具有特征判断能力的使用控制模型研究

石伟丞[1] 谭 良[1,2] 周明天[3]
(四川师范大学计算机学院 成都 610066)[1] (中国科学院计算技术研究所 北京 100080)[2]
(电子科技大学计算机科学与工程学院 成都 610054)[3]

摘 要 传统访问控制的研究重点是授权策略,关注的是如何为主体分配权限以及如何限制主体使用分配得到的权限。目前绝大多数访问控制策略仍无法识别与控制具有访问权限的非法用户。在分析传统访问控制策略不足的基础上,提出了一种基于UCON的具有访问特征判断能力的使用控制模型——C_UCON。该模型通过在UCON的基础上引入既定义务、待定义务、即定条件、待定条件以及特征和激活规则来对访问进行主观判断,从而降低或者排除具有访问权限的非法用户所带来的安全威胁。

关键词 信息安全,访问控制,使用控制,特征
中图法分类号 TP309 **文献标识码** A

Usage Control Model with the Ability of Character Judging

SHI Wei-cheng[1] TAN Liang[1,2] ZHOU Ming-tian[3]
(College of Computer, Sichuan Normal University, Chengdu 610066, China)[1]
(Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100080, China)[2]
(School of Comp. Sci. & Engn., Univ. of Electronic Sci. & Tech. of China, Chengdu 610054, China)[3]

Abstract The emphases of traditional access control studying is the policy of authorization, the studying is focus on how to distribute permissions to subject and how to restrict the using of these permissions. Based on the analysis of traditional access control, we introduced a new mode, C_UCON, which is based on the UCON and has the ability to judge the character of accessing. By introducing assure obligations, unsure obligations, assure conditions, unsure conditions, characters and active rules, the C_UCON has the ability to judge accessing subjectively, thereby reduce or exclude those threats from the illegal users who has permission.

Keywords Information security, Access control, Usage control, Character

访问控制被认为是系统资源安全必不可少的基础性防护手段,它通过某种显示的途径允许或者限制主体对于客体的访问能力和范围,达到系统资源被受控、合法地使用的目的。纵观访问控制30余年的发展历程,访问控制取得了众多的研究成果,但是值得关注的是信息安全事故依然层出不穷[1]。传统访问控制的核心是授权策略。授权策略是用于确定一个主体能否具有访问客体的权利。在传统访问控制授权策略下,只要主体被授予某种权限,那么主体就能以该权限访问客体,其形式如下:

If 拥有访问权限 Then 允许主体访问客体

然而对于访问权限的持有可能存在以下3种情况:①被合法用户持有,如图1的⑤→⑥→③→④访问过程。②由于权限泄露被非法用户非法持有,如图1的⑦→⑧→⑨→⑩访问过程。③由于合法用户的身份泄露或者被伪造而导致访问权限被非法用户持有,如图1的①→②→③→④访问过程。我们称②、③情况中的权限持有者为具有访问权限的非法用户。由于传统访问控制策略是基于用户身份验证的,一旦通过身份验证,便可以取得相应主体身份,并行使相应访问权限。而访问权限是否被"合法"使用,对于传统访问控制来说是无法辨别的,因此传统访问控制无法防止具有访问权限的非法用户所造成的威胁。例如(如图1中①→②→③→④过程)用户B的网上银行账号密码被用户A窃取,那么A可以以B的身份登录网上银行,对账户上的金额进行转账操作,导致用户B的账户金额被盗。

因此,我们认为一个完备的访问控制不仅应该具有防止权限的泄露和防止身份被窃取或者伪造的预先防护能力,还应该具备即使出现权限泄露、身份被窃取或者伪造时的后续防护能力。

到稿日期:2009-07-09 返修日期:2009-09-30 本文受国家自然科学基金项目(60970113),四川省科技厅项目(2008JY0105-2)和四川省教育厅项目(07ZA091)以及实验室专项基金(2006ZD022)资助。

石伟丞(1981—),男,硕士,主要研究方向为操作系统安全,E-mail:shi_wei_cheng727@126.com;谭 良(1972—),男,博士,主要研究方向为信息安全、分布式计算;周明天(1939—),男,教授,博士生导师,主要研究方向为计算机网络、网络计算技术、中间件技术、并行分布处理、网络与信息系统安全。

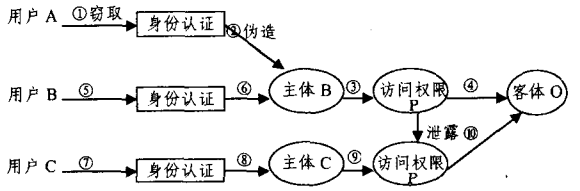

图 1　可能的访问流程

1　相关工作

如果把目前既有的访问控制模型按照授权策略来划分，那么最具代表性的是自主访问控制(DAC)、强制访问控制(MAC)、基于角色的访问控制(RBAC)。

自主访问控制策略中，允许用户按照自己的意愿将访问权限或者访问权限子集转授于其他用户或组。Lampson[2]首先提出访问控制矩阵为自主访问控制的实施提供了一个框架；随后 Graham 和 Denning 对 DAC 进行了重定义并提出了 GD[3]模型；再后来 Harrison，Ruzzo 和 Ullman 将其形式化描述为 HRU[4]模型。自主访问控制策略虽具有较高的灵活性与细粒度性，但是也存一些明显缺点，例如其授权自由度过大，容易引起权限的泄露和滥用。其最大的缺点是不能抵御木马的威胁。针对这些缺陷学者进行了进一步的完善。Bertino 等人提出的基于时间的自主访问控制模型[5]，在 DAC 的基础上引入了有效授权的时序概念以及时序依赖；随后 Bertino 又在此基础上为授权提供了周期时间的约束和基于时序依赖的推导规则[6]；后来国内的张宏等人在 Bertino 等人研究的基础上引入了委托概念，并提出了基于周期时间限制的自主访问控制委托模型[20]。改进后，从一定的程度上遏制了权限的滥用问题，授权机制也更为灵活，但是仍然不能抵御木马的威胁。

强制访问控制策略的核心是为主体和客体分配安全等级标签，通过对比主体和客体的安全等级来决定主体对客体的访问。强制访问控制策略可以分为 2 类：①基于保密原则的强制访问策略，其代表模型是 BLP[7]模型，利用不上读/不下写来保证保密性。②基于完整性的强制访问策略，其代表模型是 Biba[8]模型，利用不上写/不下读来保证完整性。其中 BLP 模型被认为是基本安全定理[9]，应用较为广泛，但是 BLP 模型本身存在安全级定义不完备、信息完整性、时域安全性和隐蔽通道等缺陷。为弥补这些缺陷，人们做了许多完善工作，其中较为重要的成果是 BLDM 模型[9]和 MBLP 模型[21]。由 NAS 开发的 SElinux[10,11]融入了域-类型(domain-type)和强制访问控制策略，同时采用了基于角色的访问控制概念。这一系列的改进虽然使信息保密性缩小了威胁的范围，但是如果出现高等级权限的泄露，仍然会对系统产生严重的影响。

角色访问控制策略中，权限不再直接赋予主体，而是将权限赋予某个角色。主体通过角色分配而获得所属角色的权限。RBAC 可以说是目前访问控制领域研究较广泛的一种技术。1992 年就出现了 RBAC 的雏形，Ferraiolo-Kuhn 模型[12]；随后 Sandhu 等人先后提出了著名的 RBAC96，ARBAC97，ARBAC99 模型；直到 2001 年 NIST 提出了 RBAC 标准[13]。对 RBAC 的扩展应用中，较具有代表性的有 T-RBAC[14]——将角色与任务关联，TRBAC[15,22]——将角色赋予时间特性，RCLT[23]——将角色引入委托的概念，等等。角色访问控制扩展研究进一步增强了角色的灵活性和时效性，但是当出现角色泄露或者被非法持有时，角色具有的权限便可能被非法利用。

可见，一直以来对于访问控制的研究重点仍然是授权策略，其关注的是如何为主体分配权限以及主体如何让用户受控地使用分配的权限，可描述为以下形式：

If 拥有访问权限 && 符合权限使用限制条件

Then 允许主体访问客体

而这一系列改进后的传统访问控制仍然是基于主体身份进行的，仍然不能够防止具有访问权限的非法用户所造成的威胁。传统访问控制策略只是专注于主体权能，即主体能以何种方式访问某个客体，忽略了主体是如何被现实用户使用的，即现实用户能如何利用主体身份来访问客体。本文后续部分将在 UCON 的基础上提出一种基于使用特征的具有主观判断能力的新型访问控制模型：C_UCON。

2　UCON 简析

Sandhu 等人于 2002 年提出了被称为下一代访问控制模型的 UCON[16]，它是凌驾于传统访问控制之上的更高抽象层次的访问控制模型。该模型由 8 个组件组成：主体 S、主体属性 ATT(S)、客体 O、客体属性 ATTR(O)、权限 R(Right)、授权 A、义务 B、条件 C。这 8 个组件的定义可参考文献[16]，在此不再累述。8 个组件之间的关系如图 2 所示。图中使用决策过程被看作是主体、客体、授权、义务以及条件之间存在的某种关系。

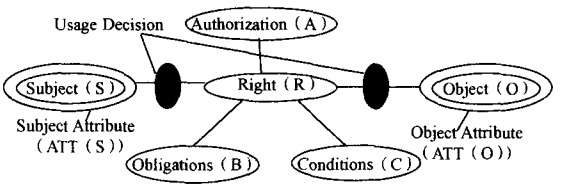

图 2　UCON 模型

这 8 个组件中，授权、义务与条件是使用决策的 3 大决定因素。授权是基于主体和客体属性进行的，义务是主体在访问前或者访问中必须完成的任务，条件是系统环境的约束。其中义务和条件是 UCON 提出的新概念，是对传统访问控制的完善，也是区别于传统访问控制的所在。UCON 可描述为以下形式：

If 主体符合授权策略 && 完成相关义务 && 符合相关条件

Then 允许主体获取或者使用权限

UCON 模型很明显的特性是使用决策的连续性和属性的易变性[17]。连续性使得访问决策可以在访问前或者访问中实施，易变性的作用在于回收不符合授权规则的访问权限。

基于这 8 个组件，文献[16]中给出了 UCON 模型如何实现 DAC，MAC，RBAC，DRM 和 Trust Management。可见，UCON 为访问控制提出了一种通用的模式。正是由于 UCON 的完备与模型的通用性，才使我们选择 UCON 作为基础模型进行研究。

3　具有特征判断能力的使用控制模型(C_UCON)

目前，对于 UCON 的研究大多是应用性研究[18,19,24]。研

究成果分别从不同的应用面对 UCON 进行了完善，但是仍然没有弥补 UCON 本身的不足。主要体现在以下 2 个方面：①在进行授权判断时，使用的义务和条件都是固定的，这种“死规矩”限制了访问判断的灵活性。②仍然是在承认当前活动主体身份的基础上进行的，依然不能判断访问权限是否被合法持有，不能防止权限泄露以及身份被窃取或者伪造所带来的威胁。针对这些不足之处，C_UCON 将 CUON 中的义务分为了既定义务 AB(Assured Obligation)和待定义务 UB(Unsure Obligation)，将条件分为了既定条件 AC(Assured Condition)和待定条件 UC(Unsure Condition)，同时增加了新的组件：激活规则 AR(Active Rule)和特征 H(cHaracter)。其中特征分为原始特征 OH(Original cHaracter)和进化特征 EH(Evolution cHaracter)。C_UCON 通过引入待定义务和待定条件增强了义务与条件的伸缩性，通过引入特征和激活规则而具有主观的判断能力，因而系统可以根据当前活动的用户的活动特征来辨别当前用户身份是否可信，并根据相应规则来决定活动主体是否需要承担额外义务或者满足额外条件来支持访问的发生或者继续。C_UCON 的模型结构如图 3 所示。下面在介绍一些基本概念的基础上对 C_UCON 模型结构进行分析，并给出如何通过特征来辨别用户身份的过程，最后列举一个实例来进行说明。

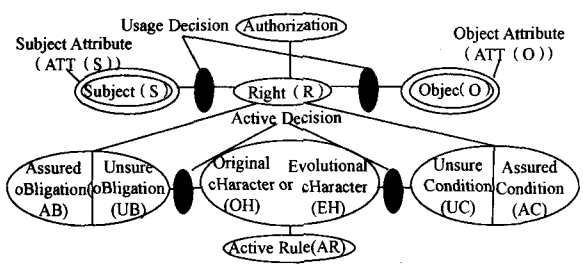

图 3　C_UCON 模型

3.1　C_UCON 基本概念

定义 1(访问，Access)　访问可以表示为 3 元组(s,o,r)，其中 s 为访问主体，o 为访问目标客体，r 为访问权限。访问是具有访问属性 AP(Access Property)的，例如访问时间、访问类型、访问方式等。根据具体应用，访问具有不同的属性。

定义 2(特征，cHaracter)　特征是从访问属性中抽象出来的一系列具有代表性的相对稳定值。其中由安全管理员直接赋予的特征称为原始特征 OH(Original cHaracter)，作用是初始化特征。在原始特征的基础上根据历史访问记录计算得到的特征称为进化特征 EH(Evolution cHaracter)，可见进化特征是原始特征进化的产物。特征反映的是主体对客体的特定使用方式或者使用习惯。

定义 3(义务，oBligation)　义务是主体在使用或者取得某特定权限时必须履行的职责。义务可以分两类：①既定义务，②待定义务。既定义务 AB(Assured Obligation)是已经明确指定主体在使用或者取得某特定权限时必须履行的职责，是带强制性的。待定义务 UB(Unsure Obligation)是主体在使用或者取得某特定权限时可能需要承担的义务。待定义务是有激活条件的，需要根据当前活动主体的访问特征来决定主体是否需要承担这个待定义务。

定义 4(条件 C，Condition)　条件是主体在使用或者取得某特定权限时系统或者执行环境必须满足的条件。条件可以分为两类：①即定条件，②待定条件。既定条件 AC(Assured Condition)是已经明确指定的主体在使用或者取得某特定权限时系统或者执行环境必须满足的条件，是强制性的。待定条件 UC(Unsure Condition)是主体在使用或者取得特定权限时系统或者执行环境可能需要满足的条件。待定条件是具有激活条件的，需要根据当前活动主体的访问特征来决定是否需要满足某种待定条件。

定义 5(激活规则 AR，Active Rule)　激活规则是由安全管理员定义的，用以根据当前用户操作特征来判断当前用户需要额外承担哪些义务或者满足哪些条件的规则。

3.2　C_UCON 模型分析

基于 3 个决定因素，授权、义务、条件以及主体属性、客体属性在访问期间的延续性和可变性，UCON 可分为 16 种可能的基本模型[14]，如表 1 中的粗体部分。C_UCON 在 UCON 的基础上引入了特征组件。C_UCON 具有 18 种可能的基本模型。

表 1　C_UCON 的 18 种基本模型

	0(immutable)	1(per-update)	2(ongoing-update)	3(post-update)
perA	**Y**	**Y**	**N**	**Y**
onA	**Y**	**Y**	**Y**	**Y**
perB	**Y**	**Y**	**N**	**Y**
onB	**Y**	**Y**	**Y**	**Y**
perC	**Y**	**N**	**N**	**N**
onC	**Y**	**N**	**N**	**N**
perH	Y	N	N	N
onH	Y	N	N	N

C_UCON 具有 4 个决定因素，分别为授权、义务、条件和特征。其中特征在模型中的决定作用是通过义务和条件来实现的，所以特征不能摆脱义务和条件而单独存在。图 4 反映了 C_UCON 可能的组合模型。

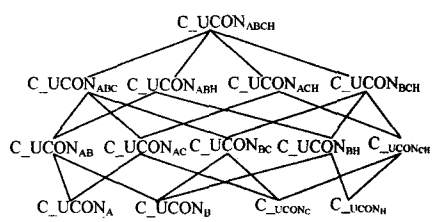

图 4　C_UCON 可能的组合模型

由这 4 个决定因素 C_UCON 可分为 8 个子模型：C_UCON_{perA}，C_UCON_{onA}，C_UCON_{perB}，C_UCON_{onB}，C_UCON_{perC}，C_UCON_{onC}，C_UCON_{perH}，C_UCON_{onH}。其中前 6 个子模型与文献[4]中完全一致，限于篇幅在此不再重复。下面着重介绍特征模型中的预先特征模型(C_UCON_{perH})与进行特征模型(C_UCON_{onH})。由定义 3，4 可知，在 C_UCON 中义务和条件需要通过特征判断结果来确定，因此从访问控制顺序上来说特征判断应先于义务执行判断与条件判断。

3.2.1　预先特征模型(C_UCON_{perH})

预先特征模型需要对主体行为进行预先判断，根据判断的结果来决定是否允许主体访问客体或者是否需要承担额外的义务和满足额外的条件才能访问客体。与条件模型[4]相似，特征模型没有属性更新过程。访问前进行特征检查的模型为 C_UCON_{perH0}，其定义如下：

定义 6　C_UCON_{perH0} 的相关组成如下：

S,O,R,UB,UC,AR 分别表示主体、客体、权限、待定义

务、待定条件、激活规则集。

$A=(s,o,r)$为访问动作，其中$(s,o,r)\in S\times O\times R$。$APL$为访问动作的属性成分集。

$perH$为预先特征断言，$perHL$为预先特征成分集，$perHL=OH$或EH，APL为当前主体访问动作的特征成分集。

$PairOfH$为特征对集，$PairOfH=\bigcup_{i=1}^{n}(perhl_i,apl_i)$，其中$i\in N,n=|APL|$为$APL$特征成分数，$perhl_i\in perHL$，$ah_i\in AH$，$(perhl_i,apl_i)\in perHL\times APL$为特征对，两者均描述同一个属性。该函数功能是实现当前访问请求A的特征成分集与预先特征成分集之间同一属性的配对。

$ActUB$:$(PairOfH,AR,UB)\rightarrow UB'$，其中$UB'\in 2^{UB}$为激活的待定义务集，该函数的功能是根据$PairOfH$和相应$AR$来激活$UB$中相应的待定义务。

$ActUC$:$(PairOfH,AR,UC)\rightarrow UC'$，其中$UC'\in 2^{UC}$为激活的待定义务集，该函数的功能是根据$PairOfH$和相应$AR$来激活$UC$中相应的待定条件。

当$perB\wedge perC=true$时，更新预先特征集合$perUpdate(perHL)$。其中$perB$和$perC$分别为预先访问证书模型[10]和预先访问条件模型[10]。

在C_UCON$_{perH0}$模型中，特征的更新是必须建立在访问成功的基础上的，因此特征反映的是历史上所有成功执行的访问特征。这样做的目的在于防止特征偏向于非法操作。

3.2.2 进行特征模型(C_UCON$_{onH0}$)

进行特征判断模型需要判断访问过程中表现出来的访问特征是否符合某种特征，来决定是否终止访问，或者让主体承担额外义务和满足额外条件来维持访问的继续。进行特征模型定义如下：

定义 7 C_UCON$_{onH0}$的相关组成如下：

S,O,R,UB,UC,AR分别表示主体、客体、权限、待定义务、待定条件、激活规则集。

$A=(s,o,r)$为访问动作，其中$(s,o,r)\in S\times O\times R$。$APL$为访问动作的属性成分集。

onH为进行特征断言，$onHL$为进行特征成分集，$onHL=OC$或EC，APL为当前主体访问动作的特征成分集。

$PairOfH$为特征对集，$PairOfH=\bigcup_{i=1}^{n}(perhl_i,apl_i)$，其中$i\in N,n=|APL|$为$APL$特征成分数，$onhl_i\in perHL$，$ah_i\in AH$，$(onhl_i,apl_i)\in onHL\times APL$为特征对，两者均描述同一个属性。该函数功能是实现当前访问请求A的特征成分集与进行特征成分集之间同一属性的配对。

$ActUB$:$(PairOfH,AR,UB)\rightarrow UB'$，其中$UB'\in 2^{UB}$为已激活的待定义务集，该函数的功能是根据$PairOfH$和相应$AR$来激活$UB$中相应的待定义务。

$ActUC$:$(PairOfH,AR,UC)\rightarrow UC'$，其中$UC'\in 2^{UC}$为已激活的待定义务集，该函数的功能是根据$PairOfH$和相应$AR$来激活$UC$中相应的待定条件。

当$\neg onB\vee\neg onC=true$时，更新预先特征集合$onUpdate(onHL)$。其中$onB$和$onC$分别为进行访问证书模型[10]和进行访问条件模型[10]。

C_UCON$_{perH0}$与C_UCON$_{onH0}$模型唯一不同的是特征更新的时间不同：C_UCON$_{perH0}$中特征更新发生于条件和义务都满足时，而C_UCON$_{onH0}$中则发生于义务和条件不再满足时。

4 应用实例分析

由于C_UCON$_{perH0}$与C_UCON$_{onH0}$模型唯一不同的是特征更新的时间不同，因此下面我们通过实例1来简要说明C_UCON$_{perH0}$是如何实现的。

实例 1 以一个网上银行的转账业务为例来说明预先特征模型是如何实现的。假设用户已有100次网上银行访问经历，特征来源于这100次访问。

S:用户$userA$；

O:账户金额SUM；

R:{查询，支付，转账}；

AB:{阅读并同意网上银行服务协议}；

UB:{回答提示问题，提供个人身份证信息，从认证邮箱获取并输入二次验证码}；

AC:{IE浏览器版本高于6.0}；

UC:{系统防火墙处于正常防护状态，系统日志记录工作正常}；

$perHL$:{历史访问IP特征:{(北京，6次)，(武汉，17次)，(成都，77次)}。

历史访问时间特征:{(0点－5点，0次)，(6点－11点，4次)，(12点－17点，15次)，(18点－23点，77次)}。

历史访问类型特征:{(查询，81次)，(支付，19次)，(转账，0次)}。

历史支付金额特征:{平均支付金额，580元}。

历史转账金额特征:{平均转账金额，0元}。

}；

$ActUB()$函数激活规则，如表2所列。

表2 待定义务激活规则

规则	描述	回答提示问题	输入身份证信息	认证邮箱获取二次验证码
规则1	当前访问IP归属地出现频率百分比	(20%，30%]	(10%，20%]	(0，10%]
规则2	当前访问时间段出现频率百分比	(20%，30%]	(10%，20%]	(0，10%]
规则3	当前访问类型出现频率百分比	(20%，30%]	(10%，20%]	(0，10%]
规则4	平均支付额度与当前支付额度差	[50%，70%)	(70%，90%]	(90%，+∞)
规则5	平均转账额度与当前转账额度差	[50%，70%)	(70%，90%]	(90%，+∞)

$ActUC()$函数激活规则，如表3所列。

表3 待定条件激活规则

规则	描述	防火墙处于正常防护状态	系统日志记录工作正常
规则6	当前访问IP归属地出现频率百分比	≤30%	≤10%
规则7	当前访问时间段出现频率百分比	≤30%	≤10%
规则8	当前访问类型出现频率百分比	≤30%	≤10%
规则9	平均支付额度与当前支付额度差	≥50%	≥90%
规则10	平均转账额度与当前转账额度差	≥50%	≥90%

以上为基础要术。以下为C_UCON$_{perH0}$访问判断过程：

若当前访问操作为($userA$，SUM，支付)；

且APL={当前访问IP:当前访问IP属于成都市；当前访问时间:当前访问时间为16:30；

当前访问类型:当前访问类型为支付;

当前支付金额:当前的支付金额为 10000 元;

}

因此:

PairOfH={{历史访问 IP 特征,当前访问 IP},{历史访问时间特征,当前访问时间},{历史访问类型特征,当前访问类型},{历史支付金额特征,当前支付金额}};

1)根据规则 1:*ActUB*({历史访问 IP 特征,当前访问 IP})=NULL;

2)根据规则 2:*ActUB*({历史访问时间特征,当前访问时间})={"提供个人身份证信息"};

3)根据规则 3:*ActUB*({历史访问类型特征,当前访问类型})=NULL;

4)根据规则 4:*ActUB*({历史支付金额特征,当前支付金额})={"从认证邮箱获取并输入二次验证码"};

5)根据规则 6:*ActUC*({历史访问 IP 特征,当前访问 IP})=NULL;

6)根据规则 7:*ActUC*({历史访问时间特征,当前访问时间})={"系统防火墙处于正常防护状态"};

7)根据规则 8:*ActUC*({历史访问类型特征,当前访问类型})=NULL;

8)根据规则 9:*ActUC*({历史支付金额特征,当前支付金额})={"系统防火墙处于正常防护状态","系统日志记录工作正常"}。

所以:

UB'={"提供个人身份证信息","从认证邮箱获取并输入二次验证码"};

UC'={"系统防火墙处于正常防护状态","系统日志记录工作正常"};

最后得到用户 *userA* 必须履行的义务为 $AB \cup UB'$={阅读并同意网上银行服务协议,"提供个人身份证信息","从认证邮箱获取并输入二次验证码"},必须满足的条件为 $AC \cup UC'$={"系统防火墙处于正常防护状态","系统日志记录工作正常"}。

若 $perB(AB \cup UB') \wedge perC(AC \cup UC') = true$,那么更新特征 *perUpdate*(*perHL*)。更新后的 *perHL* 为{历史访问 IP 特征:{(北京,6 次),(武汉,17 次),(成都,78 次)}。

历史访问时间特征:{(0 点－5 点,0 次),(6 点－11 点,4 次),(12 点－17 点,16 次),(18 点－23 点,77 次)}。

历史访问类型特征:{(查询,81 次),(支付,20 次),(转账,0 次)}。

历史支付金额特征:{平均支付金额,680 元}。

历史转账金额特征:{平均转账金额,0 元}。

};

结束语 本文提出了一种具有权限使用特征判断能力的使用控制模型,它在传统的使用控制模型基础上增加了一层访问控制预处理,即根据主体对客体的访问特征以及相应规则决定活动主体是否需要承担额外的义务或者满足额外的条件来支持或者维持主体对客体的访问。通过可伸缩的义务和条件实现对具有不同使用特征的主体的动态访问控制,其形式化表示如下:

If 主体当前活动不符合某种特征

Then 根据激活规则激活待定义务和条件

If 符合授权策略 && 完成(既定义务 + 激活的额外义务)&& 符合(既定条件+激活的额外条件)

Then 允许主体获取或者使用权限

通过这一改进使得 UCON 在访问控制判断上具有更大的灵活性,同时使得判断具有一定的主观性,访问控制的范畴也延伸到了控制现实用户行为。

参 考 文 献

[1] Richardson R. 2008 CSI Computer Crime and Security Survey [EB/OL]. Computer Security Institute. http://www.gocsi.com/forms/csi_survey.jhtml,2008

[2] Lampson B W. Protection[C]//5th Princeton Symposium on Information Science and Systems. 1971:437-443

[3] Graham G S, Denning P J. Protection-principles and practice[C]// Proc. Spring Jt. Computer Conference, volume 40. Montvale, N. J: AFIPS Press, 1972:417-429

[4] Harrison M A, Ruzzo W L, Ullman J D. Protection in operating systems[J]. Communications of the ACM (CACM), 1976, 19(8):461-471

[5] Bertino E, Bettini C, Ferrari E, et al. A temporal access control mechanism for database systems[J]. IEEE Transactions on Knowledge and Data Engineering, 1996, 8(1):67-80

[6] Bertino E, Bettini C, Ferrari E, et al. An access control model supporting periodicity constrains and temporal reasoning[J]. ACM Transaction on Database Systems, 1998, 23(3):213-285

[7] Bell D E, La Padula L J. Bell-LaPadula model for secure computer systems[R]. 1976

[8] Biba K J. Integrity considerations for secure computer systems [R]. TR-3153. Bedford, MA: The Mitre Corporation, April 1977

[9] Lin T. Bell and LaPadula Axioms: A "new" paradigm for an "old" model[C]//Proceedings of the 1992～1993 ACM SIGSAC New Security Paradigms Workshop. Little Compton, 1993:82-93

[10] Smalley S, Fraser T. A Security Policy Configuration for the Security-enhanced Linux[R]. NAI Labs, February 2001

[11] Smalley S, Vance C, Salamon W. Implementing SELinux as a Linux Security Module[R]. # 01-043. NAI Labs, December 2001

[12] Ferraiolo D, Kuhn D R. Role-based access control[C]//Proc. of the 15th National Computer Security Conf. http://csrc.nist.gov/rbac/ferraiolo-kuhn-92.pdf, 1992:554-563

[13] Ferraiolo D F, Sandhu R, Gavrila S. Proposed NIST standard for role-based access control[J]. ACM Trans. on Information and Systems Security(TISSEC), 2001, 4(3):224-274

[14] Sejong O-H, Seog P. Task-role-based Access Control Model [J]. Information System, 2003, 28:533-56

[15] Bertino E, Bonatti P, Ferrari E. TRBAC: A Temporal Role-Based Access Control Model[C]//Proceedings of the 5th ACM-Workshop on Role-Based Access Control. Berlin, Germany, 2000:21-30

[16] Park J, Sandhu R. Towards Usage Control Models: Beyond Traditional Access Control [C]//Proceedings of the 7th ACM Symposium on Access Control Models and Technologies. 2002

[17] Park J. The UCONABC Usage Control Model [J]. ACM Trans. on Information and System Security, 2004, 7(1):1-47

(下转第 96 页)

钥也是不同的，每个参与者需要经历两轮交互，发送两个消息，最多执行 6 个模指数运算和 $O(n^4)$ 个乘法运算，n 为簇头数。

3 协议分析

3.1 安全性

在被动攻击上，该协议建立在离散对数难解问题基础上，能够有效抵御被动攻击。从簇内密钥的安全性看，被动攻击者在获取 $p,g,g^{x_{ij}}$ 时，要想获得簇内共享密钥 $g^{\prod_{j=1}^{m}x_{ij}+\prod_{j'=1}^{m}x_{ij'}}$，就需要得到 $x_{i1},x_{i2},\cdots,x_{ij-1},x_{ij+1},\cdots,x_{im},k_{i1},k_{i2},\cdots,k_{ij-1},k_{ij+1},\cdots,k_{im}$。由于这些指数是保密的，对任意指数的求解，都意味着求解离散对数问题；从簇间密钥的安全性看，被动攻击者在获取 $p,g,g^{\prod_{j=1}^{m}x_{ij}+\prod_{j'=1}^{m}x_{ij'}}$ 时，要想获取簇间共享密钥 $g^{\sum_{i=1}^{k}((\prod_{j=1}^{m}x_{ij}+\prod_{j'=1}^{m}k_{ij'})(\prod_{h=1}^{m'}x_{i+1h}+\prod_{h'=1}^{m'}k_{ih'})+\sum_{i=1}^{k}(x_ix_{i+1})}$，就需要得到指数 $x_{11}x_{12}\cdots x_{1j}\cdots x_{1n},x_{21}x_{22}\cdots x_{2j}\cdots x_{2n},\cdots,x_{i1}x_{i2}\cdots x_{ij}\cdots x_{in},x_{n1}x_{n2}\cdots x_{nj}\cdots x_{m}$，和 $k_{11}k_{12}\cdots k_{1j}\cdots k_{1n},k_{21}k_{22}\cdots k_{2j}\cdots k_{2n},\cdots,k_{i1}k_{i2}\cdots k_{ij}\cdots k_{in},k_{n1}k_{n2}\cdots k_{nj}\cdots k_{m}$。由于这些指数是保密的，对任意指数的求解，也意味着求解离散对数问题，因此可以说，该协议的簇间密钥和簇内密钥的安全性都依赖于离散对数问题的困难性。密钥交换分为两个阶段，分别运行在不同规模的网络中，首先在局部的簇内，然后在簇头间，减少了被干扰的机会，当簇内部分节点受到攻击，簇头阻断被攻击节点使其不影响整体网络的密钥管理。在主动攻击上，簇内主动攻击者 A 想假冒节点 $node_i$，可以伪造 pub_i 的值为 pub_E，从而得到一个伪造的值 y_A，但是他无法计算得到 y_A 对应的秘密指数值 x_A，而不知道这个值，他就无法计算共享密钥。

3.2 效率

密钥交换首先获取自认证信息；然后在簇内协商簇内共享密钥，具有局部性，簇间使用基于自认证的 Diffie-hellman 密钥交换，根据频谱切换次数利用旅行商模型寻找最优路径来提高密钥交换效率，其效率为 $O(m)$，m 为簇内节点数；最后通过簇头协商网络共享密钥，根据频谱切换次数建立最优组播树来提高组播路径效率，其过程不需要广播，不会产生广播风暴而增加网络负载，其效率为 O(2)。其总体效率比 Diffie-hellman($O(n)$，n 网络节点数)有较大提高。密钥交换的成功率高，冲突较少。

3.3 可行性

该密钥交换协议在第一阶段可以应用多种分簇协议，不需要特定的分簇协议支持；在第二阶段，通过簇节点获取簇内的局部拓扑图，指定交换次序，簇内节点较少，不会影响效率；在第三阶段，簇间的密钥交换可以运行于现有 Ad hoc 组播路由协议之上，不需要重新设计新的协议。

结束语 本文分析了 Ad hoc 认知无线电网络中密钥交换出现的问题，当网络规模较大时，由于信道切换延迟和动态频谱选择，使得单一的密钥交换协议都不能保障 Ad hoc 认知无线电网络快速协商共享密钥。因此在分簇的基础上，结合多方密钥交换协议的优点，设计了适合 Ad hoc 认知无线电网络的密钥交换协议，利用自认证在不降低效率的同时防止了主动攻击，通过旅行商问题解决了信道切换延迟的最优路径选择问题，提高了簇内密钥交换的效率，避免了密钥交换协议运行所带来的广播风暴，减小了网络的负载，簇间通过频段范围改善了组播路由树。从安全性、效率、可行性 3 个方面分析该协议的性能，证明了该协议适合 Ad hoc 认知无线电网络。在下一步的工作中，通过仿真模拟实验进一步验证其可靠性和可行性。

参 考 文 献

[1] Mitola J, Maguire G. Cognitive radio: making software radios more personal[J]. IEEE Personal Commun, 1999, 6(4): 13-18

[2] Akyildiz I F, Lee W, Vuran M C, et al. NeXt generation /dynamic spectrum access/cognitive radio wireless networks: a survey[J]. Computer Networks J, 2006, 50(13): 2127-2159

[3] Cormiob C, Chowdhurya K R. A survey on MAC protocols for cognitive radio network[J]. Ad Hoc Networks. Elsevier B. V, 2009, 7(7): 1315-1329

[4] Zhao Q, Tong L, Swami A, et al. Decentralized cognitive MAC for opportunistic spectrum access in ad hoc networks: A POMPD framework[J]. IEEE Journal on Selected Areas in Communications(JSAC), 2007, 25(11): 589-600

[5] Su H, Zhang X. Opportunistic MAC protocols for cognitive radio based wireless networks[A]// Proceedings of the 41st IEEE CISS Conference, 2007[C]. Baltimore, MD: IEEE Information Sciences and Systems, 2007: 363-368

[6] Brodersen R W, Wolisz A, Cabric D, et al. Corvus: a cognitive radio approach for usage of virtual unlicensed spectrum[R]. Berkeley: Wireless Research Center (BWRC) White paper, 2004

[7] Aad I, Hubaux J-P, Knightly E W. Denial of service resilience in ad hoc networks[A]// Proceedings of the 10th Annual International Conference on Mobile Computing and Networking (MobiCom'04), 2004[C]. Philadelphia, PA, USA: ACM New York, NY, USA, 2004: 202-215

[8] Mathur C N, Subbalakshmi K P. Security Issues in Cognitive Radio Networks[C]// Kwang-Cheng Chen, Ramjee Prasad. Cognitive Networks. Oxford: Wiley, 2007: 272-290

[9] Joux A. An One Round Protocol for Tripartite Diffie-Hellman [A]// Algorithmic Number Theory-proceedings of ANTS, 2000 [C]. Heidelberg: Springer-Verlag, 2000: 385-394

[10] Menzes A, Qu M, Vanstone S. Some New Key Agreement Protocols Providing Mutual Implicit Authentication[A]// Selected Area in Cryptography-proceedings of SAC, 1995[C]. Nashville, TN, 1995: 22-32

[11] Bresson E, Chevassut O, Pointcheval D. Provably authenticated group Diffie-Hellman key exchange-the dynamic case[A]// Advances in Crytology-Proceedings of AsiaCrypt, 2001[C]. Heidelberg: Springer-Verlag, 2001: 290-309

[12] Burmester M, Desmedt Y. A secure and efficient conference key distribution system [A] // Advances in Cryptology-EUROCRYPT'94, 1994[C]. Heidelberg: Springer-Verlag, 1995: 275-286

[13] Girault M. Self-certified public keys [C]// Advances in cryptology: Proc. Eurocrypt'91, LNCS 434. Springer, 1991: 490-497

(上接第 90 页)

[18] Pretschner A, Hilty M, Casati F, et al. Usage control in service-oriented architecture[C]// Proc. of the 4th Intl. Conf. on Trust, Privacy & Security in Digital Business. 2007

[19] Chen L, Zhang H G, Zhang L G, et al. A Peer-to-Peer Resource Sharing Scheme Using Trusted Computing Technology[J]. 2008, 13(5): 523-527

[20] 张宏，贺也平，石志国. 基于周期时间限制的自主访问控制委托模型[J]. 计算机学报，2006，29(8)：1427-1437

[21] 李军，孙玉方. 计算级安全和安全模型[J]. 计算机研究与发展，1996，33(4)：312-320

[22] 黄建，卿斯汉，温红子. 带时间特性的角色访问控制[J]. 软件学报，2003，14(11)：1944-1954

[23] 徐震，李斓，冯登国. 基于角色的受限委托模型[J]. 软件学报，2005，16(5)：970-978

[24] 洪帆，等. 多域安全互操作的可管理使用控制模型研究[J]. 计算机科学，2006，33(3)：283-286