<<信任管理与网络安全>>

图书基本信息

书名：<<信任管理与网络安全>>

13位ISBN编号：9787302310211

10位ISBN编号：7302310211

出版时间：2012-11

出版时间：清华大学出版社

作者：蒋文保

<<信任管理与网络安全>>

内容概要

《信息安全理论与技术系列丛书:信任管理与网络安全》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。

<<信任管理与网络安全>>

书籍目录

第1章信任管理概述 1.1信任与信任管理1 1.1.1信任 1 1.1.2信任管理 2 1.2信任度评估7 1.2.1信任度评估证据 7 1.2.2信任度评估算法设计8 1.2.3信任度评估模型分类 9 1.3信任协商 11 1.3.1信任协商概述11 1.3.2信任协商关键技术 12 1.3.3信任协商方案14 1.4本章小结 16 参考文献 16 第2章基于多维证据的信任度评估模型 2.1多维证据19 2.1.1 电子商务类业务反馈证据 19 2.1.2 网络社区类业务反馈证据 20 2.1.3网络操作行为证据20 2.2 D—S证据理论及合成规则改进 21 2.2.1 D—S证据理论的基本原理 21 2.2.2 D—S合成规则改进24 2.2.3 G—Gh合成规则的评价 26 2.3 EBTrust信任度评估模型28 2.3.1模型框架 28 2.3.2证据的采集29 2.3.3证据的形式化处理29 2.3.4基本信任函数的构造 31 2.3.5证据权重的计算与处理33 2.3.6信任度的计算和管理35 2.4 EBTrust信任度评估模型的实验分析 36 2.4.1 信任度计算和管理模块的设计与实现 36 2.4.2实验分析 39 2.5本章小结 41 参考文献 42 第3章基于行为检测的信任度评估技术 3.1 网络行为检测技术 43 3.1.1入侵检测的基本概念43 3.1.2入侵检测系统的功能结构 44 3.1.3入侵检测系统的分类 45 3.1.4入侵检测的分析方法 46 3.2 基于行为检测的信任度评估模型 49 3.2.1 模型框架 49 3.2.2工作流程 50 3.3基于行为检测的信任度评估算法 51 3.3.1信任度表示与度量 51 3.3.2算法描述 51 3.3.3算法实例 53 3.3.4实验分析 54 3.4本章小结 55 参考文献 55 第4章 自适应自动信任协商模型 4.1 自适应自动信任协商模型框架56 4.2自适应自动信任协商工作流程58 4.3 自适应策略模式及分析60 4.3.1 自适应策略模式60 4.3.2实验分析 62 4.4一致性校验器63 4.4.1访问控制策略描述 64 4.4.2一致性校验算法65 4.4.3完备性分析68 4.5本章小结 69 参考文献 69 第5章 自适应信任协商系统设计 5.1系统总体设计70 5.2系统模块设计 70 5.2.1主策略模块70 5.2.2检索引擎 71 5.2.3策略管理器72 5.2.4证书管理器 72 5.2.5一致性校验器模块 72 5.2.6可视化模块 72 5.2.7信任度评估模块 73 5.2.8外部接口设计 73 5.3 AATN—Jess策略语言 74 5.3.1策略语言设计需求 74 5.3.2 AATN—Jess语言特点 75 5.3.3 AATN—Jess语法结构 75 5.3.4 AATN—Jess策略语言编辑器 77 5.4本章小结78 参考文献78 第6章信任管理与P2P网络安全 6.1 P2P网络概述 79 6.1.1 P2P网络的定义 79 6.1.2 P2P结构与C／A结构的比较 80 6.2 P2P网络的信任机制 82 6.2.1 P2P网络安全问题82 6.2.2 P2P信任的特点83 6.2.3 P2P信任模型的分类84 6.3 P2P网络信任协商系统的设计与分析 85 6.3.1 NetTrust系统需求分析85 6.3.2 NetTrust系统设计 87 6.3.3信任协商功能的实现89 6.3.4信任协商功能测试与分析 91 6.4本章小结95 参考文献 95 第7章信任管理与网格安全 7.1网格计算概述97 7.2网格安全需求 101 7.3 一种基于多种证书的网格认证与授权系统 103 7.3.1若干术语与定义 103 7.3.2 CertGSl的安全策略104 7.3.3 CertGSl的框架结构 104 7.3.4多种证书 105 7.3.5身份认证 106 7.3.6访问控制 107 7.4一种基于属性证书的委托授权模型——ACDAM 108 7.4.1若干术语与定义 108 7.4.2 网格环境下的委托问题 109 7.4.3 ACDAM框架结构 110 7.4.4 ACDAM委托协议 111 7.5 一种支持信任管理的委托授权模型——TrustDAM 114 7.5.1 网格环境下的信任管理问题 114 7.5.2 TrustDAM框架结构 115 7.5.3信任和声誉的计算方法 116 7.5.4 TrustDAM委托协议 118 7._6本章小结 119 参考文献 119 第8章信任管理与网络诚信建设 8.1网络诚信概述121 8.2软件信任评价体系 121 8.2.1软件信任评价122 8.2.2软件信任评价模型框架 124 8.2.3实例分析128 8.3 网站信任评价体系 131 8.3.1网站信任评价131 8.3.2影响网站信任度的因素 132 8.3.3 ATEMW模型框架及模型检验 138 8.3.4实例分析 143 8.4 网络个人用户信任评价体系 147 8.4.1差别化网络实名制 147 8.4.2 网络个人用户评价指标体系 148 8.4.3信任评价 149 8.5本章小结151 参考文献 151

章节摘录

 插图： 3.一致性校验器 一致性校验器是信任协商的重要组成部分，它可以判定给定的信任凭证是否能够满足针对请求资源的本地策略，从而决定是否允许对方访问资源。
在一致性校验器验证证书是否满足访问控制策略时，一致性校验器首先验证信任凭证的有效性，进行匹配时过滤掉无效的证书。
传统的一致性校验器实现其基本功能。
当一致性校验器收到一组信息时，信息内容主要包括信任凭证集合、访问控制策略以及对某资源或服务的请求，一致性校验器检验凭证是否有效，有效凭证集合是否满足本地的访问控制策略。
根据验证的结果对请求者的请求作出响应，决定对请求者提供什么样的服务，或者是否提供服务。
自动信任协商对一致性校验器提出了更高的要求，自适应信任协商要求协商双方在一致性校验失败时，即对方提供的信任凭证不能满足本地的访问控制策略时，给对方有价值的反馈信息引导信任协商的进行，由于满足一条访问控制策略的信任凭证集合往往不止一个，所以当一方提供的凭证集合不能满足对方的访问控制策略时，并不代表此次协商没有成功地路径，这时需要给提供凭证的一方有价值的反馈信息才能引导信任协商的继续。
4.协商策略 在信任协商框架中，协商策略引导一个信任协商的成功。
协商策略控制暴露哪些证书，什么时候暴露这些证书，请求哪些证书来解锁本地的证书。
并不是所有的情况下信任协商都能成功。
信任协商过程中可能存在以下情况，协商一方不具备需要的证书，双方的证书的访问控制策略存在循环依赖。
协商策略决定请求者什么时候放弃协商会话。
协商策略必须具备以下特性：首先必须具备完整性，当一次协商存在成功的路径时，协商策略能够引导协商成功地进行，当协商不能成功时，能够终止信任协商，避免暴露不必要的信任凭证。
协商策略还应该具备高效性。
一个协商策略是一个函数，输入是当前的协商状态，输出是一方向另一方显示的一个信任凭证和访问控制策略的集合。
Winsborough等人在文献[29]中介绍了两种协商策略：热心策略和吝啬策略。
热心策略中，双方互相发送自己不受保护的证书，从而进一步解锁更多的证书，当客户端收到的证书无法再解锁更多的证书且无法满足服务访问控制策略时终止信任协商。
证书交换的次数依赖于双方拥有的证书数量，以及双方最长的证书依赖链长度。
吝啬策略中，首先披露服务访问请求以及服务访问控制策略。
如果请求方存在满足服务访问控制策略的证书集，且证书集不敏感，则披露证书集。
否则披露对应的访问控制策略，服务方做同样的处理，披露足够的访问控制策略直到存在不受保护的证书可以满足策略。

<<信任管理与网络安全>>

编辑推荐

《信息安全理论与技术系列丛书:信任管理与网络安全》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。

<<信任管理与网络安全>>

版权说明