

基于语义的安全规则冲突检测

张爱娟¹, 高井祥²

(1 中国矿业大学 计算机学院, 江苏 徐州 221116; 2 中国矿业大学 环测学院, 江苏 徐州 221116)

摘 要: 在分布式系统中, 基于策略的管理能满足复杂系统模块松耦合的要求, 为了满足其复杂的安全需求特别是对资源控制细粒度的要求, 其安全策略不仅要描述针对数据本身的细粒度, 还要描述数据公开接口的粒度, 由此利用视图的概念扩展了 RBAC 模型描述客体的细粒度; 为确保策略规则的正确性, 利用约束状态和规则状态描述分析了主客体属性层次操作关联带来的多种冲突类型, 并通过词法和语法分析分解策略元素; 利用分解结果, 基于语义图设计算法, 从而判断并定位策略中的冲突。

关键词: 视图; 冲突; 语义; 冲突检测

中图分类号: TP391

文献标识码: A

文章编号: 1000-7180(2011)10-0067-04

Conflict Detection Method for Security Rules Based on Semantics

ZHANG Ai-juan¹, GAO Jing-xiang²

(1 School of Computer Science and Technology, China University of Mining and Technology, Xuzhou 221116, China;

2 School of Environment Science and Spatial Informatics,
China University of Mining and Technology, Xuzhou 221116, China)

Abstract: Policy-based management can meet the requirements of loose coupling in complex distributed system. In order to meet the complex security need, especially the requirements for fine-grained access control over resources, the security policy should not only describe the fine grains for data, but also for public interfaces of the corresponding data. This paper, extending RBAC model, proposes a view concept to describe fine grains of objects. To verify policy rules, the paper proposes constraint states concept and rule states concept to analyze several kinds of conflict caused by subject and object attribute hierarchy. By lexical and syntax analysis, policy documents are disaggregated into certain access control elements. In order to detect and locate these conflicts, semantic graphs are utilized for designing conflict detecting algorithms.

Key words: view; conflict; semantics; conflict detection

1 引言

访问控制是实现数据安全和网络安全至关重要的措施, 而安全策略则用来描述系统的高层安全需求, 是访问控制说明性的规则。随着分布式计算, 资源共享等新一代计算体系结构的大量涌现, 以策略为中心的控制管理需要面对新的问题^[1]如: 分布式资源的融合; 对客体资源的细粒度控制; 以及跨区域

的主体和客体资源的动态加入或撤出组织。这样就需要建模并实现一种适用于分布式异构环境, 可通过多种属性类型的细粒度刻画定义授权约束的访问控制策略^[2], 但与此同时也容易导致比较复杂的策略规则冲突类型^[3]如: 多规则适用于同一请求, 但最终的判定结果互斥是策略冲突的基本类型, 属性层次导致的权限继承和权限蕴含也可能引发规则冲突。本文通过分析主体约束属性层次和资源各种粒度层次, 利用它们之间关联可能导致的多种冲突

收稿日期: 2011-04-23; **修回日期:** 2011-06-27

基金项目: 国家自然科学基金(41074010, 40904004); 江苏省研究生创新计划资金(CX09B_116Z, CX10B_156Z); 高校基础科研资助专项基金(2010QNB21); 中国矿业大学青年基金(2009A052)

类型,基于语义图给出各种冲突的检测算法。

2 细粒度安全模型

授权粒度是指某一个角色所能赋予的权限的纵深度,在基于角色访问控制中,常见的粒度被划分为三种:控制到任务的访问、控制到对文档或表单的访问、控制到对表单字段的访问。对很多分布式系统如 GIS 中,对受控对象粒度的划分细化到图层,这就需要提供分层的细粒度控制^[4]。所以在细粒度的访问控制模型中,不仅主体角色之间存在层次关系,受控资源之间也存在层次关系。分布式异构系统中为了数据的统一,需要用 XML 对数据进行格式化,这样可实现不同格式数据之间的融合与共享。如下模型中在 RBAC96 模型基础上,对受控资源多了一个细化粒度的视图元素,实现细粒度控制。其模型定义如下(图 1):

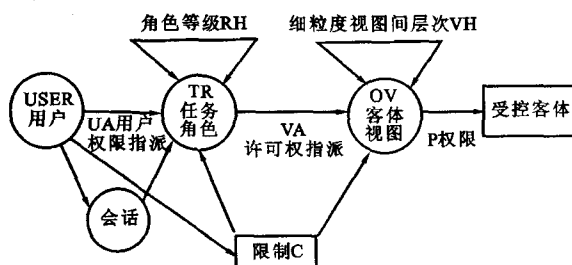


图 1 细粒度分层访问控制模型

一个视图是对某个受控客体的访问权限的集合,对同一个客体,不同的角色可控的粒度不同,所以就出现了针对一个客体的不同视图,这些视图之间存在继承的层次关系。通常情况下,上层资源属性代表粗粒度低敏感的资源内容,下层资源属性代表细粒度高敏感的资源内容,考虑信息保护并根据最小权限原则,资源属性的层次关系隐含了资源受保护的安全级别和敏感性:上层资源属性对应的正向权限不会蕴含下层资源属性,下层资源应具有明确正向授权才可以访问;若系统将负向权限作用于上层粗粒度资源,则负向权限隐含到下层细粒度敏感资源。user, roles, view, op 分别代表用户、角色、视图、对象操作。其模型的形式化描述如下所示:

$UA \subseteq users \times roles$, 用户到“角色”的映射关系。

$VA \subseteq views \times roles$, 视图到“角色”的映射关系。

$RH \subseteq roles \times roles$, 偏序集合,表示“角色”间的继承关系;若 $(a, b) \in RH$, 可以表示为 $a \rightarrow b$, 表示角色 a 继承角色 b 的所有权限。

$VH \subseteq views \times views$, 偏序集合,表示“视图”间的继承关系;若 $(a, b) \in VH$, 可以表示为 $a \rightarrow b$, 表示视图 a 为视图 b 的细粒度权限集。

$RC = \{SSD, DSD\}$ 是指角色之间的冲突关系集合

$SSD \subseteq roles \times roles$, 角色间的静态冲突关系集合;

$DSD \subseteq roles \times roles$, 角色间的动态冲突关系集合

$VC \subseteq views \times views$, 视图间的权限冲突关系结合。

综上所述,系统中的冲突来源于角色约束冲突,及其权限约束冲突。

3 安全模型的约束与冲突

细粒度访问控制模型中对于层次 RBAC 的实现则比较简单,因为视图策略语言中允许角色继承,所以可以通过 VPL 中的角色继承来实现层次 RBAC。本文验证的策略是在设计阶段完成的,所以只验证其中的静态约束。

3.1 角色的静态约束

(1)前导约束:前导约束表示一个主体拥有角色 A 之前必须拥有角色 B 。前导约束定义了角色分配的优先次序。

(2)排斥约束:排斥约束表示一个主体不能同时拥有角色 A 和角色 B 。

3.2 权限规则约束

对权限来讲,权限继承和权限蕴含是策略冲突的主要原因之一,本模型中权限冲突来源于视图的继承和角色的隐式授权。

• 权限蕴含规则

当 View2 继承 View1:

若 $State1 = (Role, View1, OpAttribute) permit$,

则不能推导出 $State1 = (Role, View2, OpAttribute) permit$;

若 $State1 = (Role, View2, OpAttribute) deny$, 则 $State1 = (Role, View2, OpAttribute) deny$

即对下层的更细粒度的资源不能默认继承上层的允许权利,但可直接继承上层粗粒度资源的禁止权利。

• 权限继承规则。

当 Role2 继承 Role1;

若 $State_i | = (Role1, View, OpAttribute) permit$,

则 $State_i | = (Role2, View, OpAttribute) permit$;

若 $State_i | = (Role1, View, OpAttribute) deny$,

则 $State_i | = (Role1, View, OpAttribute) deny$.

即当角色 Role2 继承于角色 Role1, 则 Role2 可以继承特定操作属性下 (OpAttribute) 来自 Role1 的允许权利和禁止权利.

3.3 层次关联冲突分析

有些冲突发生是因为不完全的或冲突的策略设计造成的, 所以有必要定义哪种情况被视为冲突, 以及怎样检测并解除冲突. 为次可以设计一些策略, 当冲突发生时, 通过这些策略, 来决定拒绝或者许可的优先级. 不能被这种策略解决的冲突被视为不一致, 必须把这种不一致静态地检测出来并将其删除. 下面根据权限优先级, 分析了可解决的冲突, 及无法解决的冲突.

(1) 关联视图的冲突解决

关联视图之间存在派生关系, 当派生视图重载基视图时可能存在冲突, 如图 2 所示.

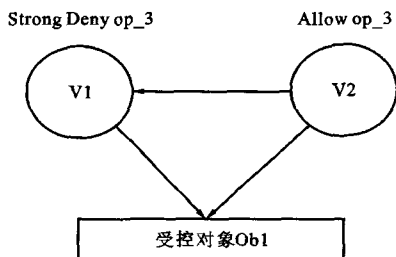


图2 关联视图可解决冲突

Ob1 客体的操作 op_3 被视图 $v1, v2$ 重载, 但授权状态分别为拒绝和允许. 说明冲突存在, 冲突解决策略依赖于视图定义中的优先级关系, 如果只有一个为 Strong, 这种冲突可解决, 否则需删除规则.

(2) 无关联视图的冲突解决

如果两个无关联视图同时控制一个对象, 冲突就有可能发生. 如图 3 所示.

视图 $v1$ 和 $v2$ 控制对象 $Ob1$ 且拥有对操作 op_3 的矛盾授权, 并同时被赋予角色 $R1$, 这就出现了冲突. 当冲突检测出之后, 通过优先级解决冲突, 如图, 只有一个 Strong 则可解决, 如果两个都是 String 冲突被视为不一致, 需检测出来并删除.

利用优先级进行预处理后, 模型中可能出现冲突的类型分析如下:

(1) 客体视图定义成层次结构这种结构本身需

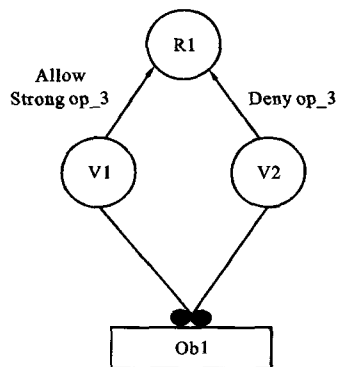


图3 无关联视图的可解决冲突

满足

偏序结构, 否则形成环路, 如图 4 所示就是错误的.

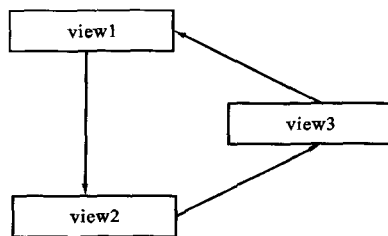


图4 客体层次冲突类型

(2) 主体需满足静态约束条件, 静态约束的冲突主要是由前导约束, 排斥约束以及这两种约束和角色继承的结合引起的, 可以把继承层次图进行扩展成静态约束图. 设: 顶点表示角色, 实线表示继承关系, B 继承 A , 表示为 $A \rightarrow B$ 虚线表示前导约束, B required A , 表示为 $A \rightarrow B$. 空心线表示排斥约束, 如 H excludes R , 则表示为 $R \rightarrow H$, $H \rightarrow R$. 这些关系都满足偏序关系, 如果这些图之间形成回路就可能存在冲突.

(3) 如果可以同时定义许可权限和拒绝权限, 权限冲突就可能发生. 下面分析一下有关联的权限规则之间的关系类型, 并求证能产生冲突的规则关系类型.

假设, 主体层次中 $RA1$ 表示上层角色, $RA2$ 表示下层角色, $RA2$ 继承来自 $RA1$ 的权限. 客体资源中对同一客体的不同粒度的视图层次中 $VA1$ 表示上层粒度, $VA2$ 表示下层粒度资源. 图 5 中前四个图描述了两条规则即存在主体属性层次也存在资源属性层次的情况. 因为属性层次关联存在交叉和同级, 结合授权结果 (permit, deny) 有四种授权规则类型. 随后的两个图描述了只存在资源视图层次的情况, 根据两种不同的授权结果, 授权规则分为两类. 最后的两个图描述了只存在主体层次的情况, 根

据两种不同的授权结果分为两种类型.. 以上类型都是规则间属性层次操作关联的原子类型,囊括了属性层次导致的各种规则冲突原因.

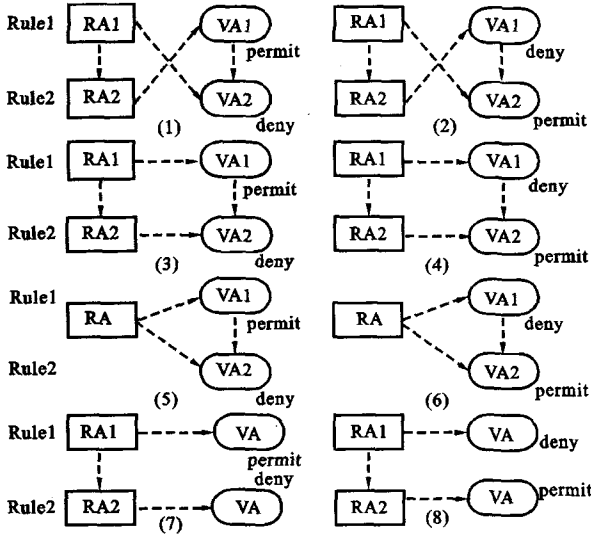


图5 主客体操作关联类型

根据权限蕴含和权限继承规则分析可知:具有上下层关系的视图如果上层视图授予拒绝权限,那下层视图如果是被授予允许权限,就肯定会引起冲突,而对同一视图资源,如果分配给有层次关联的主体,且授权状态分别为允许和拒绝,那么一定会引起冲突,所以,引起冲突的规则状态为状态类型(2)(4)(6)(7)(8). 类型(1)(3)(5)则不会引起冲突,而规则中其它约束层次引起的更复杂的冲突场景都是这些冲突类型的组合.

4 冲突的检测方法

根据细粒度访问控制语言的词法规则,通过词法分析和语法分析,把单词符号分解成各类语法单位,并对各类语法单位进行静态语义检查,继承关系检查,是否存在权限冲突检查.

首先利用 javacc 对细粒度的访问控制策略文本进行词法和语法分析, javacc 是词法分析生成器,因其基础是自顶向下的分析方法,所以必须要解决下面的问题:左递归和公因子问题.

对于含有左递归的产生式,将其转化为没有左递归的产生式:

如 $P \rightarrow Pa \mid b$ 将其修改为: $P \rightarrow bP'$

$P' \rightarrow aP' \mid \text{empty}$

细粒度策略语言文法消除回溯,提左因子.

如 将文法规则 $A \rightarrow aB \mid aC$ 修改为 $A \rightarrow aA'$

$A' \rightarrow B \mid C$

语法声明中的动作代码实际上是语法制导翻译过程. 在语法制导翻译过程中,计算节点的综合属性或者继承属性,并将这些属性填入符号表 SymbolTable 中相应的元素中. 如图 6 所示.

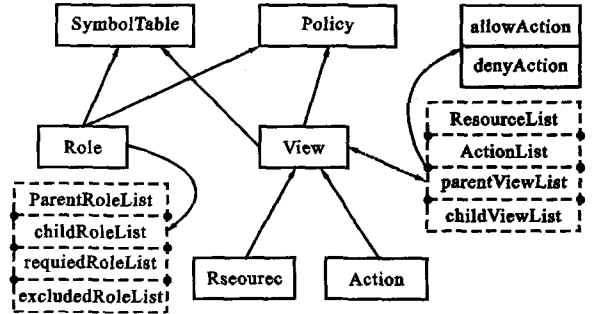


图6 语义分析数据结构

Action 类封装了视图内定义的动作属性以及对这些属性的操作. View 聚合了 Resource 类和 Action 类,在视图内部有记载继承关系的列表,资源对象列表及它们所能执行操作的列表,同时将策略内部的 permit 和 deny 类型规则分类存储,从而提高分析检测效率. 语法分析过程中识别出的细粒度策略元素以及相应的属性填入符号表 SymbolTable. 静态语义分析主要是对这个结构进行检查的.

利用权限语义图,可给出如下的基于属性层次操作关联的冲突检测算法,算法数据源为细粒度策略语言描述的策略文档,经过词法和语法分析后,进行冲突检测,输出冲突规则或者正确状态.

5 结束语

本文对面向对象系统的细粒度访问控制模型所对应的访问控制规则进行了基于语义的冲突类型检测. 但当系统中规则集非常庞大时,效率会很低,所以后续的工作需要在索引结构的基础上对搜索算法进行优化,以提高检测算法的效率.

参考文献:

- [1] Tatyana Ryutov, Group difford. Access Control Framework for Distributed Applications[EB/OL]. [2011-04-23]. http://gost.isi.edu/info/gaaapi/doc/drafts/frmw_draft5.txt, November(2005).
- [2] Mazzoleni P, Crispo B, Bertino E. XACML policy integration algorithms[J]. ACM Transactions on information and System Security, 2008, 11(1): 1-29.

(下转第 74 页)

相对于普通的 B/S 模式,该模式具有诸多优点,主要体现在安全性好、效率高;减轻了工作量并降低了成本。

4 结束语

设计了一种 DAS 模式下 xml 数据存取方案^[6],通过将 xml 数据库外包给数据服务提供者管理的方法实现。数据服务提供者存储加密数据的措施解决了数据外包的安全性威胁,而它专业的 xml 数据库管理模式给系统带来了稳定性,同时大大减小了维护成本和服务器负荷。本方案的设计,对电子商务类网站、xml 技术以及数据外包技术的发展有着积极的推动作用。

参考文献:

- [1] 孟小峰,王宇,王小峰. XML 查询优化研究[J]. 软件学报,2006,10(17):2069—2086.
- [2] Ravi Chandra Jammalamadaka, Sharad Mehrotra. Querying encrypted XML documents, Database engineering and applications symposium[C]// IDEAS '06. 10th In-

ternational India, Delhi, 2006:129—136.

- [3] Hakan Hacigümüs, Bala Iyer, Mehrotra S. Providing database as a service [C]//Proc of ICDE. Washington, DC, USA: IEEE Computer Society, 2002.
- [4] Hui Wang, Laks V S Lakshmanan. Efficient secure query evaluation over encrypted XML databases[C]//Proc of VLDB 2006. New York: ACM, 2006.
- [5] Mykletun E, Tsudik G. Incorporating a Secure Coprocessor in the Database—as—a—Service Model [C]// Innovative Architecture for Future Generation High—Performance Processors and Systems. USA: Washington, 2005.
- [6] 孔令波,唐世渭,杨冬青,等. XML 信息检索中最小子树根节点问题的分层算法[J]. 软件学报,2007,18(4):919—932.

作者简介:

- 黄显文 男,(1982—). 研究方向为数据挖掘。
 王志晓 男,(1979—),博士,讲师。研究方向为人工智能、数据挖掘。
 施海滨 男,(1987—). 研究方向为图像处理、数据挖掘。

(上接第 70 页)

- [3] Hughes G, Bultan T. Automated verification of access control policies [D]. USA: Computer Science Department, University of California, 2004.
- [4] Sloman M. Policy—driven management for distributed systems[J]. Journal of Network and Systems Management, 1994, 2(4):333—360.
- [5] Dunlop N, Indulska J, Raymond K. Dynamic conflict detection in policy—based management systems[C]// Proceedings of the 6th International Enterprise Distributed Object Computing Conference (EDOC), Lausanne,

Switzerland: IEEE, 2002:15—26.

- [6] Ernesto damiani. A fine—grained access control system for XML documents[J]. ACM Transactions on Information and System Security, 2002,5(2):169—202.

作者简介:

- 张爱娟 女,(1979—),博士研究生。研究方向为信息安全、分布式 GIS。
 高井祥 男,(1960—),博士生导师。研究方向为大地测量、矿山 GIS。