电子机构的安全性分析研究①

Security Analysis and Research for Electronic Institutions

李红霞　蔡国永　（桂林电子科技大学 计算机与控制学院 广西 桂林 541004）

摘　要：电子机构是人类机构代理的副本，为提供支持、信任和合法性商业应用而具体设计。它是以网络为基础的，一种虚拟的管制环境，然而在现有的研究中，并没有实现电子机构基于角色的访问控制。本文根据电子机构的基本概念，提出了电子机构基于角色的访问控制模型，并从系统权限、身份认证以及访问控制的角度，研究电子机构的安全性。描述了重写逻辑 Maude 工具建模的方法和过程。最后，用重写逻辑 Maude 工具实现了网上购物系统的登录身份认证。

关键词：电子机构 安全 角色 访问控制

1　引言

近几年来由于 Internet 的爆炸式使用，电子商务的迅速发展，一种现代的网络信息系统，虚拟的交易平台等得到广泛的使用，又由于计算机系统和网络在快速增长的现代社会中扮演一个越来越重要的角色，在功能性、连通性和可达性中，人们的生活变得比以前任何时候都更加与信息紧密相关。同时，人们也正努力的研究信息系统的可靠性和安全性，因为任何故障，失败，错误或攻击，都可以大大降低系统的运行能力或者造成很大的经济损失。又因为软件系统运行在开放的环境中面临着越来越多的攻击或入侵。而电子机构（Electronic Institutions）是针对一种虚拟的管治环境建立一个统一的模型。因此，在虚拟的管治环境中，安全是一项重要的保障和前提。然而，在现有的关于电子机构的文献中，主要是采用义务逻辑、状态变迁以及进程代数等方式来建模、分析、形式规约以及对电子机构开发环境和开发工具的研究等等，并没有对电子机构的安全性进行过研究。

本文主要是从系统权限、身份认证以及基于角色的访问控制的角度，研究电子机构的安全性，并提出电子机构基于角色的访问控制模型。

2　电子机构的基本概念

在信息技术、电子商务迅速发展的今天，从开始的 B2B，到 B2C，再到正在筹建的 C2C 交易平台，这些都建立在虚拟网络的基础上。在以网络为中介环境的协同工作中，电子机构[EI]是一种虚拟的管治环境，对参与到该环境中相关实体的交互行为进行管治。有关电子机构的模型请参见[1,2]。电子机构由四个要素组成[3,4] 对话框架、场景、执行结构和规范。下面一一介绍：

(1) 对话框架（Dialogical framework）

对话框架定义代理可能交互的有效表达行为，并且定义参与者角色和角色关系。对话框架提供的结构，因共同的本体，有助于异构代理共同进行交互。即，通过共享一个对话框架，使异种代理与其他代理交换知识。活动在电子机构中由不同的、可能并发的，对话式的活动等多种情况组成，每个活动包括不同的代理组，扮演不同的角色。

(2) 场景（Scene）

两个代理间的交互是通过代理组汇合点铰接，这称为场景。在场景的一些特殊状态和根据这个场景中他们的角色，代理可以进入场景或离开场景。场景之间的关系可以是一对一、一对多和多对一的关系。

① 基金项目：广西自然科学基金（NO. 0728089）

(3)执行结构(Performative structure)

执行结构指定场景之间的关系,为了捕获场景之间的关系,我们使用场景的一个特殊类型,即所谓的变迁。变迁可以被视为一个执行结构网中路由器的类型。执行结构包含多种同时正在进行的活动,由场景扮演。在执行结构之内,代理可以在同一时间用不同的角色参与到不同的场景中。

从结构的角度来看,执行结构的规范必须视为场景的网络。场景之间的连接根据他们的角色定义哪个代理,通过已经定义的变迁,可以从一个场景移到另一个场景。即,执行结构定义了哪些场景可以由每个不同的角色到达。

(4)规范(Norms)

规范定义什么是允许的,什么是禁止的以及什么是责任。执行结构的规范包含如何描述不同的角色可以合法地从场景到场景移动。

总而言之,电子机构,当调控代理之间可能发生的交互时,能代表基准系统限制参与者行为并且描述当违反标准时的惩罚。契约关系在机构内部被创建,并必须遵守强制标准,制定特殊商业关系的细节。

3 电子机构的安全性分析

电子机构[5]是包含自治、独立实体必须遵守通用、明确的交互协议的开放系统。因此在安全性方面必须具有应用系统的安全性特征[6]:完整性、可用性、保密性以及可控性。

3.1 电子机构基于角色的访问控制模型

基于角色的访问控制其核心思想[7]是在用户和权限间建立一种机制,将访问权限与角色相联系,通过给用户分配一定数量的合适的角色,让用户获得相应的访问权限。用户与角色、角色与权限、角色与资源之间的关系均是多对多的关系。在角色之间存在继承关系,即下级角色可继承上级角色的部分或全部权限,从而形成了角色层次结构。

在应用系统中,系统用户的权限是与其工作内容相关的,用户的工作内容决定了可以访问的资源和对资源的操作,同一个用户在不同的业务上下文环境中,所扮演的角色不同,因此,在涉及系统权限时,往往不是针对用户,而是针对用户在业务活动中所扮演的角色进行权限分配。根据电子机构的概念,针对电子机构中场景的角色采用访问控制,电子机构基于角色的访问控制模型如图1所示:

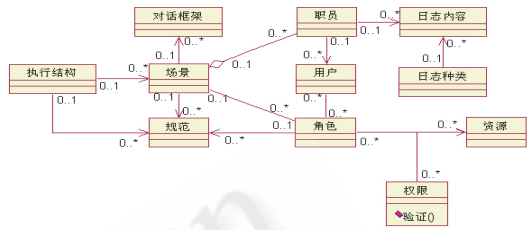

图1 电子机构基于角色的访问控制模型

说明:图1中,单箭头表示单向联接。菱形是聚合(Aggregations),是强连接,聚合是整体与个体之间的关系。

模型中引入了日志管理,这里的日志管理是应用软件本身的日志,而不是操作系统的日志管理。日志管理对于一个系统是极为重要的,日志管理对进入系统的每个用户所做的操作都要进行记录,从用户进入系统的时间到所做的各种自己权限范围内的操作都会有详细的记录。这样做的好处:1)可以反馈当时的系统情况,为工程商查找故障时提供线索;2)是落实某些操作员违反公司规定操作的责任和证据,从而也进一步保证了系统的安全操作。

3.2 身份认证

基于角色的访问控制建立在身份识别的基础上[8],根据身份对提出的资源访问请求加以控制。如果身份认证存在安全漏洞,其必将影响到访问控制策略的实施。所以访问控制技术必然和身份认证技术接合起来使用。身份认证是从用户处获取标识凭据(如用户名和密码)并通过某些授权机构验证凭据的过程;是任何信息系统或应用系统的重要环节;是基于访问控制的第一步。身份验证的过程如图2所示。

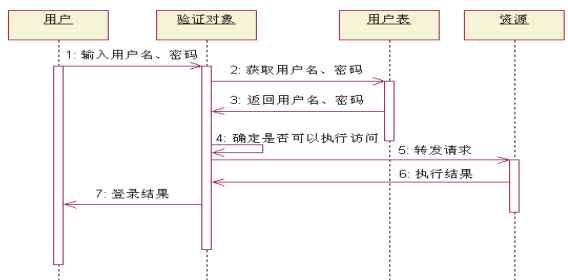

图2 身份认证过程

4 案例研究

为了具体说明电子机构的安全性,设计了简单的基于面向对象的网上购物系统模型,主要是体现图1中的验证以及对执行结构和场景的分析。在案例中买家需要先成功登录系统后,然后才可以在卖家的商店中选购商品。买家选购商品流程如图3所示:

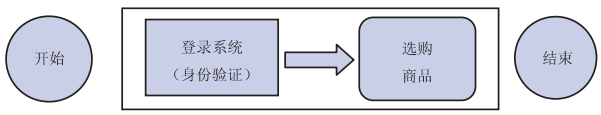

图3　买家选购商品流程

具体的业务需求如下:

1)买家先注册,成功登录系统后,才能挑选商品。

2)卖家的商品分高、中、低档三类商品,同一档次的商品价格一样。商品价格和类型卖家都需要保存在数据结构中。

3)买家在卖家中可以成为会员。会员分为:普通会员和高级会员两类。买家在卖家中的消费额是可以累积的,一个普通会员当消费额达到一定程度可以变成高级会员。

4)根据会员级别和购买商品的类型可以享受不同的优惠价格。如果买家的信誉不好,卖家停止卖商品给买家。

4.1 建模过程及方法

对网上购物这个实例,采用重写逻辑Maude工具来建模。重写逻辑是定义和构建复杂物体的技术,它根据重写规则依次替换简单初始物,从而构造出复杂对象。它对自身相似对象的建模很有效,在数千种自身相似的元素中,只用一些规则就可以通过简单物体描述复杂的对象[9],这是重写逻辑所特有的。电子机构是面向对象的、并发的、开放的系统,因此,采用Maude中,面向对象的建模方法对电子机构系统进行建模,其建模过程具体如下:

1)首先了解系统的业务需求,对整个系统进行需求分析,确定系统中的各个对象、角色以及类,并确定类的属性、类型及方法(类中使用的函数);

2)分析各个角色之间的关系,构造出各个角色之间的消息传递关系;

3)分析每个对象与哪些角色有关;

4)定义面向对象的规则(含角色及对象之间的交互规则);

5)定义业务流程,即规则之间的执行顺序;

6)建立面向对象的系统模型;

7)利用工具运行所建的模型,对其系统进行模拟。

当确定了所有的实体后,就可以建立系统模型。采用Maude中参数化面向对象模块的建模方法[10],具体如下:

1)角色中的每个关系,由类塑造以关系名作为类名,并且类的属性是参与者的标识符和关系属性的标识符;

2)每个角色由Maude类描述,在软件系统中,角色好比一个插槽,在运行的时候由对象来填补;

3)业务对象由Maude中的对象描述。在Maude中,每个对象都属于类。一个对象也可以同时属于多种角色类型,就像一个人可以扮演多种角色一样;

4)团队是由业务对象构成,因此由Maude的配置(configurations)描述;

5)系统中的动作由Maude中的规则描述;业务流程在Maude中相当于我们定义的执行策略。

4.2 网上购物系统分析

下面使用重写逻辑Maude工具来实现网上购物系统登录的身份验证。从这个系统的结构开始,可以确定三个主要的角色,即买家(purchaser)、卖家(bargainor)和商品(merchandise)。买家有两种特殊的种类——普通会员(GeneralMember)和高级会员(AdvancedMember),卖家的商品有三种种类---高档商品(SlapUpMerchandise)、中档商品(MidMerchandise)和低档商品(LowEndMerchandise)。

买家(purchaser)这个角色由Purchaser类来描述它的类型,Purchaser类有四个属性:cash(买家拥有的现金)、pay-sum(购买商品需要支付的钱)、passwd(登录密码)、loginstatus(登录系统的状态),具体的定义如下:

class Purchaser | cash:Int, pay-sum:Int, passwd:Int, loginstatus:PFun {Oid, Int}.

class GeneralMember. class AdvancedMember.

subclasses GeneralMember AdvancedMember < Purchaser.

卖家(bargainor)这个角色由 Bargainor 类来描述它的类型,Bargainor 类的属性有:discounts(折扣)、total – expenditur(消费总额)、upgrade – standard(从普通会员升级为高级会员的标准)、merchandise(商品)等属性,具体的定义如下:

class Bargainor | discounts :PFun {Tuple {Cid, Cid}, Int}, total – expenditure :PFun {Oid, Int}, credit – value :PFun {Oid, Int}, upgrade – standard :Int, receive – sum :PFun {Oid, Int}, suspended :Set {Oid}, price :PFun {Cid, Int}, userpasswd :PFun {Cid, Int}, should – pay – sum :PFun {Oid, Int}, purchaser :Set {Oid}, merchandise :Set {Oid}, calendar :Oid .

因为折扣(discounts)需要根据会员的级别以及购买商品的级别共同来确定优惠的价格,因此由局部函数 PFun {Tuple {Cid, Cid}, Int} 来定义。消费总额(total – expenditure)需要保存是哪个买家的消费额,且需要累加,用局部函数类别 PFun {Oid, Int} 返回买家的消费额。其它属性的定义也是类似。

商品角色由 Merchandise 类描述,商品的属性 status,用于记录是否已经卖出。

class Merchandise | status :Bool .

class SlapUpMerchandise . class MidMerchandise .

class LowEndMerchandise .

subclasses SlapUpMerchandise MidMerchandise LowEndMerchandise < Merchandise .

买家和卖家之间的关系由 Purchase 类来定义。

class Purchase | price :Int, pay – sum :Int, discount :Int, buyDate :Int, purchaser :Oid, merchandise :Oid .

另外,为了让这个例子在 Maude 工具中运行,我们还需要定义用户登录系统的规则 user – login,以及用户选购商品的规则 purchaser – buy – merchandise。

为了测试建立的模型是否正确,我们首先建立一个配置。框架如下:

(fmod NETWORK – TRADE – MERCHANDISE – TEST is

pr NETWORK – TRADE – MERCHANDISE .

op BargainorConf : – > Configuration [memo] .

eq BargainorConf

= ...(具体代码省略)

endfm)

在 BargainorConf 中,需要配置下列内容:1)一个卖家 B,并定义卖家的高、中、低档商品的价格;2)不同级别的顾客的折扣;3)从普通会员升级为高级会员的标准;4)配置两个买家 P1,P2;5)三类商品 M1,M2,M3 以及日历对象 C。在配置完 BargainorStrat 后,需要定义一个功能模块 REW – SEQ – TEST,在该模块中定义声明的策略作为动作执行的顺序序列。

现在我们已经建立了可执行的模型,首先测试两个不同的用户登录系统,P1 用户能够正确登录系统(密码正确),而 P2 用户则不能(密码错误)。采用系统命令 down 运行这个模型,运行结果如图 4 所示。

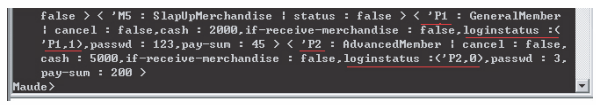

图 4　Maude 中两个不同用户登录运行的结果

用户 P1 成功登录后,选购商品的运行结果如图 5 所示:

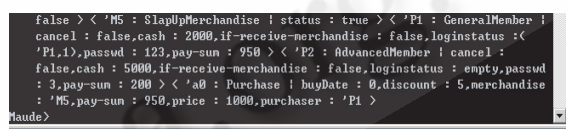

图 5　P1 用户成功登录选购商品运行结果

从图 5 我们可以看出 P1 成功登录系统后,选购了商品 M5,商品价格为 1000 元,折扣为 5(百分比),最后应支付的金额为 950 元。

用户 P2 因为登录系统失败,则不能选购商品,运行结果如图 6 所示:

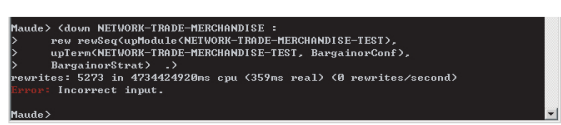

图 6　P2 用户登录失败不能选购商品运行结果

根据上面的运行结果,我们可以了解到,在重写逻辑中,我们对系统登录的身份进行了成功的验证。虽然这个例子比较简单,但是通过上面的实验,我们可以得出两点结论:(1)这个模型是一个在 Maude 中可以

执行的模型,即是一个被 Maude 所支持的合法的重写逻辑形式化模型。(2)在重写逻辑 Maude 工具中,可以对用户身份进行验证。

5 结语

在开放异构、并发、分布式的系统中,要解决系统的安全问题,本身就是一件很难的事情,需要我们从多个方面去考虑,如:操作系统、应用软件、数字签名、证书验证、加密技术等等。最好是多个结合起来使用。本文主要是从系统权限、访问控制以及身份验证这几方面讨论了电子机构的安全性。虽然本文提出了电子机构基于角色的访问控制模型,并使用重写逻辑 Maude 工具实现了网上购物系统的系统登录身份认证,但还有待于进一步完善,在实际的系统或项目中,要具体情况具体分析。下一步,我们将从多个方面,更加深入的研究电子机构的安全性。

参考文献

1 Huib Aldewereld, Frank Dignum, Andres Garcia – Camino, Pablo Noriega, Juan Antonio Rodriguez – Aguilar. Operationalisation of Norms for Electronic Institutions. Lecture Notes in Computer Science, 2007: 163 – 176.

2 蔡国永,高济,董荣胜. 电子机构的进程代数模型研究. 微电子学与计算机,2007,24(10):74 – 77.

3 Marc – Philippe Huget, Marc Esteva, Steve Phelps, Carles Sierra, Michael Wooldridge. Model Checking Electronic Institutions. In Proceedings of Model Checking and Artificial Intelligence (MoChArt). Lyon, France. 2002,07.

4 Vazquez – Salceda J, Padget J. A, Cortes U. Lopez – Navidad A., Caballero F. Formalizing an electronic institution for the distribution of human tissues. Artificial Intelligence in Medicine. Elsevier. 2003. 03,27(3): 233 – 258.

5 M. Estena . Electronic Institutions: from specification to development. PhD thesis, Technical. University of Catalonia . 2003.

6 甄镭. 信息系统升级与整合:策略·方法·技巧. 电子工业出版社,2004. 01.

7 臧洁. 角色访问控制模型在 Struts 结构下的应用研究[硕士学位论文]. 大连海事大学. 2005 年 3 月.

8 张路桥,赵军,何林波 . 基于角色的访问控制综述. 科技信息, 2007,10.

9 刘尚勤,重写技术构建动态虚拟环境的研究. 计算机时代, 2006,10.

10 F. Durán, A. Vallecillo. Writing ODP enterprise Specifications in Maude . Proceedings of ICEIS 2001, Workshop On Open Distributed Processing – WOODPECKER 2001, J. Cordeiro, H. Kilov (Eds.), Setúbal, Portugal, July 2001:55 – 68.