第 34 卷 第 7 期 计 算 机 工 程 2008 年 4 月
Vol.34 No.7 Computer Engineering April 2008
·博士论文· 文章编号：1000—3428(2008)07—0035—03 文献标识码：A 中图分类号：N945.12

一种主体行为可信度量模型

周 正[1]，李 建[2]，张 俊[1]
（1. 海军工程大学电气与信息工程学院，武汉 430033；2. 解放军信息工程大学电子技术学院，郑州 450002）

摘 要：提出一种针对计算机信息系统的主体行为进行可信度量的模型，给出模型的一个实现框架。该模型可以对主体的行为进行可信度量，根据主体行为的可信度使不合法程序和代码无法执行、合法程序和代码无法执行未授权访问，使合法程序和代码的可疑行为受到严格控制，并能根据不同阈值来保证安全性和实用性的合理折中。

关键词：执行清单；执行描述；可信度量；安全门限

Trustworthiness Measuring Model for Subject's Behaviors

ZHOU Zheng[1], LI Jian[2], ZHANG Jun[1]
(1. College of Electrical and Information Engineering, Naval University of Engineering, Wuhan 430033;
2. Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450002)

【Abstract】 A model to measure the trustworthiness of subject's behaviors is presented, and a frame to realize the model function is given. The principle to measure the trustworthiness of subject's behaviors is expatiated, which controls suspicious behavior of legal programs and codes. According to the trustworthiness measured out by the model, it can forbid the running of illegal programs and codes, and the unauthorized access of legal programs and codes. It discusses how to get a trade-off between security and practicability with certain security threshold values.

【Key words】 implementation list; implementation description; trustworthiness measuring; security threshold value

可信计算概念的提出给信息安全的研究提供了一条新思路，使得操作系统的根本作用以及计算机终端源头地位被重新认识，相关研究得到了迅猛发展。这些研究从软件的身份来源可信和完整性可信方面为系统安全提供了有力的支持，但是对通过某种途径进入系统的恶意程序代码的破坏作用以及利用合法程序本身缺陷进行恶意攻击的行为却无能为力。文献[1]的RISE模型把抗攻击免疫的重点放在了保护系统上的代码，在应对漏洞方面比较有效，但是这种模型使用起来不方便，也无法处理合法用户通过授权非法程序造成的安全事故。文献[2]提出了可信主体的概念，对解决BLP[3]和Biba[4]都无法兼顾保密性和完整性的问题进行了有益的尝试，但是对可信主体本身为何可信没有给出明确的证明，使得难以对工程实施提供可操作性的指导。而本文提出的主体行为可信度量模型可以对信息系统中主体的具体操作行为给出可信度描述，为信息系统的安全防护提供重要依据。模型原理中提出的可信规则使得不合法程序和代码不能够执行，合法程序和代码不能够执行未授权操作，合法程序和代码的可疑操作受到严格的控制。在可信度量基础上制定的阈值可以保证较高实用性和鲁棒性。

1 模型原理

首先对信息系统中的安全要素进行抽象[5]，有如下约定：

(1)主体集合 $A=\{a_1,a_2,\cdots,a_m\}$；

(2)客体集合 $B=\{b_1,b_2,\cdots,b_n\}$；

(3)行为集合 $C=\{c_1,c_2,\cdots,c_l\}$；

(4)结果集合 $D=C(A,B)=\{c_k(a_ib_j)|a_i\in A,\ b_j\in B,\ c_k\in C,\ 1\le i\le m,1\le j\le n,1\le k\le l\}=\{d_1,d_2,\cdots,d_k\}$，从信息系统安全角度可以首先分为非攻击子集 o 和攻击子集 $R-o$；

(5)零元素，为了集合参与计算所需的完备性而引入，任何集合都包含零元素，记作 0；

(6)由 A, B, C 和 D 构成的系统记为 $s(A,B,C,D)$；

(7)主体 a 对客体 b 执行 c 操作得到结果 d 表示为：$c(a,b)=d$；

(8)A, B, C 和 D 都是可列集，其中，$A\cap B$ 可能不为 ϕ，且 $C(A,B)\subseteq D$。

下面以此为基础来阐述这种自身免疫模型的理论原理。

定义 1 对于 k 时刻由 A_k, B_k, C_k 和 D_k 构成的信息系统 $s(A_k,B_k,C_k,D_k)$，如果 $D_k\subseteq o$，则称系统 k 时刻安全，记作 $s(A_k,B_k,C_k,o)$；当 k =0 时，称系统初态安全。

定义 2 $\forall\ a\in A,\forall\ b\in B,\forall\ c\in C$，$c(a,b)$ 为一个原子操作。$c(a,b)\notin o$ 表示攻击成立，$c(a,b)\in o$ 表示攻击不成立。显然，$\{c(0,b),c(a,0),0(a,b)\}\subset o$。

对于系统 $s(A,B,C,D)$，由于 $D=C(A,B)$，因此系统 $s(A,B,C,D)$ 安全与 $C(A,B)\subseteq o$ 等价。

1.1 主体行为静态可信规则

当前绝大部分抗攻击模型都未涉及如何防范由合法程序和代码执行不正当的操作造成攻击的问题，而且通过当前的特征检测方法难以发现此类问题，通过异常检测法则会产生严重的误报或者漏报问题。因此，本文的研究目标是主体工作流程的原子操作本身。通过各种检测方法分析主体进行了

基金项目：国家“863”计划基金资助项目(2002AA1Z2101)
作者简介：周 正(1978－)，男，博士研究生，主研方向：信息安全，安全操作系统；李 建、张 俊，博士研究生
收稿日期：2007-05-08 **E-mail：**zhouzheng0203@263.net

何种操作是一种比较复杂的问题，如果主体的提供者能提供主体工作流程的执行清单，会在很大程度上减轻分析运算的代价。因此，首先提出主体的执行集合的概念。

定义 3 一个主体 a 在工作流程中可能对一系列客体进行的一系列操作构成了一个集合：$\{ c_1(a,b_1), c_2(a,b_2), \cdots, c_n(a,b_n) \}$，这个集合称为主体 a 的执行集合，记作 E_a。如果在主体 a 被提交的同时要求提交一份主体 a 对哪些客体进行了哪些操作的集合$\{ c_1'(a,b'_1), c_2'(a,b_2'), \cdots, c_n'(a,b_n') \}$，这个集合称为主体 a 的执行清单，记作 L_a。

显然，只要主体 a 的执行环境和执行目标确定，E_a 就是确定的，而且主体 a 的全部工作流程都由 E_a 的元素构成。如果某主体与其他主体没有并行和交互关系，称该主体是独立的。如果系统中所有的主体都是独立的，可以得到独立主体抗攻击基本规则定理。

规则 1 假设系统中的主体都是独立的，对 $\forall a \in A$，如果 $L_a \subset o$，且 $\forall\ c(a,b) \in E_a$ 有 $c(a,b) \in L_a$，称主体 a 是静态可信的。

规则 1 通过执行清单来判断主体的可信属性。它通过单个主体的可信使得整个系统避免来自系统内部主体的攻击，给出了保证系统不发生攻击从而系统安全性得到保证的一个充分不必要条件。虽然工作流程由执行集合的原素构成，执行集合中的元素只说明了基本的原子操作，在实际工作流程中，同一个原子操作在不同的条件下所造成的结果不一定相同，在不同的时机执行，需要的条件也不一定相同。规则 1 还限制了主体的并行和交互性，这在操作系统中并行处理和交互要求愈加重要的形势下显得尤为重要。因此，需要在规则 1 的基础上研究针对存在并行和交互关系的主体的系统的解决方法。

1.2 主体行为动态可信规则

定义 4 主体 a 的执行集合 E_a 中，$\forall c_i(a,b_i) \in E_a$，取其在 E_a 中的标志 $iden_i$，不管是从 a 的工作环境条件、系统安全需要还是安全政策规定，该 $c_i(a,b_i)$ 都要满足一定的条件，称为这个原子操作的执行条件，记作 $cond_i$，这个原子操作的执行结果记作 $resu_i$，$cond_i$ 和 $resu_i$ 都是某些参数的集合。把 $(iden_i, cond_i, resu_i)$ 称为 $c_i(a,b_i)$ 的一个执行描述，记作 $desc_i$，则主体 a 的执行集合 E_a 会对应一个主体 a 的执行描述集合 $\Gamma_a = \{desc_1, desc_2, \cdots, desc_n\}$。将 E_a 具有 Γ_a 表示的描述记作 $E_a \mid \Gamma_a$。

在主体 a 的工作流程中，$c_i(a,b_i)$ 可能发生多次，每次的 $cond_i$ 和 $resu_i$ 不一定相同。这里的 $cond_i$ 和 $resu_i$ 不但包含 $c_i(a,b_i)$ 本身的条件和结果，还包含这些条件和结果对系统的影响。因此，$cond_i$ 和 $resu_i$ 能反映系统当前时刻所受影响的累加。

定义 5 如果信息系统各种安全要素确定，在确定的安全政策下可以得到影响该信息系统安全的各种条件，称这些条件的集合为系统在这个安全政策下的风险集合，记作 N_s。

定义 6 主体 a 的 $cond_i$ 和 $resu_i$ 可以分为对系统安全有影响和对系统安全没有影响，如果有影响，则分别记作 $cond_i \cap N_s \neq \phi$ 和 $resu_i \cap N_s \neq \phi$，如果没有影响，则分别记作 $cond_i \cap N_s = \phi$ 和 $resu_i \cap N_s = \phi$。

引理 $cond_i \cap N_s = \phi \wedge resu_i \cap N_s = \phi$ 意味着 $c_i(a,b_i) \in o$。

篇幅所限此处不作证明。

规则 2 如果静态可信主体工作流程中的所有执行描述都与系统安全没有影响，则该主体是可信的。

规则 2 说明，如果主体能够提供执行清单，执行过程中不涉及执行清单以外的操作，而且能够保证这些操作的条件和结果对系统安全没有任何影响，那么系统中永远不会有攻击事件发生，能保证系统的安全性。

由于 $cond_i$ 和 $resu_i$ 能反映系统当前时刻所受影响的累加，因此规则 2 对存在并行处理和交互的系统进行攻击检测和免疫时显得比较有效。但规则 2 要求系统的主体集合只能由执行条件和结果对系统安全没有任何影响的主体构成，这导致系统兼容性严重降低，而且考虑到系统安全是个动态概念，应用程序的可用性会随着系统物理条件和安全政策的变化受到严重影响。因此，本文提出了开放环境下的主体可信度量规则。

1.3 开放环境下的主体行为可信度量

定义 7 主体 a 的 $cond_i \cap N_s$ 和 $resu_i \cap N_s$ 都对应着系统安全影响的具体程度，称为安全影响度量，用整数 x 来表示，对系统安全没有影响时，记作 x =0。不同的 $cond_i \cap N_s$ 或者 $resu_i \cap N_s$ 可能对应不同的 x，如果存在 2 个度量 x_1 和 x_2，x_1 表示的安全影响比 x_2 表示的安全影响大，记作 $x_1 > x_2$，相等记作 $x_1 = x_2$，否则记作 $x_1 < x_2$。这些 x 构成安全影响度量集合，用 X 来表示。对于给定的系统 $s(A,B,C,D)$ 和安全影响度量集合 X，如果存在 $x_t \in X$ 且在 X 中具有特殊意义，则把 x_t 称作 X 的一个安全门限(阈值)。

定义 8 取 $f_{cond} : (cond_i, N_s) \to x$，如果 $\forall N_s, cond_i, \exists x \in X$ 与 $(cond_i, N_s)$ 遵循 f_{cond} 相关且唯一，则称 f_{cond} 为执行条件安全影响度量函数。同理可以定义执行结果安全度量函数：

$$f_{resu} : (resu_i, N_s) \to x$$

显然，在系统 $s(A,B,C,D)$ 和安全政策确定的情况下，定义 7 和定义 8 是确定的。通过以上的定义和规则，从独立主体构成的系统开始分析并建立规则以及开放系统下的主体行为可信度量函数。再结合安全影响度量函数和安全门限，可以得到具有调节安全门限能力的主体行为可信度量模型：

(1)系统在引入主体时能够提供主体的执行清单；

(2)通过执行清单静态检测主体的潜在攻击行为；

(3)授权的主体在执行过程中禁止执行清单以外的未知操作；

(4)授权的主体在执行操作过程中建立描述集合与系统安全的影响关系；

(5)对描述集合与系统安全的影响关系量化计算；

(6)执行机构结合安全门限值对当前操作实施控制。

其中，(1)~(3)体现了主体行为的静态可信规则；如果取门限值为 0，(4)~(6)体现了主体行为动态可信规则。这样就实现了对主体行为的可信度进行量化的描述，并且为操作的控制提供了依据，使得不合法的程序和代码不能够执行，合法的程序和代码不能够执行未授权访问，合法程序和代码的可疑行为得到量化的评估并且可以根据适当的阈值来控制。

2 模型实现框架

由于系统安全是一个动态的概念，与信息系统物理条件以及安全政策有着密切的关系，因此在模型的实现框架中引

入安全政策机构。结合各规则和定义来构造各种模块，再添加必需的安全审计和风险预警模块，构成了如图 1 所示的模型实施框架。

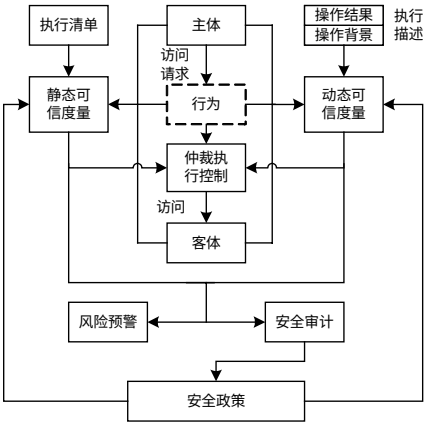

图 1　模型的实现框架

图 1 中的主体、客体以及行为这 3 个安全要素构成一个原子操作时需要经历一个访问控制过程，访问请求和访问是行为在被确认前后的 2 种不同形式。主体对客体发出的访问请求是申请建立一个原子操作阶段，经过访问控制决定是否允许这个原子操作执行。

执行清单模块对应理论模型中主体的执行集合。任何主体都要提供执行集合，这个集合是判断该主体在实际工作流程中是否确实可信的重要依据，系统中所有主体的执行集合由执行清单模块来管理。执行清单模块对主体执行集合进行的保护主要体现在存储、保护和索引等方面。

静态可信度量模块的主要功能是检测主体的执行清单中是否存在非法操作，检验主体的实际工作流程涉及的操作与提交的执行集合是否相符，如果不符则说明主体执行了某些不可信的操作。

执行描述模块把根据一次原子操作的执行条件和执行结果提交给动态可信度量模块，作为进行动态可信度量的依据。

动态可信度量模块把执行描述模块提交的执行条件和执行结果与系统安全风险之间的关系生成可度量的一系列参数，用来表示主体行为的可信度，并根据制定的安全门限决定是否允许这个操作执行。

行为仲裁控制模块根据可信度量的结果决定是否允许这个操作执行。安全门限在这个过程中发挥了重要作用。

安全政策机构是对安全政策进行管理和更新的组件，安全政策是对系统进行安全分析和制定安全门限的依据，伴随着系统的更新以及环境的变化会有相应的安全政策与之相适应，保证安全性和可用性的实效。因为安全是一个动态的概念，所以任何安全功能的实现都离不开安全政策的合理制定。

3　结束语

本文从理论上提出了一种主体行为可信度量模型，该模型是针对目前操作系统本身存在的不足，即绝大多数研究只偏重于主体身份的可信认证或者一致性检测而忽略了攻击的发生所依赖的系统本身条件这个最根本的前提，通过对实际信息系统的各种安全要素进行抽象提出的。本模型从主体的行为方面为甄别不合法的程序和代码提供依据，合法的程序和代码试图执行未授权操作也受到严密的监控，根据适当的安全政策来制定不同的安全阈值，使得在保证实用性时具有充分的主体行为可信度量依据。本模型不但能够检测出攻击和感染源，而且能对潜在的攻击进行预警，为未知攻击的免疫提供依据。目前实现本模型的关键问题是在具体信息系统环境下做出完备的安全风险评估以及确定合适的阈值。对于一些工作流程相对固定的信息系统，本模型具有较高实用性。

参考文献

[1] Barrantes E G, Ackley D H, Forrest S, et al. Randomized Instruction Set Emulation to Disrupt Binary Code Injection Attacks[C]//Proc. of CCS'03. [S. l.]: ACM Press, 2003.

[2] 李益发, 沈昌祥. 一种新的操作系统安全模型[J]. 中国科学: E 辑, 2006, 36(4): 347-356.

[3] Bell D E, LaPadula L J. Secure Computer Systems: A Mathematical Model[R]. The MITRE Corporatoin, Technical Report: M74-244, 1973.

[4] Biba K J. Integrity Considerations for Secure Computer System[R]. PSAF Electronic System Division, Hanscom Air Force Base, Technical Report: ESD-76-372, 1977.

[5] Zhou Zheng, Zhang Jun, Li Jian, et al. Protecting Terminals by Security Domain Mechanism Based on Trusted Computing[J]. Wuhan University Journal of Natural Sciences, 2006, 11(6): 1437-1440.

（上接第 31 页）

参考文献

[1] Johnson A E, Cheng Yang, Matthies L H. Machine Vision for Autonomous Small Body Navigation[C]//Proc. of IEEE Aerospace Conference. [S. l.]: IEEE Press, 2000.

[2] Shakernia O, Koo T J. Vision Guided Landing of an Unmanned Air Vehicle[C]//Proceedings of the 38th Conference on Decision & Control. Phoenix, Arizona, USA: [s. n.], 1999.

[3] 刘士清, 胡春华, 朱纪洪. 基于计算机视觉的无人直升机位姿估计方法研究[J]. 计算机工程与设计, 2004, 25(4): 564-568.

[4] 邱力为, 宋子善, 沈为群. 用于无人直升机着舰控制的计算机视觉技术研究[J]. 航空学报, 2003, 24(4): 351-354.

[5] Hartley R I. In Defence of the 8-point Algorithm[C]//Proceedings the 5th International Conference on Computer Vision. Santa Barbara, USA: [s. n.], 1995.

[6] 邱茂林, 马颂德, 李　毅. 计算机视觉中摄像机定标综述[J]. 自动化学报, 2000, 26(11): 43-55.

[7] 孟晓桥, 胡占义. 摄像机自标定方法的研究与进展[J]. 自动化学报, 2003, 29(1): 110-124.

[8] 胡占义, 雷　成, 吴福朝. 关于 P4P 问题的一点讨论[J]. 自动化学报, 2001, 27(6): 770-776.

[9] 于起峰, 陆宏伟, 刘肖琳. 基于图像的精密测量与运动测量[M]. 北京: 科学出版社, 2002.