(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 109190401 A
(43)申请公布日 2019.01.11

(21)申请号 201811068657.6

(22)申请日 2018.09.13

(71)申请人 郑州云海信息技术有限公司
地址 450018 河南省郑州市郑东新区心怡路278号16层1601室

(72)发明人 许鑫

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 罗满

(51)Int.Cl.
G06F 21/60(2013.01)
G06F 21/62(2013.01)

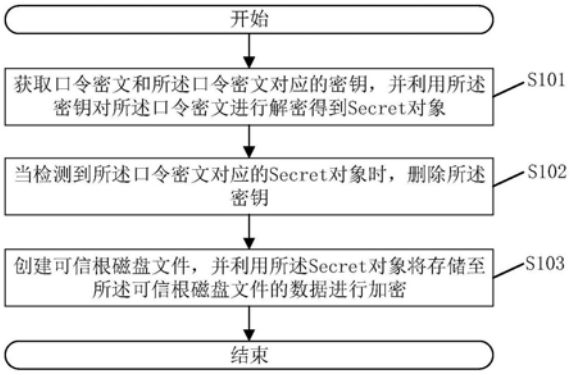
权利要求书2页 说明书8页 附图2页

(54)发明名称

一种Qemu虚拟可信根的数据存储方法、装置及相关组件

(57)摘要

本申请公开了一种Qemu虚拟可信根的数据存储方法，所述数据存方法包括获取口令密文和所述口令密文对应的密钥，并利用所述密钥对所述口令密文进行解密得到Secret对象；当检测到所述口令密文对应的Secret对象时，删除所述密钥；创建可信根磁盘文件，并利用所述Secret对象将存储至所述可信根磁盘文件的数据进行加密。本方法能够防止文件被窃取导致用户数据泄露，提高Qemu虚拟可信根的数据安全性。本申请还公开了一种Qemu虚拟可信根的数据存储系统、一种计算机可读存储介质及一种电子设备，具有以上有益效果。



CN 109190401 A

1.一种Qemu虚拟可信根的数据存储方法,其特征在于,包括:

获取口令密文和所述口令密文对应的密钥,并利用所述密钥对所述口令密文进行解密得到Secret对象;

当检测到所述口令密文对应的Secret对象时,删除所述密钥;

创建可信根磁盘文件,并利用所述Secret对象将存储至所述可信根磁盘文件的数据进行加密。

2.根据权利要求1所述数据存储方法,其特征在于,在获取口令密文和所述口令密文对应的密钥之前,还包括:

向口令管理模块发送口令生成请求,以便所述口令管理模块生成口令密文和密钥;

其中,所述口令密文由口令管理模块利用所述密钥对目标口令进行加密得到,所述目标密文和所述密钥均由所述口令管理模块利用随机数生成器得到,所述目标密文存储在所述口令管理模块的数据库中。

3.根据权利要求1所述数据存储方法,其特征在于,在删除所述密钥之后,还包括:

删除所述口令密文。

4.根据权利要求1所述数据存储方法,其特征在于,还包括:

当接收到虚拟可信根启动指令时,获取所述可信根磁盘文件的完整性信息;

判断所述完整性信息是否与预设值相同;若是,则启动虚拟可信根。

5.根据权利要求4所述数据存储方法,其特征在于,获取所述可信根磁盘文件的完整性信息包括:

获取启动口令密文和所述启动口令密文对应的启动密钥,并利用所述启动密钥对所述启动口令密文进行解密得到解密Secret对象;

当检测到所述启动口令密文对应的解密Secret对象时,删除所述启动密钥;

利用所述解密Secret对象对所述可信根磁盘文件进行解密得到磁盘数据和所述完整性信息,并计算所述磁盘数据的摘要值;

相应的,判断所述完整性信息是否与预设值相同包括:

判断所述完整性信息是否与所述摘要值相同。

6.根据权利要求1所述数据存储方法,其特征在于,利用所述Secret对象将存储至所述可信根磁盘文件的数据进行加密包括:

将所述虚拟可信根运行时的状态信息的摘要值作为完整性信息,并将所述完整性信息和所述状态信息设置为待写入数据;

利用所述Secret对象对所述待写入数据进行加密,并将所述待写入数据存储至所述可信根磁盘文件。

7.一种Qemu虚拟可信根的数据存储装置,其特征在于,包括:

数据机密模块,用于获取口令密文和所述口令密文对应的密钥,并利用所述密钥对所述口令密文进行解密得到Secret对象;当检测到所述口令密文对应的Secret对象时,删除所述密钥;

数据存储模块,用于创建可信根磁盘文件,并利用所述Secret对象将存储至所述可信根磁盘文件的数据进行加密。

8.一种虚拟化平台,其特征在于,包括如权利要求7所述的Qemu虚拟可信根的数据存储

装置和口令管理模块；

其中，口令管理模块用于当接收到所述Qemu虚拟可信根的数据存储装置发送的口令生成请求时，通过随机数生成器生成目标口令和密钥并将所述目标口令存储至数据库中，利用所述密钥加密所述目标口令得到口令密文，并将所述口令密文和所述密钥发送至所述Qemu虚拟可信根的数据存储装置。

9.一种电子设备，其特征在于，包括：

存储器，用于存储计算机程序；

处理器，用于执行所述计算机程序时实现如权利要求1至6任一项所述Qemu虚拟可信根的数据存储方法的步骤。

10.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现如权利要求1至6任一项所述Qemu虚拟可信根的数据存储方法的步骤。

一种Qemu虚拟可信根的数据存储方法、装置及相关组件

技术领域

[0001] 本发明涉及信息安全技术领域，特别涉及一种Qemu虚拟可信根的数据存储方法、Qemu虚拟可信根的数据存储装置、虚拟化平台、一种计算机可读存储介质及一种电子设备。

背景技术

[0002] 当前，信息安全已成为云计算应用与发展重要一环，密码学技术是解决云数据中心数据机密性的核心技术手段。当前，基于Qemu密码学功能的虚拟机可信根技术已经逐渐成熟。

[0003] 物理可信根的持久性数据存放在物理芯片中，因物理芯片的特性，外部很难获取芯片内部的数据，因此可以保证物理可信根数据不被破坏或窃取，而现有技术中的Qemu虚拟可信根中的持久性数据要存放在系统上层的文件中，且多数虚拟可信实现方案中该数据是以明文的形式存放，一旦虚拟可信根运行的系统被攻击，该系统上的虚拟可信根数据就面临被窃取或破坏的风险，直接威胁到虚拟机用户的数据隐秘性。

[0004] 因此，如何防止文件被窃取导致用户数据泄露，提高Qemu虚拟可信根的数据安全性是本领域技术人员目前需要解决的技术问题。

发明内容

[0005] 本申请的目的是提供一种Qemu虚拟可信根的数据存储方法、Qemu虚拟可信根的数据存储装置、虚拟化平台、一种计算机可读存储介质及一种电子设备，能够防止文件被窃取导致用户数据泄露，提高Qemu虚拟可信根的数据安全性。

[0006] 为解决上述技术问题，本申请提供一种Qemu虚拟可信根的数据存储方法，该数据存储方法包括：

[0007] 获取口令密文和所述口令密文对应的密钥，并利用所述密钥对所述口令密文进行解密得到Secret对象；

[0008] 当检测到所述口令密文对应的Secret对象时，删除所述密钥；

[0009] 创建可信根磁盘文件，并利用所述Secret对象将存储至所述可信根磁盘文件的数据进行加密。

[0010] 可选的，在获取口令密文和所述口令密文对应的密钥之前，还包括：

[0011] 向口令管理模块发送口令生成请求，以便所述口令管理模块生成口令密文和密钥；

[0012] 其中，所述口令密文由口令管理模块利用所述密钥对目标口令进行加密得到，所述目标密文和所述密钥均由所述口令管理模块利用随机数生成器得到，所述目标密文存储在所述口令管理模块的数据库中。

[0013] 可选的，在删除所述密钥之后，还包括：

[0014] 删除所述口令密文。

[0015] 可选的，还包括：

[0016] 当接收到虚拟可信根启动指令时，获取所述可信根磁盘文件的完整性信息；

[0017] 判断所述完整性信息是否与预设值相同；若是，则启动虚拟可信根。

[0018] 可选的，获取所述可信根磁盘文件的完整性信息包括：

[0019] 获取启动口令密文和所述启动口令密文对应的启动密钥，并利用所述启动密钥对所述启动口令密文进行解密得到解密Secret对象；

[0020] 当检测到所述启动口令密文对应的解密Secret对象时，删除所述启动密钥；

[0021] 利用所述解密Secret对象对所述可信根磁盘文件进行解密得到磁盘数据和所述完整性信息，并计算所述磁盘数据的摘要值；

[0022] 相应的，判断所述完整性信息是否与预设值相同包括：

[0023] 判断所述完整性信息是否与所述摘要值相同。

[0024] 可选的，利用所述Secret对象将存储至所述可信根磁盘文件的数据进行加密包括：

[0025] 将所述虚拟可信根运行时的状态信息的摘要值作为完整性信息，并将所述完整性信息和所述状态信息设置为待写入数据；

[0026] 利用所述Secret对象对所述待写入数据进行加密，并将所述待写入数据存储至所述可信根磁盘文件。

[0027] 本申请还提供了一种Qemu虚拟可信根的数据存储装置，该装置包括：

[0028] 数据机密模块，用于获取口令密文和所述口令密文对应的密钥，并利用所述密钥对所述口令密文进行解密得到Secret对象；当检测到所述口令密文对应的Secret对象时，删除所述密钥；

[0029] 数据存储模块，用于创建可信根磁盘文件，并利用所述Secret对象将存储至所述可信根磁盘文件的数据进行加密。

[0030] 本申请还提供了一种虚拟化平台，该虚拟化平台包括如上述Qemu虚拟可信根的数据存储装置和口令管理模块；

[0031] 其中，口令管理模块用于当接收到所述Qemu虚拟可信根的数据存储装置发送的口令生成请求时，通过随机数生成器生成目标口令和密钥并将所述目标口令存储至数据库中，利用所述密钥加密所述目标口令得到口令密文，并将所述口令密文和所述密钥发送至所述Qemu虚拟可信根的数据存储装置。

[0032] 本申请还提供了一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序执行时实现上述Qemu虚拟可信根的数据存储方法执行的步骤。

[0033] 本申请还提供了一种电子设备，包括存储器和处理器，所述存储器中存储有计算机程序，所述处理器调用所述存储器中的计算机程序时实现上述Qemu虚拟可信根的数据存储方法执行的步骤。

[0034] 本发明提供了一种Qemu虚拟可信根的数据存储方法，包括获取口令密文和所述口令密文对应的密钥，并利用所述密钥对所述口令密文进行解密得到Secret对象；当检测到所述口令密文对应的Secret对象时，删除所述密钥；创建可信根磁盘文件，并利用所述Secret对象将存储至所述可信根磁盘文件的数据进行加密。

[0035] 本申请通过利用密钥对口令密文进行解密得到Secret对象，该Secret对象为Qemu与形式保存密钥、口令的数据结构，可供Qemu的组件和虚拟设备运行时使用，因此利用该

Secret对象对存储至所述可信根磁盘文件的数据进行加密可以保证数据的安全性。进一步的，由于本申请在检测到所述口令密文对应的Secret对象后将密钥删除，能够保证即使虚拟可信根运行的系统被攻击，其他人也无法获取口令密文对应的口令原文，避免其他人通过非法途径获取虚拟可信根的数据。本申请可以防止文件被窃取导致用户数据泄露，提高Qemu虚拟可信根的数据安全性。本申请同时还提供了一种Qemu虚拟可信根的数据存储装置、一种虚拟化平台、一种计算机可读存储介质及一种电子设备，具有上述有益效果，在此不再赘述。

附图说明

[0036] 为了更清楚地说明本申请实施例，下面将对实施例中所需要使用的附图做简单的介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，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。

[0037] 图1为本申请实施例所提供的一种Qemu虚拟可信根的数据存储方法的流程图；

[0038] 图2为本申请实施例所提供的另一种Qemu虚拟可信根的数据存储方法的流程图；

[0039] 图3为Qemu+KVM虚拟化平台的结构示意图；

[0040] 图4为本申请实施例所提供的一种Qemu虚拟可信根的启动方法的流程图；

[0041] 图5为本申请实施例所提供的一种Qemu虚拟可信根的数据存储装置的结构示意图。

具体实施方式

[0042] 为使本申请实施例的目的、技术方案和优点更加清楚，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，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。

[0043] 下面请参见图1，图1为本申请实施例所提供的一种Qemu虚拟可信根的数据存储方法的流程图。

[0044] 具体步骤可以包括：

[0045] S101：获取口令密文和所述口令密文对应的密钥，并利用所述密钥对所述口令密文进行解密得到Secret对象；

[0046] 其中，Qemu(Quick Emulator)为一款开源的模拟器及虚拟机监管器，Qemu虚拟可信根为在虚拟化层面为虚拟机提供可信根服务的模块，虚拟可信根所能够实现的功能与物理可信根相同，本实施例的技术方案就是基于Qemu实现的。

[0047] 本步骤默认存在Qemu所在系统的口令管理模块生成口令密文和该口令密文对应的密钥的操作，具体的，口令管理模块通过随机数生成器生成口令，并将该口令存放到数据库中，口令管理模块还通过随机数生成器生成密钥，使用该密钥加密已生成的口令，并导出口令密文与对应的密钥。需要说明的是，生成口令密文和密钥的口令管理模块与Qemu均为同一虚拟化系统中的模块，Qemu可以与口令管理模块进行信息交互，如口令密文即密钥的请求与发放等。

[0048] Secret对象为Qemu运行时保存密钥、口令或是其他敏感数据的数据结构，可供

Qemu其他组件或虚拟设备运行时使用。利用所述密钥对所述口令密文进行解密可以得到Secret对象，Secret对象是口令在Qemu中存在的形态，即在Qemu中Secret对象就相当于口令。

[0049] S102：当检测到所述口令密文对应的Secret对象时，删除所述密钥；

[0050] 其中，本步骤默认存在检测是否生成口令密文对应的Secret对象的操作，而该检测操作可以在S103之后存在，因此S102与S103的执行顺序可以调换，也可以同时进行，此处作为一种优选的实施方案，当执行完S101后立即执行默认存在检测是否生成口令密文对应的Secret对象的操作，以便尽快删除密钥。

[0051] 由于Qemu虚拟可信根中的持久性数据要存放在系统上层的文件中，且多数虚拟可信根的数据是以明文的形式存放，一旦虚拟可信根运行的系统被攻击，那么该系统上的虚拟可信根数据就面临被窃取或破坏的风险，直接威胁到虚拟机用户的数据隐秘性。若在生成Secret对象之后，不将密钥删除，将会存在不法分子攻击虚拟可信根运行的系统获取Secret对象和密钥，进而获得明文状态的口令。在生成Secret对象之后，立即删除密钥能够避免因系统被攻击而带来的口令泄露的问题。

[0052] 需要说明的是，在某些应用场景下操作系统管理员会禁止文件的删除操作，因此可以在删除密钥文件前先将原密钥内容进行覆盖，保证在无法删除密钥文件的情况下密钥也不会泄露，进一步提升了Qemu虚拟可信根的安全性。

[0053] 作为一种优选的实施方式，可以在删除密钥之后将口令密文也删除，使得Qemu中只有Secret对象中记载有与口令相关的信息，而由于Secret对象的特性，不法分子无法通过攻击系统从Secret对象中获取明文形态的口令，即无法从Secret对象中获取口令的实际内容。

[0054] S103：创建可信根磁盘文件，并利用所述Secret对象将存储至所述可信根磁盘文件的数据进行加密。

[0055] 其中，本步骤中创建的可信根磁盘文件为用于存储Qemu虚拟可信根的数据的文件，每当有数据要存储至可信根磁盘文件时都会利用Secret对象进行加密，即本步骤将Secret对象设置为可信根磁盘文件的访问口令，，只有提供正确的口令才能够访问可信根磁盘文件中的内容。

[0056] 本实施例通过利用密钥对口令密文进行解密得到Secret对象，该Secret对象为Qemu与形式保存密钥、口令的数据结构，可供Qemu的组件和虚拟设备运行时使用，因此利用该Secret对象对存储至所述可信根磁盘文件的数据进行加密可以保证数据的安全性。进一步的，由于本实施例在检测到所述口令密文对应的Secret对象后将密钥删除，能够保证即使虚拟可信根运行的系统被攻击，其他人也无法获取口令密文对应的口令原文，避免其他人通过非法途径获取虚拟可信根的数据。本实施例可以防止文件被窃取导致用户数据泄露，提高Qemu虚拟可信根的数据安全性。

[0057] 下面请参见图2，图2为本申请实施例所提供的另一种Qemu虚拟可信根的数据存储方法的流程图；

[0058] 具体步骤可以包括：

[0059] S201：向口令管理模块发送口令生成请求，以便所述口令管理模块生成口令密文和密钥；

[0060] 其中,所述口令密文由口令管理模块利用所述密钥对目标口令进行加密得到,所述目标密文和所述密钥均由所述口令管理模块利用随机数生成器得到,所述目标密文存储在所述口令管理模块的数据库中。

[0061] S202:获取口令密文和所述口令密文对应的密钥,并利用所述密钥对所述口令密文进行解密得到Secret对象;

[0062] S203:当检测到所述口令密文对应的Secret对象时,删除所述密钥和所述口令密文。

[0063] S204:创建可信根磁盘文件,将所述虚拟可信根运行时的状态信息和所述状态信息的摘要值作为待写入数据;

[0064] S205:利用所述Secret对象对所述待写入数据进行加密,并将所述待写入数据存储至所述可信根磁盘文件。

[0065] 图2对应的Qemu虚拟可信根的数据存储方法可以应用于虚拟化平台的Qemu虚拟可信根初始化操作。实际应用中的虚拟可信根初始化包括文件创建、口令创建的操作,口令的明文存放在口令管理模块的数据库中保存,而每次导出口令时需要生成密钥来加密该口令,同时生成该密钥的文件。口令一旦创建,则不再改变,而每次导出口令时的密钥则是随机创建。Qemu虚拟可信根初始化操作可以包括以下步骤:

[0066] 1)生成口令:口令管理模块通过随机数生成器生成口令,并将该口令存放到数据库中。口令管理模块通过随机数生成器生成密钥,使用该密钥加密已生成的口令,并导出密文与对应的密钥;

[0067] 2)Qemu Secret管理模块恢复口令:Qemu Secret管理模块读取口令密文及密钥文件,使用密钥恢复口令,并生成Qemu运行时的Secret对象供Qemu其他模块使用。为保证口令的安全,一旦读取完密钥文件后就立即删除该文件,保证即便获取了Qemu启动参数也无法获取密钥内容。

[0068] 3)Qemu LUKS模块创建虚拟可信根磁盘文件:Qemu LUKS模块为虚拟可信根创建磁盘文件,并使用步骤2)中已生成的Secret对象的口令作为该文件的访问口令加密文件内容,即只要能提供正确的口令即可访问该文件。

[0069] 需要说明的是Qemu Secret管理模块和Qemu LUKS模块均为Qemu中的模块,Qemu中还包括Qemu虚拟可信根,虚拟化平台的具体结构可以参见图3,图3为Qemu+KVM虚拟化平台的结构示意图。图3中的LUKS模块就是Qemu LUKS模块,Secret对象管理模块就是Qemu Secret管理模块。

[0070] 下面请参见图4,图4为本申请实施例所提供的一种Qemu虚拟可信根的启动方法的流程图;

[0071] S301:当接收到虚拟可信根启动指令时,获取所述可信根磁盘文件的完整性信息;

[0072] 本实施例中的完整性信息为以数据的摘要值(如Hash)作为其完整性信息,常用的有SHA-1、SHA256、SM3等算法。只有在可信根磁盘文件的完整性信息符合预设值时,才能够正常启动Qemu虚拟可信根。

[0073] 具体的,获取完整性信息的具体操作可以包括以下步骤:

[0074] 步骤1:获取启动口令密文和所述启动口令密文对应的启动密钥,并利用所述启动密钥对所述启动口令密文进行解密得到解密Secret对象;

[0075] 需要说明的是，此处获取的启动口令密文及启动密钥与图1对应的实施例中提到的口令密文和启动密钥并不相同，但是通过启动密钥对启动口令密文解密得到的口令与通过密钥对口令密文进行解密得到的口令是相同的。因此，此处得到的解密Secret对象可以作为访问图1对应的实施例中提到的可信根磁盘文件的访问口令。

[0076] 步骤2：当检测到所述启动口令密文对应的解密Secret对象时，删除所述启动密钥；

[0077] 此处同样是出于安全性的考虑，需要及时删除启动密钥，作为一种优选的实施方式，还可以将启动口令密文删除，以免口令以明文的形式被窃取。

[0078] 步骤3：利用所述解密Secret对象对所述可信根磁盘文件进行解密得到磁盘数据和所述完整性信息，并计算所述磁盘数据的摘要值；

[0079] 需要说明的是，本实施例默认存在将虚拟可信根运行时的状态信息的摘要值作为完整性信息，将该完整性信息和状态信息作为待写入数据存储至可信根磁盘文件。将本步骤中计算的磁盘数据的摘要值与原来存在可信根磁盘文件的完整性信息进行比较则可以确定的完整性信息符合预设值时。举例说明上述过程，例如可信根运行时的状态信息A1的摘要值为a1，将摘要值a1作为完整性信息和状态信息存储至可信根磁盘文件，当接收到虚拟可信根启动指令时，利用解密Secret对象进行解密得到数据A2和完整性信息，获取数据A2的摘要值a2，若a1等于a2则说明可信根磁盘文件中的数据完整没有被破坏可以启动Qemu虚拟可信根；若a1不等于a2则说明可信根磁盘文件中的数据不完整，不可以启动Qemu虚拟可信根。

[0080] S302：判断所述完整性信息是否与预设值相同；若是，则进入S303；若否，则结束流程；

[0081] 判断所述完整性信息是否与所述摘要值相同。

[0082] S303：启动虚拟可信根。

[0083] 图3对应的Qemu虚拟可信根的数据存储方法可以应用于虚拟化平台的Qemu虚拟可信根启动操作。实际应用中的虚拟可信根启动需要初始化过程中创建的口令来解密磁盘文件内容，解密成功读取数据后则要验证数据的完整性，具体的启动步骤如下：

[0084] 1)口令管理模块导出口令：口令管理模块获取已生成的口令，生成随机密钥加密口令并导出口令密文及本次密钥至文件中；

[0085] 2)Qemu恢复磁盘文件数据：Qemu解析口令和密钥，并恢复口令生成对应的Secret对象，供LUKS解密磁盘文件，读取完口令和密钥后及时清除对应的内容及文件；

[0086] 3)Qemu LUKS模块解密磁盘中的数据：Qemu LUKS使用2)中的口令Secret对象解密虚拟可信根磁盘文件中的数据内容，供虚拟可信根使用；

[0087] 4)校验数据完整性：待Qemu LUKS完成数据解密后，获取数据中的完整性信息，并计算本次数据内容的完整性值，与完整性信息比对，判断数据是否遭受破坏。根据校验结果判断Qemu虚拟可信根是否继续运行。

[0088] 当虚拟可信根运行后，内存中的运行时状态数据发生变化时会将所有的状态数据写入磁盘的文件中保存，此时，Qemu虚拟可信根启动时存储文件口令的Secret对象依然存在与内存中，LUKS使用该对象加密待写入的状态数据，然后再写入磁盘文件。具体步骤如下：

[0089] 1)生成完整性信息:计算Qemu虚拟可信根运行时状态信息的摘要值作为完整性信息,并将该值添加至运行待写入的数据中;

[0090] 2)LUKS加密待写入数据:LUKS将完整性信息和运行时状态信息作为待写入的数据加密生成密文;

[0091] 3)写入磁盘文件:Qemu使用BlockDriver作为操作磁盘文件的对象,每一个磁盘文件对应一个BlockDriver对象,BlockDriver将步骤3)中生成的密文写入磁盘文件中。

[0092] 请参见图5,图5为本申请实施例所提供的一种Qemu虚拟可信根的数据存储装置的结构示意图;

[0093] 该装置可以包括:

[0094] 数据机密模块100,用于获取口令密文和所述口令密文对应的密钥,并利用所述密钥对所述口令密文进行解密得到Secret对象;当检测到所述口令密文对应的Secret对象时,删除所述密钥;

[0095] 数据存储模块200,用于创建可信根磁盘文件,并利用所述Secret对象将存储至所述可信根磁盘文件的数据进行加密。

[0096] 进一步的,还包括:

[0097] 口令请求模块,用于向口令管理模块发送口令生成请求,以便所述口令管理模块生成口令密文和密钥;

[0098] 其中,所述口令密文由口令管理模块利用所述密钥对目标口令进行加密得到,所述目标密文和所述密钥均由所述口令管理模块利用随机数生成器得到,所述目标密文存储在所述口令管理模块的数据库中。

[0099] 进一步的,还包括:

[0100] 口令密文删除模块,用于删除所述口令密文。

[0101] 进一步的,还包括:

[0102] 完整性验证模块,用于当接收到虚拟可信根启动指令时,获取所述可信根磁盘文件的完整性信息;判断所述完整性信息是否与预设值相同;若是,则启动虚拟可信根。

[0103] 进一步的,完整性验证模块包括:

[0104] 口令获取单元,用于获取启动口令密文和所述启动口令密文对应的启动密钥,并利用所述启动密钥对所述启动口令密文进行解密得到解密Secret对象;

[0105] 解密单元,用于当检测到所述启动口令密文对应的解密Secret对象时,删除所述启动密钥;

[0106] 摘要值确定单元,用于利用所述解密Secret对象对所述可信根磁盘文件进行解密得到磁盘数据和所述完整性信息,并计算所述磁盘数据的摘要值;

[0107] 判断单元,用于判断所述完整性信息是否与所述摘要值相同。

[0108] 进一步的,数据存储模块200用于将所述虚拟可信根运行时的状态信息的摘要值作为完整性信息,并将所述完整性信息和所述状态信息设置为待写入数据;还用于利用所述Secret对象对所述待写入数据进行加密,并将所述待写入数据存储至所述可信根磁盘文件。

[0109] 由于装置部分的实施例与方法部分的实施例相互对应,因此系统部分的实施例请参见方法部分的实施例的描述,这里暂不赘述。

[0110] 本实施例通过利用密钥对口令密文进行解密得到Secret对象，该Secret对象为Qemu与形式保存密钥、口令的数据结构，可供Qemu的组件和虚拟设备运行时使用，因此利用该Secret对象对存储至所述可信根磁盘文件的数据进行加密可以保证数据的安全性。进一步的，由于本实施例在检测到所述口令密文对应的Secret对象后将密钥删除，能够保证即使虚拟可信根运行的系统被攻击，其他人也无法获取口令密文对应的口令原文，避免其他人通过非法途径获取虚拟可信根的数据。本实施例可以防止文件被窃取导致用户数据泄露，提高Qemu虚拟可信根的数据安全性。

[0111] 本申请还提供了一种虚拟化平台，该虚拟化平台包括如上述任意一种Qemu虚拟可信根的数据存储装置和口令管理模块；

[0112] 其中，口令管理模块用于当接收到所述Qemu虚拟可信根的数据存储装置发送的口令生成请求时，通过随机数生成器生成目标口令和密钥并将所述目标口令存储至数据库中，利用所述密钥加密所述目标口令得到口令密文，并将所述口令密文和所述密钥发送至所述Qemu虚拟可信根的数据存储装置。

[0113] 本申请还提供了一种计算机可读存储介质，其上存有计算机程序，该计算机程序被执行时可以实现上述实施例所提供的步骤。该存储介质可以包括：U盘、移动硬盘、只读存储器(Read-Only Memory，ROM)、随机存取存储器(Random Access Memory，RAM)、磁碟或者光盘等各种可以存储程序代码的介质。

[0114] 本申请还提供了一种电子设备，可以包括存储器和处理器，所述存储器中存有计算机程序，所述处理器调用所述存储器中的计算机程序时，可以实现上述实施例所提供的步骤。当然所述电子设备还可以包括各种网络接口，电源等组件。

[0115] 说明书中各个实施例采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似部分互相参见即可。对于实施例公开的系统而言，由于其与实施例公开的方法相对应，所以描述的比较简单，相关之处参见方法部分说明即可。应当指出，对于本技术领域的普通技术人员来说，在不脱离本申请原理的前提下，还可以对本申请进行若干改进和修饰，这些改进和修饰也落入本申请权利要求的保护范围内。

[0116] 还需要说明的是，在本说明书中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，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、物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、物品或者设备所固有的要素。在没有更多限制的状况下，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、物品或者设备中还存在另外的相同要素。

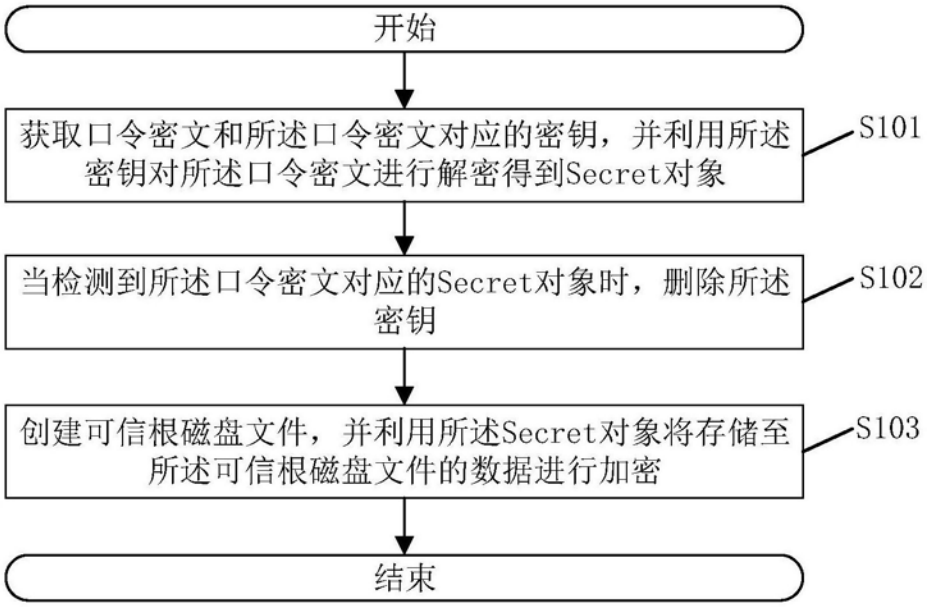

开始
获取口令密文和所述口令密文对应的密钥，并利用所述密钥对所述口令密文进行解密得到Secret对象
S101
当检测到所述口令密文对应的Secret对象时，删除所述密钥
S102
创建可信根磁盘文件，并利用所述Secret对象将存储至所述可信根磁盘文件的数据进行加密
S103
结束

图1

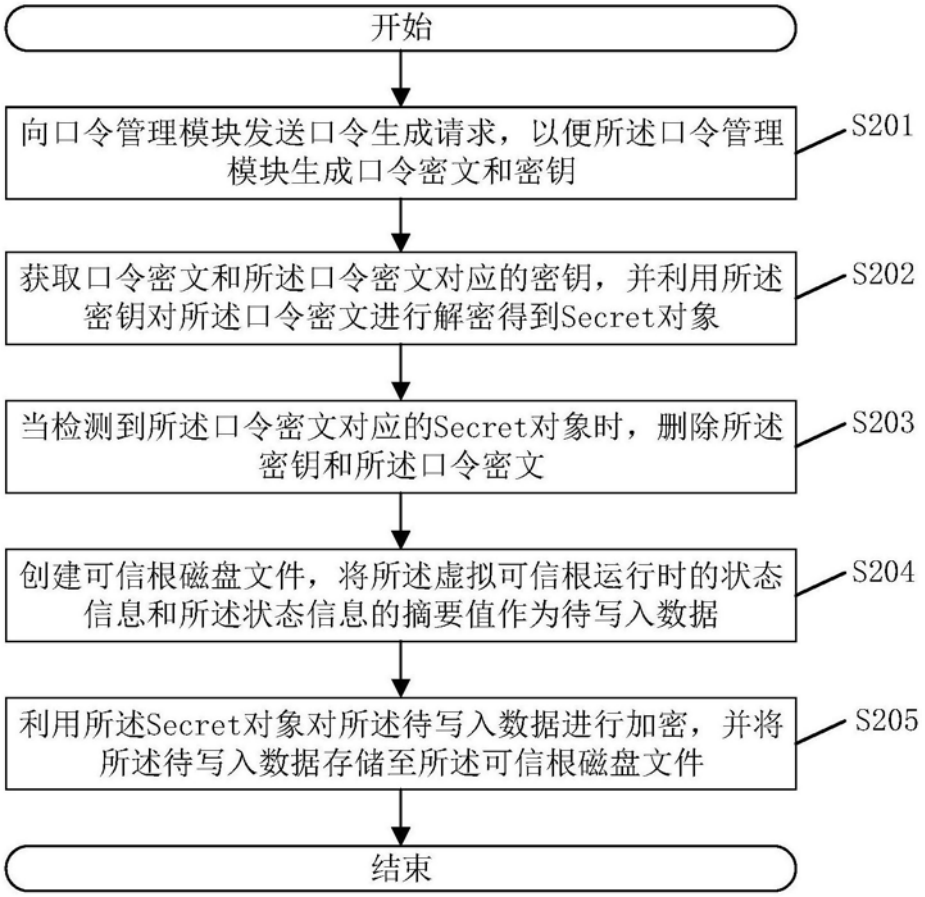

开始
向口令管理模块发送口令生成请求，以便所述口令管理模块生成口令密文和密钥
S201
获取口令密文和所述口令密文对应的密钥，并利用所述密钥对所述口令密文进行解密得到Secret对象
S202
当检测到所述口令密文对应的Secret对象时，删除所述密钥和所述口令密文
S203
创建可信根磁盘文件，将所述虚拟可信根运行时的状态信息和所述状态信息的摘要值作为待写入数据
S204
利用所述Secret对象对所述待写入数据进行加密，并将所述待写入数据存储至所述可信根磁盘文件
S205
结束

图2

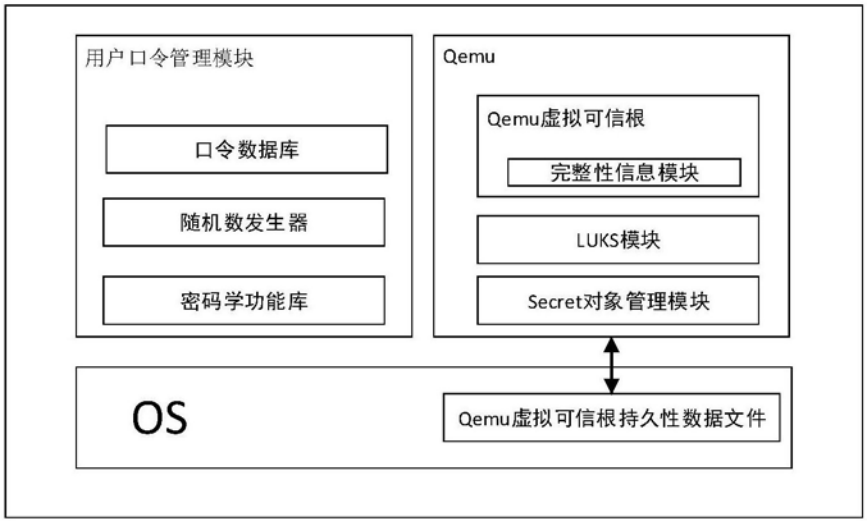

用户口令管理模块
口令数据库
随机数发生器
密码学功能库
Qemu
Qemu虚拟可信根
完整性信息模块
LUKS模块
Secret对象管理模块
OS
Qemu虚拟可信根持久性数据文件

图3

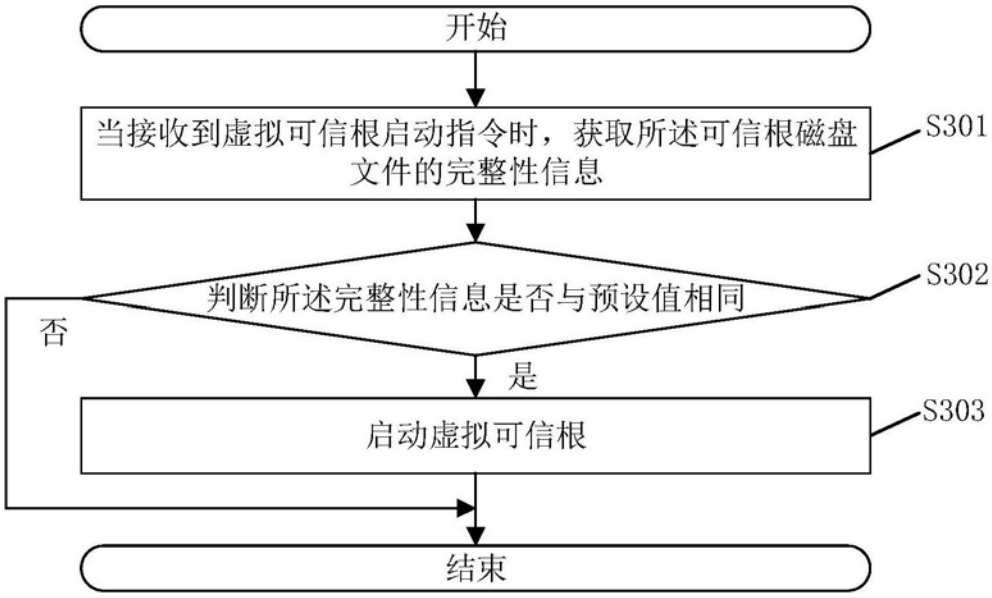

开始
当接收到虚拟可信根启动指令时，获取所述可信根磁盘文件的完整性信息
S301
判断所述完整性信息是否与预设值相同
S302
否
是
启动虚拟可信根
S303
结束

图4

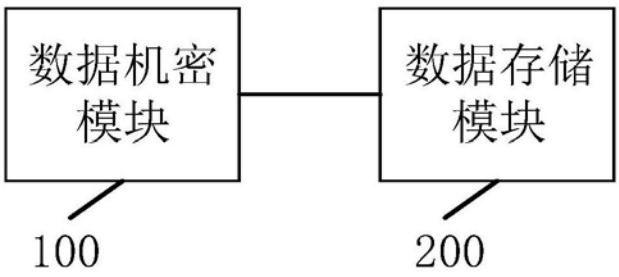

数据机密模块
数据存储模块
100
200

图5