(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115344871 A
(43)申请公布日 2022.11.15

(21)申请号 202210988426.7

(22)申请日 2022.08.17

(71)申请人 上海交通大学
地址 200240 上海市闵行区东川路800号

(72)发明人 李明煜 夏虞斌 陈海波

(74)专利代理机构 上海汉声知识产权代理有限公司 31236
专利代理师 胡晶

(51)Int.Cl.
G06F 21/57(2013.01)
G06F 21/60(2013.01)
G06F 9/455(2006.01)
G06F 11/30(2006.01)

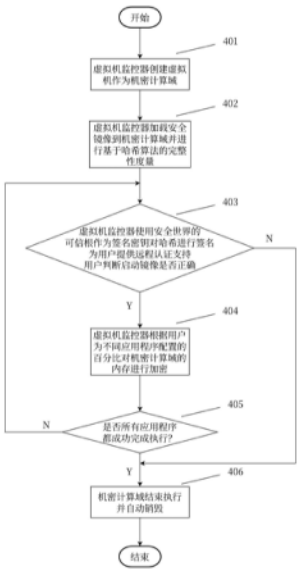
权利要求书2页 说明书5页 附图2页

(54)发明名称

基于ARM架构的机密计算环境构建方法和系统

(57)摘要

本发明提供了一种基于ARM架构的机密计算环境构建方法和系统，包括：步骤1：基于Normal World中的EL2虚拟机监控器，构建物理资源隔离域；步骤2：在机密计算域启动阶段，通过EL2虚拟机监控器对机密计算域加载的安全镜像进行基于哈希算法的完整性度量，并使用TrustZone内的安全私钥对度量生成的哈希进行签名，提供给远端用户可信的远程证明凭证；步骤3：在机密计算域运行阶段，通过EL2虚拟机监控器对机密计算域的内存进行透明加解密，机密计算域用户动态配置加密内存的百分比。本发明采用成熟的硬件虚拟化方案实现不同域的物理资源隔离，安全隔离性强、性能影响小，同时部署方便、成本低廉。



CN 115344871 A

1.一种基于ARM架构的机密计算环境构建方法,其特征在于,包括:

步骤1:基于NormalWorld中的EL2虚拟机监控器,构建3类物理资源隔离域:普通执行域、安全隔离域和机密计算域;

步骤2:在机密计算域启动阶段,通过EL2虚拟机监控器对机密计算域加载的安全镜像进行基于哈希算法的完整性度量,并使用TrustZone内的安全私钥对度量生成的哈希进行签名,提供给远端用户可信的远程证明凭证;

步骤3:在机密计算域运行阶段,通过EL2虚拟机监控器对机密计算域的内存进行透明加解密,机密计算域用户动态配置加密内存的百分比。

2.根据权利要求1所述的基于ARM架构的机密计算环境构建方法,其特征在于,所述步骤1中物理资源隔离域为虚拟机,对不同隔离域的物理内存资源、高速缓存资源、外设资源进行划分,禁止资源共享。

3.根据权利要求1所述的基于ARM架构的机密计算环境构建方法,其特征在于,所述步骤2中安全私钥是硬件生产商提供的可信根,在出厂时固化在eFUSE中。

4.根据权利要求1所述的基于ARM架构的机密计算环境构建方法,其特征在于,所述步骤3中EL2虚拟机监控器通过密码学加速器对机密计算域进行内存加密。

5.根据权利要求1所述的基于ARM架构的机密计算环境构建方法,其特征在于,所述安全镜像包括应用程序、容器和虚拟机形态。

6.一种基于ARM架构的机密计算环境构建系统,其特征在于,包括:

用户:通过网络连接机密计算域所在的虚拟机,并动态配置其加密内存的百分比;

虚拟机监控器:通过硬件虚拟化技术EL2运行多个物理资源隔离域,并提供每个域的调度和域间通信支持,以及机密计算域的内存透明加密和完整性度量支持;

虚拟机:包括机密计算域、安全隔离域和普通执行域;

硬件机器:提供硬件虚拟化和TrustZone技术,其中TrustZone提供用于签名哈希的可信根密钥;

系统运行过程为:

模块M1:基于Normal World中的EL2虚拟机监控器,构建3类物理资源隔离域:普通执行域、安全隔离域和机密计算域;

模块M2:在机密计算域启动阶段,通过EL2虚拟机监控器对机密计算域加载的安全镜像进行基于哈希算法的完整性度量,并使用TrustZone内的安全私钥对度量生成的哈希进行签名,提供给远端用户可信的远程证明凭证;

模块M3:在机密计算域运行阶段,通过EL2虚拟机监控器对机密计算域的内存进行透明加解密,机密计算域用户动态配置加密内存的百分比。

7.根据权利要求6所述的基于ARM架构的机密计算环境构建系统,其特征在于,物理资源隔离域为虚拟机,对不同隔离域的物理内存资源、高速缓存资源、外设资源进行划分,禁止资源共享。

8.根据权利要求6所述的基于ARM架构的机密计算环境构建系统,其特征在于,安全私钥是硬件生产商提供的可信根,在出厂时固化在eFUSE中。

9.根据权利要求6所述的基于ARM架构的机密计算环境构建系统,其特征在于,EL2虚拟机监控器通过密码学加速器对机密计算域进行内存加密。

10.根据权利要求6所述的基于ARM架构的机密计算环境构建系统，其特征在于，安全镜像包括应用程序、容器和虚拟机形态。

基于ARM架构的机密计算环境构建方法和系统

技术领域

[0001] 本发明涉及机密计算环境构建技术领域，具体地，涉及一种基于ARM架构的机密计算环境构建方法和系统。

背景技术

[0002] ARM的安全架构不断更新。最早在ARM v6中提出安全世界TrustZone，支持硬件级地址空间隔离和外设隔离，如今广泛用于移动端智能设备的指纹保护、人脸识别等关键服务。随着ARM在服务器领域的进一步演进，2019年ARM v8.4提出了针对TrustZone的S-EL2虚拟化技术，2021年ARM v9提出了CCA机密计算架构，引出支持内存加密和远程认证的Realm分区，用于保护服务器上的用户隐私数据。

[0003] 专利文献CN107423108A(申请号:CN201710273733.6)公开了一种基于安卓设备的ARM容器运行环境构建方法，具体地:基于ARM架构上的安卓操作系统，定制安卓内核，加入容器运行所必需的cgroup和namespace等机制;定制运行于ARM架构上的可运行容器;实现运行于安卓系统上的容器管理工具，方便容器的运行和管理;将编译后的安卓内核替换至安卓设备中，并将x86下创建的可运行容器移植至安卓设备，利用容器管理工具实现容器在安卓设备上的成功和稳定运行。

[0004] 目前，ARM上仅有TrustZone可用，用于保护用户的关键业务和敏感数据，在移动端上的广泛应用也显示其实用特性，但难以应用到服务器端。服务器端如银行、医院、政府等高敏感行业通常需要运行相对复杂的软件栈，如数据库系统、机器学习系统、大数据分析系统等，这些系统普遍采用高级语言如Python、Java进行开发，而TrustZone目前仅支持原生的C程序开发，将现有的大系统移植并适配到TrustZone需要花费大量时间和人工精力，因此对市场的大规模使用产生了制约。另一类方案是采用当前部分商用的S-EL2安全虚拟化架构，在TrustZone运行安全虚拟机，并在安全虚拟机中运行受保护的应用负载。该方案的缺点是，由于目前S-EL2的软件栈和生态均尚不成熟，难以应对现有的商业落地需求，如目前无法满足在ARM架构上同时为Normal World和Secure World(TrustZone)提供GPU安全共享支持，导致必须接入两台GPU的高昂硬件成本。另一类方案是纯硬件解决方案，即ARM v9的CCA机密计算架构，由于从硬件规范推出到真正生产落地通常需要花费5到10年的生命周期，因此从目前到未来很长一段时间内用户无法在ARM服务器上得到机密计算的安全保护。

发明内容

[0005] 针对现有技术中的缺陷，本发明的目的是提供一种基于ARM架构的机密计算环境构建方法和系统。

[0006] 根据本发明提供的基于ARM架构的机密计算环境构建方法，包括：

[0007] 步骤1:基于Normal World中的EL2虚拟机监控器，构建3类物理资源隔离域:普通执行域、安全隔离域和机密计算域;

[0008] 步骤2:在机密计算域启动阶段，通过EL2虚拟机监控器对机密计算域加载的安全

镜像进行基于哈希算法的完整性度量，并使用TrustZone内的安全私钥对度量生成的哈希进行签名，提供给远端用户可信的远程证明凭证；

[0009] 步骤3：在机密计算域运行阶段，通过EL2虚拟机监控器对机密计算域的内存进行透明加解密，机密计算域用户动态配置加密内存的百分比。

[0010] 优选的，所述步骤1中物理资源隔离域为虚拟机，对不同隔离域的物理内存资源、高速缓存资源、外设资源进行划分，禁止资源共享。

[0011] 优选的，所述步骤2中安全私钥是硬件生产商提供的可信根，在出厂时固化在eFUSE中。

[0012] 优选的，所述步骤3中EL2虚拟机监控器通过密码学加速器对机密计算域进行内存加密。

[0013] 优选的，所述安全镜像包括应用程序、容器和虚拟机形态。

[0014] 根据本发明提供的基于ARM架构的机密计算环境构建系统，包括：

[0015] 用户：通过网络连接机密计算域所在的虚拟机，并动态配置其加密内存的百分比；

[0016] 虚拟机监控器：通过硬件虚拟化技术EL2运行多个物理资源隔离域，并提供每个域的调度和域间通信支持，以及机密计算域的内存透明加密和完整性度量支持；

[0017] 虚拟机：包括机密计算域、安全隔离域和普通执行域；

[0018] 硬件机器：提供硬件虚拟化和TrustZone技术，其中TrustZone提供用于签名哈希的可信根密钥；

[0019] 系统运行过程为：

[0020] 模块M1：基于Normal World中的EL2虚拟机监控器，构建3类物理资源隔离域：普通执行域、安全隔离域和机密计算域；

[0021] 模块M2：在机密计算域启动阶段，通过EL2虚拟机监控器对机密计算域加载的安全镜像进行基于哈希算法的完整性度量，并使用TrustZone内的安全私钥对度量生成的哈希进行签名，提供给远端用户可信的远程证明凭证；

[0022] 模块M3：在机密计算域运行阶段，通过EL2虚拟机监控器对机密计算域的内存进行透明加解密，机密计算域用户动态配置加密内存的百分比。

[0023] 优选的，物理资源隔离域为虚拟机，对不同隔离域的物理内存资源、高速缓存资源、外设资源进行划分，禁止资源共享。

[0024] 优选的，安全私钥是硬件生产商提供的可信根，在出厂时固化在eFUSE中。

[0025] 优选的，EL2虚拟机监控器通过密码学加速器对机密计算域进行内存加密。

[0026] 优选的，安全镜像包括应用程序、容器和虚拟机形态。

[0027] 与现有技术相比，本发明具有如下的有益效果：

[0028] (1)本发明采用成熟的硬件虚拟化方案实现不同域的物理资源隔离，安全隔离性强、性能影响小，同时部署方便、成本低廉，无特殊硬件要求；

[0029] (2)机密计算域采用基于虚拟机监控器的内存加密支持，具备防范物理攻击的安全优势；

[0030] (3)采用国产信创厂商可信根的方式构建机密计算域的远程认证方案，满足国产信创的自主可控安全要求，可靠性高；

[0031] (4)兼容现有软硬件生态，能将普通程序直接运行在机密计算域中，同时为机密计

算域提供加速器的加速支持,如通用GPU;

[0032] (5)采用可配置窗口的内存加密方案,可以方便地针对不同应用负载调整安全和性能的比例,具有较好的灵活性。

附图说明

[0033] 通过阅读参照以下附图对非限制性实施例所作的详细描述,本发明的其它特征、目的和优点将会变得更明显:

[0034] 图1为本发明的机密计算环境构建软件流程图;

[0035] 图2为本发明的软硬件装置结构示意图。

具体实施方式

[0036] 下面结合具体实施例对本发明进行详细说明。以下实施例将有助于本领域的技术人员进一步理解本发明,但不以任何形式限制本发明。应当指出的是,对本领域的普通技术人员来说,在不脱离本发明构思的前提下,还可以做出若干变化和改进。这些都属于本发明的保护范围。

[0037] 实施例:

[0038] 本发明提供了一种适用于ARM架构的机密计算环境构建方法,该方法首先采用ARM架构支持的EL2硬件虚拟化提供三类物理资源隔离域:普通执行域、安全隔离域和机密计算域,然后通过虚拟机监控器对机密计算域提供内存加密支持,最后通过可信执行环境TrustZone的可信根提供机密计算域的完整性度量和远程验证支持,所述的构建方法包括以下步骤:

[0039] 步骤1:基于Normal World中的EL2虚拟机监控器,构建3类物理资源隔离域:普通执行域(Normal VM)、安全隔离域(Secure VM)和机密计算域(Realm VM);

[0040] 步骤2:在机密计算域(Realm VM)启动阶段,EL2虚拟机监控器对机密计算域加载的安全镜像进行基于哈希算法的完整性度量,并使用TrustZone内的安全私钥对度量生成的哈希进行签名,提供给远端用户可信的远程证明凭证;

[0041] 步骤3:在机密计算域(Realm VM)运行阶段,EL2虚拟机监控器对机密计算域的内存进行透明加解密,机密计算域用户可以动态配置加密内存的百分比。

[0042] 步骤1中物理资源隔离域为虚拟机(VM);不同隔离域的物理内存资源、高速缓存资源、外设资源都必须进行严格划分,禁止任何共享资源的存在。

[0043] 步骤2中安全私钥是硬件生产商提供的可信根(通常在出厂时固化在eFUSE中)。

[0044] 步骤3中EL2虚拟机监控器通过密码学加速器对机密计算域(Realm VM)进行内存加密。

[0045] 所述的安全镜像包括应用程序、容器、虚拟机等形态。

[0046] 本发明提供了一种适用于ARM架构的机密计算环境构建系统,包括用户、虚拟机监控器、虚拟机、硬件机器,用户通过网络连接机密计算域所在的虚拟机,并动态配置其加密内存的百分比;虚拟机监控器通过硬件虚拟化技术(EL2)运行多个物理资源隔离域,并提供每个域的调度和域间通信支持,以及机密计算域的内存透明加密和完整性度量支持;虚拟机即机密计算域、安全隔离域和普通执行域;硬件机器提供硬件虚拟化和TrustZone技术,

其中TrustZone提供用于签名哈希的可信根密钥。

[0047] 系统运行过程为:模块M1:基于Normal World中的EL2虚拟机监控器,构建3类物理资源隔离域:普通执行域、安全隔离域和机密计算域;模块M2:在机密计算域启动阶段,通过EL2虚拟机监控器对机密计算域加载的安全镜像进行基于哈希算法的完整性度量,并使用TrustZone内的安全私钥对度量生成的哈希进行签名,提供给远端用户可信的远程证明凭证;模块M3:在机密计算域运行阶段,通过EL2虚拟机监控器对机密计算域的内存进行透明加解密,机密计算域用户动态配置加密内存的百分比。

[0048] 物理资源隔离域为虚拟机,对不同隔离域的物理内存资源、高速缓存资源、外设资源进行划分,禁止资源共享。安全私钥是硬件生产商提供的可信根,在出厂时固化在eFUSE中。EL2虚拟机监控器通过密码学加速器对机密计算域进行内存加密。安全镜像包括应用程序、容器和虚拟机形态。

[0049] 如图1所示,为本发明适用于ARM的机密计算环境构建的具体流程。下面以一个机密计算域为例,结合图1对以下机密计算环境构建进行详细描述:

[0050] 在步骤401中,虚拟机监控器创建1个虚拟机,本实施例中,该新建虚拟机作为机密计算域,然后执行步骤402;

[0051] 在步骤402中,虚拟机监控器加载安全镜像到机密计算域中,并对机密计算域的内存进行基于哈希算法的完整性度量,然后执行步骤403;

[0052] 在步骤403中,虚拟机监控器使用安全世界(TrustZone)的可信根作为签名密钥对哈希进行签名,为用户提供远程认证支持,用户判断启动镜像是否正确,如果是,则执行步骤404;如果不是,则执行步骤406;

[0053] 在步骤404中,根据用户为不同应用程序配置的百分比,虚拟机监控器对机密计算域的内存进行加密,然后执行步骤405;

[0054] 在步骤405中,判断是否所有应用程序都成功完成执行,如果成功,则执行步骤406;否则,则进入步骤404中;

[0055] 在步骤406中,机密计算域结束执行,并自动销毁。

[0056] 如图2所示,本发明由ARM架构的普通世界和安全世界(即TrustZone)组成,普通世界分为虚拟机监控器和3类物理资源隔离域,分别是普通执行域(Normal VM)、安全隔离域(Secure VM)和机密计算域(Realm VM),虚拟机监控器为机密计算域提供内存加密和哈希校验支持,安全世界为哈希校验提供签名密钥支持,为机密计算域提供远程认证支持。

[0057] 本领域技术人员知道,除了以纯计算机可读程序代码方式实现本发明提供的系统、装置及其各个模块以外,完全可以通过将方法步骤进行逻辑编程来使得本发明提供的系统、装置及其各个模块以逻辑门、开关、专用集成电路、可编程逻辑控制器以及嵌入式微控制器等的形式来实现相同程序。所以,本发明提供的系统、装置及其各个模块可以被认为是一种硬件部件,而对其内包括的用于实现各种程序的模块也可以视为硬件部件内的结构;也可以将用于实现各种功能的模块视为既可以是实现方法的软件程序又可以是硬件部件内的结构。

[0058] 以上对本发明的具体实施例进行了描述。需要理解的是,本发明并不局限于上述特定实施方式,本领域技术人员可以在权利要求的范围内做出各种变化或修改,这并不影响本发明的实质内容。在不冲突的情况下,本申请的实施例和实施例中的特征可以任意相

互组合。

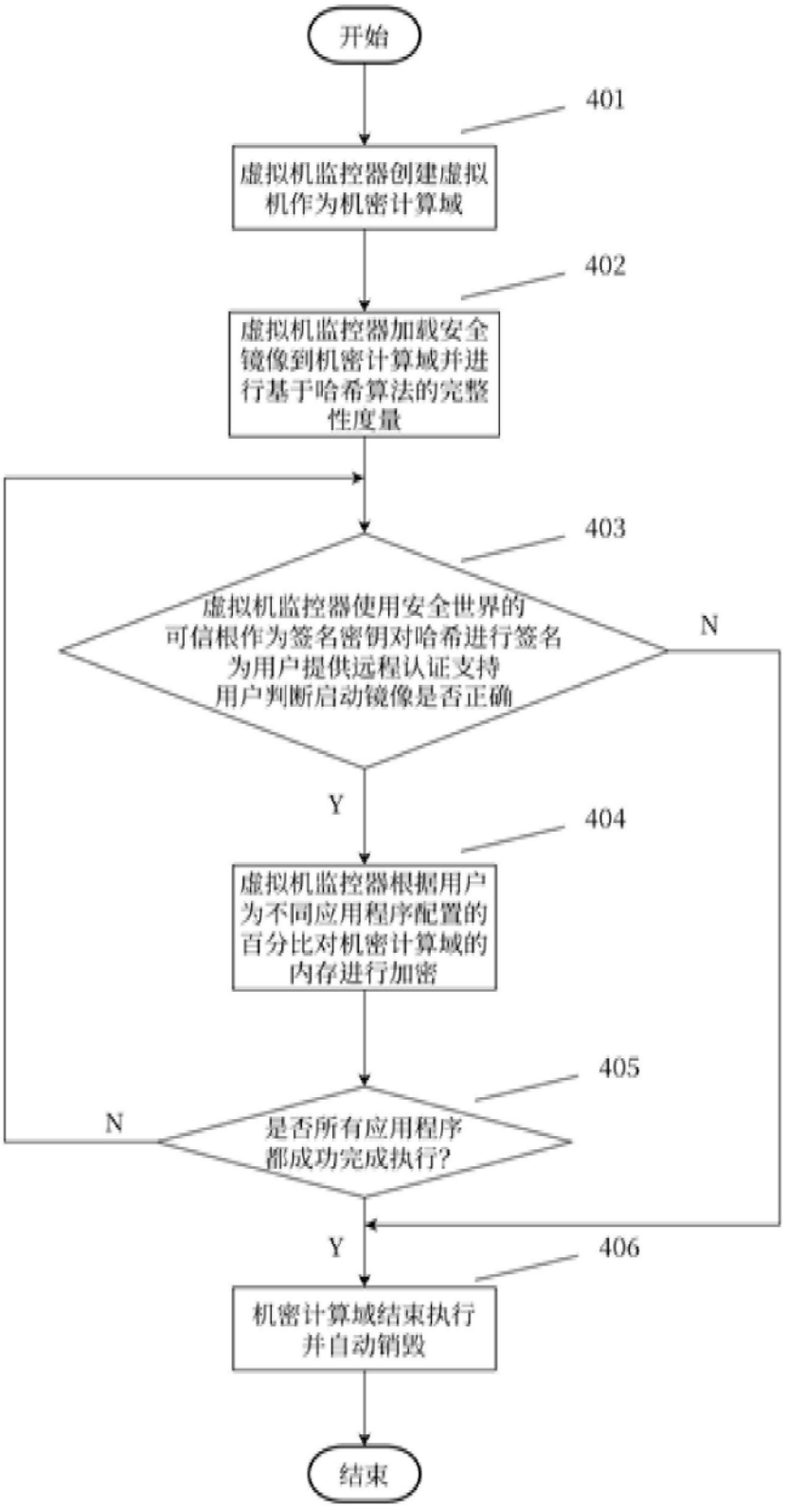

开始
401
虚拟机监控器创建虚拟机作为机密计算域
402
虚拟机监控器加载安全镜像到机密计算域并进行基于哈希算法的完整性度量
403
虚拟机监控器使用安全世界的可信根作为签名密钥对哈希进行签名为用户提供远程认证支持用户判断启动镜像是否正确
N
Y
404
虚拟机监控器根据用户为不同应用程序配置的百分比对机密计算域的内存进行加密
405
是否所有应用程序都成功完成执行?
N
Y
406
机密计算域结束执行并自动销毁
结束

图1

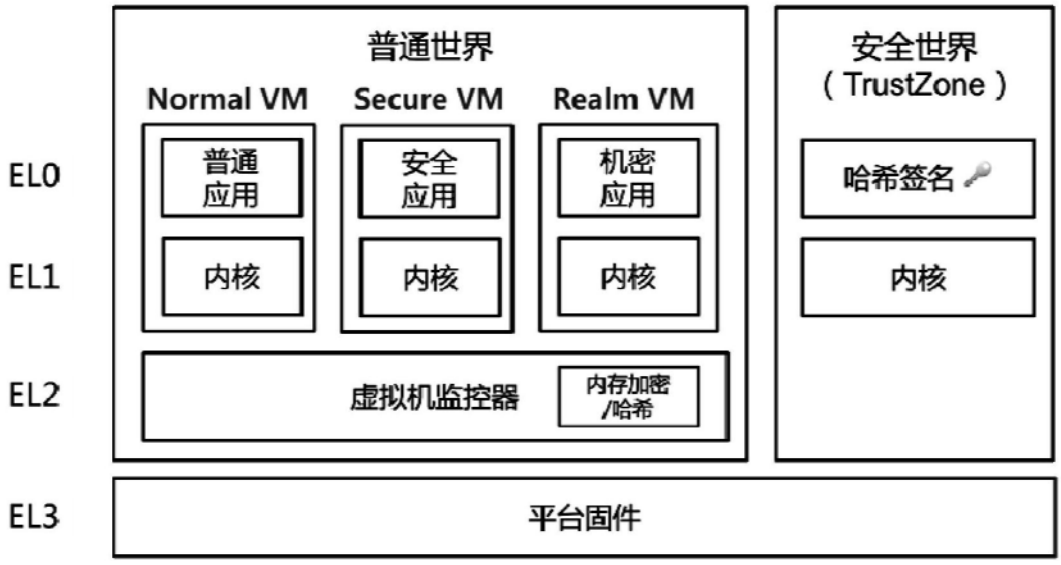

普通世界
Normal VM
Secure VM
Realm VM
普通应用
安全应用
机密应用
内核
内核
内核
虚拟机监控器
内存加密/哈希
安全世界（TrustZone）
哈希签名
内核
EL0
EL1
EL2
EL3
平台固件

图2