基于互信属性调配机制的访问控制模型

王 立,万世昌,张 珍
(陕西师范大学 计算机科学学院,陕西 西安 710062)

摘 要:在基于属性的访问控制中一个重要的问题是对属性资源的获取以及对敏感属性和敏感访问控制策略的保护。传统访问控制属性资源的获取方法已经不能满足开放式的网络环境下的访问控制要求。在自动信任协商机制基础上提出了一种新的授权决策机制——互信属性调配机制(MTAD),并将其应用到基于属性的访问控制模型中。通过对模型的分析可以看到该模型较好地解决了动态授权、访问效率、授权粒度、属性信息的安全性和敏感属性的保护等问题。

关键词:访问控制;基于属性的访问控制;互信属性调配机制;自动信任协商机制
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2009)12-0127-04

Model for Mutual Trust Attribute Deployment Mechanism Based Access Control

WANG Li, WAN Shi-chang, ZHANG Zhen
(School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

Abstract: The important problems in attribute-based access control are how to acquire attribute resources and how to control the acess to sensitive informations. With the developments of the information technology, traditional methods of obtaining the resource can not meet the new network circumstances' needs. Based on the automated trust negotiation mechanism, a new authorized decision-making mechanism—mutual trust attribute deployment mechanism was proposed. It has been applied to the attribute-based access control model, and better solved the problem of dynamic authorization, property information's security and protecting privacy-sensitive property.

Key words: access control; attribute-based access control; mutual trust attribute deployment mechanism; automated trust negotiation mechanism

0 引 言

传统的基于角色的访问控制模型的授权是基于访问资源的主体的身份。但是在开放式的网络环境下,资源和请求者通常位于不同的安全域中,它们一般事先并没有建立联系,互不知晓彼此的身份。而基于角色的访问控制的口令机制也很难确定一个实体是否值得信任。而基于属性的访问控制(Attribute-Based Access Control,ABAC)机制比基于角色的访问控制机制更适合于这种开放的环境[1,2]。

在ABAC模型中,授权决策是基于请求者的属性。一般传统的对于请求属性的获取方法有客户端发送属性和资源端请求属性两种方法。由于他们对于属性资源的安全性和隐私保护都不能提供强有力的支持,因此已经不能满足在网络环境下基于属性的访问控制的需要。

自动信任协商机制(Automated Trust Negotiation,ATN)的提出较好地解决了信息保护与隐私保护的问题。然而为了防止攻击者利用ATN过程中的信息推测访问主体和访问资源拥有的某些属性,必须将敏感属性和非敏感属性做同样的处理,这样在用户较多的环境下系统将难以负担庞大的开支。

文中在自动信任协商机制的基础上提出了一种新的授权决策:互信属性调配(Mutual Trust Attribute Deployment Mechanism,MTAD)机制,并将其应用到基于属性的访问控制模型中。给出了基于互信属性调配(MTAD)机制的基于属性的访问控制模型。这种访问控制模型通过使用MTAD机制较好地解决了动态授权、授权粒度大、属性信息的安全性和敏感属性的隐私保护等问题。

收稿日期:2009-04-18;**修回日期**:2009-07-05
基金项目:国家自然科学基金资助项目(60673065)
作者简介:王 立(1984-),男,硕士研究生,研究方向为访问控制、信息安全;导师:李顺东,博士,教授,博士生导师,研究方向为访问控制、信息安全、电子商务。

1 ABAC 与 XACML 概述

1.1 基于属性的访问控制模型(ABAC) 概述

在 ABAC 中,授权决策是基于请求者的属性。这些属性通常用数字签名的凭证(属性证书)来建立。通过属性证书,凭证颁发者(属性权威,AA)可声明某实体具有哪些属性。

图 1 为 ABAC 访问控制框架[3]。

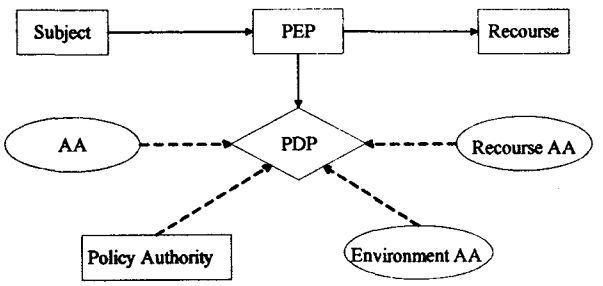

图 1 ABAC 访问控制框架

模型中术语的含义如下:

1)属性权威(Attribute Authority, AA):属性权威负责建立和管理主体属性、资源属性和环境属性。

2)策略执行点(Policy Enforcement Point, PEP):负责建立一个基于主体、资源、环境的属性的授权请求,并发送授权请求给 PDP;另外还要执行 PDP 的决策,即允许或拒绝对资源的访问请求。

3)策略决策点(Policy Decision Point, PDP):负责利用策略规则集来判断主体的访问请求是否满足要求,以便决定是允许还是拒绝请求,并将决策结果返回给 PEP。

4)策略权威(Policy Authority, PA):负责建立和管理访问控制策略,供 PDP 使用。策略中主要包含访问资源所需的决策规则、条件和其他约束。

1.2 访问控制请求/响应描述语言(XACML)概述

2003 年 OASIS(Organization for the Advancement of Structured Information Standards)制定了基于 XML (Extensible Markup Language)的访问控制策略和访问控制请求/响应描述语言规范——XACML(Extensible Access Control Markup Language)。作为一种基于属性的通用访问控制策略和请求描述语言,其能适应多种应用环境,使访问控制中间件的开发和使用成为可能,同时其拥有良好的扩展性[4]。

XACML 定义了访问请求和访问策略的语法,并且描述了访问请求判定的基本流程。在 XACML 中访问请求描述的自然语义为"在当前条件下,主体以某种方式访问资源",其中条件、主体、方式、资源是通过属性值来描述,具体在 XACML 中是通过<xacml:Environment>来描述条件,<xacml:Subject>来描述主体,<xacml:Resource> 来描述资源,<xacml:Action>来描述访问方式。

2 互信属性调配机制(MTAD)

2.1 相关定义

定义 1 属性证书。

资源请求者与资源提供者都是以属性证书作为唯一确定的实体。属性证书是资源请求者与资源提供者身份的唯一标识。资源请求者与资源提供者的属性证书由属性权威(AA)颁发,通过属性证书在 MTAD 系统注册来获得合法身份。

定义 2 访问方法。

在 MTAD 系统中访问方法被定义为一个资源请求者与资源提供者的共有属性。其中属性 attname 的取值记为 attname = value, value∈{ permit, deny, unsatisfy}。

定义 3 属性调配结果。

属性调配结果是属性匹配集(包括访问方法属性)和环境属性组成的一个集合。可用集合的形式表示为:

Result = {$Oatt_1 = Satt_1 = constant_1$, $Oatt_2 = Satt_2 = constant_2$, …, $Oatt_n = Satt_n = constant_n$, E_ constant}。其中 $Oatt_i$ 表示主体属性,$Satt_i$ 表示资源属性,$constant_i$ 为属性取值,E_ constant 是环境属性。

定义 4 属性匹配关系表。

属性匹配关系表是一张二维表。其中属性是由资源请求者与资源提供者所提供的属性和需要对方满足的属性组成。其中 Object - $Oatt_i$ 表示主体(资源请求者)提供的属性 i 的取值 $constant_i$,Object - $Satt_i$ 表示主体需要的客体属性 i 的取值 $constant_i$。Sbject - $Satt_i$ 表示客体(资源提供者)提供的属性 i 的取值 $constant_i$,Sbject - $Oatt_i$ 表示客体需要的主体属性 i 的取值 $constant_i$。在访问 MTAD 系统时,资源请求者与资源提供者提供的属性和需求的属性数是有限的,且具有匹配相关性,因此取值 $constant_i$ 在一个具体的环境下意义唯一。当且仅当属性 i 的上下取值相等时则属性 i 匹配成功。

表 1 为属性匹配关系表具体描述。

表 1 属性匹配关系表

Attitude 1	Attitude 2	…	Attitude $n-1$	Attitude n
Object - $Oatt_1$	Object - $Oatt_2$	…	Object - $Satt_1$	Object - $Satt_2$
Subject - $Oatt_1$	Subject - $Oatt_2$	…	Subject - $Satt_1$	Subject - $Satt_2$

定义 5 属性控制器。

属性控制器是 MTAD 系统与资源请求者和资源提供者属性的唯一接口。属性控制器一方面经过资源请求者与资源提供者的同意后把属性证书中的数据转化为属性匹配关系表能识别的属性值;另一方面属性控制器可以与公钥证书(PKC)结合完成属性的调配,并保证传输中安全性[5,6]。它只能读属性证书中有限的属性,防止暴露属性证书中的其他信息。它实现了对属性证书的一个"封装"(encapsulation)。把对属性证书中的数操作与属性证书分离,实现了数据的隐藏(information hiding)。

2.2　互信属性调配机制原理

MTAD 机制是一种基于属性的信任协商的策略。在这种机制中服务请求者和服务提供者处于对等的地位,都以其属性证书表示其身份。资源提供者和资源请求者通过在属性权威(AA)获得 X.509 属性证书,属性权威的数字签名保证了这种绑定的有效性和合法性。然后通过属性证书注册成为系统的合法用户。在互信属性调配机制中,资源提供者与资源请求者通过 MTAD 系统中的属性控制器调配属性证书中的属性然后在属性匹配服务模块进行属性匹配,在完成一次匹配以后将未匹配结果反馈给双方以进行下一次匹配,直至双方都获得满意的匹配结果或者一方拒绝与对方继续匹配。协商方法采用属性匹配关系表进行。

2.3　互信属性调配(MTAD)机制框架

图 2 是互信属性调配机制的框架图,其具体的调配流程如下:

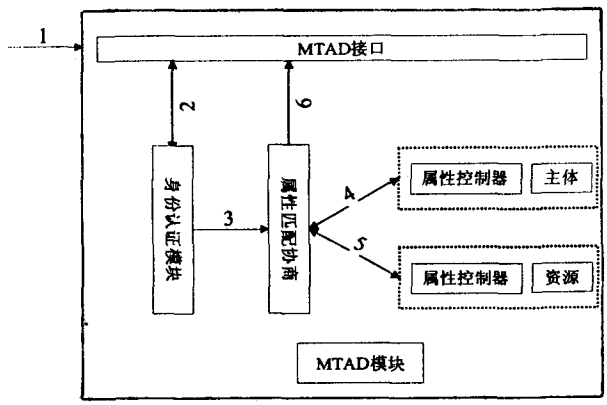

图 2　MTAD 过程示意图

(1) 访问者发送访问请求包括主体注册信息(一般为请求者 ID)和要访问的资源的注册信息(一般为资源名)。

(2) 通过在身份确认模块认证主体注册信息和资源的注册信息,确认双方是否是注册用户。若合法则进行第 3 步,并对主体和资源重定向(分配一个内存空间),准备协商。否则拒绝服务。

(3) 传递主体注册信息和资源的注册信息给属性调配协商服务模块,属性调配协商服务模块建立主体属性控制器和资源属性控制器。

(4) 属性控制器通过注册信息与主体和资源属性证书建立链接,若资源或者主体属性证书不与注册信息匹配,则返回拒接服务。否则进行下一步。

(5) 属性匹配:首先资源请求者与资源提供者都提供自己认为能够实现匹配的最小属性集和要求对方提供的属性集,通过属性控制器转化成属性匹配关系表中能识别的数据,在属性调配协商服务模块进行匹配。若双方都不能满足则把没有成功匹配的属性由属性控制器传递给资源请求者与资源提供者。然后在此基础上进行下一次调配(限定迭代次数)。最后获得双方的属性匹配结果。

(6) 将调配结果传递给 MTAD 接口。

2.4　MTAD 与传统属性获取方法比较

客户端发送属性。即客户端在请求访问某个服务时,随同请求一起将属性发送给策略执行点。这种属性获取方法使得资源请求者与资源提供者都处于盲目的状态。由于资源请求者事先不知道资源提供者需要什么属性,往往效率很低。而且这种方法不能保证资源请求者的属性的隐私性。

资源端请求属性。初始化客户端的访问请求后,资源端服务器请求客户端发送访问控制决策所需要的一些属性。这种访问控制的效率较高,但是资源请求者是被动的。资源请求者可能受到资源提供者的不合理的要求。

自动信任协商。它需要利用信任协商协议(如双方交换数字凭证)建立双方的信任关系。这种方法需要资源提供者和资源请求者不断交互,这使得协议的制定具有一定的复杂性或者不具备一般性,访问效率较低[7,8]。

MTAD 是一种在陌生人之间建立信任的方法,它以调配的方式完成了资源请求方和资源提供方的协商过程,并以面向对象方法对属性进行封装,保护了属性的安全性。通过属性调配大大提高了协商速度,降低了访问属性的粒度。在此过程中双方都只披露了自己最小粒度的属性信息,因此匹配力度小,效率高。

通过以上分析可以看出互信属性调配机制在安全性、粒度小等方面明显高于传统的属性获取方法,而其匹配效率和策略的复杂度明显高于自动信任协商机制。细心的读者可以发现,互信属性调配机制是建立在传统的属性请求方法和自动协商模型的基础之上,通过将互信属性调配机制简化可以得到传统的属性请求模型,因此 MTAD 兼容其他几种的属性请求方法,具有较强的兼容性。

3 基于 MTAD 机制的 ABAC 模型

3.1 模型架构

基于 MTAD 机制的 ABAC 模型构造如图 3 所示。

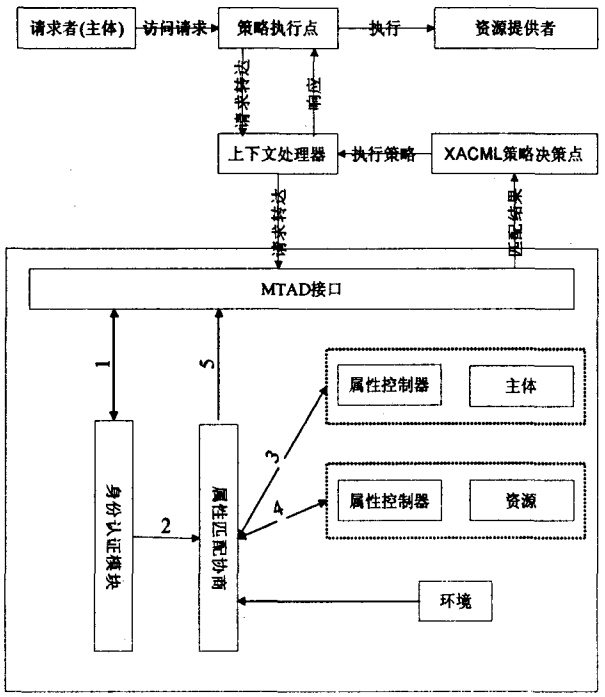

图 3 基于 MTAD 机制的 ABAC 模型

3.2 模型流程

图 3 为基于 MTAD 机制的 ABAC 模型。

在这个模型中，访问请求者并不告诉 ABAC 系统要以什么方式访问资源，只是告诉系统要访问资源的注册信息。也就是说访问请求只包含资源请求者和资源提供者的注册信息一般是双方的名称。若在 MTAD 中已经注册了主体和资源的信息，系统会经上下文处理器将两者的注册信息在 MTAD 的身份认证模块中认证。经过 MTAD 系统的处理(如前所述)，MTAD 系统将匹配好的属性信息和环境属性以属性调配结果的形式传递给 XACML 策略决策点。策略决策点将结果转化成相应的策略(一般用 SAML 表示)，然后经过上下文处理器映射成 XACML 格式。最终由策略执行点执行。

3.3 模型分析

改进的模型有以下几个优点：

(1) 避免了策略评估的复杂操作，通过属性控制器调配属性，并在属性匹配关系表中实现策略匹配，实现了对属性证书的“封装”。实现了对属性证书的操作与属性证书的属性的分离。

(2) 服务提供者和请求者相互并不了解对方的直接属性信息，通过服务匹配能够实现双方的“信息隐蔽”(information hiding)。数据隐藏有利于数据安全，防止误操作属性和非法操作属性。

(3) 整个协商过程由服务匹配完成，具有可追踪的特性。访问控制粒度更加细致，支持动态授权。

4 结束语

提出了一种互信属性调配机制(MTAD)，该机制继承了基于属性的访问控制中属性的概念。在此机制中通过对属性的匹配完成自动信任协商，提高了策略的执行效率，加强了隐私保护。另外，对资源和用户的属性的“封装”，提高了访问的安全性。最后将此机制应用到 XACML 下的 ABAC 模型中，解决了动态授权、授权粒度大、属性信息的安全性和敏感属性的保护等问题，具有一定的理论意义和实用价值。

参考文献：

[1] Sandhu R S, Coyne E J, Feinstein H L, et al. Role based access control models[J]. IEEE Computer, 1996,29(2):38 - 47.

[2] Park J, Zhang X, Sandhu R. Attribute mutability in usage control[C]// IFIP WG Working Conference on Data and Applications Security. Sitges, Spain:[s.n.], 2004:1 - 12.

[3] Yu T, Winslett M, Seamons K E. Supporting structured credentials and sensitive policies through interoperable strategies for automated trust negotiation[J]. ACM Trans. Inf. Syst. Secur., 2003,6(1):1 - 42.

[4] Yuan E, Tong J. Attributed Based Access Control (ABAC) for Web Services[C]// In ICWS'05: IEEE International Conference on Web Services. Orlando: IEEE, 2005:569 - 575.

[5] 田立勤，冀铁果，林 闯，等. 一种基于用户行为信任的动态角色访问控制[J]. 计算机工程与应用，2008,44(19):12 - 15.

[6] 李晓峰，冯登国，陈朝武，等. 基于属性的访问控制模型[J]. 通信学报，2008,29(4):90 - 98.

[7] 沈海波，洪 帆. 基于属性的授权和访问控制研究[J]. 计算机应用，2007,27(1):114 - 117.

[8] 许 峰，林果园，黄 皓. Web Services 的访问控制研究综述[J]. 计算机科学，2005,32(2):1 - 4.

中国计算机学会会刊、中国科技核心期刊
《计算机技术与发展》欢迎订阅，邮发代号：52 - 127