UCON在电子商务系统访问控制中的应用

孙月江
（青岛工学院信息工程系　山东青岛　266300）

【摘　要】访问控制技术是电子商务系统(ECS)安全的关键技术,但传统的访问控制技术在面对开放环境下的电子商务系统安全时具有明显的局限性。使用控制技术(UCON)是一种现代访问控制技术,具有访问过程的连续性控制和属性的易变性控制等新特点,具有解决电子商务系统安全的良好优势。文章选取了三个ECS中典型的访问控制应用情境,然后基于UCON模型实现了较好的应用。

【关键词】访问控制;使用控制;电子商务系统;UCON

The Application of Usage Control Model for Electronic Commerce Systems

Sun Yue-jiang
(Department of Information Engineering, Qingdao Institute of Technology　ShandongQingdao　266300)

【Abstract】The access control is the key technology for secure electronic commerce system (ECS). However, the traditional access control methods could not easily solve the problems under the open and complicated ECS environment. Usage Control (UCON) technology is a modern access control technology. It supports continually control on access process and dynamic control on varying property, which indicates that UCON can be better suit for ECS. Three typical security cases from ECS are selected for using UCON, which demonstrated its benefit.

【Keywords】usage control; access control; electronic commerce systems; UCON

1　引言

访问控制是保障电子商务系统安全的关键技术,对用户的身份认证和信息资源合法使用等进行控制。传统访问控制技术中比较有影响的主要包括:自主访问控制DAC(Discretionary Access Control)、强制访问控制MAC(Mandatory Access Control)和基于角色的访问控制RBAC(Role-based Access Control)。传统的访问控制技术主要关注封闭环境中数据保护,系统访问控制的实现主要通过识别用户,明确其已知属性并确定授权规则,在用户访问操作之前决策其对信息资源的访问控制。访问一旦被授权之后,在整个访问过程中是不加控制的。但对于基于互联网络运行的电子商务系统来说,用户属性及其信息行为具有连续性和动态易变性等特点,传统的访问控制方法无法较好地适应这方面的安全需求。

2　使用控制(UCON)

Park.J和Sundhu.R于2002年首次提出了使用控制(Usage Control,简称UCON)的概念,并于2004年提出了UCON的核心模型——UCONABC模型。模型如图1所示。

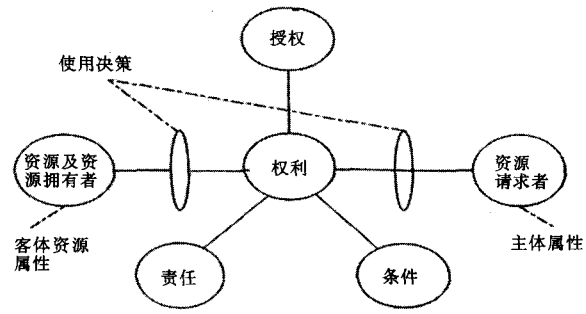

图1　UCONABC模型的组成

UCON 技术定义了授权（Authorization）、职责（Obligation）和条件（Condition）作为访问控制的三个决定性因素，同时支持访问过程的连续性控制和属性的易变性控制这两大新的特性。UCON 可保障用户在访问信息资源的整个过程中对访问请求进行实时监控，主客体属性可随着用户主体的连续性信息行为在访问过程中被动态修改。根据连续性控制的类别及属性更新的时间不同，UCONABC 模型被分为 16 种基本模型，这些基本模型在应对各种复杂的访问控制变化过程时可以单独或组合的方式进行使用。因此，UCON 从机制上比传统访问控制更完备，在现实应用上解决电子商务系统的访问控制问题也更有优势。在我国，现在只有一些较为个别、零散的对 UCON 的认识性研究，对 UCON 在电子商务系统应用方面的研究较为少见。

3 基于 UCON 的电子商务系统应用

以下选取电子商务系统中的典型访问控制情境，基于 UCON 的使用特点对情境进行形式化描述，并给出基于 C# 语言实现的关键函数。

3.1 UCON 在客户授权访问中的应用

（1）情境描述

客户只有在履行某些要求的义务后（如必须注册并在注册过程中提交必须的客户信息等），才能被赋予相应的权限，进行各类商品信息的查看、定制以及下订单和修改删除各类信息等。这在 UCONABC 模型中属于典型的预先义务 - 预先授权模式（UCONpreBpreA）。

（2）形式化描述

OBS=S

OBO={协议}

OB={同意}

registered:S->{是,否}

ATT(s)={registered}

若 registered 值为否，getPreOBL(s,o,r)=(s,协议，同意)

若 registered 值为是，getPreOBL(s,o,r)=Φ

allowed(s,o,r)=>preFulfilled(getPreOBL(s,o,r))

preUpdate(registered(s)): registered(s)= 是

说明：OBS、OBO、OB 分别代表责任主体、责任客体和责任行为。getPreOBL 是获取消费主体必须履行的义务集合的函数。preFulfilled 是用来检测 getPreOBL 中的每一个义务元素是否被满足的判断谓词。“allowed(s,o,r)=>preFulfilled(getPreOBL(s,o,r)),preUpdate(registered(s)): registered(s)= 是”表示如果主体 s 拥有对于客体 o 的权限 r，则一定满足所有要求的义务，并将主体的注册属性更新为是。

3.2 UCON 在客户购买中的过程控制

（1）情境描述

有些电子商务系统会希望根据客户当次购买情况动态决策优惠策略。如客户购买金额达到一定数量，例如 10 万元，则该客户可以被赋予以 5 折的超低价购买某些特定产品的权限；超过 20 万元，则该客户可以被赋予以 4 折的超低价购买某些特定产品的权限。这是一种比较典型的访问过程中进行授权，属性更新，访问后也要进行属性更新的情况，即 UCONonA23 模型适用的情境。在此过程中，授权决策周期性的进行检测判断，以保证当某个断言属性满足条件时，所有的授权要求可以得到满足。监测过程可以基于时间周期性的进行。这种情境中，基于本次采购金额对客户进行授权，首先确定主体的相关属性满足要求，然后判断客体的相关属性（例如，根据该属性判断是否可以打 5 折的优惠）。当然，操作完成后，需要进行相关属性的更新。

（2）形式化描述

id : S->N

AM: O->N

ATT(s): {id,M}

ATT(o): {id,AM}

allowed(s,o,r)=>(M>=AM∧o 存在)

stopped(s,o,r)<={ M<AM∨o 不存在}

onUpdate(M(s)): M(s)= M(s)+MT（当前采购金额）

postUpdate(credit(s)): credit(s)= credit(s)+fc(M)

postUpdate(degree(s)): fd(M)

说明：s 表示访问的主体，M 代表当前已采购金额，AM 代表可以进行授权的采购金额，N 代表一系列标识名称，fc(M)表示信用等级评价函数，fd(M)表示客户级别评价函数。

3.3 UCON 在客户购买后的信息属性更新

（1）情境描述

为了更为灵活有效地鼓励客户进行大额交易，有些电子商务系统会根据客户的历史交易记录决策其信用等级和折扣策略。比如，如果某客户的信用额度等级为二级，则该客户可以采用货到付款或者赊欠金额不超过 1 万元的商品；如果该客户为五星级会员，可以以 8 折的

折扣下单。在传统的访问控制策略中,客户所能够得到的折扣比率,在采购过程中一般不会改变,但是在本次订单完成后,有可能会根据该客户多次采购的金额总和重新确定他的信用等级和折扣比率。这属于访问完成后进行信息属性更新的情况,即 UCONpreA3 模型符合的情境。

(2)形式化描述

credit: S->M

value: O× R->M

ATT(s): {credit}

ATT(o,r): {value}

Allowed(s,o,r)=>credit(s) ≧value(o,r)

preUpdate(credit(s)): credit(s)= credit(s)-value(o,r)

说明:M 代表金额,credit 表示主体所具有的信誉值;value 表示客体及权限的对应的值的集合。"ATT(o,r): {value}" 表示对于客体具有 r 权限需要的值。"Allowed(s,o,r)=>credit(s) ≧value(o,r)"表示如果主体对客体具有权限 r,则主体的信誉属性值一定大于或等于客体所需要的值。"preUpdate(credit(s))"表示需要对主体属性进行预先更新。

4 总结

作为新一代访问控制技术,使用控制因其访问过程的连续性和易变属性的可控性特点使其能够较好地适应电子商务系统中的访问控制情境。文章选取了几个典型情境进行了使用描述和代码实现,这为进一步更好地解决电子商务系统的安全问题提出了一种新的思路。随着 UCON 技术的逐渐发展和成熟,将会有越来越多的软件系统对其进行应用和实践。

参考文献

[1] 颜伟东.管理信息系统中的权限管理解决方案 [D].四川大学软件工程,2005.4.

[2] 宁葵. 访问控制安全技术及应用 [M]. 电子工业出版社. 2005,10.

[3] 张绍莲,茅兵,谢立. 访问控制技术的研究和进展[J]. 计算机科学. 2001,7.

[4] Jaehong Pack, Ravi Sandhu.The UCONABC Usage Control Models [R].ACM Transactions on Information and System Security (TISSEC), 2004, (10).

[5] 聂丽平.基于 UCON 访问控制模型的分析与研究 [D].合肥工业大学计算机软件与理论,2006.5.

[6] 田跟东,甘仞初.基于角色的 MIS 系统授权机制的研究和应用[J].计算机工程与应用.2002,25(3):239~240.

[7] 刘伟. 基于角色的访问控制模型在安全操作系统中的实现 [D].中国科学院软件研究所.2003.

作者简介:

孙月江,男,汉族,山东青州人,讲师,硕士;研究和关注方向:信息安全。

【上接第 44 页】

```
<table border='0' width=250 height=50>
<tr valign='middle'>
<td align='center'>
<form name=form>
<input type=button value=' 开始抽取随机数组 ' onClick="lotto(),setTimeout('clearTimeout(T)',1000)">
</form><span id=layer1 class=a1> 显示结果 </span>
</td></tr></table></body><html>
```

4 结束语

文章对 JavaScript 做了简要的介绍,大家对 JavaScript 脚本语言有一个初步认识,并通过一个随机抽取分组数据的小实例,对 JavaScript 脚本的应用实现做一展示。该实例稍加改动即可成为随机数据源提取、福利彩随机选取等应用。

作者简介:

刘韶华(1972-),男,硕士,工程师;研究方向:信息技术工程。