可移动系统安全模型统一框架

王立斌，陈克非
（上海交通大学计算机科学与工程系，上海 200030）

摘 要： 本文的主要工作是利用可移动进程的形式化模型 π 演算为工具，考虑系统的移动性（Mobility），将系统安全属性的刻画归结为特定系统进程等价的验证，提出一种新的安全模型框架．在此框架下，可以方便表示不同的不干涉安全属性，并对其进行强弱对比；针对不同安全需求，可定义新的安全属性。并且，该框架建立一个新的安全属性研究的平台，可广泛地适用于具有移动进程的分布式系统的安全分析。

关键词： 安全模型；不干涉安全；π 演算
中图分类号： TP309 **文献标识码：** A **文章编号：** 0372-2112 (2002) 12A-2108-03

A Uniform Framework of Security Model for Mobile Systems

WANG Li-bin, CHEN Ke-fei
(*Dept. of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai* 200030, *China*)

Abstract: Reducing the characterization of systems security to characterizing the equivalence of certain processes, taking the mobility of systems into consideration, we propose a uniform framework of mobile systems security model, which is described in the setting of π-Calculus. In this framework, various noninterference security properties can be easily rephrased and evaluated, and nwe security properties can also be defined for different system requirements. Moreover, constructing a new platform for security properties analysis, this framework can be used extensively in the security analysis of mobile distributed systems, e.g., global computing system, metacomputing system.

Key words: security model; noninterference security; π-calculus

1 引言

多级安全系统（Multilevel Security System）实现中，不干涉（Noninterference）模型针对访问控制模型中的隐信道问题[4]，希望能在系统设计之初就把隐信道排除在系统之外，使隐信道分析开销尽可能小．不干涉模型不描述实现安全的特定方法，而是规范系统输入/输出关系的限制，由系统开发者决定满足该安全规范的实现方法．所谓“不干涉”，直观上就是限制高层用户的输入不能干涉低层用户的输出．最早的不干涉模型是由 Goguen 和 Meseguer 在文献[3]中提出，该模型使用 State Machine 为形式化工具，建立于确定性系统之上．之后，不干涉模型得到广泛的研究，并且被推广到不确定性系统中，主要的模型有 Noninference 模型[8]，Nondeducibility 模型[12] 和 Generalized Noninterference 模型[5]等．然而，不干涉模型在不确定性系统中变得非常微妙，甚至安全的定义都无普遍认同的答案．这些被提出来的安全属性定义，不是太强、就是太弱，或者就是表达形式复杂，不方便使用．值得注意的是，在文[2,9]中，作者分别使用进程代数建立模型，将不干涉安全的刻画归结为判断特定系统进程的弱互模拟等价，有重要的启发性意义，然而他们的模型试图重构以往提出的安全属性，没有提出新的安全属性定义，没有提供一个平台去研究发掘新的安全特性．而且他们使用的形式化工具也限制了模型的表达能力．

本文工作针以上问题，考虑系统的移动性，使用可移动进程的形式化模型 π 演算为工具．将系统的安全属性归结为验证进程的等价（Process Equivalence），提出一种新的安全模型框架．在此框架下，可以方便表示现有的主要安全属性并进行强弱对比；针对不同安全需求，可定义新的安全属性；并且，建立一个新的安全属性研究的平台，可以分析移动计算的安全，可适用于元计算（Metacomputing）、全球计算（Global Computing）等具有移动进程的分布式系统的安全分析．使用 π 演算，也试图利用其良好的理论基础和在程序语言设计上的理论新进展，使得模型最终可在程序语言级别上实现，达成基于语言的安全（Language-based Security）[11]

2 π 演算及相关定义

本文使用的形式化模型是 Milner 的 π 演算[7]．π 演算中最基本的实体是名（names），进程通过名进行交互，并且在交互中传递名，进程接收到的名又可在进一步交互中使用．假定

收稿日期：2002-06-10；修回日期：2002-10-09
基金项目：国家自然科学基金重大研究计划项目（No.90104005）；国家自然科学基金（No.69973031）

存在名的可数无限集合 N,名可用小字母表示.进程通过执行操作而演化,操作的能力表达为四类前缀:

$$\pi ::= \bar{x}y \mid x(z) \mid \tau \mid [x=y]\pi$$

第一个前缀操作表示通过名 x 输出名 y,第二个前缀的操作是通过 x 接受一个名,第三个前缀表示一个不可观测的内部操作,第四个前缀表示条件的判断,如果 x 与 y 是相同名则可操作 π.π 演算的进程可以定义如下:

定义 1(π 演算语法)　π 演算进程表达式集合用 P^{π} 表示,进程表达式通过以下语法定义:

$$P ::= M \mid P \mid P' \mid \nu zP \mid !P$$

$$M ::= 0 \mid \pi.P \mid M + M'$$

直观地,0 是空进程,不作任何操作;进程 $\pi.P$ 能作操作 π,之后继续进程 P;$P + P'$ 能选择执行 P 或 P';$P \mid P'$ 是 P 和 P' 的并行复合,进程交叉进行或发生同步,产生一个内部操作 τ;νzP 表示 z 是进程 P 中的受限名,进程 P 能通过 z 进行交互,而其它他的进程不行;最后,$!P$ 表示进程 P 的无限并行复合,即 $!P = P \mid !P$.

本文使用 π 演算的标准定义和标准语义,没有任何的扩充,在此不加说明地使用在文[7,10]中定义的所有换名规则(α-Conversion)、结构同余规则(Structural congruence)、规约规则(Reduction rules),系统转移规则(Transition rules)及互模拟等价关系(Bisimulation Relation).记函数 $\pi(P)$ 返回进程 P 的所有前缀,对 $\alpha \in \pi(P)$,$Subject(\alpha)$ 返回前缀 α 的操作子.为适用于安全分析,为系统中的每外名赋予安全标识,方便起见,安全级别分为高(H)、低(L)两层,有如下定义:

定义 2　Act_H 和 Act_L 为名的集合,分别代表高层操作与低层操作,并有 $Act_H \cap Act_L = \emptyset$.且 $\forall \alpha \in Act_H(Act_L)$,则 $\bar{\alpha} \in Act_H(Act_L)$.

定义 3　定义 P_H^{π} 为高层进程的集合,有 $P_H^{\pi} \subset P^{\pi}$,$\forall P \in P_H^{\pi}$ $\forall \alpha \in \pi(P)$,有 $Subject(\alpha) \in (Act_H \cup \tau)$.同理可定义 P_L^{π}.称特定的进程子集 $DOM \subseteq P^{\pi}$ 为域(Domain).

3　安全模型统一框架

使用 π 演算建立安全模型统一框架的直观想法是:把系统低层操作不依赖高层操作归结为系统行为的等价,即进程是行为安全的当且仅当低层用户对整个系统(有高层用户参与)所观测到的行为与没有高层操作时的行为是等价的.进一步,在考察特定的进程是否行为安全时,不仅是将该进程独立出来考察,而是要把该进程放到某个特定的系统域下考察,根据域的不同,可以得出该过程的不同安全属性.

定义 4　进程的函数 $Lowviews: P^{\pi} \to P^{\pi}$,使得 $\forall P \in P^{\pi}$,$Lowviews(P) = \nu \boldsymbol{H} P$,其中 $\boldsymbol{H}$ 为 Act_H 中所有元素的向量.

直观上,对进程 P,函数 $Lowviews(P)$ 得到进程 P 在低层用户的行为观测.

定义 5　函数 $Abs_H: P^{\pi} \to P^{\pi}$,使得 $\forall P \in P^{\pi}$,$Abs_H(P)$ 对进程 P 作如下操作,$\forall \alpha \in \pi(P)$,如果 $Subject(\alpha) \in Act_H$ 则 α 替换为 τ,得到进程 P',并且如果 $P' \to P''$,则 $Abs_H(P) \to Abs_H(P'')$.

对进程 P 函数 $Abs_H(P)$ 把进程 P 中的全部高层操作替换为 τ,直观上,就是删除所有高层操作.之所以限定 $Abs_H(P) \to Abs_H(P')$,是要求函数 Abs_H 可以删除每一次规约可能引入的高层操作,使得任何高层操作不能发生交互,直到无限次规约.

定义 6　(安全模型统一框架)对任一进程等价关系 S,任意域 $DOM \subseteq P^{\pi}$,称进程 P 在域 DOM 下是 S 行为安全,记为 $P \in NIS_S^{DOM}$,当且仅当,$\forall \varepsilon \in DOM$,有 $(Lowviews(P \mid \varepsilon), Abs_H(P \mid \varepsilon)) \in S$.

把进程 P 放到特定的域中进行考察,域代表了潜在的威胁(恶意进程),如果进程 P 与域中任意进程进行交互,而低层用户对进程 P 观察到的行为与进程 P 在没有高层操作时的行为是弱互模拟等价的,即没有任何的恶意进程能影低层操作的行为,则认为进程 P 是安全的.

命题 1　$\forall DOM \subseteq P^{\pi}$,有 $NIS_{\doteq}^{DOM} \subseteq NIS_{\approx}^{DOM} \subseteq NIS_{\approx^c}^{DOM}$,和 $NIS_{\doteq}^{DOM} \subseteq NIS_{\cong}^{DOM} \subseteq NIS_{\cong^c}^{DOM}$.其中 $\approx^c$ 是弱全互模拟等价,$\approx$ 是弱互模拟等价,$\doteq$ 是弱 Barbed 互模拟等价,$\cong$ 是弱 Barbed 等价,而 $\cong^c$ 是弱 Barbed 同余[10].

证明　易得,注意到 $\approx^c$ 蕴涵 $\approx$,$\approx$ 蕴涵 $\doteq$ 和 $\cong^c$ 蕴涵 $\cong$,$\cong$ 蕴涵 $\doteq$.

命题 2　$NIS_S^{P_H^{\pi f}} \subset NIS_S^{P_H^{\pi}} \subset NIS_S^0$.其中,$S$ 取 $\{\approx^c, \cong^c, \cong, \approx, \doteq\}$ 其中之一,不严格地使用 0 表示 $\{0\}$,即只有 0 进程的集合;而 $P_H^{\pi +}$ 表示集合 $P_H^{\pi} \cup P$,集合 $P \subseteq P^{\pi}$.

证明　易得,注意到 $0 \subset P_H^{\pi} \subset P_H^{\pi +}$.

命题 3

(ⅰ)$P \in NIS_S^0$ 当且仅当 $(Lowviews(P), Abs_H(P)) \in S$;

(ⅱ)$P \in NIS_S^{P_H^{\pi}}$ 当且仅当 $\forall \varepsilon \in P_H^{\pi}$,$(Lowviews)(P \mid \varepsilon), Abs_H(P)) \in S$.

证明

(ⅰ)由定义 6,并应用结构同余规则 $P \mid 0 \equiv P$ 可得;

(ⅱ)由定义 6,并注意到 $\forall \varepsilon \in P_H^{\pi}$,有 $Abs_H(P)\ SAbs_H(P \mid \varepsilon)$.

取 S 为 $\approx$,则 $NIS_{\approx}^0$,$NIS_{\approx}^{P_H^{\pi}}$ 分别对应文献[1]中定义的 *BSNNI* 和 *BNDC* 安全属性(分别对应着相同的直观含义,但不等价).必须注意的是,$NIS_S^{P^{\pi}} = \emptyset$,即没有进程能在任意进程的"干扰"下依然是行为安全的.表述 $NIS_S^{P_H^{\pi +}}$ 的意义在于,其一,P_H^{π} 不代表唯一的干扰源(在文[1]中,*BNDC* 只考虑高层进程的威胁),低层操作也会带来安全威胁;其次,进程的安全只能放在特定的域下进行考查,考查进程在任意"干扰"下的安全是没有意义的,即只对稳定域 $DOM \in P^{\pi}$,考查 P 是否属于 NIS_S^{DOM}.使用定义 6 的模型并结合以上命题,可以方便地定义不同强度的安全属性.以下,考查在此模型下,是否有良好的性质支持安全分析.

命题 4　(ⅰ)$\forall P, Q \in NIS_{\approx}^0 \not\Rightarrow (P \mid Q) \in NIS_{\approx}^0$

(ⅱ)$\forall P, Q \in NIS_{\approx}^{P_H^{\pi}} \not\Rightarrow (P \mid Q) \in NIS_{\approx}^{P_S^{\pi}}$

证明

(ⅰ)只需给出反例,取 $P = b^L(v) \cdot \bar{a}^H v$,$Q = a^H(y) \cdot \bar{b}^L y + \bar{b}^L y$,明显 $P, Q \in NIS_{\approx}^0$,但 $(P \mid Q) \notin NIS_{\approx}^0$,因为 $Lowviews(P \mid Q) \to \bar{a}^H x$,而 $S_{\approx}^{P_H^{\pi}} Abs_H(P \mid Q)$ 却没有与之对应的操作;

(ⅱ)注意到 $P,Q\in NIS_{\approx}^{P_H^\pi}$,且 $0\in P_H^\pi$.

命题 4 告诉我们,$NIS_{\approx}^0$ 和 $NIS_{\approx}^{P_H^\pi}$ 不满足属性的复合[13],即不能从任意两个安全的进程复合出另一个安全的进程,这不利于安全系统的模块化分析、构造.能否加强条件,得到满足复合性的安全属性呢?

命题 5 如果进程 $P\in NIS_{\cong}^0$,则 $\forall Q\in P_L^\pi$,有 $(P\mid Q)\in NIS_{\doteq}^0$.

证明 由条件 $P\in NIS_{\cong}^0$ 及命题 3,得 $Louviews(P)\cong Abs_H(P)$,由 $\cong$ 的性质[10]可知,对 $\forall R\in P^\pi$,得 $(Louviews(P)\mid R)\doteq(Abs_H(P)\mid R)$;$\forall Q\in P_L^\pi$,取 $R=Louviews(Q)$,得 $(Louviews(P)\mid Louviews(Q))\doteq(Abs_H(P)\mid Louview(Q))$;注意到 $\forall Q\in P_L^\pi$,$Louviews(Q)\equiv Abs_H(Q)$,可得 $Abs_H(P)\mid Louviews(Q)\equiv Abs_H(P)\mid Abs_H(Q)$;再由 $Louviews(P)\mid Louviews(Q)\equiv Louviews(P\mid Q)$,和 $Abs_H(P)\mid Abs_H(Q)\equiv Abs_H(P\mid Q)$,可得 $Louviews(P\mid Q)\doteq Abs_H(P\mid Q)$,由命题 3 可得证.

引理 6 $P\in NIS_S^{P_H^\pi}$ 当且仅当 $\forall\varepsilon\in P_H^\pi$,有 $(Louviews(P\mid\varepsilon),Louviews(P))\in S$.

证明 由命题 3(ⅱ)得,$P\in NIS_{\approx}^{P_H^\pi}$ 当且仅当 $\forall\varepsilon\in P_H^\pi$,有 $(Louviews(P\mid\varepsilon),Abs_H(P))\in S$;由命题 2,如果 $P\in NIS_{\approx}^{P_H^\pi}$,则有 $P\in NIS_{\approx}^0$,即 $(Louviews(P),Abs_H(P))\in S$,得证.

命题 7 如果进程 $P\in NIS_{\cong}^{P_H^\pi}$,则 $\forall Q\in P^\pi$,有 $(P\mid Q)\in NIS_{\cong}^{P_H^\pi}$.

证明 由引理 6 和初始条件,可知 $\forall\varepsilon\in P_H^\pi$,$Louviews(P)\cong Louviews(P\mid\varepsilon)$,由 $\cong$ 性质,得 $Louviews(P)\mid Louviews(Q)\doteq Louviews(P\mid\varepsilon)\,Louviews(Q)$;由 $Louviews(P)\mid Louviews(Q)\equiv Louviews(P\mid Q)$,和 $(P\mid\varepsilon)\mid Q\equiv(P\mid Q)\mid\varepsilon$ 可得 $Louviews(P\mid Q)\doteq Louviews((P\mid Q)\mid\varepsilon)$,得证.

由以上命题可知,属于"强"安全属性的进程与特定的进程复合能得到相对"弱"的安全属性.

4 结束语

本文使用 π 演算定义了一个可适用于可移动系统安全分析的安全模型统一框架,并证明相关模型特性,支持该模型下安全的定义和分析.试图建立安全模型统一框架的研究工作还出现在文献[2,6]中,本文提出的模型与之相比较表达能力更强;定义安全属性更灵活,不仅可以表述已有定义,还可发掘新的定义;并且 π 演算乐观的应用前景,使得本安全模型有望通过程序设计语言来实现.然而为完善本模型,还有许多迫切的工作需要进一步研究.首先我们需要更多的研究和分析实例来决定何种安全属性的强弱程度是合适的;其次,本模型中没有加入定时、概率的操作语义,没有分析稳定时信道和概率信道的能力;还有,能否将类型安全与行为安全更有机的结合起来将是更大的挑战.

参考文献:

[1] Focardi R, Gorrieri R. A classification of security properties for process algebra[J]. Journal of Computer Security, 1995, 3(1): 5 - 33.

[2] Focardi R, Martinelli F. A uniform approach for the definition of security properties [A]. Proceedings of FM'99 [C]. Toulouse, France: LNCS, 1999.

[3] Goguen J A, Meseguer J. Security policies and security models[A]. Propceedings of IEEE Symposium on Research in Security and Privacy [C]. IEEE, 1982.

[4] Lampson B. A note on the confinement problem[J]. Communications of the ACM, 1973, 16(10): 613 - 615.

[5] McCullough D. Specification for mulit-level security and a hook-up property[A]. Proceedings of IEEE Symposium on Research in Security and Privacy [C]. IEEE, 1987.

[6] McLean J. A general theory of composition for a class of "possibility" composability[J]. IEEE Transaction on Software Engineering, 1996, 22 (1): 53 - 67.

[7] Robin Milner. Communicating and Mobile Systems: The π-Calculus [M]. UK: Cambridge University Press, 1999.

[8] O'Halloran C. A calculus of information flow[A]. Proceedings of the European Symposium on Research in Computer Security[C]. Toulouse, France: ESRCS, 1990.

[9] Ryan P, Schneider S. Process algebra and noninterference [A]. Proceedings of 12th IEEE Computer Security Foundations Workshop[C]. IEEE, 1999.

[10] Sangiorgi D, Walkker D. A Theory of Mobile Processes[M]. 2001.

[11] Schneider F B, Morrisett G, Harper R. A language-based approach to security[A]. Informatics: 10 Years Back, 10 Years Ahead, Lecture Notes in Computer Science [C]. Volume 2000 (Reihnard Wilhelm, ed.), Springer-Verlag, Heidelberg, 2000. 86 - 101.

[12] Sutherland D. A model of Information [A]. Ninth National Computer Security Conference [C]. National Bureau of Standars/National Computer Security Center, 1986.

[13] Wang L B. Noninterference composition in distributed systems [A]. Proceedings of the Second International Workshop on Information Security Application [C]. 2001.

作者简介:

王立斌 男,1972 年 2 月生于广东省龙门县,1997 年在华南师范大学计算机科学系获硕士学位,现在上海交通大学计算机科学与工程系攻读博士学位,研究兴趣是网络信息安全,系统安全模型.

陈克非 男,1959 年 11 月生于北京,教授,博士生导师,发表学术论文 80 余篇,主要的研究方向:密码理论与技术、网络信息安全、安全数字水印、安全电子商务.