CC与SSE-CMM结合的信息安全评估方法*)

吴 丹 王志英
(国防科技大学计算机学院 长沙410073)

A Method of Information Security Evaluation Combining CC with SSE-CMM

WU Dan WANG Zhi-Ying
(School of Computer, National University of Defense Technology, Changsha 410073)

Abstract The information security evaluation is an important part of information field. It is a general method to execute evaluation to the information security products under the instruction of Common Criteria (CC). A new method of information security evaluation, based on the combination of CC and Systems Security Engineering Capability Maturity Model (SSE-CMM), has been proposed in the paper. The basic idea of this method is using the reference of the security system engineer. Based on the experiment of a Target of Evaluation (TOE) in CC, the evaluation result of security assurance by this new method is proved to be more accurate, more comprehensive and more acceptable.

Keywords Security evaluation, Security system engineer, Assurance, CC, SSE-CMM

1 引言

目前国内对安全产品进行评测主要采用攻击性测试的方式,这种对系统直接的评测是不完备的。首先,它不能检测未知的脆弱性,对于存在的"后门"程序,在一般情况下是无法通过攻击性测试来发现的,除非测试者事先知道"后门"的存在,通过测试来验证;更重要的是,其结果不能证明产品在多大程度上是安全的,即不能说明该产品/系统的安全功能正确实现的可信度是多少。对安全产品的评估不仅要求对产品安全功能 Function 加以评测,也要求对产品的安全保证即可信度 Assurance 进行评测,而且在大多数情况下,安全可信度的重要性要超过安全功能。通用标准 CC 是国际上通用的指导评估的方法,它全面地考虑了与信息技术安全性有关的所有因素,特别是安全可信度的要求。但是,由于安全可信度不是能够直接测量的量,因此可信度评估始终是信息安全评估过程的一个瓶颈,其评估结果也往往令用户难以接受。

我们希望能够结合系统安全工程的思想,把构造系统的工程队伍的能力评测结果作为衡量目标系统安全程度的依据,这种间接的评测有别于对系统的直接评测,由于可信度评估的依据由系统安全工程方法提供,因此使评估过程变得简洁而高效。在本文中,我们着重对安全可信度进行研究,提出了一种将系统安全工程能力成熟度模型 SSE-CMM 与通用标准 CC 结合的评估方法,并通过实例分析和验证,证明了其可行性。

2 CC评估与SSE-CMM评估

标准是技术性法规,没有标准,评估就无从谈起,信息安全产品安全性的衡量准则之一是安全评价标准,包括以TCSEC(桔皮书)为基础的 CC 标准,它将安全功能与安全保证分离,并按照"类-子类-部件-元素"的结构分别定义功能要求和保证要求,定义评估保证级别 EAL 表示安全级别,CC 已成为通用的信息安全产品和系统安全性评价准则;另一个是专门应用于系统安全工程的能力成熟度模型 SSE-CMM,该模型按照"过程域(PA)+能力成熟度级别"定义了一个安全工程过程应有的特征,这些特征是完善的安全工程的根本保证。

2.1 CC评估

CC 提出了目前国际上公认的表述信息安全的结构,将安全要求划分为两大类,即规范产品和系统安全行为的功能要求以及如何正确有效地实施这些功能的保证要求,即安全可信度要求。CC 提出了保护轮廓的概念,用于表达一类产品或系统的用户需求,这一方面解决了技术与真实客观需求之间的内在完备性,另一方面帮助用户分析所面临的安全问题,明确所需的安全策略,进而确定应采取的安全措施,提高安全保护的针对性和有效性。CC 标准把安全可信度与安全功能独立,根据具体系统的安全要求从保证要求中提取相应的保证部件,各部件包组成了一套评估保证等级 EAL,用 EAL 表征对系统安全级别的要求,对 EAL 评估的结果作为刻画产品安全的尺度。基于这些优势,CC 评估方法成为国际上通用的指导评估的方法。CC 评估过程如图1所示。

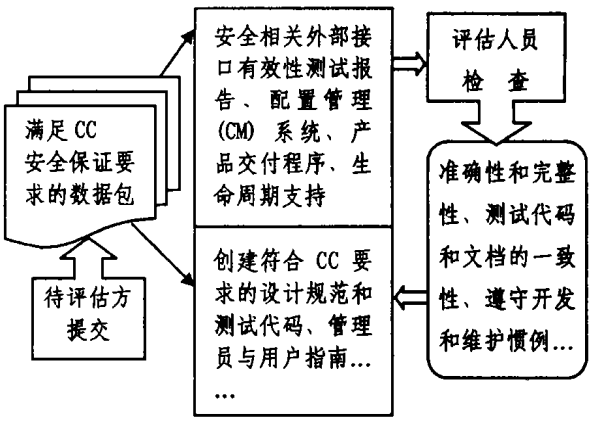

图1 CC评估过程

不难发现,CC 评估需要考虑信息安全产品的开发、评价和使用全过程的各个环节,由于安全可信度不是能够直接测量的量,对它的评测会非常复杂,而且这种复杂性会伴随系统所要求的安全级别升高而变得越复杂。如果安全可信度评测

*)基金项目:国家自然科学基金项目(No.90104025)。吴丹 硕士研究生,研究方向为计算机体系结构,信息安全。王志英 博士,教授,博士生导师,主要研究方向为新型计算机体系结构,微处理器设计,信息安全。

成为一个瓶颈，必然导致评估认证过程的繁复和高成本。按照一般的估计，在国外应用 CC 去对一个低安全级别要求的安全产品进行评测的平均周期是十八个月，甚至更长，因此，产品往往在评估的同时就被投入使用，造成评估结果无的放矢。

2.2 SSE-CMM 评估

系统安全工程能够对安全机制的正确性和有效性做出诠释，也能够证明安全系统的可信度达到了要求或系统遗留的安全薄弱性在可容许范围之内，由此 SSE-CMM 模型确定了一个评价安全工程实施的综合框架，对基于一个工程组的安全实施与过程进行成熟性评估。

SSE-CMM 模型将各种系统安全工程任务抽象、划分为十一个有明显特征的子任务，由此定义了十一项“良好”的安全工程过程即过程域(PA)，每个过程域用一组确定的单元—基本实践(basic practice，简称 BP)来描述完成的任务；设置了六个能力成熟级别，每个级别的判定反映为一组共同特性(Common Feature，简称 CF)，而每个共同特性进而通过一组确定的单元—通用实践(Generic Practice，简称 GP)来描述。于是，SSE-CMM 模型从整体上定义了一个二维架构，如图2所示，横轴上有十一个系统安全工程过程域，纵轴上有六个能力成熟度级别。如果给每个过程域赋予一个能力成熟度级别的评分，所得到的二维图形便形象地反映了一个工程队伍整体上的过程能力成熟性，也间接地反映了这个工程队伍工作结果的安全可信度。

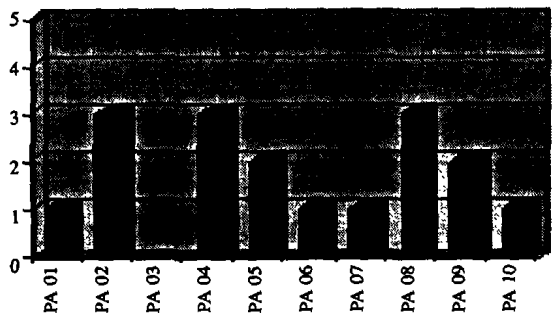

图2 SSE-CMM 模型的二维架构

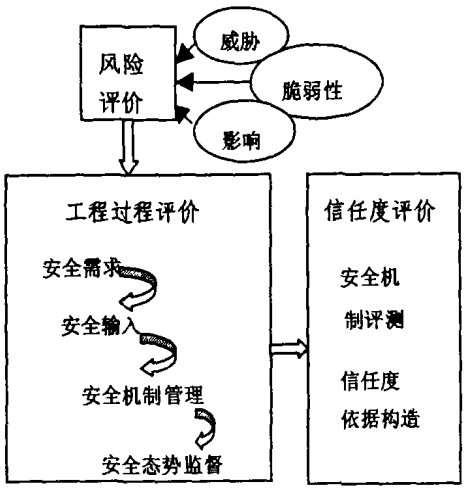

图3 SSE-CMM 评估过程

在运用 SSE-CMM 模型评估一个工程队伍的过程能力成熟性之前，应当先使用这一模型评估该工程队伍在一个或几个项目中的表现；然后针对特定的过程域判断其是否满足某个能力级别定义的全部共同特性，是则说明其工程能力成熟度达到了该级别。如果一个过程域满足了定义在 n+1级上及 n+2级上的部分共同特性，但满足了定义在 n 级上的全部共同特性，其过程能力应当为 n 级。评估过程如图3。

2.3 两种评估方法的比较

本文对两种评估方法的主要方面的性质进行了比较。

从目标来看，SSE-CMM 模型实现工程队伍能力的评定、工程队伍能力的自我改善、安全系统或安全产品的可信度的测量和改善，CC 提供安全性评估的机制和安全保证。从方法来看，SSE-CMM 模型使用安全工程实践的连续的成熟度模型并侧重于对安全工程过程的管理，CC 侧重于对系统和产品的技术指标的评估。从评估结果看，使用 SSE-CMM 模型得到改进的安全工程过程，CC 则对安全策略的应用和可信安全产品的使用提出建议。从完备性来看，SSE-CMM 模型比 CC 具有更高的完备性。

考虑到完备性对于评估方法的意义，我们集中对完备性进行分析。SSE-CMM 模型的完备性表现在两个方面：第一，用过程域描述任务时，构成过程域的单元 BP 一个也不能缺少；第二，判断一个过程的能力时，只有当某一级别的单元 GP 全部得到满足才能说明过程达到了对应的能力级别。相比之下，使用 CC 评估时，对于某一评估保证等级并不要求产品/系统满足该级规定的所有的保证元素。

3 结合的评估方法

SSE-CMM 模型来源于得到工业界广泛接受的统计质量控制原理，如果某个工程队伍的系统安全工程记录是出色的，则其软件开发过程中的代码管理、代码检查或其他好的工艺过程完全有可能杜绝“后门”代码及其他安全隐患的存在。SSE-CMM 模型强调的是一种集成，安全性问题存在于各种工程领域之中，同时也包含在模型的各个组件之中。所以，利用 SSE-CMM 模型对过程能力成熟度进行评估是可以作为可信度评估的依据，这样，按照 CC 标准评估的工作量分摊到了对工程队伍的能力成熟度的评测上，从而使目标系统的安全可信度的评测得到简化。

通过对大量的评估实例进行研究，我们认为，在按照 CC 标准对安全产品/系统进行评估的基础上，结合 SSE-CMM 模型对工程能力成熟度的评估，将成为一种新的且更完备的安全评估方法。

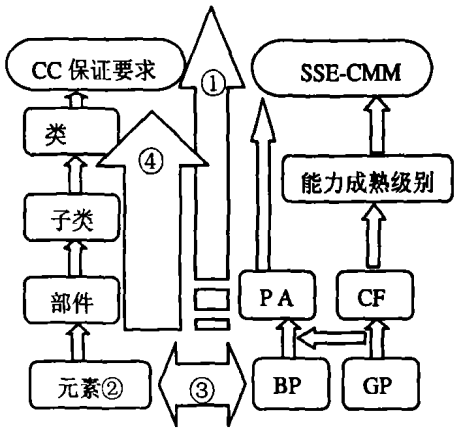

图4 新的评估方法概述

下面是对新的评估方法的描述和论证，区别于新的评估方法，我们称 CC 标准和 SSE-CMM 模型为源评估体系，称按照 CC 标准评估的方法和利用 SSE-CMM 模型评估的方法为源评估方法。

图4描述了新的评估方法。其中①说明新的评估方法采用自底向上的方式，这是因为源评估体系都是自底向上的组件构成型；②元素说明：CC 保证元素共分三类，描述开发者行为的保证元素，描述评估者行为的保证元素和描述可信度(保证)依据的保证元素，目前主要对可信度评估进行研究，所以实验元素均为描述可信度依据的保证元素，简称元素；③说明

评估是从源评估体系的最小单位出发，元素是CC能识别的最小安全需求，BP和GP是SSE-CMM模型的最小单位；④说明在评估过程中，CC的最小单位会随着下一层单位的评估结束而上升级别。

新的评估方法描述如下：

step0 提交评估目标，提交形式为源评估方法所需要的全部数据包，包括评估目标要求达到的评估保证等级及其工程能力成熟度级别，将CC评估体系中的单元依照标准中定义的顺序进行编号。

step1 （参数定义）形如X.Y.Z.e的参数来自源评估体系CC，其含义为编号为e的元素，包含于编号为Z的部件，该部件包含于编号为Y的子类，并最终包含于编号为X的类。形如PA X的参数来自源评估体系SSE-CMM模型，表示编号为X的过程域（0≤X≤10），BP s表示编号为s的基本实践，GP t表示编号为t的通用实践

step2 if 评估目标的评估保证等级EAL为N（1≤N≤7），工程能力成熟级别为M，（0≤M≤5），then，step3

step3 procedure 1{对EAL N级中所有部件
CASE X类X
CASE Y子类X.Y
CASE Z部件X.Y.Z
CASE e元素X.Y.Z.e
procedure 2{
对所有的PA，if PA X实现的任务与类X相当 then，procedure 3{
对PA X中的BP和GP，如果BP s和GP t与元素X.Y.Z.e相关，则合并两者，其结果表示PA X能够完成的任务，与元素e的内容先进行比较后进行判断，如果一致，说明BP s和GP t与元素e匹配，转到step5；否则，跳出并转向step4}}}

step4 根据不匹配的程度对BP s和GP t的内容进行重定义，返回step3

step5 元素X.Y.Z.E可以由BP s和GP t的内容保证，所以可以认定评估目标的该保证元素是可满足的，对该元素标记评估完成

step6 删去标记元素，返回step3，if 部件X.Y.Z的元素集为空，则可以认定评估目标的该保证部件是可满足的，对该部件标记评估完成，转到step7。否则，重复step3～step5

step7 最小单位自底向上变化，操作类似step6

step8 重复以上步骤，直到评估结束

step9 得出评估结论。用工程队伍能力成熟度级别直接作为可信度评估的依据，在该依据保证下，判断评估目标是否满足EAL N级的要求，是则说明通过了评估，认定该系统达到了要求的安全级别，否则为不通过，不能认定系统达到了要求的安全级别。

4 验证与分析

我们使用新的评估方法对一个评估保证等级要求为EAL3级的评估目标进行评估验证。按照自底向上的原则，首先对源评估体系的最小单位进行评估。在最小单位的选取上，从源评估体系SSE-CMM模型的基本实践BP12.02和通用实践GP2.2.1，为了对比，从源评估体系CC中选择了两个元素ACM-CAP.3.5C和ACM_CAP.3.7C

验证过程：

step0 提交评估目标，评估保证等级EAL3级，工程队伍能力成熟度级别2级，编号过程略

step1 （参数定义）①ACM：类名，表示配置管理 ②ACM-CAP：子类名，表示配置管理的能力 ③ACM-CAP.3：部件名，表示只有授权用户才能控制 ④ACM-CAP.3.5C：元素名，表示配置项目在配置管理文档中必须唯一定义 ⑤ACM_CAP.3.7C：元素名，表示配置管理计划要对配置管理系统的使用进行描述 ⑥PA09：编号为9的过程域，即配置管理过程域 ⑦BP12.02：编号为12.02的基本实践，用于确定配置单元 ⑧GP2.1.3：编号为2.1.3的基本实践，用于确定工程过程是否有文档证明 ⑨GP2.2.1编号为2.1.3的基本实践，用于确定工程过程是否使用到符合配置管理要求的计划和标准

step2 匹配性分析：合并⑦⑨，发现⑥能够完成对配置管理的使用进行描述的任务，⑦⑨与⑤匹配，因此⑤是可满足的；合并⑦⑧，发现⑥虽然能够完成对工程过程提供文档证明的任务，但不满足④要求的“唯一定义”这个条件，⑦⑧对于④只是部分匹配

step3 重定义：根据匹配结果，我们需要对⑧重定义。⑧GP2.1.3：编号为2.1.3的基本实践，用于确定工程过程有唯一的文档证明

step4 回到step2，⑦⑧与④也可以完全匹配，有了⑦⑧的保证，④也变得可满足

step5 评估结果：使用新的方法后，成功完成了对这两个元素的评估

分析：从上面的验证过程可以发现，⑧满足的工程队伍能力成熟度级别2可以直接用来作为评估CC EAL3级时的依据。该成熟度级别认定，由于过程执行前的计划和执行中的检查，使得工程队伍可以基于最终结果的质量来管理其实践活动。这样，评价一个EAL3级的安全系统/产品在主权控制方面的可信度时，这个结论可以直接为我们所用，有了这个依据，评估人员执行的质量检查可以从面向过程转为面向结果，这显然使得原先繁复的评估认证变得简洁而高效。

结论：通过验证和分析，我们发现新的评估方法结合了源评估方法的优势，使源评估体系互为补充，改进了原有的可信度评估。

结束语 尽管SSE-CMM模型具有很好的性质，但是必须明确：SSE-CMM模型针对的是工程能力，CC针对的是产品，两者是不同的体系。SSE-CMM模型作为评测工程队伍能力的方法，不能完全取代系统或产品的安全性测试和认证，但可以作为CC的辅助工具，简化安全产品可信度认证。

下一步的工作是针对CC中用来描述评估者行为的元素，完善新的评估方法，经过研究，找到了两种实现的思路：将这些元素从CC的保证部件中分离出来，作为CC的通用评估方法重新定义，或者将评估目标从CC保证元素中独立出来，用SSE-CMM模型的过程描述进行重定义。

CC已将SSE-CMM模型评估考虑为目前最有希望采用的替代认证技术，我们将继续研究源评估方法的结合，对新的安全评估方法做进一步的确立和完善，确保新方法的完备。

参考文献

1 Systems security engineering capability maturity model, model description document, Version 2.0b [EB/OL]. http://www.sse-cmm.org/,1999-10

2 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

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

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