(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 101681407 B
(45)授权公告日 2013.05.22

(21)申请号 200880015323.0
(22)申请日 2008.05.02
(30)优先权数据
11/747,416 2007.05.11 US
(85)PCT申请进入国家阶段日
2009.11.09
(86)PCT申请的申请数据
PCT/US2008/062513 2008.05.02
(87)PCT申请的公布数据
WO2008/140977 EN 2008.11.20
(73)专利权人 微软公司
地址 美国华盛顿州
(72)发明人 R·基尔纳尼 K·N·艾弗森
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 陈斌 钱静芳
(51)Int.Cl.
G06F 21/56(2013.01)
G06F 21/57(2013.01)
(56)对比文件
US 7184554 B2,2007.02.27, 说明书第3栏第29-37行,第4栏第19-32行.
US 2005/0193188 A1,2005.09.01, 全文.
US 2007/0094654 A1,2007.04.26, 全文.
审查员 孔昕

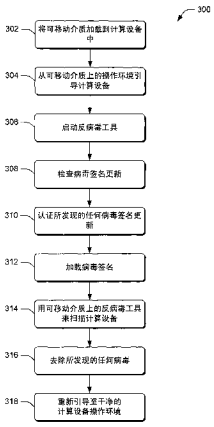
权利要求书2页 说明书6页 附图6页

(54)发明名称

用于恶意软件检测的可信操作环境

(57)摘要

本发明描述了用于扫描计算设备以查找恶意软件的技术和装置。在一个实现中,包括可信操作系统和可信反病毒工具的可信操作环境被包含在可移动数据存储介质上。计算设备然后使用可信操作系统来从可移动数据存储介质引导。可信反病毒工具在计算设备中搜索恶意软件定义更新(例如,病毒签名更新)并使用可信操作系统来扫描该计算设备以查找恶意软件。在另一实现中,计算设备从可移动设备上的可信操作系统引导并且该可移动设备上的可信反病毒工具扫描该计算设备以查找恶意软件。该可移动设备可通过在计算设备或远程资源中搜索更新并认证所定位到的任何更新来更新其自己的内部组件(例如,病毒签名和反病毒工具)。



CN 101681407 B

1. 一种用于恶意软件检测的方法，包括：

作为计算设备引导过程的一部分，将可信操作系统从可移动设备加载到所述计算设备上（404），所述可移动设备包括所述可信操作系统和反病毒工具（202），其中，所述可信操作系统是与所述计算设备的操作系统分开的另一操作系统；

从所述可移动设备中启动所述反病毒工具（406）；

用所述反病毒工具来扫描所述计算设备（408）；

搜索一个或多个可移动设备组件更新（414）；

如果定位到任何可移动设备组件更新，则向所述可移动设备写入所述可移动设备组件更新中的一个或多个（416、418）。

2. 如权利要求 1 所述的方法，其特征在于，从所述可移动设备中启动所述反病毒工具包括从所述可移动设备中加载一个或多个病毒签名。

3. 如权利要求 1 所述的方法，其特征在于，从所述可移动设备中启动所述反病毒工具包括：

搜索所述计算设备上的一个或多个病毒签名更新；

如果定位到任何病毒签名更新，则认证所述病毒签名更新；以及

利用任何通过认证的病毒签名更新来扫描所述计算设备。

4. 如权利要求 1 所述的方法，其特征在于，用所述反病毒工具来扫描所述计算设备包括去除检测到的任何病毒并使用在所述计算设备内部的操作系统来重新引导所述计算设备。

5. 如权利要求 1 所述的方法，其特征在于，所述可移动设备组件更新是病毒签名更新。

6. 如权利要求 1 所述的方法，其特征在于，所述可移动设备组件更新是反病毒工具更新。

7. 如权利要求 1 所述的方法，其特征在于，对一个或多个可移动设备组件更新的搜索至少部分地由所述可移动设备上的更新代理来执行。

8. 如权利要求 1 所述的方法，其特征在于，向所述可移动设备写入所述可移动设备组件更新中的一个或多个包括：

认证所述可移动设备组件更新；以及

只向所述可移动设备写入通过认证的可移动设备组件更新。

9. 如权利要求 8 所述的方法，其特征在于，所述认证由所述可移动设备上的认证工具来实现。

10. 一种用于恶意软件检测的装置，包括：

作为外部计算设备引导过程的一部分来从便携式设备加载到所述外部计算设备的可信操作系统组件（206），其中，所述可信操作系统是与所述外部计算设备的操作系统分开的另一操作系统；

扫描所述外部计算设备的反病毒工具组件（208）；

更新代理组件（214），所述更新代理组件用于搜索便携式设备组件更新，并且如果定位到任何便携式设备组件更新，则向所述便携式设备写入所述便携式设备组件更新中的一个或多个。

11. 如权利要求 10 所述的装置，其特征在于，还包括由所述反病毒工具使用的一个或

多个病毒签名。

12. 如权利要求 10 所述的装置，其特征在于，所述更新代理被配置成搜索在所述外部计算设备和远离所述外部计算设备的资源中的至少一个上的便携式设备组件更新。

13. 如权利要求 10 所述的装置，其特征在于，所述组件更新包括一个或多个病毒签名更新。

14. 如权利要求 10 所述的装置，其特征在于，所述组件更新包括一个或多个反病毒工具更新。

15. 如权利要求 10 所述的装置，其特征在于，还包括用于认证所述更新代理所定位到的任何便携式设备组件更新的认证工具。

16. 一种用于恶意软件检测的方法，包括：

将可移动设备与计算设备接口（602）；

作为计算设备引导过程的一部分，将可信操作系统从所述可移动设备加载到所述计算设备上，所述可移动设备包括所述可信操作系统和反病毒工具，其中，所述可信操作系统是与所述计算设备的操作系统分开的另一操作系统；

在所述计算设备上定位将被存储在所述可移动设备上的一个或多个数据文件（604）；

用驻留在所述可移动设备上的所述反病毒工具来扫描所述数据文件（606）；以及

向所述可移动设备写入所述数据文件（616）。

17. 如权利要求 16 所述的方法，其特征在于，所述扫描还包括去除在所述文件中检测到的任何病毒。

18. 如权利要求 16 所述的方法，其特征在于，所述可移动设备包括计算机可读存储器和处理器。

19. 如权利要求 16 所述的方法，其特征在于，所述可移动设备是通用串行总线设备。

用于恶意软件检测的可信操作环境

[0001] 背景

[0002] 计算机安全在当今技术驱动的文化中是一个严重的问题。计算机安全违背可在该计算机感染病毒和其他形式的恶意软件时发生。这些感染可例如在下载和打开感染恶意软件的文件（例如，电子邮件）时发生，或者感染可在恶意软件在没有任何直接用户干预的情况下通过网络来访问计算机时发生。在任一种情况下，这些安全威胁的流行已导致产生各种各样的可用于计算机的安全相关工具。这些工具的示例包括反病毒程序、广告软件扫描程序、防火墙等。尽管这些工具可用，但计算机继续感染恶意软件。

[0003] 恶意软件感染持久性的一个原因是某些恶意软件对安全工具的隐藏能力。恶意软件可通过使用 rootkit 来对许多安全工具隐藏，该 rootkit 一般而言是旨在对计算机的操作系统隐藏运行进程、文件或系统数据的一组软件工具。rootkit 可将其本身挂钩在计算机的系统中的非常低的地方（例如，在内核层）并截取计算机的操作系统和其他应用程序当在该计算机上运行时利用的主要系统服务。在一个示例中，驻留在计算机上的反病毒工具扫描计算机的硬盘以查找病毒。作为扫描过程的一部分，计算机的操作系统作出一个或多个功能调用，诸如对特定文件的“打开文件”调用。然而，驻留在计算机上的恶意软件可使用 rootkit 来截取该“打开文件”功能调用并返回“文件丢失”错误或返回错误的文件。由此，反病毒工具无法访问所请求的文件并检查该文件以查找病毒感染。如果所请求的文件感染病毒，则该感染将持续不被检测到。

[0004] 概述

[0005] 描述了用于扫描计算设备以查找恶意软件的技术和装置。在一个实现中，包括可信操作系统和可信反病毒工具的可信操作环境被包含在可移动数据存储介质上。计算设备然后使用可信操作系统来从该可移动数据存储介质引导。可信反病毒工具在计算设备中搜索恶意软件定义更新（例如，病毒签名更新）并与可信操作系统交互以扫描该计算设备以便查找恶意软件。另一实现使用诸如具有微控制器的通用串行总线 (USB) 驱动器等可移动设备来存储可信操作环境。计算设备使用可信操作系统来引导并且可信反病毒工具扫描该计算设备以查找恶意软件。该可移动设备可通过在计算设备或远程资源中搜索更新并认证所定位到的任何更新来更新其自己的内部组件（例如，病毒签名和反病毒工具）。

[0006] 提供本概述是为了以简化的形式介绍将在以下详细描述中进一步描述的一些概念。该概述不旨在标识所要求保护的主题的关键特征或必要特征，也不旨在用于帮助确定所要求保护的主题的范围。

[0007] 附图简述

[0008] 参考附图来描述该详细描述。在附图中，附图标记中的最左边的数字标识该附图标记首次出现的附图。在不同附图中使用同一附图标记来指示相似或相同的项目。

[0009] 图 1 示出了用于实现扫描计算设备以查找恶意软件的技术的示例性体系结构和可移动数据存储介质。

[0010] 图 2 示出了用于实现扫描计算设备以查找恶意软件的技术的示例性体系结构和可移动设备。

[0011] 图 3 是用于搜索恶意软件更新并扫描计算设备以查找恶意软件的示例性过程的流程图。

[0012] 图 4 是用于扫描计算设备以查找恶意软件并更新可移动设备的组件的示例性过程的流程图。

[0013] 图 5 是用于认证可移动设备组件更新的示例性过程的流程图。

[0014] 图 6 是用于安全文件存储的示例性过程的流程图。

[0015] 详细描述

[0016] 此处所描述的设备和技术提供了一种可用于扫描计算设备以查找病毒和其他形式的恶意软件并消除任何这些实体对该计算设备的感染 (disinfect) 的可信操作环境。术语“病毒”和“恶意软件”在此处可互换地使用，并且两者一般都指的是被设计成在没有所有者告知的同意的情况下渗入和 / 或破坏计算机系统的计算机代码的集合。恶意软件的其他示例包括特洛伊木马、蠕虫、间谍软件等。可信操作环境由诸如软件或硬件制造商等可信授权机构创建，并且然后被包含在可与计算设备接口的设备或计算机可读介质上。对可信操作环境的非授权访问通过使用只准许可信数据访问可信操作环境的只读介质、认证协议和微控制器来阻止。如此处所使用的，术语认证指的是可被实现来验证通信或数据文件所源自的实体的身份并确保该通信或数据文件未被非授权实体篡改或不被允许地更改的任何合适的方法或协议。

[0017] 在一个示例中，可信操作环境包括可信操作系统和可信反病毒工具。计算设备可使用可信操作系统来引导并由此避开可隐藏在该计算设备上的 rootkit 和其他恶意软件的问题。可信反病毒工具然后可扫描计算设备并确保其与可信操作系统的交互将准确地反映该计算设备的状态。

[0018] 示例性体系结构

[0019] 图 1 示出了可实现所述过程和技术的体系结构 100。计算设备 102 是体系结构 100 的一部分。尽管被示为台式 PC，但计算设备 102 可被实现为各种常规计算设备中的任一种，包括例如，服务器、笔记本或便携式计算机、工作站、大型计算机、移动通信设备、PDA、娱乐设备、机顶盒、因特网设备、游戏控制台等。

[0020] 计算设备 102 可包括但不限于，一个或多个处理器 104、存储器 106、输入 / 输出 (I/O) 设备 108(例如，键盘和鼠标) 以及操作上将包括处理器 104 在内的各种组件耦合到存储器 106 的系统总线 (未示出)。计算设备 102 的存储器包括诸如随机存取存储器 (RAM) 等易失性存储器形式的和 / 或诸如只读存储器 (ROM) 或闪速 RAM 等非易失性存储器形式的计算机可读介质。存储器 106 通常包括数据和 / 或程序模块，诸如操作系统 110 和病毒更新包 112。数字签名 114 和病毒签名更新 116 是病毒更新包 112 的一部分，这两者将在以下更详细地讨论。

[0021] 为了实现病毒扫描过程，用户将可移动数据存储介质 118 加载到计算设备 102 中以使得该计算设备可读取该可移动介质。可移动数据存储介质 118 是可与计算设备接口 (例如，通过将其插入盘驱动器中) 并在不必拆卸计算设备的情况下移除的数据存储介质。尽管可移动数据存储介质 118 在此处被示为紧致盘 (CD) 或数字多功能盘 (DVD)，但可采用任何合适的计算机可读可移动数据存储介质，包括其他光存储介质，闪存、盒式磁带、磁带、磁盘存储或其它磁存储设备，或者可用于存储所需信息并可由计算机访问的任何其它可移

动存储介质。此外，可移动数据存储介质 118 可以是只读介质以使得其上所包含的数据和文件无法被来自感染源（例如，计算设备 102）的、试图感染该存储介质的恶意软件感染。

[0022] 用户然后从可移动数据存储介质 118 引导计算设备 102。可移动数据存储介质 118 包括可移动介质存储器 120，该存储器存储用于实现所述过程的数据和 / 或程序模块和组件。如在此使用的术语“模块”或“组件”一般表示软件、固件、或者软件和固件的组合。作为引导过程的一部分，计算设备 102 从可移动介质存储器 120 中加载可信操作系统 (OS) 122。可信反病毒工具 124 然后自动或通过用户所表示的动作从可移动介质存储器 120 中启动。

[0023] 可信反病毒工具 124 然后加载存储在可移动介质存储器 120 上的病毒签名 126。病毒签名 126 是用于标识病毒的一组病毒“指纹”。示例性病毒签名是病毒的计算机代码的全部或部分的二进制模式。可信反病毒工具 124 还搜索计算设备 102 并标识当前未被存储在可移动介质存储器 120 上的任何病毒签名。在一个示例中，可信反病毒工具 124 在存储器 106 上定位包含病毒签名更新 116 的病毒更新包 112。病毒签名更新 116 包括一个或多个病毒签名，其中的某一些可以与存储在可移动数据存储介质 118 上的任何病毒签名不同（例如，它们可标识更新近编目的病毒）。在将病毒签名更新 116 用于病毒扫描之前，可信反病毒工具 124 使用认证工具 128 来验证病毒更新包 112 的真实性。

[0024] 为了验证和 / 或认证病毒更新包 112，认证工具 128 利用来自可移动介质存储器 120 的根证书 130 来认证数字签名 114。一般而言，数字签名 114 是已编码的消息或其他数据片段，将数字签名 114 与根证书 130 进行比较以确定病毒更新包 112 是否源自可信授权机构并且未被篡改。在一个示例中，数字签名 114 是诸如 X.509 证书等作为病毒更新包 112 的一部分的数字证书的一部分。如果数字签名 114 被确定为是真实的，则可信反病毒工具 124 将病毒签名更新指定为通过认证并加载该病毒签名更新。该认证方法只是出于示例的目的而给出的，并且可利用任何合适的密码、验证和 / 或认证协议来验证病毒签名更新源自可信授权机构。

[0025] 可信反病毒工具 124 然后在计算设备 102 上运行并使用病毒签名 126 以及来自病毒更新包 112 的任何通过认证的病毒签名更新来扫描计算设备 102 以查找病毒。通过在病毒扫描时与可信操作系统 122 交互，用户可确保在病毒扫描过程期间作出的操作系统调用将正确地返回所请求的文件并给出对计算设备 102 的准确描述。

[0026] 此外，对于体系结构 100，计算设备 102 可使用网络 132 来访问远程资源 134。网络 132 可包括但不限于，局域网 (LAN)、广域网 (WAN) 和城域网 (MAN)。远程资源 134 可以是 web 服务器、服务器场、大型计算机、数据中心或能够存储和 / 或传输数据的任何其他资源。由此，可信反病毒工具 124 可利用计算设备 102 和网络 132 来访问远程资源 134 并标识和下载驻留在该远程资源上的一个或多个病毒签名更新。将如以上所讨论地认证远程资源 134 上所标识的任何病毒签名更新。

[0027] 图 2 示出了可实现所述过程和技术及其变体的示例性体系结构 200。体系结构 200 包括图 1 所介绍的计算设备 102。还示出了可移动设备 202。尽管可移动设备 202 在此处被示为通用串行总线 (USB) 设备，但可利用任何合适的可移动和 / 或便携式设备，诸如 PC 卡、智能卡、火线设备等。在操作中，可移动设备 202 与计算设备 102 接口并且该计算设备从该可移动设备引导。作为引导过程的一部分，计算设备 102 访问可移动设备 202 上的存储器 204 并加载可信操作系统 206。存储器 204 通常包括可立即由微控制器 216 访问和 /

或当前正在计算设备 102 上操作的、用于实现所述过程的数据、程序模块和组件。

[0028] 可信反病毒工具 208 然后从存储器 204 中启动并且该可信反病毒工具从存储器 204 中加载病毒签名 210。可信反病毒工具 208 可任选地使用类似于以上参考图 1 所讨论的过程来在计算设备 102 上定位并认证病毒签名更新。可信反病毒工具 208 然后继续使用所加载的病毒签名来扫描计算设备 102 以查找病毒。通过与在计算设备 102 上运行的可信操作系统 206 交互，可信反病毒工具 208 可执行对计算设备 102 的彻底的病毒扫描，包括任何存储设备（例如，硬盘驱动器）、基本输入 / 输出系统 (BIOS)、硬件、固件等。如果定位到任何病毒，则从计算设备 102 中去除该病毒。计算设备 102 然后可使用其自己的内部操作系统来重新引导至干净的操作环境中。

[0029] 可移动设备 202 具有使用更新代理 214 和微控制器 216 来安全地更新自自己的内部组件的能力。微控制器 216 是包括控制可移动设备 202 的特定过程和动作所必需的组件的集成电路或微处理器。尽管未在图 2 中示出，但微控制器 216 的组件包括一个或多个处理器、一种或多种形式的存储器（例如，只读存储器和 / 或随机存取存储器）、输入 / 输出端口、定时器等。

[0030] 可更新可移动设备 202 的任何组件，包括病毒签名 210 和可信反病毒工具 208。作为更新过程的一部分，微控制器 216 可利用更新代理 214 来在计算设备 102 中搜索一个或多个可移动设备组件更新。微控制器 216 还可利用更新代理 214 来经由计算设备 102 和网络 132 访问远程资源 134 以获得所需组件更新。如果定位到任何组件更新，则认证工具 212 可使用任何合适的认证和 / 或密码协议来验证组件更新源自可信授权机构。如果认证工具 212 确定组件更新是真实的（即，该组件更新通过认证过程），则向存储器 204 写入该组件更新。否则，微控制器 216 阻止任何未通过认证的和未经授权的数据（例如，未通过认证过程的组件更新）被写入到存储器 216 上。将微控制器 216 用作“看门人”准许动态更新可移动设备 202 同时维护其内部组件的可信方面。

[0031] 示例性过程

[0032] 图 3 示出了用于执行病毒扫描的示例性过程 300。过程 300 被示为逻辑流程图中的框集合，该框集合表示可用硬件、软件或其组合来实现的操作序列。在软件的上下文中，各个框表示在由一个或多个处理器执行时执行既定操作的计算机指令。虽然以下各过程按照单独的动作来讨论，但这并非旨在是限制性的，并且在某些示例中可组合所讨论的动作。出于讨论的目的，过程 300 参考图 1 所示的体系结构 100 来描述。

[0033] 在 302，将可移动数据存储介质（诸如可移动数据存储介质 118）加载到计算设备中。在 304，从可移动数据存储介质上的可信操作环境引导计算设备。作为该引导过程的一部分，可信操作系统从可移动数据存储介质加载到计算设备上。在 306，从可移动数据存储介质中启动可信反病毒工具。动作 306 可通过从可移动数据存储介质运行可信反病毒工具或者将该可信反病毒工具加载到计算设备上并从该计算设备运行该工具来完成。在 308，可新反病毒工具搜索计算设备并定位任何病毒签名更新。病毒签名更新可以是病毒更新包的一部分，该病毒更新包包括病毒签名更新和可用于认证更新的数字签名。数字签名可以是诸如 X.509 证书等作为病毒更新包的一部分来存储在计算设备上或存储在计算设备上的其他地方的认证证书的一部分。可信反病毒工具还可利用计算设备和网络来在远程资源中搜索病毒签名更新。如果定位到和 / 或标识了任何病毒签名更新，则在 310 处认证这些更

新。在一个示例中，动作 310 包括处理数字签名以确定病毒签名更新是否源自可信授权机构。

[0034] 在 312，可信反病毒工具连同任何通过认证的病毒签名更新一起加载存储在可移动数据存储介质上的任何病毒签名。在 314，可信反病毒工具与计算设备上所加载的可信操作系统交互以扫描该计算设备以查找匹配所加载的病毒签名的任何病毒。可信反病毒工具可执行对计算设备的全面扫描，包括任何存储设备（例如，硬盘驱动器）、BIOS、硬件、固件等。在 316，从计算设备中去除所定位到的任何病毒。在 318，将计算设备重新引导至干净的内部操作环境中。该内部操作环境包括已使用此处所讨论的技术来扫描并清除了任何病毒或其他恶意软件的操作系统。

[0035] 图 4 示出了用于执行病毒扫描的示例性过程 400。过程 400 被示为逻辑流程图中的框集合，该框集合表示可用硬件、软件或其组合来实现的操作序列。在软件的上下文中，各个框表示当由一个或多个处理器执行时完成既定操作的计算机指令。出于讨论的目的，过程 400 参考图 2 所示的体系结构 200 来描述。

[0036] 在 402，将可移动设备（例如，可移动设备 202）与用户希望扫描以查找病毒的计算设备接口。在一个示例中，动作 402 通过将可移动设备插入到计算设备上的适当的端口（例如，USB 端口）中来完成。在 404，从可移动设备引导计算设备。作为该引导过程的一部分，可信操作系统从可移动设备加载到计算设备上。在 406，从可移动设备中启动可信反病毒工具。动作 406 可通过从可移动设备运行可信反病毒工具或者将该可信反病毒工具加载到计算设备上并从该计算设备运行该工具来完成。作为动作 406 的一部分，可信反病毒工具加载存储在可移动设备上的一个或多个病毒签名。可移动设备还可定位存储在计算设备和 / 或远程资源上的一个或多个病毒签名更新，认证病毒签名更新并加载任何通过认证的病毒签名更新。在 408，可信反病毒工具与计算设备上所加载的可信操作系统交互以扫描该计算设备以查找任何病毒。该反病毒工具基于存储在可移动设备上的病毒签名加上来自计算设备的任何通过认证的病毒签名更新来标识任何病毒。在 410，去除所定位到的任何病毒。

[0037] 在 412，将计算设备重新引导至包括已扫描并清除了病毒的操作系统的干净的内部环境。该内部操作系统是驻留在计算设备上的操作系统（即，该操作系统不是从可移动设备中加载的操作系统）。在 414，可移动设备然后检查对其内部组件（例如，病毒签名和反病毒工具本身）的更新。该可移动设备可在计算设备中搜索组件更新，或者可任选地访问远程资源以搜索组件更新。如果定位到任何组件更新，则在 416，使用任何合适的认证和 / 或密码过程来认证组件更新。如果任何组件更新通过该认证过程，则在 418，在可移动设备上安装组件更新。尽管此处未示出，但该过程可任选地返回到动作 404 并使用在 418 处安装在可移动设备上的任何病毒签名更新（或其他组件更新）来重新扫描计算设备以查找病毒。

[0038] 由此，如图所示，过程 400 允许使用从可移动设备中加载的可信操作系统来对计算设备执行病毒扫描。一旦已扫描计算设备并消除了任何病毒对其的感染，可移动设备然后就可搜索对其自己的内部组件的任何更新，认证所定位到的任何更新并加载通过认证的更新。在某些实现中，该过程通过在最常规的文件系统操作期间（例如，在病毒扫描期间）以只读模式操作可移动设备来实现，由此防止病毒和其他恶意软件感染该可移动设备。在

更新操作期间，组件更新包被传送到可移动设备并经受认证。可移动设备上的微控制器控制认证过程并检查组件更新包以查找签名和/或证书。如果微控制器确定特定更新包的签名和/或证书有效，则该微控制器将允许向可移动设备写入该更新包。否则，可移动设备将保持只读状态以维护其可信操作环境的完整性。

[0039] 图5示出了用于认证可移动设备组件更新的过程的一个示例，如以上在图4的动作416中所示出的。在500，定位并取得与任何可移动设备组件更新相关联的数字签名。如以上所讨论的，该数字签名可以是总认证证书的一部分。在502，根据任何合适的认证和/或密码协议来处理数字签名。在一个示例中，数字签名用存储在可移动设备上的根证书来验证。在504，确定数字签名是否通过了认证过程。如果数字签名被确定为源自可信授权机构（即，被指定为真实的），则在506，向可移动设备写入与该数字签名相关联的可移动设备组件更新。如果数字签名未通过认证过程，则在508，不向可移动设备写入可移动设备组件更新。在一个示例中，动作508可包括从计算设备中删除未通过认证过程的任何可移动设备组件更新。

[0040] 安全存储

[0041] 图6示出了用于实现安全存储设备的示例性过程600。过程600被示为逻辑流程图中的框集合，该框集合表示可用硬件、软件或其组合来实现的操作序列。在软件的上下文中，各个框表示当由一个或多个处理器执行时完成既定操作的计算机指令。出于讨论的目的，过程600参考图2所示的可移动设备202来描述。

[0042] 在602，将可移动设备与计算设备接口。在一个示例中，动作602通过将可移动设备插入到计算设备上的适当的端口（例如，USB端口）中来完成。在604，在计算设备上定位用户希望将其复制和/或传送到可移动设备的至少一个数据文件。在一个示例中，可定位多个文件，并由此将对每一个文件执行所示过程。该数据文件可本地地存储在计算设备上或者可位于可由该计算设备访问的远程资源上。在606，用驻留在可移动设备上的反病毒工具来扫描数据文件以查找病毒。在608，确定数据文件是否感染病毒或其他恶意软件。如果在数据文件中检测到任何病毒/恶意软件，则在610，使用反病毒工具来消除病毒对该数据文件的感染（即，从文件中去除病毒）。如果未在文件中检测到病毒或其他恶意软件，则在616，将该文件复制到可移动设备。在612，确定是否已成功消除受感染文件的感染。如果未成功消除文件感染，则在614，阻止将该文件复制到可移动设备。任选地，可在另一次消除文件感染的尝试时用反病毒工具来重新扫描该文件。如果已成功消除文件的感染，则在616，将消除感染的文件复制到可移动设备。可移动设备然后可将所复制的文件传送到其他设备而不害怕传播可能已感染文件的任何病毒。这在其中许多不同的用户可访问特定设备的公共终端情形（例如，图书馆）中尤其有用。在这些情况下，用户可能无意地访问受感染的文件并将其下载到公共终端上。使用该安全存储过程，用户可确保从这一终端下载的任何文件都不会受到病毒感染。

[0043] 结论

[0044] 虽然已经用对结构特征和/或方法步骤专用的语言描述了本发明，但是应当理解，所附权利要求书中定义的本发明不必限于所描述的具体特征或步骤。相反，各具体特征和步骤是作为实现所要求保护的本发明的较佳形式来公开的。

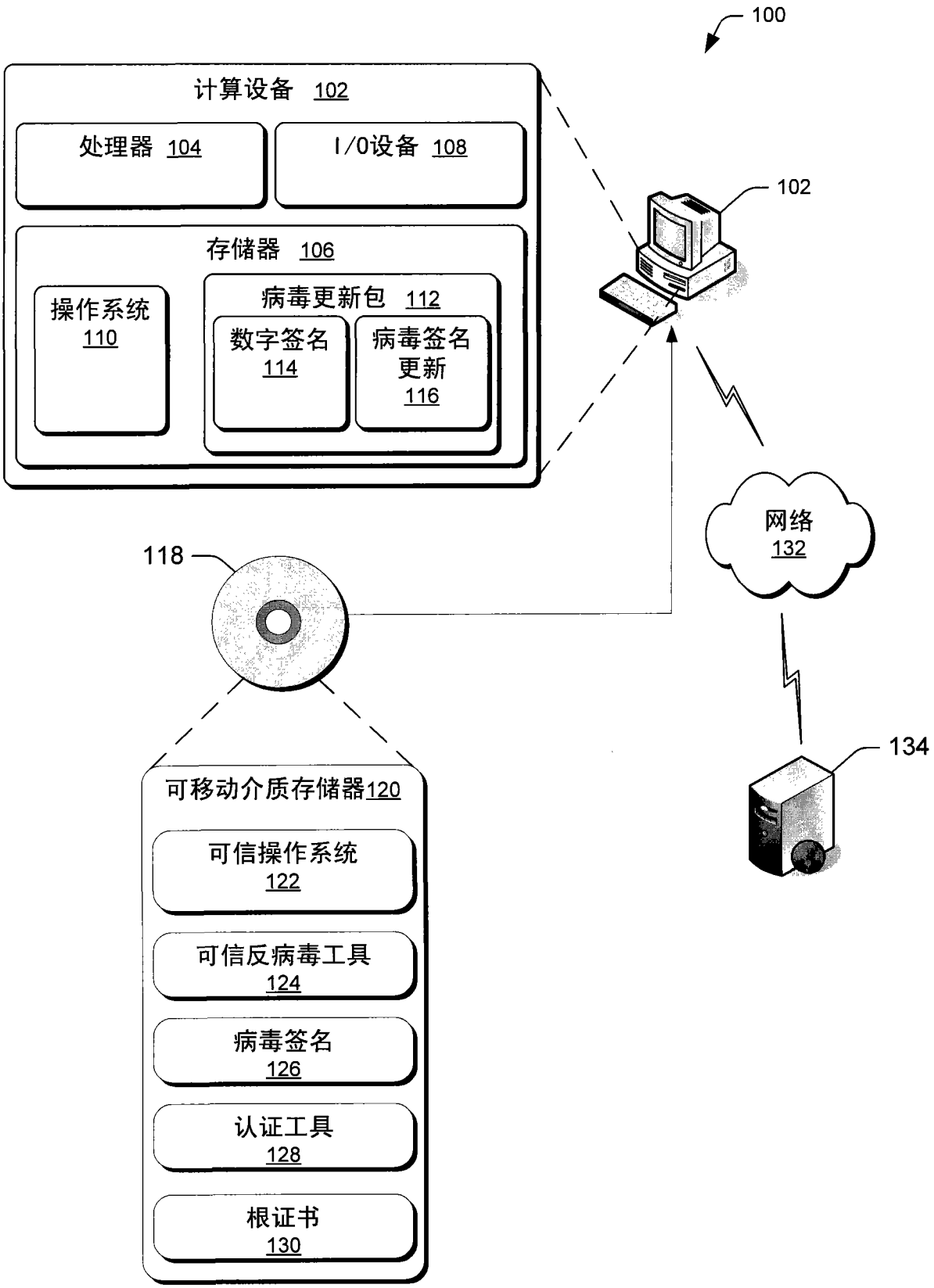

100
计算设备 102
处理器 104
I/O设备 108
存储器 106
操作系统 110
病毒更新包 112
数字签名 114
病毒签名更新 116
102
网络 132
118
134
可移动介质存储器120
可信操作系统 122
可信反病毒工具 124
病毒签名 126
认证工具 128
根证书 130

图 1

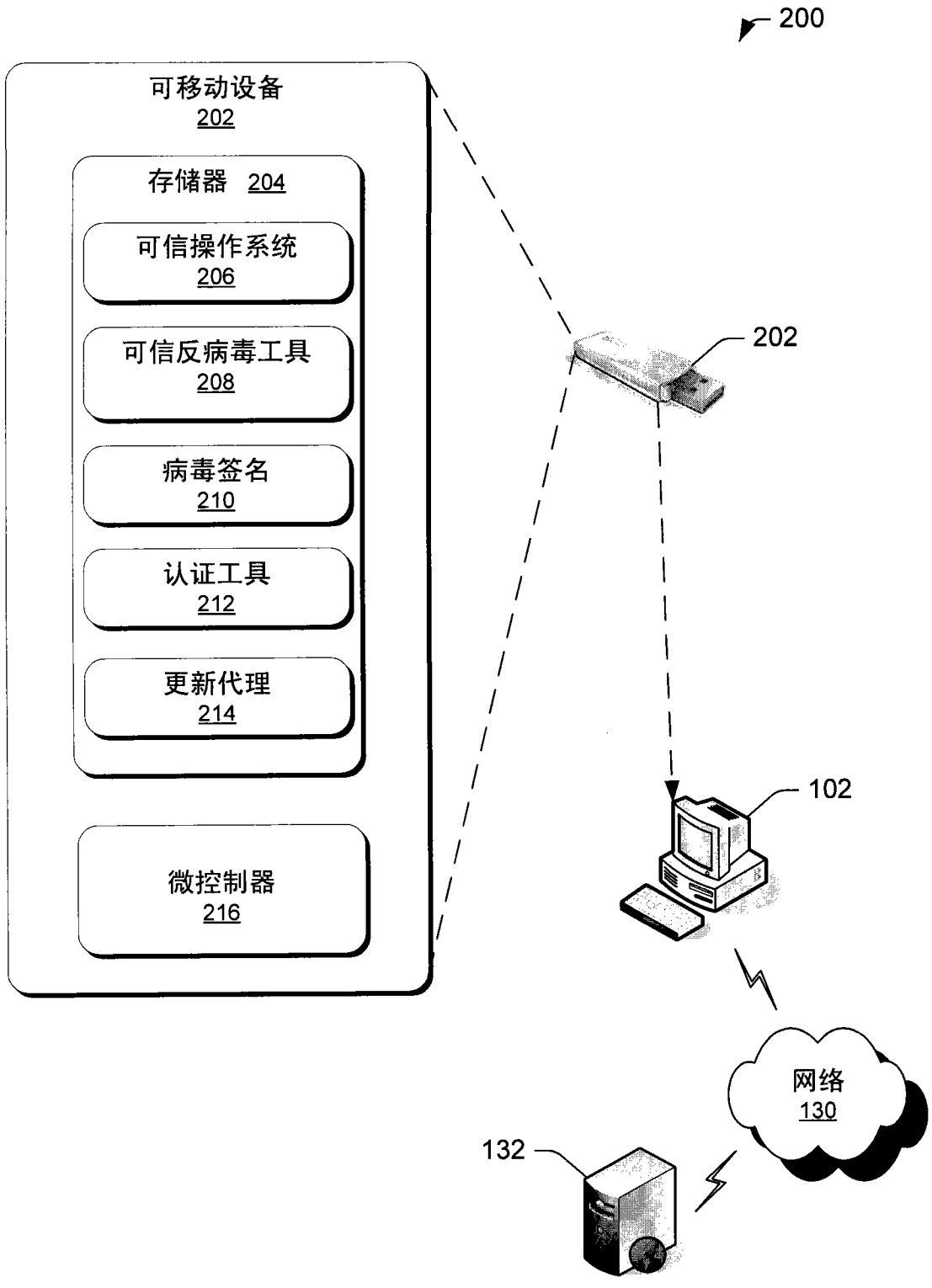

200
可移动设备
202
存储器 204
可信操作系统
206
可信反病毒工具
208
病毒签名
210
认证工具
212
更新代理
214
微控制器
216
202
102
网络
130
132

图 2

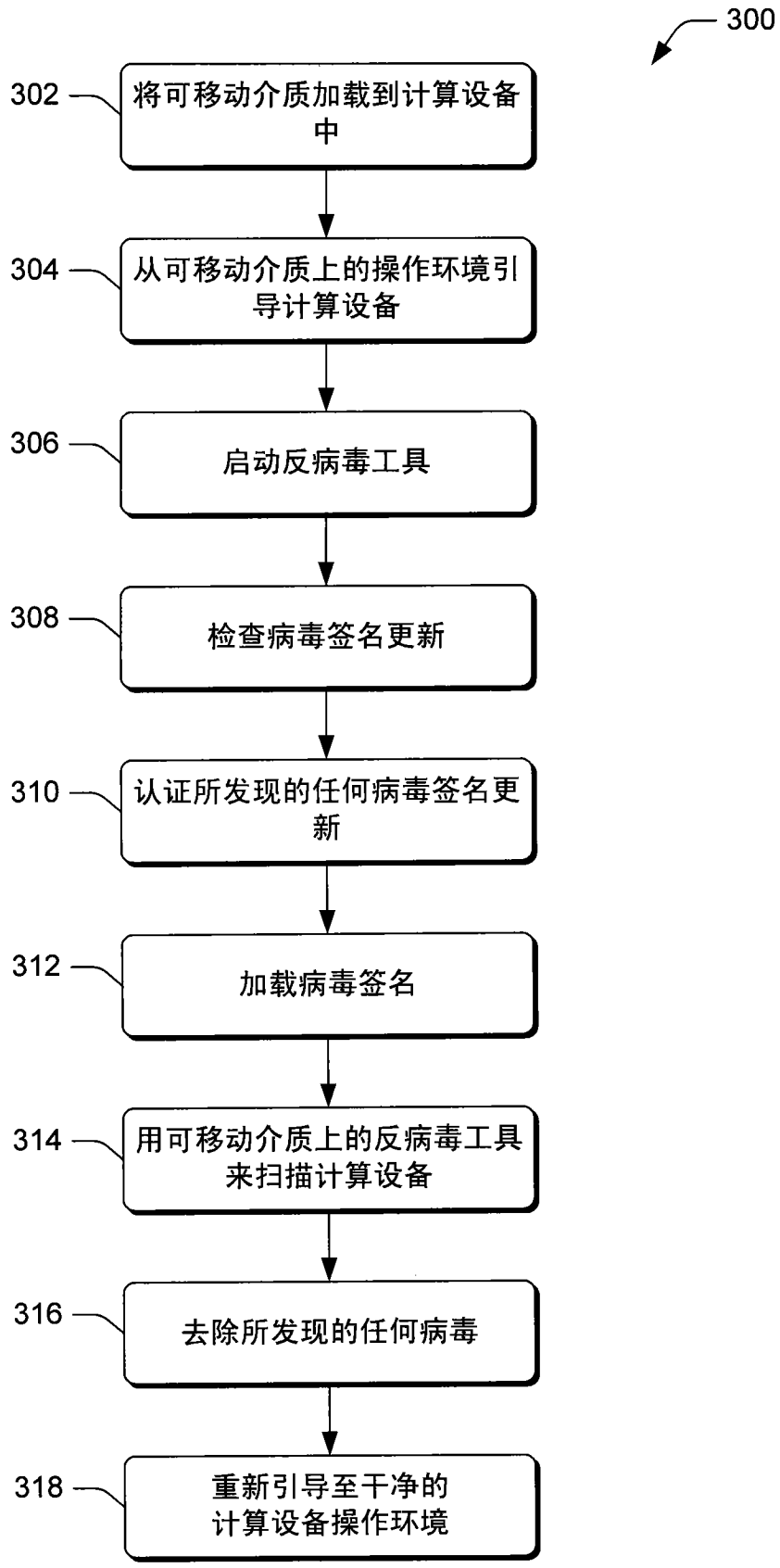

300
302
将可移动介质加载到计算设备中
304
从可移动介质上的操作环境引导计算设备
306
启动反病毒工具
308
检查病毒签名更新
310
认证所发现的任何病毒签名更新
312
加载病毒签名
314
用可移动介质上的反病毒工具来扫描计算设备
316
去除所发现的任何病毒
318
重新引导至干净的计算设备操作环境

图 3

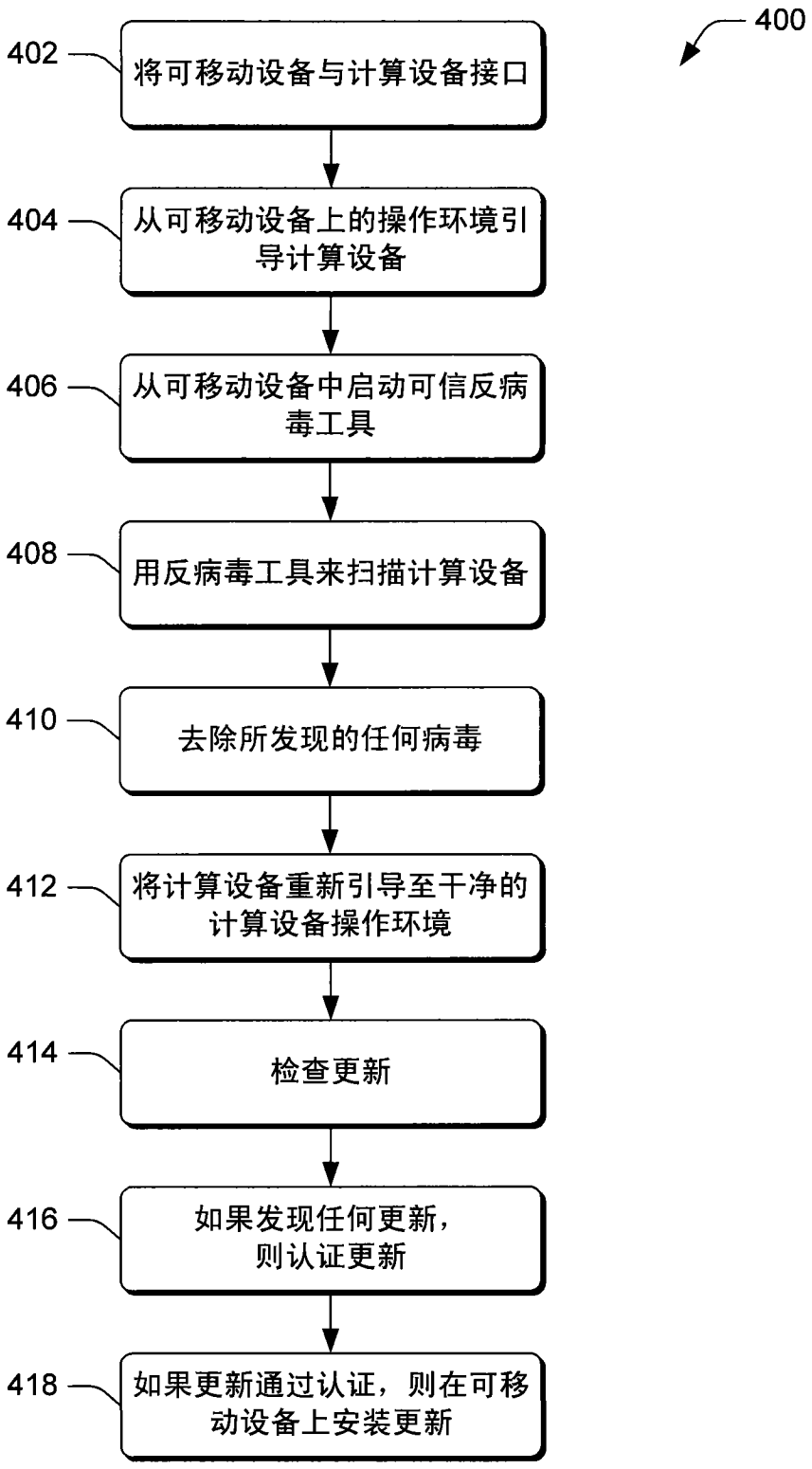

400
402
将可移动设备与计算设备接口
404
从可移动设备上的操作环境引导计算设备
406
从可移动设备中启动可信反病毒工具
408
用反病毒工具来扫描计算设备
410
去除所发现的任何病毒
412
将计算设备重新引导至干净的计算设备操作环境
414
检查更新
416
如果发现任何更新，则认证更新
418
如果更新通过认证，则在可移动设备上安装更新

图 4

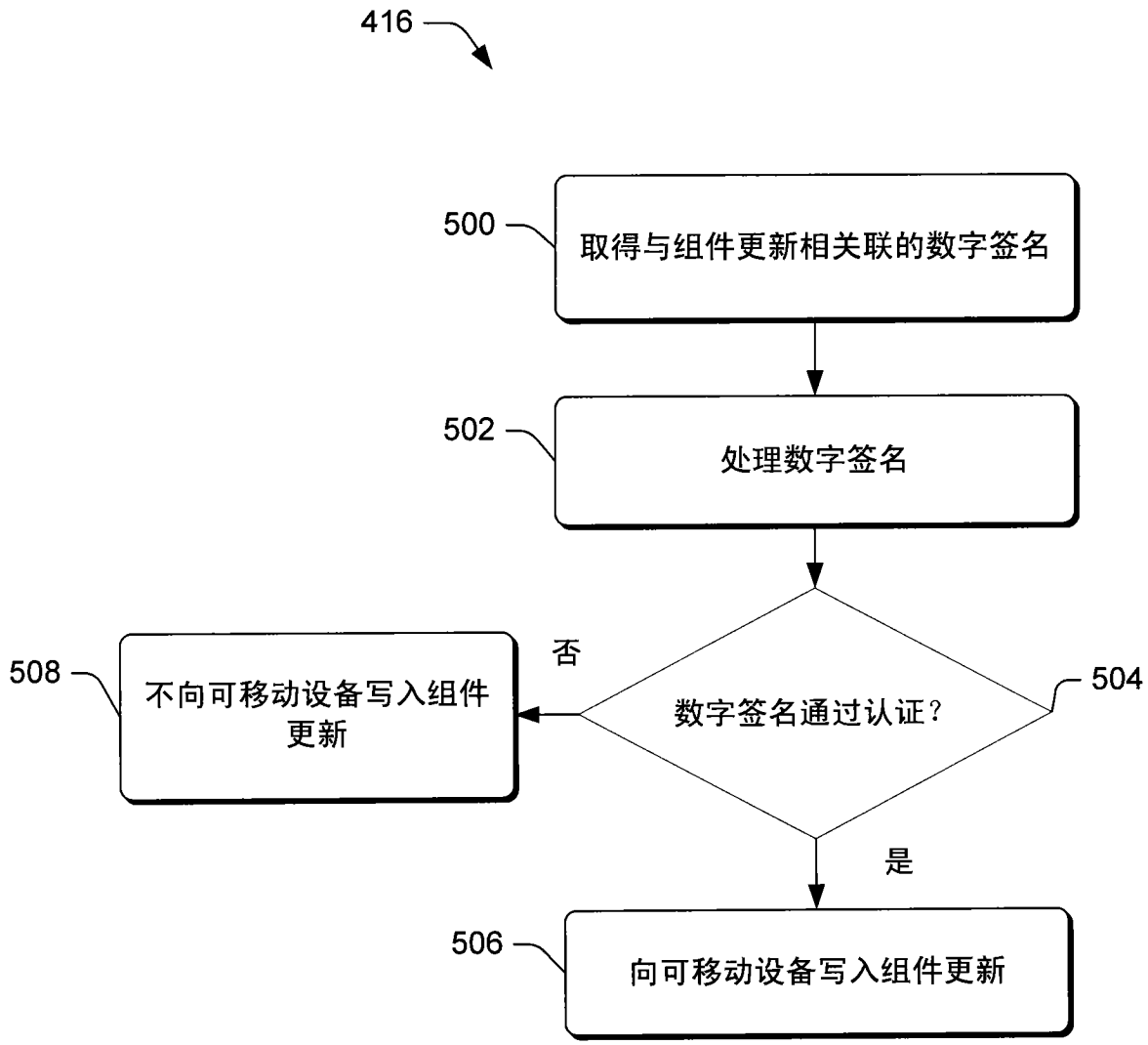

416
500
取得与组件更新相关联的数字签名
502
处理数字签名
数字签名通过认证？
504
否
508
不向可移动设备写入组件更新
是
506
向可移动设备写入组件更新

图 5

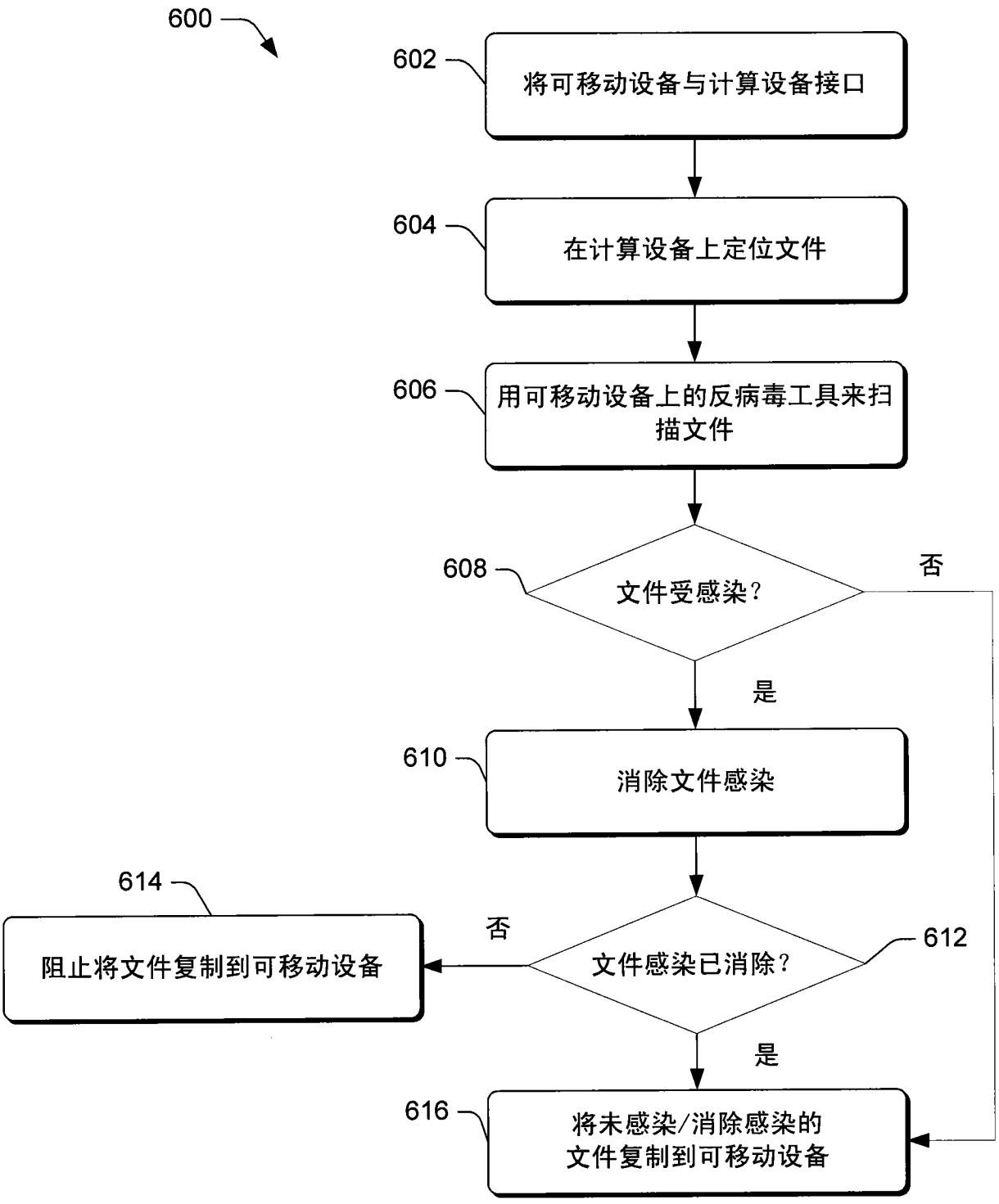

600
602
将可移动设备与计算设备接口
604
在计算设备上定位文件
606
用可移动设备上的反病毒工具来扫描文件
608
文件受感染?
否
是
610
消除文件感染
614
阻止将文件复制到可移动设备
否
文件感染已消除?
612
是
616
将未感染/消除感染的文件复制到可移动设备

图 6