软件学报 ISSN 1000-9825, CODEN RUXUEW
*Journal of Software*,2012,23(3):677−687 [doi: 10.3724/SP.J.1001.2012.03974]
©中国科学院软件研究所版权所有.
E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

# 一种实现数据主动泄漏防护的扩展中国墙模型*

马 俊+, 王志英, 任江春, 伍江江, 程 勇, 梅松竹

(国防科学技术大学 计算机学院,湖南 长沙 410073)

## Extended Chinese Wall Model for Aggressive Data Leakage Prevention

MA Jun+, WANG Zhi-Ying, REN Jiang-Chun, WU Jiang-Jiang, CHENG Yong, MEI Song-Zhu

(College of Computer, National University of Defense Technology, Changsha 410073, China)

+ Corresponding author: E-mail: majun_nudt@sohu.com

**Ma J, Wang ZY, Ren JC, Wu JJ, Cheng Y, Mei SZ. Extended Chinese wall model for aggressive data leakage prevention. *Journal of Software*, 2012,23(3):677−687.** http://www.jos.org.cn/1000-9825/3974.htm

**Abstract**: The Chinese wall model combines discretionary and mandatory aspects of access control. Hence it is widely used in commercial environments to prevent information flows from competing companies with conflicting of interests to the same consultant. However, the model gives strong constraints on both reads and writes, so it is too restrictive to be employed in a practical system. Especially for data leakage prevention (DLP), the applications not play to its advantages. This paper reconsiders the conflict of interest from the perspective of the data object and put forward the concept of aggressive conflict of interest relation. The new relation extends the constraints on two-way information flow to that of one-way flows. Based on this, the paper presents an aggressive Chinese wall model (ACWM) for initiative data leakage prevention and gives the formal description of the model as well as the related proof of the theorem. The final analysis shows that, ACWM achieves the same security goal as traditional Chinese wall models, and also provides more flexible constraints which are efficient for DLP.

**Key words**: Chinese wall policy; data leakage prevention; information flow; conflict of interest; alliance

**摘 要**: 中国墙模型具有能够同时提供自主控制和强制控制的特性,因而被广泛应用于商业领域中,以防止有竞争关系的企业之间的信息流动而导致利益冲突.但是由于对读写约束过于严格,因而应用范围有限,特别是在数据泄漏防护的应用中未能发挥其优越性.针对数据泄漏防护对信息流动的控制需求,从数据客体的角度出发,考虑中国墙模型中的利益冲突问题,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.在此基础上,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 ACWM(aggressive Chinese wall model),并给出了模型的形式化描述和相关定理的证明.分析表明,ACWM 模型可以实现传统中国墙模型的安全目标,而约束条件更加灵活,可以实现数据泄漏防护的需求.

**关键词**: 中国墙模型;数据泄漏防护;信息流;利益冲突关系;联盟关系

**中图法分类号**: TP309 **文献标识码**: A

中国墙模型是商业安全领域中的著名安全模型,最初是由 Brewer 和 Nash 在 1989 年的信息安全会议 S&P

* 基金项目: 国家自然科学基金(60903204)
收稿时间: 2010-04-30; 修改时间: 2010-08-27; 定稿时间: 2010-12-09

© 中国科学院软件研究所 http://www.jos.org.cn

上首次提出[1],又称为BN模型.其最初构想来源于证券交易中咨询顾问同时为具有竞争关系的证券公司进行咨询时导致的数据泄漏问题.在中国墙模型策略约束下,一个咨询师最初可以为任意证券公司提供咨询服务,但是一旦该咨询师确定为某一个公司 *A* 提供咨询服务,他将不能再为与 *A* 公司有竞争关系的其他公司提供咨询服务,以防止两个公司之间出现信息泄露.这种主体访问时初始选择的自由性和后续控制的强制性是其他传统安全策略模型如 BLP 模型[2]所不能描述的[1].因此,中国墙模型从提出开始就不断被扩展应用于各种需要防止内部数据泄漏的领域.

1990年,Medows[3]将中国墙模型扩展到多级安全的应用环境中,防止DBMS中不同数据聚类之间的信息泄漏;Sandhu[4]基于格模型对中国墙模型进行扩展,通过区分人类用户主体和计算机主体实现信息流控制策略;Foly[5]在 Unix 系统中基于标准 Unix 保护机制实现了中国墙策略;随后,Sailer[6]和 McCune[7]分别在虚拟机和分布式虚拟机环境下使用中国墙模型对隐形流进行约束;程戈[11]通过引入联盟关系实现访问区域的动态扩展,使中国墙模型可以更好的应用于虚拟机系统的隐形流控制;Radhakrishnan[8]研究了借助于中国墙策略实现操作系统内核中的安全分组机制,提供对应用安全的支持;赵庆松[9]和何永忠[10]先后将角色访问控制策略引入到中国墙模型中,通过RBAC配置提高中国墙策略的灵活性,使其可以直接应用于支持RBAC的系统中.这些应用中,大部分研究的核心是根据利益冲突关系划分资源的访问区域,通过禁止不同访问区域之间的信息流动来防止数据泄漏.

近年来,针对企业知识产权和个人隐私等敏感数据保护需求日益迫切,工业界提出了数据泄漏防护(data leakage prevention,简称DLP)的概念(http://security.doit.com.cn/),其目标是防止企业指定的数据以违反安全策略规定的形式流出企业.目前,已经有一些相对成熟的产品和技术解决方案,如沈昌祥院士提出“三纵三横两个中心”的分域控制框架[12]、赵勇的基于密码隔离的内网安全方案[13]等.但是数据泄漏防护理论方面的研究相对滞后,技术方案的安全性和完备性有待证明.

本文分析发现,计算机系统中数据泄漏防护的目标与中国墙模型的目标在很大程度上是一致的,但是后者更突出人类用户的因素[4],因此对于读写操作的约束也更加严格,本文第 1 节将详细分析该约束问题.基于此,本文从数据泄漏防护中信息流控制的需求出发,提出了满足信息流单向流动控制需求的主动冲突关系和主动联盟关系的概念.通过修改传统中国墙模型中的读写约束条件,扩展提出了ACWM模型,并给出了ACWM的形式化描述.同时,我们从主动冲突关系角度给出了数据泄漏一个形式化的理解.最后的分析表明,ACWM 既保留了原有模型的灵活性与安全性,又可以保证不会存在主动冲突关系导致的数据泄漏.

本文第 1 节分析中国墙模型存在的问题.第 2 节从信息流角度对中国墙模型进行改造,并给出形式描述和相关证明.第 3 节对扩展后的模型进行安全性和适应性分析.第 4 节是对全文的总结.

## 1 中国墙模型分析

在Brewer和Nash提出的BN模型中,每个公司的数据属于一个公司数据集,具有竞争关系的公司数据集构成一个利益冲突类.数据对象之间可能存在以下两种二元关系:冲突关系(conflict of interest relation,简称 CIR)和联盟关系(in ally relation,简称 IAR)(文献[11]中使用 AIR 或 AIF 表示,本文沿用 Lin 在文献[15]中的符号),并且具有冲突关系的客体之间不能有信息流动,而具有联盟关系的客体之间允许信息流动.基于此,BN 模型提供两个重要安全特性:

(1) 简单安全性:主体 *s* 可以访问数据对象 *o* 必须满足条件:*o* 与主体 s 已经访问的对象属于同一个公司数据集或者 *o* 与主体 *s* 已经访问的每一个对象都属于不同的利益冲突类;

(2) *-安全性:主体 *s* 可以写数据对象 *o* 必须满足条件:满足简单安全性并且 *o* 与主体 *s* 访问过的每一个客体属于同一个公司数据集.

为说明中国墙模型存在的强约束问题,本文结合如下例子进行说明.

例 1:假设数据库中存在 4 个敏感数据文件{$f_{bank\text{-}A}$,$f_{bank\text{-}B}$,$f_{oil\text{-}A}$,$f_{oil\text{-}B}$},分别对应两家银行和两家石油公司的数据.银行之间以及石油公司之间存在利益冲突,而银行与石油公司之间不存在利益冲突,两个访问进程{$P_a$,$P_b$},

© 中国科学院软件研究所 http://www.jos.org.cn

初始时 $P_a$ 和 $P_b$ 都没有访问上述文件.

(1) 读操作的强约束限制了某些正常应用的进程行为

由 BN 模型的简单安全性可知,进程 $P_a$ 访问文件 $f_{bank\text{-}A}$ 后,将不能访问 $f_{bank\text{-}B}$.Sandhu[4]认为,这主要是因为 BN 模型没有区分人类用户和计算机主体的差异,人类用户获取的信息可以通过超出计算机控制范围的方式泄漏到竞争对手手中.而对于计算机中的进程主体,只要 $P_a$ 不对 $f_{bank\text{-}A}$ 和 $f_{bank\text{-}B}$ 进行写操作,就不会有 $f_{bank\text{-}A}$ 和 $f_{bank\text{-}B}$ 之间的数据泄漏,因此应该允许 $P_a$ 对 $f_{bank\text{-}A}$ 和 $f_{bank\text{-}B}$ 同时进行只读访问;否则,如果 $P_a$ 是上级统计部门进行统计的一个进程,其正常功能将不能实现.

(2) 写操作的强约束限制了某些正常的信息流动

由*-安全性可知,进程 $P_a$ 访问文件 $f_{bank\text{-}A}$ 后,将不能写 $f_{oil\text{-}A}$,虽然两者之间没有冲突关系.Volker[14]从信息流的角度对该约束进行了扩展,允许 $P_a$ 对 $f_{oil\text{-}A}$ 进行写操作,但之后,进程 $P_b$ 将不能同时读取 $f_{oil\text{-}B}$ 和 $f_{bank\text{-}A}$,也不能同时读取 $f_{oil\text{-}A}$ 和 $f_{bank\text{-}B}$.程戈[11]在 Volker 的基础上引入了联盟关系 *AIR*,给予读写操作同样的约束,从而可以动态地建立访问区域.本文分析发现,联盟关系实际上是将 Volker 的读操作限制条件进行了扩展,其对冲突关系的扩展与 Volker 的改进本质上是一致的,因此也同样面临上述约束.

(3) 冲突关系的定义对访问区域划分的影响

冲突关系 *CIR* 的构造是影响中国墙模型发展的一个关键因素,而构造冲突关系的过程也就是对应访问区域的划分过程.在 BN 模型中,利益冲突关系是一个等价关系,因此所有客体可以被一个完整划分所覆盖;Lin 研究发现,冲突关系在大多数情况下并不满足传递关系,其在文献[15]中将冲突关系定义为一个对称的二元关系,并使用冲突邻域对冲突关系进行限定.2000 年,Lin[16]又将粗糙集理论中的冲突分析方法引入到中国墙模型中,通过扩展加权二元关系对中国墙模型进行改造.随后,Katsuno[17]研究了分布式环境中基于中国墙模型进行资源静态划分的问题,Jaeger[18]从控制虚拟机隐形流的角度研究了静态资源隔离划分的策略,程戈[11]则引入联盟关系实现了访问区域的动态划分.这些改进和应用,逐步完善了中国墙模型的理论基础.但是通过冲突关系划分的访问区域之间完全不存在信息流动,而实际数据泄漏防护中,大部分时候只需要控制数据的单向流动.例如,对于石油公司 *oil-A* 来说,它只关心自己的数据 $f_{oil\text{-}A}$ 会不会流动到竞争对手 *oil-B* 的数据 $f_{oil\text{-}B}$ 中,而不会阻止 $f_{oil\text{-}B}$ 的数据流入 $f_{oil\text{-}A}$ 中.

综上所述,中国墙模型关于冲突关系的定义和约束规则对于数据泄漏防护的应用限制过于严格,不具有通用性.其关键原因在于对信息流动的双向约束,即存在冲突关系的客体之间完全不存在信息流动.因此,本文从数据客体自身保护的需求出发,将信息流的双向约束转换为单向约束,并基于此对中国墙模型进行扩展,从而实现数据对象的主动泄漏防护.

## 2 扩展的中国墙模型

中国墙策略的目标是防止具有利益冲突的竞争对手之间的信息流流动,其冲突关系对信息流的约束是双向的.而在数据泄漏防护中,主要目标是防止指定的企业敏感数据泄漏到企业应用环境之外,而对于流入企业的信息没有限制.从保护的数据对象的角度看,其对信息流的约束则是单向的.因此,我们提出主动冲突关系和主动联盟关系的概念来体现对信息流的单向约束,满足主动冲突关系的数据客体之间不允许信息单向流动,而满足联盟关系的数据客体之间允许信息流动.基于此概念,本节在 Lin[15]给出的中国墙模型基础上进行扩展,使其能够实现主动数据泄漏防护.

### 2.1 模型定义

本文沿用 BLP[2]关于主体 $S$ 和客体 $O$ 的定义,$T=\{1,2,3,\ldots,t,\ldots\}$ 表示时间指标,系统访问请求集合 $b\subseteq S\times O\times\{r,w\}$,$R_t(s_i,o_j,r)\in b$ 表示 $t$ 时刻主体 $s_i$ 对客体 $o_j$ 的读操作请求,也记为 $R_t(i,j,r)$;$R_t(s_i,o_j,w)\in b$ 表示 $t$ 时刻主体 $s_i$ 对客体 $o_j$ 的写操作请求,也记为 $R_t(i,j,w)$.为方便描述,$R_t(i,j,r/w)=1$ 表示允许读/写操作请求,而 $R_t(i,j,r/w)=0$ 表示拒绝读/写操作请求.

**定义 1**. 主体 $s$ 和客体 $o$ 之间在 $t$ 时刻通过一次读或者一次写操作导致的信息流动称为直接信息流,用 $DIF_t$

© 中国科学院软件研究所 http://www.jos.org.cn

表示.有如下两种情况:

(1) $o\ DIF_t\ s \Leftrightarrow R_t(s,o,r)=1$;

(2) $s\ DIF_t\ o \Leftrightarrow R_t(s,o,w)=1$.

**定义 2**. 由多次连续的直接信息流导致的信息流动称为间接信息流(文献[11]将经过主体连续的一次读和一次写操作导致的间接信息流也定义为直接信息流),用 $CIF_{t_0}^{t}$ 表示.其中,$t_0$ 表示开始时刻,$t$ 表示结束时刻,$t_0 \leqslant t$.有如下 3 种情况:

(1) $o\ CIF_{t_0}^{t}\ s \Leftrightarrow \exists s_1,s_2,...,s_k \in S, o_1,o_2,...,o_k \in O, \exists t_0 \leqslant t_1 \leqslant ... \leqslant t_{2k}=t \in T$

$$o\ DIF_{t_0}\ s_1,...,o_{i-1}\ DIF_{t_{2(i-1)}}\ s_i,s_i\ DIF_{t_{2i-1}}\ o_i,o_i\ DIF_{t_{2i}}\ s_{i+1},...,o_k\ DIF_{t_{2k}}\ s.$$

当 $k$=0 时, $o\ CIF_{t_0}^{t}\ s = o\ DIF_t\ s$ ,即 $o$ 到 $s$ 的间接信息流就是直接信息流;

(2) $s\ CIF_{t_0}^{t}\ o \Leftrightarrow \exists s_1,s_2,...,s_k \in S, o_1,o_2,...,o_k \in O, \exists t_0 \leqslant t_1 \leqslant ... \leqslant t_{2k}=t \in T$

$$s\ DIF_{t_0}\ o_1,...,s_{i-1}\ DIF_{t_{2(i-1)}}\ o_i,o_i\ DIF_{t_{2i-1}}\ s_i,s_i\ DIF_{t_{2i}}\ o_{i+1},...,s_k\ DIF_{t_{2k}}\ o.$$

当 $k$=0 时, $s\ CIF_{t_0}^{t}\ o = s\ DIF_t\ o$ ,即 $s$ 到 $o$ 的间接信息流就是直接信息流;

(3) $o\ CIF_{t_0}^{t}\ o' \Leftrightarrow \exists s' \in S, \exists t_0 \leqslant t_1 \leqslant t_2 = t \in T, o\ CIF_{t_0}^{t_1}\ s' \wedge s'\ DIF_{t_2}\ o'$ .

从定义可以看出,直接信息流是间接信息流的一种特殊形式.为描述方便,本文后面对信息流的描述直接使用 *CIF* 表示.

主动冲突关系和主动联盟关系体现的是对信息流约束的需求,基于定义 1 和定义 2,我们给出如下定义:

**定义 3(主动冲突关系(aggressive conflict of interest relation,简称 ACIR))**. 如果从客体 $o$ 到 $o'$存在主动冲突关系,记为 $o\ ACIR\ o'$或 $o' \in ACIR(o)$,则不允许存在从 $o$ 到 $o'$的信息流,用~($o\ CIF\ o'$)表示.其中,$ACIR(o)$称为 $o$ 出发的主动冲突关系集合.

**定义 4(主动联盟关系(aggressive in ally with relation,简称 AIAR))**. 如果从客体 $o$ 到 $o'$存在主动联盟关系,记为 $o\ AIAR\ o'$或 $o' \in AIAR(o)$,则允许存在从 $o$ 到 $o'$的信息流.其中,$AIAR(o)$称为 $o$ 出发的主动联盟关系集合.

ACIR 和 AIAR 的定义都是从客体角度出发,给出的客体自身的安全保护需求,体现了客体数据泄漏防护的主动性.由定义 3 和定义 4 可知,主动冲突关系和主动联盟关系具有互斥性和完备性,即有如下引理:

**引理 1(互斥性引理)**. 从客体 $o$ 到客体 $o'$不能同时满足 ACIR 和 AIAR.

**引理 2(完备性引理)**. $\forall o,o' \in O, o' \in ACIR(o)$和 $o' \in AIAR(o)$有且仅有一个成立.

从信息流的定义可知,主动联盟关系满足传递性;而主动冲突关系不一定有传递性,但具有主动联盟关系的客体之间通过访问可以导致主动冲突关系的传递,即有引理 3.

**引理 3(主动冲突扩散引理)**. 如果从 $o$ 到 $o'$存在主动联盟关系,且存在从客体 $o$ 到 $o'$的信息流,则所有从客体 $o$ 出发存在主动冲突关系的客体,从客体 $o'$出发也存在主动冲突关系,即为

$$\forall o,o' \in O, o\ AIAR\ o' \wedge (\exists s \in S, t_0 \leqslant t_1 \leqslant t_2 \leqslant t, o\ CIF_{t_0}^{t_1}\ s, s\ CIF_{t_2}^{t}\ o') \Rightarrow \forall o'' \in ACIR(o), ACIR(o') \cup \{o''\}, AIAR(o') \setminus \{o''\}$$

其中,$ACIR(o') \cup \{o''\}$表示将 $o''$增加到 $o'$出发的主动冲突关系集合中,$AIAR(o') \setminus \{o''\}$表示将 $o''$从 $o'$出发的主动联盟关系集合中删除.

引理 3 说明,主动冲突关系集合和主动联盟关系集合会随着访问过程动态变化,也是时间相关的.分别用 $ACIR_t(o)$和 $AIAR_t(o)$表示 $t$ 时刻从客体 $o$ 出发的主动冲突关系集合和主动联盟关系集合.

为保证信息流动过程中不会出现导致违反规则的访问,Volker 引入了冲突安全[14]的概念.基于主动冲突关系,我们给出相应的扩展定义.

**定义 5**. 系统是主动冲突安全的,当且仅当

$$\forall s \in S; o,o' \in O; t \in T; o\ CIF_0^t\ s \wedge s\ CIF_0^t\ o' \Rightarrow o' \notin ACIR(o).$$

Volker 定义的冲突安全目标是防止主体同时访问两个具有利益冲突关系的客体,主动冲突安全的目标则是防止从客体 $o$ 到与其存在主动利益冲突的客体 $o'$的信息流动.

© 中国科学院软件研究所 http://www.jos.org.cn

工业界提出的数据泄漏防护的目标是防止企业数据泄漏出企业,因此,从主动冲突关系的角度理解数据泄漏,我们可以给出一个数据泄漏的形式化描述:

如果存在 $o$ 到 $o'$的信息流,且 $o$ 到 $o'$具有主动冲突关系,则认为 $o$ 发生了数据泄漏,记为 $DL(o)$,即

$$\exists o'\in O, o\ CIF\ o'\wedge o'\in ACIR(o)\Leftrightarrow DL(o).$$

### 2.2 模型描述

定义访问控制矩阵 $N:S\times O\rightarrow\{NR,NW,NN,R,W\}$,其中,

$$N(i,j)=\begin{cases} NR, & \text{禁止主体}s_i\text{对客体}o_j\text{的读操作}\\ NW, & \text{禁止主体}s_i\text{对客体}o_j\text{的写操作}\\ NN, & \text{操作未确定}\\ R, & \text{允许主体}s_i\text{对客体}o_j\text{的读操作}\\ W, & \text{允许主体}s_i\text{对客体}o_j\text{的写操作}\end{cases}.$$

基于以上定义,给出扩展后的中国墙模型.

**定义 6**. ACWM 模型是图灵机上的四元组$(S,O,N,b)$,并满足以下规则:

**规则 1**. 初始时,对所有的 $i$ 和 $j$,$N(i,j)=NN$.

**规则 2**. $N(i,j)=NN$ 时:

(1) $R_t(i,j,r)$允许,$N(i,j)=R$,同时,$\forall l\neq j, o_l\in ACIR_t(o_j)\wedge N(i,l)\neq NR, N(i,l)=NW$;

(2) $R_t(i,j,w)$允许,$N(i,j)=W$,运用规则 7 更新 $ACIR_t(o_j)$和 $AIAR_t(o_j)$,同时,$\forall h\neq j, o_j\in ACIR_t(o_h), N(i,h)=NR$.

**规则 3**. $N(i,j)=R$ 时:

(1) $R_t(i,j,r)$允许;

(2) 如果$\exists h\neq j, o_j\in ACIR_t(o_h)\wedge(N(i,h)=R\vee N(i,h)=W)$,则 $R_t(i,j,w)$拒绝;否则,$R_t(i,j,w)$允许,$N(i,j)=W$,运用规则 7 更新 $ACIR_t(o_j)$和 $AIAR_t(o_j)$,同时,$\forall h\neq j, o_j\in ACIR_t(o_h)\wedge(N(i,h)=NN\vee N(i,h)=NW), N(i,h)=NR$.

**规则 4**. $N(i,j)=W$ 时:

(1) $R_t(i,j,r)$允许;

(2) $R_t(i,j,w)$允许,运用规则 7 更新 $ACIR_t(o_j)$和 $AIAR_t(o_j)$.

**规则 5**. $N(i,j)=NW$ 时:

(1) 如果$\exists l\neq j, o_l\in ACIR_t(o_j)\wedge N(i,l)=NW$,则 $R_t(i,j,r)$拒绝;否则,$R_t(i,j,r)$允许,同时,$\forall l\neq j, o_l\in ACIR_t(o_j)\wedge N(i,l)\neq NR, N(i,l)=NW$;

(2) $R_t(i,j,w)$拒绝.

**规则 6**. $N(i,j)=NR$ 时:

(1) $R_t(i,j,r)$拒绝;

(2) $R_t(i,j,w)$拒绝.

**规则 7**. 如果 $R_t(i,j,w)$允许,$\forall h\neq j, o_j\in AIAR_t(o_h)\wedge(N(i,h)=R\vee N(i,h)=W)$,则 $R_t(i,j,w)$操作之后的时刻 $t'$有:

$$ACIR_{t'}(o_j)=ACIR_t(o_j)\cup ACIR_t(o_h), AIAR_{t'}(o_j)=AIAR_t(o_j)\backslash ACIR_t(o_h).$$

对上述规则进行分析,可以得出任意一个 $N(i,j)$取值的变迁关系如图 1 所示.其中,$r$ 和 $w$ 分别表示读操作和写操作,$S$ 表示对应的操作是对客体 $o_j$ 本身进行的,$A+$表示对应操作是对客体 $o_j$ 出发存在主动冲突关系的客体进行的,$A-$表示对应操作是对到客体 $o_j$ 存在主动冲突关系的客体进行,数字表示对应的规则序号.

传统的 BN 模型[1]和 Lin 扩展的中国墙模型 LINCWM[15]中,冲突关系都是静态的.Volker 在文献[14]中首次提出了动态改变冲突关系的思想,并根据主体对客体的读写操作动态扩大客体对应的冲突关系集.程戈在 Volker 的基础上通过引入联盟关系[11]对利益冲突关系进行扩展.由于具有联盟关系的客体具有相同的利益冲突集,所以可以通过联盟关系的动态扩展实现冲突关系的动态变化.ACWM 模型下,主动冲突关系集合和主动联盟关系集合也会由于写操作的执行而动态变化,并且规则 7 给出了这种变化的时机和原则.从该规则可以看出,主动冲突关系集合的规模会随着主体的访问增大(或者保持不变),而主动联盟关系集合则会由于写操作而

© 中国科学院软件研究所 http://www.jos.org.cn

缩小(或者保持不变).与 Volker 和程戈的动态扩展相比,ACWM 模型实质上是借助访问控制矩阵记录历史信息流,因此其动态扩展的过程更加直观,而且这种矩阵模型也更容易应用于现有安全系统中.

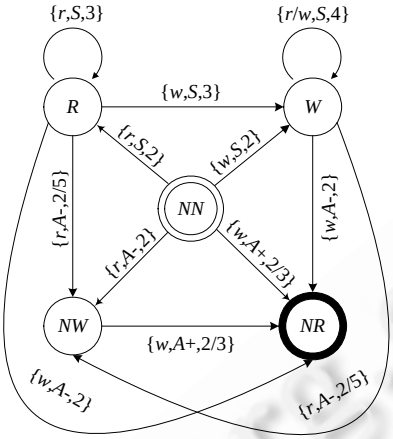



Fig.1 Value transition diagram of $N(i,j)$

图 1 $N(i,j)$取值变迁图

### 2.3 模型性质

**定理 1(简单安全性)**. 主体 $s$ 可以读取客体 $o$,则 $s$ 不允许对从 $o$ 出发存在主动冲突关系的客体具有写权限.

证明: 采用反证法证明.取 $s_i=s,o_j=o$,假设 $t$ 时刻存在 $o_k\in ACIR_t(o_j)$,且 $R_t(i,k,w)$允许操作,则由图 1 可以看出,$t$ 时刻 $N(i,k)$可能的取值有 $NN$,$R$ 和 $W$ 这 3 种:

(1) 如果 $N(i,k)=NN$,由规则 2 得知,$R_t(i,k,w)$操作后必有 $N(i,j)=NR$.从图 1 可知 $NR$ 是终态,不可能变为其他状态,由规则 5 可知,$t'>t,R_{t'}(i,j,r)$将被拒绝,与前提矛盾;

(2) 如果 $N(i,k)=R$,由规则 3 可知,$t$ 时刻 $N(i,j)\neq R$ 且 $N(i,j)\neq W$;否则,$R_t(i,k,w)$将被拒绝.因此,$R_t(i,k,w)$操作之后 $N(i,j)=NR$.由情况(1)分析知与前提矛盾;

(3) 如果 $N(i,k)=W$,由图 1 可以看出,该状态只能由 $N(i,k)=NN$ 或 $N(i,k)=R$ 经过 $R_{t''}(i,k,w)(t''\leqslant t)$操作转换得到,由情况(1)、情况(2)可知必有 $N(i,j)=NR$.与前提矛盾.

综上所述,假设 $s$ 对从 $o$ 出发存在主动冲突关系的客体 $o'$具有写权限,可以得出 $s$ 不能读取客体 $o$,与前提矛盾.因而假设不成立. □

**定理 2(*-安全性)**. 主体 $s$ 可以写客体 $o$,则不存在客体 $o'$,$s$ 读过 $o'$,且从 $o'$到 $o$ 存在主动冲突关系.

证明:采用反证法证明.取 $s_i=s,o_j=o$,假设存在这样的客体 $o'=o_l$,在 $t$ 时刻,$o_j\in ACIR_t(o_l)$,且 $R_t(i,l,r)$被允许操作.由图 1 可以看出,$t$ 时刻 $N(i,l)$可能的取值有 $NW$,$NN$,$R$ 和 $W$ 这 4 种:

(1) 如果 $N(i,l)=NW$,由规则 5 可知,$R_t(i,l,r)$操作之前 $N(i,j)\neq W$;否则,$R_t(i,l,r)$操作将被拒绝.因此,$R_t(i,l,r)$操作之后,$N(i,j)$可能的取值有 $NW$ 和 $NR$,由规则 4 和规则 5 可知,不论 $N(i,j)=NW$ 还是 $N(i,j)=NR$,$\exists t'\geqslant t$,$R_{t'}(i,j,w)$会被拒绝,与前提矛盾;

(2) 如果 $N(i,l)=NN$,由规则 2 可知,$R_t(i,l,r)$操作之后,$N(i,j)$可能的取值只有 $NW$ 和 $NR$,同情况(1)分析可知,与前提矛盾;

(3) 如果 $N(i,l)=R$,由图 1 可知,$N(i,l)=R$ 只能由 $N(i,l)=NW$ 和 $N(i,l)=NN$ 经过读操作 $R_{t''}(i,l,r)(t''\leqslant t)$转换,由情况(1)、情况(2)可知,与前提矛盾;

(4) 如果 $N(i,l)=W$,由图 1 可知,$N(i,l)=W$ 只能由 $N(i,l)=NN$ 和 $N(i,l)=R$ 经过写操作 $R_{t''}(i,l,r)(t''\leqslant t)$转换,由情况(2)、情况(3)可知,与前提矛盾.

综上所述,如果存在这样的客体 $o'=o_l,o_j\in ACIR_t(o_l)$,且 $R_t(i,l,r)$被允许操作,则$\exists t'\geqslant t,R_{t'}(i,j,w)$被拒绝,与前提矛

© 中国科学院软件研究所 http://www.jos.org.cn

盾.因而假设不成立. □

**定理 3**. $\forall o,o'\in O;o\ CIF\ o'\Rightarrow o'\notin ACIR(o)$(当时间因素没有影响时,CIF 中时间标记省略).

证明:采用归纳法证明.为方便说明,采用符号 $\overset{k}{CIF}$ 表示定义 2 中经过 $k$ 个主体连续直接信息流得到的间接信息流.

(1) $k$=0 时, $\exists s'\in S,\exists t_0\leqslant t_1\in T,(o\ DIF_{t_0}\ s'\wedge s'\ DIF_{t_1}\ o')$,即 $R_{t_0}(s',o,r)\wedge R_{t_1}(s',o',w)$,则有 $o'\notin ACIR(o)$;否则,由定理 2 可知, $R_{t_1}(s',o',w)$ 操作将会被禁止;

(2) 假设 $k$=$n$ 时成立, $\forall o,o'\in O;o\ CIF\ o'\Leftrightarrow\exists s'\in S,\exists t_0\leqslant t_1\leqslant t_2=t\in T,o\ \overset{k}{CIF}^{t_1}_{t_0}\ s'\wedge s'\ DIF_{t_2}\ o'$,则 $k$=$n$+1 时,

$\forall o,o'\in O;o\ CIF\ o'\Leftrightarrow\exists s',s''\in S,\exists o''\in O,\exists t_0\leqslant t_1\leqslant t_2\leqslant t_3\leqslant t_4\in T,o\ \overset{k}{CIF}^{t_1}_{t_0}\ s'\wedge s'\ DIF_{t_2}\ o''\wedge o''\ DIF_{t_3}\ s''\wedge s''\ DIF_{t_4}\ o'$.

由假设知 $o''\notin ACIR(o)$,由引理 2 知 $o''\in AIAR(o)$.对于 $s'\ DIF_{t_2}\ o''$,由规则 7 可知:

$$ACIR_{t_2}(o'')=ACIR_{t_1}(o'')\cup ACIR_{t_1}(o).$$

而对于 $o''\ DIF_{t_3}\ s''\wedge s''\ DIF_{t_4}\ o'$,由假设(1)可知 $o'\notin ACIR_{t_4}(o'')$,由引理 2 可知 $ACIR_{t_2}(o'')\subseteq ACIR_{t_4}(o'')$,因此必有 $o'\notin ACIR(o)$.

综上所述,对于任意 $k$ 均有结论成立. □

**定理 4(主动冲突安全)**. 基于非对称关系的中国墙模型 ACWM 是主动冲突安全的.即

$$\forall s\in S;o,o'\in O;o\ CIR\ s\wedge s\ CIR\ o'\Rightarrow o'\notin ACIR(o).$$

证明:由定义 2 可知,$\forall s\in S;o,o'\in O;o\ CIR\ s\wedge s\ CIR\ o'\Rightarrow o\ CIR\ o'$.由定理 3 可得结论成立. □

定理 1~定理 4 的证明显示,在满足规则约束下,ACWM 模型可以提供相应的简单安全性和*-安全性,并可以保证系统是主动冲突安全的.

## 3 模型比较与分析

### 3.1 与传统中国墙模型的比较

传统的中国墙策略中的冲突关系是从企业安全保护需求角度定义的,其对信息流约束是双向的;ACWM 中的主动冲突关系则是从数据泄漏防护的需求出发,对信息流的约束是单向的,见引理 4:

**引理 4**. $o'\in ACIR(o)\wedge o\in ACIR(o')\Leftrightarrow o'\in CIR(o)$.

程戈在文献[11]中定义的联盟关系 IAR 是一种等价关系,显然也有引理 5:

**引理 5**. $o'\in AIAR(o)\wedge o\in AIAR(o')\Leftrightarrow o'\in IAR(o)$.

从冲突关系和联盟关系之间的关系来看,传统中国墙模型中两者是互斥的[15],但并不互补,即~($o$ *IAR* $o'$)≠$o$ *CIR* $o'$.而 ACWM 模型下的主动冲突关系和主动联盟关系既是互斥的,又是互补的.即任意两个客体,必定可以明确二者的关系.

从信息流角度分析,传统中国墙模型的简单安全性可以表示为

$$R(s,o,r)=1\wedge o\ CIR\ o'\Rightarrow R(s,o',w)=0\wedge R(s,o',r)=0 \quad (1)$$

其中,$R(s,o',w)$=0 是简单安全性对写操作的约束,从数据泄露防护角度看,可以理解为读取了敏感客体 $o$ 的主体 $s$ 不能对与 $o$ 存在冲突关系的客体 $o'$进行写操作,从而可以防止从 $o$ 到 $o'$的信息流动;而 $R(s,o',r)$=0 是对读操作的约束,即读取了敏感客体 $o$ 的主体 $s$ 不能对与敏感客体存在冲突关系的客体 $o'$进行读操作.从信息流的角度看,这种读操作并不会直接导致敏感信息的泄露.但传统中国墙模型中,这种强制的读约束是必须的.对于人类用户而言,这种约束是为了防止同一个主体同时获取两个具有冲突关系的客体数据.而对于计算机主体而言,这种强制约束主要是由于 CIR 具有对称性导致的.因为如果没有此限制,即 $R(s,o',r)$=1,由 CIR 的对称性,同公式(1),有

$$R(s,o',r)=1\wedge o'\ CIR\ o\Rightarrow R(s,o,w)=0\wedge R(s,o,r)=0 \quad (2)$$

从而必有 $R(s,o,w)$=0.即主体 $s$ 读取敏感客体 $o$ 之后,如果再读取与 $o$ 存在冲突关系的客体 $o'$,将失去对客体 $o$ 的写操作权限.而由于冲突关系是反自反的[15],即客体 $o$ 与自身不存在利益冲突,因而主体 $s$ 读取敏感客体 $o$ 之后、

© 中国科学院软件研究所 http://www.jos.org.cn

没有读取 $o'$之前,可以对 $o$ 进行写操作.这种写操作授权的丢失将可能导致实际应用数据的丢失.而传统中国墙模型对读操作的强制约束,则可以避免出现这种情况.

综上分析,我们可以得出:冲突关系的对称性是传统中国墙模型约束过于严格的一个主要原因.在对称冲突关系下,有冲突关系的两个客体之间的双向信息流动都需要控制,这是ACWM模型中从两个客体出发均满足主动冲突关系的特例.在实际应用中,对于人类用户这一类信息输出可能超越计算机控制范围的主体,使用双向的主动冲突关系进行约束才能防止数据泄漏;而对于输出可控的计算机主体,如进程等,则只需满足单向的主动冲突关系的约束即可.

从访问控制实施的时机来看,传统中国墙模型是一种积极预防型的控制,即如果读写操作可能造成数据泄漏,即使允许当前的读操作并不会直接造成数据泄漏,也会禁止这种操作,这会导致约束范围扩大;而 ACWM 模型则提供了一种更加精确的控制,只要当前的操作没有直接导致数据泄漏,都会允许当前操作的进行.因此,ACWM 可以提供更多的灵活性.这种控制需求在集中式服务应用中普遍存在.例如,数据中心的服务器端进程可能要为具有利益冲突关系的不同分布式终端提供服务,在传统中国墙模型约束下,一个服务器进程只能提某一个公司或者部门的数据集服务;而在ACWM模型下,一个服务器进程可以在保证不存在数据泄漏的情况下同时为具有利益冲突的不同数据集提供服务.近年来,针对分布式应用中数据机密性保护的需求,研究者引入了虚拟隔离的思想控制进程对数据的使用[19],如果将 ACWM 模型应用于虚拟终端对数据中心的数据访问控制中,将可以在保证安全性的前提下进一步提高应用的灵活性.

### 3.2 模型适应性分析

ACWM 模型将传统中国墙模型中冲突关系的双向约束扩展为主动冲突关系的单向约束,在一定程度上解决了读操作和写操作约束过强导致的问题,特别是从数据客体的角度出发定义的主动冲突关系,可以较好地实现主动数据泄漏防护.

对于第 1 节例 1 中分析的传统中国墙模型的约束问题,在 ACWM 模型中,初始时 4 个文件的关系为

$$ACIR_t(f_{bank\text{-}A})=\{f_{bank\text{-}B}\},ACIR_t(f_{bank\text{-}B})=\{f_{bank\text{-}A}\},ACIR_t(f_{oil\text{-}A})=ACIR_t(f_{oil\text{-}B})=\{\},$$

$$AIAR_t(f_{bank\text{-}A})=AIAR_t(f_{bank\text{-}B})=\{f_{oil\text{-}A},f_{oil\text{-}B}\},AIAR_t(f_{oil\text{-}A})=AIAR_t(f_{oil\text{-}B})=\{f_{bank\text{-}A},f_{bank\text{-}B}\}.$$

(1) 同一个进程可以同时读取具有冲突关系的客体

进程 $P_a$ 在 $t$ 时刻读取 $f_{bank\text{-}A}$,在 $t'\geqslant t$ 时刻读取 $f_{bank\text{-}B}$,$t'$时刻前后的访问矩阵分别为

$$N=\begin{bmatrix} R & NW & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},N'=\begin{bmatrix} NW & NW & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

从访问矩阵可以看出:在 $P_a$ 读取 $f_{bank\text{-}B}$ 之前,它对 $f_{bank\text{-}A}$ 具有读写权限,对 $f_{bank\text{-}B}$ 具有读权限,而没有写权限;$P_a$ 读取 $f_{bank\text{-}B}$ 之后,它对 $f_{bank\text{-}A}$ 和 $f_{bank\text{-}B}$ 都只有读权限,没有写权限.

(2) 一个进程的写操作对其他进程后续操作的影响减小

进程 $P_a$ 在 $t$ 时刻读取 $f_{bank\text{-}A}$,在 $t'\geqslant t$ 时刻写 $f_{oil\text{-}A}$,$t'$之后,$f_{oil\text{-}A}$ 的主动冲突关系集合与主动联盟关系集合分别为 $ACIR_t(f_{oil\text{-}A})=\{f_{bank\text{-}B}\}$,$AIAR_t(f_{oil\text{-}A})=\{f_{bank\text{-}A}\}$.对应的访问矩阵为

$$N=\begin{bmatrix} R & NW & W & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

因此在 $P_a$ 写 $f_{oil\text{-}A}$ 之后,它对 $f_{bank\text{-}A}$ 和 $f_{oil\text{-}A}$ 具有读写权限,对 $f_{bank\text{-}B}$ 具有读权限,而对 $f_{oil\text{-}B}$ 具有读写权限.此后,进程 $P_b$ 可以在 $t''\geqslant t'$时刻读取 $f_{oil\text{-}B}$,在 $t'''\geqslant t''$时刻读取 $f_{bank\text{-}A}$,$t'''$前后的访问矩阵分别为

$$N'=\begin{bmatrix} R & NW & W & 0 \\ 0 & 0 & NW & R \end{bmatrix},N''=\begin{bmatrix} R & NW & W & 0 \\ R & NW & NW & R \end{bmatrix}.$$

$t'''$之后,$P_b$ 可以对 $f_{bank\text{-}A}$ 和 $f_{oil\text{-}B}$ 具有读写权限,而对 $f_{bank\text{-}B}$ 和 $f_{oil\text{-}A}$ 只有读权限.而在传统中国墙模型中,$P_b$ 不允许同时读 $f_{bank\text{-}B}$ 和 $f_{oil\text{-}A}$.

(3) 数据对象根据自身安全保护需求确定主动冲突关系集合

在ACWM模型中,不需要根据主动冲突关系对整个客体集合划分访问区域,而只需要根据数据对象的泄露

© 中国科学院软件研究所 http://www.jos.org.cn

防护需求确定自身的主动冲突关系集合即可.因此在 ACWM 中,数据对象对于进程的访问具有主动性,其主动冲突关系集合是动态变化的,因此每个进程的访问区域也是动态变化的.

针对数据泄漏防护需求,给出定理 5.

**定理 5**. 系统是主动冲突安全的,则不存在数据泄漏.

证明:采用反证法.假设存在数据泄漏,则必有$\exists o'\in O, o\ CIR\ o'\wedge o'\in ACIR(o)$.由定理 3 可知,$\exists o'\in O, o\ CIR\ o'$,则$o'\notin ACIR(o)$.存在矛盾,因而假设条件不成立. □

此定理说明,在满足 ACWM 模型规则的情况下,系统中不存在数据泄漏.从上述比较和分析也可以看出,ACWM 在保持原有中国墙模型初始自由访问特性的基础上,可以给予进程后续访问更大的灵活性,能够很好地满足数据泄露防护的需求.

### 3.3 与BLP模型比较

Lin 在文献[15]中指出,中国墙模型实质就是一个初始状态具有一定自由度的访问控制矩阵模型,该矩阵同时具有否定授权和显示授权,并且否定授权优先于显式授权.但是由于读写操作的严格限制,这种模型在实际应用中难以表达多级安全策略的需求[4].Meadows[3]通过数据聚类的方法并借助于满足格关系的标签,将中国墙模型扩展到多级应用中.Sandhu[4]在信息流模型的基础上通过一种特殊的格关系结构,使用 BLP 模型的简单安全性和*-安全性描述了中国墙策略,其标记结构为

$$LABLES=\{[i_1,i_2,...,i_n]\,|\,i_1\in COI'_1,i_2\in COI'_2,...,i_n\in COI'_n \text{ where } COI'_i=COI_i\cup\{\perp\}\},$$

其中,$COI_i$ 是利益冲突类,$i_1,i_2,\ldots,i_n$ 表示不同利益冲突类中数据,而⊥表示该主体不包含对应利益冲突类中的数据.在 Sandhu 的格关系中,标记为[1,⊥]和[⊥,2]的客体不具有可比性(incomparable)[4],因此二者之间不能存在信息流动,而且简单安全性和*-安全性约束也没有包含对这类客体关系的限制.从第 3.1 节的引理 4 和引理 5 可知,ACWM 模型中,主动冲突关系和主动联盟关系是互补的,因此任何两个客体之间都存在相应的信息流约束.在此基础上,本节通过例 2 进一步对 ACWM 与 BLP 模型的约束表达能力进行比较和分析.

例 2:假设 3 个主体 $s_1,s_2,s_3$,3 个客体 $o_1,o_2,o_3$,它们之间的关系为

$$o_1\ ACIR\ o_2, o_2\ ACIR\ o_3, o_1\ ACIR\ o_3,$$
$$o_2\ AIAR\ o_1, o_3\ AIAR\ o_2, o_3\ AIAR\ o_1.$$

初始访问矩阵 $N$ 和执行特定访问序列之后的矩阵 $N'$分别为

$$N=\begin{bmatrix} NN & NN & NN\\ NN & NN & NN\\ NN & NN & NN\end{bmatrix}, N'=\begin{bmatrix} R & NW & NW\\ W & R & NW\\ W & W & R\end{bmatrix},$$

其中,访问序列为:$R(s_1,o_1,r), R(s_2,o_2,r), R(s_3,o_3,r), R(s_2,o_1,w), R(s_3,o_1,w), R(s_3,o_2,w)$.

若假设敏感级标签的关系为:$l(s_1)=l(o_1)>l(s_2)=l(o_2)>l(s_3)=l(o_3)$,则在 BLP 模型下的访问控制矩阵为

$$A=\begin{bmatrix} rw & r & r\\ w & rw & r\\ w & w & rw\end{bmatrix},$$

其中,$r$ 和 $w$ 分别表示对应的主体对客体具有读权限和写权限.

比较 $N'$和 $A$,我们可以得出如下结论:

(1) $N'$是同时具有肯定授权和否定授权的矩阵,而 $A$ 是肯定授权矩阵.在 Saltzer 和 Schroeder 提出的失败保险(fail-safe)原则[20]下,没有明确授权的访问将被拒绝;

(2) BLP 模型下,主体的访问权限关键取决于自身敏感级标签,与主体的访问无关.虽然灵活性不够,但由于实现方便,被众多安全系统普遍采用.而 ACWM 模型中,主体的访问权限取决于历史访问过的客体,根据不同的访问序列会出现不同的限制约束,可以实现更加灵活的访问控制;

(3) $N'$可以实现 $A$ 的部分控制,如主体 $s_1$ 对 3 个客体的访问权限是相同的.但是某些约束是为了满足主动泄露防护的需求,因此比 $A$ 的控制更自由.如主体 $s_2$ 可以读写 $o_1$ 和 $o_2$,只是在执行对 $o_1$ 的读或者对 $o_2$

© 中国科学院软件研究所 http://www.jos.org.cn

的写操作之后自身的访问权限将会动态变化;而 $A$ 的约束下,主体 $s_2$ 始终都不能读 $o_1$.同样,主体 $s_3$ 具有更大的自由度.

## 4 结束语

本文将中国墙模型引入到数据泄漏防护中,通过扩展冲突关系和联盟关系对信息流的约束,从数据对象的角度出发,提出了主动冲突关系和主动联盟关系的概念.基于此概念,给出了可以实现数据主动泄漏防护的扩展中国墙模型 ACWM.分析表明,ACWM 的约束规则可以提供相应的简单安全性和*-安全性,并可以保证系统是主动冲突安全的,进而也是不存在数据泄漏的.与传统中国墙模型相比,ACWM 具有更好的适应性和灵活性,特别是在基于虚拟隔离的集中式数据访问控制中具有很好的应用前景.

**References**:

[1] Bewer DFC, Nash MJ. The Chinese wall security policy. In: Proc. of the Symp. on Security and Privacy. IEEE Computer Society, 1989. 206−214. [doi: 10.1109/SECPRI.1989.36295]

[2] Bell DE, LaPadula LJ. Secure computer systems: Mathematical foundations. ESD-TR-73-278, I(AD) 770 768, Electronic Systems Division, Air Force System Command, Hanscom AFB, 1973.

[3] Meadows C. Extending the Brewer Nash model to a multilevel context. In: Proc of the '90 IEEE Symp. on Research in Security and Privacy. Oakland, 1990. 95−102. [doi: 10.1109/RISP.1990.63842]

[4] Sandhu RS. Lattice-Based enforcement of Chinese walls. Computers & Security, 1992,11(8):753−763. [doi: 10.1016/0167-4048(92)90131-A]

[5] Foley SN. Building Chinese walls in standard unix. Unix Computers and Security Journal, 1997,16(6):551−563. [doi: 10.1016/S0167-4048(97)00010-2]

[6] Sailer R, Jaeger T, Valdez E, Cáceres R, Perez R, Berger S, Griffin JL, van Doorn L.. Building a MAC-based security architecture for the Xen open source hypcrvisor. In: Proc. of the 21st Annual Computer Security Applications Conf. (ACSAC 2005). Miami, 2005. 276−285. [doi: 10.1109/CSAC.2005.13]

[7] McCune J, Berger S, Cacerres R. Shamon: A system for distributed mandatory access control. in: Proc. of the 22nd Annual Computer Security Applications Conf. Miami Beach, 2006. 23−32. [doi: 10.1109/ACSAC.2006.47]

[8] Radhakrishnan M, Solworth JA. Application security support in the operating system kernel. In: Proc. of the 2006 ACM Symp. on Information, Computer and Communications Security. 2006. [doi: 10.1145/1128817.1128848]

[9] Zhao QS, Sun YF, Liang HL, Zhang XF, Sun B. Research and enforcement of enhanced Chinese wall security policy. ACTA ELECTRONICA SINICA, 2002,30(11):1−5 (in Chinese with English abstract). [doi: 10.3321/j.issn:0372-2112. 2002.11.019]

[10] He YZ, Li XF, Feng DG. Implementing Chinese wall policies on RBAC. Journal of Computer Research and Development, 2007, 44(4):615−622 (in Chinese with English abstract).

[11] Cheng G, Jin H, Zou DQ, Zhao F. Chinese wall model based on dynamic alliance. Jounal on Communications, 2009,30(11):93−100 (in Chinese with English abstract). http://dx.chinadoi.cn/10.3321/j.issn:1000-436X.2009.11.012

[12] Shen CX. Structure the security guarantee framework of active defence. China Information Review, 2003,(10):50−51 (in Chinese with English abstract)

[13] Zhao Y, Liu JQ, Han Z, Shen CX. The application of information leakage defendable model in enterprise intranet security. Journal of Computer Research and Development, 2007,44(5):761−767 (in Chinese with English abstract).

[14] Kessler V. On the Chinese wall model. In: Proc. of the Computer Security (ESORICS'92). 1992. 41−54. [doi: 10.1007/ BFb0013891]

[15] Lin TY. Chinese wall security policy-an aggressive model. In: Proc. of the 5th Annual Computer Security Appfications Conf. Tucson, 1989. 282−289. [doi: 10.1109/CSAC.1989.81064]

[16] Lin TY. Chinese wall security model and conflict analysis. In: Proc. of the 24th IEEE Computer Society Int'l Computer Software and Applications Conf. 2000. 25−27. [doi: 10.1109/CMPSAC.2000.884701]

© 中国科学院软件研究所 http://www.jos.org.cn

[17] Katsuno Y, Watanabe Y, Furuichi S, Kudo M. Chinese wall process confinement for practical distributed coalitions. In: Proc. of the 12th ACM Symp. on Access Control Models and Technologies. 2007. 225−234. [doi: 10.1145/1266840. 1266876]

[18] Jaeger T, Sailer R, Sreenivasan Y. Managing the risk of covert information flows in virtual machine systems. In: Proc. of the 12th ACM Symp. on Access Control Models and Technologies. Sophia Antipolice, 2007. 81−90. [doi: 10.1145/1266840. 1266853]

[19] Burdonov I, Kosachev A, Iakovenko. Virtualization-Based separation of privilege: Working with sensitive data in untrusted environment. In: Proc. of the 1st Eurosys Workshop on Virtualization Technology for Dependable Systems (VTDS 2009). 2009. 1−6. [doi: 10.1145/1518684.1518685]

[20] Saltzer JH, Schroeder MD. The protection of information in computer systems. Proc. of the IEEE, 1975,63(9):1278−1308. [doi: 10.1109/PROC.1975.9939]

**附中文参考文献:**

[9] 赵庆松,孙玉芳,梁洪亮,张相锋,孙波.“长城”安全政策的扩充研究及其实现.电子学报,2002,30(11):1−5. [doi: 10.3321/j.issn:0372-2112.2002.11.019]

[10] 何永忠,李晓峰,冯登国.RBAC 实施中国墙策略及其变种的研究.计算机研究与发展,2007,44(4):615−622.

[11] 程戈,金海,邹德清,赵峰.基于动态联盟关系的中国墙模型研究.通信学报,2009,30(11):93−100. http://dx.chinadoi.cn/10.3321/j.issn:1000-436X.2009.11.012

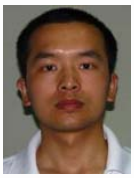
[12] 沈昌祥.基于积极防御的安全保障框架.中国信息导报,2003,(10):50−51.

[13] 赵勇,刘吉强,韩臻,沈昌祥.信息泄露防御模型在企业内网安全中的应用.计算机研究与发展,2007,44(5):761−767.

**马俊**(1982－),男,湖北枣阳人,博士,助理研究员,CCF 会员,主要研究领域为数据安全.

**伍江江**(1982－),男,博士生,主要研究领域为信息安全,数据备份与恢复.

**王志英**(1956－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为信息安全,先进计算机体系结构,微处理器设计技术研究,异步电路设计技术.



**程勇**(1986－),男,博士生,主要研究领域为网络与信息安全.

**任江春**(1979－),男,博士,副教授,主要研究领域为可信计算,信息安全.

**梅松竹**(1985－),男,博士生,主要研究领域为信息安全.

© 中国科学院软件研究所 http://www.jos.org.cn