第 33 卷 第 9 期 计 算 机 工 程 2007 年 5 月
Vol.33 No.9 Computer Engineering May 2007
·博士论文· 文章编号：1000—3428(2007)09—0052—03 文献标识码：A 中图分类号：TP309

基于 Chinese Wall 安全策略的职责分离模型

林宏刚[1,2]，戴宗坤[1]
(1. 四川大学信息安全研究所，成都 610064；2. 四川大学数学学院，成都 610064)

摘 要：职责分离是一个系统最基本的防止欺骗和错误的手段。该文在 Chinese Wall 安全策略的基础上，实现了一种基于历史记录的职责分离模型，通过跟踪用户的历史权限记录来决定用户当前分配的权限从而实现职责分离，并对其进行了形式化描述和分析，证明其满足职责分离安全原理。该模型继承了 Chinese Wall 策略和职责分离安全原则的优点，能够提供更加完善的访问控制策略。
关键词：职责分离；Chinese Wall；角色冲突

Separation of Duty Model Based on Chinese Wall Security Policy

LIN Honggang[1,2], DAI Zongkun[1]
(1. Information Security Institute, Sichuan University, Chengdu 610064; 2. School of Mathematics, Sichuan University, Chengdu 610064)

【Abstract】Separation of duty (SoD) is a fundamental means for prevention of fraud and errors. Based on the Chinese wall security policy, a model of history-based separation of duty is implemented and it tracks the history of user's previous permissions record, from which the current permissions assigned to can be determined. The formal description and analysis about the model has been done and the model has been proved a well in accordance with principle of SoD. The model inherits the advantage of Chinese Wall security policy and separation of duty, and provides a more perfect access control stratagem.
【Key words】 Separation of duty(SoD); Chinese Wall; Conflict role

1 概述

在大型应用系统中，系统安全策略要求用户不能拥有超出职位应有的访问权限，而且必须尽量减少同一个用户同时分配多个权限而产生欺骗行为的现象，职责分离原则能满足这一要求。

职责分离原则是用来阐明当需要两个或多个不同的用户对完成一个交易或相关的交易负责时，对多用户控制的安全原则，它要求两个或两个以上的用户对一个任务或一系列相关任务的完成负责，通过将完成一项任务所需的权力和相应的责任分散给多个人来减少犯罪和差错，以保证多用户协同工作的安全性。职责分离原则被广泛地用于各种领域，但在计算机系统中的应用还是一项较新的课题。Clark和Wilson强调职责分离机制在商业活动中的重要性，把它作为确保数据完整性重要机制之一； Nash和Poland[1]提出了基于对象的职责分离，强调一个对象上的每个事务由不同用户处理；Sandhu[2]在基于角色访问控制模型(RBAC)中提出了职责分离的概念，将职责分离分为静态职责分离和动态职责分离；Ferraiolo[3]提出操作上的职责分离，作为静态、动态职责分离的补充，要求没有一个角色具有完成一个业务过程所必需的所有操作权限，Simon和Zurko[4]列举了不同形式的职责分离约束，以非形式化的实现给出了各种约束的定义。

本文在分析各种实现职责分离安全原则方法的基础上，基于 Chinese Wall 安全策略，把基于对象的职责分离与基于操作的职责分离相结合，实现一种基于历史的职责分离模型，利用 Chinese Wall 安全策略的基本特性，保留每个用户历史权限记录，通过跟踪历史权限记录来判断用户当前获取权限请求是否违背职责分离模型的约束以达到职责分离的目的。该模型能够提供更加完善的访问控制策略，更好地满足实际的安全需求。

2 Chinese Wall安全策略

Chinese Wall安全策略最早是由Brewer和Nash[5]根据现实的商业策略模型提出，把所有单位的信息分在３个层次存储，底层是单个的数据对象，对应上一层是相应的单位数据集合(Company Data, CD)，最上层是根据利益冲突分类的COI类(Conflict of Interest, COI)，每个单位只能属于一个COI。初始时，一个用户可以访问任意COI类的单位数据CD，不存在访问强制限制。但是，一旦他做出了初始选择后，他就不能再访问该COI类的其它单位数据,即好似在CD周围建立了“ 城墙 ”。如图１所示，COI_1是相互竞争的机构的利益冲突类，其中CD_1是某个机构的数据集合，则当用户访问该机构的信息后，他就不能访问COI_1中其它单位信息，如CD_2，即图１中阴影部分。

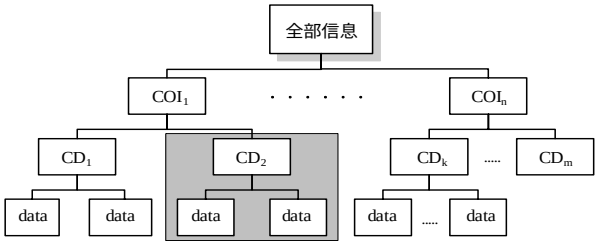


图 1 Chinese Wall 安全策略

可以类比 BLP 模型,定义 Chinese Wall 的策略规则如下：
(1)CW-简单访问规则：

作者简介：林宏刚(1976－)，男，博士生，主研方向：网络与信息安全；戴宗坤，研究员
收稿日期：2006-05-26 **E-mail：**linhonggang@126.com

主体 $s \in S$，只可在下列条件读取 $o \in O$：1)o和s以前读取的客体在同一个单位的数据集合内(即o在“墙内”)，或者 2)o属于s以前没有读取的任何数据信息的COI类(即o在“墙外”)。

(2)CW-*特性规则：

主体 $s \in S$，只可在下列条件写入 $o \in O$：1)CW-简单访问规则允许s读取的o，且 2)在其它COI类上不存在该主体可以读取的客体。

3 基于 Chinese Wall 安全策略的职责分离模型

Chinese Wall 安全策略保留每个主体历史访问记录，通过跟踪历史记录来判断主体是否违背 Chinese Wall 安全策略的约束，进而确认主体是否可以访问该数据集，随着主体访问客体数量的增多，Chinese Wall 安全策略对主体访问约束也不断增强。本文正是利用 Chinese Wall 安全策略这种特性，基于 CW-简单访问规则构建一个基于历史的职责分离模型。

3.1 职责分离模型实现

定义 1 用户：一个可以独立访问计算机系统中的数据或用数据表示其它资源的主体，用 U 表示用户的集合。

定义 2 权限：对计算机系统中的数据或用数据表示其它资源进行访问的许可。用 P 表示一个权限的集合。

定义 3 角色：一个组织或任务中的工作或位置，它代表一种资格，权力和责任。用 R 表示一个角色的集合。

定义 4 权限配置：P 和 R 之间的一个二元关系，假定 $PA \subseteq P \times R$ 是一个权限配置关系集合，那么 $(p,r) \subseteq PA$ 表示角色 r 拥有权限 p。

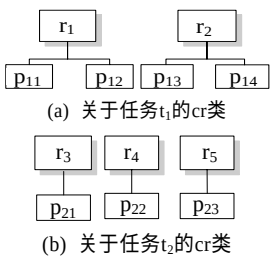
定义 5 权限函数：perm 为 $R \to 2^p$ 角色和配置给它的权限之间的映射函数，$perm(r_i) = \{p \in P \mid (p, r_i) \in PA\}$。

定义 6 安全条件：职责分离的目的是防止一个用户执行需要两个或者更多用户才能执行的任务，从而防止用户欺诈行为。如果一个任务包含多个权限，则需要将权限分配给两个或多个角色。

定义 7 冲突角色：完成同一个任务的不同角色之间互为冲突角色。

定义 8 角色冲突类：包含某个任务的所有冲突角色的集合。用 cr 表示某个任务的角色冲突类，CR 表示所有角色冲突类的集合。

根据安全条件的定义，我们把完成一个任务的权限分离，如可以把任务 t_1 的权限划分为 $P_1 = \{p_{11}, p_{12}, p_{13}, p_{14}\}$，任务 t_2 的权限划分为 $P_2 = \{p_{21}, p_{22}, p_{23}\}$。在安全条件下，需要将权限分配给两个或多个角色，完成同一个任务的角色集合构成关于这个任务的角色冲突类 cr。例如可以把任务 t_1 的权限 $P_1 = \{p_{11}, p_{12}, p_{13}, p_{14}\}$ 分给 r_1 和 r_2，$perm(r_1) = \{p_{11}, p_{12} \mid p_{11}, p_{12} \in P_1\}$，$perm(r_2) = \{p_{13}, p_{14} \mid p_{13}, p_{14} \in P_1\}$，$r_1$ 和 r_2 互为冲突角色，构成一个关于任务 t_1 的角色冲突类 cr。由此，可以得出一个基于 Chinese Wall的职责分离模型，如图 2 所示。



(a) 关于任务 t_1 的cr类

(b) 关于任务 t_2 的cr类

图 2 基于 Chinese Wall 安全策略的职责分离模型

3.2 职责分离模型形式化描述

设U为用户集，P为权限集，定义映射函数：$l_1 : P \to CR$ 和 $l_2 : P \to R$。定义访问控制矩阵 $\{H(u,p) \mid u \in U, p \in P\}$，如果矩阵元素值为真，表示 u 有权或曾经有权获取权限 p。Re(u,p) 表示 u 获取权限 p 的请求。

公理 1 对于所有的 $p, p' \in P$，如果 $l_2(p) = l_2(p')$，则 $l_1(p) = l_1(p')$。

由公理 1 可得到以下结论：

推论 对于所有的 $p, p' \in P$，如果 $l_1(p) \neq l_1(p')$，那么 $l_2(p) \neq l_2(p')$。

公理 2 用户 $u \in U$ 能获取权限 p，当且仅当对于所有的 $p' \in P$，使得 $H(u,p') = true$，有 $l_1(p) \neq l_1(p')$ 或 $l_2(p) = l_2(p')$。

这条公理就是职责分离公理：一个用户可获取某个权限，当且仅当它没有获取该权限所在 cr 类的其它冲突角色中的权限，或者它曾经获取过该权限所在冲突角色中的其它权限。

在最初用户被分配的权限是任意的，随着用户被分配的权限的增加，职责分离模型的约束也不断发展。根据公理 2 对图 2 职责分离模型作进一步分析，可以发现职责分离公理影响着对用户的权限分配：

(1)一旦用户被分配某一个cr中的任何一个权限，那么这个用户在该cr中能被分配的权限只能局限于先前所被分配的权限所对应的角色中的其它权限。例如，用户 u_1 分配了图 2 中权限 p_{11}，他就只能被分配 r_1 下的权限 p_{12}，而不能被分配该cr中其它角色所对应的权限了。上述规则的形式化描述可以由定理 1 给出。

定理 1 假设用户 $u \in U$ 曾经获取了权限 $p \in P$，如果 u 还可以获取权限 $p' \in P$，$p' \neq p$，则 $l_1(p') \neq l_1(p)$ 或者 $l_2(p') = l_2(p)$。

证明 反证。假设 u 已经获取了权限 p、p’，根据假设有

$$l_1(p) = l_1(p') \wedge l_2(p) \neq l_2(p') \tag{1}$$

不失一般性，假设 u 先获取了权限 p，那么当 u 获取权限 p’时，根据公理 2 有

$$l_1(p) \neq l_1(p') \vee l_2(p) = l_2(p') \tag{2}$$

由式(1)、式(2)可得

$$(l_1(p) = l_1(p') \wedge l_2(p) \neq l_2(p')) \wedge (l_1(p) \neq l_1(p') \vee l_2(p) = l_2(p')) \tag{3}$$

等价于

$$\begin{aligned}&(l_1(p) = l_1(p') \wedge l_2(p) \neq l_2(p') \wedge (l_1(p) \neq l_1(p')) \vee \\ &(l_1(p) = l_1(p') \wedge l_2(p) \neq l_2(p') \wedge l_2(p) = l_2(p'))\end{aligned} \tag{4}$$

但由于 $l_1(p) = l_1(p') \wedge (l_1(p) \neq l_1(p')$ 为假，且 $l_2(p) \neq l_2(p') \wedge l_2(p) = l_2(p')$ 也为假，因此式(4)为假，这与假设矛盾。因此，假设是错误的，原结论成立。

(2)在同一个cr中，一个用户最多只能被委派一个角色。例如，如果用户 u_1 被委派了图 2 中的角色 r_1，他就不能再被委派的角色 r_2。规则的形式化描述可以由定理 2 给出。

定理 2 假设用户 $u \in U$ 曾经获取了权限 $p \in P$，存在 $p' \in P$，有 $l_1(p') = l_1(p)$ 且 $l_2(p') \neq l_2(p)$，则 u 不能获取权限 p’。

证明 最初 u 没有任何权限，由公理 2 可得，对于任何权限的获取都会被许可，该定理得证。考虑另一个权限 p’，由定理 1 可得，如果 u 还可以获取权限 $p' \in P$，$p' \neq p$，则 $l_1(p') \neq l_1(p)$ 或者 $l_2(p') = l_2(p)$，其逆否命题就是 $l_1(p') = l_1(p)$ 且 $l_2(p') \neq l_2(p)$，u 不能获取权限 $p' \in P$，定理得证。

(3)在同一个cr中，完成一个任务所需的用户最小数目等于该cr中冲突角色的数目，即将完成任务权限分配的角色个

数。如图 2 所示，任务t_1至少需要 2 个不同的用户才能完成。规则的形式化描述可以由定理 3 给出。

定理 3 设 $r \in R$ ，$cr \in CR$,假设存在有 n 个满足 $l_1(p_i)=cr(1\le i\le n)$ 且 $l_2(p_i)\ne l_2(p_j)(1\le i,j\le n)$ 的权限 $p_i \in P(1\le i\le n)$ ，那么对于这样的 p，必定有一个用户 $u\in U$ 可以获取 p 当且仅当 $n\le|U|$ 。

证明 由公理 2 可得，如果 u 获取权限 $p\in P$ ，u 不能获取权限 p’，如果有 $l_1(p')=l_1(p)$ 且 $l_2(p')\ne l_2(p)$ 。由于 CR 中有 n 个这样的权限 p’,因此至少必需 n 个不同用户来满足条件。

在实际应用中，许多任务都包含有公共权限，这些权限对所有的用户都是可以拥有的，在模型中不考虑对此类权限的约束。

3.3 职责分离模型安全分析

为了判断系统是否违反了职责分离，根据安全条件，Kuhn[6]定义了安全状态，就是完成任何一个关键任务所需的权限不能被一个用户所拥有。形式化描述如下：

职责分离安全原理 $c(t):task\to 2^p$ ，完成任务 t 所需的权限的集合。

$$\forall u\subset U,\forall t\subset T,c(t)\not\subset \bigcup_{r\in role(u)} perm(r)$$

其中， $\bigcup_{r\in role(u)} perm(r)$ 表示分配给用户 u 的所有角色的权限的并集。

可证明上述职责分离模型满足这个职责分离安全原理。

证明 反证法。假设安全原理不满足，那么必然存在某些用户被分配了完成某项任务的所有权限。

$$\exists u\in U,\exists t\in T,c(t)\subseteq \bigcup_{r\in role(u)} perm(r) \quad (5)$$

由于 c(t)表示完成任务 t 所需的全部权限，那么根据安全条件，c(t)必然被划分成至少 2 个角色，则有

$$c(t)=perm(r_1)\cup perm(r_2)\cup ...$$

为简化证明，假设任务 t 委派给 2 个角色，即

$$c(t)=perm(r_1)\cup perm(r_2)$$

则式(5)可以表示为

$$\exists u\in U,\exists t\in T\ ,\ perm(r_1)\cup perm(r_2)\subseteq \bigcup_{r\in role(u)} perm(r) \quad (6)$$

r_1 和 r_2 的权限都在 $\bigcup_{r\in role(u)} perm(r)$ ，假设 $p_1\in perm(r_1)$ ，$p_2\in perm(r_2)$ ，由式(6)可得

$$p_1\in \bigcup_{r\in role(u)} perm(r) \ ,\ p_2\in \bigcup_{r\in role(u)} perm(r) \quad (7)$$

而r_1和r_2是完成同一任务的冲突角色，必有

$$l_1(p_1)=l_1(p_2) \text{ 且 } l_2(p_1)\ne l_2(p_2) \quad (8)$$

与定理 2 矛盾，假设不成立。所以，职责分离模型满足职责分离安全原理。

4 总结

职责分离是一个系统基本防止欺骗和错误的安全原则，被广泛地用于各种领域。本文深入研究各种实现职责分离安全原则的方法，基于 Chinese Wall 安全策略，实现了一种基于历史记录的职责分离模型，对其进行了形式化描述和分析，并证明了其安全性。该模型既继承了 Chinese Wall 策略的优点，又体现出职责分离安全原则，能够提供更加完善的访问控制策略。处理模型中角色间的继承关系是今后工作的一个重要研究方向。

参考文献

1 Nash M, Poland K. Some Conundrums Concerning Separation of Duty[C]//Proceedings of the Symposium on Security and Privacy. IEEE Computer Society Press, 1990: 201-207.

2 Sandhu R, Coyne E, et al. Role-based Access Control Models[J]. IEEE Computer, 1996, 29(2): 38-47.

3 David F, Ferraiolo D, Kuhn R, et al. Role Based Access Control: Features and Motivations[C]//Proceedings of Computer Security Applications Conference. IEEE Computer Society Press. 1995: 241-248.

4 Simon R, Zurko M. Separation of Duty in Role-based Environments[C]//Proceedings of the 10th IEEE Computer Security Foundations Workshop. IEEE Press, 1997: 183-194.

5 Brewer D, Nash M. The Chinese Wall Security Policy[C]//Proc. of the IEEE Symposium on Security and Privacy. IEEE Computer Society Press, 1989: 206-214.

6 Kuhn D R. Mutual Exclusion of Roles as a Means of Implementing Separation of Duty in Role-based Access Control Systems[C]// Proceedings of the 2nd ACM Workshop on Role-based Access Control. ACM Press, 1997: 23-30.

（上接第 11 页）

4 结论

综上所述，采用传统的基于 Johnson 假设的方法计算雷达景象匹配概率，由于安装在飞行器上的实孔径雷达图像质量比较差，图像中含有较多的斑点噪声，图像中的伪信息较多，其计算结果和实际匹配情况不相符。运用基于贡献像元数的匹配概率数学模型所得出的匹配概率和实际匹配结果是一致的。今后的进一步研究工作是，继续深入研究雷达图像成像特点，总结归纳出雷达图像的概率密度分布规律，从而推导出匹配定位概率的数学模型。

参考文献

1 孙仲康, 沈振康. 数字图像处理及其应用[M]. 北京: 国防工业出版社, 1985.

2 Stephen P E, Robert T G. Quantitative Evaluation of Rank-order Similarity of Images[C]//Proc. of International Conference on Image Processing. 2000.

3 Jason F R, Scott S. Scene-referenced Object Localization[C]//Proc. of Signal Processing Sensor Fusion and Target Recognition. 2004.

4 Amir A, Richard C, Ramesh H. Overlap Matching[J]. Information and Computation, 2003, 181(1): 57-74.