带有时间约束支持冲突检测的访问控制模型

张玉静,刘 军,李先珠
(解放军理工大学 指挥信息系统学院,江苏 南京 210007)

摘 要:为确保存储在系统中的访问策略都是无冲突的,提高策略冲突检测的效率,使系统能够正确有效的运行,将本体的概念应用到访问控制中,提出了一种基于本体的支持策略冲突检测的访问控制模型,并对该模型中的核心模块—策略冲突检测模块进行了详细说明。在此基础上,为使系统中的授权具有时效性,更加符合实际应用,将时间特征引入模型,根据时间约束的特征,将资源分为 4 类,细化了资源的类别,增强了系统授权的能力。最后,针对这 4 类资源的访问控制,给出了模型的时间约束算法。

关键词:访问控制;时间约束;本体;策略冲突检测
中图分类号:TP31 **文献标识码**:A **文章编号**:1673-629X(2015)02-0117-05
doi:10.3969/j.issn.1673-629X.2015.02.027

An Access Control Model of Supporting Conflict Detection with Time Constrains

ZHANG Yu-jing,LIU Jun,LI Xian-zhu
(College of Command Information Systems,PLA University of Science and Technology,
Nanjing 210007,China)

Abstract:In order to ensure the policies stored in the system are conflict-free,to improve the efficiency of strategy conflict detection and make the system operated correctly and effectively,apply the concept of ontology into the access control and propose an ontology-based access control model of supporting policy conflict detection,and has described policy detection engine in detail which is the core of the model. On this basis,the model has introduced the time constrains to make the system of authorization has timeliness. Then the resources can be divided into 4 categories according to the characters of the time constrains for corresponding to the reality,enhancing the capability of system authorization. Finally,propose a time constrains algorithm for this model according to the access control of four resource.

Key words:access control;time constrains;ontology;policy conflict detection

0 引 言

访问控制是保障数据安全的有效手段之一,通过安全策略描述系统高层安全需求是目前实现授权访问控制的主要途径[1]。在大型应用系统中就存在大量的安全策略,这些策略之间不可避免地会出现冲突问题。所谓策略冲突(Policy Conflict),就是指两条或多条策略在被执行时出现措施或结论相互矛盾的情况[2-3]。而本体是解决语义冲突的有效手段之一[4-6],因此,文中将本体引入访问控制,提出了一种基于本体的、能够支持策略冲突检测的访问控制模型。

由于访问控制中授权具有时间特性,任何形式的授权都不是永久的,都具有一定的时效性,即授权只在一定时间范围内有效[7],所以需要在模型中添加时间约束。具体地说,在资源的属性中添加时间约束,进而将资源进行分类,使模型具有了进一步刻画现实系统中授权的能力,这样既减少了对资源的不合理访问,又能提高访问控制的效率。

1 相关研究

1.1 策略描述语言 XACML

2003 年 OASIS 制定了基于 XML 的访问控制策略和访问控制请求/响应描述语言规范—XACML[8],它定义了一种通用的用于保护资源的策略语言和一种访问决策语言,允许开发者编写规定哪些用户可以访问

收稿日期:2014-02-19 **修回日期**:2014-05-25 **网络出版时间**:2014-12-27
基金项目:江苏省自然科学基金(BK2008090)
作者简介:张玉静(1989-),女,硕士研究生,研究方向为网络信息安全与对抗技术;刘 军,博士,硕士生导师,研究方向为信息安全。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20141227.1340.005.html

网络或互联网的策略,这种策略语言用来描述全面的访问控制需求。XACML 的资源访问控制策略是基于主体属性、资源属性和环境属性,而不是基于请求者的身份,提供了细粒度的访问控制机制。

1.1.1 XACML 中的术语

(1)主体(Subject):是系统中发起访问请求、具体操作资源的实体,主体包括用户、应用程序或进程等,有时也称为用户或访问者。

(2)资源(Resource):是主体要访问的实体,如:服务、数据或系统组件等。

(3)操作(Operation):是指系统中主体对资源执行的一系列操作,如读写、修改、删除等。

(4)环境(Environment):主要描述访问发生时系统当前的状态,把环境因素考虑进来,能够更好地为访问控制做出决策。环境用属性来描述,它与授权相关联。比如当前系统的时间、所使用机器的地理位置和 IP 地址等。

(5)属性(Attributes):包括主体属性、资源属性和环境属性。属性描述了所属实体的一些特性,如名称、职称、资源密级等。

(6)策略管理点(Policy Administration Point,PAP):主要任务是创建和管理系统中的访问控制策略,为 PDP 提供策略查询服务。

(7)策略决策点(Policy Decision Point,PDP):PDP 根据访问请求中的属性值在 PAP 中搜索匹配策略,然后进行授权决策,允许或是拒绝。

(8)策略执行点(Policy Enforcement Point,PEP):负责与外部应用交互,在一个具体的应用环境下,截取主体对资源的请求,然后根据 PDP 的决策结果执行相应的动作。

(9)策略信息点(Policy Information Point,PIP):主要任务是创建访问控制时需要的主体、资源、环境的属性信息,并负责管理这些属性信息。PIP 根据访问请求中的实体属性,将相应的属性信息通过上下文处理器返回给 PDP。

(10)上下文处理器(Context Handler):是一个用来转化各种语言的中间部件。主要负责 PEP 和 PDP 之间进行格式转化,并把访问请求转化为 XACML 标准格式。

1.1.2 XACML 访问控制架构

XACML 授权结构如图 1 所示。

(1)用户向保护资源的实体 PEP 发出访问某资源的请求;

(2)PEP 通过上下文处理器将请求转换成 XACML 格式,用来与 PDP 进行交互;

(3)PDP 将访问请求与预先定义好的访问控制策略进行比较,若发现匹配策略,则将结果(允许/拒绝)发送给 PEP;

(4)PEP 执行最终的操作。

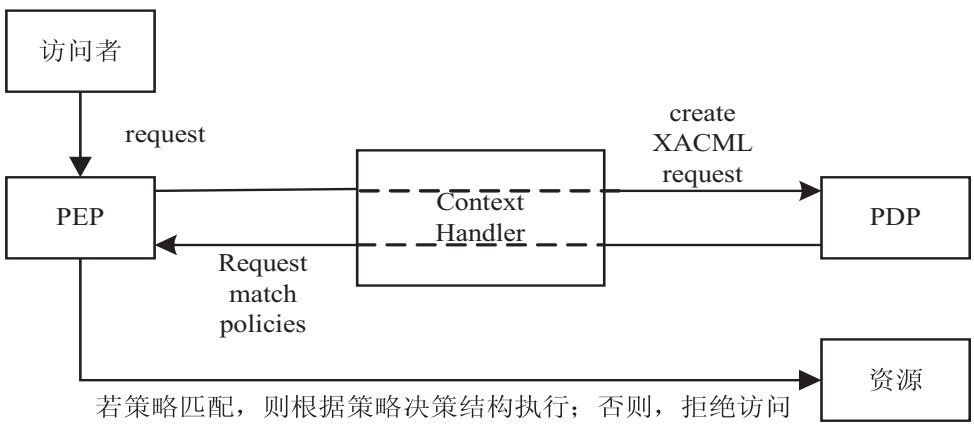

图 1 XACML 访问控制机制

1.2 本体研究

本体的定义,目前还没有统一的描述,但是,最为流行并得到广泛认可的是 1991 年 Gruber 所提出的:本体是概念模型的明确的规范说明[9]。本体可以将对象知识的概念和相互间的关系进行较为精确的定义,是领域内重要实体、属性、过程及其相互关系形式化描述的基础。本体可以在不同的建模方法、范式、语言和软件工具之间进行翻译和映射,以实现不同系统之间的互操作和继承。

下面给出本体的形式化定义。由文献[10]可知,本体由七元组定义,即 $O=(C,A^c,R,A^R,H,I,X)$。其中,C:Concept,是本体所描述的概念的集合;R:Relation,是概念之间关系的集合;A:Attribute,本体无论是描述概念还是概念之间的关系,都是通过属性来描述的,所以 A^c 是概念属性集,A^R 是关系属性集;H:Hierarchy,表示概念之间的层次;I:Instance,就是概念的实例,类似于类的实例;而 X 是本体中的公理。由本体的七元组形式可见,本体是从某一事物的所有属性中

得到的对该事物的认识。

为使人与计算机能够相互交流,就要对人机之间交流的事物概念及其关系进行统一的定义,而本体正是用来描述这些定义,并且使得这些定义唯一、无二义性。目前的计算机正在从单一的设备向进行信息交换和事务处理的世界范围网络转变,因此,支持数据、信息和知识的交换、重用和共享成了当今计算机技术要迫切面临的任务。本体结合 Web Services,成为现在已被广泛应用的语义 Web,本体还被用于信息检索、集成等领域[11]。

2　模型提出

2.1　模型概述

图 2 是模型的示意图。

该模型框架的实现流程如下[12]:

用户提出一个访问请求,PEP 收到请求后再交给 PDP,然后再交给策略存储点(Policy Store Point,PSP)。根据用户及其所申请资源的属性,PSP 搜索适合该用户访问请求的策略,然后交给 PDP 进行决策,PDP 把决策结果返回给 PEP。最后,PEP 将结果返回给用户,如果授权访问,再根据时间约束算法对资源进行访问;否则,拒绝访问。

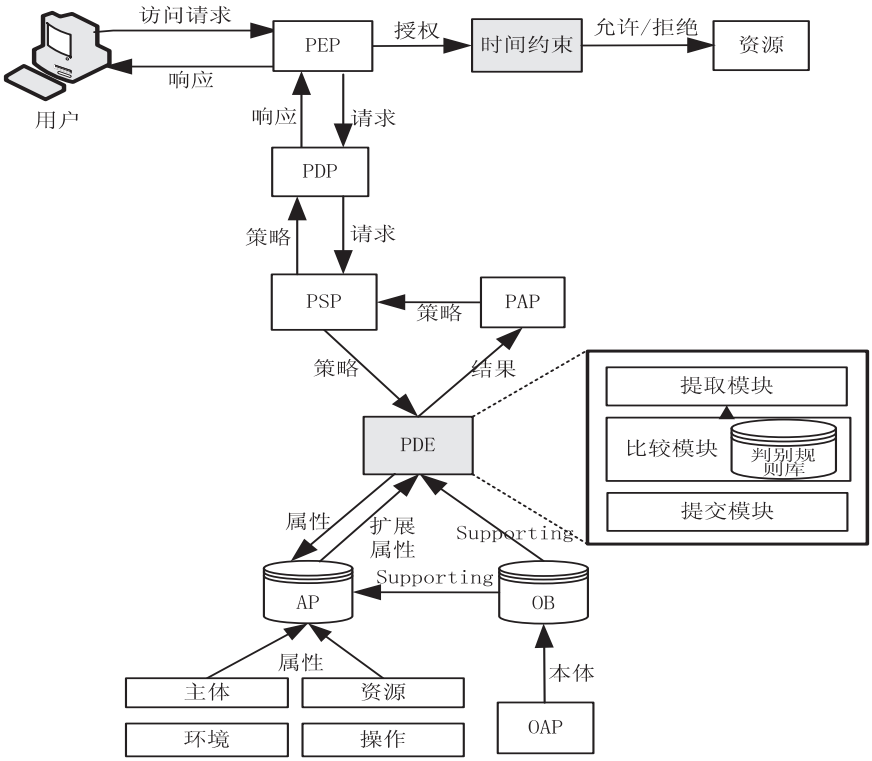

图 2　模型框架结构

这里,要保证存储在 PSP 中的策略是无冲突的,因此,从管理员向 PSP 写入策略开始,一旦 PSP 发生变化,就会触发策略检测引擎(Policy Detection Engine,PDE)。PAP 创建 XACML 策略并将其提交给 PSP,触发 PDE 用来检测存储在 PSP 中的策略之间是否存在冲突。PDE 通过从资源池(Attribute Pool,AP)中获得完整的属性集,再通过本体库(Ontology Base,OB)的支持就可以检测新写入的策略和原来存储在 PSP 中策略之间是否存在冲突。

如果存在冲突,PDE 中的提交模块将结果返回给管理员;否则,写入新的策略。

从上述可以看出,本体对策略冲突检测起到了至关重要的作用。因此,下面给出本体库的相关定义。

2.2　本体库的定义

OB 由四元组 OB = {SO,RO,EO,OO} 所定义,其中,SO、RO、EO、OO 分别表示主体域中的主体本体、资源域中的资源本体、环境域中的环境本体和操作域中的操作本体。为了更加简洁地说明提出的模型,文中建立的本体库中只考虑了四种关系,即:包含、被包含、等价于以及操作相反。

OB 的形式化定义为:$\{Ont \mid Ont = SO \cup Ont = RO \cup Ont = EO \cup Ont = OO\}$,其中,Ont 是所有域中本体的集合。每一种本体定义为:$Ont = \{A, R, <_A\}$,其中,A 是属性的集合,R 是这些属性间的语义关系,$R = \{\subset, \supset, \Leftrightarrow, against, rel\_to\}$,集合 A 上的关系 R 被称为 $<_A$,$<_A = R \rightarrow A \times A$。

R 中各符号含义如下:

$\subset$:包含于;

$\supset$:包含;

$\Leftrightarrow$:等价于;

against :操作相反;

rel_to :与之相关, rel_to = {⇔, ⊂, ⊃}

在介绍完本体库的相关定义后,下面开始介绍 PDE 模块。

2.3 PDE 的结构

一旦存储在 PSP 中的策略发生变化,就会触发 PDE。通过本体库的支持,PDE 可以检测这些策略之间是否存在冲突。从图 1 可知,PDE 由 3 个模块所组成,即提取模块、比较模块和提交模块。

2.3.1 提取模块

提取模块的主要任务是:根据新写入策略 P_{new} 的主体 S_{new},在 OB 中提取出所有与 S_{new} 相关的主体,再依照这些相关的主体,从 PB 中提取出所有的策略。对这些策略中的每一条策略 P_i,都要与 P_{new} 进行比较。(P_i , P_{new})将作为下一个模块—比较模块的输入,即 Comparison Module (P_i , P_{new})。

提取完潜在冲突策略集合和相关资源、环境、操作集合后,PDE 就可以对两条策略进行比较,检测它们之间是否存在冲突。

2.3.2 比较模块(Comparison Module)

比较模块的核心即判别规则库(Discriminant Rule Base,DRB),DRB 中存储了许多判别规则用以检测 P_i 与 P_{new} 间的冲突,这些判别规则可分为:无冲突的判别规则(Rule1 至 Rule8)、冗余判别规则(Rule9 至 Rule15)和冲突判别规则(Rule16 至 Rule18)三类。

判别规则如表 1 所示。

表 1 判别规则库中的规则

序号	R_i R_{new}	E_i E_{new}	O_i O_{new}	结果
1	⇔	⊃	⊂	无冲突
2	⇔	⊂	⊃	无冲突
3	⊃	⊂	⇔/⊃	无冲突
4	⊃	⇔/⊂/⊃	⊂	无冲突
5	⊂	⊃	⇔/⊂	无冲突
6	⊂	⇔/⊂/⊃	⊃	无冲突
7	⊃	⇔/⊂/⊃	cannot can	无冲突
8	⊂	⇔/⊂/⊃	can cannot	无冲突
9	⇔	⇔/⊂/⊃	⇔	冗余
10	⇔	⇔/⊂	⊂	冗余
11	⇔	⇔/⊃	⊃	冗余
12	⊃	⇔/⊃	⇔	冗余
13	⊃	⇔/⊃	⊃	冗余
14	⊂	⇔/⊂	⇔	冗余
15	⊂	⇔/⊂	⊂	冗余
16	⇔	⇔/⊂/⊃	against	冲突
17	⊃	⇔/⊂/⊃	can cannot	冲突
18	⊂	⇔/⊂/⊃	cannot can	冲突

实际上,待比较的两条策略,是按照这样的顺序进行比较的:首先比较它们资源之间的关系,再比较环境之间的关系,最后比较操作之间的关系,得到三者的关系后,对照表 1 得出结论。

2.3.3 提交模块(Submission Module)

提交模块负责将比较模块输出的结果 results 提交给 PAP。若策略无冲突,则直接在 PSP 中写入新的策略,否则,将结果返回给管理员处理。

3 时间约束及对资源的分类

时间是授权的重要组成部分,永久性的授权可能会给系统带来一定的安全隐患,因此需要在访问控制模型中添加时间约束。具体地,在系统资源的属性中加入时间约束这一属性,使得用户在访问资源时受到时间约束的限制,从而细化授权,增强模型的访问控制能力。

文献[13-16]把时间约束分为激活时间范围约束、激活时间长度约束、时间范围内计划时间长度约束,参考这种分类,文中将资源进行如下分类。

3.1 一般资源

这类约束规定用户只要得到授权,就可以随时访问其申请的资源。但是为了保证,这里规定了每个资源的一个最大访问时长,设为 T_{max} ,一旦用户访问资源的时长超过 T_{max} ,系统将自动撤销权限。

3.2 特定时间范围内可以访问的资源

这类约束规定用户只能在特定时间范围内访问资源。如某公司规定只能在工作时间内阅读一份文件,那么非工作时间,这份文件是不可读的。

设允许访问资源的时间段为 $[t_B, t_E]$,其中,t_B 表示允许访问的开始时刻, t_E 则表示访问的结束时刻,因此访问时长为 $L = t_E - t_B$ 。

3.3 访问时长受限的资源

这类约束规定用户每次访问资源的时长不能超过一个固定长度的时间范围。可用此类约束提高某些重要资源的利用效率,或限制资源因访问时间过长而被损坏。

此类资源的属性中要添加一个访问时长的阈值,设为 Δ,即要求 $L = t_e - t_b \leqslant \Delta$ 。

3.4 累计访问时长受限的资源

这类约束规定用户在一定时间范围内累计访问资源时间不能超过一个规定的上限,可用于控制用户访问资源的平均时间。

此类资源的属性中设定一个累计时长的阈值 $\sum \Delta$,要求 $L = t_e - t_b \leqslant \sum \Delta$ 。

3.5 时间约束算法

对添加时间约束属性的资源进行分类后,下面给出时间约束算法:

begin
if authorization　//授权用户
then t_b = get. CurrentSystemTime　//获取系统当前的时间
if resource. attribute. $[t_B, t_E]$ and $t_b \neq [t_B, t_E]$
then revoke;　//撤销授权
else permit;　//允许访问资源
t_e = get. CurrentSystemTime　//再次获取系统当前的时间
if $L = t_e - t_b$ >resource. attribute. T_{max} or
$L = t_e - t_b$ >resource. attribute. Δ or
$L = t_e - t_b$ >resource. attribute. $\sum \Delta$
then revoke;
end

4 结束语

文中为确保存储在系统中的访问策略都是无冲突的,提高策略冲突检测的效率,使系统能够正确有效的运行,将本体的概念应用到访问控制中,提出了一种基于本体的支持策略冲突检测的访问控制模型,并给出了该模型的相关定义及核心模块 PDE 的架构。为进一步增强模型的授权能力,刻画授权的时效性,文中将时间约束添加到资源的属性中,根据时间约束的分类针对资源也进行了对应的分类。最后,给出了时间约束算法,进一步完善了模型。

参考文献:

[1] 王雅哲,冯登国. 一种 XACML 规则冲突及冗余分析方法[J]. 计算机学报,2009,32(3):516-530.

[2] 何再朗,田敬东,张毓森. 策略冲突类型的细化及检测方法的改进[J]. 吉林大学学报:信息科学版,2005,23(3):287-293.

[3] 何再朗,田敬东,张毓森. 策略冲突分析、检测及解决方案[J]. 兰州理工大学学报,2005,31(5):83-86.

[4] Shen Haibo. A semantic and attribute-based framework for web services access control[C]//Proc of international workshop on intelligent systems and applications. [s. l.]: IEEE Press,2010.

[5] 刘　君,曹宝香. 基于本体的面向服务的属性访问控制模型[J]. 山东科学,2010,23(6):78-81.

[6] 胡罗凯,陈　旭,柴　新,等. 一种基于多本体体系的语义 Web 服务访问控制方法[J]. 计算机科学,2012,39(12):107-113.

[7] 夏启寿,范训礼,殷晓玲. 基于时间的 RBAC 转授权模型[J]. 西北大学学报:自然科学版,2008,38(6):932-936.

[8] Moses T. eXtensible Access Control Markup Language (XACML) Version 2.0[S]. [s. l.]:OASIS,2005.

[9] Gruber T R. A translation approach to portable ontology specifications[J]. Knowledge Acquisition,1993,5(2):199-220.

[10] 张忠平,赵海亮,张志惠. 基于 OWL 的本体集成[J]. 计算机应用,2008,28(B06):10-14.

[11] Deng Zhihong, Tang S W, Zhang M, et al. Overview of ontology[J]. Acta Scientiarum Naturalium Universitatis Pekinensis, 2002,38(5):730-738.

[12] Priebe T, Dobemeier W, Kamprath N. Supporting attribute-based access control with ontologies[C]//Proceedings of the first international conference on availability, reliability and security. [s. l.]:[s. n.],2006.

[13] Bertino E, Bonatti P A, Ferrari E. TRBAC: a temporal role-based access control model[J]. ACM Transactions on Information and Systems Security,2001,4(3):191-233.

[14] 董光宇,卿斯汉,刘克龙. 带时间特性的角色授权约束[J]. 软件学报,2002,13(8):1521-1527.

[15] 黄　建,卿斯汉,温红子. 带时间特性的角色访问控制[J]. 软件学报,2003,14(11):1944-1954.

[16] 夏启寿,殷晓玲,黄海生,等. 周期时间特性的角色访问控制[J]. 计算机应用研究,2009,26(12):4730-4734.

(上接第 41 页)

26(2):173-176.

[9] Verri A, Uras S, DeMicheli E. Motion segmentation from optical flow[C]//Proc of the 5th alvey vision conference. Brighton, UK:[s. n.],1989:209-214.

[10] Lin Hongwen, Tu Dan, Li Guohui. The method for moving target detection based on statistical background model[J]. Computer Engineering,2003,9(16):97-99.

[11] 张毅刚,曹　阳,项学智. 静态背景差分运动目标检测研究[J]. 电子测量与仪器学报,2010,24(5):494-499.

[12] Sun H, Feng T, Tan T. Robust extraction of moving objects from image sequences[C]//Proc of the fourth Asian conference on computer vision. Taiwan:[s. n.],2000:961-964.

[13] 韩剑辉,崔猛强,袁耀辉. 基于混合高斯模型的背景差分法的 FPGA 实现[J]. 哈尔滨理工大学学报,2013,18(4):89-93.

[14] 朱明旱,罗大庸,曹倩霞. 帧间差分与背景差分相融合的运动目标检测算法[J]. 计算机测量与控制,2005,13(3):215-217.

带有时间约束支持冲突检测的访问控制模型

作者： 张玉静， 刘军， 李先珠， ZHANG Yu-jing， LIU Jun， LI Xian-zhu
作者单位： 解放军理工大学 指挥信息系统学院,江苏 南京,210007
刊名： 计算机技术与发展 ISTIC
英文刊名： Computer Technology and Development
年，卷(期)： 2015(2)