<<信息系统等级保护安全设计技术实>>

图书基本信息

书名：<<信息系统等级保护安全设计技术实现与使用>>

13位ISBN编号：9787302217954

10位ISBN编号：7302217955

出版时间：2010-6

出版时间：范红、胡志昂、 金丽娜 清华大学出版社 (2010-06出版)

作者：范红，胡志昂，金丽娜 著

页数：210

前言

信息安全等级保护是我国实现国家信息安全的基本制度，1994年国务院147号令中就已规定信息系统安全实行等级保护制度，并明确指出由公安部会同有关部门制定等级保护管理办法和标准；1999年国家发布了等级保护强制性国家标准GB 17859-1999t（计算机信息系统安全保护等级划分准则》（以下简称GB 17859-1999），此后，50多个配套标准相继发布，并已形成标准体系。
这些标准的制定，为信息安全等级保护制度的实施打下了坚实的技术基础。
2003年27号文件则进一步明确规定国家实施信息安全等级保护制度，此后公安部等四部委联合相继发布了66号和43号文件，规定了等级保护系列政策和管理办法。
2007年7月，公安部、国务院信息办等四部门联合召开全国重要信息系统等级保护定级工作会议，标志着等级保护制度在全国范围内全面展开，目前全国重要信息系统定级工作已基本完成。
下一阶段的工作将对已确定安全等级的信息系统依据相关标准要求进行安全建设。
此工作将涉及大量的关键技术实现难题。
因此，深入开展信息系统等级保护安全体系结构及关键技术的研究，进行理论攻关、工程实践与标准制定，是即将开展的信息系统等级保护安全建设整改工作的迫切现实需要，也是国家信息安全等级保护制度长期实施所不可缺少的技术支持。
本书中所介绍的信息系统等级保护安全体系结构、关键技术、等级保护模拟平台、信息系统等级保护安全建设方案以及应用案例对提高我国重要信息系统和关键基础设施的安全性有重要作用，将为各行业信息系统等级保护的安全建设提供示范与参考，也将为普遍开展的信息系统等级保护安全建设提供指导。

内容概要

《信息系统等级保护安全设计技术实现与使用》对国家标准《信息安全技术——信息系统等级保护安全设计技术要求》进行详细、深入的解读，并在此基础上给出二、三、四级系统的安全设计和实现，包括各级系统的安全功能和总体结构、实现方案和设备类型、安全计算环境子系统设计和实现、安全区域边界子系统设计和实现、安全通信网络子系统设计和实现、安全管理子系统设计和实现、审计子系统设计和实现以及典型应用子系统设计和实现，并详细介绍了各级信息系统示范环境的功能使用。
书中配有各个示范环境具体操作界面的图片，使读者对示范环境有更形象生动的了解。
《信息系统等级保护安全设计技术实现与使用》还介绍了二、三、四级安全应用平台功能符合性检验工具集使用和信息安全风险评估工具使用，主要包括：各检验工具集和风险评估工具的体系结构、功能结构、设计与实现以及使用操作演示。

<<信息系统等级保护安全设计技术实>>

书籍目录

章节摘录

插图：安全区域边界是专为在安全计算环境的边界进行安全保护而设置的。
第二级安全区域边界是按照确定的第二级信息系统安全保护环境的安全设计目标和安全设计策略对区域边界的安全要求，采用具有相应安全保护能力的安全技术和安全产品构成的区域边界。
安全管理中心是专对信息系统安全保护环境进行集中管理设置的。
第二级信息系统安全保护环境的安全管理中心，统一管理和控制系统中的安全审计机制，汇集、存储并分析来自各安全机制和产品的审计信息。
安全计算环境、安全区域边界和安全通信网络三者中的安全机制，以及安全管理中心协同运行，共同实现第二级信息系统的安全保护目标。
第二级信息系统安全保护环境的安全设计应特别注重对系统安全审计的设计。
安全审计机制贯穿于整个安全系统的设计之中，使之成为一个整体。
安全审计虽然不是一种对攻击和破坏直接进行对抗的安全技术，但是完备的安全审计系统和完整的具有良好可用性的审计日志，能够有效地提供安全事件的可查性。
安全审计与严格的身份鉴别相结合，可将安全事件落实到具体的用户，从而具有很强的威慑作用。
第二级信息系统安全保护环境的安全设计，应注意在安全计算环境、安全区域边界和安全通信网络中，将安全审计和恶意代码防范等安全机制的设置统一进行考虑，使之成为一个实现全系统安全保护的整体。

编辑推荐

《信息系统等级保护安全设计技术实现与使用》：国家863高技术研究发展计划资助项目(2009AA012437)国家863高技术研究发展计划资助项目(2009AA012439)《信息系统等级保护安全设计技术实现与使用》主要面向信息安全等级保护主管部门的管理人员和专业人士、高等院校计算机、通信、信息安全等专业的教学、科研和工程技术人员，以及党政部门、企事业单位，科研机构等急需进行等级保护安全建设工作的相关人士。

版权说明