(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 112446032 A
(43)申请公布日 2021.03.05

(21)申请号 202011313471.X

(22)申请日 2020.11.20

(71)申请人 南方科技大学
地址 518055 广东省深圳市南山区西丽学苑大道1088号

(72)发明人 宁振宇 张锋巍

(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 黄广龙

(51)Int.Cl.
G06F 21/57(2013.01)
G06F 21/71(2013.01)

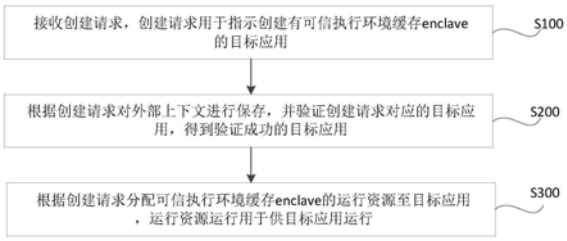
权利要求书2页 说明书9页 附图3页

(54)发明名称

可信执行环境构建方法、系统及存储介质

(57)摘要

本发明公开了一种可信执行环境构建方法、系统及存储介质，可信执行环境构建方法包括：接收创建请求，创建请求用于指示创建有可信执行环境缓存enclave的目标应用；根据创建请求对外部上下文进行保存，并验证创建请求对应的目标应用，得到验证成功的目标应用；根据创建请求分配所述可信执行环境缓存enclave的运行资源至目标应用，运行资源运行用于供目标应用运行。本发明通过接收创建请求后，根据创建请求进行外部上下文保存，再对创建请求对应的目标应用进行验证，若目标应用验证成功则分配对应的运行资源至目标应用，使得目标应用根据运行资源能够正常运行，进而使用户通过目标应用能够安全地访问I/O设备，进而提高了软件运行的安全性。



CN 112446032 A

1.可信执行环境构建方法,其特征在于,包括:

接收创建请求,所述创建请求用于指示创建有可信执行环境缓存enclave的目标应用;

根据所述创建请求对外部上下文进行保存,并验证所述创建请求对应的目标应用,得到验证成功的目标应用;

根据所述创建请求分配所述可信执行环境缓存enclave的运行资源至所述目标应用,所述运行资源运行用于供所述目标应用运行。

2.根据权利要求1所述的可信执行环境构建方法,其特征在于,所述创建请求包括:运行内存需求、运行程序请求、I/O设备请求、执行权限请求,所述运行资源包括:运行专属内存、运行程序、I/O驱动、指令执行权限。

3.根据权利要求2所述的可信执行环境构建方法,其特征在于,根据所述创建请求分配所述可信执行环境缓存enclave的运行资源至所述目标应用,包括:

根据所述运行内存需求将飞地预留内存中与所述运行内存需求对应所述运行专属内存分配至所述目标应用;

根据所述运行程序请求将所述目标应用对应的运行程序复制至所述运行专属内存;

根据所述I/O设备请求将与所述I/O设备请求对应的I/O驱动复制至所述运行专属内存;

根据所述执行权限请求将与所述执行权限请求对应所述指令执行权限分配至所述目标应用。

4.根据权利要求3所述的可信执行环境构建方法,其特征在于,还包括:

若所述飞地预留内存小于所述运行内存需求对应的内存大小,重新监听所述创建请求。

5.根据权利要求3或4任一项所述的可信执行环境构建方法,其特征在于,还包括:

接收I/O设备访问请求,根据所述I/O设备访问请求匹配所述运行专属内存中的I/O驱动;

所述I/O驱动完成与所述I/O设备访问请求对应的I/O设备的初始化。

6.根据权利要求5所述的可信执行环境构建方法,其特征在于,还包括:

监听所述I/O设备和所述目标应用的中断状态以获取中断信息;

对所述中断信息进行分析以重新在所述运行专属内存中获取与所述中断信息对应的I/O驱动;

将所述中断信息发送至所述I/O驱动,所述I/O驱动将所述中断信息处理后将与所述中断信息对应的数据或回复返回至所述目标应用。

7.根据权利要求3所述的可信执行环境构建方法,其特征在于,还包括:

接收销毁请求,

根据所述销毁请求清空并回收所述目标应用所使用的所述运行专属内存,并恢复所述外部上下文和将所述指令执行权限返回至原始应用,所述原始应用为未分配所述可信执行环境缓存enclave前的所述目标应用。

8.一种可信执行环境构建系统,其特征在于,包括:安全监视器,所述安全监视器包括:

飞地管理模块,用于接收创建请求,所述创建请求用于指示创建有可信执行环境缓存enclave的目标应用;

上下文管理模块，用于根据所述创建请求对外部上下文进行保存，并验证所述创建请求对应的目标应用，得到验证成功的所述目标应用；

所述飞地管理模块还用于根据所述创建请求分配所述可信执行环境缓存enclave的运行资源至所述目标应用，所述运行资源运行用于供所述目标应用运行。

9.根据权利要求8所述的可信执行环境构建系统，其特征在于，所述安全监控器还包括：

权限管理模块，用于对目标应用所拥有的I/O设备操作权限进行管理；

中断与异常代理模块，用于对I/O中断进行拦截与分发。

10.一种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，所述计算机可执行指令用于使计算机执行如权利要求1至7任一项所述的可信执行环境构建方法的步骤。

可信执行环境构建方法、系统及存储介质

技术领域

[0001] 本发明涉及软件运行环境的技术领域，尤其是涉及一种可信执行环境构建方法、系统及存储介质。

背景技术

[0002] 随着软件的发展，构建软件安全的软件运行环境得到了广泛的关注，其中最为典型的可信执行环境有Intel x86架构下的SGX，Arm架构下的TrustZone，以及AMD x86架构下的SEV。这些可信执行环境被大量应用于各种不同有安全需求的场景。

[0003] 与Intel x86架构不同的RISC-V架构由于开源的架构吸引了众多研究者，但是RISC-V架构中并未直接提供硬件支撑的可信执行环境，使得用户在使用RISC-V架构时无法提供一个安全的软件运行环境给软件，从而降低了软件运行的安全性。

发明内容

[0004] 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，本发明提出一种可信执行环境构建方法，能够提高软件运行的安全性。

[0005] 本发明还提出一种可信执行环境构建系统。

[0006] 本发明还提出一种计算机存储介质。

[0007] 第一方面，本发明的一个实施例提供了可信执行环境构建方法，包括：

[0008] 接收创建请求，所述创建请求用于指示创建有可信执行环境缓存enclave的目标应用；

[0009] 根据所述创建请求对外部上下文进行保存，并验证所述创建请求对应的目标应用，得到验证成功的目标应用；

[0010] 根据所述创建请求分配所述可信执行环境缓存enclave的运行资源至所述目标应用，所述运行资源运行用于供所述目标应用运行。

[0011] 本发明实施例的可信执行环境构建方法至少具有如下有益效果：通过接收创建请求后，根据创建请求进行外部上下文保存，再对创建请求对应的目标应用进行验证以得到验证成功的目标应用，根据创建请求分配可信执行环境缓存enclave的运行资源至目标应用，使得目标应用根据运行资源能够正常运行，进而使用户通过目标应用能够安全地访问I/O设备，进而提高了软件运行的安全性。

[0012] 根据本发明的另一些实施例的可信执行环境构建方法，所述创建请求包括：运行内存需求、运行程序请求、I/O设备请求、执行权限请求，所述运行资源包括：运行专属内存、运行程序、I/O驱动、指令执行权限。

[0013] 根据本发明的另一些实施例的可信执行环境构建方法，根据所述创建请求分配所述可信执行环境缓存enclave的运行资源至所述目标应用，包括：

[0014] 根据所述运行内存需求将飞地预留内存中与所述运行内存需求对应所述运行专属内存分配至所述目标应用；

[0015] 根据所述运行程序请求将所述目标应用对应的运行程序复制至所述运行专属内存；

[0016] 根据所述I/O设备请求将与所述I/O设备请求对应的I/O驱动复制至所述运行专属内存；

[0017] 根据所述执行权限请求将与所述执行权限请求对应所述指令执行权限分配至所述目标应用。

[0018] 根据本发明的另一些实施例的可信执行环境构建方法，还包括：

[0019] 若所述飞地预留内存小于所述运行内存需求对应的内存大小，重新监听所述创建请求。

[0020] 根据本发明的另一些实施例的可信执行环境构建方法，还包括：

[0021] 接收I/O设备访问请求，根据所述I/O设备访问请求匹配所述运行专属内存中的I/O驱动；

[0022] 所述I/O驱动完成与所述I/O设备访问请求对应的I/O设备的初始化。

[0023] 根据本发明的另一些实施例的可信执行环境构建方法，还包括：

[0024] 监听所述I/O设备和所述目标应用的中断状态以获取中断信息；

[0025] 对所述中断信息进行分析以重新在所述运行专属内存中获取与所述中断信息对应的I/O驱动；

[0026] 将所述中断信息发送至所述I/O驱动，所述I/O驱动将所述中断信息处理后将与所述中断信息对应的数据或回复返回至所述目标应用。

[0027] 根据本发明的另一些实施例的可信执行环境构建方法，还包括：

[0028] 接收销毁请求，

[0029] 根据所述销毁请求清空并回收所述目标应用所使用的所述运行专属内存，并恢复所述外部上下文和将所述指令执行权限返回至原始应用，所述原始应用为未分配所述可信执行环境缓存enclave前的所述目标应用。

[0030] 第二方面，本发明的一个实施例提供了可信执行环境构建系统，包括：安全监视器，所述安全监视器包括：

[0031] 飞地管理模块，用于接收创建请求，所述创建请求用于指示创建有可信执行环境缓存enclave的目标应用；

[0032] 上下文管理模块，用于根据所述创建请求对外部上下文进行保存，并验证所述创建请求对应的目标应用，得到验证成功的所述目标应用；

[0033] 所述飞地管理模块还用于根据所述创建请求分配所述可信执行环境缓存enclave的运行资源至所述目标应用，所述运行资源运行用于供所述目标应用运行。

[0034] 本发明实施例的可信执行环境构建系统至少具有如下有益效果：通过接收创建请求后，根据创建请求进行外部上下文保存，再对创建请求对应的目标应用进行验证以得到验证成功的目标应用，根据创建请求分配可信执行环境缓存enclave的运行资源至目标应用，使得目标应用根据运行资源能够正常运行，进而使用户通过目标应用能够安全地访问I/O设备，进而提高了软件运行的安全性。

[0035] 根据本发明的另一些实施例的可信执行环境构建系统，所述安全监控器还包括：

[0036] 权限管理模块，用于对目标应用所拥有的I/O设备操作权限进行管理；

[0037] 中断与异常代理模块，用于对I/O中断进行拦截与分发。

[0038] 第三方面，本发明的一个实施例提供了计算机存储介质，所述计算机可读存储介质存储有计算机可执行指令，所述计算机可执行指令用于使计算机执行如第一方面的可信执行环境构建方法的步骤。

[0039] 本发明实施例的计算机存储介质至少具有如下有益效果：通过计算机可执行指令用于使计算机执行第一方面的可信执行环境构建方法的步骤，使得可信执行环境构建方法实现简易。

[0040] 本申请的其它特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本申请而了解。本申请的目的和其他优点可通过在说明书、权利要求书以及附图中所特别指出的结构来实现和获得。

附图说明

[0041] 图1是本发明实施例中可信执行环境构建方法的一具体实施例流程示意图；

[0042] 图2是本发明实施例中可信执行环境构建方法的另一具体实施例流程示意图；

[0043] 图3是本发明实施例中可信执行环境构建方法的另一具体实施例流程示意图；

[0044] 图4是本发明实施例中可信执行环境构建方法的另一具体实施例流程示意图；

[0045] 图5是本发明实施例中可信执行环境构建方法的另一具体实施例流程示意图；

[0046] 图6是本发明实施例中可信执行环境构建方法的另一具体实施例流程示意图；

[0047] 图7是本发明实施例中可信执行环境构建系统的一具体实施例模块框图。

[0048] 附图标记：100、目标应用；200、安全监视器；210、飞地管理模块；220、上下文管理模块；230、权限管理模；240、中断与异常代理模块；300、I/O驱动。

具体实施方式

[0049] 以下将结合实施例对本发明的构思及产生的技术效果进行清楚、完整地描述，以充分地理解本发明的目的、特征和效果。显然，所描述的实施例只是本发明的一部分实施例，而不是全部实施例，基于本发明的实施例，本领域的技术人员在不付出创造性劳动的前提下所获得的其他实施例，均属于本发明保护的范围。

[0050] 在本发明的描述中，如果涉及到方位描述，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。如果某一特征被称为“设置”、“固定”、“连接”、“安装”在另一个特征，它可以直接设置、固定、连接在另一个特征上，也可以间接地设置、固定、连接、安装在另一个特征上。

[0051] 在本发明实施例的描述中，如果涉及到“若干”，其含义是一个以上，如果涉及到“多个”，其含义是两个以上，如果涉及到“大于”、“小于”、“超过”，均应理解为不包括本数，如果涉及到“以上”、“以下”、“以内”，均应理解为包括本数。如果涉及到“第一”、“第二”，应当理解为用于区分技术特征，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。

[0052] Intel SGX由Intel在2013年提出，这一技术包含了一系列新加入到Intel处理器

上的扩展指令和内存访问机制。在SGX的支持下，应用程序可以在内存中创建一个受保护的执行环境，又称飞地。每一个飞地都可以被视为一个单独的可信执行环境，飞地所使用的内存成为飞地页缓存，其安全性由基于硬件的加密机制来保证。因Arm TrustZone技术早在Armv6架构时就已提出，通过新增的处理器安全运行模式来为构建一个可信执行环境，并通过额外的硬件特性来保障可信执行环境中内存、外设等的完全隔离。AMD SEV技术沿用了Intel SGX中通过内存加密来实现可信执行环境的思想，并将这种思想推广至虚拟化环境中，允许用户在不可信的虚拟机管理器中创建一个内存完全加密的可信虚拟机。

[0053] 目前，RISC-V架构中并未直接提供硬件支持的可信执行环境，但开源的架构已经吸引了众多研究者对RISC-V架构下的可信执行环境进行探索。

[0054] 由于SGX设计的初衷并未考虑用户程序进行可信的I/O操作的需求，因此并不支持用户进行可信的系统调用。而TrustZone的设计则更多是面向硬件厂商，为一些敏感数据和关键操作预留一个可信执行环境，因此运行在可信执行环境中的程序属于系统中固件的一部分，难以在运行时动态修改和添加。虽然近年来TrustZone也被用来向应用开发者提供可信服务，但由于可拓展性较差、灵活性不足等原因，开发者实际可用的场景并不多。AMD SEV的设计倾向于云计算等虚拟化计算平台，旨在虚拟机管理器不可信的环境中保障用户虚拟机中的数据和计算的安全。然而，对于大部分非虚拟环境中的个人终端用户而言，为了保障部分计算的安全而去维护一个虚拟机的开销仍然显得过高。

[0055] Sanctum、TIMBER-V和蓬莱都需要对硬件架构进行不同程度的修改，无法直接运用于标准的RISC-V架构中，这也在一定程度上限制了他们在实际产品中的落地。对于Keystone来说，一方面，由于Keystone下的飞地需要包含运行库，这也就提高了对飞地开发者的要求，需要开发者对系统层面有一定了解才能真正有效地维护其开发的飞地的运行库。另一方面，运行在特权模式下的运行库也给予了恶意开发者更高的权限，有可能对系统造成更大的危害。虽然飞地和操作系统之间的内存隔离有效地保证了恶意开发者即使在特权模式下也不能染指操作系统的内存，但共享的I/O设备仍然使得恶意开发者有机会窃取操作系统的信息甚至阻止操作系统的正常运行。

[0056] 基于此，本申请公开了可信执行环境构建方法、系统及存储介质，能够从安全性、易用性、功能性三个方面解决现有可信执行环境的设计问题。

[0057] 参照图1，第一方面，本发明实施例公开了可信执行环境构建方法，包括：

[0058] S100、接收创建请求，创建请求用于指示创建有可信执行环境缓存enclave的目标应用；

[0059] S200、根据创建请求对外部上下文进行保存，并验证创建请求对应的目标应用，得到验证成功的目标应用；

[0060] S300、根据创建请求分配可信执行环境缓存enclave的运行资源至目标应用，运行资源运行用于供目标应用运行。

[0061] 通过系统接收创建请求，其中创建请求用于指示创建可信执行环境缓存enclave(飞地)的目标应用，通过创建可信执行环境缓存enclave(飞地)的目标应用，使得数据在目标应用进行控制更加安全。因此根据创建请求对外部上下文进行保存，然后验证创建请求对应的目标应用以得到验证成功的目标应用。得到验证成功的目标应用后根据飞地创建请求运行资源至目标应用，以便于目标应用根据运行资源运行，使得目标应用创建简易，既不

影响系统安全性，又包含了目标应用的可信执行环境缓存enclave需要运行资源，使得应用安全运行，进而提高了软件运行的安全性。

[0062] 具体地，当用户想要创建目标应用时，则发送创建请求，系统接收创建请求，系统根据创建请求触发与创建请求对应的异常，根据该异常对外部的上下文进行保存，同时对创建请求对应的目标应用进行分析验证，以判断该目标应用是否合法。若目标应用合法则认为目标应用验证成功以得到验证成功的目标应用，以分配目标应用运行所需要的运行资源至目标应用，使目标应用能够安全且正常地运行。

[0063] 在一些实施例中，创建请求包括：运行内存需求、运行程序请求、I/O设备请求、执行权限请求，运行资源包括：运行专属内存、运行程序、I/O驱动、指令执行权限。

[0064] 飞地为应用程序可以在内存中创建一个受保护的执行环境，每一个目标应用都可以被视为拥有一个单独的可信执行环境缓存enclave的应用，且飞地使用的内存称为运行专属内存，运行专属内存的安全性由基于硬件的加密机制来保障。由于建立可信执行环境，也即构建一个目标应用需要包含完整的运行资源，且目标应用所需要的运行资源包括：运行专属内存、运行程序、I/O驱动和指令执行权限中的至少一种，因此通过目标应用包含有运行专属内存、运行程序、I/O驱动和指令执行权限才能安全地运行，使应用成为目标应用后能够安全运行。

[0065] 参照图2，在一些实施例中，步骤S300包括：

[0066] S310、根据运行内存需求将飞地预留内存中与运行内存需求对应的运行专属内存分配至目标应用；

[0067] S320、根据运行程序请求将目标应用对应的运行程序复制至运行专属内存；

[0068] S330、根据I/O设备请求将与I/O设备请求对应的I/O驱动复制至运行专属内存；

[0069] S340、根据执行权限请求将与执行权限请求对应指令执行权限分配至目标应用。

[0070] 若目标应用合法则得到验证成功的目标应用，则根据运行内存需求将飞地预留内存中与运行内存需求对应的运行专属内存分配至目标应用。若飞地验证不成功，则重新提供监听创建请求。其中，在分配运行专属内存时需要判断飞地预留内存是否满足运行内存需求所对应的内存大小，若飞地预留内存大于运行内存需求对应的内存大小时，则证明飞地预留内存能够满足目标应用构建的运行内存，因此从飞地预留内存中分配一块与运行内存需求对应内存大小的运行专属内存。当运行专属内存分配完成后，根据RISC-V架构下的物理内存保护机制来保障该运行专属内存无法被目标应用以外的应用或操作系统访问，使得目标应用能够安全地运行。在分配运行专属内存至目标应用的同时，根据运行程序请求将目标应用对应的运行程序复制至运行专属内存，且根据I/O设备请求将与I/O设备请求对应的I/O驱动复制到运行专属内存中，然后再根据执行权限请求将于执行权限请求对应的指令执行权限分配至目标应用。目标应用得到指令执行权限后，可以根据运行程序、I/O驱动完成I/O设备的安全访问。通过根据I/O设备请求将与I/O设备请求对应的I/O驱动复制到对应的运行专属内存中，一方面无需将所有的I/O驱动都复制到运行专属内存中，节省了运行专属内存的空间，另一方面通过限制运行专属内存中的I/O驱动以防止目标应用随意访问I/O设备，从而提高了I/O设备访问的安全性。通过在每一个目标应用中只含有与I/O设备请求对应的I/O驱动，从而使得不同的目标应用使用不同的I/O驱动也增加了目标应用之间的隔离性，避免了目标应用之间在使用I/O设备时相互影响。

[0071] 参照图3,在一些实施例中,可信执行环境构建方法还包括:

[0072] S400、若飞地预留内存小于运行内存需求对应的内存大小,重新监听创建请求。

[0073] 若飞地预留内存小于运行内存需求对应的内存大小,则证明飞地预留内存无法满足构建一个目标应用所需要的运行专属内存,无法创建目标应用,则重新监听创建请求,以接收到创建请求中的运行内存需求对应的内存小于飞地预留内存,则可重新构建另一个目标应用。

[0074] 通过判断飞地预留内存与运行内存需求对应的内存大小,以确保飞地预留内存能满足创建一个目标应用所需要的运行专属内存,以保障目标应用能够正常运行,以实现I/O设备的安全访问。

[0075] 参照图4,在一些实施例中,可信执行环境构建方法还包括:

[0076] S500、接收I/O设备访问请求,根据I/O设备访问请求匹配运行专属内存中的I/O驱动;

[0077] S600、I/O驱动完成与I/O设备访问请求对应的I/O设备的初始化。

[0078] 其中,I/O驱动用来为目标应用提供I/O设备的访问。当目标应用需要访问I/O设备时,接收I/O设备访问请求并根据I/O设备访问请求匹配运行专属内存中的I/O驱动,I/O驱动根据I/O设备访问请求完成与I/O设备访问请求对应的I/O设备的驱动初始化,以使目标应用安全地访问I/O设备。目标应用只能根据输出的I/O设备访问请求访问时需要判断I/O设备访问请求对应的I/O驱动是否在运行专属内存中,若运行专属内存在I/O驱动,则I/O驱动完成I/O设备访问请求对应的I/O设备,若运行专属内存不存在对应的I/O驱动,则无法进行对应I/O设备的访问。通过接收I/O设备访问请求后判断I/O设备访问请求对应的I/O驱动是否存在运行专属内存,再进行I/O设备的驱动,以限制每一个目标应用可以访问的I/O设备,且访问的I/O设备通过预先复制在运行专属内存中的I/O驱动才能对I/O设备进行驱动,以由用户发送的创建请求再确定是否能对特定I/O设备进行访问,极大降低了用户所承受的风险。

[0079] 参照图5,在一些实施例中,可信执行环境构建方法还包括:

[0080] S700、监听I/O设备和目标应用的中断状态以获取中断信息;

[0081] S800、对中断信息进行分析以重新在运行专属内存中获取与中断信息对应的I/O驱动;

[0082] S900、将中断信息发送至I/O驱动,I/O驱动将中断信息处理后将与中断信息对应的数据或回复返回至目标应用。

[0083] 若I/O设备和对应的目标应用之间的连接发生中断,则拦截该中断以获取中断信息,然后对中断信息进行分析,主要分析运行专属内存中是否存在与中断信息对应的I/O驱动,若运行专属内存中存在I/O驱动,则获取与中断信息对应的I/O驱动,并将中断信息发送至可信的I/O驱动,I/O驱动将中断信息完成后会把相应数据或回复返回给目标应用,使得目标应用能够恢复访问I/O设备。若运行专属内存中不存在与中断信息对应的I/O驱动,则保存目标应用的飞地上下文,并将中断信息分发至不可信的操作系统,以通过不可信的操作系统进行监听I/O设备是否中断。

[0084] 参照图6,在一些实施例中,可信执行环境构建方法还包括:

[0085] S1000、接收销毁请求,

[0086] S1100、根据销毁请求清空并回收目标应用所使用的运行专属内存，并恢复外部上下文和将指令执行权限返回至原始应用，原始应用为未分配可信执行环境缓存enclave前的目标应用。

[0087] 当目标应用运行完成后，接收销毁请求，需要先对销毁请求进行分析验证，以判断销毁请求是否合法，若销毁请求合法，则根据销毁请求清空并回收目标应用使用的运行专属内存，并恢复外部上下文，最后将指令执行权限返回至应用，从而完成目标应用的安全访问I/O设备后，直接恢复应用与I/O设备的正常访问。若销毁请求不合法则重新监听销毁请求，以再次对销毁请求进行分析。

[0088] 下面参考图1至图6以一个具体的实施例详细描述根据本发明实施例的可信执行环境构建方法。值得理解的是，下述描述仅是示例性说明，而不是对发明的具体限制。

[0089] 当用户想要创建目标应用时，则发送创建请求，系统接收创建请求，系统根据创建请求触发与创建请求对应的异常，根据该异常对外部的上下文进行保存，同时对创建请求对应的目标应用进行分析验证，以判断该目标应用是否合法。若目标应用合法则得到验证成功的目标应用，则根据运行内存需求将飞地预留内存中与运行内存需求对应的运行专属内存分配至目标应用。若飞地验证不成功，则重新提供监听创建请求。当运行专属内存分配完成后，根据RISC-V架构下的物理内存保护机制来保障该运行专属内存无法被目标应用以外的应用或操作系统访问，使得目标应用能够安全地运行。在分配运行专属内存至目标应用的同时，根据运行程序请求将目标应用对应的运行程序复制至运行专属内存，且根据I/O设备请求将与I/O设备请求对应的I/O驱动复制到运行专属内存中，然后再根据执行权限请求将于执行权限请求对应的指令执行权限分配至目标应用。目标应用得到指令执行权限后，可以根据运行程序、I/O驱动完成I/O设备的安全访问。通过根据I/O设备请求将与I/O设备请求对应的I/O驱动复制到对应的运行专属内存中，一方面无需将所有的I/O驱动都复制到运行专属内存中，节省了运行专属内存的空间，另一方面通过限制运行专属内存中的I/O驱动以防止目标应用随意访问I/O设备，从而提高了I/O设备访问的安全性。当目标应用需要访问I/O设备时，接收I/O设备访问请求并根据I/O设备访问请求匹配运行专属内存中的I/O驱动，I/O驱动根据I/O设备访问请求完成与I/O设备访问请求对应的I/O设备的驱动初始化，以使目标应用安全地访问I/O设备。

[0090] 若I/O设备和对应的目标应用之间的连接发生中断，则拦截该中断以获取中断信息，然后对中断信息进行分析，主要分析运行专属内存中是否存在与中断信息对应的I/O驱动，若运行专属内存中存在I/O驱动，则获取与中断信息对应的I/O驱动，并将中断信息发送至可信的I/O驱动，I/O驱动将中断信息完成后会把相应数据或回复返回给目标应用，使得目标应用能够恢复访问I/O设备。

[0091] 当目标应用运行完成后，接收销毁请求，需要先对销毁请求进行分析验证，以判断销毁请求是否合法，若销毁请求合法，则根据销毁请求清空并回收目标应用使用的运行专属内存，并恢复外部上下文，最后将指令执行权限返回至应用，从而完成目标应用的安全访问I/O设备后，直接恢复应用与I/O设备的正常访问。

[0092] 参照图7，第二方面，本发明实施例还公开了可信执行环境构建系统，包括：目标应用100、安全监视器200和I/O驱动300，安全监视器200运行在RISC-V架构的设计下的机器模式，且可信驱动运行在特权模式下，目标应用100运行在用户模式下。因为RISC-V处理器及

其提供的物理内存隔离机制是可信的，所以处于硬件层的I/O设备是可信的，安全监视器200和I/O驱动300所使用的运行专属内存，且运行专属内存通过物理内存隔离机制来保证安全，从而使目标应用100能够安全地访问对应的I/O设备。

[0093] 安全监视器200用于接收创建请求，创建请求用于指示创建有可信执行环境缓存enclave的目标应用100，安全监视器200还用于根据创建请求对外部上下文进行保存，并验证创建请求对应的目标应用100；得到验证成功的目标应用100，安全监视器200还用于根据创建请求分配可信执行环境缓存enclave的运行资源至目标应用100，运行资源运行用于供目标应用100运行。

[0094] 通过安全监视器200接收目标应用100创建请求，然后根据飞地创建请求对外部上下文进行保存，并验证目标应用100创建请求对应的目标应用100，若目标应用100验证成功则分配运行资源至目标应用100，以便于目标应用100根据运行资源正常运行。

[0095] 在一些实施例中，可信执行环境构建系统还包括：安全监视器200还用于接收销毁请求，并根据销毁请求恢复外部上下文、清空和回收目标应用100的运行资源。

[0096] 其中，安全监视器200包括：飞地管理模块210、上下文管理模块220、权限管理模块230以及中断与异常代理模块240，飞地管理模块210用于根据目标应用100创建请求进行运行资源管理，创建请求用于指示创建有可信执行环境缓存enclave的目标应用。飞地管理模块210还用于接收销毁请求以清空和回收运行资源。上下文管理模块220用于根据目标应用100创建请求进行外部上下文保存，还用于根据销毁请求恢复外部上下文，且验证创建请求对应的目标应用，得到验证成功的目标应用。权限管理模块230用于对目标应用100所拥有的I/O设备操作权限进行管理，中断与异常代理模块240用于对I/O中断进行拦截与分发。

[0097] 其中，目标应用100创建请求包括：运行内存需求、运行程序请求、I/O设备请求、执行权限请求，运行资源包括：运行专属内存、运行程序、I/O驱动300、指令执行权限。

[0098] 飞地管理模块210用于运行内存需求将飞地预留内存中与运行内存需求对应运行专属内存分配至目标应用100，还用于根据运行程序请求将目标应用100对应的运行程序复制至运行专属内存；还用于根据I/O设备请求将与I/O设备请求对应的I/O驱动300复制至运行专属内存；根据执行权限请求将与执行权限请求对应指令执行权限分配至目标应用100。

[0099] 当目标应用100想要访问I/O设备时，飞地管理模块210接收I/O设备访问请求，且用于根据I/O设备访问请求匹配运行专属内存的I/O驱动300，权限管理模块230控制I/O驱动300完成与I/O设备访问请求对应的I/O设备的初始化，以实现目标应用100可以访问对应的I/O设备。

[0100] 其中，可信驱动由一组独立于操作系统的I/O设备的驱动组成，用来为目标应用100提供I/O设备的访问。目标应用100创建时，目标应用100需要向安全监视器200提供该目标应用100需要访问的I/O设备列表，而安全监视器200则会从可信驱动中将相应I/O设备的I/O驱动300拷贝到运行专属内存中。一方面，可以使得安全监视器200无需将所有驱动都拷贝至运行专属内存中，节约了运行专属内存和额外的运行专属内存拷贝。另一方面，这也有助于安全监视器200管理目标应用100对I/O设备的访问，防止恶意的目标应用100对I/O设备的未授权访问。与此同时，不同的目标应用100使用不同的I/O驱动300拷贝也增强了飞地之间的隔离性，避免了目标应用100之间在使用I/O设备时互相影响。

[0101] 首先，通过将目标应用100仅仅运行在用户模式下，使得恶意的目标应用100开发

者无法对系统或其他目标应用100造成损害。其次，完全兼容标准的RISC-V指令集和设计，无需对指令集或硬件特性进行任何新增和修改，这也使得可信执行环境构建系统具有较高的易用性，进一步促进了这一设计的推广和应用。最后，可信执行环境构建系统可以每一个目标应用100可以访问的I/O设备进行限制，可以由用户授权是否允许某一目标应用100对特定I/O设备的访问，极大地降低了用户所承受的风险。

[0102] 其中，若I/O设备和对应的目标应用100之间的连接发生中断，则中断与异常代理模块240拦截该中断以获取中断信息，然后对中断信息进行分析，主要分析运行专属内存中是否存在与中断信息对应的I/O驱动300，若运行专属内存中存在I/O驱动300，则获取与中断信息对应的I/O驱动300，并将中断信息发送至可信的I/O驱动300。I/O驱动300将中断信息完成后会把相应数据或回复返回给目标应用100，使得目标应用100能够恢复访问I/O设备。

[0103] 第三方面，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，计算机可执行指令用于使计算机执行如第一方面的可信执行环境构建方法的步骤。

[0104] 通过计算机可执行指令用于使计算机执行如第一方面的可信执行环境构建方法，使得可信执行环境构建方法执行简易。

[0105] 以上所描述的装置实施例仅仅是示意性的，其中作为分离部件说明的单元可以是或者也可以不是物理上分开的，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。

[0106] 本领域普通技术人员可以理解，上文中所公开方法中的全部或某些步骤、系统可以被实施为软件、固件、硬件及其适当的组合。某些物理组件或所有物理组件可以被实施为由处理器，如中央处理器、数字信号处理器或微处理器执行的软件，或者被实施为硬件，或者被实施为集成电路，如专用集成电路。这样的软件可以分布在计算机可读介质上，计算机可读介质可以包括计算机存储介质(或非暂时性介质)和通信介质(或暂时性介质)。如本领域普通技术人员公知的，术语计算机存储介质包括在用于存储信息(诸如计算机可读指令、数据结构、程序模块或其他数据)的任何方法或技术中实施的易失性和非易失性、可移除和不可移除介质。计算机存储介质包括但不限于RAM、ROM、EEPROM、闪存或其他存储器技术、CD-ROM、数字多功能盘(DVD)或其他光盘存储、磁盒、磁带、磁盘存储或其他磁存储装置、或者可以用于存储期望的信息并且可以被计算机访问的任何其他的介质。此外，本领域普通技术人员公知的是，通信介质通常包含计算机可读指令、数据结构、程序模块或者诸如载波或其他传输机制之类的调制数据信号中的其他数据，并且可包括任何信息递送介质。

[0107] 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。

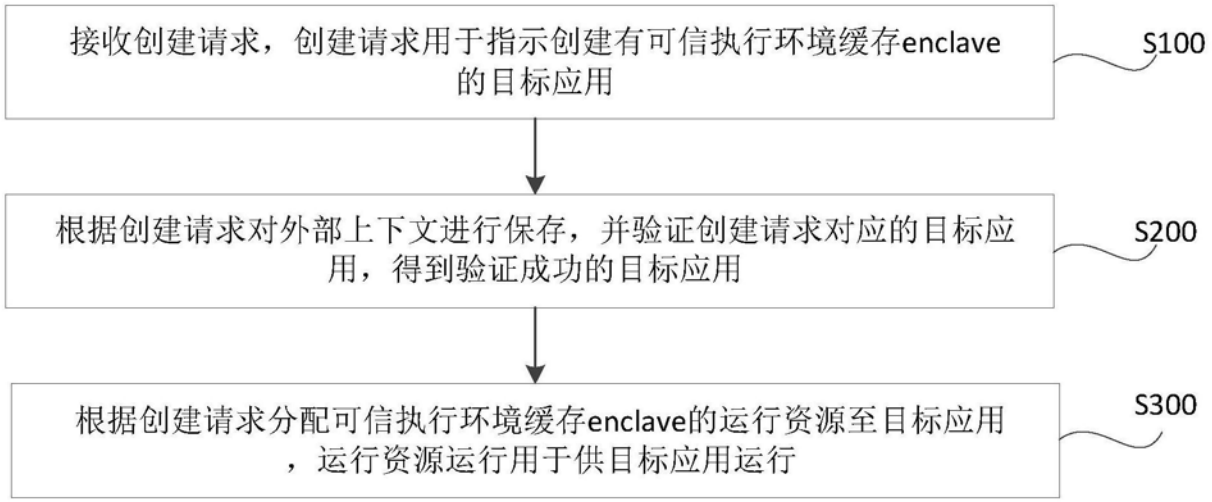

接收创建请求，创建请求用于指示创建有可信执行环境缓存enclave的目标应用
S100
根据创建请求对外部上下文进行保存，并验证创建请求对应的目标应用，得到验证成功的目标应用
S200
根据创建请求分配可信执行环境缓存enclave的运行资源至目标应用，运行资源运行用于供目标应用运行
S300

图1

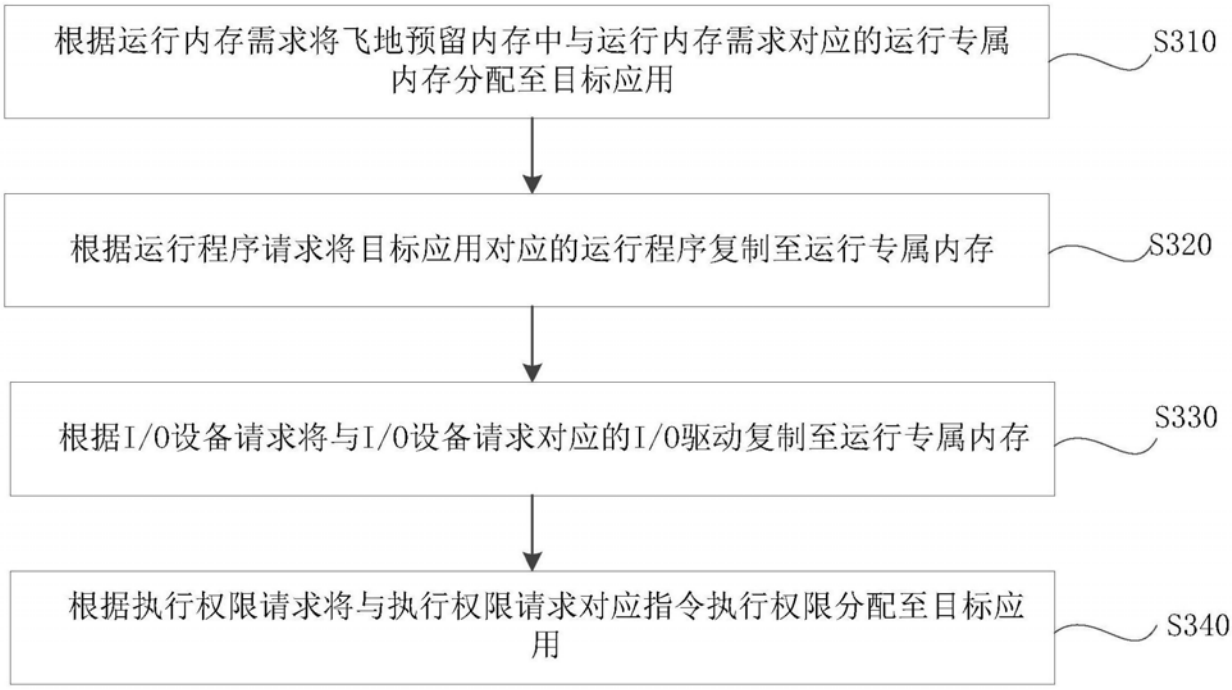

根据运行内存需求将飞地预留内存中与运行内存需求对应的运行专属内存分配至目标应用
S310
根据运行程序请求将目标应用对应的运行程序复制至运行专属内存
S320
根据I/O设备请求将与I/O设备请求对应的I/O驱动复制至运行专属内存
S330
根据执行权限请求将与执行权限请求对应指令执行权限分配至目标应用
S340

图2


根据创建请求对外部上下文进行保存，并验证创建请求对应的目标应用，得到验证成功的目标应用
S200
根据运行内存需求将飞地预留内存中与运行内存需求对应的运行专属内存分配至目标应用
S310
若飞地预留内存小于运行内存需求对应的内存大小，重新监听创建请求
S400

图3

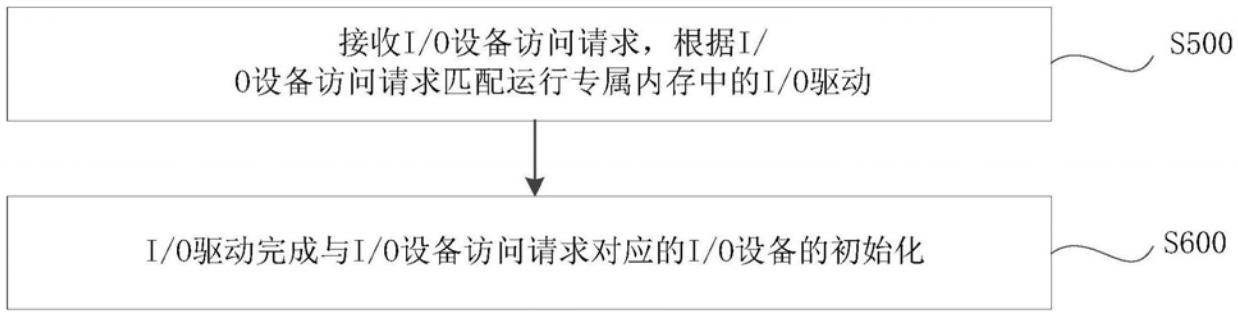

接收I/O设备访问请求，根据I/O设备访问请求匹配运行专属内存中的I/O驱动
S500
I/O驱动完成与I/O设备访问请求对应的I/O设备的初始化
S600

图4

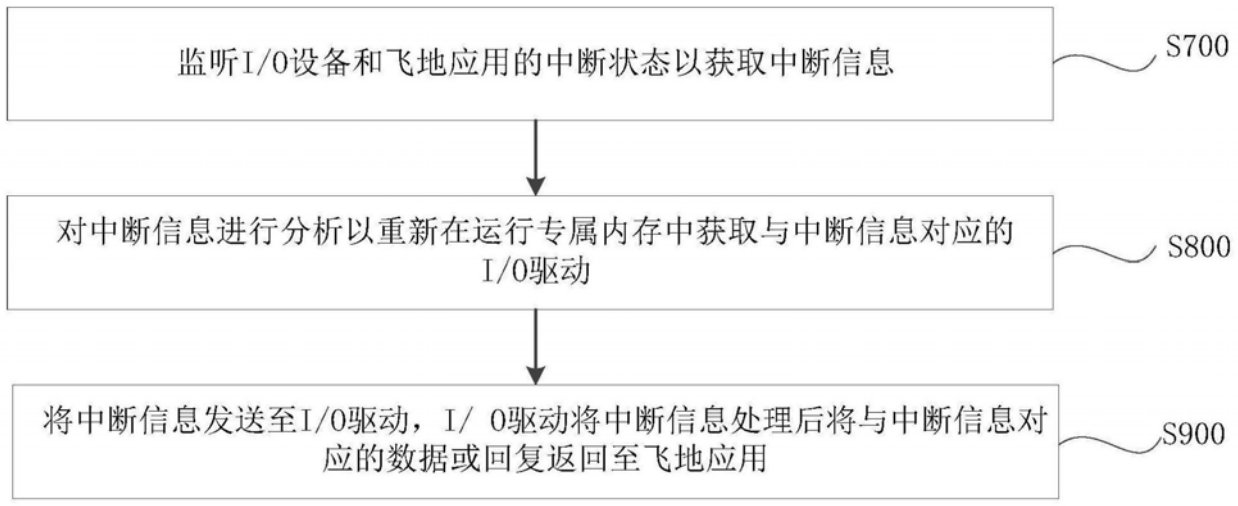

监听I/O设备和飞地应用的中断状态以获取中断信息
S700
对中断信息进行分析以重新在运行专属内存中获取与中断信息对应的I/O驱动
S800
将中断信息发送至I/O驱动，I/ O驱动将中断信息处理后将与中断信息对应的数据或回复返回至飞地应用
S900

图5


接收飞地销毁请求
S1000
根据销毁请求清空并回收目标应用所使用的运行专属内存，并恢复外部上下文和将指令执行权限返回至原始应用，原始应用为未分配可信执行环境缓存enclave前的目标应用
S1100

图6

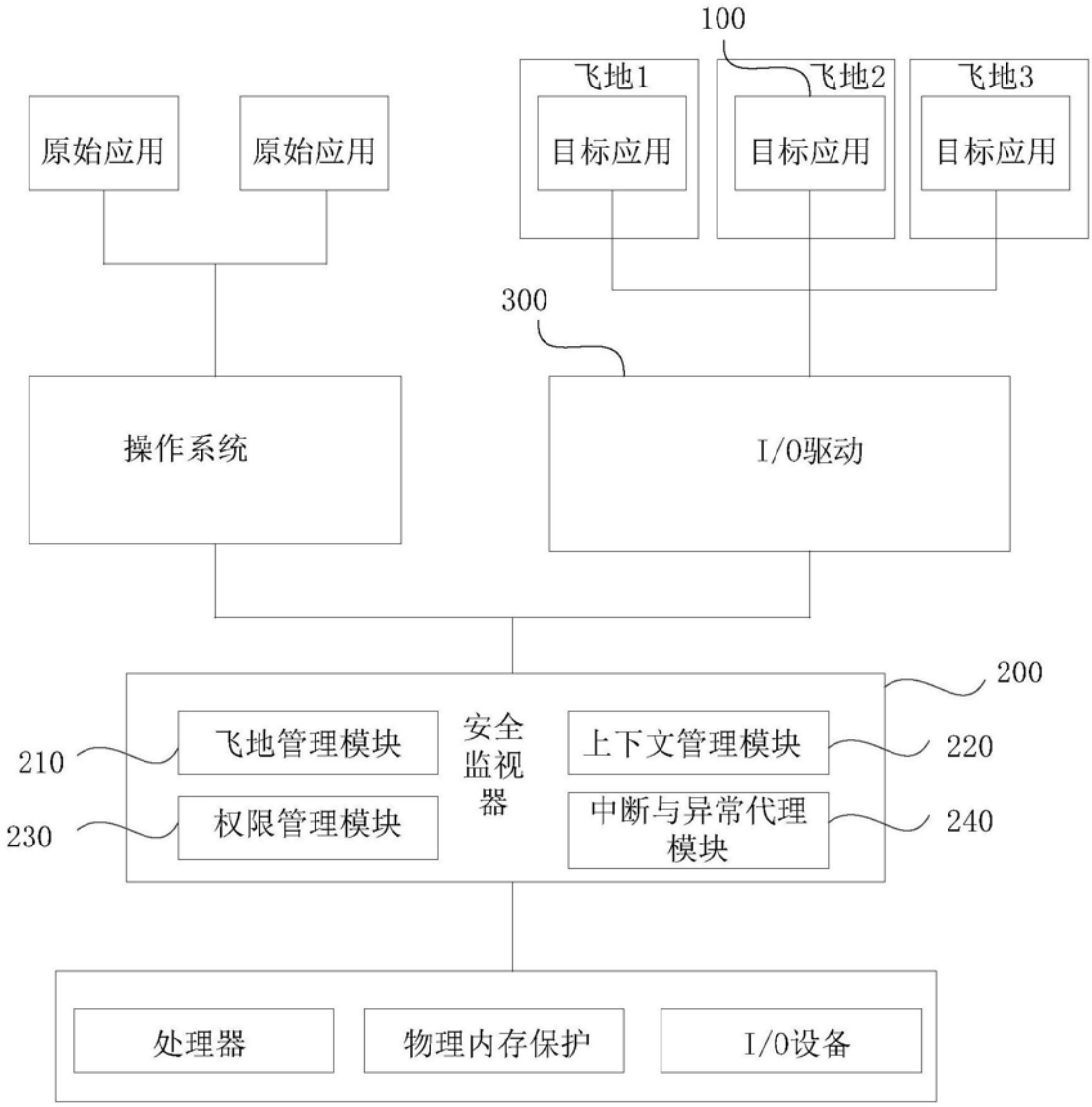

100
飞地1
飞地2
飞地3
原始应用
原始应用
目标应用
目标应用
目标应用
300
操作系统
I/O驱动
200
210
飞地管理模块
安全监视器
上下文管理模块
220
230
权限管理模块
中断与异常代理模块
240
处理器
物理内存保护
I/O设备

图7