基于SELinux的三权分离技术的研究

杨 霞[1,2]，石 鹏[1]，杨 姗[1]，任 飞[2]

(1. 电子科技大学信息与软件工程学院 成都 610054；2. 保密通信重点实验室 成都 610041)

【摘要】随着Linux操作系统的广泛使用，由于root权限过大所暴露出来的安全问题逐步被引起关注。针对Linux操作系统的特权管理问题，首先建立了三权分离安全模型，将Linux系统中的特权用户分解为系统管理员、安全管理员、审计管理员3个不同的管理员角色。然后，基于SELinux的强制访问控制技术设计并实现了三权分离机制和安全策略，对每个管理员的权限进行细粒度划分和严格的访问控制。最后，基于嵌入式平台实现了一个实验原型系统，验证了三权分离方法的正确性和可行性。该方法可广泛应用于Linux操作系统，以提高系统的安全性。

关 键 词 强制访问控制技术； 安全模型； 安全策略； SELinux； 三权分离技术

中图分类号 TP309 **文献标志码** A doi:10.3969/j.issn.1001-0548.2016.06.014

Research on the Separation of Privilege Based on SELinux

YANG Xia[1,2], SHI Peng[1], YANG Shan[1], and REN Fei[2]

(1. School of Information and Software Engineering, University of Electronic Science and Technology of China Chengdu 610054;
2. Science and Technology on Communication Security Laboratory Chengdu 610041)

Abstract With the widespread use of Linux operating systems, security problems is gradually exposed and become a hot topic because of excessive root privileges. To solve this problem and enhance security of Linux operating system, firstly, we model the separation of privilege, which divides the privilege of Linux system into three roles, system administrator, security administrator, and auditor. Then, this paper designs and implements the separation of privilege mechanism based on the SELinux's mandatory access control technology, which can define fine-grained permissions and security policy for each role and control user's access strictly. Finally, we implement a prototype system based on the embedded platform, which verifies the correctness and feasibility of our approaches presented in this paper. These approaches presented in this paper can be used in Linux operating system to enhance system security.

Key words mandatory access control technology; security model; security policy; SELinux; separation of privilege mechanism

目前，Linux操作系统已广泛应用于各种设备和产品中，如服务器、PC机、机顶盒及路由器等。随着Linux系统的不断发展和广泛应用， Linux系统的安全问题也引起越来越多的关注。在Linux操作系统中，存在一个超级用户即root用户。root也称为系统管理员，它拥有管理系统的一切权限。当一个非法用户获得root用户口令后，他就可以以超级用户的身份登录系统，然后做任何他想做的事情：如任意添加、删除用户，终止进程，删除重要文件甚至更改root用户的口令。因此，一旦root权限被恶意用户利用，就可能导致系统数据的泄密和破坏。

该问题已经引起了国家的重点关注，如国家保密标准BMB20-2007《涉及国家秘密的信息系统分级保护管理规范》中明确提出：涉密信息系统应配备系统管理员、安全保密管理员和安全审计员这三类安全保密管理人员，三员应该相互独立、相互制约、不得兼任。三个管理员之间的工作机制分为协作和制约两种机制，行使的是原超级用户的权力，即系统管理员、安全管理员和审计管理员间相互协作，共同维护系统的正常运行。制约机制指只有在当前管理员操作不影响其他管理员正在进行的操作时才被允许，从而保证了管理员行为的可预期性，避免超级用户的误操作或其身份被假冒而带来的安全隐患，增强了系统的安全性。该规范可以有效防止由系统管理员权力过大所带来的系统安全威胁和隐患[1]。

收稿日期：2015－03－29；修回日期：2016－01－06
基金项目：国家核高基重大专项(M1401060112ZX0103301)；国家科技支撑计划(2012BAH44F00)
作者简介：杨霞(1978－)，女，副教授，博士，主要从事嵌入式系统、可信计算、嵌入式操作系统安全理论和技术等方面的研究.

SELinux(security-enhanced Linux)[2]是安全增强的Linux，以强制访问控制(mandatory access control, MAC)[3]技术为基础，应用类型增强(type enforcement, TE)和基于角色访问控制(role-base access control, RBAC)两种安全策略模型。通过MAC技术可以实现对用户和进程权限的最小化，即使在系统受到攻击或者进程和用户的权限被剥夺的情况下，也不会对整个系统的安全造成重大影响。SELinux对访问的控制更彻底，它对系统中的所有文件、目录、端口资源的访问控制都基于一定的安全策略而设定。只有管理员才能定制安全策略，一般用户没有权限更改。因此SELinux为三权分离思想的实现奠定了基础。

目前，SELinux的相关研究工作主要集中在安全策略分析和配置及SELinux安全模型研究[4-5]方面。文献[6]提出了高安全等级信息系统中的权限分离模型(privilege separation model, PSM)。将原有管理员分解为3个不同角色，形式化定义了权限的支撑关系和制约关系，给出了模型中的三权分立的权限制约算法、安全定理及安全性质。文献[7]提出了一种满足高安全级信息系统最小特权需求的强制访问控制模型。然而，二者都没给出具体的实施方案。

本文基于SELinux建立了三权分离安全模型，设计了三权分离安全策略，并实现了三权分离机制，最后通过实验验证了可行性和正确性。

1　SELinux的安全技术

1.1　MAC和DAC技术分析

SELinux除了采用自主访问控制(discretionary access control, DAC)外，还在Linux内核中使用强制访问控制机制严格控制所有对系统资源的访问请求，并根据安全策略确定是否授予该请求相应的权限。MAC机制将能够发出访问请求的对象称为主体(如进程)，将系统的被访问对象(如：文件、设备、socket、端口和其他进程)称为客体，所有主体对客体的访问都必须由MAC机制通过安全策略授权。MAC机制给进程仅授予操作所需要的权限，这遵循了最小权限原则。因此，在MAC机制的保护下，即使获取root用户的权限也无法访问未授权的客体[4]。

在SELinux中，MAC与DAC机制联合，以提高系统的安全性。如图1所示当用户空间的进程发出访问客体的请求时，首先由Linux的DAC机制进行常规检查。如果DAC(依据程序的拥有者与文件资源的rwx权限来决定有无存取的能力)检查通过，再由MAC进行进一步的权限检查。MAC中的客体管理器模块存在于所有被访问的客体对象中，在进程访问客体之前，由客体管理器“截获”访问请求，并把访问请求递交给SELinux安全模块进行仲裁，SELinux安全模块根据安全策略库的安全策略对访问请求仲裁，如果安全策略已经定义了该进程对该客体的访问规则，则仲裁允许，然后进程可以访问此客体；否则，拒绝进程对此客体的访问请求。

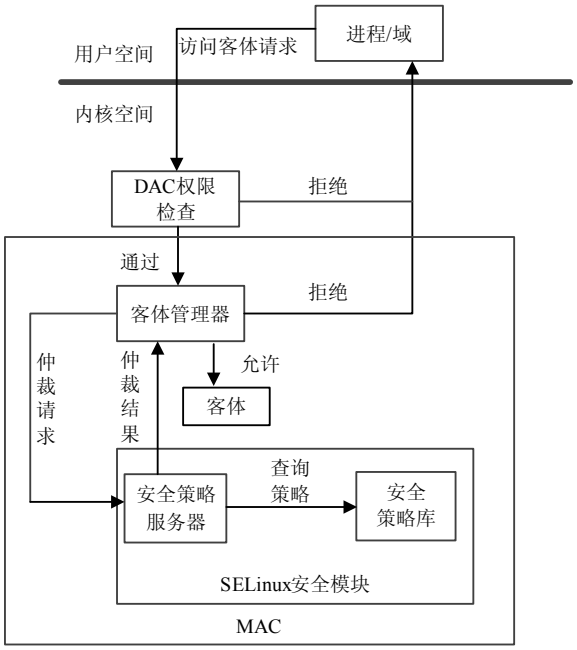

图1　SELinux的DAC与MAC

1.2　SELinux的安全策略模型[8]

安全策略作为访问控制机制权限仲裁的依据，是SELinux中非常重要的内容之一。SELinux采用TE(type enforcement)和RBAC(role-based access control)相结合的安全策略。

1.2.1　TE[9]模型

SELinux中所有的安全策略，都必须用TE规则明确地定义，没有被明确许可的其他访问方式，都被禁止(最小权限原则)。TE访问向量规则定义了主体可以访问什么类型的客体，TE转移规则定义了域类型的相互转移[10]。本文只讨论前者。

定义 1　TE模型的关键要素：

源类型(source type, ST)主体(subject)或者域的类型。目标类型(target type, TT)客体(object)的类型。对象类别(class)访问申请的某一类别资源，如：file、socket等。操作类型(opration, OPT)如：read、write等。许可权限(permission, P)表示主体对客体访问时允许的操作。

定义 2　TE策略模型：

TE策略模型可定义为：P=ST×OPT×TT，许可

权限(P)=源类型(ST)对目标类型(TT)的资源类(class)的操作(OPT)。

定义 3 根据上述TE策略模型，采用allow语法制定策略规则如下：

allow ST TT : class {opt1, opt2, …};

根据此策略规则，定义出如下安全策略：

allow user_t bin_t : file {read execute getattr};

在allow基本语法规则中包含了两个类型标识符：源类型(ST)user_t，目标类型(TT)bin_t。标识符file是定义在策略中的对象类别名称(在这里，表示一个普通的文件)，大括号中包括的操作是文件操作类型的一个子集，此安全策略示例的含义是拥有域类型user_t的进程可以读/执行或获取具有bin_t类型的文件客体的属性。

1.2.2 SELinux的RBAC模型

传统的基于角色的访问控制RBAC模型[11]，为角色授权，然后将一个或多个角色分配给一个授权用户。SELinux对RBAC模型进行了改进，提出了一种TE-RBAC联合模型，改进后的模型如图2所示，通过allow安全策略规则给源类型指定授权，然后将源类型指定给角色，最终将一个或多个角色指定给一个授权用户[7]。

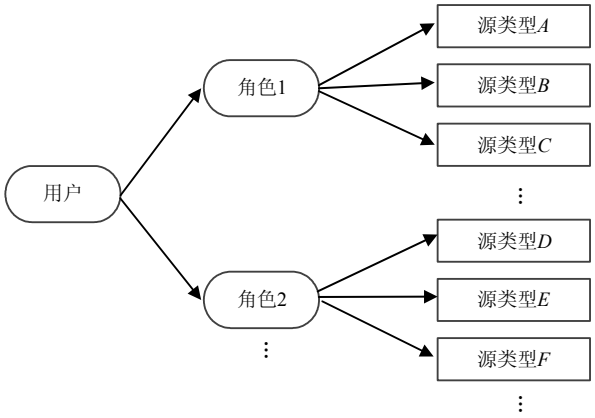

图2 SELinux的RBAC策略模型

定义 4 TE与RBAC联合模型：

声明用户及其关联的角色，user joe roles {user_r}；这个语句声明了一个用户joe，以及与之关联的角色user_r。

声明角色与其源类型关联，role user_r types user_t；这个语句将源类型user_t与角色user_r 关联起来。

2 三权分离模型

2.1 权能集定义

依据最小特权和权值分离的管理思想，本文将原超级用户的特权进行细粒度划分，分别授予不同的管理员角色，使各种管理员只具有完成其任务所需的最小特权，不同管理员间相互协作共同管理系统。从逻辑上将承担这3类职责的特权用户命名为系统管理、安全员管理员和审计员管理员[12]。

根据上述非形式化描述，为了实现三权分离机制，本文首先将系统的root权能集进行划分，并给出如下定义。

定义 5 系统root权能集C

C = { Csy, Cse, Cau}，其中Csy表示系统管理员权能集，Cse表示安全管理员权能集， Cau表示审计管理员权能集。

定义 6 三权分离权能集。根据三权分离思想，将root权限拆分成下述3个权能集：

1) 系统管理员权能集Csy

Csy管理与系统相关的资源，包括用户身份管理、系统资源配置、系统加载和启动、系统运行的异常处理[12]。

2) 安全管理员权能集Cse

Cse制定系统安全策略，负责对系统中的主体、客体进行统一标记，对主体进行授权，配置一致的安全策略，并确保标记、授权和安全策略的数据完整性[12]。

3) 审计管理员权能集Cau

Cau设置审计选项，对与安全有关的事件进行审计处理，包括监视系统的活动以及日志的处理，提供审计和监控功能，创建和维护受保护客体的访问审计跟踪记录[12]。

4) 各权能集之间相互隔离，当且仅当对任意a，$b \in T(T = \{sy, se, au\})$，$a \neq b$，有$C_a \subseteq C$，$C_b \subseteq C$，$C_a \cap C_b = \varnothing$，其中$C$=Cse∪Csy∪Cau。即每个管理员所能访问的权能集是绝对隔离的。

2.2 基于SELinux的三权分离策略模型

根据上述权能集的描述，下面基于SELinux建立一种三权分离策略模型，主要包括特权用户、特权角色和源类型集定义，以及各特权用户与对应的特权角色关联和特权角色与对应的源类型集关联。

如图3所示，首先创建3个SELinux特权用户，root(系统管理员)、secadm(安全管理员)和auditadm(审计管理员)，并定义3个SELinux特权角色：sysadm_r(系统管理角色)、secadm_r(安全管理角色)和auditadm_r(审计管理角色)。

定义 7 定义3组源类型集，STsy，STse，STau满足下列条件：

STsy ={ STasy, STbsy, …}；STse= { STase, STbse, …}；STau= { STaau, STbau, …}

并且根据SELinux的TE模型和上述全能集的定义，可得到如下3组TE策略模型：

1) Psy = STsy×OPT×TT，且Psy⊆Csy(即系统管理员各源类型的许可权限是系统管理员权能集Csy的子集)；

2) Pse = STse×OPT×TT，且Pse⊆Cse(即安全管理员各源类型的许可权限是安全管理员权能集Cse的子集)；

3) Pau = STau×OPT×TT，且Pau⊆Cau(即审计管理员各源类型的许可权限是审计管理员权能集Cau的子集)；

4) STsy集∩STse集=∅，STse集∩STau集=∅，STsy集∩STau集=∅，每组源类型集合之间都不能相交。

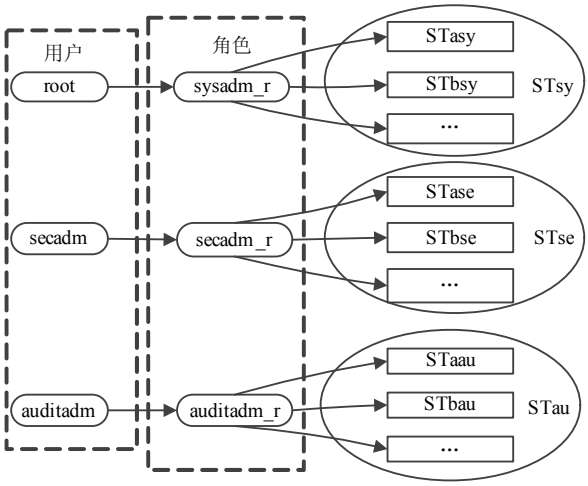

图3　三权分离策略模型

定义 8　定义三权分离的用户与角色关联

user root role sysadm_r，将root系统管理员用户与sysadm_r角色关联；

user secadm role secadm_r，将secadm安全管理员用户与secadm_r角色关联；

user auditadm role auditadm_r，将auditadm审计管理员用户与auditadm_r角色关联。

定义 9　三权分离的角色与源类型集关联

role sysadm_r types STsy={STasy, STbsy, … }
role secadm_r types STse={STase, STbse, … }
role auditadm_r types STau={ STaau, STbau, … }

本定义基于SELinux的RBAC安全模型为每个角色关联一组源类型集合，即：

sysadm_r关联STsy集；secadm_r关联STse集；auditadm_r关联STau集。

3　三权分离的安全策略设计与实现

在定义了三权分离模型后，为了在SELinux中实现该模型，必须修改SELinux已有的安全策略库，添加三权分离的安全策略。下文详细阐述基于SELinux的三权分离安全策略的设计与实现。

3.1　三权分离的安全策略设计

图4描述了系统管理员、安全管理员、审计管理员与SELinux中角色的关联关系，图中还指出了每个角色关联的源类型，这些源类型基本概括了该角色对系统所有客体所允许的访问许可。

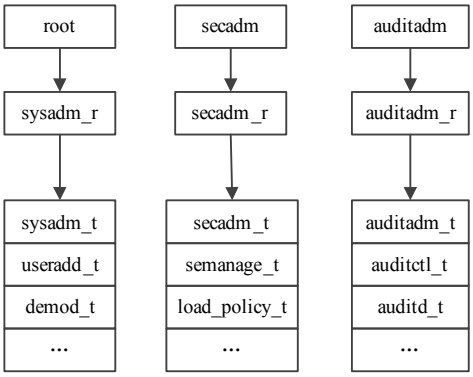

图4　三权分离的安全策略设计

3.1.1　系统管理员策略设计

根据定义6～定义9的统管理员相关描述，系统管理员root关联了角色sysadm_r，角色sysadm_r默认的源类型为sysadm_t，这个源类型允许转换到与角色sysadm_r关联的其他源类型，如图4中描述的源类型useradd_t和demod_t等。然后在TE安全策略模型实现中，为每一个源类型分配相应的权限许可。

3.1.2　安全管理员策略设计

根据定义6～定义9中安全管理员相关描述，安全管理员secadm关联了角色secadm_r，角色secadm_r默认的源类型为secadm_t，这个源类型允许转换到与角色secadm_r关联的其他源类型，如图4中描述的源类型checkpolicy_t、load_policy_t、semanage_t和setfiles_t等。然后在TE安全策略模型实现中，为每一个源类型分配相应的权限许可。

3.1.3　审计管理员策略设计

根据定义6～定义9中审计管理员相关描述，审计管理员auditadm关联了角色auditadm_r，角色auditadm_r默认的源类型为auditadm_t，这个源类型允许转换到与角色auditadm_r关联的其他源类型，如图4中描述的源类型auditctl_t和auditd_t等。然后在TE安全策略模型实现中，为每一个源类型分配相应的权限许可。

3.2 三权分离的TE策略实现

上一节中已经描述了每个用户角色所关联的源类型，下面针对每个源类型按照前面所阐述的TE模型指定具体的安全许可规则。

3.2.1 系统管理员安全策略的实现

系统管理员拥有原root用户的大部分权限，用来完成系统中日常的操作和维护，包括系统用户账户的管理、网络相关管理与操作、内核模块加载、开启和关闭系统、对文件的档案备份和恢复、安装或卸载文件系统等。以管理系统用户账户为例，其源类型为useradd_t，系统管理员拥有添加用户账号的权限，即只有系统管理员可以执行useradd命令，因此需要在策略中按TE模型的描述给useradd_t源类型定义相应的许可权限。

allow useradd_t useradd_exec_t: file {open read execute};

该allow规则定义了源类型useraddr_t对目标类型useradd_exec_t(表示useradd命令)的文件资源授予打开(open)、读(read)和执行(execute)的权限。

3.2.2 安全管理员安全策略的实现

安全管理员是整个系统安全策略的制定者，负责制定生成安全策略，修改SELinux运行模式，装载二进制安全策略，设置文件安全上下文等。以生成安全策略为例其源类型为checkpolicy_t，安全管理员拥有将策略规则源码编译成二进制策略文件的权限，即只有安全管理员可以执行checkpolicy命令，因此需要在策略中按TE模型的描述给checkpolicy_t源类型定义相应的许可权限。

allow checkpolicy_t checkpolicy_exec_t: file {open read execute};

该allow规则定义了，源类型checkpolicy_t对目标类型checkpolicy_exec_t(表示checkpolicy命令)授予打开(open)、读(read)和执行(execute)的权限。

3.2.3 审计管理员安全策略的实现

审计管理员是系统的监督者，负责设置审计开关和审计阈值，启动和关闭审计机制以及管理审计日志等。以auditadm_t源类型为例，只有审计管理员才能拥有查看审计日志的权限，在策略中按TE模型的描述给auditadm_t源类型定义相应的许可权限。

allow auditadm_t var_log_t: file {open read getattr};

该allow规则定义了源类型auditadm_t对目标类型var_log_t(表示审计日志文件)授予打开(open)、读(read)和获取属性(getattr)的权限。

4 三权分离实验

4.1 实验平台介绍

实验的硬件平台为TQ2440(基于S3C2440A CPU)嵌入式开发板，软件平台为嵌入式Linux。Linux内核为Linux 2.6.30，Linux命令工具集为Busybox-1.22.0，安全策略由策略库refpolicy-2.20090730[2]修改生成。

4.2 实验原型的实现

根据上文描述的三权分离安全策略模型，基于refpolicy策略库，在嵌入式Linux平台上，借助于SELinux模块实现了一个三权分离的实验原型系统。该系统重点实现了三权分离的安全策略，定义3个特权角色及对应的3个SELinux特权用户，并为每个用户制定详细的最小执行或访问权限。禁止各用户对其他用户私有资源的访问，最大化的限制用户的权限，以提高系统的安全性。

4.3 三权分离功能测试

4.3.1 用户角色关联测试

系统管理员(root)关联角色sysadm_r，且角色关联sysadm_t源类型，如图5a所示。安全管理员(secadm)关联角色secadm _r，且角色关联secadm _t源类型，如图5b所示。审计管理员(auditadm)关联角色auditadm _r，且角色关联auditadm _t源类型，如图5c所示。

```
[root@(none) ~]# id -z
root:sysadm_r:sysadm_t
```

a. 系统管理员安全标识

```
[secadm@(none) ~]# id -z
secadm:secadm_r:secadm_t
```

b. 安全管理员安全标识

```
[auditadm@(none) ~]# id -z
auditadm:auditadm_r:auditadm_t
```

c. 审计管理员安全标识

图5 用户角色关联标识测试

4.3.2 审计管理员功能测试

根据三权分离的设计模型，审计日志只能由审计管理员进行访问，而其他用户无权进行读操作。图6a显示审计管理员成功读取审计日志，而系统管理员读取审计日志显示“Permission denied”。

值得注意的是，如果当前以root权限登录去执行审计操作，由于root用户不具备对审计日志的访问权限，因此该请求被拒绝，如图6b所示。由此来看，本文所实现的三权分离方法可有效限制原来Linux操作系统的root权限，解决root权限过大多带来的系统危害，更好地防止恶意程序通过获取root权限对系

统的破坏。

```
[auditadm@(none) log]# head messages
Jul 12 17:21:53 (none) syslog.info syslogd started: BusyBox v1.22.0
```

a. 审计管理员访问审计日志

```
[root@(none) log]# head messages
type=1400 audit(1250957794.923:40): avc:  denied  { read } for  pid=1284 comm="h
ead" name="messages" dev=mtdblock2 ino=345 scontext=root:sysadm_r:sysadm_t tcont
ext=system_u:object_r:var_log_t tclass=file
head: messages: Permission denied
```

b. 系统管理员访问审计日志

```
[secadm@(none) ~]# setenforce 0
type=1404 audit(1250958122.081:11): enforcing=0 old_enforcing=1 auid=4294967295
ses=4294967295
```

c. 安全客理员关闭SELinux

```
[root@(none) log]# setenforce 0
type=1400 audit(1250957857.503:41): avc:  denied  { setenforce } for  pid=1285 c
omm="setenforce" scontext=root:sysadm_r:sysadm_t tcontext=system_u:object_r:secu
rity_t tclass=security
setenforce: setenforce() failed: Permission denied
```

d. 系统管理员关闭SELinux

图6　三权分离功能测试

4.3.3　安全管理员功能测试

根据三权分离的设计模型，只有安全管理员有权修改SELinux安全模式，测试结果如图6c所示，安全管理员执行该操作成功。而系统管理员无权执行该操作，因此操作请求将被拒绝，如图6d所示。由此可见，系统管理员root的权限被严格限制了。因此，即使系统管理员角色被恶意用户获得，也不会对系统造成严重的损害。

5　结 束 语

为了解决root权限过大给linux操作系统所带来的安全隐患问题，本文基于SELinux的强制访问控制技术，采用三权分离思想，建立了三权分离策略模型，实现了一个安全增强的Linux操作系统。即使特权用户的密码被恶意用户获取，也不会对系统造成很大的损害，从而将恶意攻击对系统的危害降到最低。本文的三权分离思想将Linux系统的root用户权限拆分为安全管理、系统管理、审计管理三种权限。然后定义了三权分离策略模型，并基于SELinux的安全策略库设计并实现了一套三权分离的安全策略库。最后，在嵌入式Linux平台上，借助于SELinux的强制访问控制技术实现了一个实验原型系统，并对系统各项功能进行了多次测试。实验结果表示，本文的研究工作能够严格的限制每个用户的权限，如只有审计管理员可以查看系统的审计日志，只有安全管理员可以对系统的安全策略进行管理等，从而有效解决了Linux系统由于root权限过大所带来的系统危害和被攻击的问题。本文的研究工作适合于任何Linux平台，包括嵌入式设备和服务器，通过这种三权分离机制可以克服权力过于集中给系统带来的危害，以提高Linux系统的安全性。

参 考 文 献

[1] 耿伟, 吴肖炎. 涉密信息系统安全保密管理人员的职责要求与权限划分[J]. 学术研究, 2009(7): 114-121.
GENG Wei, WU Xiao-yan. Responsibilities and divisions of authority for security-and-privacy management personnel of secret-involved[J]. Academic Research, 2009(7): 114-121.

[2] National Security Agency. Security-enhanced Linux (SELinux)[EB/OL]. [2015-3-20]. http://www.nsa.gov/research/selinux/.

[3] BRIFFAUT J, LALANDE J F, TOINARD C. Formalization of security properties: Enforcement for MAC operating systems and verification of dynamic MAC policies[J]. International Journal on Advances in Security, 2010, 2(4): 325-343.

[4] 肖永康, 纪翠玲, 谢宝恂, 等. SELinux的安全机制和安全模型[J]. 计算机应用, 2009(29): 66-68.
XIAO Yong-kan, JI Cui-ling, XIE Bao-xun, et al. Security mechanism and security model of SELinux[J]. Journal of Computer Applications. 2009(29): 66-68.

[5] 崔宾阁, 刘大昕. 强制访问控制在基于角色的保护系统中的实现[J]. 计算机工程, 2006(6): 167-169.
CUI Bin-ge, LIU Da-xin. Realization of mandatory access control in role-based protection systems[J]. Computer Engineering, 2006(6): 167-169.

[6] 李瑜, 马朝斌. 高安全等级信息系统中的权限分离模型[J]. 山东大学学报(理学版), 2012(11): 18-23.
LI Yu, MA Chao-bin. Research on the privilege separation model of high level information systems[J]. Journal of Shandong University(Natural Science), 2012(11): 18-23.

[7] 杨涛, 沈昌祥, 陈福接. 一个用于安全操作系统特权管理的改进Bell-La Padula模型[J]. 计算机研究与发展, 1993, 30(1): 45-49.
YANG Tao, SHEN Chang-xiang, CHEN Fu-jie. An improved bell-lapadula model for the privilege management of operating systems[J]. Journal of Computer Research and Development, 1993, 30(1): 45-49.

[8] AHN G J, XU W, ZHANG X. Systematic policy analysis for high-assurance services in SELinux[C]//IEEE Workshop on Policies for Distributed Systems and Networks. [S.l.]: IEEE, 2008: 3-10.

[9] MAROUF S, PHUONG D M, SHEHAB M. A learning-based approach for SELinux policy optimization with type mining[C]//Cyber Security and Information Intelligence Research. [S.l.]: ACM, 2010: 1-4.

[10] 倪继利. Linux安全体系分析与编程[M]. 北京: 电子工业出版社, 2007.
NI Ji-li. Linux security system analysis and programming [M]. Beijing: Publishing House of Electronics Industry, 2007.

[11] AMTHOR P, KUHNHAUSER W E, POLCK A. Model-based safety analysis of SELinux security policies[C]// 2011 5th International Conference Networking and System Security(NSS). [S.l.]: IEEE, 2011: 208-215.

[12] 陈亚莎, 赵勇, 刘燕, 等. 高安全级信息系统中的特权控制机制及其模型研究[J]. 山东大学学报(理学版), 2011(9): 57-60.
CHEN Ya-sha, ZHAO Yong, LIU Yan, et al. Research on the privilege control mechanism and modeling of a high level information system[J]. Journal of Shandong University: Natural Science, 2011(9): 57-60.

编　辑　蒋　晓