B2与信息安全评估*)

文立玉　陈雷霆
(电子科技大学计算机科学与工程学院　成都610054)

摘　要　本文介绍了信息系统安全评估的定义和标准,以及信息系统安全评估标准的历史,特别研究了TCSECT的CLASS B2,并比较了B2和CC的CLASS EAL5两者的特点。

关键词　信息安全,评估,可信计算机评价标准

B2 and Information System Security Evaluation

WEN Li-Yu　CHEN Lei-Ting
(School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610054)

Abstract　This paper introduces the definition of information system security evaluation, the criteria of information system security evaluation and the history of information system security evaluation criteria, especially researches the CLASS B2 of TCSEC, and compares the characters between B2 and CLASS EAL5 of CC.

Keywords　Information security, Evaluation, Trusted computer system evaluation criteria, TCB

1　信息安全评估

信息安全评估是对一个构件、产品、子系统或系统的安全属性进行的技术评价,通过评估判断该构件、产品、子系统或系统是否满足一组特定的要求。信息安全评估的另一层含义是在一定的安全策略、安全功能需求及目标保证级别下获得响应保证的过程。

2　信息安全评估标准及其发展

标准是技术性法规,作为一种依据和尺度。对于信息安全领域来说,标准是至关重要的。如果没有信息技术安全标准,与此相关的立法、执法就会因为缺乏相应的技术尺度而失之偏颇。信息安全产品的生产、销售、采购管理,对信息系统的安全管理等等,无不需要依据相应标准。

20世纪60年代后期,1967年美国国防部(DOD)成立了一个研究组,针对当时计算机使用环境中的安全策略进行研究,其研究结果是"Defense Science Board Report"。20世纪70年代的后期,DOD对当时流行的操作系统KSOS,PSOS,KVM进行了安全方面的研究。20世纪80年代中期,美国国防部发布了"可信计算机系统评估准则(TCSEC)"(即橘皮书),这是世界上第一个有关信息技术安全评估的标准。TCSEC是在20世纪70年代的基础理论研究成果Bell & La Padula模型基础上提出的,其初衷是针对操作系统的安全性进行评估,后来DOD又发布了可信数据库解释(TDI)、可信网络解释(TNI)等一系列相关的说明和指南,由于这些文档发行时封面均为不同的颜色,因此常被称为"彩虹系列"。TCSEC将信息安全等级分为A、B、C、D四类。其中D类是最低保护等级,即无保护级,是为那些经过评估,但不满足较高评估等级要求的系统设计的;D类只具有一个级别;D类系统最普通的形式是本地操作系统,或者是一个完全没有保护的网络。C类为自主保护级,具有一定的保护能力,采用的措施是自主访问控制和审计跟踪,一般只适用于具有一定等级的多用户环境,具有对主体责任及其动作审计的能力;C类分为C1(自主安全保护级)和C2(控制访问保护级)两个级别。B类为强制保护级,主要要求是TCB(Trusted Computing Base;可信计算基。计算机系统中的负责执行一个安全策略的包括硬件、软件、固体组合的保护技巧的全体)应维护完整的安全标记,并在此基础上执行一系列强制访问控制规则;B类系统中的主要数据结构必须挟带敏感标记,系统的开发者还应为TCB提供安全策略模型以及TCB规约,应提供证据证明访问监控器得到了正确的实施;B类分为B1(标记安全保护级)、B2(机构化保护级)和B3(安全区域保护级)三个类别。A类为验证保护级,A类的特点是使用形式化的安全验证方法,保证系统的自主和强制安全控制措施能够有效地保护系统中存储和处理的秘密信息或其它敏感信息,为证明TCB满足设计、开发及实现等各个方面的安全要求,系统应提供丰富的文档信息;A类分为A1(验证设计级)和A2(超A1级)两个类别。

近20年来,人们一直在努力发展安全标准,并将安全功能与安全保障分离,制定了复杂而详细的条款。但真正实用、在实践中相对易于掌握的还是TCSEC及其改进版本。在现实中,安全技术人员也一直将TCSEC的7级安全划分当做默认标准。

3　B2的内容与分析

3.1　B2的内容

B2系统必须满足:TCB通过隔离用户与数据,使用户具备更细粒度的自主访问控制能力,通过注册过程控制、审计安全相关事件以及资源隔离,使单个用户为其行为负责;提供安全策略模型的非形式化描述、数据标记以及命名主体和客体的强制访问控制,并消除测试中发现的所有缺陷;TCB建立于一个明确定义并文档化形式化安全策略模型的基础之上;在ADP(Automatic Data Processing,自动数据处理)系统中,

*)本文得到四川省科技攻关项目"信息标准技术研究和信息安全法律法规研究"(03FG013-008)支持。文立玉　硕士研究生,主要研究方向:网络安全。陈雷霆　博士,副教授,硕士生导师,主要研究方向:网络安全、网络多媒体。

要求对所有的主体与客体建立自主和强制访问控制;此外,应对隐蔽信道进行分析。在B2系统中,TCB必须结构化为关键保护元素和非关键保护元素。TCB接口必须明确定义,其设计与实现应能够经受更充分的测试和更完善的审查。鉴别机制应得到加强,提供可信设施管理以支持系统管理员和操作员的职能,并提供严格的配置管理控制。B2级系统应具备相当的抗渗透能力。对B2级系统的最低要求如下:

3.1.1 安全策略

(1)自主访问控制。在TCB应该定义和控制ADP系统中的命名用户和命名客体(如:文件和程序)。实施机制(比如,自己/组/公共控制,访问控制表)应该允许命名用户和(或)以用户组的身份规定并控制客体的共享;阻止非授权用户读取敏感信息,并控制访问权限扩散。

自主访问控制机制根据用户指定方式或默认方式,阻止非授权用户访问客体。访问控制的粒度是单个用户。没有存取权的用户只允许由授权用户指定对客体的访问权。

(2)客体重用。在计算机系统TCB的空闲存储客体空间中,对客体初始指定、分配或再分配一个主体之前,撤销该客体所含信息的所有权。当前主体不能获得包括加密信息在内的所有由原主体活动所产生的任何信息。

(3)标记。计算机信息系统TCB应维护每个与可被TCB外部的主体可访问的与ADP系统资源(比如,主体、存储对象、ROM)直接或间接相关的敏感性标记。这些标记是实施强制性访问控制的基础。为了输入未加安全标记的数据,计算机信息系统TCB将向授权用户要求和接收该数据的安全级别,而且这种行为可由TCB审计。

①标记完整性。敏感性标记应精确表述指定主体或与之相关的对象的安全级别。当敏感性标记被TCB所输出时,敏感性标记将精确地、毫无含糊地表述内部标记,而且将与输出的信息相关。

②标记信息的输出。TCB必须指定每个通信通道和I/O设备是单级还是多级。在这个指定中的任何修改都将是手工完成,而且将被TCB所审计。TCB将保留而且能够审计与通信通道或I/O设备相关的单个或多个安全级别。

·多级设备中标记信息的输出。当TCB向多级I/O设备输出了一个对象,与该对象相关的敏感性标记将也被输出而且将驻留在与输出信息同一个物理介质上,而且将保持同一种格式(比如,机器可读格式或人类可读格式)。当TCB在一个多级通信通道输出或输入某个对象时,该通道所使用的协议应提供在敏感性标记和将发出或接收的相关的信息之间毫无含糊的配对。

·单级设备中标记信息的输出。单级I/O设备和单级通信通道不要求保留它们处理的信息的敏感性标记。然而,TCB将包括一个机制,在该机制中TCB和某个已授权用户可靠地通过单级通信通道或单级I/O设备通信,来指定信息输入或输出的单安全级别。

·标记可读性输出。ADP系统管理员应具有指定与输出的敏感性标记相关的可打印标记名的能力。TCB将对所有可读的(人类可读格式)、已标注页数的硬拷贝输出(比如,行打印输出)的首部和尾部打上标记,使用人类可读的敏感性标记,该标记应该正确地表述该输出的敏感性。在默认情况下,TCB应该标记可读的(人类可读格式)、已标注页数的硬拷贝输出(比如,行打印输出)的每一页的顶部和底部,使用人类可读的敏感性标记,该标记应正确地描述该输出的整体敏感性或者正确地描述在该页上的信息的敏感性。TCB应该默认地而且在适当的方式下,标记人类可读输出的其他格式(比如,示意图、图表),使用人类可读的敏感性标记,该标记应该正确地表述该输出的敏感性。这些默认标记的任何替换值将被TCB审计。

·主体敏感性标记。在一次交互式对话中,TCB将立即注意到在与某个终端用户相关的安全级别中该用户的每次改变。一个终端用户应能够查询TCB,显示出该主体的全部敏感性标签。

·设备标记。TCB应支持对所有附属物理设备的最小和最大安全级别的分配。这些安全级别将被TCB用于实施被设备所定位的物理环境所强加的约束。

(4)强制访问控制。计算机信息系统TCB应对外部主体能够直接或间接访问的所有资源(比如,主体、存储对象和I/O设备)实施强制访问控制。应为这些主体及客体指定敏感性标记,这些标记是等级分类和非等级分类的组合,它们是实施强制访问控制的依据。计算机信息系统TCB应支持两种或两种以上的成分组成的安全级。TCB外部的所有主体对客体的直接或间接的访问应满足以下要求:1)仅当主体安全级中的等级分类高于或等于客体安全级中的等级分类,且主体安全级中的非等级类别包含了客体安全级中的全部非等级类别,主体才能读客体;2)仅当主体安全级中的等级分类低于或等于客体安全级中的等级分类,且主体安全级中的非等级类别包含于客体安全级中的全部非等级类别,主体才能读客体。计算机信息系统TCB使用身份和鉴别数据,鉴别用户的身份,保护用户创建的计算机信息系统TCB外部主体的安全级和授权受该用户的安全级和授权的控制。

3.1.2 责任(accountability——指可以追查对自动数据处理系统的侵害或试图侵害的责任者的性质或状态)

(1)身份鉴别。计算机信息系统TCB初始执行时,首先要求用户标识自己的身份。另外,计算机信息系统TCB应维护用户身份识别数据并确定用户访问权及授权数据。计算机信息系统TCB使用这些数据,鉴别用户身份,并使用保护机制(如口令)来鉴别用户的身份,并保证安全级别和TCB外部的主体的授权是由用户的访问权及授权数据来控制的,这些TCB外部的主体是被创建来代表单个用户的。TCB应阻止非授权用户访问用户身份鉴别数据。通过为用户提供唯一标识,计算机信息系统TCB能够使用户对自己的行为负责。计算机信息系统TCB还具备将身份识别与该用户所有可审计行为相关联的能力。

可信路径:对于用户的初始登录和鉴别,TCB支持在它自己与用户之间提供一个可信通信路径。该路径上的通信只能由该用户初始化。

(2)审计。计算机信息系统能创建、维护和保护受保护客体的访问审计跟踪记录,并能阻止非授权的用户对它访问或破坏。TCB应能记录以下类型的事件:1)使用身份鉴别机制;2)将客体引入用户地址空间(例如:打开文件、程序初始化);3)删除客体;4)由操作员、系统管理员或(和)系统安全管理员实施的动作,以及其他与系统安全有关的事件。

TCB应能审计可读输出标记的任何忽略。对于每一事件,其审计记录包括:事件的日期和时间、用户、事件类型、事件是否成功。对于身份鉴别事件,审计记录包含请求的来源(如终端标识符);对于客体引入用户地址空间的事件及客体删除事件,审计记录包含客体的名字及客体的安全级别。ADP系统管理员应能够选择性地审计在单个身份和/或客体安全级别的基础上的任何一个或多个用户的行为。TCB应能够审计利用隐蔽存储信道时可能被使用的事件。

3.1.3 保证

(1)操作保证

·系统结构。TCB能够为其自身的执行而维护某个范围来保护它不受外部干涉或篡改(比如,它的代码或数据结构的修改)。TCB将通过在其控制之下提供独立的地址空间来维护过程隔离。TCB被内部地构造为良好定义的大型独立模块。它将有效地使用可用的硬件来从非保护临界元素中分离出保护临界元素。TCB模块的设计原则为执行最少的特权。硬件中的特征,比如分段,应用于支持逻辑独立存储对象使用各自的属性(即可读、可写)。TCB的用户接口应完全定义,并且所有的TCB要素都被定义。

·系统完整性。应提供硬件和/或软件特征来周期性地验证站点上TCB的硬件和防火墙的正确操作。

·隐蔽信道分析。系统开发者应彻底搜索隐蔽信道,并根据实际测量或工程估算确定每一个被标识信道的最大带宽。

·可信设施管理。TCB应支持分离的操作员和管理员的功能。

(2)生命周期保障

·安全测试。应对ADP系统的安全机制进行测试,而且ADP系统的安全机制应能够按系统文档中所声明的一样工作。一个完全理解TCB的执行细节的团体在整个分析和测试应递交其的设计文档、源代码和客体代码。他们的目标应是:揭示允许TCB外部主体读、修改或删除数据的所有的设计和执行流程,这些数据通常在TCB所实施的强制性访问和自主性访问安全策略下是不允许外部主体访问的;同时保证没有任何主体(除了授权可以这样做)能够导致TCB进入它不能响应由其他用户发起的通信的状态。TCB应具有相对的抗渗透的能力。所有发现的错误都应纠正而且重新测试TCB以论证错误已经被消除而且还没有提出新的错误。测试应能证明TCB的执行与描述的最高级别规格说明书(DTLS——descriptive top-level specification)是一致的。

·设计说明书和检验。TCB所支持的所有正式的安全策略都应维护ADP系统的生命周期,这是与其原理相一致的。应对TCB的描述的最高级别规格说明书(DTLS)进行维护,它全面并精确地按例外、错误消息和作用的术语描述了TCB。它应该作为一个TCB接口的精确描述来展示。

·配置管理。在TCB的开发和维护期间,一个配置管理系统是很必要的,它用于维护控制:描述的最高级别规格说明书(DTLS)的变化,其他设计数据的变化,执行文档的变化,源代码的变化,客体代码的运行版本的变化,以及测试设备和文档的变化。配置管理系统应保证在所有的与当前版本的TCB相联系的所有文档和代码之间的一致映射。把新产生的版本与早先版本的TCB进行比较的工具也是可以获得的,进行这种比较是为了确定只有在代码中所做的有意的变化才会被实际地用作新版本的TCB。

3.1.4 文档

(1)安全特征用户指南

在用户文档中的单一的总结、章节、或指南应描述出TCB提供的保护机制,应描述出他们的使用准则和他们之间的如何相互影响。

(2)可信设施指南

提供给ADP系统管理员的指南应对功能和特权提出警示,这是在运行一个安全设施时应该控制的。在检查和维护的过程中,应当提供每种审计事件的审计文件以及审计记录结构。指南中应描述与安全相关的操作员和管理员的功能,应包含用户的安全特征的变化。它应提供在一致性和有效性方面的准则,它们是如何相互影响的,如何安全地生成一个新的TCB、设施使用流程、警告和特权,为了在安全的方式下操作设施,这些都是需要控制的。应该标识出包含参考验证机制的TCB模块。应该描述出在修改原有TCB的基础上安全地生成亲的TCB的过程。

(3)测试文档

系统开发者应向评估者提供一个文档,在该文档中描述测试计划、测试过程(说明是怎样测试安全机制的)和安全机制的功能性测试的结果。它还应包括对减少隐蔽信道带宽的方法的有效性的测试结果。

(4)设计文档

应提供一个文档,在该文档中提供描述生产商保护的基本原理,并解释该原理是怎样翻译到TCB中的;应该描述TCB模块之间的接口;应提供对TCB实施的安全策略模型的正式的描述,并证明TCB是完全能够实施该安全策略的;应标识出特定的TCB保护机制,并解释它们是怎样满足于该模型的;应提供描述的最高级别规格说明书(DTLS),将其作为对TCB接口的精确描述;文档中应描述TCB是如何实现访问监视器概念的,并解释为什么它是抗篡改的、不能被绕过的,而且是正确地实施的;文档应描述TCB是如何构造使其便于测试,使其实施最少的特权的;该文档中也应呈现隐蔽信道分析的结果和在限制该信道时所涉及的折衷办法;该文档中应该标识出可能在已知隐蔽存储信道中使用的所有可审计的事件;也应该提供已知节蔽存储信道的带宽,隐蔽存储信道的使用是不会被审计机制检测到的。

3.2 B2与CC的EAL5之比较分析

TCSEC的B2与CC的EAL5(Evaluation assurance level 5——半形式化设计和测试级)的安全要求属于同一级。

CC与TCSEC的不同在于其标准化的方法。在TCSEC中定义了一些特定的安全功能和安全测试,通过这些测试来证实某个等级如C2中预定义的安全功能被正确地实施。而CC中则提供了一个标准的、复杂的安全功能列表,以及可以用来验证其实施正确性的分析技术,CC还提供了一个执行测试的通用评估方法。另外,TCSEC将功能特性和保证组合起来,一定级别的保证与一定的功能特性集合捆绑在一起。而CC采用了独立的原则,它包含了许多不同的功能特性集合和不同的保证级别。CC的结构允许生产商根据其产品的用途来选择安全特性和保证级别,定义其威胁环境,并进行相应的评估。

CC中的EAL5,可使一个开发者从安全工程中获得最大限度的保证,这种安全工程所基于的严格的商业开发实践,是靠适度应用专业工程技术来支持的。EAL5适用于以下的情况:开发者和使用者在有计划的开发中需要一个高级别的独立保证的安全性,和在没有由专业安全工程技术引起不合理开销的条件下,需要一种严格的开发手段。

要达到EAL5应满足CC中的以下保证类:配置管理、交付和运行、开发、指导性文档、生命周期支持、测试以及脆弱性评定。

结束语 目前,国内外有很多从事信息安全的机构或公司采用TCSEC对IT产品进行评估,越来越多的IT产品希望能够通过TCSEC的B2一级的评估,本文对TCSEC的B2级标准进行了研究,为生产IT产品的企业或组织提供可操作的改进与实施方案,对于IT产品的信息安全评估具有一定的借鉴意义。

从EDOC模型到J2EE程序:一个MDA工具的实现*)

林 嵩 赵建华 李宣东 郑国梁
(南京大学软件新技术国家重点实验室 南京210093)
(南京大学计算机科学与技术系 南京210093)

摘 要 模型驱动体系结构MDA是OMG组织推出的一种新的软件开发方法。根据MDA的框架,设计者首先建立平台无关模型PIM,然后遵循一定的转换规则转化成平台相关模型PSM,最后转化成目标平台上的代码。为了体现MDA低成本、高效率的优点,模型之间、模型代码之间的自动转换就显得尤为重要。本文描述了我们实现的一个MDA转换工具。该工具可以编辑用EDOC的Entities profile和Business Process profile构建的PIM,并且辅助自动转化成基于J2EE平台的PSM,最终转化成J2EE代码。

关键词 模型驱动的软件体系结构,EDOC,J2EE,自动转换工具

From EDOC Model to J2EE Program: an Implementation of a MDA Tool

LIN Song ZHAO Jian-Hua LI Xuan-Dong ZHENG Guo-Liang
(State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093)
(Department of Computer Science and Technology, Nanjing University, Nanjing 210093)

Abstract Model Driven Architecture (MDA) is a new software development paradigm recently released by Object Management Group (OMG). According to MDA, the designer first builds a Platform Independent Model (PIM) of the system under construction, then transforms this model into a Platform Specific Model (PSM) according to some transforms rules, and/or generates code on the target platform. To increase the productivity and reduce the cost of MDA development, we should develop automatic tools for model transformation and code generation. A MDA transform tool is presented in this article. This tool can edit PIMs according to EDOC Entities profile and Business Process profile, and automatically transform the PIM to a PSM on J2EE. This tool can also directly generate J2EE code based on the PIM.

Keywords Model driven architecture, EDOC, J2EE, Automatic transform tool

1 引言

1.1 MDA的简单介绍

MDA(Model Driven Architecture)是OMG(对象管理组织)推出的一种新的软件开发方法。MDA的主要特点是将业务逻辑和应用逻辑与技术实现相分离,在体系结构上分离关注的焦点,从而提高软件产品的移植性、互操作性和重用性。在使用这个方法开发软件系统的时候,设计者首先建立一个基于UML(Unified Modeling Language,统一建模语言)的平台无关模型(PIM,Platform Independent Model)。PIM提供了关于系统的结构和功能的形式化规约。这个规约是独立于具体的实现平台的,并不涉及具体的实现细节。这里的平台可以指各种层次的平台,包括程序语言、操作系统、网络平台以及中间件平台,当然主要是征对中间件平台。软件系统最终需要在某个特定的平台上实现,与平台相关的实现细节必然要被加入到软件产品中去。在建立起系统的PIM之后,设计者可以遵循一定的转换规则将PIM转化成对应的、同样基于UML的平台相关模型(PSM,Platform Specific Model)。PSM

*)本文的研究工作得到国家863科技项目(2002AA116090),国家自然基金(6027036),江苏省自然基金(BK2002079)资助。林 嵩 硕士研究生,主要研究领域为软件工程。赵建华 副教授,主要研究领域为软件工程、形式化方法、模型检验。李宣东 教授,博士生导师,研究领域为形式化方法、模型检验。郑国梁 教授,博士生导师,研究领域为软件工程、软件开发环境。

参考文献

1 National Computer Security Center. Department of Defense Trusted Computer System Evaluation Criteria. DoD 5200. 28-STD, 1995. 12
2 The International Organization for Standardization. Information Technology Security Technology Evaluation Criteria for IT Security. ISO/IEC 15408-1,2,3,1999. 9
3 Common Criteria for Information Technology Security Evaluation. August 1999, Version 2. 1, CCIMB-99-031
4 中华人民共和国国家标准. 信息技术 安全技术 信息技术安全性评估准则. GB/T 18336. 2-2001
5 中华人民共和国国家标准. 计算机信息系统安全保护等级划分准则. GB 17859-1999
6 郭振民,胡学龙,姜会亮. 网络与信息系统安全性评估及其指标体系的研究. 现代电子技术,2003(9)
7 王志兰,赵怀勋,刘菲. 网络信息安全技术的研究. 现代电子技术,2003(8)