ICS 35.100.01
L 79

中华人民共和国国家标准

GB/T 18794.6—2003/ISO/IEC 10181-6:1996

信息技术　开放系统互连 开放系统安全框架 第6部分:完整性框架

Information technology—Open Systems Interconnection—Security frameworks for open systems—Part 6:Integrity framework

(ISO/IEC 10181-6:1996,Information technology—Open Systems Interconnection—Security frameworks for open systems: Integrity framework,IDT)

2003-11-24 发布　　2004-08-01 实施

中华人民共和国
国家质量监督检验检疫总局　发布

目　　次

前　言

GB/T 18794《信息技术　开放系统互连　开放系统安全框架》目前包括以下几个部分：

——第 1 部分(即 GB/T 18794.1)：概述

——第 2 部分(即 GB/T 18794.2)：鉴别框架

——第 3 部分(即 GB/T 18794.3)：访问控制框架

——第 4 部分(即 GB/T 18794.4)：抗抵赖框架

——第 5 部分(即 GB/T 18794.5)：机密性框架

——第 6 部分(即 GB/T 18794.6)：完整性框架

——第 7 部分(即 GB/T 18794.7)：安全审计和报警框架

本部分为 GB/T 18794 的第 6 部分，等同采用国际标准 ISO/IEC 10181-6:1996《信息技术　开放系统互连　开放系统安全框架：完整性框架》(英文版)。

按照 GB/T 1.1—2000 的规定，对 ISO/IEC 10181-6 作了下列编辑性修改：

a) 增加了我国的“前言”；

b) “本标准”一词改为“GB/T 18794 的本部分”或“本部分”；

c) 对“规范性引用文件”一章的导语按 GB/T 1.1—2000 的要求进行了修改；

d) 删除“规范性引用文件”一章中未被本部分引用的标准；

e) 在引用的标准中，凡已制定了我国标准的各项标准，均用我国的相应标准编号代替。对“规范性引用文件”一章中的标准，按照 GB/T 1.1—2000 的规定重新进行了排序。

本部分的附录 A 至附录 C 都是资料性附录。

本部分由中华人民共和国信息产业部提出。

本部分由中国电子技术标准化研究所归口。

本部分起草单位：四川大学信息安全研究所。

本部分主要起草人：罗万伯、罗建中、赵泽良、戴宗坤、崔玉华、陈一民、祝世雄。

引　言

许多开放系统应用都有依赖于数据完整性的安全需求。这样的需求可包括数据的保护，这些数据在提供其他安全服务如鉴别、访问控制、机密性、审计及抗抵赖时使用，如果攻击者能修改这些数据，则能使这些服务的效力降低或无效。

数据没有以未授权的方式修改或破坏的这一属性称为完整性。本部分定义一个提供完整性服务的通用性框架。

信息技术　开放系统互连
开放系统安全框架
第6部分:完整性框架

1　范围

本开放系统安全框架的标准论述在开放系统环境中安全服务的应用,此处术语"开放系统"包括诸如数据库、分布式应用、开放分布式处理和开放系统互连这样一些领域。安全框架涉及定义对系统和系统内的对象提供保护的方法,以及系统间的交互。本安全框架不涉及构建系统或机制的方法学。

安全框架论述数据元素和操作的序列(而不是协议元素),这两者可被用来获得特定的安全服务。这些安全服务可应用于系统正在通信的实体,系统间交换的数据,以及系统管理的数据。

本部分阐述了信息检索、传送及管理中数据的完整性:

1)　定义数据完整性的基本概念;

2)　识别可能的完整性机制分类;

3)　识别每一类完整性机制的设施;

4)　识别支持完整性机制分类所需的管理;

5)　阐述完整性机制和支持服务与其他安全服务和机制的交互。

有许多不同类型的标准可使用本框架,包括:

1)　体现完整性概念的标准;

2)　规定含有完整性的抽象服务的标准;

3)　规定使用完整性服务的标准;

4)　规定在开放系统体系结构内提供完整性服务方法的标准;

5)　规定完整性机制的标准。

这些标准可按下述方式使用本框架:

——标准类型1),2),3),4)及5)能使用本框架的术语;

——标准类型2),3),4)及5)能使用第7章所识别的设施;

——标准类型5)能基于本框架第8章定义的机制类别。

本安全框架中描述的一些规程通过应用密码技术获得完整性。这个框架并不依赖于使用特定的密码算法或其他算法,虽然某些类别的完整性机制可能依赖特定算法的特性。

注:密码算法及其登记规程应符合我国有关规定。

本部分论述的完整性是通过数据值的不变性来定义的。(数据值不变性)这一概念包含所有的实例,在这些实例中一个数值的不同表示被认为是等价的(例如同一值的不同的ANS.1编码)。在此排除其他形式的不变性。

本部分中术语数据的使用包括数据结构的一切类型(诸如数据集合或汇集、数据序列、文件系统和数据库)。

本框架阐述给那些被认为可被潜在攻击者写访问的数据提供完整性。因此,它着重于通过密码和非密码的机制提供完整性,并非专门依赖于控制访问。

2　规范性引用文件

下述文件中的条款通过GB/T 18794的本部分的引用而成为本部分的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修改版均不适用于本部分,然而,鼓励根据本部分达成