基于灰色时序的完整性规范技术*

樊爱华 陈火旺 齐治昌

(国防科技大学计算机系 长沙 410073)

摘 要 计算机系统的完整性安全策略模型与规范问题，是计算机安全研究中最重要的课题之一。已有的研究结果离实际应用还相差太远，例如 Clark-Wilson完整性模型只是提出了一个框架。本文呈现了我们构造的形式化灰色时序安全策略规范语言 (GTSL)。GTSL的理论基础是灰色系统理论和时序规范语言 LOTOS理论。由于它在完整性规范能力、完整性验证过程的构造与表示、责任分离合理性测试等一系列技术方面的完善与创新，使得 GTSL成为真正能够实际使用的完整性安全策略规范语言。

关键词 安全策略，完整性规范，灰色系统，时序规范

分类号 TP301

The Integrity Specification Techniques Based on the Grey Temporal Ordering Theory

Fan Aihua Chen Huowang Qi Zhichang

(Department of Computer Science, NUDT, Changsha, 410073)

Abstract The formal grey temporal security policy specification language (GTSL) which is designed by us is presented in this paper. The theory basis of GTSL is the theory of grey system and that of LOTOS, the language of temporal ordering specification. Due to the improvement and originality of techniques on the ability of integrity specification, the building and expression of the procedure of integrity verification, the testing of resonability on separation of duty, etc., GTSL becomes practical specification languages for integrity security policy.

Key words security policy, integrity, grey system, temporal specification

计算机安全策略通常分成保密性策略、完整性策略和可用性 (即避免拒绝服务) 策略三类。基于 Bell-LaPadula模型[1]和机制而实施的保密性技术已经比较完善，但正如 Clark和 Wilson指出的，完整性策略模型和实施机制有其独特性，应不同于保密性[2]。完整性安全需求存在于每个信息系统中；商业信息系统尤其需要实施完整性安全。在完整性方面人们已经进行了一些开拓性的研究工作，尤其是 Clark-Wilson模型构造了一个很好的完整性安全框架。但是这些研究由于未能克服一些难题而不能得到实际应用。

本文将首先简介 Clark-Wilson完整性模型，然后探讨 Clark-Wilson模型的缺陷，指出我们在规范完整性安全策略时采用的一些关键技术。接着简要介绍我们提出的灰色时序安全模型 (GTSM) 的理论基础——灰色系统[3]和 LOTOS语言[4]。最后较详细地介绍基于 GTSM 语义而构造的灰色时序安全策略规范语言 (GTSL)。

1 Clark-Wilson完整性模型

完整性是指防止信息被非法修改。完整性安全策略规定了：谁能修改数据，是否可以修改特殊的数据，哪些人的组合可共同修改数据，如何修改数据，可以修改哪些数据项的组合，及修改需遵从哪些

* 1997年 5月 20日收稿
第一作者：樊爱华，女，1966年生，博士

限制等等。Clark-Wilson完整性模型[2]和 Biba完整性模型[5]是两个最著名的完整性模型。Biba完整性模型是一个比较简单的模型，它与最著名的保密性模型 Bell-LaPadula模型正好相反，规定了“不下读”和“不上写”的规则。

Clark-Wilson完整性模型提出了的两个基本实施机制：良式交易和责任分离。系统数据项分为两类：非受限数据项（UDIs）和受限数据项（CDIs）。UDIs是不用保护完整性的客体。CDIs是为它定义了一些完整性特性的、受模型保护的客体。对 CDIs执行两个过程：完整性验证过程（IVPs）和转换过程（TPs）。IVPs定义了为使系统处于有效状态，系统的 CDIs内部之间、以及 CDIs与 CDIs之间必须存在哪些关系；IVPs是评估 CDIs是否处于有效的完整性状态的 CDIs上的布尔函数。TPs是描述了系统如何从一个有效状态转移到另一有效状态的状态转移函数。可以授权特殊的 TPs来读 UDIs、写 CDIs、执行完整性“上写”。在该模型中，完整性策略表达为 TPs和 IVPs的集合。系统必须确保：TPs只能且仅仅代表规定的用户干扰规定的 CDIs 实施面向特殊应用的完整性策略可通过验证 IVPs和 TPs来实现（良式交易）。为了满足责任分离需求，需要验证 TPs的用户处于这种特殊方式：重要的系统动作要求执行不同的 TPs、并涉及不同的用户。

Clark-Wilson模型构造了一个比较好的完整性安全框架。我们在设计网络环境下的安全监测系统时，在完整性检测方面，试图基于 Clark-Wilson模型建立安全检测模型。但是我们发现，该模型仍有一些方面需要完善，例如：

（1）从安全需求的功能范围定义上，Clark-Wilson模型

· 只定义了单层次上的安全需求，未考虑多粒度动态层次的完整性。多粒度动态层次完整性指的是嵌套交易和最低转换过程的层次动态变化。我们在 GTSL中设置了策略嵌套生成和动态灰色粒子。

· 未考虑时序限制，即执行一个逻辑任务中的各个转换过程的顺序应受到限制。我们利用基于推理系统的状态转换语义限制，在 GTSL中设置了时序算子。

· 未考虑并发限制，即多个主体的转换过程互相相关和不相关的并发限制。我们在 GTSL中设置了并发算子。

· 未考虑不可中断状态流限制，即完整地执行一个逻辑任务，而不是部分地执行一个逻辑任务。我们在 GTSL中设置了不可中断算子。

（2）Clark-Wilson模型确保完整性完全依赖于 IVPs的限制，因而不正确的 IVPs对完整性将构成极大的危害。Clark-Wilson模型在结构上显然未考虑 IVPs本身的完整性和可用性。

（3）Clark-Wilson模型把责任分离这个难题交给了安全管理人员，构成了该模型理论上虽无安全漏洞，实际上的漏洞却难以发现和预防的结果。

2 规范完整性安全策略的一些关键技术

如果以 Clark-Wilson模型作为规范完整性安全策略的主要框架，除了完善该模型的功能外，还必须进一步研究如下一些关键技术：

（1）研究表示和构造 IVPs的方法和技术

表示和构造 IVPs应朝着两个目标：（a）把验证的一部分安全负担转移到系统安全控制实施上来，即从与应用相关转移到与应用无关上来。为此，我们采取了数据语义限制（具体地就是采取载体限制）、基于推理系统的状态转换语义限制（可以进行时序限制、并发限制和不可中断状态流限制）和通用验证模型等方法。（b）应能表示 IVPs的自然性和细节封闭。我们在一般的高级语言的数据类型上又扩充了灰色数据类型，用灰色系统理论（如灰色模型、灰色方程、灰色关联）来表示和构造 IVPs。

（2）研究 TPs和实体的表示

从安全的角度看，我们认为系统的安全实施机制并不关心所有的 TPs。因此，我们将 TPs分成三类：黑色操作（系统安全实施机制一点也不关心的 TPs）、白色操作（系统安全实施机制关心所有细节的 TPs）和灰色操作（系统安全实施机制关心部分细节的 TPs）。同样地，从安全的角度看，系统安全实施机制也并不关心所有的实体，而且在规定安全策略时，并非所有的实体属性都是确定的。所以我们

自然地将实体分成三类: 黑色实体 (系统安全实施机制一点也不关心的实体), 白色实体 (系统安全实施机制关心所有属性的实体) 和灰色实体 (系统安全实施机制关心部分属性的实体)。

(3) 规范 Clark-Wilson 模型必须采取合适的理论来规范 IVPs与 TPs之间、TP与 TP之间、IVP与 IVP之间的时序关系。我们选用了面向并行分布式系统的 LOTOS的时序理论。

(4) 责任分离合理性测试

目前都由人工分配责任, 例如把权力分配交给安全管理员。无经验和不合理的责任分离会造成系统很大的损失。最好能利用计算机辅助权力分配并自动测试责任分离的合理性。我们提出了关于完整性责任分离检测的两种形式化方法: 上下级职责明确规则和旁证权力分配规则。它们可以解决大多数完整性的责任分离问题, 如“N 个人”问题, 使合理的责任分离能够达到安全漏洞少、主体数量少 (效率高)、消耗资源少 (代价低) 的目的。

(5) 研究执行 IVPs对运行效率的影响

执行 IVPs对运行效率的影响量度, 特别是在实时环境下执行 IVPs对避免拒绝服务的影响量度将直接关系到如何构造实时系统的 IVPs。

(6) 研究 IVPs的有效性对完整性的影响

IVPs的有效性是指 IVPs的正确性, 或不正确的 IVPs在多大程度上影响完整性。该问题也是风险评估中一个尚未解决的问题。

为了克服现有安全模型的一些缺陷, 也为了更面向实际应用, 我们提出了面向分布式并发系统的灰色时序安全模型 (GTSM), 建立了基于 GTSM 语义的灰色时序安全策略规范语言 (GTSL)。GTSM主要根据灰色系统理论和时序规范语言 LOTOS的理论和概念, 参考了 Bell-Lapadula模型和 Clark-Wilson模型提出的。

3 GTSL的理论基础—— LOTOS与灰色系统理论

时序规范语言 LOTOS (Language of Temproal Ordering Specification) 是一个描述分布式并发信息处理系统的 ISO 标准 (ISO 8807)。LOTOS提出基于两个基本理论: 进程代数理论 (包括 CCS和 CSP) 和 ACT ONE (抽象数据类型 ADTs) 的语言)。开发 LOTOS的基本思想是: 通过定义事件之间的时序关系可以描述系统。LOTOS的动态语义是结构化的标号转换系统。

灰色系统理论研究的是信息不完全的对象、内涵不确定的概念、关系不明确的机制。这些都是客观存在的。从白化的角度看, 灰色理论的研究内容包括七个方面: 灰色统计、灰色聚类、系统因素的关联分析、灰映射、数据的生成、灰色建模、灰色预测、灰色决策与控制。灰的主要含义是指信息不完全与非唯一性。灰色系统是指信息不完全的系统。系统是白还是灰, 往往与观测的层次有关。同一个系统, 在高层次是白的, 而到了低层次则可能是灰的。灰色系统用灰数、灰色方程、灰色矩阵、灰群来描述。

4 GTSL

GTSL的系统观是时序的, 同时也是灰色的。为了确保系统的安全, 系统不同的时刻应采用不同的安全策略, 策略应随时间而改变, 即 GTSL具有描述策略的时序性能力。GTSL同时也基于这样的认识: 在规范系统的安全策略时面对的总是一个灰色的世界, 例如, 主体不确定, 主体的行为不确定, 客体在变化, “实体的真实性”是灰色的。因此, 在静态特性上, GTSL将世界看成由白色实体和灰色实体组成; 在动态灰色特性上, GTSL可描述动作不确定的系统特性, 如描述中断、动作的不确定选择等。更进一步地, GTSL设立了动态灰色操作作为原子动作, 可用来描述广泛的灰色世界。

(1) GTSL的动态语义

GTSL的动态语义是 DGTS[6]。DGTS是一种带灰色特性和时序特性的结构化的标号转换系统, 即

$$DGTS = < S, L \cup i, N \cup j \; R, ENTS, ARITH, S\text{-}GOP\text{-}ID, ASS, T, s0 >。$$

其中, S是状态集。L、i和 N、j R分别是灰色、黑色、白色标号集。ENTS是白色实体和灰色实体的集合。ARITH 是白色或精确操作的集合。S-GOP-ID是所有灰色操作的标识符的集合。ASS是断言或交

易规则的集合。T是转移关系的集合。s0是初始状态。

(2) 数据类型

白色数据类型：普通数据类型，如 integer，character，bolean等。

灰色数据类型：如，grey integer，grey character，grey boolean等。

(3) 实体

白色实体：具有白色属性的实体；灰色实体：具有灰色属性的实体。

(4) 操作

黑色操作 (i and N i)："i"类似于LOTOS中的"i"。N i表示"i"操作连续进行有穷多次。

白色操作 ("="):对实体赋白化值或确定的灰数。

灰色操作：执行完这类操作后，唯一的记号将加在确定实体上，且它们的值为灰数。灰色操作允许嵌套构造活跃的粒子层次的动态变化。

(5) 时序算子

GTSL中涉及的LOTOS时序算子有：stop (停止运行)，exit (成功结束)，ipol内部策略事件，前缀算子 (;)，选择算子 ("[]") (条件选择、一般选择、广义选择)，并行算子 (一般并行、并联并行、无关联并行或独立并行、广义无关联并行)，中断算子等。此外，我们还增加了以下几个时序算子，从而丰富了语言的表达能力：

* 混沌时序算子%：A% B= (A; B) [] (B; A)

  广义混沌时序 choas%；如 chaos% A，B，C= A% B% C。

* <>算子：Q<>P= Q; ipol; P，表示：策略P最终会执行。

* UnInterruped算子：如，UnInterrupted (P; Q)意味着P和Q的执行不能被打断。

(6) 特性表达式

特性表达式由特性表达式的项及GTSL时序算子组成。特性表达式的项的形式为：

特性表达式项= | stop | exit | particle- id | policy- id) | ("$" + tr) | ("$" + tr- sub- item)。

例如，"add (x1，x2，x3) $ (x3≤ 100) $"是一个特性表达式项。特性表达式的例子如下：

"(x1= 1); (x2); (add (x1，x2，x3)) $x3≤ 100$); stop"。

(7) 资源不变性与交易规则

资源不变性是为了进行IVPs而提出的。例如，商品A的价格Price- of- A应当是一个有上下确界的灰数，因此我闪表示其资源不变性如下：Price- of- A∈ [P1，P2]。

交易规则或断言是交易必须遵循的规则。当构造交易规则时，灰色预测模型 (如GM (1，1)模型)可作为完整性验证模型。验证可以在不同的层次上进行：在整个过程 (如对资源不变性的IVPs)中，或在某段时间内，或在某个确定时刻进行。例如，在某商店中，当天销售的总金额应该接近于根据最近五天销售总额的灰色预测值。如果误差太大，则应向商店经理提出警告。

(8) 子策略

策略由若干个子策略组成。子策略又由若干个子子策略组成。子策略标识符将会出现在特性表达式中。子策略类似于普通高级语言程序中的子例程或子函数。

(9) GTSL规范的部件构成

包括：上下文变量的说明、资源不变性定义、交易规则、动态粒子定义、子策略定义及整个策略的特性表达式描述。

5 结语

计算机系统的完整性安全策略模型与规范问题，是计算机安全研究中最重要的课题之一。已有的研究结果离实际应用还相差太远，如Clark-Wilson完整性模型只是提出了一个框架。本文呈现了我们构造的形式化灰色时序安全策略规范语言 (GTSL)，它是在灰色系统理论和LOTOS理论基础上提出的。GTSL中引入了灰色实体、灰色数据类型、灰色操作和时序算子来描述带时序特性和灰色特性的分布式

系统安全策略；GTSL在完整性上的规范能力、完整性验证过程的构造与表示、责任分离合理性测试等一系列技术方面的完善与创新，使得它能够得到实际应用。GTSL表达能力强，且易学易用，已被我们应用在实时入侵检测系统的安全策略规范上[7]。同时，它将灰色系统的理论和思想引用到计算机安全领域上，这也是个全新的尝试。

参考文献

1 Bell D E. Secure Computer Systems: Mathematical Foundations and Models. Technical Report M 74- 244, the MITRE Corporation, Bedford, MA, 1974

2 Clark D D. Comparing the Commercial and the Military Security Policies. in Proc. 1987 Symp. on Security and Privacy

3 邓聚龙. 灰色控制系统. 武汉：华中理工大学出版社，1985

4 ISO 8807, Information Processing Systems- OSI- LOTOS

5 Biba K J. Integrity Considerations for Secure Computer Systems. Mitre TR- 3153, Mitre Corporation, Bedford, MA, April 1977

6 Fan Ahua et al. Dynamic Grey Temporal system DGTS and its application to Security Policy Specification. Colloquia of 94 Kumming International CASE Symposium, Kumming, China

7 樊爱华. 灰色时序安全策略理论及其实践——网络环境下的计算机安全监测系统 OSMIS: [学位论文]. 长沙：国防科技大学，1996