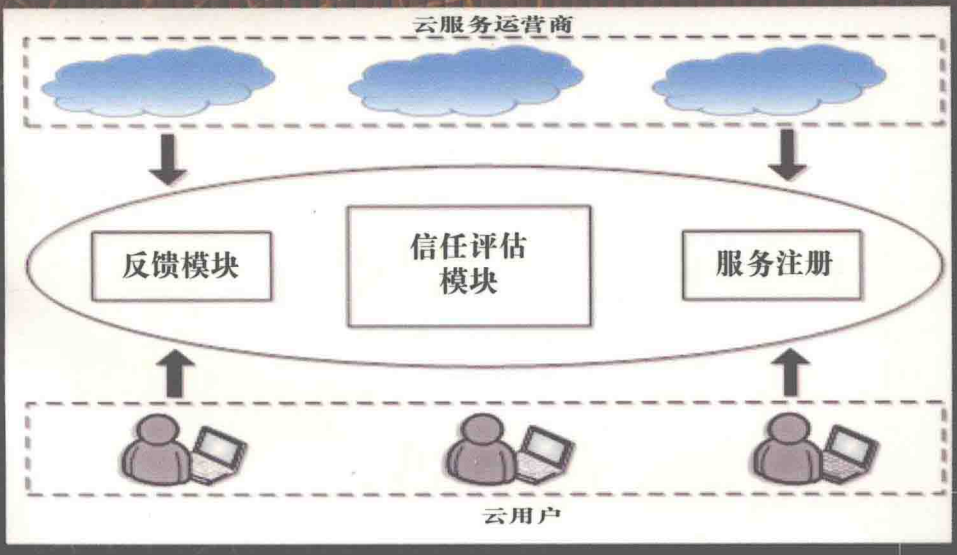
国防科技图书出版基金

网络与信息安全前沿技术丛书

网络中的信任管理体系

张文政 耿秀华 周 宇
汤殿华 张李军 穆道光 等编著

Trust Management Systems in Networks



国防工业出版社
National Defense Industry Press

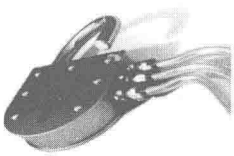
网络与信息安全前沿技术丛书

国防科技图书出版基金

张文政　耿秀华　周　宇
汤殿华　张李军　穆道光　等编著

网络中的信任管理体系

Trust Management Systems in Networks



信任管理是网络中的重要研究方面，为集中展现信任管理的概念、框架、原理和应用，本书对信任管理的研究现状及发展趋势进行了概述和总结，对SPKi/SDSI2.0的相关知识、基于可信计算平台的信任管理系统、信誉系统、基于非合作重复博弈的信任模型等进行了详细全面的论述，重点阐述了移动互联网、云计算、物联网中信任管理解决方案。本书是该领域科研和技术人员系统了解和掌握最新进展的理论著作。

国防工业出版社
National Defense Industry Press
·北京·

致　读　者

本书由中央军委装备发展部**国防科技图书出版基金**资助出版。

为了促进国防科技和武器装备发展，加强社会主义物质文明和精神文明建设，培养优秀科技人才，确保国防科技优秀图书的出版，原国防科工委于1988年初决定每年拨出专款，设立国防科技图书出版基金，成立评审委员会，扶持、审定出版国防科技优秀图书。这是一项具有深远意义的创举。

国防科技图书出版基金资助的对象是：

1. 在国防科学技术领域中，学术水平高，内容有创见，在学科上居领先地位的基础科学理论图书；在工程技术理论方面有突破的应用科学专著。

2. 学术思想新颖，内容具体、实用，对国防科技和武器装备发展具有较大推动作用的专著；密切结合国防现代化和武器装备现代化需要的高新技术内容的专著。

3. 有重要发展前景和有重大开拓使用价值，密切结合国防现代化和武器装备现代化需要的新工艺、新材料内容的专著。

4. 填补目前我国科技领域空白并具有军事应用前景的薄弱学科和边缘学科的科技图书。

国防科技图书出版基金评审委员会在中央军委装备发展部的领导下开展工作，负责掌握出版基金的使用方向，评审受理的图书选题，决定资助的图书选题和资助金额，以及决定中断或取消资助等。经评审给予资助的图书，由中央军委装备发展部国防工业出版社出版发行。

国防科技和武器装备发展已经取得了举世瞩目的成就，国防科技图书承担着记载和弘扬这些成就，积累和传播科技知识的使命。开展好评审工作，使有限的基金发挥出巨大的效能，需要不断摸索、认真总结和及时改进，更需要国防科技和武器装备建设战线广大科技工作者、专家、教授，以及社会各界朋友的热情支持。

让我们携起手来，为祖国昌盛、科技腾飞、出版繁荣而共同奋斗！

国防科技图书出版基金
评审委员会

国防科技图书出版基金
第七届评审委员会组成人员

主任委员	潘银喜			
副主任委员	吴有生	傅兴男	赵伯桥	
秘书长	赵伯桥			
副秘书长	许西安	谢晓阳		
委员 （按姓氏笔画排序）	才鸿年	马伟明	王小谟	王群书
	甘茂治	甘晓华	卢秉恒	巩水利
	刘泽金	孙秀冬	芮筱亭	李言荣
	李德仁	李德毅	杨　伟	肖志力
	吴宏鑫	张文栋	张信威	陆　军
	陈良惠	房建成	赵万生	赵凤起
	郭云飞	唐志共	陶西平	韩祖南
	傅惠民	魏炳波		

《网络与信息安全前沿技术丛书》编委会

目　录

Contents

第1章 绪论

1.1 概　述

21 世纪是信息化时代，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。由于国际互联网的巨大潜力，社会各个领域的应用越来越多地基于互联网的实现和拓展，人们也越来越依赖于所身处的信息世界，互联网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信技术的迅猛发展，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，如云计算、对等网络、Ad Hoc 网络等，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。

（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，通常是一个访问控制表（Access Control List，ACL），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。

（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的，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，它依据认证授权机构（Certificate Authority，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（Pretty Good Privacy）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，但公钥证书只是将实体身份（Identification，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”。对层次式证书体系应用于跨域访问的不足是：

（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）证书撤消列表难以集中维护，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：①谁提出了服务申请？即谁是公钥的拥有者？②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互联网网络，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，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产生一系列安全漏洞，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，提高互联网的安全性是保证互联网不断发展的关键，如何在开放的互联网环境中

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，使互联网应用向着有序性发展的关键。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 基本概念

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，信任是一个涉及面很广的话题，包括信任的建立、信任的管理以及安全性相关的问题等。在网络与分布式计算安全环境中，信任与信任关系起着非常重要的作用，是基础的和早期决策的部分之一。对于信任的定义有很多，但迄今为止还没有一个统一的定义。对信任认识缺少一致性的意见，导致在很多文献中把信任、授权和认证等不加区分地交替使用。信任在互联网应用中的一个常见定义：信任是对一个实体具有在特定环境下可信、安全、可靠地行动能力的坚定信心。

1996 年，M. Blaze、J. Feigenbaum 和 J. Lacy 首先提出了信任管理的思想，为解决分布式环境中新应用形式的安全问题提供了新思路，它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，网络环境下的每个实体（网络服务提供者）都可以将和自己相关的权限授予其他实体，也可以委托自己信任的实体来完成这种授权，授权通过发行证书来进行。信任管理引擎（Trust Management Engine，TME），也称一致性验证器（Compliance Checker），是信任管理模型中的核心组件，它以证书集合、本地安全策略及服务请求者的请求为输入，经过评估之后，将授权决策返回给服务请求者。M. Blaze、J. Feigenbaum 和 J. Lacy 还给出了一种比较完善地应用信任管理思想的系统 PolicyMaker，它能够使用多种安全的语言更加直接地处理分布式网络中的委托和授权等问题。PolicyMaker 将信任管理要回答的问题定义为："证书集合 C 能够证明某个请求 r 与本地安全策略 P 一致吗？"它提供了一个通用的、与具体应用无关的一致性检验算法，定义了描述证书与策略的高级语言，规定证书必须由它的发行者进行签名。在此之前，M. Blaze 等总结一个拥有传统签名证书的应用跨域访问时所经历的过程如下：

（1）获取证书，验证证书及应用请求上的签名，确定签名者的公钥；

（2）确定这些证书没有被撤消；

（3）查找从可信方到服务请求者之间的"可信路径"；

（4）从证书中解析名字；

（5）从数据库中查找与名字相对应的权限；