(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104102358 A
(43)申请公布日 2014.10.15

(21)申请号 201410344802.4

(22)申请日 2014.07.18

(71)申请人 北京奇虎科技有限公司
地址 100088 北京市西城区新街口外大街28号D座112室(德胜园区)
申请人 奇智软件(北京)有限公司

(72)发明人 丁祎 王浩

(74)专利代理机构 北京华沛德权律师事务所 11302
代理人 刘杰

(51)Int.Cl.
G06F 3/033(2013.01)
G06F 17/30(2006.01)

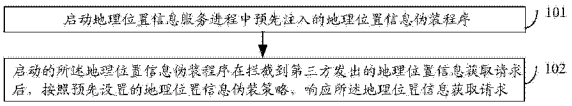
权利要求书2页 说明书18页 附图1页

(54)发明名称

隐私信息保护的方法及隐私信息保护装置

(57)摘要

本发明公开了一种隐私信息保护的方法及隐私信息保护装置。该方法包括:在隐私信息服务进程中注入隐私信息保护程序;所述隐私信息保护程序在识别到第三方应用发出的隐私信息获取请求后,按照预先设置的隐私信息保护策略,处理所述隐私信息获取请求。应用本发明,可以阻止和欺骗第三方应用获取用户隐私信息,有效提升用户隐私信息的安全性。



CN 104102358 A

1. 一种隐私信息保护的方法，包括：

在隐私信息服务进程中注入隐私信息保护程序；

所述隐私信息保护程序在识别到第三方应用发出的隐私信息获取请求后，按照预先设置的隐私信息保护策略，处理所述隐私信息获取请求。

2. 如权利要求 1 所述的方法，所述伪装隐私信息包括地理位置信息，所述按照预先设置的隐私信息保护策略，处理所述隐私信息获取请求包括：

从预先设置的地理位置信息伪装列表中，选取一伪装的地理位置信息，封装在隐私信息获取请求响应中，发送至第三方应用。

3. 如权利要求 1 所述的方法，所述伪装隐私信息包括地理位置信息，所述按照预先设置的隐私信息保护策略，处理所述隐私信息获取请求包括：

按照预先设置的基于虚拟路径规划的地理位置信息伪装算法，生成一伪装的地理位置信息，并将生成的伪装的地理位置信息封装在隐私信息获取请求响应中，发送至第三方应用。

4. 如权利要求 1 所述的方法，所述伪装隐私信息包括地理位置信息，所述按照预先设置的隐私信息保护策略，处理所述隐私信息获取请求包括：

分析隐私信息获取请求中包含的第三方应用信息，根据分析的第三方应用信息生成对应的具有时空合理性的伪装的地理位置信息，并将生成的伪装的地理位置信息封装在隐私信息获取请求响应中，发送至第三方应用。

5. 如权利要求 1 所述的方法，所述注入包括在第三方应用操作系统的隐私信息服务进程中注入，或，在智能终端设备的隐私信息服务进程中注入。

6. 如权利要求 5 所述的方法，所述在第三方应用操作系统的隐私信息服务进程中注入包括：

查找第三方应用操作系统的隐私信息服务进程中已有的用于隐私信息处理的目标程序的内存变量；

将所述已有的用于隐私信息处理的目标程序的内存变量替换为预先设置的动态目标程序的内存变量。

7. 如权利要求 6 所述的方法，所述用于隐私信息处理的目标程序为第三方应用发送地址位置信息获取请求的程序。

8. 如权利要求 6 所述的方法，所述将所述已有的用于隐私信息处理的目标程序的内存变量替换为预先设置的动态目标程序的内存变量包括：

将隐私信息保护程序的内存变量代码写入动态链接库中，利用操作系统中的 windows 钩子将写入动态链接库中的隐私信息保护程序的内存变量代码映射到远程隐私信息服务进程。

9. 一种隐私信息保护装置，该装置包括：注入模块以及识别处理模块，其中，

注入模块，用于在隐私信息服务进程中注入预先设置的隐私信息保护程序；

识别处理模块，用于在所述隐私信息保护程序识别到第三方应用发出的隐私信息获取请求后，按照预先设置的隐私信息保护策略，处理所述隐私信息获取请求。

10. 如权利要求 9 所述的装置，所述注入模块用于在第三方应用操作系统的隐私信息服务进程中预先注入动态目标程序，通过动态注入的目标程序的用于调用系统隐私信息服

务的变量或方法，替换第三方应用操作系统的目标程序的用于调用系统隐私信息服务的变量或方法。

隐私信息保护的方法及隐私信息保护装置

技术领域

[0001] 本发明涉及智能终端定位技术，具体涉及一种隐私信息保护的方法及隐私信息保护装置。

背景技术

[0002] 智能终端设备是指具有多媒体功能的设备，可以支持音频、视频、数据传输，通过采用开放式的操作系统，可装载相应的应用程序来实现相应的应用功能，为应用程序运行和内容服务提供平台，使得大量的增值业务，例如，新闻、天气、交通、商品、应用程序下载、音乐图片下载等可以基于该平台实现，包括固定智能终端设备以及移动智能终端设备。

[0003] 随着各种智能终端设备和无线网络的日益普及，智能终端设备可以同时具有移动网络连接、基站定位、无线保真 (WiFi，Wireless Fidelity) 无线局域网、GPS 定位等多种无线连接和定位功能。其中，基于地理位置信息服务的基站定位、GPS 定位等服务作为一种新型的空间信息服务模式呈现出良好的市场前景和发展势头，而且，当前的大多智能终端设备都申请了获取地理位置信息服务的权限，允许无线网络通过特定的定位技术获取智能终端设备的位置信息，提供给用户、通信系统或第三方应用，使得第三方应用通过无线网络可以获取智能终端设备的地理位置信息。虽然，在一些场景下，通过申请获取地理位置信息服务的权限，确实能方便智能终端设备用户（简称用户）的使用，但是，地理位置信息作为用户的一个重要隐私信息，标志着用户当前所在的地理位置，由于第三方应用也可通过用户申请的地理位置信息服务权限获取该用户的地理位置信息，而用户不能确认该第三方应用对用户地理位置信息的收集是否能用于合理的用途，因而，可能导致用户地理位置信息等隐私信息的泄露。

[0004] 根据地理位置信息服务的提供方式，地理位置信息服务可以分为需要智能终端设备上报地理位置信息的方式以及无需智能终端设备上报地理位置信息的方式，尤其是后者，在接收到请求后，直接提供自身的地理位置信息，由于无需智能终端设备的主动参与，用户无法确认其是否处于被定位的状态，除非用户放弃任何通信服务，否则无法隐藏智能终端设备的地理位置信息并阻止第三方应用获取用户的地理位置信息。例如，对于 WiFi 网络，如果用户在应用信息中设置了可以基于网络定位大致位置，或者，基于 GPS 和网络定位精确位置的地理位置信息服务，这样，第三方应用通过申请地理位置信息服务权限以及获取 WiFi 信息的权限，就可以通过读取智能终端设备连接的 WiFi 热点或者智能终端设备周围 WiFi 热点的服务集标识符 (SSID，Service Set Identifier)、基本服务集标识符 (BSSID，Basic Service Set Identifier) 以及信号强度，从而可以获取智能终端设备连接的基站信息，第三方应用将获取的基站信息直接通过网络传输至位置服务器，位置服务器在接收到 WIFI 信息后，通过查询数据库的方法，确定出 WIFI 的经纬度信息，从而使得第三方应用可以获取智能终端设备的大致经纬度信息（地理位置信息），造成用户隐私信息的泄漏。再例如，对于移动通信网络，由于智能终端设备无论在待机状态还是在激活状态，都需要至少与一移动通信网络，例如，基站建立联系，由于可以确定与智能终端设备通信联系的主基站，

而基站的位置是固定的且为已知；进一步地，基站的覆盖范围（小区）也是已知的，因而，第三方应用通过需要定位的智能终端设备所在的基站以及小区信息，就可以确定智能终端设备的地理位置信息。

发明内容

[0005] 鉴于上述问题，提出了本发明以便提供一种克服上述问题或者至少部分地解决上述问题的隐私信息保护的方法及隐私信息保护装置。

[0006] 依据本发明的一个方面，提供了隐私信息保护的方法，该方法包括：

[0007] 在隐私信息服务进程中注入隐私信息保护程序；

[0008] 所述隐私信息保护程序在识别到第三方应用发出的隐私信息获取请求后，按照预先设置的隐私信息保护策略，处理所述隐私信息获取请求。

[0009] 优选地，所述伪装隐私信息包括地理位置信息，所述按照预先设置的隐私信息保护策略，处理所述隐私信息获取请求包括：

[0010] 从预先设置的地理位置信息伪装列表中，选取一伪装的地理位置信息，封装在隐私信息获取请求响应中，发送至第三方应用。

[0011] 优选地，所述伪装隐私信息包括地理位置信息，所述按照预先设置的隐私信息保护策略，处理所述隐私信息获取请求包括：

[0012] 按照预先设置的基于虚拟路径规划的地理位置信息伪装算法，生成一伪装的地理位置信息，并将生成的伪装的地理位置信息封装在隐私信息获取请求响应中，发送至第三方应用。

[0013] 优选地，所述伪装隐私信息包括地理位置信息，所述按照预先设置的隐私信息保护策略，处理所述隐私信息获取请求包括：

[0014] 分析隐私信息获取请求中包含的第三方应用信息，根据分析的第三方应用信息生成对应的具有时空合理性的伪装的地理位置信息，并将生成的伪装的地理位置信息封装在隐私信息获取请求响应中，发送至第三方应用。

[0015] 优选地，所述注入包括在第三方应用操作系统的隐私信息服务进程中注入，或，在智能终端设备的隐私信息服务进程中注入。

[0016] 优选地，所述在第三方应用操作系统的隐私信息服务进程中注入包括：

[0017] 查找第三方应用操作系统的隐私信息服务进程中已有的用于隐私信息处理的目标程序的内存变量；

[0018] 将所述已有的用于隐私信息处理的目标程序的内存变量替换为预先设置的动态目标程序的内存变量。

[0019] 优选地，所述用于隐私信息处理的目标程序为第三方应用发送地址位置信息获取请求的程序。

[0020] 优选地，所述将所述已有的用于隐私信息处理的目标程序的内存变量替换为预先设置的动态目标程序的内存变量包括：

[0021] 将隐私信息保护程序的内存变量代码写入动态链接库中，利用操作系统中的windows钩子将写入动态链接库中的隐私信息保护程序的内存变量代码映射到远程隐私信息服务进程。

[0022] 优选地，所述将所述已有的用于隐私信息处理的目标程序的内存变量替换为预先设置的动态目标程序的内存变量包括：

[0023] 将隐私信息保护程序的内存变量代码写入动态链接库中，利用操作系统中的远程注入以及动态加载将写入动态链接库中的隐私信息保护程序的内存变量代码映射到远程隐私信息服务进程。

[0024] 优选地，所述将所述已有的用于隐私信息处理的目标程序的内存变量替换为预先设置的动态目标程序的内存变量包括：

[0025] 利用系统进程监视器，将隐私信息保护程序的内存变量代码复制到远程隐私信息服务进程，并利用远程注入执行。

[0026] 优选地，所述在智能终端设备的隐私信息服务进程中注入包括：

[0027] 查找智能终端设备操作系统的隐私信息服务进程中已有的用于隐私信息处理的系统定位服务程序的函数；

[0028] 将所述已有的用于隐私信息处理的系统定位服务程序的函数替换为预先设置的系统定位服务程序的函数。

[0029] 优选地，所述在隐私信息服务进程中注入隐私信息保护程序之前，所述方法进一步包括：

[0030] 获取第三方应用操作系统或智能终端设备操作系统的根权限。

[0031] 优选地，所述隐私信息保护程序在识别到第三方应用发出的隐私信息获取请求后，所述方法进一步包括：

[0032] 解析隐私信息获取请求，获取包含的智能终端设备信息，向获取的智能终端设备信息对应的智能终端设备发送提示信息，以提示用户是否选取隐私信息保护策略，并在接收到用户选取隐私信息保护策略的信息后，执行所述按照预先设置的隐私信息保护策略，处理所述隐私信息获取请求的流程。

[0033] 优选地，所述按照预先设置的隐私信息保护策略，处理所述隐私信息获取请求包括：

[0034] 从预先设置的伪装隐私信息列表中，选取一伪装隐私信息，封装在隐私信息获取请求响应中，发送至第三方应用。

[0035] 优选地，所述按照预先设置的隐私信息保护策略，处理所述隐私信息获取请求包括：

[0036] 按照预先设置的伪装隐私信息生成算法，生成一伪装隐私信息，并将生成的伪装隐私信息封装在隐私信息获取请求响应中，发送至第三方应用。

[0037] 优选地，所述伪装隐私信息生成算法为基于虚拟路径规划的生成算法。

[0038] 优选地，所述按照预先设置的隐私信息保护策略，处理所述隐私信息获取请求包括：

[0039] 分析隐私信息获取请求中包含的第三方应用信息，根据分析的第三方应用信息生成对应的具有时空合理性的伪装隐私信息，并将生成的伪装隐私信息封装在隐私信息获取请求响应中，发送至第三方应用。

[0040] 优选地，所述第三方应用通过所述隐私信息服务进程发出隐私信息获取请求。

[0041] 优选地，在所述处理所述隐私信息获取请求后，所述方法进一步包括：

[0042] 向智能终端设备发送消息提醒；和 / 或，

[0043] 对所述第三方应用进行安全扫描；和 / 或，

[0044] 卸载所述第三方应用；和 / 或，

[0045] 为所述第三方应用设置隐私访问权限。

[0046] 优选地，一种在申请了地理位置信息服务权限环境下的隐私信息保护方法，执行如权利要求 1 至 19 任一项所述的方法。

[0047] 根据本发明的另一个方面提供了一种隐私信息保护装置，该装置包括：注入模块以及识别处理模块，其中，

[0048] 注入模块，用于在隐私信息服务进程中注入预先设置的隐私信息保护程序；

[0049] 识别处理模块，用于在所述隐私信息保护程序识别到第三方应用发出的隐私信息获取请求后，按照预先设置的隐私信息保护策略，处理所述隐私信息获取请求。

[0050] 优选地，所述注入模块用于在第三方应用操作系统的隐私信息服务进程中预先注入动态目标程序，通过动态注入的目标程序的用于调用系统隐私信息服务的变量或方法，替换第三方应用操作系统的目标程序的用于调用系统隐私信息服务的变量或方法。

[0051] 优选地，所述注入模块用于在智能终端设备操作系统的隐私信息服务进程中预先注入系统定位服务程序，替换智能终端设备操作系统定位服务内的函数为注入的系统定位服务程序对应的函数。

[0052] 优选地，所述注入模块包括：第一查找单元以及第一替换单元，其中，

[0053] 第一查找单元，用于查找第三方应用操作系统的隐私信息服务进程中已有的用于隐私信息处理的目标程序的内存变量；

[0054] 第一替换单元，用于将所述已有的用于隐私信息处理的目标程序的内存变量替换为预先设置的动态目标程序的内存变量。

[0055] 优选地，所述注入模块包括：第二查找单元以及第二替换单元，其中，

[0056] 第二查找单元，用于查找智能终端设备操作系统的隐私信息服务进程中已有的用于隐私信息处理的系统定位服务程序的函数；

[0057] 第二替换单元，用于将所述已有的用于隐私信息处理的系统定位服务程序的函数替换为预先设置的系统定位服务程序的函数。

[0058] 优选地，所述识别处理模块包括：识别单元以及处理单元，其中，

[0059] 识别单元，用于在启动的隐私信息保护程序识别到第三方应用发出的隐私信息获取请求后，通知响应单元；

[0060] 处理单元，用于接收通知，按照预先设置的隐私信息保护策略，处理所述隐私信息获取请求。

[0061] 优选地，所述识别处理模块进一步包括：

[0062] 解析单元，用于接收来自识别单元的通知，解析隐私信息获取请求，获取包含的智能终端设备信息，向获取的智能终端设备信息对应的智能终端设备发送提示信息，以提示用户是否选取隐私信息保护策略，并在接收到用户选取隐私信息保护策略的信息后，通知响应单元。

[0063] 优选地，所述装置进一步包括：

[0064] 权限获取模块，用于在获取第三方应用操作系统或智能终端设备操作系统的根权

限后，通知注入模块。

[0065] 优选地，所述装置进一步包括：

[0066] 扩展模块，用于在所述处理所述隐私信息获取请求后，向智能终端设备发送消息提醒；和/或，

[0067] 对所述第三方应用进行安全扫描；和/或，

[0068] 卸载所述第三方应用；和/或，

[0069] 为所述第三方应用设置隐私访问权限。

[0070] 根据本发明的隐私信息保护的方法及隐私信息保护装置，可以通过在第三方应用或智能终端设备中注入预先设置的地理位置信息保护程序，实现控制操作系统中的任何一个系统进程，从而在第三方应用发起地理位置信息获取请求时，第三方应用操作系统或智能终端设备操作系统中预先注入的地理位置信息保护程序截获该地理位置信息获取请求，并按照预先设置的地理位置信息保护策略，将伪装的地理位置信息返回给第三方应用。由此解决了用户隐私信息泄漏的技术问题，取得了阻止和欺骗第三方应用获取用户的地理位置信息，有效提升用户隐私信息的安全性的有益效果。

[0071] 上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

[0072] 通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

[0073] 图 1 示出了本发明实施例地理位置信息保护的方法流程；以及，

[0074] 图 2 示出了本发明实施例的地理位置信息保护装置结构。

具体实施方式

[0075] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0076] 现有技术中，用户在申请了地理位置信息服务权限后，如果采用无需智能终端设备上报地理位置信息的方式共享地理位置信息服务，即第三方应用（或称第三方应用应用程序）在需要获取地理位置信息时，通过向智能终端设备发起地理位置信息获取请求，智能终端设备在接收到地理位置信息获取请求后，响应于地理位置信息获取请求，将自身的地理位置信息封装在地理位置信息获取请求响应中，返回至第三方应用，从而使得第三方应用可以获取智能终端设备的地理位置信息。由于用户无法确认其是否处于被第三方应用定位的状态，且无法阻止第三方应用获取用户的地理位置信息等隐私信息，使得用户的隐私信息被泄漏的风险大。

[0077] 实际应用中，不同的用户，对操作系统进行操作的权限可能不同。对于智能终端设

备操作系统（简称系统）来说，操作系统将用户分为不同的权限组，并为每个权限组赋予相应的操作权限，权限组可以包括：管理员权限组、高权限用户组、普通用户组、备份操作组、文件复制组以及匿名权限组等。其中，管理员权限组对应的操作权限为管理员权限，高权限用户组对应的操作权限为高权限，普通用户组对应的操作权限为普通权限等。

[0078] 本发明实施例中，考虑到不同的操作权限虽然将用户对操作系统的操作限制在相应的操作权限内，但由于各操作权限之间并不相互独立，都依赖于同样的指令完成权限操作。因而，可以利用提升权限（Adjust Token Privilege）的方法提升用户的操作权限，其中，提升权限是指程序员利用各种操作系统漏洞，突破操作系统指派的操作权限级别，将自己当前的操作权限提高一个或多个级别，从而使用户获取更多对操作系统进行操作的权限，例如，通过提升权限的方法，可以使用户获取原先未曾拥有的对系统文件的删、增、改等权限。现有提升权限的方法应用较为广泛的包括智能终端设备刷机、根权限以及越狱等。

[0079] 本发明实施例中，基于上述分析和考虑，提出一种地理位置信息保护的方法，通过利用智能终端设备的操作系统漏洞，利用提升权限的方法，获取操作系统的高级操作权限，在获取高级操作权限后，在第三方应用或智能终端设备中注入（inject）地理位置信息保护程序，可以实现控制操作系统中的任何一个进程，从而在第三方应用发起地理位置信息获取请求时，第三方应用中预先注入的地理位置信息保护程序截获该地理位置信息获取请求，使之不发向智能终端设备，并按照预先设置的地理位置信息保护策略，将保护的地理位置信息返回给第三方应用；或者，在第三方应用发起的地理位置信息获取请求到达智能终端设备后，智能终端设备中预先注入的截获该地理位置信息获取请求，并按照预先设置的地理位置信息保护策略，将保护的地理位置信息返回给第三方应用。这样，通过对用户的地理位置信息进行保护，用以阻止和欺骗第三方应用获取用户的地理位置信息，从而降低用户的地理位置信息被泄露的风险，提升用户隐私信息的安全性。

[0080] 本发明实施例中，以安装有安卓（Android）系统的智能终端设备、隐私信息为地理位置信息为例进行示例性说明，但所应说明的是，该描述仅是示例性的，本发明的范围并不限于此，本发明实施例的方法也可适用于安装有其他操作系统，例如，Linux 操作系统、iOS 操作系统、Window Phone 操作系统等的智能终端设备，隐私信息也可以是其他信息，例如，国际移动用户识别码（IMSI，International Mobile Subscriber Identification Number）信息、移动电话信息等。

[0081] 图 1 示出了本发明实施例地理位置信息保护的方法流程。参见图 1，该流程包括：

[0082] 步骤 101，启动地理位置信息服务进程中预先注入的地理位置信息伪装程序；

[0083] 本步骤中，作为可选实施例，地理位置信息伪装程序为前述的地理位置信息保护程序。可以在第三方应用操作系统的地理位置信息服务（位置服务）进程中预先注入地理位置信息保护程序（隐私信息保护程序），即动态注入目标程序，通过动态注入的目标程序的用于调用系统地理位置信息服务的变量或方法，例如内存变量或函数替换第三方应用操作系统的目标程序的用于调用系统地理位置信息服务的变量或方法，从而可以达到识别的目的，相应的，地理位置信息服务进程可以是后续第三方应用发送地址位置信息获取请求的程序对应的进程。作为另一可选实施例，也可以在智能终端设备操作系统的地理位置信息服务进程中预先注入地理位置信息保护程序，即注入系统定位服务程序，替换智能终端设备操作系统定位服务内的函数为注入的系统定位服务程序对应的函数，达到识别的目

的，相应的，地理位置信息服务进程可以是后续智能终端设备接收地址位置信息获取请求的程序对应的进程。

[0084] 本发明实施例中，在第三方应用操作系统的地理位置信息服务进程中预先注入地理位置信息保护程序包括：

[0085] A11，查找第三方应用操作系统的地理位置信息服务进程中已有的用于地理位置信息处理的目标程序的内存变量；

[0086] 本步骤中，用于地理位置信息处理的目标程序为第三方应用发送地址位置信息获取请求的程序。

[0087] A12，将所述已有的用于地理位置信息处理的目标程序的内存变量替换为预先设置的动态目标程序的内存变量。

[0088] 在智能终端设备的地理位置信息服务进程中预先注入地理位置信息保护程序包括：

[0089] B11，查找智能终端设备操作系统的地理位置信息服务进程中已有的用于地理位置信息处理的系统定位服务程序的函数；

[0090] 本步骤中，用于地理位置信息处理的系统定位服务程序为智能终端设备接收地址位置信息获取请求的程序。

[0091] B12，将所述已有的用于地理位置信息处理的系统定位服务程序的函数替换为预先设置的系统定位服务程序的函数。

[0092] 本发明实施例中，地理位置信息保护程序包括：动态目标程序以及系统定位服务程序。作为可选实施例，步骤 A12 和 B12 可以具体包括：

[0093] 将地理位置信息保护程序的内存变量代码或函数写入动态链接库 (DLL，Dynamic Link Library) 中，利用操作系统中的 windows 钩子将写入动态链接库中的地理位置信息保护程序的内存变量代码或函数映射到远程地理位置信息服务进程。

[0094] 作为另一可选实施例，步骤 A12 和 B12 也可以包括：

[0095] 将地理位置信息保护程序的内存变量代码或函数写入动态链接库 (DLL，Dynamic Link Library) 中，利用操作系统中的远程注入 (CreatRemoteThread) 以及动态加载 (LoadLibrary) 将写入动态链接库中的地理位置信息保护程序的内存变量代码或函数映射到远程地理位置信息服务进程。

[0096] 作为再一可选实施例，步骤 A12 和 B12 还可以包括：

[0097] 利用系统进程监视器 (WriteProcessMemory)，将地理位置信息保护程序的内存变量代码或函数复制到远程地理位置信息服务进程，并利用远程注入 (CreatRemoteThread) 执行。

[0098] 实际应用中，地理位置信息保护程序中存储的地理位置信息可以文件的形式进行存储，这样，可以通过统一调用读取函数去读取该文件或者该文件的内存映射。这样，可以通过注入的动态目标程序的读取函数替换第三方应用操作系统的目标程序的读取函数；或者，通过注入的系统定位服务程序的读取函数替换智能终端设备操作系统定位服务程序内的函数。本发明实施例中，具体来说，可以通过在操作系统中找到地理位置信息服务进程，在地理位置信息服务进程的位置加载地理位置信息保护程序。例如，可以通过安卓系统所基于的 Linux 系统所提供的应用程序编程接口 (API，Application Programming

Interface)，以指定模式打开一个动态链接库的 dlopen 方法，将地理位置信息保护程序加载到地理位置信息服务进程中，从而替换地理位置信息服务进程中的相关函数为地理位置信息保护程序中相对应的函数。其中，替换后的地理位置信息保护程序中相对应的函数所实现的功能与地理位置信息服务进程中的相关函数所实现的功能一致，且追加有地理位置信息获取请求识别功能。这样，在地理位置信息服务进程发送地理位置信息获取请求后，先调用地理位置信息保护程序进行处理。

[0099] 所应说明的是，本发明实施例中的注入仅是示例性的，本领域普通技术人员可以采用其他的技术来完成将地理位置信息处理程序替换为地理位置信息保护程序，本发明实施例不再一一例举。

[0100] 本发明实施例中，在地理位置信息服务进程中注入地理位置信息保护程序后，地理位置信息保护程序可以替换地理位置信息服务进程中已有的目标程序或系统定位服务程序。这样，后续应用中，可以通过底层接口识别第三方应用发出的地理位置信息获取请求，而不会影响其它应用程序的正常使用。

[0101] 作为可选实施例，在启动地理位置信息服务进程中预先注入的地理位置信息保护程序之前，该方法可以进一步包括：

[0102] 获取第三方应用操作系统或智能终端设备操作系统的根 (Root) 权限。

[0103] 本步骤中，通过预先获取第三方应用操作系统或智能终端设备操作系统的 Root 权限，从而可以实现提升权限。其中，Root 是 Linux 操作系统和 Unix 操作系统中的超级管理员用户账户，如果获得 Root 权限，表示已经获取第三方应用操作系统或智能终端设备操作系统的最高权限。这样，可以对第三方应用或智能终端设备中的任何文件（包括操作系统文件）执行增、删、改、查等操作，从而实现地理位置信息保护程序的注入。

[0104] 步骤 102，启动的所述地理位置信息伪装程序在拦截到第三方发出的地理位置信息获取请求后，按照预先设置的地理位置信息伪装策略，响应所述地理位置信息获取请求。

[0105] 本步骤中，启动的所述地理位置信息保护程序在识别到第三方应用发出的地理位置信息获取请求后，按照预先设置的地理位置信息保护策略，处理所述地理位置信息获取请求。

[0106] 启动的地理位置信息保护程序实时监测第三方应用通过隐私信息服务进程发出的地理位置信息获取请求。

[0107] 地理位置信息保护程序在识别到第三方应用发出的地理位置信息获取请求后，该方法可以进一步包括：

[0108] 解析地理位置信息获取请求，获取包含的智能终端设备信息，向获取的智能终端设备信息对应的智能终端设备发送提示信息，以提示用户是否选取地理位置信息保护策略，并在接收到用户选取地理位置信息保护策略的信息后，执行所述按照预先设置的地理位置信息保护策略，响应所述地理位置信息获取请求的流程。

[0109] 作为可选实施例，地理位置信息保护程序识别第三方应用发出的地理位置信息获取请求包括：

[0110] 在第三方应用发起地理位置信息获取请求后，第三方应用操作系统中注入的地理位置信息保护程序（动态目标程序）截获该地理位置信息获取请求，以使所述地理位置信息获取请求不发向智能终端设备；或者，

[0111] 第三方应用发起地理位置信息获取请求，发送至智能终端设备，智能终端设备操作系统中注入的地理位置信息保护程序（系统定位服务程序）截获该地理位置信息获取请求。具体地，第三方应用与智能终端设备操作系统的定位数据模块采用进程间通信机制，例如，Android 系统的 BINDER 通信机制。第三方应用调用 BINDER 通信机制接口函数，获取指向第三方应用位置服务的一个句柄（即内存变量或函数），然后，通过获取的句柄向位置服务发送跨进程的地理位置信息获取请求，通过进程间通信机制，位置服务接收地理位置信息获取请求，并再通过进程间通信机制，得到地理位置信息获取请求指向智能终端设备操作系统的定位数据模块的位置服务句柄，智能终端设备操作系统的定位数据模块的位置服务句柄接收地理位置信息获取请求，处理地理位置信息获取请求，并返回请求的数据（伪装的地理位置信息）。其中，智能终端设备操作系统的定位数据模块是一个独立的系统进程，与第三方应用不是同一个进程。

[0112] 本发明实施例中，由于第三方应用（应用程序）需要获取指向位置服务的句柄（内存变量），通过在第三方应用应用程序中注入地理位置信息保护程序，替换第三方应用应用程序获取到的指向位置服务的句柄（内存变量）为地理位置信息保护程序中设置的假句柄（内存变量），从而使得假句柄（内存变量）在被调用的时候执行识别的逻辑。或者，通过在智能终端设备操作系统中注入地理位置信息保护程序，将智能终端设备操作系统定位服务内的用于接收进程间通讯数据的句柄（内存变量）替换为地理位置信息保护程序中设置的假句柄（内存变量），使得假句柄（内存变量）优先于系统定位服务收到来自第三方应用的地理位置信息获取请求，假句柄（内存变量）在被调用时执行识别的逻辑。

[0113] 本发明实施例中，作为可选实施例，按照预先设置的地理位置信息保护策略，响应所述地理位置信息获取请求包括：

[0114] 从预先设置的伪装地理位置信息列表中，选取一伪装地理位置信息，封装在地理位置信息获取请求响应中，发送至第三方应用。

[0115] 作为可选实施例，所述伪装隐私信息包括地理位置信息，所述按照预先设置的隐私信息保护策略，处理所述隐私信息获取请求包括：

[0116] 从预先设置的地理位置信息伪装列表中，选取一伪装的地理位置信息，封装在隐私信息获取请求响应中，发送至第三方应用。

[0117] 作为另一可选实施例，所述伪装隐私信息包括地理位置信息，所述按照预先设置的隐私信息保护策略，处理所述隐私信息获取请求包括：

[0118] 按照预先设置的基于虚拟路径规划的地理位置信息伪装算法，生成一伪装的地理位置信息，并将生成的伪装的地理位置信息封装在隐私信息获取请求响应中，发送至第三方应用。

[0119] 作为再一可选实施例，所述伪装隐私信息包括地理位置信息，所述按照预先设置的隐私信息保护策略，处理所述隐私信息获取请求包括：

[0120] 分析隐私信息获取请求中包含的第三方应用信息，根据分析的第三方应用信息生成对应的具有时空合理性的伪装的地理位置信息，并将生成的伪装的地理位置信息封装在隐私信息获取请求响应中，发送至第三方应用。

[0121] 本步骤中，伪装地理位置信息列表中，既可以全部由伪装地理位置信息组成，从而隐藏用户真实的地理位置信息；也可以由伪装地理位置信息和当前实际地理位置信息组

成，通过真假地理位置信息来隐藏用户真实的地理位置信息。例如，伪装地理位置信息列表中可以包括：澳门葡京赌场、香港铜锣湾、迪拜棕榈岛、法国埃菲尔铁塔、法国巴黎圣母院以及巴厘岛等。举例来说，通过在伪装地理位置信息列表中模拟澳门葡京酒店的数据，这样，可以有效欺骗第三方应用，以为智能终端设备真的就在澳门。甚至可以欺骗第三方应用的社交软件找到虚假当地的网友。

[0122] 在选取地理位置信息时，可以是随机从伪装地理位置信息列表中选取一地理位置信息，也可以是按照等概率的方式从伪装地理位置信息列表中选取一地理位置信息。当然，实际应用中，也可以是将伪装地理位置信息列表先向用户显示，由用户进行选取，并将用户选取的地理位置信息封装在地理位置信息获取请求响应中。

[0123] 进一步地，对于选取的每一地理位置信息，还可以结合电子地图，将选取的地理位置信息标注在电子地图中，并将标注有地理位置信息的电子地图封装在地理位置信息获取请求响应中。例如，对于澳门葡京赌场，可以在电子地图中提供澳门葡京赌场具体的地理位置信息，举例来说，澳门葡京赌场对应电子地图中的澳门伦斯泰特大马路 37 号，再例如，对于 Guincho a Galera 葡国餐厅，对应电子地图中的澳门特别行政区大堂区半岛葡京路 2-4 号葡京酒店；对于 Aux Beaux Arts，对应电子地图中的澳门特别行政区大堂区半岛孙逸仙大马路美高梅酒店；对于中国银行大厦，对应电子地图中的澳门特别行政区大堂区苏亚利斯博士大马路 323 号。当然，实际应用中，也可以在电子地图中显示选取的地理位置信息周围的具体信息。

[0124] 作为一可选实施例，地理位置信息包括：纬度信息、经度信息以及海拔信息等。作为另一可选实施例，地理位置信息也可以包括：服务集标识符信息、基本服务集标识符信息、基站信息以及相邻基站信息等，或者，地理位置信息也可以包括：服务集标识符信息映射的经纬度信息等。其中，基站可以是移动网络的移动电话无线基站，也可以是无线局域网(WLAN，Wireless Local Area Networks)的无线基站，基站信息可以包括：智能终端设备电讯网络商名称信息、基站频段、基站信道、基站认证信息、基站位置坐标、基站类型、基站名称、基站型号、基站媒体接入控制层(MAC，Medium Access Control)地址、基站网络信息、基站位置区编码(LAC，Location Area Code)、基站小区标识(Cell ID)信息等。例如，当智能终端设备连接移动电话无线基站时，基站信息为基站 LAC、基站 Cell ID 等相关信息，当智能终端设备连接 WiFi 基站，例如，智能终端设备连接的 WiFi 热点，或者智能终端设备周围可以探测到的 WiFi 热点时，基站信息为基站名称、基站 MAC 地址等相关信息。

[0125] 所应说明的是，本发明实施例中，服务集标识符信息、基本服务集标识符信息、基站信息以及相邻基站信息都为智能终端设备对应的伪装信息，而非真实的信息，但该伪装信息实际上是存在的，只是未在智能终端设备当前所在的区域内。

[0126] 本发明实施例中，伪装地理位置信息列表中的地理位置信息可以来自互联网上实地采集的地址数据，也可以来自用户自己采集的地址数据，并将采集的地址数据用于伪装。

[0127] 作为另一可选实施例，按照预先设置的地理位置信息保护策略，响应所述地理位置信息获取请求包括：

[0128] 按照预先设置的伪装地理位置信息生成算法，生成一地理位置信息，并将生成的地理位置信息封装在地理位置信息获取请求响应中，发送至第三方应用。

[0129] 本步骤中，伪装地理位置信息生成算法可以是基于虚拟路径规划的生成算法。本

发明实施例中，可以通过构建虚拟路径规划来掩盖用户的真实轨迹，从而保护用户真实的地理位置信息。例如，基于虚拟路径规划的生成算法可以是预先设置的一条从哈尔滨经北京、南京至拉萨的虚拟路径规划，在虚拟路径规划中，设置多个依序相连的伪装地理位置信息，在识别到地理位置信息获取请求后，按照识别的时间顺序，将顺序标记在虚拟路径规划中的伪装地理位置信息封装在地理位置信息获取请求响应中，发送至第三方应用。当然，实际应用中，还可以根据预先设置的交通工具以及接收的前后地理位置信息获取请求之间的时间差，计算基于当前的地理位置，在所述交通工具经过所述时间差的运行后对应的地理位置，将该对应的地理位置信息封装在地理位置信息获取请求响应中。例如，上一次地理位置信息获取请求响应中返回的地理位置信息为北京，如果接收的当前与上一次地理位置信息获取请求之间的时间差为 16 小时，预先设置的交工工具为火车，则火车经过 16 小时的运行，应该达到虚拟路径规划中的长沙，则将长沙封装在当前地理位置信息获取请求响应中。

[0130] 作为再一可选实施例，按照预先设置的地理位置信息保护策略，响应所述地理位置信息获取请求包括：

[0131] 分析地理位置信息获取请求中包含的第三方应用信息，根据分析的第三方应用信息生成对应的具有时空合理性的地理位置信息，并将生成的地理位置信息封装在地理位置信息获取请求响应中，发送至第三方应用。

[0132] 本步骤中，第三方应用可能会基于不同的目的，需要向用户获取不同的隐私信息。例如，如果第三方应用为旅游类公司，则希望获取用户的旅游地点相关信息，本发明实施例中，可以在分析第三方应用为旅游相关公司后，生成伪装旅游路径对应的地理位置信息。举例来说，设置北京－三亚－澳门的旅游路线，根据接收的该第三方应用依序发送的地理位置信息获取请求，依序返回北京、三亚、澳门等地理位置信息，从而构成虚拟旅游路线信息。其中，虚拟路径可以是用户动态选择的或者预先确定的，与真实路径无关，且用户可以随时启动虚拟路径规划。

[0133] 本发明实施例中，地理位置信息获取请求响应的格式与现有地理位置信息获取请求响应格式相同，即在截获第三方应用获取地理位置信息的调用之中，按照操作系统既定格式，返回给第三方应用返回值，该返回值是操作系统固定的格式，但该返回值的内容是预先设置的伪装地理位置信息而非真实地理位置信息，例如，设置该返回值的内容为某个异地基站的真实 MAC 地址等数据，从而可以欺骗第三方应用。

[0134] 作为可选实施例，在所述处理所述隐私信息获取请求后，所述方法进一步包括：

[0135] 向智能终端设备发送消息提醒；和 / 或，

[0136] 对所述第三方应用进行安全扫描；和 / 或，

[0137] 卸载所述第三方应用；和 / 或，

[0138] 为所述第三方应用设置隐私访问权限。

[0139] 作为可选实施例，本发明实施例的方法可以应用于在申请了地理位置信息服务权限环境下的隐私信息保护方法。

[0140] 图 2 示出了本发明实施例的地理位置信息保护装置结构。参见图 2，该装置包括：注入模块、启动模块以及识别处理模块，其中，

[0141] 注入模块，用于在地理位置信息服务进程中注入预先设置的地理位置信息保护程序；

[0142] 本发明实施例中，可以在第三方应用操作系统的地理位置信息服务进程中预先注入动态目标程序，通过动态注入的目标程序的用于调用系统地理位置信息服务的变量或方法，替换第三方应用操作系统的目标程序的用于调用系统地理位置信息服务的变量或方法，或者，也可以在智能终端设备操作系统的地理位置信息服务进程中预先注入系统定位服务程序，替换智能终端设备操作系统定位服务内的函数为注入的系统定位服务程序对应的函数。

[0143] 作为可选实施例，注入模块包括：第一查找单元以及第一替换单元（图中未示出），其中，

[0144] 第一查找单元，用于查找第三方应用操作系统的地理位置信息服务进程中已有的用于地理位置信息处理的目标程序的内存变量；

[0145] 本发明实施例中，用于地理位置信息处理的目标程序为第三方应用发送地址位置信息获取请求的程序。

[0146] 第一替换单元，用于将所述已有的用于地理位置信息处理的目标程序的内存变量替换为预先设置的动态目标程序的内存变量。

[0147] 本发明实施例中，第一替换单元进行替换的具体流程如下：

[0148] 将地理位置信息保护程序的内存变量代码写入动态链接库中，利用操作系统中的windows钩子将写入动态链接库中的地理位置信息保护程序的内存变量代码映射到远程地理位置信息服务进程；或者，

[0149] 将地理位置信息保护程序的内存变量代码写入动态链接库中，利用操作系统中的远程注入以及动态加载将写入动态链接库中的地理位置信息保护程序的内存变量代码射到远程地理位置信息服务进程；或者，

[0150] 利用系统进程监视器，将地理位置信息保护程序的内存变量代码复制到远程地理位置信息服务进程，并利用远程注入执行。

[0151] 作为另一可选实施例，注入模块包括：第二查找单元以及第二替换单元，其中，

[0152] 第二查找单元，用于查找智能终端设备操作系统的地理位置信息服务进程中已有的用于地理位置信息处理的系统定位服务程序的函数；

[0153] 本发明实施例中，用于地理位置信息处理的系统定位服务程序为智能终端设备接收地址位置信息获取请求的程序。

[0154] 第二替换单元，用于将所述已有的用于地理位置信息处理的系统定位服务程序的函数替换为预先设置的系统定位服务程序的函数。

[0155] 本发明实施例中，第二替换单元进行替换的具体流程与第一替换单元进行替换的具体流程相类似，在此略去详述。

[0156] 启动模块，用于启动地理位置信息服务进程中预先注入的地理位置信息保护程序；

[0157] 本发明实施例中，启动模块为可选模块。

[0158] 识别处理模块，用于在启动的地理位置信息保护程序识别到第三方应用发出的地理位置信息获取请求后，按照预先设置的地理位置信息保护策略，处理所述地理位置信息获取请求。

[0159] 本发明实施例中，识别处理模块包括：识别单元以及处理单元（图中未示出），其

中，

[0160] 识别单元，用于在启动的地理位置信息保护程序识别到第三方应用发出的地理位置信息获取请求后，通知响应单元；

[0161] 本发明实施例中，可以是第三方应用操作系统中注入的动态目标程序截获第三方应用发起的地理位置信息获取请求；也可以是第三方应用发起的地理位置信息获取请求达到智能终端设备后，由智能终端设备操作系统中注入的系统定位服务程序截获该地理位置信息获取请求。

[0162] 处理单元，用于接收通知，按照预先设置的地理位置信息保护策略，处理所述地理位置信息获取请求。

[0163] 本发明实施例中，处理单元可以从预先设置的伪装地理位置信息列表中，选取一地理位置信息，封装在地理位置信息获取请求响应中，发送至第三方应用。或者，按照预先设置的伪装地理位置信息生成算法，生成一伪装地理位置信息，并将生成的伪装地理位置信息封装在地理位置信息获取请求响应中，发送至第三方应用。其中，伪装地理位置信息生成算法可以是基于虚拟路径规划的生成算法，从而可以通过构建虚拟路径规划来掩盖用户的真实轨迹，用以保护用户真实的地理位置信息。

[0164] 作为可选实施例，地理位置信息包括：纬度信息、经度信息以及海拔信息等。

[0165] 作为可选实施例，识别处理模块进一步包括：

[0166] 解析单元，用于接收来自识别单元的通知，解析地理位置信息获取请求，获取包含的智能终端设备信息，向获取的智能终端设备信息对应的智能终端设备发送提示信息，以提示用户是否选取地理位置信息伪装策略，并在接收到用户选取地理位置信息伪装策略的信息后，通知响应单元。

[0167] 作为可选实施例，该装置可以进一步包括：

[0168] 权限获取模块，用于在获取第三方应用操作系统或智能终端设备操作系统的根权限后，通知注入模块。

[0169] 作为可选实施例，所述装置进一步包括：

[0170] 扩展模块（图中未示出），用于在所述处理所述隐私信息获取请求后，向智能终端设备发送消息提醒；和/或，

[0171] 对所述第三方应用进行安全扫描；和/或，

[0172] 卸载所述第三方应用；和/或，

[0173] 为所述第三方应用设置隐私访问权限。

[0174] 本发明实施例中，通过地理位置信息保护装置对第三方应用发起的地理位置信息获取请求进行统一的处理，使得第三方应用发起的地理位置信息获取请求无法达到智能终端设备的定位服务程序（系统定位服务程序），直接发送到地理位置信息保护装置获取保护的地理位置信息，并向第三方应用返回保护的地理位置信息。因而，避免了业务网站或服务提供商（SP，Service Provider）等第三方应用获得用户地理位置信息，导致用户地理位置信息泄漏的风险。

[0175] 在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种

编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

[0176] 在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

[0177] 类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

[0178] 本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和／或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0179] 此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0180] 本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本发明实施例的地理位置信息保护装置中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站服务器上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

[0181] 应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为

名称。

[0182] 本发明公开了 A1. 一种隐私信息保护的方法，包括：

[0183] 在隐私信息服务进程中注入隐私信息保护程序；

[0184] 所述隐私信息保护程序在识别到第三方应用发出的隐私信息获取请求后，按照预先设置的隐私信息保护策略，处理所述隐私信息获取请求。

[0185] A2. 根据 A1 所述的方法，所述伪装隐私信息包括地理位置信息，所述按照预先设置的隐私信息保护策略，处理所述隐私信息获取请求包括：

[0186] 从预先设置的地理位置信息伪装列表中，选取一伪装的地理位置信息，封装在隐私信息获取请求响应中，发送至第三方应用。

[0187] A3. 根据 A1 所述的方法，所述伪装隐私信息包括地理位置信息，所述按照预先设置的隐私信息保护策略，处理所述隐私信息获取请求包括：

[0188] 按照预先设置的基于虚拟路径规划的地理位置信息伪装算法，生成一伪装的地理位置信息，并将生成的伪装的地理位置信息封装在隐私信息获取请求响应中，发送至第三方应用。

[0189] A4. 根据 A1 所述的方法，所述伪装隐私信息包括地理位置信息，所述按照预先设置的隐私信息保护策略，处理所述隐私信息获取请求包括：

[0190] 分析隐私信息获取请求中包含的第三方应用信息，根据分析的第三方应用信息生成对应的具有时空合理性的伪装的地理位置信息，并将生成的伪装的地理位置信息封装在隐私信息获取请求响应中，发送至第三方应用。

[0191] A5. 根据 A1 所述的方法，所述注入包括在第三方应用操作系统的隐私信息服务进程中注入，或，在智能终端设备的隐私信息服务进程中注入。

[0192] A6. 根据 A5 所述的方法，所述在第三方应用操作系统的隐私信息服务进程中注入包括：

[0193] 查找第三方应用操作系统的隐私信息服务进程中已有的用于隐私信息处理的目标程序的内存变量；

[0194] 将所述已有的用于隐私信息处理的目标程序的内存变量替换为预先设置的动态目标程序的内存变量。

[0195] A7. 根据 A6 所述的方法，所述用于隐私信息处理的目标程序为第三方应用发送地址位置信息获取请求的程序。

[0196] A8. 根据 A6 所述的方法，所述将所述已有的用于隐私信息处理的目标程序的内存变量替换为预先设置的动态目标程序的内存变量包括：

[0197] 将隐私信息保护程序的内存变量代码写入动态链接库中，利用操作系统中的 windows 钩子将写入动态链接库中的隐私信息保护程序的内存变量代码映射到远程隐私信息服务进程。

[0198] A9. 根据 A6 所述的方法，所述将所述已有的用于隐私信息处理的目标程序的内存变量替换为预先设置的动态目标程序的内存变量包括：

[0199] 将隐私信息保护程序的内存变量代码写入动态链接库中，利用操作系统中的远程注入以及动态加载将写入动态链接库中的隐私信息保护程序的内存变量代码映射到远程隐私信息服务进程。

[0200] A10. 根据 A6 所述的方法，所述将所述已有的用于隐私信息处理的目标程序的内存变量替换为预先设置的动态目标程序的内存变量包括：

[0201] 利用系统进程监视器，将隐私信息保护程序的内存变量代码复制到远程隐私信息服务进程，并利用远程注入执行。

[0202] A11. 根据 A5 所述的方法，所述在智能终端设备的隐私信息服务进程中注入包括：

[0203] 查找智能终端设备操作系统的隐私信息服务进程中已有的用于隐私信息处理的系统定位服务程序的函数；

[0204] 将所述已有的用于隐私信息处理的系统定位服务程序的函数替换为预先设置的系统定位服务程序的函数。

[0205] A12. 根据 A1 所述的方法，所述在隐私信息服务进程中注入隐私信息保护程序之前，所述方法进一步包括：

[0206] 获取第三方应用操作系统或智能终端设备操作系统的根权限。

[0207] A13. 根据 A1 所述的方法，所述隐私信息保护程序在识别到第三方应用发出的隐私信息获取请求后，所述方法进一步包括：

[0208] 解析隐私信息获取请求，获取包含的智能终端设备信息，向获取的智能终端设备信息对应的智能终端设备发送提示信息，以提示用户是否选取隐私信息保护策略，并在接收到用户选取隐私信息保护策略的信息后，执行所述按照预先设置的隐私信息保护策略，处理所述隐私信息获取请求的流程。

[0209] A14. 根据 A1 所述的方法，所述按照预先设置的隐私信息保护策略，处理所述隐私信息获取请求包括：

[0210] 从预先设置的伪装隐私信息列表中，选取一伪装隐私信息，封装在隐私信息获取请求响应中，发送至第三方应用。

[0211] A15. 根据 A1 所述的方法，所述按照预先设置的隐私信息保护策略，处理所述隐私信息获取请求包括：

[0212] 按照预先设置的伪装隐私信息生成算法，生成一伪装隐私信息，并将生成的伪装隐私信息封装在隐私信息获取请求响应中，发送至第三方应用。

[0213] A16. 根据 A15 所述的方法，所述伪装隐私信息生成算法为基于虚拟路径规划的生成算法。

[0214] A17. 根据 A1 所述的方法，所述按照预先设置的隐私信息保护策略，处理所述隐私信息获取请求包括：

[0215] 分析隐私信息获取请求中包含的第三方应用信息，根据分析的第三方应用信息生成对应的具有时空合理性的伪装隐私信息，并将生成的伪装隐私信息封装在隐私信息获取请求响应中，发送至第三方应用。

[0216] A18. 根据 A1 所述的方法，所述第三方应用通过所述隐私信息服务进程发出隐私信息获取请求。

[0217] A19. 根据 A1 所述的方法，在所述处理所述隐私信息获取请求后，所述方法进一步包括：

[0218] 向智能终端设备发送消息提醒；和 / 或，

[0219] 对所述第三方应用进行安全扫描；和 / 或，

[0220] 卸载所述第三方应用；和 / 或，

[0221] 为所述第三方应用设置隐私访问权限。

[0222] A20. 一种在申请了地理位置信息服务权限环境下的隐私信息保护方法，执行如权利要求 1 至 19 任一项所述的方法。

[0223] A21. 一种隐私信息保护装置，该装置包括：注入模块以及识别处理模块，其中，

[0224] 注入模块，用于在隐私信息服务进程中注入预先设置的隐私信息保护程序；

[0225] 识别处理模块，用于在所述隐私信息保护程序识别到第三方应用发出的隐私信息获取请求后，按照预先设置的隐私信息保护策略，处理所述隐私信息获取请求。

[0226] A22. 根据 A21 所述的装置，所述注入模块用于在第三方应用操作系统的隐私信息服务进程中预先注入动态目标程序，通过动态注入的目标程序的用于调用系统隐私信息服务的变量或方法，替换第三方应用操作系统的目标程序的用于调用系统隐私信息服务的变量或方法。

[0227] A23. 根据 A21 所述的装置，所述注入模块用于在智能终端设备操作系统的隐私信息服务进程中预先注入系统定位服务程序，替换智能终端设备操作系统定位服务内的函数为注入的系统定位服务程序对应的函数。

[0228] A24. 根据 A21 所述的装置，所述注入模块包括：第一查找单元以及第一替换单元，其中，

[0229] 第一查找单元，用于查找第三方应用操作系统的隐私信息服务进程中已有的用于隐私信息处理的目标程序的内存变量；

[0230] 第一替换单元，用于将所述已有的用于隐私信息处理的目标程序的内存变量替换为预先设置的动态目标程序的内存变量。

[0231] A25. 根据 A21 所述的装置，所述注入模块包括：第二查找单元以及第二替换单元，其中，

[0232] 第二查找单元，用于查找智能终端设备操作系统的隐私信息服务进程中已有的用于隐私信息处理的系统定位服务程序的函数；

[0233] 第二替换单元，用于将所述已有的用于隐私信息处理的系统定位服务程序的函数替换为预先设置的系统定位服务程序的函数。

[0234] A26. 根据 A21 所述的装置，所述识别处理模块包括：识别单元以及处理单元，其中，

[0235] 识别单元，用于在启动的隐私信息保护程序识别到第三方应用发出的隐私信息获取请求后，通知响应单元；

[0236] 处理单元，用于接收通知，按照预先设置的隐私信息保护策略，处理所述隐私信息获取请求。

[0237] A27. 根据 A26 所述的装置，所述识别处理模块进一步包括：

[0238] 解析单元，用于接收来自识别单元的通知，解析隐私信息获取请求，获取包含的智能终端设备信息，向获取的智能终端设备信息对应的智能终端设备发送提示信息，以提示用户是否选取隐私信息保护策略，并在接收到用户选取隐私信息保护策略的信息后，通知响应单元。

[0239] A28. 根据 A21 所述的装置，所述装置进一步包括：

[0240] 权限获取模块，用于在获取第三方应用操作系统或智能终端设备操作系统的根权限后，通知注入模块。

[0241] A29. 根据 A21 所述的装置，所述装置进一步包括：

[0242] 扩展模块，用于在所述处理所述隐私信息获取请求后，向智能终端设备发送消息提醒；和 / 或，

[0243] 对所述第三方应用进行安全扫描；和 / 或，

[0244] 卸载所述第三方应用；和 / 或，

[0245] 为所述第三方应用设置隐私访问权限。

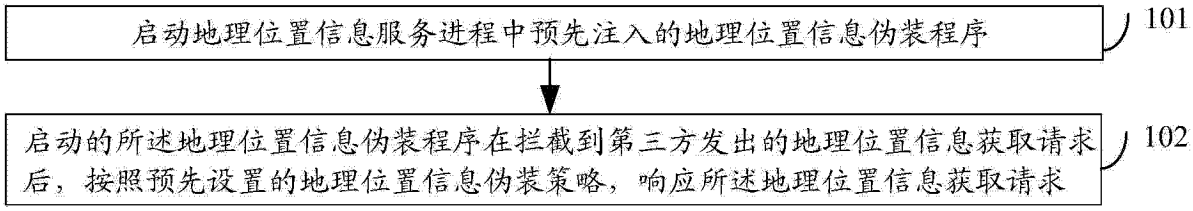

启动地理位置信息服务进程中预先注入的地理位置信息伪装程序
101
启动的所述地理位置信息伪装程序在拦截到第三方发出的地理位置信息获取请求后，按照预先设置的地理位置信息伪装策略，响应所述地理位置信息获取请求
102

图 1

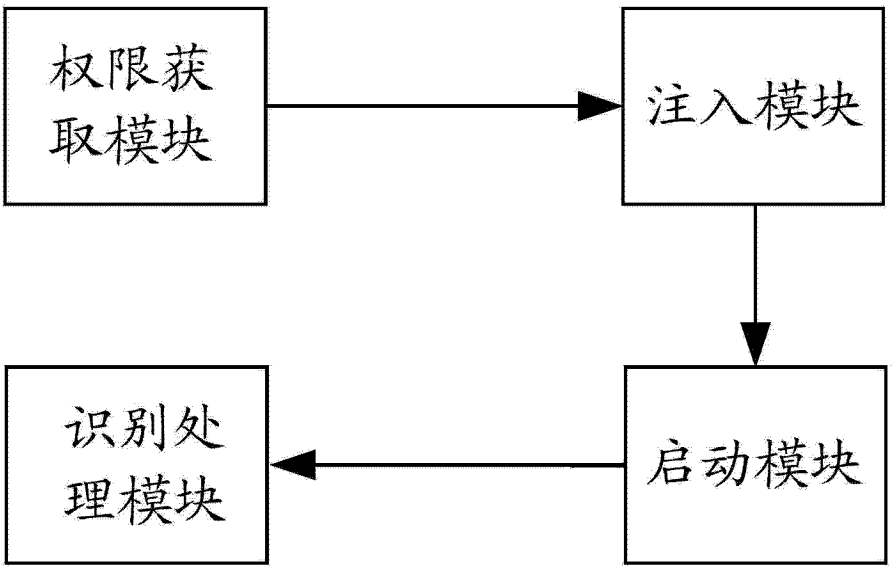

权限获取模块
注入模块
识别处理模块
启动模块

图 2