(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 102609662 B
(45)授权公告日 2015.08.05

(21)申请号 201110431392.3

(22)申请日 2011.12.20

(30)优先权数据
12/972,534 2010.12.20 US

(73)专利权人 微软公司
地址 美国华盛顿州

(72)发明人 P·巴勒姆 J·N·菲格罗亚

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 杨洁

(51)Int.Cl.
G06F 21/30(2013.01)

(56)对比文件
US 2008/0046965 A1,2008.02.21,说明书第0049,0054-0058,0065,0068,0070-0071,0085,0135-0138,0182-0183,0187,0210,0228-0230,0244-0246,0260,0274-0280段、说明书附图2A,2B,3C,4A,4B,5A,5B,5C,5D,5E,5F,7.
US 2008/0046965 A1,2008.02.21,说明书第0049,0054-0058,0065,0068,0070-0071,0085,0135-0138,0182-0183,0187,0210,0228-0230,0244-0246,0260,0274-0280段、说明书附图2A,2B,3C,4A,4B,5A,5B,5C,5D,5E,5F,7.
US 2003/0217137 A1,2003.11.20,说明书第0073,0109段.
CN 1489736 A,2004.04.14,全文.
US 7624424 B2,2009.11.24,全文.

审查员 朱江岩

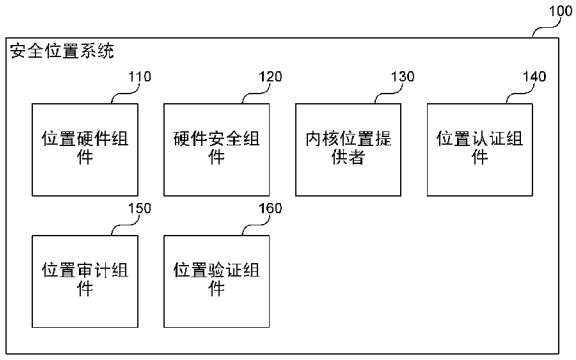
权利要求书2页 说明书7页 附图3页

(54)发明名称

防篡改的位置服务

(57)摘要

本发明涉及防篡改的位置服务。此处描述了利用基于位置的软件和硬件来作出访问决定的安全位置系统。很多移动计算机具有位置设备,诸如GPS。它们还具有受信平台模块(TPM)或其他安全设备。目前,使GPS位置数据对使用简单协议的非受信应用代码是直接可以访问的。安全位置系统提供了安全机制,操作系统内核和TPM可借此对计算机在具体时间的GPS位置进行证实。安全位置系统使用指示活动时计算设备的地理位置的标记将用户活动记入日志。安全位置系统可以通过组合内核模式GPS访问以及TPM安全硬件来提供难以伪造、带时间戳的位置。由此,安全位置系统将安全位置信息并入授权和其他操作系统决定中。



CN 102609662 B

1. 一种基于位置信息来设置对资源的访问许可的计算机实现的方法，所述方法包括：

接收更新对所标识的资源的许可以便包括基于位置的许可信息的许可更新请求(210)，包括获取指示计算机系统的当前地理位置的证书，所述基于位置的许可信息至少包括定义所述基于位置的许可所应用的地理区域的地理位置信息，所述证书包括对计算设备的位置以及生成证书的时间的经签署的指示，并提供可验证的以及可审核的位置指示；

定位所述所标识的资源 (220)；

定位与所述所标识的资源相关联的访问控制信息 (230)；

从伴随所述请求的所述基于位置的许可信息确定一个或多个被允许的动作 (240)；

更新所定位的访问控制信息以包括被允许的基于位置的动作 (250)；以及

存储与所述所标识的资源相关联的已更新的访问控制信息 (260)，使得随后的访问所述所标识的资源的尝试将受到指定的基于位置的访问信息的限制，

其中，前面的各步骤由至少一个处理器来执行。

2. 如权利要求 1 所述的方法，其特征在于，所标识的资源是由操作系统管理的包括相关联的安全信息的对象，包括至少一个访问控制列表 ACL 或访问控制条目 ACE。

3. 如权利要求 1 所述的方法，其特征在于，接收所述许可更新请求包括通过操作系统应用编程接口 API 从应用接收所述请求。

4. 如权利要求 1 所述的方法，其特征在于，接收所述许可更新请求包括接收由路径标识所述资源的信息，以及接收包括地理位置作为至少一个访问准则的访问控制信息。

5. 如权利要求 1 所述的方法，其特征在于，定位所述所标识的资源包括访问磁盘上、配置数据库内、或配置目录内的所述资源，以及访问与所述资源相关联的有关访问控制元数据。

6. 如权利要求 1 所述的方法，其特征在于，定位所述访问控制信息包括调用操作系统应用编程接口 API 以便导航和 / 或修改包括基于位置的信息的访问控制信息。

7. 如权利要求 1 所述的方法，其特征在于，确定一个或多个被允许的动作包括基于所述资源存储在其上的计算设备的地理位置，确定所述资源是否可被读、写、或包括在列表中。

8. 如权利要求 1 所述的方法，其特征在于，确定一个或多个被允许的动作包括基于地理区域的一个或多个指定边界，确定所述地理区域。

9. 如权利要求 1 所述的方法，其特征在于，更新所述访问控制信息包括添加分层的访问控制条目 ACE，所述访问控制条目指示了许可与所述所标识的资源有关的指定动作的地理区域。

10. 如权利要求 1 所述的方法，其特征在于，更新所述访问控制信息包括对基于位置的访问控制信息与非基于位置的访问控制信息进行组合，以指示访问所述所标识的资源的一个或多个准则。

11. 一种向软件应用提供防篡改的位置服务的计算机系统，所述系统包括：

位置硬件组件 (110)，提供指示所述系统的当前地理位置的硬件信号；

硬件安全组件 (120)，提供对运行在所述系统上的软件代码的可信计算保证；

被配置成执行包含在以下组件内的软件指令的处理器和存储器；

内核位置提供者 (130)，提供从操作系统内核到使用地理位置信息的用户模式服务和

应用的接口；

位置认证组件 (140)，用来自所述位置硬件组件和所述硬件安全组件的信息来获取指示所述计算机系统的当前地理位置的证书，所述证书包括对计算设备的位置以及生成证书的时间的经签署的指示，并提供可验证的以及可审核的位置指示；

位置审计组件 (150)，存储与所述计算机系统相关联的安全位置信息的审计踪迹，所述位置审计组件还被配置来周期性地查询所述位置硬件组件，以获取所述系统的当前地理位置信息；以及

位置验证组件 (160)，向所述内核位置提供者请求位置信息，并且基于已接收的位置信息来执行一个或多个动作。

12. 如权利要求 11 所述的系统，其特征在于，所述位置硬件组件包括接收 GPS 信号并确定所述系统的位置的全球定位系统 GPS 硬件设备。

13. 如权利要求 11 所述的系统，其特征在于，所述硬件安全组件包括提供与计算设备的安全性有关的可密码验证的权威信息的受信平台模块 TPM。

14. 如权利要求 11 所述的系统，其特征在于，所述硬件安全组件和位置硬件组件经由用于通信的安全通道而连接。

15. 如权利要求 11 所述的系统，其特征在于，所述硬件安全组件对与所述位置硬件组件相关联的软件驱动程序的认证信息进行验证，以创建从所述位置硬件组件到所述操作系统的安全信任链。

防篡改的位置服务

技术领域

[0001] 本发明涉及位置服务，尤其是防篡改的位置服务。

背景技术

[0002] 位置服务正变为普通计算设备的更为常见的部分。虽然全球定位系统 (GPS) 芯片首先在提供方向的专用设备中常见，但在移动电话、便携式游戏设备、和膝上型计算机中变得越来越常见。计算软件正开始使用设备当前位置来提供各种服务，诸如位置列表（例如，用于餐厅或其他服务）、方向、天气信息等。某些操作系统已被更新为包括软件应用可以调用来以一致的方式（例如，在不为不同的硬件类型作出修改的情况下）得到位置信息的位置服务应用编程接口 (API)。

[0003] 地理位置影响远不止用户可能感兴趣发现的零售商的类型。例如，很多国家具有限制可在那些国家内的设备中包括的加密类型的出口法律。其他国家限制对受版权保护的内容的传输。由此，用户的位置可以改变影响如何许可用户使用计算设备的法律框架。

[0004] 操作系统通常负责实施对数据和服务的访问控制，并且有时期望操作系统提供示出用户执行哪些动作的审计踪迹。当前，访问控制决定通常基于最经常由用户标识符（例如，用户名和密码）而非其他所标识的安全主体的概念。对于移动计算设备，可以在各种各样的地理位置访问数据和服务。操作系统当前不利用位置信息来作出决定。还存在期望能够证明具体动作执行时计算机位于特定位置的情形，但是如今位置服务并不用于这种实例。

发明内容

[0005] 此处描述了利用基于位置的服务和硬件来作出访问决定的安全位置系统。很多移动计算机具有位置设备，诸如 GPS。它们还具有受信平台模块 (TPM) 或其他安全设备。目前，使 GPS 位置数据对使用简单协议的非受信应用代码是直接可以访问的。安全位置系统提供了安全机制，操作系统内核和 TPM 可借此证实计算机在具体时间的 GPS 位置。在某些实施例中，安全位置系统使用指示活动时计算设备的地理位置的标记将用户活动记入日志。安全位置系统可以通过组合内核模式 GPS 访问以及 TPM 安全硬件来提供难以伪造（即防篡改）、带时间戳的位置。

[0006] 在某些实施例中，系统提供了可用于验证在特定位置发生的特定动作的安全审计踪迹。系统还可基于地理位置和 / 或时间来限制对操作系统服务的使用或对访问控制决定的改变。安全位置系统通过使 GPS 硬件仅可由内核访问来执行这些动作。TPM 确保操作系统和引导加载器代码来自受信源。操作系统读取安全的 GPS 位置，并将经证实的 GPS/ 时间数据提供给用户空间进程。系统形成从早至引导过程到用户进程的执行的信任链，该用户进程的执行监视并控制应用如何提供并使用 GPS 信息。由此，安全位置系统将安全位置信息并入授权和其他操作系统决定中。

[0007] 提供本发明内容以便以简化的形式介绍将在以下具体实施方式中进一步描述的

一些概念。本发明内容并不旨在标识所要求保护主题的关键特征或必要特征，也不旨在用于限制所要求保护主题的范围。

附图说明

[0008] 图 1 是示出一个实施例中的安全位置系统的组件的框图。

[0009] 图 2 是示出一个实施例中的基于位置信息来设置资源许可的安全位置系统的处理的流程图。

[0010] 图 3 是示出一个实施例中的使用基于位置的访问许可来访问资源的安全位置系统的处理的流程图。

具体实施方式

[0011] 此处描述了利用基于位置的服务和硬件来作出访问决定的安全位置系统。例如，可以想到的是，操作系统应该基于计算机的物理位置来许可对文件和服务的不同子集的访问，例如，当在各个国家或办公室以外时不允许对特定文件的访问。很多移动计算机具有位置设备，诸如 GPS。它们还具有受信平台模块 (TPM) 或其他安全设备。目前，使 GPS 位置数据对使用简单协议 (例如，RS232 或 USB) 的非受信应用代码是直接可以访问的。安全位置系统提供安全机制，操作系统内核和 TPM 可借此证实计算机在具体时间的 GPS 位置。在某些实施例中，安全位置系统使用指示活动时计算设备的地理位置的标记将用户活动记入日志。

[0012] 安全位置系统可以通过组合内核模式 GPS 访问以及 TPM(或类似的) 安全硬件来提供难以伪造 (即防篡改)、带时间戳的位置。在某些实施例中，系统提供了可用于验证在特定位置发生的特定动作的安全审计踪迹。系统还可基于地理位置和 / 或时间来限制对操作系统服务的使用或对 (文件) 访问控制决定的改变。例如，一个公司可在一膝上型计算机位于公司的企业总部内时提供对该计算机上的一文件集的访问，但在该计算机被带到别处时可将访问减少为针对文件的较小的子集。作为另一个示例，安全位置系统可在计算设备位于允许 56 位加密限制的国家时使用一种类型的加密 (例如，用于安全网页访问)，而在位于允许更高加密级别的国家时使用另一种类型的加密。在该示例中，尽管共享的二进制模块集可被发送到每一地点，但操作系统厂商可向每个位置证实操作系统遵守该国的法律。

[0013] 安全位置系统通过使 GPS 硬件仅可由内核可能通过私有加密通道访问来执行这些动作。TPM 确保操作系统和引导加载器代码来自受信源。操作系统读取安全的 GPS 位置，并将经证实的 GPS/ 时间数据提供给用户空间进程。系统形成从早至引导过程到用户进程的执行的信任链，该用户进程的执行监视并控制应用如何提供并使用 GPS 信息。系统可包括经修改的文件、目录、和其他资源元数据以包括嵌入地理区域的访问控制列表。例如，管理员不仅可以指定谁，还可以指定在哪里 (以及甚至是什么时候) 了访问文件。文件和目录时间戳 (访问时间 (atime)、改变时间 (ctime)、修改时间 (mtime)) 可被扩充以包括地理位置。操作系统使用安全的 GPS 位置数据来扩充其用户活动日志 (例如，MICROSOFT TM WINDOWS TM 安全事件日志)。应用可以读取并获得位置的证书。在应用读取文件时，可以基于位置在操作系统或更安全的级别选择其得到的数据。在某些实施例中，安全位置系统

可基于计算机目前所位于的国家/地区，在用户级替换整个文件系统外观（例如，使用隐写文件系统）。由此，安全位置系统将安全位置信息并入授权和其他操作系统决定中。

[0014] 图 1 是示出一个实施例中的安全位置系统的组件的框图。系统 100 包括位置硬件组件 110、硬件安全组件 120、内核位置提供者 130、位置认证组件 140、位置审计组件 150、和位置验证组件 160。这些组件中的每一个都在此处进一步详细讨论。

[0015] 位置硬件组件 110 提供指示系统的当前地理位置的硬件信号。例如，组件 110 可包括提供纬度和经度坐标、从其可得出纬度和经度的三角测量信息、或其他位置信息的 GPS、Wi-Fi、或蜂窝式芯片。移动设备可使用硬化和其他信息（例如，所分配的因特网协议（IP）地址）的组合来确定计算设备的大致或精确位置。位置硬件系统 110 提供从其确定系统的位置的根信息。

[0016] 硬件安全组件 120 提供对运行在系统上的软件代码的可信计算保证。组件 120 可包括 TPM、处理器序列号、秘密的信任链、或被设计为提供关于计算设备的安全性的权威信息的其他硬件和软件组件。在某些情形中，系统可包括由 TPM 内的密钥加密和解密地存储的引导加载器代码。这允许 TPM 验证该引导加载器代码是安全的并且来自受信源。在某些情形中，密钥是公钥 / 私钥对的公共部分，并且使用公钥的成功解密指示了该代码是由私钥的持有者所签署的。在对引导加载器代码解密之后，硬件安全组件 120 可以继续以相似的方式来加载操作系统，验证正被执行的代码。同样，系统可以验证位置硬件组件 110 的驱动程序，使得创建从位置硬件到操作系统的安全的信任链。

[0017] 内核位置提供者 130 提供从操作系统内核到使用位置信息的用户模式服务和应用的接口。该接口可包括应用或操作系统服务可用来接收安全位置信息并且基于计算设备的当前位置作出决定的一个或多个 API。内核位置提供者 130 可包括用于提供驱动程序或其他软件的可插入的模型，该驱动程序或其他软件用于与各种位置和安全硬件设备交互以按照常见的方式向应用和服务展示安全位置信息。

[0018] 位置认证组件 140 根据位置硬件组件 110 和硬件安全组件 120 获取指示当前位置的证书。该证书可包括对计算设备的位置以及生成证书的时间的经签署的指示。硬件安全组件 120 可以使用密钥或其上生成证书的计算设备专用的其他密码标识符来签署该证书，来作为位置信息的源的标志。应用可将证书存储为所采取的动作是基于可验证的位置信息而执行的证明。

[0019] 位置审计组件 150 存储与计算设备相关联的安全位置信息的审计踪迹。该组件可以存储指示设备在各个时间的一个或多个位置的一个或多个文件、数据库条目或其他结构化数据。在某些实施例中，每次应用或服务向位置认证组件 140 请求位置证书时，位置审计组件 150 都存储对设备的位置的指示。系统 100 还可以周期性地指示位置审计组件 150 从位置硬件组件 110 获得位置信息，并且将审计踪迹与已接收的信息存储在一起。这允许管理员或其他用户稍后验证计算设备曾到过哪里，以及在每个位置可能执行了什么动作。在某些实施例中，管理员可以将周期性地将审计踪迹上传到中央储存库的软件安装到计算设备上，使得机构可以跟踪与该机构相关联的设备在哪里以及如何被使用。如果例如设备被带到已定义的可接受位置边界以外，则系统 100 还可向 IT 人员提供警告或通知。例如，公司可能想要防止发布之前的计算设备离开测试实验室或企业大楼。

[0020] 位置验证组件 160 向内核位置提供者 130 请求位置信息，并且基于已接收的位置

信息来执行一个或多个动作。计算设备可以具有包括位置验证组件 160 的很多应用和服务，该位置验证组件 160 基于设备的当前位置作出决定。例如，文件系统过滤器可以基于设备的当前位置来确定哪些文件应用可以访问。地图位置可以基于设备的当前位置来显示地图和其他信息。操作系统可以基于当地法律来启用和禁用特征，或者基于设备的位置来启用或禁用其他限制。从设备的最早引导到内核层实施的信任链允许应用和服务信任从操作系统接收的位置信息。

[0021] 在其上面实现了安全位置系统的计算设备可包括中央处理单元、存储器、输入设备（例如，键盘和指向设备）、输出设备（例如，显示设备），以及存储设备（例如，磁盘驱动器或其他非易失性存储介质）。存储器和存储设备是可以用实现或启用该系统的计算机可执行指令（例如，软件）来编码的计算机可读存储介质。此外，数据结构和消息结构可被存储或经由诸如通信链路上的信号等数据传送介质发送。可以使用各种通信链路，诸如因特网、局域网、广域网、点对点拨号连接、蜂窝电话网络等。

[0022] 该系统的实施例可以在各种操作环境中实现，这些操作环境包括个人计算机、服务器计算机、手持式或膝上型设备、多处理器系统、基于微处理器的系统、可编程消费电子产品、数码照相机、网络 PC、小型计算机、大型计算机、包括任何上述系统或设备、机顶盒、片上系统 (SOC) 等中任一种的分布式计算环境等。计算机系统可以是蜂窝电话、个人数字助理、智能电话、个人计算机、可编程消费电子设备、数码相机等。

[0023] 该系统可以在由一个或多个计算机或其他设备执行的诸如程序模块等计算机可执行指令的通用上下文中描述。一般而言，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。通常，程序模块的功能可在各个实施例中按需进行组合或分布。

[0024] 图 2 是示出一个实施例中的基于位置信息来设置资源许可的安全位置系统的处理的流程图。资源可包括文件、目录、打印机、配置条目、用户帐户、或操作系统内通常包括安全信息的任何其他对象，诸如访问控制列表 (ACL) 或访问控制条目 (ACE)。安全位置系统对这些数据结构进行扩展以包括位置信息作为访问资源的许可准则。

[0025] 在框 210 中开始，系统接收更新对所标识的资源的许可以便包括基于位置的许可信息的许可更新请求。例如，应用可以通过操作系统 API 来发送该请求，或者用户可以使命令行解释 (shell) 程序或其他工具来提交该请求。该请求通过路径或其他标识符来标识资源，并且包括访问控制信息，诸如包括地理位置作为至少一个访问准则的 ACL 和 / 或 ACE。例如，请求可以指示对只能从美国访问文件的许可。

[0026] 继续到框 220，系统定位所标识的资源。该资源可存储在磁盘（例如，文件或文件夹）上、在配置数据库（例如，注册表条目）内、在目录（例如，活动目录资源）内等。系统定位资源以检索与该条目相关联的任何有关的访问控制元数据。例如，该资源可包括连续地存储的或与该资源相关联的记录，该记录指定了访问控制信息。

[0027] 继续到框 230，系统定位与所标识的资源相关联的访问控制列表。在某些实施例中，系统修改现有的操作系统 API 以定位并检索地理访问限制的访问控制信息。操作系统通常包括用于导航并修改与各种类型的资源相关联的访问控制信息的健壮的安全 API 集。

[0028] 继续到框 240，系统从伴随该请求的基于位置的许可信息中确定一个或多个被允许的动作。动作可包括资源是否可被读、写、包括在列表中等。基于位置的许可信息可以标

识有界地理区域，诸如边由坐标定义的矩形、或其他合适的区域。例如，系统可以接收中心点和该中心点周围的、标识允许或不允许发生动作的地理区域的半径。许可在本质上既可以是正面的也可以是负面的，指示了关于所标识的资源允许或者不允许的东西。

[0029] 继续到框 250，系统更新已定位的访问控制列表以包括被允许的基于位置的动作。访问控制列表通常包括与用户可执行哪些动作有关的许可数据的分层结构，并且系统修改这些列表以包括可在哪里执行动作。可将基于位置的访问控制信息与其他访问控制信息进行组合，使得例如管理员可以在任何位置读文件，但受到更大限制的用户只能在指定的地理区域内读文件。

[0030] 继续到框 260，系统存储与所标识的资源相关联的已更新的访问控制列表，使得随后访问所标识的资源的尝试将受到指定的基于位置的访问信息的限制。例如，如果访问控制列表指示可执行动作的具体区域，则系统将在允许访问之前测试访问请求是否在该区域发生。参考图 3 进一步描述这一过程。在框 260 之后，这些步骤结束。

[0031] 图 3 是示出一个实施例中的使用基于位置的访问许可来访问资源的安全位置系统的处理的流程图。计算系统内的资源可包括位置信息作为访问资源的多个准则之一。例如，文件可包括用户和位置限制，使得特定的用户只能从指定的位置访问该文件。

[0032] 在框 310 中开始，系统接收访问所标识的资源的请求，其中所标识的资源包括基于位置的访问信息。例如，资源可包括文件、目录、打印机、计算机外设、配置数据库条目、或操作系统为其定义并实施访问控制的其他资源。该请求可以来自应用调用用于访问文件或其他资源的操作系统 API。请求包括标识与该请求相关联的安全主体的安全令牌。

[0033] 继续到框 320，系统访问位置信息的安全源。例如，系统可以调用向 GPS 和 / 或 TPM 硬件请求位置证书的操作系统 API，该位置证书提供可验证的以及可审核的位置指示。位置指示可包括纬度和经度坐标、或其他位置说明、以及时间戳和确认位置信息是当前的并且未被篡改的其他标识信息。计算设备可包括创建信任链的安全引导进程，该信任链确保操作系统对位置硬件具有控制以及与从操作系统接收的位置有关的输出是可信的。

[0034] 继续到框 330，系统从位置信息的安全源接收位置证书，该位置证书指示接收请求的计算设备的当前地理位置。该证书可包括签名或对位置信息的源的其他可密码验证的指示。接收者可以查询 TPM 或其他安全硬件以验证该签名，从而确保未发生对证书中提供的位置信息的篡改。系统还可创建已颁发的位置证书的日志，该日志形成用于对在特定位置执行的动作的任何日后调查的审计踪迹。

[0035] 继续到框 340，系统将已接收的位置证书所提供的基于位置的信息与和所标识的资源相关联的访问控制列表中的至少一个基于位置的限制进行比较。例如，访问控制列表可以指定资源无法在美国以外被读或写，可在美国内的任意地方被读取，以及仅能在特定城市内被写。这只是一个示例，并且本领域技术人员将意识到，访问控制列表许可访问限制的各种组合，以便为任何特定目的定制对资源的访问。

[0036] 继续到判决框 350，如果比较指示了对资源的所请求的访问在当前位置未被许可，那么系统在框 360 继续，否则系统在框 370 继续。继续至框 360，系统拒绝访问请求。系统可提供出错消息或请求被拒绝的其他指示。在某些实施例中，系统可以好像资源不存在那样来动作，在访问由于位置或其他未满足的限制而不被许可时有效地隐藏该资源。在某些实施例中，系统可以提供指示资源可在哪些条件下被访问的出错消息，使得例如用户可以

将设备移动至被允许的位置。

[0037] 继续到框 370，系统允许访问请求并且提供对资源的所请求的访问。例如，如果资源是文件，则系统可以允许打开并查看文件内容的请求。在某些实施例中，系统可以允许访问请求，但是基于设备的已确定的位置替换文件数据。例如，系统可在设备位于某些位置时返回充满令人不感兴趣的数据的文件系统，但在设备位于其他位置时返回秘密信息。在框 370 之后，这些步骤结束。

[0038] 在某些实施例中，安全位置系统方便对隐写文件系统的实现。隐写文件系统提供对存储设备上的数据的访问层。例如，基层是在没有密钥的情况下或从任何位置都可以访问的，并且包括对安全性不是特别敏感的良性数据。基于设备的当前位置，TPM 或其他安全硬件可以响应于访问请求而提供密码密钥。更高的层可以向那些具有适合的密钥的一方提供对敏感数据的越来越多的访问。以此方式，计算机可以在一个位置看起来被填满良性数据，但在另一个位置具有安全敏感信息。这可以为计算机用户提供如下保证 :如果计算设备被盗，则恶意用户将无法访问敏感的用户信息。

[0039] 在某些实施例中，安全位置系统允许操作系统基于运行系统的计算设备的位置来提供不同的特征。例如，安全位置系统可在计算设备位于限制使用 cookies 的国家时关闭 web 浏览器内的 cookies。作为另一个示例，操作系统可以基于设备正被使用的当地法律来改变用于安全套接字层 (SSL) 或其他加密通信的加密级别。操作系统厂商目前管理各自在特定国家发货的操作系统的多种库存单元 (SKU)。不仅对这种 SKU 的管理是困难的，而且在特定的国家出售特定 SKU 也无法保证某些人不会将不符合的 SKU 带入一国家。使用安全位置系统，操作系统厂商可以运送单个 SKU，该 SKU 基于对其被使用的位置的安全知识，自动地修改其行为，降低或消除了对多个 SKU 的需要并且减少了管理成本。

[0040] 在某些实施例中，安全位置系统用于嵌入式设备以便于基于位置的决定。例如，租车公司可包括在其出租的车队中实现该系统的设备以实施关于允许车队中的车辆被驾驶到哪里的地理限制。某些租车公司可能不希望车辆离开特定的国家或州、并且可以使用该系统来实施这种类型的限制。在其他实现中，公司可允许在其他地理区域中使用，但可记录信息，使得可针对该车辆所使用的每个区域的租金收取不同的费率。

[0041] 在某些实施例中，安全位置系统用各种基于位置的硬件来操作。如今来自很多不同厂商的设备中的 GPS 芯片是共同的，并且系统可被修改为与其中每一个共同工作。另外，系统可以采用包括每个 GPS 芯片基本唯一的标识符的 GPS 硬件，该基本唯一的标识符可被捕捉作为位置证书的一部分来标识提供位置信息的具体的位置机构。出于密码和标识目的，处理器和 TPM 使用了唯一的序列号，使得如果它们被破坏和出于其他理由，可以禁止具体的实例。类似的技术可被应用于 GPS 硬件以唯一地标识每个 GPS 单元，并且能够拒绝对不可信实例的访问。

[0042] 在某些实施例中，安全位置系统使用位置硬件和安全硬件之间的安全数据通信通道，诸如 GPS 模块和 TPM。该通道可包括已加密的通信，该通信允许 TPM 对 GPS 芯片的输出进行证实并且确保 GPS 硬件和操作系统或应用之间防篡改的信任链。在某些实施例中，可以用 TPM 或其他安全硬件管理的密码密钥来保护对资源的访问，并且 TPM 可以基于从位置硬件得出的设备的当前位置，交出有时间限制的密钥。

[0043] 在某些实施例中，安全位置系统使用位置信息来在移动计算设备上实施网络安全

策略。例如，系统可使用如下信息，膝上型计算机最近在外国，以确定病毒扫描应在设备可访问企业网络之前完成。为此，网络基础结构访问存储在计算设备上的历史位置信息，该历史位置信息提供设备自从上一次安全检查（如果有的话）以来曾经到过哪里的审计踪迹。系统可以限制传入或传出的联网通信，或二者都有。这些或其他策略可由安全位置系统来实施。

[0044] 从前面的描述中可以看出，可以理解，此处描述的安全位置系统的特定实施例只是为了说明，但是，在不偏离本发明的精神和范围的情况下，可以进行各种修改。因此，本发明只受所附权利要求限制。

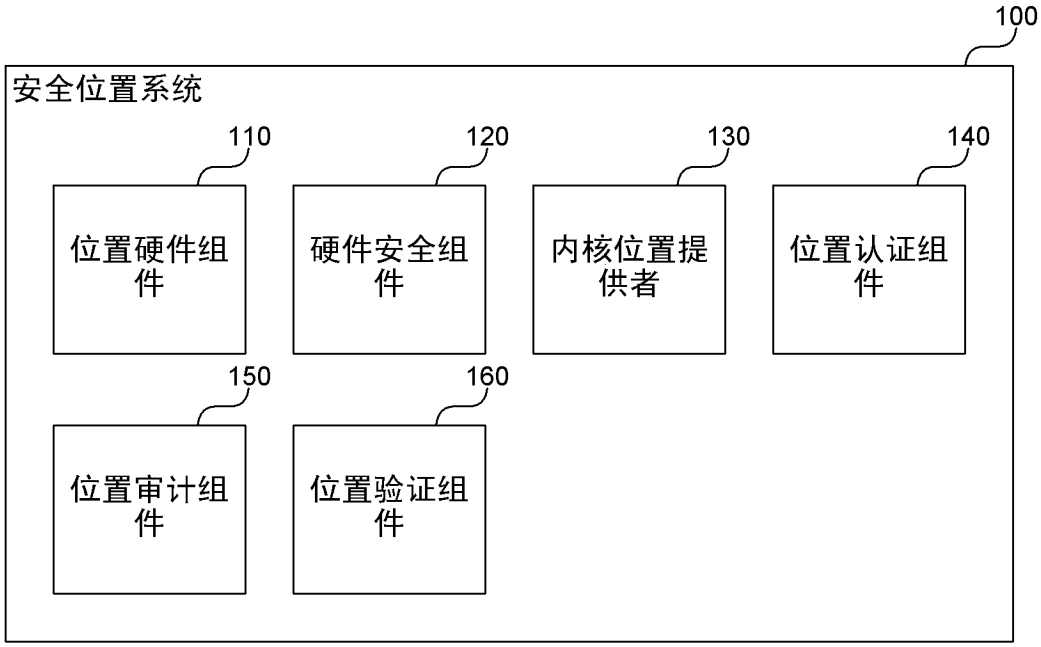

100
安全位置系统
110
位置硬件组件
120
硬件安全组件
130
内核位置提供者
140
位置认证组件
150
位置审计组件
160
位置验证组件

图 1

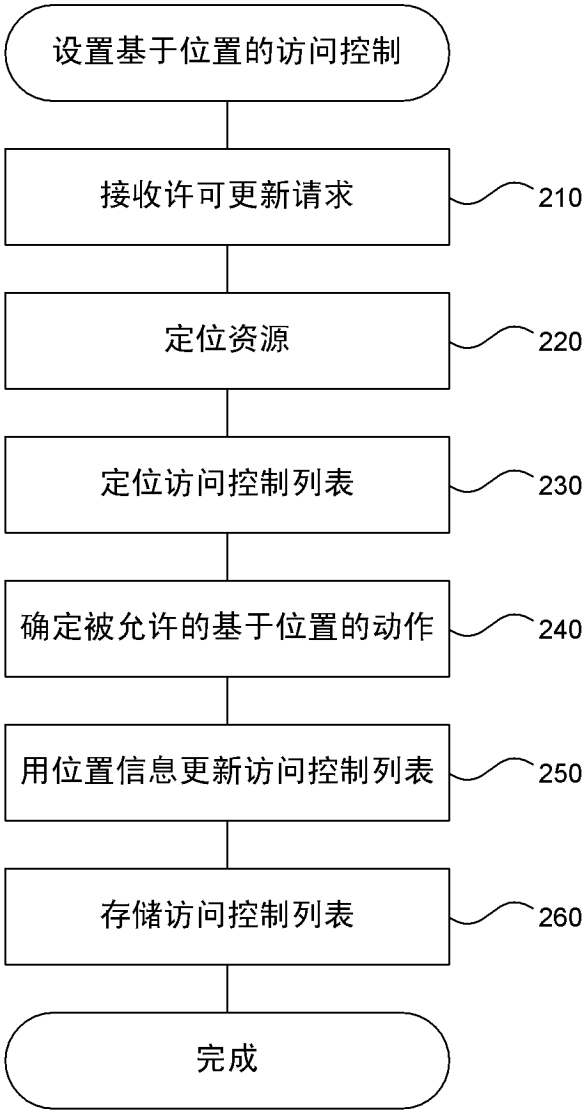

设置基于位置的访问控制
接收许可更新请求
210
定位资源
220
定位访问控制列表
230
确定被允许的基于位置的动作
240
用位置信息更新访问控制列表
250
存储访问控制列表
260
完成

图 2

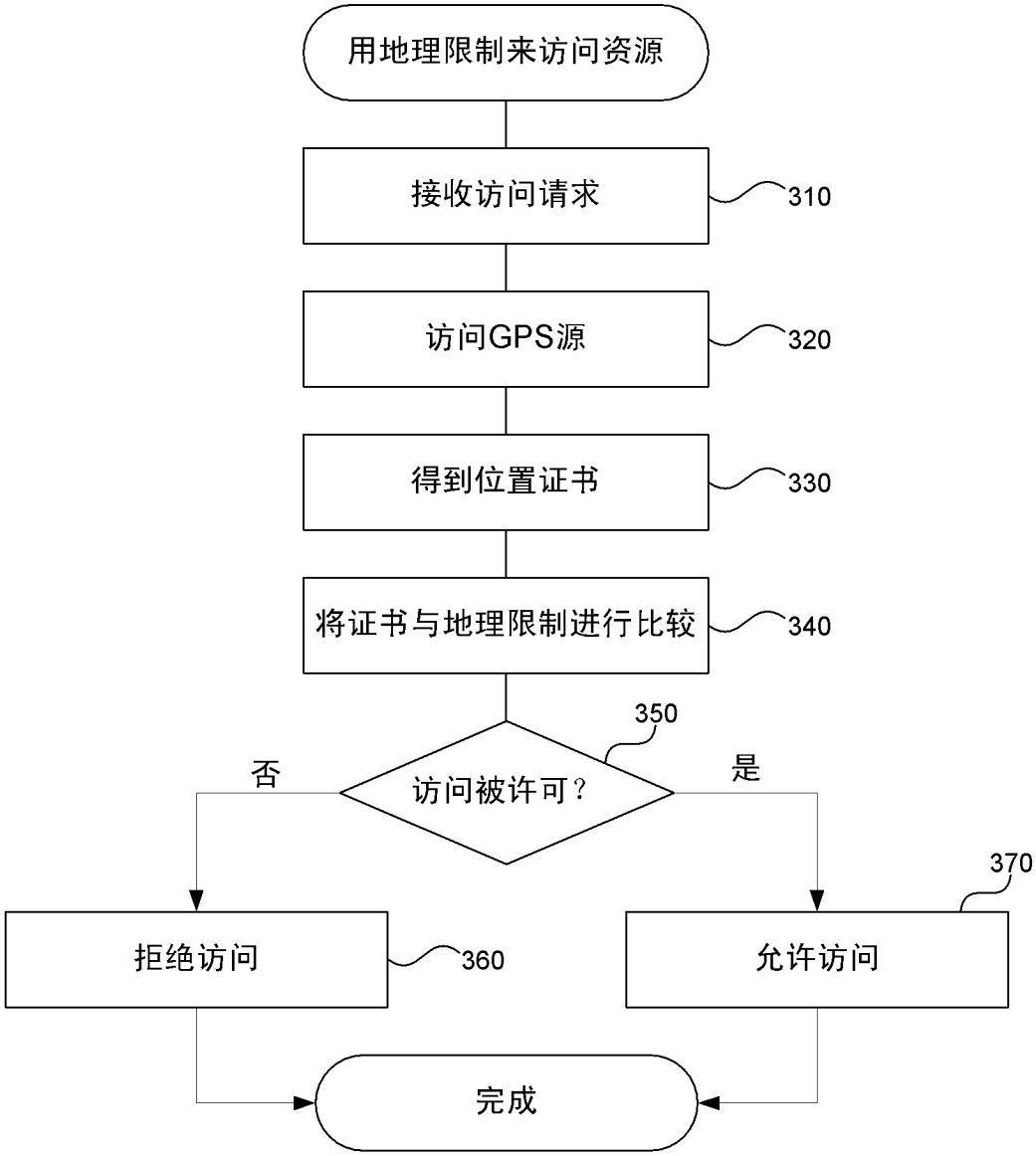

用地理限制来访问资源
接收访问请求
310
访问GPS源
320
得到位置证书
330
将证书与地理限制进行比较
340
350
访问被许可？
否
是
拒绝访问
360
允许访问
370
完成

图 3