

ICS 35.020
L 09

GA

中华人民共和国公共安全行业标准

GA/T 708—2007

GA/T 708—2007

信息安全技术 信息系统安全等级保护体系框架

Information security technology—
Architecture framework of security classification
protection for information system

中华人民共和国公共安全
行业标准
信息安全技术
信息系统安全等级保护体系框架
GA/T 708—2007

*

中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045

网址 www.spc.net.cn

电话:68523946 68517548

中国标准出版社秦皇岛印刷厂印刷

各地新华书店经销

*

开本 880×1230 1/16 印张 2.5 字数 68 千字

2007年12月第一版 2007年12月第一次印刷

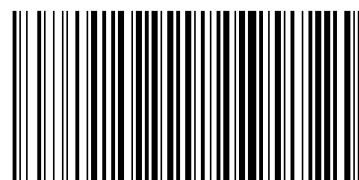
*

书号:155066·2-18278 定价 28.00 元

如有印装差错 由本社发行中心调换

版权专有 侵权必究

举报电话:(010)68533533



GA/T 708—2007

2007-08-13 发布

2007-10-01 实施

中华人民共和国公安部 发布

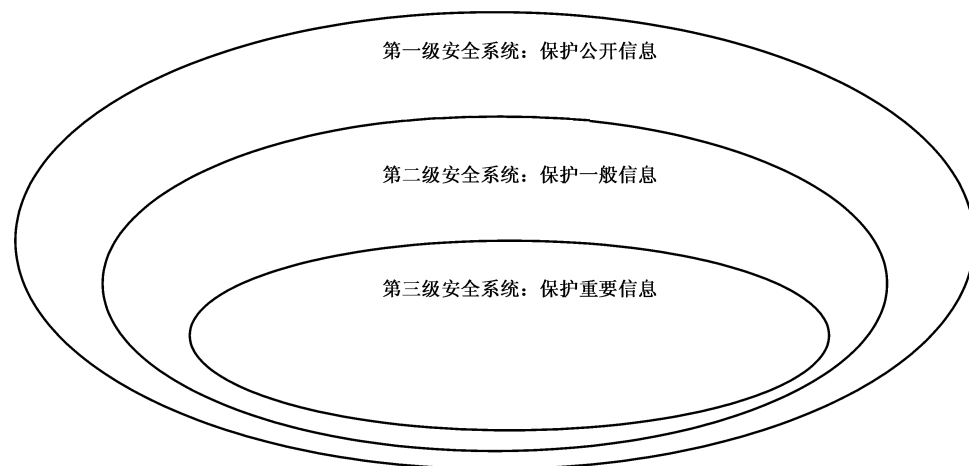


图 B.1 分层虚拟安全系统基本思想示意图

其中,对每类数据信息的保护,需要建立一个相应安全保护等级的虚拟安全系统。

这种对不同类型数据实施不同安全保护的虚拟分层思想,在实际的应用中也是常见的。比如,在一个信息系统中,对某些数据的传输进行加密保护,而对另一些数据的传输则不进行加密保护。又如,可以定义对某类数据实施自主访问控制和强制访问控制,而对另一类数据只实施自主访问控制等等。

目 次

| | |
|-----------------------------|-----|
| 前言 | III |
| 引言 | IV |
| 1 范围 | 1 |
| 2 规范性引用文件 | 1 |
| 3 术语和定义 | 1 |
| 4 信息系统安全等级保护体系简介 | 2 |
| 4.1 信息系统安全等级保护体系的组成 | 2 |
| 4.2 信息系统安全等级保护体系概要说明 | 2 |
| 5 信息系统安全等级保护法律法规和政策依据 | 3 |
| 5.1 法律法规和政策分类 | 3 |
| 5.2 信息系统安全等级保护的现有政策法规 | 3 |
| 6 信息系统安全等级保护标准体系 | 3 |
| 6.1 标准的分类 | 3 |
| 6.2 标准的具体组成 | 4 |
| 6.2.1 基础性标准 | 4 |
| 6.2.2 系统设计指导类标准 | 4 |
| 6.2.3 系统实施指导类标准 | 4 |
| 6.2.4 要求类标准 | 4 |
| 6.2.5 检查/测评类标准 | 5 |
| 6.2.6 各应用领域实施指导方案 | 6 |
| 6.3 标准所涉及的内容 | 6 |
| 6.4 各类标准的作用及编写要求 | 7 |
| 6.4.1 基础性标准 | 7 |
| 6.4.2 系统设计指导类标准 | 7 |
| 6.4.3 要求类标准 | 8 |
| 6.4.4 检查/测评类标准 | 9 |
| 6.4.5 实施指导类标准 | 11 |
| 6.4.6 各应用领域实施指导方案 | 11 |
| 7 信息系统安全等级保护管理体系 | 11 |
| 7.1 信息系统安全工程管理 | 11 |
| 7.1.1 目标 | 11 |
| 7.1.2 内容 | 11 |
| 7.1.3 工程管理分等级要求 | 12 |
| 7.2 安全系统运行管理 | 13 |
| 7.2.1 目标 | 13 |
| 7.2.2 内容 | 13 |
| 7.2.3 运行管理分等级要求 | 15 |
| 7.3 信息系统安全监督检查和管理 | 16 |

| | |
|--------------------------|----|
| 8 信息系统安全等级保护技术体系 | 16 |
| 8.1 信息系统安全的基本属性 | 16 |
| 8.2 信息系统安全的组成与相互关系 | 16 |
| 8.3 信息系统的安全等级 | 17 |
| 8.3.1 五个安全等级 | 17 |
| 8.3.2 安全保护等级的确定 | 20 |
| 8.4 信息系统安全等级保护基本框架 | 21 |
| 8.4.1 信息系统安全保护总体框架 | 21 |
| 8.4.2 信息系统安全等级保护的基本原理和方法 | 22 |
| 8.5 信息系统安全等级保护基本技术 | 24 |
| 8.5.1 标识与鉴别技术 | 24 |
| 8.5.2 访问控制技术 | 24 |
| 8.5.3 存储和传输数据的完整性保护技术 | 25 |
| 8.5.4 存储和传输数据的保密性保护技术 | 25 |
| 8.5.5 边界隔离与防护技术 | 25 |
| 8.5.6 系统安全运行及可用性保护技术 | 25 |
| 8.5.7 密码技术 | 26 |
| 8.6 信息系统安全等级保护支撑平台 | 26 |
| 8.6.1 信息系统密码基础设施平台 | 26 |
| 8.6.2 信息系统应用安全支撑平台设计 | 26 |
| 8.6.3 信息系统灾难备份与恢复平台 | 27 |
| 8.6.4 信息系统安全事件应急响应与管理平台 | 27 |
| 8.6.5 信息系统安全管理平台 | 28 |
| 8.7 等级化安全信息系统构建技术 | 29 |
| 附录 A (资料性附录) 基本概念说明 | 30 |
| A.1 业务应用软件系统及其子系统 | 30 |
| A.2 信息系统及其子系统 | 30 |
| A.3 关于安全域 | 30 |
| 附录 B (资料性附录) 实施等级保护的方法 | 31 |
| B.1 全系统同一安全等级安全保护 | 31 |
| B.2 分系统不同安全等级安全保护 | 31 |
| B.3 虚拟系统不同安全等级安全保护 | 31 |
| 参考文献 | 33 |

附 录 B

(资料性附录)

实施等级保护的方法

B.1 全系统同一安全等级安全保护

所谓全系统同一安全等级安全保护是指,对于一个需要进行安全等级保护的信息系统,其所存储、传输和处理的所有数据信息,在组成系统的任何部分,都需要进行相同安全保护等级的安全保护。

当所要保护的数据信息无论处于系统中的任何位置,进行任何形式的处理,都需要实施相同安全保护等级的保护时,需要按照全系统同一安全等级安全保护的方法进行系统的安全性设计,提供所要求的安全保护。

需要特别指出的是,这里所说的相同安全保护等级的安全保护是指按照 GB 17859—1999 规定的的安全保护等级某一等级的要求,进行全系统的安全设计,而并非按照多级安全模型实现的强制访问控制中主、客体标记所设置的级别和范畴中的级别。因为在后者中可能出现这样的情况:实施强制访问控制的客体,当其位于信息系统的不同部位时,其作为强制访问控制基础的级别,根据需求可能会有所不同。这就如同我们在对保密文件的管理中常常规定,当文件带出单位或带到异地时需要升高文件的保密等级一样。

B.2 分系统不同安全等级安全保护

所谓分系统不同安全等级安全保护是指,对于一个需要进行安全等级保护的信息系统,其所存储、传输和处理的数据信息,可按照信息在组成信息系统的各个子系统不同保护要求,实施不同安全保护等级的安全保护。

当处于信息系统不同子系统中的数据信息,需要实施不同安全等级的安全保护时,需要按照子系统不同安全等级安全保护的方法进行系统的安全性设计。

这种安全设计既可按数据服务器为单元实施安全保护,也可按网络或子网为单元实施安全保护。在有多个数据服务器的系统中,不同的数据服务器可根据其所存储和处理的数据信息的类型,提供不同的安全保护等级的安全保护。在一个具有各类数据信息的信息系统中,把数据分类存放在不同的数据服务器/网络存储器中,就可以按这种方法设计安全保护。

按网络或子网实施安全保护,通常是网络或子网具有较高安全保护等级的安全保护。这时,需要在网络或子网的前端设置边界防护,防止数据随意在内、外部之间流动。根据需要,边界防护既可对进入网络或子网的用户进行更严格的检查和认证,又可对进/出的数据信息按规定进行控制。

B.3 虚拟系统不同安全等级安全保护

在一个信息系统中,不同类型的数据往往有不同的安全保护要求。对不同类型的数据信息的安全保护,可以通过建立一个相应安全保护等级的分层虚拟安全系统来实现。

按照虚拟系统的概念,建立分层的虚拟安全系统,可实现不同类型信息的安全保护等级的安全保护。图 B.1 为具有三级安全的分层虚拟安全系统的示意图。