(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104318156 B
(45)授权公告日 2017.07.25

(21)申请号 201410566662.5

(22)申请日 2014.10.22

(65)同一申请的已公布的文献号
申请公布号 CN 104318156 A

(43)申请公布日 2015.01.28

(73)专利权人 上海斐讯数据通信技术有限公司
地址 201616 上海市松江区思贤路3666号

(72)发明人 王赞 朱为朋 朱军

(74)专利代理机构 杭州千克知识产权代理有限公司 33246
代理人 周希良

(51)Int.Cl.
G06F 21/52(2013.01)

审查员 张文波

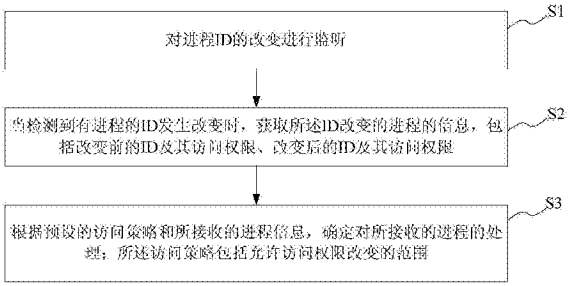
权利要求书1页 说明书5页 附图1页

(54)发明名称

一种进程访问安全方法及系统

(57)摘要

本发明提供一种进程访问安全方法及系统。所述进程访问安全方法包括:对进程ID的改变进行监听;当检测到有进程的ID发生改变时,获取所述ID改变的进程的信息,包括改变前的ID及其访问权限、改变后的ID及其访问权限;根据预设的访问策略和所述发生ID改变的进程信息,确定对所述发生ID改变的进程的处理;所述访问策略包括允许访问权限改变的范围。本发明的技术方案能够防止与检测出进程的不正当提权行为,保护系统不受恶意程序通过提高进程访问权限来获取、修改、泄露系统中的重要资源和数据,从而大大提高了系统的安全性。



CN 104318156 B

1.一种进程访问安全系统，其特征在于，所述进程访问安全系统包括可信模块和进程访问控制模块，其中：

可信模块，包括可信服务单元；所述可信服务单元用于为所述进程访问控制模块提供可信的软件服务；

进程访问控制模块，包括进程检测控制单元与访问策略管理单元；

所述进程检测控制单元用于对进程ID的改变进行监听，当检测到有进程的ID发生改变时，获取所述ID改变的进程的信息，包括改变前的ID及其访问权限、改变后的ID及其访问权限，将所述ID改变的进程的信息发送给所述访问策略管理单元；所述ID包括UID或EUID中的任一种；

所述访问策略管理单元，与所述可信服务单元相连，用于根据预设的访问策略和所述发生ID改变的进程信息，确定对所述发生ID改变的进程的处理；所述访问策略包括允许访问权限改变的范围。

2.根据权利要求1所述的进程访问安全系统，其特征在于：所述可信模块还包括完整性度量单元，所述完整性度量单元用于对所述进程访问控制模块进行完整性验证。

3.根据权利要求1所述的进程访问安全系统，其特征在于：所述可信模块基于TrustZone技术实现。

4.根据权利要求1所述的进程访问安全系统，其特征在于：所述对所述发生ID改变的进程的处理包括：当所述发生ID改变的进程信息中的所述改变前的进程访问权限小于所述改变后的进程访问权限且不在所述访问策略允许范围时，清除所述发生ID改变的进程。

5.根据权利要求1所述的进程访问安全系统，其特征在于：所述访问控制控制模块还包括访问策略修改模块，所述访问策略修改模块用于接收策略控制命令，根据所述策略控制命令修改所述访问策略。

6.根据权利要求5所述的进程访问安全系统，其特征在于：所述策略控制命令包括通过所述可信服务单元发出的策略控制命令。

7.一种进程访问安全方法，其特征在于：所述进程访问安全方法包括：

对进程ID的改变进行监听；

当检测到有进程的ID发生改变时，获取所述ID改变的进程的信息，包括改变前的ID及其访问权限、改变后的ID及其访问权限；所述ID包括UID或EUID中的任一种；

根据预设的访问策略和所述发生ID改变的进程信息，确定对所述发生ID改变的进程的处理；所述访问策略包括允许访问权限改变的范围。

8.根据权利要求7所述的进程访问安全方法，其特征在于：所述对所述发生ID改变的进程的处理包括：当所述发生ID改变的进程信息中的所述改变前的进程访问权限小于所述改变后的进程访问权限且不在所述访问策略允许范围时，清除所述发生ID改变的进程。

9.根据权利要求7所述的进程访问安全方法，其特征在于：所述方法还包括：接收策略控制命令，根据所述策略控制命令修改所述访问策略。

10.根据权利要求7所述的进程访问安全方法，其特征在于：所述进程访问安全方法是基于TrustZone技术构建的可信服务实现的。

一种进程访问安全方法及系统

技术领域

[0001] 本发明涉及一种计算机安全技术，特别是涉及一种进程访问安全方法及系统。

背景技术

[0002] 在计算机系统中，所有的应用程序都是以进程的方式运行的，进程在运行时会根据应用程序的需要访问相应的资源。不同的应用程序在运行时可以有不同的资源访问需求，访问权限，相应的，进程在运行时可以有不同的访问权限。通常，进程的访问权限是在进程创建时确定的，但在进程运行时，也可以动态的改变进程的访问权限。恶意程序也可以通过改变进程的访问权限来获取或操作更多的资源。

[0003] 由于通过改变进程的访问权限来获得对系统更高的访问权限的恶意程序的不断增加，计算机系统的安全受到越来越严重的威胁。当恶意程序获得足够的访问权限时，现有的系统安全防护机制无法阻止恶意程序访问、修改、泄漏系统中的重要资源和数据，该系统安全带来巨大的威胁。在采用Android系统的移动终端中这种威胁尤其明显。特定的情况下，病毒或木马等恶意程序很容易利用系统中的漏洞获取系统超级用户权限，从而完全控制移动终端，以致于在移动终端上偷话费、窃取短信、通信录等用户隐私甚至监听通话，危害极大。

[0004] 鉴于此，如何在移动终端的系统中保证进程访问权限的安全性，从而保护系统安全就成为本领域技术人员亟待解决的问题。

发明内容

[0005] 鉴于以上所述现有技术的缺点，本发明的目的在于提供一种进程访问安全方法及系统，用于解决现有技术中计算机操作系统的进程访问权限安全防范的问题。

[0006] 为实现上述目的及其他相关目的，本发明提供一种进程访问安全系统，所述进程访问安全系统包括可信模块和进程访问控制模块，其中：可信模块，包括可信服务单元；所述可信服务单元用于为所述进程访问控制模块提供可信的软件服务；进程访问控制模块，包括进程检测控制单元与访问策略管理单元；所述进程检测控制单元用于对进程ID的改变进行监听，当检测到有进程的ID发生改变时，获取所述ID改变的进程的信息，包括改变前的ID及其访问权限、改变后的ID及其访问权限，将所述ID改变的进程的信息发送给所述访问策略管理单元；所述访问策略管理单元，与所述可信服务单元相连，用于根据预设的访问策略和所述发生ID改变的进程信息，确定对所述发生ID改变的进程的处理；所述访问策略包括允许访问权限改变的范围。

[0007] 可选地，所述可信模块还包括完整性度量单元，所述完整性度量单元用于对所述进程访问控制模块进行完整性验证；

[0008] 可选地，所述ID包括UID或EUID中的任一种。

[0009] 可选地，所述可信模块基于TrustZone技术实现。

[0010] 可选地，所述对所述发生ID改变的进程的处理包括：当所述发生ID改变的进程信

息中的所述改变前的进程访问权限小于所述改变后的进程访问权限且不在所述访问策略允许范围时，清除所述发生ID改变的进程。

[0011] 可选地，所述访问控制控制模块还包括访问策略修改模块，所述访问策略修改模块用于接收策略控制命令，根据所述策略控制命令修改所述访问策略。

[0012] 可选地，所述策略控制命令包括通过所述可信服务单元发出的策略控制命令。

[0013] 本发明还提供一种进程访问安全方法，所述进程访问安全方法包括：对进程ID的改变进行监听；当检测到有进程的ID发生改变时，获取所述ID改变的进程的信息，包括改变前的ID及其访问权限、改变后的ID及其访问权限；根据预设的访问策略和所述发生ID改变的进程信息，确定对所述发生ID改变的进程的处理；所述访问策略包括允许访问权限改变的范围。

[0014] 可选地，所述ID包括UID或EUID中的任一种。

[0015] 可选地，所述对所述发生ID改变的进程的处理包括：当所述发生ID改变的进程信息中的所述改变前的进程访问权限小于所述改变后的进程访问权限且不在所述访问策略允许范围时，清除所述发生ID改变的进程。

[0016] 可选地，所述方法还包括：接收策略控制命令，根据所述策略控制命令修改所述访问策略。

[0017] 可选地，所述进程访问安全方法是基于TrustZone技术构建的可信服务实现的。

[0018] 如上所述，本发明的一种进程访问安全方法及系统，具有以下有益效果：能够防止与检测出进程的不正当提权行为，保护系统不受恶意程序通过提高进程访问权限来获取、修改、泄露系统中的重要资源和数据，从而大大提高了系统的安全性。

附图说明

[0019] 图1显示为本发明一种进程访问安全系统的一实施例的模块示意图。

[0020] 图2显示为本发明的一种进程访问安全方法的一实施例的方法流程示意图。

[0021] 元件标号说明

[0022]	1	进程访问安全系统
[0023]	11	可信模块
[0024]	111	可信服务单元
[0025]	112	完整性度量单元
[0026]	12	进程访问控制模块
[0027]	121	进程检测控制单元
[0028]	122	访问策略管理单元
[0029]	123	访问策略修改单元
[0030]	S1～S3	步骤

具体实施方式

[0031] 以下通过特定的具体实例说明本发明的实施方式，本领域技术人员可由本说明书所揭露的内容轻易地了解本发明的其他优点与功效。本发明还可以通过另外不同的具体实施方式加以实施或应用，本说明书中的各项细节也可以基于不同观点与应用，在没有背离

本发明的精神下进行各种修饰或改变。

[0032] 需要说明的是，本实施例中所提供的图示仅以示意方式说明本发明的基本构想，遂图式中仅显示与本发明中有关的组件而非按照实际实施时的组件数目、形状及尺寸绘制，其实际实施时各组件的型态、数量及比例可为一种随意的改变，且其组件布局型态也可能更为复杂。

[0033] 本发明提供一种进程访问安全系统。如图1所示，在一个实施例中，所述进程访问安全系统1包括可信模块11和进程检测控制模块12。其中：

[0034] 可信模块11，包括可信服务单元111；所述可信服务单元111用于为所述进程访问控制模块12提供可信的软件服务。在一个实施例中，所述可信模块11基于可信硬件构建，所述可信硬件基于TrustZone技术。TrustZone(TM)技术出现在ARMv6KZ以及较晚期的应用核心架构中。它提供了一种低成本的方案，针对系统单芯片(SoC)内加入专属的安全核心，由硬件建构的存取控制方式支援两颗虚拟的处理器。这个方式可使得应用程式核心能够在两个状态之间切换(通常改称为领域(worlds)以避免和其他功能领域的名称混淆)，在此架构下可以避免资讯从较可信的核心领域泄漏至较不安全的领域。这种内核领域之间的切换通常是与处理器其他功能完全无关联性(orthogonal)，因此各个领域可以各自独立运作但却仍能使用同一颗内核。内存和周边装置也可因此得知目前内核运作的领域为何，并能针对这个方式来提供对装置的机密和编码进行存取控制。典型的TrustZone技术应用是要能在一个缺乏安全性的环境下完整地执行操作系统，并在可信的环境下能有更少的安全性的编码。

[0035] 进程访问控制模块12，包括进程检测控制单元121，访问策略管理单元122。所述进程检测控制单元121用于对进程ID的改变进行监听，当检测到有进程的ID发生改变时，获取所述ID改变的进程的信息，包括改变前的ID及其访问权限、改变后的ID及其访问权限，将所述ID改变的进程的信息发送给所述访问策略管理单元122。在一个实施例中，所述进程ID(Identity，标识号码)为进程的UID(用户ID)，在另一个实施例中，所述进程ID为进程的EUID(有效用户ID)。当进程ID改变时，进程的访问权限也常常会发生改变，此时，进程检测控制单元121获取发生进程ID改变的进程的信息，包括发生进程ID改变前的进程ID以及进程访问权限，发生进程ID改变后的进程ID以及进程访问权限。

[0036] 程序检测控制单元121对进程的监听是以一定的周期对系统运行的所有进程进行扫描，并记录进程的所有信息，包括进程的ID、用户信息等。当下一个周期到来时，程序检测控制单元121会继续扫描全部进程信息，并与上次的进程扫描结果进行比较。此时，如果比较结果有新增root用户进程，则程序检测控制单元121会对该进程做进一步处理。如果比较结果有某一进程的ID发生变化，且该进程的用户已变为root用户，则程序检测控制单元121会对该进程做进一步处理。如果结果无异常则不做任何处理。

[0037] 上述的记录进程信息不仅限于进程的ID，用户，还包括该进程的启动命令，启动时间、父进程等详细信息。前后2次扫描结果，均以进程ID进行排序，找到新增的进程ID和消失的进程ID。如果没有，结果无异常。如果有，继续。对新增进程和消失进程信息进行比较，如果某一进程的启动命令、启动时间、父进程等信息前后均无变化，仅进程ID有改变，则记为该进程ID发生变化。进一步，如果该进程的用户信息也发生改变，且变为root用户，则对该进程做进一步处理。其余新增的进程，如果用户信息不是root用户，不做处理。如果是root

用户，则对该进程做进一步处理。

[0038] 访问策略管理单元122，与所述进程检测控制单元121相连，用于根据预设的访问策略和所述发生ID改变的进程信息，确定对所述发生ID改变的进程的处理；所述访问策略包括允许访问权限改变的范围。具体地，所述访问策略包括了系统允许访问权限改变的范围，如系统允许的情况：改变前的进程访问权限为能够访问哪些资源，改变后的进程访问权限为能够访问哪些资源。在一个实施例中，所述对所述发生ID改变的进程的处理包括：当所述发生ID改变的进程信息中的所述改变前的进程访问权限小于所述改变后的进程访问权限且不在所述访问策略允许范围时，清除所述发生ID改变的进程。如果所述发生ID改变的进程信息中所述改变前的进程访问权限小于所述改变后的进程访问权限，当该改变在访问策略允许范围内，即系统允许这种情况发生，此时，不清除所述发生ID改变的进程。如果所述发生ID改变的进程信息中所述改变前的进程访问权限大于或等于所述改变后的进程访问权限，不清除所述发生ID改变的进程。

[0039] 访问策略管理单元122执行的访问策略为在系统启动时，根据预设的系统规则，每一个进程对应的权限访问列表，此列表为预置的，用于限制系统进程的资源访问。比如：A进程在系统设计时，仅可以访问蓝牙设备，不可以访问wifi设备。那么，A进程的权限列表中会有此访问规则。如果A进程有超越了权限列表所规定的范围，则视此进程为越权进程。权限列表范围不仅限于对设备资源的访问，也包括对用户敏感数据访问的限制。

[0040] 在一个实施例中，所述可信模块11还包括完整性度量单元112，所述完整性度量单元112用于对所述进程访问控制模块12进行完整性验证。在一个实施例中，所述完整性度量程序112主要是在系统启动时对进程访问控制模块12的完整性做校验，包括采用hash算法或其他算法，对即将要加载的进程访问控制模块进行校验。当采用hash算法时，如果hash与初始值不一致，则说明系统可能被破坏且出现严重问题，此时系统将停止运行。如果一致则继续。

[0041] 在一个实施例中，所述访问控制控制模块12还包括访问策略修改模块123，所述访问策略修改模块123用于接收策略控制命令，根据所述策略控制命令修改所述访问策略。在一个实施例中，所述策略控制命令包括通过所述可信服务单元112发出的策略控制命令。所述策略控制命令可以包括用户或应用程序通过可信服务单元112提供的接口发出。当所述访问策略修改模块123接收到所述策略控制命令时，将根据所述策略控制命令修改所述访问策略。即修改系统允许的进程访问权限改变的范围。

[0042] 本发明还提供一种进程访问安全方法。在一个实施例中，所述进程访问安全方法是基于TrustZone技术构建的可信服务实现的。如图2所示，在一个实施例中，所述进程访问安全方法包括：

[0043] 步骤S1，对进程ID的改变进行监听。具体地，所述进程ID包括进程UID(用户ID)及EUID(有效用户ID)中的一种。在一个实施例中，所述对进程ID的改变进行监听是基于TrustZone技术构建的可信服务实现的。

[0044] 步骤S2，当检测到有进程的ID发生改变时，获取所述ID改变的进程的信息，包括改变前的ID及其访问权限、改变后的ID及其访问权限。具体地，当检测到有进程的ID发生改变时，获取所述ID改变的进程的信息，包括改变前的ID及其访问权限、改变后的ID及其访问权限。在一个实施例中，所述进程ID(Identity，标识号码)为进程的UID(用户ID)，在另一个实

施例中，所述进程ID为进程的EUID(有效用户ID)。当进程ID改变时，进程的访问权限也常常会发生改变，此时，进程检测控制单元121获取发生进程ID改变的进程的信息，包括发生进程ID改变前的进程ID以及进程访问权限，发生进程ID改变后的进程ID以及进程访问权限。

[0045] 步骤S3，根据预设的访问策略和所述发生ID改变的进程信息，确定对所述发生ID改变的进程的处理；所述访问策略包括允许访问权限改变的范围。具体地，所述访问策略包括了系统允许访问权限改变的范围，如系统允许的情况：改变前的进程访问权限为能够访问哪些资源，改变后的进程访问权限为能够访问哪些资源。在一个实施例中，所述对所述发生ID改变的进程的处理包括：当所述发生ID改变的进程信息中的所述改变前的进程访问权限小于所述改变后的进程访问权限且不在所述访问策略允许范围时，清除所述发生ID改变的进程。如果所述发生ID改变的进程信息中所述改变前的进程访问权限小于所述改变后的进程访问权限，当该改变在访问策略允许范围内，即系统允许这种情况发生，此时，不清除所述发生ID改变的进程。如果所述发生ID改变的进程信息中所述改变前的进程访问权限大于或等于所述改变后的进程访问权限，不清除所述发生ID改变的进程。

[0046] 在一个实施例中，所述方法还包括：接收策略控制命令，根据所述策略控制命令修改所述访问策略。在一个实施例中，所述策略控制命令包括通过所述可信服务接口发出。当接收到所述策略控制命令时，将根据所述策略控制命令修改所述访问策略。即修改系统允许的进程访问权限改变的范围。

[0047] 综上所述，本发明一种进程访问安全方法及系统，能够防止与检测出进程的不正当提权行为，保护系统不受恶意程序通过提高进程访问权限来获取、修改、泄露系统中的重要资源和数据，从而大大提高了系统的安全性。所以，本发明有效克服了现有技术中的种种缺点而具高度产业利用价值。

[0048] 上述实施例仅例示性说明本发明的原理及其功效，而非用于限制本发明。任何熟悉此技术的人士皆可在不违背本发明的精神及范畴下，对上述实施例进行修饰或改变。因此，举凡所属技术领域中具有通常知识者在未脱离本发明所揭示的精神与技术思想下所完成的一切等效修饰或改变，仍应由本发明的权利要求所涵盖。

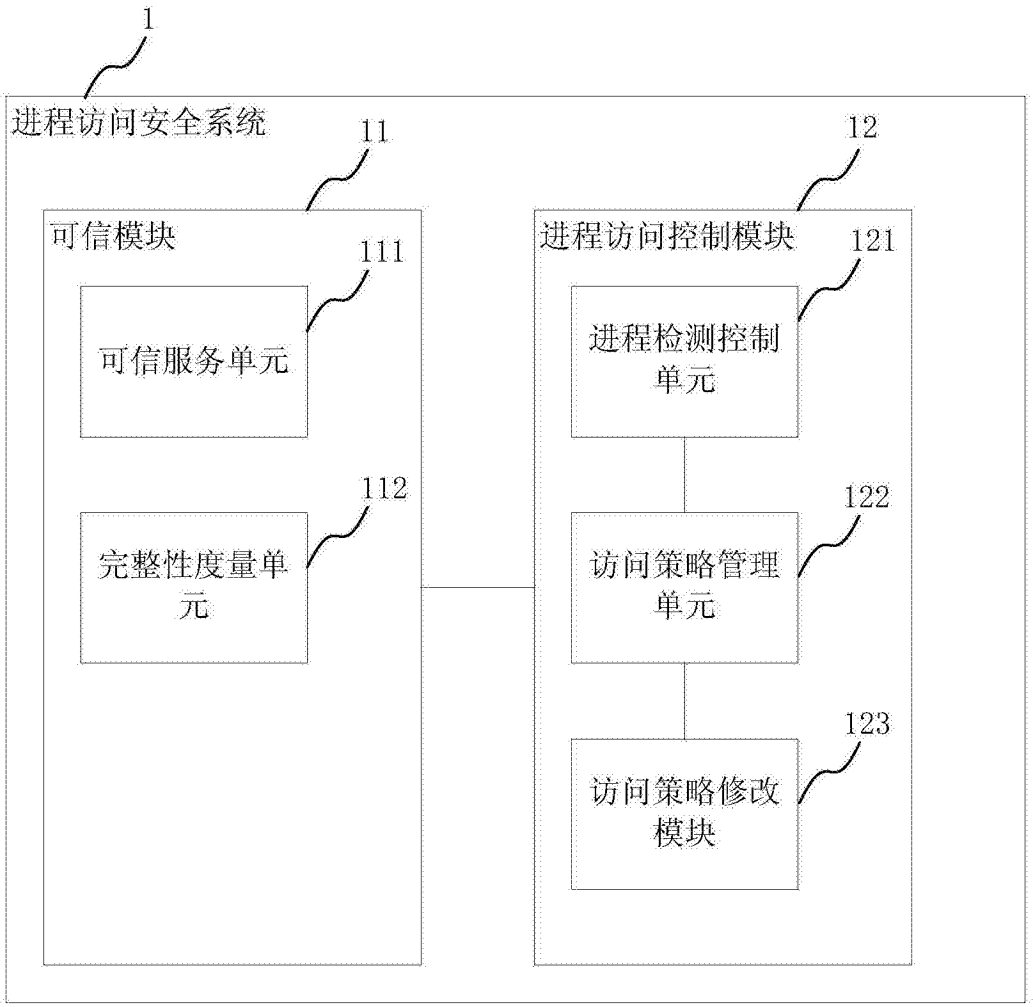

1
进程访问安全系统
11
可信模块
111
可信服务单元
112
完整性度量单元
12
进程访问控制模块
121
进程检测控制单元
122
访问策略管理单元
123
访问策略修改模块

图1

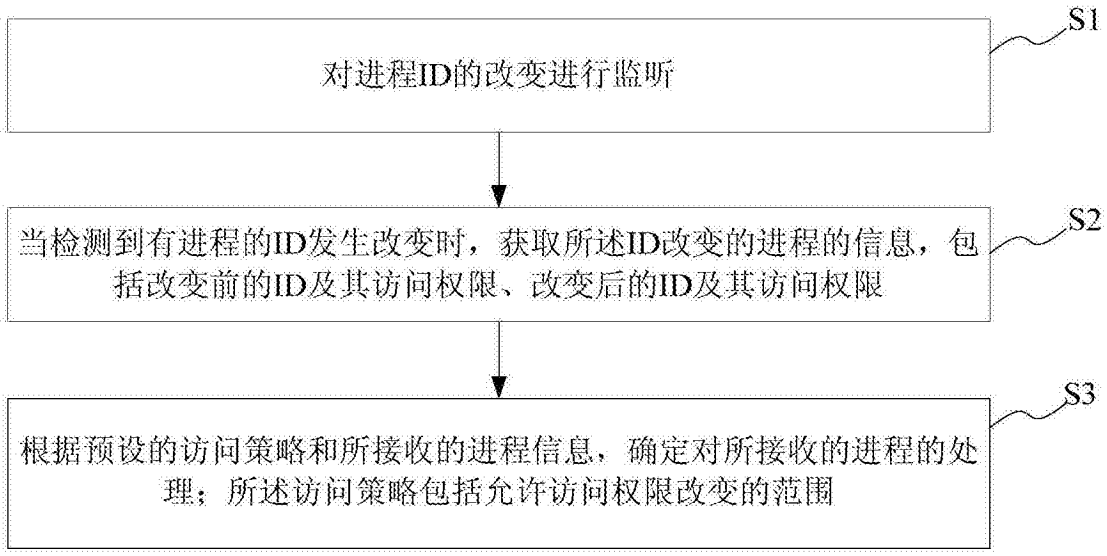

S1
对进程ID的改变进行监听
S2
当检测到有进程的ID发生改变时，获取所述ID改变的进程的信息，包括改变前的ID及其访问权限、改变后的ID及其访问权限
S3
根据预设的访问策略和所接收的进程信息，确定对所接收的进程的处理；所述访问策略包括允许访问权限改变的范围

图2