基于动态属性的域间使用控制模型研究

徐长征 王清贤
(解放军信息工程大学信息工程学院网络工程系 郑州 450002)

摘 要 在分析多域交互主要特性的基础上,提出了一种多安全域下的动态使用控制模型(DAB-UCON)。该模型以下一代访问控制 $UCON_{ABC}$ 核心模型为基础,将属性、授权(A)、义务(B)、条件(C)等各个组件作为一个动态实体进行扩展。提出一种属性分类方法,即按照属性定义时间和应用范围分别进行模型描述。最后对模型进行讨论,引入属性谓词等来满足动态多域交互条件下的系统需求。扩展后的模型有助于访问控制中动态的策略构建和授权。

关键词 访问控制,动态属性,多安全域,使用控制
中图法分类号 TP309 **文献标识码** A

Towards a Dynamic-attribute-based Multi-domain Usage Control Model

XU Chang-zheng WANG Qing-xian
(Department of Network Engineering, Information Engineering University, Zhengzhou 450002, China)

Abstract On the basis of analyzing multiple domain interaction, we proposed a dynamic attribute based multiple domain usage control model. The model DAB-UCON is based on the next generation access control model $UCON_{ABC}$, and extends the dynamic characteristics of the $UCON_{ABC}$ components of authorization, obligation and conditions. Then we classified dynamic attributes according to the time of definition and the scope applied, which facilitate modeling each component as a dynamic entity. At last we discussed the extended model by formalizing, and introduced new predicates to accommodate requirements of multi-domain dynamic interaction, which will be useful for dynamic policy constructing and authorization in access control.

Keywords Access control, Dynamic attribute, Multiple domain, Usage control

1 引言

随着高带宽的网际互联和高性能的移动设备的出现,用户可以随时随地接入各种丰富、实时的应用中。而且,这些计算设备上下文感知能力不断增强,能根据用户所处的操作环境,动态地调整应用。在向用户提供丰富服务的同时,开放环境下资源共享所带来的安全问题引起了广泛关注。

当主体跨多个安全域(以下简称为域)进行交互时,可以从中获取上下文信息。为了能把该信息(属性)应用到其它域,外域需要动态地解释,进而向主体授权。区别于动态变化的属性值,对某个域来说,主体带来的是一种新生属性,也就意味着必须在交互时刻动态、实时地为该主体授权。在已有的研究中,Freudenthal 等人提出了一种跨域的系统访问控制机制 dRBAC[2]。dRBAC 是一种分布式的基于角色访问控制,其基于角色控制各种活动行为,允许跨域的角色委派。Covington等提出了一个基于上下文属性的访问控制模型(CABAC),其中访问判定完全基于属性进行,在制定授权策略过程中,没有将主客体对象纳入判定之中[3]。在文献[4]中,作者指出了开放环境中的访问控制需求,提出了基于属性的语义感知的访问控制模型,但其不能跨多个系统进行动态地创建和解释属性。总的来说,基于属性的访问控制模型主要存在两种局限性:一是在单一域框架(简称单域)中,属性是预先定义好的;二是在多域框架中,典型的如分布式系统,这类模型尚缺乏对新生属性的支持,需要属性语法的广泛一致[5,6]。本文通过示例分析多域交互条件下的主要特性,在下一代访问控制 UCON(Usage Control)核心模型[1]基础之上,提出了一种基于动态属性的多安全域使用控制(Dynamic Attribute based UCON)DAB-UCON 模型原型,用于满足动态、多域系统的需求。扩展后的模型有助于访问控制中动态的策略构建和授权。

2 多域交互的特性

本节通过一个购物示例分析用户与多域系统交互的特性。如图 1 所示,当主体 SA 从音像店域(Domain Video,简记为 DV)移动到书店域(Domain Book,简记为 DB)时,SA 能从 DV 获取上下文信息(信誉卡),DB 将其解释后再进行访问判定。

SA 在音像店(DV)进行了一笔 100 元的交易,为表达惠

到稿日期:2009-01-06 返修日期:2009-03-17 本文受国家高技术研究发展计划(八六三计划)基金资助项目(2006AA10Z409),河南省基础与前沿技术研究计划(082300410150)资助。

徐长征(1976—),男,博士生,主要研究方向为安全操作系统结构研究、访问控制,E-mail:zachxu@gmail.com;王清贤(1960—),教授,博士生导师,主要研究方向为信息安全、算法分析等。

顾谢意，DV 向 SA 提供了一张价值 10 元的信誉卡。凭此卡可用于其它店铺，比如书店(DB)。随后 SA 持卡到 DB 购书。该信誉卡作为 SA 从 DV 获取的上下文信息，影响 DB 的访问决策。通过该示例，分析得出多域交互主要存在以下特性。

(1)跨安全域的交互。主体、客体与多个系统进行交互，从管理上说这是完全不同的安全域。

(2)信息是动态的，可用于系统之外。根据移动互联性，信息可以从某一系统移动到其它系统，并影响其它系统的访问决策。

(3)无预先配置。为了跨域解释信息，系统间必须交换该信息的语义。但在移动的场景中，信息可能是动态创建的，因此它的语义不可能在所有的系统中得到一致的认可。所以在授权时刻就必须对它加以明确解释。如上例中，在 SA 持信誉卡买书时，DB 把“信誉”解释为货币值(通过与 DV 协商)。而在 DB 与 DV 之间预先进行“信誉”语义的交换是不现实的，因为商家 DV 或许还会给顾客其它奖励方式。例如，DV 给顾客办理积分卡，其语义只是购物积分，不同于信誉卡所代表的货币值含义。

除了以上主要特性外，多域交互还应具备以下特性。

(4)支持保留隐私。保护主体交互的隐私是信息系统一个重要的安全要素。如上例中 SA 可以不必让 DV 知道他在何处使用该信誉卡，或不让 DB 知道他是从何处获得的信誉卡等。主体可以从某个系统中接受、拒绝或清除信息(但不能更改)；对于是否暴露该信息给其它系统，主体有决定权。

(5)不需要预先进行注册。主体无需预先注册到某一系统进行交互。进而，系统也无需记住和主体进行过的交互。

(6)信息可被转移。策略允许的情况下，允许主体与其他主体共享从某个系统收到的信息。如 SA 可以转让 5 元(从他的 10 元信誉卡中)给其它主体进行消费。

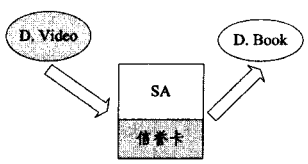

图 1　多安全域交互示例

3　$UCON_{ABC}$ 核心模型分析

本节中，简要描述并分析使用控制 $UCON_{ABC}$ 模型。UCON 模型包含 6 个组件：主体及其属性、客体及其属性、权限集、授权、义务及条件，其中授权规则(A)、义务(B)、条件(C)为使用控制判定的构成要素。该模型将属性抽象化，在每个系统状态下，属性作为一个变量都有赋值，如主体的角色、安全级、客体的分类、用户的信誉卡等。UCON 能够清晰描述 DAC，MAC 和 RBAC 等传统的访问控制思想，涵盖了数字版权管理 DRM(digital rights management)、信任管理等现代商务和信息系统需求中的安全和隐私这两个重要的问题。

在 UCON 中，一个完整的使用过程包括 3 个阶段，即使用前、使用中、使用后，如图 2 所示。只有前两个阶段需要检查并实施控制判定。使用进行中的判定说明了 UCON 判定的持续性质。UCON 的另外一个重要性质是属性可变性，即主客体的属性值在这 3 个阶段都可以被更新。传统的访问控制模型中的属性概念一般是指不可变属性，仅能通过管理行为改变，而可变属性会随着访问对象的结果而改变。这一点也是 UCON 模型与其他访问控制模型的最大差别。

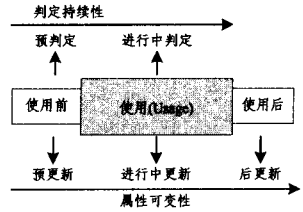

图 2　UCON 持续性和可变性

UCON 模型为研究下一代访问控制提供了一种新方法，被称作下一代访问控制模型[7]，也称为 ABC 模型[8]。

4　动态授权的使用控制扩展模型

4.1　DAB-UCON 模型原型

针对上述多域交互的各种特性，目前在单域和多域授权系统中都缺乏对这些特性的支持。其中，特性 1、特性 2 需要“多域属性”的概念，此属性要能够在跨域时进行解释。而特性 3 需要“动态属性”的概念，亦即属性动态创建而非预定义。上述示例中信誉卡就是由 DV 动态创建的，DB 不能提前写好授权策略来使用信誉卡，那么在 SA 用它来买书时，书店需要动态解释信誉卡的语义。这里“信誉”是一种属性，且用在多域环境(DV，DB)下，这样它就是一个动态的多域属性。注意区别于“动态变化的属性值”，动态属性是一种动态创建的新生属性。我们提出的基于动态属性的扩展模型主要能够满足以上所述 3 种特性。

可以看出，标准 UCON 模型针对多域环境下的交互，缺乏对动态、多域属性的支持。本节通过进一步划分该模型的属性、授权、义务、条件等组件，对模型进行了扩展。图 3 表示带扩展组件的使用控制模型，我们称之为基于动态属性的使用控制模型(Dynamic Attribute based UCON)DAB-UCON。下面将系统研究 DAB-UCON 的组件，用以支持多域的动态授权。

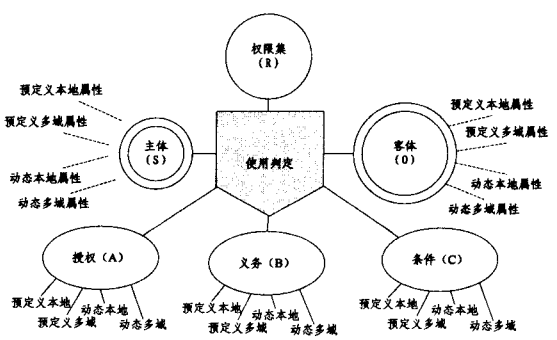

图 3　DAB-UCON 模型原型

4.2　DAB-UCON 属性

在 UCON 中，属性指的是用于使用判定的主客体性质。本小节研究 DAB-UCON 属性，首先根据属性定义时间进行分类。

• 预定义的属性：在系统进行初始配置时，属性的语义已由管理员定义好。同于 UCON 模型中属性的定义。

• 动态的属性：运行时刻定义的属性。在前述示例中，DV 系统可以在不同时间、不同场合动态地定义类似于信誉卡的各种奖励措施。如 DV 给顾客创建积分卡属性，而该属

性的含义不同于信誉卡所代表的货币值。

另外，还可以根据属性应用的范围对属性进行如下分类。

·本地属性：只能在单域中加以语义解释的属性。这些属性的值也只能在本域可见。换言之，本地属性在其被定义的系统之外没有意义。

·多域属性：是指能跨域加以语义解释的属性。

这样，存在4种DAB-UCON可支持的属性类。

(1)预定义的本地属性：与当前基于属性的模型(也包括UCON模型)定义属性的方式一致。

(2)预定义的多域属性：当前分布式系统中访问控制主要方法里就有PMA这个概念。

(3)动态的本地属性：允许系统动态创建属性，该属性在本地系统中可解释。这样的一个行为通常视为系统管理员任务。

(4)动态的多域属性(DMA)：系统可以动态地定义属性，该属性在多域中需要能被解释。在这种情况下多域间的预先配置已不起作用，因为新属性会随时被创建，而其他系统也不能提前写好策略描述。这也就需要动态地创建授权策略。

如图3所示，主体和客体都有一个属性集。为了支持模型新生属性的动态创建和属性集的动态更新，在UCON模型基础上增加了如下谓词。

·属性创建谓词：*AttSetPreUpdate*

·属性赋值谓词：*AttValPreUpdate*

·属性类型谓词：*AttTypePreUpdate*

本文的示例其实已经给出了一个清晰的DMA范例，主体SA所持有的信誉卡就是一种动态多域的属性动态多域属性既可以用于主体，也可以用于客体。考虑客体的DMA属性，例如病人(主体)拥有他们的病历(客体)，医生或医院使用该记录时，可以每天在该病历上创建多个DMA属性，例如“检查过病历的医务人员”、“最后检查日期”等。病人在跨不同医院或药房时，病人病历的DMA语义需要得到明确解释。至于如何解释，这是管理模型的一部分，涉及访问控制机制的实现，本文不做重点讨论。

4.3 ABC扩展组件

为了支持动态多域属性，需要相应地扩展UCON模型中授权(A)、义务(B)、条件(C)等组件。

在UCON中，授权组件包括基于主客体属性的授权规则。由于授权包含规则的构建是基于主客体属性的，因此在DAB-UCON模型中类似地将授权分类为：预定义本地(PL)授权、预定义多域(PM)授权、动态本地(DL)授权、动态多域(DM)授权。其中，DM授权通过解释动态多域属性的语义，动态地进行授权规则的构建。

UCON中义务是指访问被允许之前主体需要执行的一系列动作。类似地，基于范围和定义时间将DAB-UCON义务分类为：预定义本地(PL)义务、预定义多域(PM)义务、动态本地(DL)义务、动态多域(DM)义务。其中，DM义务是指动态定义的且授权时刻在多系统中可解释的义务。需要强调DM义务是为了在不同系统中使用多域属性而需履行的义务。如SA在DB使用来自DV的信誉卡，假设还有一家位于书店内的音像店(DV@DB)，在DB允许用信誉卡购书之前，有一项义务要求SA与DV@DB进行交易。DB系统在授权使用多域属性信誉卡时刻，解释并要求主体SA履行该义务，即动态的多域义务。

在标准UCON模型中，条件是指系统级的因素，也是访问被允许的前提条件，如一个服务器的最大连接数、系统被访时间等。与属性相类似，基于范围和定义时间将DAB-UCON条件分类为：预定义本地(PL)条件、预定义多域(PM)条件、动态本地(DL)条件、动态多域(DM)条件。其中DM条件是指动态定义的条件，且在授权时刻多域系统中可解释。如示例中DB发现SA在使用信誉卡时有一个条件：DV系统发行该卡的有效日期为2009年12月31日，进而动态解释该条件的语义，此即动态的多域条件。

4.4 DAB-UCON场景应用

如前所述，为了支持动态、多域交互的特性，需要在系统运行时刻(为主体或客体)创建新的属性、义务和条件。如例中SA在与DV系统交互之前他还不具有信誉卡属性，和DV交互过后，DV动态地为他创建多域属性，进一步该属性可用于DB系统中。在信誉卡属性使用过程中，相应地还需要满足动态的条件和义务以支持访问授权判定。需要说明的是，在标准UCON模型中，创建新的属性、条件和义务(预定义组件)是一种管理员行为，即管理模型的一部分。而对于动态的、多域系统来说，这些组件需要在运行时刻定义，创建这样的新组件(动态组件)不再属于DAB-UCON中管理模型内容，而是DAB-UCON使用控制模型的一部分。

为描述方便，此处沿用前面讨论过的关于动态多域属性、义务和条件的示例场景。在系统DB中，*id*为SA在书店的身份标识，*price*为SA要买的书的价格。主体*S*(SA)和客体*O*(书)具有本地属性：

$LocalAtt(S) \supseteq \{id\}$

$LocalAtt(O) \supseteq \{price\}$

DV系统动态地为SA发行信誉卡属性的同时，还动态定义了与该属性相关的某种义务。令OB表示义务本身(这种情况下即进行交易)，OBS为该义务的主体*S*(这种情况下即SA)，OBO是该义务的客体(这种情况下即书店内的音像店，即DV@DB)。在DB系统内SA使用“信誉”买书(*buywithCredit*)之前，有义务与DV@DB做一项交易。通过UCON模型中获取义务谓词*getPreOBL*，有：

$OBS=S, OBO=DV@DB, OB=transact$

$getPreOBL(S, buywithCredit, O) = (OBS, OBO, OB)$

另外，DV系统动态地定义了条件，该条件也与“信誉”有关。在信誉卡有效期内，SA(即*S*)可以使用信誉卡属性(*buywithCredit*)买书(即*O*)。*getPreCON*是UCON模型获取的条件谓词：

$getPreCON(S, buywithCredit, O) = \{ DATE \leqslant 2009\text{-}12\text{-}31\}$

当SA使用*buywithCredit*属性在DB买书时，在动态多域授权、义务和条件的基础上，由DB解释属性的语义(构建授权规则)及其相关的动态多域义务执行情况和条件判断，进一步做出使用判定。使用“*allowed*”谓词对授权、义务和条件进行评估判定，有：

$allowed(S, buywithCredit, O) \Rightarrow$

$preFulfilled(getPreOBL(S, buywithCredit, O))$

$\hat{}\, preConChecked(getPreCON(S, buywithCredit, O))$

(下转第80页)

了一个基于此方案的 P2P 识别流量模型。本方法基于 P2P 流特征的机器学习方法，克服了传统的基于端口和特征字方法的不足，并实际考虑了由于流量误识别带来的风险。实验表明，本方法适合实时流量检测，而且通过调整系统参数可以实现高精度检测。下一步的研究目标，首先要进一步地完善本方案，如通过仿真实验和原型系统运行，确定流统计的精确时间间隔、(L_{21}，L_{12}) 的选择等；然后实现方案和特征字匹配的融合，从而更准确地判别 P2P 流量并进行应用级分类。

参 考 文 献

[1] Sen S, Wang J. Analyzing Peer to Peer Traffic Across Large Networks[J]. ACM/IEEE Transactions on Networking, 2004, 12(2): 137-150

[2] Sen S, Spatscheck O, Wang D M. Accurate, Scalable In-Network Identification of P2P Traffic Using Application Signatures[C]// Proc. of 13th International Conference on WWW. New York, NY, 2004: 512-521

[3] Karagiannis T, Broido A, Faloutsos M, et al. Transport Layer Identification of P2P Traffic[C] // Proc. of ACM SIGCOMM IMC. Taormina, Sicily, Italy, 2004: 121-134

[4] Moore A, Zuev D. Internet traffic classification using bayes ananalysis[C] // Proceedings of International Conference on Measurement and Modeling of Computer Systems. 2005: 50-60

[5] Zuev D, Moore A. Traffic classification using a statistical approach[J]. Lecture Notes in Computer Science, 2005, 3431: 321-324

[6] Constantinou F, Mavrommatis P. Identifying Known and Unknown Peer-to-Peer Traffic[C]// Proceedings of Fifth IEEE International Symposium on Network Computing and Applications. 2006: 93-102

[7] 王锐. P2P 流量检测技术研究[D]. 长沙：国防科学技术大学，2006

[8] Liu Hui, Feng Wenfeng. A Peer-To-Peer Traffic Identification Method Using Machine Learning[C]// International Conference on Networking, Architecture, and Storage. 2007: 155-160

[9] 翟永杰，韩璞，王东风，等. 基于损失函数的 SVM 算法及其在轻微故障诊断中的应用[J]. 中国电机工程学报，2003, 23(9)

[10] (美)瓦普尼克. 统计学习理论[M]. 许建华，等译. 北京：水利电力出版社，2004

[11] 肖健华. 智能模式识别方法[M]. 广州：华南理工大学出版社，2006

[12] Waikato Environment for Knowledge Analysis (Weka) [EB / OL]. http: // www. cs. waikato. ac. nz/ml/weak/

[13] Zander S. NetMate0. 9. 4 [EB/OL]. [2008201208]. http: / / www. ip2measurement. org/ tools/ netmate/

[14] Erman J, Mahanti A, Arlitt M, et al. Offline / realtime traffic classification using semi-supervised learning[J]. 26th International Symposium on Computer Performance, Modeling, Measurements, and Evaluation, 2007, 64(9-12): 1194-1213

[15] Li Wei, Moore A W. A Machine Learning Approach for Efficient Traffic Classification[C]// Proceedings of the IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS). Istanbul, Turkey, 2007

[16] Risso F, Baldini A, Bonomi F. Extending the NetPDL Language to Support Traffic Classification[C]// Global Telecommunications Conference, 2007. Nov. 2007: 22-27

(上接第 75 页)

$DA(S).credit \geqslant price(O)$

$id(S) =$ "SA1"

$preUpdate(DA(S).credit): credit' = credit - price(O)$

其中，DA(S)表示多域条件下主体 S 的动态属性集。

在 DB 系统中，当主体 SA 使用来自 DV 的动态多域属性信誉卡时，DB 也为 SA 动态地创建某属性 T(如电影票)：

$AttSetPreUpdate\ (DA(S)): DA' = DA \cup \{ticket\}$

$AttValPreUpdate\ (DA(S).ticket): ticket' = 20$

$AttTypePreUpdate\ (DA(S).type): type' =$ "*Dynamic-Multidomain*"

这样 SA 就可以跨系统使用该属性 T，进而满足了多域交互时刻支持动态属性的系统需求。

结束语 本文对多安全域条件下的动态使用控制问题进行了研究。当前的访问控制模型都是预先定义它们的属性及组件，通过场景示例，论证了这种静态定义不能满足移动的和动态多域的交互需求。为了支持多域的应用环境，我们明确主客体的属性、授权、义务和条件动态特性，在下一代使用控制模型 UCON 的基础之上提出了一种使用控制扩展模型 DAB-UCON，以表示动态授权策略。基于属性定义时间和作用范围，将属性、授权、义务和条件进行分类，扩展后的动态组件有助于动态策略的构建。隐私特性是一个重要的系统安全需求，主体还应具备将属性转移到其它主体的能力。要支持这些特性，还有待于进一步研究。

参 考 文 献

[1] Park J, Sandhu R. The ucon abc usage control model[J]. ACM Transactions on Information and System Security, 2004, 7(1): 128-174

[2] Freudenthal E, Pesin T, Port L, et al. drbac: Distributed role-based access control for dynamic coalition environments[C]// Proceedings of the Twenty-second IEEE International Conference on Distributed Computing Systems (ICDCS). 2002: 411-420

[3] Covington M, Sastry M. A contextual attribute - based access control model[C]// Second International Workshop on Context-Aware Mobile Systems, LNCS 2006. November 2006

[4] Damiani E, Vimercati S, Samarati P. New paradigms for access control in open environments[C]// Proc. of the 5th IEEE International Symposium on Signal Processing and Information. December 2005

[5] Lepro R. Cardea: Dynamic access control in distributed systems [M]. NASA Advanced Supercomputing (NAS) Division, 2003

[6] Hayton R J, Bacon J M, Moody K. Access control in an open distributed environment[C]// 1998 IEEE Symposium on Security and Privacy. May 1998: 3-14

[7] Lin Chuang, Feng Fu-jun. Access control in new network environment[J]. Journal of Software, 2007, 18(4): 955-966

[8] Sandhu R, Park J. Usage control: A vision for next generation access control[C]// Proc. of the 2nd Int'l Workshop on Mathematical Methods, Models and Architectures for Computer Networks Security. LNCS 2776. Berlin: Springer-Verlag, 2003: 17-31