基于轨迹的策略描述和复合*)

訾小超 茅 兵 谢 立
(南京大学计算机软件新技术国家重点实验室 南京 210093)
(南京大学计算机科学与技术系 南京 210093)

Composing and Merging Policies Based on Trace

Zi Xiao-Chao Mao Bing Xie Li
(State Key laboratory for Novel Software Technology, Nanjing University, Nanjing 210093)
(Department of Computer Science and Technology, Nanjing University, Nanjing 210093)

Abstract The diversity of security requirements demands that information systems flexibly support policies, and uniform policy description is important to implement policy-flexible system. This paper brings up new method to descript policies based on trace, which can be applied to many policies used currently. Subsequently this paper refines this method in order to be applicable to actual system, and discusses how to merge multiple policies.

Keywords Information security, Policy-flexible, Composing policies, Merging multiple policies

1 引言

随着计算机信息系统在众多领域的广泛应用,民用尤其是商用计算机系统安全也逐渐引起人们的重视。在军用计算机系统领域,安全需求相对来讲比较单一和稳定(随着网络应用的发展,军用系统安全需求也有所变化),Bell&LaPadula(BLP)模型[1]描述的多级军事安全(Multilevel Security, MLS)策略体现了军用系统的主要安全需求。但在民用领域很难找到这样统一的安全需求,与军用系统相比,民用系统安全需求的最大特点在于它的多样化和不固定性[2]。

安全需求多样化的发展趋势给信息系统提出了策略灵活支持的要求:根据应用领域的安全特点和主要安全威胁,针对性地扩展新的安全策略,针对性的安全策略有助于提高信息系统的实际安全效果[3];用户能够根据具体应用场景动态调整相应的安全策略,这有助于缓解信息系统的安全性和可用性之间的矛盾[4]。近年来,安全策略灵活相关的研究工作逐渐引起人们的重视,这方面的研究已经成为计算机安全的研究热点之一。

把策略具体内容直接嵌入到系统实现代码中不利于安全策略的灵活调整和扩展,要实现不依赖具体策略的策略支撑机制需要不局限于特定策略的策略表示方法[5]。本文首先提出了基于轨迹的策略描述,该描述技术能够适用于目前大多数安全策略,针对该描述方法难以在实际系统的实施过程中使用,随后本文对这种描述方法进行了必要的简化,并在此基础上讨论多个安全策略在系统中的复合。

2 基于轨迹的安全策略描述

从广义上讲,一个组织就敏感信息的管理、保护、分发而制定的规则和准则的集合都称为安全策略[2],计算机信息系统是对应用领域信息处理过程的抽象和模拟,实际的信息系统不可能原封不动实现组织安全策略,要使组织安全策略在信息系统中得到支持,需要进行相应的精化(refinement)和转化[6]。下面首先把实际信息系统抽象为进行自动化信息处理的事件系统,然后在事件系统的基础上讨论安全策略。

2.1 事件系统的概念

定义 1 事件系统 ES 对应二元组$\langle S_0, E\rangle$,S_0 表示事件系统初始状态,E 对应所有能被系统接受的外部事件的集合。

事件系统中的每个事件具有原子性,该事件要么在事件系统得到完整执行,要么得到拒绝,不存在部分执行的情况。

信息系统可以看作是接收外来事件,进行内部状态转换的自动机系统,那么在初始状态一定的情况,信息系统的当前状态完全由外界所输入的事件序列唯一确定。

定义 2 事件系统的运行轨迹 t(Trace)对应由 E 中的事件所组成的事件序列,即 $t\in E^*$(E^* 表示由 E 中的事件所组成的事件序列的全集)。

2.2 安全策略的描述

按照 ITSEC 关于安全策略的定义,信息系统中所有关于信息安全的约定都可以称为安全策略[7],但现实系统中大部分的安全策略都表现为对系统操作的限制,本文把这些对系统操作的限制称为控制策略。

定义 3 事件系统 ES$\langle S_0, E\rangle$中的控制策略 CP 可以表示 T(CP,ES),$T(CP,ES)\subseteq E^*$,对任意 $t\in T(CP,ES)$,ES 按照轨迹 t 运行符合策略 CP,此外,ES 按任意轨迹 $t'(t'\notin T(CP,ES))$运行都违背策略 CP。

事件系统 ES 完全按照 T(ES,CP)中的轨迹运行,假定 ES 已运行了事件序列 X,外界请求 ES 执行事件 e,若事件序列 $X.e\in T(CP,ES)$,则 CP 许可执行事件 e。否则,CP 不许可执行 ES 执行事件 e。(X.e 表示在 X 序列后面添加事件 e 构成的事件序列)。

从定义 3 可以看出,对特定的安全策略 CP,事件 e 是否能够执行,只与它在此前执行的事件序列有关,与未来所发生的事件无关。不难想象,策略 CP 的轨迹集合 T(CP,ES)中任意元素 t 要实际起作用需满足:

$$\forall t_1 \forall t_2((t_1.t_2=t)\rightarrow(t_1\in T(CP,ES)))$$

否则,事件系统 ES 实际上不可能沿轨迹 t 运行。既然集合 T(CP,ES)满足前缀闭包特性,我们可以简化 T(CP,ES),即省

*)本课题得到国家"863"高技术(NO:2001AA144010)经费资助。訾小超 博士生,研究方向:安全操作系统。茅 兵 教授,研究方向:安全操作系统。谢 立 教授,博导,研究方向:信息安全。

去那些被其它轨迹所包含的前缀，简化后的轨迹集合 T′(CP，ES)满足规则：

$\forall t((t\in T'(CP,ES))\rightarrow\forall t_1(t.t_1\notin T'(CP,ES)))$

$\forall t((t\in T(CP,ES))\rightarrow\exists t_1(t.t_1\in T'(CP,ES)))$

$\forall t((t\in T'(CP,ES))\rightarrow t\in T(CP,ES))$

上面的第一条规则保证 T′(CP，ES)中不存在被其他轨迹所包含的前缀轨迹，后两条规则保证 T′(CP，ES)和 T(CP，ES)在描述轨迹上的等价性。

3 面向应用实施的简化

2 节给出控制策略的描述，从理论上讲，信息系统中所采用的大部分安全策略都可以归结到这种描述上。但是现实系统描述安全策略时，并没有给出所允许的轨迹集合，而是通过简单的规则来表示达到同样的效果。实际上，信息系统中所采用的安全策略所对应轨迹集合并非杂乱无章，其中存在一定的规律，通过这些规律，安全策略对应的轨迹集合可以得到进一步的简化。

本节主要根据实际策略轨迹集合的特点，逐步把定义 3 中给出的策略描述转变成能够在实际系统中所采用的形式。

3.1 策略无关事件的消除

通过对实际系统操作事件的分析可以发现，并不是所有的事件都受到策略的约束，如操作系统获取进程自身信息的事件等。

定义 4(策略无关事件) 对事件系统 ES(S_0，E)、安全策略 CP 和事件 e($e\in E$)，若对任意轨迹 t($t\in T'(CP,ES)$)，存在

$\forall t_1\forall t_2((t_1.t_2=t)\rightarrow(t_1.e.t_2\in T'(CP,ES)))$

则称 e 为针对 CP 的策略无关事件。

从定义 4 可以看出在事件系统 ES 中，策略 CP 并不约束 e 的执行，同时 e 是否执行也不会对后继事件能否执行产生影响。因为 e 不受策略约束，即使 e 是否执行影响后继事件的运行，外部主体可以任意执行 e 为后继事件的运行创造条件，相当于 e 不能影响后继事件的运行。事件系统在接受到这些事件请求时，一律满足这些事件请求。那么我们在描述策略对应的轨迹集合时完全可以不考虑这类事件。

若用 E_IRRP(Event IRRelated to Policy)表示在 ES 中针对策略 CP 的无关事件集合，相对于策略无关事件，我们称剩余的事件为策略有关事件，其集合记作 E_RP(Event Related to Policy)。则策略 CP 在不考虑策略无关事件后所对应轨迹的集合 T″(PC，ES)需满足：

$\forall e\forall t_1\forall t_2(((e\in E\_IRRP)\wedge(t_1.t_2\in T''(CP,ES)))\rightarrow(t_1.e.t_2\in T'(CP,ES)))$

$\forall t((t\in T'(CP,ES))\rightarrow\exists t'((t'\in T''(CP,ES))\wedge(t'=Project_{E\_RP}(t))))$

投影运算 $Project_{E_RP}(t)$表示事件序列 t 中只保留 E_RP 事件(移去其它事件)所获得的事件序列。注意，策略无关事件是针对具体的控制策略而言，当在一个事件系统中复合多个安全策略时，这些不可见事件可能需要加以考虑。

3.2 安全策略的规则描述

若 $t_1.e.t_2\in T''(CP,ES)$，对于事件 e 来讲，如果前面执行了事件序列 t_1，那么事件 e 就可以执行，我们可以把 t_1 看成是事件 e 得以执行的条件。从该角度讲，我们可得到 T″(CP，ES)的等价规则表示 R(CP，ES)，$R(CP,ES)\subseteq\{t\rightarrow e\mid(e\in E\_RP\}\wedge(t\in E\_RP^*)\}$，且满足：

$\forall(t\rightarrow e)(((t\rightarrow e)\in R(CP,ES))\rightarrow\exists t'(t.e.t'\in T''(CP,ES)))$

$\forall t\forall t'\forall e((t.e.t'\in T''(CP,ES))\rightarrow((t\rightarrow e)\in R(CP,ES)))$

上述两个表达式保证了 T″(CP，ES)和 R(CP，ES)在描述策略上的等价性。

3.3 非授权事件的消除

在忽略策略无关事件之后，通过对 T″(CP，ES)中轨迹分析可以发现，有些事件的执行与否不会影响到其他后继事件的执行，而另一些事件影响到其他后继事件的执行。从授权的角度上讲，后一类事件的执行引发相应的权限转移。根据是否影响后继事件的执行，本文把策略有关事件又进一步细分为授权事件和非授权事件。

定义 5(授权事件和非授权事件) 对事件系统 ES(S_0，E)、安全策略 CP 和事件 e($e\in E\_RP$)，若对任意轨迹 t($t\in T''(CP,ES)$)，存在

$\forall t_1\forall t_2(((t_1.t_2=t)\wedge(t_1.e\in T''(CP,ES)))\rightarrow(t_1.e.t_2\in T''(CP,ES)))$

则对策略 CP 称 e 为非授权事件；否则称 e 为授权事件。

把策略相关事件划分为授权事件和非授权事件(下面分别用 E_Auth 和 E_NAuth 表示针对事件系统 ES 和策略 CP 的授权事件集合和非授权事件集合)，有利于进一步简化事件系统中的策略表示。因为非授权事件不影响后继事件能否执行，事件系统判断是否执行后继事件请求时，只需关心已经执行过的授权事件序列即可。因此，安全策略 CP 可以用更加精简的规则 R′(CP，ES)表示：

$R'(CP,ES)\subseteq\{t\rightarrow e\mid(t\in E\_Auth^*)\wedge(e\in E\_IRP)\}$

在经过上述简化后，事件系统依照 CP 策略运行且收到事件 e 的操作请求时，若已执行过的授权事件轨迹为 t，那么在 R′(CP，ES)集合中查找是否有 $t\rightarrow e$ 的规则。若有则执行该事件请求，否则拒绝该请求。

3.4 相同授权事件的压缩

不难想象，在同一个序列中，对同一个授权事件的多次出现，真正能够对后继事件产生影响的是最后一次出现。

根据该特点，我们可以把 R′(CP，ES)规则的条件部分 t 作进一步的简化，得到规则集合 R″(CP，ES)。对规则 $t\rightarrow e$ 来讲，循环进行 I 处理，直到满足 II 中条件：

I：若满足$\exists t_1\exists t_2\exists t_3\exists e_i\exists e_j((t_1.e_i.t_2.e_j.t_3=t)\wedge(e_i=e_j))$，则把规则 $t\rightarrow e$ 替换为规则 $t_1.t_2.e_j.t_3\rightarrow e$

II：t 中不再出现相同授权事件

对 R′(CP，ES)的所有规则进行上述处理，就可以得到简化的规则集合 R″(CP，ES)。

经过相同事件的压缩后，每个规则的条件部分不再是有效的轨迹，如存在规则 $t\rightarrow e$，这并不表明策略 CP 允许 ES 可以完全按 t 指明的轨迹运行。

3.5 策略描述的重新定义

随着事件系统 ES 中针对策略 CP 的事件分类：策略无关事件、授权事件和非授权事件，下文用 ES〈S_0，E_IRRP∪E_Auth∪E_NAuth〉表示策略 CP 控制下的事件系统。

定义 6 事件系统 ES〈S_0，E_IRRP∪E_Auth∪E_NAuth〉中的控制策略 CP 可以表示为满足如下条件的规则集合 Rule(PC，ES)：

$Rule\subseteq\{t\rightarrow e\mid t\in E\_Auth^*\wedge e\in(E\_NAuth\cup E\_Auth)\}$

$\forall t_1\forall t_2\forall t_3\forall e_i\forall e_j\forall e(((t_1.e_i.t_2.e_j.t_3\rightarrow e)\in Rule)\rightarrow(e_i\neq e_j))$

事件系统 ES 的策略描述发生变化后，ES 解释策略的方式也发生相应的改变：假定当前系统所运行的事件序列为 t，首先作投影运算 $t'=Project_{E\_Auth}(t)$，然后去掉 t′序列中对同

一授权事件的多次出现，只保留最后一次出现，获得 t''。对接受到的下一事件 e，若 $e \in E\_IRRP$，直接执行事件 e，否则若 $(t'' \rightarrow e) \in Rule(CP, ES)$，则执行事件 e，否则拒绝事件 e。

实际上，在事件系统运行策略的过程中，可以只记录授权事件发生的序列，且对同一授权事件只保留最后一次出现，因为其它事件的发生影响不到对策略 CP 的解释。

3.6 基于轨迹描述的策略实现

尽管定义 6 给出的规则描述形式比定义 4 中轨迹集合描述的形式更加简洁，也更容易被实际系统采用，但现实系统实施安全策略时，人们很少直接通过以前所发生的授权事件来表示安全策略。实际系统在实施安全策略时常常采用间接的方式来表示安全策略，即引入一些系统状态变量（下文把这些系统状态变量作为策略相关的安全属性）来间接表示所发生的授权事件轨迹。那么定义 6 以相关授权事件为条件的规则表达式，也相应表示为以安全属性值为条件的授权表达式。

尽管实际系统以安全属性为条件表示安全策略，但上面的定义和分析仍然适用。定义 5 中授权操作对应那些修改安全属性的操作，只有这些操作改变了安全属性，才影响到后继操作能否执行。对同一授权事件的多次运行，经过它多次修改安全属性值，但只有最后一次修改结果才保存下来，对后继事件发生影响，这也从另一个侧面反映 3.4 节相同授权事件压缩的合理性。

4 多策略复合

4.1 多策略复合的必要性

尽管从理论上可以把限制系统状态转变的所有约束认为是一个安全策略，但从实践的角度讲，很多系统在实施安全策略时都把系统安全策略认为是多个策略的复合，如按照 TCSEC 标准研制的安全操作系统大都把安全策略分别实现为自主控制策略和强制控制策略。

把系统安全策略视为多个安全策略的复合有利于系统对安全策略的支持：首先，这有利于安全策略的扩展和动态调整，当系统新添加一个安全策略时，没必要修改原来的安全策略，只需解释新添安全策略并处理好与原来安全策略之间的关系即可；其次，从安全策略的形成来讲，安全策略主要用于满足应用领域的安全需求，很多情况下，应用领域的安全需求可能涉及到多个方面，如一般资源访问、特殊资源访问、系统管理等，这需要分别设计具体的安全策略来满足安全需求的特定方面，把系统安全策略视为多个安全策略的复合有利于人们对安全策略的理解，也有利用验证是否满足应用需求。

4.2 策略复合的形式化分析

假定存在事件系统 ES 和分别运行在其上的两个安全策略 CP_1、CP_2，ES 需要同时满足这两个安全策略，我们首先在定义 5 的基础上分析事件系统依据策略 $CP(CP_1 \wedge CP_2)$ 的事件分类 $E\_IRRP \cup E\_NAuth \cup E\_Auth$ 和策略规则描述 Rule(PC,ES)。

CP_1：ES(S_0, $E\_IRRP_1 \cup E\_NAuth_1 \cup E\_Auth_1$)，Rule($CP_1$,ES)。

CP_2：ES(S_0, $E\_IRRP_2 \cup E\_NAuth_2 \cup E\_Auth_2$)，Rule($CP_2$,ES)。

显然，存在下列简单关系：

$E\_IRRP = E\_IRRP_1 \cap E\_IRRP_2$：只有在两个策略下都是策略无关事件才在复合安全策略下是策略无关事件。

$E\_NAuth = (E\_NAuth_1 \cap E\_NAuth_2) \cup (E_1RRP_1 \cap E\_NAuth_2) \cup (E\_NAuth_1 \cap E\_IRRP_2)$：只有在两个策略下都为非授权事件，或者在一个策略下为非授权事件，在另一个策略下为无关事件，在复合安全策略下才是非授权事件。

$E\_Auth = E\_Auth_1 \cup E\_Auth_2$：只要在其中一个策略下为授权事件，在复合安全策略下就为授权事件。

显然不能简单认为 CP 的策略规则 $Rule = Rule_1 \cup Rule_2$（下文用 Rule、$Rule_1$、$Rule_2$ 分别表示 Rule(CP,ES)、Rule(CP_1,ES)、Rule(CP_2,ES)。我们在给出具体的求解算法以前，首先给出以下定理：

定理 1 对同一事件系统策略规则 $(t_1 \rightarrow e) \in Rule_1$、$(t_2 \rightarrow e) \in Rule_2$，令 $E\_BothAuth = E\_Auth_1 \cap E\_Auth_2$，若 $Project_{E\_BothAuth}(t_1) \neq Project_{E\_BothAuth}(t_2)$，那么在事件系统 ES 中不存在事件轨迹 t 同时满足这两个规则。

假定事件序列 $t \rightarrow e$ 同时满足这两条策略规则，即 $Project_{E\_Auth1}(t) = t_1$、$Project_{E\_Auth2}(t) = t_2$，显然 $Project_{A \wedge B}(t) = Project_A(Project_B(t))$，那么

$$Project_{E\_BothAuth}(t_1) = Project_{E\_BothAuth}(Project_{E\_Auth1}(t)) = Project_{E\_BothAuth \cap E\_Auth1}(t) = Project_{E\_BothAuth}(t)$$

$$Project_{E\_BothAuth}(t_2) = Project_{E\_BothAuth}(Project_{E\_Auth2}(t)) = Project_{E\_BothAuth \cap E\_Auth2}(t) = Project_{E\_BothAuth}(t)$$

$$Project_{E\_BothAuth}(t_1) = Project_{E\_BothAuth}(t_2)$$ □

通过定理 1 可知只有 $Project_{E\_BothAuth}(t_1) = Project_{E\_BothAuth}(t_2)$ 时才可能出现同时满足两个策略的授权事件轨迹。我们可很容易构造出事件系统同时满足这两个策略的规则，即：根据 $Project_{E\_BothAuth}(t_1)/Project_{E\_BothAuth}(t_2)$，把 t_1 和 t_2 同时分解成 n+1 段（n 为 $Project_{E\_BothAuth}(t_1)/Project_{E\_BothAuth}(t_2)$ 的序列长度），那么构造出的新规则也由 n+1 段组成，新规则的第 I 段由两条旧规则的第 I 段组成；由于 t_1 的第 I 段的所有事件对 CP_2 来讲都是非授权事件，反之亦然，我们可以任意组合这两条规则的第 I 段获得新规则的第 I 段。

结束语 安全需求的多样化对信息系统提出策略灵活性的要求，策略的形式化描述是实现系统灵活支持安全策略的重要基础，本文给出了基于轨迹的策略描述方法，并在此基础上提出面向系统实现的简化，及关于多策略复合的形式化分析。

参考文献

1 America Department of Defense. Trusted Computer System Evaluation Criteria, CSC-STD-001-83, Aug. 1983

2 Clark, David D, Wilson D R. A Comparison of Commercial and Military Computer Security Policies. In: Proc. of the 1987 Symposium on Security and Privacy

3 Schneider E A. Security architecture-based system design. In: Proc. of the 1999 workshop on New Security paradigm

4 Zurko M E, Simon R T. User-centered security. ACM New Security Paradigms Workshop, 1996

5 Bonatti P, et al. A modular approach to composing access control policies. In: Proc. of the 7th ACM conf. on Computer and communication security, 2000

6 Olson I M, Abrams M D. Information Security Policy, Information Security: An Integrated Collection of Essays. IEEE Computer Society Press

7 France-Germany-the Netherlands-the United Kingdom. Information Technology Security Evaluation Criteria, 1991