

一种动态配置安全内存的方法、设备、装置及存储介质

技术领域

[01]本说明书涉及计算机领域，尤其涉及一种动态配置安全内存的方法、设备、装置及存储介质。

背景技术

[02]随着互联网相关技术的发展，信息的流通方式也变得多种多样。与此同时，人们对信息保护的意识也越来越强，目前可基于可信区（trustzone）技术，在用户的设备中构建可信执行环境（Trusted Execution Environment, TEE）。通过可信执行环境在用户的设备中提供一个与通用执行环境（Rich Execution Environment, REE）隔离的安全环境，保护在该可信执行环境内运行的应用的安全，有利于隐私保护。

[03]而如何配置 TEE 运行所需的安全内存是亟待解决的问题，为此本说明书提供一种动态配置安全内存的方法。

发明内容

[04]本说明书提供一种动态配置安全内存的方法、设备、装置及存储介质。

[05]本说明书采用下述技术方案：本说明书提供了一种动态配置安全内存的方法，所述方法应用于可信应用，包括：接收安全内存的注册指令，所述注册指令中携带有客户端申请的内存地址；根据所述注册指令，调用可信执行环境的操作系统的注册接口，向处理器可信框架单元发送安全内存的注册请求，使所述处理器可信框架单元根据所述注册请求，将所述内存地址对应的内存空间的属性更新为安全属性。

[06]本说明书提供了一种动态配置安全内存的方法，所述方法应用于可信执行环境的操作系统，包括：接收可信应用对注册接口的调用请求，所述调用请求携带通用执行环境中的客户端申请的内存地址；根据所述调用请求生成注册请求，向处理器可信框架单元发送所述注册请求，使所述处理器可信框架单元根据所述注册请求，将所述内存地址对应的内存空间的属性更新为安全属性。

[07]本说明书提供一种动态配置安全内存的方法，所述方法应用于处理器可信框架单元，包括：接收可信执行环境的操作系统发送的注册请求，所述注册请求包含内存地址；根据所述注册请求，将所述内存地址对应的内存空间的属性更新为安全属性。

[08]本说明书提供一种动态配置安全内存的设备，所述设备包括通用执行环境中的客户端、可信执行环境的操作系统、可信应用以及处理器可信框架单元，包括：所述客户端，用于确定在所述可信执行环境执行业务所需的内存地址；向所述可信应用发送注册指令，所述注册指令中携带有所述内存地址；所述可信应用，用于接收所述客户端发送的注册指令；根据携带所述内存地址的所述注册指令，生成调用所述可信执行环境的操作系统中的注册接口的调用请求；所述可信执行环境的操作系统，用于接收所述可信应用对所述注册接口的调用请求；根据所述调用请求生成注册请求，向处理器可信框架单元发送所述注册请求；所述处理器可信框架单元，用于接收所述可信执行环境的操作系统发送的所述注册请求；根据所述注册请求，将所述内存地址对应的内存空间的属性更新为安全属性。

[09]本说明书提供一种动态配置安全内存装置，包括：接收模块，用于接收安全内存的注册指令，所述注册指令中携带有客户端申请的内存地址；内存配置模块，用于根据所述注册指令，调用可信执行环境的操作系统的注册接口，向处理器可信框架单元发送安

全内存的注册请求，使所述处理器可信框架单元根据所述注册请求，将所述内存地址对应的内存空间的属性更新为安全属性。

[10]本说明书提供一种动态配置安全内存装置，包括：接收模块，用于接收可信应用对注册接口的调用请求，所述调用请求携带通用执行环境中的客户端申请的内存地址；

[11]内存配置模块，用于根据所述调用请求生成注册请求，向处理器可信框架单元发送所述注册请求，使所述处理器可信框架单元根据所述注册请求，将所述内存地址大小对应的内存空间的属性更新为安全属性。

[12]本说明书提供一种动态配置安全内存装置，包括：接收模块，接收可信执行环境的操作系统发送的注册请求，所述注册请求包含内存地址；内存配置模块，根据所述注册请求，将所述内存地址对应的内存空间的属性更新为安全属性。

[13]本说明书提供一种计算机可读存储介质，所述存储介质存储有计算机程序，所述计算机程序被处理器执行时实现上述动态配置安全内存的方法。

[14]本说明书采用的上述至少一个技术方案能够达到以下有益效果：在本说明书提供的动态配置安全内存的方法中，通用执行环境中的客户端向可信执行环境中的可信应用发送安全内存的注册指令，其中，注册指令中携带客户端申请的内存地址。可信应用根据所述注册指令，调用可信执行环境的操作系统的注册接口，向处理器可信框架单元发送安全内存的注册请求，使处理器可信框架单元根据注册请求，将内存地址对应的内存空间的属性更新为安全属性。

[15]从上述方法中可以看出，本方法通过动态配置安全内存的方法既满足了安全要求，又减少了内存资源的浪费。

附图说明

[16]此处所说明的附图用来提供对本说明书的进一步理解，构成本说明书的一部分，本说明书的示意性实施例及其说明用于解释本说明书，并不构成对本说明书的不当限定。

[17]图 1 为本说明书实施例中一种动态配置安全内存方法的流程示意图。

[18]图 2 为本说明书实施例提供的一种客户端通过处理器可信框架单元与可信应用交互的示意图。

[19]图 3 为本说明书实施例提供的一种动态配置安全内存方法的流程示意图。

[20]图 4 为本说明书实施例提供的一种动态配置安全内存方法的流程示意图。

[21]图 5a 为本说明书实施例提供的一种动态配置安全内存的设备示意图。

[22]图 5b 为本说明书实施例提供的一种动态配置安全内存的设备示意图。

[23]图 6 为本说明书实施例提供的一种客户端、处理器可信框架单元、可信应用于可信执行环境的操作系统交互的详细过程示意图。

[24]图 7 为本说明书实施例提供的一种动态配置安全内存装置的示意图。

[25]图 8 为本说明书实施例提供的一种动态配置安全内存装置的示意图。

[26]图 9 为本说明书实施例提供的一种动态配置安全内存装置的示意图。

具体实施方式

[27]为使本说明书的目的、技术方案和优点更加清楚，下面将结合本说明书具体实施例及相应的附图对本说明书技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本说明书一部分实施例，而不是全部的实施例。基于本说明书中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

[28]区别于设备在启动阶段在内存访问控制单元初始化时进行安全内存的配置的方法，本说明书实施例提出一种新的配置安全内存的方法，避免了由于固定的安全内存大小导

致的内存资源浪费。还可以解决为满足可信执行环境内的可信应用的正常运行，设备按照在可信执行环境内运行的可信应用所需内存上限配置安全内存的大小，导致内存资源紧张加剧的问题。

[29]目前，在设备中构建可信执行环境的目的之一，是为了提高设备中客户端（Client Application, CA）运行时的数据安全，规避风险。一般地，客户端在执行业务时，若该业务涉及到用户的敏感数据，或者涉及到安全计算等内容，则该客户端将相应的业务步骤转移至可信执行环境中的可信应用（Trust Application, TA）中执行。由于可信执行环境与通用执行环境是相互隔离的环境，因此通用执行环境中的恶意软件，无法获取可信执行环境中的敏感数据。同样的，客户端也无法获取敏感数据，而只是向可信应用提供执行业务所需的数据，得到可信应用返回的业务执行结果，具体如何得到业务执行结果对于处于通用执行环境中的客户端来说，就像一个“黑盒”，无法获取内部的数据。

[30]以下结合附图，详细说明本说明书各实施例提供的技术方案。

[31]图 1 为本说明书中一种动态配置安全内存的方法的流程示意图，包括步骤 S100 至步骤 S102。

[32]S100：接收安全内存的注册指令，所述注册指令中携带有客户端申请的内存地址。

[33]由于，可信应用执行业务，需要处理器、存储器等硬件设备资源的支持，因此需要在可信应用执行业务前，预先为该可信应用配置安全内存。安全内存，属于设备内存中的一部分，通过将设备内存中的部分内存地址配置为安全属性，使得只有可信执行环境中的可信应用可以访问该内存地址的数据，而通用执行环境的客户端不可访问该内存地址的数据。

[34]为了避免目前配置固定大小的安全内存引起的一系列问题，在本说明书一个或多个实施例中，设备在启动时不再通过内存访问控制单元，配置固定大小的安全内存。而是当客户端执行业务时需要可信执行环境中可信应用协助执行业务时，再配置安全内存。

[35]以在设备的可信执行环境中运行的可信应用为执行主体，该可信应用可接收客户端发送的注册指令。由于该注册指令是用于将设备的内存注册为安全内存的指令，而该可信应用执行业务需要多少内存空间，是该可信应用无法确定的，因此该注册指令中携带有该客户端申请的内存地址。

[36]进一步地，由于可信执行环境可包含多个可信应用，且可信执行环境下的每个可信应用之间是相互隔离的，在未授权的情况下每个可信应用不能互相访问。而其中，通常只有一个可信应用是后续用于执行隐私业务的可信应用。例如，假设可信执行环境中包含可信应用 A、B、C，分别用于进行人脸识别、指纹识别以及声纹识别，而可信应用要执行业务是人脸支付，则只有可信应用 A 是执行后续业务所需的可信应用。

[37]于是，该客户端在发送注册指令之前，可从可信执行环境中各可信应用中，确定后续执行业务时需要的可信应用。具体的，该客户端可从可信执行环境的各可信应用中，确定后续执行业务所需的可信应用，并向该可信应用发送验证请求，以验证可信应用是否可以执行业务。而可信应用可根据验证请求，返回确认信息或否认信息。客户端在接收到确认信息后，便可继续执行后续步骤 S102，否则可以展示错误提示信息，以提示用户无法在可信执行环境内执行业务。当然，具体客户端如何确定可信应用是否可正常提供业务支持已经是较为成熟的技术，本说明书不再赘述。

[38]更进一步地，由于通用执行环境和可信执行环境是两个相互隔离的环境，若客户端直接将注册指令发给可信应用，存在一定风险。比如，客户端处理的业务是指纹支付，但同时伴有盗取指纹信息情况，由于客户端直接将注册指令发给可信应用，通用执行环境获取到加密指纹数据的验证信息，则可信执行环境不再安全，用户的指纹数据就可能被盗取。所以目前通常是由处理器可信框架单元（ARM Trusted Firmware, ATF）转发

注册指令。

[39]图 2 为本说明书提供的一种客户端 (CA) 通过处理器可信框架单元 (ATF) 与可信应用 (TA) 交互的示意图, 其中可见, 左侧是通用执行环境 (REE), 其中的客户端向处理器可信框架单元发送注册指令, 中间是处理器可信框架单元, 用于分发客户端发送的注册指令, 右侧是可信执行环境 (TEE), 其中的可信应用接收处理器可信框架单元转发的注册指令。

[40]可信应用对发送注册指令的客户端进行验证, 若验证发送方是有权调用自身的客户端, 则接收由处理器可信框架单元转发的注册指令。若验证发送方不是有权调用自身的客户端, 则拒绝接收该客户端发送的注册指令。

[41]另外, 一个可信应用可处理一个或多个客户端的业务。例如, 可信执行环境中的可信应用 D 可处理安全校验业务, 现通用执行环境中有多多个客户端请求处理安全校验业务, 可信应用 D 在对各个客户端进行验证后, 各个客户端将进行安全校验业务的相关数据通过处理器可信框架单元转发至该可信应用 D, 该可信应用 D 接收各个客户端发送的数据后, 利用该数据分别处理各个客户端的安全校验业务。

[42]S102: 根据所述注册指令, 调用可信执行环境的操作系统的注册接口, 向处理器可信框架单元发送安全内存的注册请求, 使所述处理器可信框架单元根据所述注册请求, 将所述内存地址对应的内存空间的属性更新为安全属性。

[43]可信应用在接收到注册指令之后, 由于该可信应用自身并没有将设备的内存的属性更新为安全属性的权限, 因此可以根据该注册指令, 调用可信执行环境的操作系统的注册接口, 通过可信执行环境的操作系统向处理器可信框架单元发送安全内存的注册请求。则该处理器可信框架单元可根据该注册请求, 将该内存地址对应的内存空间的属性更新为安全属性。如此, 该内存空间只可由该可信应用访问, 保证后续业务执行的安全, 减少用户隐私泄露的风险。

[44]具体的, 首先, 由于一般可信执行环境的操作系统会为各可信应用提供不同实现功能或服务的接口, 因此该可信应用需要先确定进行安全内存注册的接口, 以便调用该接口进行安全内存的注册。于是, 该可信应用可根据接收到的该注册指令, 查询该可信执行环境的操作系统的各接口的功能, 并从中确定用于注册安全内存接口, 即注册接口。

[45]之后, 当该可信应用查询到该注册接口后, 便可调用该注册接口, 将该内存地址发送给该可信执行环境的操作系统。

[46]然后, 该可信执行环境的操作系统, 可根据注册接口对应业务逻辑, 向该处理器可信框架单元发送安全内存的注册请求, 该注册请求中携带该内存地址。通过该处理器可信框架单元将该内存的属性更新为安全属性, 实现该内存只允许相应的可信应用使用。

[47]其中, 该可信执行环境的操作系统可根据注册接口对应业务逻辑, 以及调用请求携带的内存地址, 生成注册请求。

[48]具体的, 该注册接口接受该可信应用的调用后, 可信执行环境的操作系统对应的业务逻辑层根据该内存地址建立业务流程, 运行该注册接口对应的业务逻辑的代码, 以生成该注册请求。即按照业务逻辑生成符合语法规定的实现生成该注册请求的代码, 运行该代码并生成注册请求。其中, 该注册请求中携带该内存地址。

[49]再后, 在该可信执行环境的操作系统向该处理器可信框架单元发送该注册请求后, 该处理器可信框架单元根据该注册请求, 向内存保护控制器 (TrustZone Address Space Controller, TZASC) 发送调用指令, 该调用指令携带该内存地址。其中, 可信执行环境的操作系统向处理器可信框架单元发送注册请求, 以及处理器可信框架单元接收发送的注册请求都可先进行验证, 在验证通过后, 再进行下一步操作, 若验证不通过, 则返回错误信息, 错误信息用于提示存在安全隐患。当然, 由于如何进行程序间的验证 (如,

鉴权)的技术已经是较为成熟的技术,本说明书不再赘述,也不限制具体采用何种方式进行验证。

[50]最后,该内存保护控制器可根据该处理器可信框架单元的调用指令,确定该内存地址,并从内存空闲的存储空间中确定内存要注册为安全内存的连续物理地址。并将确定出的连续物理地址的属性,更新为安全属性。内存保护控制器更新该连续物理地址的属性后,还可向该处理器可信框架单元返回确认信息。该处理器可信框架单元接收到该确认信息后,确定安全内存注册成功,并向该可信执行环境的操作系统返回安全内存注册完成的信息。该可信执行环境的操作系统接收到该安全内存注册完成的信息后,对该内存地址进行映射,即对该连续物理地址进行映射,生成对应的映射表,映射表包含该连续物理地址对应的虚拟地址以及两者的映射关系。本说明书对其映射关系不做限制。也就是说,对该连续物理地址进行映射时,其映射关系可为A对应A或其他逻辑关系,只要能体现对该连续物理地址进行映射即可。将物理地址转换为虚拟地址后,再将安全内存注册完成的信息及虚拟地址返回至该可信应用,该可信应用在接收到该安全内存注册完成的信息及虚拟地址之后,确定可与客户端共同执行安全业务。于是,该可信应用可通过处理器可信框架单元通知该客户端,安全内存注册完毕,使该客户端根据通知,确定可以执行业务。

[51]例如,客户端需要执行基于生物特征的登录业务,其中,生物特征的匹配过程由于涉及到用户隐私,为了保证数据安全以及用户隐私,该匹配过程可由可信执行环境内的可信应用执行。于是,该客户端在步骤S100之前可通过处理器可信框架单元向该可信执行环境内用于进行生物特征匹配的可信应用发送安全内存的注册指令,在步骤S102通过内存保护控制器注册完成安全内存后,该可信应用在接收到安全内存注册完成的信息时,可通过处理器可信框架单元向该客户端发送安全内存注册完毕的通知。则该客户端在接收到该通知后,可确定可信执行环境内的可信应用已经准备完毕,确定可以执行登录业务。则可调用通用执行环境的接口通过设备的图像传感器,采集待匹配的图像,并通过处理器可信框架单元将待匹配的图发送给可信应用进行生物特征匹配。可信应用则可基于已经注册的安全内存,存储待匹配的图像以及从服务器获取的目标图像,以及基于该安全内存执行生物特征匹配的业务。将匹配结果通过处理器可信框架单元返回客户端。

[52]基于图1所示的动态配置安全内存的方法,可见在本说明书提供的动态配置安全内存的方法中,通用执行环境中的客户端向可信执行环境中的可信应用发送安全内存的注册指令,注册指令中携带客户端申请的内存地址。可信应用根据所述注册指令,调用可信执行环境的操作系统的注册接口,向处理器可信框架单元发送安全内存的注册请求,使处理器可信框架单元根据注册请求,将内存地址对应的内存空间的属性更新为安全属性。

[53]从上述方法中可以看出,本方法是在客户端处理敏感数据涉及的业务时,将该业务转移至可信执行环境中的可信应用中处理,并且在可信应用处理之前,客户端会预估处理该业务所需的安全内存大小,再配置安全内存。即通过即时配置安全内存的方式,减少内存浪费问题,提高了内存利用率,还达到了保护敏感信息的目的。

[54]另外,在步骤S102中,该可信应用在调用该可信执行环境的操作系统的注册接口时,为了提高安全,还可对可信应用进行鉴权,当确定该可信应用具有注册安全内存的权限,该注册接口再生成向处理器可信框架单元发送的注册请求。

[55]具体的,该可信执行环境的操作系统的为了对调用该系统的各接口的可信应用进行鉴权,可预先针对每个接口,配置该接口的可信应用名单。不同的接口的可信应用名单不完全相同,可根据需要设置,本说明书不做限制。

[56]于是,该可信执行环境的操作系统的注册接口,也可配置有可信应用名单,该可信

应用名单包含：有权调用该注册接口的可信应用的标识。则该可信执行环境的操作系统的注册接口在接收到调用请求后，可确定该调用请求中携带的该可信应用的标识，并根据该调用请求中携带的标识与该可信应用名单中的各标识进行对比，判断该可信应用是否有权调用该注册接口。

[57]其中，该注册接口将该可信应用携带的标识与该可信应用名单中的各标识进行对比，若该可信应用携带的标识与该注册接口中包含的有权调用本身的可信应用名单中的任一可信应用的标识一致，则确定该可信应用有权调用该注册接口，则该注册接口接受该可信应用的调用。即，根据该可信应用的调用请求运行该注册接口对应的代码，执行相应的业务。若该可信应用携带的标识与该注册接口中包含的有权调用本身的可信应用名单中各可信应用的标识均不一致，则可确定该可信应用无权调用该注册接口，拒绝该可信应用的调用。并且，该可信执行环境的操作系统还可向该可信应用发送信息错误的提示，该提示用于使该可信应用确定自身无权调用该注册接口。

[58]例如，假设该可信执行环境中包含三个可信应用，分别是可信应用 A、可信应用 B 以及可信应用 C，可信应用 A 携带的标识为 1，可信应用 B 携带的标识为 2，可信应用 C 携带的标识为 3。注册接口 M 中包含有权调用该注册接口 M 本身的可信应用名单，该可信应用名单包含标识 1 以及标识 2。若可信应用 A、B、C 均发送调用注册接口 M 的调用请求，则该注册接口 M 在接收到各调用请求后，可分别根据调用请求中携带的可信应用的标识 1、2、3，以及自身包含的可信应用名单，进行可信应用的标识与可信应用名单的对比。根据对比结果可确定可信应用 A 及可信应用 B 可调用该注册接口 M，而由于标识 2 与可信应用名单的任一标识均不一致，因此可信应用 B 无权调用注册接口 M，所以注册接口 M 接受可信应用 A 及可信应用 B，向可信应用 C 发送信息错误的提示，拒绝可信应用 C 的调用。

[59]另外，当该可信执行环境的操作系统向该可信应用发送信息错误的提示后，该可信应用可确定无法继续执行业务。当然，该可信应用还可以通过处理器可信框架单元，将无权调用该注册接口的结果返回该客户端。则该客户端可确定业务执行失败，并可进一步展示该无权调用该注册接口的结果，使发起业务的用户可以确定业务执行存在问题。

[60]更进一步地，在本说明书一个或多个实施例中，通常处理器可信框架单元并不具备在未配置安全内存的情况下，将内存的属性变更为安全属性的功能。为了实现步骤 S102 中所述的该处理器可信框架单元根据该注册请求，调用内存保护控制器将内存空闲的存储空间中确定内存要注册为安全内存的连续物理地址的功能，可预先对处理器可信框架单元的代码进行更新。通过更新，增加处理器可信框架单元实现上述注册安全内存功能的代码，如，注册接口的接口代码以及进行内存的属性更新的代码，使得处理器可信框架单元在接收到注册请求后，可执行步骤 S102 中所述的操作，调用内存保护控制器实时进行安全内存的注册。实现动态配置安全内存，提高设备的内存利用率。

[61]基于图 1 所示的动态配置安全内存的流程，本说明书实施例还提供一种可信执行环境的操作系统执行的动态配置安全内存的流程，如图 3 所示，包括步骤 S200 至步骤 S202。

[62]S200：接收可信应用对注册接口的调用请求，所述调用请求携带通用执行环境中的客户端申请的内存地址。

[63]在本说明书一个或多个实施例中，以设备的可信执行环境的操作系统为执行主体，对动态配置安全内存的流程进行说明。在本说明书一个或多个实施例中，动态配置的安全内存是为了支持可信应用执行业务，而非支持该系统运行，因此该可信执行环境的操作系统可接收可信应用对注册接口的调用请求。其中，该调用请求携带通用执行环境中的客户端申请的内存地址。该通用执行环境中的客户端申请内存地址的具体过程及原因已在上文说明，在此不再赘述。

[64]在该客户端确定该内存地址后，该客户端可将该内存地址经由处理器可信框架单元

分发至可信应用，而该可信应用可请求调用该可信执行环境的操作系统的注册接口，并将该内存地址发送给该可信执行环境的操作系统。

[65]另外，该可信执行环境的操作系统在根据调用请求通过该注册接口的代码执行业务之前，可通过该调用请求中携带的可信应用的标识确定该可信应用是否有权调用该注册接口。

[66]具体的，该可信执行环境的操作系统的为了对调用该系统的各接口的可信应用进行鉴权，可预先针对每个接口，配置该接口的可信应用名单。不同的接口的可信应用名单不完全相同，可根据需要设置，本说明书不做限制。

[67]于是，该可信执行环境的操作系统的注册接口，也可配置有可信应用名单，该可信应用名单包含：有权调用该注册接口的可信应用的标识。则该可信执行环境的操作系统的注册接口在接收到调用请求后，可确定该调用请求中携带的该可信应用的标识，并根据该调用请求中携带的标识与该可信应用名单中的各标识进行对比，判断该可信应用是否有权调用该注册接口。

[68]上述鉴权的具体操作过程包括，该注册接口将该可信应用携带的标识与该可信应用名单中的各标识进行对比，若该可信应用携带的标识与该注册接口中包含的有权调用本身的可信应用名单中的任一可信应用的标识一致，则确定该可信应用有权调用该注册接口，则该注册接口接受该可信应用的调用。即，根据该可信应用的调用请求运行该注册接口对应的代码，执行相应的业务。若该可信应用携带的标识与该注册接口中包含的有权调用本身的可信应用名单中各可信应用的标识均不一致，则可确定该可信应用无权调用该注册接口，拒绝该可信应用的调用。并且，该可信执行环境的操作系统还可向该可信应用发送信息错误的提示，该提示用于使该可信应用确定自身无权调用该注册接口。

[69]例如，假设该可信执行环境中包含三个可信应用，分别是可信应用 A、可信应用 B 以及可信应用 C，可信应用 A 携带的标识为 1，可信应用 B 携带的标识为 2，可信应用 C 携带的标识为 3。注册接口 M 中包含有权调用该注册接口 M 本身的可信应用名单，该可信应用名单包含标识 1 以及标识 2。若可信应用 A、B、C 均发送调用注册接口 M 的调用请求，则该注册接口 M 在接收到各调用请求后，可分别根据调用请求中携带的可信应用的标识 1、2、3，以及自身包含的可信应用名单，进行可信应用的标识与可信应用名单的对比。根据对比结果可确定可信应用 A 及可信应用 B 可调用该注册接口 M，而由于标识 2 与可信应用名单的任一标识均不一致，因此可信应用 B 无权调用注册接口 M，所以注册接口 M 接受可信应用 A 及可信应用 B，向可信应用 C 发送信息错误的提示，拒绝可信应用 C 的调用。

[70]另外，当该可信执行环境的操作系统向该可信应用发送信息错误的提示后，该可信应用可确定无法继续执行业务。当然，该可信应用还可以通过处理器可信框架单元，将无权调用该注册接口的结果返回该客户端。则该客户端可确定业务执行失败，并可进一步展示该无权调用该注册接口的结果，使发起业务的用户可以确定业务执行存在问题。

[71]S202: 根据所述调用请求生成注册请求，向处理器可信框架单元发送所述注册请求，使所述处理器可信框架单元根据所述注册请求，将所述内存地址对应的内存空间的属性更新为安全属性。

[72]由于可信执行环境的操作系统是一个隔离环境，因此通常不能直接对设备的内存属性进行更新，也就是说不能由可信执行环境的操作系统直接进行安全内存的配置。于是，在本说明书一个或多个实施例中，在该可信执行环境的操作系统通过注册接口接收到该调用请求后，该可信执行环境的操作系统根据该注册接口对应业务逻辑，以及该调用请求携带的内存地址，生成注册请求，将该注册请求发送至处理器可信框架单元，通过该处理器可信框架单元调用内存保护控制器，将内存空间的属性更新为安全属性，实现该内存只允许相应的可信应用使用的目的。

[73]具体的,首先,该可信执行环境的操作系统,可根据该可信应用调用的该注册接口,确定该内存地址。并根据该注册接口对应业务逻辑,运行该注册接的接口代码。

[74]然后,通过运行该接口代码,该可信执行环境的操作系统,可基于该调用请求携带的内存地址,生成注册请求。

[75]最后,该可信执行环境的操作系统向处理器可信框架单元发送该注册请求,通过该处理器可信框架单元调用内存保护控制器,将内存空间的属性更新为安全属性。

[76]其中,通常处理器可信框架单元并不具备在未配置安全内存的情况下,将内存的属性变更为安全属性的功能。为了实现通过该处理器可信框架单元根据该注册请求,调用内存保护控制器将内存空闲的存储空间中确定内存要注册为安全内存的连续物理地址的功能,可预先对处理器可信框架单元的代码进行更新。通过更新,增加处理器可信框架单元实现上述注册安全内存功能的代码。如,注册接口的接口代码以及进行内存的属性更新的代码,使得处理器可信框架单元在接收到注册请求后,可执行上述操作,调用内存保护控制器实时进行安全内存的注册。实现动态配置安全内存,提高设备的内存利用率。

[77]在本说明书一个或多个实施例中,该内存保护控制器具备更新内存空间的属性的功能,则在处理器可信框架单元的调用下,可根据该内存地址,确定对应的连续物理地址,并将该连续物理地址的属性更新为安全属性。之后,该内存保护控制器可向该处理器可信框架单元返回确认信息。该处理器可信框架单元接收到确认信息后,向该可信执行环境的操作系统返回安全内存注册完成的信息,该可信执行环境的操作系统该可信执行环境的操作系统接收到该安全内存注册完成的信息后,对该内存地址进行映射,即对该连续物理地址进行映射,生成对应的映射表,该映射表包含该连续物理地址对应的虚拟地址以及两者的映射关系。本说明书对其映射关系不做限制。也就是说,对该连续物理地址进行映射时,其映射关系可为A对应A或其他逻辑关系,只要能体现对该连续物理地址进行映射即可。将物理地址转换为虚拟地址后,再将安全内存注册完成的信息及虚拟地址返回至该可信应用,该可信应用在接收到该安全内存注册完成的信息及虚拟地址之后,确定可与客户端共同执行安全业务。

[78]另外,可信执行环境的操作系统向处理器可信框架单元发送注册请求,以及处理器可信框架单元接收发送的注册请求都可先进行验证,在验证通过后,再进行下一步操作,若验证不通过,则返回错误信息,错误信息用于提示存在安全隐患。当然,由于如何进行程序间的验证(如,鉴权)的技术已经是较为成熟的技术,本说明书不再赘述,也不限制具体采用何种方式进行验证。

[79]基于图1所示的动态配置安全内存的流程,本说明书实施例还提供一种处理器可信框架单元执行的动态配置安全内存的流程,如图4所示,包括步骤S300至步骤S302。

[80]S300:接收可信执行环境的操作系统发送的注册请求,所述注册请求包含内存地址。

[81]在本说明书一个或多个实施例中,在该处理器可信框架单元接收该可信执行环境的操作系统发送的该安全内存的注册请求之前,先接收通用执行环境中的客户端发送的注册指令并将该注册指令转发至可信应用。其中,该注册指令中携带有该客户端向连续内存分配器发送请求得到的连续的内存地址。该客户端得到该连续的内存地址的过程及通过该处理器可信框架单元转发该注册指令的原因在上述已经说明,故不在此赘述。该可信应用接收该注册指令后,向该可信执行环境的操作系统发送调用请求,该可信执行环境的操作系统根据该调用请求生成注册请求,并将该注册请求发送至该处理器可信框架单元。其中,该注册请求包含内存地址。

[82]S302:根据所述注册请求,将所述内存地址对应的内存空间的属性更新为安全属性。

[83]该处理器可信框架单元根据该注册请求,向内存保护控制器发送调用指令,该调用

指令携带该内存地址。该内存保护控制器可根据该处理器可信框架单元的调用指令，确定该内存地址，并从内存空闲的存储空间中确定内存要注册为安全内存的连续物理地址。并将确定出的连续物理地址的属性，更新为安全属性。上述内存保护控制器将内存空间的属性更新为安全属性的具体过程已作详细说明，故不再赘述。

[84]另外，计算机设备内有一电子元件，该电子元件有自己的存储空间，该内存空间存储了内存的配置信息，启动该电子元件之后，该电子元件根据该配置信息判断哪些是安全内存，哪些是非安全内存，以及处理器执行对应业务时，有权访问上述安全内存的业务名单。在本说明书一个或多个实施例中，在处理器访问安全内存之前要先经过该电子元件的鉴权。鉴权的具体过程如下：该处理器在访问安全内存之前，将访问该安全内存的请求发送至该电子元件，该电子元件接收访问请求后，将该电子元件自身存储的有权访问安全内存的对应业务名单与该业务进行对比，若该业务存在于该电子元件存储的有权访问安全内存对应业务的名单中，则确定处理该业务时的处理器有权使用该安全内存，同意其进行安全内存访问。若该业务不存在于该电子元件存储的有权访问安全内存对应业务的名单中，则确定处理该业务时的处理器无权使用该安全内存，拒绝其进行安全内存访问。

[85]本说明书中在启动时该电子元件不再进行此项鉴权操作，而是实时进行鉴权，且由内存保护控制器发送内存属性变更信息至该电子元件，该电子元件根据该信息存储变更为安全内存的内存信息以及对应业务名单。信息变更之后，该电子元件对该处理器进行鉴权时，根据最新的内存信息判断处理器是否有权访问该安全内存。

[86]在该连续物理地址的属性更新为安全属性以及该电子元件变更内存信息之后，后续步骤不再复述。

[87]基于图 1、图 3 以及图 4 所示的动态配置安全内存的流程，本说明书实施例还提供一种动态配置安全内存的设备示意图，如图 5a 所示，进行动态配置安全内存的设备中，至少安装有以下程序：客户端 400、可信应用 402、可信执行环境的操作系统 404 以及处理器可信框架单元 406。

[88]其中，客户端 400 运行在通用执行环境（REE）中，可信应用 402 及可信执行环境的操作系统 404 运行在可信执行环境（TEE）中，处理器可信框架单元 406 为可信执行环境与通用执行环境的中间件，用于提供可信执行环境中可信应用 402 与通用执行环境中客户端 400 交互的服务。

[89]该客户端 400，用于确定在该可信执行环境执行业务所需的内存地址；向该可信应用 402 发送注册指令，该注册指令中携带有该内存地址。

[90]该可信应用 402，用于接收该客户端 400 发送的注册指令；根据携带该内存地址的该注册指令，生成调用该可信执行环境的操作系统 404 中的注册接口的调用请求。

[91]该可信执行环境的操作系统 404，用于接收该可信应用 402 对该注册接口的调用请求；根据该调用请求生成注册请求，向处理器可信框架单元 406 发送该注册请求。

[92]该处理器可信框架单元 406，用于接收该可信执行环境的操作系统 404 发送的该注册请求；根据该注册请求，将该内存地址对应的内存空间的属性更新为安全属性。

[93]当然，在本说明书一个或多个实施例中，如图 5b 所示，该动态配置安全内存的设备还可包括：内存保护控制器 408。

[94]该处理器可信框架单元 406，接收该可信执行环境的操作系统 404 发送的该注册请求后，还用于根据该注册请求向该内存保护控制器 408 发送调用指令。

[95]而该内存保护控制器 408，用于根据该调用指令，将该内存地址对应的内存空间的属性更新为安全属性。

[96]上述动态配置安全内存的流程中涉及到的各方的交互过程，如图 6 所示，具体包括步骤 S500 至步骤 S507。

[97]S500：所述客户端确定在可信执行环境执行业务所需的内存地址。

[98]S501：所述客户端向处理器可信框架单元发送注册指令，所述注册指令中携带有所述内存地址。

[99]在本说明书一个或多个实施例中，客户端用于确定在可信执行环境执行业务所需的内存大小，向连续内存分配器发送携带该内存大小的内存分配请求。接收该连续内存分配器返回的内存地址。根据该内存地址，生成注册指令。将该注册指令发送至处理器可信框架单元。上述过程具体内容可参考图 1 的相关描述。

[100]S502：所述处理器可信框架单元将注册指令转发给可信应用。

[101]S503：所述可信应用接收所述处理器可信框架单元发送的注册指令。

[102]S504：所述可信应用根据所述注册指令，调用可信执行环境的操作系统中的注册接口。

[103]该可信应用接收注册指令后，再根据该注册指令，从可信执行环境的操作系统的接口中，查询注册接口。调用该注册接口，将内存地址发送给该可信执行环境的操作系统，使得该可信执行环境的操作系统根据该注册接口对应业务逻辑，向该处理器可信框架单元发送安全内存的注册请求，且该注册请求携带该内存地址。上述过程具体内容可参考图 1 的相关描述

[104]S505：所述可信执行环境的操作系统接收所述可信应用对所述注册接口的调用请求。

[105]S506：所述可信执行环境的操作系统根据所述调用请求生成注册请求，向处理器可信框架单元发送所述注册请求。

[106]具体的，可信执行环境的操作系统根据注册接口对应业务逻辑，以及调用请求携带的内存地址，生成注册请求。向处理器可信框架单元发送该注册请求，使处理器可信框架单元调用内存保护控制器，将内存空间的属性更新为安全属性。且该注册请求包含所述内存地址。上述过程具体内容可参考图 3 的相关描述

[107]S507：所述处理器可信框架单元根据所述注册请求，将所述内存地址对应的内存空间的属性更新为安全属性。

[108]具体的，处理器可信框架单元根据注册请求，调用内存保护控制器将内存空间的属性更新为安全属性。另外，该处理器可信框架单元还用于接收客户端发送的注册指令，将该注册指令转发给可信应用。

[109]基于图 1、图 3 以及图 4 所示的动态配置安全内存的流程，本说明书实施例还提供相应的动态配置安全内存装置，如图 7 所示。

[110]图 7 为本说明书提供的动态配置安全内存装置包括：第一接收模块 600，用于接收安全内存的注册指令，所述注册指令中携带有客户端申请的内存地址；内存配置模块 602，用于根据所述注册指令，调用可信执行环境的操作系统的注册接口，向处理器可信框架单元发送安全内存的注册请求，使所述处理器可信框架单元根据所述注册请求，将所述内存地址对应的内存空间的属性更新为安全属性；第二接收模块 604，用于接收所述可信执行环境的操作系统返回的虚拟地址，以根据所述虚拟地址调用所述安全内存执行业务，其中，所述虚拟地址为所述可信执行环境的操作系统确定的，与所述内存地址存在映射关系的虚拟地址。

[111]可选地，所述第一接收模块 600，具体用于接收所述处理器可信框架单元转发的安全内存的注册指令，所述注册指令为通用执行环境中的客户端调用所述处理器可信框架

单元的接口发送的；其中，所述内存地址为所述客户端向连续内存分配器发送请求得到的。

[112]可选地，所述内存配置模块 602，具体用于根据所述注册指令，从所述可信执行环境的操作系统的接口中，查询注册接口；调用所述注册接口，将所述内存地址发送给所述可信执行环境的操作系统，使所述可信执行环境的操作系统根据所述注册接口对应业务逻辑，向所述处理器可信框架单元发送安全内存的注册请求，所述注册请求携带所述内存地址。

[113]基于图 1、图 3 以及图 4 所示的动态配置安全内存的流程，本说明书实施例还提供相应的动态配置安全内存装置，如图 8 所示。

[114]图 8 为本说明书提供的动态配置安全内存装置包括：接收模块 700，用于接收可信应用对注册接口的调用请求，所述调用请求携带通用执行环境中的客户端申请的内存地址；内存配置模块 702，用于根据所述调用请求生成注册请求，向处理器可信框架单元发送所述注册请求，使所述处理器可信框架单元根据所述注册请求，将所述内存地址对应的内存空间的属性更新为安全属性。

[115]可选地，内存配置模块 702，具体用于根据所述注册接口对应业务逻辑，以及所述调用请求携带的所述内存地址，生成注册请求；向处理器可信框架单元发送所述注册请求，使所述处理器可信框架单元调用内存保护控制器，将所述内存空间的属性更新为安全属性，所述注册请求包含所述内存地址。

[116]可选的，内存配置模块 702，还用于确定所述内存地址对应的内存空间的属性更新为安全属性后，生成所述内存地址对应的虚拟地址，并确定所述内存地址与所述虚拟地址的对应关系；将所述虚拟地址返回所述可信应用，使所述可信应用执行业务时根据所述虚拟地址调用安全内存。

[117]基于图 1、图 3 及图 4 所示的动态配置安全内存的流程，本说明书实施例还提供相应的动态配置安全内存装置，如图 9 所示。

[118]图 9 为本说明书提供的动态配置安全内存装置包括：转发模块 800，用于接收通用执行环境中的客户端发送的注册指令，其中，所述注册指令中携带有所述客户端向连续内存分配器发送请求得到的连续的内存地址；将所述注册指令转发至所述可信应用；

[119]接收模块 802，用于接收可信执行环境的操作系统发送的注册请求，所述注册请求包含内存地址；内存配置模块 804，用于根据所述注册请求，将所述内存地址对应的内存空间的属性更新为安全属性。

[120]可选地，内存配置模块 804，具体用于根据所述注册请求，调用内存保护控制器，将所述内存地址对应的内存空间的属性更新为安全属性。

[121]本说明书还提供了一种计算机可读存储介质，该存储介质存储有计算机程序，计算机程序可用于执行上述图 1、图 3 以及图 4 提供的动态配置安全内存方法。

[122]在 20 世纪 90 年代，对于一个技术的改进可以很明显地区分是硬件上的改进（例如，对二极管、晶体管、开关等电路结构的改进）还是软件上的改进（对于方法流程的改进）。然而，随着技术的发展，当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此，不能说一个方法流程的改进就不能用硬件实体模块来实现。例如，可编程逻辑器件（Programmable Logic Device，PLD）（例如现场可编程门阵列（Field Programmable Gate Array，FPGA））就是这样一种集成电路，其逻辑功能由用户对器件编程来确定。由设计人员自行编程来把一个数字系统“集成”在一片 PLD 上，而不需要请芯片制造厂商来设计和制作专用的集成电路芯片。而且，如今，取代手工地制作集成电路芯片，这种编程也多半改用“逻辑编译器（logic compiler）”软件来实现，它与

程序开发撰写时所用的软件编译器相类似，而要编译之前的原始代码也得用特定的编程语言来撰写，此称之为硬件描述语言（Hardware Description Language, HDL），而 HDL 也并非仅有一种，而是有许多种，如 ABEL（Advanced Boolean Expression Language）、AHDL（Altera Hardware Description Language）、Confluence、CUPL（Cornell University Programming Language）、HDL、JHDL（Java Hardware Description Language）、Lava、Lola、MyHDL、PALASM、RHDL（Ruby Hardware Description Language）等，目前最普遍使用的是 VHDL（Very-High-Speed Integrated Circuit Hardware Description Language）与 Verilog。本领域技术人员也应该清楚，只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中，就可以很容易得到实现该逻辑方法流程的硬件电路。

[123] 控制器可以按任何适当的方式实现，例如，控制器可以采取例如微处理器或处理器以及存储可由该（微）处理器执行的计算机可读程序代码（例如软件或固件）的计算机可读介质、逻辑门、开关、专用集成电路（Application Specific Integrated Circuit, ASIC）、可编程逻辑控制器和嵌入微控制器的形式，控制器的例子包括但不限于以下微控制器：ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20 以及 Silicone Labs C8051F320，存储器控制器还可以被实现为存储器的控制逻辑的一部分。本领域技术人员也知道，除了以纯计算机可读程序代码方式实现控制器以外，完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器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功能的装置也可以视为硬件部件内的结构。或者甚至，可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

[124] 上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机。具体的，计算机例如可以为个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。

[125] 为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本说明书时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[126] 本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[127] 本申请是参照根据本申请实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[128] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[129] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或

其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的步骤。

[130]在一个典型的配置中, 计算设备包括一个或多个处理器 (CPU)、输入/输出接口、网络接口和内存。

[131]内存可能包括计算机可读介质中的非永久性存储器, 随机存取存储器 (RAM) 和/或非易失性内存等形式, 如只读存储器 (ROM) 或闪存 (flash RAM)。内存是计算机可读介质的示例。

[132]计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括, 但不限于相变内存 (PRAM)、静态随机存取存储器 (SRAM)、动态随机存取存储器 (DRAM)、其他类型的随机存取存储器 (RAM)、只读存储器 (ROM)、电可擦除可编程只读存储器 (EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器 (CD-ROM)、数字多功能光盘 (DVD) 或其他光学存储、磁盒式磁带, 磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质, 可用于存储可以被计算设备访问的信息。按照本文中的界定, 计算机可读介质不包括暂存电脑可读媒体 (transitory media), 如调制的数据信号和载波。

[133]还需要说明的是, 术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含, 从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素, 而且还包括没有明确列出的其他要素, 或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下, 由语句“包括一个……”限定的要素, 并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[134]本领域技术人员应明白, 本说明书的实施例可提供为方法、系统或计算机程序产品。因此, 本说明书可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且, 本说明书可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质 (包括但不限于磁盘存储器、CD-ROM、光学存储器等) 上实施的计算机程序产品的形式。

[135]本说明书可以在由计算机执行的计算机可执行指令的一般上下文中描述, 例如程序模块。一般地, 程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本说明书, 在这些分布式计算环境中, 由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中, 程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[136]本说明书中的各个实施例均采用递进的方式描述, 各个实施例之间相同相似的部分互相参见即可, 每个实施例重点说明的都是与其他实施例的不同之处。尤其, 对于系统实施例而言, 由于其基本相似于方法实施例, 所以描述的比较简单, 相关之处参见方法实施例的部分说明即可。

[137]以上所述为本说明书的实施例, 并不用于限制本说明书。对于本领域技术人员来说, 本说明书可以有各种更改和变化。凡在本说明书的精神和原理之内所作的任何修改、等同替换、改进等, 均应包含在本申请的权利要求范围之内。

权利要求书

- 1、一种动态配置安全内存的方法，所述方法应用于可信应用，所述方法包括：
接收安全内存的注册指令，所述注册指令中携带有客户端申请的内存地址；
根据所述注册指令，调用可信执行环境的操作系统的注册接口，向处理器可信框架单元发送安全内存的注册请求，使所述处理器可信框架单元根据所述注册请求，将所述内存地址对应的内存空间的属性更新为安全属性。
- 2、如权利要求1所述的方法，接收安全内存的注册指令，包括：
接收所述处理器可信框架单元转发的安全内存的注册指令，所述注册指令为通用执行环境中的客户端调用所述处理器可信框架单元的接口发送的；
其中，所述内存地址为所述客户端向连续内存分配器发送请求得到的连续的内存地址。
- 3、如权利要求1所述的方法，根据所述注册指令，调用可信执行环境的系统中的注册接口，向所述处理器可信框架单元发送安全内存的注册请求，包括：
根据所述注册指令，从所述可信执行环境的操作系统的接口中，查询注册接口；
调用所述注册接口，将所述内存地址发送给所述可信执行环境的操作系统，使所述可信执行环境的操作系统根据所述注册接口对应业务逻辑，向所述处理器可信框架单元发送安全内存的注册请求，所述注册请求携带所述内存地址。
- 4、如权利要求1所述的方法，所述方法还包括：
接收所述可信执行环境的操作系统返回的虚拟地址，以根据所述虚拟地址调用所述安全内存执行业务，其中，所述虚拟地址为所述可信执行环境的操作系统确定的，与所述内存地址存在映射关系的虚拟地址。
- 5、一种动态配置安全内存的方法，所述方法应用于可信执行环境的操作系统，所述方法包括：
接收可信应用对注册接口的调用请求，所述调用请求携带通用执行环境中的客户端申请的内存地址；
根据所述调用请求生成注册请求，向处理器可信框架单元发送所述注册请求，使所述处理器可信框架单元根据所述注册请求，将所述内存地址对应的内存空间的属性更新为安全属性。
- 6、如权利要求5所述的方法，根据所述调用请求生成注册请求，向处理器可信框架单元发送所述注册请求，使所述处理器可信框架单元根据所述注册请求，将所述内存地址对应的内存空间的属性更新为安全属性，包括：
根据所述注册接口对应业务逻辑，以及所述调用请求携带的所述内存地址，生成注册请求；
向处理器可信框架单元发送所述注册请求，使所述处理器可信框架单元调用内存保护控制器，将所述内存空间的属性更新为安全属性，所述注册请求包含所述内存地址。
- 7、如权利要求5所述的方法，所述方法还包括：
确定所述内存地址对应的内存空间的属性更新为安全属性后，生成所述内存地址对应的虚拟地址，并确定所述内存地址与所述虚拟地址的对应关系；
将所述虚拟地址返回所述可信应用，使所述可信应用执行业务时根据所述虚拟地址调用安全内存。
- 8、一种动态配置安全内存的方法，所述方法应用于处理器可信框架单元，所述方法包括：
接收可信执行环境的操作系统发送的注册请求，所述注册请求包含内存地址；
根据所述注册请求，将所述内存地址对应的内存空间的属性更新为安全属性。
- 9、如权利要求8所述的方法，在处理器可信框架单元接收可信执行环境的操作系统发送的安全内存的注册请求之前，所述方法还包括：
接收通用执行环境中的客户端发送的注册指令，其中，所述注册指令中携带有所述客户端向连续内存分配器发送请求得到的连续的内存地址；

将所述注册指令转发至所述可信应用。

10、如权利要求 8 所述的方法，根据所述注册请求，将所述内存地址对应的内存空间的属性更新为安全属性，包括：

根据所述注册请求，调用内存保护控制器，将所述内存地址对应的内存空间的属性更新为安全属性。

11、一种动态配置安全内存的设备，所述设备包括通用执行环境中的客户端、可信执行环境的操作系统、可信应用以及处理器可信框架单元，其中：

所述客户端，用于确定在所述可信执行环境执行业务所需的内存地址；向所述可信应用发送注册指令，所述注册指令中携带有所述内存地址；

所述可信应用，用于接收所述客户端发送的注册指令；根据携带所述内存地址的所述注册指令，生成调用所述可信执行环境的操作系统中的注册接口的调用请求；

所述可信执行环境的操作系统，用于接收所述可信应用对所述注册接口的调用请求；根据所述调用请求生成注册请求，向处理器可信框架单元发送所述注册请求；

所述处理器可信框架单元，用于接收所述可信执行环境的操作系统发送的所述注册请求；根据所述注册请求，将所述内存地址对应的内存空间的属性更新为安全属性。

12、如权利要求 11 所述的设备，所述客户端，用于确定在所述可信执行环境执行业务所需的内存大小，向连续内存分配器发送携带所述内存大小的内存分配请求；接收所述连续内存分配器返回的连续的内存地址；根据所述内存地址，生成注册指令；将所述注册指令发送至所述处理器可信框架单元；

所述处理器可信框架单元，还用于接收所述客户端发送的所述注册指令，将所述注册指令转发给所述可信应用；

所述可信应用，用于接收所述处理器可信框架单元转发的注册指令。

13、如权利要求 11 所述的设备，所述可信应用，用于根据携带所述内存地址的所述注册指令，从所述可信执行环境的操作系统的接口中，查询注册接口；根据所述注册指令，生成针对所述注册接口的调用请求，并向所述可信执行环境的操作系统发送所述调用请求。

14、如权利要求 11 所述的设备，所述可信执行环境的操作系统，用于接收所述调用请求，确定所述注册接口；根据所述注册接口对应业务逻辑，以及所述调用请求携带的所述内存地址，生成注册请求。

15、如权利要求 11 所述的设备，所述设备还包括：内存保护控制器；

所述处理器可信框架单元，用于根据所述注册请求，向所述内存保护控制器发送调用指令；

所述内存保护控制器，用于根据所述调用指令，将所述内存地址对应的内存空间的属性更新为安全属性。

16、如权利要求 11 所述的设备，所述处理器可信框架单元，还用于确定所述内存地址对应的内存空间的属性更新为安全属性后，向所述可信执行环境的操作系统返回确认信息；

所述可信执行环境的操作系统，还用于根据接收到的确认信息，生成所述内存地址对应的虚拟地址，并确定所述内存地址与所述虚拟地址的对应关系；将所述虚拟地址返回所述可信应用；

所述可信应用，还用于接收所述可信执行环境的系统发送的虚拟地址，以根据所述虚拟地址调用所述安全内存执行业务。

17、一种动态配置安全内存装置，所述装置包括：

接收模块，用于接收安全内存的注册指令，所述注册指令中携带有客户端申请的内存地址；

内存配置模块，用于根据所述注册指令，调用可信执行环境的操作系统的注册接口，向处理器可信框架单元发送安全内存的注册请求，使所述处理器可信框架单元根据所述注册请求，将所述内存地址对应的内存空间的属性更新为安全属性。

18、一种动态配置安全内存装置，所述装置包括：

接收模块，用于接收可信应用对注册接口的调用请求，所述调用请求携带通用执行环境中的客户端申请的内存地址；

内存配置模块，用于根据所述调用请求生成注册请求，向处理器可信框架单元发送所述注册请求，使所述处理器可信框架单元根据所述注册请求，将所述内存地址对应的内存空间的属性更新为安全属性。

19、一种动态配置安全内存装置，所述装置包括：

接收模块，接收可信执行环境的操作系统发送的注册请求，所述注册请求包含内存地址；

内存配置模块，根据所述注册请求，将所述内存地址对应的内存空间的属性更新为安全属性。

20、一种计算机可读存储介质，所述存储介质存储有计算机程序，所述计算机程序被处理器执行时实现上述权利要求 1~10 中任一项所述的方法。