(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 106156619 A
(43)申请公布日 2016.11.23

(21)申请号 201510197322.4

(22)申请日 2015.04.23

(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振兴路赛格科技园2栋东403室

(72)发明人 杨学营

(74)专利代理机构 广州华进联合专利商标代理有限公司 44224
代理人 黄晓庆 王茹

(51)Int.Cl.
G06F 21/56(2013.01)

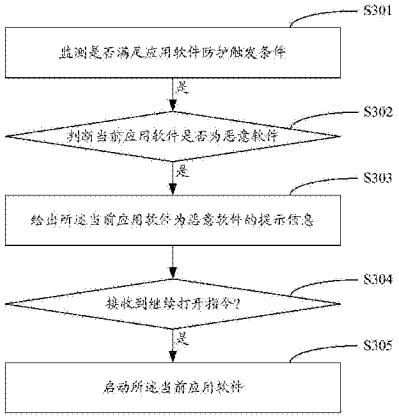
权利要求书3页 说明书8页 附图12页

(54)发明名称

应用安全防护方法及装置

(57)摘要

一种应用安全防护方法及装置，该方法包括步骤：监测是否满足应用软件防护触发条件；若满足，判断当前应用软件是否为恶意软件；若是，给出所述当前应用软件为恶意软件的提示信息；在接收到继续打开所述当前应用软件的继续打开指令时，启动所述当前应用软件。本发明实施例方案极大地提高了终端运行应用程序的安全性。



CN 106156619 A

1. 一种应用安全防护方法，其特征在于，包括步骤：

监测是否满足应用软件防护触发条件；

若满足，判断当前应用软件是否为恶意软件；

若是，给出所述当前应用软件为恶意软件的提示信息；

在接收到继续打开所述当前应用软件的继续打开指令时，启动所述当前应用软件。

2. 根据权利要求 1 所述的应用安全防护方法，其特征在于，在给出所述提示信息后，还包括步骤：

在接收到取消打开指令时，终止所述当前应用软件的启动。

3. 根据权利要求 2 所述的应用安全防护方法，其特征在于，在终止所述当前应用软件的启动之后，还包括步骤：

给出是否卸载所述当前应用软件的提示信息；

在接收到软件卸载指令时，根据该软件卸载指令卸载所述当前应用软件。

4. 根据权利要求 1 所述的应用安全防护方法，其特征在于：

监测所在终端最近打开的应用软件；

判断最近打开的应用软件是否为预定应用类型的应用软件；

若是，则判定满足应用保护触发条件。

5. 根据权利要求 1 所述的应用安全防护方法，其特征在于，在接收到当前应用软件打开指令时，判定满足应用软件防护触发条件。

6. 根据权利要求 5 所述的应用安全防护方法，其特征在于，在接收当前应用软件打开指令之前，还包括步骤：

获取本地终端安装的预定应用类型的应用软件列表；

判断所述应用软件列表中的各应用软件是否为恶意软件；

若是，对判定为恶意软件的应用软件进行标识。

7. 根据权利要求 6 所述的应用安全防护方法，其特征在于，在获取所述应用软件列表之前，还包括步骤：

获取本地终端上安装的所有应用软件的信息；

从所述所有应用软件中筛选出预定应用类型的应用软件的信息，生成所述应用软件列表。

8. 根据权利要求 7 所述的应用安全防护方法，其特征在于，在生成所述应用软件列表之后，还包括步骤：

启动对所述应用软件列表中的各应用软件的扫描，并获得对所述应用软件列表中的各应用软件进行扫描的扫描结果；

根据扫描结果判断对应的应用软件是否为恶意软件；

若是，识别该对应的应用软件的恶意类型，并根据恶意类型将该对应的应用软件的信息添加到本地恶意软件库。

9. 根据权利要求 2 所述的应用安全防护方法，其特征在于，将所述提示信息以弹出框的方式进行显示。

10. 根据权利要求 9 所述的应用安全防护方法，其特征在于，所述弹出框上设置有打开控件、终止控件，通过所述打开控件接收所述继续打开指令，通过所述终止控件接收所述取

消打开指令。

11. 一种应用安全防护装置，其特征在于，包括：

监测模块，用于监测是否满足应用软件防护触发条件；

第一恶意软件判断模块，用于在所述监测模块监测到满足应用软件防护触发条件时，判断当前应用软件是否为恶意软件；

提示模块，用于在所述第一恶意软件判断模块的判定结果为是时，给出所述当前应用软件为恶意软件的提示信息；

启动控制模块，用于在接收到继续打开所述当前应用软件的继续打开指令时，启动所述当前应用软件。

12. 根据权利要求 11 所述的应用安全防护装置，其特征在于，还包括：

取消控制模块，用于在接收到取消打开指令时，终止所述当前应用软件的启动。

13. 根据权利要求 12 所述的应用安全防护装置，其特征在于，还包括软件卸载控制模块；

所述提示模块，还用于在所述取消控制模块终止所述当前应用软件的启动之后，给出是否卸载所述当前应用软件的提示信息；

所述软件卸载控制模块，用于在接收到软件卸载指令时，根据该软件卸载指令卸载所述当前应用软件。

14. 根据权利要求 11 所述的应用安全防护装置，其特征在于，所述监测模块包括：

终端打开应用监测模块，用于监测所在终端最近打开的应用软件；

应用类型判断模块，用于判断所述最近打开的应用软件是否为预定应用类型的应用软件；

条件确定模块，用于在所述应用类型判断模块的判定结果为是时，判定满足应用保护触发条件。

15. 根据权利要求 11 所述的应用安全防护装置，其特征在于，所述检测模块在接收到当前应用软件打开指令时，判定满足应用软件防护触发条件。

16. 根据权利要求 15 所述的应用安全防护装置，其特征在于，还包括：

列表获取模块，获取本地终端安装的预定应用类型的应用软件列表；

第二恶意软件判断模块，用于判断所述应用软件列表中的各应用软件是否为恶意软件；

标识模块，用于对所述第二恶意软件判断模块判定为恶意软件的应用软件进行标识。

17. 根据权利要求 16 所述的应用安全防护装置，其特征在于，还包括：

软件信息获取模块，用于获取本地终端上安装的所有应用软件的信息；

列表生成模块，用于从所述所有应用软件中筛选出预定应用类型的应用软件的信息，生成所述应用软件列表。

18. 根据权利要求 17 所述的应用安全防护装置，其特征在于，还包括步骤：

扫描控制模块，用于启动对所述应用软件列表中的各应用软件扫描，并获得对所述应用软件列表中的各应用软件进行扫描的扫描结果；

恶意软件分析模块，用于根据扫描结果判断对应的应用软件是否为恶意软件；

类型识别模块，用于识别恶意软件分析模块确定的恶意软件的恶意类型，并根据恶意

类型将该对应的应用软件的信息添加到本地恶意软件库。

19. 根据权利要求 12 所述的应用安全防护装置，其特征在于，所述提示模块将所述提示信息以弹出框的方式进行显示。

20. 根据权利要求 19 所述的应用安全防护装置，其特征在于，所述弹出框上设置有打开控件、终止控件，所述启动控制模块通过所述打开控件接收所述继续打开指令，所述取消控制模块通过所述终止控件接收所述取消打开指令。

应用安全防护方法及装置

技术领域

[0001] 本发明涉及应用安全领域，特别涉及一种应用安全防护方法及装置。

背景技术

[0002] 目前智能手机、平板电脑等终端的普及，针对终端应用所开发的应用程序也越来越多，终端上安装的应用程序的来源也日益广泛，从而终端安装应用程序所存在的安全风险也逐步增大，例如病毒、恶意传播、系统破坏、欺诈行为等等。针对终端上的应用程序的安全保护，以游戏软件为例，目前都是通过杀毒软件后定期扫描，如果扫描出是恶意软件则提示用户，以此达到安全保护的目的。然而，如果用户忽略或错过了杀毒软件的病毒提醒，那么用户在打开该游戏软件时就有可能导致损失，从而存在极大的安全风险。

发明内容

[0003] 基于此，本发明实施例的目的在于提供一种应用安全防护方法及装置，其可以提高终端运行应用程序的安全性。

[0004] 为达到上述目的，本发明实施例采用以下技术方案：

[0005] 一种应用安全防护方法，包括步骤：

[0006] 监测是否满足应用软件防护触发条件；

[0007] 若满足，判断当前应用软件是否为恶意软件；

[0008] 若是，给出所述当前应用软件为恶意软件的提示信息；

[0009] 在接收到继续打开所述当前应用软件的继续打开指令时，启动所述当前应用软件。

[0010] 一种应用安全防护装置，包括：

[0011] 监测模块，用于监测是否满足应用软件防护触发条件；

[0012] 第一恶意软件判断模块，用于在所述监测模块监测到满足应用软件防护触发条件时，判断当前应用软件是否为恶意软件；

[0013] 提示模块，用于在所述第一恶意软件判断模块的判定结果为是时，给出所述当前应用软件为恶意软件的提示信息；

[0014] 启动控制模块，用于在接收到继续打开所述当前应用软件的继续打开指令时，启动所述当前应用软件。

[0015] 根据如上所述的本发明实施例的方案，其在监测到满足应用软件防护触发条件、且当前应用软件为恶意软件时，进行该当前应用软件为恶意软件的信息提示，并在接收到继续打开指令的情况下，才启动当前应用软件，即可以在当前应用软件被启动前进行风险提示，从而即便是用户忽略或错过了杀毒软件的病毒提醒，也可以在应用软件启动前对其进行风险提示，极大地提高了终端运行应用程序的安全性。

附图说明

[0016] 图 1 是一个实施例中的本发明方案的工作环境示意图；

[0017] 图 2 是一个实施例中智能终端的组成结构示意图；

[0018] 图 3 是一个实施例中的应用安全防护方法的流程示意图；

[0019] 图 4 是另一个具体示例中的应用安全防护方法的流程示意图；

[0020] 图 5 是另一个具体示例中的应用安全防护方法的流程示意图；

[0021] 图 6 是一个具体示例中生成应用安全列表的流程示意图；

[0022] 图 7 是一个具体示例中扫描到有新安装的应用软件的处理过程的流程示意图；

[0023] 图 8 是一个具体示例中对恶意软件进行标识的终端界面示意图；

[0024] 图 9 是一个具体示例中对恶意软件进行二次提醒的终端界面示意图；

[0025] 图 10 是一个实施例中的应用安全防护装置的结构示意图；

[0026] 图 11 是一个具体示例中的应用安全防护装置的结构示意图；

[0027] 图 12 是另一个具体示例中的应用安全防护装置的结构示意图；

[0028] 图 13 是另一个具体示例中应用安全防护装置的结构示意图；

[0029] 图 14 是另一个具体示例中应用安全防护装置的结构示意图。

具体实施方式

[0030] 为使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步的详细说明。应当理解，此处所描述的具体实施方式仅仅用以解释本发明，并不限定本发明的保护范围。

[0031] 图 1 示出了本发明一个实施例中的工作环境示意图。智能终端 100 通过网络与服务器 101 连接，智能终端 100 通过网络与服务器 101 进行交互，可以从服务器 101 获得应用程序后，将获得的应用程序安装在智能终端 100 上并进行应用。然而，智能终端 100 从服务器 101 获得的应用程序可能会存在安全风险，例如恶意扣费、隐私窃取、远程控制、恶意传播、资费消耗、系统破坏、欺骗欺诈、流氓行为等等，进而影响到智能终端的应用安全。本发明实施例针对的是对智能终端安装的应用程序的防护方案，尤其是针对特定应用类型的应用程序的防护方案。

[0032] 智能终端 100 在一个实施例中的结构示意图如图 2 所示。该智能终端包括通过系统总线连接的处理器、存储介质、通信接口、电源接口和内存。其中，智能终端 100 的存储介质存储有一种应用安全防护装置，该装置用于实现对智能终端上安装的应用程序的安全防护。智能终端 100 的通信接口用于与服务器 101 连接和通信，智能终端 100 的电源接口用于与外部电源连接，外部电源通过该电源接口向智能终端 100 供电。智能终端 100 可以是任何一种能够实现智能输入输出的设备，例如移动终端，比如手机、平板电脑等；也可以是其它具有上述结构的设备，比如个人计算机。

[0033] 结合图 1、图 2 所示的示意图，以下对应用安全防护方法及应用安全防护装置的各实施例进行说明。

[0034] 图 3 中示出了一个实施例中的应用安全防护方法的流程示意图。如图 3 所示，本实施例中的方法包括步骤：

[0035] 步骤 S301：监测是否满足应用软件防护触发条件，若满足，进入步骤 S302；

[0036] 步骤 S302：判断满足应用软件防护触发条件的当前应用软件是否为恶意软件，若

是，进入步骤 S303 ；

[0037] 步骤 S303 ：给出所述当前应用软件为恶意软件的提示信息 ；

[0038] 步骤 S304 ：判断是否接收到继续打开所述当前应用软件的继续打开指令，若接收到，则进入步骤 S305 ；

[0039] 步骤 S305 ：启动所述当前应用软件。

[0040] 其中，在上述步骤 S303 中给出所述提示信息后，基于实际考虑因素可能不再打开该当前应用软件，因而还可能会接收到取消打开指令，在接收到取消打开指令时，则可以终止所述当前应用软件的启动。

[0041] 在终止所述当前应用软件的启动之后，还可以进一步给出是否卸载所述当前应用软件的提示信息 ；在接收到软件卸载指令时，根据该软件卸载指令卸载所述当前应用软件。从而可以从根本上杜绝该当前应用软件对智能终端带来的安全性风险。

[0042] 上述应用保护触发条件，可以基于实际应用需要做各种不同的设置。在其中一个具体示例中，通过监测终端最近打开的应用软件来判断是否满足应用保护触发条件。在另一个具体示例中，可以通过是否接收到应用软件打开指令来判断是否满足应用保护触发条件。

[0043] 以通过是否接收到应用软件打开指令来判断是否满足应用保护触发条件为例，图 4 示出了一个具体示例中的应用安全防护方法的流程示意图。在该具体示例中，需要先获取预定应用类型的应用软件列表以打开相应的应用软件。

[0044] 如图 4 所示，在该示例中，首先获取本地安装的预定应用类型的应用软件的应用软件列表，并判断应用软件列表中的各应用软件是否为恶意软件，并对判定为恶意软件的应用软件进行标识。

[0045] 随后，接收针对某一个当前应用软件的打开指令，该当前应用软件是上述引用软件列表中的其中一个，并判断该当前应用软件是否为恶意软件。

[0046] 若当前应用软件不是恶意软件，则可以直接打开该当前应用软件。

[0047] 若当前应用软件是恶意软件，则给出该当前应用软件是恶意软件的提示信息，实现二次提醒。基于该提示信息，智能终端的用户可以选择继续打开该当前应用软件，也可以选择取消打开该当前应用软件。

[0048] 若智能终端的用户继续打开该当前应用软件，会接收到继续打开该当前应用软件的继续打开指令，在接收到该继续打开指令后，启动该当前应用软件。

[0049] 若智能终端的用户取消打开该当前应用软件，会接收到取消打开指令，在接收到取消打开指令后，终止该当前应用软件的启动，同时可给出是否需要卸载该当前应用软件的提示信息，并在接收到卸载指令后，将该当前应用软件卸载。

[0050] 以通过监测终端最近打开的应用软件来判断是否满足应用保护触发条件为例，图 5 示出了一个具体示例中的应用安全防护方法的流程示意图。

[0051] 如图 5 所示，该示例中的方法包括过程 ：

[0052] 首先，监测所在智能终端最近打开的应用软件，智能终端上会有特定的结构来保存最近打开的应用软件的信息，以 Android 系统的智能终端为例，会有一个特定的栈来保存最近打开的应用的信息，例如如果智能终端依次打开了 A、B、C 三个应用软件，则栈中的内容会包括有 C、B、A，其中 C 存在栈顶，即栈顶保存的是当前打开的应用程序的信息，因此

可以从栈顶获得最近打开的应用软件的信息。

[0053] 然后，判断最近打开的该当前应用软件是否为预定应用类型的软件，例如判断该当前应用软件是否为游戏软件，具体的判断方式可以是将获得的当前应用软件的信息与游戏软件库进行比对，若比对一致，则可以判定为是游戏软件。

[0054] 若是预定应用类型的软件，则进一步判断该当前应用软件是否为恶意软件。若不是恶意软件，则可以直接打开该当前应用软件。

[0055] 若当前应用软件是恶意软件，则给出该当前应用软件是恶意软件的提示信息，实现二次提醒。基于该提示信息，智能终端的用户可以选择继续打开该当前应用软件，也可以选择取消打开该当前应用软件。

[0056] 若智能终端的用户继续打开该当前应用软件，会接收到继续打开该当前应用软件的继续打开指令，在接收到该继续打开指令后，启动该当前应用软件。

[0057] 若智能终端的用户取消打开该当前应用软件，会接收到取消打开指令，在接收到取消打开指令后，终止该当前应用软件的启动，同时可给出是否需要卸载该当前应用软件的提示信息，并在接收到卸载指令后，将该当前应用软件卸载。

[0058] 图 6 示出了一个具体示例中生成应用安全列表的流程示意图。如图 6 所示，上述应用安全列表可以通过下述方式生成：

[0059] 首先，获取智能终端本地安装的所有应用软件的信息；

[0060] 随后，从所述所有应用软件中筛选出预定应用类型的应用软件，并生成预定应用类型的应用软件列表。该应用软件列表中包括有筛选出的各预定应用类型的应用软件的信息。

[0061] 其中，从所有应用软件中筛选出预定应用类型的应用软件的过程，可以是采用下述方式进行：

[0062] 其中一种方式，可以是将各应用软件与智能终端本地的预定应用类型的软件数据库进行比对，若比对结果为一致，则判定是预定应用类型的应用软件，若比对结果为不一致，则判定不是预定应用类型的应用软件。

[0063] 此外，也可以是将获得的各应用软件的信息传输到云端服务器，由云端服务器将各应用软件的信息与云端数据库进行比对后，基于比对结果筛选出是预定应用类型的应用软件的信息，并将筛选出的信息返回给智能终端。

[0064] 在必要的情况下，智能终端本地比对与云端服务器比对的方式可以同时进行。智能终端基于智能终端本地比对、云端服务器比对的结果生成上述预定应用类型的应用软件列表，该应用软件列表中可包括有筛选出的是预定应用类型的应用软件的信息。

[0065] 如图 6 所示，在得到应用软件列表后，还可以进一步启动对应用软件列表中的各应用软件的扫描，获得对应用软件列表中的各应用软件的扫描结果。

[0066] 对各应用软件的扫描，可以直接调用本地的病毒扫描软件进行，也可以是将各应用软件的信息发送至云端服务器，由云端服务器进行扫描后获得扫描结果。

[0067] 基于智能终端本地的病毒扫描软件或者云端服务器的扫描结果，可对对应的应用软件是否为恶意软件进行判断，若是恶意软件，则基于扫描结果识别出该恶意软件的恶意类型，并基于恶意类型将对应的应用软件的信息添加到智能终端本地的恶意软件库。

[0068] 从而，在上述图 4、图 5 对应的实施例中，在对当前应用软件是否为恶意软件进行

判断时，可以直接将该当前应用软件的信息与智能终端本地的恶意软件库进行比对即可。若比对结果为不一致，则可以判定该当前应用软件不是恶意软件；若比对结果为一致，则可以直接判定为是恶意软件，且可以确定该恶意软件的恶意类型以对智能终端的用户进行提示。

[0069] 在智能终端的应用过程中，智能终端可能会持续安装新的不同的应用软件，因而也需要对新安装的应用软件进行安全防护。图 7 示出了一个具体示例中扫描到有新安装的应用软件的处理过程的流程示意图。

[0070] 如图 7 所示，具体处理过程如下所述：

[0071] 获取智能终端本地安装的所有应用软件的信息，并判断智能终端本地是否有新安装的预设应用类型的应用软件，判断是否为预设应用类型的应用软件的方式可以与上述图 6 对应的示例中相同的方式进行。

[0072] 若有新安装的预设应用类型的应用软件，则将该新安装的预设应用类型的应用软件的信息添加到上述预定应用类型的应用软件列表，并启动对该新安装的预定应用类型的应用软件的扫描，获得扫描结果。具体的扫描方式可以采用与上述图 6 对应的示例中相同的方式进行。

[0073] 随后，基于扫描结果对该新安装的预定应用类型的应用软件是否为恶意软件进行判断，若是恶意软件，则基于扫描结果识别出该恶意软件的恶意类型，例如恶意扣费、隐私窃取、远程控制、恶意传播、资费消耗、系统破坏、欺骗欺诈、流氓行为等，并基于恶意类型将对应的应用软件的信息添加到智能终端本地的恶意软件库。

[0074] 基于如上各实施例所述的应用安全防护方法，以下结合其中一个具体示例中的应用安全防护方法进行详细说明。在该具体示例中，是以确定了应用软件列表以及恶意软件的信息已经存储到恶意软件库为例进行说明。

[0075] 首先，获取上述建立的预定应用类型的应用软件列表，并基于恶意软件库判断应用软件列表中的各应用软件是否为恶意软件，并对判定为恶意软件的应用软件进行标识。具体的标识方式可以采用任何可能的方式进行，例如角标、不同的颜色、突出显示等等，以采用角标方式进行标识时，一个具体的终端界面示意图可以是如图 8 所示。基于标识的方式，可以对智能终端的用户进行首次提醒，说明有标识的应用软件为恶意软件。

[0076] 基于该标识，智能终端的用户可能选择不再继续打开该应用软件，也可能选择继续打开该应用软件。若需要继续打开该应用软件，智能终端的用户点击该如图 8 所示的该应用软件的图标后，本发明实施例方法对应的软件会接收到的针对该应用软件的打开指令。

[0077] 在接收到打开指令后，若当前应用软件不是恶意软件，则可以直接打开该当前应用软件。若当前应用软件是恶意软件，则给出该当前应用软件是恶意软件的提示信息，以对智能终端的用户进行二次提醒。该提示信息可以以各种可能的方式给出，例如弹出框。以弹出框为例，图 9 中示出了一个具体示例中进行二次提醒的终端界面示意图。如图 9 所示，该弹出框中包括有打开控件和终止控件。基于该提示框中的提示信息，智能终端的用户可以选择继续打开该当前应用软件，也可以选择取消打开该当前应用软件。

[0078] 若智能终端的用户继续打开该当前应用软件，可以通过打开控件输入继续打开指令，本发明实施例方法通过打开控件接收到该继续打开指令后，启动该当前应用软件。

[0079] 若智能终端的用户取消打开该当前应用软件，可以通过取消控件输入取消打开指令，本发明实施例方法通过取消控件接收到取消打开指令后，终止该当前应用软件的启动，同时可给出是否需要卸载该当前应用软件的提示信息，该提示信息也可以通过弹出框的方式实现，弹出框中可设置有卸载控件，用以接收卸载指令。若智能终端的用户选择卸载该软件，则可以通过该卸载控件接收到卸载指令，并基于该卸载指令将该当前应用软件卸载。

[0080] 基于与上述应用安全防护方法相同的思想，本发明实施例还提供一种应用安全防护装置，以下针对应用安全防护装置的各实施例进行详细说明。

[0081] 图 10 中示出了一个实施例中的应用安全防护装置的结构示意图，如图 10 所示，本实施例中的装置包括：

[0082] 监测模块 1001，用于监测是否满足应用软件防护触发条件；

[0083] 第一恶意软件判断模块 1002，用于在监测模块 1001 监测到满足应用软件防护触发条件时，判断当前应用软件是否为恶意软件；

[0084] 提示模块 1003，用于在第一恶意软件判断模块 1002 的判定结果为是时，给出当前应用软件为恶意软件的提示信息；

[0085] 启动控制模块 1004，用于在接收到继续打开所述当前应用软件的继续打开指令时，启动当前应用软件。

[0086] 其中，在提示模块 1003 给出提示信息后，基于实际考虑因素可能不再打开该当前应用软件，因而还可能会接收到取消打开指令，因此，如图 10 所示，本实施例中的装置还可以包括：

[0087] 取消控制模块 1005，用于在接收到取消打开指令时，终止所述当前应用软件的启动。

[0088] 其中，上述提示模块 1003 可以以各种可能的方式进行信息提示时，例如弹出框。在提示模块 1003 将所述提示信息以弹出框的方式进行显示时，弹出框上可设置有打开控件、终止控件，启动控制模块 1004 可以通过打开控件接收继续打开指令，取消控制模块 1005 通过终止控件接收所述取消打开指令

[0089] 此外，如图 10 所示，本实施例中的装置还可以包括有软件卸载控制模块。在终止所述当前应用软件的启动之后，还可以进一步给出是否卸载所述当前应用软件的提示信息，实现对该当前软件的卸载，从而可以从根本上杜绝该当前应用软件对智能终端带来的安全性风险。因此：

[0090] 上述提示模块 1003，还用于在取消控制模块 1005 终止当前应用软件的启动之后，给出是否卸载所述当前应用软件的提示信息，该提示信息也可以以弹出框的方式进行展示，该弹出框中可设置有卸载控件；

[0091] 上述软件卸载控制模块 1006，用于在接收到软件卸载指令时，根据该软件卸载指令卸载所述当前应用软件，该卸载指令可以通过卸载控件接收。

[0092] 上述应用保护触发条件，可以基于实际应用需要做各种不同的设置。在其中一个具体示例中，通过监测终端最近打开的应用软件来判断是否满足应用保护触发条件。在另一个具体示例中，可以通过是否接收到应用软件打开指令来判断是否满足应用保护触发条件。

[0093] 以通过是否接收到应用软件打开指令来判断是否满足应用保护触发条件为例，图

11 示出了一个具体示例中的应用安全防护装置的结构示意图。

[0094] 如图 11 所示，在图 10 对应的应用安全防护装置的基础上，本实施例中的装置还包括有：

[0095] 列表获取模块 1101，获取本地终端安装的预定应用类型的应用软件列表；

[0096] 第二恶意软件判断模块 1102，用于判断所述应用软件列表中的各应用软件是否为恶意软件；

[0097] 标识模块 1103，用于对第二恶意软件判断模块 1102 判定为恶意软件的应用软件进行标识。

[0098] 在此情况下，上述监测模块 1001 在接收到当前应用软件打开指令时，判定满足应用软件防护触发条件。

[0099] 以通过监测终端最近打开的应用软件来判断是否满足应用保护触发条件为例，图 12 示出了另一个具体示例中的应用安全防护装置的结构示意图。

[0100] 如图 12 所示，在图 10 对应的应用安全防护装置的基础上，上述监测装置 1001 包括有：

[0101] 终端打开应用监测模块 10011，用于监测所在终端最近打开的应用软件；

[0102] 应用类型判断模块 10012，用于判断所述最近打开的应用软件是否为预定应用类型的应用软件；

[0103] 条件确定模块 10013，用于在应用类型判断模块 10012 的判定结果为是时，判定满足应用保护触发条件。

[0104] 参见图 13、图 14 中所示的另两个具体示例中的应用安全防护装置，在图 10、图 11、图 12 对应的装置的基础上，本发明实施例的装置还可以包括：

[0105] 软件信息获取模块 1301，用于获取本地终端上安装的所有应用软件的信息；

[0106] 列表生成模块 1302，用于从所述所有应用软件中筛选出预定应用类型的应用软件的信息，生成所述应用软件列表。

[0107] 其中，列表生成模块 1302 从所有应用软件中筛选出预定应用类型的应用软件的过程，可以是采用下述方式进行：

[0108] 其中一种方式，可以是将各应用软件与智能终端本地的预定应用类型的软件数据库进行比对，若比对结果为一致，则判定是预定应用类型的应用软件，若比对结果不一致，则判定不是预定应用类型的应用软件。

[0109] 此外，也可以是将获得的各应用软件的信息传输到云端服务器，由云端服务器将各应用软件的信息与云端数据库进行比对后，基于比对结果筛选出是预定应用类型的应用软件的信息，并将筛选出的信息返回给智能终端。

[0110] 在必要的情况下，列表生成模块 1302 进行智能终端本地比对与云端服务器比对的方式可以同时进行。列表生成模块 1302 基于智能终端本地比对、云端服务器比对的结果生成上述预定应用类型的应用软件列表，该应用软件列表中可包括有筛选出的是预定应用类型的应用软件的信息。

[0111] 如图 13、14 所示，本发明实施例的装置还可以进一步包括：

[0112] 扫描控制模块 1303，用于启动对所述应用软件列表中的各应用软件扫描，并获得对所述应用软件列表中的各应用软件进行扫描的扫描结果；

[0113] 恶意软件分析模块1304，用于根据扫描结果判断对应的应用软件是否为恶意软件；

[0114] 类型识别模块1305，用于识别恶意软件分析模块确定的恶意软件的恶意类型，并根据恶意类型将该对应的应用软件的信息添加到本地恶意软件库。

[0115] 从而，在上述第一恶意软件判断模块1002、第二恶意软件判断模块1102对当前应用软件是否为恶意软件进行判断时，可以直接将该当前应用软件的信息与智能终端本地的恶意软件库进行比对即可。若比对结果为不一致，则可以判定该当前应用软件不是恶意软件；若比对结果为一致，则可以直接判定为是恶意软件，且可以确定该恶意软件的恶意类型以对智能终端的用户进行提示。

[0116] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体(Read-Only Memory，ROM)或随机存储记忆体(Random Access Memory，RAM)等。

[0117] 以上所述实施例的各技术特征可以进行任意的组合，为使描述简洁，未对上述实施例中的各个技术特征所有可能的组合都进行描述，然而，只要这些技术特征的组合不存在矛盾，都应当认为是本说明书记载的范围。

[0118] 以上所述实施例仅表达了本发明的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对发明专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干变形和改进，这些都属于本发明的保护范围。因此，本发明专利的保护范围应以所附权利要求为准。

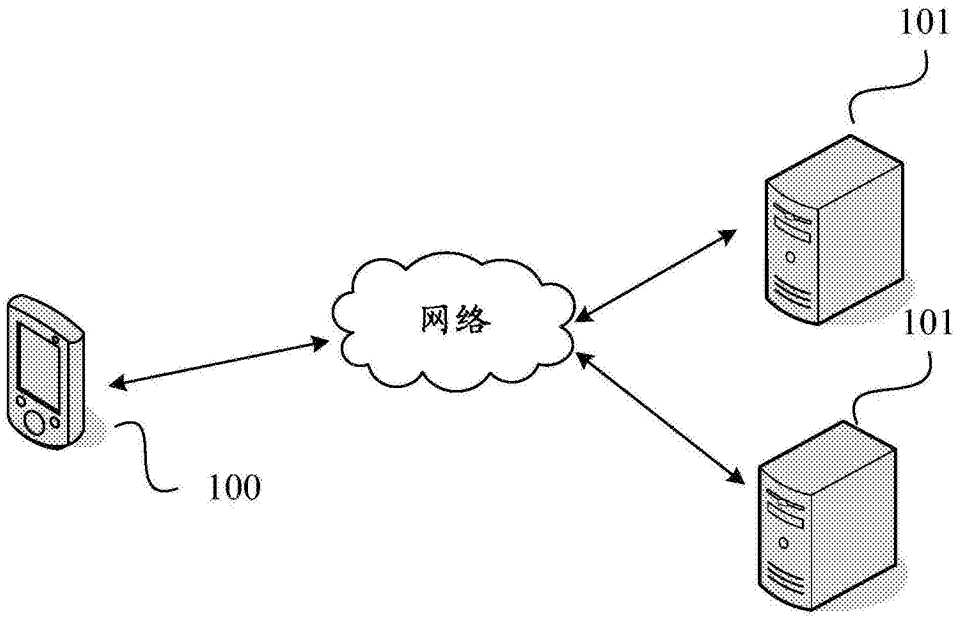


图 1

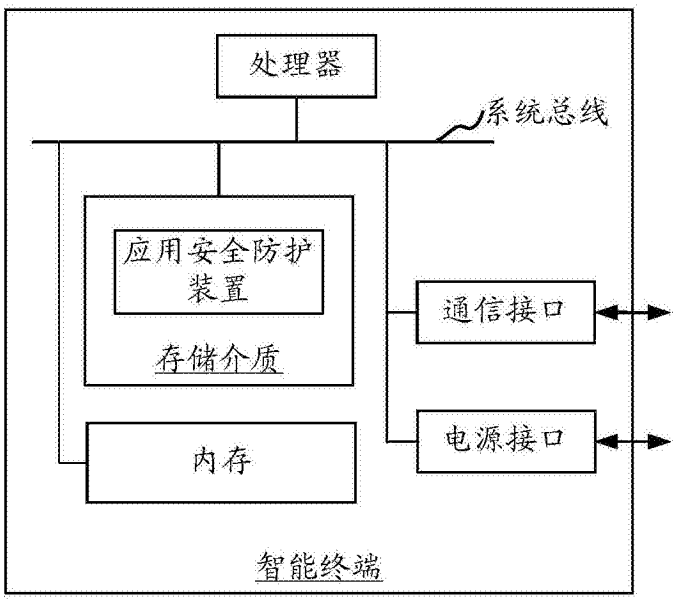


图 2

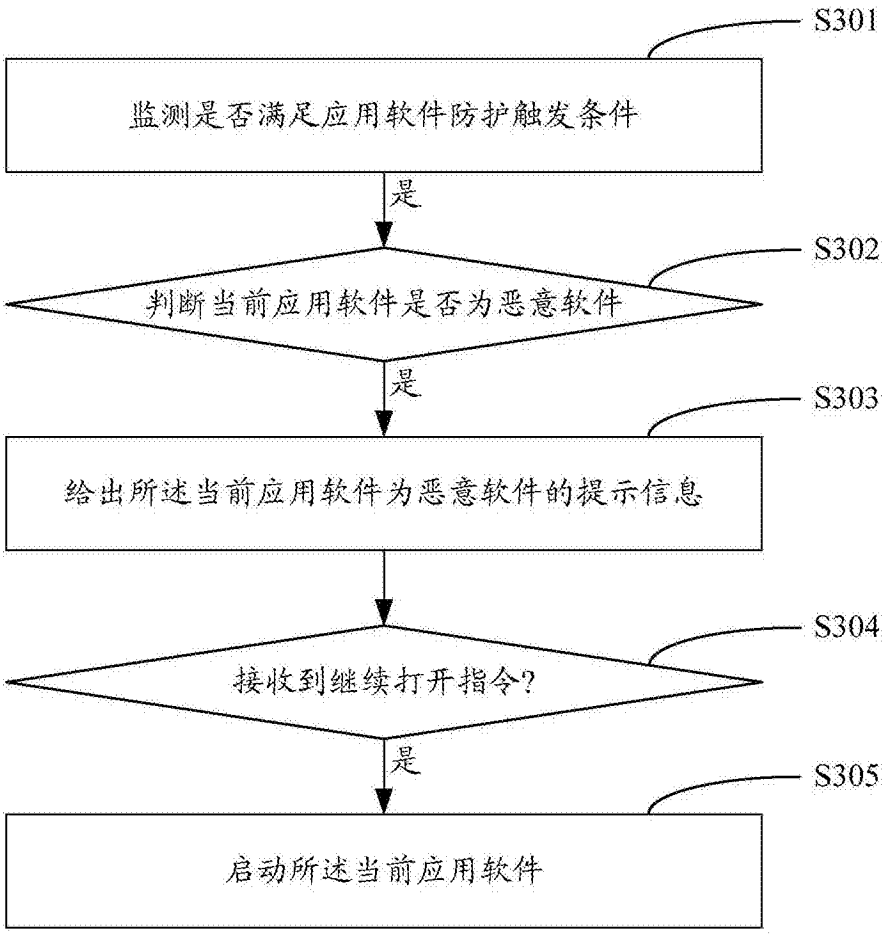

S301
监测是否满足应用软件防护触发条件
是
S302
判断当前应用软件是否为恶意软件
是
S303
给出所述当前应用软件为恶意软件的提示信息
S304
接收到继续打开指令?
是
S305
启动所述当前应用软件

图 3

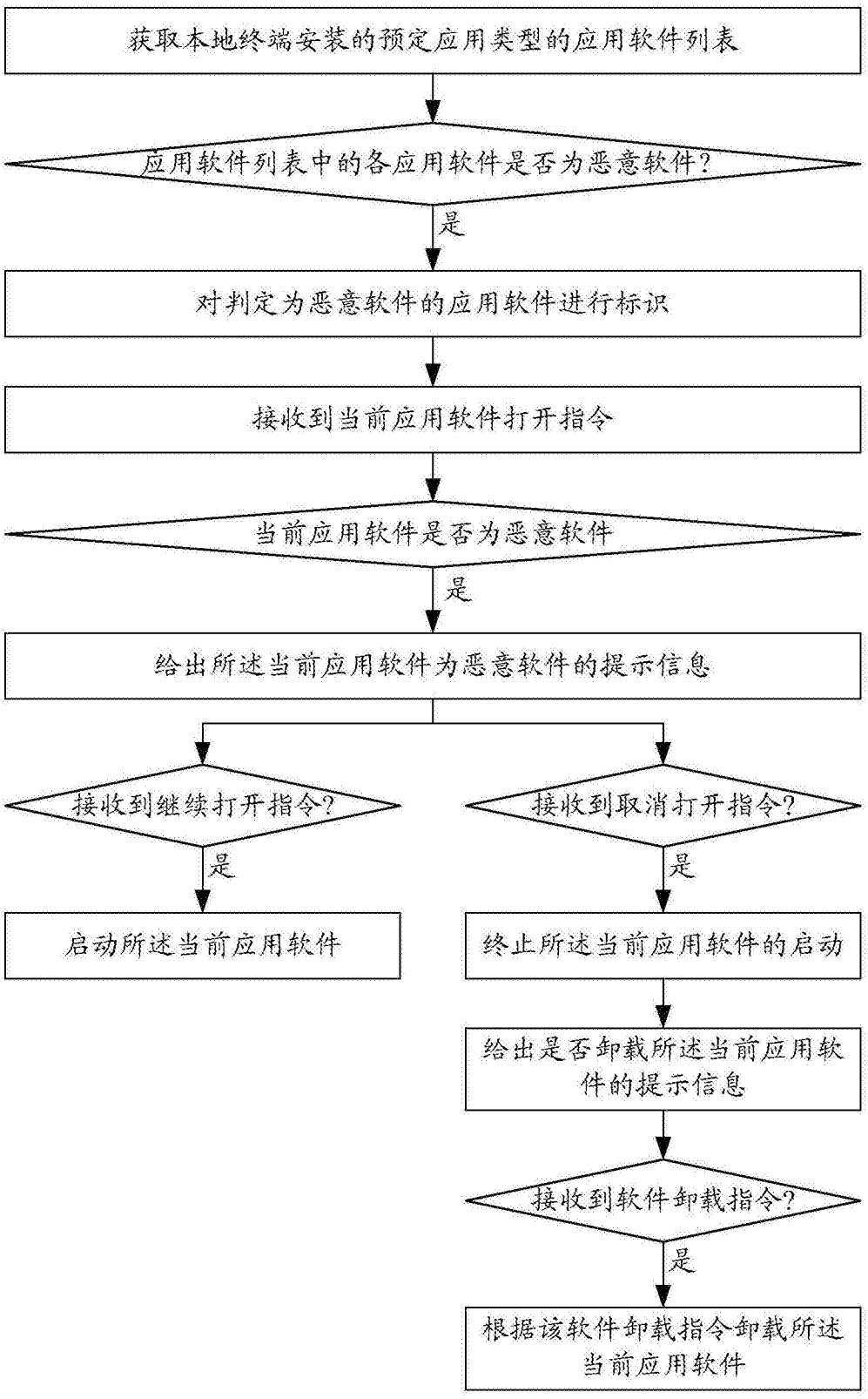

获取本地终端安装的预定应用类型的应用软件列表
应用软件列表中的各应用软件是否为恶意软件?
是
对判定为恶意软件的应用软件进行标识
接收到当前应用软件打开指令
当前应用软件是否为恶意软件
是
给出所述当前应用软件为恶意软件的提示信息
接收到继续打开指令?
是
启动所述当前应用软件
接收到取消打开指令?
是
终止所述当前应用软件的启动
给出是否卸载所述当前应用软件的提示信息
接收到软件卸载指令?
是
根据该软件卸载指令卸载所述当前应用软件

图 4

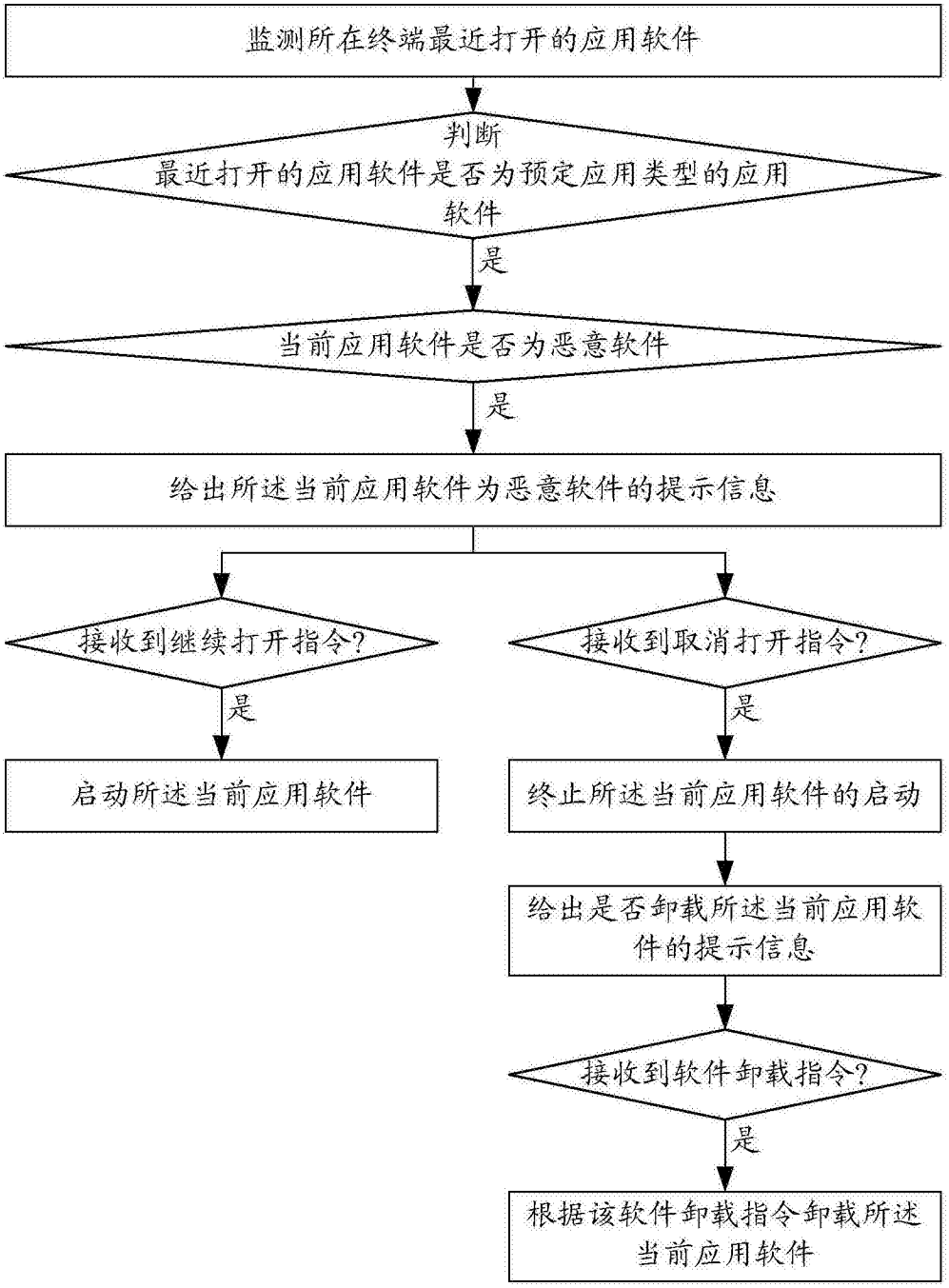

监测所在终端最近打开的应用软件
判断
最近打开的应用软件是否为预定应用类型的应用软件
是
当前应用软件是否为恶意软件
是
给出所述当前应用软件为恶意软件的提示信息
接收到继续打开指令?
是
启动所述当前应用软件
接收到取消打开指令?
是
终止所述当前应用软件的启动
给出是否卸载所述当前应用软件的提示信息
接收到软件卸载指令?
是
根据该软件卸载指令卸载所述当前应用软件

图 5

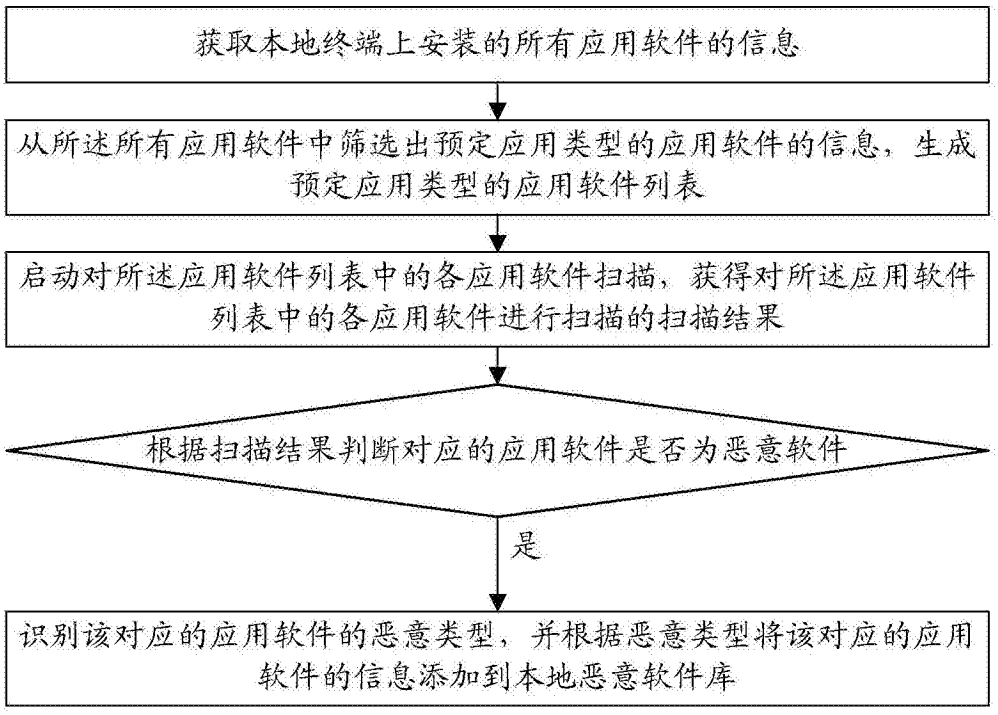

获取本地终端上安装的所有应用软件的信息
从所述所有应用软件中筛选出预定应用类型的应用软件的信息，生成预定应用类型的应用软件列表
启动对所述应用软件列表中的各应用软件扫描，获得对所述应用软件列表中的各应用软件进行扫描的扫描结果
根据扫描结果判断对应的应用软件是否为恶意软件
是
识别该对应的应用软件的恶意类型，并根据恶意类型将该对应的应用软件的信息添加到本地恶意软件库

图 6

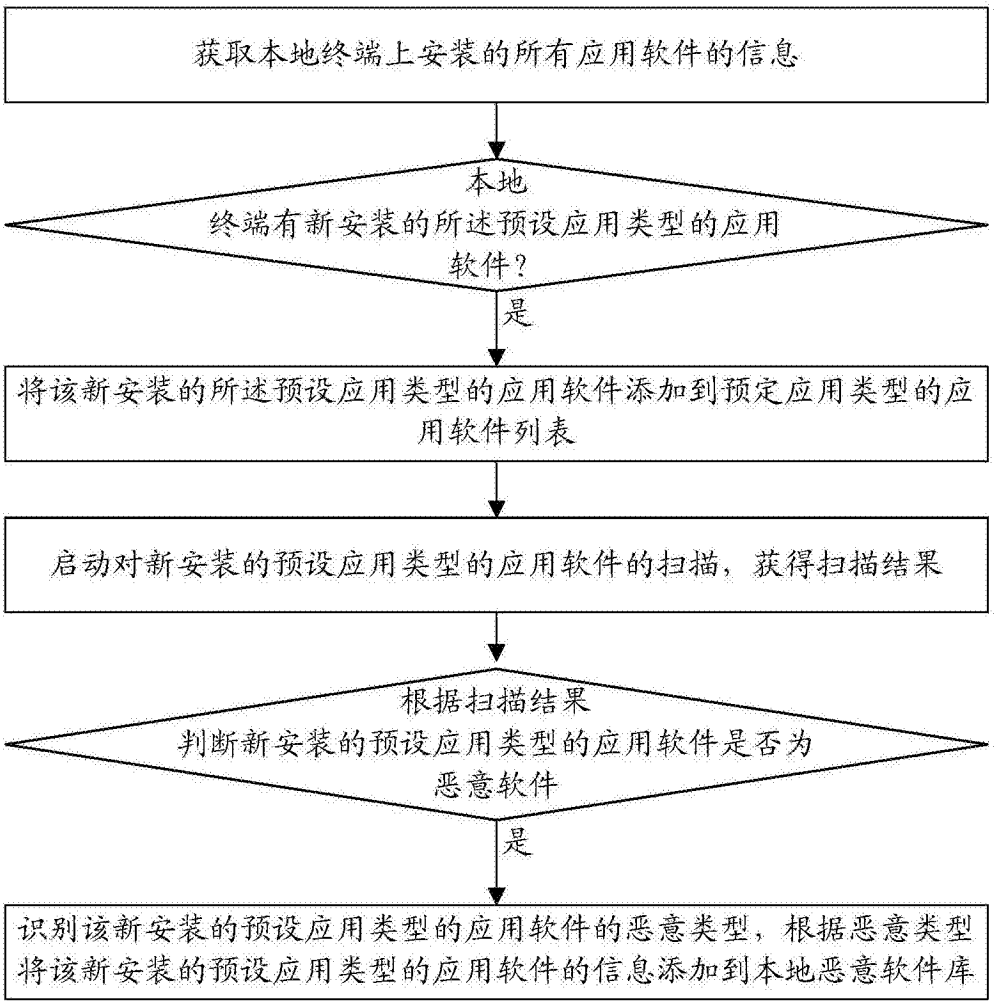

获取本地终端上安装的所有应用软件的信息
本地终端有新安装的所述预设应用类型的应用软件？
是
将该新安装的所述预设应用类型的应用软件添加到预定应用类型的应用软件列表
启动对新安装的预设应用类型的应用软件的扫描，获得扫描结果
根据扫描结果判断新安装的预设应用类型的应用软件是否为恶意软件
是
识别该新安装的预设应用类型的应用软件的恶意类型，根据恶意类型将该新安装的预设应用类型的应用软件的信息添加到本地恶意软件库

图 7

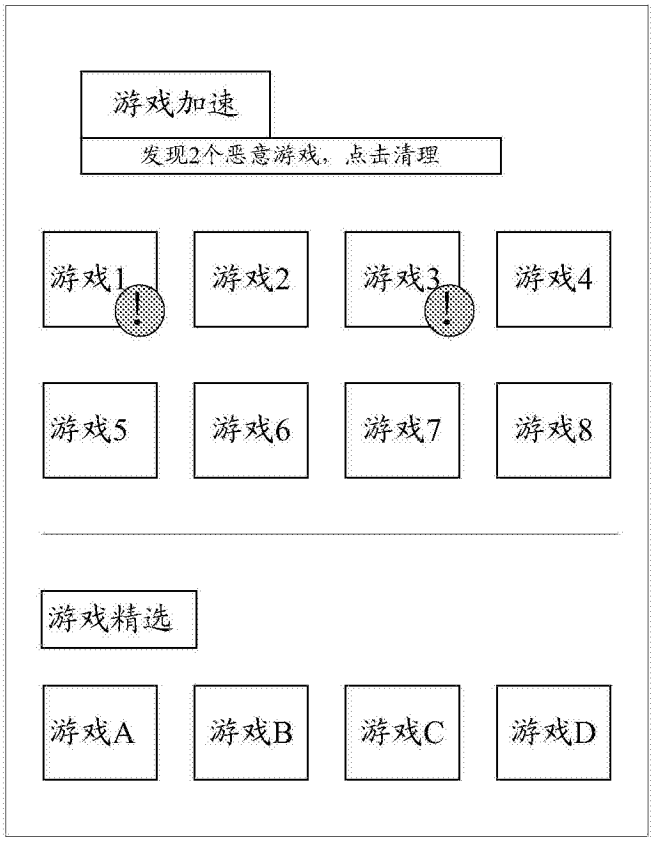

游戏加速
发现2个恶意游戏，点击清理
游戏1
游戏2
游戏3
游戏4
游戏5
游戏6
游戏7
游戏8
游戏精选
游戏A
游戏B
游戏C
游戏D

图 8

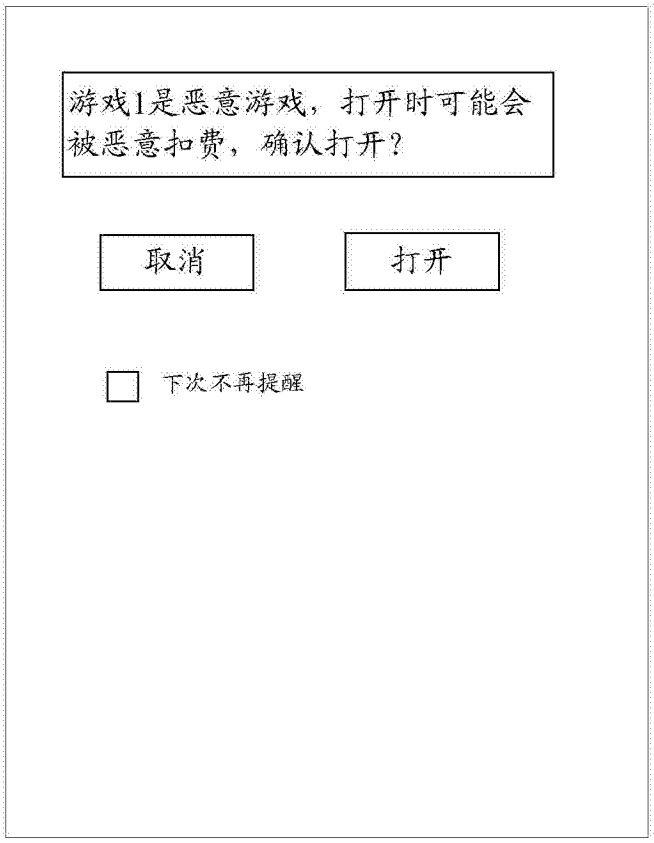

游戏1是恶意游戏，打开时可能会被恶意扣费，确认打开？
取消
打开
下次不再提醒

图 9

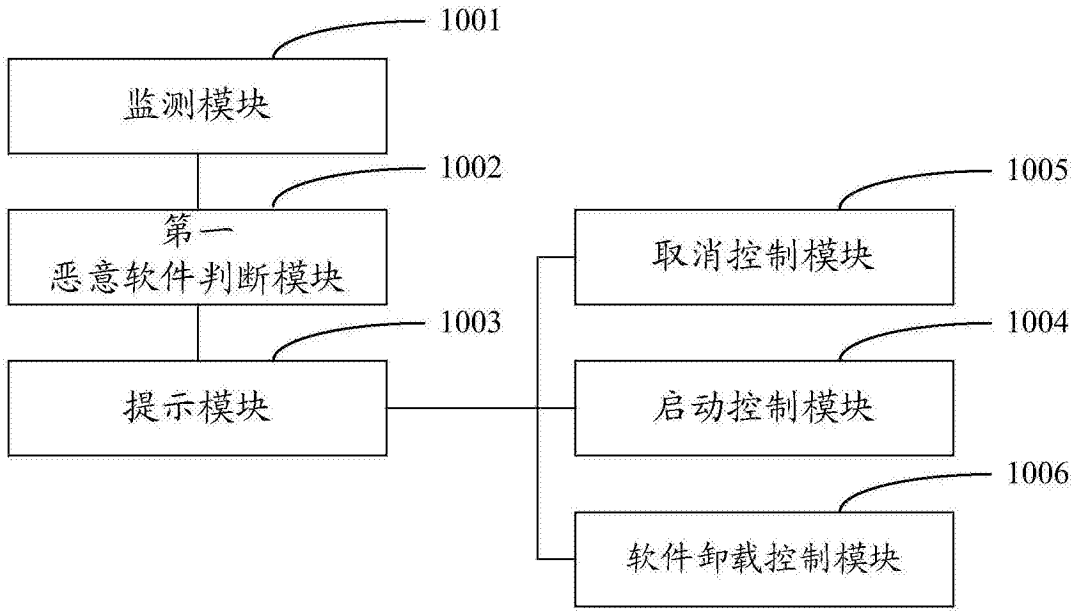

1001
监测模块
1002
第一
恶意软件判断模块
1003
提示模块
1005
取消控制模块
1004
启动控制模块
1006
软件卸载控制模块

图 10

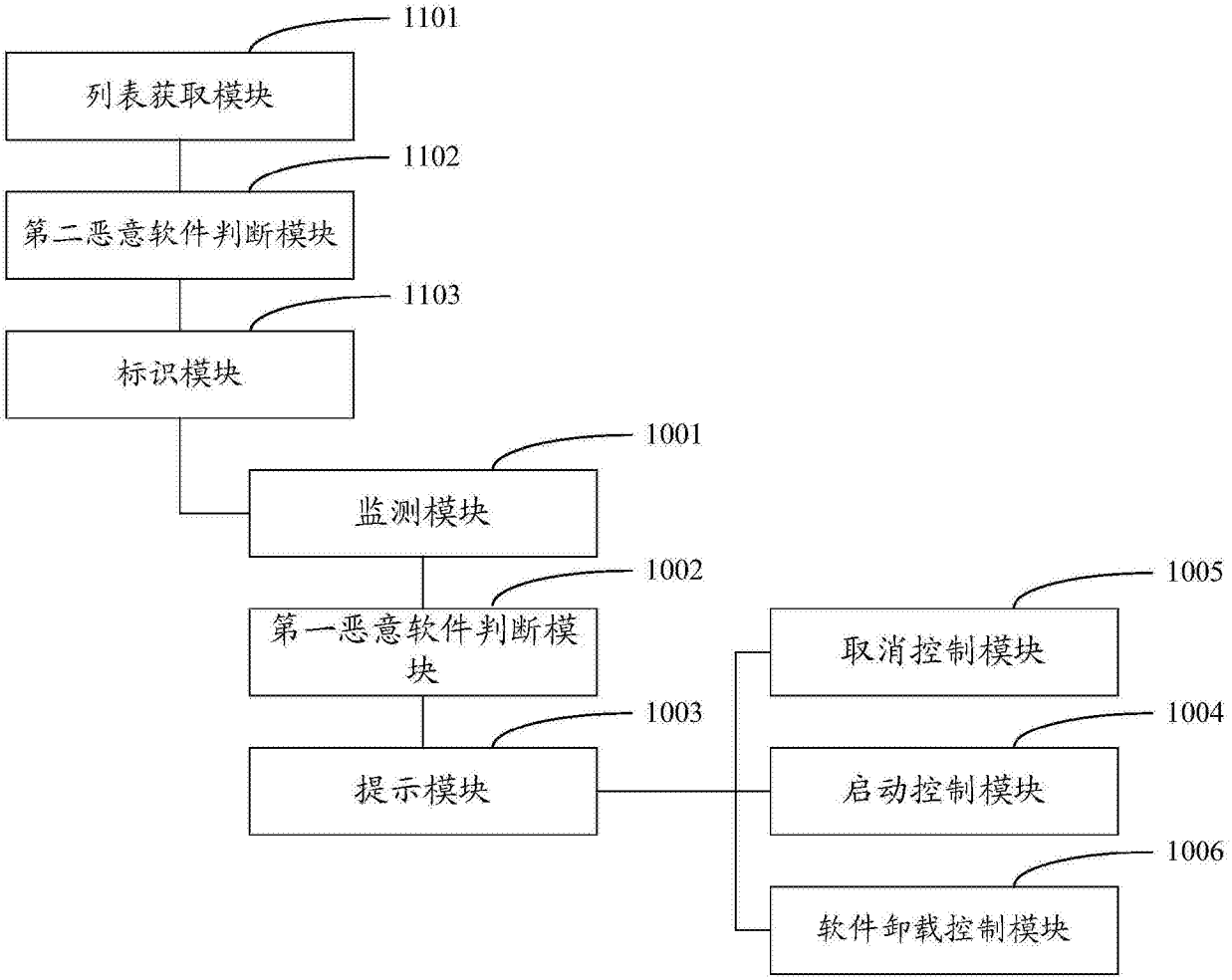

1101
列表获取模块
1102
第二恶意软件判断模块
1103
标识模块
1001
监测模块
1002
第一恶意软件判断模块
1003
提示模块
1005
取消控制模块
1004
启动控制模块
1006
软件卸载控制模块

图 11

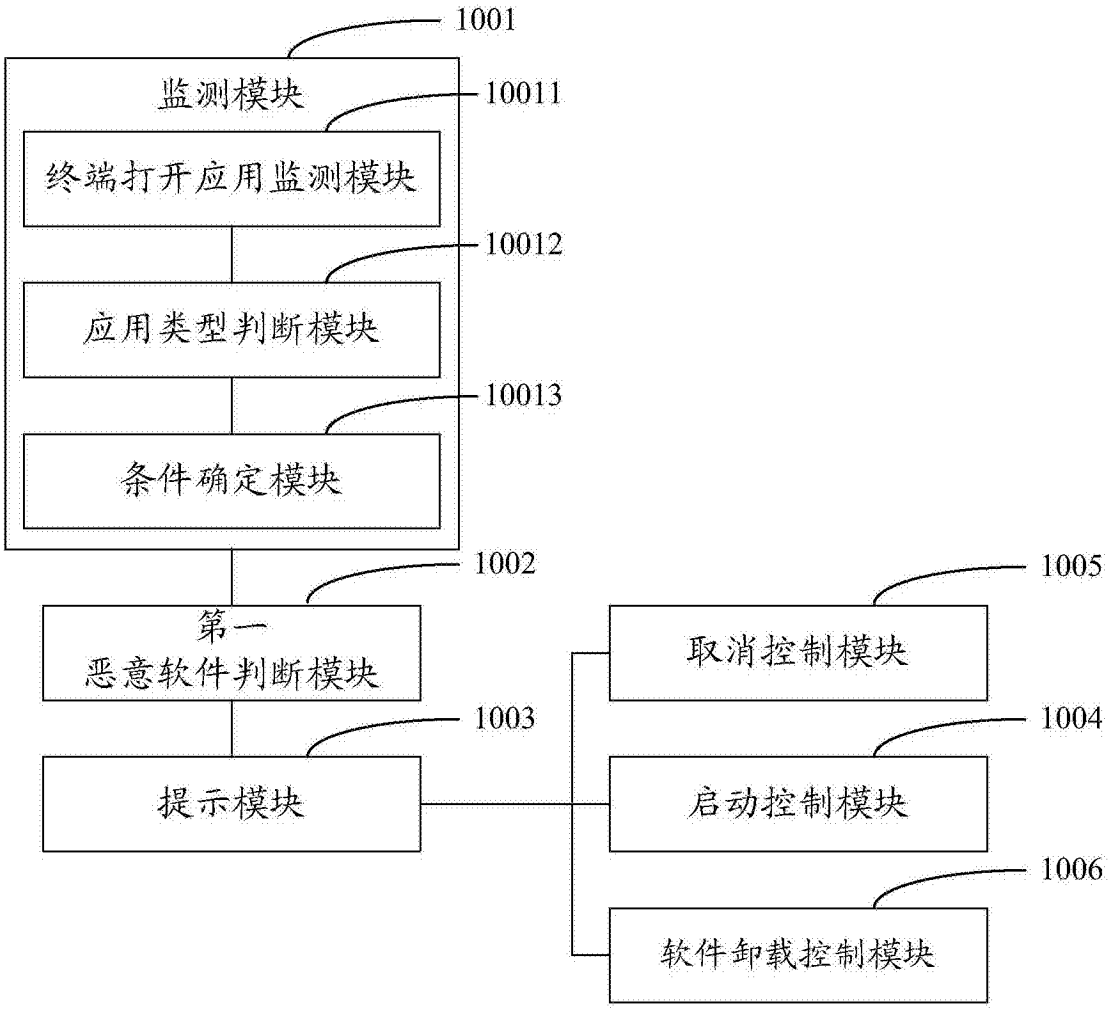

1001
监测模块
10011
终端打开应用监测模块
10012
应用类型判断模块
10013
条件确定模块
1002
第一
恶意软件判断模块
1003
提示模块
1005
取消控制模块
1004
启动控制模块
1006
软件卸载控制模块

图 12

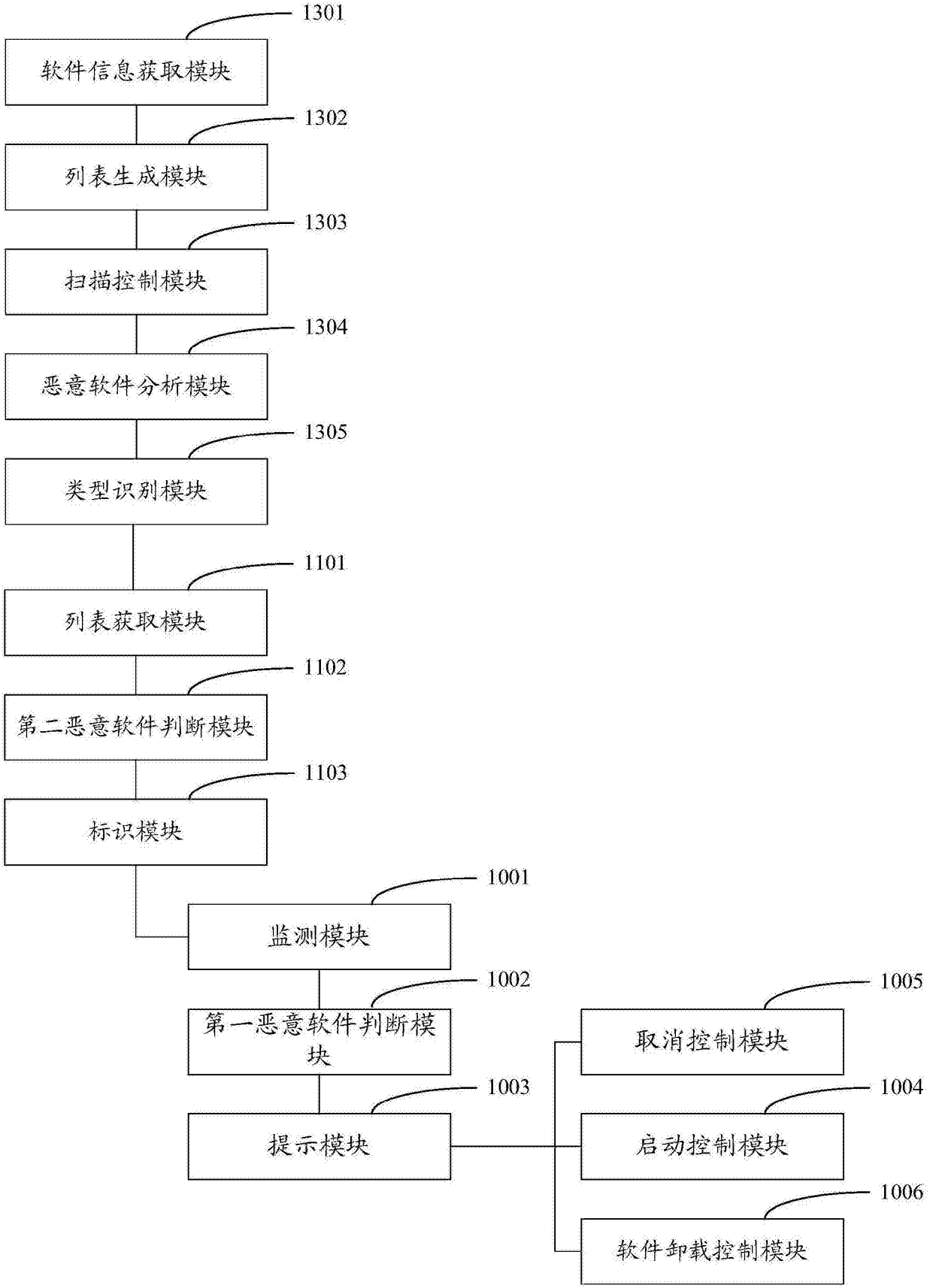

1301
软件信息获取模块
1302
列表生成模块
1303
扫描控制模块
1304
恶意软件分析模块
1305
类型识别模块
1101
列表获取模块
1102
第二恶意软件判断模块
1103
标识模块
1001
监测模块
1002
第一恶意软件判断模块
1003
提示模块
1005
取消控制模块
1004
启动控制模块
1006
软件卸载控制模块

图 13

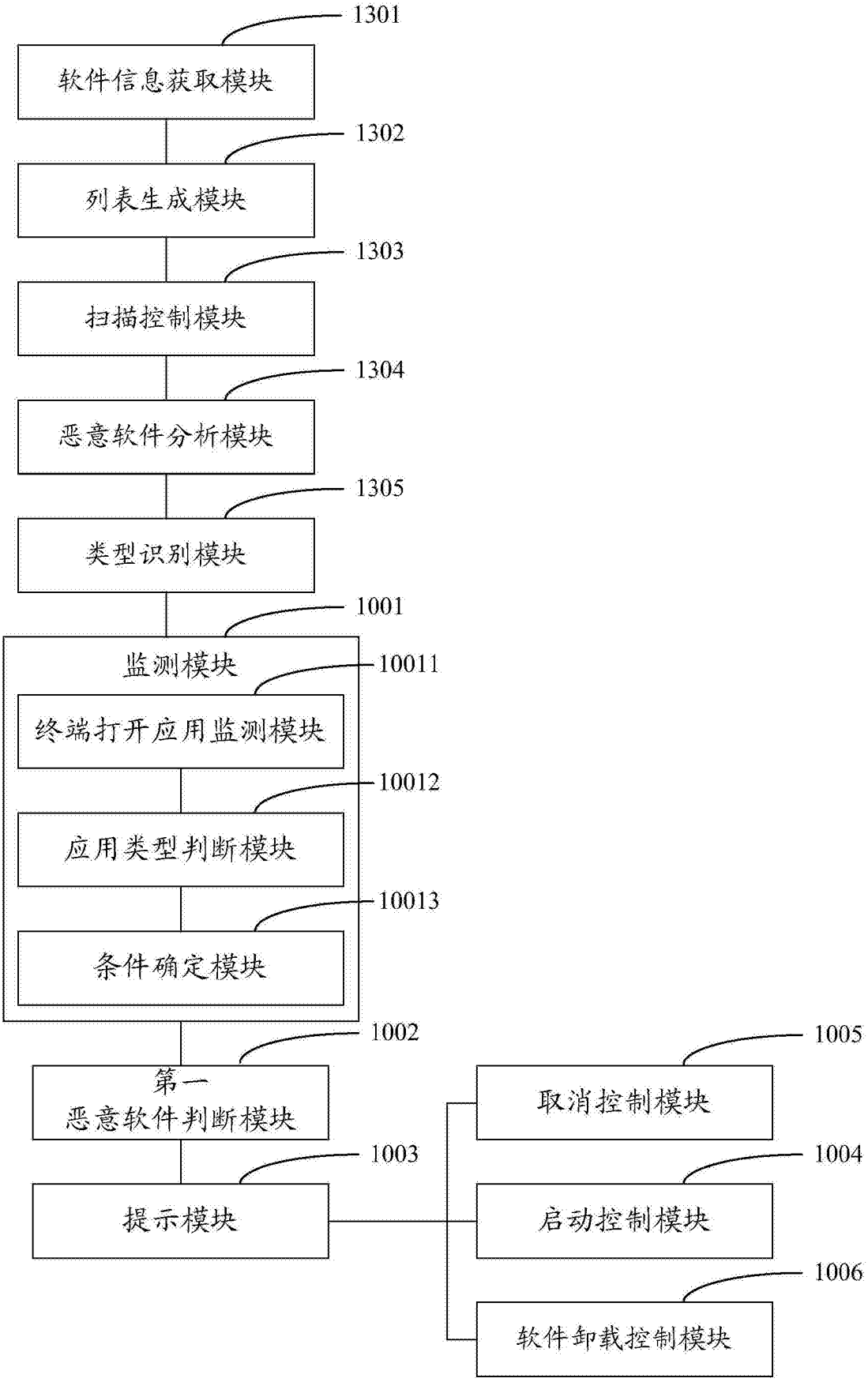

1301
软件信息获取模块
1302
列表生成模块
1303
扫描控制模块
1304
恶意软件分析模块
1305
类型识别模块
1001
监测模块
10011
终端打开应用监测模块
10012
应用类型判断模块
10013
条件确定模块
1002
第一
恶意软件判断模块
1003
提示模块
1005
取消控制模块
1004
启动控制模块
1006
软件卸载控制模块

图 14