基于认证数据结构模型的安全事务管理机制研究

胡显伟·著

辽宁人民出版社

基于认证数据结构模型的安全事务管理机制研究

胡显伟 著

辽宁人民出版社

图书在版编目（CIP）数据

基于认证数据结构模型的安全事务管理机制研究 / 胡显伟著. —沈阳：辽宁人民出版社，2012.1
ISBN 978-7-205-07262-9

Ⅰ. ①基… Ⅱ. ①胡… Ⅲ. ①电子邮件—安全技术 Ⅳ. ①TP393.098

中国版本图书馆CIP数据核字（2012）第006507号

出版发行：辽宁人民出版社
地址：沈阳市和平区十一纬路25号 邮编：110003
http://www.lnpph.com.cn
印 刷：沈阳全成广告印务有限公司
幅面尺寸：170mm×230mm
印 张：11.25
插 页：2
字 数：100千字
出版时间：2012年1月第1版
印刷时间：2012年1月第1次印刷
责任编辑：艾明秋 娄 瓠
封面设计：杜 江
版式设计：王珏菲
责任校对：周 健
书 号：ISBN 978-7-205-07262-9
定 价：25.00元

法律顾问：陈 光 咨询电话：13940289230

摘 要

随着计算机技术和网络的普遍应用，在Internet上时刻都在进行着大量的数据查询和事务处理。传统的数据结构是按一种或多种特定关系组织起来的数据集合，其拥有者和使用者都是同一个实体，它提供对数据集合的高效查询并返回查询结果。随着Web Service和Pervasive计算技术的出现，数据结构的所有者和使用者往往不再是同一个实体，这样就产生了数据结构被非法篡改（数据内容的篡改、数据关系的篡改等）的可能性。在分布式环境下，数据源通常被存放在离用户较近的缓存服务器（响应服务器）上，以期获得较高的数据访问效率。但这给安全问题带来了新的挑战，即如何保证所有数据和事务的完整性以及端到端的可信性，是一个亟待解决的研究课题。

认证数据结构是一个分布式计算模型，由目录或响应者代替可信的数据源对用户的查询请求进行应答，并为用户提供一个验证应答是否正确的密码学证明。数据源对数据内容（按照某种数据结构的方式来组织和存储）的密码学摘要进行签名，并把它发送给目录。该签名的摘要和对应的查询应答证明与查询应答信息一同被目录或响应者应答给用户。为了验证查询应答的正确性，用户通过查

询应答证明来重新计算数据的摘要，然后把这个计算出来的摘要与数据源签名的原始摘要做比较来判断应答的真实性。

本文针对分布式环境下的大量数据与事务认证问题进行比较深入的研究，提出了基于认证数据结构模型方法的解决方案。为实现这个新构思，从解决其基本理论与关键技术问题为切入点，利用理论研究与实际方案构建相结合的方法，建立认证数据结构模型的理论框架体系以及认证代价分析与计算方法；构建了一个基于Web Service的认证数据结构服务模型；实现了一个基于可信DNS的安全电子邮件解决方案。主要在以下几个方面取得了一些研究成果：

（1）通过对认证字典相关定义的研究和分析，给出了认证数据结构模型的概念和定义，并从理论上给出了系统化的定义和描述。本文对认证数据结构模型的关键实现方法做了深入的研究和分析，给出了认证跳表的基本操作以及查询和认证实现算法。并将安全事务管理机制的相关计算抽象成一个认证数据结构模型，这为安全事务管理机制的深入研究奠定了理论基础。

（2）应用分层数据处理理论和概率统计方法从理论上对认证数据结构模型的认证代价进行分析，并给出了一个理论上的认证数据结构代价分析模型。该模型给出了认证数据结构模型的认证代价的相关定义、定理和计算方法，并利用分层数据处理理论对其进行了理论上的分析与证明。该模型的提出可以有效地对认证数据的代价进行分析，为今后进一步深入研究认证数据结构奠定了坚实的理论基础。

（3）认证数据结构的代价性能很大程度上依赖于所使用的哈希

函数和采用的哈希方案。如何设计一个高效的哈希方案，就成为构建认证数据实现方法的重要研究内容。应用分层数据处理理论的一个重要结论，即在数据结构本身保持不变的情况下，将哈希模式从数据结构中分离出来而独立的定义哈希模式，可以有效地降低查询应答代价。基于此思想本文设计了基于多维跳表的认证数据结构方法，与已有的实现方法技术相比，该方法具有计算代价低、存储量小的优点。

（4）针对电子邮件系统中存在的不安全因素，特别是垃圾邮件泛滥成灾的问题，应用认证数据结构模型并结合信誉认证机制，设计并实现了一个基于可信DNS的安全电子邮件解决方案。该方案保证了电子邮件的机密性、完整性和不可否认性，同时也为防止垃圾邮件的泛滥提供了有力的技术支撑。

（5）设计并实现了一个针对安全事务管理机制的基于Web Service的认证数据结构服务模型。给出了该Web服务的系统结构的四方实体，对实体间的通信过程做了详细的阐述，并对四方实体进行了类设计。采用SOAP消息格式以及基于XML的签名认证方案，将此封装成一个独立、快速、高效、平稳、富有弹性的安全事务管理Web服务。为网络环境下安全事务的建立、传递、保持、验证提供理论和技术上的支撑，并且可以与现有的Internet基础设施、协议、计算平台很好地进行无缝连接和协同工作，易于部署和维护。

关键词：安全事务管理；认证数据结构；分层数据处理理论；可信DNS；Web服务

Abstract

With the popularity of the computer technology and network, there are a large number of data querying and transaction processing in Internet all the time. Traditional data structure is a data collection organized by one or more specific relations, and its owners and users are the same entity, which provides highly efficient query on the data collection and returns the query results. With the advent of Web Service and Pervasive Computing technology, the owners and users of the data structure are usually no longer the same entity, which brings on the possibility that the data structure is to be illegally tampered (eg, data content's being tampered, data relations' being tampered). In a distributed environment, the data source is usually kept in the cache server (response server) in close to user, in order to get a higher efficiency of data access. But it causes new challenge to security issue, namely, how to ensure the integrity of all the data and transactions, and the credibility of the end-to-end, which is a research topic urgent to be solved.

Authenticated data structure is a distributed computing model, where responders or directory make a response to user's query request instead of data source, and provide a cryptography proof that can verify the response. Data source signs the digest of the data content (organized and stored by means of certain data structure), and sends it to the directory. This signed digest and the corresponding query response information and its proof are responded to users by directory or responders. In order to verify the correctness of the query response, users recalculate the digest of the data through the query response proof, and compare the calculated digest with the original signed digest, to judge the authenticity of response.

This paper makes an in-depth research to a large number of data and transaction authentication issues in distributed environment, and proposes the solutions based on the authentication data structure model. To achieve this new design, from the point of solving the basic theory and key technical issues, using the method combined by theoretical research and practical program constructions, we establish the theory framework of authenticated data structure model and the method of authentication cost analysis and calculation; construct a authenticated data structure service model based on Web Service; realize a Secure E-mail solution based on a credible DNS. There is some research production mainly in the following as-

pects:

(1) Through the research and analysis of authenticated dictionary, give the concept and definition of authenticated data structure model, and show the systematic definition and description in theory. We make a research and analysis on the key implement method of authenticated data structure model deeply, and give the basic operations of authenticated skip list , the query and authentication algorithms. We also abstract the related calculation in secure transaction management mechanism to an authenticated data structure model, which settles the theoretical basis for the further study of secure transaction management mechanism.

(2) Analyze the authentication cost of authenticated data structure model in theory, applying the hierarchical data processing theory and probabilistic statistical methods, and give a theoretical authenticated data structure cost analysis model. These models show the related definition, theorem and calculation method on the authentication cost of the authenticated data structure model and give theoretical analysis and prove using the hierarchical data processing theory. This model can efficiently do analysis on the cost of authenticated data, and settles a solid theoretical foundation for further research on authenticated data structure.

(3) The cost and performance of an Authenticated Data Struc-

ture almost completely depend on the hash function and hash scheme used in it. So how to design an efficient hash scheme becomes an important research topic on building a data authenticated method. An important conclusion has been drawn by the application of the hierarchical data processing, namely, under the circumstances of keeping the data structure itself unchanged, defining a hash scheme in an independent mode separated from that in a data structure can effectively reduce the cost of answer. Based on this idea this thesis designs the construction algorithm of Authenticated Data Structure based on the multi-way Skip List. Comparing with previous realization, this algorithm has lower calculation cost as well as smaller storage overhead.

(4) Aiming at the insecurity factors existing in E-mail system, especially the overrun of junk mail, we design and implement a credible DNS-based secure E-mail scheme by the Authenticated Data Structure model and the credibility authentication mechanism, which not only guarantees confidentiality, integrity and non-repudiation of E-mail, but also lend strong technical support to prevent the overrun of junk mail.

(5) We design and implement service architecture of authenticated data structure model based on Web Service for secure transaction management system. Give the four entities in the system struc-

ture of Web Service, exposit the communication process among the entities in detail, and make class design for the four entities. We adopt SOAP message formats as well as XML-based signature authentication scheme, package all the operations into an independent, fast, highly efficient, stable and flexible Web Service for secure transaction management. We provide theoretical and technical support in network environment for the establishment of security, transmission, maintenance and authentication, and can seamlessly connect and work together with the existing Internet infrastructure, agreements and computing platforms, which is easy to be deployed and maintained.

Keywords: Secure Transaction Management; Authenticated Data Structure; Hierarchical Data Processing Theory; Trusted DNS; Web Service

目 录

第一章 绪 论

1.1 信息安全所面临的主要威胁

随着计算机技术和网络技术的广泛应用，全球信息一体化的步伐越来越快，网络信息系统已经成为国家、企业、个人不可缺少的重要组成部分，并已经渗透到人们的日常生活、经济、军事、科技和教育等多个领域，其基础性、全局性的地位与作用日益加强。

但是，网络在给人们带来便利的同时也暴露出越来越严重的安全问题，例如，网页信息的非法篡改[1~4]、垃圾邮件的泛滥[5, 6]、电子商务中的身份的非法冒充及欺骗[7, 8]、网络中信息的非法获取和查看、甚至黑客攻击等。如果上述问题不能得到很好的解决，将会危及国家安全，引起社会混乱，造成重大损失。因此确保计算机和数据通信网络的安全已是人们广泛关注的问题，并成为计算机科学技术的热点研究领域[9, 10]。

目前信息安全所面临的主要问题[11, 12]有以下内容：

（1）非法入侵者

入侵者[13~15]是指利用不正当的手段窃取计算机网络系统的口令

和密码，从而非法进入计算机网络的人。入侵者通常分为以下三类：

假冒者：指未经授权使用计算机的人和穿透系统的存取控制冒用合法用户账户的人。

非法者：指未经授权访问数据、程序和资源的合法用户；或者已经获得授权访问，但是错误使用权限的合法用户。

秘密用户：夺取系统超级控制并使用这种控制权逃避审计和访问控制或者抑制审计记录的个人。

（2）恶意代码

代码是指计算机程序代码，可以被执行完成特定的功能。而恶意代码[16]就是指起破坏作用的计算机程序，如蠕虫病毒[17]就是典型的恶意代码。

（3）计算机病毒

计算机病毒[18]最早是由美国计算机病毒研究专家Fred Cohen博士正式提出的。《中华人民共和国计算机信息系统安全保护条例》认为："计算机病毒是指编制者在计算机程序中插入的破坏计算机功能或者数据，影响计算机使用并能够自我复制的一组计算机指令或者程序代码"。由于计算机病毒具有传染性、隐蔽性、潜伏性、多态性、破坏性，因此其对信息系统具有极大的破坏作用。

（4）网络拒绝服务

网络拒绝服务[19, 20]是指攻击者通过对数据或资源的干扰、非法占有、超负荷使用、对网络或服务基础设施的摧毁，造成系统永久或暂时不可用，合法用户被拒绝或需要额外等待，从而达到破坏的

目的。

（5）垃圾邮件

垃圾邮件[21, 22]（Spam）可以简单的定义为向未主动请求的用户发送的电子邮件广告、刊物、其他资料或者不良信息；没有明确的退信方、发信人、回信地址等邮件。垃圾邮件主要包括：商业广告，政治言论，色情邮件，蠕虫病毒邮件，恐吓、欺骗性邮件。这些垃圾邮件占用了邮件服务单位大量网络资源、系统资源、存储资源，浪费了服务器的处理资源；垃圾邮件攻击会导致系统瘫痪、服务中断；各种垃圾广告邮件，阻碍正常通讯，增加用户对邮件的处理时间；垃圾邮件作为病毒的主要传播方式之一，会导致系统崩溃、信息丢失等一系列严重的后果。

（6）网页信息的非法篡改

在互联网飞速发展的今天，Web网站已成为各个单位连接Internet与外界交流的主流渠道，但由于互联网在安全方面的脆弱性，使黑客对Web网站的攻击成为可能。很多黑客并不是一定要把Web服务器破坏掉，而是热衷于对服务器上页面的篡改，比如将一些标志企业形象的图标改换成其他无聊的图片，或者将页面重要内容信息进行篡改，误导浏览者等，这些问题都会使企事业单位遭受难以估量的损失。

1.2 分布式数据和事务认证

20世纪70年代以前，信息安全的主要研究内容是计算机系统中