(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106295355 A
(43)申请公布日 2017.01.04

(21)申请号 201610656020.3

(22)申请日 2016.08.11

(71)申请人 南京航空航天大学
地址 210016 江苏省南京市秦淮区御道街29号

(72)发明人 薛明富 郭克君 栾俊超 王箭

(74)专利代理机构 南京瑞弘专利商标事务所（普通合伙）32249
代理人 严巧巧

(51)Int.Cl.
G06F 21/57(2013.01)
H04L 29/06(2006.01)

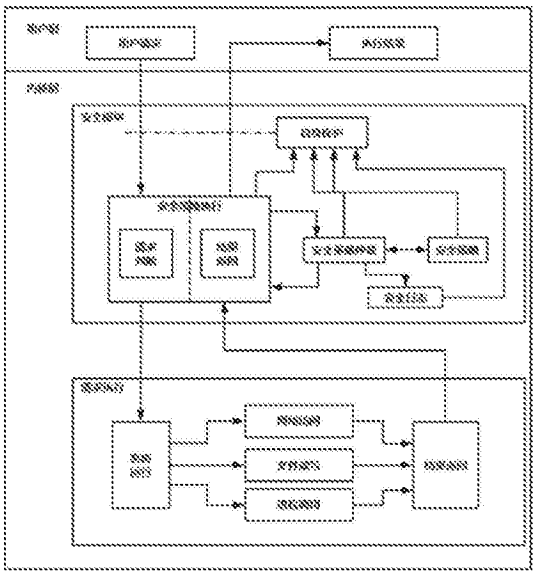
权利要求书3页 说明书9页 附图2页

(54)发明名称

一种面向Linux服务器的主动安全保障方法

(57)摘要

本发明提供一种面向Linux操作系统的主动安全保障方法作为可以独立运行的安全模块将嵌入系统内核，与操作系统紧密结合，克服现有Linux操作系统在系统资源管理、进程管理、防火墙管理、用户管理、文件管理、日志安全审计以及状态监控等方面不足的问题，采用多模块工作方式，将策略执行、策略仲裁、策略保存、日志记录相互独立，确保系统正常工作。



CN 106295355 A

1.一种面向Linux服务器的主动安全保障方法，其特征在于：编译Linux系统内核，将安全模块嵌入在Linux系统内核中，并且在Linux系统内核加载阶段即加载安全模块，设置安全模块处于内核级运行状态；

所述安全模块包括安全策略执行模块、安全策略仲裁模块、安全日志记录模块以及自身保护模块，安全策略执行模块将所有用户请求加以拦截并提交安全策略仲裁模块进行仲裁，当安全策略仲裁模块仲裁为允许时，安全策略执行模块放行该请求，当安全策略仲裁模块仲裁为禁止时，安全策略执行模块禁止该请求；用户请求运行结束后，系统先将运行结果返回安全模块，由安全模块记录信息后返回给用户结果；系统运行全过程中，自身保护模块实时检测安全模块运行状态，一旦发现安全模块运行出错立即冻结系统状态，检查并重新运行安全模块，直到安全模块恢复后再恢复系统状态；安全日志记录模块记录系统全部操作日志，实时备份操作日志并加密。

2.根据权利要求1所述的面向Linux服务器的主动安全保障方法，其特征在于：所述安全模块对用户进程、系统防火墙、系统资源、文件系统均采用建立黑白灰名单进行管理：

对于用户进程，安全模块为用户进程建立用户进程白名单、黑名单和灰名单，当系统试图运行某个进程时，安全模块对该用户进程进行仲裁：针对属于进程白名单中的用户进程，安全模块允许系统调用该用户进程，并提醒用户该用户进程已经运行；针对属于进程黑名单中的用户进程，安全模块禁止系统调用该用户进程，并提醒用户该用户进程已经禁止运行；针对属于进程灰名单中的用户进程，安全模块定期询问用户是否允许该用户进程运行，如果用户许可运行，则将其从用户进程灰名单中删除并加入用户进程白名单中，如果用户不允许运行，则将其从用户进程灰名单中删除并加入用户进程黑名单中；

对任意一个用户进程，当该用户进程首次运行时，安全模块针对该用户进程记录用户进程的状态，包括：文件读写、进程调用、运行线程和网络访问，后续该用户进程再次运行时，若发现有与首次运行时记录的用户进程的状态不同的行为，则将该用户进程放入用户进程灰名单中，并提醒用户该用户进程的越权行为，并再次请求用户许可；

对于系统防火墙，安全模块为用户进程的网络访问请求建立系统防火墙白名单、黑名单和灰名单，设置初始的系统防火墙策略为禁止所有的内外部网络访问请求；当某个用户进程试图访问网络时，安全模块对该网络访问请求进行仲裁：针对属于系统防火墙白名单中的网络访问请求，安全模块允许该网络访问请求，并更新系统防火墙策略，将该网络访问请求所对应的防火墙策略加入系统防火墙策略表，并提醒用户已经放行该网络访问请求，当该网络访问请求结束时，立即再次更新系统防火墙策略，将该网络访问请求所对应的防火墙策略从系统防火墙策略表中移除；针对属于系统防火墙黑名单中的网络访问请求，安全模块阻止该网络访问请求，并提醒用户已经禁止该网络访问请求；针对属于系统防火墙灰名单中的网络访问请求，安全模块实时询问用户是否许可该网络访问请求，若用户许可，则将该网络访问请求加入系统防火墙白名单，若用户不许可，则将该网络访问请求加入系统防火墙黑名单；

对任意一个网络访问请求，当其在首次加入系统防火墙白名单时，安全模块针对网络访问请求记录该网络访问请求的状态，包括：IP地址、端口号、协议以及调用后运行的时间和流量消耗统计，在后续该网络访问请求再次请求时，若发现有与首次加入系统防火墙白名单时所记录的该网络访问请求的状态不同的行为，则重新将网络访问请求放入系统防火

墙灰名单中，并提醒用户该网络访问请求的越权行为，再次请求用户许可；

对于系统资源，安全模块建立包括CPU占用率、内存占用率、硬盘占用率在内的系统资源表，实时监控查询各类系统资源占用情况；同时，为用户进程建立系统资源占用白名单、黑名单和灰名单，系统资源占用白名单、黑名单和灰名单中分别记录位于其中的用户进程对于各个类型系统资源的最大请求数目，许可范围为每类系统资源的最大请求数目不超过该类系统资源总体的50％，针对系统资源占用白名单中的用户进程所请求的系统资源占用给予放行，针对系统资源占用黑名单中的用户进程所请求的系统资源请求禁止运行，针对系统资源占用灰名单中的用户进程所请求的系统资源请求主动问询用户是否放行；

对于任意一个用户进程首次运行时，安全模块记录该用户进程的资源请求状态和资源访问，并不断监控后续该用户进程运行时对系统资源的占用情况，并根据其运行状态动态调整系统资源占用，一旦某次调整前后的可占用系统资源的百分比的差值超过5％，则重新将该用户进程放入系统资源占用灰名单中，并提醒用户该用户进程的越权行为，再次请求用户许可；

一旦出现总体系统资源异常情况，则主动冻结系统状态，逐一检查系统资源占用情况，将出现异常资源占用的用户进程从系统资源占用白名单中移除并放入系统资源占用灰名单，然后恢复系统运行，同时提醒用户这一异常，如果用户许可，再将该用户进程重新加入系统资源占用白名单中；

对于文件系统，安全模块建立文件系统管理表，实时监控查询文件系统读写情况；同时，为用户进程建立文件读写请求白名单、黑名单和灰名单，采用最小特权许可的文件访问请求，针对文件读写请求白名单中的用户进程的文件读写请求给予放行，针对文件读写请求黑名单中的用户进程的文件读写请求禁止运行，针对文件读写请求灰名单中的用户进程的文件读写请求主动问询用户是否放行，直到用户许可后才会放行该文件读写请求；

对于任意一个用户进程首次运行时，安全模块记录该用户进程的文件请求状态和文件访问状态，包括：文件名、读写请求、文件属性、文件大小变动，并不断监控后续该用户进程运行时对文件请求的使用情况，一旦出现异常读写情况，则重新将用户进程放入文件读写请求灰名单中，并提醒用户该用户进程的越权行为，再次请求用户许可；

一旦出现总体文件系统异常情况，安全模块主动冻结系统状态，逐一检查文件系统访问情况，将出现异常文件访问的用户进程从文件读写请求白名单中移除并加入文件读写请求灰名单中，然后恢复系统运行，同时提醒用户这一异常，如果用户许可，再重新将该用户进程从文件读写请求灰名单中移除并加入文件读写请求白名单中；

安全模块针对所有用户进程建立单独的运行用户、创建独立的用户名，并设定专用运行域，专用运行域中记录的内容包括该用户进程可调用的其他用户进程或系统进程、可请求的线程数目、可占用的系统资源类型和数量、可使用的网络访问请求以及可访问文件区域；初始化专用运行域，建立前述用户进程、系统防火墙、系统资源、文件系统4种黑白灰名单，将4种黑白灰名单中的成员首先全部加入至各自对应的灰名单中，后续根据用户对于每一项请求的许可或者禁止情况再加入各自对应的白名单或者黑名单中；情况1：用户进程第一次运行时，将其从用户进程灰名单加入用户进程白名单、从系统资源占用灰名单加入系统资源占用白名单中，然后许可该用户进程运行；如果整个运行过程中，该用户进程不产生网络访问且系统资源占用不超过许可范围，同时不产生文件系统的读写，则不产生其他名

单变化；

情况2：若情况1中的用户进程运行产生了网络访问请求，则记录该用户进程的运行状态，并临时停止该用户进程，同时将该用户进程分别从用户进程白名单移入用户进程灰名单、从系统资源占用白名单移入系统资源占用灰名单；如果用户允许该网络访问请求，则恢复该用户进程的运行状态并将该用户进程分别从用户进程灰名单中移入用户进程白名单、从系统资源占用灰名单移入系统资源占用白名单，并将该网络访问请求加入系统防火墙白名单；如果用户禁止该网络访问请求，则将该用户进程完全停止，并将其分别从用户进程灰名单移入用户进程黑名单、从系统资源占用灰名单移入系统资源占用黑名单；

情况3：若情况1中的用户进程运行产生了文件读写请求，则记录该用户进程的运行状态，并临时停止该用户进程，同时将该用户进程分别从用户进程白名单移入用户进程灰名单、从系统资源占用白名单移入系统资源占用灰名单；如果该用户进程产生过情况2中的网络访问请求，将该用户进程的网络访问请求从系统防火墙白名单移入系统防火墙灰名单；如果用户允许该用户进程进行文件读写，则恢复该用户进程的运行状态，并将用户进程分别从用户进程灰名单移入用户进程白名单、从系统资源占用灰名单移入用户进程白名单；如果该用户进程产生了情况2中的网络访问请求，则将该用户进程的网络访问请求从系统防火墙灰名单移入系统防火墙白名单，并将该用户进程从文件读写请求灰名单移入文件读写请求白名单；如果用户禁止该用户进程进行文件读写，则将该用户进程停止，并将该用户进程分别从用户进程灰名单移入用户进程黑名单、从系统资源占用灰名单移入系统资源占用黑名单，将该用户进程的网络访问请求从系统防火墙灰名单移入系统防火墙黑名单；

情况4：若情况1中的用户进程在情况2中描述的网络访问请求发生并被用户允许后再一次发生网络访问请求，若本次网络访问请求与情况2中的网络访问请求的IP或者端口不同，则将本次该用户进程的网络访问请求从系统防火墙白名单移入系统防火墙灰名单；如果用户允许了该用户进程的本次网络访问请求，将该用户进程的本次网络访问请求从系统防火墙灰名单移入系统防火墙白名单，并允许该用户进程的本次网络访问请求；如果用户禁止了该用户进程的本次网络访问请求，则将该用户进程的本次网络访问请求从系统防火墙灰名单移入系统防火墙黑名单中，并禁止该用户进程的本次网络访问请求；

情况5：若情况1中的用户进程在情况3中描述的文件读写请求发生并被用户允许后再一次发生文件读写请求，若本次文件读写请求与情况3中的文件读写请求不同，则将本次文件读写请求的用户进程加入文件读写请求灰名单；如果用户允许了该用户进程的本次文件读写请求，将本次文件读写请求的用户进程从文件读写请求灰名单移入文件读写请求白名单，并允许该用户进程的本次文件读写请求；如果用户禁止了该用户进程的本次文件读写请求，将本次文件读写请求的用户进程从文件读写请求灰名单移入文件读写请求黑名单，并禁止该用户进程的本次文件读写请求。

3.根据权利要求1所述的面向Linux服务器的主动安全保障方法，其特征在于：安全模块针对系统运行日志和安全日志进行实时审计，建立专用的日志审计管理用户，非审计用户不能删除、修改日志；同时，在系统多个位置建立日志存储区域，实时同步记录完整日志，并采用高级加密标准AES对日志进行加密。

一种面向Linux服务器的主动安全保障方法

技术领域

[0001] 本发明属于一种操作系统安全保护方法。

背景技术

[0002] 目前黑客攻击层出不穷，甚至愈演愈烈，针对网络、操作系统、应用等各个层面的攻击行为，最终目的是为了获取主机中的资源和权限。对用户来说核心是保护操作系统中的数据信息，保障操作系统安全是信息安全的基础。

[0003] 目前的操作系统环境下，使用超级用户登陆可以控制任何应用系统，每个应用系统之间无法做到完全隔离，如果拥有超级用户的权限，就意味着可以在服务器中做任何事情，数据的保密性和完整性根本无法保证，更无法满足信息系统安全要求。同时，如果操作系统中某一应用出现漏洞，就可能导致整个操作系统沦陷，从而让整个服务器数据信息遭到破坏和窃取。

[0004] 当前国内使用的操作系统主要是来自国外(如Windows/Linux/Unix)，系统漏洞一直影响操作系统的安全，而系统漏洞是当初设计操作系统时有意或无意留下的缺陷，黑客根据危害程度不同的漏洞发动攻击，轻则可以获取系统敏感信息，重则可以获取系统控制权限。

[0005] 目前修复漏洞主要的途径是通过更新厂商(如Microsoft、SUN、IBM、HP等)提供的补丁。由于多数商业服务器操作系统不开源，即使知道漏洞产生的原因，也不能对操作系统源码进行修改并重新编译；而开源的Linux操作系统出现漏洞，绝大多数用户也无技术能力进行漏洞修复。所以一旦发现漏洞，只能完全依赖厂商发布补丁，如果在厂商未出补丁或维护人员没有安装补丁这段时间内遭受攻击，操作系统将会面临严重威胁。

[0006] 在国内，当前很多实际的安全操作系统已经被设计和开发出来。其中，最为重要的是基于Flask体系结构的动态策略安全操作系统，以及随后出现的迄今最有影响力的安全操作系统Security Linux和它的实现机制LSM(Linux Security Modle)。

[0007] Flask体系结构由客体管理器和安全服务器组成，优点是将策略实施与策略决策分开。主要目标是提供安全策略的灵活和可变通性，支持动态策略，在一个系统的安全策略需要修改的时候，不需要修改引用监控器等其他关键组件，而只需要更新安全策略服务器中存储的策略即可。

[0008] LSM采取了系统钩子函数的方法来控制系统对核心客体(如进程、节点、打开文件、IPC等)的存取访问。每当系统通过了Linux系统自带的自主访问控制DAC策略检查而试图对一个客体进行访问时，借助于插入到核心代码中的钩子函数来仲裁对该客体的访问。LSM并不为该函数提供具体的实现，仅仅是调用挂在它上面的某个具体安全模块的函数。主体是否能对客体进行访问完全取决于具体的安全模块函数，安全模块根据自己的安全策略来判断访问请求是通过还是拒绝并强制返回一个错误码。

[0009] 现有的安全操作系统在访问控制方面表现不错，但是在系统资源统一管理、进程名单管控、文件最小特权访问、防火墙动态策略更新和进程运行域管理方面存在缺陷：系统

资源管理与操作系统耦合度较低，不能依据资源状态感知系统安全；进程管控依赖钩子函数，没有将安全模块完整内嵌进入系统内核；文件管理采用自主访问控制，没有启用强制访问控制策略；防火墙策略需要手动配置，不能实时更新。

发明内容

[0010] 发明目的：为了克服现有Linux操作系统在系统资源管理、进程管理、防火墙管理、用户管理、文件管理、日志安全审计以及状态监控等方面不足的问题，本发明专利提供了一套采用黑白灰名单制管理的Linux操作系统安全保障方案。

[0011] 技术方案：

[0012] 本发明专利为了解决上述技术问题所采用的总体技术方案如下：通过重新编译内核，将安全保障模块嵌入在Linux系统内核中，在Linux系统内核加载阶段即加载系统安全模块，保证安全模块处于内核级运行状态，不会被其他模块关闭或者卸载。

[0013] 所述安全模块包括安全策略执行模块、安全策略仲裁模块、安全日志记录模块以及自身保护模块，安全策略执行模块将所有用户请求加以拦截并提交安全策略仲裁模块进行仲裁，当安全策略仲裁模块仲裁为允许时，安全策略执行模块放行该请求，当安全策略仲裁模块仲裁为禁止时，安全策略执行模块禁止该请求；用户请求运行结束后，系统先将运行结果返回安全模块，由安全模块记录信息后返回给用户结果；系统运行全过程中，自身保护模块实时检测安全模块运行状态，一旦发现安全模块运行出错立即冻结系统状态，检查并重新运行安全模块，直到安全模块恢复后再恢复系统状态；安全日志记录模块记录系统全部操作日志，实时备份操作日志并加密。

[0014] 进一步的，在本发明中，所述安全模块对用户进程、系统防火墙、系统资源、文件系统均采用建立黑白灰名单进行管理：

[0015] 对于用户进程，安全模块为用户进程建立用户进程白名单、黑名单和灰名单，当系统试图运行某个进程时，安全模块对该用户进程进行仲裁：针对属于进程白名单中的用户进程，安全模块允许系统调用该用户进程，并提醒用户该用户进程已经运行；针对属于进程黑名单中的用户进程，安全模块禁止系统调用该用户进程，并提醒用户该用户进程已经禁止运行；针对属于进程灰名单中的用户进程，安全模块定期询问用户是否允许该用户进程运行，如果用户许可运行，则将其从用户进程灰名单中删除并加入用户进程白名单中，如果用户不允许运行，则将其从用户进程灰名单中删除并加入用户进程黑名单中；

[0016] 对任意一个用户进程，当该用户进程首次运行时，安全模块针对该用户进程记录用户进程的状态，包括：文件读写、进程调用、运行线程和网络访问，后续该用户进程再次运行时，若发现有与首次运行时记录的用户进程的状态不同的行为，则将该用户进程放入用户进程灰名单中，并提醒用户该用户进程的越权行为，并再次请求用户许可；

[0017] 对于系统防火墙，安全模块为用户进程的网络访问请求建立系统防火墙白名单、黑名单和灰名单，设置初始的系统防火墙策略为禁止所有的内外部网络访问请求；当某个用户进程试图访问网络时，安全模块对该网络访问请求进行仲裁：针对属于系统防火墙白名单中的网络访问请求，安全模块允许该网络访问请求，并更新系统防火墙策略，将该网络访问请求所对应的防火墙策略加入系统防火墙策略表，并提醒用户已经放行该网络访问请求，当该网络访问请求结束时，立即再次更新系统防火墙策略，将该网络访问请求所对应的

防火墙策略从系统防火墙策略表中移除；针对属于系统防火墙黑名单中的网络访问请求，安全模块阻止该网络访问请求，并提醒用户已经禁止该网络访问请求；针对属于系统防火墙灰名单中的网络访问请求，安全模块实时询问用户是否许可该网络访问请求，若用户许可，则将该网络访问请求加入系统防火墙白名单，若用户不许可，则将该网络访问请求加入系统防火墙黑名单；

[0018] 对任意一个网络访问请求，当其在首次加入系统防火墙白名单时，安全模块针对网络访问请求记录该网络访问请求的状态，包括：IP地址、端口号、协议以及调用后运行的时间和流量消耗统计，在后续该网络访问请求再次请求时，若发现有与首次加入系统防火墙白名单时所记录的该网络访问请求的状态不同的行为，则重新将网络访问请求放入系统防火墙灰名单中，并提醒用户该网络访问请求的越权行为，再次请求用户许可；

[0019] 对于系统资源，安全模块建立包括CPU占用率、内存占用率、硬盘占用率在内的系统资源表，实时监控查询各类系统资源占用情况；同时，为用户进程建立系统资源占用白名单、黑名单和灰名单，系统资源占用白名单、黑名单和灰名单中分别记录位于其中的用户进程对于各个类型系统资源的最大请求数目，许可范围为每类系统资源的最大请求数目不超过该类系统资源总体的50％，针对系统资源占用白名单中的用户进程所请求的系统资源占用给予放行，针对系统资源占用黑名单中的用户进程所请求的系统资源请求禁止运行，针对系统资源占用灰名单中的用户进程所请求的系统资源请求主动问询用户是否放行；

[0020] 对于任意一个用户进程首次运行时，安全模块记录该用户进程的资源请求状态和资源访问，并不断监控后续该用户进程运行时对系统资源的占用情况，并根据其运行状态动态调整系统资源占用，一旦某次调整前后的可占用系统资源的百分比的差值超过5％，则重新将该用户进程放入系统资源占用灰名单中，并提醒用户该用户进程的越权行为，再次请求用户许可；

[0021] 一旦出现总体系统资源异常情况，则主动冻结系统状态，逐一检查系统资源占用情况，将出现异常资源占用的用户进程从系统资源占用白名单中移除并放入系统资源占用灰名单，然后恢复系统运行，同时提醒用户这一异常，如果用户许可，再将该用户进程重新加入系统资源占用白名单中；

[0022] 对于文件系统，安全模块建立文件系统管理表，实时监控查询文件系统读写情况；同时，为用户进程建立文件读写请求白名单、黑名单和灰名单，采用最小特权许可的文件访问请求，针对文件读写请求白名单中的用户进程的文件读写请求给予放行，针对文件读写请求黑名单中的用户进程的文件读写请求禁止运行，针对文件读写请求灰名单中的用户进程的文件读写请求主动问询用户是否放行，直到用户许可后才会放行该文件读写请求；

[0023] 对于任意一个用户进程首次运行时，安全模块记录该用户进程的文件请求状态和文件访问状态，包括：文件名、读写请求、文件属性、文件大小变动，并不断监控后续该用户进程运行时对文件请求的使用情况，一旦出现异常读写情况，则重新将用户进程放入文件读写请求灰名单中，并提醒用户该用户进程的越权行为，再次请求用户许可；

[0024] 一旦出现总体文件系统异常情况，安全模块主动冻结系统状态，逐一检查文件系统访问情况，将出现异常文件访问的用户进程从文件读写请求白名单中移除并加入文件读写请求灰名单中，然后恢复系统运行，同时提醒用户这一异常，如果用户许可，再重新将该用户进程从文件读写请求灰名单中移除并加入文件读写请求白名单中；

[0025] 安全模块针对所有用户进程建立单独的运行用户、创建独立的用户名，并设定专用运行域，专用运行域中记录的内容包括该用户进程可调用的其他用户进程或系统进程、可请求的线程数目、可占用的系统资源类型和数量、可使用的网络访问请求以及可访问文件区域；初始化专用运行域，建立前述用户进程、系统防火墙、系统资源、文件系统4种黑白灰名单，将4种黑白灰名单中的成员首先全部加入至各自对应的灰名单中，后续根据用户对于每一项请求的许可或者禁止情况再加入各自对应的白名单或者黑名单中；

[0026] 情况1：用户进程第一次运行时，将其从用户进程灰名单加入用户进程白名单、从系统资源占用灰名单加入系统资源占用白名单中，然后许可该用户进程运行；如果整个运行过程中，该用户进程不产生网络访问且系统资源占用不超过许可范围，同时不产生文件系统的读写，则不产生其他名单变化；

[0027] 情况2：若情况1中的用户进程运行产生了网络访问请求，则记录该用户进程的运行状态，并临时停止该用户进程，同时将该用户进程分别从用户进程白名单移入用户进程灰名单、从系统资源占用白名单移入系统资源占用灰名单；如果用户允许该网络访问请求，则恢复该用户进程的运行状态并将该用户进程分别从用户进程灰名单中移入用户进程白名单、从系统资源占用灰名单移入系统资源占用白名单，并将该网络访问请求加入系统防火墙白名单；如果用户禁止该网络访问请求，则将该用户进程完全停止，并将其分别从用户进程灰名单移入用户进程黑名单、从系统资源占用灰名单移入系统资源占用黑名单；

[0028] 情况3：若情况1中的用户进程运行产生了文件读写请求，则记录该用户进程的运行状态，并临时停止该用户进程，同时将该用户进程分别从用户进程白名单移入用户进程灰名单、从系统资源占用白名单移入系统资源占用灰名单；如果该用户进程产生过情况2中的网络访问请求，将该用户进程的网络访问请求从系统防火墙白名单移入系统防火墙灰名单；如果用户允许该用户进程进行文件读写，则恢复该用户进程的运行状态，并将用户进程分别从用户进程灰名单移入用户进程白名单、从系统资源占用灰名单移入用户进程白名单；如果该用户进程产生了情况2中的网络访问请求，则将该用户进程的网络访问请求从系统防火墙灰名单移入系统防火墙白名单，并将该用户进程从文件读写请求灰名单移入文件读写请求白名单；如果用户禁止该用户进程进行文件读写，则将该用户进程停止，并将该用户进程分别从用户进程灰名单移入用户进程黑名单、从系统资源占用灰名单移入系统资源占用黑名单，将该用户进程的网络访问请求从系统防火墙灰名单移入系统防火墙黑名单；

[0029] 情况4：若情况1中的用户进程在情况2中描述的网络访问请求发生并被用户允许后再一次发生网络访问请求，若本次网络访问请求与情况2中的网络访问请求的IP或者端口不同，则将本次该用户进程的网络访问请求从系统防火墙白名单移入系统防火墙灰名单；如果用户允许了该用户进程的本次网络访问请求，将该用户进程的本次网络访问请求从系统防火墙灰名单移入系统防火墙白名单，并允许该用户进程的本次网络访问请求；如果用户禁止了该用户进程的本次网络访问请求，则将该用户进程的本次网络访问请求从系统防火墙灰名单移入系统防火墙黑名单中，并禁止该用户进程的本次网络访问请求；

[0030] 情况5：若情况1中的用户进程在情况3中描述的文件读写请求发生并被用户允许后再一次发生文件读写请求，若本次文件读写请求与情况3中的文件读写请求不同，则将本次文件读写请求的用户进程加入文件读写请求灰名单；如果用户允许了该用户进程的本次文件读写请求，将本次文件读写请求的用户进程从文件读写请求灰名单移入文件读写请求

白名单，并允许该用户进程的本次文件读写请求；如果用户禁止了该用户进程的本次文件读写请求，将本次文件读写请求的用户进程从文件读写请求灰名单移入文件读写请求黑名单，并禁止该用户进程的本次文件读写请求。

[0031] 进一步的，在本发明中，安全模块针对系统运行日志和安全日志进行实时审计，建立专用的日志审计管理用户，非审计用户不能删除、修改日志；同时，在系统多个位置建立日志存储区域，实时同步记录完整日志，并采用高级加密标准AES对日志进行加密。

[0032] 有益效果：

[0033] 本发明的面向Linux操作系统的主动安全保障方法作为可以独立运行的安全模块将嵌入系统内核，与操作系统紧密结合，克服现有Linux操作系统在系统资源管理、进程管理、防火墙管理、用户管理、文件管理、日志安全审计以及状态监控等方面不足的问题，采用多模块工作方式，将策略执行、策略仲裁、策略保存、日志记录相互独立，确保系统正常工作；具体优点如下：

[0034] 本发明专利在系统资源管理方面，改进了原有Linux系统不能统一管理系统资源的缺陷，采用内核嵌入模块方式进行实时系统资源接口查询和管理，能够实时检测并统一管理系统资源。

[0035] 本发明专利在进程管理方面，改进了原有Linux系统不能实时检测并分析进程的缺陷，能够实时检测并设计了进程黑白灰名单机制，针对进程行为进行分析，能够方便安全保证系统进程安全；

[0036] 本发明专利在防火墙管理方面，改进了原有Linux系统不能够实时动态更新策略的缺陷，能够实时动态更新系统防火墙策略并针对系统进程设计防火墙黑白名单进行分析，保证操作系统网络安全。

[0037] 本发明专利在用户管理方面，改进了原有Linux系统用户管理策略不能动态改进的缺陷，将所有的用户进程建立不同的用户和运行域，保证所有的用户进程运行在单独的用户名下并设立独立的运行域，保证用户权限安全和用户隐私安全；

[0038] 本发明专利在文件管理方面，改进了原有Linux系统文件访问时没有专门的用户访问权限管理机制的缺陷，采用最小权限机制实现安全文件访问；

[0039] 本发明专利在日志安全审计方面，改进了原有Linux系统仅能记录日志，没有安全分析，没有日志安全保障的缺陷，能够实现安全日志独立审计和独立存储，对系统日志进行安全分析，查看各类安全事件。

附图说明

[0040] 图1为本发明的各部分之间结构示意图；

[0041] 图2为本发明的流程示意图。

具体实施方式

[0042] 下面结合附图对本发明做更进一步的解释。

[0043] 本发明的安全保障方法提供了一种全局安全策略，主要包括以下9个方面：

[0044] 1、重新编译内核，将安全保障模块嵌入在Linux内核中。

[0045] 2、在Linux系统内核加载阶段即加载系统安全模块。

[0046] 3、安全策略执行模块将所有用户请求(包括进程执行、网络访问、文件读写等)加以拦截并提交安全策略仲裁进行判断。

[0047] 4、策略仲裁为白名单项目时,执行模块放行该请求。

[0048] 5、策略仲裁为黑名单项目时,执行模块会禁止该请求。

[0049] 6、策略仲裁为灰名单项目时,执行模块会禁止该请求,然后请求用户是否允许该请求。如果用户许可,加入白名单,如果用户禁止,加入黑名单。

[0050] 7、运行结束后,系统将运行结果返回安全模块,由安全模块记录信息后返回给用户结果。

[0051] 8、系统运行全过程中,自身保护模块实时检测安全模块运行状态,一旦发现安全模块运行出错会立即冻结系统状态,检查并重新运行安全模块功能,直到安全模块恢复后恢复系统状态。

[0052] 9、系统运行全过程中,安全日志记录模块记录系统全部操作日志,多个位置实时备份日志并加密。

[0053] 具体来说,所述安全模块对用户进程、系统防火墙、系统资源、文件系统均采用建立黑白灰名单进行管理:

[0054] 对于用户进程,安全模块为用户进程建立用户进程白名单、黑名单和灰名单,当系统试图运行某个进程时,安全模块对该用户进程进行仲裁:针对属于进程白名单中的用户进程,安全模块允许系统调用该用户进程,并提醒用户该用户进程已经运行;针对属于进程黑名单中的用户进程,安全模块禁止系统调用该用户进程,并提醒用户该用户进程已经禁止运行;针对属于进程灰名单中的用户进程,安全模块定期询问用户是否允许该用户进程运行,如果用户许可运行,则将其从用户进程灰名单中删除并加入用户进程白名单中,如果用户不允许运行,则将其从用户进程灰名单中删除并加入用户进程黑名单中;

[0055] 对任意一个用户进程,当该用户进程首次运行时,安全模块针对该用户进程记录用户进程的状态,包括:文件读写、进程调用、运行线程和网络访问,后续该用户进程再次运行时,若发现有与首次运行时记录的用户进程的状态不同的行为,则将该用户进程放入用户进程灰名单中,并提醒用户该用户进程的越权行为,并再次请求用户许可;

[0056] 对于系统防火墙,安全模块为用户进程的网络访问请求建立系统防火墙白名单、黑名单和灰名单,设置初始的系统防火墙策略为禁止所有的内外部网络访问请求;当某个用户进程试图访问网络时,安全模块对该网络访问请求进行仲裁:针对属于系统防火墙白名单中的网络访问请求,安全模块允许该网络访问请求,并更新系统防火墙策略,将该网络访问请求所对应的防火墙策略加入系统防火墙策略表,并提醒用户已经放行该网络访问请求,当该网络访问请求结束时,立即再次更新系统防火墙策略,将该网络访问请求所对应的防火墙策略从系统防火墙策略表中移除;针对属于系统防火墙黑名单中的网络访问请求,安全模块阻止该网络访问请求,并提醒用户已经禁止该网络访问请求;针对属于系统防火墙灰名单中的网络访问请求,安全模块实时询问用户是否许可该网络访问请求,若用户许可,则将该网络访问请求加入系统防火墙白名单,若用户不许可,则将该网络访问请求加入系统防火墙黑名单;

[0057] 对任意一个网络访问请求,当其在首次加入系统防火墙白名单时,安全模块针对网络访问请求记录该网络访问请求的状态,包括:IP地址、端口号、协议以及调用后运行的

时间和流量消耗统计，在后续该网络访问请求再次请求时，若发现有与首次加入系统防火墙白名单时所记录的该网络访问请求的状态不同的行为，则重新将网络访问请求放入系统防火墙灰名单中，并提醒用户该网络访问请求的越权行为，再次请求用户许可；

[0058] 对于系统资源，安全模块建立包括CPU占用率、内存占用率、硬盘占用率在内的系统资源表，实时监控查询各类系统资源占用情况；同时，为用户进程建立系统资源占用白名单、黑名单和灰名单，系统资源占用白名单、黑名单和灰名单中分别记录位于其中的用户进程对于各个类型系统资源的最大请求数目，许可范围为每类系统资源的最大请求数目不超过该类系统资源总体的50％，针对系统资源占用白名单中的用户进程所请求的系统资源占用给予放行，针对系统资源占用黑名单中的用户进程所请求的系统资源请求禁止运行，针对系统资源占用灰名单中的用户进程所请求的系统资源请求主动问询用户是否放行；

[0059] 对于任意一个用户进程首次运行时，安全模块记录该用户进程的资源请求状态和资源访问，包括CPU占用率、内存占用率、硬盘占用率，并不断监控后续该用户进程运行时对系统资源的占用情况，并根据其运行状态动态调整系统资源占用，一旦某次调整前后的可占用系统资源的百分比的差值超过5％，则重新将该用户进程放入系统资源占用灰名单中，并提醒用户该用户进程的越权行为，再次请求用户许可；

[0060] 一旦出现总体系统资源异常情况，则主动冻结系统状态，逐一检查系统资源占用情况，将出现异常资源占用的用户进程从系统资源占用白名单中移除并放入系统资源占用灰名单，然后恢复系统运行，同时提醒用户这一异常，如果用户许可，再将该用户进程重新加入系统资源占用白名单中；

[0061] 对于文件系统，安全模块建立文件系统管理表，实时监控查询文件系统读写情况；同时，为用户进程建立文件读写请求白名单、黑名单和灰名单，采用最小特权许可的文件访问请求，针对文件读写请求白名单中的用户进程的文件读写请求给予放行，针对文件读写请求黑名单中的用户进程的文件读写请求禁止运行，针对文件读写请求灰名单中的用户进程的文件读写请求主动问询用户是否放行，直到用户许可后才会放行该文件读写请求；

[0062] 对于任意一个用户进程首次运行时，安全模块记录该用户进程的文件请求状态和文件访问状态，包括：文件名、读写请求、文件属性、文件大小变动，并不断监控后续该用户进程运行时对文件请求的使用情况，一旦出现异常读写情况，则重新将用户进程放入文件读写请求灰名单中，并提醒用户该用户进程的越权行为，再次请求用户许可；

[0063] 一旦出现总体文件系统异常情况，安全模块主动冻结系统状态，逐一检查文件系统访问情况，将出现异常文件访问的用户进程从文件读写请求白名单中移除并加入文件读写请求灰名单中，然后恢复系统运行，同时提醒用户这一异常，如果用户许可，再重新将该用户进程从文件读写请求灰名单中移除并加入文件读写请求白名单中；

[0064] 安全模块针对所有用户进程建立单独的运行用户、创建独立的用户名，并设定专用运行域，专用运行域中记录的内容包括该用户进程可调用的其他用户进程或系统进程、可请求的线程数目、可占用的系统资源类型和数量、可使用的网络访问请求以及可访问文件区域；初始化专用运行域，建立前述用户进程、系统防火墙、系统资源、文件系统4种黑白灰名单，将4种黑白灰名单中的成员首先全部加入至各自对应的灰名单中，后续根据用户对于每一项请求的许可或者禁止情况再加入各自对应的白名单或者黑名单中；

[0065] 情况1：用户进程第一次运行时，将其从用户进程灰名单加入用户进程白名单、从

系统资源占用灰名单加入系统资源占用白名单中，然后许可该用户进程运行；如果整个运行过程中，该用户进程不产生网络访问且系统资源占用不超过许可范围，同时不产生文件系统的读写，则不产生其他名单变化；

[0066] 情况2：若情况1中的用户进程运行产生了网络访问请求，则记录该用户进程的运行状态，包括：IP地址、端口号，协议，以及调用后运行的时间和流量消耗统计，并临时停止该用户进程，同时将该用户进程分别从用户进程白名单移入用户进程灰名单、从系统资源占用白名单移入系统资源占用灰名单；如果用户允许该网络访问请求，则恢复该用户进程的运行状态并将该用户进程分别从用户进程灰名单中移入用户进程白名单、从系统资源占用灰名单移入系统资源占用白名单，并将该网络访问请求加入系统防火墙白名单；如果用户禁止该网络访问请求，则将该用户进程完全停止，并将其分别从用户进程灰名单移入用户进程黑名单、从系统资源占用灰名单移入系统资源占用黑名单；

[0067] 情况3：若情况1中的用户进程运行产生了文件读写请求，则记录该用户进程的运行状态，包括：文件名、读写请求、文件属性、文件大小变动，并临时停止该用户进程，同时将该用户进程分别从用户进程白名单移入用户进程灰名单、从系统资源占用白名单移入系统资源占用灰名单；如果该用户进程产生过情况2中的网络访问请求，将该用户进程的网络访问请求从系统防火墙白名单移入系统防火墙灰名单；如果用户允许该用户进程进行文件读写，则恢复该用户进程的运行状态，并将用户进程分别从用户进程灰名单移入用户进程白名单、从系统资源占用灰名单移入用户进程白名单；如果该用户进程产生了情况2中的网络访问请求，则将该用户进程的网络访问请求从系统防火墙灰名单移入系统防火墙白名单，并将该用户进程从文件读写请求灰名单移入文件读写请求白名单；如果用户禁止该用户进程进行文件读写，则将该用户进程停止，并将该用户进程分别从用户进程灰名单移入用户进程黑名单、从系统资源占用灰名单移入系统资源占用黑名单，将该用户进程的网络访问请求从系统防火墙灰名单移入系统防火墙黑名单；

[0068] 情况4：若情况1中的用户进程在情况2中描述的网络访问请求发生并被用户允许后再一次发生网络访问请求，若本次网络访问请求与情况2中的网络访问请求的IP或者端口不同，则将本次该用户进程的网络访问请求从系统防火墙白名单移入系统防火墙灰名单；如果用户允许了该用户进程的本次网络访问请求，将该用户进程的本次网络访问请求从系统防火墙灰名单移入系统防火墙白名单，并允许该用户进程的本次网络访问请求；如果用户禁止了该用户进程的本次网络访问请求，则将该用户进程的本次网络访问请求从系统防火墙灰名单移入系统防火墙黑名单中，并禁止该用户进程的本次网络访问请求；

[0069] 情况5：若情况1中的用户进程在情况3中描述的文件读写请求发生并被用户允许后再一次发生文件读写请求，若本次文件读写请求与情况3中的文件读写请求不同，则将本次文件读写请求的用户进程加入文件读写请求灰名单；如果用户允许了该用户进程的本次文件读写请求，将本次文件读写请求的用户进程从文件读写请求灰名单移入文件读写请求白名单，并允许该用户进程的本次文件读写请求；如果用户禁止了该用户进程的本次文件读写请求，将本次文件读写请求的用户进程从文件读写请求灰名单移入文件读写请求黑名单，并禁止该用户进程的本次文件读写请求。

[0070] 整个运行过程中，安全模块针对系统运行日志和安全日志进行实时审计，包括进程情况、防火墙情况、文件访问情况、系统资源情况、用户和角色、安全域变化等，建立专用

的日志审计管理用户，非审计用户不能删除、修改日志；同时，在系统多个位置建立日志存储区域，实时同步记录完整日志，并采用高级加密标准AES对日志进行加密。

[0071] 根据上述实施例，可以更好的理解本发明。然而，本领域的技术人员容易理解，实施例所描述的具体的物料配比、工艺条件及其结果仅用于说明本发明，而不应当也不会限制权利要求书中所详细描述的本发明。

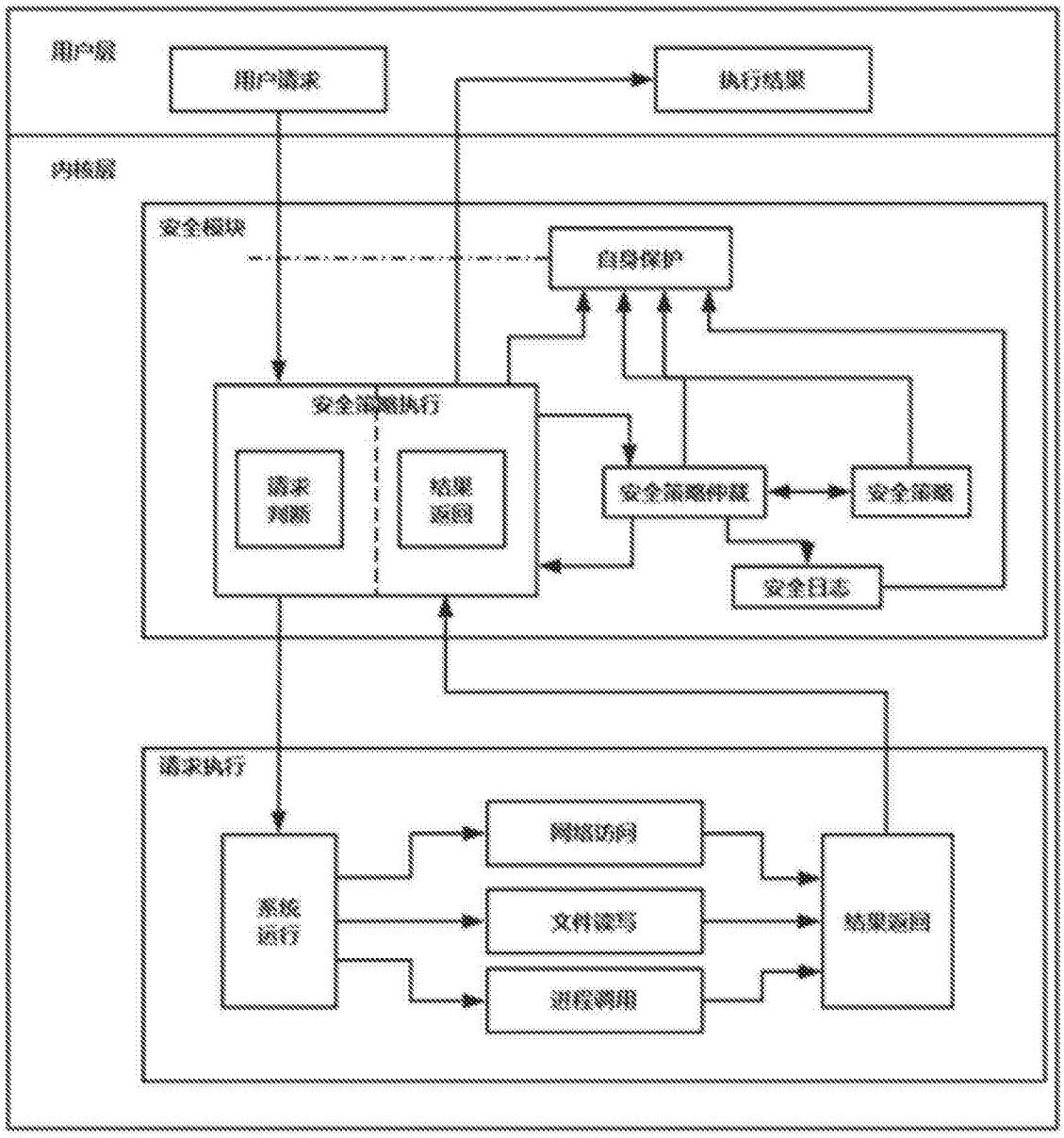


图1

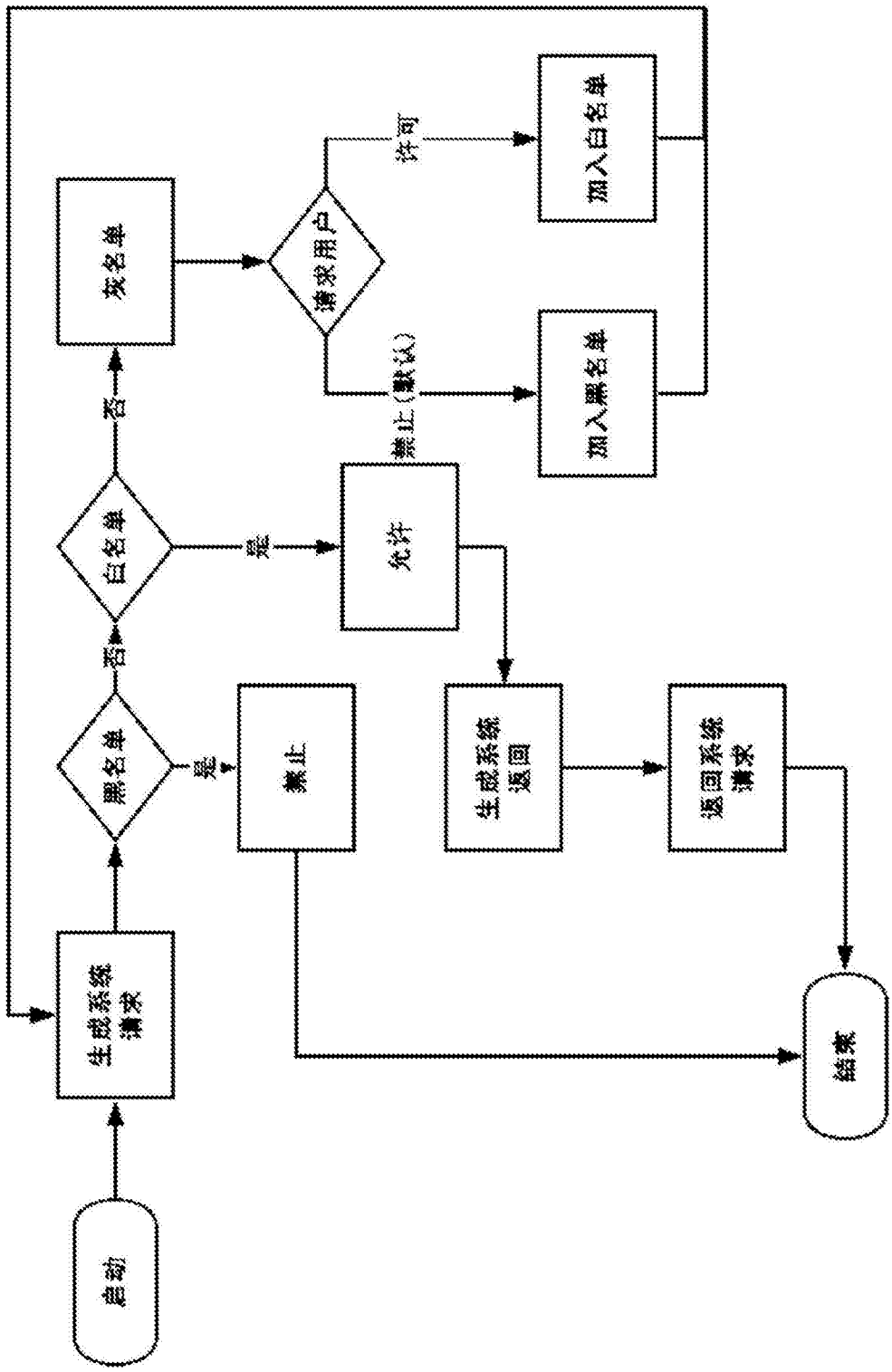

启动
生成系统请求
黑名单
是
否
禁止
白名单
是
否
允许
禁止(默认)
请求用户
许可
发名单
加入白名单
加入黑名单
生成系统返回
返回系统请求
结束

图2