**项目总体设计报告**

**项目名称：基于系统调用重载的程序权限管理系统**

**姓名：陈晨 邹涛旭 孟详贺 王思皓**

**学号（519021910-）： -176 -075 -190 -160**

**学院：电子信息与电气工程学院**

**报告完成日期：2022年10月23日**

## 1 系统需求分析

* 1. **需求分析**

Linux系统中现有的访问控制机制只描述了用户对系统资源的访问权限，没有进一步准确指明用户执行的每个程序应该享有该用户的哪些权限，而是默认用户执行的每个程序都能享有该用户的所有权限。这种授权方式意味着用户把自己的所有权限都赋予所启动发进程，进程代码可以任意访问该用户所能使用的资源，任意进行该用户所能执行的操作。

如果用户所运行的程序都是善意的、可信的，linux系统的这种授权机制是合理的，但是一旦用户特别是管理员有意或无意地运行了恶意程序，该恶意程序就能够使用该用户的权限为所欲为。为了保护系统中的重要文件不被非法访问，防止应用程序有意或无意地越过运行权限，对操作系统和其他应用程序造成破坏，我们的基于系统调用重载的程序运行权限管理是十分有实际意义的。

* 1. **总体功能要求**

为了实现基于系统调用重载的程序运行权限管理，我们系统的总体功能重点实现对下列权限的控制：

1. 文件访问类操作。包括对文件或目录的创建、打开、读写、执行以及删除等。
2. 通信类操作。包括进程间通信、网络通信等。
3. 管理权限类操作。包括关机、重启、内核模块加载等。这一部分作为本次项目的拓展，有时间再完成。

同时我们进行程序操作审计，实现程序权限控制机制，应用程序可能会涉及到多个访问对象和多种类型的操作，因此需要对权限配置和存储进行涉及处理。

* 1. **软件开发平台要求**

操作系统为Ubuntu 18.10，采用的内核版本为Linux version 4.18.0-10-generic

* 1. **运行环境要求**

需要预先安装gcc、binutils、libelf-dev库，若后续进行前端图形化界面开发，则还需要依赖Qt开发平台。

## 2 计划进度安排

|  |  |
| --- | --- |
| **时间** | **工作安排** |
| 6~7周 | 完成开发环境搭建 成功进行内核态编译，初步实现系统调用重载功能 |
| 8~10周 | 完成程序权限数据库配置  完成程序审计数据库配置  实现内核态系统调用审计功能 |
| 11~12周 | 实现用户态对权限控制数据库的完整控制流程  实现内核态系统调用重载，对程序操作进行审核、审计 |
| 13~16周 | **机动时间**，视进度进行完善优化，或进一步完成：  用户态应用程序前端设计与优化 |

## 3 系统总体架构

**3.1 平台架构**

系统运行在Ubuntu18.10上，Linux内核版本为4.18.0-10。

编译环境：gcc-8.3

**3.2 总体架构**

系统总体分为**用户态策略配置模块**与**内核态系统调用重载模块**，前者负责配置程序的系统调用权限，后者利用重载函数覆盖原系统调用函数，负责在系统调用发生时执行安全性检查，与在策略配置模块中设定的权限策略进行比对，并选择允许或拒绝本次调用。

系统总体的功能逻辑如图：

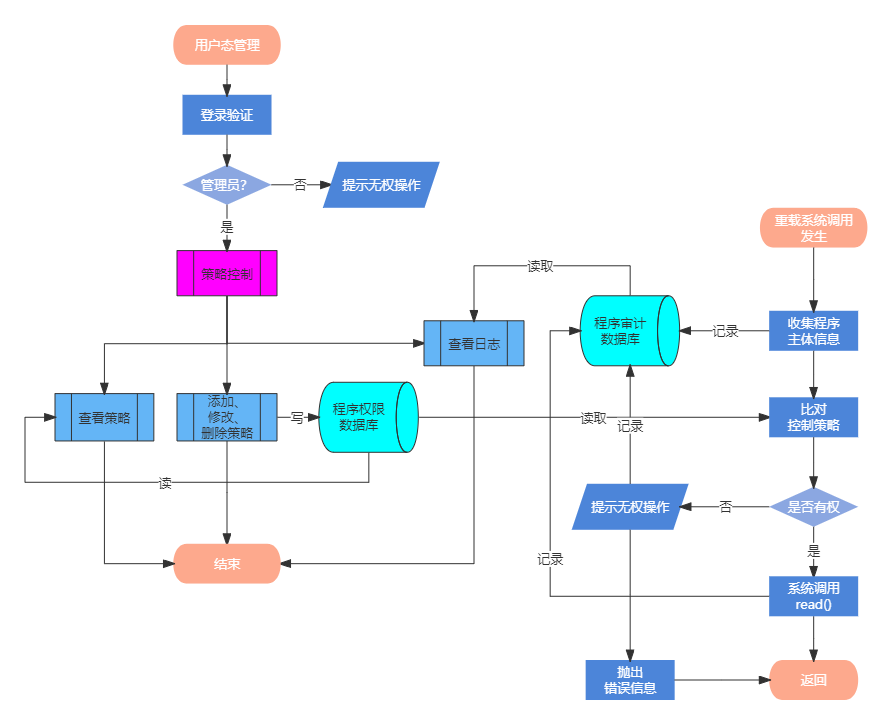


图 1 系统总体功能逻辑图

## 4 用户策略配置模块

**4.1 模块结构**

用户态管理模块主要负责对添加、修改、删除策略的操作，并将所有策略写入程序权限数据库，以便内核模块利用。子模块主要包括程序权限管理数据库、登录验证、策略控制。

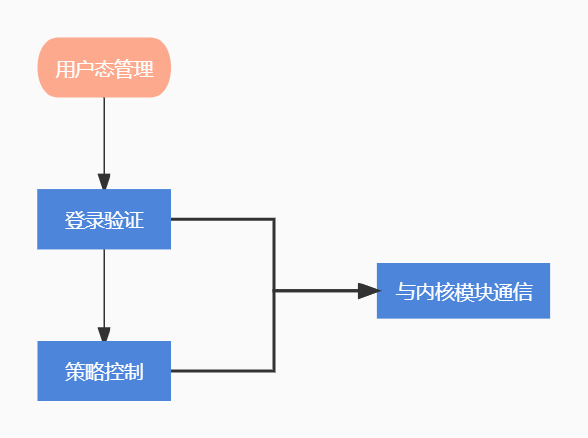


图 2 用户策略配置模块结构

**4.2 登录验证模块**

该模块主要用于判断用户是否具有管理员权限来决定是否赋予其策略控制的权限，若没有管理员权限，则提示无权操作，仅可查看策略，而无法对策略进行配置。

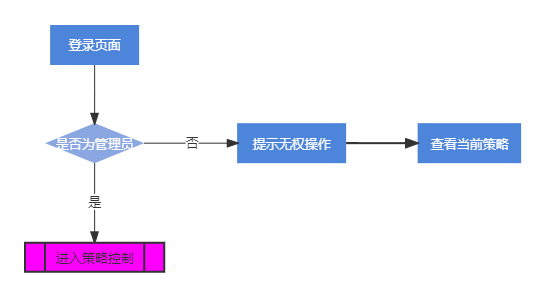


图 3 登录验证模块

**4.3 策略控制模块**

该模块主要用于添加、修改、删除程序策略，并将对应修改后的策略写入程序权限数据库中。选择使用MySQL数据库存储相关规则策略，并使用netlink对数据库进行读写的操作。查看当前策略则是从当前程序权限数据库中读取所有的规则策略。

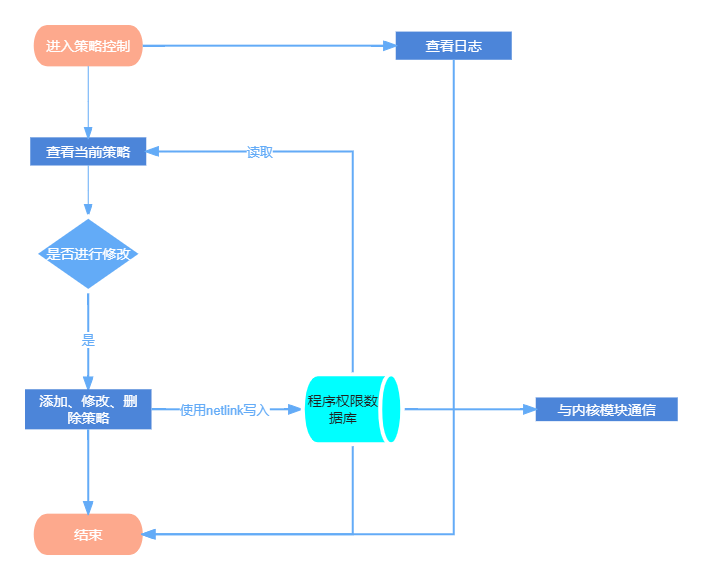


图 4 策略控制模块

## 5系统内核模块

**5.1 模块结构**

内核模块向上承接应用层程序权限数据库的规则策略，通过对系统调用函数的重载给应用程序划定权限的范围。子模块主要包括程序审计数据库、初始化模块、注销模块、基于netlink的信息发送模块。

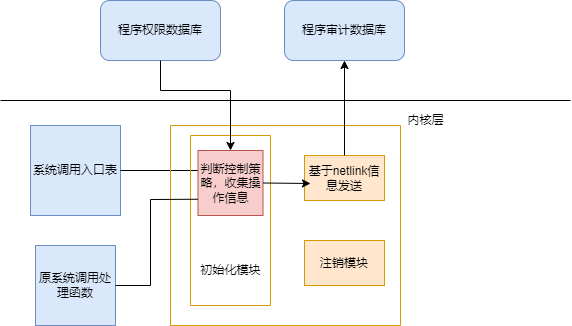


图 5 系统重载调用内核模块结构

**5.2 初始化模块**

该模块主要完成两方面的工作，一是对系统调用函数的重载，即对权限策略进行判断来决定是否赋予进程相应权限；二是完成netlink接口的初始化工作，包括创建相应的套接字接口，以及获得后台应用程序的PID，以便于将日志信息发送至审计数据库。

**5.3 注销模块**

该模块在内核模块注销时被linux内核自动调用。该函数将系统调用入口表中的重载的系统调用函数入口地址恢复，另外还负责回收netlink套接字接口所分配的资源。

**5.4 基于netlink的信息发送模块**

将收集到的权限控制情况构造成相应的netlink报文，通过netlink接口将报文发送到程序审计数据库。

## 6 运行平台

**6.1 软件平台**

Ubuntu18.10，内核版本4.18.0-10，建议使用虚拟机运行

**6.2 硬件平台**

无特殊需求

## 7 接口设计

用户态策略控制模块：

isAdmin(uid): 查询是否为管理员

showRules(): 显示当前策略集

addRule(rule): 添加策略

delRule(rule): 删除相应策略

modRule(rid, rule): 修改策略，rid为策略编号

showLog(): 显示程序审计日志

…

内核接口：

admissionReq(pid): 利用netlink向程序权限数据库发送查询，获知程序是否有对应权限

infoCollect(pid): 收集程序信息并写入日志

infoReturn(rslt): 返回程序执行结果并写入日志

hackCreat(): 创建文件权限检查

hackRead(): 读取文件权限检查

hackWrite(): 写入文件权限检查

hackChmod(): 文件权限改变权限检查

hackGethostid(): 获取主机标识符权限检查

…

## 8 系统出错处理设计

妥善考虑边界情况，定义异常的类型