信息安全理论与技术系列丛书

信任管理与网络安全

蒋文保 著

清华大学出版社

信息安全理论与技术系列丛书

信任管理与网络安全

蒋文保 著

清华大学出版社
北京

内 容 简 介

本书运用信任管理思想方法，深入探讨了电子商务、移动计算和云计算等所有开放式网络应用环境中共同面临的安全和信任问题。首先系统地介绍信任和信任管理等基本概念和思想方法；其次结合作者多年的科研成果，分析信任管理领域的两个重要研究方向——信任度评估和信任协商的研究内容，重点阐述作者的课题组提出的一些新技术和新方法；最后探讨信任管理思想方法在 P2P 网络安全、网格安全和网络诚信建设 3 个具体问题中的运用。全书共分 8 章，内容包括信任管理概述、基于多维证据的信任度评估模型、基于行为检测的信任度评估技术、自适应自动信任协商模型、自适应信任协商系统设计、信任管理与 P2P 网络安全、信任管理与网格安全以及信任管理与网络诚信建设等。

本书适合网络安全与电子商务相关研究、开发人员阅读，还可以作为计算机及其相关专业研究生和高年级本科生的参考教材，以及培训机构的培训教材。

图书在版编目（CIP）数据

信任管理与网络安全/蒋文保著. —北京：清华大学出版社，2012.11
信息安全理论与技术系列丛书
ISBN 978-7-302-31021-1

Ⅰ. ①信…　Ⅱ. ①蒋…　Ⅲ. ①计算机网络－安全技术　Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2012)第 304364 号

责任编辑：张　玥　战晓雷
封面设计：傅瑞学
责任校对：白　蕾
责任印制：宋　林

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 装 者：北京鑫海金澳胶印有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：10.25　　**字　　数**：240 千字
版　　次：2012 年 11 月第 1 版　　**印　　次**：2012 年 11 月第1 次印刷
印　　数：1～2500
定　　价：25.00 元

产品编号：032388-01

前言

目前，基于开放网络环境下的电子商务、移动计算、网络游戏和云计算等新型网络应用正在不断渗入和扩散到国民经济和社会发展的各个领域。在开放的互联网中，由于参与主体数量的规模大、运行环境的异构性、活动目标的动态性以及自主性等特点，各资源主体往往隶属于不同的管理机构，不同的管理域对安全控制的需求和采用的安全策略可能完全不同，使得传统的安全技术和手段，尤其是安全授权机制，如访问控制列表、一些传统的公钥证书体系等，在跨域进行授权及访问控制时显得力不从心，暴露出许多弱点。因此，如何在开放的互联网中建立和维护不同管理域之间以及各个交互主体之间的信任关系，并以此实现它们之间的协同工作，是当前各种新型网络应用所共同面临的一个基础性问题。

1996 年，M. Blaze 等学者为解决 Internet 网络服务的安全问题首次使用了“信任管理”的概念，并在此基础上研制了相应的信任管理系统。M. Blaze 等人将信任管理定义为采用一种统一的方法描述和解释安全策略、安全凭证以及用于直接授权关键性安全操作的信任关系。信任管理的意义在于提供一个基于安全凭证的通用安全决策支持框架，它比较适合应用于开放的网络环境。与此同时，A. Adul-Rahman 等学者从“信任”的概念出发，对信任内容和信任程度进行划分，并从信任的主观性入手给出信任的数学模型用于信任评估。D. Povey 在 M. Blaze 定义的基础上，结合 A. Adul-Rahman 等人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，即信任管理是信任意向的获取、评估和实施。目前，许多学者趋于认为信任管理是一种为确定用于决策的信任而通过搜集、分析和编码相关证据以进行决策评价的行为，它实际上是一种决策支持技术。在开放网络环境中，各系统之间相互独立，但只有建立相互信任关系，系统之间才能实现有效交互，所以信任管理作为网络安全技术的重要前提和基础，正日益成为网络安全研究的热点。

在跨域网络协同环境中，由于交互主体间的生疏性以及共享资源的敏感性，陌生的主体之间很难建立信任关系。为了解决上述问题，2000 年 Winsborough 等人提出了“自动信任协商”的概念，它是“通过凭证、访问控制策略的交互披露，资源的请求方和提供方自动地建立信任关系”。目前，自动信任协商的研究已得到迅速发展，并成为当前的一个重要研究方向，其研究和应用在国际上备受关注。

信任管理和信任协商等概念和思想的出现，为所有基于开放、分布、动态特性环境的安全和信任问题提供了新的解决思路。本书运用信任管理思想方法，深入探讨电子商务、移动计算和云计算等所有开放式网络应用环境中共同面临的安全和信任问题。首先，系统地介绍“信任”和“信任管理”等基本概念和思想方法；其次，结合作者多年的科研成果，分析信任管理领域的两个重要研究方向——信任度评估和信任协商的研究内容，重点阐述作者的课

题组提出的一些新技术和新方法；最后，探讨信任管理思想方法在 P2P 网络安全、网格安全和网络诚信建设 3 个具体问题中的运用。

全书共分 8 章。第 1 章“信任管理概述”对信任管理思想方法加以概述。本章对信任管理的思想方法和技术要领进行了简明扼要的阐述，首先介绍信任和信任管理的基本概念，讨论信任管理产生背景、基本内涵、主要内容以及国内外研究现状；然后概要地讨论信任度评估涉及的主要内容，介绍信任协商的基本概念、关键技术和解决方案，以作为本书其他章节的引子。

第 2 章和第 3 章是关于信任度评估方面的研究内容。其中，第 2 章“基于多维证据的信任度评估模型”提出一种基于多维证据的信任度评估模型，该模型基于交易反馈和网络操作行为两个层面的多维证据源进行信任计算，扩展了证据源，突破了只依据单一种类证据源进行信任评估而引起的缺陷；另外，应用改进的 D-S 证据理论来合成多维证据，较好地解决了证据不确定性的问题。第 3 章“基于行为检测的信任度评估技术”专门阐述一种基于网络操作行为的信任度评估模型和算法，这种模型着重考虑了用户的网络操作行为，以用户的日常网络操作行为和交易行为作为信任度评估的依据。

第 4 章和第 5 章是关于信任协商方面的研究内容。其中，第 4 章“自适应自动信任协商模型”提出一种新的信任协商模型，即一种自适应自动信任协商模型（简称 AATN），它能根据信任度评估结果动态调整访问控制策略和协商策略，对于信任度高的协商方可提供快速响应的策略，而对于信任度低的协商方则提供更为谨慎安全的策略，以有效兼顾信任协商中效率和安全两个方面的需求。第 5 章“自适应信任协商系统设计”在第 4 章提出的自适应信任协商模型的基础上，主要讨论自适应信任协商系统的设计和实现问题。

第 6～8 章探讨信任管理思想方法在具体网络安全问题中的运用。其中，第 6 章“信任管理与 P2P 网络安全”主要阐述使用信任协商技术解决 P2P 网络安全问题，重点设计并分析一种 P2P 网络信任协商系统 NetTrust。第 7 章“信任管理与网格安全”在全面分析网格安全需求的基础上，基于信任和信任管理的思想方法深入探讨网格安全解决方案。第 8 章“信任管理与网络诚信建设”探讨在网络诚信建设中如何管理和规范网络主体行为的问题，主要论述软件信任评价体系、网站信任评价体系和网络个人用户信任评价体系 3 种网络主体信任评价体系。

本书作为一本学术专著，来源于科学研究的实践。作者从 2000 年以来一直针对分布式跨域协作环境下的安全问题进行研究，2002 年年底结合网格技术在高能物理领域的应用，完成了中国科学院博士学位论文《网格环境下的安全技术研究》。在此基础上，2005 年 1 月完成清华大学博士后研究报告《开放网络环境下的若干安全问题研究》。在攻读博士学位和进行博士后研究期间，作为主要研究人员参加了中国科学院知识创新工程重大项目之子项目“黑客防范体系”、国家重点基础研究发展规划项目（973）“信息与网络安全体系研究”中的“信息分析和监控”，以及国家 973 项目“信息技术中的应用理论与高性能软件”中的“密码算法研究与网络安全系统研制”等大型项目的研究与开发工作。从 2005 年起任职于北京信息科技大学后，主持承担了北京市教委科技计划项目“基于信任管理的网格安全模型及应用研究”和北京市自然科学基金项目“网格自适应信任协商若干关键问题研究”，2008 年开始主持承担国家自然科学基金项目“一种自适应信任协商模型研究”。作者在梳理这十多年研究经历和研究积累的过程中，深刻认识到信任和信任管理思想方法对于解决开放网络协作环

境下安全问题的重要性，因此下定决心撰写了本书，提供给从事相关技术开发和科学研究的专业人员参考和借鉴。

在研究和写作过程中，本人主要得益于我的研究生杨东浩、刘思征、郭少旭、陈文亮、吴洋、韩莹莹、晁储频、王鸿、汪秋云，本书的很多思想方法是我在指导他们完成科研项目研究和硕士学位论文中产生的，同时他们还帮助我整理书稿，做了许多烦琐的工作。因此，我要对他们表示衷心的感谢！

我还要感谢中国科学院高能物理研究所的杨大鉴老师和许榕生老师，清华大学的戴一奇老师和林闯老师，他们对我在攻读博士学位期间和博士后研究工作中给予了极大的指导和帮助。同时感谢北京信息科技大学各位领导和同事的鼎力相助，感谢清华大学出版社编辑张玥的辛勤工作。

由于时间仓促，加上信任管理是一个较新的研究领域，因此本书错误之处在所难免，欢迎广大读者批评指正。

作者

2012 年 11 月

目录

第 1 章　信任管理概述

目前，基于开放网络环境下的电子商务、云计算、移动计算、网络游戏和物联网等新型网络应用逐渐成为一种主流应用模式。在开放的互联网中，由于参与主体数量的规模大、运行环境的异构性、活动目标的动态性以及自主性等特点，各资源主体往往隶属于不同的管理机构，不同的管理域对安全控制的需求和采用的安全策略可能完全不同，使得传统的安全技术和手段，尤其是安全授权机制，如访问控制列表(ACL)、一些传统的公钥证书体系(PKI)等，在跨域进行授权及访问控制时显得力不从心，暴露出许多弱点。因此，如何在开放的互联网中建立和维护不同管理域之间以及各个交互主体之间的信任关系，并以此实现它们之间的协同工作，是当前各种新型网络应用所共同面临的一个基础性问题。

为了解决上述问题，近年来信息安全领域出现了一个新的重要研究方向——信任管理，目前信任管理技术为所有基于开放、分布、动态特性环境的安全和信任问题提供了新的解决思路。本章对信任管理的思想方法和技术要领进行简明扼要的阐述，以作为本书其他章节的引子。

1.1　信任与信任管理

1.1.1　信任

信任是一个很难严格定义的抽象概念，目前还没有一个精确的、广泛可接受的定义，不同的研究往往倾向于在所处的上下文中对信任这个概念作不同的定义。到目前为止，信任概念在信息技术领域中得到了广泛应用，不同的学者基于不同的目的和角度对信任有不同的定义和理解。

Gambetta[1]于 1990 年给出了信任的定义，他认为在多代理环境中，信任是在不能提前监控某代理特定行为及影响该行为的相关内容的前提下，在一定程度上某代理能完成该特定行为的主观可能性。随后 K. Konrad[2]提出信任是一个与诚实、相信、竞争以及可靠等联系在一起的一个主体概念。

Kini 和 Choobineh[3]在他们的关于信任的理论架构中认为，信任就是：

(1) 一个对某一个人或者事情可靠性的预测。其信任度取决一个被信任者的特征、能力、力量以及真实度。

(2) 一份对诺言(约定)或者一个关系的条件的责任。

(3) 对某一个实体给予信心。

Grandison[4]认为，信任是在特定的环境中对于一个实体具有诚实、安全和可靠行动的能力的坚定信念。Tyrone[5]等在 2003 年认为，信任是在特定上下文中，信任者对于被信任者能力、诚实性、安全性和可靠性的量化信念。Mui[6]则将信任定义为某一代理对另一代理未来行为的主观期待。Wang[7]认为，信任是某代理根据自身的直接经验对另一节点能力、诚实度和可信赖程度的信念。Hussain[8]认为，在面向服务的网络环境中，信任是评估代理

对于被评估代理在某既定时间内，按照双方已达成一致的内容，成功地提交该行为的意愿和能力的信念。

总之，信任是一个很广阔的概念，它与忠诚、信赖、安全、可靠和能力等概念都有联系；另外，它在多个学科领域都有涉及，如心理学、社会学、经济学、进化生物学、组织行为学、哲学以及计算机科学等。

文献[9]提出一种方法，将社会学、哲学、管理学、经济学和政治学等领域对信任的研究成果进行划分，从概念上把信任分为六大类。

(1) 倾向信任(disposition)：即人们自然地倾向于信任实体 A。

(2) 环境信任(situation)：即实体 A 信任某一特定的情景(scenario)。

(3) 结构信任(structure)：即实体 A 客观地相信结构 B 是某个整体的一部分。

(4) 信念信任(belief)：即实体 A 相信实体 B 是值得信赖的。

(5) 意图信任(intention)：即实体 A 乐于依靠实体 B。

(6) 行为信任(behaviour)：即实体 A 自愿依靠实体 B。

本书所研究的信任应属于第 4 种信任，即信念信任。我们可以将信任定义为：实体 A 根据相关证据对实体 B 在一定环境下完成特定行为的一种信念。信任具有以下几个主要特征：

(1) 主观性，即信任是一种信念，是一种主观评价。

(2) 非对称性，即实体 A 信任实体 B 并不意味着 B 也信任 A。

(3) 动态性，即实体 A 在经验及所掌握的信息发生变化的情况下对于 B 的信任也会发生变化。

(4) 非完全传递性，即实体 C 向 A 推荐其信任的 B，而 A 根据自己的经验并非一定信任 B。

(5) 环境相关性，即实体 A 在特定环境下信任 B 并不意味着在其他环境下也信任 B。

1.1.2 信任管理

1996 年，M. Blaze 等学者为解决 Internet 网络服务的安全问题首次使用了“信任管理(trust management)”的概念[10]，并在此基础上研制了相应的信任管理系统 PolicyMaker[10] 和 KeyNote[11]。M. Blaze 等人将信任管理定义为采用一种统一的方法描述和解释安全策略、安全凭证以及用于直接授权关键性安全操作的信任关系。基于该定义，信任管理的内容包括制订安全策略、获取安全凭证以及判断安全凭证集是否满足相关的安全策略等。这类信任管理系统的意义在于提供了一个基于安全凭证的、独立于具体应用的、综合的安全决策框架。其本质是使用一种精确的、理性的方式来描述和处理复杂的信任关系。但在这种信任管理思想提出之前和之后，都有一些学者，如 A. Abdul-Rahman 等人认为信任是非理性的[12,13]，是一种经验的体现，不仅要有具体的内容，还应有程度的划分。

A. Abdul-Rahman 等学者从信任的概念出发，对信任内容和信任程度进行划分，并从信任的主观性入手给出信任的数学模型用于信任评估。D. Povey 在 M. Blaze 定义的基础上，结合 A. Abdul-Rahman 等人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，即信任管理是信任意向的获取、评估和实施[14]。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期，取决于经验，并随着客体行为的结果变化而不断修正。

这类信任模型所关注的内容主要有信任表述、信任度量和信任度评估。这样的一个信任模型与安全策略的实施相结合同样可以构成一个一般意义上的信任管理系统。

我们把上述两种不同类型的信息管理思想分别称为基于凭证的信息管理和基于行为的信任管理，即 M. Blaze 等学者所研究的信任管理模型是一种基于凭证的信任管理模型，而 A. Abdul-Rahman 等人提出的主观信任模型实质上是一种基于行为的信任管理模型。

1. 基于凭证的信任管理

PolicyMaker 是 M. Blaze 等人依据他们所提出的信任管理思想较早实现的信任管理系统，PolicyMaker 为网络服务安全授权提供了一个完整而直接的解决方法，取代了传统的认证和访问控制相结合的做法，并且给出了一个独立于特定应用的一致性证明验证算法，用于服务请求安全凭证和安全策略的匹配。PolicyMaker 是一个实验性质的信任管理系统，其功能相对简单，不提供安全凭证的收集和验证的功能。应用系统必须负责收集并保证足够的安全凭证用于验证相关的操作请求，还需根据安全凭证的公钥信息验证其可靠性，而 PolicyMaker 仅根据应用系统输入的操作请求安全策略集和安全凭证集来完成最后的一致性证明验证工作。这种信任管理引擎与应用系统的功能划分加重了应用系统的负担，而且可能会因为安全凭证收集不充分而导致一致性证明验证的失败。但应用系统负责安全凭证的可靠性验证，使其在选择签名算法时具有一定的灵活性[15]。

KeyNote 是 M. Blaze 等人实现的第 2 个信任管理系统。不同于 PolicyMaker，KeyNote 在设计之初就希望能够促进信任管理系统的标准化并使其易于集成到应用系统中。为此，KeyNote 在系统的设计和实现上与 PolicyMaker 存在着很大的差别。目前，KeyNote 已在 IPsec 协议和网上交易的离线支付等方面进行了一些应用研究。KeyNote 采用一种类似于电子邮件信头的格式来描述安全策略和安全凭证断言。KeyNote 提供一种专门的语言来描述安全策略和安全凭证断言，并且负责安全凭证的可靠性验证。这样一方面减轻了应用系统的负担，使 KeyNote 更容易与应用系统集成；另一方面则有利于安全策略和安全凭证描述格式的标准化，使应用系统能够更有效地传播、获取以及使用安全策略和安全凭证。

REFEREE[16]是 Y. H. Chu 等人为解决 Web 浏览安全问题而开发的信任管理系统。虽然其设计目标比较单一，但可以较完整地实现信任管理模型所列出的各要素。REFEREE 采用了与 PolicyMaker 类似的完全可编程的方式描述安全策略和安全凭证。在 REFEREE 系统中，安全策略和安全凭证均被表达为一段程序，但程序必须采用 REFEREE 约定的格式来描述。REFEREE 灵活的一致性证明验证机制一方面使其具有较强的处理能力，另一方面也导致其实现代价较高。而允许安全策略和安全凭证程序间的自主调用则存在较大的安全隐患。另外，必须看到 REFEREE 的验证结果可能会出现未知的情况。REFEREE 能够在一致性证明验证时自动收集并验证安全凭证的可靠性，应用系统仅需给出初始的安全策略安全凭证和验证内容以及一些必要的验证上下文信息。这一点有利于该信任管理系统的使用。

2. 基于行为的信任管理

1) A. Abdul-Rahman 信任管理模型

A. Abdul-Rahman 信任管理模型是基于社会学特征的信任模型，该模型支持下面的一些社会信任属性：

(1) 信任是依赖于上下文的；

(2) 尽管在一个小的信任值范围内，该模型支持 Agent 诚信的消极和积极信任度；

(3) 信任是基于以前的经验，代理能够识别重复有相似背景和相同代理商的经验；

(4) Agent 通过推荐交换评估信息，从而支持了声誉机制以协助信任决策；

(5) 信任是不可传递的，所有推荐的信任将考虑到推荐的源的信任；

(6) 信任是主观的，不同的观察者对于相同的代理的诚信度可能有不同的看法；

(7) 信任是动态的和非单调的，进一步的经验和推荐能提高或降低另一名代理人的信任程度；

(8) 只有人际信任的支持，在这个阶段中，我们排除倾向性和系统信任。

A. Abdul-Rahman 提出的模型是基于经验和声望的行为信任模型，该模型允许实体决定哪些实体是值得信赖的，并且允许实体调整关于其他实体推荐的知识。该模型可描述为：

(1) 实体直接信任的集合 Q；

(2) 推荐者集合 R；

(3) $C=\{c_1,c_2,\cdots,c_n\}$是实体 x 所知的上下文环境集合；

(4) $A=\{a_1,a_2,\cdots,a_n\}$代表一组实体，直接或者间接与实体 x 进行交易；

(5)经验 e 的结果级别为：$E=\{\mathrm{vg},g,b,\mathrm{vb}\}$。

直接信任评估：直接信任是在一定的上下文中，一个实体信任另一个实体的可信度，用 td 表示。其值的计算取决于直接交易的经验结果：

$$\exists\,\mathrm{td}\in E\,\forall s_e\in s,(s_e=\max(s))\Rightarrow(\mathrm{td}=e);\tag{1.1}$$

其中，s_j 是当经验 $e=j$ 时的经验累加值；如果 $\max(s)$返回的是多个值，那么 td 被分配为不确定的值有如下 3 种情况：当 e 为 vg^g^? 时，td 为 u+，意为：大部分是好的，小部分是不好的；当 e 为 vb^b^? 时，td 为 u−，意为：大部分不好，小部分好；当 e 为其他组合的时候，td 为 u0，意为：不好的和好的一样多。

推荐信任：在特定的上下文中 c，一个实体 a 对另一个实体 b 的信任程度 rtd 是由其他实体的推荐信任所给出的。当决定实体 a 在上下文环境是 c 的推荐信任 rtd 时，首先能找到实体 a 在推荐集合 R 里的一个关系(c,a,t)，其中 $t=(T_{\mathrm{vg}},T_g,T_b,T_{\mathrm{vb}})$，$T_a=T_{\mathrm{vg}}\cup T_g\cup T_b\cup T_{\mathrm{vb}}$。所以 rtd 的值为

$$\mathrm{rtd}=\mathrm{mod}(\{\forall x\in T^a\,||\,x\,|\})\tag{1.2}$$

在 A. Abdul-Rahman 的模型中，除了直接信任和推荐信任的评估，还要进行语义距离的评估和推荐本身的信任评估，评估值公式分别为：

$$\forall e\in E,\mathrm{sd}_e=\mathrm{mod}(T_e)\tag{1.3}$$

$$\mathrm{rd}^*=\mathrm{rd}\oplus\mathrm{sd}_{\mathrm{rd}}\tag{1.4}$$

最终的信任值更新包括了更新经验和结合推荐：

$$s_e=s_e+1\tag{1.5}$$

$$T_{\mathrm{rd}}=T_{\mathrm{rd}}\cup\{(e\diamond\mathrm{rd})\}\tag{1.6}$$

$$\forall e\in E\,\forall w_i\in L_e,\quad \mathrm{sum}_e=\sum^{|L_e|}w_i\tag{1.7}$$

其中，w_i 为推荐者的权重，L_e 为那些与 e 的推荐者相关的权重。

2) Beth 信任管理模型

Beth 信任管理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度推导和综合计算公式。在 Beth 信任管理模型中，经验被定义为对某个实体完成某项任务的情况记录。对应于任务的成败，经验被分为肯定经验和否定经验，若实体任务成功则对其肯定经验记数增加，若实体任务失败则否定经验记数增加。模型中的经验可以由推荐获得，而推荐经验的可信度问题同样是信任问题。为此，模型将信任分为直接信任和推荐信任，分别用于描述主体与客体、主体与客体经验推荐者之间的信任关系。即主体对客体的经验既可以直接获得，又可以通过推荐者获得，而推荐者提供的经验同样可以通过其他推荐者获得。直接信任关系和推荐信任关系形成了一条从主体到客体的信任链，而主体对客体行为的主观预期则取决于这些直接的和间接的经验。Beth 信任管理模型所关注的内容主要有信任表述、信任度量和信任度评估。信任度评估是整个信任管理模型的核心，因此信任管理模型也称为信任度评估模型。信任度评估与安全策略的实施相结合同样可以构成一个一般意义上的信任管理系统。P. Herrmann 等人提出了一个“信任适应的安全策略实施”(Trust-adapted Enforcement of Security Policy)的概念，并在这方面做了一些初步的研究。

直接信任定义为“若 P 对 Q 的所有(包括直接的或由推荐获得的)经验均为肯定经验，则 P 对 Q 存在直接信任关系”。当 Q 被信任时，Q 能成功完成任务的概率被用于评价这种信任关系，而概率的计算则取决于 P 对 Q 的肯定经验记录。Beth 采用式(1.8)描述直接信任度与肯定经验记录的关系：

$$V_q(p) = 1 - a^p \tag{1.8}$$

其中，p 是 P 所获得的关于 Q 的肯定经验数，是对 Q 成功完成一次任务的可能性期望。式(1.8)基于 Q 完成一次任务的可能性在[0,1]上服从均匀分布这一假设。

推荐信任定义为“若 P 愿意接受 Q 提供的关于目标实体的经验，则 P 对 Q 存在推荐经验关系”。Beth 采用肯定经验与否定经验相结合的方法描述推荐信任度。推荐信任度与经验记录的关系采用如下公式描述：

$$v_r(p,n) = \begin{cases} 1 - a^{p-n} & p > n \\ 0 \end{cases} \tag{1.9}$$

其中，p 和 n 分别是 P 所获得的关于 Q 的肯定经验和否定经验数。

在 Beth 信任管理模型中，经验可以通过推荐获得。而对于同一个信任关系，多个不同的经验推荐者可能形成多条不同的推荐路径。这就需要有一个计算方法能够推导并综合所有推荐路径的经验信息，以获得一致的信任度。Beth 分别对直接信任和推荐信任进行了讨论，并给出了相应的信任度推导和综合计算公式。假设 A 对 B 的推荐信任度为 V_1，B 对 C 的直接信任度为 V_2，B 对 D 的推荐信任度为 V_3，则 A 对 C 的直接信任度推导公式表述为

$$V_1 \odot V_2 = 1 - (1 - V_2)^{V_1} \tag{1.10}$$

A 对 D 的推荐信任度可以简单地表述为 $V_1 \times V_3$。Beth 模型还给出了推荐信任度综合计算公式：

$$V_{\text{com}} = \frac{1}{n} \sum_{i=1}^{n} V_i \tag{1.11}$$

其中，V_i 是由单个推荐路径推导出的信任度，综合推荐信任度 V_{com} 是这些单个信任度的简

单算术平均。设 $P_i(i=1,2,\cdots,m)$是推荐路径上各不相同的最终推荐实体，V_{ij}表示其最终推荐实体为 P 的各条推荐路径的信任度，则直接信任度综合计算公式表述为

$$V_{\text{com}} = 1 - \prod_{i=1}^{m} n_i \sqrt{\prod_{j=1}^{n_i}(1-V_{i,j})} \tag{1.12}$$

式(1.12)考虑了同一个经验推荐者出现在不同推荐路径上的情况。相同经验信息经不同的路径被多次传递，产生不同的推导结果。该公式采用取推导值平均的方法得到一个唯一值。

在 Beth 信任管理模型中，以实体完成任务的期望为基础，根据肯定经验和否定经验计算出实体能够完成任务的概率，并以此概率作为实体信任度的度量，给出了信任推导和综合规则及相应的信任度的计算方法。但该信任管理模型的不足之处在于简单地应用概率模型对主观信任进行建模，实际上将信任的主观性和不确定性等同于随机性，在多个推荐信任值进行综合时，简单地采用了均值的方法，因而无法真实地反映信任关系的真实情况。除此之外，Beth 模型对直接信任的定义比较严格，仅采用肯定经验对信任关系进行度量。另外，其信任度综合计算采用简单的算术平均，无法很好地消除恶意推荐所带来的影响。

3) Jøsang 信任管理模型

A. Jøsang 提出了基于主观逻辑(sub-jective logic)的信任管理模型，引入了证据空间(evidence space)和观念空间(opinion space)的概念来描述和度量信任关系，并定义了一组主观逻辑(Subjective Logic)运算子用于信任度的推导和综合计算[17]。

证据空间由一系列实体产生的可观察到的事件组成。实体产生的事件被简单地划分为肯定事件(positive event)和否定事件(negative event)。Jøsang 基于 Beth 分布函数描述二项事件(binary event)后验概率的思想，给出了一个由观察到的肯定事件数和否定事件数决定概率确定性密度函数 pcdf，并以此来计算实体产生某个事件概率的可信度。设概率变量为 θ，r 和 s 分别表示观测到的实体所产生的肯定事件数和否定事件数，则 pcdf 公式表述为

$$\varphi(\theta \mid r,s) = \frac{\Gamma(r+s+2)}{\Gamma(r+1)\Gamma(s+1)}\theta(1-\theta)^3 \quad 0 \leqslant \theta \leqslant 1, r \geqslant 0, s \geqslant 0 \tag{1.13}$$

观念空间由一系列对陈述的主观信任评估组成。主观信任度由三元组 $W=\{b,d,u\}$描述。该三元组满足

$$b+d+u, \{b,d,u\} \in [0,1]^3 \tag{1.14}$$

其中，b、d、u 分别描述对陈述的信任程度、不信任程度和不确定程度。

Jøsang 使用如下公式将 ω 定义为观念空间中肯定事件数 r 和否定事件数 s 的函数：

$$b = \frac{r}{r+s+1}, \quad d = \frac{s}{r+s+1}, \quad u = \frac{1}{r+s+1} \tag{1.15}$$

并认为 ω 与 pcdf 在主观信任度的表达上是等价的，即可以通过观念空间的统计事件来描述主观信任度。

在 Jøsang 信任管理模型中提供了一套主观逻辑算子，用于信任度之间的运算。其主要的运算有合并(conjunction)、合意(consensus)和推荐(recommendation)。其中，合并用于不同信任内容的信任度综合计算；合意根据参与运算的观念(信任度)之间的关系分为独立观念间的合意、依赖观念间的合意和部分依赖观念间的合意 3 类(所谓观念依赖是指观念是否部分或全部由观察相同的事件形成)，合意主要用于对多个相同信任内容的信任度综合计

算；推荐主要用于信任度的推导计算。详细的主观逻辑算子的描述参见文献[36]。

与 Beth 模型相比，Jøsang 模型对信任的定义较宽松，同时使用了观念空间中的肯定事件和否定事件对信任关系进行度量。模型没有明确区分直接信任和推荐信任，但提供了推荐算子用于信任度的推导。Jøsang 模型的信任度使用三元组来表示，而不是 Beth 模型中的单一数值。但 Jøsang 模型同样无法有效地消除恶意推荐带来的影响。另外，在 Jøsang 信任管理模型中提供了一套主观逻辑算子，用于信任度之间的运算，因此 Jøsang 模型实际上也认为信任的主观性和不确定性与随机性是等同的。

1.2　信任度评估

如前所述，主观信任管理所关注的内容主要有信任的表述、信任度量和信任度评估，其中信任度评估是核心。信任度评估定义了信任关系的量化表示方法、操作、信任关系的传递途径和计算方法。信任度评估采用一种相对的方法对安全信息进行度量和评估，其直接目的是为信任决策提供支持以确立信任关系，与安全策略的实施相结合可以构成一个一般意义上的信任管理系统。信任度评估可以抽象地理解为用一个或者一组算法对影响主体信任度的相关证据进行处理并获得信任度的过程。

1.2.1　信任度评估证据

目前信任度评估所依据的证据通常有两类，即凭证证据和行为证据。凭证证据是指网络主体所拥有的某些数字凭证。基于凭证证据的信任评估通常运用在安全授权、访问控制及信任协商等系统中，这类信任度评估的基本思想是：如果主体 B 拥有并提供主体 A 所要求的相关数字凭证，那么 A 就信任 B。行为证据是指可证明网络主体的网络行为的事实或者记录。相对于基于凭证证据的信任度评估，有人将基于行为证据的信任度评估称为主观信任度评估，这类信任度评估的主要思想是通过考察主体过去的行为来判断是否信任该主体。

在进行信任度评估时需要对证据进行处理，其基本方法是根据原始证据提取出影响目标主体信任度的因子（本书称之为信任因子），并根据需要选取一组影响因子进行信任度评估。

现有信任度评估模型中最常出现的信任因子主要有交易额、交易量、交易时间、交易结果和交易评价等。

（1）交易额和交易量。交易额和交易量是对货币与货物的计量，通常情况下人们对于交易额和交易量较高的交易会比较重视，所以交易额和交易量较高的证据在信任评估中对于信任度的影响程度也应该较高。因此，很多学者将交易额和交易量作为信任因子引入自己的信任评估模型中。另外，网络上的交易行为不仅限于货物与货币的交换，在其他交易活动中，交易额和交易量可演化为其他标识交易重要程度的变量，比如在网格计算中演化为运算量或者数据交换总流量等。

（2）交易时间。随着时间的推移，主体在某一时刻的行为对于主体信任的支持力度将会衰减，这与人类社会中人与人之间的信任关系的特点相一致。通常情况下，对于多年未见并失去联系的老友，我们可能很难像以前那样信任他了。因此在很多信任评估模型中，时间