数字版权管理中的访问控制研究

张 伟,王 立,李 岩
(陕西师范大学 计算机科学学院,陕西 西安 710062)

摘 要:访问控制问题是数字版权管理中的一个重要安全问题。为了提高数字版权管理中的访问控制效率并降低系统实现难度,在数字版权管理系统中提出一种基于属性的访问控制模型(Attribute-Based Access Control, ABAC),并将该模型成功运用到数字化考试阅卷系统中。基于属性的访问控制模型具有逻辑严密、访问控制和安全控制具有一致性、符合面向对象设计的方法,系统易于实现等优点。该模型的提出,一方面为数字版权管理中的访问控制提供了一条新的解决方案,另一方面该模型对研究访问控制也具有一定的理论和现实意义。

关键词:数字版权管理; 基于属性的访问模型; 系统设计
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2011)07-0168-04

Research on Access Control in Digital Rights Management

ZHANG Wei, WANG Li, LI Yan
(School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

Abstract: Access control has become a difficult and important question of the digital rights management. In order to improve the efficiency of digital rights management and reduce the access cost of control system implementation, propose an attribute-based access control model of digital rights management system. The model can also be successfully applied to the scoring system of digital examination. The analysis of this model shows that security performance and the adaptability is stronger. On the one hand this model propose a new way to research on access control in digital rights management ,on the other hand it also contributes to the access control theory.

Key words: digital right management (DRM); attribute-based access control; system design

0 引 言

数字版权管理(Digital Rights Management, DRM)系统利用密码、数字水印、权限描述等技术对数字作品的创建、分发、传输和使用等各个环节进行版权保护和权限控制[1]。数字版权管理系统中的访问控制模型是数字版权管理的重要问题。国内对数字版权管理中访问控制的研究主要集中在控制模型研究。使用控制将访问授权策略建立在授权、职责和条件三种决策因素上,支持可变属性和持续授权,使用控制实质也是一种 ABAC 模型[2]。在开发研究适用于大规模用户群而且属性需要动态扩展的系统时,使用控制暴露出其授权管理结构复杂、系统维护困难的缺点。

文献[3]利用可计算集合理论中的集合限制理论提出了 ABAC 的逻辑框架(LABAC),使用 CLP 中的集合来描述属性和服务。文献[4]提出的基于属性的 Web 服务访问控制模型具有较强的表达能力,其访问控制决策依据的属性同时包括了主体属性、资源属性和环境属性。文献[5]提出了使用上下文属性来捕获移动环境动态性质的上下文敏感的 ABAC 模型,适合于移动环境下的访问授权。

文中通过对多种访问控制模型的研究,在数字版权管理系统学中提出了一种基于属性的访问控制模型。通过对该模型的分析,说明该模型安全性能强,易于管理,自适应性强。

1 数字版权管理基于属性的访问控制模型

1.1 基于属性的访问控制(Attribute-Based Access Control, ABAC)模型的构成

基于属性的访问控制的核心思想是访问决定(Access Decision)取决于属性。文中所提的 ABAC 主要包含属性集(Attribute Set, ATTS)、行为(Action, ACT)、审核(Audit)、主体(Subject)、客体(Object)、授权(Authorization, AUT)、权利(Right)。

基于属性的访问控制模型(Attribute-Based Access Control basic model)如图 1 所示。

(1)属性集(Attribute Set, ATTS)。属性集是一个包含主体属性、客体属性、条件(conditions)属性的一

收稿日期:2010-12-13;**修回日期**:2011-03-17
基金项目:国家自然科学基金项目(60673065)
作者简介:张 伟(1986-),男,硕士,研究方向为网络与信息安全。

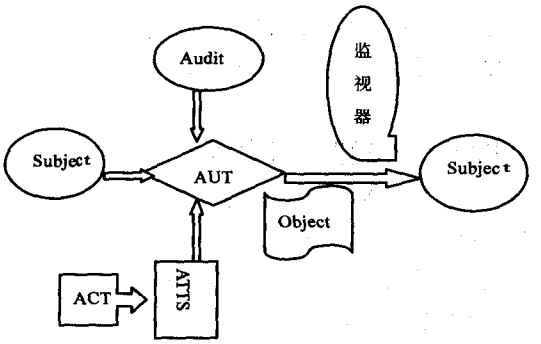

图1　ABAC基本模型

个集合。这有别于文献[6]所述的基于属性的访问控制。通过对数字版权管理系统的研究发现,需要考虑的条件因素和影响条件因素的变量并不多,因此文中将条件因素作为属性集的一个子集。属性通常有可变属性和不可变属性之分,一般根据不同的系统而定。

文中主体属性和客体属性包含两方面内容,一方面主体和客体都包含自有属性(Original Attributes),例如账户信息(credit)、属性类别、IP地址等。另一方面系统会为主体和客体建立相关的派生属性(Derivative Attributes),包括属性更新信息,使用次数(Usage Counter)、安全级别(Safety Level)、使用时间等。派生属性是进行安全性控制的属性信息。在ABAC中,主客体属性包含两方面因素,从而实现安全性控制与访问控制同时进行。条件属性通常包括系统时间、访问列表、访问人数限制等。图2是一个主体属性表(Subject Attribute table)。

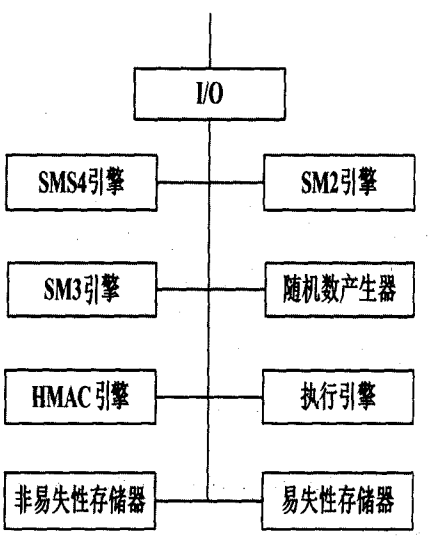

图2　主体属性表

(2)行为(Action,ACT)。行为:现代访问控制中往往由于系统的开放性以及分布式和普适计算的要求,往往要求主客体属性和条件属性都能进行必要的更新。

(3)审核(Audit)。审核模块一方面对属性的更新和行为发展进行跟踪,并为之提供凭证。另一方面它为系统恢复和备份以及叛逆者追踪提供依据。审核与数字版权管理模块中安全模块直接通信。

(4)主体(Subject)。通常持有客体的某种权限和访问控制权限。主要包括:提供者(provider),消费者(consumer)。主体以其属性标识其身份。

(5)客体(Object)。数字版权管理系统的保护对象。客体以其属性标识其身份[7,8]。

(6)权利(Right)。权利就其功能而言是主体拥有相关客体的特权总和。权利通常包括产品消费者的权利(Consumer Right,CR)、供应商的权利(Provider Right,PR)、审计权利(Audit Right,AR)、代理权利(Delegate Right,DR)、访问权利(Access Right,AR)。R={V, W, E},V代表可见,W代表可更新,E代表可验证。V,W,E={0,α,1},其中α<1。权利通常可以用属性的形式表示如ATT(R)表示某些权利[9,10]。

(7)授权(Authorization,AUT)。在ABAC中,授权完全是基于属性。

1.2　数字版权管理中ABAC的形式化定义

访问控制一般都是基于时间逻辑进行控制[11,12]。下面采用时间逻辑行为(Temporal Logic of Action,TLA)来说明ABAC的授权过程。

定义1:在ABAC中,属性集(Attribute Set,ATTS)包含主体属性(AAT(S))、客体属性(AAT(O))、条件属性(AAT(C)),即ATTS={AAT(S), AAT(O), AAT(C)}。属性的状态是属性的取值。

规则一:条件属性在ABAC中是可变的。

定义2:系统状态可以用集合V={initial,requesting,denied, access-permitted,accessing,revoked,end}来表示。

定义3:一个谓词predicate(P)是定义在属性集(ATTS)上的逻辑表达式。

在ABAC中通常包含三种谓词:一元谓词、二元谓词、三元谓词:如P(AAT(S))、P(AAT(O),AAT(C))、P(AAT(S),AAT(O),AAT(C))。

定义4:行为(ACT)是定义在属性集上的部分函数,它将属性的状态(含系统状态)转换到另一个状态。ACT={Provision,Obligation,Compensation}。

规则二:行为(ACT)只能通过以下五种方式进行属性更新:独有性/共有性、可消耗性/增值性、变化的限制性、认证性、直接撤消性。

规则三:行为(ACT)有预先作为(Provision)、当下作为(Obligation)、事后作为(Compensation)三种作用方式。

规则四:行为可能引起两方面的变化:第一:改变属性集中的属性。第二:引起其他相关的行为。

说明:行为可以产生属性的变化,同时也可以产生

新的行为,而该行为又可能产生新的访问控制或者相关变化等,它是基于属性的访问控制的核心。

定义 5:ABAC 的授权模型是一个从 S、P、A 到系统状态的一个映射。其中 S:属性集,P:断言,A:行为。

1.3 数字版权管理中 ABAC 的逻辑模型

模型 1

ATTS ∧ p_1 ⋯ ∧ p_i⇒permit(S,R,O)

permitacce ss(S,R,O)⇒Once(accessrequest(S,R,O) ∧ (ATTS ∧ p_1 ⋯ ∧ p_i⇒provision(ATTS)))

说明:该模型适用于数字版权管理中的一次付费一次使用(Pay-Per-Use);访问控制开始前制定授权规则。第一条授权规则:满足属性集信息集 ATTS 和断言 $P_i(i=1\cdots n)$ 则允许 S 可以使用权利 R 访问客体 O。第二条说明:当访问请求及属性集满足授权规则时允许访问,在访问之前对属性做预先作为。Once 表示一次。

模型 2

permitaccess(S,R,O)⇒Alays((¬ ATTS ∧ p_1 ⋯ ∧ p_n ∨ V! =accessing)⇒revokeaccess(S,R,O))

If V=end

endaccess(S,R,O)⇒

Once((ATTS ∧ p_1 ⋯ ∧ p_i ⇒ Compensation1 (ATTS)))

if V=revoke

revokeaccess(S,R,O)⇒

Once((ATTS ∧ p_1 ⋯ ∧ p_i ⇒ Compensation2 (ATTS)))

说明:该模型是访问后制定授权规则,访问后进行更新的模型。访问进行中,当不满足属性集、断言和系统状态时终止访问,否则正常访问。当主体退出访问和被系统拒绝访问时主体都要做事后行为。

模型 3

ATTS ∧ p_1 ⋯ ∧ p_n⇒permit(S,R,O)

permitaccess(S,R,O)⇒Once(accessrequest(S,R,O))

∧ ATTS ∧ p_1 ⋯ ∧ p_n

permitaccess(S,R,O)⇒Alays((¬ ATTS ∧ p_1 ⋯ ∧ p_n ∨ V! =accessing) ⇒revokeaccess(S,R,O))

if V=end

endaccess(S,R,O)⇒Once((ATTS ∧ p_1 ⋯ ∧ p_i ⇒Compensation1(ATTS)))

if V=revoke

revokeaccess(S,R,O)⇒ Once((AT TS ∧ p_1 ⋯ ∧ p_i⇒Compensation2 (ATTS)))

说明:该模型是访问控制开始前制定授权规则,持续访问控制,访问后更新模型。持续访问期间对属性持续监控,不满足则终止访问。当主体退出访问和被系统拒绝访问时主体都要做必要的行为。

2 ABAC 的模型应用举例

数字化考试阅卷系统中试卷可以作为数字版权管理中的客体 O,考试人被认为是一个主体 S1,出题者和阅卷者可以认为是另一个主体 S2。考试一般都以持续时间为系统约束条件。系统实现如下:

ATT(S1)={S1S,S1E},其中 S1S 为开考时间,S1E 为结束时间。

ATT(S2)={S2S,S2E},其中 S2S 为开始阅卷时间,S2E 为结束阅卷时间。

ATT(O)={S1LIST,S2LIST,S1T,S2T}

其中 S1LIST 表示可访问的 S1 列表,S2LIST 表示可访问的 S2 列表,S1T 表示 S1 持续访问时间,S2T 表示 S2 持续访问时间。

系统模型:

Step1:ATT(S1) ∧ ATT(S2) ∧ ATT(O) ∧ p_1... ∧ p_n⇒permit(S,R,O)

Step2: permitaccess(S,R,O)⇒Once(accessrequest(S,R,O)) ∧ (ATT(S1)⇒(provision(ATTS1)) ∧ (ATT(S2)⇒provision(ATTS2)) ∧ (ATT(O)⇒provision(ATTO)) ∧ p_1... ∧ p_n

Step3:((S1 ∉ S1LIST ∨ (S1.S1E-S1.S1S) ≥ S1T ‖ S2 ∉ S2LIST ∨ (S2.S2E-S2.S2S) ≥ S2 T)⇒revokeaccess(S,R,O)

Step4: endaccess(S,R,O) ∨ revokeaccess(S,R,O) ⇒Even((ATTS ∧ p_1 ⋯ ∧ p_i⇒compensation(ATTS)))

说明:系统初始化,预先授权模型,满足相关属性和谓词才能获得授权许可。允许访问主体以某种权利访问之前必须对主客体属性进行预先作为,对属性进行必要的更新。终止访问条件:访问主体不满足客体条件,访问时间超过了限制。访问正常结束或者访问被终止后要对属性进行访问后更新。

3 数字版权管理中基于属性控制的访问控制分析

文中首先在数字版权管理系统中提出一种基于属性的访问控制模型。该模型有如下特点:

1)逻辑简单而且严密。ABAC 授权是基于属性这个单一因素,因此逻辑严密。相对于使用控制授权模型逻辑简单且易于实现。

2)访问和安全控制具有一致性。属性包含原始属性和派生属性,在实现访问控制的同时实现系统安

全的控制。自动审计部件记录行为的变化,可以实现灾难恢复和叛逆者的追逐,适用于分布式系统。

3)符合面向对象设计的方法,系统易于实现。对于每一个主体或者客体都具备自己的属性,这可以视为该抽象数据类型数据,而改变属性的行为可认为是抽象数据类型的方法。

4)行为有别于使用控制中的责任,基于属性的访问控制中的行为将可能产生灵活的动态效果,首先可以在访问控制的任何时段改变属性信息。第二行为的级联和嵌套符合大型数据库系统及现代访问控制的要求。

4　结束语

作者在研究数字化考试及阅卷系统时,由于考试和阅卷系统的特殊性及试卷信息的敏感性,非常需要一种高效的安全的数字版权管理系统。文中提出的数字版权管理中的基于属性的访问控制模型满足了该系统的要求。该模型比使用控制更符合网上阅卷系统的要求。

文中提出的基于属性的访问控制模型,一方面为数字版权管理中的访问控制提供了一条新的解决方案,另一方面该模型对研究访问控制也具有一定的理论和现实意义。

参考文献:

[1] Zhang Ru, Yang Yu. Digital rights management [M]. Beijing: Beijing University of Post and Telecommunications Press, 2008.

[2] Zou D Q, He L G, Jin H, et al. CRBAC: Imposing multi-grained constraints on the RBAC model in the multi-application environment [J]. Journal of Network and Computer Applications, 2009, 32(2):402-411.

[3] Wang L Y, Wijesekera D, Jajodia S. A logic-based framework for attribute based access control [C] // Proceedings of the 2004 ACM Workshop on Formal Methods in Security Engineering. New York: ACM, 2004:45-55.

[4] Yuan E, Tong J. Attributed based access control (ABAC) for web services [C] // Proceedings of the IEEE International Conference on Web Services. Washington: IEEE Computer Society, 2005:561-569.

[5] Michael J, Manoj R. A contextual attribute-based access control model [C] // Proceedings of 2006 Workshops on the Move to Meaningful Internet Systems. Berlin: Springer, 2006: 1996-2006.

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

[7] 王　立,万世昌,张　珍. 基于互信属性调配机制的访问控制模型[J]. 计算机技术与发展,2009,19(12):127-130.

[8] 张海鑫,程丽红,李顺东. 数字版权管理系统中的使用控制模型[J]. 计算机技术与发展,2009,19(12):135-138.

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

[10] 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.

[11] 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.

[12] 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.

(上接第167页)

明,与现有系统进行比较,该系统具有较低的能耗、较低的检测率和较高的误报率。

参考文献:

[1] 裴庆祺,沈玉龙,马建峰. 无线传感器网络安全技术综述[J]. 通信学报,2007,28(8):114-122.

[2] Ian F, Akyildiz, Su Weilian, et al. Wireless Sensor Networks: A Survey[J]. Computer Networks, 2002, 38(4): 393-442.

[3] 孙利民,李建中. 无线传感器网络[M]. 北京:清华大学出版社,2006.

[4] 杨黎斌,慕德俊,蔡晓妍. 无线传感器网络入侵检测研究[J]. 计算机应用研究,2008,25(11): 3205-3209.

[5] 何泾沙,邢　利,张　婷,等. 分簇无线传感器网络的动态入侵检测算法[J]. 北京工业大学学报,2010, 36(6):845-850.

[6] Su W, Chang K, Kuo Y. eHIP: An Energy-Efficient Hybrid Intrusion Prohibition System for Cluster-Based Wireless Sensor Networks[J]. Computer Networks, 2007, 51(4):1151-1168.

[7] 周贤伟,覃伯平. 基于能量优化的无线传感器网络安全路由算法[J]. 电子学报,2007,35(1):54-57.

[8] 李　玲,王新华,车长明. 基于信誉机制的传感器网络安全路由协议设计[J]. 计算机技术与发展,2010,20(9):131-135.

[9] 户晓玲,曾建潮. 基于微粒群模型的移动传感器网络部署研究[J]. 计算机技术与发展,2009,19(10):81-85.

[10] Ngaie E C H, Liu J C, Lyu M R. An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks[J]. Computer Communications, 2007, 30 (11-12): 2353-2364.

[11] Meka A, Singh A. Distributed Spatial Clustering in Sensor Networks[J]. Lecture Notes in Computer Science, 2006, 3896: 980-1000.

[12] 武春涛,胡艳军. 无线传感器网络 LEACH 算法的改进[J]. 计算机技术与发展,2009,19(3):80-83.