**项目需求分析报告**

**项目名称：基于LSM 的程序运行权限管理**

**姓名： 傅雨东**

**学号： 5110369036**

**学院： 电子信息与电气工程学院信息安全专业**

**报告完成日期：2014.10.20**

## 引言

### 1.1编写目的

为明确软件需求、安排项目规划与进度、组织软件开发与测试，撰写本文档。本文档供开发人员参考。

### 1.2项目背景

Linux主要依据进程的启动用户判断进程的操作权限，这意味着进程可以共享启动用户的所有权限。这种权限授权方式违背信息安全的最小特权原则，最小特权原则指明按一个主体（进程等）完成它正常任务所需要的最小权限进程授权，如果一种权限对该主体正常运行不是必需的，就不要赋予该主体这种权限。

基于LSM框架，可以实现接近于最小特权管理的一种权限控制机制，管理员可以给一个可执行程序配置响应的运行权限，这种机制保证按管理员的权限配置对该可执行程序（实际上是该执行程序对应的进程）进行运行权限控制。

针对应用程序的运行权限控制给该应用程序划定一个运行权限范围，防止应用程序程序有意或无意的越过该运行权限，对操作系统和其他应用程序的运行构成破坏。在国外的操作系统安全相关研究中，这类权限控制机制被称为sandbox，在多种安全操作系统中得到支持和应用。

### 1.3定义

LSM：LSM是Linux Secrity Module的简称，即linux安全模块。其是一种轻量级通用访问控制框架，适合于多种访问控制模型在它上面以内核可加载模块的形实现。用户可以根据自己的需求选择合适的安全模块加载到内核上实现。

### 1.4参考资料

《信息安全技术解析与开发实践》，訾小超、薛质、姚立红、蒋兴浩、潘理

## 总体要求

### 2.1 总体功能要求

完成配置程序使用户能方便地通过配置程序对规则进行查看、增加、修改、删除操作。

完成程序运行权限管理，包括文件访问类操作、通信类操作、管理类操作，其中以文件访问类操作为主。

### 2.2 软件开发平台要求

①以Linux系统为宜

②内核版本不宜过高，因为过高会导致要用到的一些函数没导出

③2.6.10以上内核版本需要去除已经注册的其他安全机制

### 2.3 运行环境要求

①以Linux系统为宜

②内核版本不宜过高，因为过高会导致要用到的一些函数没导出

③2.6.10以上内核版本需要去除已经注册的其他安全机制

## 外部接口需求

### 3.1 用户界面：

命令行界面即可，不需要太友好的界面

### 3.2 硬件接口：

无

### 3.3 软件接口：

无

### 3.4 通讯接口：

无

## 系统功能需求

### 4.1系统各子功能说明

#### 4.1.1. 权限配置程序

① 权限的配置操作（包括权限的查看、添加、删除、修改）

② 权限的配置文件操作（包括权限的配置文件的导入、导出）

#### 4.2.2. 程序运行权限管理

① 文件访问类操作

1. 各类文件（或目录）的创建
2. 各类文件（或目录）的打开
3. 各类文件（或目录）的读
4. 各类文件（或目录）的写
5. 各类文件（或目录）的执行
6. 各类文件（或目录）的删除

② 通信类操作：以实现文件访问类为主，该类尽可能实现网络类的操作

③ 管理类操作：以实现文件访问类为主，该类尽可能实现关机、重启操作

### 4.2输入/输出数据

#### 4.2.1输入

字符串，用户输入的控制信息

#### 4.2.2输出

无，表现为被设置的可执行程序的各项操作的权限设置

## 其它非功能需求

### 5.1性能需求

无性能需求，与原来持平或慢1-5秒都可接受

### 5.2安全性需求

本程序本身实现即是为安全目的，因此尽可能使本程序本身的控制配置不被外部突破即可

**项目总体设计报告**

**项目名称：基于LSM 的程序运行权限管理**

**姓名： 傅雨东**

**学号： 5110369036**

**学院： 电子信息与电气工程学院信息安全专业**

**报告完成日期：2014.10.20**

## 引言

### 1.1编写目的

根据《项目需求分析报告》进行功能和体系结构分析设计

### 1.2 适用范围

适用于《基于LSM 的程序运行权限管理》项目的系统分析和设计过程

### 1.3 术语和缩写

|  |  |  |
| --- | --- | --- |
| 术语和缩写 | 解释 | 备注 |
| LSM | LSM是Linux Secrity Module的简称，即linux安全模块。其是一种轻量级通用访问控制框架，适合于多种访问控制模型在它上面以内核可加载模块的形实现。用户可以根据自己的需求选择合适的安全模块加载到内核上实现。 | 无 |

### 1.4 参考文献

《信息安全技术解析与开发实践》，訾小超、薛质、姚立红、蒋兴浩、潘理

## 设计概述

基于老师提供的简单的原型程序，以该原型程序为框架，在它的基础上进行进一步修改和设计。

### 2.1 设计约束

#### 2.1.1需求约束

参见上面的《需求分析报告》

#### 2.2.2隐含约束

由于本程序实际目的是为了完成一项作业并向老师进行演示，因此本程序在用户体验方面并不会考虑太多，以功能实现为主，使用人员限定为本人即开发者。

### 2.2 设计策略

①扩展策略：在现有框架上拓展修改。

②复用策略：无。

③折衷策略：以完成主体功能为主。

### 2.3 技术实现

LSM：LSM是Linux Secrity Module的简称，即linux安全模块。其是一种轻量级通用访问控制框架，适合于多种访问控制模型在它上面以内核可加载模块的形实现。用户可以根据自己的需求选择合适的安全模块加载到内核上实现。

## 系统概述

基于LSM框架，实现接近于最小特权管理的一种权限控制机制，管理员可以给一个可执行程序配置响应的运行权限，这种机制保证按管理员的权限配置对该可执行程序（实际上是该执行程序对应的进程）进行运行权限控制。

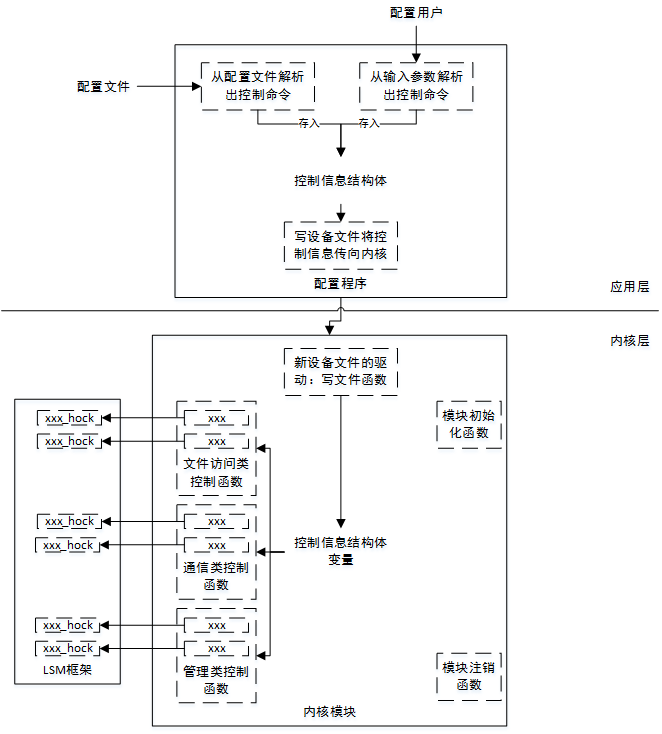
针对应用程序的运行权限控制给该应用程序划定一个运行权限范围，防止应用程序程序有意或无意的越过该运行权限，对操作系统和其他应用程序的运行构成破坏。

## 系统总体架构

### 4.1 平台架构

单主机，不需要网络连接，测试时可能需要网络环境

### 4.2 总体架构



## 系统功能模块划分

① 配置程序：负责从用户输入或配置文件中得到控制信息，并转换为一个结构体，并将该结构体通过写新的设备文件将控制信息从用户态传到核心态。

② 新设备文件的驱动：完成应用程序向内核模块发送配置信息，接收配置程序写入的控制信息，然后将该内容保存在控制信息结构体中。

③ 辅助模块：完成一些辅助功能，如根据PID得到实际的程序完整路径。

④ 一组访问控制函数：根据钩子函数传入的参数信息与辅助模块传入的进程信息，解析出哪个程序要执行什么操作，然后与控制信息结构体中的内容进行比对，如果要禁止则返回1否则返回0.

⑤ 内核模块的初始化：完成两方面的初始化工作，一是注册新设备文件的驱动程序，二是将预先设计好的相关控制函数注册到LSM框架中。

⑥ 内核模块的注销：完成设备文件驱动的卸载，以及从LSM框架中注销所注册的钩子函数。

## 运行平台

### 6.1 软件平台

操作系统：Fedora Core 6

内核版本：2.6.18去除已注册的其他安全机制

编译器：gcc 4.1.1

### 6.2 硬件平台

Vmware Workstation 8.0.4

## 接口设计

① 配置程序模块与新设备文件的驱动模块之间使用write\_controlledinfo，该函数是新注册设备的一个驱动函数，用于处理设备文件的写操作，其主要任务是调用函数copy\_from\_user()，将来自应用层空间的缓冲区中的内容复制到内核层空间的缓冲区。

② 一组访问控制函数模块与辅助模块之间使用get\_fullpath，该函数从参数pid寻找该进程对应的程序，并返回该程序所在的全路径名。

③ 一组访问控制函数模块与辅助模块之间使用myown\_check，该函数检查进程所对应的程序所执行的操作是否被允许。

## 系统出错处理设计

|  |  |  |
| --- | --- | --- |
| 错误产生原因 | 提示信息 | 建议处理办法 |
| 内核版本过高 | 加载模块失败 | 使用低版本内核 |
| 文件访问类控制错误 | 无提示信息（表示应该被禁止的操作成功被执行） | debug代码 |
| 通信类控制错误 | 如ping命令的显示结果 | debug代码 |
| 管理类控制错误 | 关机页面 | debug代码 |