第 37 卷 第 2 期
Vol.37 No.2

计 算 机 工 程
Computer Engineering

2011 年 1 月
January 2011

• 安全技术 •

文章编号：1000—3428(2011)02—0120—03 文献标识码：A 中图分类号：TP309

电子机构的信息流控制研究

史 磊，蔡国永，隋 新

(桂林电子科技大学计算机与控制学院，广西 桂林 541004)

摘 要：电子机构是解决自治主体间业务可信协同的一种开发框架，但其缺乏对信息流进行灵活控制的安全机制，可能会造成对机密信息的威胁。为此，在扩充电子机构语义的前提下，设计一种动态检测信息传递的安全模型。该模型根据强制访问控制的特点，依照级别标签来控制信息“不向下写”，对传输数据的安全级别进行单独赋值，确保电子机构中所有授权通信路径的安全。将该安全模型引入电子机构可有效防止信息的非授权泄露，提高机构的信息流安全性。

关键词：电子机构；访问控制；信息流

Research on Information Flow Control in Electronic Institution

SHI Lei, CAI Guo-yong, SUI Xin

(School of Computer and Control, Guilin University of Electronic Technology, Guilin 541004, China)

【Abstract】 Electronic Institution(EI) as a development framework is good for developing dependable distributed collaboration. However, due to its lack of information flow control mechanism, the confidentiality of information may be threatened. By extending the semantics of electronic institution, this paper designs a security model that dynamically checks information transfer. As a result, all authorized communication paths are secure. The control process of the security model is illustrated via an example. The security model can prevent unauthorized information leakage and enhance securities of EI based systems.

【Key words】 Electronic Institution(EI); access control; information flow

DOI: 10.3969/j.issn.1000-3428.2011.02.041

1 概述

在开放异构的全球网络基础上，构建安全可信的虚拟组织系统是当前软件开发亟需解决的问题。电子机构(Electronic Institution, EI)模型[1]就是采用组织的方式管理个体间语言交互的一种较系统的概念框架。现有文献中介绍的电子机构模型主要采用非规范的义务逻辑或状态变迁系统来建模和分析，对其中信息传递的安全性没有进行深入的分析。在分布式系统中确保信息的安全传递是十分重要的，因此，有必要展开进一步的研究。本文为提高数据的机密性和信息流的安全性，对电子机构的语义进行了安全级别扩充，并结合自主访问控制(Discretionary Access Control, DACDAC)和强制访问控制(Mandatory Access Control, MAC)的优点，设计了用来动态检测信息流动的安全模型，将其引入电子机构的分析框架，能有效防止非法信息流的产生，且不损失系统的灵活性。

2 电子机构模型规约

2.1 电子机构的演算规约

电子机构的演算规约语言(EIC)[2]是结合电子机构的概念对 π 演算的一种扩展。令 A 表示参与场景并扮演角色的主体的标识集，SI 表示场景标识的有限集，R 表示角色标识集，SC 表示场景的通道。基于这些基本集合的元素，对 EIC 的语法介绍如下：

主体的格局表示为元组，即$<agent>::=<u,b,a,R,P,I>$，其中，u 表示主体自身的约束或策略；b 表示主体的局部信念；a 表示主体的物理标识；R 表示主体扮演的场景的角色集；P 表示场景角色的交互行为进程；I 表示主体的初始程序或决策进程，它为主体的角色进程执行创建策略上下文。相应的主体的角色集为 $R::=\{r_1,r_2,\cdots,r_n\}$。令 M 表示 EIC 的基本能力项，则 M 的 BNF 文法定义为：$M::=msg!sc|\ msg?sc|\#|\ ?blf|\ !blf|\ enter(a,r)!sc|\ leave(a,r)!sc$，其中，$msg!sc$ 表示向场景通道 sc 发送消息 msg；$msg?sc$ 表示从场景通道 sc 接收消息，并存入变量 msg 中；$\#$表示不需要关注的主体内部其他能力抽象；$?blf$ 为检查表达式 blf 是否被主体信念库所蕴含；$!blf$ 为更新主体信念；$enter(a,r)!sc$ 为当主体想进入一个场景并扮演某一角色时，则向场景通道发送消息 $enter(a,r)$；$leave(a,r)!sc$ 表示当主体想退出场景，停止其扮演的角色时，则发送消息 $leave(a,r)$。

令 P 表示 EIC 的顺序进程，则 P 定义为：$P::=nil|m|?blf\rightarrow P|P;P|P+P|P=c(P)|P_1\&P_2$，其中，$nil$ 表示无能力进程；$m\in M$ 表示基本能力项；$?blf\rightarrow P$ 表示如果$?blf$ 测试成功，则执行进程 P；“；”和“+”分别表示顺序组合与不确定组合算子；$P=c(P)$ 表示卫式递归进程；“&”表示并行组合算子。

主体的行为语义定义为一个变迁系统，其变迁规则在文献[2]中具体给出。主体不可避免地要在一定的环境中存在。场景便是主体的一种社交环境，其简化的格局定义为：$<Scene>::=<SI,SU,SCi,SCo,CR,HR,SA,SP>$，其中，$SI$ 表示场景标识；SU 表示场景约束集；SC_i、SC_o 分别表示场景消息的输入和输出通道集；CR 表示当前主体角色扮演关系的配置，表示为谓词公式集；HR 表示主体角色配置的历史记录集；SA 表示角色主体当前的活动状态；SP 表示场景的进程。文献[2]给出了场景的形式化语义变迁规则，本文不再详述。

2.2 电子机构演算的安全级扩展

为了保证电子机构中信息的安全传输，对模型中主体 a、角色 r 和传送的消息 msg 赋予安全级别 λ，并对 EIC 的基本

基金项目：广西自然科学基金资助项目(0728089)

作者简介：史 磊(1984－)，男，硕士研究生，主研方向：可信计算，电子机构；蔡国永，教授、博士；隋 新，硕士研究生

收稿日期：2010-06-10 **E-mail：**shigod2002@yahoo.com.cn

能力项 M 进行扩充，将电子机构变为多安全级别系统，从而提供了一个引入安全模型的前提条件。r^{λ} 表示角色 r 被赋予安全级别 λ，角色安全级别的赋值是根据整个系统的安全策略划分的，并且安全级别遵循偏序关系(≥)。例如，在医院中角色医生 r_D 的安全级别 λ_D 要高于角色护士 r_N 的安全级别 λ_N ($\lambda_D \geq \lambda_N$)。主体 a 安全级别的赋值为：$r_i^{\lambda_i} \gg a_j^{\lambda_0}$ 表示主体 a_j 从加入的角色 r_i 中继承安全级别 λ_i，相应的变迁规则为：$r_i^{\lambda_i} \gg a_j^{\lambda_0} \longrightarrow a_j^{\lambda_i}$，当主体没有加入角色时，其默认的安全级别为 λ_0 且为最低。对主体 a 发送的消息 msg 赋予安全级别：$a^{\lambda_i} \triangleright [msg(x), \lambda_{in}]$ 表示当已加入角色的主体 a^{λ_i} 要发送消息 msg 时，给消息 msg 赋予安全级别 λ_{in}，x 为发送消息的参数，相应的变迁规则为：$\dfrac{r_i^{\lambda_i} \gg a_j^{\lambda_0} \longrightarrow a_j^{\lambda_i}}{a^{\lambda_i} \triangleright [msg(x), \lambda_{in}] \longrightarrow msg^{\lambda_{in}}(x)}$。主体的安全级别从角色继承，但是主体发送消息的安全级别却被独立赋值，这样做是为了增加整个系统信息传输的灵活性(在第 3.1 节给出说明)。扩展后的基本能力项为：

$M ::= msg^{\lambda_{in}}!sc \mid msg^{\lambda_{in}}?sc \mid \#|?blf|!blf|enter(a,r)!sc|leave(a,r)!sc \mid r_i^{\lambda_i} \gg a_j^{\lambda_0} \mid a^{\lambda_i} \triangleright [msg(x), \lambda_{in}]$

3　安全模型

3.1　访问控制模型

多级安全模型(MLS)是 MAC 模型的典型代表，本文在基于其分级概念的基础上设计安全模型，实现类似于 BLP 模型“不向下写，不向上读”的安全控制策略，同时又结合自主访问控制列表来满足一些特殊要求的信息传递，提高了灵活性，更好地适应实际系统的应用要求。首先介绍此安全框架中的一些概念：$\mathcal{S}$是角色内所有作为发送方和接收方的具有安全级别主体的集合；$\mathcal{D}$是主体发送或接受到的数据集合，$msg \in \mathcal{D}$；$\mathcal{R}$是场景中角色的集合，$r_i \in \mathcal{R}$。

用$\mathcal{A}$表示符合安全策略的所有主体行为的集合。下面是有关安全机制的概念：$\mathcal{L}$是安全级别 λ 的有限集合，且具有偏序关系≥，$\forall i \in \mathcal{S} \cup \mathcal{D} \cup \mathcal{R}$，$\lambda_i \in \mathcal{L}$；$\mathcal{T} \subseteq \mathcal{S} \times \mathcal{S} \times \mathcal{A}$(发送方、接收方、行为)表示安全策略授权的动作；$\mathcal{M}$为$\mathcal{S} \times \mathcal{S} \to \mathcal{P}(\mathcal{A})$表示带有安全级别的对数据操作的授权访问控制列表，对于每个发送-接收主体对，列表中都给出允许的行为和允许传输的数据安全级别；$\mathcal{P}(\mathcal{A})$表示授权列表中允许的行为集的集合。

下面给出安全模型中行为的特征函数：

(1) $SE_{\alpha^{\lambda_\alpha} \to \beta^{\lambda_\beta}}(msg^{\lambda_{in}})$ 表示主体 α^{λ_α} 向场景通道发送消息 $msg^{\lambda_{in}}$，此消息的接收主体为 β^{λ_β}。

(2) $RE_{\beta^{\lambda_\beta} \leftarrow \alpha^{\lambda_\alpha}}(msg^{\lambda_{in}})$ 表示主体 β^{λ_β} 从场景通道中接收到消息 $msg^{\lambda_{in}}$，且消息的发送主体为 α^{λ_α}。

依照本文的控制策略，电子机构中信息的安全传输条件式定义如下：

定义 1 (安全的消息发送)

$$\forall \alpha, \beta \in \mathcal{S}, (\alpha, \beta, SE_{\alpha^{\lambda_\alpha} \to \beta^{\lambda_\beta}}(msg^{\lambda_{in}})) \in \mathcal{T} \Leftrightarrow (\lambda_{in} \leq \lambda_\beta) \wedge \left(\left((\lambda_\alpha > \lambda_{in}) \wedge SE_{\alpha^{\lambda_\alpha} \to \beta^{\lambda_\beta}}(msg^{\lambda_{in}}) \in \mathcal{M}(\alpha, \beta) \right) \vee (\lambda_\alpha \leq \lambda_{in}) \right)$$

数据传输原则上是遵循高安全级别主体不向低安全级别主体发送消息。当发送消息的安全级别 λ_{in} 高于发送方的安全级别 λ_a 时，则在发送方、传输的消息和接收方三者的安全级上形成偏序关系($\lambda_\alpha \leq \lambda_{in} \leq \lambda_\beta$)，即低安全级别对象的信息写入高安全级别对象，符合安全机制，允许消息的发送；另一种情况是当发送消息的安全级别 λ_{in} 低于发送方的安全级别 λ_a 时(数据的降级传输)，此时不能确定发送方和接收方谁的安全级别更高，则需要查看授权访问控制列表中是否对此行为授权，如果授权则允许消息发送，但降级消息的安全级别必须小于接收方的安全级别。此处将传输消息的安全级别单独进行讨论，而不是简单地继承发送方的安全级别，就是为了增加单纯依据安全标签控制信息流向的灵活性。

定义 2(安全的消息接收)

$$\forall \alpha, \beta \in \mathcal{S}, (\alpha, \beta, RE_{\beta^{\lambda_\beta} \leftarrow \alpha^{\lambda_\alpha}}(msg^{\lambda_{in}})) \in \mathcal{T} \Leftrightarrow (\lambda_{in} \leq \lambda_\beta)$$

安全的消息接收只要求收到的消息的安全级别比接收方的安全级别低，即满足“不向上读”的机制。表 1 给出了加入安全模型后电子机构中主体和场景的部分语义变化情况。

表 1　扩展的变迁规则

$a^{\lambda_i} \triangleright [msg(x), \lambda_{in}] \longrightarrow msg^{\lambda_{in}}(x)$ $(\alpha, \beta, SE_{\alpha^{\lambda_\alpha} \to \beta^{\lambda_\beta}}(msg^{\lambda_{in}})) \in \mathcal{T}$ $< msg^{\lambda_{in}}!sc > \xrightarrow{msg^{\lambda_{in}}:sc} < nil >$	sec-send
$(\alpha, \beta, RE_{\beta^{\lambda_\beta} \leftarrow \alpha^{\lambda_\alpha}}(msg^{\lambda_{in}})) \in \mathcal{T}$ $< msg^{\lambda_{in}}?sc > \xrightarrow{msg^{\lambda_{in}}:sc} < nil >$	sec-receive
$CR = R_1^{\lambda_1}\{\cdots\}, \cdots, R_i^{\lambda_i}\{\cdots a^{\lambda_i}\}, \cdots, R_n^{\lambda_n}\{\cdots\}$ $< accept(a,r,sa)?sc_i > \xrightarrow{msg^{\lambda_{in}}:sc_o} < nil >$ $< SA, accept(a,r,t)?sc_i > \xrightarrow{msg^{\lambda_{in}}:sc_o} < SA', nil >$ $SA' = sa_1\{\cdots\}, \cdots, sa_i\{started\}, \cdots, sa_m\{\cdots\}$	sec-start
$CR = R_1^{\lambda_1}\{\cdots\}, \cdots, R_i^{\lambda_i}\{\cdots a^{\lambda_i}\}, \cdots, R_n^{\lambda_n}\{\cdots\}$ $SA = sa_1\{\cdots\}, \cdots, sa_i\{start\}, \cdots, sa_m\{\cdots\}$ $< inform(a,r,sa_i)?sc_i > \xrightarrow{msg^{\lambda_{in}}:sc_o} < nil >$ $< CR, SA, accept(a,r,t)?sc_i > \xrightarrow{msg^{\lambda_{in}}:sc_o} < CR, SA', nil >$ $SA' = sa_1\{\cdots\}, \cdots, sa_i\{finished\}, \cdots, sa_m\{\cdots\}$	sec-finish

3.2　安全信息流

首先讨论主体间信息流的概念。所考虑的主体包括它自身、给它发消息的主体和它将要发送消息的目的主体。从整个系统来看，信息流为一条信息传输的路径，路径由信息的传送方向决定，并由从开始节点到目标节点途中信息经过的所有主体顺序构成，这条路径定义为流路径 $fp := \alpha.\beta.\cdots$。例如，$\Im_{\gamma.\delta}(\alpha, \beta)$ 表示信息从主体 α 传到主体 β，途中经过主体 γ 和主体 δ。每一个信息的流动都是由主体的发送和接收发起的，整个信息流也是由主体与主体之间的信息传递组成的，为了保证整个信息流的安全性，检测路径上每一个信息传输单元。将安全机制引入流路径，当流路径上所有主体的发送和接收消息都为安全时，那么从源节点到目的节点的信息流传输是安全的。给出形式化定义如下：

定义 3(安全信息流)

$$\frac{Sec\Im_{fp_1}(\alpha, \gamma) \wedge Sec\Im_{fp_2}(\gamma, \beta)}{Sec\Im_{fp_1.\gamma.fp_2}(\alpha, \beta)}$$

$$\frac{(\alpha, \beta, SE_{\alpha^{\lambda_\alpha} \to \beta^{\lambda_\beta}}(msg^{\lambda_{in}})) \in \mathcal{T}}{(\alpha, \beta, RE_{\beta^{\lambda_\beta} \leftarrow \alpha^{\lambda_\alpha}}(msg^{\lambda_{in}})) \in \mathcal{T}}$$

$$\frac{}{Sec\Im_{\phi}(\alpha, \beta)}$$

一个信息流是安全的，当且仅当它的流路径也是安全的。

性质(安全的信息流路径)

$$Sec\Im_{\gamma_1, \gamma_2, \cdots, \gamma_n}(\alpha, \beta) \Leftrightarrow Sec\Im_{\phi}(\alpha, \gamma_1) \wedge Sec\Im_{\phi}(\gamma_1, \gamma_2) \wedge \cdots \wedge Sec\Im_{\phi}(\gamma_n, \beta)$$

此性质的证明是显而易见的，可结合定义 3 由信息流路

径的长度归纳求得。此性质体现了本模型的特殊性，在不危及到信息流安全的前提下结合 MAC 和 DAC 的特点，放宽了一些对信息传递的限制，增加了整体的灵活性。尤其要指出的是，流路径是根据授权访问控制列表的变化进行动态调整的，对消息单独进行安全级别的赋值也是为了在信息流中对其进行降级传输。

4 电子机构安全信息流实例

设有一个虚拟的医院(HOS)治疗(cure)场景，场景中的角色有医生(*D*)、护士长(*HN*)、护士(*N*)和病人(*P*)。病人向医生讲述自己的症状；医生得到病人的症状信息后，进行分析并给出对应的治疗方案，然后把所有病人的治疗方案统一发送给护士长；护士长收到所有人的治疗方案后对其进行整理，再把单个病人的治疗方案发送给护士；由护士将药方信息通知病人。场景中的信息流动如图 1 所示。

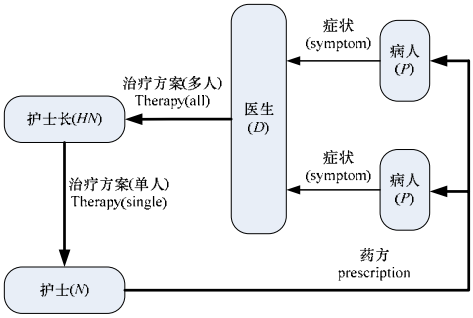

图 1 实例场景信息传递示意图

本文给出各角色的安全级别为：$\lambda_D > \lambda_{HN} > \lambda_N > \lambda_P$。医生被赋予最高的安全级别是因为医生了解病情且给出治疗方案；护士长安全级别次之，因为护士长需要对所有病人的治疗方案进行分类，且要把每个病人的方案分发给相应的护士；病人拥有最低的安全级别，因为有些信息是要对病人本人保密的。安全级别的划分是一个偏序关系，但是有些信息要求从高级别角色传向低级别角色，例如图中粗箭头所示的信息传输。因此，授权访问控制列表$\mathcal{M}$如表 2 所示。

表 2 授权访问控制列表

发送方	接收方	数据级别	授权动作
D	*HN*	$\lambda_{in}=\lambda_{HN}$	$SE_{D^{\lambda_D}\to HN^{\lambda_{HN}}}(msg^{\lambda_{in}})$
HN	*N*	$\lambda_{in}=\lambda_N$	$SE_{HN^{\lambda_{HN}}\to N^{\lambda_N}}(msg^{\lambda_{in}})$
N	*P*	$\lambda_{in}=\lambda_P$	$SE_{N^{\lambda_N}\to P^{\lambda_P}}(msg^{\lambda_{in}})$

假设有主体 *x*、*y*、*z*、*k* 分别加入病人、护士长、医生和护士角色，则相应的各角色行为规约用安全级扩展的 EIC 演算表示如下。

病人的行为规约如下所示：

$enter(x, HOS.cure.P)!sc(HOS.cure);//[1]$

$msg^{\lambda_0}(x.result)?sc(HOS.cure);//[2]$

$?(x.result = accept)\to$

$\{r_P^{\lambda_P} \gg x;//[3]$

$x^{\lambda_P} \triangleright [msg(x.symptom),(\lambda_{in}=\lambda_P)];//[4]$

$[(P,D,SE_{P^{\lambda_P}\to D^{\lambda_D}}(msg^{\lambda_{in}}))\in\mathcal{T}]//[5]$

$\to msg^{\lambda_{in}}(x^{\lambda_P}, HOS.cure.P, symptom)!sc(HOS.cure.D);//[6]$

$\cdots$

$[(P,D,SE_{P^{\lambda_P}\to D^{\lambda_D}}(msg^{\lambda_{in}}))\notin\mathcal{T}]\to nil;[7]$

$\}$

$?(x.result = refuse)\to nil;//[8]$

当有主体 *x* 进入场景，希望加入病人角色时，向场景管理器发送请求([1])；场景管理器收到请求后进行处理，将处理的结果返回给主体 *x*([2])；如果主体 *x* 被允许加入，则主体从加入的病人角色继承安全级别([3])；获得相应的安全级别之后，主体 *x* 对将要发送的自己的症状信息赋予相应的安全级别([4])；当检测发送消息的行为符合安全机制时([5])，病人 *x* 将自己的症状信息发送给医生([6])；如果检测发送消息的行为不符合安全机制，则对行为进行禁止([7])；语句[8]为场景管理器不允许主体 *x* 加入病人角色。

医生的行为规约如下：

$enter(z, HOS.cure.D)!sc(HOS.cure);$

$msg^{\lambda_0}(z.result)?sc(HOS.cure);$

$?(z.result = accept)\to$

$\{r_D^{\lambda_D} \gg z;$

$[(P,D,RE_{D^{\lambda_D}\leftarrow P^{\lambda_P}}(msg^{\lambda_{in}}))\in\mathcal{T}]//[1]$

$\to msg^{\lambda_{in}}(x^{\lambda_P}.symptom)?sc(HOS.cure.D);//[2]$

$\cdots$

$[(P,D,RE_{D^{\lambda_D}\leftarrow P^{\lambda_P}}(msg^{\lambda_{in}}))\notin\mathcal{T}]\to nil;//[3]$

$z^{\lambda_D} \triangleright [msg(all.therapy),(\lambda_{in}=\lambda_{HN})];$

$[(D,HN,SE_{D^{\lambda_D}\to HN^{\lambda_{HN}}}(msg^{\lambda_{in}}))\in\mathcal{T}]$

$\to msg^{\lambda_{in}}(all, HOS.cure.P, therapy)!sc(HOS.cure.HN);//[4]$

$\cdots$

$[(D,HN,SE_{D^{\lambda_D}\to HN^{\lambda_{HN}}}(msg^{\lambda_{in}}))\in\mathcal{T}]\to nil;$

$\}$

$?(z.result = refuse)\to nil;$

医生在接收病人症状消息之前对行为进行安全检测([1])，如果符合安全机制才对消息进行接收([2])，如果不符合则对行为进行禁止([3])；([4])是医生向护士长发送所有病人的治疗方案，是一个从高级别角色向低级别角色发送数据的过程，在对行为进行安全检测时，此行为要在授权访问控制列表中进行授权后才能被执行。鉴于篇幅有限，护士长与护士的行为规约在此不再详细给出。

此例子展示了结合安全模型的电子机构中主体传输信息的运行模式，在每个主体进行发送和接收消息之前，都要对其进行安全检测，如果不符合安全机制则禁止行为运行，确保流路径上每个单元的信息传输都是被授权的，从而保证了整个信息流的安全性。例如，从 *D* 向 *P* 经过 *HN* 和 *N* 发送的药方信息就是一个安全的信息流 $Sec\Im_{HN.N}(D,P)$，因为每一步的信息传输都是授权访问控制列表中授权的，符合安全策略；但是如果 *D* 向 *P* 发送其他信息(如病人的病情)，行为就会被禁止，因为违反了“不向下写”的原则且在授权访问控制列表中也没有进行授权操作。

5 结束语

进程代数方法由于具有强大的组合能力、操作语义和各种形式的互模拟分析技术，因此在分布式软件的建模分析上有独特的优势。Henessy 和 Riely 在文献[3]中对 π 演算进行了扩展，针对用户给出了安全类型，保证分布式系统中信息的传输安全；文献[4]提出了一个基于 SSA 的信息流分析方法，此方法在搜索隐性信息流上具有更好的时空效率；文献[5]分析了基于角色的访问控制在保证安全性上的缺陷，并开发出一个信息流控制器监测信息的发送与接收，杜绝非法的信息传输；在工程方面，可以对像 Java 这类语言植入特征标记，

(下转第 125 页)