

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))。

Linux 系统安全应用的软件框架及创建方法

本申请要求在 2021 年 8 月 12 日提交中国专利局、申请号为 202110924877.X 的中国专利申请的优先权，该申请的全部内容通过引用结合在本申请中。

技术领域

本公开涉及计算机基础软件技术领域，例如涉及一种 Linux 系统安全应用的软件框架及创建方法。

背景技术

可信执行环境（Trusted Execution Environment, TEE），该环境可以保证计算不被常规操作系统干扰，因此称为“可信”。TEE 通常用于运行关键的操作，例如：(1)、移动支付：指纹验证、个人识别码（Personal Identification Number, PIN）输入等；(2)、机密数据：私钥、证书等的安全存储；(3)、内容保护：数字版权保护（Digital Rights Management, DRM）等。

由于 TEE 模块的正常运行依赖 Android 系统的基础框架，因此如何使得兼容 Android 系统的安全应用在 Linux 系统中正常运行成为相关技术中要解决的主要技术问题。

发明内容

本公开提供一种 Linux 系统安全应用的软件框架及创建方法，可以避免相关技术中兼容 Android 系统的安全应用在 Linux 系统中不兼容运行的情况，实现兼容 Android 系统的安全应用在 Linux 系统中正常运行。

本公开提供一种 Linux 系统安全应用的软件框架，所述软件框架可以应用包的形式部署在 Linux 系统上并在 Linux 系统上运行；所述应用包包括：安全应用、可信执行环境模块以及 Android 基础框架；

所述安全应用为在 Linux 系统上运行的安全类应用；

所述可信执行环境模块设置为对所述安全应用提供可信的运行基础；

所述 Android 基础框架设置为对所述可信执行环境模块提供运行基础。

本公开还提供一种计算机程序产品，包括存储在非暂态计算机可读存储介质上的计算机程序，所述计算机程序包括程序指令，当所述程序指令被计算机执行时，计算机可执行根据如上述任一种所述 Linux 系统安全应用的软件框架创建方法的步骤。

本公开还提供一种电子设备，包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述处理器执行所述程序时实现如上述任一种所述 Linux 系统安全应用的软件框架创建方法的步骤。

附图说明

图 1 是相关技术的 Android 系统中安全应用所在的软件框架的架构示意图；

图 2 是本公开提供的 Linux 系统安全应用的软件框架的结构示意图；

图 3 是本公开提供的 Linux 系统安全应用的软件框架的架构示意图；

图 4 是本公开提供的 Linux 系统安全应用的软件框架创建方法流程图；

图 5 是图 4 中步骤 430 的流程图。

图 6 是本公开提供的电子设备的结构示意图。

具体实施方式

可信执行环境 (Trusted Execution Environment, TEE)，其内部运行一个完整的操作系统，与 REE (Rich Execution Environment) (如 Android 系统或者 Linux 系统) 隔离运行，REE 为移动设备提供通用环境，运行通用的操作系统 (Operating System, OS)，例如 Android、IOS 系统等。TEE 模块与 REE 模块通过共享内存进行交互。

TEE 模块内部分为内核态与用户态，TEE 的用户态可以运行多个不同的安全应用 (Trusted Application, TA)。在 REE 模块中应用 TEE 模块的最直接的方法是同 TEE 模块中的 TA 进行通信，因此 REE 模块中的与 TA 进行通信的部分称为客户端应用程序，(Client Application, CA)。

如图 1 所示为相关技术中 Android 系统上安全应用的软件框架示意图，在图中左侧对应 TEE 模块的 REE 模块侧中的 TEE 驱动、TEE 基础库、TEE 管理服务以及多个 CA 均属于 TEE 模块的组件，图中列举了解密、指纹、人脸三项安全应用 (服务)。在图 1 中 REE 侧系统中的每个安全应用的 CA 依赖于 TEE 基础库，TEE 模块本身的 TEE 管理服务组件也依赖于 TEE 基础库，而 TEE 基础库又依赖于 Android 基础框架以及 TEE 内核，而 TEE 内核位于 Android 系统所依赖的 Linux 内核中而且不容易改动、移植。

TEE 的方案有很多种，基于不同的 TEE 内核，衍生出多套 TEE 方案，例如：op-tee、trusty、QSEE 等。其中，op-tee 是 Linux 内核主线支持的 TEE 方案，针对 op-tee 内核，Linux 内核提供驱动、上层管理服务和基础库的支持；trusty 是 Android 中采用的 TEE 方案，给出了基础的框架 (基础库/管理服务)，以及 trusty 内核；QSEE 是高通平台采取的 TEE 方案。

另外，同为 Android 系统的 trusty 解决方案，每个芯片商提供出来的基于 trusty 的 TEE 也可能有所不同，每个厂商可能会根据自己的芯片特点修改管理服务、基础库接口等。而且，TA 的加载验证签名过程也不同。Android 设备商也会根据每个芯片商的不同提供不同版本的设备 TEE 应用方案。

基于以上原因，导致最终的产品集成商，基本无法自行“创造”新的 TEE 方案，甚至不能微调原有方案。这样，当原有方案的 REE 系统不是产品商要采用的系统时就显得问题格外棘手。

Android 系统目前在世界各地已经占到举足轻重的地位，芯片商和设备商都纷纷为 Android 系统提供软硬件解决方案，这其中就包括 TEE 方案。

相关技术中，由于操作系统内核依赖于多个设备驱动，将兼容 Android 系统的安全应用移植到 Linux 系统上并进行运行，大多采取容器的方案，即将 Android 系统放入 Linux 系统的某个容器内 (每个 TEE 模块的组件也位于容器中)，使得在 Android 系统上运行的安全应用快速移植到 Linux 系统并运行。

容器方案是将整个 Android 系统或者大部分关键组件放入容器中，导致容器的属性必须设置成高度隔离的方式 (例如，容器内外使用不同的进程标识体系，容器内外的进程间通信

(Inter Process Communication, IPC) 通信受限, 容器的存储部分或者全部隔离), 否则会造成容器内和容器外资源冲突。由此, 容器外的 Linux 系统应用生态中众多应用, 就不能很方便地使用位于容器内的 Android 系统的 TEE 模块, 即使可以使用, 也需要修改已有 Linux 系统生态中的应用的源代码 (例如修改进程间通信方式) 才能使用容器内的 TEE, 给开发带来很多负担。

因此, 将兼容 Android 系统的安全应用快捷、方便地部署并运行在 Linux 系统中, 成为亟需要解决的技术问题。

在本公开的实施例中, 本领域技术人员可以理解, Android 是 Google 公司开发的移动终端上的操作系统, 在该系统的开源版本 Android 开放源代码项目 (Android Open-Source Project, AOSP) 的基础上, 多家企业衍生开发了诸如 MIUI、EMUI、One UI 等版本以及开源社区的 Pixel Experience、Lineage OS 等定制版, 本公开所称的 Android 涵盖上述多种实现情况。

在本公开的实施例中, Linux 系统包括以 Linux kernel 为基础的多种 Linux OS 发行版, 如 Ubuntu、RedHat、Jing OS 等。

在本公开的实施例中, 所称的 Android 基础框架包括用于支持 Android OS 运行的基础组件 Android Framework。

如图 2 所示, 本公开实施例提供一种 Linux 系统安全应用的软件框架, 容易理解, 该软件框架可以应用包的形式部署在 Linux 系统上, 并在 Linux 系统上运行; 所述应用包包括: 安全应用 210、可信执行环境模块 220 以及 Android 基础框架 230;

所述安全应用 210 为在 Linux 系统上运行的安全类应用;

所述可信执行环境模块 220 设置为对所述安全应用提供可信的运行基础;

所述 Android 基础框架 230 设置为对所述可信执行环境模块提供运行基础。

本公开实施例中, 安全应用是指与安全功能相关的应用, 例如与指纹识别、人脸识别、金融支付、加解密等依赖于 TEE 模块提供的可信任环境的应用, “可信执行环境模块” 以下简称 “TEE 模块”, 由于与安全功能相关的应用依赖于 TEE 模块提供的可信任环境, 因此安全应用的正常运行依赖于 TEE 模块中的 TEE 组件提供支持, 而 TEE 组件的运行依赖相关的 TEE 基础库, 而 TEE 基础库依赖 Android 基础框架, 将安全应用或服务依赖的多个部分都打包在应用包内, 以使得应用包在 Linux 系统中正常运行, 从而避免依赖 Android 基础框架的安全应用在 Linux 系统中的兼容运行情况。

本公开实施例中, TEE 模块包括基础类组件、安全支持类组件及基础库;

所述基础类组件及安全支持类组件分别对应自身运行所依赖的所述基础库;

所述基础类组件设置为对安全支持类组件提供基础支持; 所述安全支持类组件设置为对所述安全应用运行提供可信执行环境的支持。

本公开实施例中, TEE 模块中的每个组件的开发各有分工, 一般基础类组件, 如 TEE 内核、TEE 管理服务等由芯片商负责开发, CA (客户端应用程序) 和对应的 TA (安全应用) 由设备商负责开发、集成商负责集成。

以典型的依赖应用 TEE 模块的安全应用指纹识别功能为例进行说明。指纹商在 TEE 基础框架上从非安全世界运行的 CA 发送请求至运行在安全世界的 TA, TA 负责高安全级别的处理, 把结果返回给 CA。TEE 基础框架不关注 CA 和 TA 之间的业务逻辑, 只提供基础服务,

如通信通道建立、TA 的身份校验等。

本公开实施例中，Linux 系统安全应用的软件框架还包括管理软件包，所述管理软件包部署在 Linux 系统上，并在 Linux 系统上运行；

所述管理软件包包括：所述基础类组件、所述基础类组件依赖的基础库以及 Android 基础框架。

本公开实施例中，将安全支持类组件依赖的基础类组件，以及基础类组件相关的基础库及 Android 基础框架进行软件打包部署在 Linux 系统上，是为了对安全支持类组件在 Linux 系统上的正常运行提供支持。如在图 3 中，将属于基础类组件的 TEE 管理服务与其依赖的 TEE 基础库以及 Android 基础框架进行打包形成一个独立的管理软件包部署在 Linux 系统上。

例如，本公开实施例中的应用包包括：至少一个所述安全应用，每个所述安全应用依赖的所述安全支持类组件、每个所述安全支持类组件依赖的基础库以及 Android 基础框架。

例如，本公开实施例中的软件框架包括至少一个所述应用包。

本公开实施例，可将每一安全应用分别独立打包在应用包中，也可将几个或者全部安全应用全部打包在同一应用包中，对外提供综合功能。应用包对外呈现可以是单个应用或者是中间服务。

如图 3 所示为本公开实施例提供的 Linux 系统安全应用的软件框架架构示意图之一，以 snap 形式的应用包为例，图 3 中每个 snap 包包括 Android 基础框架，snap 包内 Android 基础框架和 TEE 基础库及安全应用对应的客户应用程序不依赖于 Linux 框架，但 snap 包内的其他部分依赖于 Linux 框架，snap 机制本身依赖于 Linux 框架及基础服务。

下面对本公开实施例提供的 Linux 系统安全应用的软件框架创建方法进行描述，下文描述的 Linux 系统安全应用的软件框架创建方法与上文描述的 Linux 系统安全应用的软件框架可相互对应参照，如图 4 所示，本公开实施例提供一种 Linux 系统安全应用的软件框架创建方法，包括以下步骤：

步骤 410：确定在 Linux 系统上运行的安全应用与可信执行环境模块中组件的依赖关系；其中，所述可信执行环境模块包括组件及基础库；

本步骤中，确定 Linux 系统上开发的每个安全应用与 TEE 模块中安全支持类组件的对应关系。本步骤中，在 Linux 系统上开发的每个安全应用依赖于 TEE 模块中的安全支持类组件 TEE 组件。本步骤中的安全应用是指 Linux 系统上与 TEE 模块相关的系统安全相关的应用或服务，这些应用或者服务的正常运行都依赖于 TEE 模块的功能，以完成某项安全的功能，例如指纹识别、人脸识别、文档解密等。

步骤 420：确定所述安全应用依赖的所述组件对应的基础库；

步骤 430：将所述安全应用、所述安全应用依赖的组件、所述组件对应的基础库以及所述基础库依赖的 Android 基础框架，进行设定格式的软件打包，得到应用包；

本步骤中将 Linux 系统中每个安全应用依赖的 TEE 基础库以及整个 Android 框架中的部分的基础框架进行软件打包，形成应用包，将其直接移植在 Linux 系统中，使得 TEE 模块在 Linux 系统上支持每个安全应用的正常运行。

在本步骤的一些实施例中，将所述安全应用、所述安全应用依赖的安全支持类组件、所述安全支持类组件对应的基础库以及所述基础库依赖的 Android 基础框架，进行软件打包，得到 snap 形式的应用包。

本实施例中,采用 Linux 上特有的 snap 技术可以避免原有 TEE 模块在 Linux 系统中由于环境变化而不能运行的情况。

通过打包应用直接依赖的本属于系统部分基础组件,与应用共同制作成为一个 snap 应用包,这样的应用包安装在不同的运行环境都可以正常运行。

把 TEE 模块依赖的 Android 的基础框架同 Linux CA 一起打包成为一个 snap 包,将 snap 包部署在 Linux 系统中,使得安全应用在 Linux 系统中正常运行。

在本步骤的一些实施例中,将所述安全应用、所述安全应用依赖的安全支持类组件、所述安全支持类组件对应的基础库以及所述基础库依赖的 Android 基础框架,进行软件打包,得到 flatpak 形式的应用包。

本实施例中,采用 Linux 上特有的 flatpak 技术可以避免原有 TEE 模块在 Linux 系统中由于环境变化而不能运行的情况。

flatpak 是一个程序包管理实用程序,可分发安装和管理软件,而不必担心依赖项,运行时或 Linux 分发。可以安装软件而与 Linux 发行版无关(无论是基于 Debian 的发行版还是基于 Arch 的发行版),因此 flatpak 称为通用软件包。

本公开实施例提供的技术方案可以适用的前提是应用包中仅包括 TEE 模块依赖的 Android 基础框架,所以用 snap 或 flatpak 更为灵活,能抛弃容器的隔离限制。除此之外,TEE 模块的特殊性还在于 TEE 模块的驱动与诸如蓝牙音频、GPS 等的驱动有区别,TEE 模块驱动本身就支持多个访问者同时使用(可以容器内 Android 系统和容器外 Linux 系统同时访问),所以 TEE 模块可以在无需移植其驱动的情况下使用本公开实施例提供的方案即可满足安全应用需求。

在构建了上述软件包后,用户或系统发行者可以执行步骤 440:将所述应用包部署在 Linux 系统上,并在需要执行所述安全应用的时候运行所述软件包。

本步骤的应用包根据实际系统情况部署在 Linux 系统,以使得每个应用包在 Linux 系统上正常运行,为每个安全应用在 Linux 系统上正常运行提供安全运行环境的支持。

本公开实施例中, TEE 模块的多个组件分别依赖于相应的基础库,而所依赖的基础库可能同样依赖其他基础库,因此在步骤 430 中需要找到安全应用间接依赖的所有基础库,并将所被依赖的所有基础库封装在应用包内。

本公开的一些实施例中,如图 5 所示,步骤 430 之后还包括:

步骤 510: 将所述基础类组件、所述基础类组件对应的基础库以及所述基础库依赖的 Android 基础框架,进行软件打包,得到 snap 或者 flatpak 形式的管理软件包;

在得到所述管理软件包后,系统发行者可以执行步骤 520:将所述管理软件包部署在 Linux 系统上,从而提供给用户使用。

下面结合图 6 描述本公开实施例提供的一种电子设备的实体结构示意图,如图 6 所示,该电子设备可以包括:处理器(processor)610、通信接口(Communications Interface)620、存储器(memory)630 和通信总线 640,其中,处理 610,通信接口 620,存储 630 通过通信总线 640 完成相互间的通信。处理器 610 可以调用存储器 630 中的逻辑指令,以执行 Linux 系统安全应用的软件框架创建方法,该方法包括:确定在 Linux 系统上运行的安全应用与可信执行环境模块中组件的依赖关系;其中,所述可信执行环境模块包括组件及基础库;确定所述安全应用依赖的所述组件对应的基础库;将所述安全应用、所述安全应用依赖的组件、所述组件

对应的基础库以及所述基础库依赖的 Android 基础框架，进行设定格式的软件打包，得到应用包；将所述应用包部署在 Linux 系统上并运行。

此外，上述的存储器 630 中的逻辑指令可以通过软件功能单元的形式实现并作为独立的产品销售或使用，可以存储在一个计算机可读取存储介质中。基于这样的理解，本公开实施例的技术方案本质上或者说对相关技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本公开多个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁碟或者光盘等多种可以存储程序代码的介质。

在上述终端设备实施例中，应理解，处理器 610 可以是中央处理单元（英文：Central Processing Unit，简称：CPU），还可以是其他通用处理器、数字信号处理器（英文：Digital Signal Processor，简称：DSP）、专用集成电路（英文：Application Specific Integrated Circuit，简称：ASIC）等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本公开所公开的方法的步骤可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件模块组合执行完成。

另一方面，本公开实施例还提供一种计算机程序产品，所述计算机程序产品包括存储在非暂态计算机可读存储介质上的计算机程序，所述计算机程序包括程序指令，当所述程序指令被计算机执行时，计算机可执行上述多个方法所提供的 Linux 系统安全应用的软件框架创建方法，该方法包括：确定在 Linux 系统上运行的安全应用与可信执行环境模块中组件的依赖关系；其中，所述可信执行环境模块包括组件及基础库；确定所述安全应用依赖的所述组件对应的基础库；将所述安全应用、所述安全应用依赖的组件、所述组件对应的基础库以及所述基础库依赖的 Android 基础框架，进行设定格式的软件打包，得到应用包；将所述应用包部署在 Linux 系统上并运行。

又一方面，本公开实施例还提供一种非暂态计算机可读存储介质，其上存储有计算机程序，该计算机程序被处理器执行时实现以执行上述多个实施例提供的 Linux 系统安全应用的软件框架创建方法：确定在 Linux 系统上运行的安全应用与可信执行环境模块中组件的依赖关系；其中，所述可信执行环境模块包括组件及基础库；确定所述安全应用依赖的所述组件对应的基础库；将所述安全应用、所述安全应用依赖的组件、所述组件对应的基础库以及所述基础库依赖的 Android 基础框架，进行设定格式的软件打包，得到应用包；将所述应用包部署在 Linux 系统上并运行。

以上所描述的装置实施例仅仅是示意性的，其中所述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，作为单元显示的部件可以是或者也可以不是物理单元，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。本领域普通技术人员在不付出创造性的劳动的情况下，即可以理解并实施。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到多个实施方式可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件。基于这样的理解，上述技术方案本质上或者说对相关技术做出贡献的部分可以以软件产品的形式体现出来，该计算机

软件产品可以存储在计算机可读存储介质中，如 ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行多个实施例或者实施例的某些部分所述的方法。

本公开提供的 Linux 系统安全应用的软件框架及创建方法，通过将要在 Linux 系统中运行的安全应用，与其依赖的可信执行环境模块及 Android 基础框架以应用包的形式部署在 Linux 系统中，从而方便兼容 Android 系统的安全应用在 Linux 系统快速移植并实现兼容 Android 系统的安全应用在 Linux 系统中的正常运行。

权利要求书

1、一种 Linux 系统安全应用的软件框架，所述软件框架可以应用包的形式部署在 Linux 系统上并在 Linux 系统上运行；所述应用包包括：安全应用、可信执行环境模块，以及安卓 Android 基础框架；

所述安全应用为在所述 Linux 系统上运行的安全类应用；

所述可信执行环境模块设置为对所述安全应用提供可信的运行基础；

所述 Android 基础框架设置为对所述可信执行环境模块提供运行基础。

2、根据权利要求 1 所述的软件框架，其中，所述可信执行环境模块包括基础类组件、安全支持类组件及基础库；

所述基础类组件及安全支持类组件分别对应自身运行所依赖的所述基础库；

所述基础类组件设置为对所述安全支持类组件提供基础支持；

所述安全支持类组件设置为对所述安全应用运行提供可信执行环境的支持。

3、根据权利要求 2 所述的软件框架，还包括管理软件包，所述管理软件包可部署在所述 Linux 系统上并在所述 Linux 系统上运行；

所述管理软件包包括：所述基础类组件、所述基础类组件依赖的基础库，以及 Android 基础框架。

4、根据权利要求 3 所述的软件框架，其中，所述应用包包括：至少一个所述安全应用，每个安全应用依赖的所述安全支持类组件、每个所述安全支持类组件依赖的基础库以及 Android 基础框架。

5、根据权利要求 4 所述的软件框架，其中，所述软件框架包括至少一个所述应用包。

6、一种 Linux 系统安全应用的软件框架创建方法，所述方法包括：

确定所述在 Linux 系统上运行的安全应用与可信执行环境模块中组件的依赖关系；其中，所述可信执行环境模块包括所述组件及基础库；

确定所述安全应用依赖的所述组件对应的基础库；

将所述安全应用、所述安全应用依赖的组件、所述组件对应的基础库，以及所述基础库依赖的 Android 基础框架，进行设定格式的软件打包，得到应用包。

7、根据权利要求 6 所述的方法，其中，所述组件包括基础类组件、安全支持类组件；

所述将所述安全应用、所述安全应用依赖的组件、所述组件对应的基础库以及所述基础库依赖的 Android 基础框架，进行设定格式的软件打包，得到应用包，包括：

将所述安全应用、所述安全应用依赖的安全支持类组件、所述安全支持类组件对应的基础库以及所述基础库依赖的 Android 基础框架，进行软件打包，得到 snap 或者 flatpak 形式的应用包。

8、根据权利要求 7 所述的方法，所述将所述安全应用、所述安全应用依赖的组件、所述组件对应的基础库以及所述基础库依赖的 Android 基础框架，进行设定格式的软件打包，得到应用包之后，还包括：

将所述基础类组件、所述基础类组件对应的基础库以及所述基础库依赖的 Android 基础框架，进行软件打包，得到 snap 或者 flatpak 形式的管理软件包。

9、一种计算机程序产品，包括存储在非暂态计算机可读存储介质上的计算机程序，所述计算机程序包括程序指令，当所述程序指令被计算机执行时，计算机可执行根据权利要求 6 至 8 中任一项所述 Linux 系统安全应用的软件框架创建方法的步骤。

10、一种电子设备，包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述处理器执行所述程序时实现如权利要求 6 至 8 所述 Linux 系统安全应用的软件框架创建方法的步骤。

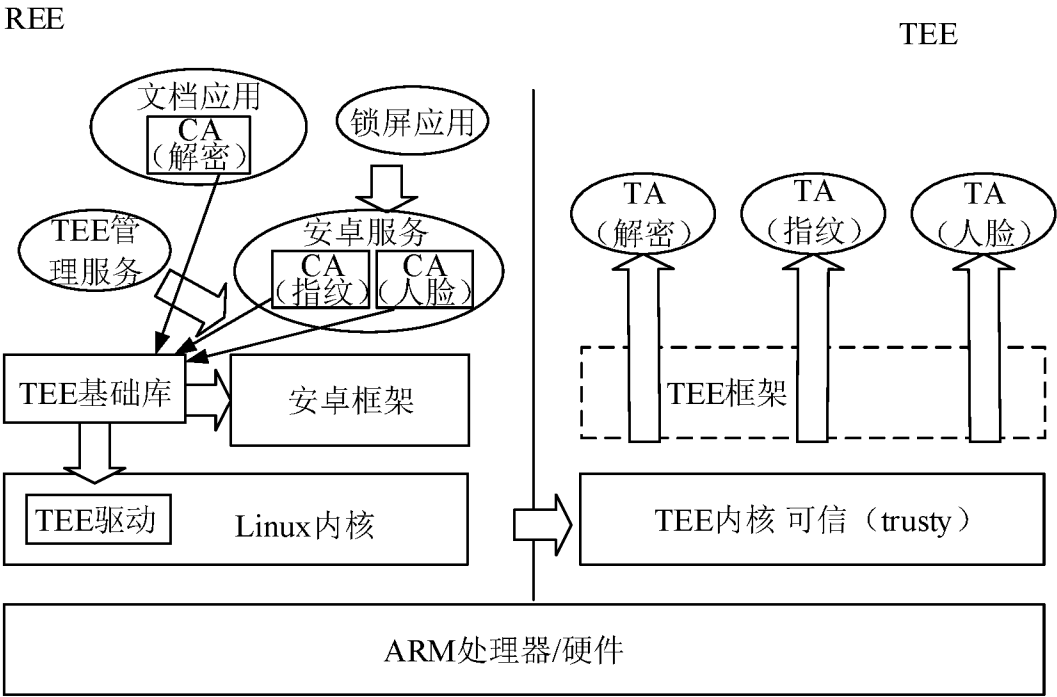


图 1

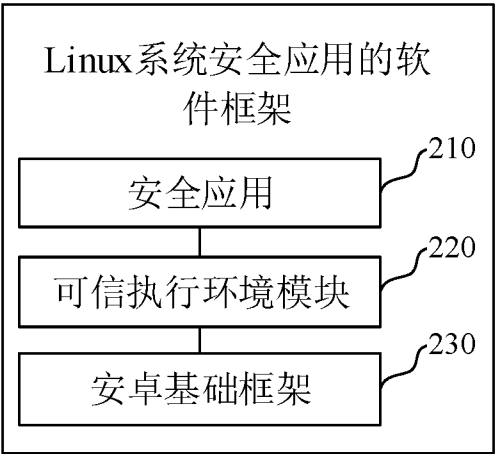


图 2

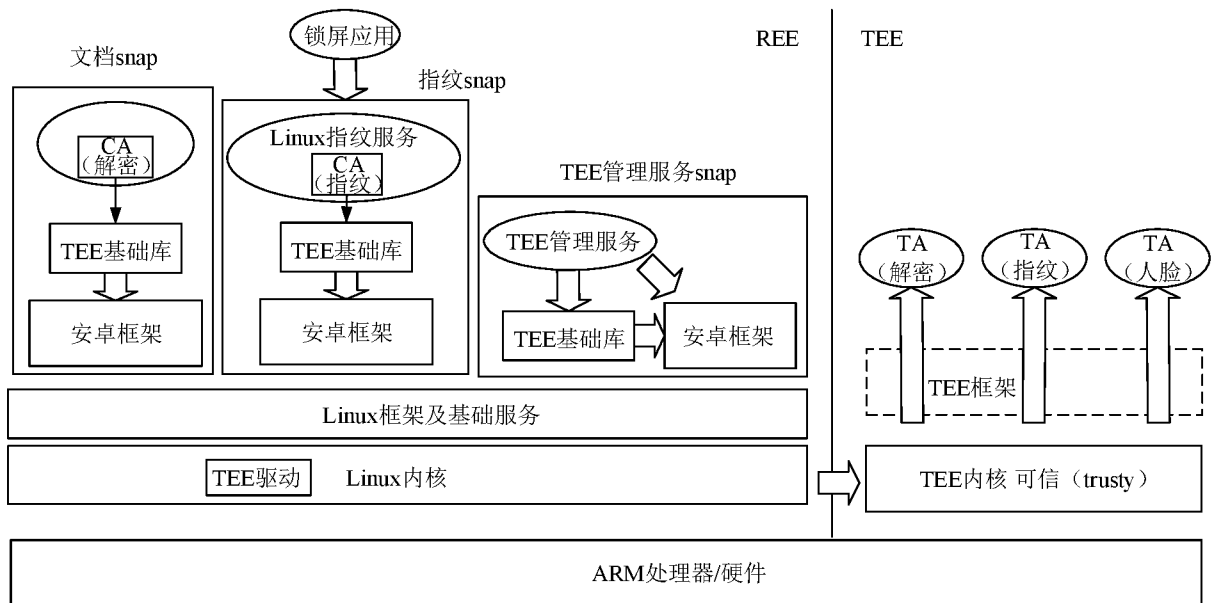


图 3

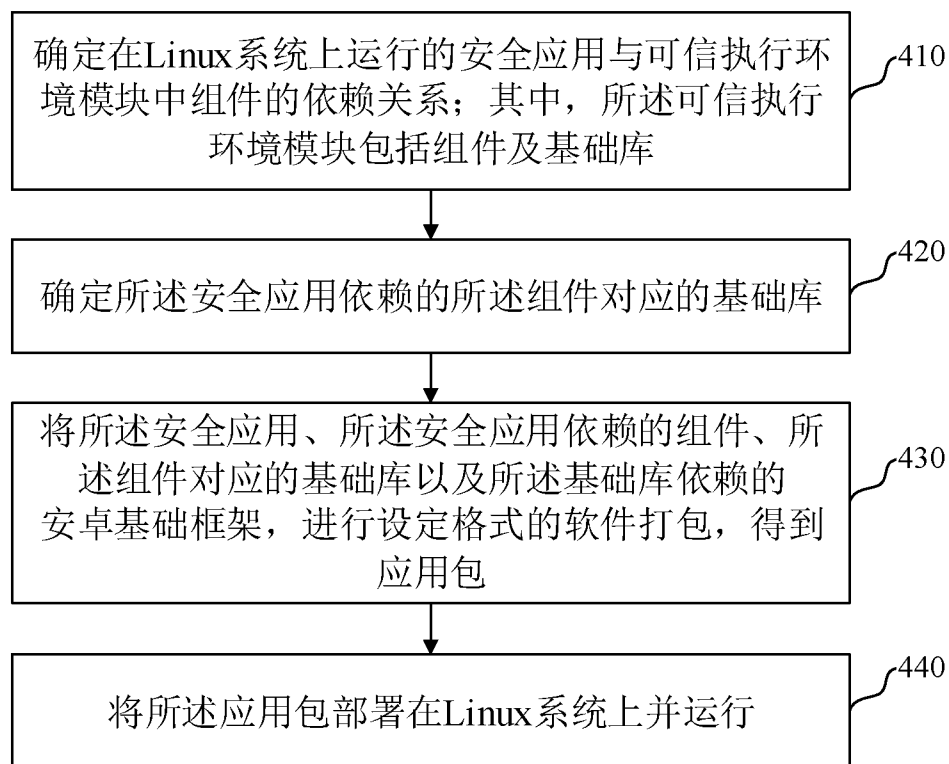


图 4

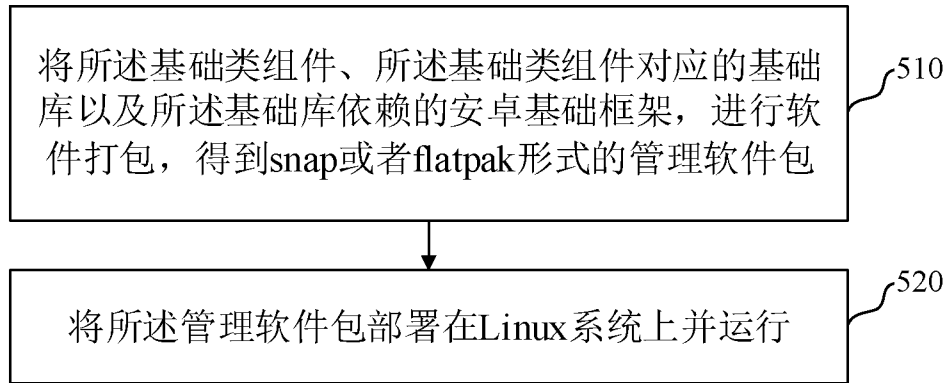


图 5

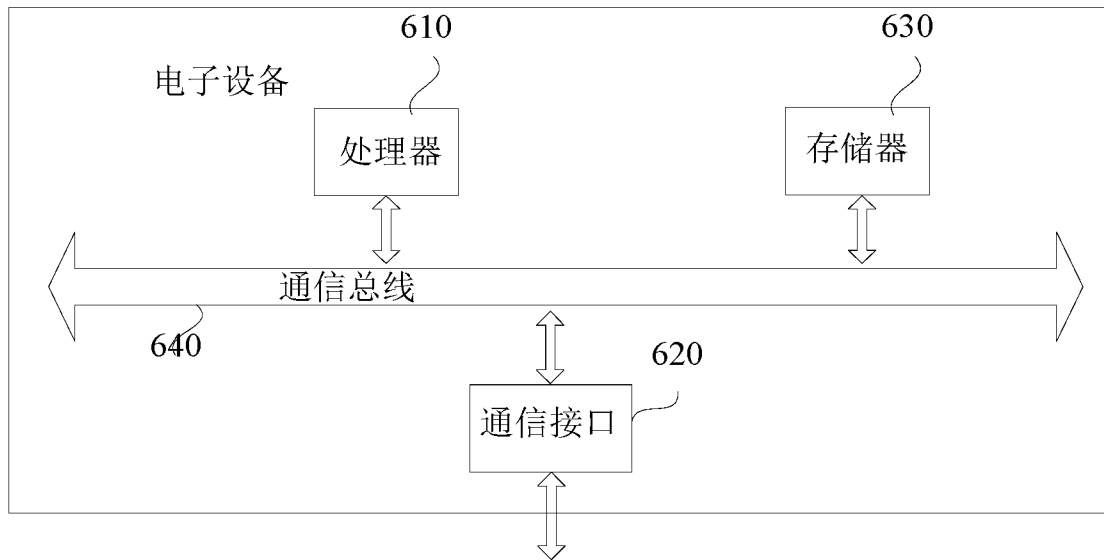


图 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2022/104299

A. CLASSIFICATION OF SUBJECT MATTER

G06F 8/61(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)

CNPAT, CNKI, BAIDU, EPODOC, WPI, IEEE: 安卓, 可信执行环境, 应用包, 软件包, 安全应用, 基础框架, 操作系统, 基础, 安全支持, 依赖, 打包, Android, Linux, trusted execution environment, TEE, application, package, software, security, base, framework, operating system, support, dependency, snap, flatpak

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 113703790 A (BEIJING JINGLING INFORMATION SYSTEM TECHNOLOGY CO., LTD.) 26 November 2021 (2021-11-26) claims 1-10	1-10
Y	CAI, Zephyr. "Android可信执行环境TEE最全介绍 (Non-official translation: The most complete introduction to Android Trusted Execution Environment TEE)" https://blog.csdn.net/caizehui/article/details/114638207 , 10 March 2021 (2021-03-10), pp. 2-9	1-10
Y	US 2017031680 A1 (MECHDOME, INC.) 02 February 2017 (2017-02-02) description, paragraphs [0030]-[0125], and figures 1-8	1-10
A	CN 112486512 A (HUNAN QILIN XIN'AN TECHNOLOGY CO., LTD.) 12 March 2021 (2021-03-12) entire document	1-10
A	CN 109086100 A (INSTITUTE OF INFORMATION ENGINEERING, CHINESE ACADEMY OF SCIENCES) 25 December 2018 (2018-12-25) entire document	1-10



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

18 September 2022

Date of mailing of the international search report

30 September 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/CN2022/104299

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	113703790	A	26 November 2021	None			
US	2017031680	A1	02 February 2017	WO	2017019284	A1	02 February 2017
CN	112486512	A	12 March 2021	None			
CN	109086100	A	25 December 2018	None			

国际检索报告

国际申请号

PCT/CN2022/104299

A. 主题的分类

G06F 8/61 (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))

CNPAT, CNKI, BAIDU, EPODOC, WPI, IEEE: 安卓, 可信执行环境, 应用包, 软件包, 安全应用, 基础框架, 操作系统, 基础, 安全支持, 依赖, 打包, Android, Linux, trusted execution environment, TEE, application, package, software, security, base, framework, operating system, support, dependency, snap, flatpak

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 113703790 A (北京鲸鲮信息系统技术有限公司) 2021年11月26日 (2021 - 11 - 26) 权利要求1-10	1-10
Y	Zephyr Cai. "Android可信执行环境TEE最全介绍" https://blog.csdn.net/caizehui/article/details/114638207 , 2021年3月10日 (2021 - 03 - 10), 第2-9页	1-10
Y	US 2017031680 A1 (MECHDOME, INC.) 2017年2月2日 (2017 - 02 - 02) 说明书第[0030]-[0125]段, 附图1-8	1-10
A	CN 112486512 A (湖南麒麟信安科技股份有限公司) 2021年3月12日 (2021 - 03 - 12) 全文	1-10
A	CN 109086100 A (中国科学院信息工程研究所) 2018年12月25日 (2018 - 12 - 25) 全文	1-10

☐ 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9月18日

国际检索报告邮寄日期

2022年9月30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

徐淑娴

电话号码 86-(10)-53961535

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2022/104299

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	113703790	A	2021年11月26日	无	
US	2017031680	A1	2017年2月2日	W0	2017019284 A1 2017年2月2日
CN	112486512	A	2021年3月12日	无	
CN	109086100	A	2018年12月25日	无	