信息安全评估研究

陈雷霆[1]，文立玉[1]，李志刚[2]

(1. 电子科技大学计算机科学与工程学院 成都 610054; 2. 河北省教育考试院 石家庄 050091)

【摘要】介绍了信息安全评估的定义、标准及其发展，重点讨论了可信计算机系统评估准则中机构化保护级评估标准安全策略中的自主访问控制、客体重用、标记(标记完整性和标记信息的输出)和强制访问控制；责任中的身份鉴别和审计；保证中的操作保证(系统结构、系统完整性、隐蔽信道分析和可信设施管理)和生命周期保障(安全测试、设计说明书和检验以及配置管理)；文档中的安全特征用户指南、可信设施指南、测试文档和设计文档。最后，将机构化保护级与信息技术安全评估通用准则中的测试级5进行了比较分析。

关 键 词 信息安全; 评估; 可信计算机系统评估准则; 可信计算基

中图分类号 TP393 文献标识码 A

Research of Information System Security Evaluation

CHEN Lei-ting[1]，WEN Li-yu[1]，LI Zhi-gang[2]

(1. School of Computer Science and Engineering，UEST of China Chengdu 610054;

2. Hebei Education and Examination Institution Shijiazhuang 050091)

Abstract This paper introduces the definition, standard and development on evaluation of information security; emphasis on Class of B2 in TCSEC, especially the security policy of B2, such as discretionary access control, object reuse, Labels (label integrity and exportation of labeled information) and mandatory access control. this paper also studies and analyses the other requirements for class B2, such as identification and authentication in the requirement of accountability; operational assurance (system architecture, system integrity, covert channel analysis and trusted facility management) and life-cycle assurance (security testing, design specification and verification and configuration management) in the requirement of assurance; security features user's guide, trusted facility manual, test documentation and design documentation in the requirement of documentation. in the end of this paper, we study and comparatively analyses the class of B2 with the class of EAL5 in CC.

Key words information security; evaluation; trusted computer system evaluation criterial; trusted calculate base

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[1]。

收稿日期：2004 – 05 – 13

基金项目：四川省科技攻关项目(03FG013-008)

作者简介：陈雷霆(1966 –)，在职博士，副教授，硕士生导师，主要从事网络安全、网络多媒体方面的研究；文立玉(1979 –)，女，硕士生，主要从事网络安全方面的研究.

2 信息安全评估标准及其发展

20世纪80年代中期，美国国防部(Department of Defence, DOD)发布了《可信计算机系统评估准则(Trusted Computer system Evaluation Criteria, TCSEC)》橘皮书，这是世界上第一个有关信息技术安全评估的标准[2]。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，后来美国国防部DOD又发布了可信数据库解释(Trusted Data-Base Interpret, TDI)、可信网络解释(Trusted Network Interpret, 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[3, 4]。其中D类是最低保护等级。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，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，主要要求是可信计算基(Trusted Calculate Base, TCB)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；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；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

3.1.1 B2级的安全策略

1) 自主访问控制

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自动数据处理(Automation Data Processing, ADP)系统资源(比如主体、存储对象、只读存储器)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，而且所有这些行为可由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、毫不含糊地表述内部标记，而且与被输出的信息相关。

(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的，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，如多级设备中标记信息的输出、单级设备中标记信息的输出、标记可读输出、主体敏感性标记、设备标记。

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。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；

3.1.2　B2级的责任

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，使用保护机制来鉴别用户的身份，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。

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，即使用身份鉴别机制；将客体引入用户地址空间；删除客体；由操作员、系统管理员或(和)系统安全管理员实施的动作等事件，以及其他与系统安全有关的事件。

TCB应能审计对可读输出标记的任何忽略。ADP系统管理员应能选择性地审计在单个身份和/或客体安全级别基础上的任何一个或多个用户的行为。TCB应能审计利用隐蔽存储信道时可能被使用的事件。

3.1.3　B2级的保证

1) 操作保证

(1) 系统结构。TCB能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。TCB将通过在其控制之下提供的独立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，应用于支持逻辑独立存储对象使用各自的属性。TCB的用户接口应完全定义，并且所有的TCB要素都被定义。

(2) 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。

(3) 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被标识信道的最大带宽。

(4) 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

(1) 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按系统文档中所声明的一样工作。其目标应是揭示允许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，保证没有任何主体能够导致TCB进入它不能响应由其他用户发起的通信状态。

(2) 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(Descriptive Top-Level Specification, 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TCB，应该作为一个TCB接口的精确描述来展示。

(3) 配置管理。在TCB的开发和维护期间，配置管理系统用于维护控制所描述的DTLS的变化、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。

3.1.4　B2级的文档

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，并应描述出它们的使用准则和它们之间如何相互影响。

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。在检查和维护过程中，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，包含用户的安全特

征的变化；应提供在一致性和有效性方面的准则，即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；应标识出包含参考验证机制的TCB模块；应描述出在修改原有TCB的基础上安全地生成新的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、测试过程和安全机制的功能性测试结果。此外，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

在设计文档中应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DTLS，将其作为对TCB接口的精确描述；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；应描述TCB是如何构造使其便于测试的；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；应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；应提供已知隐蔽存储信道的带宽，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信息技术安全评估通用准则(Common Criteria, CC)的半形式化设计和测试级(Evalua-tion Assurance level, EAL) 5的安全要求属于同一级[5]。

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。而在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[6]。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功能的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[7]。EAL5适用于开发者和使用者在有计划的开发中需要高级别的独立保证安全性和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。

4 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。

参 考 文 献

[1] GB/T 18336.2-2001. 信息技术 安全技术 信息技术安全性评估准则[S]. 2001

[2] 王志兰, 赵怀勋, 刘 菲. 网络信息安全技术的研究[J]. 现代电子技术, 2003, 151(8): 39-41

[3] DoD 5200.28-STD. Department of defense trusted computer system evaluation criteria[S]. 1995

[4] GB/T 17859-1999, 计算机信息系统安全保护等级划分准则[S]. 1999

[5] 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[J]. 现代电子技术, 2003, 152(9): 9-11

[6] CCIMB-99-031. Common criteria for information technology security evaluation(Version 2.1)[S]. 1999

[7] ISO/IEC 15408-1,2,3. Information technology security technology evaluation criteria for IT security[S]. 1999

编 辑 熊思亮