基于SOA和PKI/PMI的访问控制方案

周光明，赵莉莉，彭长根
（贵州大学 计算机软件与理论研究所，贵州 贵阳 550025）

摘 要：构建安全、高效和公平的企业系统资源的统一访问控制系统，是目前一个重要的研究方向。分析了面向服务的架构技术（SOA）、面向角色的访问控制（RBAC）技术、公钥基础设施PKI和权限管理基础设施PMI在安全管理方面的作用，并重点分析了欧共体PERMIS工程的优缺点，在此基础上把SOA和PKI/PMI很好地结合起来构建了访问控制子系统，克服了PERMIS工程的不足，实现了企业系统的安全、高效的访问控制功能，为企业系统的访问控制提供了一种参考方案。

关键词：SOA；PKI/PMI；访问控制；安全性；公平性
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1673-629X(2009)04-0170-04

Access Control Systems Based on SOA and PKI/PMI

ZHOU Guang-ming, ZHAO Li-li, PENG Chang-gen
(Institute of Computer Software & Theory, Guizhou University, Guiyang 550025, China)

Abstract: It is an important research direction to build a safer, efficient and fair access control system for business system resources. Analyses the use of the service-oriented architecture (SOA) technology, role based access control (RBAC) technology, public key infrastructure (PKI) and privilege management infrastructure (PMI) in safety management, and analyses the advantages and disadvantages of the EC PERMIS. And then it builds access control subsystem in the base of integrating the SOA and PKI / PMI. So it overcomes the deficiencies of the PERMIS project, and has secure and efficient access control of enterprise system. And it provides a reference scheme for enterprise access control system.

Key words: SOA; PKI/PMI; access control; security; fairness

0 引 言

企业为了提高全球竞争力而进行构建适合我国企业的信息化、网络化的平台系统，整合企业资源，降低成本，提高客户服务水平时，会面临着多个系统之间的数据共享、统一实现系统的安全的访问控制管理、充分利用现有资源以节约企业信息化成本等众多的问题。这些问题的解决需要有一个好的系统设计架构和统一的简单易用的安全策略，通过面向服务架构SOA和PKI/PMI的结合可以为以上问题的解决提供一个良好的参考方案。

SOA(service-oriented architecture，也叫面向服务的体系结构或面向服务架构)，是由1996年Gartner最早提出的，是指为了解决在Internet环境下业务集成的需要，通过连接能完成特定任务的独立功能实体实现的一种软件系统架构。SOA是一个组件模型，它将应用程序的不同功能单元(称为服务)通过这些服务之间定义良好的接口和契约联系起来。接口是采用中立的方式进行定义的，它应该独立于实现服务的硬件平台、操作系统和编程语言。这使得构建在各种这样的系统中的服务可以以一种统一和通用的方式进行交互。SOA作为一种体系结构，目标就是要实现交互软件代理之间的松耦合。SOA具有三大基本特征：独立的功能实体、大数据量低频率访问、基于文本的消息传递。面向服务的结构SOA结合了模型驱动模型MDA和敏捷方法AM的优点，将平台无关模型、模型和实践连接起来得到一个一致的架构方法。

公钥基础设施(PKI，Pubic Key Infrastructure)又叫公钥体系，是一种遵循既定标准的密钥管理平台，是为网络应用提供加密和数字签名等密码服务及所需密钥和证书的管理体系。它可以为电子商务的开展提供一套安全基础平台的技术和规范。PKI基础设施采用数字证书来管理公钥，通过第三方的可信任机构——认证机构CA，把用户的公钥和用户的其他标识信息捆绑

收稿日期：2008-08-18
基金项目：教育部博士点基金项目(20070657003)；贵州大学引进人才科研项目(2007-040)
作者简介：周光明(1980-)，男，贵州威宁人，硕士研究生，主要从事计算机应用技术研究；彭长根，博士，教授，研究方向为密码学与信息安全。

在一起,在 Internet 网上验证用户的身份。PKI 方案的核心就是数字证书。由 CA 中心签发的证书叫公钥证书 PKC。PKI 的基本机制是定义和建立身份、认证和授权技术,然后分发、交换这些技术,在网络之间解释和管理这些信息。PKI 对数据加密、数字签名、防抵赖、数据完整性以及身份鉴别所需的密钥和认证实施统一的集中化管理,支持电子商务的参与者在网络环境下建立和维护平等的信任关系,保证信息传输及商务活动的网络化、电子化安全发展。

Privilege Management Infrastructure (PMI) 即权限管理基础设施或授权管理基础设施,是属性证书、属性权威、属性证书库等部件的集合体,用来实现权限和证书的产生、管理、存储、分发和撤销等功能。在 1997 年 X.509(V3)中定义了基本的属性证书语法(属性证书第1版本),在 2000 年发布的 X.509(V4)中定义了 PMI 的框架结构,其中定义了扩展属性证书的语法(第2版),定义了 PMI 模型,规定了委托路径处理,定义了标准 PMI 扩展集,并增加了目录服务对象定义。

PKI 和 PMI 之间的主要区别在于:PMI 主要进行授权管理,证明这个用户有什么权限,能干什么,即"你能做什么";PKI 主要进行身份鉴别,证明用户身份,即"你是谁"。

2002 年 12 月,Gartner 提出 SOA 是"现代应用开发领域最重要的课题",还预计到 2008 年,SOA 将成为占有绝对优势的软件工程实践方法,主流企业现在就应该在理解和应用 SOA 开发技能方面进行投资。文中正是结合了 SOA、PKI、PMI 理论和技术,来设计了企业资源的访问控制方案,具有一定的实际意义。

1　相关研究工作的比较

SAML 是安全性断言标记语言(Security Assertion Markup Language)规范的简称,是 2003 年初,由 OASIS 小组批准的,是基于 XML(可扩展标记语言)面向 Web 服务的架构。Rafae Bhatti 等人在开放系统中的联邦身份和特权管理一文[1]中,分析了 SAML 本身对单点登录效率不高,因为缺乏对授权和验证的支持,所以他们使用 X-GTRBAC(XML-based Generalized Temporal Role Based Access Control)去实现访问控制。但是对所有的策略都需要从 SAML 翻译成 X-GTRBAC,这就大大影响了效率和可理解性。Blobel 等人使用 PKI 对 HAR 对 HCSP 进行验证,使用 PMI 进行授权和访问控制[2],并对客户端用 Applet 进行安全通道的通信,增加了安全性,但是此平台是针对医院管理系统的,没有提出一个通用的架构,不具有通用性,且效率有待进一步测试。Gutierrez 等人提出了基于服务的架构来提供对访问控制的管理,对所有的应用程序提供统一的访问控制的管理[3],具有一定的通用性,但在组织架构模型上,是用他们自己提出的符号语言来表示的,没有形成标准,对于广泛的推广应用有难度,不利于多系统的集成。

李涛,徐建良等人将 PMI、基于角色和任务的访问控制引入到工作流管理系统中,扩展了基于角色的 PMI 授权策略[4]。杨柳等采用面向服务的架构方式(SOA)来架构电信运营支撑系统[5]。陈飞等人利用 PKI 技术来保证电子商务交易系统的安全,优点是保证了交易信息传输的安全性,但实际使用中可能会涉及到效率等问题[6]。王秋玲等人用 PMI 来控制 Web 资源安全访问,将角色写入属性证书,形成权力证书,通过权力证书间接为用户授权,可简化复杂的授权[7]。David 等人把 PKI 和 PMI 很好地结合起来[8],把证书分发子系统和权限验证子系统分离开来,所有的工作都建立在 X.509 标准之上,并把访问控制用 Java 语言做成 PERMIS API,这些接口可以从 http://sec.cs.kent.ac.uk/permis/中获得。这提高了可通用性,使得在众多系统中可以重用这些接口,为各企业的访问控制统一管理做出了重要贡献。但是,此平台也存在缺点:此平台假设访问控制决策单元 AEF 和访问目标可以在一个可信的局域网内互相安全地访问,但现实中这完全不可能,Internet 实际上是一个充满了变数、安全问题严重的网络。而且,这些接口没有做成 Web 服务,不利于跨平台的实现。另外,由于属性证书和公钥证书是绑定在一起的,所以没有对用户信息进行隐藏,当服务请求用户请求服务时,服务请求用户的某些隐私信息就可能暴露给服务提供者,但服务请求用户可能得不到所请求的服务,所以对服务请求用户来说会处于不利地位。

2　基于 SOA 和 PKI/PMI 的访问控制设计

实现 SOA 架构的技术有 CORBA、DCOM、Web Services 等,文中所讨论的是用 Web Services 技术来实现 SOA 架构设计的。Endrei 等人在文献[1]中提出了一个公式:Web services = XML + transport protocol (such as HTTP)。图1展示了在 SOA 中的协作。协作主要是通过"找到(find),绑定(bind)和调用(invoke)"来实现的。服务消费者向服务注册(Service Rigestry)提出请求调用满足条件的服务,服务注册(Service Rigestry)查找服务,如果服务存在,服务注册(Service Rigestry)给请求者提供接口协议和服务地址。请求者从而可以调用服务完成相关功能,这就实现了动态服务的过程[9]。

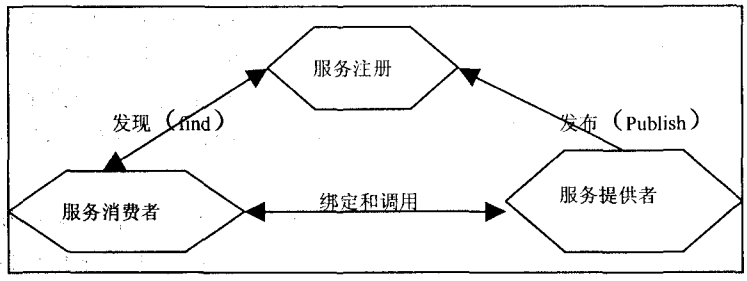

图 1 SOA 的各方协作

授权策略需要说明在哪种条件下,谁在哪种目标上被授予了哪种类型的行为能力。域管理组织(授权源组织)将规定整个域的策略,所以所有的目标将以相同的规则来控制。相应的授权策略语言也有多种,比如 Ponder 语言、Keynote 策略语言等。不过这两种语言都不适合我们的系统。我们需要一种既能被计算机轻易解析的策略语言,也能被各组织轻易阅读的策略语言。因此以 XML 语言作为策略说明语言,因为它已经变成了一种工业标准,且原 XML 语言可以被许多技术人员理解。由于需要一种适合于 X.509 和 RBAC 的语言,所以定义了数据类型定义(DTD)。

2.1 证书分发子系统

图 2 是证书分发的系统图,用户首先向 PKI 平台申请公钥证书 PKC,PKI 平台的 CA 中心校验用户相关信息满足要求后,分发公钥证书给用户,公钥证书由用户名和用户公钥绑定在一起而形成,用户拥有自己的私钥。同时 PKI 把用户公钥证书放到公钥证书 LDAP 目录中,以便于在验证时取用。如果某一用户的公钥证书被撤消,则由 PKI 发送证书撤消列表 ACL 到 LDAP 目录。

用户在获取 PKC 后,由 PMI 的授权证书分发器分配属性证书 AC 给用户,同时把用户 AC 放到属性证书 LDAP 目录中。

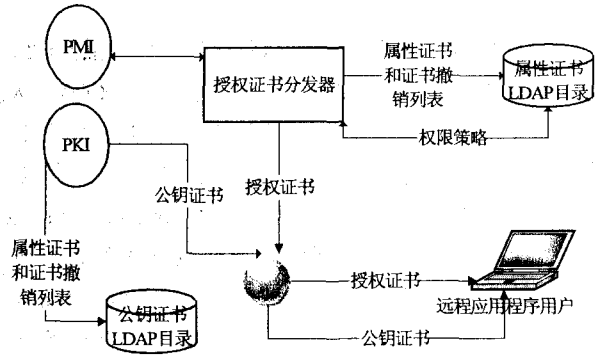

图 2 证书分发子系统

PMI 中一个非常重要的部分是访问控制,X.509 属性证书支持 MAC(Mandatory Access Control)和基于角色的访问控制 RBAC(Role - Based Access Control)。2000 年 NIST(National Institute of Standards and Technology)发布了基于角色的访问控制建议标准,定义了 RBAC(Role - Based Access Control)的参考模型。RBAC 相对于 MAC 和 DAC 而言,具有可控性和可测量性,因为角色数量相对用户数量来说会少得多[8]。所以在 AC 中采用的是 RBAC,并通过扩展基本 RBAC 到分层 RBAC(Hierarchical RBAC)来进行组织架构的分层管理,使得对角色的管理更加简洁。另外通过约束 RBAC(Constrained RBAC)来对证书的有效时间等进行管理。

2.2 访问控制子系统

从图 3 可以看出,把访问控制以 SOA 架构建立了企业服务总线 ESB,这样就把访问控制独立出来了,有利于众多系统进行共用。其整个流程如下:

1)远程服务提供者向 ESB 发出注册请求,ESB 通过验证注册请求者的公钥证书和属性证书,如通过验证则根据服务注册策略在 UDDI 服务注册中心进行注册。

2)远程服务请求者通过服务请求代理系统向 ESB 发出调用服务请求,ESB 通过验证请求者的公钥证书和属性证书,如通过验证则在 UDDI 服务注册中心查找相应的服务,如找到则可以两种方式进行处理:(1)ESB 直接调用相关服务,然后把调用结果返回给远程服务请求者;(2)ESB 不直接调用服务,只是把调用服务年需的相关信息返回给远程服务请求者,由远程服务请求者和远程服务提供者互相直接交互。具体采用哪种方式,可以根据具体情况而定。

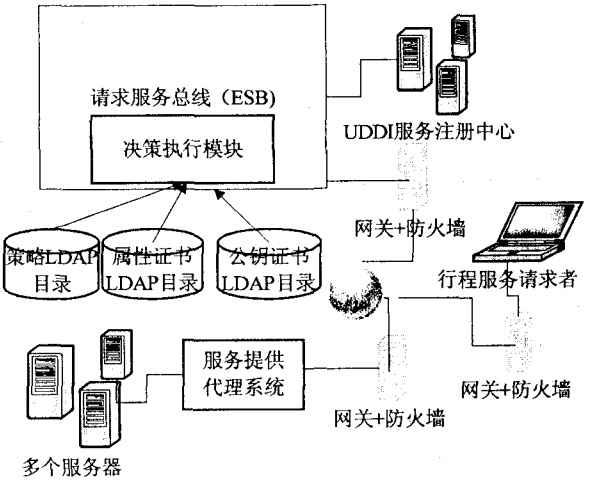

图 3 访问控制的逻辑结构图

下面对此子系统进行相应的分析:

①由于把访问控制子系统基于 SOA 架构建立起来,所以在构建决策执行模块时,可以用多语言来实现,因为 SOA 是跨平台的。

②在 ESB、远程服务提供者、远程服务请求者三者

之间的通信都是建立在安全的机制之上的,它们之间的会话采用 SSL 连接,因此保证了传输信息的安全性。这可以在 ESB、服务请求代理系统、服务提供代理系统中用 Java 的 JSSE 包来实现,在文献[10]中提供了用 Java 的 JSSE 包来实现 Java 应用程序的例子。这就克服了文献[8]中假设访问控制决策单元 AEF 和访问目标在一个可信的局域网内互相安全地访问的缺点。

③由于服务提供者在注册服务之前通过了验证,服务请求者在发送请求时也进行了验证,所以就不存在对哪一方不公平的现象,因为 ESB 是中立的,对于两方来说都进行了验证,不会使哪一方处于不利的地位。此种方式克服了文献[5]中没有对用户信息进行隐藏,当服务请求者请求服务时,服务请求者的某些隐私信息就可能暴露给服务提供者,但服务请求者可能得不到所请求的服务而导致处于不利地位的缺点。因为只要是注册成功的就能够访问。

3　结束语

提出了用公钥基础设施的公钥证书进行身份验证,用 X.509 属性证书进行访问控制的策略,把整个访问控制系统以面向服务架构 SOA 的方式建立起来,使得平台具有了跨平台性等众多优点,并在各方连接中使用 SSL 会话连接,保证了传输信息的安全性,以 ESB 作为中立的系统,保证了参与各方的公平性,为构建高效通用的访问控制系统提供了参考,有一定的实用价值和意义。在今后的工作中将进一步研究如何对参与各方的隐私信息进行有效保护以及在此系统中如何使代理能简单有效地实现。

参考文献:

[1] Bhatti R, Bertino E, Ghafoor A. An Integrated Approach to Federated Identity and Privilege Management in Open Systems[J]. Communications of the ACM, 2007, 50(2): 81 - 87.

[2] Blobel B, Hoepner P, Joop R, et al. Using a privilege management infrastructure for secure web - based e - health applications[J]. Computer Communications, 2003, 26: 1863 - 1872.

[3] Vela F L G, Montes J L I, Rodriguez P P, et al. An architecture for access control management in collaborative enterprise systems based on organization models[J]. Science of Computer Programming, 2007, 66: 44 - 59.

[4] 李　涛,徐建良,王晓燕. 基于 PMI 的工作流管理系统安全模型[J]. 微计算机信息,2008(9):57 - 59.

[5] 杨　柳,李秉智. SOA 架构下的电信运营支撑系统[J]. 微计算机信息,2007(1):248 - 249.

[6] 陈　飞,傅德胜. 基于 PKI 的电子商务交易系统及交易中信息安全的实现[J]. 微计算机信息,2004(5):115 - 117.

[7] 王秋玲,陈性元,张　斌,等. 基于 PMI 的 Web 资源安全访问控制系统设计[J]. 微计算机信息,2006(27):41 - 43.

[8] Chadwick D W, Otenko A. The PERMIS X.509 role based privilege management infrastructure[J]. Future Generation Computer Systems, 2003, 19: 277 - 289.

[9] Endrei M, Ang J, Arsanjani A, et al. Patterns: Service - oriented Architecture and Web Services (Redbook)[M]. [s.l.]: IBM TSO, 2004.

[10] 孙卫琴. Java 网络编程精解[M]. 北京:电子工业出版社,2007.

(上接第 159 页)

通过多段机器人足球比赛视频序列的验证,实验结果表明,文中提出的算法具有较高的准确性和鲁棒性。

4　结束语

提出了一种在复杂运动情况下基于卡尔曼滤波改进算法的目标跟踪新方法。在该新方法跟踪的过程中,对运动目标建立二维场景模型,对其下一运动可能发生的情况进行预判,在目标做复杂运动时,将其运动进行有效划分,并根据相关参数估计其后续状态。实验结果表明,该算法效率高,对不同的目标复杂运动均有很强的实用性。

参考文献:

[1] Arulampalam M S, Maskell S, Gordon N, et al. A tutorial on particle filters for online nonlinear/non - Gaussian Bayesian tracking[J]. IEEE transactions on signal processing, 2002, 50(2): 174 - 188.

[2] Moscheni F. Spatio - temporal segmentation and object tracking: An application to second generation video coding[D]. Lausanne: Swiss Federal Institute of Technology, 1997.

[3] 夏伟才,曾致远. 一种基于卡尔曼滤波的背景更新算法[J]. 计算机技术与发展,2007,17(10):134 - 136.

[4] Taubin G, Cooper D B. Object recognition based on moment (or algebraic) invariants[M]. [s.l.]: MIT Press, 1992: 375 - 397.

[5] LI Pei - hua, Zhang Tian - wen, MA Bo. Unscented Kalman Filter for Visual Cure Tracking[J]. Image and Vision Computing, 2004, 22(2): 157 - 160.

[6] 姚红革,耿军雪. 基于卡尔曼预测的视频目标实时跟踪[J]. 西安工业大学学报,2007,4(2):171 - 175.

[7] 陈　阳,周明全,耿国华. 基于卡尔曼滤波器的交通参数采集系统[J]. 微机发展(现更名:计算机技术与发展),2004,14(12):7 - 9.

[8] 王江涛,杨静宇. 遮挡情况下基于 Kalman 均值偏移的目标跟踪[J]. 系统仿真学报,2007,9(19):4216 - 4220.