[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/22 (2006.01)
G06F 21/00 (2006.01)
G06F 9/06 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200780035702.1

[43] 公开日 2009 年 8 月 26 日

[11] 公开号 CN 101517591A

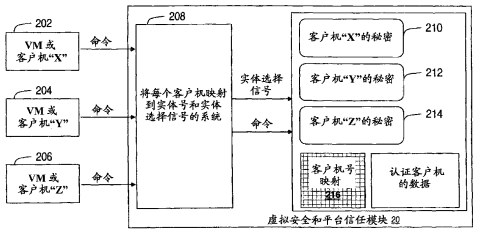
[22] 申请日 2007.9.26
[21] 申请号 200780035702.1
[30] 优先权
[32] 2006. 9.29 [33] US [31] 11/529,987
[86] 国际申请 PCT/US2007/020797 2007.9.26
[87] 国际公布 WO2008/042191 英 2008.4.10
[85] 进入国家阶段日期 2009.3.26
[71] 申请人 英特尔公司
地址 美国加利福尼亚州
[72] 发明人 D·M·奥康诺 J·P·布里泽克
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 朱海煜 王丹昕
权利要求书 3 页 说明书 6 页 附图 3 页

[54] 发明名称

虚拟安全模块的体系结构

[57] 摘要

一种装置支持通过安全识别并区分客户机发出的命令的映射系统来处理处理器中的多个活动应用。 映射系统生成实体选择信号以通知处理器处理算法并使用识别的该客户机的命令和客户机跟踪系统所允许的用于该客户机的数据来向该特定客户机提供服务。 当处理算法时，限制对其他客户机识别的命令和其他数据访问。



1.一种具有认证能力的处理系统，包括:

第一客户机和第二客户机;

映射装置，用于接收由第一客户机和第二客户机发出的命令并生成将由第一客户机发出的命令从由第二客户机发出的命令中唯一识别出来的信号；以及

能够为第一客户机和第二客户机访问存储数据的处理装置，其中，通过识别为来自第一客户机的命令所请求的操作局限于与之前指定给第一客户机的权利相关的数据，并且通过识别为来自第二客户机的命令所请求的操作局限于与之前指定给第二客户机的权利相关的数据。

2.如权利要求 1 所述的处理系统，其中所述唯一识别命令的信号是专用信号。

3.如权利要求 1 所述的处理系统，其中所述用于接收由第一客户机和第二客户机发出的命令的映射装置与所述处理装置嵌入在一起。

4.如权利要求 1 所述的处理系统，其中所述处理系统还包括通过空中信号进行接收的收发器。

5.如权利要求 1 所述的处理系统，其中所述与之前指定给第一客户机的权利相关的数据包括为第一客户机预留的秘密。

6.一种支持处理器中的多个活动应用的方法，包括:

将由第一客户机发出的命令从由其他客户机发出的命令中识别出来；以及

使用为第一客户机识别的、访问客户机跟踪系统所允许的用于第一客户机的数据的命令来为第一客户机处理算法，同时在处理所述算法时，限制对数据的访问，并限制执行为其他客户机识别的命令。

7.如权利要求 6 所述的方法，其中将由第一客户机发出的命令从由其他客户机发出的命令中识别出来还包括生成实体选择信号以识

别第一客户机。

8.如权利要求 7 所述的方法，还包括：在使用所述命令处理所述算法之前，使用所述实体选择信号来识别第一客户机。

9.如权利要求 6 所述的方法，其中所述处理器还包括通过使用所述实体选择信号区分第一客户机的命令和对数据的访问来同时处理所述多个活动应用。

10.一种装置，包括：

跟踪系统，用于将客户机发出的命令与用于在执行与所述客户机关联的应用的操作时限制命令和对数据的访问的实体选择信号进行链接。

11.如权利要求 10 所述的装置，其中所述跟踪系统还使得能够根据所述实体选择信号访问数据和命令。

12.如权利要求 10 所述的装置，其中所述跟踪系统支持通过将由所述客户机发出的命令从由其他客户机发出的命令中识别并区分出来的映射系统来处理处理器中的多个活动应用。

13.如权利要求 10 所述的装置，其中所述映射系统还包括所述客户机与秘密之间的映射关联以允许多个客户机同时与一组相同的秘密关联。

14.如权利要求 10 所述的装置，其中相同程序的多个实例在不同的虚拟机下运行，并且单个虚拟机与多组秘密关联。

15.一种处理系统，包括：

第一虚拟机和第二虚拟机；

映射装置，用于将第一实体选择信号与由第一虚拟机发出的命令关联并将第二实体选择信号与由第二虚拟机发出的命令关联；以及

处理装置，用于接收第一实体选择信号并执行由第一虚拟机发出的命令，并且使得能够在执行与第一虚拟机关联的应用的操作时访问数据并限制对与第二虚拟机关联的命令和数据的访问。

16.如权利要求 15 所述的处理系统，其中所述处理装置接收第二

实体选择信号并执行由第二虚拟机发出的命令，并且使得能够在执行与第二虚拟机关联的应用的操作时访问数据并限制对与第一虚拟机关联的命令和数据的访问。

17.如权利要求 15 所述的处理系统，还包括映射系统，用于生成识别第一虚拟机的第一实体选择信号和识别第二虚拟机的第二实体选择信号。

虚拟安全模块的体系结构

背景技术

用于商业和贸易的相连移动计算和无线通信技术需要保护用户数据和秘密。体系结构可包括执行数字签名和密钥包装操作、散列操作和随机数生成的安全引擎，其中硬件和支持软件提供加密和解密能力以确保数据保密和增强的安全性。

这些系统中的体系结构限制了秘密的使用，使得只有经过授权的应用才能使用特定的秘密，但是目前使用秘密的每个命令都要经过密码授权检验。这就需要一种机制能够支持同时执行的多个活动应用而无需对每个命令检验授权。

附图说明

在说明书的结论部分中特别指出本发明的主题并清楚地对本发明的主题要求权利。然而，通过参考附图阅读下面的详细描述，可最佳地理解本发明的组织和操作方法及其目标、特征和优点，在附图中：

图 1 是示出根据本发明支持同时执行的多个活动应用的虚拟安全和平台信任模块的无线装置的实施例的图；

图 2 是示出根据本发明用于区分并保护客户机秘密的映射系统的框图；

图 3 是示出根据本发明识别由特定客户机发出的命令并为该客户机处理访问存储器数据的算法的方法的流程图。

将意识到，为了简单和清楚地说明，附图中示出的元件并不一定按比例绘制。例如，为了清楚起见，其中一些元件的尺寸可相对于其他元件有所夸大。而且，在认为合适的情况下，在附图中重复使用附图标记，以指示对应或类似的元件。

具体实施方式

在下面的详细描述中，阐述了多个具体细节以便充分理解本发明。然而，本领域的技术人员将理解，无需这些具体细节也可实现本发明。在其他情况下，未详细描述众所周知的方法、过程、组件和电路，以免使本发明含混不清。

如图 1 所示，可在装置 10 中示出本发明的实施例，装置 10 包括允许在 RF/位置空间中与其他装置通信的无线电。因此，装置 10 可以是拥有标准化操作系统并能在各种应用之间处理多项任务且能在无线网络中操作的诸如智能电话的通信装置，但应该理解，本发明也可结合在除无线装置之外的装置中。

图 1 示出从一个或多个天线接收并发送调制信号的收发器 12。处理器 14 接收下变频滤波信号，将其转换为基带数字信号。处理器 14 通常处理用于提取指令、生成解码、查找操作数、并执行适当动作的算法函数，然后存储结果。处理器 14 可使用多个核 16 和 18 来计算基带和应用处理函数，其中可在这些核之间共享处理工作负荷。处理器 14 可通过存储器接口 22 将数据传送到系统存储器 24，系统存储器 24 可包括诸如随机存取存储器（RAM）、只读存储器（ROM）和非易失性存储器的存储器组合，但系统存储器 24 中包含的存储器的类型和种类都不是对本发明的限制。

装置 10 采用虚拟安全和平台信任模块 20，该模块 20 包括配置成执行密码功能的硬件和用于保护秘密免受攻击者侵害的软件。一般而言，模块 20 可创建、存储和管理密码密钥，执行数字签名操作，并锚接密钥和数字证书的信任链。因此，模块 20 提供各种服务以保护文件和文件夹的安全并保护对用户信息、用户名、密码和个人信息的存储和管理的安全。

图 2 示出根据本发明在虚拟机（VM）或安全域（SD）与属于特定客户机的各组秘密之间创建关联的模块 20 的一部分。VM 可以是利用有关网络的普通规则和过程来管理的一组处理核或处理装置。而且，VM 或域可以是具有使得能够执行任务的资源的软件实体。

图 2 示出用于将由客户机发出的命令与经生成用于识别具有这

些命令的该客户机的实体选择信号进行映射的映射系统208。然后，可将命令和实体选择信号传送到一起执行服务的各个硬件和软件组件的配置中。虚拟机或客户机202、204或206可将命令发出到平台特有的指示中以用于信息流和访问控制。例如，一旦客户机“X”202发出命令，映射系统208便接收该命令并生成实体选择信号以清楚地识别该命令与客户机202。然后，利用命令和实体选择信号来配置受保护的执行环境以便仅使用指定给客户机“X”的秘密210来执行算法并执行计算。诸如客户机“Y”的秘密212和客户机“Z”的秘密214的其他秘密属于其他客户机（分别为客户机“Y”204和客户机“Z”206），并且受到限制而不可用于为客户机“X”202执行的算法和计算。

因此，装置10是具有认证能力以支持多个活动应用的处理系统。映射系统208接收由多个客户机202、204和206发出的命令，将这些命令以及将这些命令具体识别为与该客户机关联的实体选择信号一起传送到处理装置。然后，可执行操作，这些操作专用于由实体选择信号所识别的客户机。而且，针对所识别的客户机的操作限于使用与之前指定给该客户机的权利相关的命令和存储的数据。与指定给其他客户机的权利相关的存储的数据是受限的数据并且不可用。

图2示出使用实体选择信号和来自由该信号所识别的客户机的命令来为所请求的服务提供安全和操作管理的客户机号映射块216。映射系统208与客户机号映射216合作通过使得能够灵活部署安全服务来简化大分布式系统中的信任管理。通过仅准许由映射系统208识别且由客户机号映射216启用的特定客户机访问那些秘密，来维护并保护专用于各个客户机的秘密的集合。

装置10中的虚拟安全和平台信任模块20设计为在处理服务之前向为特定客户机预留的秘密提供明确且自主的保护。解除了应用开发者针对为服务处理发出的每个命令实现和验证安全相关的密码验证功能的负担。并不是按用户或按系统单独指定，而是要运行的应用或服务维护虚拟机或安全域与发送给该装置的所有随后命令的指定一

组秘密之间的关联，直到将应用与这些秘密分离为止。

图 3 是根据本发明的多个实施例示出根据本发明识别由特定客户机发出的命令并为该客户机处理访问存储器数据的算法的方法的流程图。因此，可在支持多个虚拟机或多个安全域的计算机系统中使用方法 300，以保护允许应用使用的秘密。方法 300 安全地维护虚拟机或安全域与发送给处理装置的所有随后命令的指定一组秘密之间的关联，直到将应用与这些秘密分离为止。

在一些实施例中，方法 300 或其部分由控制器、处理器或电子系统（其实施例如各图所示）执行。方法 300 不限于由特定类型的设备、软件元素或系统来执行该方法。方法 300 中的各个动作可按示出的顺序执行，也可按不同的顺序执行。而且，在一些实施例中，方法 300 可省去图 3 中列出的一些动作。

图中示出方法 300 从方框 302 开始，在方框 302，监视器块（例如图 1 中所示的映射系统 208）监视从多个虚拟机或多个安全域发出的命令。源自客户机的命令被识别为是由那些特定客户机发出的。在方框 302 执行的方法生成实体选择信号以识别正在其中运行应用的 VM/SD，并在每次将命令发送到装置时将该标识传送到外围装置。将标识符提供给装置中的客户机号映射 218。

方框 304 示出装置使用为该客户机识别的命令为该客户机处理算法。可访问存储在高速缓存和系统存储器中的数据，但是存储在存储器中的秘密仅可按客户机跟踪系统（客户机号映射 218，见图 2）所允许的来进行访问。映射系统 208 和客户机号映射 218 对资源进行控制以允许从操作系统（OS）或管理程序到装置的关于应当允许应用使用装置中的哪些秘密和哪些命令的安全通信。方框 306 示出，通过维护 VM 或 SD 与发送给装置的所有随后命令的指定一组秘密之间的关联，直到将应用与这些秘密分离为止，而防止应用使用可能危及系统安全性的秘密。

在操作中，处理器中的硬件可包括唯一地识别每个 VM 或 SD 的状态位。在一些处理器中，这可以是进程标识符（PID）或地址空间

标识符（ASID）。当在 VM 或 SD 中运行的应用向外围设备发送命令时，处理器硬件将信号发送到外围设备，以通知外围设备哪个 VM 或 SD 正在发送命令。该信令可通过由处理器输出的专用信号或通过将信息编码到诸如地址总线的其他信号中来实现。然后，外围设备可确保所发送的命令和用于执行这些命令的数据对于发送命令的 VM 或 SD 是适合的。

从一个运行到下一个运行，与运行特定应用的 VM 或 SD 相关联的标识符可能会改变，所以提供从 SD/VM 标识符到一组秘密的动态映射。当启动使用秘密的应用时，OS（或管理程序）首先认证应用，以检查其完整性及其标识。一旦认证了应用，则 OS 将 VM/SD 标识符和对该应用的该组相关联的存储秘密和该组允许的操作的使用解除锁定的令牌传送到外围设备。当停止或暂停应用时，OS 将另一个命令发送到外围设备以取消关联。应用也可自己结束关联，但是仅为其本身结束在适当位置的关联。OS 可包括专用 VM/SD 标识符，硬件使用该标识符以便仅 OS 可发送命令来将 VM/SD 标识符与一组秘密关联。

应指出，外围设备可同时存储 VM/SD 和秘密之间的多个关联。还可将多个 VM 或 SD 同时与相同一组秘密关联。当相同程序的多个实例在不同的 VM 或 SM 下运行时，以及单个 VM 或 SD 与多组秘密关联时，可能存在这种情况。

现在，很显然，已经提供了支持在处理器中处理多个活动应用的电路和方法。本发明的实施例通过将由第一客户机发出的命令从由其他客户机发出的命令中识别出来的映射系统、结合软件将安全性向下推至硬件级。由映射系统生成的实体选择信号用信号通知处理器使用为第一客户机识别的命令和客户机跟踪系统针对第一客户机所允许的数据来为第一客户机处理算法。当处理算法时，限制为其他客户机识别的其他数据访问和命令。

虽然本文说明和描述了本发明的某些特征，但本领域的技术人员现在可联想到许多修改、替换、变化及等效物。因此，应理解，所附

权利要求要涵盖落在本发明的真正精神内的所有此类修改和变化。

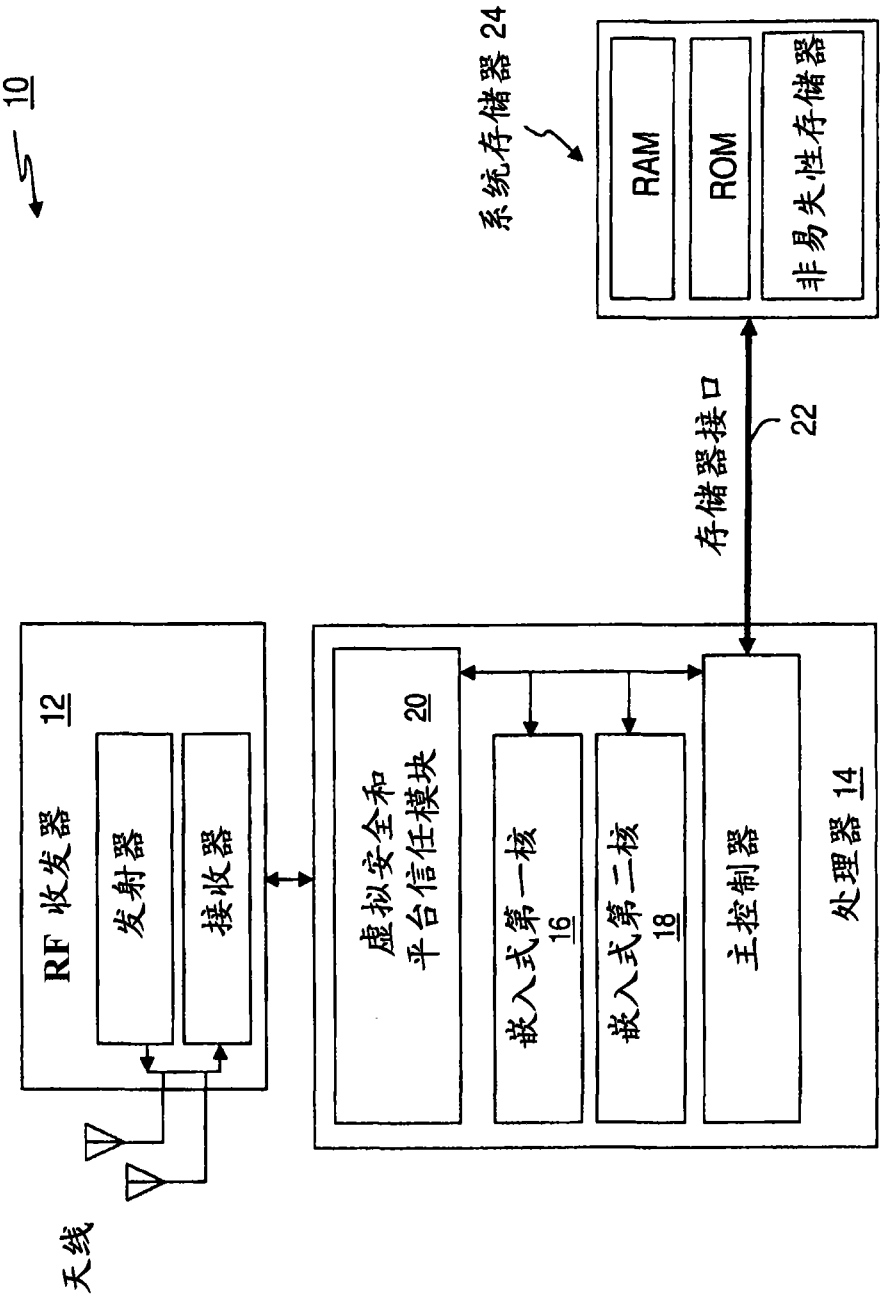

10
系统存储器 24
RAM
ROM
非易失性存储器
存储器接口
22
RF 收发器 12
发射器
接收器
虚拟安全和平台信任模块 20
嵌入式第一核 16
嵌入式第二核 18
主控制器
处理器 14
天线

图 1

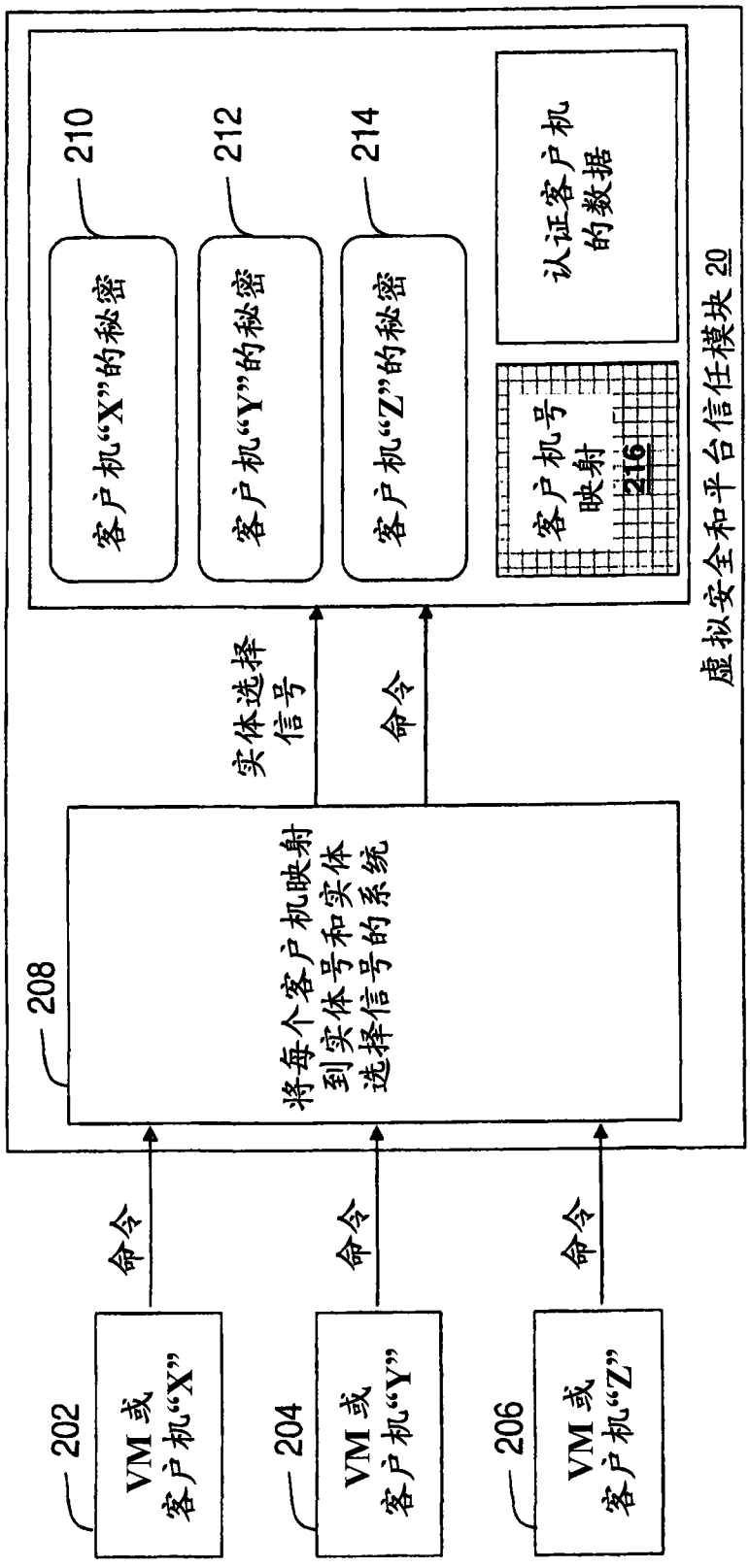

202
VM 或
客户机“X”
204
VM 或
客户机“Y”
206
VM 或
客户机“Z”
命令
命令
命令
208
将每个客户机映射
到实体号和实体
选择信号的系统
实体选择
信号
命令
虚拟安全和平台信任模块 20
210
客户机“X”的秘密
212
客户机“Y”的秘密
214
客户机“Z”的秘密
认证客户机
的数据
客户机号
映射
216

图 2

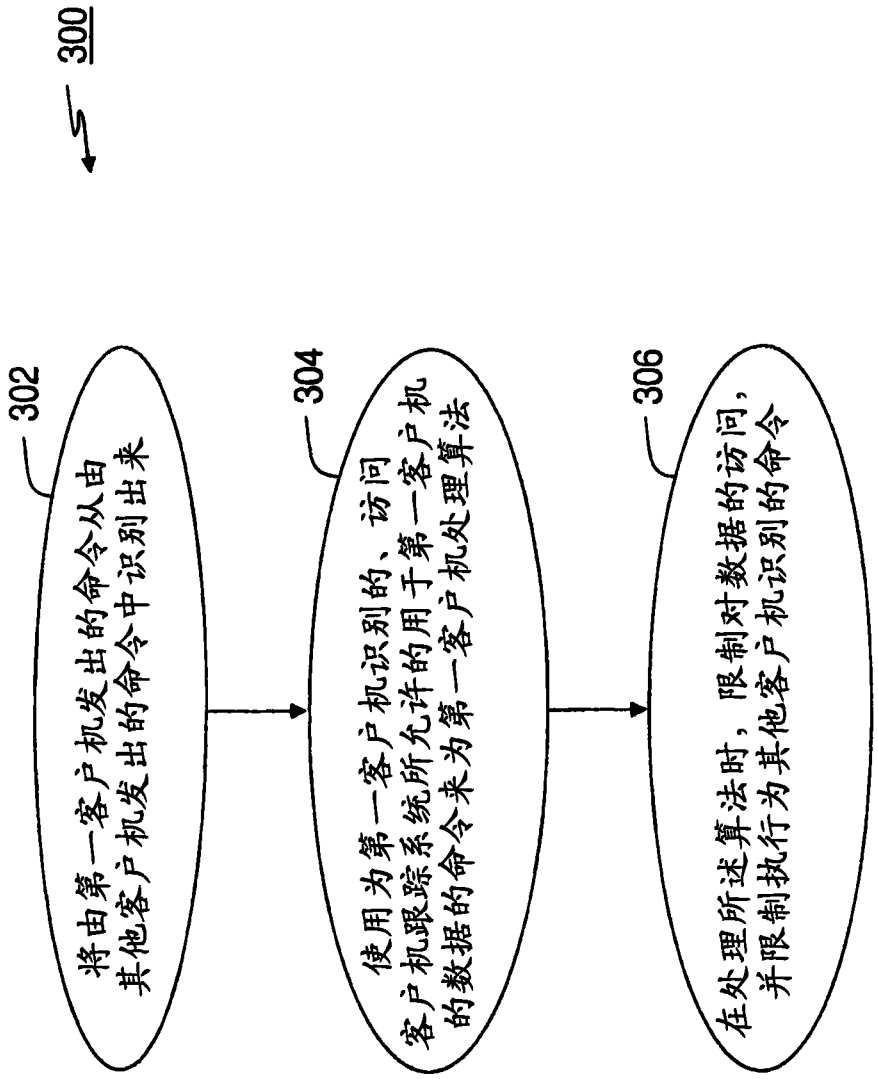

300
302
将由第一客户机发出的命令从由其他客户机发出的命令中识别出来
304
使用为第一客户机识别的、访问客户机跟踪系统所允许的用于第一客户机的数据的命令来为第一客户机处理算法
306
在处理所述算法时，限制对数据的访问，并限制执行为其他客户机识别的命令

图 3