(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 108885665 A
(43)申请公布日 2018.11.23

(21)申请号 201780022020.0

(22)申请日 2017.03.29

(30)优先权数据
62/317,804 2016.04.04 US
15/471,981 2017.03.28 US

(85)PCT国际申请进入国家阶段日
2018.09.30

(86)PCT国际申请的申请数据
PCT/EP2017/057422 2017.03.29

(87)PCT国际申请的公布数据
WO2017/174418 EN 2017.10.12

(71)申请人 比特梵德知识产权管理有限公司
地址 塞浦路斯尼科西亚

(72)发明人 R·卡拉杰亚

(74)专利代理机构 北京律盟知识产权代理有限责任公司 11287
代理人 张世俊

(51)Int.Cl.
G06F 21/56(2006.01)

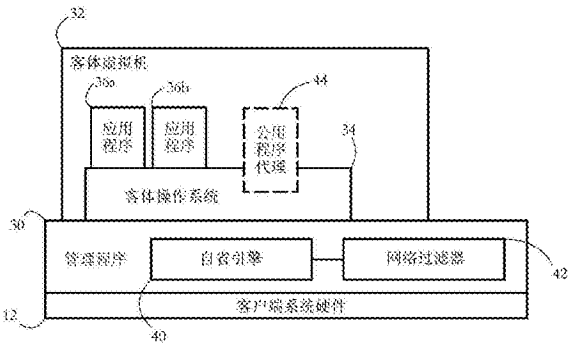
权利要求书4页 说明书14页 附图8页

(54)发明名称

用于解密虚拟化环境中的网络流量的系统和方法

(57)摘要

所描述的系统和方法实现针对例如恶意软件的检测和分析、入侵检测和监视外加其它的应用程序实现在客户端系统与远程方之间的加密通信的解密。所述客户端系统执行虚拟机和在所述虚拟机外的自省引擎。所述自省引擎被配置成识别其内容已在第一会话事件(例如,ServerHello消息)与第二会话事件(例如,ClientFinished消息)之间改变的存储页面。所述相应存储页面有可能含有用于所述相应通信会话的加密密钥材料。解密引擎可接着尝试使用从所述识别的存储页面的所述内容导出的信息解密所述相应通信会话的加密的有效载荷。



CN 108885665 A

1.一种客户端系统，其包括硬件处理器和存储器，所述硬件处理器被配置成执行虚拟机和自省引擎，其中：

所述虚拟机被配置成进行与远程方的通信会话，所述通信会话包括握手消息，跟着为加密的有效负载，其中所述握手消息含有由所述客户端系统用以导出加密密钥的加密参数，且其中所述加密的有效负载用所述加密密钥加密；以及

所述自省引擎在所述虚拟机外执行且被配置成：

根据目标存储页面的内容在所述通信会话的第一会话事件的发生与所述通信会话的第二会话事件的发生之间是否已改变而在所述存储器内识别所述目标存储页面，以及

作为响应，将所述目标存储页面的所述内容发射到被配置成根据所述内容解密所述加密的有效负载的解密引擎。

2.根据权利要求1所述的客户端系统，其中所述第一会话事件包括将所述握手消息从所述客户端系统发送到所述远程方或在所述客户端系统处接收所述握手消息。

3.根据权利要求2所述的客户端系统，其中所述通信会话用传输层安全TLS协议编译，且其中所述握手消息包括ClientHello消息或ServerHello消息。

4.根据权利要求1所述的客户端系统，其中所述第二会话事件包括将加密的数据包从所述客户端系统发送到所述远程方或在所述客户端系统处接收所述加密的数据包，且其中所述数据包是用所述加密密钥加密。

5.根据权利要求4所述的客户端系统，其中所述通信会话用传输层安全协议编译，且其中所述数据包包括ClientFinished消息的部分或ServerFinished消息的部分。

6.根据权利要求4所述的客户端系统，其中所述数据包包括所述加密的有效负载的部分。

7.根据权利要求1所述的客户端系统，其中识别所述目标存储页面包括：从由所述虚拟机使用的存储页面的集区选择候选存储页面；

响应于检测到所述第二会话事件的所述发生，根据所述候选存储页面的页表项确定在所述第二会话事件的所述发生前所述候选存储页面是否已被写入；

响应于确定所述候选存储页面是否已被写入，当所述候选存储页面已被写入时，选择所述候选存储页面作为所述目标存储页面。

8.根据权利要求1所述的客户端系统，其中所述至少一个硬件处理器被配置成进一步执行在所述虚拟机外的网络过滤器，所述网络过滤器控制所述客户端系统的网络适配器，其中：

所述网络过滤器被配置成拦截所述握手消息，且作为响应，将通知发射到所述自省引擎；以及

所述自省引擎被进一步配置成根据所述通知推断所述第一会话事件的所述发生。

9.根据权利要求1所述的客户端系统，其中所述至少一个硬件处理器被配置成进一步执行在所述虚拟机外的网络过滤器，所述网络过滤器控制所述客户端系统的网络适配器，其中：

所述自省引擎被进一步配置成响应于所述第二会话事件的所述发生，复制所述目标存储页面的所述内容，且作为响应，将通知发射到所述网络过滤器；以及

所述网络过滤器被配置成拦截指定用于所述虚拟机的数据包，且作为响应，延迟所述

数据包到所述虚拟机的传递，直到接收到所述通知。

10.根据权利要求1所述的客户端系统，其中所述自省引擎被进一步配置成响应于第三事件的发生，进一步根据所述目标存储页面的所述内容在所述第一会话事件的所述发生与所述第三事件的所述发生之间是否已改变来识别所述目标存储页面，其中所述第三事件的所述发生是由与所述通信会话同时的另一通信会话造成。

11.一种服务器计算机系统，其包括被配置成执行解密引擎的硬件处理器，所述解密引擎被配置成进行针对多个客户端系统的解密程序，解密程序包含：

接收所述多个客户端系统中的客户端系统的目标存储页面的内容；

接收在于所述客户端系统上执行的虚拟机与远程方之间进行的通信会话的加密的有效负载；以及

作为响应，根据所述目标存储页面的所述内容解密所述加密的有效负载，

其中所述通信会话包括握手消息，跟着为所述加密的有效负载，其中所述握手消息含有由所述客户端系统用以导出加密密钥的加密参数，且其中所述加密的有效负载用所述加密密钥加密，且

其中所述客户端系统被配置成在所述虚拟机外执行自省引擎，所述自省引擎被配置成根据所述目标存储页面的所述内容在所述通信会话的第一会话事件的发生与所述通信会话的第二会话事件的发生之间是否已改变来识别在所述客户端系统的存储器内的所述目标存储页面。

12.根据权利要求11所述的服务器计算机系统，其中解密所述加密的有效负载包括：

从所述目标存储页面的所述内容导出候选解密密钥；以及

尝试使用所述候选解密密钥解密所述加密的有效负载。

13.根据权利要求11所述的服务器计算机系统，其中所述第一会话事件包括将所述握手消息从所述客户端系统发送到所述远程方或在所述客户端系统处接收所述握手消息。

14.根据权利要求13所述的服务器计算机系统，其中所述通信会话用传输层安全协议编译，且其中所述握手消息包括ClientHello消息或ServerHello消息。

15.根据权利要求13所述的服务器计算机系统，其中所述第二会话事件包括将加密的数据包从所述客户端系统发送到所述远程方或在所述客户端系统处接收所述加密的数据包，且其中所述数据包是用所述加密密钥加密。

16.根据权利要求15所述的服务器计算机系统，其中所述通信会话用传输层安全协议编译，且其中所述数据包包括ClientFinished消息的部分或ServerFinished消息的部分。

17.根据权利要求15所述的服务器计算机系统，其中所述数据包包括所述加密的有效负载的部分。

18.根据权利要求11所述的服务器计算机系统，其中识别所述目标存储页面包括：

从由所述虚拟机使用的存储页面的集区选择候选存储页面；

响应于检测到所述第二会话事件的所述发生，根据所述候选存储页面的页表项确定在所述第二会话事件的所述发生前所述候选存储页面是否已被写入；

响应于确定所述候选存储页面是否已被写入，当所述候选存储页面已被写入时，选择所述候选存储页面作为所述目标存储页面。

19.根据权利要求11所述的服务器计算机系统，其中所述客户端系统被进一步配置成

执行在所述虚拟机外的网络过滤器，所述网络过滤器控制所述客户端系统的网络适配器，其中：

所述网络过滤器被配置成拦截所述握手消息，且作为响应，将通知发射到所述自省引擎；以及

所述自省引擎被进一步配置成根据所述通知推断所述第一会话事件的所述发生。

20.根据权利要求11所述的服务器计算机系统，其中所述客户端系统被进一步配置成执行在所述虚拟机外的网络过滤器，所述网络过滤器控制所述客户端系统的网络适配器，其中：

所述自省引擎被进一步配置成响应于所述第二会话事件的所述发生，复制所述目标存储页面的所述内容，且作为响应，将通知发射到所述网络过滤器；以及

所述网络过滤器被配置成拦截指定用于所述虚拟机的数据包，且作为响应，延迟所述数据包到所述虚拟机的传递，直到接收到所述通知。

21.根据权利要求11所述的服务器计算机系统，其中所述自省引擎被进一步配置成响应于第三事件的发生，进一步根据所述目标存储页面的所述内容在所述第一会话事件的所述发生与所述第三事件的所述发生之间是否已改变来识别所述目标存储页面，其中所述第三事件的所述发生是由与所述通信会话同时的另一通信会话造成。

22.根据权利要求11所述的服务器计算机系统，其中所述硬件处理器被进一步配置成根据解密所述加密的有效负载的结果确定所述客户端系统是否包括恶意软件。

23.一种非暂时性计算机可读媒体，其存储指令，所述指令在由进一步包括存储器的客户端系统的硬件处理器执行时使所述硬件处理器形成在于所述客户端系统上执行的虚拟机外执行的自省引擎，其中：

所述虚拟机被配置成进行与远程方的通信会话，所述通信会话包括握手消息，跟着为加密的有效负载，其中所述握手消息含有由所述客户端系统用以导出加密密钥的加密参数，且其中所述加密的有效负载用所述加密密钥加密；以及

所述自省引擎被配置成：

根据目标存储页面的内容在所述通信会话的第一会话事件的发生与所述通信会话的第二会话事件的发生之间是否已改变而在所述存储器内识别所述目标存储页面，以及

作为响应，将所述目标存储页面的所述内容发射到被配置成根据所述内容解密所述加密的有效负载的解密引擎。

24.一种解密客户端系统与远程方之间的加密通信的方法，其中所述客户端系统被配置成执行虚拟机，其中：

所述虚拟机被配置成进行与所述远程方的通信会话，所述通信会话包括握手消息，跟着为加密的有效负载，其中所述握手消息含有由所述客户端系统用以导出加密密钥的加密参数，且其中所述加密的有效负载用所述加密密钥加密，

所述方法包括：

使用至少一个硬件处理器根据目标存储页面的内容在所述通信会话的第一会话事件的发生与所述通信会话的第二会话事件的发生之间是否已改变而在所述客户端系统的存储器内识别所述目标存储页面；

使用至少一个硬件处理器采集所述加密的有效负载；以及

使用至少一个硬件处理器根据所述目标存储页面的所述内容解密所述加密的有效负载。

用于解密虚拟化环境中的网络流量的系统和方法

[0001] 相关申请

[0002] 本申请要求申请日为2016年4月4日申请的题目为“用于解密虚拟化环境中的网络流量的系统和方法(Systems and Methods for Decrypting Network Traffic in a Virtualized Environment)”的美国临时专利申请第62/317,804号的权益,所述申请的全部内容被以引用的方式并入本文中。

背景技术

[0003] 本发明涉及电脑安全系统和方法,并且明确地说,涉及加密的电子通信。

[0004] 所述现代数字世界中,广泛多种产品和服务依赖于数据加密。加密的通信尤其实现通过例如因特网的数据网络进行的在线商务、在线银行和电话。加密还广泛用以保护用户的隐私和个人数据。在互连电子装置(物联网)的增长的年代里,对加密的依赖很强,但却也很脆弱。

[0005] 近年来,加密被日益用于恶意目的,例如,用以隐藏恶意软件的活动,或用以将有价值数据用于敲诈。恶意软件活动的一个典型实例包含设置劫持的计算系统的网络——通常被称为僵尸网络,和使用相应网络启动针对目标网络服务器的分布式服务拒绝攻击。作为设置僵尸网络的部分,使用各种方法(例如,直接黑客、钓鱼等)使软件代理渗透到每一僵尸网络部件内。代理可接着使用加密来难以察觉地与远程服务器通信,例如,以接收目标网络的地址,和/或协调与其它僵尸网络部件的攻击。已描述防止或抵制此类恶意活动的各种方法,但此类对策可因恶意软件的高效使用加密而受到破坏。

[0006] 反恶意软件操作因硬件虚拟化技术的出现而进一步复杂化,硬件虚拟化技术实现通常被称为虚拟机的模拟电脑环境的创建。若干虚拟机可同时在同一物理机器上运行,在其间共享硬件资源,因此减少投资和操作成本。每一虚拟机可与其它虚拟机分开来运行其自身的操作系统和/或软件应用程序。针对各种原因部署硬件虚拟化,例如,以确保软件的便携性或加强安全性。在通用名“云计算”下已知的硬件虚拟化的其它流行应用程序包含网络服务器农场和虚拟桌面基础设施(VDI)。在典型VDI配置中,软件应用程序在第一计算机系统上执行,同时用户使用第二计算机系统(终端)与相应应用程序交互。运行相应的应用程序的虚拟机按需求在第一计算机系统上具现化,这可最终为多个远程用户执行数百个此类VM。归因于恶意软件的平稳增长,每一虚拟机潜在地需要针对恶意软件的保护。

[0007] 逐步增加的安全性威胁和对虚拟化的增加需求产生了对开发被设计成解决硬件虚拟化的难题的高效反恶意软件系统和方法的强烈兴趣。

发明内容

[0008] 根据一个方面,一种客户端系统包含硬件处理器和存储器,所述硬件处理器被配置成执行虚拟机和自省引擎。所述虚拟机被配置成进行与远程方的通信会话,所述通信会话包括握手消息,跟着为加密的有效载荷,其中所述握手消息含有由所述客户端系统用以导出加密密钥的加密参数,且其中所述加密的有效载荷用所述加密密钥加密。所述自省引

擎在所述虚拟机外执行，且被配置成根据目标存储页面的内容在所述通信会话的第一会话事件的发生与所述通信会话的第二会话事件的发生之间是否已改变而在所述存储器内识别所述目标存储页面。所述自省引擎被进一步配置成将所述目标存储页面的所述内容发射到被配置成根据所述内容解密所述加密的有效载荷的解密引擎。

[0009] 根据另一方面，一种服务器计算机系统包括被配置成执行解密引擎的硬件处理器，所述解密引擎被配置成进行针对多个客户端系统的解密程序。解密程序包括接收所述多个客户端系统中的客户端系统的目标存储页面的内容，接收在于所述客户端系统上执行的虚拟机与远程方之间进行的通信会话的加密的有效载荷，和作为响应，根据所述目标存储页面的所述内容解密所述加密的有效载荷。所述通信会话包括握手消息，跟着为所述加密的有效载荷，其中所述握手消息含有由所述客户端系统用以导出加密密钥的加密参数，且其中所述加密的有效载荷用所述加密密钥加密。所述客户端系统被配置成在所述虚拟机外执行自省引擎，所述自省引擎被配置成根据所述目标存储页面的所述内容在所述通信会话的第一会话事件的发生与所述通信会话的第二会话事件的发生之间是否已改变来识别在所述客户端系统的存储器内的所述目标存储页面。

[0010] 根据另一方面，一种非暂时性计算机可读媒体存储指令，所述指令在由进一步包括存储器的客户端系统的硬件处理器执行时使所述硬件处理器形成在于所述客户端系统上执行的虚拟机外执行的自省引擎。所述虚拟机被配置成进行与远程方的通信会话，所述通信会话包括握手消息，跟着为加密的有效载荷，其中所述握手消息含有由所述客户端系统用以导出加密密钥的加密参数，且其中所述加密的有效载荷用所述加密密钥加密。所述自省引擎被配置成根据目标存储页面的内容在所述通信会话的第一会话事件的发生与所述通信会话的第二会话事件的发生之间是否已改变而在所述存储器内识别所述目标存储页面。所述自省引擎被进一步配置成将所述目标存储页面的所述内容发射到被配置成根据所述内容解密所述加密的有效载荷的解密引擎。

[0011] 根据另一方面，一种解密客户端系统与远程方之间的加密通信的方法。所述客户端系统被配置成执行虚拟机。所述虚拟机被配置成进行与所述远程方的通信会话，所述通信会话包括握手消息，跟着为加密的有效载荷，其中所述握手消息含有由所述客户端系统用以导出加密密钥的加密参数，且其中所述加密的有效载荷用所述加密密钥加密。所述方法包括使用至少一个硬件处理器根据目标存储页面的内容在所述通信会话的第一会话事件的发生与所述通信会话的第二会话事件的发生之间是否已改变而在所述客户端系统的存储器内识别所述目标存储页面。所述方法进一步包括使用至少一个硬件处理器采集所述加密的有效载荷，和使用至少一个硬件处理器根据所述目标存储页面的所述内容解密所述加密的有效载荷。

附图说明

[0012] 在阅读以下详细描述后并且在参看图式后，本发明的前述方面和优点将变得更好理解，其中：

[0013] 图1说明根据本发明的一些实施例的示范性配置，其中客户端系统与安全服务器合作以解密潜在恶意网络流量。

[0014] 图2-A说明根据本发明的一些实施例的客户端系统的示范性硬件配置。

[0015] 图2-B说明根据本发明的一些实施例的安全服务器的示范性硬件配置。

[0016] 图3展示根据本发明的一些实施例的通过在客户端系统上执行的管理程序公开的客体虚拟机(VM)，和在客体VM外执行的自省引擎。

[0017] 图4展示在如图3中所说明的硬件虚拟化配置中的示范性存储器地址转译。

[0018] 图5展示根据本发明的一些实施例的由自省引擎进行以拦截进入或离开客体VM的加密的流量的示范性步骤序列。

[0019] 图6展示根据本发明的一些实施例的由自省引擎执行以获得客体VM的优化的存储快照的示范性步骤序列。

[0020] 图7说明根据本发明的一些实施例的由自省引擎执行以获得多个同时加密通信会话的优化的存储快照的示范性步骤序列。

[0021] 图8展示根据本发明的一些实施例的在安全服务器上执行的示范性解密引擎。

[0022] 图9展示根据本发明的一些实施例的由解密引擎执行的示范性步骤序列。

具体实施方式

[0023] 在以下描述中，应理解，结构之间的所有所叙述的连接可以是直接操作性连接，或者通过中间结构的间接操作性连接。一组元件包含一或多个元件。对元件的任何叙述应理解为指至少一个元件。多个元件包含至少两个元件。除非另外指定，否则“或”的任何使用指非排他性或。除非另有需要，否则不需要必然以特定所说明的次序执行任何所描述的方法步骤。从第二元件导出的第一元件(例如，数据)涵盖等于第二元件的第一元件，以及通过处理第二元件和任选地其它数据产生的第一元件。根据参数作出确定或决策涵盖根据参数和任选地根据其它数据作出确定或决策。除非另外指定，否则某一数量/数据的指示符可以是数量/数据本身，或者是不同于数量/数据本身的指示符。计算机安全涵盖保护用户和设备免受对数据和/或硬件的无意或未授权存取，免受数据和/或硬件的无意或未授权修改，和免受数据和/或硬件的损坏。计算机程序是进行任务的一连串处理器指令。在本发明的一些实施例中描述的计算机程序可为独立的软件实体或其它计算机程序的子实体(例如，子例程、库)。除非另外指定，否则客体软件在虚拟机内执行。当程序在相应虚拟机的虚拟处理器上执行时，其被称为在虚拟机内执行。过程是计算机程序的例子，例如，操作系统的应用程序或一部分，且特性化为具有至少执行线程和分派到它的虚拟存储空间，其中相应虚拟存储空间的内容包含可执行代码。除非另外指定，否则页面表示可个别地映射到主机系统的物理存储的虚拟存储的最小单位。除非另外指定，否则客户端系统/虚拟机的存储快照包括由相应客户端系统/虚拟机使用的存储器段的内容的复本。计算机可读媒体涵盖非暂时性媒体，例如，磁性、光学和半导体存储媒体(例如，硬盘驱动器、光盘、闪存、DRAM)，以及例如传导性电缆和光纤链路的通信链路。根据一些实施例，本发明尤其提供包括被编程以执行本文中所描述的方法的硬件(例如，一或多个微处理器)以及编码指令以执行本文中所描述的方法的计算机可读媒体的计算机系统。

[0024] 以下描述通过实例且未必通过限制来说明本发明的实施例。

[0025] 图1展示根据本发明的一些实施例的示范性配置，其中客户端系统12a-d的集合与安全服务器15合作以拦截和解密在相应客户端系统12a-d与说明为内容服务器13的远程方之间发生加密的网络流量。服务器13和15中的每一个一般表示可或可不相互物理接近的互

连的计算系统的集合。

[0026] 示范性客户端系统12a-d包含公司计算系统，并且还有个人计算机系统、移动计算平台(膝上型计算机、平板电脑、移动电话)、可佩戴电子装置(智能手表)、家用电器(智能TV、恒温器、家用监视/安全系统)或具有处理器和存储器且支持硬件虚拟化的任一其它电子装置。对于计算机安全特别关注的一个示范性客户端系统是被配置为蜜罐的计算机。蜜罐是在所属技术中用以描述用于针对数据搜集引诱恶意实体和恶意软件的研究的一组系统和方法。示范性蜜罐包括明显无保护的计算机系统，其可以允许黑客或恶意软件代理进入、安装软件和/或通过网络与其它计算机通信。

[0027] 说明的客户端系统经由例如公司网络或本地网络的本地通信网络10互连。本地网10的部分可包含区域网路(LAN)。网关装置14可实现客户端系统12a-d对扩展网络11(例如，因特网)的访问，使得在客户端系统12a-d与远程方之间的全部或部分网络流量穿过网关装置14。示范性网关装置14包括例如路由器和/或交换机的物理器具。

[0028] 图2-A展示根据本发明的一些实施例的客户端系统12的示范性硬件配置。客户端系统12可表示图1中的系统12a-d中的任一个。为简单起见，说明的客户端系统为个人计算机；例如移动电话、平板电脑等的其它客户端系统的硬件配置可与图2-A的所说明配置稍有不同。客户端系统12包括一组物理装置，包含硬件处理器16和存储器单元18。处理器16包括被配置成用一组信号和/或数据执行计算和/或逻辑运算的物理装置(例如，微处理器、形成于半导体衬底上的多核集成电路等)。在一些实施例中，按一连串处理器指令(例如，机器代码或其它类型的编码)的形式将此类运算传递到处理器16。存储器单元18可包括存储由处理器16存取或产生的指令和/或数据的易失性计算机可读媒体(例如，DRAM、SRAM)。

[0029] 输入装置20可包含计算机键盘和鼠标外加其它，从而允许用户将数据和/或指令引入到系统12内。输出装置22可包含例如监视器的显示装置。在一些实施例中，输入装置20和输出装置22可以共享一件共同的硬件，如在触摸屏装置的情况下。存储装置24包含实现软件指令和/或数据的非易失性存储、读取和写入的计算机可读媒体。示范性存储装置24包含磁盘和光盘和闪存装置以及例如CD和/或DVD磁盘和驱动器的可去除媒体。网络适配器26使系统12能够连接到网络10和/或连接到其它机器/计算机系统。控制器集线器28一般表示多个系统、外围装置和芯片组总线和/或实现系统12的装置16-26的相互通信的所有其它电路系统。举例来说，控制器集线器28可包含存储器控制器、输入/输出(I/O)控制器和中断控制器外加其它。在另一实例中，集线器28可包括将处理器16连接到存储器18的北桥总线，和/或将处理器16连接到装置20、22、24和26外加其它的南桥总线。

[0030] 图2-B展示根据本发明的一些实施例的安全服务器15的示范性硬件配置。在所说明的配置中，服务器15包括服务器处理器16、服务器存储器18、一组服务器存储装置124和一组网络适配器126。处理器116可包括微处理器或被配置成用数据集执行数学和/或逻辑运算的或物理装置。存储器18可包括存储指令和/或数据以用于由处理器116执行和/或处理的易失性计算机可读媒体。服务器存储装置124包括非易失性计算机可读媒体，例如，硬盘驱动器、CD和DVD ROM和闪存外加其它。服务器网络适配器126使安全服务器15能够经由扩展网络11连接到其它电子装置和与其它电子装置交换数据。

[0031] 图3展示根据本发明的一些实施例的典型软件配置。客户端系统12被配置成公开一组虚拟机(VM)。虽然图3仅展示一个客体VM 32，但一些实施例可托管同时操作的多个VM

(例如,数百个)。每一虚拟机包括实际物理机器/计算机系统的仿真,且可执行操作系统和多种软件应用程序。如图3中所说明的实施例可用以针对恶意软件(例如,尝试盗窃专属、私人和/或机密数据的软件,或尝试劫持客户端系统12并将其变换成僵尸网络部件的软件)保护云计算的客户。在此类实施例中,客户端系统12可表示云服务提供商的服务器计算机系统。在其它示范性实施例中,客户端系统12表示用户的私人装置,例如,个人计算机或移动电话。此类装置常常使用硬件虚拟化,例如,以增加软件便携性或加强安全性。在又一示范性实施例中,客户端系统12可被配置为蜜罐。在此类实施例中,客户端系统12可公开多个虚拟机,例如,一个伪装为网络服务器,另一个伪装为连接到公司网络的个人计算机,等等。

[0032] 在一些实施例中,管理程序30在客户端系统12上执行,管理程序30包括被配置成创造或启用多个虚拟化的装置(例如,虚拟处理器和虚拟存储管理单元)和代替客户端系统12的真实物理装置将此类虚拟化的装置对软件呈现的软件。此类操作在所属领域中通常被称为公开虚拟机。管理程序30可进一步使多个虚拟机能够共享主机系统12的硬件资源,使得每一VM独立地操作且意识不到同时在客户端系统12上执行的其它VM。流行管理程序的实例包含来自VMware公司的VMware vSphere™和开源Xen管理程序外加其它。

[0033] 在图3中说明的示范性配置中,客体VM 32执行客体操作系统(OS)34和一组应用程序36a-b。客体OS 34可包括任一广泛可用的操作系统(例如,Microsoft Windows®、MacOS®、Linux®、iOS®或Android™,外加其它),其提供在VM 32内执行的应用程序与客体VM 32的虚拟化的硬件装置之间的接口。应用程序36a-b一般表示任一用户应用程序,例如,字处理器、电子表格应用程序、图形应用程序、浏览器、社交媒体应用程序和电子通信应用程序,外加其它。客体OS 34和应用程序36a-b在本文中被称为在客体VM 32内执行,即,它们在VM 32的虚拟处理器上执行。相比之下,管理程序30被称为在客体VM 32外执行。

[0034] 在一些实施例中,公开客体VM 32包括配置由管理程序30用以管理客体VM 32的操作的数据结构。此结构将在本文中被称为虚拟机状态对象(VMSO)。示范性VMSO包含在Intel®平台上的虚拟机控制结构(VMCS),和在AMD®平台上的虚拟机控制块(VMCB)。在一些实施例中,处理器16使存储器中的区域与每一VMSO相关联,使得软件可使用存储器地址或指针(例如,Intel®平台上的VMCS指针)来参考具体VMSO。

[0035] 每一VMSO可包括表示在客户端系统12上公开的相应虚拟化的处理器的当前状态的数据。在多线程配置中,硬件处理器16可操作多个核心,每一核心进一步包括多个逻辑处理器,其中每一逻辑处理器可独立于其它逻辑处理器和与其它逻辑处理器同时地处理过程线程。多个逻辑处理器可共享一些硬件资源,例如,共同MMU。在多线程实施例中,可针对每一截然不同的逻辑处理器设置截然不同的VMSO。每一VMSO可包括客体状态区和主机状态区,客体状态区拥有相应VM的(即,相应虚拟化的处理器的)CPU状态,且主机状态区存储管理程序30的当前状态。在一些实施例中,VMSO的客体状态区包含控制寄存器(例如,CR0、CR3等)、指令指针(例如,RIP)、通用寄存器(例如,EAX、ECX等)和相应VM的虚拟处理器的状态寄存器(例如,EFLAGS)外加其它的内容。VMSO的主机状态区可包含到被配置以用于针对相应VM的地址转译的页表的指针(例如,在Intel®平台上的EPT指针)。

[0036] 在一些实施例中,处理器16可将VMSO的一部分存储于专用内部寄存器/高速缓冲存储器内,而相应VMSO的其它部分可驻留在存储器18中。在任何给定时间,可将至多一个VMSO(本文中被称为当前VMSO)装载到逻辑处理器上,从而识别当前具有对相应逻辑处理器

的控制的虚拟机。当处理器16从在VM内执行软件(例如,图3中的应用程序36a)切换到在相应VM(例如,管理程序30)外执行软件时,处理器16可将当前处理器状态保存到当前VMSO的客体状态区,且将VMSO的主机状态装载到处理器上。相反地,当处理器16从在VM外执行软件切换到在相应VM内执行软件时,处理器16可将当前处理器状态保存到VMSO的主机状态区,且将当前VMSO的客体状态装载到处理器16上。

[0037] 在一些实施例中,自省引擎40在公开于相应客户端系统上的所有客体VM外执行。自省是在硬件虚拟化的技术中的建立的术语,一般表示从在相应VM外的位置搜集关于虚拟机的操作的各种方面的信息。在本发明的一些实施例中,自省包括例如以下的操作:监测在客体VM 32内执行的过程,拦截执行客体VM 32内的某一OS功能或处理器指令的尝试,拦截存取由客体VM 32使用的存储页面的尝试,和确定存储器18中存储由客体VM使用的具体数据的位置,外加其它。引擎40可并入到管理程序30内,或可作为与管理程序30截然不同且独立但在与管理程序30大体上类似的处理器特权等级下执行的软件组件传递。单个引擎40可被配置成自省在客户端系统12上执行的多个VM。引擎40可与管理程序30合作以解密进入和/或离开客户端系统12的通信。更具体地说,引擎40可被配置成在存储器18内大致定位用以加密由客体VM 32发送或接收的消息的加密密钥,如下详述。

[0038] 在客户端系统12上执行的软件可进一步包括网络过滤器42,其被配置成拦截进入或离开客体VM 32的通信,和与自省引擎40交换信息。过滤器42可收听具体网络端口,例如,用于遵守TLS协议的连接的端口443。过滤器42可在VM 32内或外执行。当在VM 32外执行时,单个网络过滤器可监测进入或离开在客户端系统12上执行的多个VM的通信。为达成此监测,管理程序30可通过网络过滤器42导引到客户端系统12内和/或离开客户端系统12的所有通信。过滤器42可具有网络适配器26的独占式控制,可(例如)使用来自Intel®的VT-d®技术实施所述网络适配器的配置。当监测多个VM时,过滤器42可维持VM具体包队列,即,使每一拦截的网络包与源和/或目的地VM相关联。

[0039] 在一些实施例中,自省引擎40通过检测在软件在客体VM 32内的执行期间发生的各种事件来操作。由自省引擎40检测的示范性事件包含(例如)处理器异常和/或中断、执行客体OS 34的特定功能的尝试、处理器特权(例如,系统调用)的改变、存取特定存储器位置(从特定存储器位置读取、写入到特定存储器位置和/或从特定存储器位置执行)的尝试等。自省引擎40可被进一步配置成判定在客体VM 32内执行的各种软件组件的存储器地址,如下文进一步描述。

[0040] 一些实施例进一步包括在客体VM 32内执行的公用程序代理44,代理44与自省引擎40合作以检测和分析在客体VM 32内发生的事件。代理44可包括(例如)在客体OS 34的处理器特权等级(例如,环0、内核模式)下执行的驱动程序,且可注册为用于例如页面错误和硬件中断的各种处理器事件的处理程序。此类配置的一个优点是,一些信息从VM内部比从相应VM外容易得多地获得,这是由于内部代理能够存取客体OS 34的所有功能性。缺点是,在客体VM 32内执行的代理潜在地易受在相应VM内执行的恶意软件攻击。为了减轻这个风险,一些实施例可仅临时在客体VM 32内部注入代理44,且可在代理44完成执行后擦除代理44。

[0041] 为了检测在客体VM 32内发生的事件,自省引擎40可使用在虚拟化的技术中已知的任何方法。一个重要种类的方法将存取特定存储器位置的尝试用作特定事件的发生的指

示符。为了检测此存储器存取尝试，一些实施例设置存储器存取许可使得尝试将违反相应许可。所述违规然后由自省引擎和/或公用程序代理44拦截。虚拟机通常按虚拟化的物理存储(在所属领域中也被称为客体物理存储)操作。虚拟化的物理存储包括实际物理存储18的抽象表示，例如，作为具体针对每一VM的地址的邻接空间，其中所述空间的部分映射到在物理存储18和/或物理存储装置24内的地址。在现代硬件虚拟化平台中，此映射通常经由由处理器16控制的专用数据结构和机制来达成，被称为第二层级地址转译(SLAT)。流行的SLAT实施方案包含在Intel®平台上的扩展页表(EPT)和在AMD®平台上的快速虚拟化索引(RVI)/嵌套式页表(NPT)。在此类系统中，按所属领域中被称为页面的单位分割虚拟化的物理存储，页面表示经由SLAT个别地映射到物理存储的虚拟化的物理存储的最小单位，即，按页面精细度执行在物理与虚拟化的物理存储之间的映射。所有页面通常具有预定大小，例如，4千字节、2兆字节等。虚拟化的物理存储到页面的分割通常由管理程序30配置。在一些实施例中，管理程序30也配置SLAT结构，和因此物理存储与虚拟化的物理存储之间的映射。在一些实施例中，将到SLAT数据结构(例如，到页表)的指针存储于相应虚拟机的VMSO内。虚拟化的物理存储器地址到物理存储器地址的实际映射(转译)可包括查找客户端系统12的转译后备缓冲器(TLB)中的物理存储器地址。在一些实施例中，地址转译包括执行页面查核行程(其包含在页表集和/或页面目录集中的一组连续地址查询)，和执行例如将页面相对于相应页面的偏移添加到地址的计算。

[0042] 图4说明在如图3中展示的实施例中的存储器地址的此映射。在由管理程序30公开后，客体VM 32将虚拟化的物理存储空间218看作其自身的物理存储空间。在客体VM 32内执行的软件对象(例如，应用程序36a)由客体OS 34指派虚拟存储空间318。当软件对象尝试存取空间318a的示范性存储页面50a的内容时，页面50a的地址由客体VM 32的虚拟化的处理器根据由客体OS 34配置和控制的页表转译成虚拟化的物理存储空间218的页面50b的地址。页面50b的地址进一步由物理处理器16使用由管理程序30配置的SLAT映射到在物理存储18内的页面50c的地址。

[0043] 虚拟地址空间218在所属领域中通常被称为客体物理存储，并且在一个此存储器空间内的地址被称作客体物理地址(GPA)。地址空间318通常被称为客体虚拟存储，并含有客体虚拟地址(GVA)。在物理存储18内的地址通常被称作主机物理地址(HPA)。例如图4中之52的地址转译/映射因此被称为GVA到GPA转译。相比之下，例如54的地址转译通常被称为GPA到HPA转译。

[0044] 在一些实施例中，管理程序30设置其自身的虚拟存储空间418(包括物理存储18的表示)，且使用转译机制(例如，页表)将空间418中的地址映射地址物理存储18中的地址。图4中，此示范性映射将在虚拟空间418内的页面50f的地址转译到页面50c的物理地址，且将页面50d的地址转译到页面50e的物理地址。此映射潜在地允许在管理程序30的处理器特权等级下执行的任何软件对象管理属于在于客户端系统12上运行的各种VM内执行的软件对象的存储页面。明确地说，存储器自省引擎40可因此对由在客体VM 32内执行的任何过程使用的物理存储页面枚举、读取、写入和控制存取。

[0045] 在一些实施例中，检测在客体VM 32内发生的事件包括自省引擎40与管理程序30合作以设定在SLAT数据结构内的存储器存取许可。此类特征可为平台具体性，但通常按页面精细度来设定存取许可。举例来说，在支持虚拟化的Intel®平台上，每一存储页面的EPT

项包含一组存取许可位，其分别指示是否可从相应页面读取、写入到相应页面和执行相应页面。当尝试存取特定存储页面违反针对相应存储页面设定的存取许可时，所述相应尝试可触发处理器事件，例如，异常或虚拟机退出事件(在Intel®平台上的VMExit)。响应于处理器事件，处理器16可切换到执行在相应VM外的事件处理程序例程，这允许自省引擎40检测相应存取违规的发生。在替代性实施例中，存储器存取违规可触发处理器异常(例如，虚拟化异常或在Intel®平台上的#VE)。响应于此类处理器事件，处理器16可切换到执行在相应VM内的事件处理程序例程，即，不退出相应VM。在具有如图4中所展示的公用程序代理44的实施例中，可将代理44注册为虚拟化异常处理程序，因此检测到存储器存取违规。

[0046] 在一些实施例中，存储页面的SLAT项进一步包括指示是否已存取相应页面和/或是否已写入到相应页面的域(例如，位)。此类位通常叫作已存取的且页面重写标志位。一些实施例使用已存取的和/或页面重写标志位识别有可能含有加密密钥的存储页面，如下进一步展示。

[0047] 在本发明的一些实施例中，自省引擎40被配置成监测进入或离开客体VM的加密通信。通信会话通常包括在当事人之间的初步协商，跟着为经加密消息的实际交换。在所属领域中，前者通常被叫作握手，而消息的内容通常被称为有效载荷。握手包括尤其指定用于导出加密密钥的密码(即，加密算法)和成分的一组交换。示范性密码包含高级加密标准(AES)导出的分块密码和例如ChaCha-20的流密码。在一些实施例中，握手可包括根据具体协议执行的实际密钥交换，和/或用于验证任一个或两个当事人的身份的额外步骤。取决于密码，用于导出加密密钥的成份可包括一组随机数、通信方的公用密钥等。

[0048] 安全通信协议的具体实例为(例如)在因特网工程任务小组(IETF)网络工作组的请求注解(RFC)5246中描述的传输层安全(TLS)协议。TLS协议当前由大多数浏览器、电子商务和安全电子银行应用程序使用。TLS会话尤其包含唯一会话识别符、密码规范和在通信方之间共享的主秘密。主秘密通常由每一方使用在握手期间交换的成份分开来计算。TLS握手协议包括以下步骤/阶段：

[0049] a)交换问候(hello)消息以对用于通信的密码编译参数达成一致。从客户端发送到服务器的客户端问候消息可指示一列支持的密码，且包含客户端供应的随机数，外加其它。从服务器发送到客户端的服务器问候消息可指示从由客户端提议的密码选择一个，且包含服务器供应的随机数。

[0050] b)执行当事人的认证。服务器可发送确认其身份的证书，且又可向客户端请求证书。这步骤可包括来自客户端的ClientCertificate消息和来自服务器的ServerCertificate消息。

[0051] c)交换必要密码编译参数以允许客户端和服务器对共享秘密(例如，预先主秘密)达成一致或计算。密码编译参数可包括根据所选择的密码的一组密钥或其它信息。举例来说，在这阶段交换的密钥可为客户端和服务器的公用密码密钥(李维斯特-沙米尔-阿德尔曼(Rivest-Shamir-Adleman)、迪菲-海尔曼(Diffie-Hellman)等)。这步骤可包括由客户端发射的ClientKeyExchange消息和/或由服务器发射的ServerKeyExchange消息。当将李维斯特-沙米尔-阿德尔曼(RSA)用于服务器认证和密钥交换时，预先主秘密由客户端产生，在服务器的公用密钥下加密，且发送到服务器作为ClientKeyExchange消息的部分。服务器然后使用其私用密钥解密预先主秘密。当使用迪菲-海尔曼时，每一侧根据协商的密钥计算其

自身的预先主秘密。

[0052] d)交换ChangeCipherSpec消息以指示每一发送方将此后使用达成一致的密码编译参数加密会话的传出消息。

[0053] e)交换结束(Finished)消息(ClientFinished和ServerFinished)以在形式上结束会话握手。为了允许客户端和服务器验证其对等体已接收到和/或计算正确的安全参数(例如,共享秘密)且握手在未受到攻击者篡改的情况下发生,对ClientFinished和ServerFinished消息加密。每一接收方必须尝试解密接收到的结束消息;成功解密指示成功握手。

[0054] 在TLS协议中,每一方根据在握手期间交换的密码编译参数计算主秘密,例如,根据预先主秘密和客户端与服务器供应的随机数。从主秘密,每一侧可接着判定一组会话密钥。术语"会话密钥"将在本文中用以一般表示用于加密和/或解密在当前会话期间的通信的密码编译参数值。示范性会话密钥包括预先主秘密、主秘密、客户端和服务器侧写入密钥、初始化向量/临时乱数和消息认证码(MAC),外加其它。在使用对称加密的实施例中,加解密处理密钥相同,因此知晓加密密钥满足解密。在非对称密码术中,加密与解密密钥不同。使用会话密钥的方式因此取决于协商的密码。

[0055] 本发明的一些实施例依赖于以下观测:在发出握手的结束消息前,用于在当前会话期间的加密的会话密钥必须由每一侧计算(否则不能加密相应消息)。此外,用于导出会话密钥的成份由每一侧接收为握手的部分,例如,作为ServerHello、ClientKeyExchange和ServerKeyExchange消息的部分。因此,会话密钥有可能在握手期间有时出现在客户端系统的存储器中。本发明的一些实施例使用握手的时序确定会话密钥的大致存储器位置。

[0056] 图5展示根据本发明的一些实施例的由自省引擎40执行的示范性步骤序列。在步骤序列502-504中,引擎40可与网络过滤器42合作以检测在客户端系统12到远程方(例如,图1中的内容服务器13)之间发射的握手消息。在一个实例中,连接请求可来自在客体VM 32内执行的应用程序(例如,浏览器),且可指示起始加密的通信会话(例如,TLS会话、SSH会话、VPN会话等)的意图。因而,连接请求可包括到服务器13的握手消息(例如,ClientHello)。在另一实例中,检测到的握手消息包括响应于从客户端系统12接收的ClientHello而发生的来自服务器13的消息(例如,ServerHello)。

[0057] 当检测到握手消息时,在步骤506中,自省引擎40可提取一组握手参数(例如,会话ID和密码的指示符)以用于会话。在监测TLS连接的实施例中,步骤506可进一步提取例如服务器和/或客户端供应的随机数的密码编译参数。自省引擎40可然后指导网络过滤器42将握手消息转发到其既定接收者VM(例如,图3中的客体VM 32)。

[0058] 在步骤508中,自省引擎40可获得客体VM 32的优化的存储快照。存储快照包括由相应VM使用的存储页面集的内容的复本。在一些实施例中,优化的快照包括最可能含有会话密钥的存储页面集的内容,或至少用以导出当前通信会话的会话密钥的密码编译参数值。用于获得优化的快照的示范性方法在以下进一步描述。

[0059] 步骤510可通过从网络过滤器42获得相应有效载荷的复本来采集当前会话的加密的有效载荷。在一些实施例中,网络过滤器42被配置成维持多个数据队列,例如,由会话ID和/或虚拟机索引。网络过滤器42可因此明确且一致地恢复会话的加密的有效载荷,甚至当将相应有效载荷划分成散布于其它通信当中的多个包。接下来,在步骤512中,自省引擎40

可将采集的优化的存储快照、握手参数和加密的有效载荷发射到安全服务器15供分析。

[0060] 图6展示由自省引擎40执行以获得客体VM 32的优化的存储快照的示范性步骤序列。为了导出会话密钥的大致存储器位置，本发明的一些实施例识别其内容已在时间间隔期间改变的存储页面集，所述时间间隔与产生相应会话密钥的时间大致重合。

[0061] 其内容最近已改变的存储页面(即，最近写入到的页面)可使用所属领域中已知的任何方法来识别。在一个实例中，自省引擎40可将由客体VM 32使用的存储页面集标记为在与客体VM 32相关联的SLAT数据结构中不可写入。修改此页面的内容的任何后续尝试将接着构成存储器存取违规，且因此触发处理器事件(例如，VM退出或虚拟化异常)，这将然后由自省引擎40和/或公用程序代理44拦截。响应于拦截所述事件，引擎40可将相应页面标记为可写入，且再次启动相应VM，以允许相应写入继续进行。以此方式，引擎40可结束于一列“页面重写标志”存储页面，其内容构成所要的优化的存储快照。

[0062] 以上情境相当低效且计算成本高。关于选定硬件平台的若干优化是可能的。举例来说，关于支持已存取的和/或页面重写标志位的平台，一些实施例可将由客体VM 32使用的存储页面的页表项(Intel®平台上的EPT项)的页面重写标志位复位，且在某一稍后时间检查页面重写标志位的值以确定相应页面是否已被写入。这机制可进一步优化。举例来说，Intel®处理器的某些产生拥有叫作页面修改记录(PML)的特征，其自动将其内容已改变的一列页面输出到存储器自省引擎40可存取的存储器位置。

[0063] 另一可能优化策略使用一些管理程序(例如，Xen®)用以有效地迁移和/或克隆虚拟机的动态迁移特征。围绕自动跟踪已被写入到的页面且根据时间表输出一列此类页面的一组日志-页面重写标志基元建造相应特征。

[0064] 图6中说明的步骤的序列识别已在第一种类的会话事件与第二种类的会话事件之间的时间间隔期间修改的页面。本文中的会话事件表示通信协议的各种阶段，例如，如上关于TLS协议所描述。示范性会话事件包括(例如)发送和/或接收形成特定通信会话的部分的消息(例如，在客户端系统12与服务器13之间发射的握手消息、含有相应会话的加密的有效载荷的部分的消息等)。第1种事件的检测(步骤522-524)接通页面修改监测(步骤526)。在一些实施例中，步骤526包括暂停客体VM 32的操作，重新设定对应于由客体VM 32使用的存储页面的SLAT项目的页面重写标志位，和重新启动客体VM 32。在一些实施例中，待针对写入监测的存储页面的集合可变窄，例如，变窄到由进行当前通信会话的过程(例如，浏览器)或由处置加密/解密(例如，Windows®中的LSASS.EXE)的过程使用的页面集。存储器自省引擎40可通过对由客体OS 34用以管理线程和过程的数据结构查核行程来识别由相应过程/应用程序使用的页面。可通过与在客体VM 32内执行的公用程序代理44合作而使识别此类存储页面的任务更容易——代理44通常能够存取比引擎40多得多的信息。

[0065] 在检测到第二种会话事件的发生(步骤528-530)后，例如，接收到相应会话的另一握手消息，那么切断针对写入的监测(步骤534)。步骤532可暂停客体VM 32的执行，以防止对存储器的修改在拍摄存储快照时发生。在步骤536-538的再一序列中，引擎40识别在第一与第二会话事件之间已被写入的页面，且将此类页面的内容的复本识别为优化的存储快照。在再一步骤540中，自省引擎40可重新启动客体VM 32。

[0066] 在替代性实施例中，在采集优化的存储快照的持续时间内不暂停客体VM 32的执行。此类暂停有可能使系统放慢，且影响用户体验。此外，出于安全目的，暂停客体VM 32可

能不合乎需要，这是由于其可能泄漏相应VM正被监测的实情。由于通常将会话密钥写入一次且会话密钥不在存储器中四处移动，因此不需要由客体VM 32使用的所有页面的一致性。人们必须简单地确保在复制脏页前当前会话不结束(且因此，密钥不变为零)。替代停止客体VM 32，一些实施例使用网络过滤器42操纵进入或离开客体VM 32的通信流。举例来说，过滤器42可在存储快照的采集的持续时间内延迟数据包从服务器13到客体VM 32的传递。延迟可对在客体VM 32内执行的软件显得为相当正常的网络等待时间。为了达成延迟功能性，一些实施例使用过程间通知机制在引擎40与网络过滤器42之间通信。举例来说，引擎40可响应于优化的存储快照的成功采集来通知过滤器42。又，过滤器42可响应于拦截到某些网络包(例如，ServerFinished消息的ServerHello)而通知引擎40。

[0067] 在观测到通常在会话的握手部分期间导出会话密钥后，本发明的各种实施例使用各种握手事件作为第1和第2种类的会话事件。举例来说，在一些实施例中，第1种类的事件(接通页面监测)包含由网络过滤器42进行的对网络包的拦截，所述网络包包括用于导出用于相应会话的会话密钥的成分。示范性成份包含随机数、密钥和共享秘密，外加其它。第1种类的一个此示范性会话事件是从服务器13接收的ServerHello消息。其它实施例可以使用。用于第1种类的事件的其它可能选择包含来自客体VM 32的ClientHello消息、ClientKeyExchange和ServerKeyExchange消息。至于第2种类的会话事件——切断页面监测，一些实施例使用由网络过滤器42进行的对发射到客体VM 32或从客体VM 32发射的经加密消息的拦截。第2种类的事件的一个实例是ClientFinished或ServerFinished消息的拦截。第2种类的另一可能选择事件是包括使用当前会话的会话密钥加密的有效载荷的部分的包的拦截。

[0068] 以上关于图5-6描述的示范性方法适用于单个通信会话。在实践中，可在单个VM内同时进行多个会话，例如，由浏览器的多个个例(如在标签式浏览中)，或由同时运行的截然不同的应用程序。一些实施例被配置成针对每一会话分开来跟踪脏页。为了清晰起见，以下描述将聚焦于采集TLS会话的存储快照的特定任务，每一快照包括在每一会话的ServerHello消息与相应会话的ClientFinished消息之间修改的存储页面。

[0069] 得到会话具体优化的快照造成了解开会话事件的任意序列的附加挑战。一些实施例配置页面监测机制以识别已写入到两个连续事件之间的所有页面。然而，此类事件可属于截然不同的会话，且可属于第一种类或第二种类(以借用以上关于图6使用的命名法)。为了说明此不明确性，自省引擎40的一些实施例维持当前作用中会话的全局列表，列表的每一项包括例如以下的信息：会话ID、源因特网协议(IP)地址、源端口编号、目的地IP地址、目的地端口编号和相应会话的ServerHello消息的时间戳。引擎40可进一步维持时间戳的全局阵列，从而存储用于每一监测的存储页面的至少一个时间戳。所述阵列的每一时间戳可指示相应页面已被写入的时刻。出于这个原因，时间戳阵列将在本文中被视为页面修改时间戳阵列。

[0070] 图7展示在被配置成跟踪多个同时TLS会话的实施例中由存储器自省引擎执行的示范性步骤序列。步骤552初始化页面修改时间戳阵列。步骤552可进一步包括配置页面修改检测机制(例如，PML、复位页面重写标志位等)。步骤554-556的序列收听问候或结束种类的事件。当检测到事件时，在步骤558中，自省引擎40可调用页面修改检测机制以识别当前脏页，即，自从先前检测到的事件以来内容已改变的存储页面，这与其是是问候还是结束消

息无关。步骤560可然后更新页面修改时间戳阵列，使得将对应于脏页的时间戳更新到当前时间戳，或更新到指示当前检测到的事件的发生的时间戳。当相应事件属于第1种类(例如，ServerHello)时，在步骤564中，引擎40可初始化新会话数据结构，从而填充会话ID、源和目的地IP地址和端口，外加其它。再一步骤566记录指示当前ServerHello事件的时间戳，其将在本文中被视为相应会话的问候时间戳。

[0071] 当当前检测到的事件属于第2种类(例如，ClientFinished)时，在步骤570中，自省引擎40可对页面修改时间戳阵列查核行程。对于每一页面，一些实施例可比较相应页面的页面修改时间戳与相应会话的(即，当前检测到的事件所属的会话的)问候时间戳。当修改时间戳指示已在相应会话的问候事件后写入到相应页面时，引擎40可包含到相应会话的优化的存储快照内的相应页面。

[0072] 图8展示根据本发明的一些实施例的在包含解密引擎60的安全服务器15上执行的示范性软件。对于每一监测的通信会话，引擎60可接收来自相应客户端系统(例如，图1中的客户端系统12a-d)的会话数据，例如，一组握手参数72、优化的存储快照70和/或加密的有效载荷74。此数据可进一步包括明确地使每一项目与特定客户端系统、VM和/或通信会话相关联的指示符。握手参数72可包括用以加密有效载荷74的密码的指示符。优化的存储快照70包括如上所述的客户端系统的存储页面的内容的复本。有效载荷74包括加密通信的部分(例如，网络包)。

[0073] 图9展示根据本发明的一些实施例的由解密引擎60执行的示范性步骤序列。响应于接收到来自客户端系统12的会话数据(步骤582)，在步骤584中，引擎60可从会话数据提取在相应会话中使用的密码的指示符。解密引擎60可然后根据密码选择解密程序/算法。接下来，循环重复步骤586-588-590的序列，直到满足完成条件，例如，直到达成有效载荷的成功解密，或直到分配用于解密的时间周期到期。

[0074] 对解密有效载荷的尝试可根据在密码术的所属领域中已知的任何方法继续进行。用于采集优化的存储快照的程序经精心制作，使得会话密钥或至少用以导出用于相应会话的加密与解密密钥的密码编译参数值有可能驻留在相应存储快照内。会话密钥的字节大小可先验已知，或可从接收自客户端系统12的加密参数导出。然而，在快照内的会话密钥的精确位置可能不为所知。一些实施例可因此以试差方式搜索密钥材料。在图9中说明的一个此实例中，步骤586可从优化的存储快照导出候选解密密钥。在使用对称密码术(例如，TLS协议)的实施例中，加密与解密密钥相同，因此，候选解密密钥可包括(例如)快照的一连串字节，所述序列具有所需的字节大小。在步骤588中，引擎60可尝试使用候选密钥解密相应会话有效载荷的至少一部分。可以使用所属领域中已知的各种方法评估成功。举例而言，一些实施例计算经解密消息的信息熵。低熵通常指示成功的解密，但此类方法已知会产生错误肯定或错误否定。

[0075] 替代性解密方法使用在所属领域中被称为已知明文攻击的方法。一个此实施例采用以下事实：解密引擎60能够存取已知消息的经加密型式，例如，能够存取在所述会话期间交换的(经加密)ClientFinished和/或ServerFinished消息的内容。此类消息的格式和明文先验已知，记录在TLS协议中。

[0076] 本发明的一些实施例允许解密客户端系统与远程方之间的一些或所有通信。此类通信的实例包含使用对称或不对称密钥算法加密的任何通信，所述算法包含安全套接层

(SSL)/传输层安全(TLS)连接、安全外壳(SSH)、虚拟专用网络(VPN)连接和洋葱路由/匿名网络连接(例如,TOR软件)。所公开方法的示范性应用包含恶意软件的检测和分析、入侵检测和监视,外加其它。

[0077] 在一个示范性应用中,托管解密系统的至少一部分的计算机系统形成蜜罐系统的部分。蜜罐通常被配置成允许安装恶意软件,和/或允许入侵者控制相应计算机系统的一些方面。恶意软件和入侵者可然后使用加密的信道与例如命令和控制(C&C)服务器的外侧实体通信。通过实现此类通信的解密,一些实施例可有助于对恶意软件、入侵和/或黑客攻击方法的研究。

[0078] 一些实施例的另一示范性反恶意软件使用包括在其渗透客户端系统前检测恶意内容。在一些先进的恶意软件攻击情境中,恶意软件代理经由与另外良好服务器的加密通信而到达客户端,例如,经由电子邮件(钓鱼)或在线广告。由于加密,因此通常直到代理已解封装且将自身安装于主机上,或甚至直到稍后当其执行一些恶意软件指示动作时,它才能被检测到。本发明的一些实施例可以允许此类代理的早先检测和功能丧失。

[0079] 在另一示范性应用中,云服务提供商可使用一些实施例准实时地检验加密的流量,和快速检测循环到其服务器或从其服务器循环的恶意数据。此检测可防止相应服务器充当用于恶意攻击(例如,分布式拒绝服务(DDOS)攻击)的启动板。

[0080] 加密通信的解密为非常困难的事。破坏加密的一些常规方法尝试完全避免解密。此类方法包含(例如)修改加密库以提供额外信息,或引入允许用户不太显眼地获得对相应通信的明文或对实际加密密钥或对有益于密钥的一些其它信息的存取的“后门”。此类方法被看作是危险的,这是由于从长远看来,它们可削弱因特网安全性。它们也因通常为非便携式(即,仅在某些硬件平台和/或操作系统上有效)而不方便。另一不便是,对密码编译库的修改对在相应客户端上执行的软件可见,且可因此被检测到和抵消。

[0081] 现代密码可仅使用强行攻击的某一型式来破坏,这通常携带着大的计算成本。一个此攻击包括试验多个候选密钥,直到一个最终起作用。一些常规解密系统/方法搜索在客户端系统的存储器内的密钥材料。然而,由于对于搜索所需的巨大计算花费,不知道密钥材料的实际位置可使此类方法不切实际。此外,在获取大存储器信息转储所需的时间内停止相应机器有可能负面地影响用户体验。一些常规方法尝试通过设定“分接头点”来优化对密钥材料的搜索,以便在某些执行时刻获得存储器信息转储。然而,分接头点被预定义,且因此如果更新基础系统和/或通信软件,那么分接头点可破坏。

[0082] 本发明的一些实施例依赖于两个密钥观测结果。首先,潜在地受益于解密的大量客户端系统在硬件虚拟化配置(虚拟机)中执行。实例包含服务器场和虚拟桌面基础设施的云提供商。为了利用此类配置,本发明的一些实施例将自省引擎放置于在公开相应VM的管理程序的处理器特权等级下进行加密通信的虚拟机外。自省引擎可使用虚拟化的所属领域的技术存取和检验由相应VM使用的存储器的内容,潜在地不知道在相应VM内执行的软件或无来自所述软件的干扰。单个自省引擎可因此不太明显地监测由在相应客户端系统上同时执行的多个VM进行的通信。

[0083] 第二观测结果是,加密密钥或至少用以导出相应密钥的密码编译参数由通信伙伴在会话的具体阶段期间(例如,在握手期间)交换。一些实施例使用此观测结果导出会话密钥的大致位置,因此允许存储器搜索面积从常规方法中的数百个兆字节到数个存储页面

(例如,数十个千字节到数个兆字节)的减小。这大体上减少了解密的计算精力,从而使强行攻击可行。

[0084] 一些实施例使用现代处理器的硬件优化(例如,在页表项内设定存取和/或脏旗标的能力,或一些Intel®处理器的页面修改记录(PML)特征),以识别其内容在包含会话密钥的交换和/或产生的时间间隔期间改变的一组存储页面。一些实施例接着搜索在相应存储页面的内容内的密钥材料。

[0085] 通过根据通信协议的特征定位会话密钥,而非依赖于客户端系统/虚拟机的具体硬件或软件特征,一些实施例实现在各种装置(个人计算机、移动电话、家用电器等)上以及在执行多个异质虚拟机的客户端系统中的通信的解密,与操作系统和通信应用程序(例如,浏览器、消息传递应用程序、VPN软件等)无关。

[0086] 为了避免由在监测的VM内执行的软件检测,一些实施例将由采集相应VM的优化的存储快照造成的偶然延迟伪装为网络等待时间。在一个实例中,自省引擎与网络过滤器合作以在存储快照的获取的持续时间内延迟将某些网络包传递到监测的VM。对于在VM内部执行的软件,此类延迟可显得是由网络上的发射问题造成。并且,为了避免影响用户体验,一些实施例将解密的计算负担分担到单独的机器(安全服务器)上。因此可离线进行实际解密。

[0087] 所属领域的技术人员将清楚,在不脱离本发明的范围的情况下,以上实施例可以以多种方式更改。因此,应通过所附权利要求书和其合法等效内容来确定本发明的范围。

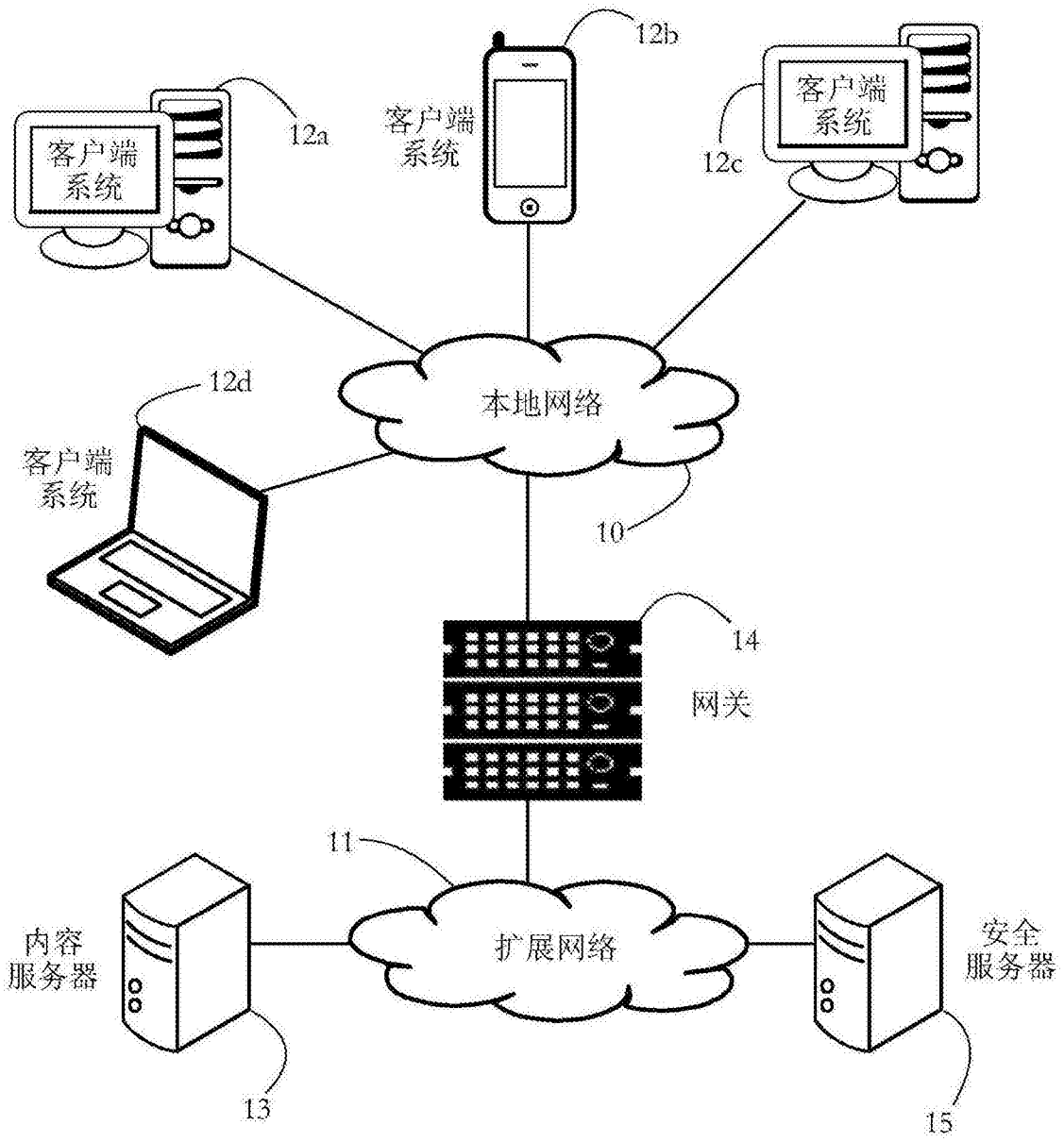

客户端
系统
12a
客户端
系统
12b
客户端
系统
12c
客户端
系统
12d
本地网络
10
14
网关
11
扩展网络
内容
服务器
13
安全
服务器
15

图1

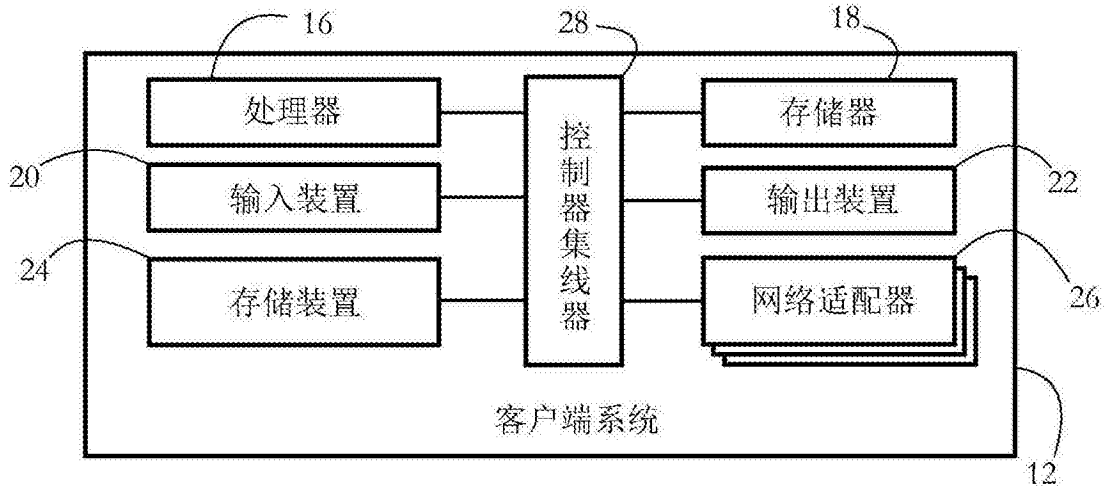

16
28
18
处理器
控制器集线器
存储器
20
输入装置
输出装置
22
24
存储装置
网络适配器
26
客户端系统
12

图2-A

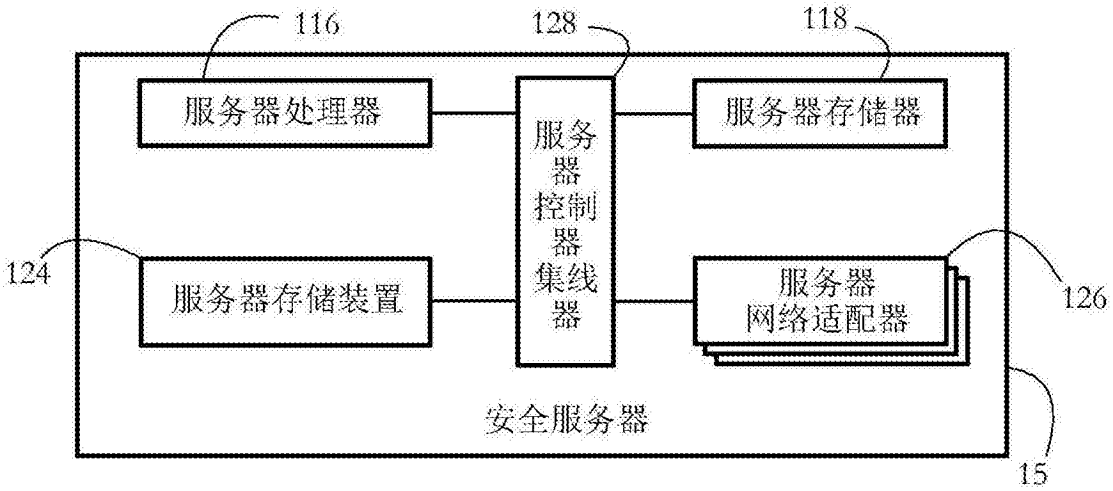

116
128
118
服务器处理器
服务器控制器集线器
服务器存储器
124
服务器存储装置
服务器网络适配器
126
安全服务器
15

图2-B

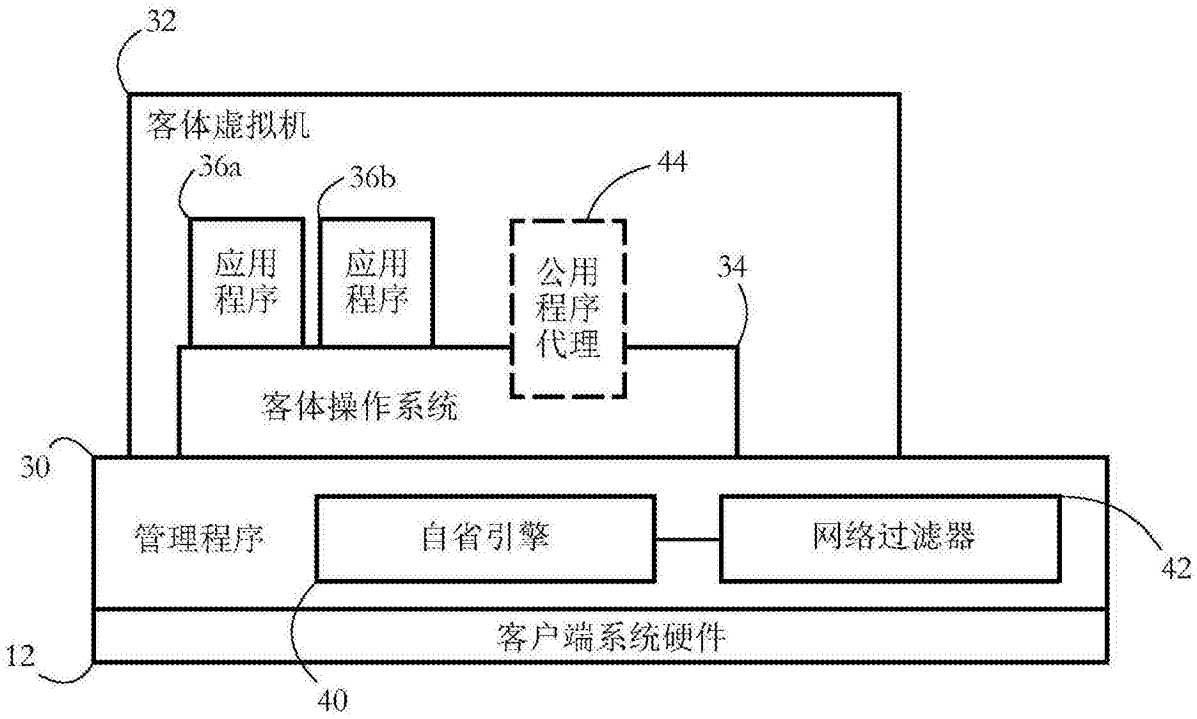

32
客体虚拟机
36a
36b
44
应用程序
应用程序
公用程序代理
34
客体操作系统
30
管理程序
自省引擎
网络过滤器
42
客户端系统硬件
12
40

图3

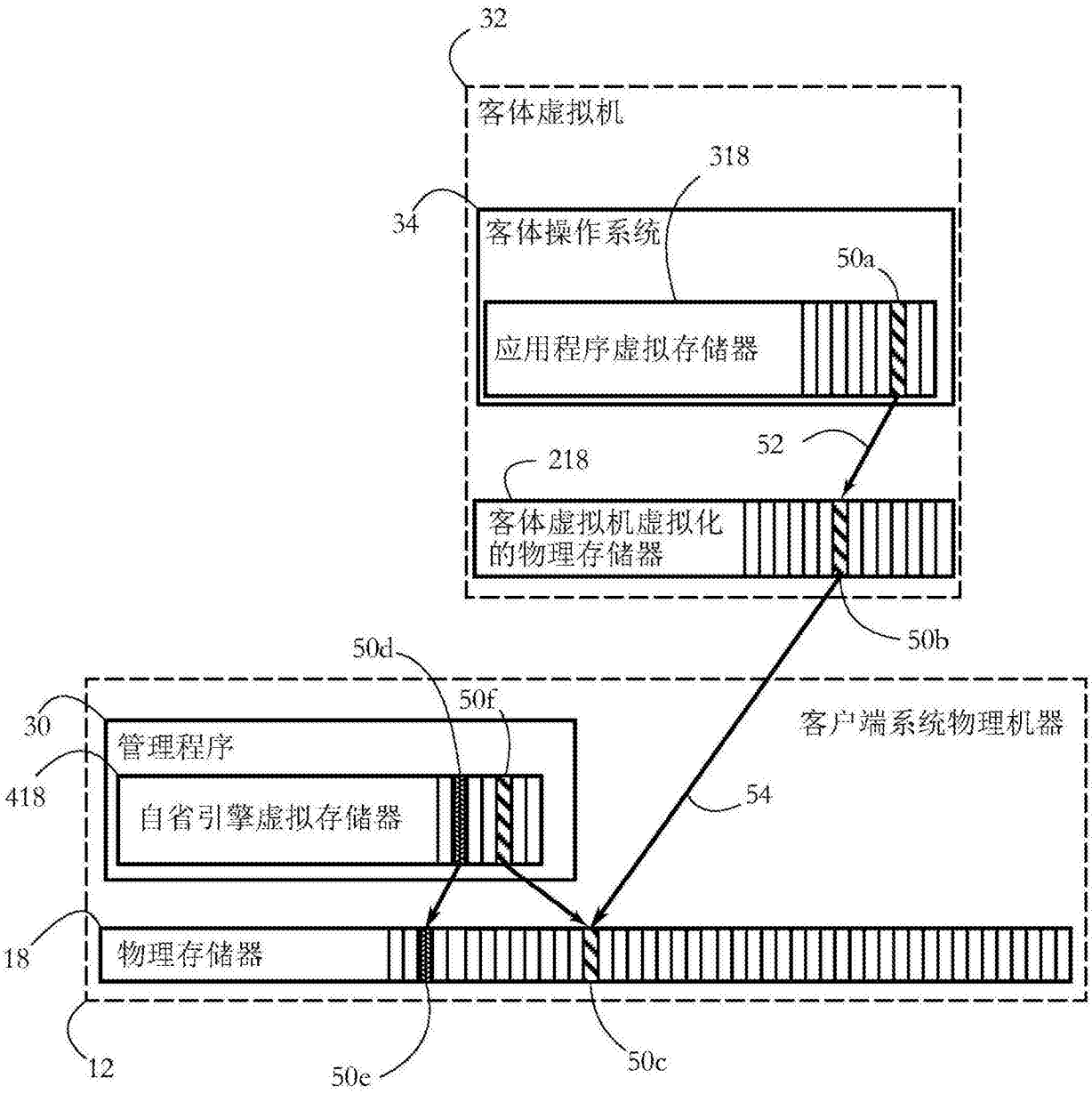

32
客体虚拟机
318
34
客体操作系统
50a
应用程序虚拟存储器
52
218
客体虚拟机虚拟化的物理存储器
50b
50d
50f
30
管理程序
客户端系统物理机器
418
自省引擎虚拟存储器
54
18
物理存储器
12
50e
50c

图4

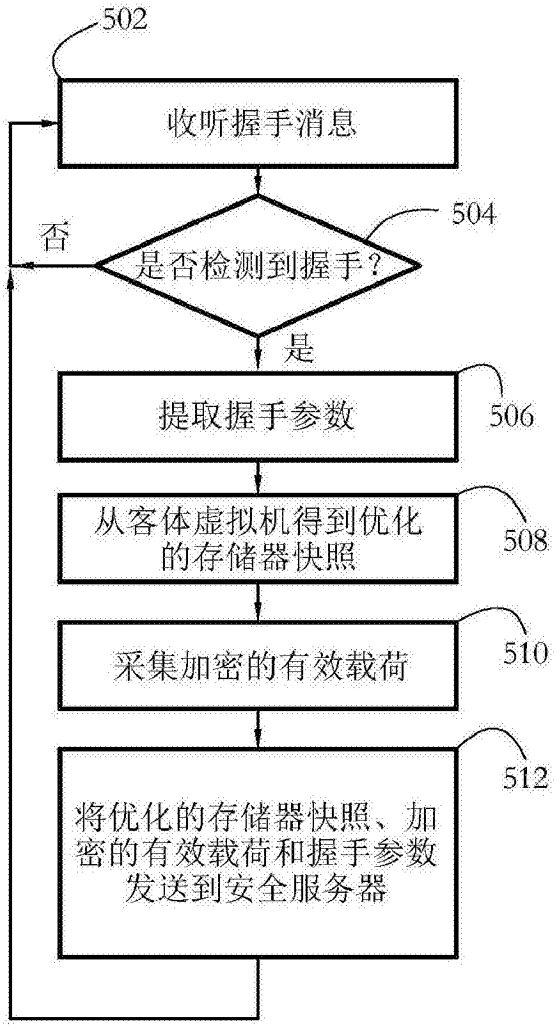

502
收听握手消息
504
否
是否检测到握手？
是
提取握手参数
506
从客体虚拟机得到优化的存储器快照
508
采集加密的有效载荷
510
512
将优化的存储器快照、加密的有效载荷和握手参数发送到安全服务器

图5

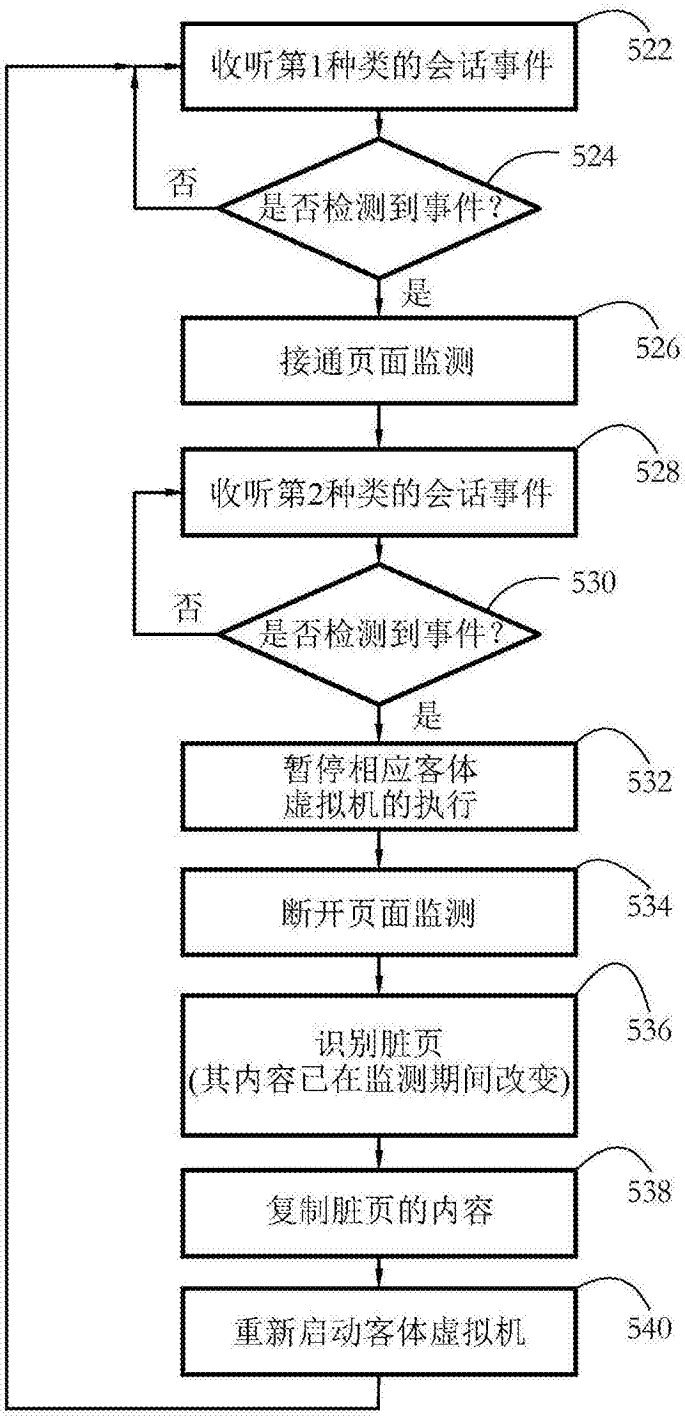

收听第1种类的会话事件
522
是否检测到事件?
524
否
是
接通页面监测
526
收听第2种类的会话事件
528
是否检测到事件?
530
否
是
暂停相应客体
虚拟机的执行
532
断开页面监测
534
识别脏页
(其内容已在监测期间改变)
536
复制脏页的内容
538
重新启动客体虚拟机
540

图6

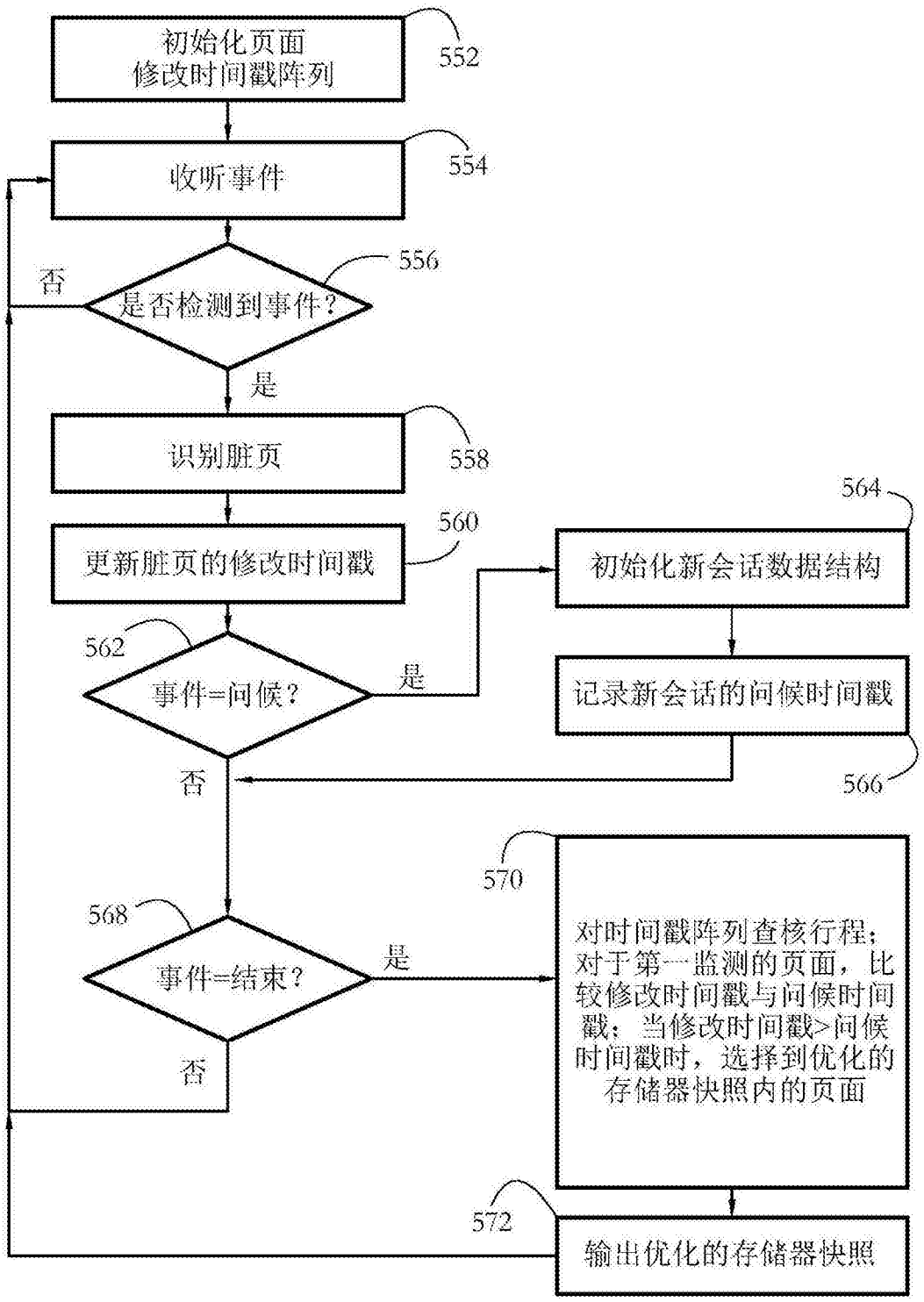

初始化页面
修改时间戳阵列
552
收听事件
554
否
是否检测到事件？
556
是
识别脏页
558
更新脏页的修改时间戳
560
562
事件=问候？
是
否
564
初始化新会话数据结构
记录新会话的问候时间戳
566
570
568
事件=结束？
是
否
对时间戳阵列查核行程；对于第一监测的页面，比较修改时间戳与问候时间戳；当修改时间戳>问候时间戳时，选择到优化的存储器快照内的页面
572
输出优化的存储器快照

图7

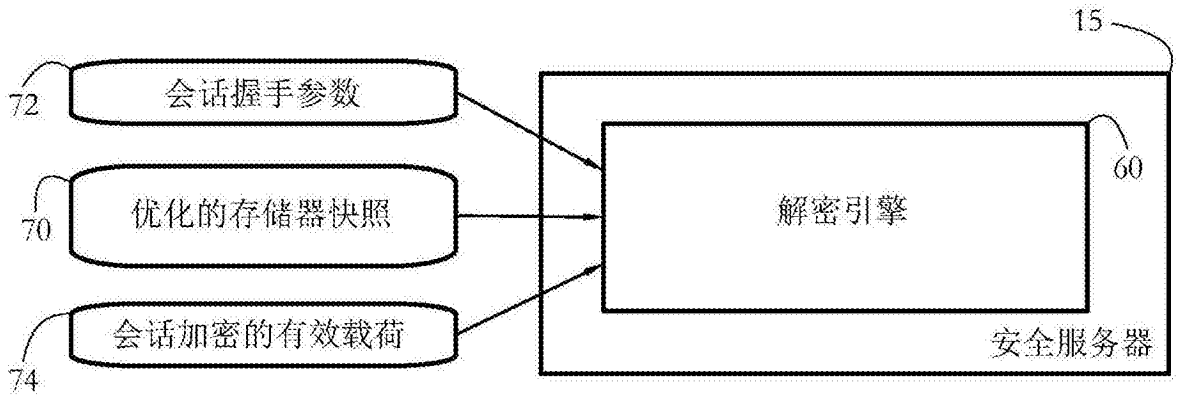

15
72
会话握手参数
70
优化的存储器快照
74
会话加密的有效载荷
解密引擎
60
安全服务器

图8

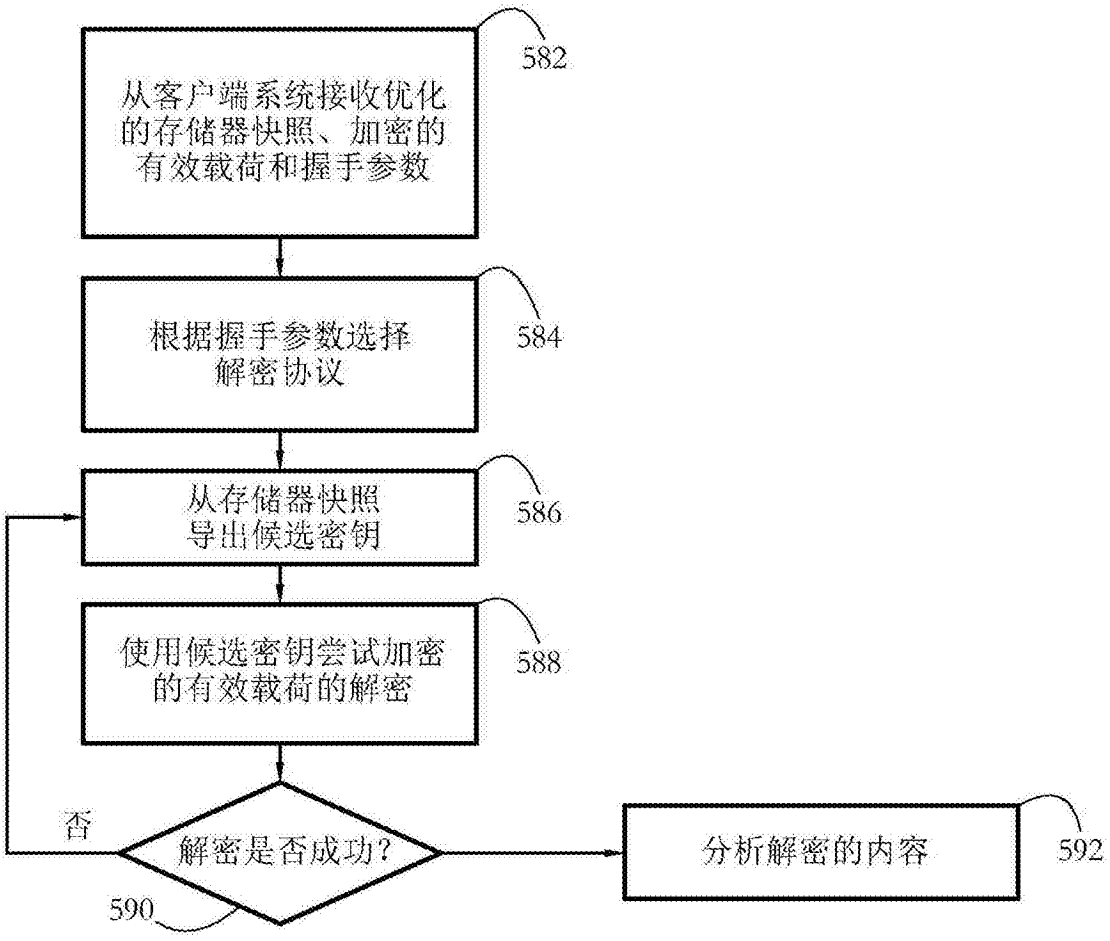

582
从客户端系统接收优化的存储器快照、加密的有效载荷和握手参数
584
根据握手参数选择解密协议
586
从存储器快照导出候选密钥
588
使用候选密钥尝试加密的有效载荷的解密
否
解密是否成功?
590
分析解密的内容
592

图9