Linux安全访问控制模型应用及方案设计 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/260/2021_2022_Linux_E5_AE_89_E5_85_c103_260891.htm 摘要：本文介绍了BLP、DTE和RBAC三种访问控制模型，并结合这三种安全策略模型，提出了一个安全系统的组成和功能的具体实现方案。 关键字：信息安全；访问控制模型；操作系统安全。 1.引言 本文通过研究安全操作系统的访问控制模型，结合国内、外的相关安全标准和已有的先进技术，将密码服务与高级别存取控制机制有机地结合起来，形成一个适应各类安全2级实用操作系统。该安全服务器将在Linux操作系统的基础上（目前Linux操作系统主要发行版本的安全性大致处于《TCSEC》标准[1，2]的C2 级），参照GB/T 18336（等同采用CC标准）安全保证级别EAL4，开发符合GB 17859中规定的结构化保护级（相当于TCSEC中规定的B2级）功能要求的安全操作系统。 1. 安全策略访问控制模型 该类模型是从访问控制的角度描述安全系统，主要针对系统中主体对客体的访问及其安全控制。[2] 1.1 BLP模型 Bellshy.shy.是由shy.shy.Bell和Lapadula于1973年提出并于1976年修定、整合和完善的安全模型，它是最典型的信息保密性多级安全模型，通常是处理多级安全信息系统的设计基础。 BLP模型的安全策略包括强制访问控制和自主访问控制两部分。强制访问控制中的安全特性,要求对给定安全级别的主体，仅被允许对同一安全级别和较低安全级别上的客体进行“ 读 ”，对给定安全级别上的主体，仅被允许向相同安全级别或较高安全级别上的客体进行“ 写 ”，任意访问控制允许用户自行定义是否让个人或组织存取数据。 BLP模型为

通用的计算机系统定义了安全性属性,即以一组规则表示什么是一个安全的系统。其优点是这种基于规则的模型比较容易实现。但是它不能更一般地以语义的形式阐明安全性的含义。因此，这种模型不能解释主、客体框架以外的安全性问题，还不能较好的处理隐蔽通道的问题。 1.2 DTE模型 DTE（Domain and Type Enforcement）模型[5]是由O’Brien and Rogers于1991年提出的一种访问控制技术。它通过赋予文件不同的型（type）、赋予进程不同的域（domain）来进行访问控制，从一个域访问其他的域以及从一个域访问不同的型都要通过DTE策略的控制。 近年来DTE模型被较多的作为实现信息完整性保护的模型。该模型定义了多个域（Domain）和型（Type），并将系统中的主体分配到不同的域中，不同的客体分配到不同的型中，通过定义不同的域对不同的型的访问权限，以及主体在不同的域中进行转换的规则来达到保护信息完整性的目的。 DTE使域和每一个正在运行的进程相关联，型和每一个对象（e.g.文件、包）相关联。如果一个域不能以某种访问模式访问某个型，则这个域的进程不能以该种访问模式去访问那个型的对象。当一个进程试图访问一个文件时，DTE 系统的内核在做标准的系统许可检查之前，先做DTE许可检查。如果当前域拥有被访问文件所属的型所要求的访问权，那么这个访问得以批准，继续执行正常的系统检查。 1.3 RBAC模型 RBAC模型[5]是基于角色的访问控制模型。该模型主要用于管理特权，在基于权能的访问控制中实现职责隔离及极小特权原理。 RBAC包含以下基本要素：用户集(Users)，主体进程集(Subjects)，角色集(Roles)，操作集(Operations)，操作对象集(Objects)，操作集和操作对象集

形成一个特权集(Privileges)；用户与主体进程的关系(subject_user),用户与角色的关系(user_role), 操作与角色的关系(role_operations)， 操作与操作对象的关系(operation_object)。 通常subject_user是一个多对一的关系，它把多个主体进程映射到一个用户，这些进程都是替代该用户的主体进程；在本模型中它就是一个典型的多对一的关系。user_role可以是多对多的关系，但在本模型中它被简化为一对一的关系。role_operations是一个一对多的关系，它把一个角色映射到多个操作，是角色被授权使用的操作的集合；operation_object是一个一对多的关系，它把一个操作映射到多个操作对象，是操作被授权作用的操作对象集。 在本模型中，替代用户的主体进程可能只激活用户角色的被授权的操作的一部分，而且操作也可能仅作用在被授权作用的操作对象集的一个子集合上。在本系统中，将实现基于角色的授权和控制，支持角色互斥，不支持角色的继承，不支持同一个用户的多个角色。 2. 安全系统的设计 2.1 安全模型的设计 参照GB 17859中结构化保护级的安全功能特性要求，本系统中的安全服务器将遵循改进的BLP模型、DTE模型以及RBAC模型来实现系统的安全策略。其中，BLP模型是多级安全模型，保护信息的机密性；DTE模型是多域模型，保护信息的完整性；RBAC模型是基于角色的访问控制模型，是授权模型。通过三种模型的相互作用和制约，保证系统中的信息以及系统自身的安全性。 授权策略RBAC是整个系统的基础，它通过为用户设置特定角色，影响IA控制、特权控制、多域访问控制和强制访问控制等基本功能，达到控制系统中用户/主体对客体/对象的访问的目的。在本系统中，每个用户都有且只有一

个角色。为某个用户给定一个角色，相当于给定该用户的最大特权集、安全标记范围、DTE域范围和最小审计掩码。该用户的上述属性只能够在给定角色的范围内指定。RBAC是通过最小特权、强制访问控制（包括MAC机密性保护和DTE完整性保护）和安全审计等功能组合实现的。 而多域策略DTE和多级安全策略BLP则是在授权策略授权的基础上，调用多域访问控制和强制访问控制功能，实现对客体/对象信息的完整性和机密性保护。 