(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 113886288 A
(43)申请公布日 2022.01.04

(21)申请号 202111148236.6

(22)申请日 2021.09.29

(71)申请人 南方科技大学
地址 518055 广东省深圳市南山区桃源街道学苑大道1088号

(72)发明人 宁振宇 张锋巍 王晨旭 陈胤桦

(74)专利代理机构 广州嘉权专利商标事务所有限公司 44205
代理人 廖慧贤

(51)Int.Cl.
G06F 12/1009(2016.01)
G06F 21/57(2013.01)

权利要求书2页 说明书9页 附图4页

(54)发明名称

基于ARM架构的资源访问控制方法、系统、设备及存储介质

(57)摘要

本发明公开了一种基于ARM架构的资源访问控制方法、系统、设备及存储介质。属于可信执行技术领域，本发明的基于ARM架构的资源访问控制方法通过采用获取预设的一级转换表和虚拟访问地址；根据虚拟访问地址和预设的一级转换表，得到目标中间地址；获取二级转换表；根据目标中间地址和二级转换表，得到目标关键资源的目标物理地址；根据目标物理地址访问目标关键资源。能够在不增加过多系统负荷的前提下，实现对资源访问的控制。

CN 113886288 A

1.基于ARM架构的资源访问控制方法,其特征在于,包括:

获取预设的一级转换表和虚拟访问地址;

根据所述虚拟访问地址和所述预设的一级转换表,得到目标中间地址;

获取二级转换表;

根据所述目标中间地址和所述二级转换表,得到目标关键资源的目标物理地址;

根据所述目标物理地址访问目标关键资源。

2.根据权利要求1的基于ARM架构的资源访问控制方法,其特征在于,所述获取预设的一级转换表和虚拟访问地址之前,方法还包括:

获取所述预设的一级转换表,并根据所述预设的一级转换表,得到包含所述目标中间地址的中间地址表;

获取全部关键资源和每一关键资源的物理地址;

根据所述包含目标中间地址的所述中间地址表和所述每一关键资源的物理地址,生成二级转换表;

将所述二级转换表存储至安全空间。

3.根据权利要求2的基于ARM架构的资源访问控制方法,其特征在于,所述将所述二级转换表存储至安全空间之后,还包括:

获取所述安全空间内的所述二级转换表的存储地址;

将所述存储地址存储至地址寄存器。

4.根据权利要求2的基于ARM架构的资源访问控制方法,其特征在于,所述获取预设的一级转换表和虚拟访问地址表之前,方法还包括:

获取设备树和至少一块连续的物理内存;

确定所述设备树和所述物理内存的地址映射关系;

更改所述地址映射关系,以生成所述安全空间。

5.根据权利要求3的基于ARM架构的资源访问控制方法,其特征在于,所述根据所述目标中间地址和所述二级转换表,得到目标关键资源的目标物理地址,包括:

访问所述地址寄存器,并获取所述二级转换表的存储地址;

根据所述存储地址,读取所述二级转换表,并根据所述二级转换表,得到包含所述目标中间地址的中间地址表和所述每一关键资源的物理地址以获取所述目标关键资源的目标物理地址。

6.基于ARM架构的资源访问控制系统,其特征在于,包括:

请求收集模块,用于获取预设的一级转换表和虚拟访问地址;

目标中间地址获取模块,用于根据所述虚拟访问地址和所述预设的一级转换表,得到目标中间地址;

二级转换表获取模块,用于获取二级转换表;

目标物理地址生成模块,用于根据所述目标中间地址和所述二级转换表,得到目标关键资源的目标物理地址;

目标关键资源访问模块,用于根据所述目标物理地址访问所述目标关键资源。

7.根据权利要求6的基于ARM架构的资源访问控制系统,其特征在于,基于ARM架构资源访问控制系统还包括:

中间地址表生成模块，用于获取所述预设的一级转换表，并根据所述预设的一级转换表，得到包含所述目标中间地址的中间地址表；

资源地址获取模块，用于获取全部关键资源和每一关键资源的物理地址；

二级转换表生成模块，用于根据所述包含目标中间地址的所述中间地址表和所述每一关键资源的物理地址，生成所述二级转换表；

二级转换表存储模块，用于将所述二级转换表存储至安全空间；

二级转换表地址获取模块，用于获取所述安全空间内的所述二级转换表的存储地址；

地址存储模块，用于将所述存储地址存储至地址寄存器；

设备树与内存获取模块，用于获取设备树和至少一块连续的物理内存；

地址映射获取模块，用于确定所述设备树和所述物理内存的地址映射关系；

安全空间生成模块，用于更改所述地址映射关系，以生成所述安全空间。

8.根据权利要求6的基于ARM架构的资源访问控制设备，其特征在于，目标物理地址生成模块包括：

寄存器读取单元，用于访问地址寄存器，并获取二级转换表的存储地址；

目标物理地址生成单元，用于根据所述存储地址，读取所述二级转换表，并根据所述二级转换表，得到包含目标中间地址的中间地址表和每一关键资源的物理地址以获取目标关键资源的目标物理地址。

9.基于ARM架构的资源访问控制设备，其特征在于，包括：

至少一个处理器，以及

与至少一个处理器通信连接的存储器，其中，

所述存储器存储有指令，指令被所述至少一个处理器执行，以使所述至少一个处理器执行所述指令时，实现如权利要求1至5任一项所述的基于ARM架构的资源访问控制方法。

10.计算机可读存储介质，其特征在于，所述计算机可读存储介质存储有计算机可执行指令，可用于执行如权利要求1至5任一项所述的基于ARM架构的资源访问控制方法。

基于ARM架构的资源访问控制方法、系统、设备及存储介质

技术领域

[0001] 本发明涉及可信执行技术领域，尤其是一种基于ARM架构的资源访问控制方法、系统、设备及存储介质。

背景技术

[0002] 相关技术中，通常采用授予动态权限的技术手段实现关键资源的访问和控制，这种方法要求的性能更高，系统延迟也会因此增加。因此，如何提供一种能够降低系统负荷的资源访问控制方法，成为了亟待解决的问题。

发明内容

[0003] 本发明旨在至少解决现有技术中存在的技术问题之一。为此，本发明提出一种基于ARM 架构的资源访问控制方法，能够在不增加过多系统负荷的前提下，实现对资源访问的控制。

[0004] 本发明还提出一种具有上述基于ARM架构的资源访问控制方法的基于ARM架构的资源访问控制系统。

[0005] 本发明还提出一种具有上述基于ARM架构的资源访问控制方法的基于ARM架构的资源访问控制设备。

[0006] 本发明还提出一种具有上述基于ARM架构的资源访问控制方法的计算机可读存储介质。

[0007] 根据本发明的第一方面实施例的基于ARM架构的资源访问控制方法，包括：

[0008] 获取预设的一级转换表和虚拟访问地址；

[0009] 根据虚拟访问地址和预设的一级转换表，得到目标中间地址；

[0010] 获取二级转换表；

[0011] 根据中间物理地址和二级转换表，得到目标关键资源的目标物理地址；

[0012] 根据目标物理地址访问目标关键资源。

[0013] 根据本发明实施例的基于ARM架构的资源访问控制方法，至少具有如下有益效果：本发明所提供的基于ARM架构的资源访问控制方法通过获取预设的一级转换表和虚拟访问地址，并根据预设的一级转换表中的地址映射关系，得到虚拟访问地址所对应的目标中间地址；通过获取二级转换表，并根据二级转换表中的地址映射关系得到目标中间地址所对应的关键资源的目标物理地址，并根据目标物理地址访问目标关键资源。该方法在提高了对目标关键资源的访问的安全性的同时，通过二级转换表获取目标关键资源以实现对目标关键资源的访问，能够有效地降低系统负荷。

[0014] 根据本发明的一些实施例，获取预设的一级转换表和虚拟访问地址之前，方法还包括：

[0015] 获取预设的一级转换表，并根据预设的一级转换表，得到包含目标中间地址的中间地址表；

[0016] 获取全部关键资源和每一关键资源的物理地址；

[0017] 根据包含目标中间地址的中间地址表和每一关键资源的物理地址，生成二级转换表；

[0018] 将二级转换表存储至安全空间。

[0019] 根据本发明的一些实施例，将二级转换表存储至安全空间之后，还包括：

[0020] 获取安全空间内的二级转换表的存储地址；

[0021] 将存储地址存储至地址寄存器。

[0022] 根据本发明的一些实施例，获取预设的一级转换表之前，方法还包括：

[0023] 获取设备树和至少一块连续的物理内存；

[0024] 确定设备树和物理内存的地址映射关系；

[0025] 更改地址映射关系，以生成安全空间。

[0026] 根据本发明的一些实施例，根据中间物理地址和二级转换表，得到目标关键资源的目标物理地址，包括：

[0027] 访问地址寄存器，并获取二级转换表的存储地址；

[0028] 根据存储地址，读取二级转换表，并根据二级转换表，得到包含目标中间地址的中间地址表和每一关键资源的物理地址以获取目标关键资源的目标物理地址。

[0029] 根据本发明的第二方面实施例的基于ARM架构的资源访问控制系统，包括：

[0030] 获取模块，用于获取预设的一级转换表和虚拟访问地址；

[0031] 目标中间地址获取模块，用于根据虚拟访问地址和预设的一级转换表，得到目标中间地址；

[0032] 二级转换表获取模块，用于获取二级转换表；

[0033] 目标物理地址生成模块，用于根据中间物理地址和二级转换表，得到目标关键资源的目标物理地址；

[0034] 目标关键资源访问模块，用于根据目标物理地址访问目标关键资源。

[0035] 根据本发明实施例的基于ARM架构的资源访问控制系统，至少具有如下有益效果：通过请求收集模块获取一级转换表和虚拟访问地址，通过目标中间地址获取模块获取虚拟访问地址和预设的一级转换表，以得到目标中间地址；通过二级转换表获取模块获取二级转换表；通过目标物理地址生成模块获取目标中间地址和二级转换表，以得到目标关键资源的目标物理地址；通过目标关键资源访问模块获取目标物理地址，并根据目标物理地址访问目标关键资源。该方法在提高了对目标关键资源的访问的安全性的同时，通过二级转换表获取目标关键资源以实现对目标关键资源的访问，能够有效地降低系统负荷。

[0036] 根据本发明的一些实施例，基于ARM架构资源访问控制系统还包括：

[0037] 中间地址表生成模块，用于获取预设的一级转换表，并根据预设的一级转换表，得到包含目标中间地址的中间地址表；

[0038] 资源地址获取模块，用于获取全部关键资源和每一关键资源的物理地址；

[0039] 二级转换表生成模块，用于根据包含目标中间地址的中间地址表和每一关键资源的物理地址，生成二级转换表；

[0040] 二级转换表存储模块，用于将二级转换表存储至安全空间。

[0041] 二级转换表地址获取模块，用于获取安全空间内的二级转换表的存储地址；

[0042] 地址存储模块，将存储地址存储至地址寄存器。

[0043] 设备树与内存获取模块，用于获取设备树和至少一块连续的物理内存；

[0044] 地址映射获取模块，用于确定设备树和物理内存的地址映射关系；

[0045] 安全空间生成模块，用于更改地址映射关系，以生成安全空间。

[0046] 根据本发明的一些实施例，目标物理地址生成模块包括：

[0047] 寄存器读取单元，用于访问地址寄存器，并获取二级转换表的存储地址

[0048] 目标物理地址生成单元，用于根据存储地址，读取二级转换表，并根据二级转换表，得到包含目标中间地址的中间地址表和每一关键资源的物理地址以获取目标关键资源的目标物理地址

[0049] 根据本发明的第三方面实施例的基于ARM架构的资源访问控制设备，包括：

[0050] 至少一个处理器，以及

[0051] 与至少一个处理器通信连接的存储器，其中，

[0052] 存储器存储有指令，指令被至少一个处理器执行，以使至少一个处理器执行指令时，实现如本发明第一方面实施例的基于ARM架构的资源访问控制方法。

[0053] 根据本发明实施例的基于ARM架构的资源访问控制设备，至少具有如下有益效果：本发明提供的基于ARM架构的资源访问控制设备通过执行本发明第一方面实施例所提供的基于ARM架构的资源访问控制设备方法，可以实现通过获取预设的一级转换表和虚拟访问地址，并根据预设的一级转换表中的地址映射关系，得到虚拟访问地址所对应的目标中间地址；通过获取二级转换表，并根据二级转换表中的地址映射关系得到目标中间地址所对应的关键资源的目标物理地址，并根据目标物理地址访问目标关键资源。该方法在提高了对目标关键资源的访问的安全性的同时，通过二级转换表获取目标关键资源以实现对目标关键资源的访问，能够有效地降低系统负荷。

[0054] 根据本发明的第四方面实施例的计算机可读存储介质，包括：

[0055] 计算机可读存储介质存储有计算机可执行指令，可用于执行如本发明第一方面实施例的基于ARM架构的资源访问控制方法。

[0056] 根据本发明实施例的计算机可读存储介质，至少具有如下有益效果：本发明提供的一种计算机可读存储介质存储有计算机可执行指令，可用于执行如本发明第一方面实施例的基于 ARM架构的资源访问控制方法，从而实现通过获取预设的一级转换表和虚拟访问地址，并根据预设的一级转换表中的地址映射关系，得到虚拟访问地址所对应的目标中间地址；通过获取二级转换表，并根据二级转换表中的地址映射关系得到目标中间地址所对应的关键资源的目标物理地址，并根据目标物理地址访问目标关键资源。该方法在提高了对目标关键资源的访问的安全性的同时，通过二级转换表获取目标关键资源以实现对目标关键资源的访问，能够有效地降低系统负荷。

[0057] 本发明的附加方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本发明的实践了解到。

附图说明

[0058] 下面结合附图和实施例对本发明做进一步的说明，其中：

[0059] 图1为本发明实施例基于ARM架构的资源访问控制方法的流程图。

[0060] 图2为本发明实施例基于ARM架构的资源访问控制方法的又一流程图。

[0061] 图3为本发明实施例基于ARM架构的资源访问控制方法的又一流程图。

[0062] 图4为本发明实施例基于ARM架构的资源访问控制方法的又一流程图。

[0063] 图5为图1中步骤S400的具体流程图。

[0064] 图6为本发明实施例基于ARM架构的资源访问控制系统的结构示意图。

[0065] 图7为本发明实施例基于ARM架构的资源访问控制系统的又一结构示意图。

[0066] 图8为图7中目标物理地址生成模块400的具体结构示意图。

[0067] 附图标记:100、请求收集模块;200、目标中间地址获取模块;300、二级转换表获取模块;400、目标物理地址生成模块;500、目标关键资源访问模块;600、中间地址表生成模块; 700、资源地址获取模块;800、二级转换表生成模块;900、二级转换表存储模块;1000、二级转换表地址获取模块;1100、地址存储模块;1200、设备树与内存获取模块;1300、地址映射获取模块;1400、安全空间生成模块;410、寄存器读取单元;420、目标物理地址生成单元;

具体实施方式

[0068] 下面详细描述本发明的实施例,实施例的示例在附图中示出,其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的,仅用于解释本发明,而不能理解为对本发明的限制。

[0069] 在本发明的描述中,需要理解的是,涉及到方位描述,例如上、下、前、后、左、右等指示的方位或位置关系为基于附图所示的方位或位置关系,仅是为了便于描述本发明和简化描述,而不是指示或暗示所指的装置或元件必须具有特定的方位、以特定的方位构造和操作,因此不能理解为对本发明的限制。

[0070] 在本发明的描述中,若干的含义是一个以上,多个的含义是两个以上,大于、小于、超过等理解为不包括本数,以上、以下、以内等理解为包括本数。如果有描述到第一、第二只是用于区分技术特征为目的,而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量或者隐含指明所指示的技术特征的先后关系。

[0071] 本发明的描述中,除非另有明确的限定,设置、安装、连接等词语应做广义理解,所属技术领域技术人员可以结合技术方案的具体内容合理确定上述词语在本发明中的具体含义。

[0072] 本发明的描述中,参考术语“一个实施例”、“一些实施例”、“示意性实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中,对上述术语的示意性表述不一定指的是相同的实施例或示例。而且,描述的具体特征、结构、材料或者特点可以在任何的一个或多个实施例或示例中以合适的方式结合。

[0073] 第一方面,参照图1,本发明提供了一种基于ARM架构的资源访问控制方法,其特征在于,包括:

[0074] S100,获取预设的一级转换表和虚拟访问地址;

[0075] S200,根据虚拟访问地址和预设的一级转换表,得到目标中间地址;

[0076] S300,获取二级转换表;

[0077] S400,根据中间物理地址和二级转换表,得到目标关键资源的目标物理地址;

[0078] S500,根据目标物理地址访问目标关键资源。

[0079] 本方法通过获取预设的一级转换表和虚拟访问地址,根据预设的一级转换表中的地址映射关系,可以得到虚拟访问地址所对应的目标中间地址;通过获取二级转换表,并根据二级转换表中的地址映射关系,本方法可以得到目标中间地址所对应的关键资源的目标物理地址,并根据目标物理地址访问目标关键资源。本方法在提高了对目标关键资源的访问的安全性的同时,通过二级转换表获取目标关键资源以实现对目标关键资源的访问,实现了降低系统负荷的效果,提供了一种能够降低系统负荷的资源访问控制方法。

[0080] 在一些具体的实施例中,本方法采取将资源访问控制机制的权限布置在ARM管理程序中,以限制权限在本方法提供的资源访问控制机制之下的外部资源访问要求,有效的降低了外部低权限访问、篡改和攻击关键资源的风险。

[0081] 在一些其他的实施例中,本发明中的基于ARM架构的资源访问控制方法具备EL2权限,系统权限为EL1权限。在ARM架构中,外部访问要求在仅获取EL1权限的前提下,无法绕过本申请中置于EL2权限的基于ARM架构的资源访问控制方法进行直接访问,该方法能有效地提高资源访问过程的安全性。其中,EL1权限即为系统权限,其权限等级小于EL2权限。具有EL1权限的外部访问请求无法对EL2权限内的存储信息进行访问,从而有效的提升了资源访问过程的安全性。

[0082] 在一些其他的实施例中,本申请提供的基于ARM架构的资源访问控制方法通过屏蔽系统权限层软件对关键资源的访问实现,当开发者需要获取关键资源时,仅需要提供具备权限的访问请求,获取二级转换表,并过二级转换表获取关键资源即可实现,其整个访问控制过程仅需要一次地址映射转换,过程简单,可以有效降低系统负荷。其中关键资源可以是异常向量表,中断向量表,以及一些系统的关键配置等,不做限制。

[0083] 参照图2,在一些实施例中,步骤S100之前还包括:

[0084] S600,获取预设的一级转换表,并根据预设的一级转换表,得到包含目标中间地址的中间地址表;

[0085] S700,获取全部关键资源和每一关键资源的物理地址;

[0086] S800,根据包含目标中间地址的中间地址表和每一关键资源的物理地址,生成二级转换表;

[0087] S900,将二级转换表存储至安全空间。

[0088] 本发明中所提供的基于ARM架构的资源访问控制方法,通过获取预设一级转换表,并读取其中所预存的地址映射,可以获取到全部关键资源中对应具体目标中间地址的中间地址表。通过获取到的全部关键资源和每一关键资源的物理地址,本方法将中间地址表中对应具体目标中间地址与每一关键资源的物理地址一一对应,生成目标中间地址和目标物理地址间的地址映射关系,并生成第二转换表,并将第二转换表存储至安全空间。这一方法能够可以将目标中间地址和目标物理地址之间映射关系一一对应,同时生成相对于系统权限具有更高权限的二级转换表,有效的提高了关键资源访问的安全性。

[0089] 在一些具体的实施例中,获取一级转换表仅需要系统权限,即EL1权限,用户可以直接访问,不需额外权限。通过一级转换表获取到的目标中间地址无法直接访问目标关键资源的物理地址,仅能通过二级转换表对目标中间地址进行转换,以获取可以直接访问目

标关键资源的目标物理地址。

[0090] 在一些具体的实施例中,第二转换表内的地址映射关系建立方法为现有技术,具体地,可以通过ARM手册中的使用方法进行更改,如:对于一次二级地址转换,它细分成若干个层(level),同时每层都需要有一些页表表项(entry)来协助翻译。在每个层上,我们将输入地址按照ARM手册上规定的翻译方式来结合本层的页表表项,以此获得存有下一层页表表项的目标地址。每个页表表项能够反映一些地址转换的详细信息,例如这一段地址空间的读写权限,以及是否要进行下一层的转换,或者是到此为止。相关实现方法不再赘述。

[0091] 参照图3,在一些实施例中,S900之后还包括

[0092] S1000,获取安全空间内的二级转换表的存储地址;

[0093] S1100,将存储地址存储至地址寄存器。

[0094] 本发明中所提供的基于ARM架构的资源访问控制方法,通过获取安全空间内的二级转换表的存储地址,并将存储地址存储至地址寄存器,有效的避免了关键资源访问的请求直接通过访问安全空间,导致安全空间被恶意攻击。通过在地址寄存器存储安全空间内第二转换表的存储地址的手段,本方法可以通过地址寄存器间接获取二级转换表,提高了基于ARM 架构的资源访问控制方法的安全性,有效的降低了由于安全空间地址被泄露产生的风险。

[0095] 在一些具体的实施例中,寄存器需要进行提前配置,以实现二级转换的技术效果。本发明所提供的基于ARM架构的资源访问控制方法采用虚拟化配置寄存器实现对存储地址的保护,并通过修改虚拟化配置寄存器的虚拟化使能位来开启转换,从而使MMU处理关于关键资源的访问请求时可以运作二级转换;本发明所提供的方法还通过设置虚拟转换表基地址寄存器基地址位为该转换表的基地址,实现获取并保护存储地址的技术效果。

[0096] 参照图4,在一些实施例中,S100之前还包括:

[0097] S1200,获取设备树和至少一块连续的物理内存;

[0098] S1300,确定设备树和物理内存的地址映射关系更改地址映射关系,以生成安全空间;

[0099] S1400,更改地址映射关系,以生成安全空间。

[0100] 本发明中所提供的基于ARM架构的资源访问控制方法,通过获取设备树和至少一块连续的物理内存,以确定物理内存在设备树中的地址映射关系,并更改地址映射关系,以防止可以通过设备树可以直接访问所需要保护的物理内存,实现了对安全空间的创建。本方法通过创建安全空间以存储第二转换表,实现对第二转换表的存储地址的保护,从而提高本申请所提供的基于ARM架构的资源访问控制方法的安全性。

[0101] 在一些具体的实施例中,通过选定随机存储器的至少一块连续内存,本方法可以实现取消其与设备树之间物理地址映射关系,以实现保护这块连续内存的技术效果。在一些其他的实施例中,存储器的类型也可以是其他,不限于此。

[0102] 在另一些具体的实施例中,通过更改设备树种所选取的物理内存的属性,可以取消设备树与物理内存之间的地址映射。具体地,在ARM架构下的物理内存,通过更改其属性为“no-map”,实现在设备树开机运行时,内核的其它进程不会对这块选定的物理内存进行占用与更改,在一些实施例中可以是其它,不限于此。

[0103] 参照图5,在一些实施例中,S400包括:

[0104] S410,访问地址寄存器,并获取二级转换表的存储地址;

[0105] S420,根据存储地址,读取二级转换表,并根据二级转换表,得到包含目标中间地址的中间地址表和每一关键资源的物理地址以获取目标关键资源的目标物理地址。

[0106] 本发明中所提供的基于ARM架构的资源访问控制方法,通过访问地址寄存器获取二级转换表的存储地址,并根据存储地址读取二级转化表,根据二级转换表中的目标中间地址与目标物理地址之间的一一映射关系,获取所需要获取的目标关键资源所对应的目标物理地址,能够通过地址寄存器间接获取第二转化表,从而实现虚拟访问地址—目标中间地址—目标物理地址之间的转化,避免资源访问请求对目标物理地址的直接获取,提高了访问过程的安全性。

[0107] 第二方面,参照图6,本发明提供了一种基于ARM架构的资源访问控制系统,包括:

[0108] 请求收集模块100,用于获取预设的一级转换表和虚拟访问地址;

[0109] 目标中间地址获取模块200,用于根据虚拟访问地址和预设的一级转换表,得到目标中间地址;

[0110] 二级转换表获取模块300,用于获取二级转换表;

[0111] 目标物理地址生成模块400,用于根据目标中间地址和二级转换表,得到目标关键资源的目标物理地址;

[0112] 目标关键资源访问模块500,用于根据目标物理地址访问目标关键资源。

[0113] 本发明中所提供了一种基于ARM架构的资源访问控制系统,通过请求收集模块100获取一级转换表和虚拟访问地址,通过目标中间地址获取模块200获取虚拟访问地址和预设的一级转换表,以得到目标中间地址;通过二级转换表获取模块300获取二级转换表;通过目标物理地址生成模块400获取目标中间地址和二级转换表,以得到目标关键资源的目标物理地址;通过目标关键资源访问模块500获取目标物理地址,并根据目标物理地址访问目标关键资源。本方法在提高了对目标关键资源的访问的安全性的同时,通过二级转换表获取目标关键资源以实现对目标关键资源的访问,实现了降低系统负荷的效果,提供了一种能够降低系统负荷的资源访问控制方法。

[0114] 参照图7,在一些实施例中,基于ARM架构的资源访问控制系统,还包括:

[0115] 中间地址表生成模块600,用于获取预设的一级转换表,并根据预设的一级转换表,得到包含目标中间地址的中间地址表;

[0116] 资源地址获取模块700,用于获取全部关键资源和每一关键资源的物理地址;

[0117] 二级转换表生成模块800,用于根据包含目标中间地址的中间地址表和每一关键资源的物理地址,生成二级转换表;

[0118] 二级转换表存储模块900,用于将二级转换表存储至安全空间;

[0119] 二级转换表地址获取模块1000,用于获取安全空间内的二级转换表的存储地址;

[0120] 地址存储模块1100,用于将存储地址存储至地址寄存器;

[0121] 设备树与内存获取模块1200,用于获取设备树和至少一块连续的物理内存;

[0122] 地址映射获取模块1300,用于确定设备树和物理内存的地址映射关系;

[0123] 安全空间生成模块1400,用于更改地址映射关系,以生成安全空间。

[0124] 本发明提供的基于ARM架构的资源访问控制系统,通过中间地址表生成模块600获取预设的一级转换表,并根据预设的一级转换表,得到包含目标中间地址的中间地址表;通

过资源地址获取模块700获取全部关键资源和每一关键资源的物理地址;通过二级转换表生成模块800根据包含目标中间地址的中间地址表和每一关键资源的物理地址,生成二级转换表;通过二级转换表存储模块900将二级转换表存储至安全空间;通过二级转换表地址获取模块 1000获取安全空间内的二级转换表的存储地址;通过地址存储模块1100将存储地址存储至地址寄存器;通过设备树与内存获取模块1200获取设备树和至少一块连续的物理内存;通过地址映射获取模块1300确定设备树和物理内存的地址映射关系;通过安全空间生成模块1400 更改地址映射关系,生成安全空间。本发明提供的基于ARM架构的资源访问控制系统可以实现对安全空间的构建,存储二级转换表,防止由于关键资源进行访问时直接获取到二级转换表的地址以直接获取目标关键资源的物理地址而产生的安全隐患。本发明提供的基于ARM 架构的资源访问控制系统还可以根据系统预设的以及转换表和关键资源的地址生成包含目标中间地址与目标物理地址之间的地址映射,实现从虚拟访问地址—目标中间地址—目标物理地址之间的转换,有效的提高了系统的安全性。本发明提供的基于ARM架构的资源访问控制系统还可以提供存储有安全空间内的第二转换表的存储地址的地址寄存器,实现对第二转换表存储地址的保护,避免外部访问直接与安全空间实现通信、进一步是提升了系统的安全性。此外,本方法通过第二转换表进行目标中间地址与目标物理地址之间的转换,有效的简化了资源访问控制机制,提高了访问效率,降低了系统负荷。

[0125] 参照图8,在一些实施例中,目标物理地址生成模块400包括:

[0126] 寄存器读取单元410,用于访问地址寄存器,并获取二级转换表的存储地址

[0127] 目标物理地址生成单元420,用于根据存储地址,读取二级转换表,并根据二级转换表,得到包含目标中间地址的中间地址表和每一关键资源的物理地址以获取目标关键资源的目标物理地址。

[0128] 本发明提供的基于ARM架构的资源访问控制系统,通过目标物理地址生成模块400中的寄存器读取单元410访问地址寄存器,并获取二级转换表的存储地址;通过目标物理地址生成单元420根据存储地址,读取二级转换表,并根据二级转换表,得到包含目标中间地址的中间地址表和每一关键资源的物理地址以获取目标关键资源的目标物理地址。通过采取寄存器读取单元410和目标物理地址生成单元420,本发明提供的基于ARM架构的资源访问控制系统有效的避免了关键资源访问的请求直接通过访问安全空间,导致安全空间被恶意攻击。通过在地址寄存器存储安全空间内第二转换表的存储地址的手段,本系统可以通过寄存器读取单元410和目标物理地址生成单元420间接获取二级转换表,提高了基于ARM架构的资源访问控制系统的安全性,有效的降低了由于安全空间地址被泄露产生的风险。

[0129] 第三方面,本发明提供了一种基于ARM架构的资源访问控制设备,包括:

[0130] 至少一个处理器,以及

[0131] 与至少一个处理器通信连接的存储器,其中,

[0132] 存储器存储有指令,指令被至少一个处理器执行,以使至少一个处理器执行指令时,实现如本发明第一方面实施例的基于ARM架构的资源访问控制方法。

[0133] 本发明提供的基于ARM架构的资源访问控制设备通过执行本发明第一方面实施例所提供的基于ARM架构的资源访问控制方法,可以实现通过获取预设的一级转换表和虚拟访问地址,并根据预设的一级转换表中的地址映射关系,得到虚拟访问地址所对应的目标

中间地址;通过获取二级转换表,并根据二级转换表中的地址映射关系得到目标中间地址所对应的关键资源的目标物理地址,并根据目标物理地址访问目标关键资源。本方法在提高了对目标关键资源的访问的安全性的同时,通过二级转换表获取目标关键资源以实现对目标关键资源的访问,实现了降低系统负荷的效果,提供了一种能够降低系统负荷的资源访问控制方法。

[0134] 第四方面,本发明提供了一种计算机可读存储介质,计算机可读存储介质存储有计算机可执行指令,可用于执行如本发明第一方面实施例的基于ARM架构的资源访问控制方法,从而实现通过获取预设的一级转换表和虚拟访问地址,并根据预设的一级转换表中的地址映射关系,得到虚拟访问地址所对应的目标中间地址;通过获取二级转换表,并根据二级转换表中的地址映射关系得到目标中间地址所对应的关键资源的目标物理地址,并根据目标物理地址访问目标关键资源。本方法在提高了对目标关键资源的访问的安全性的同时,通过二级转换表获取目标关键资源以实现对目标关键资源的访问,实现了降低系统负荷的效果,提供了一种能够降低系统负荷的资源访问控制方法。

[0135] 上面结合附图对本发明实施例作了详细说明,但是本发明不限于上述实施例,在所属技术领域普通技术人员所具备的知识范围内,还可以在不脱离本发明宗旨的前提下作出各种变化。此外,在不冲突的情况下,本发明的实施例及实施例中的特征可以相互组合。

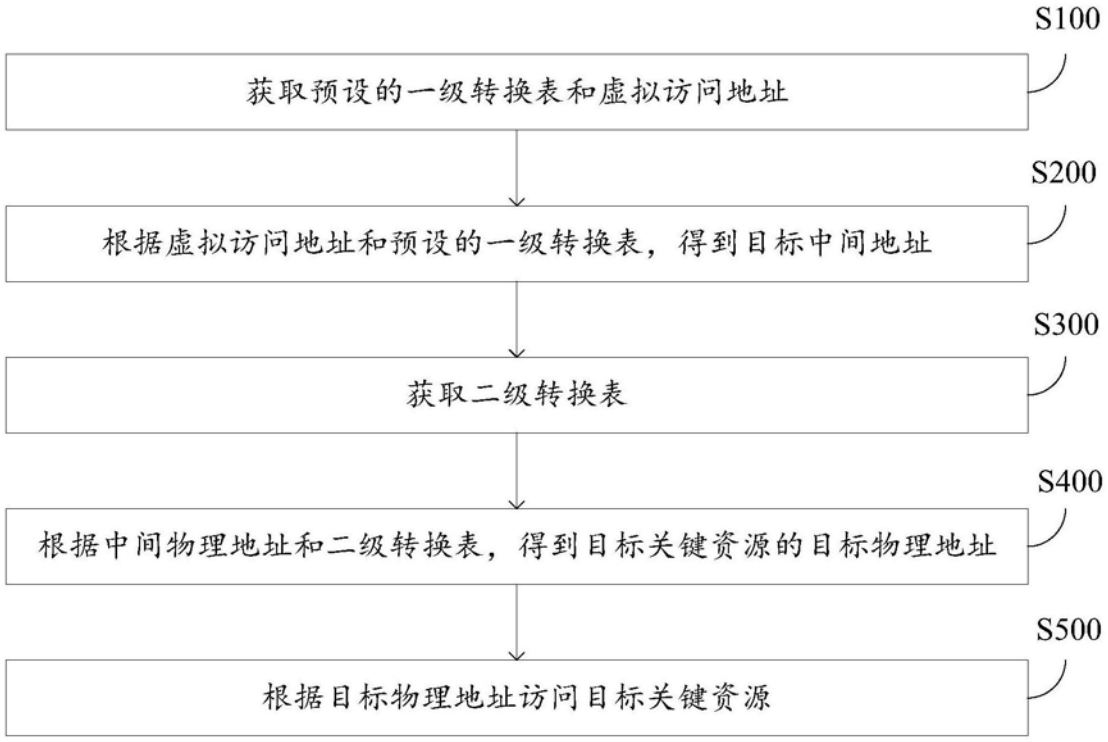
S100
获取预设的一级转换表和虚拟访问地址
S200
根据虚拟访问地址和预设的一级转换表，得到目标中间地址
S300
获取二级转换表
S400
根据中间物理地址和二级转换表，得到目标关键资源的目标物理地址
S500
根据目标物理地址访问目标关键资源

图1

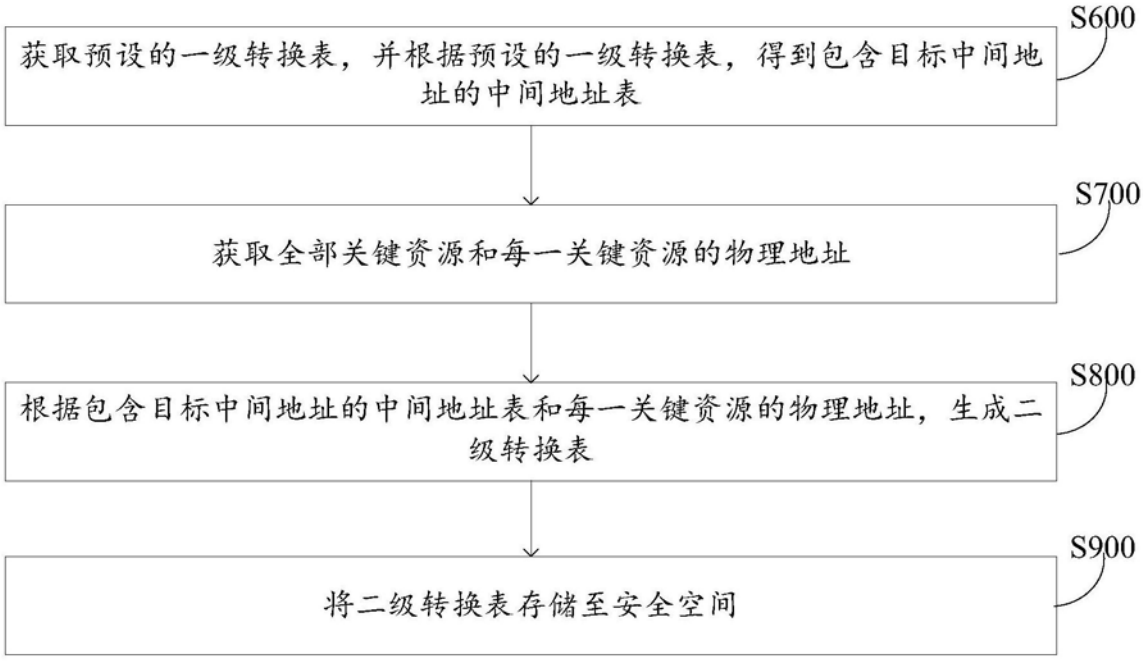
S600
获取预设的一级转换表，并根据预设的一级转换表，得到包含目标中间地址的中间地址表
S700
获取全部关键资源和每一关键资源的物理地址
S800
根据包含目标中间地址的中间地址表和每一关键资源的物理地址，生成二级转换表
S900
将二级转换表存储至安全空间

图2

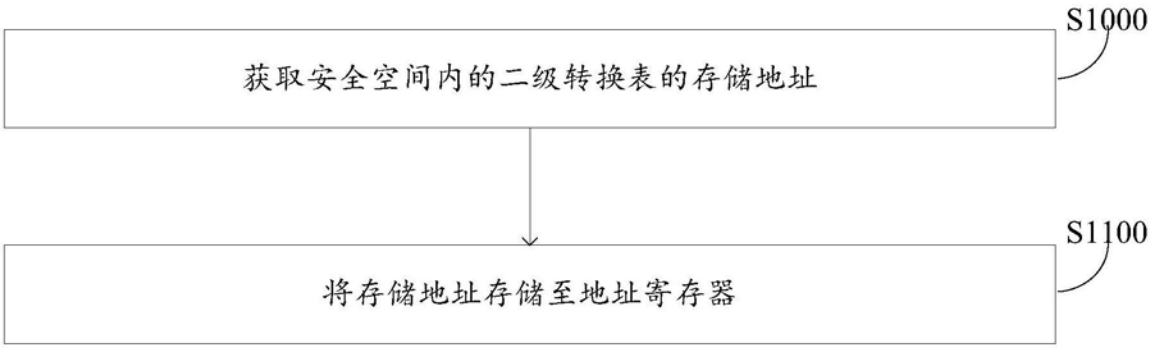
S1000
获取安全空间内的二级转换表的存储地址
S1100
将存储地址存储至地址寄存器

图3

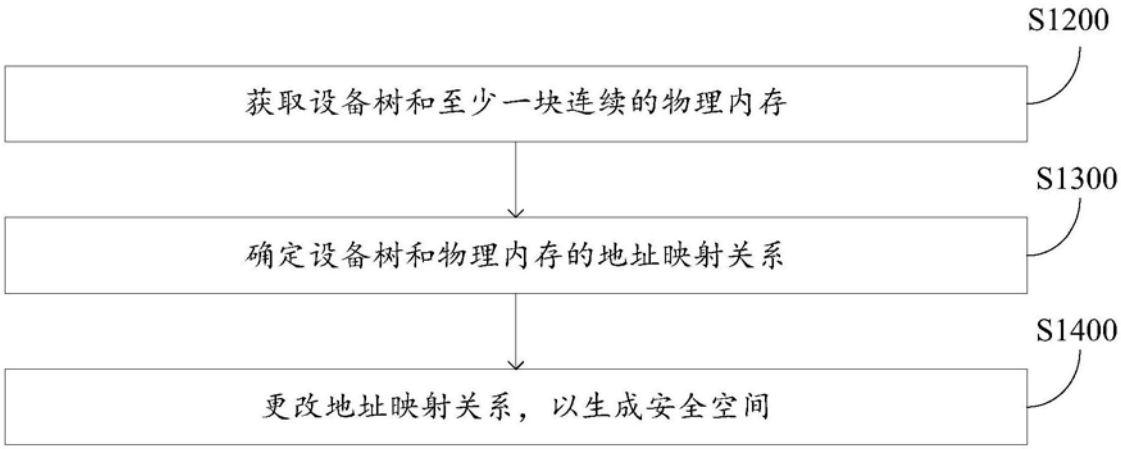
S1200
获取设备树和至少一块连续的物理内存
S1300
确定设备树和物理内存的地址映射关系
S1400
更改地址映射关系，以生成安全空间

图4

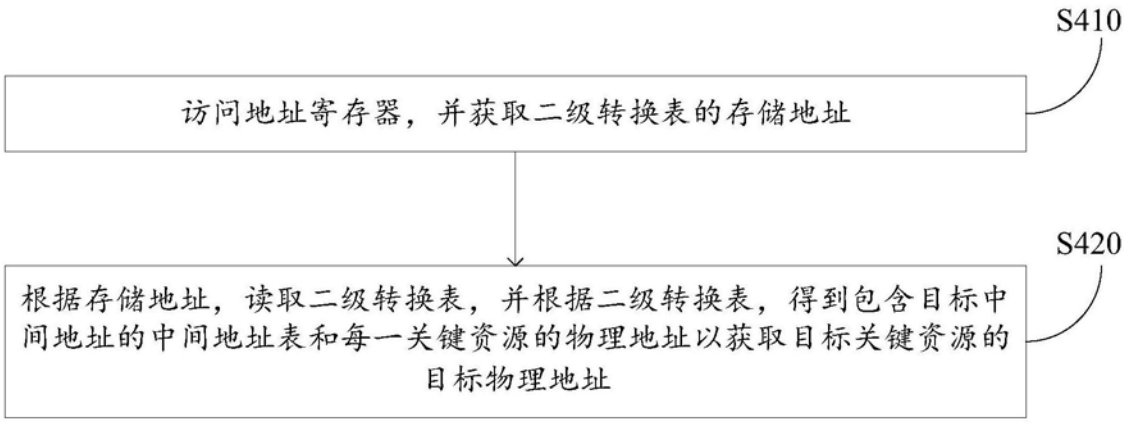
S410
访问地址寄存器，并获取二级转换表的存储地址
S420
根据存储地址，读取二级转换表，并根据二级转换表，得到包含目标中间地址的中间地址表和每一关键资源的物理地址以获取目标关键资源的目标物理地址

图5

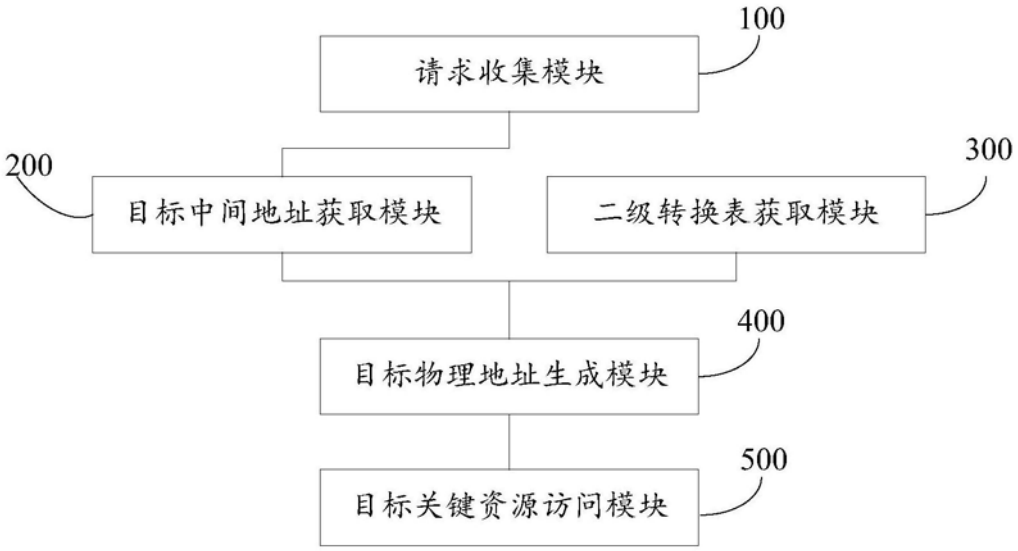
100
请求收集模块
200
目标中间地址获取模块
300
二级转换表获取模块
400
目标物理地址生成模块
500
目标关键资源访问模块

图6

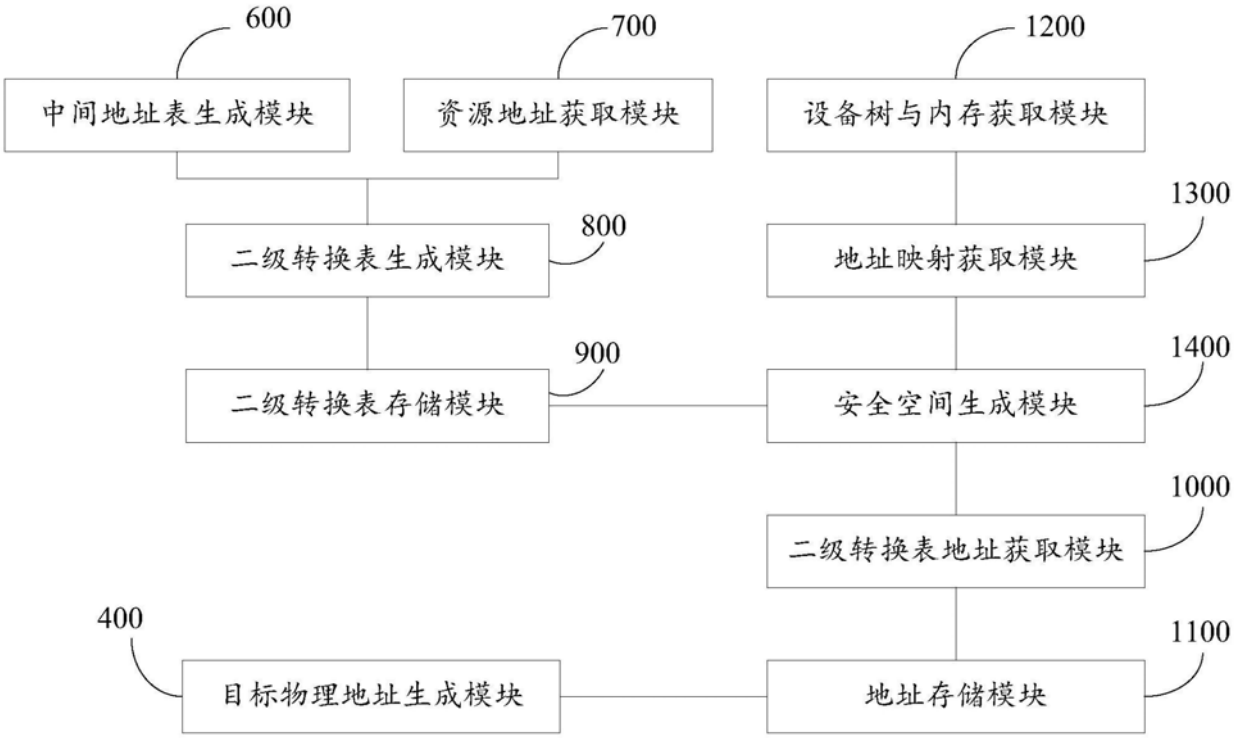
600
中间地址表生成模块
700
资源地址获取模块
1200
设备树与内存获取模块
800
二级转换表生成模块
1300
地址映射获取模块
900
二级转换表存储模块
1400
安全空间生成模块
1000
二级转换表地址获取模块
400
目标物理地址生成模块
1100
地址存储模块

图7

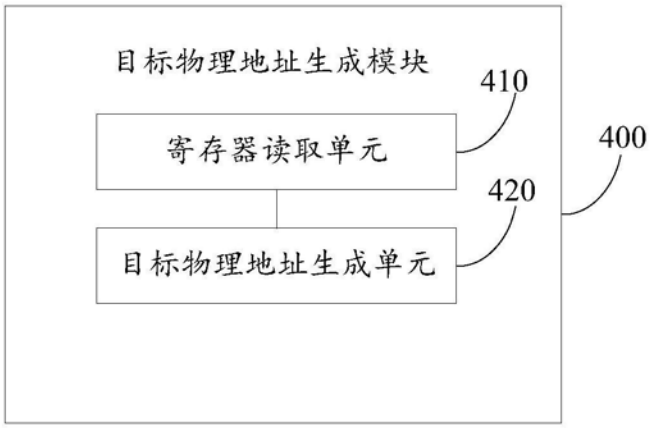

图8