DOI: 10.13656/j.cnki.gxkx.2002.01.001
广西科学 Guangxi Sciences 2002, 9 (1): 1~5

# CC标准框架下安全确信度的定量描述方法*

# An Approach for Quantitative Description of Security Assurance under the Common Criteria Framework

石文昌 孙玉芳
Shi Wenchang Sun Yufang

(中国科学院软件研究所 北京中关村南四街 4号 100080)
(Institute of Software, Chinese Academy of Sciences, 4 Fourth South Street, Zhongguancun, Beijing, 100080, China)

摘要 结合安全操作系统的一个研究实验, 对 CC标准框架下的安全产品开发过程进行了概括和抽象, 借助主观逻辑, 针对在 CC标准框架下建立的安全产品的安全确信度, 提出安全确信度的一种定量描述方法.
关键词 CC标准 安全 确信度 定量描述
中图法分类号 TP309; TP316

**Abstract** With an research experiment of a secure operating system, an outline and abstraction of the development process of security products under the Common Criteria (CC) framework is made, based upon which, with subjective logic, an approach for quantitative description of security assurance that may be established under the CC framework is proposed.
**Key words** the Common Criteria, security, assurance, quantitative description

为了确定计算机安全产品评价的国际共同标准(CC)[1~3]的前景,需要开展多方面的工作[4],其中,研究在 CC标准框架下可以取得的安全确信度就是一项重要的工作. 通常,确信度被定义为安全性的需要得到满足的可信程度[5,6]. 对确信度进行定量的度量是一件非常困难的事情[7].

在本文的工作之前, 我们对 CC标准在为安全产品建立安全确信度方面可以发挥的作用进行了探讨[8,9],但讨论仅限于定性分析的范围. G. F. Jelen和 J. R. Williams提出了定量度量确信度的一个框架[7],但该框架不适合于用来描述在 CC标准框架下开发安全产品所建立的产品安全性的确信度.

本文在已开展的定性研究工作[8,9]的基础上, 提出一个借助 A. Josang的主观逻辑[10,11]定量地表示由 CC标准的理念建立的计算机安全产品的安全确信度的思想.

2001-10-08收稿, 2001-12-03修回.
* 国家自然科学基金项目(60073022)、国家 863高技术研究发展项目(863-306-ZD12-14-2)和中国科学院知识创新工程项目 (KGCX1-09) 资助.

## 1 CC标准框架下的安全确信度

本节对 CC标准框架下的安全产品开发过程进行概括和抽象, 为安全确信度的讨论建立基本前提.

### 1.1 产品开发过程描述

CC标准认为, 计算机安全产品安全性的可信程度可以通过产品的开发、评价和使用过程中的活动来建立. 从本文的讨论角度出发, 作者把在 CC标准框架下开发一个安全产品的全过程描述为图 1的形式.

在图 1形式的产品开发过程中,步骤 1根据现实世界的安全问题建立安全环境,步骤 2根据安全环境确立安全目标, 步骤 3根据安全目标描述安全需求, 步骤 4根据安全需求定义安全功能,步骤 5根据安全功能开发安全产品,步骤 6把安全产品投放到应用环境中. 这个过程蕴涵着产生于现实世界、服务于应用环境的哲理.

为了研究产品的安全确信度的需要,作者根据图 1描述的安全产品开发过程定义下面的命题.

命题 $p1$ 步骤 1建立的安全环境能够清楚地定义要处理的现实世界安全问题的本质和范围.

命题 ***p2*** 步骤 2确立的安全目标能够简明扼要地表达对步骤 1建立的安全问题的响应或解决办法.

命题 ***p3*** 步骤 3描述的安全需求能够达到步骤 2确立的安全目标.

命题 ***p4*** 步骤 4定义的安全功能能够满足步骤 3描述的安全需求.

命题 ***p5*** 步骤 5开发的安全产品能够实现步骤 4定义的安全功能.

命题 ***p6*** 欲在应用环境中使用的安全产品确实是开发人员在步骤 5中开发的产品并且能够按照预期的方式进行工作.

命题 ***p*** 欲在应用环境中使用的安全产品能够有效地处理现实世界中遇到的安全问题.

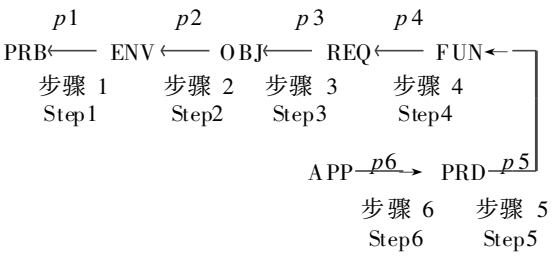


图 1 CC标准框架下的安全产品开发过程

Fig. 1 The development process of a security product under the CC framework

← 衍生自 Derived from; PRB 现实安全问题 Real world security problems; ENV: 安全环境标识 Security environment identification; OBJ 安全目标表述 Security objective description; REQ 安全需求定义 Security requirement definition; FUN: 安全功能说明 Security function specification; PRD 安全产品 Security product; App: 应用环境中的安全产品 Security product in application environment; *p*1~ *p*6 命题 Propositions; 步骤 1~ 步骤 6 Step 1 to 6 安全产品开发步骤 Product production steps

### 1.2 安全保障措施

考虑到历史上评价过的计算机安全产品的安全确信度大部分都介于 EAL3与 EAL4之间这个实情[12], 不失一般性, 这里仍然结合我们的 RS-Linux安全操作系统研究实验,以定位在增强的 EAL3安全保障等级的安全确信度等级为例进行讨论,该保障等级包含表 1列出的所有保障需求组件. 下面给出这些保障需求组件的简要说明.

ADV_ FSP. 1组件: 非形式化的功能性描述.

ADV_ HLD. 2组件: 安全性实施的高级设计.

ADV_ RCR. 1组件: 非形式化的一致性证明.

ADV_ SPM. 1组件: 非形式化的安全政策模型化.

ALC_ DVS. 1组件: 开发环境安全措施的描述.

ACM_ SCP. 1组件: 配置管理的覆盖范围.

ACM_ CAP. 3组件: 配置管理的授权控制.

ATE_ COV. 2组件: 测试的覆盖范围分析.

ATE_ DPT. 1组件: 高级设计的测试.

ATE_ FUN. 1组件: 功能性测试.

ATE_ IND. 2组件: 独立抽样测试.

AVA_ MSU. 1组件: 指南审查.

AVA_ SOF. 1组件: 安全性强度评价.

AVA_ VLA. 1组件: 开发人员对脆弱性的分析.

AGD_ ADM. 1组件: 管理员指南.

AGD_ USR. 1组件: 用户指南.

ADO_ DEL. 1组件: 交货程序.

ADO_ IGS. 1组件: 安装、生成和启动程序.

表 1 一个增强的 **EAL3**安全保障等级的安全保障措施

**Table 1 Security assurance measures for an EAL3-augmented level**

| 安全保障组件 Assurance component | 目标步骤 Step to ensure | 安全保障组件 Assurance component | 目标步骤 Step to ensure |
|---|---|---|---|
| *E*01: ADV_ FSP. 1 | 5 | *E*10: ATE_ FUN. 1 | 5 |
| *E*02: ADV_ HLD. 2 | 5 | *E*11: ATE_ IND. 2 | 5 |
| *E*03: ADV_ RCR. 1 | 5 | *E*12: AVA_ MSU. 1 | 5 |
| *E*04: ADV_ SPM. 1 | 5 | *E*13: AVA_ SOF. 1 | 5 |
| *E*05: ALC_ DVS. 1 | 5 | *E*14: AVA_ VLA. 1 | 5 |
| *E*06: ACM_ SCP. 1 | 5 | *E*15: AGD_ ADM. 1 | 5 |
| *E*07: ACM_ CAP. 3 | 5 | *E*16: AGD_ USR. 1 | 5 |
| *E*08: ATE_ COV. 2 | 5 | *E*17: ADO_ DEL. 1 | 6 |
| *E*09: ATE_ DPT. 1 | 5 | *E*18: ADO_ IGS. 1 | 6 |

## 2 CC标准的安全确信度的表示

安全产品的评价应该客观、公正, 但评价本身属于主观行为, 作者认为 Josang的主观逻辑为这种主观行为的描述提供了一种有效的手段. 本节首先讨论 Josang主观逻辑的基本精神, 进而根据这些基本精神给出 CC标准框架下的安全确信度的一种定量描述思想.

### 2.1 主观逻辑的基本思想

下面简要描述作为我们进一步讨论的基础的 Josang主观逻辑的一些基本思想,详细的内容可参见文献 [10, 11].

定义 **1** (意见) 设 $\Theta$ 是一个有 2个状态 $x$ 和 $\neg x$ 的二元辨别体系,设 $b(x)$, $d(x)$, $u(x)$ 和 $a(x)$ 分别是 $x$ 上的信念、负信念、不确定性和相对原子度函数,那么,一个主体持有的关于 $x$ 的意见 (用 $k_x$ 表

示) 由以下四元组定义:

$$k_x \equiv (b(x), d(x), u(x), a(x)).$$

一个辨别体系是一个可能性情形的集合,它为一个给定的系统界定一组有可能出现的状态.

信念表示一个主体认为一个命题为真的程度,负信念表示一个主体认为一个命题为假的程度,不确定性表示一个主体不能确定命题的真假的程度.

为了简单起见,信念、负信念、不确定性和相对原子度可以分别表示为 $b_x$, $d_x$, $u_x$ 和 $a_x$. 为了明确主体和命题的关系,一个主体 $A$ 持有的关于一个命题 $x$ 的意见可以表示为 $k_x^A$.

定理 **1**(命题的合取) 设 $\Theta_X$ 和 $\Theta_Y$ 是 2个不同的二元辨别体系,$x$ 和 $y$ 分别是关于 $\Theta_X$ 和 $\Theta_Y$ 中的状态的命题,令 $k_x = (b_x, d_x, u_x, a_x)$ 和 $k_y = (b_y, d_y, u_y, a_y)$ 分别是一个主体持有的关于 $x$ 和 $y$ 的意见,令:

$$b_{x\wedge y} = b_x b_y,$$

$$d_{x\wedge y} = d_x + d_y - d_x d_y,$$

$$u_{x\wedge y} = b_x u_y + u_x b_y + u_x u_y,$$

$$a_{x\wedge y} = \frac{b_x u_y a_y + u_x a_x b_y + u_x a_x u_y a_y}{b_x u_y + u_x b_y + u_x u_y},$$

则 $k_{x\wedge y} = (b_{x\wedge y}, d_{x\wedge y}, u_{x\wedge y}, a_{x\wedge y})$ 表示该主体持有的关于命题 $x$ 和 $y$ 同时为真的意见,$k_{x\wedge y}$ 称为 $k_x$ 和 $k_y$ 的命题合取,表示为:

$$k_{x\wedge y} \equiv k_x \wedge k_y.$$

定理 **2**(一致性) 设 $k_x^A = (b_x^A, d_x^A, u_x^A, a_x^A)$ 和 $k_x^B = (b_x^B, d_x^B, u_x^B, a_x^B)$ 分别是主体 $A$ 和 $B$ 持有的关于同一个命题 $x$ 的意见,令:

$$b_x^{A,B} = (b_x^A u_x^B + b_x^B u_x^A)/k,$$

$$d_x^{A,B} = (d_x^A u_x^B + d_x^B u_x^A)/k,$$

$$u_x^{A,B} = (u_x^A u_x^B)/k,$$

$$a_x^{A,B} = \frac{a_x^B u_x^A + a_x^A u_x^B - (a_x^A + a_x^B) u_x^A u_x^B}{u_x^A + u_x^B - 2u_x^A u_x^B},$$

其中,$k = u_x^A + u_x^B - u_x^A u_x^B$,使得 $k \neq 0$,当 $u_x^A, u_x^B = 1$ 时,令 $a_x^{A,B} = (a_x^A + a_x^B)/2$.

则 $k_x^{A,B} = (b_x^{A,B}, d_x^{A,B}, u_x^{A,B}, a_x^{A,B})$ 表示同时代表主体 $A$ 和主体 $B$ 的想象中的主体 $[A,B]$ 持有的关于 $x$ 的意见,$k_x^{A,B}$ 称为 $k_x^A$ 和 $k_x^B$ 之间的一致性,表示为:

$$k_x^{A,B} \equiv k_x^A \oplus k_x^B.$$

定义 **2**(意见的比较) 设 $k_x$ 和 $k_y$ 是 2个意见,它们可以按照以下条件的优先次序进行比较:

1) 概率期望值大的意见的影响程度高;

2) 不确定性值小的意见的影响程度高;

3) 相对原子度值小的意见的影响程度度高.

比较两个意见时,首先按照 1)进行比较,如果概率期望值相同;再按照 2)进行比较;如果还区分不出高低,再按照 3)进行比较.

对于二元辨别体系来说,容易证明,意见的概率期望值可由公式 (1) 计算:

$$E(k_x) = b_x + u_x a_x. \quad (1)$$

**2.2** 确信度的定量表示方法

从安全产品的整个开发过程考虑,作者认为在 CC标准框架下开发的产品的安全性可信程度可以描述为命题 $p$ 为真的程度,因而,在 CC标准框架下开发的安全产品的安全确信度可以由关于命题 $p$ 的意见来表示.

设 $k_{p1} \equiv (b_{p1}, d_{p1}, u_{p1}, a_{p1})$ 是一个主体关于命题 $p1$ 的真实性的意见,类似地,定义 $k_{p2}, k_{p3}, k_{p4}, k_{p5}, k_{p6}$ 和 $k_p$ 分别是关于命题 $p2, p3, p4, p5, p6$ 和 $p$ 的意见. 命题 $p$ 反映整个开发过程的确信度,而命题 $p1, p2, p3, p4, p5$ 和 $p6$ 反映各个子过程的确信度. 利用定理 1中给出的命题合取运算,我们可以通过公式 (2) 计算在 CC标准框架下开发的一个安全产品的安全性可信程度:

$$k_p = k_{p1} \wedge k_{p2} \wedge k_{p3} \wedge k_{p4} \wedge k_{p5} \wedge k_{p6}. \quad (2)$$

CC标准框架下的安全产品的开发实施表 1列出的每一个保障措施,以确保步骤 5和步骤 6能完成相应的任务.

例如,第 $E01$ 号措施从其中一个角度确保步骤 5能得出正确的工作结果. 换句话说,可以从第 $E01$ 号措施的角度出发,确保命题 $p5$ 的真实性. 最终得到的实际效果就是,从第 $E01$ 号措施方面考虑,命题 $p5$ 为真,至于命题 $p5$ 为真的程度,则由安全产品的评价人员去确定,这可以解释为一个考虑第 $E01$ 号措施的想象中的主体持有的关于命题 $p5$ 的意见,相应地,我们就把这个想象中的主体命名为 $E01$. 这样,实施第 $E01$ 号措施建立的安全确信度便可以描述为主体 $E01$ 关于命题 $p5$ 的意见.

设 $k_{p5}^{E01} \equiv (b_{p5}^{E01}, d_{p5}^{E01}, u_{p5}^{E01}, a_{p5}^{E01})$ 是想象中的主体 $E01$ 关于命题 $p5$ 的意见,类似地,定义 $k_{p5}^{E02}, \cdots, k_{p5}^{E16}$. 步骤 5中建立的安全保障程度实际上是关于在这个步骤中实施的所有保障措施所发挥的作用的一个一致性意见,即是主体 $E01, E02, \cdots, E16$ 关于命题 $p5$ 的各个意见的一致性总体意见. 根据定理 2,我们有:

$$k_{p5} = k_{p5}^{E01} \oplus k_{p5}^{E02} \oplus \cdots \oplus k_{p5}^{E16}. \quad (3)$$

采用同样的方法,我们有:

$$k_{p6} = k_{p6}^{E17} \oplus k_{p6}^{E18}. \quad (4)$$

作为以上讨论的结果,我们得出了计算 $k_{p5}$ 和 $k_{p6}$ 以及最终的 $k_p$ 的方法,即公式 (2) ~ (4),而 $k_p$ 就是我们需要的安全确信度的定量表示结果. 公式 (2)~(4)右端的其它有关意见则由评价人员在安全产品的

评价过程中根据产品的开发情况分别确定 .

概括起来就是 , 在按照 CC标准对安全产品进行评价时 , 产品评价人员首先确定以下意见:

$k_{p1}$ 至 $k_{p4}$, $k_{p5}^{E01}$ 至 $k_{p5}^{E16}$、$k_{p6}^{E17}$ 和 $k_{p6}^{E18}$.

然后 ,根据公式 (3) 计算 $k_{p5}$,根据公式 (4) 计算 $k_{p6}$,最后 ,根据公式 (2) 计算产品的安全确信度 $k_p$.

产品的确信度可以根据定义 2进行比较 ,定义 2中“影响程度高” 的解释就是“确信度高” .

## 3 确信度定量表示方法的实际意义

前面的讨论是抽象的 ,下面通过几个例子进一步阐述安全确信度定量表示方法的实际意义 .

例 **1** 设 SP1是在 CC标准框架下开发的一个安全产品 ,在产品的评价过程中 ,评价人员对步骤 1至步骤 4的工作给出了相同的评价意见 ,对步骤 5中各个安全保障措施的实施情况给出了相同的评价意见 , 对步骤 6中的安全措施的实施情况也给出了相同的评价意见 ,具体意见如下:

$$k_{p1} = k_{p2} = k_{p3} = k_{p4} = (0.9,\ 0.05,\ 0.05,\ 0.5), \quad (5)$$

$$k_{p5}^{E01} = k_{p5}^{E02} = \cdots = k_{p5}^{E16} = (0.7, 0.1, 0.2, 0.5), \quad (6)$$

$$k_{p6}^{E17} = k_{p6}^{E18} = (0.8,\ 0.1,\ 0.1,\ 0.5). \quad (7)$$

我们需要计算产品 SP1的安全确信度 $k_p$.

根据公式 (4) 和定理 2计算出 $k_{p6}$的值如下:

$$k_{p6} = (0.8, 0.1, 0.1, 0.5) \oplus (0.8, 0.1, 0.1, 0.5) = (0.842\,1,\ 0.105\,3, 0.052\,6, 0.5). \quad (8)$$

根据公式 (3)和定理 2计算 $k_{p5}$的值 ,计算过程由表 2表示 .

按照公式 (3) 进行计算时 ,需要从左到右依次进行 15次意见的一致性运算 ,表 2给出了每一次运算得到的中间结果 ,表中的 $k_{p5}^{E01}$ 至 $k_{p5}^{E02}$, $k_{p5}^{E01}$ 至 $k_{p5}^{E03}$,… , $k_{p5}^{E01}$ 至 $k_{p5}^{E16}$分别表示:

$k_{p5}^{E01} \oplus k_{p5}^{E02}$,

$k_{p5}^{E01} \oplus k_{p5}^{E02} \oplus k_{p5}^{E03}$,

…,

$k_{p5}^{E01} \oplus k_{p5}^{E02} \oplus \cdots \oplus k_{p5}^{E16}$.

所以 ,表 2中最后一行给出的就是所需的结果 , 即:

$$k_{p5} = (0.861\,6, 0.123\,0, 0.015\,4, 0.5). \quad (9)$$

表 2还给出了各中间结果对应的概率期望值 ,概率期望根据公式 (1) 计算 . 表 2的概率期望值表明 , 随着计算步数的增加 ,概率期望值增大 ,这意味着在产品开发阶段增加安全保障措施可以提高产品在开发阶段的安全确信度 .

表 **2** 步骤 **5**的评价意见 $\omega_{p5}$的计算过程

**Table 2 Computing process of evaluation opinions about step 5**

| 一致性运算 Consensus | 运算结果 Computation result | | | | 概率期望 Probability expectation |
|---|---|---|---|---|---|
| | $b_x$ | $d_x$ | $u_x$ | $a_x$ | |
| $k_{p5}^{E01}$ | 0.7 | 0.1 | 0.2 | 0.5 | 0.8 |
| $k_{p5}^{E01}$ 至 $k_{p5}^{E02}$ | 0.777 8 | 0.111 1 | 0.111 1 | 0.5 | 0.833 4 |
| $k_{p5}^{E01}$ 至 $k_{p5}^{E03}$ | 0.807 7 | 0.115 4 | 0.076 9 | 0.5 | 0.846 2 |
| $k_{p5}^{E01}$ 至 $k_{p5}^{E04}$ | 0.823 5 | 0.117 7 | 0.058 8 | 0.5 | 0.852 9 |
| $k_{p5}^{E01}$ 至 $k_{p5}^{E05}$ | 0.833 3 | 0.119 1 | 0.047 6 | 0.5 | 0.857 1 |
| $k_{p5}^{E01}$ 至 $k_{p5}^{E06}$ | 0.840 0 | 0.120 0 | 0.040 0 | 0.5 | 0.86 |
| $k_{p5}^{E01}$ 至 $k_{p5}^{E07}$ | 0.844 8 | 0.120 7 | 0.034 5 | 0.5 | 0.862 1 |
| $k_{p5}^{E01}$ 至 $k_{p5}^{E08}$ | 0.848 5 | 0.121 2 | 0.030 3 | 0.5 | 0.863 7 |
| $k_{p5}^{E01}$ 至 $k_{p5}^{E09}$ | 0.851 4 | 0.121 6 | 0.027 0 | 0.5 | 0.864 9 |
| $k_{p5}^{E01}$ 至 $k_{p5}^{E10}$ | 0.853 7 | 0.121 9 | 0.024 4 | 0.5 | 0.865 9 |
| $k_{p5}^{E01}$ 至 $k_{p5}^{E11}$ | 0.855 6 | 0.122 2 | 0.022 2 | 0.5 | 0.866 7 |
| $k_{p5}^{E01}$ 至 $k_{p5}^{E12}$ | 0.857 2 | 0.122 4 | 0.020 4 | 0.5 | 0.867 4 |
| $k_{p5}^{E01}$ 至 $k_{p5}^{E13}$ | 0.858 5 | 0.122 6 | 0.018 9 | 0.5 | 0.868 0 |
| $k_{p5}^{E01}$ 至 $k_{p5}^{E14}$ | 0.859 7 | 0.122 8 | 0.017 6 | 0.5 | 0.868 5 |
| $k_{p5}^{E01}$ 至 $k_{p5}^{E15}$ | 0.860 7 | 0.122 9 | 0.016 4 | 0.5 | 0.868 9 |
| $k_{p5}^{E01}$ 至 $k_{p5}^{E16}$ | 0.861 6 | 0.123 0 | 0.015 4 | 0.5 | 0.869 3 |

有了 $k_{p5}$和 $k_{p6}$的值 ,根据公式 (2) 和定义 1便可计算出 $k_p$的值 ,表 3给出了计算的过程 . 表 3的结果与表 2相似 ,表 3中的最后一行给出的就是所需的结果 ,即:

$$k_p = (0.476\,0, 0.360\,9, 0.163\,0, 0.469\,9), \quad (10)$$

$$E(k_p) = 0.552\,6. \quad (11)$$

表 **3** 整体评价意见 $\omega_p$的计算过程

**Table 3 Computing process of the whole evaluation opinion**

| 合取运算 Conjunction | 运算结果 Computation result | | | | 概率期望 Probability expectation |
|---|---|---|---|---|---|
| | $b_x$ | $d_x$ | $u_x$ | $a_x$ | |
| $k_{p1}$ | 0.9 | 0.05 | 0.05 | 0.5 | 0.925 |
| $k_{p1}$ 至 $k_{p2}$ | 0.81 | 0.097 5 | 0.092 5 | 0.493 2 | 0.855 6 |
| $k_{p1}$ 至 $k_{p3}$ | 0.729 | 0.142 6 | 0.128 4 | 0.486 5 | 0.791 5 |
| $k_{p1}$ 至 $k_{p4}$ | 0.656 1 | 0.185 5 | 0.158 4 | 0.479 7 | 0.732 1 |
| $k_{p1}$ 至 $k_{p5}$ | 0.565 3 | 0.285 7 | 0.149 0 | 0.477 2 | 0.636 4 |
| $k_{p1}$ 至 $k_{p6}$ | 0.476 0 | 0.360 9 | 0.163 0 | 0.469 9 | 0.552 6 |

这就是根据评价人员给出的评价意见得出的关于产品的安全确信度的定量表示数据 , 显然 , 这是一种多维形式的表示法 . 利用这些定量数据 ,根据定义 2便可以对安全确信度进行定量比较 .

例 **2** 设 SP2是在 CC标准框架下开发的一个安全产品 , 在产品评价过程中 , 除了 $k_{p5}^{E16}$以外 , 评价人员给出的其它评价意见与产品 SP1相同 , $k_{p5}^{E16}$意见如下:

$$k_{p5}^{E16} = (0.5, 0.2, 0.3, 0.5). \quad (12)$$

根据表 2的计算过程 ,可计算出:

$$k_{p5} = (0.855\,3, 0.128\,9, 0.015\,8, 0.5). \quad (13)$$

根据表 3的计算过程 ,可计算出:

$k_p$ = (0.472 6, 0.365 2, 0.162 2, 0.469 8). (14)

$E(k_p)$ = 0.548 8. (15)

例 3 设 SP3是在 CC标准框架下开发的一个安全产品,在产品评价过程中,评价人员给出的评价意见类似于产品 SP2, $k_{p5}^{E16}$意见如下:

$k_{p5}^{E16}$ = (0.8, 0.1, 0.1, 0.5). (16)

用与例 2相同的方法,可计算出:

$k_{p5}$ = (0.864 3, 0.121 4, 0.014 3, 0.5), (17)

$k_p$ = (0.477 6, 0.369 7, 0.162 8, 0.470 0). (18)

$E(k_p)$ = 0.554 1. (19)

综合例 1、例 2和例 3,我们假定 SP1、SP2和 SP3是同类产品,并且选定了相同的安全保障等级.我们可以根据式 (10)、(14) 和 (18) 对这三个产品进行定量分析比较,结合式 (11)、(15) 和 (19),由于:

[式 (15) 的值] < [式 (11) 的值] < [式 (19) 的值]

根据定义 2就有以下结论:

确信度 (SP2) <确信度 (SP1) <确信度 (SP3)

这是由于式 (6)、(12) 和 (16) 中给出的不同评价意见引起的.

## 4 结语

本文结合 RS-Linux安全操作系统研究实验,对 CC标准框架下的安全产品开发过程进行了概括和抽象,借助 A. Josang的主观逻辑,针对在 CC标准框架下建立的安全产品的安全确信度,提出了安全确信度的一种定量表示方法.

常规的安全产品评价方法给出的评价结果是定性的,它常常是一个断定安全产品“通过”或“未通过”评价的结论[13]. 这类方法只能在通过评价的产品和未通过评价的产品之间画一个界限,但无论是对已通过评价的产品之间的比较还是对未通过评价的产品之间的比较都无能为力.美国国家安全局的 K. G. Olthoff指出[4], 这类方法存在很多弊端,不利于安全产品的发展,有碍于安全技术的进步.

本文的研究工作为解决常规安全评价方法中存在的问题增加了一条有效的途径.本文的研究成果一方面可用于定量地表示产品的安全确信度,为实际应用中产品安全性的定量比较提供了一种有效的依据;另一方面可用于刻画 CC标准在提高安全确信度方面所能发挥的作用,为安全评价标准推动安全技术进步的潜动力的研究提供了一种新的手段.

## 参考文献


1 Joint Technical Committee 1. Evaluation Criteria for IT Security-Part 1: Introduction and General Model. ISO/IEC 15408-1: 1999 (E), The International Organization for Standardization and the International Electrotechnical Commission, 1999.

2 Joint Technical Committee 1. Evaluation Criteria for IT Security-Part 2 Security Functional Requirements. ISO/IEC 15408-2: 1999(E), The International Organization for Standardization and the International Electrotechnical Commission, 1999.

3 Joint Technical Committee 1. Evaluation Criteria for IT Security-Part 3 Security Assurance Requirements. ISO/IEC 15408-3: 1999(E), The International Organization for Standardization and the International Electrotechnical Commission, 1999.

4 Kenneth G Olthoff. Thoughts and Questions on Common Criteria Evaluations. 23rd. National Information Systems Security Conference, Baltimore, Maryland, USA, Oct, 2000, 16~19.

5 National Institute of Standards and Technology. A Head Start on Assurance. Proceedings of an Invitational Workshop on Information Technology (IT) Assurance and Trustworthiness, NISTIR 5472, USA, Mar, 1994.

6 SSE-CMM Project. Systems Security Engineering Capability Maturity Model (SSE-CMM) Model Description Document. Version 2.0. National Security Agency, Office of the Secretary of Defense, and Communications Security Establishment (Canada), Apr, 1, 1999.

7 George F Jelen, Jeffrey R Williams. A Practical Approach to Measuring Assurance. Proceedings of the 14th Annual Computer Security Applications Conference, IEEE Computer Society, 1998.

8 Wenchang Shi, Yufang Sun. An Investigation of CC's Contribution to Confidence in Security. The 2001 International Conference on Computer Network and Mobile Computing, Los Alamitos, CA, USA: IEEE Computer Society Press, Oct, 2001, 333~338.

9 石文昌,孙玉芳.通过 CC标准的思想确定 RS-Linux的安全可信度.广西科学, 2001, 8 (1): 15~18.

10 Audun Josang. A logic for uncertain probabilities. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2001, 9 (3): 279~311.

11 Audun Josang, Viggo A Bondi. Legal reasoning with subjective logic. Artificial Intelligence and Law, 2001, 8 (4): 289~315.

12 Richard E Smith. Trends in government endorsed security product evaluations. 23rd National Information Systems Security Conference, Baltimore, Maryland, USA, Oct, 2000, 16~19.

13 Common Criteria Interpretation Management Board. Common evaluation methodology for information technology Security. Part 2 Evaluation Methodology. Version 1.0. CEM-99/045, Common Criteria Project Sponsoring Organizations, Aug, 1999.


(责任编辑: 蒋汉明)