[19] 中华人民共和国国家知识产权局

[12] 发明专利说明书

专利号 ZL 200610092754.X

[51] Int. Cl.
H04L 12/24 (2006.01)
H04L 12/26 (2006.01)
H04L 9/00 (2006.01)
G06F 12/14 (2006.01)
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)

[45] 授权公告日 2009 年 3 月 4 日

[11] 授权公告号 CN 100466547C

[22] 申请日 2006.6.13
[21] 申请号 200610092754.X
[30] 优先权
[32] 2005.6.29 [33] EP [31] 05254068.9
[73] 专利权人 捷讯研究有限公司
地址 加拿大安大略省沃特卢市
[72] 发明人 尼尔·P·亚当斯
赫伯特·A·利特尔
[56] 参考文献
CN1322432A 2001.11.14
CN1265489A 2000.9.6
JP2003-58764A 2003.2.28

Analysis of the Security of Windows NT. HANS HEDBOM, STEFAN LINDSKOG, STEFANAXELSSON, ERLAN JONSSON. ANALYSIS OF THE SECURITY OF WINDOWS NT. 1999

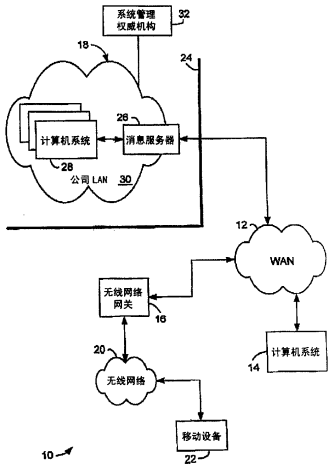
Using Software Restriction Policies in Windows XP andWindows . NET Server to Protect Against UnauthorizedSoftware. MICROSOFT WINDOWS XP AND WINDOES . NET TECHNICAL ARTICLE. 2002
审查员 左子湄
[74] 专利代理机构 中科专利商标代理有限责任公司
代理人 王 玮
权利要求书 3 页 说明书 14 页 附图 5 页

[54] 发明名称

特权管理和撤消系统和方法

[57] 摘要

本公开涉及一种系统和方法，用于管理与特定应用程序相关的特权，并且即时地和以鲁棒方式来撤消这些特权。 例如，该设备跟踪哪些应用程序对哪些特权进行访问。 当策略或应用程序控制改变时，该系统检测针对哪些应用程序已经撤消了哪些特权。 这可以简单地通过将较早特权集合与新特权集合的比较来实现。 对于给定应用程序的每一个撤消特权，该系统确定该应用程序过去是否曾经访问过该特权。 如果应用程序过去已经访问了现在被撤消的特权，该设备被复位。 为了确保可能在应用程序之间传递的特权不被忽略，该设备配置为如果可由该设备访问的任何撤消特权是可以在应用程序之间传递的特权，则执行复位。



1. 一种在电子系统中管理与应用程序相关的特权的方法，包括：

监控电子系统中的设备，以检测正在由所述电子系统中的任意设备使用的应用程序（300）对特权的使用；

记录哪些应用程序已经访问了哪些特权（302）；

检测所述系统的特权的变化（304）；

将应用程序先前所访问的已记录特权与特权变化集合进行比较（306）；

根据所述比较步骤（306）的结果来识别要撤消的任意特权（308）；

当识别了要撤消的特权时，关闭先前已经访问所述撤消特权的应用程序（310）；以及

重新启动由于已经访问撤消特权而被关闭的任意应用程序（312）。

2. 根据权利要求 1 所述的方法，其特征在于所述记录步骤包括：

存储与已经访问了特权的应用程序相关的应用程序标识符；以及

将所述标识符与由应用程序访问的特权相关联。

3. 根据权利要求 2 所述的方法，其特征在于与所述已记录特权相关的数据存储在列出了应用程序标识符和与应用程序标识符相关的特权的数据表中。

4. 根据权利要求 1 所述的方法，其特征在于所述特权变化集合包括要撤消的特权。

5. 根据权利要求 1 所述的方法，其特征在于所述特权变化集合包括能够使用的所有特权的列表，而并不包括要撤消的特权。

6. 根据权利要求 1 所述的方法，其特征在于所述设备包括无线移动电子通信设备。

7. 根据权利要求 1 所述的方法，其特征在于还包括：连续重复所述监控、记录、检测、比较、识别、关闭和重新启动步骤。

8. 根据权利要求 1 所述的方法，其特征在于所述特权变化是系统 IT 策略变化的结果。

9. 一种在包括多个电子设备的系统中管理特权的方法，所述方法包括：

由系统的每一个设备监控每一个设备上的哪些应用程序能够访问哪些特权（600）；

记录能够经由驻留在系统的每一个设备上的应用程序访问的特权（602）；

检测能够用于所述系统中的所述设备的特权变化（604）；

将较早特权集合与新特权集合进行比较（606），所述新特权集合对应于所述特权变化；

根据所述比较（606）来确定是否要撤消任何特权（608）；

复位能够访问要撤消的特权的每一个设备（610）；

确定要撤消的任何特权是否能够在应用程序之间传递（614）；以及

当要撤消的特权能够在应用程序之间传递时，复位能够访问能够在应用程序之间传递的要撤销的所述特权的每一个设备（610）。

10. 根据权利要求 9 所述的方法，其特征在于所述特权变化是系统 IT 策略变化的结果。

11. 根据权利要求 9 所述的方法，其特征在于所述特权变化包括要撤消特权的指示。

12. 根据权利要求 9 所述的方法，其特征在于所述复位能够访问要撤消的特权的每一个设备以及所述复位能够访问能够在应用程序之间传递的要撤销的所述特权的每一个设备的步骤使所述系统进入已知状态。

13. 根据权利要求 12 所述的方法，其特征在于还包括：在能够访问要撤消的特权的每一个设备以及能够访问能够在应用程序之间传递的要撤销的所述特权的每一个设备已经被复位之后，重新启动每个对应设备（612）。

14. 根据权利要求 9 所述的方法，其特征在于所述电子设备包括

移动无线通信设备。

15. 一种在包括多个电子设备（500）的网络中管理特权的系统，所述系统包括：

驻留在系统的每一个设备上的处理器（538），用于监控每一个设备上的哪些应用程序能够访问哪些特权；

存储器（524），记录能够经由系统的每一个设备上驻留的应用程序访问的特权；以及

其中所述处理器能够操作来：

检测能够用于所述系统中的所述设备的特权变化；

将较早特权集合与新特权集合进行比较，所述新特权集合对应于所述特权变化；

根据所述比较（606）来确定是否要撤消任何特权；

复位能够访问要撤消的特权的每一个设备；以及

确定要撤消的任何特权是否能够在应用程序之间传递，并且当要撤消的特权能够在应用程序之间传递时，复位能够访问能够在应用程序之间传递的要撤销的所述特权的每一个设备。

特权管理和撤消系统和方法

技术领域

本发明通常涉及与可由诸如网络计算机、移动无线通信设备等电子设备的用户访问的特定应用程序相关的特权的管理。特别地，本公开涉及一种管理与特定应用相关的特权和按照即时和鲁棒方式来撤消这些特权的系统和方法。

背景技术

如所公知的，诸如网络计算机、移动无线通信设备等特定电子设备包括驻留在能够对特定特权进行访问的一些设备上的应用程序，所述特权使应用程序能够执行各种功能。典型地，系统管理员可以使用IT策略和应用程序控制来设置与存在于受到管理员控制的设备上的各种应用程序相关的特权。特权示例可以包括诸如：允许应用程序使用处理间通信（IPC）、实现内部和外部连接的开放、实现浏览过滤器的插入、实现Bluetooth™功能、实现电子邮件的使用、实现个人信息管理（PIM）功能的使用、应用程序接口（API）的使用等。对于系统管理员重要的是，能够跟踪哪些应用程序能够访问哪些特权，并且能够按照需要来撤消特权。

例如，如果应用程序能够访问特权，且系统撤消该特权，则应用程序应该立即、或者在较小的时间窗之内被拒绝访问该特权。换句话说，应该尽可能快地撤消该特权。可以触发特权撤消的事件可以包括诸如：在IT管理员/应用程序控制数据存在于该设备上之前应用程序被加载；应用程序被发现是无赖应用程序；或者公司策略改变，导致了对特定应用程序和/或与之相关的特权的使用的限制。

与特权撤消的理由无关，必须按照安全方式和按照防止恶意应用程序或个人的可能侵入（work arounds）的方式来实现这样的撤消。

通常，根据当前特权撤消策略，典型地，在第一次访问特权时，执行该特权校验。例如，应用程序利用应用程序登记处与IPC通信。一旦应用程序具有到应用程序登记处的引用（例如指针），则难以使该引用脱离该应用程序。在另一示例中，如果应用程序已经利用IPC将其的一部分特权传递给另一应用程序，传统系统可以检测第一应用程序能够对IPC进行访问，但是不存在检测所述另一应用程序已经被传递了该特权的方式。

因此，需要一种系统和方法，用于有效地管理与应用程序相关的特权，特别是当需要特权撤消时，按照即时和鲁棒方式来撤消这些特权。

发明内容

考虑到以上描述，现在已经发现了一种有效、精确、鲁棒和易于实现的系统和方法，用于管理与特定应用程序相关的特权并按照即时和可靠的方式来撤消这些特权。

根据典型实施例，可以关闭具有要撤消的特权的应用程序。当该应用程序重新启动时，对撤消的特权的访问将会被拒绝。为了跟踪哪些应用程序需要被关闭和复位，该系统必须跟踪哪些应用程序已经访问了哪些特权。为了实现对由应用程序访问的特权的监控，每一次当应用程序使用特权时，该系统记录应用程序标识符、以及哪些特权已经被访问。这可以按照任意数量的传统方法来实现，例如，列出应用程序标识符和与应用程序标识符相关的相应访问特权的数据表。当系统管理员或任意其他权威结构设立特权变化时，该系统访问哪些应用程序已经访问了哪些特权的记录。执行访问过的特权与要撤消的特权的比较。由系统识别已经访问了要撤消的特权的每一个应用程序，并关闭该应用程序。当应用程序重新启动时，该应用程序将不能够对任何撤消的特权进行访问。

在另一实施例中，可以执行设备复位。通过复位设备，使系统进入已知状态。根据该实施例，系统管理员或任何其他权威机构指定：当设立撤消（或改变）特权的新策略时，必须对设备进行复位。可以

在管理员或权威机构认为需要这样做的任何时候，设立设备复位。例如，无论何时当设立了包括特权撤消的新策略时，可以进行设备复位。然而，这可能会导致大量不必要的设备复位事件，可能给用户带来不方便，并且可能会干扰设备的使用。可选地，该系统可以跟踪哪些设备包括哪些应用程序，并且使用该信息来确定较为不会造成干扰的设备复位日程。例如，仅复位具有可能会受到策略变化影响的应用程序的那些设备。

在另一优选实施例中，组合先前所述的实施例的方案，以提供有效的特权管理和撤消。根据该典型实施例，该系统管理员或其他权威机构对何时复位设备没有实际控制。该管理员仅管理系统的特权和特定应用程序。该设备本身负责在需要时进行复位。在该实施例中，该设备跟踪哪些设备对哪些特权进行访问。当策略或应用程序控制改变时，该系统检测针对哪些应用程序已经撤消了哪些特权。这可以简单地通过将较早特权集合与新特权集合的比较来实现。对于给定应用程序的每一个撤消特权，该系统确定该应用程序过去是否曾经访问过该特权。如以上所提到的，该系统自从系统第一次被启动时开始就对此进行跟踪。如果应用程序过去已经访问了现在被撤消的特权，该设备被复位。对于一些特权（例如IPC），仍然不能够确定作为从另一应用程序被传递的结果，是否已经使用了特权。为了克服当应用程序在其间传递特权时遗漏特权的撤消的可能性，例如，如果IPC（或能够在应用程序之间传递的任意其他特权）被从任意应用程序上撤消，则与系统是否已经检测到应用程序已经访问了该特权无关，该设备必须被复位。该复位将使设备回到已知状态。仅当需要时执行设备复位，从而限制了复位的数量并解决了与已经在应用程序之间传递的特权相关的问题。

这些实施例的每一个可用于从低级、低优先权（其中需要适度等级的特权撤消安全性，产生了较为不太鲁棒系统）到高度重要的超鲁棒环境(其中用户方便对于特权策略的绝对确定性的需要是第二位的）的范围内的各种特权管理环境。

附图说明

参考以下附图，将描述这些和其他实施例及其附加优点，在附图中，参考的参考符号表示相同的组件，其中：

图1是示出了其中使用了运行了能够对相关特权进行访问的应用程序的电子设备的计算机网络和通信系统的方框图；

图2是作为运行有能够访问相关特权的应用程序的电子设备的示例的无线移动通信设备的方框图；

图3是示出了根据典型实施例的撤消应用程序的方法的流程图；

图4是示出了根据另一典型实施例的撤消特权的方法的流程图；

图5是示出了根据另一典型实施例的撤消特权的另一方法的流程图。

具体实施方式

图1是示出了其中使用了运行了能够对相关特权进行访问的应用程序的电子设备的计算机网络和通信系统的方框图。该计算机网络18包括诸如各种网络计算机28、以及可选地消息服务器26，均经由局域网（LAN）30链接在一起。该通信系统包括与计算机系统14、无线网络网关16和计算机网络18的LAN 30相连的广域网（WAN）12。该无线网络网关16还与无线通信网络20相连，无线移动通信设备22（此后称为“移动设备”）配置在无线通信网络20中以进行操作。典型地，整个系统10尤其由系统管理员或类似权威机构32来管理。

该计算机系统14可以是桌面或膝上型个人计算机，配置来与WAN 12或任意其他适当网络通信，诸如因特网。诸如计算机系统14等个人计算机典型地经由因特网服务提供商（ISP）、应用程序服务提供商（ASP）等来访问因特网。

该LAN 30是典型工作计算机网络环境的示例，其中多个计算机28连接在网络中。该计算机网络18典型地位于安全防火墙24之后。在LAN 30内，操作在防火墙24之后的计算机上的消息服务器26可以充当计算机网络18的拥有者的主接口，以便在LAN 30内和经由WLAN 12与其他外部消息传递客户端交换消息。已知消息服务器包括诸如Microsoft

Outlook™、Lotus Notes™、Yahoo!™消息器、AOL即时消息器、或各种体系结构下的任意其他客户端-服务器或对等或类似消息传递客户端。将由消息服务器26接收到的消息分配到针对在接收到的消息中所寻址的用户帐户的邮箱，然后由用户通过在计算机系统28上操作的消息传递客户端来访问。前面的描述仅是示例性描述，示出了客户端-服务器体系结构，而绝非表示这样的体系结构是必须的，可以使用本领域的技术人员已知的其他适当体系结构。

尽管在LAN 30中仅示出了消息服务器26，但是本领域的技术人员将会意识到:LAN可以包括支持网络计算机系统28之间共享的资源的其他类型的服务器，以及该消息服务器26还可以具备附加功能，例如数据的动态数据库存储，所述数据诸如但不局限于日历、to-do列表、任务列表、电子邮件和文档。仅出于说明的目的描述了消息服务器26和电子消息传递。用于管理和撤消特权的系统和方法可应用于较宽范围的电子设备，而绝不局限于具有消息传递能力的电子设备。

该无线网关16提供了到无线网络20的接口，通过该无线网络20，可以与移动设备22交换消息。由无线网关16来执行诸如寻址移动设备22、编码或转换无线传输的消息和任意其他接口功能等功能。该无线网关16可以配置来与多于一个无线网络20进行操作，在该情况下，该无线网络20还确定最可能的网络，用于在用户在国家或网络之间漫游时，定位给定的移动设备22和可能地跟踪移动设备。

该移动设备22是诸如数据通信设备、语音通信设备、双模式通信设备（例如同时具有数据和语音通信功能的许多现代蜂窝电话）、能够进行语音、数据和其他类型的通信的多模设备、为无线通信而实现的个人数字助理（PDA）、或者具有无线调制解调器的膝上型或桌面计算机系统。

任意对WAN 12进行访问的计算机系统可以通过无线网络网关16与移动设备22交换消息。可选地，可以实现诸如无线虚拟专用网（VPN）路由器等专用无线网络网关，以提供到无线网络的专用接口。在LAN 30中实现的无线VPN路由器提供了从LAN 30通过无线网络20到一个或多个诸如22的移动设备的专用接口。还可以通过提供与消息服务器26进

行操作的消息转发或重定向系统，将到移动设备22的专用接口有效扩展到LAN 30外部的实体。在美国专利No. 6,219,694中公开了这样的消息重定向系统，该专利内容包括在本申请中作为参考。在该类型的系统中，通过无线网络接口（或者无线VPN路由器、无线网关16、或者其他接口）将由消息服务器26接收到且寻址到移动设备22的用户的输入消息发送到诸如无线网络20和用户的移动设备22。到消息服务器26上的用户邮箱的另一可选接口可以是无线应用协议（WAP）网关。通过WAP网关，可以将消息服务器26上的用户邮箱中的消息列表、以及可能地每一个消息或每一个消息的一部分发送到移动设备22。正常地，无线网络20经由基站和设备之间的RF传输，向和从诸如移动设备22等通信设备传递消息。例如，该无线网络20可以是数据为中心的无线网络、语音为中心的无线网络、或者能够在相同的基础设施上同时支持语音和数据通信的双模式网络。最近发展起来的网络包括码分多址接入（CDMA）网络和通用分组无线服务（GPRS）网络。诸如全球演进增强数据速率（EDGE）和通用移动通信网络（UMTS）等所谓的第三代（3G）网络当前正在开发中。较早的数据为中心的网络包括但不局限于Mobitex™无线电网络（“Mobitex”）和DataTAC™无线电网络（“DataTAC”）。诸如个人通信系统（PCS）网络等语音为中心的数据网络（包括全球移动通信系统（GSM）和时分多址接入（TDMA）系统）已经在北美和世界范围内得到多年的应用。

图2是作为电子设备的示例的典型无线移动通信设备的方框图。然而，应该理解，这里所公开的系统和方法可以用于许多不同类型的设备，诸如个人数字助理（PDA）、桌面计算机等。

优选地，移动设备500是至少具有语音和数据通信能力的双向通信设备。优选地，该移动设备500具有与因特网上的其他计算机系统通信的能力。根据由移动设备所提供的功能，该移动设备可以被称为数据消息传递设备、双向寻呼机、具有数据消息传递能力的蜂窝电话、无线因特网设备、或数据通信设备（具有或没有电话能力）。如上所提到的，这样的设备通常被称为移动设备。

该移动设备500包括收发器511、微处理器538、显示器522、非易

失性存储器524、随机存取存储器（RAM）526、辅助输入/输出（I/O）设备528、串行端口530、键盘532、扬声器534、麦克风536、短距离无线通信子系统540，并且还可以包括其他设备子系统542。该收发器511优选地包括发射和接收天线516、518、接收器（Rx）512、发射器（Tx）514、一个或多个本地振荡器（LO）513、以及数字信号处理器（DSP）520。在非易失性存储器524内，该移动设备500包括多个能够由微处理器538（和/或DSP 520）执行的多个软件模块524A-524N，包括语音通信模块524A、数据通信模块524B、和用于实现多个其他功能的多个其他操作模块524N。

优选地，该移动设备500是具有语音和数据通信能力的双向通信设备。因此，例如，该移动设备500可以在诸如模拟或数字蜂窝网络的任一个的语音网络上通信，并且还可以在数据网络上通信。该语音和数据网络在图2中由通信塔519示出。这些语音和数据网络可以是利用分离基础设施（例如基站、网络控制器等）的分离通信网络，或者其也可以被集成到单个的无线网络。因此，对网络519的参考应该被解释为同时包括单个语音和数据网络和分离的网络。

该通信子系统511用来与网络519进行通信。DSP 520用来向和从发射器514和接收器512发送和接收通信信号，并且还与发射器514和接收器512交换控制信息。如果语音和数据通信出现在高频率处或近距离间隔集合的频率处，则单个LO 513可以与发射器514和接收器512结合在一起使用。可选地，如果不同的频率分别用于语音通信与数据通信，或者使移动设备500能够在多于一个的网络519上通信，则多个LO 513可以用来产生与网络519中所使用的频率相对应的频率。尽管在图2中示出了两个天线516、518，该移动设备500可以使用单个天线结构。经由DSP 520和微处理器538之间的链路，向和从通信模块511通信包括语音和数据信息的信息。

通信子系统511的详细设计（诸如频带、组件选择、功率水平等）取决于移动设备500想要在其中操作的通信网络519。例如，想要在北美操作的移动设备500可以包括通信子系统511，设计来利用Mobitex或DataTAC移动数据通信网络操作且还设计来利用各种各样的任意语

音通信网络操作，例如AMPS、TDAM、CDMA、PCS等，而想要在欧洲使用的移动设备500可以配置来利用GPRS数据通信网络和GSM语音通信网络来操作。还可以将其他类型的数据和语音网络（分离的和集成的）用于移动设备500。

移动设备500的通信网络访问需求还根据网络519的类型而变化。例如，在Mobitex和DataTAC数据网络中，利用与每一个设备相关的唯一标识号将移动设备登记在网络上。然而，在GPRS数据网络中，网络访问与移动设备500的订户或用户相关。典型地，GPRS设备需要订户身份模块（“SIM”），需要用来在GPRS网络上操作移动设备500。本地或非网络功能（如果存在）可以在没有SIM的情况下操作，但是除了法律所要求的操作（例如“911”紧急呼叫）以外，移动设备500不能够实现涉及网络519上的通信的功能。

在已经完成任意所需网络登记或激活过程之后，移动设备500能够通过网络519发送和接收通信信号，优选地，包括语音和数据信号。由天线516从通信网络519中接收到的信号被路由到接收器512，该接收器512提供信号放大、降频转换、滤波、信道选择等，并且还可以提供模拟到数字转换。接收信号的模拟到数字转换允许更为复杂的通信功能，例如，数字解调和解码，利用DSP 520来执行。按照相似的方式，对要传送到网络519的信号进行处理，包括诸如由DSP 520来调制和编码，然后提供发射器514，进行数字到模拟转换、升频转换、滤波、放大和经由天线518向通信网络519发射。尽管对于语音和数据通信示出了单个收发器511，但是在可选实施例中，该移动设备500可以包括多个不同收发器，例如用于发送和接收语音信号的第一收发器、以及发送和接收数据信号的第二收发器，或者第一收发器配置为在第一频带内操作，而第二收发器配置为在第二频带内操作。

除了处理通信信号之外，该DSP 520还提供接收器和发射器控制。例如，可以通过在DSP 520中实现的自动增益控制算法来自适应地控制应用于接收器512和发射器514中的通信信号的增益水平。还可以在DSP 520中实现其他收发器控制算法，以便提供对收发器511的更为高级的控制。

优选地，微处理器538管理和控制移动设备500的整个操作。这里可以使用许多类型的微处理器或微控制器，或者可选地，可以使用单个的DSP 520来实现微处理器538的功能。通过收发器511中的DSP 520来执行至少包括数据和语音通信的低级通信功能。将包括语音通信应用程序524A和数据通信应用程序524B的高级通信应用程序存储在非易失性存储器524中，以便由微处理器538来执行。例如，语音通信模块524A可以提供高级用户接口，可操作来经由网络519在移动设备500和多个其他语音设备之间传送和接收语音呼叫。类似地，该数据通信模块524B可以提供高级用户接口，可操作来经由网络519在移动设备500和多个其他数据设备之间发送和接收数据，例如电子邮件消息、文件、组织者信息、短文本消息等。

该微处理器538还与其他设备子系统进行交互，例如显示器522、RAM 526、辅助I/O设备528、串行端口530、键盘532、扬声器534、麦克风536、短距离通信子系统540和通常指定为542的其他任意设备子系统。例如，该模块524A-N由微处理器538来执行，并且可以具有在移动设备和移动设备的用户之间的高级接口。该接口典型地包括：通过显示器522提供的图形组件、以及通过辅助I/O设备528、键盘532、扬声器534或麦克风536提供的输入/输出组件。附加地，该微处理器538能够运行可以存在于设备的非易失性存储器524上的各种应用程序，包括能够对各种特权进行访问的应用程序，如这里详细描述的。

图2所示的一些子系统执行通信相关功能，而其他子系统可以提供“驻留”或设备上功能。注意，诸如键盘532和显示器522等一些子系统可以同时用于通信相关功能（例如输入在数据通信网络上传输的文本消息）、以及设备驻留功能（例如计算器或任务列表或其他PDA类型功能）。

优选地，由微处理器538使用的操作系统软件存储在永久存储器中，例如非易失性存储器524。除了操作系统和通信模块524A-N之外，该非易失性存储器524可以包括用于存储数据的文件系统。该非易失性存储器524还可以包括针对拥有者信息和拥有者控制信息的数据存储单元。可以将操作系统、特定设备应用程序或模块或其一部分临时加

载到易失性存储器中，例如RAM 526，以便更快速地操作。而且，还在将接收到的通信信号永久地写入到位于非易失性存储器524中的文件系统之前，将其临时存储到RAM 526中。该非易失性存储器524可以由诸如闪速存储器、非易失性RAM或电池备份RAM来实现。

可以加载到移动设备500上的典型应用程序模块524N是提供诸如日历事件、约会和任务项等PDA功能的PIM应用程序。该模块524N还可以与语音通信模块524A交互以管理电话呼叫、语音邮件等，并且还可以与数据通信模块524B交互以管理电子邮件通信和其他数据传输。可选地，可以将语音通信模块524A和数据通信模块524B的所有功能集成到PIM模块中。

优选地，该非易失性存储器524提供了文件系统以便于PIM数据项在设备上的存储。优选地，该PIM应用程序包括经由无线网络519来发送和接收数据项的能力，或者通过其自身或者与语音和数据通信模块524A、524B结合。优选地，经由无线网络519，利用所存储的或者与主计算机系统相关的数据项的相应集合，对PIM数据项进行无缝地集成、同步和更新，从而创建与特定用户相关的数据项的镜像系统。

通过将移动设备500放置在将移动设备500的串行端口530与主机系统的串行端口相耦合的接口底座中，将移动设备500与主机系统手动地同步。该串行端口530还可以用来将拥有者信息和拥有者控制信息插入到移动设备500上，并下载其他应用程序模块524N，以便安装在移动设备500上。该有线下载路径还可以用来将加密密钥加载到移动设备500上，用于安全通信，这是比经由无线网络519交换加密信息更安全的方法。

可以通过网络519、通过辅助I/O子系统528、通过短距离通信子系统540或通过其他任意适当子系统542，将拥有者信息、拥有者控制信息和附加应用程序模块524N加载到移动设备500上，并且由用户安装在非易失性存储器524或RAM 526中。在应用程序安装上的这样的灵活性增加了移动设备500的功能，并且可以提供增强的设备上功能、通信相关功能或两者。例如，安全通信应用程序可以利用移动设备500来执行电子商务功能和其他这样的金融交易。

当移动设备500在数据通信模式下操作时，诸如文本消息或网页下载的接收信号将由收发器511来处理，并提供给微处理器538，优选地，该微处理器538处理接收信号以便输出到显示器522、或可选地输出到辅助I/O设备528。如上所述，对拥有者信息、拥有者控制信息、与拥有者信息或拥有者消息信息相关的命令或请求、以及由收发器511接收到的软件应用程序进行处理。移动设备500的用户还可以利用键盘532来构造诸如电子邮件消息等数据项，优选地，该键盘为以QWERTY风格布局的完整字母数字键盘，尽管也可以使用诸如已知的QVORAK风格的其他风格的完整字母数字键盘。利用多个辅助I/O设备528来进一步增强了对移动设备500的用户输入，该辅助I/O设备528可以包括拇指轮输入设备、触摸板、各种开关、摇杆输入开关等。然后，在通信网络519上经由收发器511来传送由用户输入的构造的数据项。

当移动设备500在语音通信模式下操作时，移动设备500的整个操作与数据模式实质上是类似的，除了将接收到的数据输出到扬声器534和用于传输的语音信号由麦克风536产生之外。此外，上述安全消息传送技术可以不一定应用于语音通信。还可以在移动设备500上实现可选的语音或音频I/O设备，例如语音消息记录子系统。尽管语音或音频信号输出通过扬声器534来实现，还可以显示器522来提供呼叫方的身份指示、语音呼叫持续时间或其他语音呼叫相关的信息。例如，与语音通信模块524A和操作系统软件结合，该麦克风538可以检测输入语音呼叫的呼叫方识别信息，并将其显示在显示器522上。

短距离通信子系统540也包括在移动设备500中。例如，该子系统540可以包括红外设备和相关电路和组件、或者蓝牙或802.11短距离无线通信模块，以提供与类似功能的系统和设备的通信。因此，可以在移动设备500上经由串行端口530或其他短距离通信子系统540来实现如上所述的拥有者信息插入、拥有者控制信息插入和应用程序加载操作。

图2示出了其中可以实现这里所述的拥有者控制系统和方法的电子设备的特定示例。在比图2所示具有更少或不同组件的其他电子设备中实现这样的系统和方法对本领域的技术人员显而易见，该应用与本

申请的范围相关并因而被认为位于本申请的范围内。

图3是示出了根据典型实施例的撤消特权的方法的流程图。在该示例中，必须关闭具有要撤消的特权的应用程序。当该应用程序重新开始时，将拒绝对撤消的特权的访问。为了跟踪哪些应用程序需要被关闭和复位，该系统必须对哪些应用程序能够访问哪些特权进行跟踪。为了实现这一点，例如，该系统监控和检测应用程序300对特权的使用。该系统可以记录与特定应用程序相关的应用程序标识符、以及哪一个特权已经由应用程序302访问。这可以在对本领域的技术人员显而易见的任意数量的传统方法中实现。例如，数据表列出了应用程序标识符，且具有指向由应用程序访问或与应用程序标识符相关的特权的指针。然后，该系统继续监控可能会导致特权304的撤消的任何系统变化，例如，IT策略的变化。只要在判定块304中未检测到这样的变化，则该系统继续监控和跟踪应用程序和相关特权。

在判定块304检测到将会导致系统中的应用程序访问的特权的撤消的变化时，例如IT策略的变化，执行与所访问的特权相关的记录数据与列出的新特权的比较306。例如，将步骤302中记录的应用程序标识符和相关访问的特权与新特权列表或撤消特权列表进行比较306。典型地，这里所讨论的变化典型地由负责系统的操作和管理的系统管理员或其他权威机构来设立和管理。

作为比较306的经过，由系统识别308能够访问要撤消的特权的每一个应用程序。在识别了这些应用程序时，该系统实现对这些识别的应用程序310的关闭。当重新开始312这些应用程序时，这些应用程序将不能够对任意撤消的特权进行访问。该系统将继续如上所述监控和检测特权和相关应用程序的访问。

在另一实施例中，如图4的流程图所示，可以执行设备复位。根据该示例，对系统中的所有设备进行监控400。例如，系统管理员或其他权威机构指定：无论何时当发生需要特权402的撤消或改变的系统策略变化时，必须复位404系统中的所有设备。复位这些设备使系统进入已知状态，即，其中系统知道在整个系统中哪些应用程序能够访问哪些特权的状态。在设备复位404之后重新启动这些应用程序406时，该

应用程序将不再能够访问任意撤消的特权。根据该示例，任何时候当系统管理员或权威机构决定需要这样做时，可以发起设备复位。例如，无论何时当设立包括特权撤消的新策略时，可以进行设备复位。结果，该解决方案可以调用打扰用户和对用户不方便的大量（可能不必要）设备复位事件。然而，该实施例提供了非常鲁棒和即时的特权撤消，并且因而适合于特权管理比用户方便更为重要的高度安全系统。

现在转到图5，示出了参考图3和4描述的实现这两个实施例的特征的另一优选实施例。根据该示例，将先前所述实施例的方案进行组合以提供高效和即时的管理和撤消。在该示例中，该系统管理员或权威机构对设备何时复位不进行实际控制。该管理员或权威机构仅管理系统和特定应用程序的特权。该设备自身负责根据需要进行复位。

在该示例中，该设备监控设备的哪些应用程序能够访问哪些特权600，并且保持602设备的特权日志。该设备监控604系统中是否进行了策略或应用程序控制改变。如果未检测到变化604，则该设备继续监控应用程序并保持针对设备的特权日志600、602。如果在步骤604中检测到策略和应用程序控制的变化，则该系统通过将日志的较早特权集合与从系统管理员606接收到的新特权集合进行比较，来确定针对哪些应用程序已经撤消了哪些特权。然后，该设备确定任意撤消的特权是否存在于设备608上。如果检测到撤消的特权，例如，如果应用程序在过去的任意时刻已经访问过现在被撤消的特权，则该设备将复位610。如上所述，复位该设备使系统进入其中所有应用程序和特权是已知的已知状态。在设备复位610之后，在612处重新启动。在重新启动612时，该设备应用程序将能够访问正确的特权。有利地，如果在步骤608中检测到未撤消特权，则该设备执行另一检查，以确保在应用程序之间传递的特权没有遗漏。如以上所解释的，对于一些特权，例如IPC，不能够确定作为从另一应用程序传递的结果，是否已经使用了特权。为了克服当应用程序在其间传递特权时遗漏对特权的撤消的可能性，该系统检查能够在应用程序（例如IPC）之间传递的特权614。如果从任何应用程序中撤消了能够在应用程序之间传递的特权，与系统是否已经检测到应用程序已经访问了特权614无关，该设备必须被复位610，以

使系统进入已知状态。在复位之后，重新启动该设备612，并且现在将仅能够访问正确的特权。按照该方式，仅在需要时执行设备复位，从而限制了复位的数量，并解决了由于其能够在应用程序之间传递而造成的未检测的特权相关的问题。

尽管该公开描述了特定典型实施例，但是明显地，许多替换、修改和变化对本领域的技术人员将是显而易见的。因此，这里所述的典型实施例是说明性的而非限定性的。在不脱离所附权利要求限定的本发明的真正精神和全部范围的情况下，可以进行各种改变。

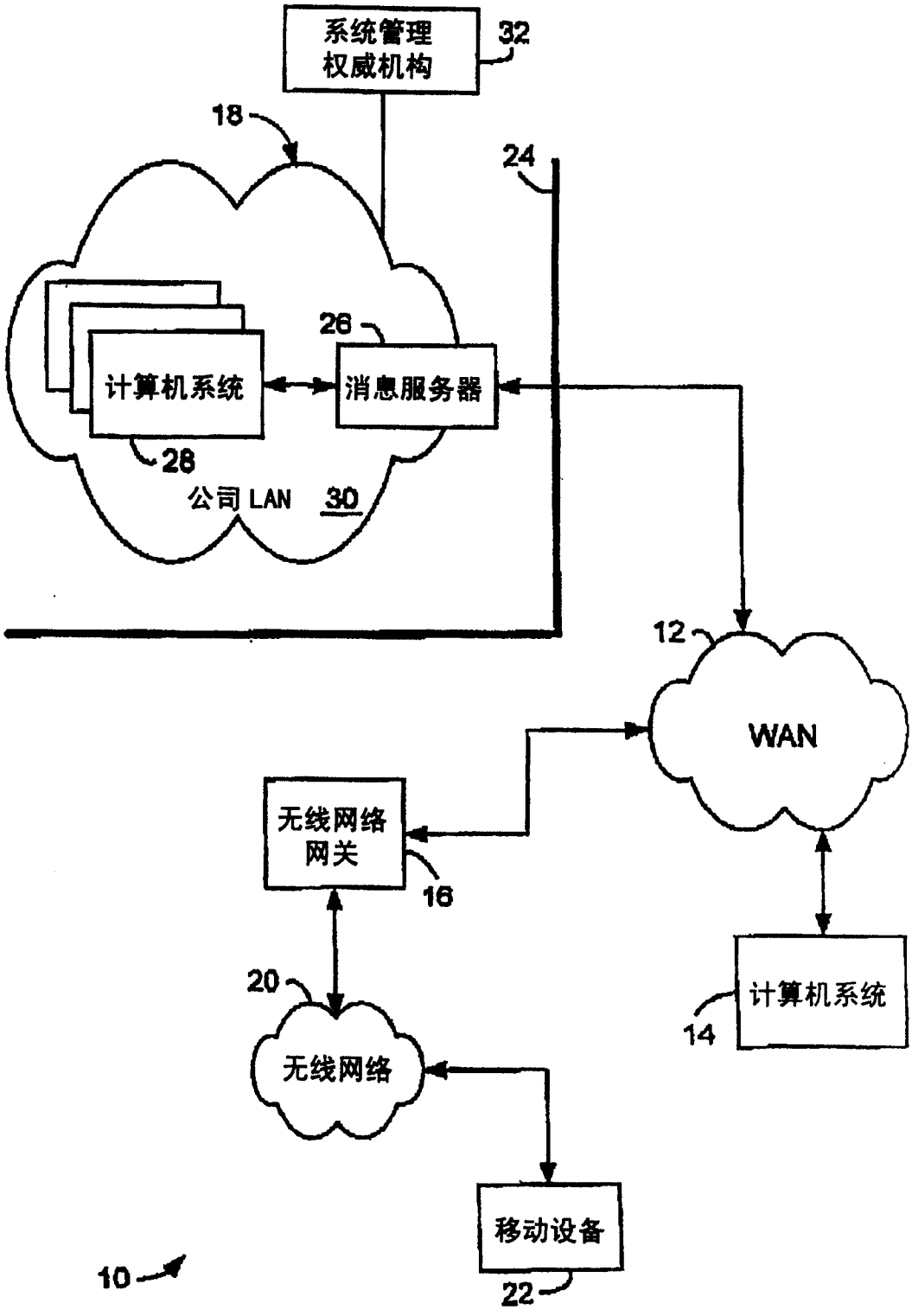

系统管理
权威机构
32
18
24
26
计算机系统
消息服务器
28
公司 LAN
30
12
WAN
无线网络
网关
16
20
无线网络
计算机系统
14
移动设备
22
10

图 1

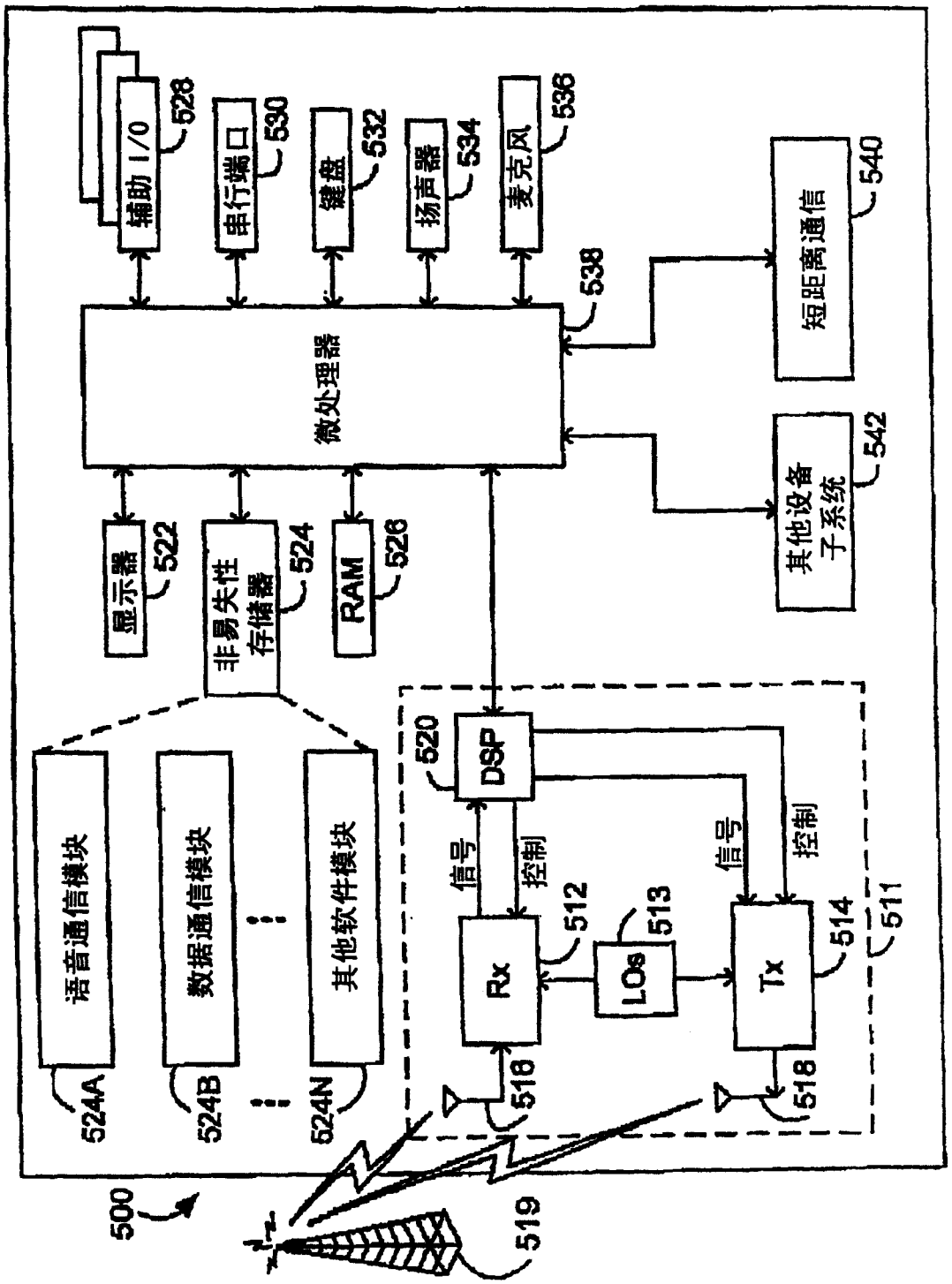

辅助 I/O
528
串行端口
530
键盘
532
扬声器
534
麦克风
536
微处理器
538
短距离通信
540
其他设备子系统
542
显示器
522
非易失性存储器
524
RAM
526
语音通信模块
数据通信模块
其他软件模块
524A
524B
524N
DSP
520
信号
控制
Rx
512
LOs
513
Tx
514
511
518
519
500

图 2

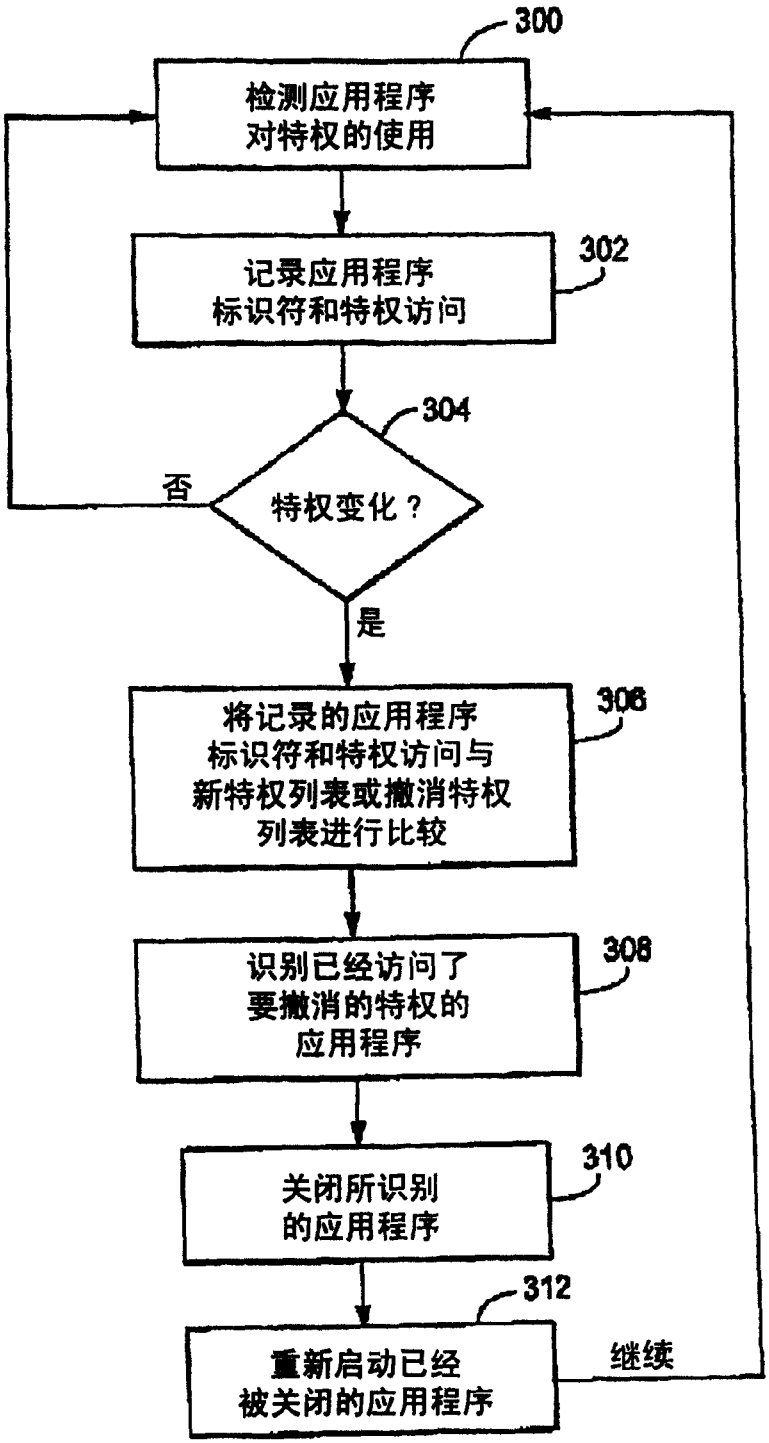

300
检测应用程序
对特权的使用
302
记录应用程序
标识符和特权访问
304
特权变化？
否
是
306
将记录的应用程序
标识符和特权访问与
新特权列表或撤消特权
列表进行比较
308
识别已经访问了
要撤消的特权的
应用程序
310
关闭所识别
的应用程序
312
重新启动已经
被关闭的应用程序
继续

图 3

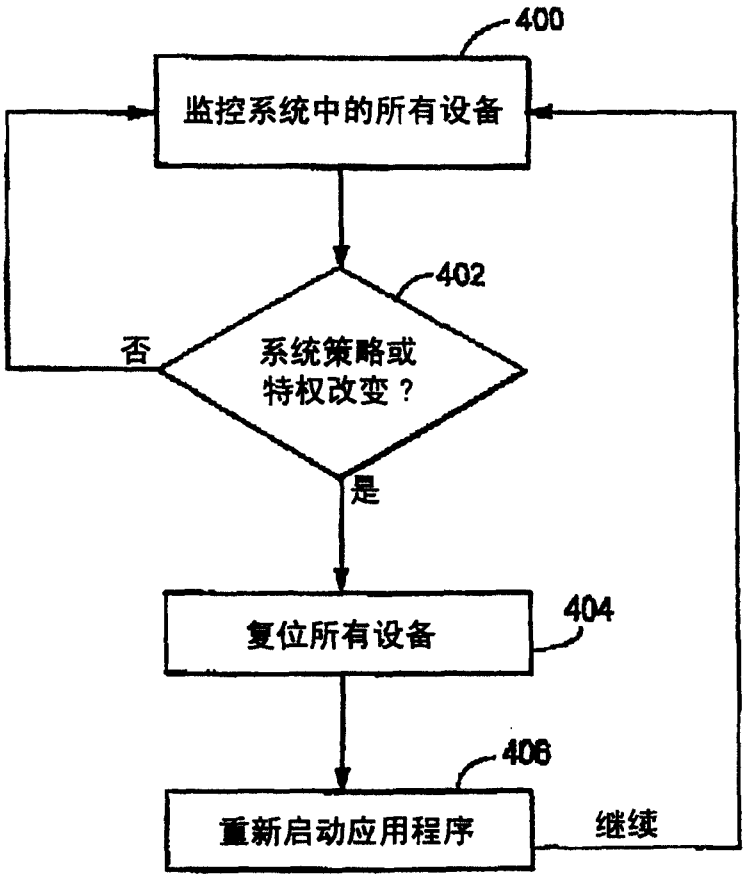


图 4

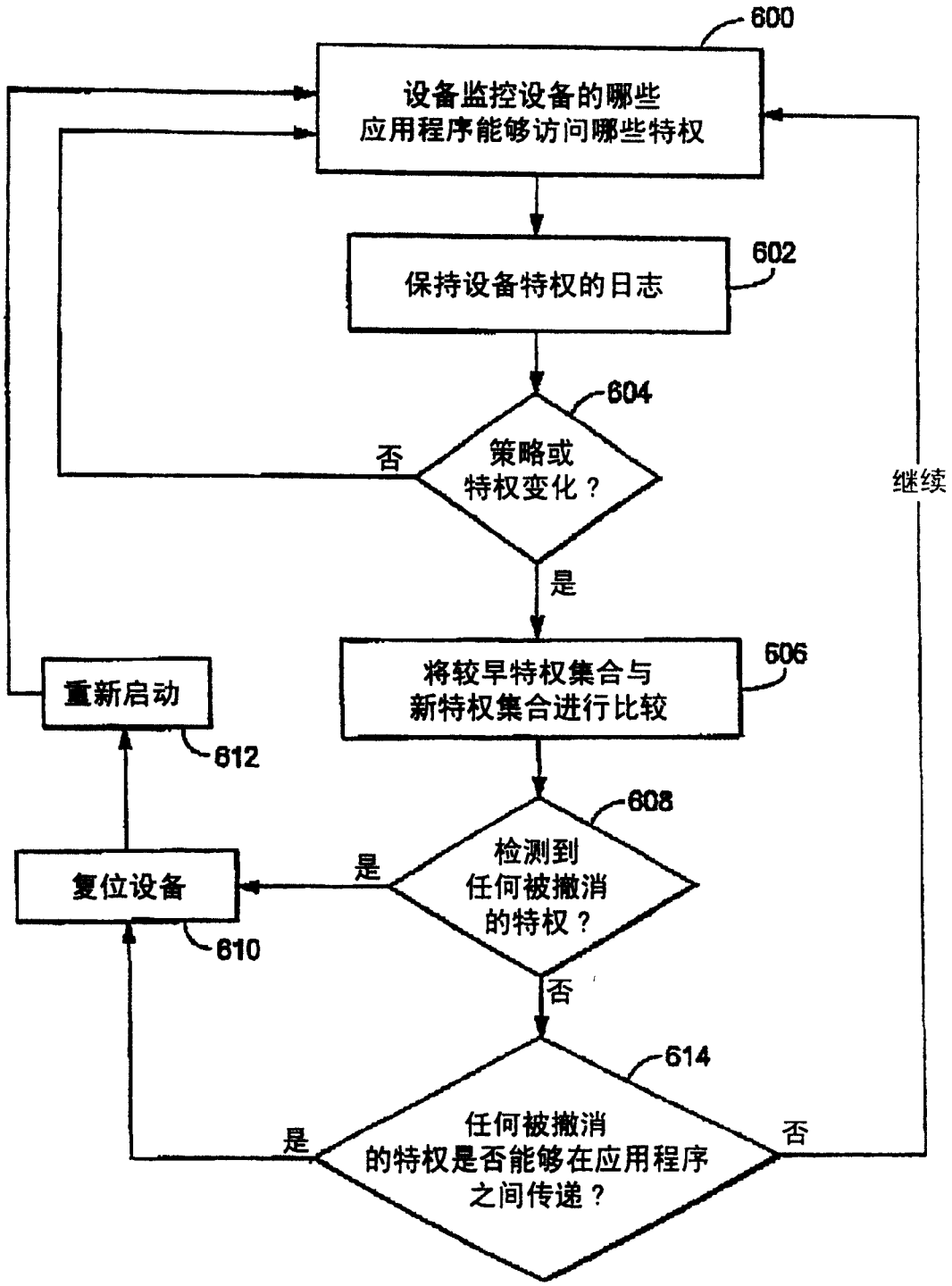

600
设备监控设备的哪些
应用程序能够访问哪些特权
602
保持设备特权的日志
604
策略或
特权变化？
否
是
继续
606
将较早特权集合与
新特权集合进行比较
608
检测到
任何被撤消
的特权？
是
否
复位设备
610
重新启动
612
614
任何被撤消
的特权是否能够在应用程序
之间传递？
是
否

图 5