一种跨域网络资源的安全互操作模型

唐成华[1,2] 张 鑫[1] 王 璐[3] 王 宇[2] 强保华[1,3]
(桂林电子科技大学广西信息科学实验中心 桂林 541004)[1]
(迪肯大学信息技术系 墨尔本 VIC3125)[2]
(桂林电子科技大学广西可信软件重点实验室 桂林 541004)[3]

摘 要 网络资源需要在安全策略控制下共享与互操作。针对多异构安全域域间资源互操作的安全问题,提出了一种基于RBAC安全策略的跨域网络资源的安全互操作模型。首先引入域间角色的概念,并定义跨域资源共享访问的要求;其次在跨域操作准则的基础上,提出异构域间资源安全互操作模型和访问算法;最后以实例场境对模型和算法进行了应用分析。结果表明,该方法针对性强,权限控制有效,为实现多域资源共享和互操作的安全保障提供了一种可行的途径。

关键词 异构,跨域,安全域,安全互操作,网络安全
中图法分类号 TP301 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.6.029

Security Interoperation Model of Cross-domain Network Resources

TANG Cheng-hua[1,2] ZHANG Xin[1] WANG Lu[3] WANG Yu[2] QIANG Bao-hua[1,3]
(Guangxi Experiment Center of Information Science, Guilin University of Electronic Technology, Guilin 541004, China)[1]
(School of Information Technology, Deakin University, Melbourne VIC3125, Australia)[2]
(Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin 541004, China)[3]

Abstract Network resources are in need of sharing and interoperability under the control of security policy. Aiming at the interoperability security problem of the resources among the heterogeneous security domains, a security interoperation model of accessing to cross-domain network resources based on RBAC security policy was proposed. Firstly, the concept of inter-domain role was introduced, and the requirement of accessing to cross-domain resources sharing was defined. Secondly, based on the cross-domain operation criteria, the security interoperation model and access algorithm of heterogeneous inter domain resources were put forward. Finally, The model and algorithm were analyzed through the application environment of a real project case. Results show that this method has the characteristics of high pertinence and effective access control, and provides a feasible way for the security implementation of resources sharing and interoperation.

Keywords Heterogeneous, Cross-domain, Security domain, Security interoperation, Network security

网络安全已经成为国家安全和人们日常生活安全的重要组成部分。随着越来越多的小型局域网分布式系统接入到Internet中,非法访问或资源被窃取等诸多网络安全问题由此产生。为了方便管理,很多系统管理员将大型的网络环境划分为多个安全域。安全域是同一网络环境内具有相同安全保护需求、保护策略、相互信任的网络元素的集合。不同的网络环境所划分出来的安全域有着很大的差异性,体现为网络实体结构、网络设备、安全策略模型、数据模式和约束上的差异,称之为网络的异构性[1]。尽管如此,不同的安全域仍遵守各自的安全策略,这些安全策略反映了与系统安全相关的需求,是指在相应的安全域中对人和资源进行安全控制的规则集合,是一种贴近人类思维的高层指导网络安全行为的方法[2]。

由于网络并非各自独立,各个安全域之间需要进行跨域的相互操作来实现协同工作。而跨越具有不同安全策略的异构的安全域进行操作,往往暴露出匿名访问、权限隐蔽提升等问题。大量研究表明,未授权的访问请求,特别是来自系统内部人员的非法访问请求,已成为跨安全域操作的一个主要威

到稿日期:2015-05-12 返修日期:2015-08-11 本文受国家自然科学基金(61462020,61163057,61363006),广西自然科学基金(2014GXNSFAA118375),广西信息科学实验中心基金(20130329),广西可信软件重点实验室基金,广西高等学校高水平创新团队及卓越学者计划资助。
唐成华(1974-),男,博士后,副教授,硕士生导师,CCF会员,主要研究方向为网络信息安全、智能信息处理,E-mail:tch@guet.edu.cn;张 鑫(1990-),男,硕士生,主要研究方向为网络信息安全;王 璐(1991-),女,硕士生,主要研究方向为网络信息安全;王 宇(1983-),男,博士,主要研究方向为网络与移动计算;强保华(1972-),男,博士后,教授,主要研究方向为智能信息处理。

胁[3]。因此，如何保证多域异构网络之间互操作的安全，是一个亟待解决的问题。

研究人员提出了多种异构网络系统之间的互操作模型，如通过访问的映射来完成多级安全数据库之间的互操作[4]，采用自组协同的安全互操作模式来实现协同工作流系统[5]，利用通用数据交互模型描述交换信息来解决分布式体系结构互联时的互操作问题[6]等。通常，基于信任度或可信等级的访问控制方式是实现跨域安全互操作的主要途径，典型地，如在基于 P2P 协作或可靠多会话中的自动信任协商[7]。文献[8]引入自治域信任度描述，以及用户行为评价和经验偏差反馈的方法实现组织间安全互操作。文献[9]针对域间互操作模型中的用户平台问题，引入用户、平台和域的可信等级等概念，制定了域间安全互操作方法，其用户与平台存在于自身所在安全域内。在云计算平台中，由于诸多不同的系统区域安全机制，基于系统中的主体类型来研究互操作映射的策略是一个重要的研究方向。考虑用户的身份以及虚拟组织层次结构的公共特征，文献[10]提出了一种通用的安全互操作流程，并将其应用于网格计算中。文献[11]针对同一角色对不同安全域的作用程度和域与域间信任级别不同的问题，引入角色映射阈值属性和安全域阈值属性等概念，实现了不同组织域间细粒度的访问控制。文献[12]提出一种以基于角色访问控制(RBAC)为基础的多域动态访问授权模型，以权限最小化的角色集挖掘算法实现了跨多企业环境下服务组合的动态访问控制机制，但其定义的是单域 RBAC 策略，跨域角色映射是基于域间协商和角色继承的过程，并不存在第三方的角色协调者。

实际上，对于单纯的域内角色，在不同安全域中的安全策略约束条件可能是不一样的，映射过程缺乏环境的条件因素，因此角色映射应针对具体的主体和可操作的资源。本文在确保原有安全域安全策略不变的前提下，以 RBAC 策略为基础，提出了一个针对异构安全域之间互操作问题的模型；引入域间角色的概念，并提出一种根据安全域中资源的重要程度以及域内操作来完成域间角色映射及权限分配的算法。该方法针对性强、简单有效且实用，为实现多域之间的资源共享和安全互操作提供了有益的探索。

1 基本概念

定义 1(主体，Subject) 能发出动作或执行动作，它可以是用户(User)，也可以是进程(Process)，通常与角色(Role)相关联。主体 S 描述如下：

用户集合：$U=\{user_1, user_2, \cdots, user_\alpha\}$；

进程集合：$P=\{pro_1, pro_2, \cdots, pro_\beta\}$；

角色集合：$R=\{role_1, role_2, \cdots, role_\gamma\}$；

主体：$S=(U \cup P)|R$。

定义 2(资源，Resource) 是网络系统中所有可被访问客体的集合。资源客体可以是文件、可执行代码、应用服务或 IP 地址等。资源由资源客体(Object)、资源类型(Type)和资源等级(Grade)定义。由系统管理员对各资源在所处安全域中的重要程度划分等级。资源 Re 描述如下：

资源客体：$O=\{object_1, object_2, \cdots, object_\delta\}$；

资源类型：$T=\{type_1, type_2, \cdots, type_\epsilon\}$；

资源等级：$G=\{grade_1, grade_2, \cdots, grade_\theta\}$；

资源：$Re \subseteq O \times T \times G$。

定义 3(动作，Action) 是针对资源进行的全部可执行操作的集合。可执行操作是对一个资源的最小的、不可分割的具体行为。动作 A 描述如下：

$A=\{action_1, action_2, \cdots, action_\omega\}$

定义 4 (安全域，SecurityDomain) 是在安全策略(SecurityPolicy)控制下，由相关的主体、资源和动作等所构成的一个具有实体边界或逻辑边界的区域，并由系统管理员来制定和管理其中的安全策略。不同安全域可以采用不同的安全策略模型、数据结构，以及相关约束等。在安全策略 P 下的安全域 D 描述如下：

$D=(S \cup Re \cup A)|P$

定义 5(操作权限，OperatingPermission) 是在一定的作用范围内允许主体对资源执行的动作集合。操作权限的作用范围可以是一个安全域内，也可以是多个安全域间。操作权限 OP 描述如下：

$OP \subseteq A|(S \times Re)$

定义 6(域间角色，RoleinDomain) 是在多个安全域之间进行互操作的主体表示单位的集合。每个域中的用户、进程等主体，可以生成唯一的域间角色，并符合相关安全策略的约束。域间角色定义了主体可以操作的所有资源类型和相对应的等级。域间角色 RD 描述如下：

$RD \subseteq R|(S \times (T \times G))|SecurityPolicy$

定义 7(跨域资源的共享访问) 是指主体对其他安全域中的资源进行操作时，具有与本身所在安全域中操作相同类型资源的相等权限等级，可描述为：

$\forall S_1 \in (S \cap D_1)$，

if{

$\forall t \in T.\ \exists g \in G.\ o, o' \in O$，

$\exists r_e=(o,t,g) \in (R_e \cap D_1)$，

$action_1 \in A \Rightarrow op_1=(S_1, r_e, action_1)$

}

then{

$\exists r_e'=(o',t,g) \in (R_e \cap D_2)$，

$op_2=(S_1, r_e', action_1)$

}

2 异构域的资源安全互操作模型

2.1 跨域操作准则

为了实现多域之间的资源共享和安全互操作，首先给定以下操作准则。

安全准则(SecurityCriterion)：确保在跨域操作中，信息不会泄露或被更改。

合法准则(CorrectCriterion)：确保资源只能由被授权的角色访问和操作。

自治准则(AutonomyCriterion):确保一个在域内被允许的操作,在域间也被允许。

责任分离准则(DutySeparationCriterion):确保每个动作都可以追溯到唯一的动作发出者。

2.2 RTG-RBAC 模型

由于角色在分配和权限管理上具有很好的灵活性,因此基于 RBAC 模型,采用对网络中资源划分等级的方式建立异构安全域之间的互操作模型 RTG-RBAC(Resource Type Grade-RBAC),如图 1 所示。

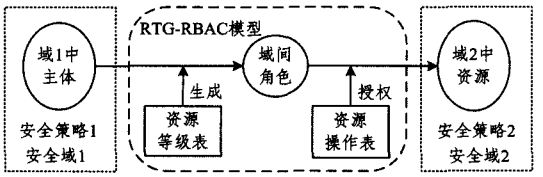

图 1 RTG-RBAC 模型

2.3 异构域间资源访问算法

在 RTG-RBAC 模型中,对每个安全域中的每个资源和主体,根据其可以访问本域中资源的类型和资源等级,生成一个可动态维护的主体资源等级表,每个域中的资源或主体发生变化时可及时地修改相应数据。表 1 记录了每个资源的等级和每个可以访问该资源的主体。

表 1 主体资源等级表

资源客体	类型	等级	可对其进行操作的主体
$object_1$	$type_1$	1 级	s_1, s_3
$object_2$	$type_2$	1 级	s_1, s_2
$object_3$	$type_2$	2 级	s_1, s_2, s_3
$object_4$	$type_2$	2 级	s_1, s_2, s_3, s_5
$object_5$	$type_3$	3 级	s_1, s_2, s_3, s_4
$object_6$	$type_4$	3 级	s_1, s_2, s_3, s_5, s_6

同时,对每个安全域中的主体和资源生成一张主体资源操作表。表 2 记录了每个主体对每种资源的操作权限。

表 2 主体资源操作表

	s_1	s_2	s_3	s_4
$object_1$	$action_1, action_2$	$action_2$	$action_2$	$action_1$
$object_2$	$action_2$	$action_2, action_3$	$action_4$	$action_2$
$object_3$	$action_3$	$action_2$	$action_2$	$action_3, action_4$
$object_4$	$action_1, action_2$	$action_1$	$action_3$	$action_4$

异构安全域间资源访问算法主要完成:为安全域 D_i 中的主体 s 对安全域中 D_j 中的资源 re 进行操作的申请进行相关的授权。算法描述如下:

算法 1 异构安全域间的资源访问

```
Input:Di 中申请访问主体 s,Dj 中资源 re
Output:主体 s 的域间角色 RDi 及操作权限 OPj
Begin{
1. struct RDi
  { Subject s;
    Type t;
    Grade g;
  };/*域间角色结构体,包括主体、类型、等级*/
2. struct Re
  { Object o;
    Type t;
    Grade g;
  };/*资源结构体,包括资源客体、类型、等级*/
3. struct OP
  { Action a;
    Subject s;
    Resource re;
  };/*操作权限结构体,包括动作、主体、资源*/
4. create resource_grade table for every domain;
5. create subject_action table for every resource;
6. s∈(S∩Di),re∈(Re∩Dj),s request to access re. o;
7. create RDi for s;
  /*查找 Di 的主体资源等级表,对主体 s 生成所有域间角色 RDi*/
  a)RDi={};
  b)search resource_grade tablei of domaini;
  c)while (s in tablei and tablei. item !=null):
      get t and g where s in table. item;
      RDi rdi;
      rdi. s=s,rdi. t=t,rdi. g=g;
      add rdi to RDi_list;
      tablei. item=tablei. nextItem;
  d)return RDi;
8. get re. t and re. g in domianj:
  /*查找 Dj 的主体资源等级表,确定 re 的类型 re. t 及其等级 re. g*/
    a)search tablej of domainj;
    b)if(re. o in tablej):
        return t and g;
      else:return null;
9. find g′ in rdi:
  /*查找域间角色 RDi_list 中类型 t 所对应等级中的最大等级 g′*/
    a)if (t in RDi):return g′=Max(g) where rdi. t=t;
    b)else:return null;
10. compare re. g and g′:
  /*比较 re. g 和 g′,若 g′≥re. g,则对角色 RDi 授权可操作 re*/
  a)if (g′≥re. g):
      authorize RDi;
      ①get opi of s in Di:
        /*获取主体 s 在 Di 中对 t 类型资源客体的操作权限 OPi*/
          a)get object in Di which type=re. t;
          b)search subject_action tablei of Di;
          c)if(object in table. item ):
              Return actions of s;
          d)else:return null;
      ②copy the op to rdi:
        /*将操作权限 OPi 迁移到域间角色 RDi。即域间角色 RDi 可以对资源 re 进行主体 s 在域 Di 中的操作动作*/
          a)OP opj;
          b)opj. s=s,opj. re=Re,opj. a=actions;
          c)return opj;
11)s in Di access the re in Dj through RDi with opj;}
End
```

算法 1 的优点在于,不需要考虑各自域内的具体安全策

略，只要保证各个安全域内的资源按等级分配，主体资源等级表和主体资源操作表一次生成，并易于维护，授权过程有效且针对性强。

3 模型应用结果及分析

3.1 应用场境

将 RTG-RBAC 模型应用到一个实际项目中：医院 C 和研究所 R 打算合作进行医疗健康方面的研究。

其中，医院 C 的网络采用 DAC 策略作为其安全策略。医院 C 参与项目人员有 Doctor1，Doctor2，Nurse，网络系统管理员为 SystemAdmin。医院 C 对外提供的共享服务资源为 Patient Records，Research Files，Medicine Records，database。医院内 Doctor1 可以对 Patient Records 进行操作：Write，Read，Copy，Delete，可以对 Research Files 进行操作：Read。Doctor2 可以对 Patient Records 进行操作：Read，Copy。按照资源的重要程度，医院 C 的网络系统管理员对其资源划分的等级为：Medicine Records 是 1 级资源；Patient Records，Research Files 是 2 级资源；database 是 3 级资源。

研究所 R 的网络采用 RBAC 作为其安全策略。参与项目人员有 Tom，Mike，Frank，Jason。其中，Tom 在研究中的角色为研究员 Researcher，Mike 为研究助理 Assistant，Frank 为网络系统管理员 SysAdmin，Jason 为学生 Student。研究所对外提供的共享资源有一台 Web 服务器（用于进行数据分析）、一个 App 应用、病人数据 patient data、数据分析 data Analysis 服务。研究所中 Researcher 可以对 data Analysis 服务进行操作：Execute，可以对 patient data 进行操作：Read，Write。SysAdmin 可以对 Web 服务器进行操作：Open，Shutdown。按照资源的重要程度，研究所 R 的网络系统管理员对其资源划分等级为：App 应用是 1 级资源；Web 服务器与 data Analysis 服务是 2 级资源；patient data 是 3 级资源。

3.2 结果及分析

Tom 现在想对医院的 Patient Records 进行写更新。应用 RTG-RBAC 模型，数据集表示如下：

Dc：医院网络域

Dr：研究所网络域

Dc = {Doctor1, Doctor2, Nurse, SystemAdmin, Patient Records, Research Files, Medicine Records, database, Write, Read, Copy, Delete}

Dr = {Tom, Mike, Frank, Jason, Researcher, Assistant, Student, Web Serivce, App, data Analysis Serivce, Read, Write, Execute, Open, Shutdown}

S = {Doctor1, Doctor2, Nurse, Researcher, Assistant, SysAdmin, Student}

A = {Write, Read, Copy, Delete, Execute, Open, Shutdown}

Re = {(Patient Records, Research, 2), (Research Files, Research, 2), (Medicine Records, hospital, 1), (database, system, 3), (Web Service, public, 2), (App, hospital, 1), (data Analysis Service, Research, 2), (patient data, Research, 3)}

OP = {(Doctor1, (Patient Records, Research, 2), Write), (Doctor1, (Patient Records, Research, 2), Read), (Doctor1, (Patient Records, Research, 2), Copy), (Doctor1, (Patient Records, Research, 2), Delete), (Doctor1, (Research Files, Research, 2), Read), (Doctor2, (Patient Records, Research, 2), Read), (Doctor2, (Patient Records, Research, 2), Copy), (Researcher, (patient data, Research, 3), Write), (Researcher, (patient data, Research, 3), Read), (Researcher, (data Analysis, Research, 2), Execute), (SysAdmin, (Web Service, public, 2), Open), (SysAdmin, (Web Service, public, 2), Shutdown)}

采用 RTG-RBAC 模型实现 Tom 对资源 Patient Records 的操作过程如下：

(1)Tom 所在的研究所网络域 Dr 采用 RBAC 作为安全策略，Tom 在 Dc 中的角色身份为 Researcher，即操作主体 s 为 Researcher。

(2)根据主体 s 查找 Dr 的主体资源等级表，可以得出表 3 所列内容（因篇幅限制，略去整个主体资源等级表）。

表 3 Dr 中主体资源等级表

资源客体	类型	等级	可对其进行操作的主体
data Analysis	Research	2 级	Researcher
patient data	Research	3 级	Researcher

(3)根据主体资源等级表，由 s 所生成的域间角色 RD_C = {Researcher, Research, 3 级}。

(4)根据资源 re = Patient Records 查找 Dc 的主体资源等级表，可得出表 4 所列内容。可得出 $re.t$ = Research；$re.g$ = 2。

表 4 Dc 中主体资源等级表

资源客体	类型	等级	可对其进行操作的主体
Patient Records	Research	2 级	Doctor1

(5)根据 t = Research 查找 RD_C，可得 g = 3。

(6)$g = 3 > re.g = 2$，则对域间角色 RD_C 进行授权。

(7)根据 $re.t$ = Research 查找 Dr 的资源等级表，得到 Dr 中 Research 类型的资源客体为 data Analysis 和 patient data；根据资源客体查找 Dr 的资源操作表，可得表 5 所列内容。得出主体为 Researcher 可以对 data Analysis 进行的操作有：Read，Write，Execute。

表 5 Dr 中资源操作表

	Researcher	Assistant	SysAdmin	Student
data Analysis	Execute	—	—	—
patient data	Read, Write	—	—	—

(8)角色 Researcher 在 Dr 中的操作权限为 OP_{Dr} = {(Researcher, (patient data, Research, 3), Write), (Researcher, (patient data, Research, 3), Read), (Researcher, (data Analysis, Research, 2), Execute)}。

(9)迁移 Researcher 的操作权限到域间角色 RD_c，即 $OP_{Dc} = OP_{Dr}$。

(10)域间角色 RD_C 可以对域 Dc 中的资源 Patient Records 进行 Read，Write，Execute 操作。

(11)Tom 可以对 Patient Records 进行写更新。

以上跨域应用中的主体对异域资源的操作申请与授权过程如图 2 所示。

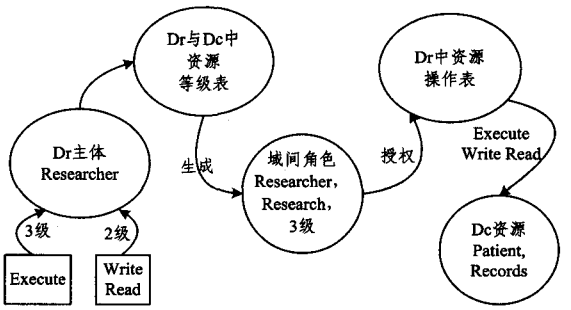

图 2　跨域操作实例

在上述过程中，*Dr* 中主体 *s* 的权限变化如下：

(1)访问开始 *s* 申请跨域访问时，*s* 根据域 *Dr* 中的安全策略，可以对域 *Dr* 中的 3 级 Research 类型资源进行 Read、Write 操作，并且可以对域 *Dr* 中的 2 级 Research 类型资源进行 Execute 操作。

(2)生成域间角色后，*s* 所映射的域间角色可以对域 *Dc* 中的 3 级及以下资源进行 Read，Write，Execute 操作。

这里似乎有一个提权的安全隐患，即主体 *s* 原本只能对 3 级资源进行 Execute 操作，而不能对其进行 Read，Write 操作；在经过域间角色映射后，可以对 3 级资源进行 Execute，Read，Write 操作。由于本模型是独立于域内安全策略的，即主体访问同一个域中的资源时，依照域内原有的安全策略进行访问，只有在进行跨域访问时，才会通过域间角色映射来进行权限划分。因此主体 *s* 对域 *Dr* 中的 3 级资源仍然只具有 Execute 操作权限，上述隐患实际并不存在。

结束语　目前安全域内的安全策略大多数是采用诸如 RBAC 模型、DAC 模型及 MAC 模型等访问控制类的安全策略。这几种模型各有优点，可以对安全域内的客体资源进行很好的保护。但是在进行域间操作时，尤其在采用不同安全策略模型的异构安全域间进行互操作时，不能很好地实现一个安全域中的主体跨域对另一个安全域中的客体进行操作。本文提出了一种基于 RBAC 模型的域间操作模型 RTG-RBAC，重点解决异构安全域之间的跨域资源互操作，而不关心各安全域内部安全策略。同时本模型以客体资源等级属性作为授权的判断依据，可以实现粒度较小的访问控制，模型遵守相关跨域操作准则。通过实际应用可以得出，该模型可以有效地解决异构安全域之间的资源共享互操作问题。

参 考 文 献

[1] Xiong Y, Zhu Y, Yu P S. Top-k Similarity Join in Heterogeneous Information Networks[J]. IEEE Transactions on Knowledge and Data Engineering, 2015, 27(6): 1710-1723

[2] David B, Vincent J, Felix K, et al. Enforceable security policies revisited[J]. ACM Transactions on Information and System Security, 2013, 16(1): 31-56

[3] Jin Li, Lu Zheng-ding, Zhao Feng. Research development on Secure Interoperation in multi-domain environment[J]. Computer Science, 2009, 36(2): 47-54(in Chinese)
金莉，卢正鼎，赵峰. 多域环境下安全互操作研究进展[J]. 计算机科学，2009，36(2)：47-54

[4] Gong L, Qian X. Computational issues in secure interoperation [J]. IEEE Transactions on Software and Engineering, 1996, 22 (1): 43-52

[5] Demchenko Y, Gommans L, Tokmakoff A, et al. Policy Based Access Control in Dynamic Grid-based Collaborative Environment[C]//Proceedings of the 2006 Int. Symposium on Collaborative Technologies and Systems. Las Vegas, USA: IEEE Computer Society, 2006: 64-73

[6] Dong Zhi-hua, Zhu Yuan-chang, Di Yan-qiang. Multi-architecture system interoperability approach using common data exchange model[J]. Journal of Beijing University of Technology, 2015, 41(1): 60-67(in Chinese)
董志华，朱元昌，邸彦强. 利用通用数据交换模型实现多体系结构系统互操作的方法[J]. 北京工业大学学报，2015，41(1)：60-67

[7] Squicciarini A C, Bertino E, Trombetta A, et al. A Flexible Approach to Multisession Trust Negotiations[J]. IEEE Transactions on Dependable and Secure Computing, 2012, 9(1): 16-29

[8] Liu Wei, Cai Jia-yong, He Ye-ping. A trustworthiness based adhoc secure interoperation method[J]. Journal of Software, 2007, 18(8): 1958-1967(in Chinese)
刘伟，蔡嘉勇，贺也平. 一种基于信任度的自组安全互操作方法[J]. 软件学报，2007，18(8)：1958-1967

[9] Xie Si-jiang, Zha Ya-xing, Chi Ya-ping. Trust level based secure interoperation model[J]. Application Research of Computer, 2012, 29(5): 1922-1925(in Chinese)
谢四江，查雅行，池亚平. 一种基于可信等级的安全互操作模型[J]. 计算机应用研究，2012，29(5)：1922-1925

[10] Zou De-qing, Zou Yong-qiang, Qiang Wei-zhong, et al. Grid security interoperation and its application[J]. Chinese Journal of Computers, 2010, 33(3): 514-525(in Chinese)
邹德清，邹永强，羌卫中，等. 网格安全互操作及其应用研究[J]. 计算机学报，2010，33(3)：514-525

[11] Ye Chun-xiao, Guo Dong-heng. Research on secure interoperation in multi-domain environment[J]. Journal of Computer Applications, 2012, 32(12): 3422-3425(in Chinese)
叶春晓，郭东恒. 多域环境下安全互操作研究[J]. 计算机应用，2012，32(12)：3422-3425

[12] Zhang Shuai, Sun Jian-ling, Xu Bin, et al. RBAC based access control model for services compositions cross multiple enterprises[J]. Journal of Zhejiang University (Engineering Science), 2012, 46(11): 2035-2043(in Chinese)
张帅，孙建伶，徐斌，等. 基于 RBAC 的跨多企业服务组合访问控制模型[J]，浙江大学学报(工学版)，2012，46(11)：2035-2043