(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 106295267 A
(43)申请公布日 2017.01.04

(21)申请号 201510314210.2

(22)申请日 2015.06.09

(71)申请人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼资本大厦一座四层847号邮箱

(72)发明人 党茂昌

(74)专利代理机构 北京汉昊知识产权代理事务所(普通合伙) 11370
代理人 朱海波

(51)Int.Cl.
G06F 21/31(2013.01)
G06F 21/62(2013.01)
G06F 21/78(2013.01)

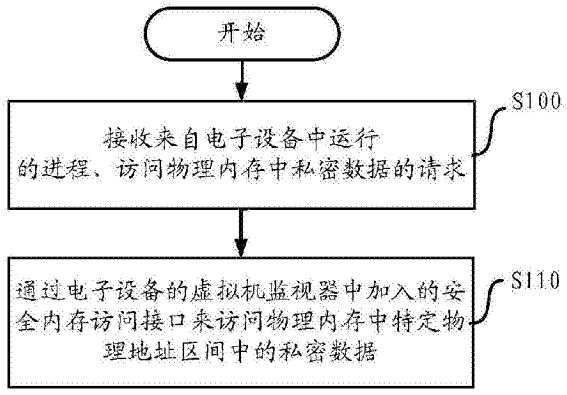
权利要求书2页 说明书8页 附图3页

(54)发明名称

一种访问电子设备的物理内存中私密数据的方法和装置

(57)摘要

本申请提供了一种访问电子设备的物理内存中私密数据的方法和装置,其中所述方法包括:接收来自电子设备中运行的进程、访问物理内存中私密数据的请求;通过电子设备的虚拟机监视器中加入的安全内存访问接口来访问物理内存中特定物理地址区间中的私密数据,其中在电子设备的内存管理单元中不建立该特定物理地址区间的映射关系,所述安全内存访问接口被预先设计成实现对物理内存中所述特定物理地址区间中的私密数据的访问。本申请的方法和装置可以提升私密数据在物理内存中的安全性。



CN 106295267 A

1. 一种访问电子设备的物理内存中私密数据的方法，所述方法包括：

接收来自电子设备中运行的进程、访问物理内存中私密数据的请求；

通过电子设备的虚拟机监视器中加入的安全内存访问接口来访问物理内存中特定物理地址区间中的私密数据，其中在电子设备的内存管理单元中不建立该特定物理地址区间的映射关系，所述安全内存访问接口被预先设计成实现对物理内存中所述特定物理地址区间中的私密数据的访问。

2. 根据权利要求 1 所述的方法，其中所述访问包括读和 / 或写。

3. 根据权利要求 1 所述的方法，其中通过电子设备的虚拟机监视器中加入的安全内存访问接口来访问物理内存中特定物理地址区间中的私密数据的步骤包括：

通过该安全内存访问接口为要访问的私密数据分配对应的位于所述特定物理地址区间中的物理地址子区间；

在所述物理地址子区间中执行对所述私密数据的访问。

4. 根据权利要求 3 所述的方法，还包括：

响应于预定条件，释放所述特定物理地址区间中的私密数据对应的物理地址子区间。

5. 根据权利要求 1 所述的方法，其中接收来自电子设备中运行的进程、访问物理内存中私密数据的请求的步骤包括：

接收来自电子设备中运行的进程的、访问物理内存中数据的请求；

判断所述请求要访问的数据是私密数据。

6. 根据权利要求 5 所述的方法，其中判断所述请求要访问私密数据的步骤包括：

如果所述请求要访问的数据是将存储器上的密文文件解密成的明文，判断所述请求要访问的数据是私密数据。

7. 根据权利要求 5 所述的方法，其中判断所述请求要访问私密数据的步骤包括：

如果所述请求要访问的数据是电子设备的程序运行时产生的数据，通过判断例程判断出所述请求要访问的数据是私密数据。

8. 根据权利要求 5 所述的方法，其中判断所述请求要访问私密数据的步骤包括：

如果所述请求要访问的数据是电子设备从外部获取的数据，向用户提示是否需要将从外部获取的数据作为私密数据存储；

响应于用户确认需要将从外部获取的数据作为私密数据存储，判断出所述请求要访问的数据是私密数据。

9. 根据权利要求 1 所述的方法，还包括：

提示用户输入用于访问私密数据的认证信息；

对用户输入的认证信息进行鉴权，其中只有在鉴权通过的前提下才执行通过电子设备的虚拟机监视器中加入的安全内存访问接口来访问物理内存中特定物理地址区间中的私密数据的步骤。

10. 一种访问电子设备的物理内存中私密数据的装置，所述装置包括：

接收单元，被配置为接收来自电子设备中运行的进程、访问物理内存中私密数据的请求；

访问单元，被配置为通过电子设备的虚拟机监视器中加入的安全内存访问接口来访问物理内存中特定物理地址区间中的私密数据，其中在电子设备的内存管理单元中不建立该

特定物理地址区间的映射关系，所述安全内存访问接口被预先设计成实现对物理内存中所述特定物理地址区间中的私密数据的访问。

11. 根据权利要求 10 所述的装置，其中所述访问包括读和 / 或写。

12. 根据权利要求 10 所述的装置，其中所述访问单元被配置为：

通过该安全内存访问接口为要访问的私密数据分配对应的位于所述特定物理地址区间中的物理地址子区间；

在所述物理地址子区间中执行对所述私密数据的访问。

13. 根据权利要求 12 所述的装置，其中所述访问单元还被配置为：

响应于预定条件，释放所述特定物理地址区间中的私密数据对应的物理地址子区间。

14. 根据权利要求 10 所述的装置，其中所述接收单元被配置为：

接收来自电子设备中运行的进程、访问物理内存中数据的请求；

判断所述请求要访问的数据是私密数据。

15. 根据权利要求 14 所述的装置，其中所述接收单元判断所述请求要访问的数据是私密数据的过程包括：

如果所述请求要访问的数据是将存储器上的密文文件解密成的明文，判断所述请求要访问的数据是私密数据。

16. 根据权利要求 14 所述的装置，其中所述接收单元判断所述请求要访问的数据是私密数据的过程包括：

如果所述请求要访问的数据是电子设备的程序运行时产生的数据，通过判断例程判断出所述请求要访问的数据是私密数据。

17. 根据权利要求 14 所述的装置，其中所述接收单元判断所述请求要访问的数据是私密数据的过程包括：

如果所述请求要访问的数据是电子设备从外部获取的数据，向用户提示是否需要将从外部获取的数据作为私密数据存储；

响应于用户确认需要将从外部获取的数据作为私密数据存储，判断出所述请求要访问的数据是私密数据。

18. 根据权利要求 10 所述的装置，还包括：

提示单元，被配置为提示用户输入用于访问私密数据的认证信息；

鉴权单元，被配置为对用户输入的认证信息进行鉴权，

其中所述访问单元被配置为只有在鉴权通过的前提下才通过电子设备的虚拟机监视器中加入的安全内存访问接口来访问物理内存中特定物理地址区间中的私密数据。

一种访问电子设备的物理内存中私密数据的方法和装置

技术领域

[0001] 本申请涉及电子技术领域，尤其涉及一种访问电子设备的物理内存中私密数据的方法和装置。

背景技术

[0002] 对于目前的大多数电子设备而言，例如计算机、手机等，由于现有技术中缺乏对电子设备物理内存中私密数据（诸如用户付款的账户名称、支付密码等）的保护，私密数据和普通数据都无差别地基于内存管理单元来管理，而操作系统在任何情况下都可以基于内存管理单元所建立的地址映射关系来访问物理内存中的私密数据，因而黑客可以利用恶意程序或病毒攻击操作系统来获得操作系统的访问权限，从而随意地访问电子设备中的私密数据，从而严重威胁到用户的隐私安全。

发明内容

[0003] 本申请的目的之一是提升私密数据在物理内存中的安全性。

[0004] 根据本申请的一个方面，提供了一种访问电子设备的物理内存中私密数据的方法，所述方法包括：

[0005] 接收来自电子设备中运行的进程、访问物理内存中私密数据的请求；

[0006] 通过电子设备的虚拟机监视器中加入的安全内存访问接口来访问物理内存中特定物理地址区间中的私密数据，其中在电子设备的内存管理单元中不建立该特定物理地址区间的映射关系，所述安全内存访问接口被预先设计成实现对物理内存中所述特定物理地址区间中的私密数据的访问。

[0007] 根据本申请的另一个方面，还提供了一种访问电子设备的物理内存中私密数据的装置，所述装置包括：

[0008] 接收单元，被配置为接收来自电子设备中运行的进程、访问物理内存中私密数据的请求；

[0009] 访问单元，被配置为通过电子设备的虚拟机监视器中加入的安全内存访问接口来访问物理内存中特定物理地址区间中的私密数据，其中在电子设备的内存管理单元中不建立该特定物理地址区间的映射关系，所述安全内存访问接口被预先设计成实现对物理内存中所述特定物理地址区间中的私密数据的访问。

[0010] 与现有技术相比，本申请通过在电子设备的虚拟机监视器中加入安全内存访问接口，从而实现对物理内存中私密数据的访问只有通过安全内存访问接口才能进行，而无法通过操作系统正常地访问物理内存中的私密数据，进而防止恶意程序或病毒通过获取操作系统的访问权限来截取物理内存中的私密数据（截取的方式包括 dump 内存（dump 内存可以指将内存中的数据转存到另一个存储装置）、复制内存等），提升私密数据在物理内存中的安全性。

附图说明

[0011] 通过阅读参照以下附图所作的对非限制性实施例所作的详细描述，本申请的其它特征、目的和优点将会变得更明显：

[0012] 图 1 为根据本申请一个优选实施例的访问电子设备的物理内存中私密数据的方法的流程图；

[0013] 图 2 提供了现有技术中基于内存管理单元对电子设备中的物理内存的地址设置映射关系的示意图；

[0014] 图 3 提供了本实施例中对安全物理内存地址空间的私密数据的访问的结构示意图；

[0015] 图 4 为根据本申请另一个优选实施例的访问电子设备的物理内存中私密数据的方法的流程图；

[0016] 图 5 为根据本申请一个优选实施例的访问电子设备的物理内存中私密数据的装置的示意性框图；

[0017] 图 6 为根据本申请一个优选实施例的访问电子设备的物理内存中私密数据的装置的示意性框图；

[0018] 附图中相同或相似的附图标记代表相同或相似的部件。

具体实施方式

[0019] 下面结合附图对本申请作进一步详细描述。

[0020] 在更加详细地讨论示例性实施例之前应当提到的是，一些示例性实施例被描述成作为流程图描绘的处理或方法。虽然流程图将各项操作描述成顺序的处理，但是其中的许多操作可以被并行地、并发地或者同时实施。此外，各项操作的顺序可以被重新安排。当其操作完成时所述处理可以被终止，但是还可以具有未包括在附图中的附加步骤。所述处理可以对应于方法、函数、规程、子例程、子程序等等。

[0021] 在上下文中所称“计算机”，也称为“电脑”，是指可以通过运行预定程序或指令来执行数值计算和 / 或逻辑计算等预定处理过程的智能电子设备，其可以包括处理器与存储器，由处理器执行在存储器中预存的存续指令来执行预定处理过程，或是由 ASIC、FPGA、DSP 等硬件执行预定处理过程，或是由上述二者组合来实现。计算机包括但不限于服务器、个人电脑、笔记本电脑、平板电脑、智能手机等。

[0022] 所述计算机包括用户设备与网络设备。其中，所述用户设备包括但不限于电脑、智能手机、PDA 等；所述网络设备包括但不限于单个网络服务器、多个网络服务器组成的服务器组或基于云计算 (Cloud Computing) 的由大量计算机或网络服务器构成的云，其中，云计算是分布式计算的一种，由一群松散耦合的计算机集组成的一个超级虚拟计算机。其中，所述计算机可单独运行来实现本申请，也可接入网络并通过与网络中的其他计算机的交互操作来实现本申请。其中，所述计算机所处的网络包括但不限于互联网、广域网、城域网、局域网、VPN 网络等。

[0023] 需要说明的是，所述用户设备、网络设备和网络等仅为举例，其他现有的或今后可能出现的计算机或网络如可适用于本申请，也应包含在本申请保护范围以内，并以引用方式包含于此。

[0024] 后面所讨论的方法（其中一些通过流程图示出）可以通过硬件、软件、固件、中间件、微代码、硬件描述语言或者其任意组合来实施。当用软件、固件、中间件或微代码来实施时，用以实施必要任务的程序代码或代码段可以被存储在机器或计算机可读介质（比如存储介质）中。（一个或多个）处理器可以实施必要的任务。

[0025] 这里所公开的具体结构和功能细节仅仅是代表性的，并且是用于描述本申请的示例性实施例的目的。但是本申请可以通过许多替换形式来具体实现，并且不应当被解释成仅仅受限于这里所阐述的实施例。

[0026] 应当理解的是，虽然在这里可能使用了术语“第一”、“第二”等等来描述各个单元，但是这些单元不应当受这些术语限制。使用这些术语仅仅是为了将一个单元与另一个单元进行区分。举例来说，在不背离示例性实施例的范围的情况下，第一单元可以被称为第二单元，并且类似地第二单元可以被称为第一单元。这里所使用的术语“和/或”包括其中一个或更多所列出的相关联项目的任意和所有组合。

[0027] 应当理解的是，当一个单元被称为“连接”或“耦合”到另一单元时，其可以直接连接或耦合到所述另一单元，或者可以存在中间单元。与此相对，当一个单元被称为“直接连接”或“直接耦合”到另一单元时，则不存在中间单元。应当按照类似的方式来解释被用于描述单元之间的关系的其他词语（例如“处于...之间”相比于“直接处于...之间”，“与...邻近”相比于“与...直接邻近”等等）。

[0028] 这里所使用的术语仅仅是为了描述具体实施例而不意图限制示例性实施例。除非上下文明确地另有所指，否则这里所使用的单数形式“一个”、“一项”还意图包括复数。还应当理解的是，这里所使用的术语“包括”和/或“包含”规定所陈述的特征、整数、步骤、操作、单元和/或组件的存在，而不排除存在或添加一个或更多其他特征、整数、步骤、操作、单元、组件和/或其组合。

[0029] 还应当提到的是，在一些替换实现方式中，所提到的功能/动作可以按照不同于附图中标示的顺序发生。举例来说，取决于所涉及的功能/动作，相继示出的两幅图实际上可以基本上同时执行或者有时可以按照相反的顺序来执行。

[0030] 根据本申请的一个实施例，提供了一种访问电子设备的物理内存中私密数据的方法。

[0031] 其中所述访问包括读数据和/或写数据。

[0032] 所述电子设备包括但不限于本地计算机、云端计算机、平板电脑、手机等。

[0033] 所述物理内存可以指电子设备上主板内存槽上的内存条的存储空间。

[0034] 所述私密数据可以指使用电子设备的用户不愿意对外公开的、存储在所述电子设备的物理内存中的信息，如个人照片、视频、银行账户等等，也可以指与电子设备运行安全有关的数据（这些数据即使对电子设备的用户也是不可见的）。本实施例中，所述私密数据包括但不限于存储器上的密文文件解密成的明文、电子设备的程序运行时产生的私密数据、电子设备从外部输入设备（例如通过数据线外连的手机）获取的私密数据（包括视频、音频、照片或/和图片）等。

[0035] 所述访问电子设备的物理内存中私密数据的方法可以在电子设备的内存管理系统中执行。

[0036] 请参考图1，所述访问电子设备的物理内存中私密数据的方法包括：

[0037] S100，接收来自电子设备中运行的进程访问物理内存中私密数据的请求。

[0038] 所述进程通常可以指电子设备（例如计算机）中正在运行的程序实例，例如当运行某一个即时通信应用程序 A 时，则该应用程序在该电子设备上运行的进程可能包括 Aprotect.exe 和 A.exe 两个进程。

[0039] 通常对于在电子设备上运行的每个应用程序的进程而言，每个进程都可以被赋予它自己的私有的物理地址区间，并且通常只可以访问（读或 / 和写）属于自己私有的物理地址区间的数据。

[0040] 所述私密数据如上文所述，包括但不限于存储器上的密文文件解密成的明文、电子设备的程序运行时产生的数据、电子设备从外部获取的数据（包括视频、音频、照片或 / 和图片）等。

[0041] 所述访问物理内存中私密数据的请求包括为私密数据分配该物理内存中的存储区间、将该私密数据写入物理内存的某一存储区间、从物理内存中的某一存储区间读取所述私密数据或 / 和释放为该私密数据预先分配的物理内存中的某一存储区间等请求。

[0042] 可选地，所述 S100 包括：

[0043] - 接收来自电子设备中运行的进程访问物理内存中数据的请求；

[0044] - 判断所述请求要访问的数据是私密数据。

[0045] 其中所述判断可以通过电子设备中的应用程序自动执行来实现，也可以通过响应于用户的操作来实现。

[0046] 例如，所述判断可以通过以下中的至少之一来实现：

[0047] 1) 如果所述请求要访问的数据是将存储器上的密文文件解密成的明文，判断所述请求要访问的数据是私密数据。

[0048] 2) 如果所述请求要访问的数据是电子设备的程序运行时产生的数据，通过判断例程判断出所述请求要访问的数据是私密数据。

[0049] 其中所述判断例程可以预先存储在电子设备的数据库里，当电子设备的程序运行时，该判断例程可以自动判断出程序运行过程中产生的数据是否为私密数据。

[0050] 电子设备的程序运行时产生的数据，有些是不需要私密保护的普通参数，有些是需要私密保护的数据，因此，通过事先编好的例程进行判断属于哪类数据。目前，这种例程对于本领域技术人员来说是已知的。

[0051] 3) 如果所述请求要访问的数据是电子设备从外部获取的数据，向用户提示是否需要将从外部获取的数据作为私密数据存储，响应于用户确认需要将从外部获取的数据作为私密数据存储，判断出所述请求要访问的数据是私密数据。

[0052] 从外部获取的数据，情况比较复杂。有些从外部获取的数据仅是一般性的数据，不需要作为私密数据保护，有的则是一些机密数据，需要作为私密数据保护。而且，这样的数据是无法通过编写例程来判断的，因为从外部获取的数据情况很复杂。因此，往往需要让用户确认该数据是否需要私密保护。

[0053] 例如，当通过数据线将所述电子设备与手机关联，而该电子设备上安装有管理该手机应用的手机应用管理程序 m，进而在所述电子设备上运行该手机应用管理程序 m 的过程中，该手机应用管理程序 m 所包括的在该电子设备上运行的进程要访问从外连的手机获取的数据，则在这种情况下，则可以由该电子设备向用户提示是否需要将从外连的手机获

取的数据作为私密数据存储，如果用户确认需要，则响应于用户确认需要，将从外部获取的数据作为私密数据存储，并判断所述请求要访问的数据是私密数据。

[0054] 请继续参考图 1，所述访问电子设备的物理内存中私密数据的方法包括：

[0055] S110，通过电子设备的虚拟机监视器中加入的安全内存访问接口来访问物理内存中特定物理地址区间中的私密数据，其中在电子设备的内存管理单元中不建立该特定物理地址区间的映射关系，所述安全内存访问接口（API）被预先设计成实现对物理内存中所述特定物理地址区间中的私密数据的访问。

[0056] 其中所述虚拟机监视器（Hypervisor）可以指运行在电子设备（例如计算机）的系统软件，用于维护不同进程之间相对独立的环境，该环境支持不同进程去访问物理内存上存储的相应数据。

[0057] 其中所述安全内存访问接口（API）可以指预先定义的函数或子程序、程序，并被设计成使安全应用程序实现对物理内存中特定物理地址区间中的私密数据的访问。

[0058] 其中所述安全应用程序可以指基于该安全内存访问接口所开发的应用程序，例如，将该安全内存访问接口提供给某通讯软件应用程序的开发者，该开发者基于该安全内存访问接口将该通讯软件应用程序中的一段代码 A 替换成另一段代码 B，进而使该通信软件应用程序转变为安全的通信软件应用程序，从而该安全的通信软件应用程序可以基于所述安全内存访问接口（API）实现对物理内存中特定物理地址区间中的私密数据的访问。

[0059] 为了安全起见，该安全内存访问接口（API）由所述电子设备的厂商定制，从而针对每台电子设备而言，从设备级的维度来提升电子设备的物理内存中私密数据的安全。

[0060] 所述物理内存中特定物理地址区间可以指在物理内存中预留的一段连续的安全物理内存地址区间，该安全物理内存地址区间不在电子设备的内存管理单元中设置映射关系。

[0061] 对于所述映射关系的理解可以参考图 2，图 2 提供了现有技术中基于内存管理单元对电子设备中的物理内存的地址设置映射关系的示意图。

[0062] 在现有技术中，以电子设备为计算机举例，由于计算机的物理内存有限，现有技术往往采用虚拟内存技术（诸如虚拟内存分页管理技术、虚拟内存段页式存储管理等）来缓解内存的紧张。在采用虚拟内存技术的情况下，通过内存管理单元（为了区别于下文中的虚拟内存管理单元，在此也可以称为真实内存管理单元）设置物理内存中的地址与虚拟计算机的伪物理地址之间的映射关系，并设置所述伪物理地址与进程被赋予的虚拟地址的映射关系，由此，计算机操作系统则可以利用地址的映射关系对物理内存进行访问。

[0063] 更具体地，参考图 2 而言，在应用虚拟内存技术对计算机物理内存进行管理的过程中，往往为每个进程分配属于它自己的虚拟地址空间，并且通过建立在计算机基础上的虚拟计算机操作系统的虚拟内存管理单元（虚拟 MMU）将该虚拟地址空间与虚拟计算机上的伪物理地址映射，以及通过虚拟机监视器（Hypervisor）将该伪物理地址与物理内存中的物理内存地址映射。实际上，无论是从虚拟地址映射到伪物理地址，还是从伪物理地址映射到物理内存地址，都可以看作是由计算机的真实内存管理单元来统一设置的，只是该统一设置是基于真实内存管理单元对虚拟内存管理单元（虚拟 MMU）和虚拟机监视器（Hypervisor）的管理来实现的。

[0064] 如上文所述，对于设置了映射关系的物理内存，计算机操作系统则可以利用地址

的映射关系对物理内存进行访问，因而黑客可以利用恶意程序攻击计算机操作系统来获取计算机操作系统的操作权限而随意地访问电子设备中的私密数据，从而严重威胁到用户的隐私安全。

[0065] 为了解决上述问题，提升私密数据在物理内存的安全性，请参考图 3，本实施例中，在电子设备的内存管理单元中不建立所述特定物理地址区间的映射关系，而是通过在虚拟机监视器中加入的安全内存访问接口来访问特定物理地址区间（即安全物理内存地址空间）的私密数据，也即对于私密数据的访问而言，在虚拟内存管理单元（虚拟 MMU）中不为该私密数据的访问建立虚拟地址与伪物理地址之间的映射关系，而是由虚拟内存管理单元基于安全内存访问接口来访问安全物理内存地址空间中的私密数据。

[0066] 由于本实施例中的该安全内存访问接口（API）由所述电子设备的厂商定制，只会提供给该厂商认证过的安全程序的开发者，因而该安全内存访问接口（API）通常不会被恶意程序的开发者获取，进而恶意程序在未通过该安全内存访问接口访问电子设备的物理内存的情况下，无法通过攻击计算机操作系统利用地址映射关系对物理内存中的私密数据进行访问，提升了私密数据在物理内存的安全性。

[0067] 对于图 3，需要说明的是，虽然没有在图 3 中示出如图 2 所示的伪物理地址，但是这只是为了更清楚地描述对安全物理内存地址空间中的私密数据进行访问的结构，并不表示对计算机物理内存中除安全物理内存地址空间以外的数据的访问就不可以参考图 2 所示的虚拟内存技术来管理。

[0068] 可选地，所述 S110 包括：

[0069] - 通过该安全内存访问接口为要访问的私密数据分配对应的位于所述特定物理地址区间中的物理地址子区间。

[0070] 例如，所述特定物理地址区间大于 1GB（起始地址例如为 0x80000000），则为该私密数据分配位于所述特定物理地址区间中的物理地址子区间为 1GB（起始地址例如为 0x80000000，结束地址为 0xBFFFFFFF）

[0071] - 在所述物理地址子区间中执行对所述私密数据的访问。

[0072] 例如，将所述私密数据写入所述分配的物理地址子区间中。

[0073] 可选地，所述访问电子设备的物理内存中私密数据的方法还包括：

[0074] - 响应于预定条件，释放所述特定物理地址区间中的私密数据对应的物理地址子区间。

[0075] 其中，所述预定条件可以指需要访问该私密数据的进程的运行终止。当一个进程运行终止时，为了提升物理内存的利用率，可以将该进程的私密数据之前所占有的物理地址子区间释放。

[0076] 可选地，请参考图 4，所述访问电子设备的物理内存中私密数据的方法还包括：

[0077] S120，提示用户输入用于访问私密数据的认证信息；以及

[0078] S130，对用户输入的认证信息进行鉴权，其中只有在鉴权通过的前提下才执行通过电子设备的虚拟机监视器中加入的安全内存访问接口来访问物理内存中特定物理地址区间中的私密数据的步骤。

[0079] 其中，所述用户输入用于访问私密数据的认证信息的方式包括但不限于用户输入个人身份认证信息（诸如登录账户和密码、头像认证等）、运行安全应用程序等。

[0080] 以用户输入的个人身份认证信息为例，所述鉴权可以指对该个人身份认证信息进行验证，判断是否为用户本人的信息；以运行安全应用程序为例，所述鉴权可以指判断所述安全应用程序是否为提供安全内存访问接口的厂商认证的安全应用程序。

[0081] 根据本发明的一个实施例，提供了一种访问电子设备的物理内存中私密数据的装置，所述访问电子设备的物理内存中私密数据的装置可以实现为电子设备上管理物理内存的完全软件，也可以实现为电子设备上管理物理内存的软件或硬件的结合。

[0082] 请参考图 5，所述访问电子设备的物理内存中私密数据的装置包括：

[0083] 接收单元 200，被配置为接收来自电子设备中运行的进程、访问物理内存中私密数据的请求。

[0084] 访问单元 210，被配置为通过电子设备的虚拟机监视器中加入的安全内存访问接口来访问物理内存中特定物理地址区间中的私密数据，其中在电子设备的内存管理单元中不建立该特定物理地址区间的映射关系，所述安全内存访问接口被预先设计成实现对物理内存中所述特定物理地址区间中的私密数据的访问。

[0085] 可选地，所述访问包括读和 / 或写。

[0086] 可选地，所述接收单元 200 被配置为：

[0087] - 接收来自电子设备中运行的进程、访问物理内存中数据的请求；

[0088] - 判断所述请求要访问的数据是私密数据。

[0089] 可选地，所述接收单元 200 判断所述请求要访问的数据是私密数据的过程包括：

[0090] - 如果所述请求要访问的数据是将存储器上的密文文件解密成的明文，判断所述请求要访问的数据是私密数据。

[0091] 可选地，所述接收单元 200 判断所述请求要访问的数据是私密数据的过程包括：

[0092] - 如果所述请求要访问的数据是电子设备的程序运行时产生的数据，通过判断例程判断出所述请求要访问的数据是私密数据。

[0093] 可选地，所述接收单元 200 判断所述请求要访问的数据是私密数据的过程包括：

[0094] - 如果所述请求要访问的数据是电子设备从外部获取的数据，向用户提示是否需要将从外部获取的数据作为私密数据存储；

[0095] - 响应于用户确认需要将从外部获取的数据作为私密数据存储，判断出所述请求要访问的数据是私密数据。

[0096] 可选地，所述访问单元 210 被配置为：

[0097] - 通过该安全内存访问接口为要访问的私密数据分配对应的位于所述特定物理地址区间中的物理地址子区间；

[0098] - 在所述物理地址子区间中执行对所述私密数据的访问。

[0099] 可选地，所述访问单元 210 被配置为：

[0100] - 响应于预定条件，释放所述特定物理地址区间中的私密数据对应的物理地址子区间。

[0101] 可选地，请参考图 6，所述访问电子设备的物理内存中私密数据的装置还包括：

[0102] 提示单元 220，被配置为提示用户输入用于访问私密数据的认证信息；

[0103] 鉴权单元 230，被配置为对用户输入的认证信息进行鉴权，

[0104] 其中所述访问单元 210 被配置为只有在鉴权通过的前提下才通过电子设备的虚

拟机监视器中加入的安全内存访问接口来访问物理内存中特定物理地址区间中的私密数据。

[0105] 应当理解，图5和图6所述的结构框图仅仅是为了示例的目的，而不是对本申请范围的限制。在某些情况下，可以根据具体情况增加或减少某些单元。

[0106] 所属技术领域的技术人员知道，本申请可以实现为系统、方法或计算机程序产品。本领域技术人员应能理解，上述各单元仅为示例，在实践中，它们可以是分别独立的单元，或者任意两个单元集成在一个单元中，也可全部集成在一个单元中。

[0107] 附图中的流程图和框图显示了根据本申请的多个实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段或代码的一部分，所述模块、程序段或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个连续的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合，可以用执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0108] 对于本领域技术人员而言，显然本申请不限于上述示范性实施例的细节，而且在不背离本申请的精神或基本特征的情况下，能够以其他的具体形式实现本申请。因此，无论从哪一点来看，均应将实施例看作是示范性的，而且是非限制性的，本申请的范围由所附权利要求而不是上述说明限定，因此旨在将落在权利要求的等同要件的含义和范围内的所有变化囊括在本申请内。不应将权利要求中的任何附图标记视为限制所涉及的权利要求。

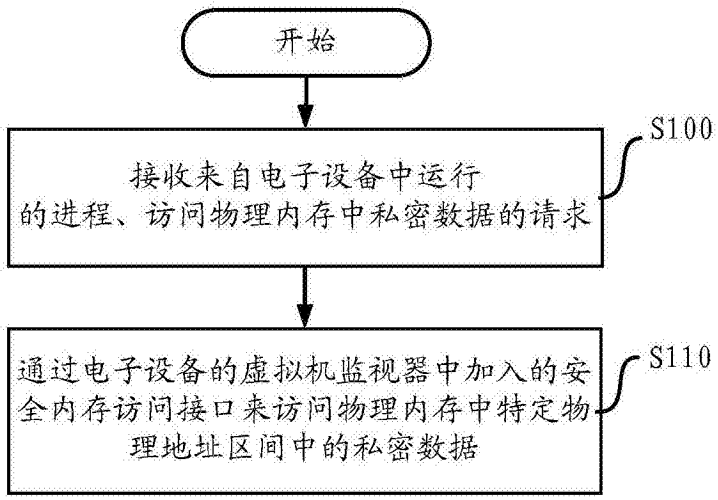

开始
接收来自电子设备中运行的进程、访问物理内存中私密数据的请求
S100
通过电子设备的虚拟机监视器中加入的安全内存访问接口来访问物理内存中特定物理地址区间中的私密数据
S110

图 1

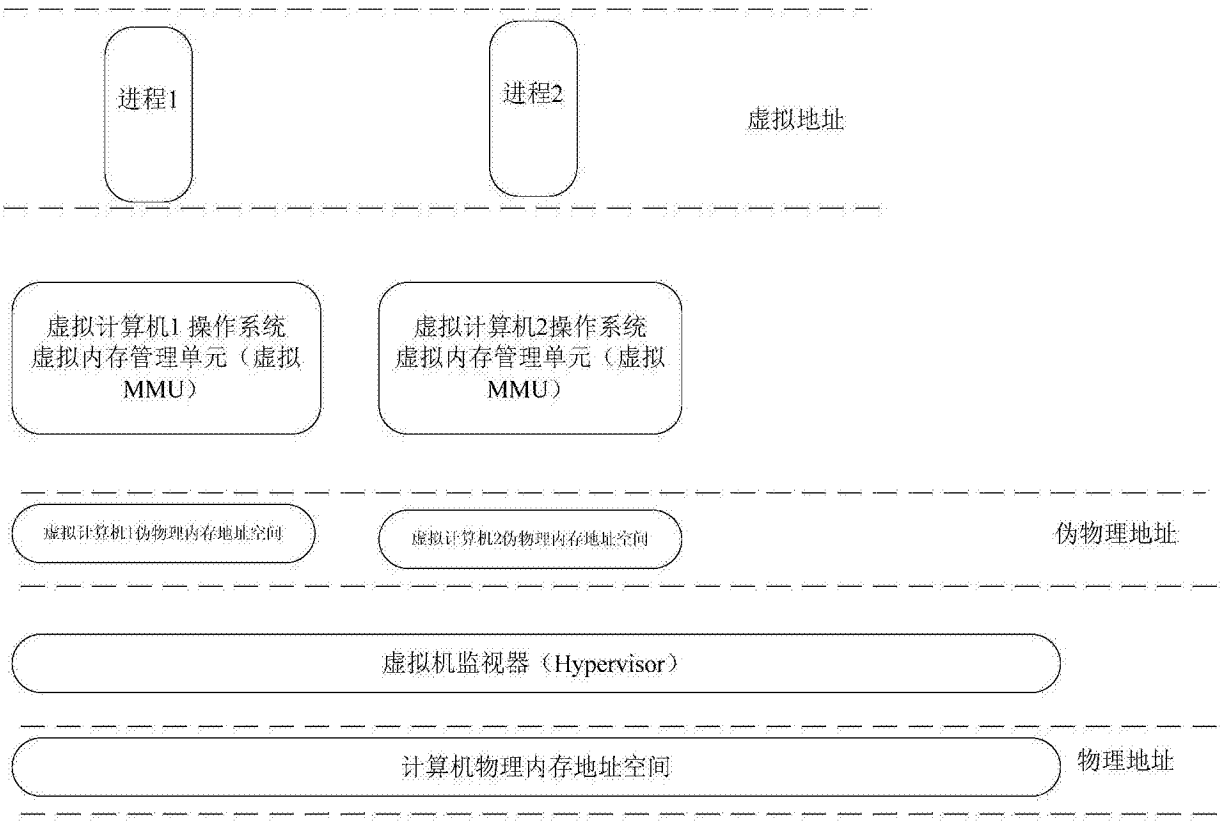

进程1
进程2
虚拟地址
虚拟计算机1 操作系统 虚拟内存管理单元（虚拟MMU）
虚拟计算机2操作系统 虚拟内存管理单元（虚拟MMU）
虚拟计算机1伪物理内存地址空间
虚拟计算机2伪物理内存地址空间
伪物理地址
虚拟机监视器（Hypervisor）
计算机物理内存地址空间
物理地址

图 2

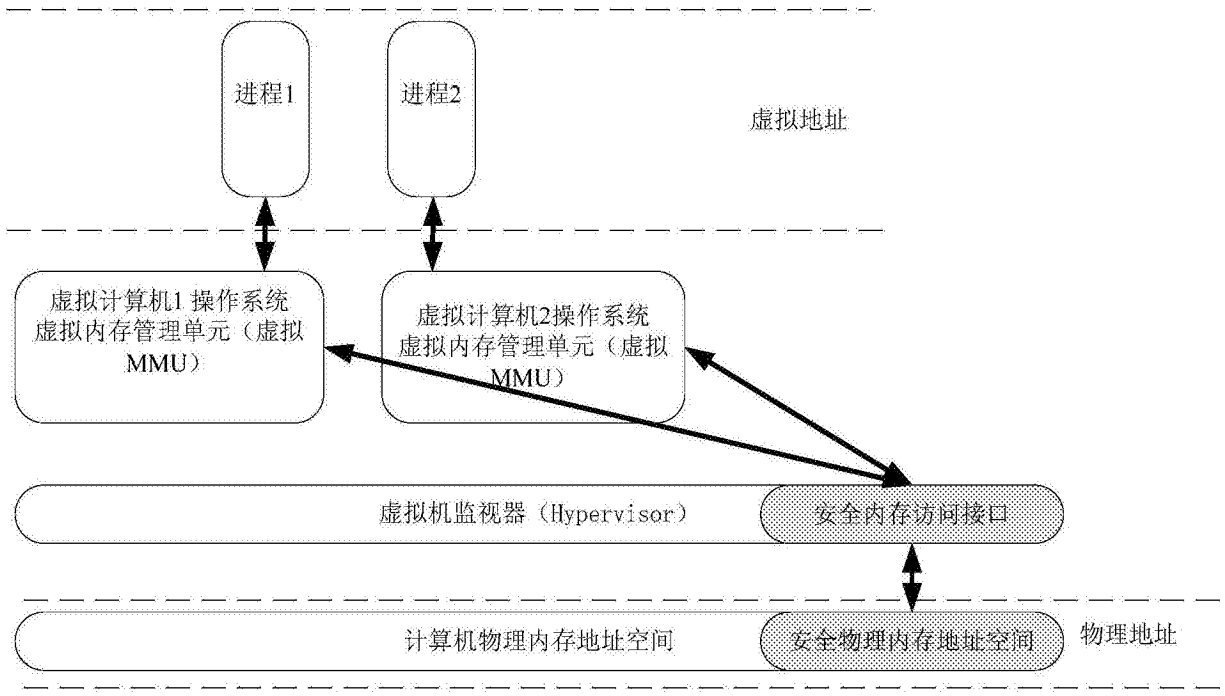

进程1
进程2
虚拟地址
虚拟计算机1 操作系统
虚拟内存管理单元（虚拟MMU）
虚拟计算机2操作系统
虚拟内存管理单元（虚拟MMU）
虚拟机监视器（Hypervisor）
安全内存访问接口
计算机物理内存地址空间
安全物理内存地址空间
物理地址

图 3

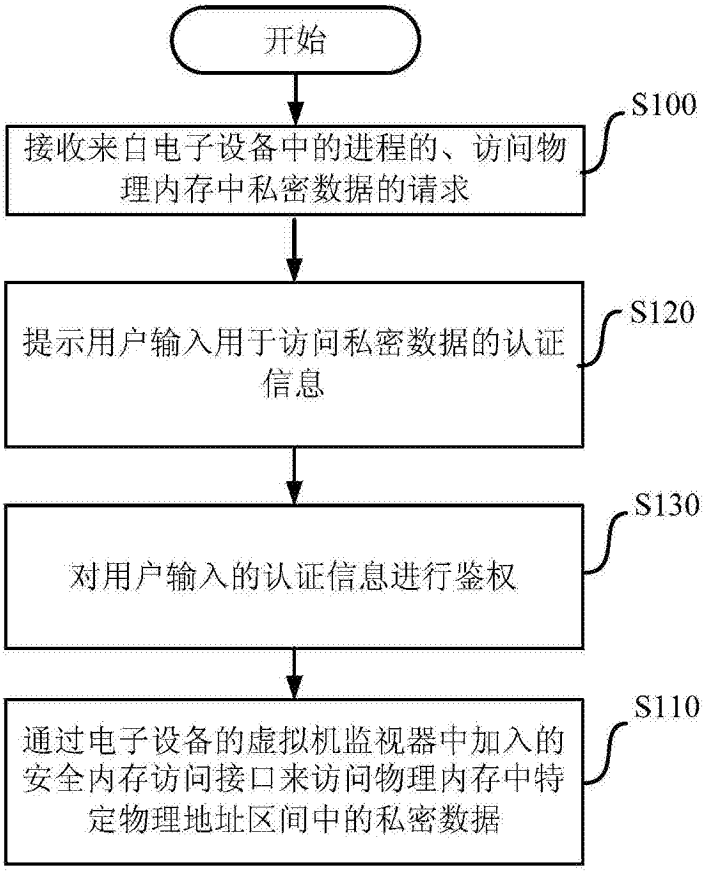

开始
S100
接收来自电子设备中的进程的、访问物理内存中私密数据的请求
S120
提示用户输入用于访问私密数据的认证信息
S130
对用户输入的认证信息进行鉴权
S110
通过电子设备的虚拟机监视器中加入的安全内存访问接口来访问物理内存中特定物理地址区间中的私密数据

图 4

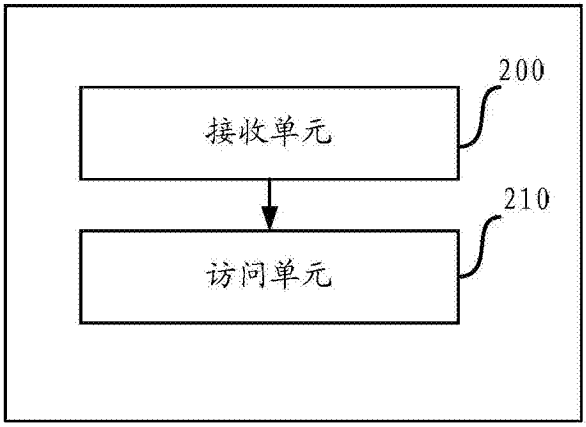


图 5

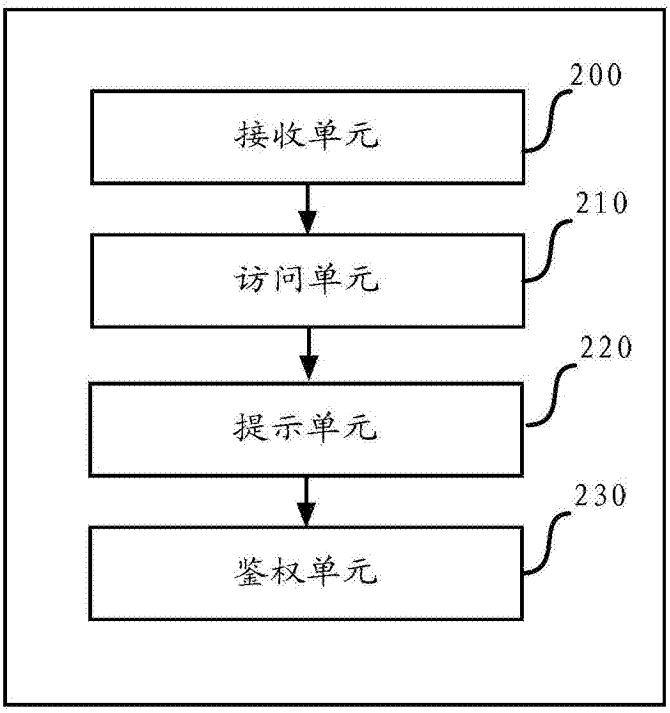


图 6