

基于动态可信度量的敏感信息安全控制模型

费稼轩，张 涛，林为民，陈亚东，曾 荣

（中国电力科学研究院，江苏 南京 211106）

摘 要：随着信息技术的高速发展，计算机系统处理的敏感信息规模不断增长，确保敏感信息的安全变得非常重要。本文对传统的多级安全模型 BLP 模型进行了分析，指出其对敏感信息完整性保护不足的安全隐患。针对该安全隐患，本文设计了基于动态可信度量的敏感信息安全控制模型（DTMSISCM）并给出了其实现架构，DTMSISCM 通过实施基于可信度的敏感信息安全控制，在维持和 BLP 模型相同保密性的基础上，保证了敏感数据的完整性，提高了系统敏感信息安全控制的可用性。

关键词：多级安全，敏感标记，可信计算，动态度量，可信度

0 引言

敏感信息的保密性、完整性和可用性关系到国家的安全、企业的核心竞争力和个人的隐私。随着信息技术的发展，计算机和计算机网络作为重要的信息载体和信息传输渠道，存储、共享和管理着规模巨大的敏感信息，如何对计算系统中的这些敏感信息进行安全控制作为信息安全领域中的重要课题，正越来越受到关注。

强制访问控制策略是目前各种安全系统中应用最广泛的一类安全策略，将该策略应用于敏感信息安全控制，对计算机系统内的主体、客体指定敏感标记，可以有效地防止敏感信息的泄漏^[1,2]。强制访问控制策略的核心是多级安全策略（multi-level security，简称MLS），多级安全的经典模型是BLP保密模型^[11,12]，该模型定义了简单安全条件与*_属性两条规则，简单安全条件规则规定主体不能读访问敏感级别高于自己的客体，*_属性规则规定主体不能写访问敏感级别低于自己的客体^[3,4,5]。

虽然BLP模型能够很好地防止敏感信息的非授权泄漏，保护敏感信息的保密性，但是BLP模型规定的敏感信息单向流动无法满足系统的可用性^[6]；BLP模型的另一缺点是没有考虑敏感信息的完整性，它允许低敏感级别的主体写访问高敏感级别的客体，从而可能会破坏高敏感级别客体的完整性^[8]。为了提高系统的可用性，Bell在文献[4]中引入可信主体，通过可信主体的违规操作保证实际系统的正常运行，但是该方法并没有给出判定可信度的依据，导致实施困难，同时没有对可信主体的访问权限实施限制，影响系统敏感信息的保密性。

针对上述问题：本文提出一种基于动态可信度量的敏感信息安全控制模型，其思想主要来源于可信计算：按照可信计算组织的定义，一个实体一直以一种可预期的方式为特定的目标运行，就认为它是可信的^[7]。动态可信度量是对计算机系统内的进程进行动态的可信度量（完整性度量），即在任意时刻，对正在运行的系统中的进程（以及模块）的有机构成进行完整性的度量，并在度量的过程中使用可信平台模块（Trusted Platform Module, TPM）保护度量架构和对度量结果进行签名^[9,10]。本文所提出的模型在BLP模型定义的敏感级别的基础上，通过采用可信平台的动态可信度量技术定义判定主体可信度，对主体在运行过程中可信度变化和调节制定规则：对不同可信度主体结合BLP模型的规则分别实施敏感信息安全控制，对可信主体可以在动态可信度量的控制下不受BLP简单安全条件与*_属性规则的约束，提高系统的可用性；对中等可信度主体严格按照BLP模型规则，保证了敏感信息的保密性；对低可信主体严格限制其对敏感信息的操作行为，保证敏感信息的完整性。

本文其余内容组织如下：第 1 章详细介绍基于动态可信度量的敏感信息安全控制模型的设计、形式化描述及主体可信度规则和敏感信息安全控制规则，第 2 章描述基于动态可信度量的敏感信息安全控制模型的一个基于可信平台的实现架构及流程，第 3 章对基于动态可信度量的敏感信息安全控制模型的安全性进行分析，第 4 章是总结与展望。

1 基于动态可信度量的敏感信息安全控制模型

本文以保证敏感信息的保密性、完整性和可用性为目标，在传统 BLP 模型的基础上，增加主体动态可信度量及可信分级，提出了基于动态可信度量的敏感信息安全控制模型 (Dynamic Trust Measurement based Sensitive Information Secure Control Model, DTMSISCM)，利用动态可信度量技术对计算机系统上主体的可信度进行实时度量和定级，在不影响计算机系统数据访问可用性的前提下，确保敏感信息的安全可靠，有效防范敏感数据被篡改和泄漏。

本节首先提出模型的设计思想，定义模型的组成元素，给出主体可信度规则、敏感信息安全控制规则的形式化描述，从而形成基于动态可信度量的敏感信息安全控制模型 DTMSISCM。

1.1 DTMSISCM 模型的设计

DTMSISCM 的总体框架如图 1 所示，纵向上分为三个层次，从下到上为：可信度量层，采取可信平台的动态可信度量为可信度提供可信依据；实体层，包含计算机系统的主、客体，其中主体表示为用户及其启动的进程的二元形式；标记层，在标记层设计主体可信级别标记和主/客体敏感标记及其规则。

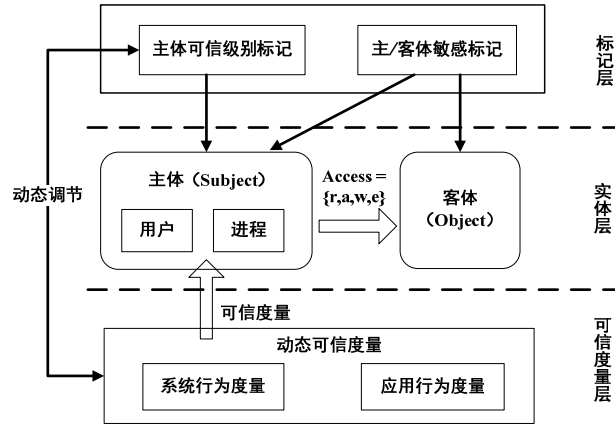


图 1 DTMSISCM 模型框架

1.2 DTMSISCM 模型的描述

1.2.1 DTMSISCM 的组成元素

定义 1 基本变量， S 为主体集，可以看作用户集 U 及启动进程集 P 的有序对，有 $S = (U, P)$ 。 O 为客体敏感信息集，对于单个客体 o ，有 $o \in O$ 。

定义 2 主体对客体敏感信息操作方式集合，在 DTMSISCM 中，主体 S 对客体 O 的访问集合 $A = \{r, a, w, e\}$ ，其中：只读 r (write)：读包含在客体中的信息；添加 a (append)：向客体中添加信息，且不读客体中的信息，称为“追加写”。执行 e (execute)：执行一个客体(可执行文件)。读写 w (write)：向客体中同时读和添加信息，通常又称为“写”。

定义 3 主体对客体敏感信息的操作行为集合，记录主体对客体的访问操作集合， $B = (S \times O \times A)$ 。

定义 4 主/客体敏感标记集合，单个主/客体的敏感级别 $l_s, l_o \in L$ ， $L = \{(c, k) | c \in C, k \in K\}$ ， L 表

示主/客体敏感标记集合，其中 $C = \{public, secret, topSecret\}$ 表示主/客体的密级集合， c_s, c_o 分别表示主/客体的密级， K 表示主/客体的范畴集合，表示主/客体非等级的应用领域或类别；敏感标记之间具有偏序关系 $\{=, f, p\}$ ，分别表示相等、支配和被支配关系。

定义 5 主体可信度, 单个主体可信度 $d_{Ts} \in D_{Ts}$, 表示对实体保持安全性和可靠性的可置信程度, D_{Ts} 代表主体可信度集合, $D_{Ts} = \{trust, midtrust, lowtrust\}$, 其中 $trust$ 表示可信, $midtrust$ 表示中等可信级别, $lowtrust$ 表示低可信级别, 按照可信度的高低, 有: $trust > midtrust > lowtrust$ 。

对主体的单个用户 $u \in U$, 用户可信度表示为 $d_{Tu} \in D_{Tu}$, 对于用户可信度的判定主要建立在可信认证的基础上; 对主体的单个进程 $p \in P$, 进程可信度表示为 $d_{Tp} \in D_{Tp}$, 对于进程的可信度判定主要建立在动态可信度量的基础上。

定义 6 主体进程动态可信度量值, 对主体的单个进程 $p \in P$, 可信度量值表示为 $m_{Tp} \in M_{Tp}$, 表示对主体的进程实施度量的结果值。可信度量值是进程的可信状态的客观依据, 具有惟一性, 因此可以通过一定的映射关系获得进程的可信度, 作为安全控制的依据。

定义 7 主体进程动态可信度映射, 为实现可信度量值到可信度的映射关系, 根据可信度量值的惟一性, 参考现有的标准安全漏洞库, 定义主体进程动态可信度映射表, 表示主体进程动态可信度量值所对应的可信度集合, 根据定义 2 中对主体进程可信度的定义, 有 $D_{Tpknown} = \{trust, midtrust, lowtrust\}$, 分别具有如下含义:

$\forall d_{Tpknown} \in D_{Tpknown}, d_{Tp} = trust$, 进程不含已知的安全漏洞, 为可信进程;

$\forall d_{Tpknown} \in D_{Tpknown}, d_{Tp} = midtrust$, 进程存在安全漏洞, 但是该类进程可以通过可信计算完整性度量机制对该类漏洞进行监控, 可信度为中级可信。

$\forall d_{Tpknown} \in D_{Tpknown}, d_{Tp} = untrust$, 进程存在网络安全漏洞, 易被远程攻击者利用实施攻击, 该类攻击并不能通过 TPM 的度量机制进行监控, 可信度为低级可信或进程为已知各类攻击程序。

定义 8 可信度映射函数, 主体进程可信度映射函数 $f_{d_{Tp}} : M_{Tp} \rightarrow D_{Tpknown}$, 表示主体进程的动态可信度量值到可信度的映射关系, 主体可信度映射函数 $f_{d_{Ts}} : U \times P \rightarrow D_{Ts}$, 表示主体的用户和对应启动的进程到主体可信度的映射关系。具体映射关系将在基于动态可信度量的主体可信度规则中的可信度映射规则给出。

定义 9 主/客体敏感标记函数, 主体敏感标记函数: $f_s : S \rightarrow L$ 表示单个主体到其敏感标记的映射关系; 客体敏感标记函数: $f_o : O \rightarrow L$ 表示单个客体到其敏感标记的映射关系。

1.2.2 基于动态可信度量的主体可信度规则

该规则主要定义主体进程动态可信度量值到主体进程可信度的映射关系, 并给出主体可信度的判定规则, 进一步为反映计算机系统上主体的实时变化情况, 对主体可信度动态调节规则进行了定义。

(1) 主体进程可信度映射规则

根据定义 6，对主体进程 $\forall p \in P$ ，其可信度量值 $m_{Tp} \in M_{Tp}$ ，定义 8 中的可信度映射函数

$f_{d_{Tp}} : M_{Tp} \rightarrow D_{Tpknown}$ 定义如下：

$\exists(m_{Tpknown}, d_{Tpknown}), m_{Tp} = m_{Tpknown} \rightarrow d_{Tp} = d_{Tpknown}$ 该映射规则表示当主体进程可信度量值和主体动态

可信度映射表中已知进程的度量值匹配时，该主体进程可信度为已知标准进程的可信度；

(2) 主体可信度判定规则

根据定义 5，对单个主体 $s \in S$ ，其可信度为 d_{Ts} ，对应主体用户可信度及启动进程的可信度 d_{Tu} d_{Tp} 。

定义 8 中的主体可信度映射函数 $f_{d_{Ts}} : U \times P \rightarrow D_{Ts}$ 定义为： $f_{d_{Ts}}(u, p) = \min(d_{Tu}, d_{Tp})$ ，即主体的可信度为对应用户及启动进程可信度的最小值。

(3) 主体可信度动态调节规则

为保证对终端上主体的实时监控，需要动态度量主体的可信度，根据定义 8 和规则 1)、2)，该规则定义为：

$$d'_{Ts} = \min(d'_{Tu}, d'_{Tp}) = \min(d'_{Tu}, f_{d_{Tp}}(m'_{Tp}))$$

其中 d'_{Ts} 表示对 s 调节后的目标可信度， d'_{Tu} 表示对 u 新实施可信认证后获得的可信度， d'_{Tp} 表示对 p 重新度量后获得的度量值。

1.2.3 敏感信息安全控制规则

本规则主要在上述(1)-(3)的主体可信度规则的基础上，对不同等级的可信主体，定义基于动态可信度的敏感信息安全控制规则。

(1) 可信主体敏感信息操作规则

对于可信主体在操作客体敏感信息时，通过动态可信度量保证了其行为的可信，从而允许可信主体一定程度上违反 BLP 安全模型的简单安全条件和*_属性规则，以提高计算机系统敏感信息操作的可用性，该规则定义如下：

$$(\exists d_{Ts} = trust) \cap (f_o(o) \text{ f } f_s(s)) \rightarrow \exists b = (s \times o \times r), r \in A \quad (\exists d_{Ts} = trust) \cap (f_o(o) \text{ p } f_s(s)) \rightarrow \exists b = (s \times o \times w), w \in A$$

该规则表示可信主体允许读取敏感标记级别高于其的客体敏感信息，允许向敏感标记低于其标记的客体写数据。

(2) 中等可信度主体敏感信息操作规则

为防止计算机系统上敏感信息的泄漏，必须限制其对客体敏感信息的操作行为，该规则定义如下：

$$(\exists d_{Ts} = midtrust) \cap (f_o(o) \text{ p } f_s(s)) \rightarrow \exists b = (s \times o \times r), r \in A$$

$$(\exists d_{Ts} = midtrust) \cap (f_o(o) \text{ f } f_s(s)) \rightarrow \exists b = (s \times o \times w), w \in A$$

该规则表示中等可信度主体对客体敏感信息的操作和 BLP 安全模型一致。

(3) 低可信度主体敏感信息操作规则

对于第可信度主体需要严格限制其对客体敏感信息的操作行为，该规则定义如下：

$$(\exists d_{Ts} = lowtrust) \cap (f_o(o) = f_s(s)) \rightarrow \exists b = (s \times o \times w), w \in A$$

该规则表示低可信度主体只允许写和其敏感标记级别一致的客体，该规则违反了 BLP 安全模型的*_属性规则，保证了客体敏感信息的完整性。

上述规则针对不同可信度主体实施对客体敏感信息的操作控制，使得敏感信息的操作范围和主体可信度保持一致，在保证终端上敏感信息保密性和完整的同时，提高系统的可用性。

2 基于动态可信度量的敏感信息安全控制流程

在第 1 章提出的 DTMSISCM 模型的基础上, 本文设计了计算机系统上一个基于动态可信度量的计算机系统敏感信息安全控制架构。该架构如图 2 所示: 以可信计算平台为支撑, 提供用户可信认证和动态可信度量服务; 由安全控制模块依据 1.2.2 和 1.2.3 中定义的规则和标准可信度表、可信级别表及敏感标记表对敏感信息的操作进行安全控制, 保证计算机系统上敏感信息的保密性、完整性和可用性。

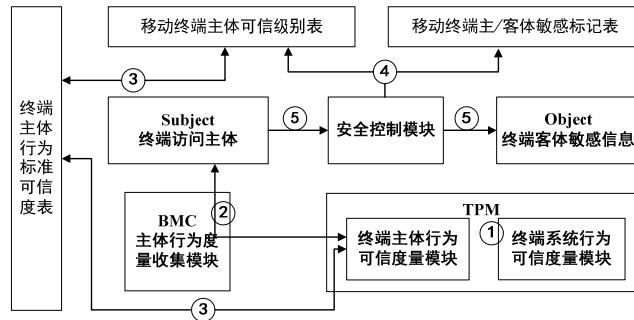


图 2 基于动态可信度量的计算机系统敏感信息安全控制架构

该架构的具体工作流程如下:

Step1 可信平台的终端系统行为可信度量模块从其内置的可信度量根开始，建立一条从计算机系统 BIOS、操作系统（OS）到服务的可信链，建立计算机系统可信系统环境；

Step2 主体行为度量收集模块（BMC）实时收集计算机系统主体（用户及其启动的进程）行为信息，作为终端主体行为可信度量模块的输入，终端主体行为可信度量模块按照定义 6 计算主体进程动态可信度量值并存储在 PCR 中；

Step3 终端主体行为可信度量模块按照 1.2.2 的主体进程可信度映射规则和主体可信度判定规则，对主体进程可信度量值对照终端主体行为标准可信度表将度量值映射到主体可信级别表中的主体可信度；BMC 模块实时收集主体进程信息，由终端主体行为可信度量模块按照 1.2.2 的主体可信度动态调节规则调节主体可信度；

Step4 安全控制模块依据 1.2.3 中定义的不同可信度的可信主体操作敏感信息规则确定主体集合 S 对客体集合 O 的操作行为集合 B;

Step5 计算机系统主体集合 S 按照安全控制模块计算的操作行为集合 B 操作可信敏感信息集合 O。

3 DTMS/SCM 安全分析

3.1 DTMS-SCM 保密性分析

DTMSISCM 模型在传统 BLP 模型的基础上，增加了基于可信计算平台的动态可信度量技术，模型利用定义的敏感信息安全控制规则，对可信主体允许其在实时的动态可信度量的控制下违反 BLP 模型的简单安全条件规则和*_属性规则，由于可信主体的行为是受到实时度量的，可以保证终端敏感数据的保密性；对中等可信主体，模型严格使用 BLP 模型规则来保证终端上敏感信息的保密性；对低可信度主体模型严格限制其行为，限制其对敏感信息的操作。在 DTMSISCM 模型中从可信和传统的 BLP 模型安全规则两个维度来保证敏感信息的保密性。

3.2 DTMS/SCM 完整性及可用性分析

在传统 BLP 模型中定义的规则中,主体不能读取敏感标记高于其敏感标记的客体,不能写入敏感标记低于其敏感标记的客体,从而防止敏感信息的泄漏。

但是该规则允许低敏感级别的主体向高敏感级别的客体进行写入操作，如果写入的信息含有恶意代码，会破坏高敏感级别客体的完整性；进一步如果系统严格按照传统的 BLP 模型规则来定义主/客体的操作规则，几乎无法构造出一个可用的计算机系统，无法保证可用性。

DTMSISCM 对其进行了改进, 通过将主体可信度量值映射到不同等级的可信度, 从而实施不同的敏感信息安全控制策略来保证完整性和可用性。对可信的主体允许其在动态可信度量的基础上违反 BLP 的简单安全条件和*_属性规则, 提高了系统的可用性, 如图 3 所示, 可以看到对可信主体其读写范围要高于 BLP 模型的读写范围。

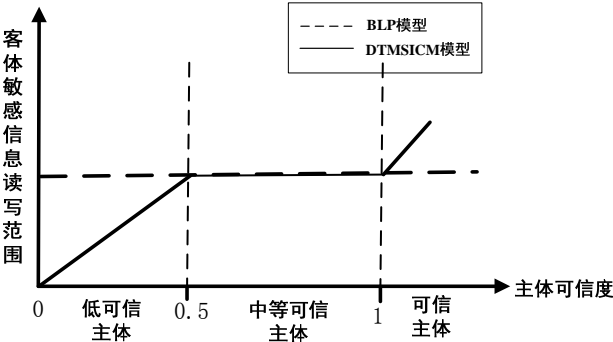


图 3 不同等级可信主体读写范围

对低可信度的主体, 由于严格限制了其对敏感信息的操作行为, 其读写范围要小于传统 BLP 安全模型, 如图 3 所示; 同时根据 DTMSISCM 模型中敏感信息安全控制规则的第(3)条规则, 低可信主体违反 BLP 模型的*_属性规则 (如表 1 所示), 禁止向高敏感级别的客体进行写入, 只允许写同敏感级别的客体, 保证了计算机系统上敏感信息的完整性。

表 1 多级可信主体的安全规则

BLP 安全模型规则	低可信主体	中等可信主体	可信主体
	[0,0.5)	[0.5,1)	[1]
简单安全条件	√	√	×
*-属性	×	√	×

4 总结与展望

本文对传统的敏感信息安全控制多级安全模型 BLP 模型进行了分析, 指出传统 BLP 模型在敏感信息安全控制上存在的无法保证客体敏感信息可用性及完整性的安全隐患。针对该安全隐患, 文本提出了一个基于动态可信度量的敏感信息安全控制模型 DTMSISCM 及其实现架构, 通过传统 BLP 模型基础上增加主体动态可信度量及可信度分级, 并定义主体可信度规则和敏感信息安全控制规则, 对不同可信度的主体实施与其可信度相适应的敏感信息安全控制规则。通过对 DTMSISCM 的安全性分析, 在维持与 BLP 模型相同的保密性的基础上, 提高了系统在敏感信息安全控制方面的可用性和完整性。

未来, 将进一步结合可信计算的技术研究如何更加准确地度量主体的可信度, 提高主体动态度量的实时性。

参考文献:

[1] 杨智, 金舒原, 段毅, 等. 多级安全中敏感标记的最优化挖掘[J]. 软件学报, 2011, 22(5): 1020-1030.

[2] 武延军, 梁洪亮, 赵琛. 一个支持可信主体特权最小化的多级安全模型[J]. 软件学报, 2007, 18(3): 730-738.

[3] T Bell D E, LaPadula L J. Secure computer system: Unified exposition and multics interpretation[R]. MTR-2997, Bedford, MA: THE MITRE Corporation, 1976.

[4] T Bell D E, LaPadula L J. Secure computer systems: mathematical foundations[R]. MTR-2547 Volume I, Bedford, MA: Electronic Systems Division, Air Force System Command, Hanscom AFB, 1973.

[5] Bell D E, LaPadula L J. Secure computer systems: A mathematical model[R]. MTR-2547 Volume II, Bedford, MA: Electronic

Systems Division, Air Force System Command, Hanscom AFB, 1973.

- [6] 季庆光,卿斯汉,贺也平.一个改进的可动态调节的机密性策略模型[J].软件学报, 2004,15(10):1547-1557
- [7] Trusted Computing Group, TCG Specification Architecture Overview Revision 1.4[S]. TCG published, 2007.
- [8] 石文昌,孙玉芳,梁洪亮.经典BLP安全公理的一种适应性标记实施方法及其正确性[J].计算机研究与发展, 2001, 38(11): 1366-1372.
- [9] 季庆光, 卿斯汉, 贺也平.一个改进的可动态调节的机密性策略模型[J].软件学报, 2004, 15(10):1547-1557.
- [10] 张晓菲,许访,沈昌祥.基于可信状态的多级安全模型及其应用研究[J].电子学报, 2007, 35(8):1511-1515.
- [11]Trusted Information System Inc., Trusted mach mathematical model[R]. TIS TMACH EDOC-0017-96B, Trusted Information System Inc., 1996.
- [12] TMP L. Using mandatory integrity to enforce commercial security[A]. Proceedings of the IEEE Symposium on Security and Privacy[C]. 1988.140-146.

作者简介:

费稼轩 (1984-), 男, 硕士/助理工程师, 主要研究领域为信息安全, 可信计算, 通信地址: 南京市江宁区胜利西路9号 (211106);

张 涛, 男, 高级工程师/研究所副总工, 主要研究领域为信息安全;

林为民, 男, 教授级高级工程师/研究所副所长, 主要研究领域为信息安全;

陈亚东, 男, 硕士/工程师, 主要研究领域为密码学;

曾 荣, 男, 硕士/工程师, 主要研究领域为密码学。