信息安全国际标准 CC 的结构模型分析*)

An Analysis of the International Common Criteria for Information Technology Security Evaluation

石文昌　孙玉芳

(中国科学院软件研究所　北京 100080)

Abstract The Common Criteria for Information Technology Security Evaluation(CC)jointly developed by the United States, Canada, the United Kingdom and other countries were approved and accepted as an international standard by the International Organization for Standardization in 1999. Since then, in the United States, no new evaluations may be conducted against the Orange Book, whereas, all new evaluations of security offered by information products must be carried out against CC. CC takes security function and security assurance measure as separate concepts. It advocates the development of security products on security engineering, gaining confidence in IT security through actions that may be taken during the processes of development, evaluation and operation. This paper presents the general structural model of CC by giving an analysis to this criteria with an emphasis on the definition of security requiremtnts, the usage of requirement definitions, the level of confidence in security, the development of secure products and the security evaluation of products. At the end, the basic methodology to develop a secure operating system kernel based on this model is stated

Keywords Information security, Evaluation, Common criteria, Security requirement, Evaluation assurance level

一、引言

信息安全产品或系统(以下统称产品)安全性的衡量准则之一是安全评价标准。美、加、英、法、德、荷等国家联合推出的"信息技术安全评价共同标准"(简记CC)于一九九九年七月通过国际标准化组织认可，确立为信息安全评价国际标准。一直以来，作为第一个信息安全评价标准，美国国防部于一九八三年推出并于一九八五年修定的"可信计算机安全评价标准"(又称"橙皮书")[1]在国际上起着很大的作用。CC 标准确立后，美国不再受理以橙皮书为尺度的新的评价申请，今后的安全产品评价工作均按 CC 标准进行[2]。

谈及产品的安全性，涉及到两个重要因素，其一是产品提供哪些安全功能，其二是安全功能的可信度有多大。同样的安全功能，可以有不同的安全可信度。CC 标准充分体现了这一思想，推行产品安全功能与安全保证措施相独立的观念。

从组织形式上，CC 标准分为三个部分，第一部分描述标准的概貌和有关基本概念[3]，第二部分对一系列公认的安全功能加以定义[4]，第三部分对为取得安全可信度应采取的一系列保证措施加以定义[5]。CC 标准提倡安全工程的思想，通过信息安全产品的开发、评价、使用全过程的各个环节的综合考虑来确保产品的安全性。

下面通过安全需求的定义、需求定义的用法、安全可信度级别、安全产品的开发和产品安全性评价等几个方面的分析，给出 CC 标准的结构模型，最后给出我们根据这个模型研制操作系统安全核心系统的基本做法。

二、安全需求的定义

众所周知，软件开发的工程过程是从需求分析开始的，弄清了需求，才能确定软件系统的最终使命。安全产品的开发也不例外，必须从安全需求分析开始。CC 标准对安全需求的表示形式给出了一套定义方法，同时，对公认的一系列安全需求给出了明确的定义，供安全产品的开发人员、未来用户、评价人员等参照使用。

2.1　安全需求定义方式

在 CC 标准中，安全需求以类、族、组件的形式进行定义，这给出了对安全需求进行分组归类的方法。首先，对安全需求的全集，根据不同的侧重点，划分成若

*)国家 863 高科技项目(863-306-ZD12-14-2)基金支持。石文昌　博导，主要研究方向为系统软件和中文信息处理。孙玉芳　博士生，主要研究方向为系统软件安全性。研究员，

干大组，每个大组就称为一个类。每个类的安全需求，根据不同的安全目标，又划分成若干小组，每个小组就称为一个族。每个族的安全需求，根据不同的安全强度或能力，再进一步划分成更小的组，每一个这样的更小的组用一个组件来表示。这样，安全需求由类构成，类由族构成、族由组件构成。组件是CC标准中最小的可选安全需求集，是安全需求的具体表现形式。

例如，身份识别和认证方面的需求归为一个类；这个类中，身份识别方面的需求归为一个族；这个族中，缓时识别方面的需求构成一个组件；所谓缓时识别是指允许用户在身份识别前执行适当的操作。

CC标准将安全需求分成产品安全功能方面的需求和安全保证措施方面的需求两个独立的范畴来定义。产品安全功能方面的需求称为安全功能需求，在标准的第二部分中定义[4]，用于描述产品应该提供的安全功能。安全保证措施方面的需求称为安全保证需求，在标准的第三部分中定义[5]，用于描述产品的安全可信度及为获取一定的可信度应该采取的措施。

2.2 安全功能需求

CC标准定义了十一个公认的安全功能需求类，即：安全审计类、通信类、加密支持类、用户数据保护类、身份识别与认证类、安全管理类、隐私类、安全功能件保护类、资源使用类、安全产品访问类和可信路径/通道类。

安全审计类涉及与安全有关的操作信息的识别、记录、存储和分析等方面的需求。通信类涉及数据交换双方的身份确保等方面的需求，包括收、发双方的防抵赖等。加密支持类涉及密钥管理和加密操作等方面的需求。用户数据保护类涉及对用户数据进行保护的安全功能和安全策略等方面的需求。身份识别与认证类涉及证实用户身份和确立安全属性等方面的需求。安全管理类涉及对产品的安全功能件中的属性、数据和功能等进行管理方面的需求。隐私类涉及确保用户身份的隐蔽性和防止用户身份被盗用等方面的需求。安全功能件保护类涉及确保安全功能件中的有关机制和数据的完整性等方面的需求。资源使用类涉及对需要访问的资源的可用性给以支持等方面的需求。安全产品访问类涉及对人(用户)机(安全产品)会话过程的建立进行控制等方面的需求。可信路径/通道类涉及在用户与安全功能件之间建立可信通讯路径、在安全功能件与其它可信IT产品之间建立可信通讯通道等方面的需求。

2.3 安全保证需求

CC标准定义了七个公认的安全保证需求类，即：构造管理类、发行与使用类、开发类、指南文档类、生命周期支持类、测试类和脆弱性评估类。

构造管理类涉及确保产品的功能需求和规格说明在最终的安全产品中得以实现方面的需求。发行与使用类涉及安全产品的正确发行、安装、生成和投入运行等方面的需求。开发类涉及四大方面的需求：一是安全功能件在不同抽象层次上的表示；二是不同抽象层次上的安全功能件表示之间的一致性；三是安全策略模型的建立及安全策略、安全策略模型与功能描述之间的一致性。指南文档类涉及产品的用户指南、管理员指南等文档资料方面的需求。生命周期支持类涉及产品的开发、维护过程中有关开发、维护模式以及安全措施等方面的需求。测试类涉及产品测试方面的需求。脆弱性评估类涉及对产品可能存在的脆弱性(如隐通道等)进行分析等方面的需求。

三、需求定义的用法

安全需求定义中的类和族反映的是分类方法，具体的安全需求由组件体现。选择一个需求组件等同于选择一项安全需求。CC标准鼓励人们尽可能选用该标准中已定义的安全需求组件，也允许人们自行定义其它必要的安全需求组件。

每个安全需求组件表示的是某项具体的安全需求。通常，一个安全产品总是融多项安全需求于一身，需要用多个需求组件以一定的组织方式组合起来进行表示。CC标准定义了三种类型的用于描述产品安全需求的组织结构：安全组件包、保护轮廓定义书(简记为PP)和安全对象定义书(简记为ST)。安全需求组件可以在这三种类型的组织结构中得到使用。

3.1 安全组件包

把多个安全需求组件组合在一起所得到的结果就叫做一个安全组件包。安全组件包可用于构造更大的安全组件包或用于构造PP和ST。安全组件包可以表示一组安全功能需求或安全保证需求，这些需求可以满足预定安全目标中的某个子目标的需要。

3.2 保护轮廓定义书(PP)

保护轮廓定义书(PP)是一份安全需求说明书，CC标准对它的格式有明确的规定。PP针对某一类安全环境确立相应的安全目标，进而定义为实现这些安全目标所需要的安全需求。PP给出的是一个与实现无关的安全需求定义，它所定义的这些需求没有针对具体的某一种安全产品，只针对比较明确的安全目标。通常，同一个PP中所定义的安全需求可以在多种不同的安全产品中实现。每个PP都必须指定一个安全可信度级别，这是按照该PP研制的安全产品所应该达到的安全可信度级别。

PP是抽象层次较高的安全需求说明书，可以由产品的用户或开发者或其他第三方来定义，它为用户陈述特定的安全需要提供了一种方法。在PP的定义中，通常都使用CC中定义好的需求组件或由这些组件构成的组件包，同时，也可以使用自行定义的需求组件。在安全产品的开发过程中，PP通常是在ST的定义中

被引用。

PP 的结构由以下几个部分组成:PP 简述、产品说明、安全环境、安全目标、安全需求、PP 应用注释和理论依据等。

PP 简述部分给出 PP 的标识和概貌信息。产品说明部分描述将要实现 PP 所定义的安全需求的安全产品的类型和一般特性。安全环境部分描述安全产品的使用环境中的有关安全因素,包括产品可能面临的安全威胁和产品的使用机构要实施的安全策略等。安全目标部分定义为解决安全环境中的各种安全问题所应确立的安全目标。安全需求部分定义安全产品为达到已确立的安全目标而应该满足的安全需求,包括安全功能需求和安全保证需求。PP 应用注释部分可有可无,它可以包含安全产品的研制、评价和使用等方面的附加支持信息。

理论依据部分为以下论点提供证明依据:一、该 PP 是一个完全的、一致的需求集合;二、符合该 PP 要求的安全产品能在其安全环境中提供有效的安全对策。这个部分包含两个方面的内容:安全目标理论依据和安全需求理论依据。安全目标理论依据需要证明:PP 中的安全目标是从安全环境中导出的并能涵盖其中安全问题的各个方面;安全需求理论依据需要证明:PP 中的安全需求是从安全目标中导出的并能满足安全目标各个方面的要求。

3.3 安全对象定义书(ST)

安全对象定义书(ST)是一份安全需求与概要设计说明书,CC 标准对它的格式有明确的规定。ST 的安全需求定义与 PP 非常相似,不同的是 ST 的安全需求是为某一特定的安全产品而定义的,ST 的安全需求可通过引用某个(或多个)PP 来定义,也可采用与定义 PP 相同的方法从头定义。ST 除包含 PP 所具有的内容外,还包含产品的概要说明。

ST 的结构由以下几个部分组成:ST 简述、产品说明、安全环境、安全目标、安全需求、产品概要说明、PP 引用声明和理论依据等。

其中 ST 简述、产品说明、安全环境、安全目标和安全需求等部分与 PP 中的相应部分相似。概要说明部分对安全需求给出例化定义,一方面,针对安全功能需求定义满足这些需求的安全功能,另一方面,针对安全保证需求定义满足这些需求的安全保证措施。安全功能以非形式化的方式定义,描述要达到一定的详细程度,能把有关的实现情况表达清楚;安全保证措施可适当结合有关质量计划、生命周期计划和管理计划等加以定义。

如果 ST 中有对 PP 的引用,则 PP 引用声明部分陈述有关援引 PP 的情况,包括:ST 与 PP 间需求的一致性、ST 中对 PP 需求的进一步限定、ST 中在 PP 基础上的需求扩展等。

理论依据部分为以下论点提供证明依据:一、该 ST 是一个完全的、一致的需求集合;二、符合该 ST 要求的安全产品能在其安全环境中提供有效的安全对策;三、产品概要说明涵盖了所定义的所有安全需求;四、PP 一致性声明是有效的。这个部分包含四个方面的内容:安全目标理论依据、安全需求理论依据、概要说明理论依据和 PP 声明理论依据;安全目标理论依据和安全需求理论依据与 PP 中的类似;概要说明理论依据需要证明,用 ST 中设计的安全功能和安全措施去实现安全需求中的要求是合适的。如果 ST 引用了 PP,并且,ST 中的需求与 PP 不完全相同,则 PP 声明理论依据需要对其间的差别给予解释。

四、安全可信度级别

CC 标准定义了一套评价保证级别(简记为 EAL),作为刻画产品的安全可信度的尺度。EAL 是由 CC 中定义的安全保证需求组件构成的一个特定的组件包,由此可见,CC 对产品安全可信度的衡量是与产品的安全功能相对独立的。EAL 在产品的安全可信度与获取相应可信度的可行性及所需付出的代价之间给出了不同等级的权衡。

EAL 通过构造管理、发行与使用、开发、指南文档、生命周期支持、测试和脆弱性评估等方面所采取的措施来确立产品的安全可信度。按安全可信度由低到高依次递增的顺序,CC 定义了 EAL1、EAL2、EAL3、EAL4、EAL5、EAL6 和 EAL7 等七个安全可信度级别。

EAL 的各个级别都涉及了 CC 中定义的安全保证需求的各个类的内容,例外的是:EAL1 和 EAL2 不涉及生命周期支持类,同时,EAL1 不涉及脆弱性评估类。

EAL1 是职能式测试级,它表示信息保护问题得到了适当的处理。EAL2 是结构式测试级,它要求评价时在设计信息和测试结果的提供方面得到开发人员的配合,该级提供低中级的独立安全保证。EAL3 是基于方法学的测试与检查级,它要求在设计阶段实施积极的安全工程思想,提供中级的独立安全保证。EAL4 是基于方法学的设计、测试与审查级,它要求按照良好的商业化开发惯例实施积极的安全工程思想,提供中高级的独立安全保证。EAL5 是半形式化的设计与测试级,它要求按照严格的商业化开发惯例、应用专业安全工程技术实施安全工程思想,提供高等级的独立安全保证。EAL6 是半形式化验证的设计与测试级,它通过在严格的开发环境中应用安全工程技术来获取高的安全保证,使产品能在高度危险的环境中使用。EAL7 是形式化验证的设计与测试级,它的目标是使产品能在

极端危险的环境中使用，目前，该级别的实际应用只限于其安全功能可以进行广泛的形式化分析的安全产品。

五、安全产品的开发

通过前面的分析我们可以看出，CC 标准体现了软件工程与安全工程相结合的思想。信息安全产品必须按照软件工程和安全工程的方法进行开发才能较好地获得预期的安全可信度。这里，我们仅就如何确定产品的安全功能和如何使这些安全功能比较可信等问题加以探讨。

从需求分析到产品实现的进展角度，安全产品的开发过程可依次分为以下阶段：现实应用环境分析、确立产品安全环境、确立产品安全目标、确立产品安全需求、安全产品概要设计、安全产品实现等。一般而言，各个阶段依次顺序进行，前一个阶段的工作结果是后一个阶段的工作基础。必要时，也需要根据后面阶段工作的反馈，进一步开展前面阶段的工作，形成循环往复的过程。开发出来的产品经过安全性评价和可用性鉴定后，再投入实际使用。

从安全职能的表现形式的角度，安全产品的开发过程可依次分为以下阶段：需求组件定义、组件包定义、PP 定义、ST 定义、产品实现等。可以认为：组件用于构造组件包，组件包用构造 PP，PP 用于构造 ST，ST 用于作为产品的实现依据。但也不绝对，比如，PP 和 ST 都可以直接由组件来构造，而 PP 和 ST 又都必须引用 EAL 组件包。CC 建议尽量使用其中预定义的组件，也允许自行定义组件；CC 还允许在引用 EAL 组件包前，向该包增加其他组件，或者，把该包中的某组件替换成相应的强度更高的组件。

六、产品安全性评价

CC 标准把待评价的安全产品及其相关指南文档资料称为评价对象（简记为 TOE）。从某种意义上说，本文提到的安全产品均等同于 TOE。

CC 定义了三种评价类型，按照评价的先后次序分别为：PP 评价、ST 评价和 TOE 评价。PP 评价的目的是要证明：被评价的 PP 是完全的、一致的和技术良好的，能用作可评价的 TOE 的需求表示。ST 评价的目的是要证明：被评价的 ST 是完全的、一致的和技术良好的，可作为相应 TOE 评价的基础；同时，如果被评价的 ST 中含有 PP 一致性的声明，还要证明：被评价的 ST 能完全满足 PP 中的需求。TOE 评价的目的是要证明：被评价的 TOE 能满足 ST 中的安全需求。

TOE 是针对 ST 中的安全需求进行评价的，ST 中的安全需求可来自 PP，而 PP 可由用户来定义，很明显，CC 标准中的安全评价，就是要确定安全产品的安全性是否能够满足用户在安全方面的需要。

CC 中专门定义了两个需求类，分别作为 PP 和 ST 的评价标准。另外，CC 也为可信度维护定义了一个需求类。可信度维护的目的是要确保：当一个已评价的 TOE 的环境发生了变化或该 TOE 被加以修改时，如何保证该 TOE 能继续满足其安全需求并拥有其原来的可信度。

结束语 以上我们对 CC 标准进行了比较全面的分析，给出了该标准的结构模型，在 CC 中，TOE 的评价是以 ST 为基础的。不管我们通过什么方式来定义 ST，经过分解，它本质上就是通过需求组件来构造的。因此，需求组件和 PP、ST 等其他结构一起，构成了 CC 标准对信息安全产品评价的基本框架。

CC 标准的评价框架面向所有信息安全产品，提供安全性评价的基本尺度和指导思想。它不限定哪类产品应该提供哪些安全功能，也不限定哪些安全功能应该具有哪个级别的安全可信度；所有这些，由产品的用户、开发人员或其他第三方在实际应用中根据实际需要来确定。

目前，我们正在按照该标准的指导思想研制操作系统的安全核心系统。操作系统应该提供哪些安全功能，这个问题在国际上尚处于不断探索之中。我们的基本做法是：从概念上认定操作系统的安全核心系统由多个子系统组成，这些子系统有些是已知的，有些是未知的；在探讨未知子系统的同时，研制已知子系统；对于已知的子系统，设计出其相应的 ST，并逐步使之付诸实现和得到评价；通过这种不断扩充的方法来增强操作系统核心的安全能力。

参 考 文 献

1 Department of Defense, Department of Defense Trusted Computer System Evaluation Criteria. DoD 5200. 28-STD, Washington, DC, Dec. 1985

2 The Trust Technology Assessment Program, The Computer Security Evaluation Frequently Asked Questions (V3), National Security Agency, 1999. Available at: http://www.radium.ncsc.mil/tpep/process/faq.html

3 The International Organization for Standardization, Common Criteria for Information Technology Security Evaluation-Part 1: Introduction and General Model, ISO/IEC 15408-1:1999(E), 1999

4 The International Organization for Standardization, Common Criteria for Information Technology Security Evaluation-Part 2: Security Functional Requirements, ISO/IEC 15408-2:1999(E), 1999

5 The International Organization for Standardization, Common Criteria for Information Technology Security Evaluation-Part 3: Security Assurance Requirements, ISO/IEC 15408-3:1999(E), 1999