安全政策格及一个格的修正*)

石文昌
(中国科学院软件研究所　北京100080)

摘　要　对安全政策灵活性的支持是现代安全操作系统追求的重要目标，安全政策格为安全政策灵活性的研究提供了一个很好的手段。本文通过分析DTOS项目的研究成果讨论安全政策格的基本思想，介绍DTOS项目中设计的一个安全政策格，并针对该安全政策格中存在的问题给出一个修正结果。
关键词　计算机安全，安全政策，安全政策格，安全操作系统

Security Policy Lattice and the Modification of a Lattice

SHI Wen-Chang
(Institute of Software, Chinese Academy of Sciences, Beijing 100080)

Abstract　To support the flexibility of security policies is an important goal of modern secure operating systems. Security policy lattice provides a good way for the research on the flexibility of security policies. Through the analysis of research results achieved in the Distributed Trusted Operating System (DTOS) project, this paper discusses the fundamental concept of security policy lattice, introduces a practical security policy lattice designed in the DTOS project, and presents a modification to that security policy lattice to eliminate an incorrectness existsing in it.
Keywords　Computer security, Security policy, Security policy lattice, Secure operating system

1　引言

安全操作系统的发展进入多政策时期[1,2]之后，面临的一个突出问题是多种不同的安全政策在同一个系统中的共存，因为不同的用户群体、不同的应用环境、不同的安全威胁，要求安全操作系统必须能够灵活地对范围广阔的各种安全政策进行支持。这样，剖析和表达安全政策之间的关系就成了一个迫切的需要，安全政策格就是顺应这种需要而诞生的思想。

美国国家安全局支持的DTOS[3]项目对安全政策的特征进行了划分，提出了安全政策格(lattice)的思想[4]，通过格的结构描述多种安全政策之间的关系和系统安全机制对安全政策的支持能力，为安全政策灵活性的研究提供了一个很好的手段。

本文通过分析DTOS项目的研究成果讨论安全政策格的基本思想，介绍DTOS项目中设计的一个安全政策格，并针对该安全政策格中存在的问题给出一个修正结果。

2　安全政策格的基本思想

一个格是一个偏序集，集合中任意两个元素都有一个最小上界和一个最大下界。安全政策格是由安全政策的特征集构成的格，格中的每一个元素(也称为节点)是安全政策的一个特征集，格中的关系称为支配(dominance)关系，其实际内涵由集合的包含关系定义。

从严格的意义上说，安全政策与安全政策模型是两个既有联系又有区别的概念，但在安全政策格的意义上，我们没有必要考虑它们之间的区别，在本文的讨论中，它们被视为相同的概念。

安全政策可以放到安全政策格的节点上，定位方法是，在安全政策格中找出一个特征集等于安全政策所具有的特征的集合的节点，该节点就是为相应安全政策确定的位置。

安全系统(或者子系统，统称为系统)也可以放到安全政策格的节点上，定位方法与安全政策的定位方法相似，要求是格节点的特征集等于安全系统所能支持的安全特征的集合。

安全政策格的重要意义是为剖析安全系统对安全政策的支持能力提供了一个非常有效的途径。

一方面，把安全系统定位到安全政策格节点上，有助于确定安全系统应支持的安全政策的特征。把一个安全系统定位到节点 N 上，意味着该安全系统将支持位于节点 N 所支配的所有节点(包括节点 N)上的每一个安全政策。

另一方面，把安全政策与安全政策格节点对应起来，有助于发掘重要的安全政策特征，为以支持安全政策灵活性为设计目标的安全系统的设计提供更充足的素材。

再一方面，在安全政策格结构的基础上开展工作，可以降低安全系统分析的复杂性。对支持 p 个安全政策的 m 个安全系统进行分析，其复杂性可由 $O(mp)$ 降低为 $O(m+p)$。

3　安全政策特征

根据安全政策格概念的定义，显然，确定安全政策的特征是构造安全政策格的关键。安全政策的特征可以划分为输入特征、敏感性特征、撤权特征和传递性特征等四大类。

3.1　输入特征

进行安全判定需要有判定依据，提供给安全判定子系统的判定依据属于输入信息。对于一次安全判定来说，在判定依据的信息数量方面，很多安全政策之间是有区别的。例如，类型裁决(TE)政策[5]只需要两个安全属性作为判定依据，一个是域属性，一个是类型属性。而Clark-Wilson政策[6]所需要的安全属性的数量是不确定的，其形式是：

$(UserID, TP, (CDI_1, CDI_2, \cdots, CDI_n))$

其中，$UserID$ 是用户标识，TP 是转换过程，CDI 是受控制的数据项，n 是不确定的，由实际请求决定。

在安全政策格的研究中，用 C 表示用于一次安全判定的安全属性个数，对于像TE这样的政策，我们说 $C=2$，对于像Clark-Wilson这样的政策，我们说 $C>2$。

在安全判定的依据中，除了安全属性外，还可以有对所请

*)国家863高技术研究发展项目(2002AA141080)和国家自然科学基金项目(60073022)资助。石文昌　博士，研究员，主要研究方向为计算机安全与系统软件。

求的操作进行描述的其它数据。例如，当一个主体请求改变自己的调度优先级时，主体指定的优先级就属于这类数据。如果一个安全政策的安全判定需要考虑这类信息，我们就称这个安全政策为带参量的(parametric)安全政策。

3.2 敏感性特征

提供给安全判定子系统的输入信息(即，安全属性和参量)是影响安全判定的主要因素，然而，有些安全政策的安全判定还会受到其它信息的影响。对于这样的安全政策，我们说它们对其它信息是敏感的，是敏感的安全政策。由于这种对其它信息的敏感性的作用，在不同的背景下，就算提供相同的输入信息，也可能产生不同的安全判定结果。

相对而言，安全判定只依赖于输入信息的安全政策则属于非敏感的安全政策，称为静态安全政策。非静态的安全政策就称为动态安全政策。

中国墙政策[7]就是一个动态安全政策。该政策采用两级分组方法，首先把客体按照公司进行分组，再把公司按照利益冲突类进行分组。在初始状态，一个用户可以对系统中的所有文件进行读访问，然而，当用户 u 对文件 f 进行了读访问之后，该用户就失去了对其它一些文件进行读访问的能力，这些文件属于文件 f 所属的利益冲突类但不属于文件 f 所属的公司。这样，对文件 f 进行读访问的副作用使得用户 u 失去了对其它相关文件进行读访问的能力。这就是说，中国墙政策对读访问操作的历史是敏感的。

安全政策的敏感性可进一步分为历史敏感性、环境敏感性、自主敏感性和弃权敏感性等四种类型。

与中国墙政策一样，很多安全政策对访问操作的历史是敏感的，即，以前的访问操作对以后的安全判定会产生副作用，这种敏感性称为历史敏感性。推广到更一般的情形，如果在一个安全政策中，以前的服务请求的执行对以后的安全判定会产生副作用，则就说这个安全政策具有历史敏感性。

有的安全政策对时间或系统工作方式之类的因素是敏感的，这种敏感性称为环境敏感性。时间因素的例子是，在5PM至9PM之间禁止进行写访问。系统工作方式的例子有训练方式、正常方式和应急方式等。

在有的安全政策中，如IBAC政策[4,8]等，用户可以请求改变与该用户所拥有的客体有关的判断准则，比如，用户 u_1 可以授权用户 u_2 访问由用户 u_1 拥有的文件 f，这样的安全政策称为自主安全政策，相应地，我们说它们具有自主敏感性。

进程可以请求获得某项未拥有的权限，当然也可以放弃某项已拥有的权限。例如，当一个进程关闭一个文件时，该进程就放弃了对该文件的所有访问权限。真正的弃权效应将意味着在提出新的权限申请之前该进程不可能再打开已关闭的文件。如果一个安全政策的安全判断会受到放弃权限的行为的影响，则称该安全政策具有弃权敏感性。

3.3 撤权特征

把先前已经授予的权限撤消掉是很多动态安全政策需要的能力，需要这种能力的安全政策称为具有撤权特征的安全政策。应该注意，这里只关心已经授予的权限，并不关心未曾授予的权限。清除一项可以授予的但并未曾授予的权限，不会使一个安全政策具有撤权特征。

以中国墙政策为例，设文件 f_1 与 f 属于同一个利益冲突类，但不属于同一个公司，u 是一个用户。在初始状态，“u 读 f_1”是一项可以授予的权限。当用户 u 读文件 f 时，“u 读 f_1”便变成了一项不可授予的权限。至此，“u 读 f_1”权限显然已被清除，但该权限并不属于已经授予的权限，所以，这种清除权限的作用与撤权特征无关。

撤权与弃权有相似之处，结果都是失去权限。但是，撤权是安全政策强行撤消进程的权限，而弃权是进程自愿放弃权限。

3.4 传递性特征

在一个系统中，多个主体有可能联合起来获取系统中的信息或影响系统的状态，这是定义安全政策时需要注意的问题。

以MLS政策为例，主体写客体的条件是客体的安全等级支配主体的安全等级。由于安全等级的支配关系具有传递性，因此，写权限也具有传递性。设等级A的主体能够写等级B的客体，等级B的主体能够写等级C的客体，那么，等级A的主体就能够写等级C的客体。读的情况也相似。

以上类型的安全政策称为具有传递性特征的安全政策。一般地，在一个具有传递性的安全政策中，如果主体 A 能够修改数据项 d_A，主体 B 能够检测到 A 对 d_A 的修改，并且，B 能够修改数据项 d_B，那么，A 也能够修改 d_B。

安全政策具有传递性并不是一件好事情，所以，传递性不是安全政策中需要的特征，安全政策中需要的是不可传递性特征。

4 基于特征的安全政策分类

借助以上讨论的安全政策特征，文[4]对MLS政策、TE政策、IBAC政策、Clark-Wilson政策、动态N-人政策[4,9]、ORCON政策[4,10]和中国墙政策等著名安全政策进行了分类。在分类过程中，也对这些安全政策的一些变种进行了讨论，这些变种是非撤权的IBAC政策、零碎的Clark-Wilson政策、零碎的动态N-人政策、上锁的ORCON政策和静态中国墙政策等。分类结果如表1所示。

表1 若干著名安全政策的特征

安全政策		输入特征		敏感性特征					撤权特征	传递性特征	DTOS支持
		C>2	带参量的	动态/静态	自主的	历史的	环境的	弃权的			
MLS/BLP				静						√	Y
Biba				静						√	Y
类型裁决(TE)				静							Y
IBAC	撤权的			动	√				√*rew*		N_b
	非撤权的			动	√						Y
Clark-Wilson	完全的	√		静							N_a
	零碎的			动		√*we*					Y
动态N-人	完全的	√		动		√*e*					N_a
	零碎的			动		√*we*					Y
ORCON	完全的			动		√*rwe*			√*re*		N_b
	上锁的			动		√*rew*		√			N_c
中国墙	完全的			动		√*rw*					Y
	静态的	√		静							N_a

r：读，*w*：写，*e*：执行，在历史敏感性栏中，表示与敏感性相关的操作，在撤权特征栏中，表示应撤消的权限。Y表示DTOS系统支持相应的政策，N表示不支持，下标说明不支持的原因，即，N_a：因为一个请求中的安全标识符个数不确定，N_b：因为需要撤权，N_c：因为弃权敏感性。√表示拥有相应特征。

5 DTOS安全政策格及其修正结果

在第4节给出的分类结果的基础上，文[4]构造了DTOS安全政策格。DTOS安全政策格的最底层节点的安全政策特征集为空集，表示不含安全政策特征的安全政策。紧接着的一层节点的安全政策特征集均含一个安全政策特征，表示仅含一个安全政策特征的安全政策，它们支配最底层节点。DTOS安全政策格的一个局部结构如图1所示。

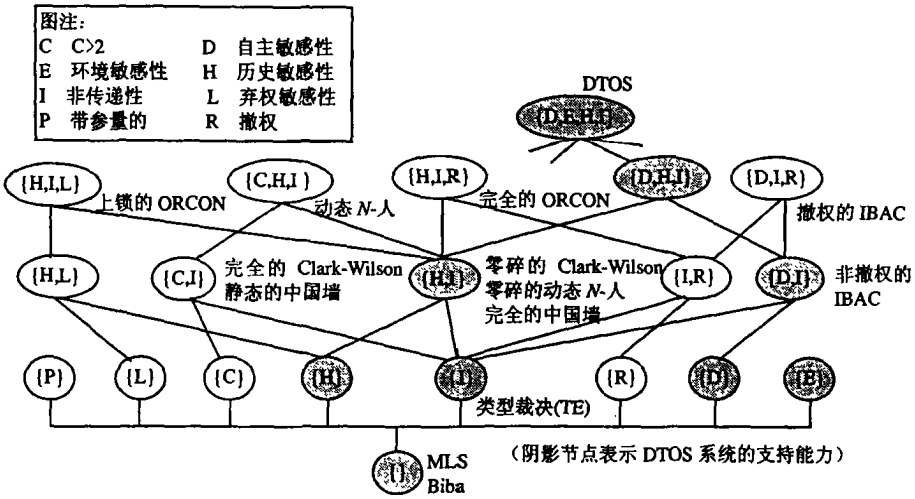

图1 DTOS 安全政策格的一个局部结构

在 DTOS 安全政策格中,多级安全性(MLS)政策被认定为是静态安全政策,表1清楚地反映了这个结论。然而,这只是 MLS 安全政策在常规实施方法中的体现。我们可以为 MLS 安全政策设计一种适应性实施方法(称为 ABLP 实施方法),使 MLS 安全政策具有历史敏感性[11],进而,具有动态特征。由此可见,DTOS 安全政策格中对 MLS 安全政策的处理是不合理的。

为了克服 DTOS 安全政策格在处理 MLS 安全政策问题上的不合理性,我们把 MLS 安全政策分成两种情形处理:常规 MLS 和 ABLP 式 MLS。采取这种方法,我们对图1给出的安全政策格的局部结构进行修正后得到的结果如图2所示。

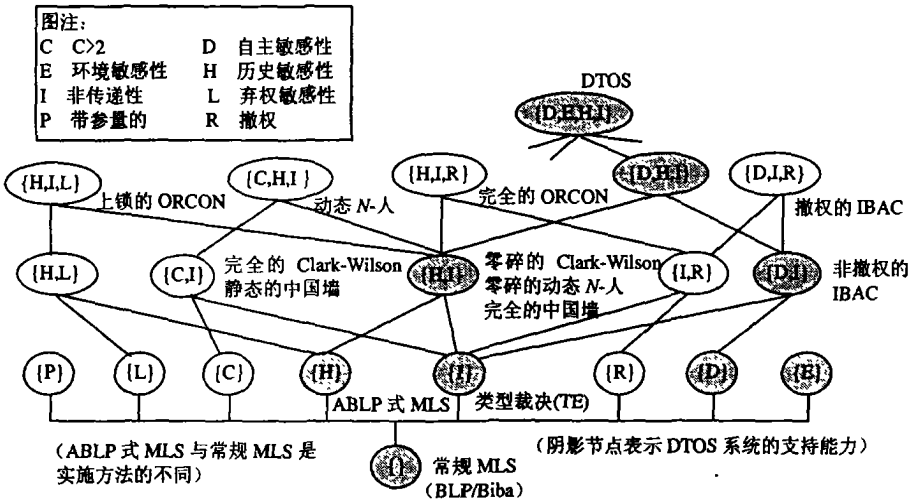

图2 修正后的 DTOS 安全政策格的局部结构

结束语 对安全政策灵活性的支持是现代安全操作系统追求的重要目标,刻画多种安全政策之间的相互关系是为了实现这样的目标而无法回避的迫切需要,这种需要是食谱时期的开发范型所无需面对的,是进入多政策时期后出现的新的挑战,安全政策格是在这种需要的驱使下诞生的。本文对安全政策格的基本思想进行了讨论。

文[4]提出了安全政策格的思想,并构造了一个描述若干著名安全政策之间关系的 DTOS 安全政策格,为多种安全政策的支持方法的研究建立了一个富有创新意义的有效途径。然而,在 DTOS 安全政策格中,MLS 政策被断定为静态安全政策,我们认为这个结论是不正确的。本文给出了 DTOS 安全政策格的一个修正结果。

参 考 文 献

1 石文昌,孙玉芳. 安全操作系统研究的发展(上). 计算机科学,2002,29(6):5~12
2 石文昌,孙玉芳. 安全操作系统研究的发展(下). 计算机科学,2002,29(7):9~12
3 Secure Computing Corporation. DTOS Lessons Learned Report. CDRL Sequence No. A008, Secure Computing Corporation, Roseville, Minnesota, Jun. 1997
4 Secure Computing Corporation. DTOS Generalized Security Policy Specification. DTOS CDRL A019, Secure Computing Corporation, Roseville, Minnesota, Jun. 1997
5 Badger L, Sterne D F, Sherman D L, et al. Practical Domain and Type Enforcement for UNIX. In: 1995 IEEE Symposium on Security and Privacy, 1995. 66~77
6 Clark D D, Wilson D R. A Comparison of Commercial and Military Computer Security Policies. In: Proc. 1987 IEEE Symposium on Research in Security and Privacy, Oakland, CA, USA, May 1987. 184~194
7 Brewer D F C, Nash M J. The Chinese Wall Security Policy. IEEE Symposium on Security and Privacy, Oakland, CA, USA, May 1989. 206~214
8 Woo T Y C, Lam S S. Authorization in Distributed Systems: A New Approach. Journal of Computer Security, 1993(2): 107~136
9 Nash M J, Poland K R. Some Conundrums Concerning Separation of Duty. IEEE Symposium on Security and Privacy, Oakland, CA, USA, May 1990. 201~207
10 Abrams M D. Renewed Understanding of Access Control Policies. In: Proc. of the 16th National Computer Security Conf. Baltimore, MD, USA, Sep. 1993. 87~96
11 石文昌,孙玉芳. 多级安全性政策的历史敏感性. 软件学报,2003,14(1):91~96