(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1794131 B
(45)授权公告日 2011.11.30

(21)申请号 200510127119.6
(22)申请日 2005.11.21
(30)优先权数据
11/019,094 2004.12.21 US
(73)专利权人 微软公司
地址 美国华盛顿州
(72)发明人 B·阿姆斯特朗 J·加姆斯
K·D·雷 M·克莱默 P·英格兰德
S·A·菲尔德
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 张政权
(51)Int.Cl.
G06F 1/00(2006.01)
(56)对比文件
CN 1538296 A,2004.10.20, 全文.

审查员 林亮亮

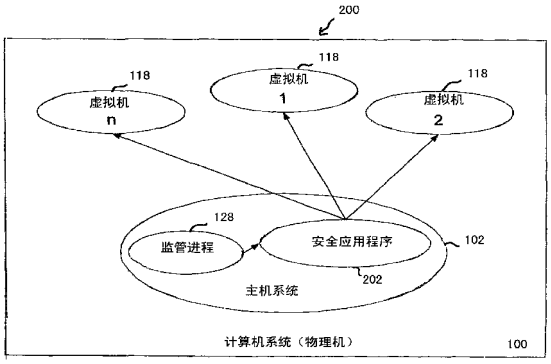
权利要求书 2 页 说明书 9 页 附图 10 页

(54)发明名称

诸如虚拟机或硬化操作系统中的计算机安全管理

(57)摘要

一种安全方案为在计算机上执行的一个或多个自包含的操作环境实例提供安全。该安全方案可包括实现一组可由监管进程控制的安全应用程序等等。这组安全应用程序和监管进程都可在计算机的主机系统上运行，主机系统还可提供用于执行一个或多个自包含的操作环境的平台。该安全方案保护运行于一个或多个自包含的操作环境的进程以及运行于计算机上自包含的操作环境之外的进程。



CN 1794131 B

1. 在计算机中的一种用于监视和保护包含的进程执行环境的多个实例的方法，其中，所述多个实例的每一个都访问所述计算机的仿真资源，所述方法包括：

在所述计算机上执行至少一个安全应用程序，所述安全应用程序用于监视包含的进程执行环境的多个实例的每一个以检测有害进程，其中，所述至少一个安全应用程序在包含的进程执行环境的多个实例之外执行；以及

通过单组安全应用程序帮助扫描包含的进程执行环境的多个实例的每一个的虚拟资源，其中，所述虚拟资源包括所述计算机的仿真资源，并且其中，所述帮助包括配置该组安全应用程序以了解由所述计算机的主操作系统所察觉的资源。

2. 如权利要求 1 所述的方法，其特征在于，所述至少一个安全应用程序通过与相应代理安全进程的通信来访问包含的进程执行环境的多个实例的每一个，所述相应代理安全进程以一对一的对应关系运行在包含的进程执行环境的多个实例的每一个中。

3. 如权利要求 1 所述的方法，其特征在于，所述至少一个安全应用程序通过提供统一接口的虚拟机对象接口来访问包含的进程执行环境的多个实例的每一个，通过所述统一接口，所述至少一个安全应用程序能访问所述仿真资源。

4. 如权利要求 1 所述的方法，其特征在于，所述至少一个安全应用程序在由所述计算机提供的主机系统中执行，并且其中，包含的进程执行环境的多个实例的每一个也在所述主机系统中执行。

5. 如权利要求 1 所述的方法，其特征在于，所述至少一个安全应用程序在由所述计算机提供的主机系统中执行，其中，包含的进程执行环境的多个实例的每一个也在所述主机系统中执行，且其中，所述至少一个安全应用程序至少部分地是由在所述主机系统中执行的监管进程控制的。

6. 如权利要求 1 所述的方法，其特征在于，通过单组安全应用程序帮助扫描包含的进程执行环境的多个实例的每一个的虚拟资源包括提供对关联于包含的进程执行环境的多个实例之一的虚拟存储器结构的访问。

7. 如权利要求 1 所述的方法，其特征在于，通过单组安全应用程序帮助扫描包含的进程执行环境的多个实例的每一个的虚拟资源包括提供对关联于包含的进程执行环境的多个实例之一的虚拟硬盘结构的访问。

8. 如权利要求 1 所述的方法，其特征在于，通过单组安全应用程序帮助扫描包含的进程执行环境的多个实例的每一个的虚拟资源包括提供对关联于包含的进程执行环境的多个实例之一的虚拟网络适配器结构的访问。

9. 如权利要求 1 所述的方法，其特征在于，通过单组安全应用程序帮助扫描包含的进程执行环境的多个实例的每一个的虚拟资源包括提供对关联于包含的进程执行环境的多个实例之一的虚拟驱动器结构的访问。

10. 如权利要求 1 所述的方法，其特征在于，还包括：

在包含的进程执行环境的多个实例之一中检测到有害进程时，

如果该实例尚未被去活，则去活该实例；以及

修复该实例；以及

将所修复的实例载入所述计算机的主机环境中以便它变为活动的。

11. 在计算机系统中的一种用于保护操作系统不受不合需要的进程作用引起的破坏的

方法，所述方法包括：

暂停运行于所述操作系统上的内核，其中，所述操作系统至少部分地隔离于所述计算机系统的基础结构的核心方面；

检查所述内核以判定是否存在不合需要的进程作用的证据，其中，所述检查至少部分地是由独立于所述至少部分隔离的操作系统的监管进程执行的；以及

在所述至少部分隔离的操作系统中存在不合需要的进程作用的证据时，采取遏制所述不合需要的进程作用的步骤。

12. 如权利要求 11 所述的方法，其特征在于，遏制所述不合需要的进程作用的步骤包括挂起所述至少部分隔离的操作系统并执行进一步的监视。

13. 如权利要求 11 所述的方法，其特征在于，遏制所述不合需要的进程作用的步骤包括挂起运行于所述至少部分隔离的操作系统上的选择进程。

14. 如权利要求 11 所述的方法，其特征在于，遏制所述不合需要的进程作用的步骤包括终止关联于所述不合需要的进程作用的进程。

15. 一种用于保护对关联于计算机系统的核心组件的特许操作的访问的计算机系统，所述系统包括：

处理器；

与所述处理器通信的主存储器设备；

次级存储器设备；

操作系统；以及

主机系统，其中，所述主机系统包括：

一个或多个虚拟机，其中，所述一个或多个虚拟机的每一个都与所述计算机系统的核心组件隔离，从而当运行于关联于所述虚拟机的环境中时，有害进程不能直接访问所述核心组件，并且其中，所述一个或多个虚拟机的每一个包括虚拟操作系统的实例、对虚拟存储器的访问以及至少一个虚拟驱动器；以及

至少一个监管进程，用于结合安全应用程序监视所述一个或多个虚拟机，其中，所述监视包括对有害进程的可能检测，并且其中，所述至少一个监管进程和安全应用程序都与所述虚拟机隔离。

16. 如权利要求 15 所述的系统，其特征在于，所述监视还包括监视所述虚拟存储器的地址空间。

17. 如权利要求 15 所述的系统，其特征在于，所述虚拟机还包括对一个或多个仿真设备的访问，并且其中，所述监视还包括监视所述仿真设备。

18. 如权利要求 15 所述的系统，其特征在于，所述虚拟机还包括对仿真硬盘驱动器的访问，并且其中，所述监视还包括监视所述仿真硬盘驱动器。

19. 如权利要求 15 所述的系统，其特征在于，所述监视还包括对到运行于所述虚拟机的进程的输入或来自所述进程的输出执行完整性验证。

20. 如权利要求 15 所述的系统，其特征在于，所述虚拟机还包括对仿真硬盘驱动器的访问，并且其中，所述监视还包括检查驻留在所述虚拟存储器或所述仿真硬盘驱动器上的文件的完整性。

诸如虚拟机或硬化操作系统中的计算机安全管理

技术领域

[0001] 所描述技术一般涉及维护计算机操作系统的安全性与完整性。

背景技术

[0002] 当被特别设计成损害或破坏系统的软件（例如，恶意软件或“malware（恶意软件）”）入侵计算机系统时，计算机操作系统的完整性以及因此整个计算机系统遭受危害。尽管假设病毒、蠕虫和特洛伊木马威胁的出现，计算机用户的安全考虑和需求的范围是广泛的，然而大多数计算机用户关心的是诸如操作系统进程、存储器进程等其计算机的关键基础结构组件的完整性。

[0003] 某些类型的恶意软件使用了操作系统的特许操作来攻击计算机。这样的特许操作一般包括只能由特许用户或进程访问的指令或指令集。例如，当恶意软件不知何故能够访问这些特许操作中的一个或多个时，这可能导致操作系统文件的删除或破坏、对存储器中的操作系统组件的攻击、用户文件的删除、以及许多其它有害的可能性。在某些情况下，甚至非恶意进程也可能通过访问特许操作的无意行为而损坏计算机系统。更普遍地，几乎任何进程都可能通过简单地假冒特许用户的身份而获得对特许操作的访问。

[0004] 通常，操作系统提供用于主存进程并为那些进程提供系统服务的基础结构。操作系统一般提供基本安全保护，诸如在系统资源上实施访问控制和所有权权限。例如，在正常的操作系统环境中，诸如主机防火墙、易受攻击性评价、补丁检测、行为阻断、主机或网络入侵检测以及反病毒技术等保护性安全服务都作为操作系统中的本机应用程序来运行。尽管有这些措施，然而操作系统有时仍不能准确判定是否受到了攻击。特别地，一旦一段恶意代码或其它恶意软件攻击了计算机系统并获得足够的控制（例如，管理员级访问），则操作系统用来判定它是否处于攻击之下的所有进一步尝试都不再有价值，因为用于这种尝试的机制也被破坏了。这是因为恶意代码可有效地修改操作系统或者用来保护它的应用程序所使用的存储器内或盘上结构的任何内容。

[0005] 一种保护计算机系统及其操作系统的方法涉及安装一组安全应用程序，诸如反病毒软件、个人防火墙及入侵检测系统。在有多个计算机系统的系统中，诸如计算机网络或布署在阵列中的计算机系统的集群，每个独立计算机系统运行它自己的那组安全应用程序。这是因为网络或阵列中的每个计算机系统都是具有其自己网络附件、它自己的中央处理单元、它自己的操作系统实例等的物理上独立的实体。尽管这样的安全应用程序可安装在每个计算机系统上以防止计算机系统及其操作系统受到危害，但这样的安全应用程序可能太易于失败而不能保护计算机系统，因为就象任何运行在计算机系统上的其它应用程序一样，它们也易于受到攻击。

[0006] 在保护计算机系统及其操作系统的另一种方法中，计算机系统的各方面，如存储器，都由计算机系统的隔离方面保护。

发明内容

[0007] 这里所描述的计算机安全技术提供了各种不同的安全特征，包括使用单个安全进程（或安全进程组）来监视、保护和修复运行在主机系统上的多个逻辑上隔离的虚拟机。在某些实施例中，该安全技术对在计算机上执行的一个或多个自包含的操作环境实例提供了安全性。该安全技术可包括实现可由监管进程控制的安全应用程序。安全应用程序可监视一个或多个虚拟机。这种监视可使用各种不同的技术来完成，包括由安全应用程序对虚拟机的离线扫描、实现运行于每个虚拟机上的代理安全进程等等。

[0008] 在某些实施例中，这组安全应用程序和监管进程都可运行于计算机的主机系统上，它可提供用于执行一个或多个自包含操作环境的平台。该安全技术可保护运行于一个或多个自包含操作环境中的进程以及运行于计算机上在自包含操作环境之外的进程。

附图说明

[0009] 图 1 是示出在一个实施例中用于实现安全技术的系统示例的框图。

[0010] 图 2 是示出图 1 系统中的虚拟机的离线扫描的示例的框图。

[0011] 图 3A 是示出图 1 系统中的虚拟机的离线扫描的可选示例的框图。

[0012] 图 3B 是示出图 1 系统中的虚拟机的离线扫描的另一示例的框图。

[0013] 图 3C 是示出图 1 系统中的虚拟机的离线扫描的又一示例的框图。

[0014] 图 4 是示出由监管进程执行的监视图 1 的系统中的操作系统的例程的流程图。

[0015] 图 5 是示出使用周期性扫描来监视图 1 的系统中的虚拟机的安全监控例程的示例的流程图。

[0016] 图 6 是示出使用虚拟机结构安装来监视图 1 的系统中的虚拟机的安全监控例程的第二示例的流程图。

[0017] 图 7 是示出不使用虚拟机结构安装来监视图 1 的系统中的虚拟机的安全监控例程的第三示例的流程图。

[0018] 图 8 是示出使用运行于虚拟机中的代理进程来监控图 1 的系统中的虚拟机的安全监控例程的第二示例的流程图。

[0019] 在附图中，同样的参考标号标识相同或基本相似的元素或动作。为便于对任意特定元素或动作的讨论，参考标号中的最高一位数字指的是首次引入该元素的图号（例如，元素 204 是关于图 2 第一次引入和讨论的）。

具体实施方式

[0020] 现在将参考各实施例描述本发明。以下描述提供了用于本发明这些实施例的全面理解和开放描述的特定细节。然而，本领域的技术人员将理解，本发明可不采用这些细节而实施。在其它实例中，没有详细示出或描述众所周知的结构和功能，以免不必要地模糊对本发明实施例的描述。

[0021] 所呈现描述中使用的术语旨在以其最广泛合理的方式解释，即使是与本发明某个特定实施例的详细描述结合起来使用的。某些术语会在下面强调；然而，旨在以任何受限方式解释的任何术语都将公开而明确地如本详细描述部分中这样定义。

[0022] I. 综述

[0023] 这里所描述的计算机安全技术提供了各种不同的安全特征，包括使用单个安全进

程（或安全进程组）来监视、保护和修复运行于主机系统上的多个逻辑上隔离的虚拟机。

[0024] 在某些实施例中，在物理机上执行的主机系统提供了其上可执行操作系统和应用程序的虚拟机。尽管许多进程可在虚拟机上执行，但通常执行于虚拟机上的操作系统和应用程序不能访问资源（例如存储器和设备），除非提供虚拟机的主机系统允许或者由已经分配给虚拟机的询问指定。

[0025] 如果虚拟机执行了恶意软件，任何损害都被限制在虚拟机的操作系统、应用程序和可访问资源中。这样，计算机可充分受保护而不被虚拟机上执行的恶意软件影响。

[0026] 在某些实施例中，主机系统可防止在虚拟机上执行的操作系统和应用程序进行可引起对物理机的资源或操作系统的不合需要的改变的特许操作。例如，在虚拟机上执行的操作系统可在虚拟机中给以管理员权限，但不是在物理机内。

[0027] 在某些实施例中，主机系统实现抢先安全进程。这样的安全进程的示例包括主机防火墙监控程序、易受攻击性评价监控程序、补丁检测监控程序、行为阻断监控程序、主机或网络入侵检测监控程序以及反病毒技术。通常，配置安全进程来增强虚拟机、主机系统以及进而是物理机的安全性。

[0028] 在某些实施例中，安全进程被实施为或受控于运行在主机系统上的监管进程。监管进程可有助于或为安全进程提供对虚拟机组件的某种级别的访问或可见性，包括虚拟存储器、虚拟盘、虚拟网络适配器、虚拟驱动器等（例如，以存储器中的数据结构或对象模型的形式）。例如，监管进程可允许安全进程扫描存储器中或存储在对应于虚拟机的虚拟硬盘的磁盘上的数据结构以寻找恶意软件或安全漏洞的证据。此外（或可供选择地），当提供了由主机系统支持的对象模型时，监管进程可帮助返回有关虚拟机状态（诸如存储器状态或通信状态）的信息至主机系统。通常，由于主机系统和监管进程提供了某种级别的隔离，安全进程可监管和监视虚拟机的安全，同时还保持对这些虚拟机中执行的有害程序的不可访问。这样，保护安全进程不被它们所要监控的程序篡改或摧毁。

[0029] 在某些实施例中，安全进程可用于监视和修复处于已保存状态的虚拟机，其中虚拟机监控程序的执行已停止，且所有关于虚拟机存储器、设备和 CPU 状态的信息都写出到物理文件中。安全进程还可用来监视和修复处于暂停状态的虚拟机，这一般是由虚拟机管理器调用的。在暂停状态期间，虚拟机停止执行，但保持准备好继续下一指令或处理。不论在暂停还是已保存状态情况下，虚拟机内部的虚拟操作系统不知道状态改变。同样地，安全进程可具有在载入主机系统前扫描和修复或清除虚拟机的能力。

[0030] 在某些实施例中，主机系统可安装虚拟机的硬盘，如同它是一个物理盘一样，并随后在块级别上扫描虚拟硬盘（如同任意其它已安装盘一样）。例如，主机系统可使用能够载入物理机操作系统的盘驱动器。这个盘驱动器随后可解释虚拟硬盘，并将作为本地附加盘呈现给主机系统。

[0031] 监视虚拟机的另一方法是在每个虚拟机中运行“代理”安全进程。这样，代理安全进程关联于主机系统上的主安全进程。代理安全进程打开到主安全进程的通信信道，并帮助发现对虚拟机的攻击并从中恢复。尽管这种情况可能涉及在攻击期间代理安全进程被危害的风险，但代理还有可用于它的经由主安全进程的外部恢复选项。在某些情况下（例如涉及系统管理程序使用的情况），代理可运行于不同的虚拟机中而不是其实际监控的虚拟机。

[0032] 在某些实施例中，主机系统可拍摄每个虚拟机完整状态的周期性快照。理论上，这种快照拍摄可瞬间执行，具有较小的性能开销。然而这种技术的许多变体都是可能的。如果安全进程检测到虚拟机内的异常（例如，恶意软件覆写了操作系统或者恶意软件把自己表示为存储器中的程序），则主机系统可将虚拟机状态恢复到最后的快照状态，采取措施来防止异常的再次发生，并重启虚拟机。

[0033] II. 代表性系统

[0034] 图 1-5 和以下讨论提供了本发明可在其中实现的合适环境的简要描述。尽管不要求，但本发明的诸方面可诸如由通用计算机（例如服务器计算机、无线设备或个人 / 膝上型计算机）执行的例程等在计算机可执行指令的通用上下文环境中描述。相关领域中的技术人员将理解，本发明可用其它通信、数据处理或计算机系统配置来实施，包括因特网装置、手持设备（包括个人数字助理 (PDA)）、可穿戴计算机、各种蜂窝或移动电话、嵌入式计算机（包括耦合到汽车上的那些）、多处理器系统、基于微处理器或可编程消费电子产品、机顶盒、网络 PC、小型计算机、大型计算机等等。

[0035] 本发明诸方面可在被特别编程、配置或构造以执行一个或多个在这里详细解释的计算机可执行指令的专用计算机或数据处理器上实施。本发明的诸方面还可在分布式计算环境中实施，其中任务或模块由通过通信网络连接的远程处理设备执行。在分布式计算环境中，程序模块可位于本地或远程存储器存储设备中。

[0036] 本发明的诸方面可存储或分布在计算机可读介质上，包括磁或光可读的计算机盘，作为半导体存储器、纳米技术存储器、有机或光存储器或其它便携式数据存储介质上的微码。事实上，本发明诸方面中的计算机实现的指令、数据结构、屏幕显示和其它数据可分布于因特网或其它网络（包括无线网）上、一段时间内传播介质（例如电磁波、声波等）上的传播信号上、或者可在任意模拟或数字网络（分组交换、电路交换或其它方案）上提供。相关领域的技术人员将认识到，本发明的各部分驻留在服务器计算机上，同时相应部分驻留在如移动设备的客户机计算机上。

[0037] 参考图 1，其上可实现计算机安全技术的计算机系统（物理机）100 配备了各种组件。这些组件包括被配置为在计算机系统 100 上运行的主机系统 102，它附加于、与之结合或代替标准或通用计算机操作系统 104。在某些实施例中，可配置主机系统 102，以使它不能访问除了本机和 / 或特许监管和安全功能之外的任何内容。主机系统 102 可与一个或多个计算机资源接口，诸如带有存储器管理单元 (MMU)108 的处理器 106、磁盘 110、存储器 112、通信子系统 114 以及一个或多个系统驱动器 116。

[0038] 在某些实施例中，一个或多个虚拟机 118 运行于主机系统 102 的控制之下并可从属于主机系统 102。虚拟机 118 的每一个可包括有助于处理器和其它机器资源虚拟化或仿真的组件集合。例如，如说明的实施例所示，每个虚拟机 118 可访问一组仿真资源，包括虚拟网络适配器 119、虚拟存储器 120（它可包括物理机存储器 112 的已分配部分）、虚拟盘 122 以及各自代表非虚拟系统驱动器 116 的虚拟实例的虚拟驱动器 124。虚拟操作系统实例 126 运行在这些虚拟机 118 的每一个上。在某些实施例中，虚拟操作系统实例 126 可以是物理机操作系统 104 的全部或部分副本。

[0039] 通常，虚拟机 118 可依靠 MMU 108 来提供各种页面级保护。通常，运行在每个虚拟机上的应用程序或进程 129 只使用它们各自的虚拟机的仿真资源（例如，虚拟存储器 120、

虚拟盘 122、虚拟驱动器 124、操作系统 126 等）。这样的应用程序或进程 129 有时被称为“客户”码 (guset code)。仿真资源通常假定是可信的，其意义在于它们遵从于主机系统 102 上的标准保护机制并不暴露任何主机系统用户数据给客户码，除非明确地命令这么做。

[0040] 在某些实施例中，仿真资源可使用若干集成技术，诸如 I/O 端口访问、存储器映射的寄存器、直接存储器存取 (DMA)、中断等，在主机系统 102 和运行在虚拟机 118 上的客户码之间交换数据。其它数据交换技术包括剪贴板共享、文件拖放、时间同步等。为支持这类数据交换技术，虚拟机 118 可提供几种能力，包括异步客户事件、同步主机调用、在客户码和主机系统 102 之间数据传输、集成服务注册等。

[0041] 虚拟机 118 可在主机系统 102 上使用几种可能技术中的任一种创建或启动。例如，在一个实施例中，主机系统 102 可创建并启动虚拟机的实例并在创建时为虚拟机配置参数。在某些实施例中，主机系统 102 可将现存虚拟机映像放在盘 110（或许在共享上）上，并将该映像载入为新虚拟机实例。在某些情况下，这种载入称为“导入”虚拟机实例，且在某种程度上可比作将数据从一个应用程序带入另一个应用程序的“导入”功能。

[0042] 在某些实施例中，一组一个或多个监管进程 128 运行在主机系统 102 上。在某些实施例中，一个或多个监管进程 128 可具有对虚拟操作系统实例 126 的完全或部分访问，并可为每个虚拟机 118 提供安全服务。在某些实施例中，监管进程 128 还可处理诸如数字权限管理 (DRM) 和许可控制等活动。由于这种配置规定运行于虚拟机 118 上的任意恶意软件不能访问每个虚拟机外的资源，监管进程 128 一般是安全的，免于恶意软件的破坏。

[0043] 在某些实施例中，一个或多个监管进程 128 控制一组可保护和 / 或监管主机系统 102 上的所有虚拟机 118 的安全应用程序（例如，反病毒软件、个人防火墙、入侵检测系统等）。例如，一个或多个监管进程可通过该组安全应用程序便于多个虚拟机的离线扫描。离线扫描可包括配置该组安全应用程序来了解每个虚拟机的虚拟资源，因为它们作为虚拟对象驻留在计算机系统（物理机）上。这样，该组安全应用程序可检查（扫描）那些来自虚拟机之外的虚拟资源（例如，使用虚拟机数据结构的内部格式的知识）。

[0044] 尽管在这里使用了术语“安全应用程序”和“监管进程”，但这些概念并不限于应用程序或进程。相反，任何被配置成为虚拟机提供服务的实用程序或攻击和 / 或其资源可在主机系统上实现，以达到所需结果而不脱离本发明范围。这种实用程序和工具的某些示例包括反广告实用程序、反间谍软件实用程序、词盘碎片整理器等。

[0045] 虚拟机资源的离线扫描可在虚拟机正在运行或睡眠状态（例如在暂停或已保存状态中）时发生。例如，在虚拟机可通过定位和载入现有虚拟机映像到主机系统 102 上来创建的情况下，离线扫描（和任何必需的清除和修复）可在“导入”虚拟机实例之前发生。可在暂停或已保存状态中扫描的虚拟机资源包括虚拟硬盘、虚拟机存储器内容、虚拟通信端口缓冲器结构等。在某些实现中，访问暂停的虚拟机的存储器是不可能的。但是，虚拟机存储器在虚拟机处于保存状态或通过虚拟机快照仍然是可访问的。

[0046] 参考图 2，示出了离线扫描配置 200 的一个示例，它例示了图 1 的各种组件。在这种配置中，安全应用程序 202 和可任选的监管进程 128 驻留在主机系统 102 上。安全应用程序 202 可至少部分地由监管进程 128 控制，它将虚拟机 118 的资源视为可扫描安全漏洞证据的数据结构或数据结构组。为允许它以原始形式访问虚拟机 118 的资源并准确检测安全漏洞，安全应用 202 可依赖关于关联于资源的数据结构的语义和配置的信息。在某些实

施例中，更新这种信息以反映数据结构的语义和配置中任何故意的改变。

[0047] 例如，图 2 的安全应用程序 202 可以是一个反病毒扫描引擎，它扫描虚拟机 118 以检测它是否感染了一个或多个已知病毒或蠕虫。为开始扫描过程，反病毒引擎 202 载入当前特征定义文件到它的程序存储器。例如，特征定义文件可定义虚拟机的虚拟硬盘结构的语义和配置，从而在其当前状态下扫描虚拟机的硬盘时给反病毒引擎提供参考点。

[0048] 接下来，反病毒引擎指挥其扫描来读取和虚拟机的虚拟硬盘相关的物理机硬盘部分。这样，反病毒引擎有效地读取了虚拟硬盘的内容，并使用本领域技术人员检测恶意软件所用的方法和技术，将其内容（例如，内容对象）与其已知恶意内容列表进行比较。为此示例起见，虚拟硬盘内的内容对象可以是文件，或者由操作系统操纵的另一对象，诸如来自微软 Windows 系统的注册表键，或者能够被标识为恶意或非希望软件实例的一部分的盘上的任何其它对象。在发现恶意软件的基础上，反病毒引擎可试图删除任何损坏的对象，或删除位于对象内的感染。

[0049] 图 3A 提供了离线扫描配置 300 的第二示例。在这个配置中，由监管进程 128 支持的虚拟机对象接口 302 提供了一个统一接口，通过该接口，安全应用程序 304 可访问虚拟机的资源。虚拟机对象接口 302 可将在各虚拟机之间变化的虚拟机数据结构映射到可由安全应用程序 304 为扫描和其它活动而访问的共同格式。这样，只需要开发安全应用程序 304 来访问这个共同格式而不是虚拟机可能具有的每个格式变体。例如，主机系统 102 可发现关于虚拟机 118 的状态（诸如盘状态、存储器状态或通信状态）的信息，以便安全应用程序 304 可监视它们、查找安全漏洞或其它问题。此外，虚拟机对象接口 302 可提供可由多个安全应用程序使用的功能。例如，虚拟机对象接口 302 可提供允许另一安全进程扫描虚拟机的虚拟网络适配器以查找具有诸如蠕虫负载等恶意内容的传入网络分组的功能。

[0050] 这种配置为虚拟机的设计者和安全应用程序的设计者提供了某些灵活性。例如，虚拟机的设计者可改变虚拟机的数据结构而没有对安全应用程序设计者产生后果。因此，只需要开发安全应用 304 来访问这个共同格式而不是虚拟机可能具有的每个格式变体。

[0051] 在某些实施例中，离线扫描技术有助于虚拟机当前状态与安全应用程序感知为虚拟机的当前状态的同步，从而提供更准确而一致的扫描能力。这种同步在虚拟机状态快速变化的情况下可能是很有用的。

[0052] 参考图 3，可实现这种同步的一种方法是通过运行提供虚拟机的接近实时自相一致的视图的代理进程 322。代理进程 322 可运行于虚拟机 118 上，随后可输出该虚拟机的视图到虚拟机对象接口 302，后者随后可提供适当信息给监管进程和 / 或安全应用程序。在某些实施例中，代理进程 322 可提供应用程序编程接口 (API) 供虚拟机对象接口 302 使用。（可供选择地，安全应用程序可提供类似的 API 供虚拟机对象接口 302 使用。）

[0053] 可实现这种同步的可供选择的方法是让虚拟机 118 创建其状态的恒定快照，并将这些快照存储在存储器或盘上。尽管这些快照可能是“过时”几秒的，但它们是自相一致的。

[0054] 参考图 3C，用于提供虚拟机的安全扫描的一种可供选择的技术是配置的系统 330，以便安全应用程序 336 和监管进程 334 运行在指定的虚拟机 332 上（而非直接运行在主机系统 102 上）。安全应用程序 336 和监管进程 334 随后可监视和 / 或扫描其它虚拟机 118 以检测问题。这样，可保护指定的虚拟机 332（它可专用于提供安全监视）不受攻击。

[0055] III. 系统流程

[0056] 图 4 到 8 是示出在图 1 系统内发生的过程的代表性流程图。这些流程图不示出所有功能或数据交换，而是提供了对在此系统下交换的命令和数据的理解。相关领域的技术人员将认识到，某些功能或命令和数据的交换可以重复、变化、省略或补充，而未示出的其它方面也很容易实现。

[0057] 参考图 4，例如由图 1 的监管进程执行的监管例程 400 可运行在主机系统之上（或离线），来监视、修改和 / 或配置运行于虚拟机上的进程或虚拟操作系统。可供选择地，监管例程 400 可监视、修改和 / 或配置运行在硬化操作系统（但不是虚拟的）上的进程。

[0058] 在方框 401，例程 400 暂停虚拟机操作系统。在判定框 402，例程 400 检查在虚拟机内发生的损害活动（例如欺诈进程）导致的变化。例如，例程 400 可扫描虚拟机操作系统内核的一部分以检查问题。作为监视虚拟操作系统内核的一个替换（或除此之外），例程 400 可监视连接到虚拟（或硬化）操作系统的其它各方面。例如，例程 400 可监视虚拟地址空间、监视仿真设备、监视仿真硬盘驱动器、执行完整性验证（例如，进行校验和）、检查驻留在虚拟盘或存储器中的文件的完整性等。

[0059] 在判定框 402，如果例程 400 未检测到损害活动导致的变化，则例程 400 前进到方框 404，在结束前重启虚拟操作系统内核。但在某些实施例中（未例示），例程 400 可循环返回到方框 401（在一个时间段过去后），以再次执行暂停和检查步骤（除非虚拟操作系统实例终止）。但在判定框 402，如果例程 400 检测到损害活动导致的变化，则例程前进到方框 403，在那里例程启动遏制动作。示例遏制动作可包括诸如挂起客户操作系统以进行附加扫描、挂起选择进程、清除恶意软件并重新格式化虚拟操作系统以修复任何损坏、在拍摄“快照”后关闭虚拟机，以便一旦虚拟机重启，虚拟机环境可或多或少恢复等。

[0060] 图 5 给出了离线扫描例程示例 500，它由控制一组被配置成执行运行在主机系统上的虚拟机的离线扫描和修复的安全应用程序（例如，反病毒软件）的监管进程协助完成。在框 501，例程 500 检索运行着的虚拟机当前状态的周期性快照。在框 502，例程扫描所检索的周期性快照。在判定框 503，如果检测到问题，则例程前进到框 504，其中例程向运行着的虚拟机通知有关问题，或者可供选择地，指示虚拟机退回到问题发生前最后保存的状态。如果在判定框 503 例程 500 未检测到问题，则例程返回到框 501 以检索下一周期性快照。

[0061] 图 6 给出了离线扫描例程示例 600，它由控制一组被配置成执行运行在主机系统上的多个虚拟机的离线扫描和修复的安全应用程序（例如，反病毒软件）的监管进程协助完成。例如，例程 600 可用来检测和恢复由于恶意软件入侵而不可用的虚拟机。在框 601，例程 600 以类似于安装物理盘的方式安装虚拟机的下一结构或组件到主机系统上。这样，结构或组件结合为计算机操作系统的一部分，而不是视作外部扫描的对象。结构或组件可以是从主机系统角度看上去的仿真组件。在某些实施例中，虚拟机的结构或组件可被对象化，因而主机系统可为该组安全应用程序提供扫描它们的接口。例如，虚拟机的存储器可被对象化来扫描存储器中的恶意软件。

[0062] 在框 602，该组安全应用程序扫描虚拟硬盘驱动器结构（或存储器中的结构等）。在判定框 603，如果被扫描的结构是受到危害的，则例程 600 继续到框 604，其中安全应用程序修复虚拟硬盘驱动器结构（或存储器中的结构）。但如果在判定框 603 扫描组件未受危害，则例程前进到判定框 605。

[0063] 在判定框 605，如果虚拟机所有的结构或组件都已被扫描过，则例程结束。否则，例

程循环返回到框 601 以安装下一虚拟机结构或组件。

[0064] 在某些实施例中，例程 600 可结合追踪在每个虚拟机硬盘驱动器中扫描之间发生的变化的优化技术来使用。这样，例程 600 可只扫描自上次扫描后的变化，从而提高扫描效率。例如，优化例程可在块级别上追踪虚拟机的硬盘驱动器中的变化。块级别上的变化随后可为扫描目的而映射到文件级的变化（因为典型的反病毒软件在文件级上扫描）。可供选择地，变化可通过查看对主文件表结构的修改来追踪。这可能涉及主机系统中先前的主文件表的检验点存储。

[0065] 图 7 给出了离线扫描例程示例 700，它由控制一组被配置成执行运行在主机系统上的多个虚拟机的离线扫描和修复的安全应用程序（例如，反病毒软件）的监控进程协助完成。例如，例程 700 可用来检测和恢复由于恶意软件入侵而不可用的虚拟机。与在扫描前安装虚拟机结构或组件的图 6 的离线扫描例程相反，图 7 的例程在外部扫描结构或组件。在框 701，例程 700 扫描虚拟机的下一结构或组件。结构或组件可以是从主机系统角度看上去的仿真组件。在某些实施例中，虚拟机结构或组件可被对象化，这样主机系统可为该组安全应用程序提供扫描它们的接口。例如，虚拟机存储器可被对象化来扫描存储器中的恶意软件。

[0066] 在判定框 702，如果被扫描的结构受到危害，则例程 700 继续到框 703，其中安全应用程序修复虚拟硬盘驱动器结构（或存储器中的结构）。但如果在判定框 702 被扫描的组件未受到危害，则例程前进到判定框 704。在判定框 704，如果虚拟机的所有结构或组件都已被扫描过，则例程结束。否则，例程返回到框 701，以安装下一虚拟机结构或组件。

[0067] 图 8 是给出离线扫描例程的第二示例 800 的流程图，它由控制一组被配置成执行运行在主机系统上的多个虚拟机的离线扫描或修复的安全应用程序（例如，反病毒软件）的监控进程协助完成。在例程 800 中，诸如图 3B 的代理进程 322 等代理进程使其正被扫描的虚拟机实际状态能与被安全应用感知的虚拟机状态同步。

[0068] 在框 801，例程 800 通过某个机器间通信接口建立安全应用程序（诸如图 3B 的安全应用程序 304，它运行在主机系统或者虚拟机对象接口上）与代理进程之间的通信。在框 802，例程 800 建立对虚拟机存储器的访问。例如，运行在主机系统上的代理进程可提供对相应于虚拟机应用程序存储器的虚拟缓冲区的访问。例程继续到框 803，其中安全应用程序扫描存储器以找出安全问题的证据。例如，当安全应用程序是反病毒扫描引擎时，反病毒扫描引擎可扫描存储器，以查找匹配已知恶意软件特征的代码模式。在判定框 804，如果虚拟机的任意结构或组件已受到危害，则例程 800 继续到方框 805，其中安全应用程序和 / 或代理进程清除计算机存储器。可供选择地，安全应用程序可用信号通知代理进程采取针对虚拟机的纠正动作。但如果在判定框 804 没有结构或组件受到危害，则例程结束。

[0069] IV. 结论

[0070] 除非上下文明确要求，否则在本描述和权利要求书通篇中，词汇“包括”、“包含”等都要按包含意思解释，而不是排它或详尽的意思；即“包括，但不限于”的意思。此外，词汇“这里”、“以上”、“以下”和类似含义的词汇在用于本申请时，是指本申请为一整体而不是本申请的任何具体部分。当权利要求书在对两个或多个项的列表使用词汇“或者”时，该词汇涵盖该词所有下列解释：列表中任意项、列表中所有项以及列表中各项的任意组合。

[0071] 本发明实施例的以上详细描述并不旨在穷尽或限制本发明于以上所揭示的精确

形式。尽管为说明起见，以上描述了本发明的特定实施例和示例，但正如相关领域的技术人员将认识到的，在本发明的范围内，各种等价的修改都是可能的。例如，尽管进程或框是以给定顺序呈现的，但可供选择的实施例可用不同顺序执行具有这些步骤的例程或者使用具有这些框的系统，而且某些进程或框可被删除、移动、添加、细分、结合和／或修改。这些进程或框的每一个都可用各种不同的方法来实施。而且，尽管进程或框有时被示出为串行执行，但这些进程或框可改为并行执行，或者可在不同时间执行。在上下文环境允许的地方，以上详细描述中使用单数或复数的词汇也可分别在上下文环境允许的地方包括复数或单数。

[0072] 这里所给出的本发明内容可应用于其它系统，而不必需是这里所描述的系统。以上描述的各个不同实施例的元素和动作可结合起来提供更多的实施例。

[0073] 可对本发明按照以上详细描述作出这些和其它变化。尽管以上描述详细说明了本发明的某些实施例并描述了预期的最佳模式，但不管以上文本中出现多么详细的说明，本发明还可以用许多方法来实施。如以上所提到的，在描述本发明的某些特征或方面时所使用的特定术语不应理解为暗示该术语在这里被重定义以受限于该术语所关联的本发明的任何具体特性、特征或方面。通常，在所附权利要求书中所使用的术语不应解释为将本发明限于在本说明书中所揭示的特定实施例，除非以上详细描述部分明确定义了这类术语。因此，本发明的实际范围不仅包括所揭示的实施例，而且还包括在所附权利要求书中实施或实现的本发明的所有等价方法。尽管本发明的某些方面是以某些权利要求的形式呈现的，但发明人以任何数量的权利要求形式构想本发明的不同方面。例如，尽管只有本发明的一个方面被阐述为包含在计算机可读介质中，但其它方面也同样可包含在计算机可读介质中。因此，发明人保留在提交本申请后增加附加权利要求的权利，以对本发明其它方面继续这样的附加权利要求形式。

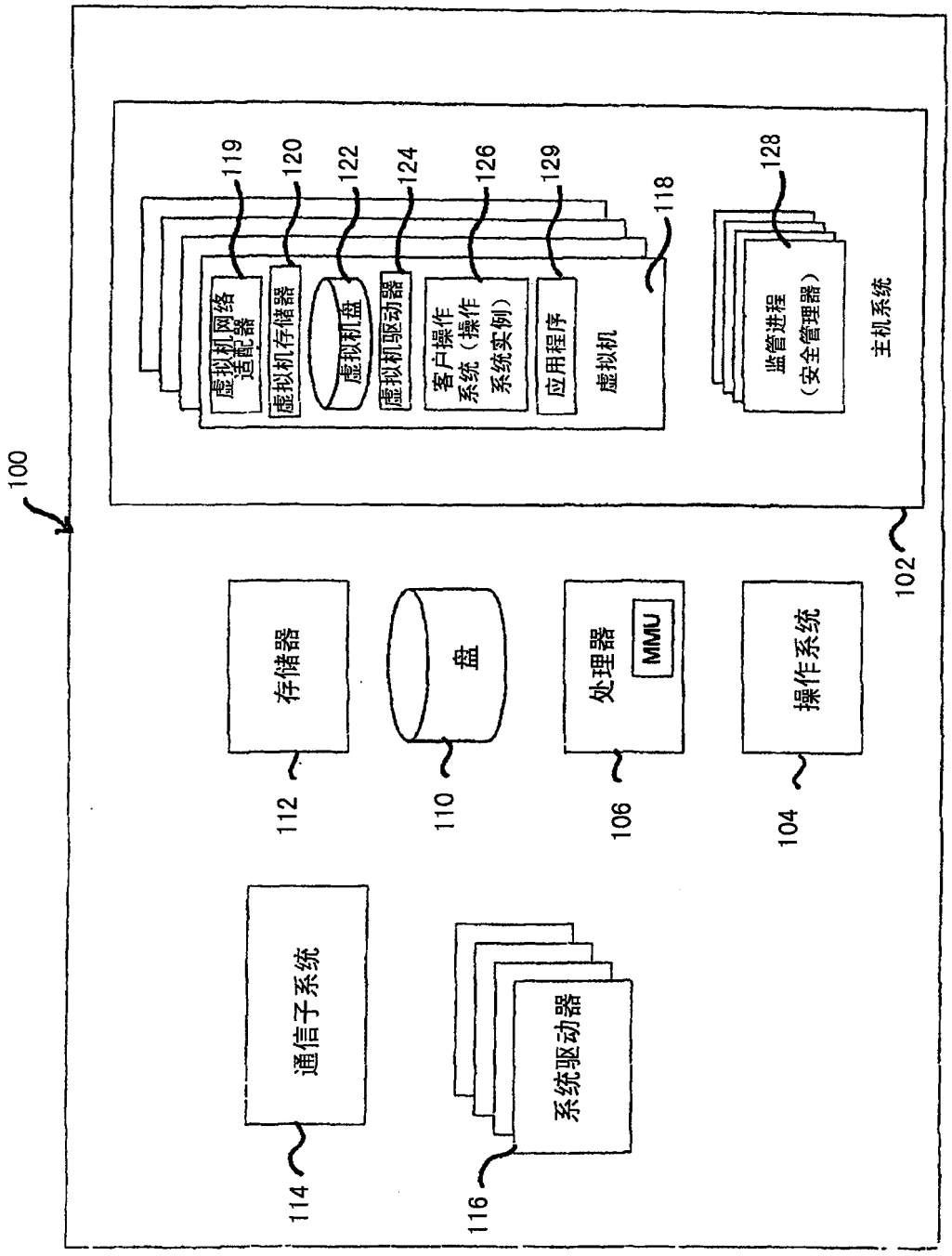

100
主机系统
102
虚拟机
118
虚拟机网络适配器
119
虚拟机存储器
120
虚拟机盘
122
虚拟机驱动器
124
客户操作系统（操作系统实例）
126
应用程序
129
监管进程（安全管理器）
128
存储器
112
盘
110
处理器
MMU
106
操作系统
104
通信子系统
114
系统驱动器
116

图 1

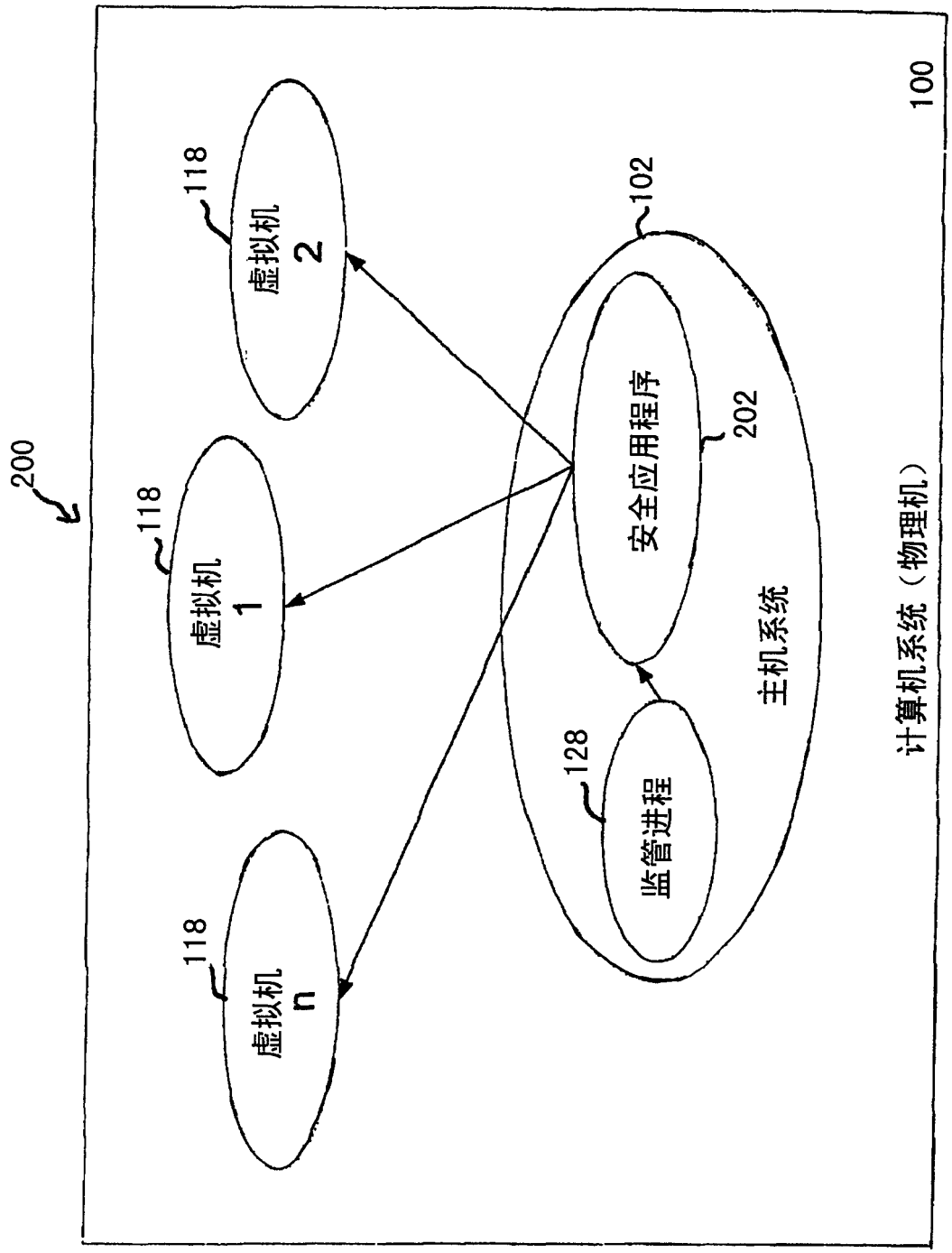

200
100
计算机系统（物理机）
虚拟机 1
118
虚拟机 2
118
虚拟机 n
118
102
主机系统
安全应用程序
202
监管进程
128

图 2

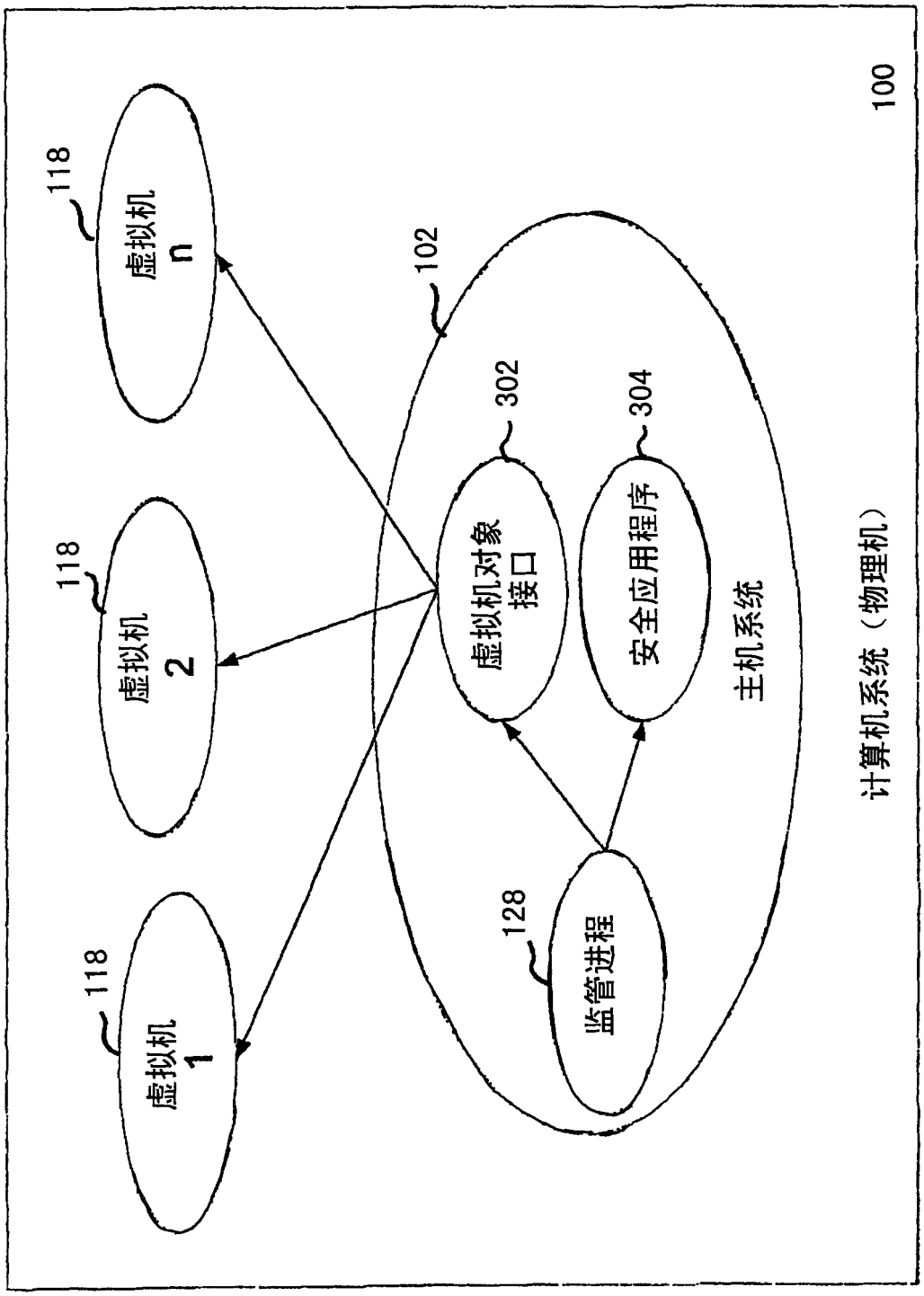

100
计算机系统（物理机）
主机系统
102
虚拟机对象接口
302
安全应用程序
304
监管进程
128
虚拟机 1
118
虚拟机 2
118
虚拟机 n
118

图 3A

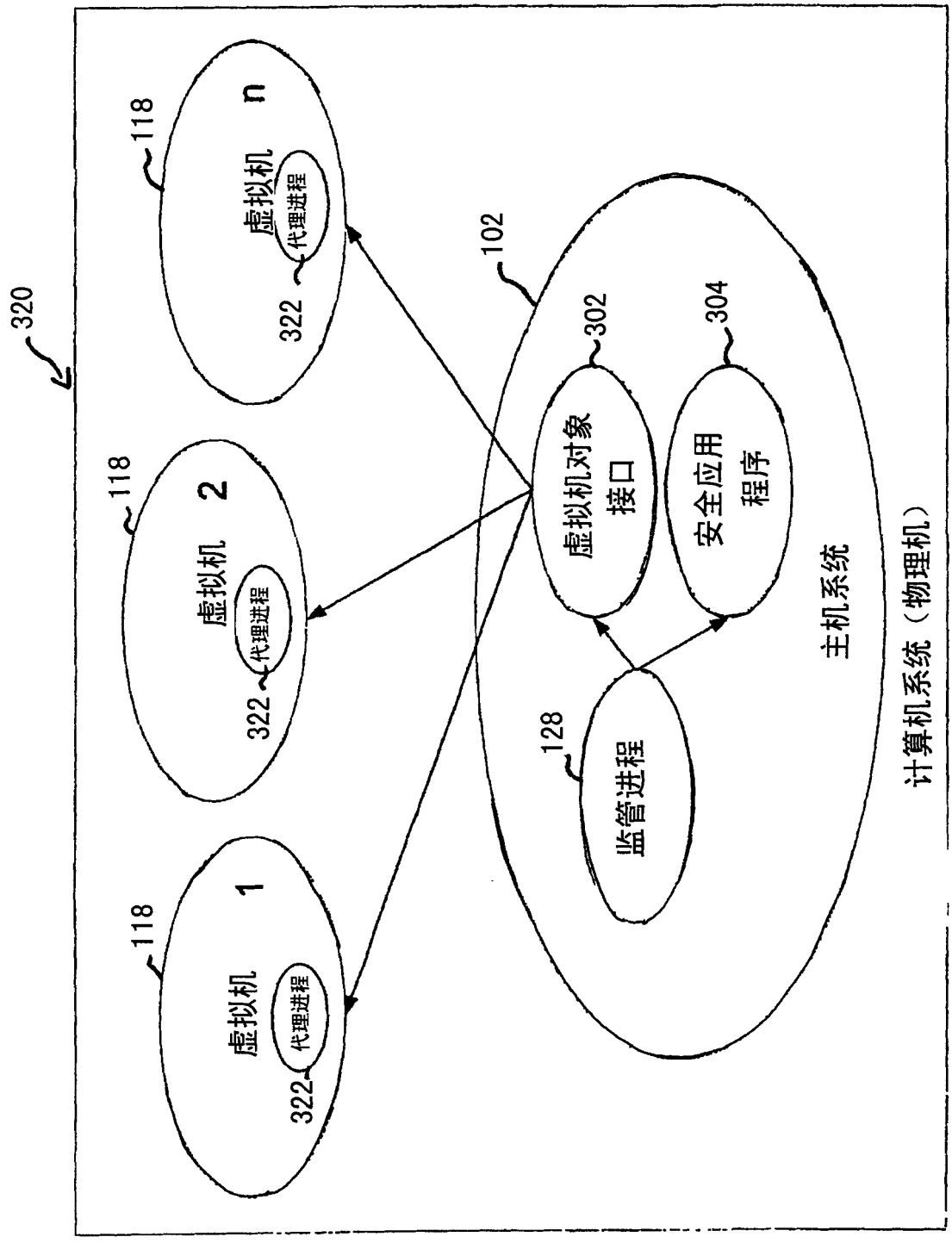

320
118
虚拟机 n
代理进程
322
118
虚拟机 2
代理进程
322
118
虚拟机 1
代理进程
322
102
虚拟机对象接口
302
安全应用程序
304
监管进程
128
主机系统
计算机系统（物理机）

图 3B

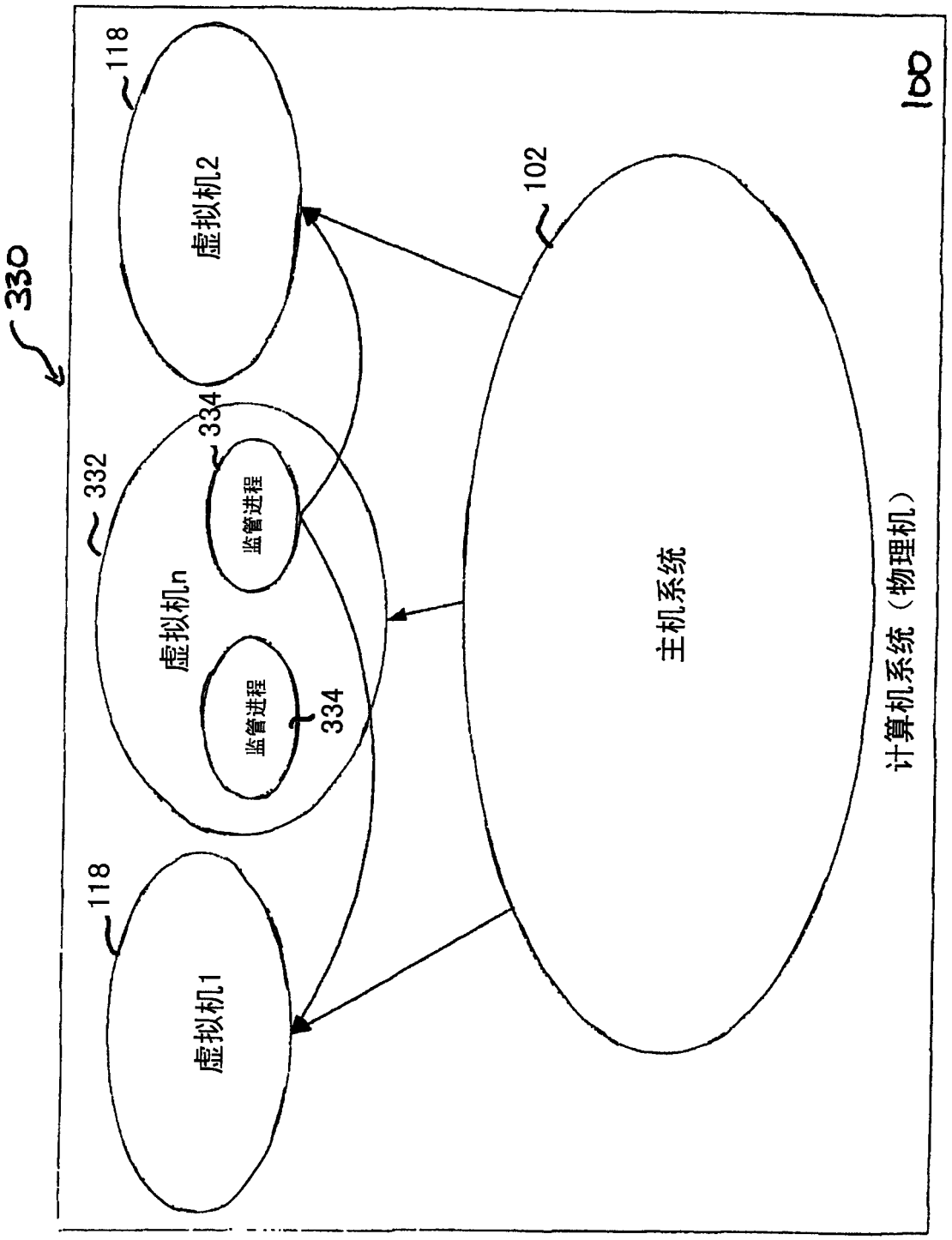

330
118
虚拟机2
102
334
332
监管进程
虚拟机n
监管进程
334
主机系统
118
虚拟机1
计算机系统（物理机）
100

图 3C

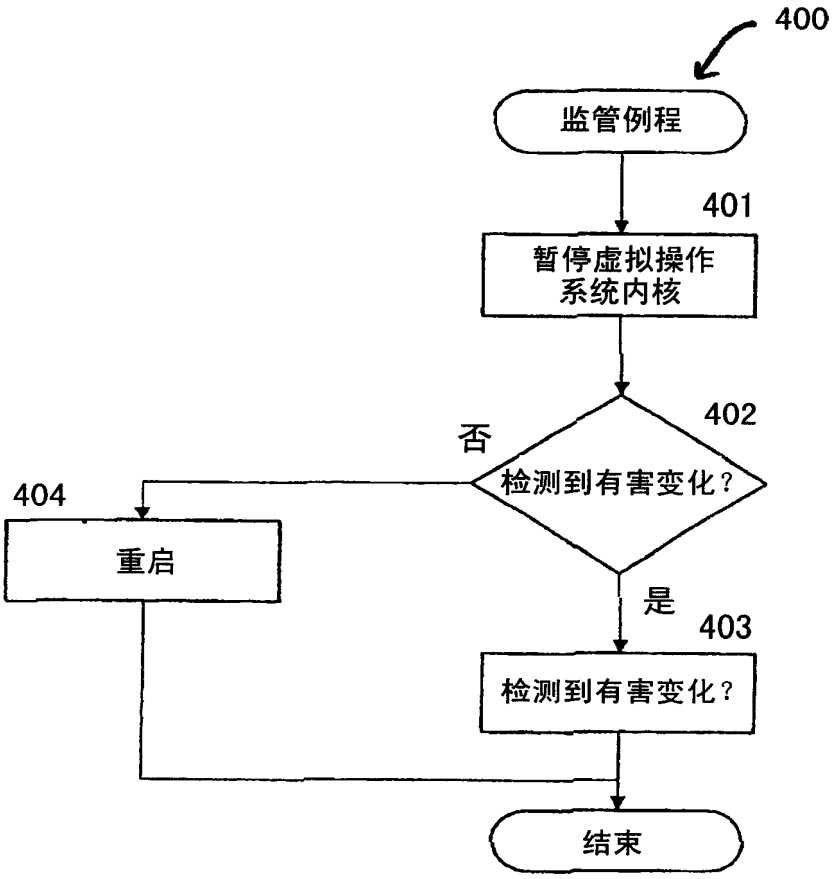


图 4

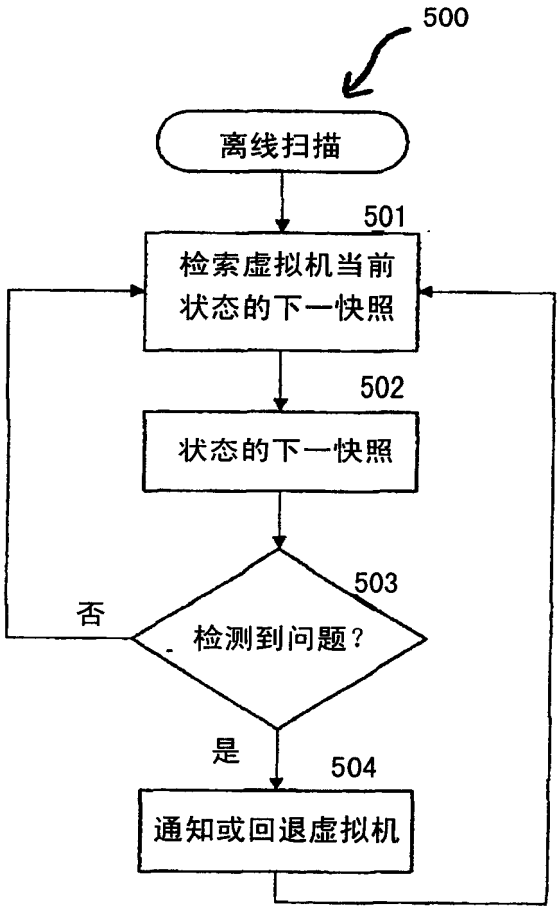

500
离线扫描
501
检索虚拟机当前状态的下一快照
502
状态的下一快照
503
检测到问题？
否
是
504
通知或回退虚拟机

图 5

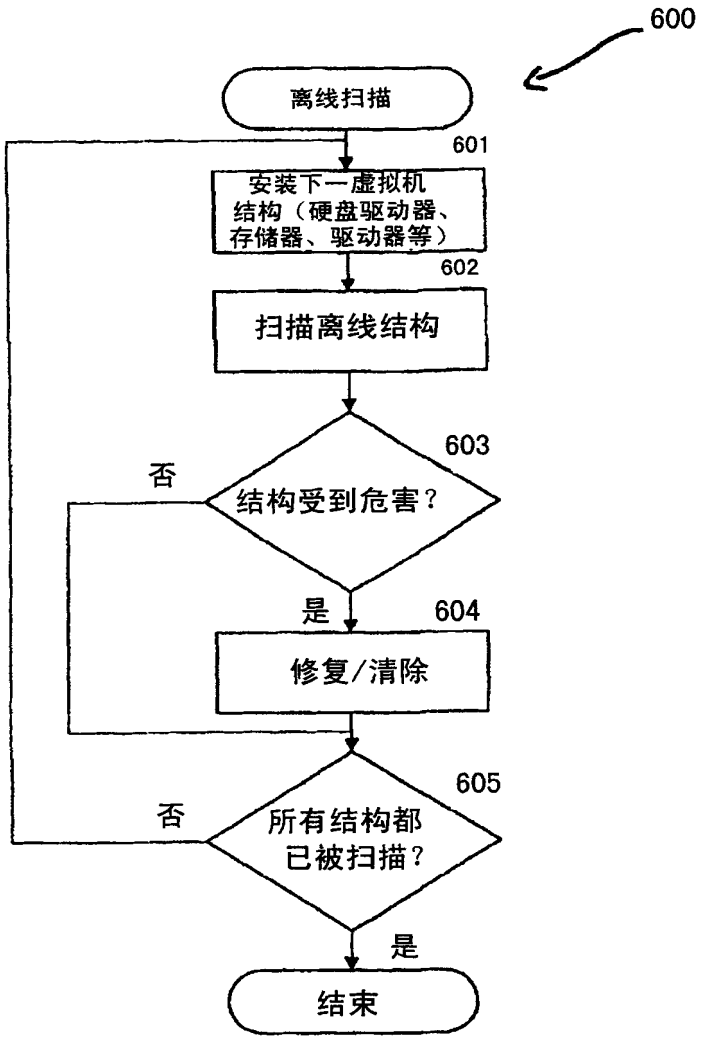

600
离线扫描
601
安装下一虚拟机结构（硬盘驱动器、存储器、驱动器等）
602
扫描离线结构
603
否
结构受到危害？
是
604
修复/清除
605
否
所有结构都已被扫描？
是
结束

图 6

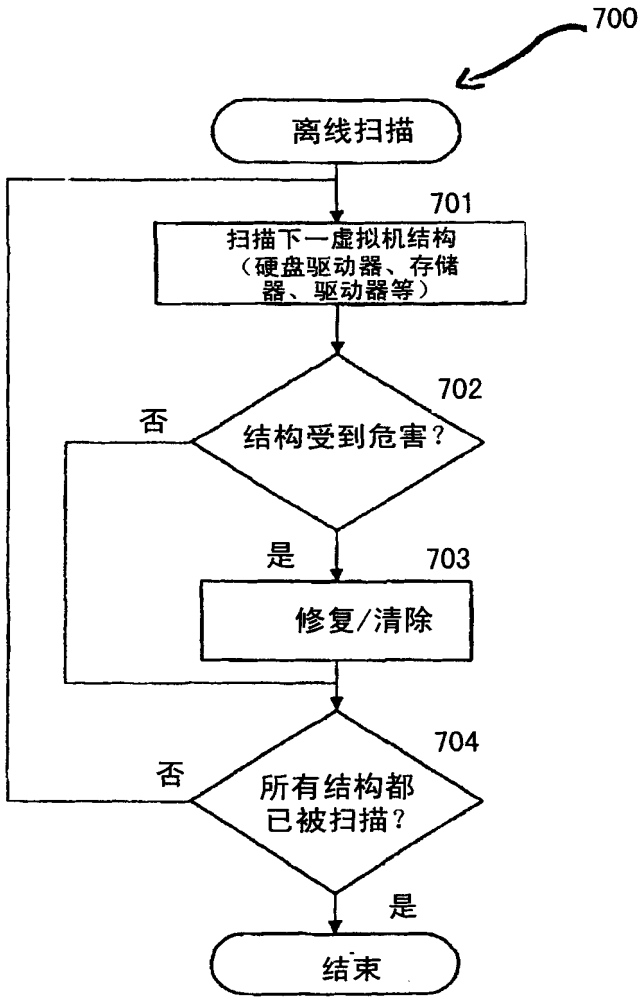

700
离线扫描
701
扫描下一虚拟机结构（硬盘驱动器、存储器、驱动器等）
702
结构受到危害？
否
是
703
修复/清除
704
所有结构都已被扫描？
否
是
结束

图 7

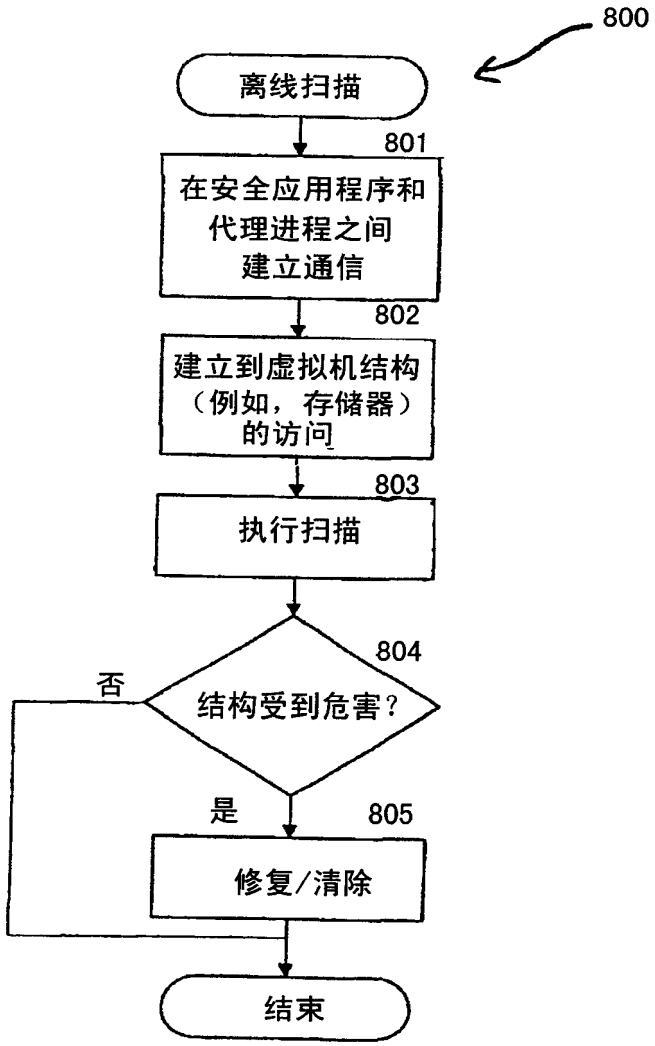

800
离线扫描
801
在安全应用程序和代理进程之间建立通信
802
建立到虚拟机结构（例如，存储器）的访问
803
执行扫描
804
结构受到危害？
否
是
805
修复/清除
结束

图 8