

LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX,
MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL,
PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US,
UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区
保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ,
NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM,
AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG,
CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,
IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,
RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI,
CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告 (条约第21条(3))。

(57) 摘要: 说明书实施例提供了一种在目标平台上启动应用程序的方法及装置, 目标平台至少包含可验证启动芯片和可信执行环境, 该方法包括: 按预设的启动次序依次启动多个系统启动项, 其中, 对于多个系统启动项中包含的第一启动项的启动包括, 对于其下一个启动项进行度量, 并将度量结果记录到可验证启动芯片中; 基于可信执行环境启动验证代理程序; 基于可信执行环境启动第一用户应用程序, 并由验证代理程序基于可信执行环境中的本地验证, 确定第一用户应用程序对应的第一验证信息。

在目标平台上启动应用程序的方法及装置

技术领域

[01] 本说明书一个或多个实施例涉及数据安全领域，尤其涉及用于在目标平台上启动应用程序的方法及装置。

背景技术

[02] 当前，在多方计算、数据外包、敏感数据处理等场景下，在计算平台上保障程序的代码/数据不被攻击者窃取或破坏，成为技术上的刚需。现有技术中，虽然有一些方案用于保障程序的代码/数据的安全，但是仍旧存在保障有漏洞、依赖远程验证服务等缺点。

[03] 因此，对于计算平台上的程序的代码/数据进行保护是亟需解决的问题。

发明内容

[04] 本说明书中的实施例旨在提供更为有效地保障计算平台上的程序的代码/数据的方法，解决现有技术中的不足。

[05] 根据第一方面，一种在目标平台上启动应用程序的方法，所述目标平台至少包含可验证启动芯片和可信执行环境，所述方法包括：按预设的启动次序依次启动多个系统启动项，其中，对于多个系统启动项中包含的第一启动项的启动包括，对于其下一个启动项进行度量，并将度量结果记录到可验证启动芯片中；基于可信执行环境启动验证代理程序；基于可信执行环境启动第一用户应用程序，并由所述验证代理程序基于可信执行环境中的本地验证，确定所述第一用户应用程序对应的第一验证信息。

[06] 在一个实施例中，所述方法还包括，将第一验证信息记录到可验证启动芯片中。

[07] 在一个实施例中，所述方法还包括，响应于所述目标平台的远程用户对所述可验证启动芯片的访问请求，向所述远程用户提供可验证启动芯片根据所述第一验证信息生成的第一记录；使得所述远程用户根据第一记录，确定第一用户应用程序的安全性，和/或，所述目标平台的安全性。

[08] 在一个实施例中，所述第一验证信息由所述验证代理程序维护；所述方法还包括，响应于远程用户对所述可验证启动芯片的访问请求，向所述远程用户提供第二记录，所述第二记录为可验证启动芯片根据所述多个系统启动项中的尾启动项启动时所记录的

第一度量结果生成；所述验证代理程序响应于所述远程用户基于第一度量结果的连接请求，建立与该远程用户的信任通道，通过所述信任通道向其提供所述第一验证信息。

[09]在一个实施例中，所述第二记录用于远程用户根据第二记录，确定所述目标平台的安全性。

[10]在一个实施例中，所述第一验证信息用于远程用户根据第一验证信息，确定第一用户应用程序的安全性。

[11]在一个实施例中，根据第二记录，确定所述目标平台的安全性，包括，根据第二记录，验证目标平台启动的操作系统 OS 和/或虚拟机监视器 VMM 的版本是否为预定版本，根据验证结果确定所述目标平台的安全性。

[12]在一个实施例中，所述可验证启动芯片包括可信平台模块 TPM 芯片、可信密码模块 TCM 芯片、可信平台控制模块 TPCM 芯片、Titan 芯片中的一种。

[13]在一个实施例中，所述方法，还包括，在启动第一用户应用程序之后：基于可信执行环境启动第二用户应用程序，由所述验证代理程序基于可信执行环境中的本地验证，确定所述第二用户应用程序对应的第二验证信息。

[14]在一个实施例中，所述多个系统启动项中的首个启动项为可信度量根核心 CRTM。

[15]在一个实施例中，所述多个系统启动项还包括，引导加载程序 BootLoader、操作系统 OS、虚拟机监视器 VMM 中的若干项。

[16]在一个实施例中，验证代理程序至少包括可信部分；所述启动验证代理程序，至少包括，在可信执行环境中执行所述可信部分；所述多个系统启动项中最后一项的启动，包括，对于所述可信部分进行度量，并将度量结果记录到可验证启动芯片中。

[17]在一个实施例中，第一用户应用程序至少包括可信部分；基于可信执行环境启动第一用户应用程序，至少包括，在可信执行环境中执行所述可信部分；所述验证代理程序基于可信执行环境中的本地验证，确定第一用户应用程序的第一验证信息，包括，所述验证代理程序基于可信执行环境中的本地验证，根据所述可信部分，确定第一用户应用程序对应的第一验证信息。

[18]在一个实施例中，所述验证代理程序基于可信执行环境中的本地验证，确定第一用户应用程序对应的第一验证信息，包括，验证代理程序调用软件保护扩展 SGX 的本地验证指令，得到第一用户应用程序对应的第一验证信息。

[19]根据第二方面,提供了一种在目标平台上启动应用程序的装置,所述目标平台至少包含可验证启动芯片和可信执行环境,所述装置包括:系统启动单元,配置为,按预设的启动次序依次启动多个系统启动项,其中,对于多个系统启动项中包含的第一启动项的启动包括,对于其下一个启动项进行度量,并将度量结果记录到可验证启动芯片中;验证代理启动单元,配置为,基于可信执行环境启动验证代理程序;用户应用启动单元,配置为,基于可信执行环境启动第一用户应用程序,并由所述验证代理程序基于可信执行环境中的本地验证,确定所述第一用户应用程序对应的第一验证信息。

[20]根据第三方面,提供了一种计算机可读存储介质,其上存储有计算机程序,当所述计算机程序在计算机中执行时,令计算机执行第一方面所述的方法。

[21]根据第四方面,提供了一种计算设备,包括存储器和处理器,其特征在于,所述存储器中存储有可执行代码,所述处理器执行所述可执行代码时,实现第一所述的方法。

[22]利用以上各个方面中的方法、装置、计算设备、存储介质中的一个或多个,可以更有效地解决保障计算平台上的程序的代码/数据的问题。

附图说明

[23]为了更清楚说明本发明实施例的技术方案,下面将对实施例描述中所需使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

[24]图1示出根据本说明书实施例的一种在目标平台上启动应用程序的方法的原理示意图;

[25]图2示出根据本说明书实施例的一种在目标平台上启动应用程序的方法的流程图;

[26]图3示出根据本说明书实施例的一种在目标平台上启动应用程序的方法的一种实施方式的流程图;

[27]图4示出根据本说明书实施例的一种在目标平台上启动应用程序的方法的又一种实施方式的流程图;

[28]图5示出根据本说明书实施例的一种在目标平台上启动应用程序的装置的结构图;

具体实施方式

[29]下面将结合附图，对本发明书提供的方案进行描述。

[30]如前所述，目前的保障程序的代码/数据的安全的方法，仍旧存在保障有漏洞、依赖远程验证服务等缺点。发明人对于启动程序的代码/数据的现有的保障方法进行了研究，并得到以下结论。

[31]目前，常用的计算平台上程序的代码/数据的保障方法，主要有基于可验证启动的方案和基于可信执行环境的方案。其中，可验证启动是指，具备逐级完整性校验的系统启动过程。基于可验证启动方案的原理为，系统从可信根出发，一步一步启动到用户程序，每启动一步都对下一步启动项进行度量、校验，并写入可验证启动芯片中的可信记录。以采用 TPM (Trusted Platform Module) 技术为例，即是下一步启动项的哈希值写入 TPM 芯片中的平台配置寄存器 PCR 中。用户可以远程调取启动可信记录（该记录会被签名来保证完整性和真实性）来判定系统是否维持了预期的启动项及启动顺序。然而，可验证启动的缺点在于，只能保证启动时的安全，如果是启动之后完成的动态攻击，该方案很难检测和抵御。

[32]可信执行环境是指加密或隔离的、因而被认为安全可信的执行环境，因此，代码和数据在加密或隔离的环境里不易受来自环境外的攻击。基于可信执行环境 (Trusted Execution Environment, 简称 TEE) 的方案原理为，将高权限的操作系统 OS 或虚拟机管理器 (Virtual Machine Monitor, 简称 VMM) 排除在信任基 (Trusted Computing Base, 简称 TCB) 之外，让用户放心地在不可信的操作系统或 VMM 之上运行需要保护的代码和数据，并提供远程校验的能力。然而，基于可信执行环境的方案的首要缺点是只防御来自恶意操作系统或 VMM 的直接攻击，却无法抵御侧信道攻击 (Side-channel Attack)。此外，基于可信执行环境的方案多少都依赖第三方厂商提供的远程校验服务，产生了外部可用性 (Availability) 依赖，同时也需要假设这些第三方厂商不会作恶（例如，假设不发生共谋攻击 Collusion Attack 或内部攻击 Insider Attack）。

[33]发明人为了解决上述技术方案存在的问题，在本说明书中的实施例中，提出一种在目标平台上启动应用程序的方法及装置。在该方案中，一方面，将用户应用程序的可信逻辑放在可信执行环境里隔离执行，从而防止恶意 VMM/操作系统的（非侧信道）直接攻击；另一方面，用户在验证程序时可以同时获取启动链和平台的校验信息，从而能验证所启动的 VMM/操作系统是预期状态（例如是一个可信的、TCB 很小的、具备侧信道攻

击监控的版本)，既而提高对侧信道攻击的防御能力。再一方面，程序验证建立在可验证启动和本地验证相结合的机制上，不需要依赖诸如 IAS 之类的外部可信执行环境校验服务，大大提升了程序验证的可靠性和安全性。

[34]下面进一步说明该方法的基本思想。

[35]图 1 示出根据本说明书实施例的一种在目标平台上启动应用程序的方法的原理示意图。如图 1 所示，目标平台至少包含可验证启动芯片、可信执行环境、以及多个启动项，多个启动项按启动次序包括多个系统启动项（如图中 1 所示 CRTM、Bootloader/OS，第一个系统启动项为可信度量根核心 CRTM）、验证代理程序、若干用户应用程序（用户应用 1、用户应用 2）。首先，依次启动多个系统启动项，在任意一个系统启动项的启动中，对于其下一个启动项进行度量，并将度量结果记录到可验证启动芯片中。然后，在 TEE 中启动验证代理程序（或其可信部分）。最后，启动用户应用程序，验证代理程序至少通过调用可信执行环境中的本地验证，得到该用户应用程序对应的验证信息，验证代理程序可以维护用户应用程序对应的验证信息，也可以将其记录到可验证启动芯片中。

[36]使用该方法在目标平台上启动应用程序，在可信执行环境里执行用户应用程序，可以防止来自恶意 VMM/操作系统的攻击，并且，在可信执行环境对应用程序的验证中，通过验证代理程序调用本地验证进行，不再依赖外部可信执行环境校验服务。还可以利用可验证启动芯片根据记录到其中的度量/验证信息生成的可信纪录，验证所启动的程序和 VMM/操作系统是否为预期状态，进而根据验证结果对侧信道攻击进行防御。

[37]下面进一步阐述该方法的具体过程。

[38]图 2 示出根据本说明书实施例的一种在目标平台上启动应用程序的方法的流程图。目标平台至少包含可验证启动芯片和可信执行环境，该方法至少包括如下步骤。

[39]在步骤 21，按预设的启动次序依次启动多个系统启动项，其中，对于多个系统启动项中包含的第一启动项的启动包括，对于其下一个启动项进行度量，并将度量结果记录到可验证启动芯片中。

[40]如前所述，可验证启动是指具备逐级完整性校验的系统启动过程，其原理是对启动项进行可以据以施行逐级完整性校验的可信纪录，该可信纪录通常是依赖于独立的可验证启动芯片实现。在不同的实施例中，可验证启动芯片可以采用不同种类的可验证启动芯片，本说明书对于具体采用何种可验证启动芯片不做限定。在一个实施例中，可验证启动芯片可以包括可信平台模块 TPM 芯片、可信密码模块 TCM 芯片、可信平台控制模

块 TPCM 芯片、Titan 芯片中的一种。

[41]对启动项的度量(measurement)可以包括,对启动项内容的汇总、表征或是标识。根据一种实施方式,可以对下一个启动项进行哈希(hash)计算,从而获得其度量结果。在另一个例子中,也可以对下一个启动项的 hash 计算的结果,进行 hash 扩展后获取度量结果进行纪录。所谓的 hash 扩展是指根据先获得 hash 计算结果,和添加的计算项,进行一次以上嵌套的 hash 运算,以获得计算结果的过程。

[42]在一个实施例中,在该步骤中,系统启动顺序如图 1 所示,可信度量根核心(CRTM,Core Root of Trust Measurement),是目标平台最开始的启动组件,也是整个系统的可信根基。CRTM 启动后会启动下一个启动项(例如,基本输入输出系统 BIOS),然后 BIOS 会启动进一步的启动项(例如引导加载程序 Bootloader、VMM、操作系统等等),如此迭代,直到启动用户态程序。在此过程中,为了建立启动关系的信任链,像常规可验证启动一样,CRTM 启动后会对下一个启动项(例如 BIOS)予以度量,然后 BIOS 会对进一步的启动项(例如 Bootloader)予以度量,直到度量到用户态程序。每一个度量结果都会写入相应的可信记录(可验证芯片中)里,事后可以出示给远程用户。

[43]在一个实施例中,多个系统启动项中的首个启动项为可信度量根核心 CRTM。在另一个实施例中,多个系统启动项还可以包括,引导加载程序 BootLoader、操作系统 OS、虚拟机监视器 VMM 中的若干项。在又一个实施例中,也可以采用动态 CRTM(D-CRTM, Dynamic CRTM)方案,在 D-CRTM(Dynamic CRTM)方案中, BIOS 先于 D-CRTM 启动,在 BIOS 启动中激发动态启动事件 DL Event(dynamic launch event),从而启动 D-CRTM,但是 BIOS 启动中,并不会对于下一个启动项的度量,并记录到可启动验证芯片。也就是说,无论是采用常规 CRTM(或称静态 CRTM, S-CRTM, Static CRTM)、或是 D-CRTM,对于下一个启动项的度量,并记录到可启动验证芯片,均由 CRTM(S-CRTM 或 D-CRTM)启动开始。

[44]在一个实施例中,在最后一个系统启动项的启动中,对于验证代理程序进行度量,并将度量结果记录到可验证启动芯片中。该实施例的详情将在本说明书后文中阐述。

[45]在步骤 22,基于可信执行环境启动验证代理程序。

[46]可信执行环境(TEE),是主处理器(CPU)中的一个安全区域,作为一种隔离执行环境,它可以确保在内部加载的代码和数据在机密性和完整性方面得到保护。例如,TEE 提供了通过 TEE 隔离执行的应用程序的完整性以及其资源的机密性。或者说,TEE

提供了一个执行空间，该执行空间为设备上运行的受信任应用程序提供了比操作系统（OS）高的安全性。

[47]在不同的实施例，TEE可以在不同的主处理器上实现，而在不同的主处理器上实现TEE具有不同的具体实施方式。例如在某种CPU上实现TEE的SGX方案，在另一种CPU实现TEE的TrustZone方案，等等。本说明书对TEE的具体实施方式不做限制。

[48]该步骤中，与常规可验证启动不同的是，在用户程序Apps之前启动一个验证代理程序。验证代理程序和未来要启动的用户程序Apps一样借助可信执行环境技术运行。在一个例子中，可以将验证代理程序的可信部分（Trusted Logic）加载到可信执行环境里隔离加密执行。

[49]与常规可验证方式启动不同之处还在于，常规可验证启动方式由在系统启动项的启动过程中直接进入对用户程序Apps进行度量。而本说明书实施例中，如上文所述的，在多个系统启动项中最后一项的启动中，对于验证代理程序进行度量并将度量结果记录到可验证启动芯片中。也就是说系统项的最后度量和纪录结果的对象不同。在一个实施例中，验证代理程序可以至少包括可信部分。该实施例中，在步骤21中对于多个系统启动项中最后一项的启动，其具体实施方式可以是，对于所述可信部分进行度量，并将度量结果记录到可验证启动芯片中。

[50]在步骤23，基于可信执行环境启动第一用户应用程序，并由验证代理程序基于可信执行环境中的本地验证，确定第一用户应用程序对应的第一验证信息。

[51]该步骤中，在验证代理程序之后启动的用户应用程序，由验证代理程序至少通过调用可信执行环境中的本地验证，获取其验证信息。例如，在一个例子中，可以在SGX平台上调用SGX的本地验证（Local Attestation），获取应用程序的验证信息。在另一个例子中，验证代理程序也可以在调用可信执行环境中的本地验证对该用户程序进行验证获得的信息的基础上，叠加其他数据项后进行扩展计算，如hash扩展计算后，获得该应用程序的验证信息。本质上，由于验证代理程序和用户应用程序运行在同一目标平台上的TEE中，因此，验证代理程序可以通过调用TEE中的本地验证(Local Attestation)来实现对用户应用程序的身份验证，而避免借助于第三方的远程验证。

[52]在一个实施例中，第一用户应用程序可以至少包括可信部分；在可信执行环境中执行所述可信部分；验证代理程序基于可信执行环境中的本地验证，根据所述第一用户应用程序的可信部分，确定对应的第一验证信息。在一个具体的实施例中，验证代理程序

可以调用软件保护扩展 SGX 的本地验证指令，得到第一用户应用程序对应的第一验证信息。

[53] 在一个实施例中，还可以在启动第一用户应用程序之后，基于可信执行环境启动第二用户应用程序，由所述验证代理程序基于可信执行环境中的本地验证，确定所述第二用户应用程序对应的第二验证信息。也就是说，在验证代理程序启动之后启动的各个用户应用程序，均由验证代理程序基于 TEE 中的本地验证，确定其验证信息。这与可验证启动中，链式地依次验证下一启动程序的方式，再次形成不同。

[54] 在不同的实施方式中，用户应用程序对应的验证信息，可以被写入可验证启动芯片，也可以不被写入该芯片、而仅由验证代理程序维护，从而可以对上述启动程序进行远程验证的用户提供不同的远程校验方式。

[55] 因此，根据一种实施方式，如图 3 所示，可以将第一验证信息记录到可验证启动芯片中。在一个实施例中，当目标平台的远程用户希望对目标平台的安全性进行远程校验时，该用户可以对目标平台中的可验证启动芯片发出访问请求。响应于该访问请求，目标平台可以向所述远程用户提供可验证启动芯片根据所述第一验证信息生成的第一记录。如此，该远程用户可以根据该第一记录，确定第一用户应用程序的安全性，和/或，所述目标平台的安全性。

[56] 在该实施方式中的一个例子中，远程用户可以在其自己的平台上根据目标平台上的启动项的程序版本号，搭建与目标平台相同的运行环境，并据以获得第一记录的对应值，根据第一记录的对应值和第一记录，确定目标平台启动链上各启动项（包括系统启动项和用户应用程序启动项）的安全性。在一个例子中，如果第一记录的对应值和第一记录相匹配，则说明目标平台的启动链上各启动项均是完整和正确的，也就是说目标平台和其上启动的应用程序均是安全的；如果第一记录的对应值和第一记录不匹配，则说明目标平台启动链上各启动项中至少有一项是不完整或不正确的，也就是说目标平台和其上启动的应用程序中有一项或多项是不安全的。

[57] 在该实施方式中的另一个例子中，远程用户也可以从例如信任的第三方获得第一记录的对应值，其余的执行过程同于上一个例子中执行过程中相应的部分，这里不再赘述。

[58] 根据另一种实施方式，如图 4 所示，第一验证信息可以由验证代理程序维护。在一个实施例中，在目标平台的远程用户希望对目标平台的安全性进行远程校验时，该用户仍然可以对目标平台中的可验证启动芯片发出访问请求。响应于该访问请求，目标平台

向该远程用户提供第二记录，所述第二记录为可验证启动芯片根据所述多个系统启动项中的尾启动项启动时所记录的第一度量结果生成。需要理解，尾启动项是最后一个系统启动项，在其之后启动的程序为验证代理程序，因此，尾启动项启动时所记录的第一度量结果，即对应于验证代理程序的度量结果。于是，远程用户可以基于该第一度量结果，向该验证代理程序发出连接请求。响应于该连接请求，验证代理程序可以建立与该远程用户的信任通道，通过所述信任通道向其提供所述第一验证信息。

[59] 在一个例子中，第一验证信息可以用于远程用户根据第一验证信息，确定第一用户应用程序的安全性。另一个例子中，第二记录可以用于第一远程用户根据第二记录，确定所述目标平台的安全性。在一个具体的例子中，第二记录可以用于第一远程用户根据第二记录，验证目标平台启动的操作系统 OS 和/或虚拟机监视器 VMM 的版本是否为预定版本，根据验证结果确定所述目标平台的安全性。

[60] 具体的，远程用户可以在其自己的平台上根据目标平台上的各启动项的程序版本号，搭建与目标平台相同的运行环境，从而获得其自己平台上第二记录和第一验证信息的对应值，根据第二记录的对应值和第二记录，确定目标平台上启动链上系统启动项和验证代理程序的安全的。在一个例子中，如果第二记录的对应值和第二记录相匹配，则可确定目标平台上启动链上各系统启动项和验证代理程序均是完整的、正确的，也就是说可以确定目标平台运行的系统是安全的。然后，在另一个例子中，还可以根据第一验证信息的对应值和第一验证信息，确定第一用户应用程序的完整性和正确性，如果第一验证信息的对应值和第一验证信息相匹配，则可确定第一用户应用程序安全的。

[61] 在另一个例子中，远程用户也可以从例如信任的第三方获得第二记录和第一验证信息的对应值，其余的执行过程同于上一个例子中执行过程中相应的部分，这里不再赘述。

[62] 图 5 示出根据本说明书实施例的一种在目标平台上启动应用程序的装置的结构图。目标平台至少包含可验证启动芯片和可信执行环境，如图 5 所示，该装置 500 包括：系统启动单元 51，配置为，按预设的启动次序依次启动多个系统启动项，其中，对于多个系统启动项中包含的第一启动项的启动包括，对于其下一个启动项进行度量，并将度量结果记录到可验证启动芯片中；验证代理启动单元 52，配置为，基于可信执行环境启动验证代理程序；用户应用启动单元 53，配置为，基于可信执行环境启动第一用户应用程序，并由所述验证代理程序基于可信执行环境中的本地验证，确定所述第一用户应用程序对应的第一验证信息。

[63] 在一个实施例中，该装置 500 还可以包括，记录单元，配置为，将第一验证信息记

录到可验证启动芯片中。

[64]在一个例子中，该装置 500 还可以包括，第一响应单元，配置为，响应于所述目标平台的远程用户对所述可验证启动芯片的访问请求，向所述远程用户提供可验证启动芯片根据所述第一验证信息生成的第一记录；使得所述远程用户根据第一记录，确定第一用户应用程序的安全性，和/或，所述目标平台的安全性。

[65]在一个实施例，用户应用启动单元 53，可以进一步配置为，所述第一验证信息由所述验证代理程序维护；该装置 500 还可以包括，第二响应单元，配置为，响应于远程用户对所述可验证启动芯片的访问请求，向所述远程用户提供第二记录，所述第二记录为可验证启动芯片根据所述多个系统启动项中的尾启动项启动时所记录的第一度量结果生成；第三响应单元，配置为，所述验证代理程序响应于所述远程用户基于第一度量结果的连接请求，建立与该远程用户的信任通道，通过所述信任通道向其提供所述第一验证信息。

[66]在一个例子中，所述第二记录用于远程用户根据第二记录，确定所述目标平台的安全性。

[67]在一个例子中，所述第一验证信息可以用于远程用户根据第一验证信息，确定第一用户应用程序的安全性。

[68]第二响应单元，可以进一步配置为，根据第二记录，确定所述目标平台的安全性，包括，根据第二记录，验证目标平台启动的操作系统 OS 和/或虚拟机监视器 VMM 的版本是否为预定版本，根据验证结果确定所述目标平台的安全性。

[69]在一个实施例，所述可验证启动芯片可以包括可信平台模块 TPM 芯片、可信密码模块 TCM 芯片、可信平台控制模块 TPCM 芯片、Titan 芯片中的一种。

[70]在一个实施例，用户应用启动单元，可以进一步配置为，在启动第一用户应用程序之后：基于可信执行环境启动第二用户应用程序，用户应用启动单元，可以进一步配置为，由所述验证代理程序基于可信执行环境中的本地验证，确定所述第二用户应用程序对应的第二验证信息。

[71]在一个实施例，多个系统启动项中的首个启动项可以为可信度量根核心 CRTM。在一个例子中，多个系统启动项还可以包括，引导加载程序 BootLoader、操作系统 OS、虚拟机监视器 VMM 中的若干项。

[72]在一个实施例，验证代理程序可以至少包括可信部分；验证代理启动单元，可以

进一步配置为，在可信执行环境中执行所述可信部分；系统启动单元，可以进一步配置为，对于所述可信部分进行度量，并将度量结果记录到可验证启动芯片中。

[73] 在一个实施例中，第一用户应用程序至少包括可信部分；用户应用启动单元，可以进一步配置为，在可信执行环境中执行所述可信部分；所述验证代理程序基于可信执行环境中的本地验证，根据所述可信部分，确定第一用户应用程序对应的第一验证信息。

[74] 在一个实施例中，用户应用启动单元，可以进一步配置为，验证代理程序调用软件保护扩展 SGX 的本地验证指令，得到第一用户应用程序对应的第一验证信息。

[75] 本说明书另一方面提供一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行上述任一项方法。

[76] 本说明书另一方面提供一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现上述任一项方法。

[77] 需要理解，本文中的“第一”，“第二”等描述，仅仅为了描述的简单而对相似概念进行区分，并不具有其他限定作用。

[78] 本领域技术人员应该可以意识到，在上述一个或多个示例中，本发明所描述的功能可以用硬件、软件、固件或它们的任意组合来实现。当使用软件实现时，可以将这些功能存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令或代码进行传输。

[79] 以上所述的具体实施方式，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施方式而已，并不用于限定本发明的保护范围，凡在本发明的技术方案的基础之上，所做的任何修改、等同替换、改进等，均应包括在本发明的保护范围之内。

权利要求书

1.一种在目标平台上启动应用程序的方法,所述目标平台至少包含可验证启动芯片和可信执行环境,所述方法包括:

按预设的启动次序依次启动多个系统启动项,其中,对于多个系统启动项中包含的第一启动项的启动包括,对于其下一个启动项进行度量,并将度量结果记录到可验证启动芯片中;

基于可信执行环境启动验证代理程序;

基于可信执行环境启动第一用户应用程序,并由所述验证代理程序基于可信执行环境中的本地验证,确定所述第一用户应用程序对应的第一验证信息。

2.根据权利要求1所述的方法,还包括,将第一验证信息记录到可验证启动芯片中。

3.根据权利要求2所述的方法,还包括,

响应于所述目标平台的远程用户对所述可验证启动芯片的访问请求,向所述远程用户提供可验证启动芯片根据所述第一验证信息生成的第一记录;使得所述远程用户根据第一记录,确定第一用户应用程序的安全性,和/或,所述目标平台的安全性。

4.根据权利要求1所述的方法,其中,所述第一验证信息由所述验证代理程序维护;所述方法还包括,

响应于远程用户对所述可验证启动芯片的访问请求,向所述远程用户提供第二记录,所述第二记录为可验证启动芯片根据所述多个系统启动项中的尾启动项启动时所记录的第一度量结果生成;

所述验证代理程序响应于所述远程用户基于第一度量结果的连接请求,建立与该远程用户的信任通道,通过所述信任通道向其提供所述第一验证信息。

5.根据权利要求4所述的方法,其中,所述第二记录用于远程用户根据第二记录,确定所述目标平台的安全性。

6.根据权利要求4所述的方法,其中,所述第一验证信息用于远程用户根据第一验证信息,确定第一用户应用程序的安全性。

7.根据权利要求5所述的方法,其中,根据第二记录,确定所述目标平台的安全性,包括,根据第二记录,验证目标平台启动的操作系统 OS 和/或虚拟机监视器 VMM 的版本是否为预定版本,根据验证结果确定所述目标平台的安全性。

8.根据权利要求1所述的方法,其中,所述可验证启动芯片包括可信平台模块 TPM 芯片、可信密码模块 TCM 芯片、可信平台控制模块 TPCM 芯片、Titan 芯片中的一种。

9.根据权利要求1所述的方法,还包括,在启动第一用户应用程序之后:

基于可信执行环境启动第二用户应用程序，

由所述验证代理程序基于可信执行环境中的本地验证，确定所述第二用户应用程序对应的第二验证信息。

10.根据权利要求 1 所述的方法，其中，所述多个系统启动项中的首个启动项为可信度量根核心 CRTM。

11.根据权利要求 10 所述的方法，其中，所述多个系统启动项还包括，引导加载程序 BootLoader、操作系统 OS、虚拟机监视器 VMM 中的若干项。

12.根据权利要求 1 所述的方法，其中，验证代理程序至少包括可信部分；

所述启动验证代理程序，至少包括，在可信执行环境中执行所述可信部分；

所述多个系统启动项中最后一项的启动，包括，对于所述可信部分进行度量，并将度量结果记录到可验证启动芯片中。

13.根据权利要求 1 所述的方法，其中，第一用户应用程序至少包括可信部分；

基于可信执行环境启动第一用户应用程序，至少包括，在可信执行环境中执行所述可信部分；

所述验证代理程序基于可信执行环境中的本地验证，确定第一用户应用程序的第一验证信息，包括，

所述验证代理程序基于可信执行环境中的本地验证，根据所述可信部分，确定第一用户应用程序对应的第一验证信息。

14.根据权利要求 1 所述的方法，所述验证代理程序基于可信执行环境中的本地验证，确定第一用户应用程序对应的第一验证信息，包括，验证代理程序调用软件保护扩展 SGX 的本地验证指令，得到第一用户应用程序对应的第一验证信息。

15.一种在目标平台上启动应用程序的装置，所述目标平台至少包含可验证启动芯片和可信执行环境，所述装置包括：

系统启动单元，配置为，按预设的启动次序依次启动多个系统启动项，其中，对于多个系统启动项中包含的第一启动项的启动包括，对于其下一个启动项进行度量，并将度量结果记录到可验证启动芯片中；

验证代理启动单元，配置为，基于可信执行环境启动验证代理程序；

用户应用启动单元，配置为，基于可信执行环境启动第一用户应用程序，并由所述验证代理程序基于可信执行环境中的本地验证，确定所述第一用户应用程序对应的第一验证信息。

16.一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机

中执行时，令计算机执行权利要求 1-14 中任一项的所述的方法。

17. 一种计算设备，包括存储器和处理器，其特征在于，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现权利要求 1-14 中任一项所述的方法。

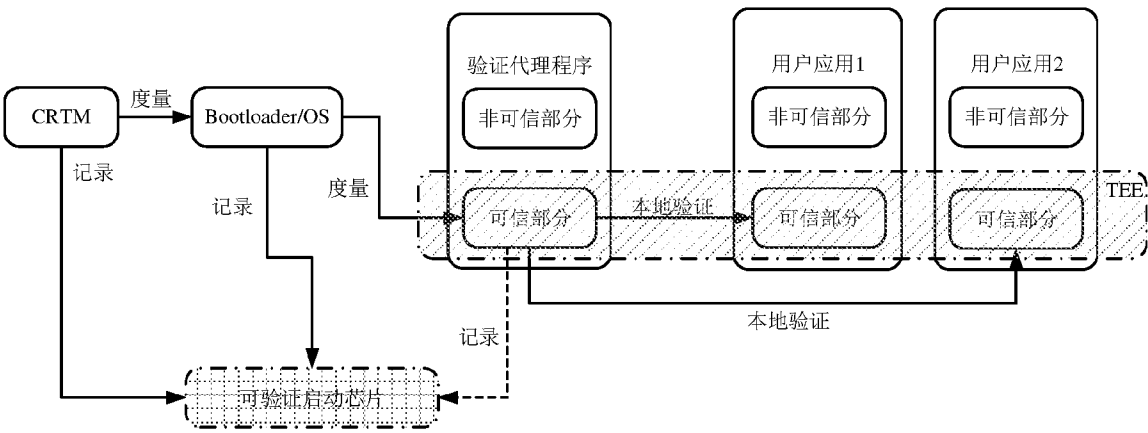


图 1

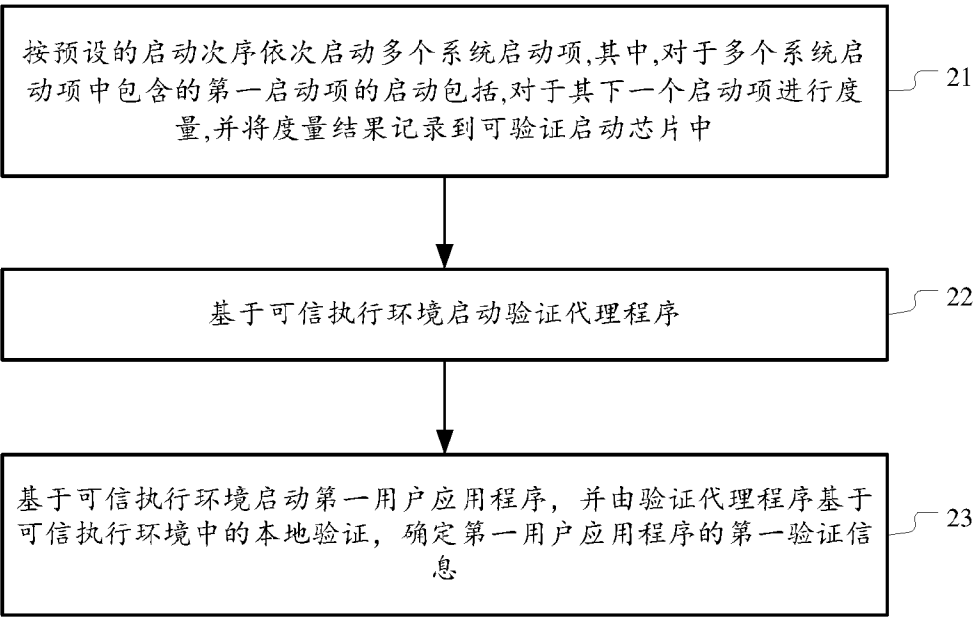


图 2

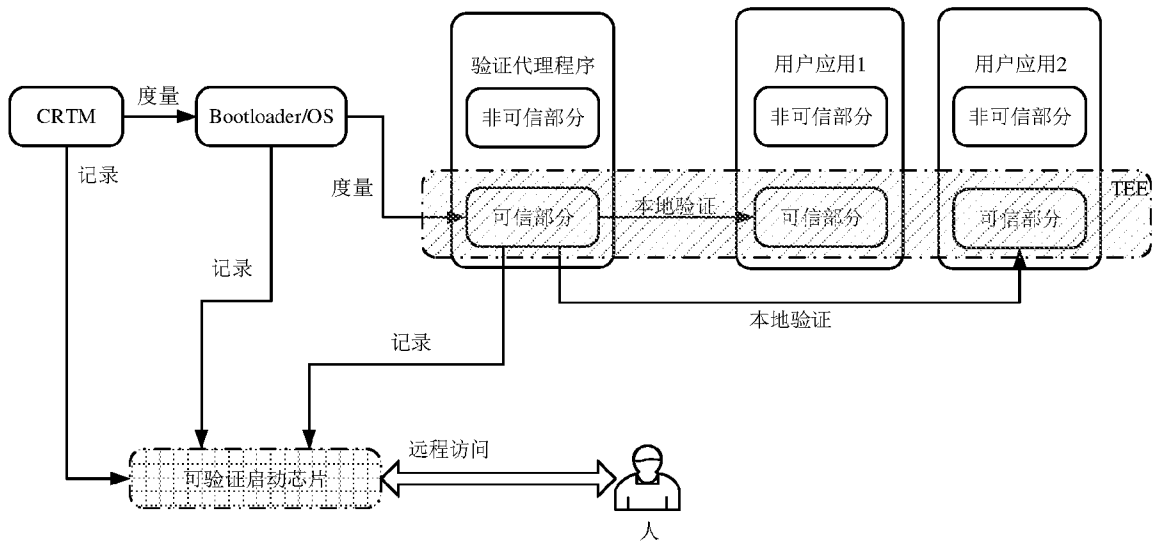


图 3

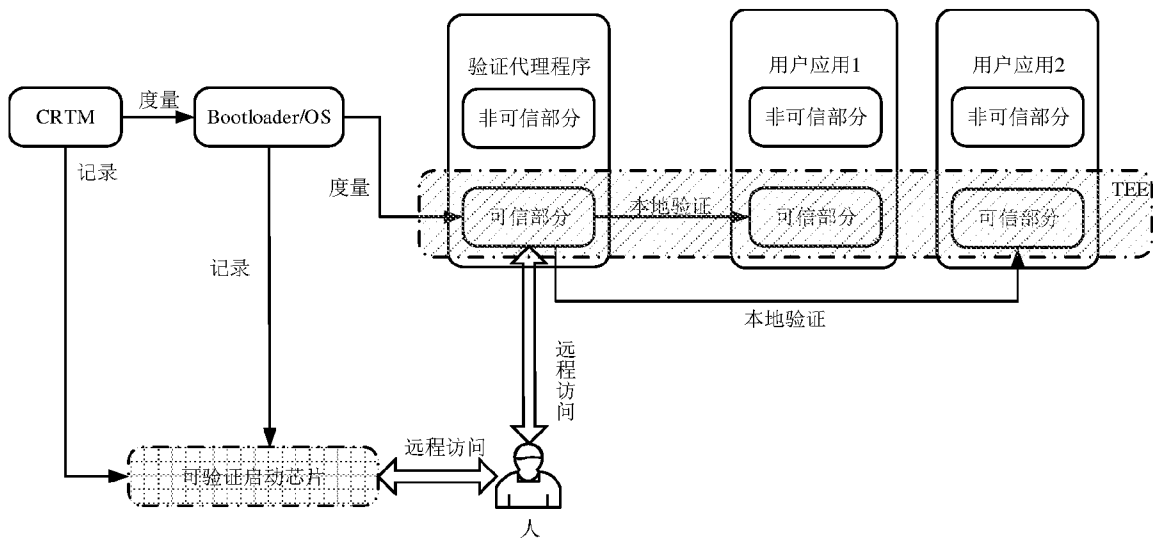


图 4

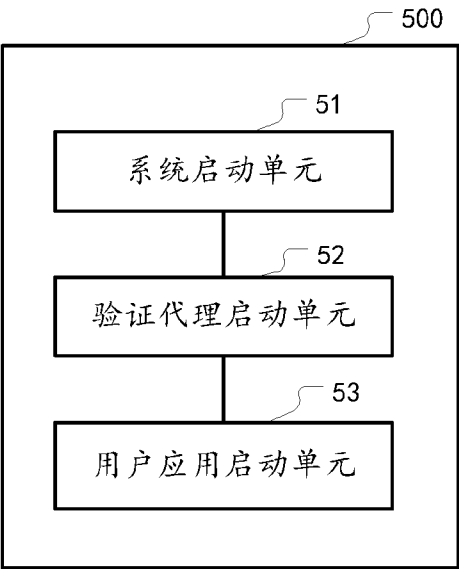


图 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2022/073725

A. CLASSIFICATION OF SUBJECT MATTER

G06F 9/445(2018.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNTXT, ENTXT, ENTXTC, DWPI, CNKI: 本地, 验证, 启动, 度量, 可信执行环境, local, verification, start, measuring, trusted execution environment

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 112988262 A (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) 18 June 2021 (2021-06-18) description paragraphs [0001]-[0103]	1-17
X	CN 102332070 A (ARMY NAVY INSTITUTE OF COMPUTING TECHNOLOGY, PLA) 25 January 2012 (2012-01-25) description, paragraphs [0027]-[0033], and figures 1-2	1-3, 8-17
A	CN 112329005 A (CHINA ELECTRONICS CORPORATION; KYLIN SOFTWARE CO., LIMITED et al.) 05 February 2021 (2021-02-05) entire document	1-17
A	CN 107533609 A (INTEL CORPORATION) 02 January 2018 (2018-01-02) entire document	1-17
A	US 2015188944 A1 (TRAPEZOID, INC.) 02 July 2015 (2015-07-02) entire document	1-17



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

29 March 2022

Date of mailing of the international search report

06 April 2022

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing
100088, China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2022/073725

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	112988262	A	18 June 2021	None			
CN	102332070	A	25 January 2012	None			
CN	112329005	A	05 February 2021	None			
CN	107533609	A	02 January 2018	CN	107533609	B	14 December 2021
				US	2016350534	A1	01 December 2016
				WO	2016195880	A1	08 December 2016
				EP	3304401	A1	11 April 2018
				EP	3304401	A4	03 April 2019
US	2015188944	A1	02 July 2015	US	9258331	B2	09 February 2016
				US	9674183	B2	06 June 2017
				US	2016119336	A1	28 April 2016
				WO	2015100035	A1	02 July 2015

国际检索报告

国际申请号

PCT/CN2022/073725

A. 主题的分类

G06F 9/445 (2018.01) i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CNTXT, ENTXT, ENTXTC, DWPI, CNKI:本地, 验证, 启动, 度量, 可信执行环境, local, verification, start, measuring, trusted execution environment

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
PX	CN 112988262 A (支付宝杭州信息技术有限公司) 2021年6月18日 (2021 - 06 - 18) 说明书第[0001]-[0103]段	1-17
X	CN 102332070 A (中国人民解放军海军计算技术研究所) 2012年1月25日 (2012 - 01 - 25) 说明书第[0027]-[0033]段, 附图1-2	1-3、8-17
A	CN 112329005 A (中国电子信息产业集团有限公司 等) 2021年2月5日 (2021 - 02 - 05) 全文	1-17
A	CN 107533609 A (英特尔公司) 2018年1月2日 (2018 - 01 - 02) 全文	1-17
A	US 2015188944 A1 (TRAPEZOID, INC.) 2015年7月2日 (2015 - 07 - 02) 全文	1-17

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2022年3月29日

国际检索报告邮寄日期

2022年4月6日

ISA/CN的名称和邮寄地址

中国国家知识产权局(ISA/CN)

中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

受权官员

刘瑛

电话号码 010-62412234

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2022/073725

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	112988262	A	2021年6月18日	无			
CN	102332070	A	2012年1月25日	无			
CN	112329005	A	2021年2月5日	无			
CN	107533609	A	2018年1月2日	CN	107533609	B	2021年12月14日
				US	2016350534	A1	2016年12月1日
				WO	2016195880	A1	2016年12月8日
				EP	3304401	A1	2018年4月11日
				EP	3304401	A4	2019年4月3日
US	2015188944	A1	2015年7月2日	US	9258331	B2	2016年2月9日
				US	9674183	B2	2017年6月6日
				US	2016119336	A1	2016年4月28日
				WO	2015100035	A1	2015年7月2日