基于动态分集的中国墙模型研究

姜 路 鹤荣育 魏彦芬
(解放军信息工程大学密码工程学院 郑州 450000)

摘 要 BN(Brewer-Nash)中国墙模型对写操作有着严格的限制,它只从客体方面考虑了冲突关系,且需要事先静态划分访问区域,不适宜动态变化的系统。定义"分集"的概念,并在此基础上提出基于分集的中国墙模型,该模型能够从主体和客体两方面出发研究系统中的冲突关系,并动态地扩充访问区域。证明了该模型是冲突安全的,并通过一个实例说明了该模型的应用。

关键词 访问控制,中国墙模型,冲突关系,动态分集
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.1.037

Chinese Wall Model Based on Dynamic Divided-set

JIANG Lu HE Rong-yu WEI Yan-fen
(The PLA Information Engineering University, Cryptogram Engineering College, Zhengzhou 450000, China)

Abstract The Chinese wall model gives much constraint on write permission, while its access regions need to predetermined and divided statically. Its conflict of interest relation was defined by the object's interest. A modified vision of Chinese wall was proposed to solve this problems. The divided-sets was defined and both the interest of subject and object were considered to analyze the system's conflict of interest relation. In this model, objects and subjects can be divided into different access regions which can be extended dynamically. At last, the security of this model was proved. The application of the model was showed by a simple example.

Keywords Access control, Chinese wall model, Conflict, Divided-set

1989年,Brewer和Nash提出了商用的中国墙模型(Chinese Wall Security Model),该模型根据现实的商业策略,防止了私密信息在有竞争关系的对手间流动,从而保证了信息的机密性。此模型也称为BN中国墙模型[1]。BN中国墙模型提出了冲突关系,并依据主体的访问历史,防止有冲突关系的两个对象之间的信息流动,从而保证了信息的机密性。

自中国墙模型提出以来,很多学者对其做了深入的研究。Lin等人[2]主要集中于对冲突关系的研究,并据此对中国墙进行了扩展;Sobel[3]通过利用迹的方法,深入研究了中国墙模型,提出了一种时间间隔和访问权利撤销的新思想。Sandhu[4]利用格的概念,并使用RBAC访问控制模型来对中国墙进行实施。何永忠等[5]提出了使用RBAC实施自主访问控制和强制访问控制。秦超等[6]把中国墙模型部署在多级安全环境中。

Foley[7]利用UNIX的简单保护机制,使用用户组的概念在UNIX中构造了中国墙模型,用户组是一个用户的集合。初始化时用户组为空,但该方法的使用性受到了系统结构的局限。夏少君等[8]基于格的属性对实体分配了敏感标记,提出了保护应用程序的中国墙模型。马俊等[9]提出了主动冲突关系的概念,将原来对信息双向流动的约束转换为对单向流动的约束,提出了一种可以实现数据主动泄漏防护的扩展中国墙模型。

文献[10]提出了一种联盟关系,基于这种客体与客体之间的联盟关系,对访问区域进行动态划分。文献[11]和文献[12]为解决虚拟机隐形流问题,在虚拟机和分布式虚拟系统中部署中国墙模型。文献[13]提出了基于安全域隔离的访问控制模型,实施了分区间信息流隔离控制机制。文献[14]在实施细粒度访问控制时,静态地将资源分成不同的域,信息只能在域中流动,如果资源加入一个域中,则不能改变。文献[15]为实现虚拟机系统的隐形流控制,静态地将资源划分成不同的隔离域,域间也是隔离的,并采用中国墙的冲突集划分通信区域。

前面提到的模型中,很多需要静态划分访问区域,但在很多系统中很难实现这一点。随着系统的运行,访问区域往往是动态变化的。当前的很多模型把研究重点都放在了对客体之间的冲突关系和访问区域划分上,这并不符合一些系统的实际。比如在云计算中,以进程为粒度的系统,一个进程可以是访问的主体,也可以是访问的客体。进程主体/客体的身份没有必要分得很清楚。所以需要系统从主体的角度考虑冲突关系的发展,考虑主体与主体之间的二元关系,以及主体与客体之间的二元关系。

根据以上需求,本文提出了一种基于动态分集的中国墙

到稿日期:2014-01-02 返修日期:2014-03-28

姜 路(1990-),男,硕士生,主要研究方向为云计算、虚拟机隔离,E-mail:849148146@qq.com;**鹤荣育**(1966-),男,教授,硕士生导师,主要研究方向为信息安全、云计算;**魏彦芬**(1988-),女,硕士生,主要研究方向为网络与信息安全。

模型，不仅研究了客体之间的冲突关系，也从主体与客体、主体与主体的关系方面研究了冲突关系，以及主体对客体的访问对冲突关系的影响；定义了“分集”的概念，动态地对系统中的资源进行划分；规定了安全读写规则，并证明了其安全性；最后用一个实例来说明本模型的实用性。

1 利益冲突关系数据模型

本模型沿用 BN 模型中的一些定义，并对其进行一定的修改，引入分集的概念，在初始化时依据其属于的分集，限定元素的分集属性。分集的属性会影响其访问权限。元素是否属于分集也会动态地发生变化，从而适应系统的灵活性。

把系统中的所有的主体和客体的集合表示为 U，U 中的元素用 $u_1,u_2,\cdots$ 表示。其中元素 u 可能是客体，也可能是主体。特别地，用 O 表示客体集，客体元素用 $o_1,o_2,\cdots$ 表示。用 S 表示主体集，主体元素用 $s_1,s_2,\cdots$ 表示。用 $T=\{0,1,2,\cdots,t,\cdots\}$ 表示时间，特别地，当 $t=0$ 时，表示初始时刻。

1.1 利益冲突关系描述

BN 模型在客体 o 的集合 O 中定义了二元关系“利益冲突关系”，用 CIR 表示。$CIR=\{(u,v)\}\subseteq O\times O$。相似地，本文定义元素间的利益冲突关系：$CIR=\{(u,v)\}\subseteq U\times U$。$(u_1,u_2)\in CIR$ 表示元素 u_1,u_2 是利益冲突关系，$(u_1,u_2)\notin CIR$ 表示元素 u_1,u_2 不是利益冲突关系。把与 u_1 利益冲突的集合记为：$CIS(u_1)=\{u_2\mid(u_1,u_2)\in CIR\}$。用 $CIS(u_1)$ 表示与 u_1 有利益冲突关系的集合，其中 $CIS(u_1)$ 中的任意元素 u_2 都与 u_1 冲突。

易知利益冲突关系有如下性质：对称性、非自反性和非传递性。下面对此作简要说明。如果元素 u_1,u_2 是利益冲突关系，即 $(u_1,u_2)\in CIR$，则 u_2,u_1 也是利益冲突，即 $(u_2,u_1)\in CIR$，所以 CIR 满足对称性。元素 u_1 与它自己本身没有利益冲突，所以 CIR 不满足自反性。如果元素 u_1,u_2 满足利益冲突关系，且元素 u_2,u_3 也满足利益冲突关系，再假设 u_1,u_3 不利益冲突，这种假设并不能推出矛盾，且是有可能成立的，所以 CIR 不满足传递性。故利益冲突关系是对称、非自反和非传递的二元关系。

1.2 分集数据模型定义

建立新的数据模型，此数据模型把主体和客体统一视为元素，系统初始化时将每个元素分配到相应的集合中。随着系统运行，元素所属集合会有所改变。

定义 1(分集) 在系统中，部分元素会结成关系较为密切的集合，称为分集。同一分集中的元素都不利益冲突。不同分集之间相互没有交集，且不同分集中的元素相互冲突。分集集合用 FC 表示。FC 中的元素用 $A,B,C\cdots$ 表示。即分集的性质可表示如下：

$\forall A\in FC,\forall u_1,u_2\in U,u_1,u_2\in A\Rightarrow(u_1,u_2)\notin CIR$

$\forall A,B\in FC,u_1\in A,u_2\in B\Rightarrow(u_1,u_2)\in CIR$

$\forall A,B\in FC\Rightarrow A\cap B=\varnothing$

由于分集是动态变化的，用 A_t 表示 t 时刻的分集 A 的状态。特别地，初始状态即 $t=0$ 时的分集 A_0 叫做初始分集。

根据系统元素是否属于分集、是否被分配，可以将元素划分成不相交的 3 个集合：(1)还未分配的元素集 US；(2)已经被分配到分集中的元素集 AS；(3)已经被分配但没有被分配到分集中的元素集 NS。用 U 表示全集，则有如下关系：

$US\cup AS\cup NS=U$

$US\cap AS=US\cap NS=AS\cap NS=\varnothing$

显然，分集 $A,B,C\cdots$ 都是 AS 的子集，即：

$A\cup B\cup C\cup\cdots=AS$

系统中所有集合如图 1 所示。

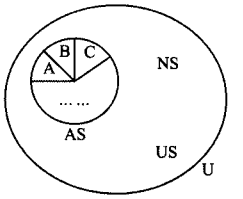

图 1 集合结构

系统运行时，元素所属集合会发生变动。系统初始化时，US 中的元素比较多。随着系统运行，US 中的元素将被分配，可能被分配到 AS 中，也可能被分配到 NS 中。

被分配到 NS 中的元素，如果被分集中的元素写操作，则会并入该分集中。而元素一旦分配，就不会再进入 US 中，进入 AS 中的元素也不会离开这个集合。所以元素流动有方向性，如图 2 所示。

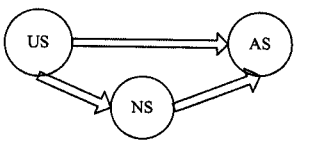

图 2 元素在集合中流动

读控制矩阵用 $R(s,o)$ 表示，写控制矩阵用 $W(s,o)$ 表示，其中矩阵中的元素的取值集合为 $\{0,1\}$。0 表示没有读/写权限，1 表示有读/写权限。在 t 时间的读控制矩阵表示为：$R_t(s,o)$。

2 基于动态分集的中国墙模型

2.1 模型的信息流

为了实现保密性，必须防止有利益冲突的集合之间的信息流。信息流通过主体对客体的读写访问直接或间接地在主体与客体之间传递。动态分集的中国墙模型通过写操作来控制访问区域的范围，从而限制信息流的传递。如果系统在某时刻 $t_1\in T$，主体 s_1 能够读客体 o_1，则存在客体 o_1 到主体 s_1 的读信息流。用 RIF 表示这种信息流。在另一个时刻 $t_2\in T$，主体 s_2 能够写客体 o_2，则存在主体 s_2 到客体 o_2 的写信息流。用 WIF 表示这种信息流。这种直接信息流的定义如下。

定义 2 对于 $o_1,o_2\in O,s_1,s_2\in S,t_1,t_2\in T$：

(1)$o_1RIFs_1\Rightarrow R_{t_1}(s_1,o_1)=1$

(2)$s_2WIFo_2\Rightarrow W_{t_2}(s_2,o_2)=1$

此定义说明如果存在直接的信息流，则在读写信息流的时刻，读写访问是允许的。

除了上述直接的信息流，系统中还会产生间接的信息流。如果系统在 $t_1\in T$ 时刻存在信息流 o_1RIFs_1，在 $t_1\leqslant t_2\in T$ 时刻存在信息流 s_1WIFo_2，那么则存在 o_1 到 o_2 间接的信息流。这种间接的信息流用 CIF 表示。同理，还存在一个主体到另一个主体，主体和客体之间的间接信息流。形式化地定义两种间接信息流 $oCIFs$、$oCIFo'$ 如下。

定义 3 对于 $s\in S,o,o'\in O,t\leqslant t'\in T$

(1)$oCIFs\Rightarrow\exists s_1,s_2,\cdots,s_k=s\in S;o_1,o_2,\cdots,o_{k-1}=o\in O;$

$\exists t \leqslant t_1 \leqslant t_2 \leqslant \cdots t_{2k-1} \leqslant t' \in T$;

$R_1(s_1, o)=1 \wedge \forall i=1,2,\cdots,k-1$:

$W_i(s_i, o_i)=1 \wedge R_{i+1}(s_{i+1}, o_i)=1$;

(2)$oCIFo' \Rightarrow \exists s_1, s_2, \cdots s_k \in S; o=o_1, o_2, \cdots, o_{k+1}=o' \in O$;

$\exists t \leqslant t_1 \leqslant t_2 \leqslant \cdots t_{2k} \leqslant t' \in T$;

$\forall i=1,2,\cdots,k: R_{2i-1}(s_i, o_i)=1 \wedge W_{2i}(s_i, o_{i+1})=1$

由以上定义可以看出，只要能限制写信息流，就可以控制间接信息流。

根据中国墙的安全要求，需要两个有利益冲突的元素之间不能存在信息流，据此我们定义模型的冲突安全性。

定义 4(定义系统冲突安全性) 系统是冲突安全的，如果 $\forall u_1 \in U, \forall u_2 \in U, \forall u_3 \in U, \forall t_1, t_2 \in T$:

$u_2 CIF_{t_1} u_1 \wedge u_3 CIF_{t_2} u_1 \Rightarrow u_2 \notin CIS(u_3)$

此定义从有利益冲突的元素不能存在信息流出发，定义了系统的冲突安全性。系统中任意两个元素，如果都与另一个元素存在信息流，那么这两个元素不能是利益冲突的。

2.2 同集关系

为了更直观地看出关系密切的一些元素的关系，我们引入同集关系，直观地，就是它们处在同一个分集中。

定义 5 在 $t \in T$ 时刻，元素 $u_1, u_2 \in U$，若 $\exists A \in FC: u_1 \in A \wedge u_2 \in A$，则称二元关系 (u_1, u_2) 是同集关系，用 TSR 表示。在 t 时刻，如果元素 u_1, u_2 是同集关系，则表示为 $u_1 TSR_t u_2$。

由定义易知，同集关系 TSR 满足自反性、对称性和传递性，所以同集关系是 $AS \times AS$ 上的等价关系。每一个等价关系都对应着一个分类，所以分集就是 AS 上的一个分类。由同集关系的定义可知，在同一分集中的元素都不利益冲突，所以拥有同集关系的元素都不利益冲突。

2.3 模型的安全规则

新的模型一定要与 BN 模型拥有相同的安全性，能阻止信息在有冲突的利益集团之间流动。

规则 1(初始分集分配规则) 在系统初始状态下，系统根据同集关系与利益冲突关系把一些元素被分配到若干分集中，规则如下：

(1)$t=0, \forall u_1, u_2 \in U, \exists A \in FC, u_1, u_2 \in A \Rightarrow u_1 \notin CIS(u_2)$。

(2)$t=0, \forall u_1 \notin AS, \forall u \in U \Rightarrow u \notin CIS(u_1)$。

(3)$t=0, \forall u_1 \in U, \forall u_2 \in U, u_1 \in CIS(u_2) \Leftrightarrow \exists A \in FC, \exists B \in FC, A \neq B, u_1 \in A, u_2 \in B$。

式(1)表示在系统初始状态下，若干不存在利益冲突的元素被分配到同一个分集中。式(2)表示没有被加入分集的元素与任何元素都没有利益冲突。式(3)表示在初始状态下，所有有利益冲突的元素都被分配到分集中，且相互利益冲突的元素被分到不同的分集中。分集的初始分配主要依据系统的需要和利益冲突关系来确定分集中的元素的分配。系统初始化时，一些元素存在着利益冲突关系，我们把这些有着相同利益的元素放在同一个分集中，有利益冲突的元素放在不同的分集中，并且把这些元素全部分尽，不同的分集之间都有利益冲突，以便通过访问控制规则来限定信息的流动，实现冲突安全。

规则 2(分集动态扩展规则) 在系统运行时，分集是动态变化的。其规则如下。

(1)$\forall t \in T, \forall u_2 \in U, \exists A \in FC, \exists u_1 \in U: u_1 \in A_t \wedge u_1 WIF_t u_2 = 1 \Rightarrow u_2 \in A_{t+1}$。

(2)$\forall t \in T, \forall u_2 \in U, \exists A \in FC, \exists u_1 \in U: u_1 \in A_t \wedge u_2 RIF_t u_1 = 1 \Rightarrow o \in NS$。

式(1)表示若分集中的元素对分集外的元素有了写操作，则被写的元素加入该分集。式(2)表示若分集中的元素对分集外的元素有了读操作，则被读元素加入 NS 中。此规则给出了元素在集合 US、NS 和 AS 之间的流动方向，也给出了分集的扩展规则。分集的扩展规则是写扩展，即被分集中的元素写过的元素就加入该分集，从而保证了分集中的信息不会流出分集，所以就能保证冲突安全。而分集中的元素对其他元素读操作则没有扩展动作，读操作是信息流入分集中，且访问控制规则保证了流入分集中的信息都是与该分集没有利益冲突的元素中的。

定理 1 一个分集中的主体在访问其他客体的过程中，不会使信息流出分集。

证明：下面对分集中的主体的访问分类讨论。

1)主体进行读操作：主体无论是读分集内的客体还是分集外的客体，都是信息流入分集，故分集中的信息不会流出分集。

2)主体进行写操作：如果主体写分集中的客体，则信息只在分集中流动，没有流出分集；如果主体写分集之外的客体，根据规则 2 的式(1)可知，这个客体将加入该分集，所以信息也没有流出分集。证毕。

文献[10]中的安全规则规定在系统初始化时系统的主体可以读任何客体。其认为冲突关系只存在于客体与客体之间，主体之间、主体与客体之间都不存在冲突关系。故能在初始状态保证冲突安全。而这种假设不符合一部分系统，比如 A、B 两个公司，则在初始状态下 A 公司的员工与 B 公司的私密信息可能存在着利益冲突关系，所以分集的概念中假设主体与客体、主体与主体之间都可能存在利益冲突关系。其访问规则如下：

规则 3(访问控制规则) 系统中的元素的读写遵循以下规则：$\forall u_1 \in U, \forall u_2 \in U, \exists A \in FC$:

$$(1)R_t(u_1, u_2)=\begin{cases}1, & \text{if } u_1 TSR_t u_2 \vee u_2 \notin AS \\ 0, & \text{其他}\end{cases}$$

$$(2)W_t(u_1, u_2)=\begin{cases}1, & \text{if } u_1 TSR_t u_2 \vee u_2 \notin AS \\ 0, & \text{其他}\end{cases}$$

从规则 3 可以看出，要么元素 u_2 与 u_1 是同集关系，要么就不是分集中的元素才能被 u_1 访问。本规则实现了对访问的控制，限制了信息的流动，保证了信息不会在有利益冲突的分集之间流动。本规则禁止元素访问另一个分集中的元素，从而阻止了这种分集间直接的信息流动。

引理 1 一个分集中的元素，只有这个分集中的主体才能访问它。

证明：由规则 3 可知，若 $R_t(u_1, u_2)=1$，则只有满足条件 $u_1 TSR_t u_2 \vee u_2 \notin AS$。若被访问元素在分集中，即 $u_2 \in AS$，那么只有满足条件 $u_1 TSR_t u_2$，即 u_1, u_2 在同一个分集中。

定理 2 分集中的客体被主体访问时，信息不会流出分集。

证明：由引理 1 可知，只有这个分集中的主体才能访问此分集中的客体，所以分集中的客体被访问时信息只在该分集

中流动，故信息不会流出分集。证毕。

3 模型的安全性及其应用

3.1 模型的安全性证明

动态分集模型应该与 BN 中国墙模型有着相同的安全性。即信息只能在某一个利益集团中流动。敏感信息不会因为主体访问而使敏感信息泄漏到冲突利益集团中。下面分析并证明其安全性。

定理 3 系统的安全规则能够控制利益冲突集合之间的信息流，使系统冲突安全。

证明：由定义 4 可知，要证明系统是冲突安全的，就要证明 $\forall u_1 \in U, \forall u_2 \in U, \forall u_3 \in U, \forall t_1, t_2 \in T: u_2 CIF_{t_1} u_1 \wedge u_3 CIF_{t_2} u_1 \Rightarrow u_2 \notin CIS(u_3)$。

我们对元素 u_1, u_2, u_3 是否属于分集做分类讨论：

(1)若 $u_2 \notin AS, u_3 \notin AS$：则由规则 1 的式(3)可知，若 $u_2 \in CIS(u_3)$，则有 $\exists A \in FC, \exists B \in FC, A \neq B, u_1 \in A, u_2 \in B$，即 $u_2 \in AS, u_3 \in AS$。然而 $u_2 \notin AS, u_3 \notin AS$，故 $u_2 \notin CIS(u_3)$。得证。

(2)若 $u_2 \in AS, u_3 \in AS$：因为 u_2 在分集中，那么根据定理 1 可知，u_2 在访问其他客体时，u_2 的信息不会流出分集；根据定理 2 可知，当 u_2 被其他主体访问时，u_2 的信息也不会流出分集。然而存在信息流 $u_2 CIF_{t_1} u_1$，所以 u_1 也位于 u_2 所在的分集中，即 $u_2 TSR u_1$。同理有 $u_3 TSR u_1$。又因为同集关系是等价关系，满足传递性，所以 $u_2 TSR u_3$，因此 $u_2 \notin CIS(u_3)$。得证。

(3)$u_2 \in AS, u_3 \notin AS$：由规则 1 的式(2)可知，在初始状态下，$u_3 \notin AS$，得出 u_3 与任何元素都不利益冲突。而随着系统运行，并没有分集的信息流入 u_3，故 u_3 的利益冲突关系没有改变，即 u_3 不与任何元素利益冲突。所以有 $u_2 \notin CIS(u_3)$。得证。

对于 $u_2 \notin AS, u_3 \in AS$ 的情况，与步骤(3)情况相同，不再赘述。综上有系统的安全规则能够使系统冲突安全。证毕。

3.2 模型应用

在云计算中，虚拟机监视器一般对信息流实施访问控制，以达到云系统安全的目的。然而由于隐形流的存在，运行在一起的虚拟机之间不能保证没有信息的流动，因此需要更强的隔离机制。用动态分集的中国墙模型来限制信息的流动，因为要限制所有的用户虚拟域之间的信息流，所以假定每一个用户虚拟机的资源都与其他的虚拟机有利益冲突。把模型在云平台上做以下部署：

全集 U：云平台中所有能供虚拟机使用的资源的合集，比如进程、内存、磁盘、外设等都是全集 U 中的元素。

AS：已经被虚拟机占用的资源，这些元素包含了虚拟机中的信息。

US：还没被虚拟机占用的资源，这些元素不包含虚拟机中的元素，也可称为清洁资源。

分集：把每一个虚拟机划定在一个分集中，即分集中的元素都包含了虚拟机自启动以来所携带的信息。

在部署中，访问的主体一般为进程，而被访问的客体可以是进程资源，也可以是一些静态的资源，如内存、代码、磁盘信息、外设信息等。在一些特定的情况下，分集中的访问主体与客体是可以转换的，文献[10]提出的联盟关系只存在于客体之间，且主体与客体是不会发生变化的，这不符合云系统信息流控制的情况。

在 VM(客户虚拟机)初始化时，每一个 VM 被分配到一个分集中，且每个分集中只有一个 VM，如图 3 所示。

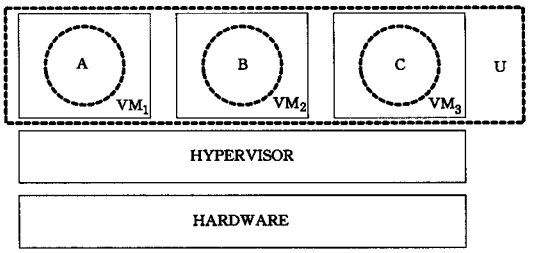

图 3 模型在云平台下的应用

在图 3 中，我们用实框表示虚拟机的系统划分，用虚框表示本模型对元素的划分。由图可见，最底层为云平台的硬件部分(Hardware)，在硬件的上层是虚拟机监视器层(Hypervisor)，虚拟机监视器负责管理顶层的虚拟机。在初始化时，每个虚拟机中的资源都会被分配到一个分集中。随着系统的运行，分集按照规则 2 进行扩充，分集中的元素都包含了该虚拟机的信息。我们假定虚拟机之间都是有利益冲突的，虚拟机使用规则 3 对访问进行控制，从而达到云平台中的虚拟机的隔离，使云平台机密性得以保证。

结束语 传统的中国墙模型过多地关注了客体相互之间的冲突关系，并需要根据客体之间的冲突关系对客体进行访问区域的静态划分。本文依据中国墙的 BN 模型，从主体出发，考虑了系统中主体间的关系，以及主体与客体之间的关系，定义了分集的概念，动态地划分了访问区域，并规定了各访问区域互相访问的规则，实现了访问控制，并证明了该模型的安全性。

作为总结，本模型与文献[10]提出的中国墙模型的变种进行了一个有益的对比。本文把所有资源都定义为元素，并在元素之间定义冲突关系、冲突安全性及模型，并没有把系统的资源局限为访问的主体与客体，文献[10]只从客体的角度划分联盟关系；本模型的主体与客体在特定的条件下可以转换，而文献[10]中的主体与客体是一成不变的，这不符合某些系统的实际；本文给出了分集动态扩展规则，而文献[10]没有明确给出；本文的访问规则操作较为简单，有着较高的效率，而文献[10]在访问规则中需要检查主体的所有联盟中的客体与要访问联盟的所有客体之间的冲突关系，实现效率较低。

文献[7]利用组的概念构造中国墙模型，并给文件(即是访问操作的客体)定义了一个标签，标签中给出了文件的拥有者、文件所属的组和文件被访问的规则，也给出了组的扩展规则。

相比之下，文献[7]是区别对待主体与客体，而本文用元素表示所有资源；文献[7]中的文件(客体)的标签给出了各个主体的访问权限，而不是根据文件的组属性确定其访问权限；文献[7]的扩展规则是通过访问扩展组中的用户，而本文通过写操作扩展分集中的元素。

本模型在分集间禁止信息的流动，从而实现强隔离。但强隔离使信息的共享变得困难，从而需要其他辅助手段进行信息的共享。在本模型中，主体和客体都是在系统初始化时存在的，对于系统能够动态产生和消除的元素，还有待进一步研究。

参 考 文 献

[1] Brewer D F C, Nash M J. The Chinese wall security policy[C]// Proceedings of the 1989 IEEE Symposium on Security and Privacy. Oakland, CA, USA, 1989. 206-214

[2] Lin T Y. Chinese wall security policy-an aggressive model[C]// Fifth Annual Computer Security Application Conference. Tucson, Arizona, USA, 1989: 282-289

[3] Sobel A E K, Alves F J. A trace-based model of the Chinese wall security policy[C]// Proceedings of the 22nd National Information Systems Security Conference. Arlington, Virginia, USA, 1999. 231-240

[4] Sandhu R. A lattice interpretation of the Chinese wall policy [C]// Proc of the 15th NIST--NCSC National Computer Security Conference. Washington, USA, 1992: 329-339

[5] 何永忠,李晓峰,冯登国. RBAC 实施中国墙模型及其变种的研究[J]. 计算机研究与发展,2007,44(4):615-622

[6] 秦超,陈钟,段云所. Chinese wall 策略及其在多级安全环境中的扩展[J]. 北京大学学报,2002,138(3):369-374

[7] Foley S N. Building Chinese walls in standard unixTM[J]. Unix Computers and Security Journal, ACM, 1997, 16(6): 551-563

[8] 夏少君,魏玲玲. 一种基于中国墙策略的应用程序保护模型研究[C]//第 27 次全国计算机安全学术交流会论文集. 2012: 212-214

[9] 马俊,王志英,任江春,等. 一种实现数据主动泄漏防护的扩展中国墙模型[J]. 软件学报,2012,23(3):677-687

[10] 程戈,金海,邹德清,等. 基于动态联盟关系的中国墙模型研究[J]. 通信学报,2009,11:93-100

[11] Sailer R, Jaeger T, Valdez E. Building a MAC-based security architecture for the Xen open source hypervisor[C]// Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC2005). Miami, FL, USA, 2005: 276-285

[12] Mccune J, Berger S, Cacerres R. Shamon: a system for distributed mandatory access control[C]// Preceedings of the 22nd Annual Computer Security Applications Conference. Miami Beach, Florida, USA, 2006: 23-32

[13] 牛文生,李亚晖,张亚棣. 基于安全域隔离的嵌入式系统的访问控制机制研究[J]. 计算机科学,2013,40(Z6):320-322,326

[14] Katsuno Y, Watanabe Y, Furuichi S. Chinese wall process confinement for practical distributed coalitions[C]// Proceedings of the 12th ACM Symposium on Access Control Models and Technologies. NY, USA, 2007: 225-234

[15] Jaeger T, Sailer R, Sreenivasan Y. Managing the risk of covert information flows in virtual machine systems[C]// Proceedings of the 12th ACM Symposium on Access Control Models and Technologies. Sophia Antipolice, France, 2007: 81-90

(上接第 136 页)

[5] Ahmad A, Hadgkiss J, Ruighaver A B. Incident response teams-Challenges in supporting the organizational security function [J]. Computers & Security, 2012, 31(5): 643-652

[6] Gonzalez J W J J, Kossakowski K P, Wiik J. Limits to Effectiveness in Computer Security Incident Response Teams[C]// Proc. of Twenty Third International Conference of the System Dynamics Society. Boston, Massachusetts, 2005

[7] Hashemi S H, Babaeizadeh M, Nowruzi M, et al. A comprehensive semi-automated incident handling workflow[C]// Proc. of IEEE Symp on Sixth International Telecommunications (IST). 2012: 1065-1070

[8] Ping L, Haifeng Y, Guoqing M. An incident response decision support system based on CBR and ontology[C]// Proc. of the 2010 Int Conf on Computer Application and System Modeling (ICCASM). IEEE, 2010, 11: 337-340

[9] Nowruzi M, Jazi H H, Dehghan M, et al. A comprehensive classification of incident handling information[C]// Proc. of IEEE Symp on Sixth International Telecommunications (IST). 2012: 1071-1075

[10] 罗杰文,施智平,何清,等. 一种 CBR 与 RBR 相结合的快速预案生成系统[J]. 计算机研究与发展,2007,44(4):660-666

[11] Aamodt A, Plaza E. Case-based reasoning: Foundational issues, methodological variations, and system approaches [J]. AI communications, 1994, 7(1): 39-59

[12] Gómez-Albarrán M, González-Calero P A, Díaz-Agudo B, et al. Modelling the CBR Life Cycle Using Description Logics[M]. Case-Based Reasoning Research and Development. Springer Berlin Heidelberg, 1999: 147-161

[13] Zeghib Y, De Beuvron F Ç, Kullmann M. Using description logics for designing the case base in a hybrid approach for diagnosis integrating model and case-based reasoning[M]. Case-Based Reasoning Research and Development. Springer Berlin Heidelberg, 2001: 561-575

[14] 方滨兴. 建设网络应急体系保障网络空间安全[J]. 通讯学报,2002,23(5):4-8

[15] Bergmann R, Kolodner J, Plaza E. Representation in case-based reasoning[J]. The Knowledge Engineering Review, 2005, 20(3): 209-213

[16] 刘欣然. 一种新型网络攻击分类体系[J]. 通信学报,2006,27(2):160-167

[17] Cunningham P. A Taxonomy of Similarity Mechanisms for Case-Based Reasoning[J]. IEEE Trans on Knowledge and Data Engineering, 2009, 21(11): 1532-1543

[18] Sánchez-Ruiz A A, Ontañón S, González-Calero P A, et al. Measuring similarity in description logics using refinement operators[M]// Case-Based Reasoning Research and Development. Springer Berlin Heidelberg, 2011: 289-303

[19] Sánchez-Ruiz A A, Ontañón S, González-Calero P A, et al. Refinement-Based Similarity Measure over DL Conjunctive Queries [M] // Case-Based Reasoning Research and Development. Springer Berlin Heidelberg, 2013: 270-284

[20] Amailef K, Lu J. Ontology-supported case-based reasoning approach for intelligent m-Government emergency response services[J]. Decision Support Systems, 2013, 55(1): 79-97

[21] Vander Laag P R J, Nienhuys-Cheng S H. Completeness and properness of refinement operators in inductive logic programming[J]. The Journal of Logic Programming, 1998, 34(3): 201-225

[22] Lehmann J, Hitzler P. Foundations of refinement operators for description logics[M]// Inductive Logic Programming. Springer Berlin Heidelberg, 2008: 161-174