对军用安全模型的扩展

肖军模

(解放军理工大学通信工程学院 南京 210007)

【摘要】军用安全模型是一种适合于诸如政府部门、军队等涉密组织，信息系统内对信息流进行控制的多级安全模型，原理是依据线性格与子集格的乘积格实施信息流控制的，但所描述的关系在实际应用中存在着缺陷。新模型则利用敏感级格与组织内部的层次格的乘积格反映组织内部带敏感性的“层级”关系，然后再与信息的子集格相乘形成更为合理的访问控制与信息流控制关系，从而使其更适合于军队、政府部门或各类涉密组织的信息系统对信息和信息流的安全控制要求。

关 键 词 军用安全模型; 信息流策略; 多级安全; 格安全模型

中图分类号 TP309 文献标识码 A

Extension to Military Security Model

XIAO Jun-mo

(Institute of Communication Engineering ICE, PLAUST Nanjing 210007)

Abstract The military security model (MSM) is a multilevel security model which used to control information flows within an information system with secret (such as government department, military etc.) . In the old model, it depends on product lattice of linear lattice and subset lattice for information flow control. But relationships described in this model exists drawbacks in applications. In the new model, the product lattice which is a sensitivity lattice multiplying by organization level lattice is mapped to level relations with sensitivity within an organizations. Then, a more proper relationships which is multiplying the product lattice by lattice of information subset are formed for access control and flow control. So it make the new model more suitable to control the information flow security for information systems of military , government departments or various organizations.

Key words military security model; information flow police; multilevel security; lattice security model

军用安全模型是一种基于格理论的信息流安全模型，该种模型是文献[1,2]于1976年前后提出的，是一种应用非常广泛的安全模型，在文献[3]中给出了该模型的完整形式化描述，在文献[4，5]中对该模型作了全面介绍。涉密组织的信息系统是一个多级安全的保护系统，其中信息被划分为无密、秘密、机密和绝密四个互不相交的敏感级别，系统中的主体(用户、进程等)根据最小特权原则被赋予相应权限，并根据知其所需原则访问或使用信息，但可能包括不同级别的信息。这就是涉密组织信息系统中对信息流的控制要求，军用安全模型就能反映这种要求。但原模型的安全控制策略不能完全满足我国实际政府、企业等部门中对信息的访问与控制要求，本文将研究一种改进模型，并从原理上讨论军用模型存在的缺陷。

1 原模型的理论基础与缺陷

军用安全模型是利用线性格与子集格的乘积格来描述涉密组织信息系统的多级安全需求的。图1是由0、

收稿日期：2003 – 10 – 08
基金项目：国家自然科学基金资助项目(69931040)
作者简介：肖军模(1947 –)，男，教授，博士生导师，主要从事网络信息安全、软件工程方面的研究.

1组成的线性格和集合{*x*, *y*, *z*}的子集格的乘积。如果0和1分别代表无密和有密两个安全级别，*x*、*y*、*z*分别代表不同的信息内容，图1所示给出了一个最简单的军用安全模型。

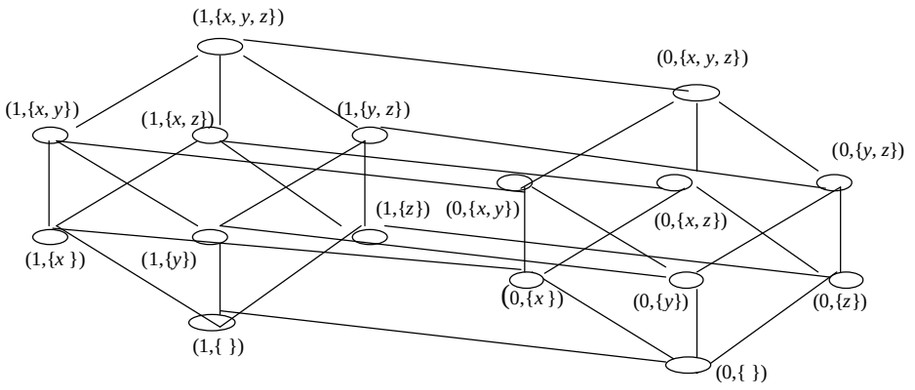

图 1　两个格的乘积

在实际系统中，线性格中包括绝密、机密、秘密和无密四个敏感级别，子集格则是由所有信息主题集合的子集组成的。在安全模型中每个格元素都是用二元组(*R*，*C*)表示的，其中*R*表示安全级别或职权的级别，*C*表示由信息主题组成的子集，简称信息子集。把这样的格元素称为一个安全类*SC*(security class)，*SC*表示安全类的集合。

在信息系统中信息流控制策略可用有限格(*SC*，≤)描述。如果sc_1、$sc_2 \in SC$，且$sc_1 \le sc_2$，则说明信息sc_1的安全类低于sc_2的安全类。对于子集格，关系≤表示子集间的包含关系。根据格的安全性策略一般是：只能允许信息在同一个类的内部或向高级别的类流动，但不允许流向低于自己级别的类或流向无关的类。

对安全类*sc*=(*R*，*C*)的含义有两种：一是针对系统中的访问对象，*C*表示信息范围，*R*表示该范围的密级；二是针对系统中主体(用户或进程)，*C*表示某个主体有权知道的信息范围，*R*表示该主体的职权等级。假定两个安全类分别为(R_1，C_1)和(R_2，C_2)，则在乘积格中以下结论成立：1) (R_1，C_1)≤(R_2，C_2)当且仅当$R_1 \le R_2$，$C_1 \subseteq C_2$；2) (R_1，C_1)⊕(R_2，C_2)= (max(R_1，R_2)，$C_1 \cup C_2$)；最小上界的安全类；3) (R_1，C_1)⊙(R_2，C_2)= (min(R_1，R_2)，$C_1 \cap C_2$)；最大下界的安全类；4) LOW= (1，{ })= (无密，{ })；格中最小安全类(幺元)；5) HIGH= (绝密，信息主题全集)；格中最大安全类。

在1)中规定的安全类之间的关系≤，用于限定一个主体可能访问的信息的敏感级和内容，它表明一个主体可以访问一个目标，仅当该主体的职权等级至少和该信息的敏感级别一样高，并且该主体需要知道该信息范围中所涉及到的所有信息内容。

根据关系≤所规定的原则，在图1中，安全类(1, {*z*})可以流向安全类(1, {*y*, *z*})和(1, {*x*, *z*})但不能流向安全类(1, {*x*, *y*})；尽管安全类(1, {*y*, *z*})和(1, {*x*, *z*})有相同的安全级，但它们的信息子集互不包含，所以这两个类之间没有关系。类(0, {*z*})和类(1, {*y*，*z*})和(1, {*x*, *z*})也应该有直接的连线，但图1中未给出，主要是为了使图更清晰。类似的情况对类(0, {*x*})和(0, {*y*})也有。

模型所反映的安全策略，不能完全满足实际系统的要求。例如，假定生产经理的安全类为(机密，{生产、进货、技术、工艺、奖金})和销售经理的安全类为(机密，{销售、市场、生产})，但根据上述安全策略的要求，他们之间不能有任何信息的交流。虽然生产经理和销售经理都知道生产方面的信息，但他们还是不能互相交谈的，即使这两个人在一起开会也不允许交谈，这在实际工作中是行不通的。这是军用安全模型的主要缺陷，另一种缺陷是该模型没有反映实际组织系统中的层次关系，应该允许生产经理与销售经理这样同级领导之间讨论他们共同知道的信息。造成这些缺陷基本原因是，军用安全模型是依据线性格和子集格的乘积格来实现信息流控制的，而线性格无法反映现实系统中层次与敏感级所形成的复杂关系。

2　对模型的扩展

在实际的涉密组织(如政府)系统中，每个主体(人)不仅被赋予敏感级，而且还被划分为不同的层次，例

如，被划分为高层、中层和基层领导以及职员4个层次(等级)。层次与敏感级未必是一一对应的，高层次的人未必都被赋予高的敏感级，低层次的人可能因工作需要而被赋予高敏感级。例如，机要员可以由低级人员兼任，但他可以掌握最高秘密的密码。为了使模型更加接近于实际系统，需要增加以下能力：1) 反映组织内部主体的“层级”关系；2) 允许同层同职权级人员之间交流他们共同知道的信息。

扩展后的模型可以半形式化地描述如下：设$S=(H, \leq)$是一个映射层级关系的线性格，$T=(R, \leq)$是一个映射敏感级关系的线性格，关系≤的意义如前所述，根据格的积代数概念，S和T的乘积形成一个新的格系统$G=(K, \leq)$，其中，集合K中的元素(h, r)是由层次h与权利r构成的偶对，且新格中的元素按照关系“≤”排序，$(h_1, r_1)\leq(h_2, r_2)$当且仅当$h_1\leq h_2$与$r_1\leq r_2$。例如，若$S=(\{0, 1\}, \leq)$，$T=(\{3, 4, 5\}, \leq)$，则新的格系统$G=(\{(1, 5), (1, 4), (1, 3), (0, 5), (0, 4), (0, 3), \leq\})$。显然$G$是一个非线性格。再设$L=(M, \leq)$是一子集格，其中$M$是信息子集的集合，则$G$与$L$的乘积格$G\times L=(K\times M, \leq)$便形成扩展后的军用安全模型，其中每个格元素(或称安全类)的形式是$((h, r), C)$，其中(h, r)的含义如上所述，$C\in M$是一个信息子集。设两个安全类分别为$((h_1, r_1), C_1)$和$((h_2, r_2), C_2)$，则以下结论成立：

1) $((h_1, r_1), C_1)\leq((h_2, r_2), C_2)$当且仅当$(h_1, r_1)\leq(h_2, r_2)$，$C_1\subseteq C_2$；

2) $((h_1, r_1), C_1)\oplus((h_2, r_2), C_2)=(\max((h_1, r_1), (h_2, r_2)), C_1\cup C_2)$；最小上界的安全类；

3) $((h_1, r_1), C_1)\odot((h_2, r_2), C_2)=(\min((h_1, r_1), (h_2, r_2)), C_1\cap C_2)$；最大下界的安全类；

4) $\mathrm{LOW}=(\min(H), \min(R)), \{\ \})$；最小安全类，$H$是层次级别集，$R$是敏感级别集；

5) $\mathrm{HIGH}=(\max(H), \max(R))$，信息全集$M$)；最大安全类，$H$、$R$同4)。

由(1)可知模型扩展后仍支持原先的信息流的安全策略。至此我们已经完成了上述扩展要求的第一个能力的扩展，扩展后的安全模型是由一个非线性格与一个子集格的乘积格描述的。对于第二个能力的扩展可根据以下原则进行：

1) 如果两个安全类之间存在关系$((h_1, r_1), C_1)\leq((h_1, r_2), C_2)$，则保持之；

2) 有关系的两个安全类$((h_1, r_1), C_1)$和$((h_1, r_2), C_2)$，如果$C_1\subseteq C_2$不成立，且$C_1\ \ C_2=P$，则在两个安全类之间建立一个关联，表示为：$((h_1, r_1), C_1)\overset{p}{\leftrightarrow}((h_1, r_2), C_2)$。

其中符号$\overset{p}{\leftrightarrow}$表示允许两个安全类之间交流信息子集$P$中的内容，$P$是$C_1$与$C_2$的交集。

如果两个格元素(安全类)之间允许关联，那么在格的哈斯图中这两个元素间用双向箭头的线连接，并在其上标记这两个格元素共同的信息子集。

由于两个安全类间所交流的信息是双方共知的，因此，不存在信息泄漏的问题。进一步讲，由于扩展并不改变各格元素之间原有的关系≤，因此也不会改变模型所描述的信息流策略。

3 新模型的应用

企业信息系统是一个典型的涉密信息系统，涉及到的信息种类很多，可以划分为不同的信息主题，如编制、生产、销售、制度、文化、培训、奖金、技术、工艺、市场、进货、项目、财务等。根据业务管理的需要，这些主题会被组合成不同的信息子集，并对应不同的敏感级别。

企业同时又是一个庞大的组织系统，由不同职能人员组成，如总管、总工、技术总监、销售经理、生产经理、办公室主任、会计等。根据最小特权原则，这些人只能管辖自己的业务；根据知其所需原则，他们需要知道的信息范围也是局限于自己业务范围。同时系统内的管理者是分层次的，如可以分为高层干部、中层干部、基层干部。根据业务工作需要，即使同一层次的人员接触信息的敏感级也可能不一样。层次级别的线性格与敏感级别的线性格的乘积形成了一个非线性格，其格元素可按序排列成下面的矩阵形式：

(高层，绝密) (高层，机密) (高层，秘密) (高层，无密)
(中层，绝密) (中层，机密) (中层，秘密) (中层，无密)
(基层，绝密) (基层，机密) (基层，秘密) (基层，无密)

其中左上角元素(高层，绝密)是最大元素，右下角元素(基层，无密)是最小元素。每一个元素表示一种层次与敏感级的搭配。例如，会计可分配为(基层，机密)的权利。在实际系统中，根据知其所需原则，需要根据每一个管理人员的权限规定他所能了解信息的范围。例如：

主体	权限等级	信息范围
1) 总　　管	(高层，绝密)	{全部信息}；
2) 总　　工	(高层，绝密)	{编制，生产、销售、市场、技术、进货、项目、培训、工艺}；
3) 技术总监	(中层，绝密)	{生产、项目、技术、培训、市场}；
4) 销售经理	(中层，机密)	{销售、市场、生产}；
5) 生产经理	(中层，机密)	{生产、进货、技术、工艺、奖金}；
6) 办公室主任	(中层，绝密)	{编制、制度、奖金、账目}；
7) 会　　计	(基层，机密)	{编制、奖金、账目}；
8) 普通职员	(基层，无密)	{工艺、技术}。

图2中给出了这8个格元素的相互关系，用虚线双箭头连接的各个元素(都表示中层干部)之间可以相互交流他们两两之间共同知道的信息，分别由子集*A*至*F*所限定，其中*B*与*F*是空集，说明元素6与3，4与6之间没有可以互相交流的共同信息，他们之间的关联可以不画出来。从该例子可以看出，虽然技术总监的敏感级高于生产经理的敏感级，但只允许他们之间交流他们都知道的生产与技术信息，所以并没有泄漏其他信息，因此模型扩展后并没有破坏原有的信息流安全策略。

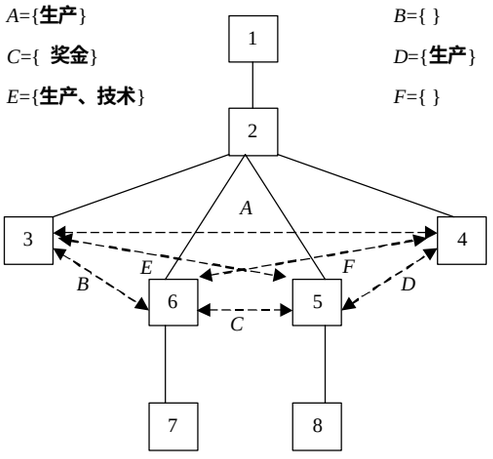

图2　扩展组织格安全模型应用举例

参　考　文　献

[1] Denning D E. Secure information flow in computer systems: [ph. D Thesis] [D]. Purdue Univ, W Lafayette, Ind 1975

[2] Denning D E. A lattice model of secure information flow [J]. Comm ACM, 1976, 19(5): 236-243

[3] Landwehr C E, Heitmeyer C L, Mclean J. A security model for military message systems[J]. ACM Transactions on Computer Systems, 1984, 9(3): 198-222

[4] 蒋继洪, 黄江月. 计算机系统、数据库系统和通信网络的安全与保密[M]. 成都: 电子科技大学出版社, 1995, 185-187

[5] 肖军模, 刘　军, 周海刚. 网络信息安全[M]. 北京: 机械工业出版社, 2003, 85-88

编　辑　孙晓丹