doi:10.3969/j.issn.1000-436x.2014.12.017

基于无干扰理论的交换行为可信性分析方法

孙奕[1,2,3]，陈性元[4]，杜学绘[2,3]，雷程[4]

（1. 北京交通大学 计算机与信息技术学院，北京 100044；2. 解放军信息工程大学 四院，河南 郑州 450004；
3. 数学工程与先进计算国家重点实验室，河南 郑州 450004；4. 解放军信息工程大学 三院，河南 郑州 450004）

摘 要：针对目前数据安全交换中缺乏对交换行为的动态监管，无法保障数据交换的安全实施问题，提出一种基于无干扰理论的交换行为可信性分析方法。该方法首先从交换进程的角度对交换行为进行形式化建模，然后将无干扰理论与可信计算的思想相结合，提出不同阶段、不同模式下交换行为可信的约束规则，交换行为可信性判定定理及安全证明，最后结合一个具体的应用示例说明该方法的可用性。

关键词：无干扰策略；受控交换；进程行为；可信

中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2014)12-0144-09

Method for trust analysis of exchange process behavior based on noninterference

SUN Yi[1,2,3], CHEN Xing-yuan[4], DU Xue-hui[2,3], LEI Cheng[4]

(1. School of Computer&Information Technology, Beijing Jiaotong University, Beijing 100044, China;
2. The Fourth College, PLA Information Engineering Universiry, Zhengzhou 450004, China;
3. State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450004, China;
4. The Thind College, PLA Information Engineering University, Zhengzhou 450004, China)

Abstract: Aiming at the problem of dynamic data security exchange behavior cannot be controlled, methods for trusted analysis of exchange process behavior based on noninterference are proposed. First, the exchange behavior model is formalized from the perspective of the exchange process. Then, the exchange behavior trust constraint rules, exchange behavior trust judgment theorem and security proof are given in different stages and different mode. Finally, a concrete application example shows the availability of the method.

Key words: noninterference policy; controlled exchange; process behavior; trust

1 引言

随着云计算、物联网、P2P 等大规模复杂网络的快速发展，信息安全共享与交换问题变得越来越重要。人们在享受信息共享、互联互通所带来方便的同时，也面临着敏感信息泄露、隐私泄露等安全威胁。因此实现安全的数据交换是目前网络安全中亟待解决的问题。

数据安全交换所面临的主要安全威胁之一是对交换行为的攻击，通过执行来自内部的或外部的恶意代码，对交换进程进行破坏、伪装或劫持，使交换行为无法正确执行，间接造成信息的篡改、泄漏和非授权访问等安全威胁。因此确保交换行为的可信性是实现数据安全交换的关键。

本文主要针对目前数据安全交换中缺乏对交换行为的动态监管，无法保障数据交换的安全实施问题，从信息流的角度，结合可信计算的思想提出一种基于无干扰理论的交换行为可信性分析方法，

收稿日期：2013-10-03；**修回日期**：2013-12-31

基金项目：国家重点基础研究发展计划（“973”计划）基金资助项目（2011CB311801）；国家高技术研究发展计划（“863”计划）基金资助项目（2012AA012704）；河南省科技创新人才计划基金资助项目（114200510001）

Foundation Items: The National Basic Research Program of China (973 Program)(2011CB311801); The National High Technology Research and Development Program of China (863 Program)(2012AA012704); Innovation Scientists and Technicians Troop Construction Projects of Henan Province (114200510001)

为交换行为的动态管控提供理论依据。

2　相关工作

2.1　无干扰理论概述

Goguen 和 Meseguer 在文献[1]中第一次提出了无干扰概念。无干扰概念是信息流形式化定义或表示不同安全域间的因果关系的主要方法之一，为规范和分析安全策略提供一个理论基础。关于无干扰理论早期的工作主要用于多级安全系统，处理确定性系统和具有偏序关系的信息流策略。简单地说就是 2 个不同等级的安全域 H 和 L 的域间策略，即可以是 $L \to H$ 但不能是 $H \to L$ 。这种策略是一种传递性策略，基于这些限制又提出了许多无干扰的定义[2~6]。传递性无干扰策略成功的为多级安全策略（MLS）提供了支撑基础并给出了形式化证明的方法[7,8]。

虽然传统的无干扰理论成功地解决了多级安全策略，但是一些实际的安全问题超出了他们最初定义的形式化描述。这些模型在现实应用中有很大的局限性。例如作战指挥系统，该系统基于 MLS 只允许信息从低等级域到高等级域，这样下级向上级汇报工作时，不会由于木马攻击导致信息泄漏。但是当上级需要下发作战数据协调指挥整体作战时就存在了很大的问题，需要系统允许受限的信息流从高等级域流转到低等级域。也就是说需要限制信息流从高等级域流向低等级域只能通过一个可信的控制域（例如降级处理、脱密处理或加密设备），不能直接从高等级域到低等级域。因此在现实世界中更多的需要的是一种非传递的信息流策略。早期 Rushby 在这方面做出了许多努力，第一次提出了“信道控制”的概念[9]。随后，Boebert 和 Kain 在文献[10]中采用“类型强制 (type enforcement)”和“可信管道(assured pipelines)”来处理这些特殊的信息流。典型的例子是“标记”问题，这种系统策略要求只有被标记过的文件才能被打印。

虽然 Goguen 和 Meseguer 在文献[7]中扩展了他们的工作来描述这些关心的问题，但第一次真正完整描述非传递无干扰理论的是 Haigh 和 Young 在文献[11]中提出的。Rushby 在文献[12]中进一步描述了非传递无干扰策略，将非传递无干扰策略作为一个信息控制策略模型、无干扰的一般化模型和类型强制模型进行了介绍，得出一个对于信道控制例子的展开定理，展示了当干扰关系具有传递性时，传统的多级安全策略是信道控制策略的一个特例，并且讨论了早期形式化的脆弱性并给出了一个十分详细的形式化证明。有关无干扰理论具体概念、定义及定理见文献[12]，这里不再赘述。

最近，Van Der Meyden 等[13,14]针对非传递无干扰策略安全定义存在的缺陷，提出一些改进的定义——TA-security 和 TO-security。Meyden 指出传递性无干扰理论是 P-security，要求最为严格，非传递无干扰理论是 IP-security，要求又太弱。因此给出了介于 2 种定义强度之间的定义 TA-security 和 TO-security，并对这 4 种无干扰策略的复杂度进行了对比与分析。Meyden 第一次建立了一个在系统中允许的可操作的最大信息流模型，并且将实际的信息流和这个最大信息流进行了比较。改进的定义避免了非传递的基于 ipurge 函数定义的一些缺陷，引出了比 Rushby 工作中更满意的证明理论和访问控制系统。此外，近年来无干扰策略除了在理论方面的研究，在实践上也获得了新的进展，如 Sfaxi 等[15]实现了一种用于实现无干扰策略的工具，使用这些工具可以检测系统的安全漏洞，保证系统代码的安全性。

2.2　行为可信性研究现状

针对行为可信性方面的研究主要集中在采用概率论和数理统计的方法对系统行为进行建模和评估[16~19]，基于无干扰理论分析系统行为可信性的研究较少。本文研究基于无干扰理论分析交换进程行为可信性的主要思路是：首先根据 TCG，从进程角度给出行为可信的判定式，即一个实体的行为是可信的，如果它的行为总是以所期望的方式朝着预期的目标执行；然后给出一定的约束规则；最后基于无干扰理论对行为的可信性进行证明。文献[20~24]结合可信计算从进程角度分析了传递无干扰模型。文献[25]进一步扩展分别给出了基于传递无干扰和非传递无干扰理论的软件动态行为可信性推演方法。但是现有研究未考虑网络环境下安全交换行为的特征，而且随着无干扰理论的进一步发展，对基于无干扰理论的行为可信性分析提出新的挑战，因此为了更加准确的分析交换行为的可信性，本文结合新的无干扰理论研究成果[13,14]，提出分阶段、分模式对交换行为进行分析，给出相应的可信性推演方法，为实现交换行为可信性判定提供理论依据。

3　一种数据安全交换行为可信性分析方法

本节提出一种基于无干扰理论的数据安全交

换进程行为可行性分析方法。

3.1 交换行为的形式化建模

首先对数据安全交换中关键元素和函数进行定义，然后从交换进程的角度对交换行为进行建模。

定义 1 交换节点

交换节点表示网络环境下参加数据交换的节点。用集合 $N \subseteq MN \cup SN$ 表示交换节点集合，其中，MN 表示主交换节点集合，SN 表示从交换节点集合。

定义 2 交换进程

交换进程表示数据交换系统中用于完成交换任务的专用交换进程。用 $P \subseteq MP \cup SP$ 表示交换进程集合，其中，MP 表示主交换进程集合，SP 表示从交换进程集合。用 $\lambda = p*$ 来表示交换进程集合的子集合。λ 是 p 的传递闭包，表示执行的进程集合列表。

交换进程与交换节点存在关系 $res: P \to N$，即如果 $res(p) \in MN$ 表示进程运行在主交换节点上，交换进程 $p \in MP$；如果 $res(p) \in SN$ 表示交换进程运行在从交换节点上，则交换进程 $p \in SP$。换句话说这里以节点为单位定义交换进程执行环境，一个交换进程执行所需要的资源集合环境定义为一个节点。

定义 3 交换进程状态转移函数

单步状态转移函数 $next: X \times \Sigma \to X$，定义进程执行单步操作的状态迁移函数。其中，

1) $X = \{x, y, z, \cdots\}$ 定义进程状态集合，$x_0 \in X$ 表示初始状态；

2) $\Sigma = \{\sigma_1, \sigma_2, \cdots, \sigma_n\}$ 定义进程执行的操作集合，l 是 σ 的传递闭包，表示执行的操作序列集合。如 $x, y \in X, \sigma \in \Sigma$，则 $next(x, \sigma) = y$。

3) 操作与交换进程间的映射函数 $pro: \Sigma \to P: pro(\sigma)$ 表示执行操作 σ 的进程。

多步状态迁移函数 $run: X \times \Sigma^* \to X$，定义进程执行多步操作的状态迁移函数。则

$$run(x, \Lambda) = x \quad (\Lambda \text{表示空操作})$$

$$run(x, \sigma \circ l) = run(next(x, \sigma), l)$$

多进程行为迁移函数 $exc: X \times P^* \to X$，定义多进程执行后的状态迁移函数。

$$exc(x, \varepsilon) = x \quad (\varepsilon \text{ 表示无进程执行})$$

$$exc(x, pro(\sigma) \circ \lambda) = exc(next(x, \sigma), \lambda) = run(next(x, \sigma), l)$$

定义 4 交换行为

$$\begin{array}{ccccccccc} x_0 & \xrightarrow{pro(\sigma_0)} & x_1 & \xrightarrow{pro(\sigma_1)} & x_2 & \xrightarrow{pro(\sigma_2)} & x_3 & \cdots & \xrightarrow{pro(\sigma_{n-1})} x_n \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ o_0 & & o_1 & & o_2 & & o_3 & & o_n \end{array}$$

用上式来表示执行一次交换任务的行为，记为 $A(X, \Sigma, O)$。其中，交换进程行为轨迹集合 $B = \{B_{p_1}, B_{p_2}, \cdots, B_{p_n}\}$ 表示交换进程的行为轨迹集合。

行为轨迹集合中的每一个行为轨迹用成对出现的状态和操作来描述，记为 $B_{p_i}(X, \Sigma)(1 \leqslant i \leqslant n)$。行为轨迹中除了初始状态以外，每一个状态都与一个操作相对应。特别地，当 p_i 相同时，表示一个进程执行一系列操作产生的行为轨迹。

行为输出集合 $O = \{o_1, o_2, \cdots, o_n\}$ 表示进程执行操作后产生的可观测输出集合。

定义 5 交换进程行为函数

视图函数 $view: X \times P \times \Sigma \to O$，表示进程 P 在状态下 X 执行操作 σ 后产生的输出值。

轨迹函数 $Trace: P \times X \to B$，表示进程在状态 X 下执行后产生的行为轨迹。轨迹函数本质上是一个二元数组，记录了进程行为中配对的状态和操作集合。

定义 6 进程间通信策略 $\mapsto$

设 $\mapsto$ 是 $P \times P$ 上的自反关系，即 $\mapsto \subseteq P \times P$。

进程间通信策略定义了交换进程之间的干扰关系，或者说是信息流动的方式。$p_i \mapsto p_j$ 表示交换进程 p_i 满足策略 $\mapsto$ 时可以和进程 p_j 通信，反之 $p_i \not\mapsto p_j$ 表示专用交换进程 p_i 不能和进程 p_j 通信。直观上说 p_i 可以和进程 p_j 通信，意味着有信息从 p_i 流向进程 p_j。

定义 7 等价关系

设 $\approx^p$ 是 $X \times X$ 上的等价关系，$\forall x, y \in X$, 若

$$Trace(p, x) = Trace(p, y)$$

且 $view(pro(\sigma), x) = view(pro(\sigma), y)$

则 $x \approx^p y$

如果进程 p 在状态 x 和 y 下执行 σ 后的行为是一致的，则 x 和 y 对于进程 p 是等价的。

为了更加准确分析交换行为的可信性，根据数据安全交换的特征，交换行为主要分为 2 个阶段：单交换进程运行阶段和多交换进程交换阶段。下面分别从这 2 个阶段对交换进程行为的可信性进行分析。

3.2 单交换进程行为可信性分析方法

单交换进程运行阶段是指从交换进程在接入交换网络之前，独立运行在从交换节点的阶段，该阶段主要完成从数据源提取交换数据及对交换数

据进行转换的操作，交换数据的传递都是在单交换进程内部进行的，因此单交换进程运行阶段交换行为本质上是一种传递性无干扰关系。也就是说，从交换节点上交换进程行为的可信性可以依据传递性无干扰策略进行判定。下面基于传递性无干扰策略给出对单交换进程行为可信性进行分析的具体方法。

定义 8　隔离函数

$$Iso(\Lambda, p) = \Lambda$$

$$Iso(l \circ \sigma, p) = \begin{cases} Iso(l, p) \circ \sigma, & pro(\sigma) \mapsto p \\ Iso(l, p), & \text{其他} \end{cases}$$

隔离函数是清除了安全策略中不允许的来自系统或其他进程的操作，即只保留了预期允许干扰从交换进程的操作集合。隔离函数为交换进程提供了一个理想的、不受非法干扰的、相对隔离的执行环境，确保交换进程在提取数据时行为的可信性。

定义 9　单交换进程行为可信性判定式

$$Trace(p, run(x_0, l)) = Trace(p, run(x_0, Iso(l, p)))$$

等式左边表示交换进程实际执行的行为轨迹，等式右边表示在经过隔离函数清除后，理想情况下交换进程行为轨迹。如果 2 种情况下进程行为轨迹是一致的，则交换进程行为是可信的。

定义 10　交换进程行为是一致的，当且仅当交换进程行为满足以下约束。

约束 1：$x \approx^{pro(\sigma)} y \rightarrow next(x, \sigma) \approx^{pro(\sigma)} next(y, \sigma)$

约束 2：$pro(\sigma) \not\rightarrow p \rightarrow x \approx^{p} next(x, \sigma)$

约束 3：$x \approx^{p} y \rightarrow Trace(p, x) = Trace(p, y)$

约束 1 要求如果进程在 2 个等价状态下执行相同的单步操作，则执行操作后迁移的状态也是等价的。约束 2 要求如果操作 σ 的执行不能干扰进程 p，则操作执行前和执行后的状态是等价的。约束 3 要求如果进程在 2 个状态下是等价，则执行操作 σ 后产生的行为轨迹是一致的。

定理 1　如果交换进程行为满足定义 10 中约束条件则单交换进程行为是动态可信的。

证明　即证明 $Trace(p, run(x_0, l)) = Trace(p, run(x_0, Iso(l, p)))$ 可通过对 l 的长度进行归纳来证明。

基础：如果 $l = \Lambda, run(l, x) = x$ 且 $Iso(\Lambda, p) = \Lambda$，则命题成立。

假设：如果 $l = \sigma_1, \cdots, \sigma_n$，则 $x \approx^{p} y \Rightarrow run(x, l) \approx^{p} run(y, Iso(l, p))$。

归纳：考虑 $l \circ \sigma$。假设 $x \approx^{p} y$，对 $run(y, Iso(l \circ \sigma, p))$，考虑 2 种不同情况。

①如果 $pro(\sigma) \rightarrow p$

由 *run* 函数的定义 $run: X \times \Sigma^* \rightarrow X$ 得

$$\begin{aligned} & l \circ \sigma = p_1, \cdots, p_n, \sigma \Rightarrow run(x, l \circ \sigma) \\ & = step(step(p_n, \cdots, step(p_1, x)), \sigma) \\ & \Rightarrow run(x, l \circ \sigma) = step(run(x, l), \sigma) \end{aligned} \tag{1}$$

由隔离函数 Isolation 的定义得

$$Iso(l \circ \sigma, p) = Iso(l, p) \circ \sigma \tag{2}$$

由式(1)、式(2)得

$$\begin{aligned} run(y, Iso(l \circ \sigma, p)) &= run(y, Iso(l, \sigma) \circ p) \\ &= next(run(y, Iso(l, \sigma)), p) \end{aligned} \tag{3}$$

由于系统满足约束 1，得

$$x \approx^{pro(\sigma)} y \rightarrow next(x, \sigma) \approx^{pro(\sigma)} next(y, \sigma) \tag{4}$$

由式(3)及根据归纳假设可以得到

$$next(run(x, l), p) \approx^{p} next(run(y, Iso(l, p)), \sigma) \tag{5}$$

由式(3)、式(5)得

$$step(run(x, l), \sigma) \approx^{p} run(y, Iso(l \circ \sigma, p)) \tag{6}$$

根据式(1)，式(6)可转化为

$$run(x, l \circ \sigma) \approx^{p} run(y, Iso(l \circ \sigma, p)) \tag{7}$$

假设得证。

②如果 $pro(\sigma) \not\rightarrow p$

根据隔离函数的定义得

$$Iso(l \circ \sigma, p) = Iso(l, p) \tag{8}$$

进一步得出

$$run(y, Iso(l \circ \sigma, p)) = run(y, Iso(l, p)) \tag{9}$$

根据归纳假设可得

$$run(x, l) \approx^{p} run(y, Iso(l \circ \sigma, p)) \tag{10}$$

由于系统满足约束 2，对于任意 x 有 $x \approx^{p} step(x, \sigma)$ 得出

$$next(run(x, l), \sigma) \approx^{p} run(x, l)$$

将上式代入式(10)得

$$\begin{aligned} & next(run(x, l), \sigma) = run(x, l \circ \sigma) \\ & run(x, l \circ \sigma) \approx^{p} run(y, Iso(l \circ \sigma, p)) \end{aligned}$$

假设成立。在上述 2 种情况下，假设总是成立的。归纳步骤结束。

根据以上的归纳假设，又根据系统满足约束 3，

令 $l\circ\sigma=l, x=y=x_0$，得出

$$Trace(p, run(x_0, l))=Trace(p, run(x_0, Iso(l, p)))$$

证毕。

3.3 多交换进程行为可信性分析方法

多交换进程交换阶段主要发生在从交换进程接入交换网络之后，与主交换进程之间进行交互实现交换数据的传递。而不同从交换进程之间不能直接通信必须在主交换进程的控制下间接通信，因此多进程交换阶段的进程行为本质上是一种非传递性无干扰关系。也就是说此时交换进程行为的可信性可以依据非传递性无干扰策略进行判定。由于从交换进程通过主交换进程进行安全交换时可以通过集中式和分布式 2 种模式来实现，而且 2 种情况下对交换行为可信性的要求是不同，因此下面分别从集中式和分布式 2 种模式，给出对交换进程行为可信性分析的具体方法。

3.3.1 集中式多交换进程行为可信性分析方法

在多进程交换阶段，为了实现不同从交换进程之间的受控交换，需要放宽隔离的条件。

隔离函数是清除所有在策略 $\mapsto$ 下不允许与进程 p 通信的一系列进程。这种要求过于苛刻，无法实现受控交换，所谓受控交换就是在主交换进程控制下完成不同从交换进程之间的受限信息交换。为了实现受控交换，首先定义交换进程列表函数，该函数表明，一个进程执行之前产生的操作是否影响了 q，决定于是否存在 $q\in list(l,p)$ 并且满足 $pro(\sigma)\mapsto q$。在此基础上，定义交换链函数。

定义 11 交换进程列表函数 *list*

$list:\Sigma^*\times P\to\delta(P)$　　$\delta(P)$表示p的幂集

$list(\Lambda,p)=\{p\}$

$$list(l\circ\sigma,p)=\begin{cases}list(l,p)\cup\{pro(\sigma)\},\\ \exists q: q\in list(l,p)\wedge pro(\sigma)\mapsto q\\ list(l,p),\text{其他}\end{cases}$$

定义 12 交换链函数 *chain*

$chain:P^*\times P\to P^*$

$chain(\Lambda,p)=\Lambda$

$$chain(l\circ\sigma,p)=\begin{cases}\sigma\circ chain(l,p),\\ pro(\sigma)\in list(l\circ\sigma,p)\\ chain(l,p),\text{其他}\end{cases}$$

交换链函数定义了清除所有不能直接或间接干扰给定进程 p 的进程执行序列。换句话说是定义了参与一次交换过程中预期执行的交换进程集合。

定义 13 集中式多交换进程行为可信性判定式

$$Trace(p, run(x_0, l))=Trace(p, exc(x_0, chain(\lambda, p)))$$

等式左边表示多交换进程实际执行的行为轨迹，等式右边表示在经过交换链函数清除后，理想情况下集中式多交换进程行为轨迹。如果 2 种情况下进程行为轨迹是一致的，则集中式多交换进程行为是动态可信的。

为了确保在数据交换阶段进程行为的可信性，交换进程对于非传递无干扰策略 $\mapsto$ 是安全的，需要对定义 10 中的约束 1 进行弱化，给出约束 4。这允许从交换进程干扰主交换进程，主交换进程干扰从交换进程，或者从交换进程和主交换进程一起干扰从交换进程，但不允许从交换进程直接干扰从交换进程，具体定义如下：$sp_i\mapsto np; np\mapsto sp_j; sp_i\not\mapsto sp_j$。这是一种非传递的无干扰策略。

约束 4：$x\approx^p y\wedge x\approx^{pro(\sigma)} y\to next(x,\sigma)\approx^p next(y,\sigma)$

约束 4 要求如果 2 个状态对于进程 p 是等价的并且对于执行 σ 的进程也是等价的，则在这 2 个状态下执行 σ 后的迁移状态对于进程 p 依然是等价的。也就是说，在非传递无干扰策略中允许存在其他进程的操作，只要该进程执行后的迁移状态依然是等价的。

定理 2 如果交换进程行为满足约束 2~约束 4 则集中式多交换进程行为是动态可信的。

证明 即证明

$$Trace(p, run(x_0, l))=Trace(p, exc(x_0, chain(\lambda, p)))$$

可通过对 l 的长度进行归纳来证明。以下证明方法与定理 1 类似，这里不再赘述。

3.3.2 分布式多交换进程行为可信性分析方法

当数据安全交换通过统一的可信交换节点进行交换时以上情况是安全的。但是在分布式模式下由多个主交换进程向一个从交换进程交换信息时，负责接收的从交换进程可以根据进程行为轨迹的序列来进行隐蔽通信。举例说明如下。

实例 在分布式数据安全交换系统中，用 S、C、R 分别表示交换数据发送方、交换控制方、交换数据接收方。其中发送方 S 分别有 2 个发送进程 S_1，S_2；控制方也有 2 个主交换进程 C_1，C_2 其信息传递情况如图 1 所示。

根据非传递无干扰策略，由于策略允许 $S\to C\to R$，所以可能出现的情况就是如果存在 2 个高安全域 S_1、S_2，它们分别通过不同的主交换进

程 C_1、C_2 向同一个 R 传递信息。根据 *chain* 函数的定义 C_1、C_2 只能观测到与它直接相关的 S_1、S_2 的行为，并将其传递给 R，而 R 本身可以观测到整个行为序列。那么，假设 C_1、C_2 先后顺序是固定的，令 $\alpha = s_1, s_2, c_1, c_2; \beta = s_2, s_1, c_1, c_2$，根据以上的非传递无干扰策略判定行为是可信的，但由于 R 可以观测整个行为序列因此可以识别出 α, β 的不同，而这种区别 C_1 和 C_2 是不知道，这样就在 S 和 R 之间形成了隐信道。

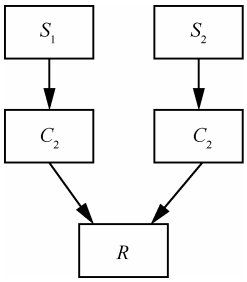

图 1　信息传递

为了解决以上问题 Van Der Meyden 在文献[14]对非传递无干扰策略的安全定义进行改进。称能够满足改进的非传递无干扰策略的系统是 TA-security。本文基于改进的非传递性无干扰理论对交换链函数进行改进给出交换树函数的定义。

首先定义一个二叉树 $T(S, \Sigma)$，其中，$S \subseteq P$。二叉树的构成如下：把初始状态 x_0 作为树的根节点，操作序列 Σ 中的元素作为树的内节点，交换进程集合 S 中的元素作为树的叶子节点。

定义 14　交换树函数

$$trm: l \to T(\{\Lambda\}, \sigma)$$

$$trm(\Lambda, p) = \Lambda$$

$$trm(l \circ \sigma, p) = \begin{cases} trm(l, p), & pro(\sigma) \not\mapsto p \\ (trm(l, p), trm(l, pro(\sigma), \sigma)), & \\ pro(\sigma) \mapsto p & \end{cases}$$

根据 TA-security 的定义，定义了交换进程的交换树函数，该函数可以区别不同序列的交换链从而有效地防止了通过改变行为序列进行的信息传递，消除了基于交换进程行为序列的隐信道。

分布式交换进程行为的可信性判定方法介于以上 2 种方法之间，没有第一种方法苛刻但又比第二种方法要求严格。

定义 15　分布式多交换进程行为可信性判定式

$$Trace(p, run(x_0, l)) = Trace(p, exc(x_0, trm(l, p))))$$

该等式表示分布式多交换进程实际执行的行为轨迹与经过交换树函数清除后分布式多交换进程行为轨迹是一致的，则分布式多交换进程行为是动态可信的。

分布式多交换进程行为的可信性，我们需要考虑一种特殊的等价关系即约束 5，利用此等价关系来扩展无干扰理论展开条件的完整性。

约束 5：$\forall l \subseteq \Sigma^*, x \approx^p y \to run(x, l) \approx^p run(y, l)$

定理 3　如果分布式交换进程行为满足约束 2~约束 5，则分布式多交换进程行为是动态可信的。

证明　即证明

$$Trace(p, run(x_0, l)) = Trace(p, exc(x_0, trm(l, p)))$$

由约束 5 对于 $\forall l, l' \subseteq \Sigma^*, p \in P$ 如果 $trm(l, p) = trm(l', p)$，则 $run(x_0, trm(l, p)) \approx^p run(x_0, trm(l', p))$。

由约束 3 和 $exc(x, pro(\sigma) \circ \lambda) = exc(next(x, \sigma), \lambda) = run(next(x, \sigma), l)$，得出

$$Trace(p, run(x_0, trm(l, p))) = Trace(p, exc(x_0, trm(l', p)))$$

问题即可得证。因此问题转化为证明

$$trm(l, p) = trm(l', p)$$
$$\Rightarrow run(x_0, trm(l, p)) \approx^p run(x_0, trm(l', p))$$

下面通过对 l 和 l' 的长度进行归纳来证明。

显然 $l = l' = \Lambda$（Λ 为空），结论成立。

假设下式成立：

$$trm(l, p) = trm(l', p)$$
$$\Rightarrow run(x_0, trm(l, p)) \approx^p run(x_0, trm(l', p)) \quad (11)$$

归纳：考虑 $l \circ \sigma$，则只需证明下式成立即可。

$$trm(l, p) = trm(l', p)$$
$$\Rightarrow run(x_0, trm(l, p) \circ \sigma) \approx^p run(x_0, trm(l', p))$$

下面分 2 种情况讨论。

① 如果 $pro(\sigma) \mapsto p$

$$trm(l \circ \sigma, p) = (trm(l, p), trm(l, pro(\sigma)), \sigma) \quad (12)$$

式(12)隐含表达了对进程 p 有干扰的操作 σ 也出现在 l' 中，不妨设为 l' 中的最后一个操作，则 l' 可记做 $l' = \lambda\sigma$。

$$trm(l', p) = trm((\lambda \circ \sigma), p)$$
$$trm((\lambda \circ \sigma), p) = (trm((\lambda, p), trm(\lambda, pro(\sigma)), \sigma) \quad (13)$$

由于

$$trm(l \circ \sigma, p) = trm(l', p) \quad (14)$$

由式(12)，式(13)得

$$trm(l, p) = trm(\lambda, p) \quad (15)$$

$$trm(l, pro(\sigma)) = trm(\lambda, pro(\sigma)) \tag{16}$$

由式(11)、式(15)得

$$run(x_0, trm(l, p)) \approx^{p} run(x_0, trm(\lambda, p)) \tag{17}$$

由式(11)、式(16)得

$$run(x_0, trm(l, pro(\sigma))) \approx^{pro} run(x_0, trm(\lambda, pro(\sigma))) \tag{18}$$

由式(17)、式(18)和约束 4 得

$$next(run(x_0, trm(l, p)), \sigma) \approx^{p} next(run(x_0, trm(\lambda, p)), \sigma) \tag{19}$$

$$next(run(x_0, trm(l, p)), \sigma) = run(x_0, trm(l, p) \circ \sigma) \tag{20}$$

$$next(run(x_0, trm(\lambda, p)), \sigma) = run(x_0, trm(\lambda, p) \circ \sigma) = run(x_0, trm(l', p)) \tag{21}$$

由式(19)~式(21)得

$$run(x_0, trm(l, p) \circ \sigma) \approx^{p} run(x_0, trm(l', p))$$

假设成立。

② 如果 $pro(\sigma) \not\sim p$

$$trm(l, p) = trm(l \circ \sigma, p) = trm(l', p) \tag{22}$$

由约束 2 得

$$run(x_0, trm(l, p) \circ \sigma) = next(run(x_0, trm(l, p)), \sigma)$$

$$next(run(x_0, trm(l, p)), \sigma) \approx^{p} run(x_0, trm(l, p)) \tag{23}$$

根据归纳假设、式(11)和式(23)得出

$$trm(l \circ \sigma, p) = trm(l', p)$$

$$\Rightarrow run(x_0, trm(l, p) \circ \sigma) \approx^{p} run(x_0, trm(l', p))$$

假设成立。

在上述 2 种情况下，假设总是成立的。归纳步骤结束。证毕。

4 交换进程行为可信性分析在数据安全交换中的应用

根据基于互联网电子政务信息实施指南 GB/Z 24294[26]中分域控制的要求，互联网电子政务安全域划分为内部数据处理区域、公开数据处理区域、其中公开数据处理区域用来承载处理公开信息的电子政务应用系统及其数据库，处理对公众和企业开放的服务，如政策发布、政府网站或便民服务等，这些都是提供给公众访问的公开数据。内部数据处理区用来承载处理内部信息的电子政务应用系统及其数据库，处理政府内部和部门之间的业务，这些是仅允许系统内部人员访问的内部数据。

为了解决互联网电子政务信息的安全共享与交换问题，需要在内部数据处理区与公开数据处理区之间实现数据安全交换。图 2 描述了基于交换进

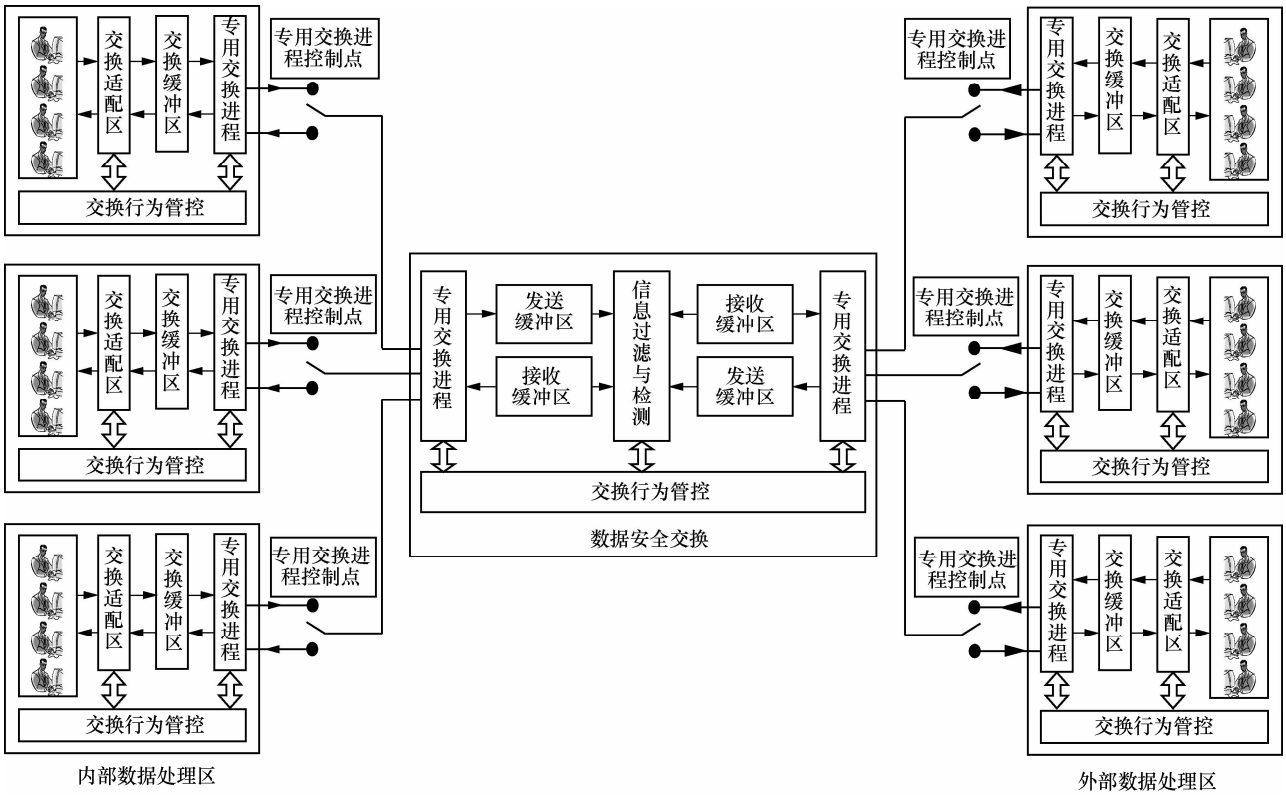

图 2 基于交换进程的数据安全交换系统框架

程的数据安全交换系统框架。首先内部数据处理区中的交换适配区根据定制的交换策略从政务办公系统中提取交换信息，将交换信息转换为统一的 XML 格式，放入交换缓冲区。接着合闭专用进程控制点，启动内部处理区和交换主节点的专用进程将信息从内部处理区的缓冲区交换到主节点的缓冲区中，任务完成后打开专用进程控制点。然后对缓冲区中的信息进行过滤并依据定制的交换任务将过滤后的信息调度到相应的接收缓冲区中，最后交换主节点和公开数据处理区的专用交换进程控制点合闭，启动专用进程将信息交换到公开数据处理区的交换缓冲区中，经过适配区的转换发送给公共服务系统。整个交换过程均在交换行为的管控下进行，当出现异常行为时立即终止信息交换。

图 3 描述了实现数据安全交换进程行为可信性分析的工作原理。交换行为收集器(BeCollect, behavior collector)负责对专用交换进程的执行环境和运行时信息进行收集和检查，并将结果交予交换进程行为控制裁决器；交换行为控制裁决器（BeControl, behavior control decision）负责将收集到行为轨迹与可信环境下交换行为轨迹进行完整性匹配，并根据匹配结果裁决交换进程行为是否可信；从而决定是否允许从交换进程接入交换网络；交换行为完整性根（BeIntR, behavior integrity root）管理可信环境下交换进程行为模型，是交换进程行为完整性判断的依据。

在从交换节点上，每个从交换进程 SP 通过信道调用系统服务，调用被 BeCollect 捕获，BeCollect 通过信道获得来自 BeControl 对单交换进程行为可信性分析的裁决结果，控制从交换进程的接入访问。

在主交换节点上，每个主交换进程 MP 通过信道调用系统服务，调用被 BeCollect 捕获，BeCollect 通过信道获得来自 BeControl 对多交换进程行为可信性分析的裁决结果，控制主交换进程对交换区（ExArea, exchange area）的访问。

综上所述，单交换进程行为可信性分析方法，为交换进程连接交换网络提供依据，交换进程行为裁决器可以根据对单交换进程行为可信性分析结果来判断从交换节点上交换进程行为的可行性，裁决是否允许交换进程连接交换网络，从而保证只有可信的交换进程才能接入交换网络，防止恶意进程连接交换网络，保障了数据交换网络的连接可控。多交换进程行为可信性分析方法，为交换网络中多交换进程交互行为可信性提供依据，交换进程行为裁决器可以根据对多交换进程行为可信性分析结果判断不同交换进程之间交互的安全性，确保了数据交换过程的可管可控。

5　结束语

本文首先对交换行为进行形式化建模，然后结合数据安全交换行为特征分别从单交换进程行为、集中式多交换进程行为和分布式多交换进程行为 3 个方面对交换行为的可信性进行分析。最后给出相

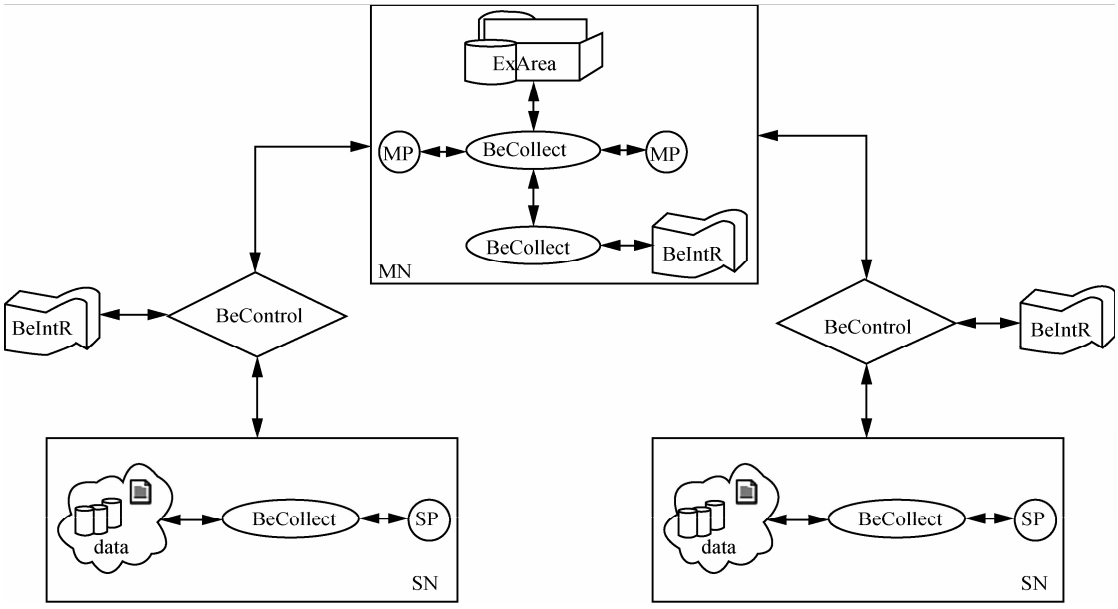

图 3　工作原理

应的行为可信性判定定理和约束条件，并对定理的正确性进行了证明。

交换行为可信性分析是研究数据安全交换必须解决的关键问题之一。伴随着网络技术的快速发展，以及人们对信息共享的强烈需求，如何确保信息的安全交换与共享必然成为人们关注的主要问题，研究交换行为可信性正是解决这些问题的关键所在。目前针对交换行为可信性的研究还主要集中在工程方面缺乏理论方面的研究，本文给出的基于无干扰理论的交换行为可信性分析方法，从理论上给出了分析交换行为可信性的依据，为进一步的工程实现提供理论支撑。

参考文献：

[1] GOGUEN J, MESEGUER J. Security policies and security models[A]. Proc IEEE Symp on Security and Privacy[C]. Oak-land, 1982.11-20.

[2] SUTHERL D. A model of information[A]. Proc 9th National Computer Security Conf[C]. 1986.175-183.

[3] WITTBOLD J T, JOHNSON M. Information flow in non- deterministic systems[A]. IEEE Symposium on Security and Privacy[C]. 1990.144-161.

[4] MCCULLOUGH D. Noninterference and the composability of security properties[A]. Proc IEEE Symp on Security and Privacy[C]. 1988.177-186.

[5] FOCARDI R, GORRIERI R. Classification of security properties(Part I: information flow)[J]. Foundations of Security Analysisand Design, 2001, 2171:331-396.

[6] RYAN P. Mathematical models of computer security[J]. Foundations of Security Analysis and Design, 2001, 2171: 1-62.

[7] GOGUEN J, MESEGUER J. Unwinding and inference control[A]. IEEE Symp on Security and Privacy[C]. 1984.75

[8] ROSCOE A W, GOLDSMITH M H. What is intransitive noninterference[A]. Proceedings of the 12th IEEE Computer Security Foundations Workshop[C]. 1999.228-238.

[9] RUSHBY J M. Design verification of secure systems[A]. Proceedings of the eighth ACM symposium on Operating systems principles[C]. 1981.12-21.

[10] BOEBER E, KAIN R. A practical alternative to hierarchical integrity policies[A]. Proceedings of the Computer Security Initiative Conference[C]. 1985.

[11] HAIGH J, YOUNG W. Extending the noninterference version of MLS for SAT[J]. IEEE Trans. on Software Engineering, 1987,13(2): 141-150.

[12] RUSHBY J. Noninterference, transitivity, and channel-control security policies[EB/OL]. http://www.csl.sri.com/papers/csl-92-2/,1992.

[13] VAN DER MEYDEN R. Architectural refinement and notions of intransitive noninterference[J]. Formal Aspects of Computing, 2012,24(4):769-792.

[14] EGGERT S, VAN DER MEYDEN R, SCHNOOR H, *et al*. The complexity of intransitive noninterference[A]. 2011 IEEE Symposium on Security and Privacy (SP)[C]. 2011.196-211.

[15] SFAXI L, ABDELLATIF T, ROBBANA R, *et al*. Information flow control of component-based distributed systems[J]. Concurrency and Computation: Practice and Experience, 2013,25(2):161-179.

[16] ZHANG Z, NAIT-ABDESSELAM F, HO P H. Boosting Markov reward models for probabilistic security evaluation by characterizing behaviors of attacker and defender[A]. Third International Conference on Availability, Reliability and Security[C]. 2008.352-359.

[17] YANG X, LIU L, ZOU R. A statistical user-behavior trust evaluation algorithm based on cloud model[A]. 2011 6th International Conference on Computer Sciences and Convergence Information Technology (ICCIT)[C]. 2011.598-603.

[18] LI J, HE P. The application of fuzzy Markov chains in the analysis of internet glance behavior[A]. 2010 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT)[C]. 2010. 608-611.

[19] VASSILIOU P C G, VASILEIOU A. Asymptotic behaviour of the survival probabilities in an inhomogeneous semi-Markov model for the migration process in credit risk[J]. Linear Algebra and its Applications, 2013, 438(7):2880-2903.

[20] 吴瀛, 江建慧. 基于进程轨迹最小熵长度的系统调用异常检测[J]. 计算机应用,2012, 32(10):3439-3444.
WU Y, JIANG J H. System call anomaly detection with least entropy length based on process traces[J]. Journal of Computer Applications, 2012,32(10):3439-3444.

[21] 张兴, 陈幼雷, 沈昌祥. 基于进程的无干扰可信模型[J]. 通信学报, 2009, 30(13):6-11.
ZHANG X, CHEN Y L, SHEN C X. Non-interference trusted model based on processes[J]. Journal on Communications, 2009,30(13):6-11.

[22] 刘巍伟, 韩臻, 沈昌祥. 基于终端行为的可信网络连接控制方案[J]. 通信学报, 2009, 30(11): 127-134.
LIU W W, HAN Z,SHEN C X. Trusted network connect control based on terminal behavior[J]. Journal on Communications, 2009, 30(11): 127-134.

[23] 谭良, 陈菊. 可信终端动态运行环境的可信证据收集代理[J]. 软件学报, 2012,23(8):2084-2103.
TAN L, CHEN J. Trusted agent for collecting trustworthiness evidence in terminal dynamical running environment[J]. Journal of Software,2012, 23(8):2084-2103.

[24] 杨蓓, 吴振强, 符湘萍. 基于可信计算的动态完整性度量模型[J]. 计算机工程,2012,38(2):78-81.
YANG B, WU Z Q, FU X P. Dynamic integrity measurement model based on trusted computing[J]. Computer Engineering, 2012,38(2): 78-81.

[25] 张帆, 江敏, 吴怀广等. 一种基于无干扰的软件动态行为可信性分析方法[J]. 计算机科学, 2012,39(1):101-103.
ZHANG F,JIANG M ,WU H G, *et al*. Approach for trust analysis of software dynamic behavior based on noninterference[J]. Computer Science,2012,39(1):101-103.

[26] GB/Z 24294 基于互联网电子政务信息安全实施指南[S].
GB/Z 24294. Guide of implementation for Internet-based E-government information security[S].

作者简介：

孙奕（1979-），女，河南郑州人，解放军信息工程大学讲师，主要研究方向为网络与信息安全、数据安全交换。

陈性元（1963-），男，安徽无为人，博士，解放军信息工程大学教授、博士生导师，主要研究方向为网络与信息安全。

杜学绘（1968-），女，河南辉县人，博士，解放军信息工程大学教授、博士生导师，主要研究方向为多级安全、算法分析。

雷程（1989-），男，北京人，解放军信息工程大学硕士生，主要研究方向为网络与信息安全、数据安全交换。