基于 CC 与 SSE-CMM 的高确信度信息安全系统的开发方法*)

谭 良[1,2] 刘 震[1] 周明天[1]

(电子科技大学计算机科学与工程学院 成都 610054)[1] (四川师范大学 成都 610066)[2]

摘 要 尽管 CC 和 SSE-CMM 均可通过对信息安全产品或系统的开发、评价、使用过程等各个环节实施安全工程来确保产品或系统的安全确信度,但 CC 和 SSE-CMM 是两个不同的安全评估标准。文中分别介绍 CC 和 SSE-CMM 的结构模型和特点,并对 CC 和 SSE-CMM 进行比较分析。最后,针对 CC 与 SSE-CMM 具有互补性的特点,提出了将 CC 与 SSE-CMM 结合起来开发高确信度信息安全产品或系统的开发方法。

关键词 安全评估标准,安全工程,CC,SSE-CMM,高确信度

Development Method of High Assurance Information Security System Based on CC and SSE-CMM

TAN Liang[1,2] LIU Zhen[1] ZHOU Ming-Tian[1]

(School of Comp. Sci. & Engn., Univ. of Electronic Sci. & Tech. of China, Chengdu 610054)[1]

(Sichuan Normal University, Chengdu 610066)[2]

Abstract By implementing security engineering in the process of development, evaluation, use, and so on, CC (Common Criteria) and SSE-CMM (Systems Security Engineering Capability Maturity Model) ensure security assurance of products or systems, but CC and SSE-CMM are different. In this paper, structure mode and character of CC and SSE-CMM are introduced, and compared each other. Finally, according to the complementary character between CC and SSE-CMM, a development method of high assurance to information security systems or products is presented by combining the CC and SSE-CMM.

Keywords Security evaluation criteria, Security engineering, CC, SSE-CMM, High assurance

1 引言

随着 Internet 应用的广泛深入,人们对信息技术的依赖越来越强,信息安全问题日益引起人们的高度重视。但由于信息安全技术的复杂性使得信息系统的购买者越来越难以判定所提供的系统是否能够满足他们的安全要求。所以,对信息系统或产品的安全评估就成了人们关注的一个重要课题[1~3]。

信息安全评估是指评估机构依据信息安全评估标准,采用一定的方法(方案)对信息安全产品或系统的安全性进行评价[4]。国际上的信息安全评估标准从 TCSEC[5]、ITSEC[6] 发展到 CC(ISO15408)[7];在国内,与 TCSEC 相对应的标准是 GB-17859-1999《计算机信息安全保护等级划分准则》[8],与 CC 相对应的是 GB-18336-2001《信息技术安全技术信息技术安全性评估准则》[8]。目前,国际上用得最多是 CC,CC 定义了作为评估信息技术产品和系统安全性的基础准则,提出了目前国际上公认的表述信息技术安全性的结构 PP 和 ST,并分离了功能与保证。CC 与早期的评估标准相比,其优势体现在其结构的开放性、表达方式的通用性以及结构和表达方式的内在完备性和实用性三个方面。

由于 CC 是面向最终系统的安全可信度评估标准,评估费用昂贵、耗时费力,并且评估结果缺少继承性,即当前产品的安全确信度与同一工程队伍、依照类似工程过程从前开发的产品的安全确信度并无直接关系。而系统安全工程能力成熟度模型 SSE-CMM[9~11] 是一种衡量系统安全工程实施能力的评估标准,是一种使用面向工程过程的方法。SSE-CMM 的基本思想是:通过对安全工程过程进行管理的途径,将系统安全工程转变为一个完好定义的、成熟的、可测量的过程,具有此类成熟过程的组织开发的安全系统或产品具有较高安全确信度和可重复性,但缺少对安全工程过程中安全需求和保障需求的标准描述。

显然,CC 与 SSE-CMM 具有互补性。对于组织开发的安全系统和产品的测评来说,组织的 SSE-CMM 和安全评估标准 CC 之间存在一定的关系。CC 标准可以用于辅助安全产品的开发,SSE-CMM 可以提高安全系统或产品的工程过程的成熟度。本文首先分别介绍 CC 和 SSE-CMM 的结构模型和特点,然后对 CC 和 SSE-CMM 进行比较分析;最后提出将 CC 与 SSE-CMM 结合起来开发高确信度信息安全产品或系统的开发方法。应用该开发方法,可以缩短评估周期、降低评估费用、节约企业成本。

2 CC 和 SSE-CMM 的结构模型和特点

2.1 CC 的结构模型和特点

CC 定义了作为评估信息技术产品和系统安全性的基础

*)基金项目:国家 863 宽带 VPN 项目 863-104-03-01 课题资助、2003 年度四川省科技攻关项目 03GG007-007 支持。谭 良 博士,主要研究方向为信息安全、中间件;刘 震 博士研究生,主要研究方向为网络计算、信息安全;周明天 教授,博士生导师,主要研究方向为网络计算、信息安全、并行分布计算、中间件技术。

准则，提出了目前国际上公认的表述信息技术安全性的结构，即把安全要求分为规范产品和系统安全行为的功能要求以及解决如何正确有效地实施这些功能的保证要求。功能和保证要求又以“类-子类-组件”的结构表述，组件作为安全功能的最小构件块，可以用于“保护轮廓”、“安全目标”和“包”的构建。另外，功能组件还是连接 CC 与传统安全机制和服务的桥梁，以及解决 CC 同已有准则如 TCSEC、ITSEC 的协调关系，如功能组件构成 TCSEC 的各级要求。

CC 分为 3 个部分：第 1 部分“简介和一般模型”，正文介绍了 CC 中的有关术语、基本概念和一般模型以及与评估有关的一些框架，附录部分主要介绍“保护轮廓”和“安全目标”的基本内容；第 2 部分“安全功能要求”，按类-子类-组件”的方式提出安全功能要求，每一个类除正文以外，还有对应的提示性附录做进一步解释；第 3 部分“安全保证要求”，定义了评估保证级别，介绍了“保护轮廓”和“安全目标”的评估，并按“类-子类-组件”的方式提出安全保证要求。CC 的 3 个部分相互依存，缺一不可。其中，第 1 部分是介绍 CC 的基本概念和基本原理，第 2 部分提出了技术要求，第 3 部分提出了非技术要求和对开发过程、工程过程的要求。这 3 部分的有机结合具体体现在“保护轮廓”和“安全目标”中，“保护轮廓”和“安全目标”的概念和原理由第 1 部分介绍。“保护轮廓”和“安全目标”中的安全功能要求和安全保证要求在第 2、3 部分选取，这些安全要求的完备性和一致性由第 2、3 部分来保证。CC 标准的核心思想有两点：一是信息安全技术提供的安全功能本身和对信息安全技术的保证承诺之间独立；二是安全工程的思想，即通过对信息安全产品的开发、评价、使用全过程的各个环节实施安全工程来确保产品的安全性。CC 标准强调在 IT 产品和系统的整个生命周期确保安全性，因此 CC 标准可以同时面向消费者、开发者、评价者 3 类用户，同时支持他们的应用。对应 3 种不同的用户，CC 标准有 3 种主要应用方式：定义安全需求、辅助安全产品开发、评价产品安全性。

2.2 SSE-CMM 的结构模型和特点

SSE-CMM 可以用于确认一个安全工程组织中某安全工程各领域过程的成熟度。这种结构的目标就是将安全工程的基础特性与管理制度特性区分清楚。为确保这种区分，模型中建立了两个维度——“域维”和“能力维”。“域维”包含所有集中定义的安全过程的所有实施活动，共 60 个基本实施（Basic Pratice：BP），这些基本实施被组成 11 个安全工程过程区（Process Area：PA）：PA01——实施安全控制、PA02——评估影响、PA03——评估安全风险、PA04——评估威胁、PA05——评估脆弱性、PA06——建立保证论据、PA07——协调安全、PA08——监控安全态势、PA09——提供安全输入、PA10——确定安全需求和 PA11——验证和证实安全，每一个过程区包括一组目标，必须执行了该过程区的所有 BP 才能达到这组目标。这些过程区覆盖了安全工程的所有领域。“能力维”代表反映过程管理与制度能力的实施。被分组成若干个被称作“共同特征”的逻辑区域，每个逻辑区域包括多个通用实施（Generic Practice：GP），这些“共同特征”又被分作 5 个能力水平：1 级——非正规实施级、2 级——规划和跟踪级、3 级——充分定义级、4 级——量化控制级和 5 级——持续改进级，分别代表组织能力的不同层次。与“域维”中的基础实施不同的是，“能力维”中的一般实施是根据成熟性进行排序的。因此，代表较高过程能力的一般实施会位于“能力维”的顶层。

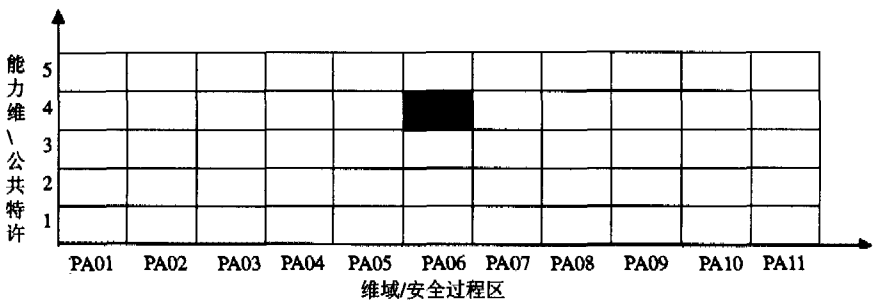

图 1　SSE-CMM 的二维结构

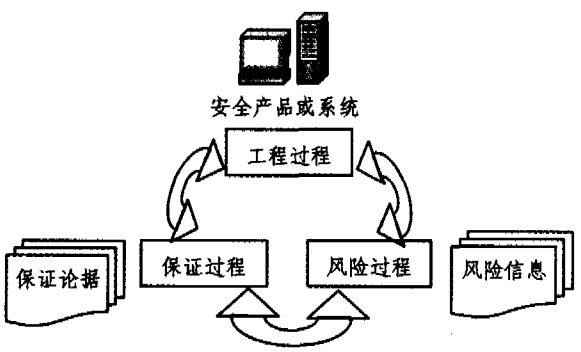

图 2　SSE-CMM 的安全工程过程

SSE-CMM 将系统安全工程过程化分为风险过程（Risk Process）、工程过程（Engineering Process）和保证过程（Assurance Process）3 个基本的过程。如图 2。它们相互独立，但又有着有机的联系。风险过程识别出所开发的产品或系统的危险，并对这些危险进行优先级排序。风险过程包括 4 个过程区：PA04、PA05、PA02 和 PA03。针对危险所面临的安全问题，工程过程要与其他工程一起来确定和实施解决方案。工程过程包括 5 个过程区：PA01、PA07、PA08、PA09 和 PA10。最后，由安全保证过程建立起解决方案的可信性并向用户转达这种安全可信度，保证过程包括两个过程区：PA06 和 PA11。

3　CC 和 SSE-CMM 的比较分析

CC 是国际标准，是面向最终产品的方法，即通过对所有文档和产品（包括中间产品，如源程序）的严格分析和测试来建立确信度指标。而 SSE-CMM 还没有正式成为国际标准，针对安全工程过程。下面对 CC 与 SSE-CMM 进行比较分析。

3.1 SSE-CMM 与 CC 针对的问题和具体目的不同

SSE-CMM 是目前针对信息系统安全问题而提供的具有

较高可靠性的解决方法。它主要用于对一个工程队伍的安全工程过程能力进行评定或自我改善，提高系统安全工程队伍自身的能力，从而最大限度地保证系统的相对安全性；也可用于对一个安全系统或安全产品的信任度测量和改善。改进安全工程实施的现状，达到提高安全系统、安全产品和安全工程服务的质量和可用性并降低成本的目的。

CC是目前针对信息技术产品和系统安全性的评估问题提供的国际性通用准则，是信息技术安全性评估结果国际互认的基础。CC提出了目前国际上公认的表述信息技术安全性的结构，分离了功能与保证，即把安全要求分为规范产品和系统安全行为的功能要求以及解决如何正确有效地实施这些功能的保证要求。

3.2 SSE-CMM和CC对用户的作用不同

SSE-CMM与CC主要适合于安全的工程组织、获取组织和评估组织。工程组织包括系统集成商、应用开发商、产品提供商和服务提供商等；获取组织包含采购系统、产品，以及从外部/内部资源和最终用户处获得服务的组织；评估组织包括认证组织、系统授权组织、系统和产品评估组织。表1列出了SSE-CMM与CC对不同用户的主要作用。

表1 SSE-CMM与CC对不同用户的作用

组织 / 标准	工程组织	获取组织	评估组织
SSE-CMM	·通过可重复和可预测的过程或实施来减少返工、提高质量和降低成本 ·获得真正的工程过程能力认可 ·可度量组织的资质 ·过程改进	·减少选择不合格投资者的风险 ·减少争议 ·在产品生产或提供服务的过程中，建立起可预测和可重复的可信度	·获得独立于系统或产品的可重用的过程评估结果 ·获得能力表现的可信度，减少评估工作量
CC	·支持和帮助开发高安全可信度的产品或系统，并在国际上的推广 ·确保安全产品或系统与安全需求的一致性 ·描述安全需求	·减少选择不合格安全产品或系统的风险 ·表达需求	·按照要求组织评估

3.3 SSE-CMM和CC在安全工程过程中的关注点不同

SSE-CMM和CC的一个共同核心思想是安全工程的思想，即通过对信息安全产品的开发、评价、使用全过程的各个环节实施安全工程来确保产品的安全性。

对于开发过程，CC虽然指出应从安全环境的分析开始，但CC更强调安全需求（包括功能要求和性能要求）描述和描述的一致性，并将其贯穿于安全工程过程的始终。而SSE-CMM将系统安全工程过程化分为风险过程、工程过程和保证过程3个基本的过程，强调安全适度原则。并指出对于开发过程，应从风险分析开始，分析威胁、脆弱性和影响，得出安全需求。因此，SSE-CMM强调安全需求分析，即怎么得到适度的安全需求，而CC更强调安全需求描叙和描述的一致性。

另外，对于工程过程，SSE-CMM规定了11个安全过程区，每一个过程区均有安全目标，并定义了必须执行的基本实施。而CC对工程过程并没有进行要求与定义。因此，CC关注的是最终目标以及为获得最终目标采取的保障措施，而SSE-CMM更关注工程过程。

3.4 SSE-CMM和CC的评估级别反映的实质不同

SSE-CMM和CC的评估结果均能反映安全产品或系统的确信度，但评估结果反映的实质不同。为了刻画产品的安全确信度的尺度，CC定义了一套评价保障等级EAL，保障级别越高，产品的安全确信度越高。而SSE-CMM为了刻画过程管理与制度能力的尺度，定义了5个能力级别，一般说来，能力级别越高，组织的安全工程过程越成熟，开发的安全产品或系统的安全确信度越高。因此，CC的评估结果反映的是为实现安全需求而采用的保障措施，而SSE-CMM反映的是组织的安全工程过程成熟度。

4 CC与SSE-CMM相结合开发高确信度系统的开发方法

CC标准和SSE-CMM框架中有关计算机安全产品评价的一个主导思想认为，计算机安全产品的安全确信度是通过人们在计算机安全信息系统或安全产品的开发、评价和使用过程中的行为来体现的。为了讨论CC标准和SSE-CMM框架下安全信息系统或安全产品的开发方法和安全确信度的建立问题，需要确定出在CC标准和SSE-CMM框架下开发一个安全信息系统或安全产品必须经历的开发过程的全貌，并在这个过程全貌的基础上，对整个过程的每一步工作中，CC和SSE-CMM在建立产品的安全确信度中所起的作用进行分析。

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：需求阶段、设计阶段、实现阶段、测试阶段、运行维护阶段。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。为了方便讨论CC与SSE-CMM相结合开发高确信度安全系统或产品，我们将安全产品的开发过程分成3个阶段：安全功能的确定阶段、安全功能的实现阶段和交货使用阶段。

4.1 安全功能的确定阶段

安全功能的确定阶段实际上就是安全需求阶段，下面我们结合CC与SSE-CMM，给出需求阶段应该经历的相关步骤。如图3。

·首先，根据CC的要求，明确安全系统或产品运行的安全环境。安全环境阐明安全系统或产品将用在什么样的环境中，并定义安全系统或产品拟处理的安全问题的性质和范围，这包括安全假设、风险等内容。

·然后，根据SSE-CMM的要求，对安全系统或产品在安全环境中的运行进行相关风险分析。风险就是有害事件发生的可能性及其危害后果。一个有害事件由威胁、脆弱性和影响3个部分组成，脆弱性包括可被威胁利用的资产性质。

（下转封四）

(上接第 251 页)

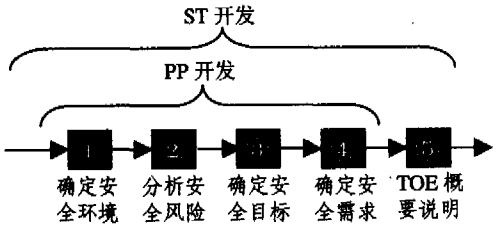

图 3 安全功能确定阶段 CC 与 SSE-CMM 的结合

• 第三,根据风险分析的结果,按照 SSE-CMM 的"安全适度原则",确定安全系统或产品应该达到的"安全目标",安全目标是对安全问题的响应或解决方案的简明陈述。

• 第四,根据安全目标确定安全需求。

• 最后,根据 CC 的要求,形成 TOE"概要说明",概要说明定义满足所有 SFR(Security Functional Requirement)要求的所有安全功能,包括这些安全功能的 PP 和 ST。

4.2 安全功能的实现阶段

安全功能的实现阶段一般包括概要设计阶段、详细设计阶段、实现阶段和测试阶段。下面我们讨论在安全功能的实现阶段,SSE-CMM 和 CC 的相关思想如何结合的问题。

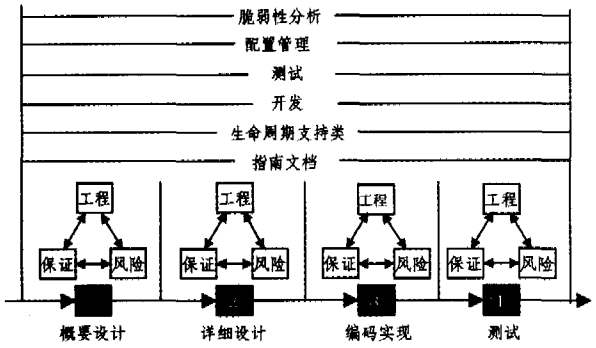

图 4 安全功能实现阶段 CC 与 SSE-CMM 的结合

从图 4 可以看出,在安全功能实现的每一个阶段,均要运用 SSE-CMM 的安全工程过程和 CC 标准的安全保障功能类。

应用 SSE-CMM 的安全工程过程有两层含义:其一是在各个阶段均要对安全产品或系统的风险进行分析和监控;第二,安全功能实现的每一个阶段要防止由于解决问题的需要引入的新的风险。另外,在整个安全功能实现的过程中,充分应用了 CC 的安全保障功能,包括:配置管理、指南文档、生命周期支持、测试、开发和脆弱性分析类。值得注意的是,SSE-CMM 的安全工程过程包括 PA06 和 PA11 两个保证过程区,保证过程区的基本实施与 CC 的安全保证功能有一定的联系。在 SSE-CMM 的 PA06 和 PA11 两个保证过程区中,基本实施只是定性地说明要做哪些保障工作,而 CC 则定义这些保障功能应该怎么描述和描述的一致性。因此,在安全产品或系统的开发过程中,将 SSE-CMM 与 CC 结合起来,可以完成具有高确信度的安全功能。

4.3 安全系统交货使用阶段

在安全产品或系统的交货使用阶段,需要开发方提供运行维护支持。在这个阶段,SSE-CMM 与 CC 也可以紧密结合。在交货运行阶段,SSE-CMM PA11 过程区的基本实施,定性描述了交货使用阶段的保障需求;而 CC 的"交货和使用"保障功能类,详细定义了交货使用阶段应该完成的保障功能。因此,在交货使用的过程中,将 SSE-CMM 与 CC 结合起来,可以完成具有高确信度的运行维护功能。

总结 由于 CC 与 SSE-CMM 具有互补性,我们在开发安全系统和产品的过程中,将 SSE-CMM 和 CC 紧密结合,已初见成效,它能指导我们开发出高确信度的产品、缩短评估周期、降低评估费用、节约企业成本。SSE-CMM 的能力级别与 CC 的保障级别还有什么更深层次的关系,原型采用什么样的开发方法既可以提高自己的 SSE-CMM 能力级别又可以提高产品或系统的保障级别,这是我们下一步的工作。

参 考 文 献

1 Pfleeger C P. Security in Computing [M]. Second Edition. Prentice Hall PTR,1997
2 Smith R E. Trends in Government Endorse Security Product Evaluations [C]. 23rd National Information Systems Security Conference, Baltimore, Maryland, USA,Oct16-19,2000
3 The National Information Assurance Partnership. Common Criteria NIAP Validated Products List [S]. http://niap. nist. gov/cc-scheme/ValidatedProducts. html, Mar2001
4 守鹏,吴希唐. 信息安全评估中的重要概念[J]. 计算机安全,2003,11:2~3
5 US DoD 5200. 28-STD, Trusted Computer Systems Evaluation Criteria [S]. 1985
6 Information Technology Security Evaluation Criteria. Version 1. 2 [S]. Office for Official Publications of the European Communities. 1991
7 SO/IEC 15408-1: 1999(E). The International Organization for Standardization and the International Electro technical Commission [S],1999
8 中国信息安全产品测评认证中心. GB-17859-1999 、GB-18336-2001 介绍[S]. http://www. itsec. gov. cn
9 SSE-CMM Model Description Document version2. 0 (EB/OL) [S]. 1999,http:\www. sse-cmm. org
10 SSE-CMM Appraisal Method version2. 0(EB/OL)[S], 1999,http:\www. sse-cmm. org
11 SSE-CMMAppraisalMethodversion2. 0(EB/OL)[S],1999,http:\www. sse-cmm. org

计算机科学

(1974 年 1 月创刊)
第 33 卷第 3 期 (月刊)
2006 年 3 月 25 日出版

国际标准连续出版物号 ISSN 1002-137X
国内统一连续出版物号 CN50-1075/TP

定价:30.00 元 国外定价:5 美元
邮发代号:78-68
发行范围:国内外公开

主管单位:国家科学技术部
主办单位:国家科技部西南信息中心
编辑出版:《计算机科学》杂志社
重庆市渝中区胜利路 132 号 邮政编码:400013
电话:(023) 63500828 E-mail:jsjkx@swic. ac. cn
网址:www. jsjkx. com
社 长:牟炳林
总 编:彭 丹
主 编:朱宗元
主编助理:徐书令
印 刷 者:重庆科情印务有限公司
总发行处:重庆市邮政局
订 购 处:全国各地邮政局
国外总发行:中国国际图书贸易总公司(北京 399 信箱)
国外代号:6210-MO