(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 102799812 A
(43)申请公布日 2012.11.28

(21)申请号 201210218429.9

(22)申请日 2012.06.28

(71)申请人 腾讯科技(深圳)有限公司
地址 518000 广东省深圳市福田区赛格科技园 2 栋东 403 室

(72)发明人 邓欣 刘庆海

(74)专利代理机构 北京三高永信知识产权代理有限责任公司 11138
代理人 罗振安

(51)Int.Cl.
G06F 21/00(2006.01)

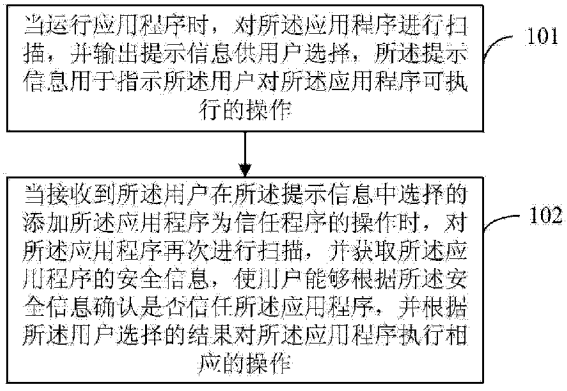
权利要求书 2 页 说明书 9 页 附图 2 页

(54)发明名称

应用程序的处理方法和装置

(57)摘要

本发明公开了一种应用程序的处理方法和装置，属于通信技术领域。所述方法包括：当接收到所述用户在所述提示信息中选择的删除所述应用程序的操作时，将所述应用程序放到恢复区；当接收到还原所述恢复区中的所述应用程序的指示时，对所述应用程序再次进行扫描，并获取所述应用程序的安全信息，使用户能够根据所述安全信息确认是否信任所述应用程序，并根据所述用户选择的结果对所述应用程序执行相应的操作。



CN 102799812 A

1. 一种应用程序的处理方法，其特征在于，所述方法包括：

当运行应用程序时，对所述应用程序进行扫描，并输出提示信息供用户选择，所述提示信息用于指示所述用户对所述应用程序可执行的操作；

当接收到所述用户在所述提示信息中选择的添加所述应用程序为信任程序的操作时，对所述应用程序再次进行扫描，并获取所述应用程序的安全信息，使用户能够根据所述安全信息确认是否信任所述应用程序，并根据所述用户选择的结果对所述应用程序执行相应的操作。

2. 根据权利要求 1 所述的方法，其特征在于，所述对所述应用程序再次进行扫描，并获取所述应用程序的安全信息，包括：

向服务器端查询所述应用程序的安全信息；

接收并输出所述服务器端返回的所述应用程序的安全信息。

3. 根据权利要求 2 所述的方法，其特征在于，所述向服务器端查询所述应用程序的安全信息，包括：

获取所述应用程序的 MD5 值；

将所述 MD5 值发送给服务器端，使所述服务器端根据所述 MD5 值查询所述应用程序的安全信息。

4. 根据权利要求 2 所述的方法，其特征在于，所述向服务器端查询所述应用程序的安全信息之前，还包括：

判断添加所述应用程序为信任程序的操作是否为用户发起的，如果是，则执行向服务器端查询所述应用程序的安全信息的操作，否则，拒绝执行对所述应用程序的操作。

5. 根据权利要求 1 所述的方法，其特征在于，所述安全信息包括：应用程序的类型、应用程序的行为描述和应用程序的危害等级中的一个或多个。

6. 根据权利要求 1 所述的方法，其特征在于，所述方法还包括：

当接收到所述用户在所述提示信息中选择的删除所述应用程序的操作时，将所述应用程序放到恢复区；

当接收到还原所述恢复区中的所述应用程序的指示时，对所述应用程序再次进行扫描，并获取所述应用程序的安全信息，使用户能够根据所述安全信息确认是否信任所述应用程序，并根据所述用户选择的结果对所述应用程序执行相应的操作。

7. 根据权利要求 1 或 6 所述的方法，其特征在于，所述根据所述用户选择的结果对所述应用程序执行相应的操作，包括：

当所述用户的选择结果为信任所述应用程序时，将所述应用程序添加到预设位置；

当所述用户的选择结果为拒绝信任所述应用程序时，删除所述应用程序。

8. 一种应用程序的处理装置，其特征在于，所述装置包括：

一次扫描模块，用于当运行应用程序时，对所述应用程序进行扫描，并输出提示信息供用户选择，所述提示信息用于指示所述用户对所述应用程序可执行的操作；

二次扫描模块，用于当接收到所述用户在所述提示信息中选择的添加所述应用程序为信任程序的结果时，对所述应用程序再次进行扫描，并获取所述应用程序的安全信息，使用户能够根据所述安全信息确认是否信任所述应用程序，并根据所述用户选择的结果对所述应用程序执行相应的操作。

9. 根据权利要求 8 所述的装置，其特征在于，所述二次扫描模块，包括 ：

查询单元，用于向服务器端查询所述应用程序的安全信息 ；

接收单元，用于接收并输出所述服务器端返回的所述应用程序的安全信息。

10. 根据权利要求 9 所述的装置，其特征在于，所述查询单元，包括 ：

获取子单元，用于获取所述应用程序的 MD5 值 ；

发送子单元，用于将所述 MD5 值发送给服务器端，使所述服务器端根据所述 MD5 值查询所述应用程序的安全信息。

11. 根据权利要求 9 所述的装置，其特征在于，所述二次扫描模块还包括 ：

判断单元，用于判断添加所述应用程序为信任程序的操作是否为用户发起的，如果是，则所述二次扫描模块执行向服务器端查询所述应用程序的安全信息的操作，否则，所述二次扫描模块拒绝执行对所述应用程序的操作。

12. 根据权利要求 8 所述的装置，其特征在于，所述安全信息包括 ：应用程序的类型、应用程序的行为描述和应用程序的危害等级中的一个或多个。

13. 根据权利要求 8 所述的装置，其特征在于，所述装置还包括 ：

添加模块，用于当接收到所述用户在所述提示信息中选择的删除所述应用程序的操作时，将所述应用程序放到恢复区 ；

所述二次扫描模块还用于当接收到还原所述恢复区中的所述应用程序的指示时，对所述应用程序再次进行扫描，并获取所述应用程序的安全信息，使用户能够根据所述安全信息确认是否信任所述应用程序，并根据所述用户选择的结果对所述应用程序执行相应的操作。

14. 根据权利要求 8 或 13 所述的装置，其特征在于，所述二次扫描模块，包括 ：

第一执行单元，用于当所述用户的选择结果为信任所述应用程序时，将所述应用程序添加到预设位置 ；

第二执行单元，用于当所述用户的选择结果为拒绝信任所述应用程序时，删除所述应用程序。

应用程序的处理方法和装置

技术领域

[0001] 本发明涉及通信技术领域，特别涉及一种应用程序的处理方法和装置。

背景技术

[0002] 由于互联网的方便快捷，目前许多用户都会通过网络下载或是传输应用程序，这就让恶意程序有了可乘之机。恶意程序可能会被携带在用户下载或是需要传输的应用程序中，当用户运行该应用程序时，恶意程序就会被激活，从而被植入到用户的客户端中，影响用户客户端的使用。

[0003] 现有技术中，为了保护客户端不被恶意程序侵扰，为客户端提供了多种可选择的客户端安全软件，当一个程序运行时，客户端安全软件先扫描该程序，如果发现该程序可能存在恶意行为，则在客户端界面上输出：“立即删除”、“暂不处理”、“添加信任”的选项给用户选择，并建议该用户删除该程序，以免该恶意程序对电脑造成损坏。但是如果用户选择“添加信任”，则安全软件将该程序直接添加到本地的可信任区域。

[0004] 在实现本发明的过程中，发明人发现现有技术至少存在以下问题：

[0005] 恶意程序在与安全软件的对抗中，技术也越来越成熟，危害也越来越大，现有的安全软件在对程序进行扫描后，如果发现该程序为恶意程序，则会给用户提示一些关于该恶意程序的代码，但是对于普通用户并不能直接识别这些代码的危害，一般用户都会直接将该程序添加为可信任程序，继续运行该程序，这就让一些恶意程序有了可乘之机，所以安全软件将程序直接添加到可信任区域时会存在一定的风险，不能有效的避免恶意程序通过该方式的植入，因此降低了客户端的安全性能。

发明内容

[0006] 为了提高客户端的安全性能，本发明实施例提供了一种应用程序的处理方法和装置。所述技术方案如下：

[0007] 一方面，提供了一种应用程序的处理方法，所述方法包括：

[0008] 当运行应用程序时，对所述应用程序进行扫描，并输出提示信息供用户选择，所述提示信息用于指示所述用户对所述应用程序可执行的操作；

[0009] 当接收到所述用户在所述提示信息中选择的添加所述应用程序为信任程序的操作时，对所述应用程序再次进行扫描，并获取所述应用程序的安全信息，使用户能够根据所述安全信息确认是否信任所述应用程序，并根据所述用户选择的结果对所述应用程序执行相应的操作。

[0010] 所述对所述应用程序再次进行扫描，并获取所述应用程序的安全信息，包括：

[0011] 向服务器端查询所述应用程序的安全信息；

[0012] 接收并输出所述服务器端返回的所述应用程序的安全信息。

[0013] 所述向服务器端查询所述应用程序的安全信息，包括：

[0014] 获取所述应用程序的 MD5 值；

[0015] 将所述 MD5 值发送给服务器端，使所述服务器端根据所述 MD5 值查询所述应用程序的安全信息。

[0016] 所述向服务器端查询所述应用程序的安全信息之前，还包括：

[0017] 判断添加所述应用程序为信任程序的操作是否为用户发起的，如果是，则执行向服务器端查询所述应用程序的安全信息的操作，否则，拒绝执行对所述应用程序的操作。

[0018] 所述安全信息包括：应用程序的类型、应用程序的行为描述和应用程序的危害等级中的一个或多个。

[0019] 所述方法还包括：

[0020] 当接收到所述用户在所述提示信息中选择的删除所述应用程序的操作时，将所述应用程序放到恢复区；

[0021] 当接收到还原所述恢复区中的所述应用程序的指示时，对所述应用程序再次进行扫描，并获取所述应用程序的安全信息，使用户能够根据所述安全信息确认是否信任所述应用程序，并根据所述用户选择的结果对所述应用程序执行相应的操作。

[0022] 所述根据所述用户选择的结果对所述应用程序执行相应的操作，包括：

[0023] 当所述用户的选择结果为信任所述应用程序时，将所述应用程序添加到预设位置；

[0024] 当所述用户的选择结果为拒绝信任所述应用程序时，删除所述应用程序。

[0025] 另一方面，提供了一种应用程序的处理装置，所述装置包括：

[0026] 一次扫描模块，用于当运行应用程序时，对所述应用程序进行扫描，并输出提示信息供用户选择，所述提示信息用于指示所述用户对所述应用程序可执行的操作；

[0027] 二次扫描模块，用于当接收到所述用户在所述提示信息中选择的添加所述应用程序为信任程序的结果时，对所述应用程序再次进行扫描，并获取所述应用程序的安全信息，使用户能够根据所述安全信息确认是否信任所述应用程序，并根据所述用户选择的结果对所述应用程序执行相应的操作。

[0028] 所述二次扫描模块，包括：

[0029] 查询单元，用于向服务器端查询所述应用程序的安全信息；

[0030] 接收单元，用于接收并输出所述服务器端返回的所述应用程序的安全信息。

[0031] 所述查询单元，包括：

[0032] 获取子单元，用于获取所述应用程序的 MD5 值；

[0033] 发送子单元，用于将所述 MD5 值发送给服务器端，使所述服务器端根据所述 MD5 值查询所述应用程序的安全信息。

[0034] 所述二次扫描模块还包括：

[0035] 判断单元，用于判断添加所述应用程序为信任程序的操作是否为用户发起的，如果是，则所述二次扫描模块执行向服务器端查询所述应用程序的安全信息的操作，否则，所述二次扫描模块拒绝执行对所述应用程序的操作。

[0036] 所述安全信息包括：应用程序的类型、应用程序的行为描述和应用程序的危害等级中的一个或多个。

[0037] 所述装置还包括：

[0038] 添加模块，用于当接收到所述用户在所述提示信息中选择的删除所述应用程序的

操作时，将所述应用程序放到恢复区；

[0039] 所述二次扫描模块还用于当接收到还原所述恢复区中的所述应用程序的指示时，对所述应用程序再次进行扫描，并获取所述应用程序的安全信息，使用户能够根据所述安全信息确认是否信任所述应用程序，并根据所述用户选择的结果对所述应用程序执行相应的操作。

[0040] 所述二次扫描模块，包括：

[0041] 第一执行单元，用于当所述用户的选择结果为信任所述应用程序时，将所述应用程序添加到预设位置；

[0042] 第二执行单元，用于当所述用户的选择结果为拒绝信任所述应用程序时，删除所述应用程序。

[0043] 本发明实施例提供的技术方案带来的有益效果是：当运行应用程序时，对所述应用程序进行扫描，并输出提示信息供用户选择，所述提示信息用于指示所述用户对所述应用程序可执行的操作；当接收到所述用户在所述提示信息中选择的添加所述应用程序为信任程序的操作时，对所述应用程序再次进行扫描，并获取所述应用程序的安全信息，使用户能够根据所述安全信息确认是否信任所述应用程序，并根据所述用户选择的结果对所述应用程序执行相应的操作。其中通过对需要添加的信任程序进行二次扫描进一步提高客户端的安全性能。

附图说明

[0044] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0045] 图 1 是本发明实施例 1 提供的一种应用程序的处理方法流程图；

[0046] 图 2 是本发明实施例 2 提供的一种应用程序的处理方法流程图；

[0047] 图 3 是本发明实施例 3 提供的一种应用程序的处理方法流程图；

[0048] 图 4 是本发明实施例 4 提供的一种应用程序的处理装置结构示意图；

[0049] 图 5 是本发明实施例 4 提供的另一种应用程序的处理装置结构示意图。

具体实施方式

[0050] 为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明实施方式作进一步地详细描述。

[0051] 实施例 1

[0052] 参见图 1，本实施例中提供了一种应用程序的处理方法，所述方法包括：

[0053] 101、当运行应用程序时，对所述应用程序进行扫描，并输出提示信息供用户选择，所述提示信息用于指示所述用户对所述应用程序可执行的操作；

[0054] 102、当接收到所述用户在所述提示信息中选择的添加所述应用程序为信任程序的操作时，对所述应用程序再次进行扫描，并获取所述应用程序的安全信息，使用户能够根据所述安全信息确认是否信任所述应用程序，并根据所述用户选择的结果对所述应用程序

执行相应的操作。

[0055] 其中，所述对所述应用程序再次进行扫描，并获取所述应用程序的安全信息，包括：

[0056] 向服务器端查询所述应用程序的安全信息；

[0057] 接收并输出所述服务器端返回的所述应用程序的安全信息。

[0058] 其中，所述向服务器端查询所述应用程序的安全信息，包括：

[0059] 获取所述应用程序的 MD5 值；

[0060] 将所述 MD5 值发送给服务器端，使所述服务器端根据所述 MD5 值查询所述应用程序的安全信息。

[0061] 可选地，所述向服务器端查询所述应用程序的安全信息之前，还包括：

[0062] 判断添加所述应用程序为信任程序的操作是否为用户发起的，如果是，则执行向服务器端查询所述应用程序的安全信息的操作，否则，拒绝执行对所述应用程序的操作。

[0063] 可选地，所述安全信息包括：应用程序的类型、应用程序的行为描述和应用程序的危害等级中的一个或多个。

[0064] 可选地，所述方法还包括：

[0065] 当接收到所述用户在所述提示信息中选择的删除所述应用程序的操作时，将所述应用程序放到恢复区；

[0066] 当接收到还原所述恢复区中的所述应用程序的指示时，对所述应用程序再次进行扫描，并获取所述应用程序的安全信息，使用户能够根据所述安全信息确认是否信任所述应用程序，并根据所述用户选择的结果对所述应用程序执行相应的操作。

[0067] 其中，所述根据所述用户选择的结果对所述应用程序执行相应的操作，包括：

[0068] 当所述用户的选择结果为信任所述应用程序时，将所述应用程序添加到预设位置；

[0069] 当所述用户的选择结果为拒绝信任所述应用程序时，删除所述应用程序。

[0070] 本实施例的有益效果是：当运行应用程序时，对所述应用程序进行扫描，并输出提示信息供用户选择，所述提示信息用于指示所述用户对所述应用程序可执行的操作；当接收到所述用户在所述提示信息中选择的添加所述应用程序为信任程序的操作时，对所述应用程序再次进行扫描，并获取所述应用程序的安全信息，使用户能够根据所述安全信息确认是否信任所述应用程序，并根据所述用户选择的结果对所述应用程序执行相应的操作。其中通过对需要添加的信任程序进行二次扫描进一步提高客户端的安全性能。

[0071] 实施例 2

[0072] 本实施例中提供了一种应用程序的处理方法，本实施例中的客户端安装了预设的安全软件，当客户端中运行应用程序时，安全软件会对该应用程序扫描，以确认该应用程序是否安全，从而实现对客户端的保护。

[0073] 本实施例中，在客户端运行应用程序时，安全软件会对应用程序进行扫描，如果发现该程序可能存在恶意行为，则在客户端界面上输出提示信息，用于指示用户对所述应用程序可执行的操作，如输出“立即删除”、“暂不处理”、“添加信任”的选项给用户选择，当用户选择“添加信任”时，不直接将应用程序添加到信任区域，而是对应用程序进行二次扫描，输出应用程序的安全信息，使用户能够根据安全信息对应用程序做直接的判断该程序是否

存在潜在的风险，是否能够将该程序添加为信任程序。

[0074] 本实施例中在后台服务器中预设新的数据库，该数据库用于存储应用程序的安全信息。其中，数据库中的安全信息可以由人工分析得来，也可以由计算机统计得来，对此本实施例不做具体限定。具体方法可以是，对被添加为信任的文件或是被恢复的文件进行统计，选取其中被信任或是恢复次数多的文件，通过人为或是专门的病毒分析程序分析这些文件，并给出这些文件的安全信息。其中安全信息包括但不限于：应用程序的类型、应用程序的行为描述和应用程序的危害等级中的一个或多个。应用程序的类型包括：外挂、后门程序、监控程序、盗号木马等；应用程序的行为描述是指这个应用程序可能会执行的操作，例如，如果应用程序是外挂程序，则要具体描述该应用程序会不会盗号，如果应用程序是网游盗号程序，则需要描述该应用程序盗取的是哪一或是哪几款网游帐号和密码等；可以根据应用程序的类型和应用程序的行为定义应用程序的危害等级，例如危害越大，等级越高，对此本实施例不做具体限定。值得说明的是，服务器端的数据库中的数据也会不断的更新，对此本实施例不做具体限定。本实施例中的预设操作是指调用安全软件信任接口的操作，包括用户选择的添加信任的操作或是将程序从恢复区恢复的操作等，对此本实施例不做具体限定。

[0075] 参见图 2，具体的本实施例中提供的应用程序的处理方法包括：

[0076] 201、当运行应用程序时，对所述应用程序进行扫描，并输出提示信息供用户选择，所述提示信息用于指示所述用户对所述应用程序可执行的操作。

[0077] 该步骤与现有技术中的扫描步骤类似，对此本实施例不再赘述。

[0078] 202、当接收到所述用户在所述提示信息中选择的添加所述应用程序为信任程序的操作时，对所述应用程序再次进行扫描，并获取所述应用程序的安全信息，使用户能够根据所述安全信息确认是否信任所述应用程序。

[0079] 本步骤中，客户端运行应用程序时，安全软件对该应用程序先进行扫描，输出“添加信任”、“阻止程序运行”或“删除文件”的选项，如果输出的是“添加信任”的选项，当用户选择了该选项后，客户端并不直接将该应用程序添加到信任区域，而是对该应用程序进行二次扫描，查询该应用程序的安全信息。其中，对所述应用程序再次进行扫描，并获取所述应用程序的安全信息，包括：向服务器端查询所述应用程序的安全信息；接收并输出所述服务器端返回的所述应用程序的安全信息。

[0080] 本实施例中，为了避免添加信任的操作是恶意程序调用安全软件的信任接口触发的操作，可选地，在向服务器端查询所述应用程序的安全信息之前，还包括：判断添加所述应用程序为信任程序的操作是否为用户发起的，如果是，则执行向服务器端查询所述应用程序的安全信息的操作，否则，拒绝执行对所述应用程序的操作。这样，如果预设操作是恶意程序发起的，就能够及时阻止该程序的运行。本实施例中预设操作是指添加应用程序为信任程序的操作。具体的判断预设操作是否为用户发起的包括：判断发出此操作的进程是否安全软件自身进程，如果是，则放过此操作，对该应用程序进行二次云查，如果不是，则默认禁止该操作；或是，在安全软件中预设一个自定义的消息，当用户点击信任时，安全软件对这个消息进行检查，如果有收到这个消息，那么说明该添加操作是用户行为，相反，则是恶意软件的行为。其中判断预设操作是否为用户发起的还可以有其它方法，对此本实施例不做具体限定。

[0081] 本步骤中，向服务器端查询所述应用程序的安全信息，包括：获取所述应用程序的MD5值；将所述MD5值发送给服务器端，使所述服务器端根据所述MD5值查询所述应用程序的安全信息。其中，对应用程序扫描，获取应用程序的MD5值的方法与现有技术类似，对此本实施例不再赘述。

[0082] 本步骤中，由于服务器端预先存储了各种应用程序的安全信息，所以当客户端将MD5值发送给服务器端时，服务器端根据该MD5值查找与其对应的安全信息，并返回给客户端。

[0083] 值得说明的是，本实施例中服务器端的数据库中存储了应用程序的MD5值与其安全信息的对应关系，所以客户端可以根据应用程序的MD5值获取到安全信息，当数据库中存储的是应用程序的其它相关信息与其安全信息的对应关系时，客户端也可以根据应用程序的其它相关信息获取到安全信息，例如，数据库中存储了应用程序的名称与其安全信息的对应关系。对此本实施例不做具体限定。

[0084] 本实施例中，如果服务器端未查询到应用程序的安全信息，则返回没有查询结果的信息给客户端，具体该信息以何种形式返回，对此本实施例不做具体限定。

[0085] 本实施例中，如果一次扫描后输出的是“阻止程序运行”或“删除文件”的选项时，执行步骤与现有技术类似，对此本实施例不再赘述。

[0086] 本步骤中，客户端接收服务器端返回的查询结果，当返回的查询结果为应用程序的安全信息时，将该安全信息输出，其中安全信息包括但不限于：应用程序的类型、应用程序的行为描述和应用程序的危害等级中的一个或多个。客户端输出该应用程序的安全信息后，用户可以直观的看到该应用程序的具体功能和行为，以及会造成哪些危害，用户可以根据该安全信息进一步判断是否存在潜在的风险，是否要将其添加为信任程序。

[0087] 203、当所述用户的选择结果为信任所述应用程序时，将所述应用程序添加到预设位置。

[0088] 本步骤中，在用户了解了该应用程序的安全信息后，如果用户认为该应用程序可以信任，将其添加为信任程序，则安全软件将其添加到预设的位置，其中预设的位置是指可信任区域。本实施例中，对终端的使用区域进行划分，分为可信任区域和恢复区域，如果文件处在可信任区域，则表明该文件是可信任的，用户可以放心使用该文件，当文件处在恢复区域时，则表明该文件存在一定的风险，用户需要谨慎使用该文件。

[0089] 其中将应用程序添加到可信任区域的过程与现有技术类似，对此本实施例不再赘述。

[0090] 204、当所述用户的选择结果为拒绝信任所述应用程序时，删除所述应用程序。

[0091] 本步骤中，在用户分析了应用程序的安全信息后，如果认为该应用程序存在一定的风险，则可以选择拒绝信任该应用程序，如果用户选择拒绝添加该应用程序为信任程序，则安全软件可以直接将该应用程序删除。

[0092] 其中可选地，在删除该应用程序之前还可以输出文件删除提示框，该提示框用于告知该应用程序将被删除，以免将用户想要保留的应用程序直接删除后，影响用户的体验感。

[0093] 本实施例的有益效果是：当运行应用程序时，对所述应用程序进行扫描，并输出提示信息供用户选择，所述提示信息用于指示所述用户对所述应用程序可执行的操作；当接

收到所述用户在所述提示信息中选择的添加所述应用程序为信任程序的操作时，对所述应用程序再次进行扫描，并获取所述应用程序的安全信息，使用户能够根据所述安全信息确认是否信任所述应用程序，并根据所述用户选择的结果对所述应用程序执行相应的操作。其中通过对需要添加的信任程序进行二次扫描进一步提高客户端的安全性能。且在对应用程序进行查询操作之前先判断对应用程序的操作是否为用户发起的，如果不是用户发起的，则拒绝执行任何操作，从而进一步阻止了恶意程序调用安全软件的信任接口，提高了系统的安全性能。

[0094] 实施例 3

[0095] 本实施例中提供了一种应用程序的处理方法，本实施例中当运行应用程序时，对实施例 2 中的应用程序进行扫描，当接收到所述用户在提示信息中选择的删除该应用程序的操作时，将所述应用程序放到恢复区，当用户想要还原文件恢复区的应用程序时，客户端不直接将文件进行还原，而是对应用程序进行二次扫描，输出应用程序的安全信息，使用户能够根据安全信息对应用程序做直接的判断该程序是否存在潜在的风险，是否能够还原该程序。

[0096] 参见图 3，具体的本实施例中提供的应用程序的处理方法包括 ：

[0097] 301、当接收到还原所述恢复区中的所述应用程序的指示时，对所述应用程序再次进行扫描，并获取所述应用程序的安全信息，使用户能够根据所述安全信息确认是否信任所述应用程序。

[0098] 本步骤中，应用程序已经被放到恢复区，用户需要将恢复区的应用程序还原到原始位置，则对所述应用程序再次进行扫描，并获取所述应用程序的安全信息，具体的扫描过程与实施例 2 中的查询过程类似，对此本实施例不再赘述。其中，将恢复区的应用程序恢复到原始位置的操作也可能是恶意程序调用安全软件的信任接口触发的操作。所以本实施例中可选地，在向服务器端查询所述应用程序的安全信息之前，还包括 ：判断还原所述恢复区中的所述应用程序的指示是否为用户发起的，如果是，则执行向服务器端查询所述应用程序的安全信息的操作，否则，拒绝执行对所述应用程序的操作。这样，如果预设操作是恶意程序发起的，就能够及时阻止该程序的运行。其中预设操作是指恢复应用程序的操作。其中如何判断该预设操作是用户发起的方法与实施例 2 中的方法类似，对此本实施例不再赘述。

[0099] 302、当所述用户的选择结果为信任所述应用程序时，将所述应用程序添加到预设位置。

[0100] 本步骤中，在用户了解了该应用程序的安全信息后，如果用户认为该应用程序可以信任，将其从恢复区中还原，则安全软件将其还原到预设的位置，其中预设的位置是指文件存储的原始位置，即文件被删除之前存放在存储介质上的位置。

[0101] 303、当所述用户的选择结果为拒绝信任所述应用程序时，删除所述应用程序。

[0102] 本步骤与实施例 2 中的步骤 204 类似，对此本实施例不再赘述。

[0103] 本实施例的有益效果是 ：当接收到所述用户在所述提示信息中选择的删除所述应用程序的操作时，将所述应用程序放到恢复区 ；当接收到还原所述恢复区中的所述应用程序的指示时，对所述应用程序再次进行扫描，并获取所述应用程序的安全信息，使用户能够根据所述安全信息确认是否信任所述应用程序，并根据所述用户选择的结果对所述应用程

序执行相应的操作。其中通过对需要恢复的应用程序进行二次扫描进一步提高客户端的安全性能。且在对应用程序进行查询操作之前先判断对应用程序的操作是否为用户发起的，如果不是用户发起的，则拒绝执行任何操作，从而进一步阻止了恶意程序调用安全软件的信任接口，提高了系统的安全性能。

[0104] 实施例 4

[0105] 参见图 4，本实施例中提供了一种应用程序的处理装置，所述装置包括：一次扫描模块 401 和二次扫描模块 402。

[0106] 一次扫描模块 401，用于当运行应用程序时，对所述应用程序进行扫描，并输出提示信息供用户选择，所述提示信息用于指示所述用户对所述应用程序可执行的操作；

[0107] 二次扫描模块 402，用于当接收到所述用户在所述提示信息中选择的添加所述应用程序为信任程序的结果时，对所述应用程序再次进行扫描，并获取所述应用程序的安全信息，使用户能够根据所述安全信息确认是否信任所述应用程序，并根据所述用户选择的结果对所述应用程序执行相应的操作。

[0108] 其中，参见图 5，所述二次扫描模块 402，包括：

[0109] 查询单元 402a，用于向服务器端查询所述应用程序的安全信息；

[0110] 接收单元 402b，用于接收并输出所述服务器端返回的所述应用程序的安全信息。

[0111] 其中，所述查询单元 402a，包括：

[0112] 获取子单元，用于获取所述应用程序的 MD5 值；

[0113] 发送子单元，用于将所述 MD5 值发送给服务器端，使所述服务器端根据所述 MD5 值查询所述应用程序的安全信息。

[0114] 可选地，所述二次扫描模块 402 还包括：

[0115] 判断单元 402c，用于判断添加所述应用程序为信任程序的操作是否为用户发起的，如果是，则所述二次扫描模块执行向服务器端查询所述应用程序的安全信息的操作，否则，所述二次扫描模块拒绝执行对所述应用程序的操作。

[0116] 可选地，所述安全信息包括：应用程序的类型、应用程序的行为描述和应用程序的危害等级中的一个或多个。

[0117] 可选地，参加图 5，所述装置还包括：

[0118] 添加模块 403，用于当接收到所述用户在所述提示信息中选择的删除所述应用程序的操作时，将所述应用程序放到恢复区；

[0119] 所述二次扫描模块 402 还用于当接收到还原所述恢复区中的所述应用程序的指示时，对所述应用程序再次进行扫描，并获取所述应用程序的安全信息，使用户能够根据所述安全信息确认是否信任所述应用程序，并根据所述用户选择的结果对所述应用程序执行相应的操作。

[0120] 参加图 5，所述二次扫描模块 402，包括：

[0121] 第一执行单元 402d，用于当所述用户的选择结果为信任所述应用程序时，将所述应用程序添加到预设位置；

[0122] 第二执行单元 402e，用于当所述用户的选择结果为拒绝信任所述应用程序时，删除所述应用程序。

[0123] 本实施例的有益效果是：当运行应用程序时，对所述应用程序进行扫描，并输出提

示信息供用户选择，所述提示信息用于指示所述用户对所述应用程序可执行的操作；当接收到所述用户在所述提示信息中选择的添加所述应用程序为信任程序的操作时，对所述应用程序再次进行扫描，并获取所述应用程序的安全信息，使用户能够根据所述安全信息确认是否信任所述应用程序，并根据所述用户选择的结果对所述应用程序执行相应的操作。其中通过对需要添加的信任程序进行二次扫描进一步提高客户端的安全性能。

[0124] 需要说明的是：上述实施例提供的应用程序的处理装置实施例中，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将设备的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。另外，上述实施例提供的应用程序的处理装置与应用程序的处理方法实施例属于同一构思，其具体实现过程详见方法实施例，这里不再赘述。

[0125] 上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[0126] 本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件来完成，也可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等。

[0127] 以上所述仅为本发明的较佳实施例，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

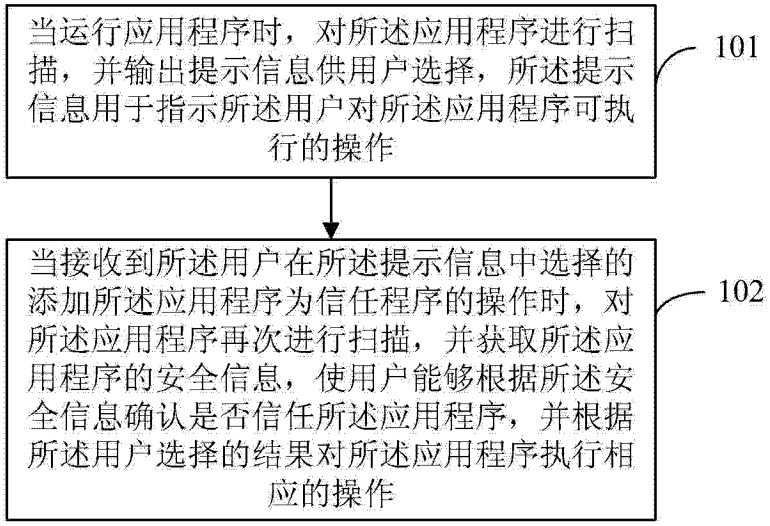

当运行应用程序时，对所述应用程序进行扫描，并输出提示信息供用户选择，所述提示信息用于指示所述用户对所述应用程序可执行的操作
101
当接收到所述用户在所述提示信息中选择的添加所述应用程序为信任程序的操作时，对所述应用程序再次进行扫描，并获取所述应用程序的安全信息，使用户能够根据所述安全信息确认是否信任所述应用程序，并根据所述用户选择的结果对所述应用程序执行相应的操作
102

图 1

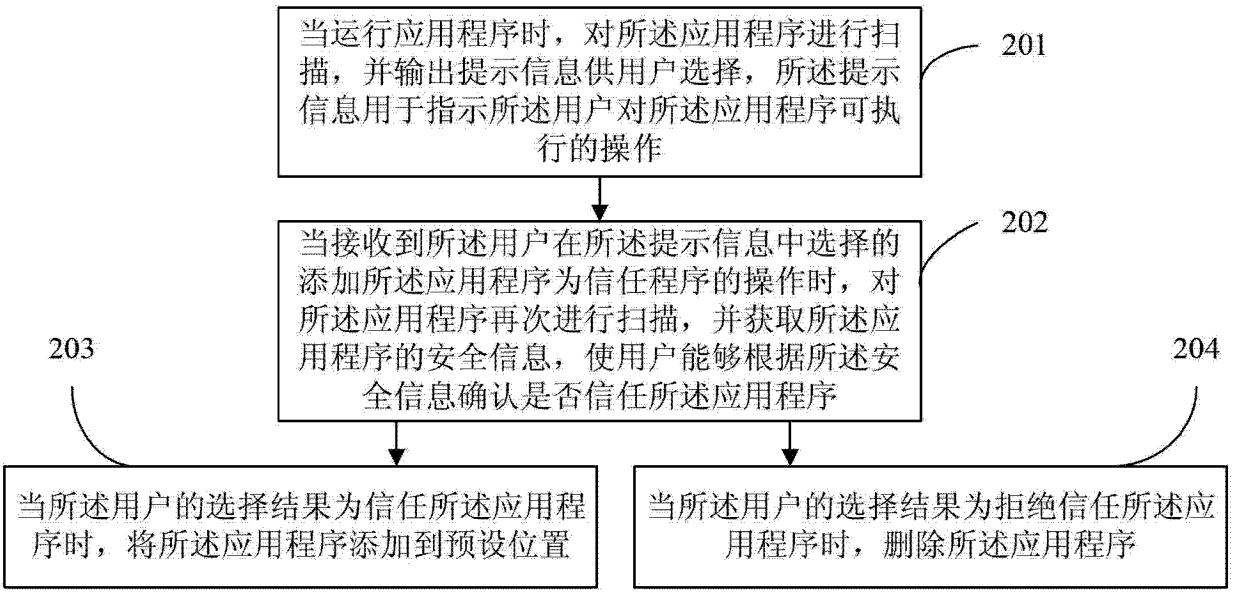

当运行应用程序时，对所述应用程序进行扫描，并输出提示信息供用户选择，所述提示信息用于指示所述用户对所述应用程序可执行的操作
201
当接收到所述用户在所述提示信息中选择的添加所述应用程序为信任程序的操作时，对所述应用程序再次进行扫描，并获取所述应用程序的安全信息，使用户能够根据所述安全信息确认是否信任所述应用程序
202
203
204
当所述用户的选择结果为信任所述应用程序时，将所述应用程序添加到预设位置
当所述用户的选择结果为拒绝信任所述应用程序时，删除所述应用程序

图 2

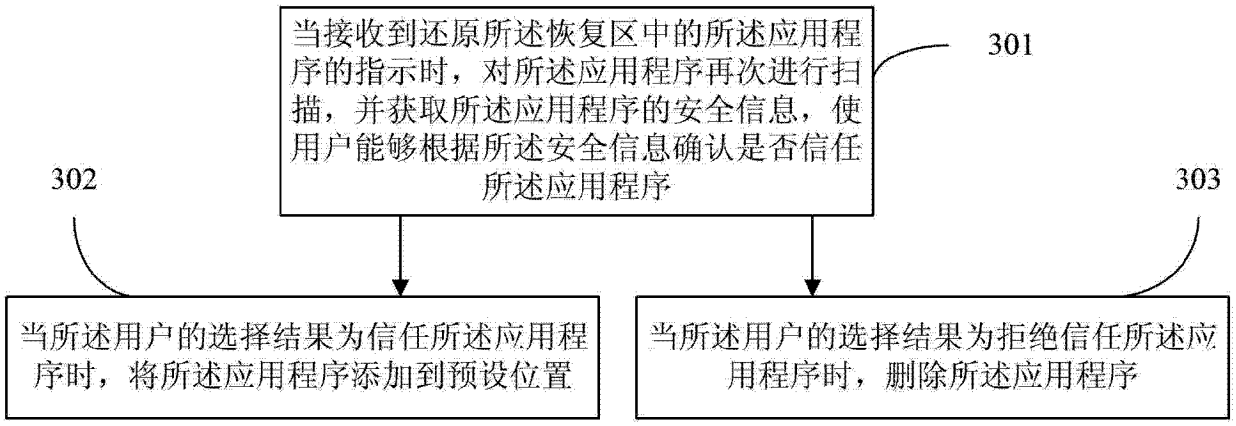

当接收到还原所述恢复区中的所述应用程序的指示时，对所述应用程序再次进行扫描，并获取所述应用程序的安全信息，使用户能够根据所述安全信息确认是否信任所述应用程序
301
302
303
当所述用户的选择结果为信任所述应用程序时，将所述应用程序添加到预设位置
当所述用户的选择结果为拒绝信任所述应用程序时，删除所述应用程序

图 3

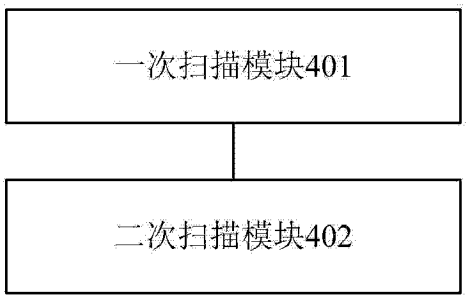

一次扫描模块401
二次扫描模块402

图 4

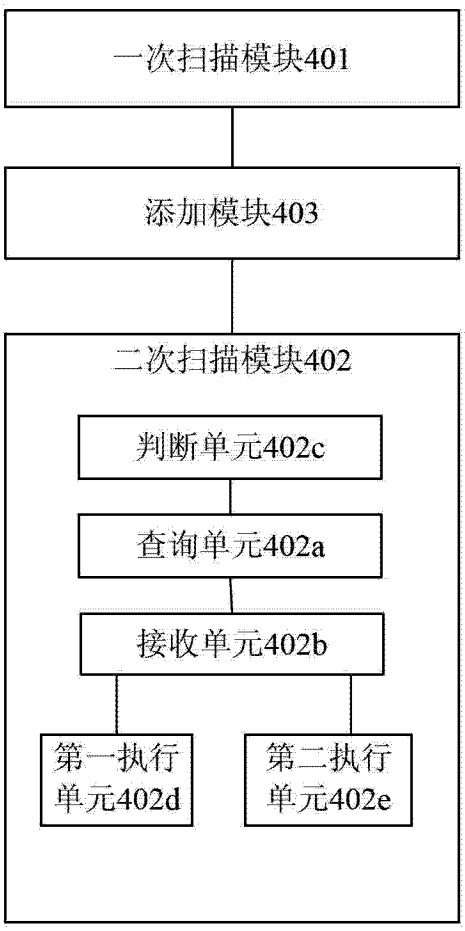

一次扫描模块401
添加模块403
二次扫描模块402
判断单元402c
查询单元402a
接收单元402b
第一执行单元402d
第二执行单元402e

图 5