(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 107124400 A
(43)申请公布日 2017.09.01

(21)申请号 201710214747.0

(22)申请日 2017.04.01

(71)申请人 中国科学院信息工程研究所
地址 100093 北京市海淀区闵庄路甲89号

(72)发明人 朱大立 金昊 杨莹

(74)专利代理机构 北京路浩知识产权代理有限公司 11002
代理人 王庆龙

(51)Int.Cl.
H04L 29/06(2006.01)
G06F 21/55(2013.01)
G06F 21/56(2013.01)

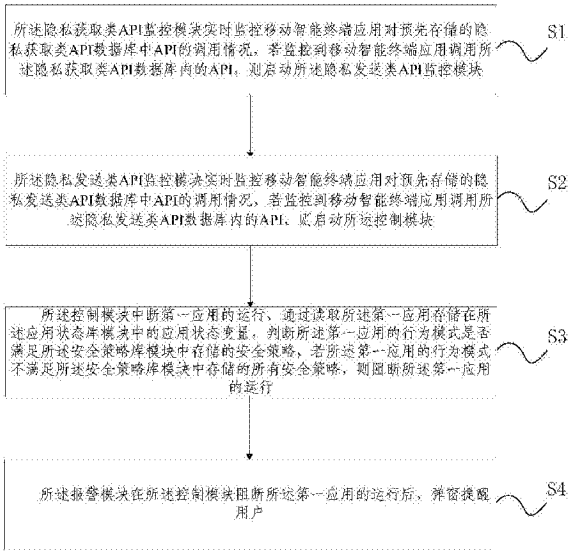
权利要求书2页 说明书11页 附图3页

(54)发明名称

基于安全策略的入侵防御装置及方法

(57)摘要

本发明公开一种基于安全策略的入侵防御装置及方法，能够在不修改操作系统，不影响手机安全应用正常运行，不需要用户频繁参与决策的情况下，有效地阻断隐私窃取行为并检测隐私窃取应用。该装置包括：隐私获取类API监控模块，用于若监控到移动智能终端应用调用隐私获取类API数据库内的API，则启动隐私发送类API监控模块；隐私发送类API监控模块，用于若监控到移动智能终端应用调用隐私发送类API数据库内的API，则启动控制模块；控制模块，用于中断第一应用的运行，若判断获知第一应用的行为模式不满足安全策略库模块中存储的所有安全策略，则阻断第一应用的运行；报警模块，用于在控制模块阻断第一应用的运行后，弹窗提醒用户。



CN 107124400 A

1.一种基于安全策略的入侵防御装置,其特征在于,包括:

隐私获取类API监控模块、隐私发送类API监控模块、应用状态库模块、安全策略库模块、控制模块和报警模块;其中,

所述隐私获取类API监控模块,用于实时监控移动智能终端应用对预先存储的隐私获取类API数据库中API的调用情况,若监控到移动智能终端应用调用所述隐私获取类API数据库内的API,则启动所述隐私发送类API监控模块,其中,所述隐私获取类API数据库中存储有至少一个隐私获取类API;

所述隐私发送类API监控模块,用于实时监控移动智能终端应用对预先存储的隐私发送类API数据库中API的调用情况,若监控到移动智能终端应用调用所述隐私发送类API数据库内的API,则启动所述控制模块,其中,所述隐私发送类API数据库中存储有至少一个隐私发送类API;

所述控制模块,用于中断第一应用的运行,通过读取所述第一应用存储在所述应用状态库模块中的应用状态变量,判断所述第一应用的行为模式是否满足所述安全策略库模块中存储的安全策略,若所述第一应用的行为模式不满足所述安全策略库模块中存储的所有安全策略,则阻断所述第一应用的运行,其中,所述第一应用为所述隐私发送类API监控模块监控到的调用所述隐私发送类API数据库内的API的移动智能终端应用,所述应用状态库模块中存储有隐私类应用的应用状态变量;

所述报警模块,用于在所述控制模块阻断所述第一应用的运行后,弹窗提醒用户。

2.根据权利要求1所述的装置,其特征在于,所述安全策略库模块中存储的安全策略包括以下三条:

(1)应用不向用户隐藏其发送隐私数据的行为;

(2)应用在产生获取隐私数据行为后的T时间单元内不向外发送这些隐私数据,其中,T为预设的时长;

(3)应用被监控到第一次对外发送隐私数据时,提醒用户。

3.根据权利要求2所述的装置,其特征在于,T为5s。

4.根据权利要求2所述的装置,其特征在于,所述装置还包括:

已知的隐私类应用库模块,用于存储可信任的隐私类应用;

所述应用状态变量包括第一变量Known、第二变量GatherTime、第三变量FirstTime和第四变量State,其中,

Known为一个布尔变量,当应用存储在所述已知的隐私类应用库模块时,该值为真;

GatherTime为一个时间变量,用于记录应用调用隐私获取类API的时间;

FirstTime为一个布尔变量,当应用是第一次调用所述隐私发送类API时,该值为真;

State为一个枚举变量,表示应用当前所处的状态,包括第一状态Unauthorized State、第二状态Pre-authorized State、第三状态Middle State、第四状态Authorized State、第五状态User Judgement State和第六状态Blocked State六个取值,各个状态的说明及转换如下:

移动智能终端应用被所述隐私获取类API监控模块监控到调用了所述隐私获取类API,其进入Unauthorized State,在Unauthorized State状态下,如果该应用被所述隐私发送类API监控模块监控到调用了所述隐私发送类API,同时该应用的Known值为真,其进入

Authorized State,或者,如果该应用被所述隐私发送类API监控模块监控到调用了所述隐私发送类API,同时该应用的Known值为假,其进入Pre-authorized State;

当移动智能终端应用处于Pre-authorized State状态下时,所述应用状态库模块计算当前时间CurrentTime和该应用的GatherTime值的差值,如果该差值小于T,则该应用进入User Judgement State,否则,该应用进入Middle State;

当移动智能终端应用处于Middle State状态下时,如果该应用的FirstTime值为真,则进入User Judgement State,否则则进入Authorized State;

当移动智能终端应用处于Authorized State状态下时,该应用被授权可以发送隐私数据;

当移动智能终端应用处于User Judgement State状态下时,所述应用状态库模块调用所述报警模块,以弹出包括该应用即将发送的隐私信息的对话框,帮助用户判断该隐私发送行为是否由其产生。同时,启动一个计时器,在该计时器计时结束前,若用户通过所述对话框确定该隐私发送行为由其产生,则该应用将进入Authorized State,否则,若用户通过所述对话框确定该隐私发送行为不是由其产生,则该应用将进入Blocked State,或者在该计时器计时结束时,用户都没有通过所述对话框做出回应,则该应用进入Blocked State;

当移动智能终端应用处于Blocked State状态下时,该应用的运行被所述控制模块阻断。

5.根据权利要求4所述的装置,其特征在于,所述控制模块,还用于:若所述第一应用的行为模式满足所述安全策略库模块中存储的一条安全策略,则恢复所述第一应用正常运行。

6.根据权利要求5所述的装置,其特征在于,所述控制模块,具体用于:

判断所述第一应用是处于Blocked State状态还是Authorized State状态,若所述第一应用处于Authorized State状态,则确定所述第一应用的行为模式满足所述安全策略库模块中存储的一条安全策略,恢复所述第一应用正常运行,或者若所述第一应用处于Blocked State状态,则确定所述第一应用的行为模式不满足所述安全策略库模块中存储的所有安全策略,阻断所述第一应用的运行。

7.一种基于权利要求1至6任一项所述的装置的入侵防御方法,其特征在于,包括:

所述隐私获取类API监控模块实时监控移动智能终端应用对预先存储的隐私获取类API数据库中API的调用情况,若监控到移动智能终端应用调用所述隐私获取类API数据库内的API,则启动所述隐私发送类API监控模块;

所述隐私发送类API监控模块实时监控移动智能终端应用对预先存储的隐私发送类API数据库中API的调用情况,若监控到移动智能终端应用调用所述隐私发送类API数据库内的API,则启动所述控制模块;

所述控制模块中断第一应用的运行,通过读取所述第一应用存储在所述应用状态库模块中的应用状态变量,判断所述第一应用的行为模式是否满足所述安全策略库模块中存储的安全策略,若所述第一应用的行为模式不满足所述安全策略库模块中存储的所有安全策略,则阻断所述第一应用的运行,其中,所述第一应用为所述隐私发送类API监控模块监控到的调用所述隐私发送类API数据库内的API的移动智能终端应用;

所述报警模块在所述控制模块阻断所述第一应用的运行后,弹窗提醒用户。

基于安全策略的入侵防御装置及方法

技术领域

[0001] 本发明涉及移动智能终端隐私保护及入侵防御技术领域，具体涉及一种基于安全策略的入侵防御装置及方法。

背景技术

[0002] 随着移动智能终端的普及，越来越多的移动智能终端用户将个人信息存储在他们的设备上，智能手机上的隐私窃取攻击和入侵防御技术因此成为移动互联网安全领域的热门话题。

[0003] 针对不同的隐私数据，目前主要存在五种类型的隐私窃取攻击，隐私窃取攻击1主要关注移动智能终端的标识符，包括IMEI、IMSI、ICCID和手机号码等。这些标识符作为手机的标志，经常被应用绑定在个人账户或其他用户个人信息上。隐私窃取攻击2主要关注用户的位置信息。隐私窃取攻击3滥用移动智能终端的通讯服务，包括自主发送付费短信、拨打付费电话；窃取短信息和通话记录；窃听用户通话等。隐私窃取攻击4通过收集和分析用户的网页浏览记录，获取账号、登录账户、日志等信息。隐私窃取攻击5通过主动且隐蔽地接听或拨打黑客的电话号码，将设备转换成环境窃听器。通过分析，这五种类型的隐私窃取攻击主要由两个步骤组成，步骤一从数据源获取隐私数据，步骤二将获取到的隐私数据发送出去。

[0004] 针对以上隐私窃取攻击，目前存在的入侵防御技术主要包括以下两种种：定制系统及应用重打包。

[0005] 1、定制系统。由于Android操作系统的开源性，许多研究者通过对操作系统进行定制，加强访问控制机制，以防御隐私泄露。例如，通过监控与通话相关的API和系统调用，从而对用户通话安全进行防护。

[0006] 该类入侵防御技术需要重新定制系统，会破坏原生操作系统的完整性；在引入防护机制的同时可能产生新的漏洞；并且由于Android操作系统的碎片化问题，定制操作系统只能针对特定机型，无法进行大规模推广。

[0007] 2、应用重打包。应用重打包技术不需要修改操作系统。通过反编译技术获取应用程序的代码，然后在可疑API(包括获取隐私信息的API和发送隐私信息的API)处插入监控代码，最后重新打包形成新的应用。在不影响应用正常功能的情况下，可以有效阻断隐私窃取攻击。

[0008] 该类入侵防御技术容易被恶意攻击绕过，因为监控代码很难覆盖所有的可疑API；如果某个隐私窃取攻击是通过注入so库实现的，该类技术难以实现防御；每当一个可疑API调用被发现时，用户都需要参与判断当前的获取隐私行为或发送隐私行为是否是由自己主导产生，在某种程度上，会影响用户的操作体验。

发明内容

[0009] 为了防御以上的隐私窃取攻击，最大程度地保护移动智能终端用户的隐私安全，

同时不影响移动智能终端上其他应用的正常运行以及用户体验，设计了一种基于安全策略的入侵防御机制。该技术不需要改变操作系统以及被监控应用的原有结构。通过观察大量隐私窃取类恶意应用的行为模式发现，大部分恶意应用会在获取隐私数据后的极短时间α(α<T)内将其发送出去。基于这个发现，制定一系列的安全策略对隐私窃取攻击进行防御。在该项技术中，用户只需要在T时间单元内参与判断发送隐私的行为是否由自己产生，不需要面对频繁弹出的提醒框，因此不影响正常的使用。同时，该技术实现简单，能有效地防御隐私窃取攻击的入侵。

[0010] 一方面，本发明实施例提出一种基于安全策略的入侵防御装置，包括：

[0011] 隐私获取类API监控模块、隐私发送类API监控模块、应用状态库模块、安全策略库模块、控制模块和报警模块；其中，

[0012] 所述隐私获取类API监控模块，用于实时监控移动智能终端应用对预先存储的隐私获取类API数据库中API的调用情况，若监控到移动智能终端应用调用所述隐私获取类API数据库内的API，则启动所述隐私发送类API监控模块，其中，所述隐私获取类API数据库中存储有至少一个隐私获取类API；

[0013] 所述隐私发送类API监控模块，用于实时监控移动智能终端应用对预先存储的隐私发送类API数据库中API的调用情况，若监控到移动智能终端应用调用所述隐私发送类API数据库内的API，则启动所述控制模块，其中，所述隐私发送类API数据库中存储有至少一个隐私发送类API；

[0014] 所述控制模块，用于中断第一应用的运行，通过读取所述第一应用存储在所述应用状态库模块中的应用状态变量，判断所述第一应用的行为模式是否满足所述安全策略库模块中存储的安全策略，若所述第一应用的行为模式不满足所述安全策略库模块中存储的所有安全策略，则阻断所述第一应用的运行，其中，所述第一应用为所述隐私发送类API监控模块监控到的调用所述隐私发送类API数据库内的API的移动智能终端应用，所述应用状态库模块中存储有隐私类应用的应用状态变量；

[0015] 所述报警模块，用于在所述控制模块阻断所述第一应用的运行后，弹窗提醒用户。

[0016] 可选地，所述安全策略库模块中存储的安全策略包括以下三条：

[0017] (1)应用不向用户隐藏其发送隐私数据的行为；

[0018] (2)应用在产生获取隐私数据行为后的T时间单元内不向外发送这些隐私数据，其中，T为预设的时长；

[0019] (3)应用被监控到第一次对外发送隐私数据时，提醒用户。

[0020] 可选地，所述T为5s。

[0021] 可选地，所述装置还包括：

[0022] 已知的隐私类应用库模块，用于存储可信任的隐私类应用；

[0023] 所述应用状态变量包括第一变量Known、第二变量GatherTime、第三变量FirstTime和第四变量State，其中，

[0024] Known为一个布尔变量，当应用存储在所述已知的隐私类应用库模块时，该值为真；

[0025] GatherTime为一个时间变量，用于记录应用调用隐私获取类API的时间；

[0026] FirstTime为一个布尔变量，当应用是第一次调用所述隐私发送类API时，该值为

真；

[0027] State为一个枚举变量，表示应用当前所处的状态，包括第一状态Unauthorized State、第二状态Pre-authorized State、第三状态Middle State、第四状态Authorized State、第五状态User Judgement State和第六状态Blocked State六个取值，各个状态的说明及转换如下：

[0028] 移动智能终端应用被所述隐私获取类API监控模块监控到调用了所述隐私获取类API，其进入Unauthorized State，在Unauthorized State状态下，如果该应用被所述隐私发送类API监控模块监控到调用了所述隐私发送类API，同时该应用的Known值为真，其进入Authorized State，或者，如果该应用被所述隐私发送类API监控模块监控到调用了所述隐私发送类API，同时该应用的Known值为假，其进入Pre-authorized State；

[0029] 当移动智能终端应用处于Pre-authorized State状态下时，所述应用状态库模块计算当前时间CurrentTime和该应用的GatherTime值的差值，如果该差值小于T，则该应用进入User Judgement State，否则，该应用进入Middle State；

[0030] 当移动智能终端应用处于Middle State状态下时，如果该应用的FirstTime值为真，则进入User Judgement State，否则则进入Authorized State；

[0031] 当移动智能终端应用处于Authorized State状态下时，该应用被授权可以发送隐私数据；

[0032] 当移动智能终端应用处于User Judgement State状态下时，所述应用状态库模块调用所述报警模块，以弹出包括该应用即将发送的隐私信息的对话框，帮助用户判断该隐私发送行为是否由其产生。同时，启动一个计时器，在该计时器计时结束前，若用户通过所述对话框确定该隐私发送行为由其产生，则该应用将进入Authorized State，否则，若用户通过所述对话框确定该隐私发送行为不是由其产生，则该应用将进入Blocked State，或者在该计时器计时结束时，用户都没有通过所述对话框做出回应，则该应用进入Blocked State；

[0033] 当移动智能终端应用处于Blocked State状态下时，该应用的运行被所述控制模块阻断。

[0034] 可选地，所述控制模块，还用于：若所述第一应用的行为模式满足所述安全策略库模块中存储的一条安全策略，则恢复所述第一应用正常运行。

[0035] 可选地，所述控制模块，具体用于：

[0036] 判断所述第一应用是处于Blocked State状态还是Authorized State状态，若所述第一应用处于Authorized State状态，则确定所述第一应用的行为模式满足所述安全策略库模块中存储的一条安全策略，恢复所述第一应用正常运行，或者若所述第一应用处于Blocked State状态，则确定所述第一应用的行为模式不满足所述安全策略库模块中存储的所有安全策略，阻断所述第一应用的运行。

[0037] 另一方面，本发明实施例提出一种基于安全策略的入侵防御方法，包括：

[0038] 所述隐私获取类API监控模块实时监控移动智能终端应用对预先存储的隐私获取类API数据库中API的调用情况，若监控到移动智能终端应用调用所述隐私获取类API数据库内的API，则启动所述隐私发送类API监控模块；

[0039] 所述隐私发送类API监控模块实时监控移动智能终端应用对预先存储的隐私发送

类API数据库中API的调用情况，若监控到移动智能终端应用调用所述隐私发送类API数据库内的API，则启动所述控制模块；

[0040] 所述控制模块中断第一应用的运行，通过读取所述第一应用存储在所述应用状态库模块中的应用状态变量，判断所述第一应用的行为模式是否满足所述安全策略库模块中存储的安全策略，若所述第一应用的行为模式满足所述安全策略库模块中存储的一条安全策略，则恢复所述第一应用正常运行，否则，则阻断所述第一应用的运行，其中，所述第一应用为所述隐私发送类API监控模块监控到的调用所述隐私发送类API数据库内的API的移动智能终端应用，所述应用状态库模块中存储有隐私类应用的应用状态变量；

[0041] 所述报警模块在所述控制模块阻断所述第一应用的运行后，弹窗提醒用户。

[0042] 本发明实施例提供的基于安全策略的入侵防御装置及方法，针对当前存在的几种隐私窃取攻击技术，主要利用隐私窃取攻击在获取隐私数据和发送隐私数据时表现出的时序逻辑关系，设计一系列的入侵防御安全策略，其中，隐私获取API监控模块及隐私发送API监控模块：全面考虑到针对多种隐私数据的攻击场景，维护了两个能够不断更新的API数据库，采用API Hooking技术监控移动智能终端应用对API的调用；安全策略模块：基于隐私窃取类恶意应用的行为模式制定一系列的安全策略，不需要用户频繁参与判断和决策，在确保入侵防御的准确率的同时，尽量地不影响用户体验；控制模块：面对可疑的应用(被监控到调用隐私发送API的应用)，采取先暂停后释放的处理方式，将对安全应用正常运行带来的性能影响降到最低。整个方案设计考虑全面，构建了智能移动终端隐私保护和入侵防御的安全机制，能够在不修改操作系统，不影响手机安全应用正常运行，不需要用户频繁参与决策的情况下，有效地阻断隐私窃取行为并检测隐私窃取应用。

附图说明

[0043] 图1为本发明基于安全策略的入侵防御装置一实施例的结构示意图；

[0044] 图2为隐私窃取攻击的生命周期示意图；

[0045] 图3为图1中控制模块5的执行流程图；

[0046] 图4为第四变量State的各个状态的转换关系示意图；

[0047] 图5为本发明基于安全策略的入侵防御装置的入侵防御方法一实施例的流程示意图。

具体实施方式

[0048] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0049] 参看图1，本实施例公开一种基于安全策略的入侵防御装置，包括：

[0050] 隐私获取类API监控模块1、隐私发送类API监控模块2、应用状态库模块3、安全策略库模块4、控制模块5和报警模块6；其中，

[0051] 所述隐私获取类API监控模块1，用于实时监控移动智能终端应用对预先存储的隐私获取类API数据库中API的调用情况，若监控到移动智能终端应用调用所述隐私获取类

API数据库内的API，则启动所述隐私发送类API监控模块2，其中，所述隐私获取类API数据库中存储有至少一个隐私获取类API；

[0052] 所述隐私发送类API监控模块2，用于实时监控移动智能终端应用对预先存储的隐私发送类API数据库中API的调用情况，若监控到移动智能终端应用调用所述隐私发送类API数据库内的API，则启动所述控制模块5，其中，所述隐私发送类API数据库中存储有至少一个隐私发送类API；

[0053] 所述控制模块5，用于中断第一应用的运行，通过读取所述第一应用存储在所述应用状态库模块3中的应用状态变量，判断所述第一应用的行为模式是否满足所述安全策略库模块4中存储的安全策略，若所述第一应用的行为模式不满足所述安全策略库模块4中存储的所有安全策略，则阻断所述第一应用的运行，其中，所述第一应用为所述隐私发送类API监控模块2监控到的调用所述隐私发送类API数据库内的API的移动智能终端应用，所述应用状态库模块3中存储有隐私类应用的应用状态变量；

[0054] 所述报警模块6，用于在所述控制模块5阻断所述第一应用的运行后，弹窗提醒用户。

[0055] 本发明实施例提供的基于安全策略的入侵防御装置，针对当前存在的几种隐私窃取攻击技术，主要利用隐私窃取攻击在获取隐私数据和发送隐私数据时表现出的时序逻辑关系，设计一系列的入侵防御安全策略。方案设计考虑全面，构建了智能移动终端隐私保护和入侵防御的安全机制，能够在不修改操作系统，不影响手机安全应用正常运行，不需要用户频繁参与决策的情况下，有效地阻断隐私窃取行为并检测隐私窃取应用。

[0056] 下面对本发明基于安全策略的入侵防御装置进行详细说明。

[0057] 本发明通过分析大量隐私窃取类恶意应用的行为模式，总结隐私窃取攻击的生命周期如图2所示。发明人在实施本发明的过程中发现大部分恶意应用会在进入p2后的很短时间内进入p3，也就是说，恶意应用会在获取隐私数据后的极短时间(α<T，T预先设置，根据需要可以取5s、10s等值)内将其发送出去，以确保为攻击者提供最新的用户隐私数据，同时在被发现之前获取最大的利益。基于此，本发明制定一系列的安全策略。本发明主要分为七个功能模块——已知的隐私类应用库模块、隐私获取类API监控模块、隐私发送类API监控模块、应用状态库模块、安全策略库模块、控制模块和报警模块。

[0058] 1、已知的隐私类应用库模块。用户掌握该模块的管理权，可以注册并向其中添加可信任的隐私类应用。例如，用户可以将系统自带的短信应用app1添加进该模块，之后app1对敏感API的调用将不会受到监控模块(包括隐私获取类API监控模块和隐私发送类API监控模块)的监控。同时，用户可以从模块中删除其不再信任的隐私类应用。例如，用户可以从模块中删除app1，之后app1对敏感API的调用将再次受到监控模块的监控。

[0059] 2、隐私获取类API监控模块。该模块存储了一个隐私获取类API数据库，如下表所示。

[0060]

隐私数据源	Key	Value
手机标识符	Phone Number	getLine1Number(),
	IMEI	getDeviceId()
	IMSI	getSubscriberId()
	ICCID	getSimSerialNumber()
位置信息	Location information	getLastKnownLocation(), requestLocationUpdates(), getLatitude(), getLongitude()
通讯服务	Phone call	listen(PhoneStateListener listener, int events), onCallStateChanged(int state, String incomingNumber)
	SMS message	getContentResolver().

[0061]

网页浏览记录	Key log	getAllVisitedUrls()
	Browsed web log	
环境窃听	Background audio	AudioRecord.read(), MediaRecorder.start()
	Background video	setPreviewDisplay(), MediaRecorder.start()

[0062] 同时，该模块实时监控移动智能终端应用对数据库中API的调用情况，一旦发现某个应用调用了数据库内某个隐私获取API，则立刻启动隐私发送类API监控模块。

[0063] 3、隐私发送类API监控模块。该模块存储了一个隐私发送类API数据库，如下表所示。

[0064]

Key	Value
SMS message	sendTextMassage(), sendMultipartTextMessage(), sendDataMessage()
Phone call	Uri.parse("tel:")
Http connection	getNetworkInfo(),isConnected(),getState(),setWifiEnabled(), getWif-iState(), url.openConnection()
Socket connection	getInputStream(),getOutputStream(),bind(),connect(),getInetAddress()

[0065] 同时，该模块实时监控应用对数据库中API的调用情况，一旦发现某个应用调用了数据库内某个隐私发送API，则启动控制模块，以使控制模块根据安全策略库中的安全策略，做出相应的安全控制行为。

[0066] 4、控制模块。控制模块的启动发生在监控模块监控到某个应用app_sink调用了隐私发送类API时，其流程图如图3所示：

[0067] 首先，控制模块中断应用app_sink的运行。如果移动智能终端已经被root，本发明的控制模块也将具有root权限，调用简单的命令kill-STOP<pid>就可以中断应用程序的运行。然而，大部分的移动智能终端是没有被root的，因此控制模块在应用层很难取得root权限。这种情况下，控制模块将利用killBackgroundProcesses接口关闭整个目标应用，参数是应用app_sink的包名。

[0068] 然后，控制模块通过读取应用app_sink存储在应用状态库模块中的应用状态参数，判断应用app_sink的行为模式是否满足安全策略库模块中制定的安全策略。如果满足，则恢复其正常运行。如果移动智能终端已经root，控制模块调用kill-CONT<pid>命令重新释放应用进程。如果没有被root，控制模块将无法调用命令释放应用进程。但是Android提供了相关机制，确保应用进程在被停止前调用onSaveInstanceState存储运行状态，并在重启时恢复。因此，控制模块的操作对安全应用带来的性能影响是较小的。如果不满足任何一条安全策略，则彻底阻断应用的运行。

[0069] 5、报警模块。在控制模块运行的过程中，需要启动报警模块与用户进行交互。报警模块的启动主要发生在以下两种情况下：

[0070] (1)在匹配安全策略的过程中，可能需要弹窗提醒用户，让其判断监控到的隐私发送行为是否由其调用应用时自主产生；

[0071] (2)在阻断某个行为模式不符合安全策略的应用后，会弹窗提醒用户对该应用做进一步的处理，如：提交应用到安全软件进行检测或直接强制卸载等。

[0072] 6、安全策略库模块。本发明通过观察大量隐私窃取类恶意应用的行为模式，总结出以下几条安全策略，并存储在安全策略库中。如果某个被监控应用满足以下任一条安全策略，则可以称它是安全的。

[0073] (1)一个应用必须不能向用户隐藏其发送隐私数据的行为；

[0074] (2)一个应用必须不能在产生获取隐私数据行为后的T时间单元内向外发送这些隐私数据；

[0075] 策略(1)可以用来防御那些完全执行隐私窃取行为的恶意应用；策略(2)同时可以防御通过重打包安全应用实现隐私窃取行为的恶意应用，该类应用可能在执行正常隐私相关行为的同时发起隐私窃取攻击。本发明认为T时间单元是用户判断时间，在这段时间内监控到的隐私发送行为，需要用户参与判断是否由其产生。

[0076] 同时，本发明发现，尽管大部分的恶意应用会在获取隐私数据后的T时间单元内产生发送隐私数据的行为，但是也有部分恶意应用在T时间单元内保持静默以躲避检测。在T时间单元之后才开始执行恶意行为。为了处理这种特殊情况，本发明在安全策略库中补充了以下策略：

[0077] (3)如果一个应用被监控到第一次对外发送隐私数据，提醒用户。在这种情况下，如果应用是恶意的，那它必然是隐蔽执行恶意发送隐私数据的行为，因此可以及时提醒用户并阻断该应用的执行。

[0078] 6、应用状态库模块。对于每个隐私类应用，本发明为其设置并存储了4种应用状态变量：

[0079] (1)Known，一个布尔变量，当应用存储在已知的隐私类应用库时，该值为真；

[0080] (2)GatherTime，一个时间变量，记录应用调用隐私获取类API的时间；

[0081] (3)FirstTime，一个布尔变量，当应用是第一次调用隐私发送类API时，该值为真；

[0082] (4)State，一个枚举变量，表示应用当前所处的状态。包括Unauthorized State、Pre-authorized State、Middle State、Authorized State、User Judgement State和Blocked State。应用的状态以及本发明的上述处理方法可以用图4的有限状态机表示。其中：

[0083] (a)Unauthorized State：一旦一个应用被监控到调用了获取隐私API，它将进入Unauthorized State。在这个状态下，如果该应用被监控到调用了发送隐私API，同时Known值为真，表示该应用是可信的，它将进入Authorized State。相反，如果Known值为假，应用将进入Pre-authorized State作下一步的判断。

[0084] (b)Pre-authorized State。该状态下，所述应用状态库模块计算当前时间CurrentTime和GatherTime的差值，如果该值小于T，应用进入User Judgement State；否则，应用进入Middle State。

[0085] (c)Middle State。该状态下，本发明判断这是否是应用第一次调用发送隐私API。如果FirstTime为真，表示应用第一次调用发送隐私API，应用同样进入User Judgement State；否则，应用直接进入Authorized State。

[0086] (d)Authorized State。该状态下，应用被授权可以发送隐私数据。

[0087] (e)User Judgement State。该状态下，所述应用状态库模块调用报警模块，弹出包括即将发送的隐私信息的对话框，帮助用户判断该隐私发送行为是否由其产生。同时，本发明启动一个计时器。如果用户的回答Response是肯定的，应用将进入Authorized State；如果用户的答案是否定的，应用将进入Blocked State。同时，如果在计时器计时结束时，用户都没有做出回应。本发明认为，用户在此时并没有操作其设备，这也意味着该发送隐私的行为不可能由其自身产生。在这种情况下，应用同样进入Blocked State。

[0088] (f)Blocked State。该状态下，应用被认为是恶意的，其运行被阻断。同时，会启动报警模块，提醒用户卸载应用确保隐私安全。可以理解的是，控制模块在对某一应用进行安全策略匹配时，只需要判断该应用是处于Blocked State状态还是Authorized State状态，若该应用处于Authorized State状态，则确定该应用的行为模式满足所述安全策略库模块中存储的一条安全策略，否则，若该应用处于Blocked State状态，则确定该应用的行为模式不满足所述安全策略库模块中存储的所有安全策略。

[0089] 参看图5，本实施例公开一种基于前述实施例所述的基于安全策略的入侵防御装置的入侵防御方法，包括：

[0090] S1、所述隐私获取类API监控模块实时监控移动智能终端应用对预先存储的隐私获取类API数据库中API的调用情况，若监控到移动智能终端应用调用所述隐私获取类API数据库内的API，则启动所述隐私发送类API监控模块；

[0091] S2、所述隐私发送类API监控模块实时监控移动智能终端应用对预先存储的隐私发送类API数据库中API的调用情况，若监控到移动智能终端应用调用所述隐私发送类API数据库内的API，则启动所述控制模块；

[0092] S3、所述控制模块中断第一应用的运行，通过读取所述第一应用存储在所述应用状态库模块中的应用状态变量，判断所述第一应用的行为模式是否满足所述安全策略库模块中存储的安全策略，若所述第一应用的行为模式满足所述安全策略库模块中存储的一条安全策略，则恢复所述第一应用正常运行，否则，则阻断所述第一应用的运行，其中，所述第一应用为所述隐私发送类API监控模块监控到的调用所述隐私发送类API数据库内的API的移动智能终端应用，所述应用状态库模块中存储有隐私类应用的应用状态变量；

[0093] S4、所述报警模块在所述控制模块阻断所述第一应用的运行后，弹窗提醒用户。

[0094] 本发明实施例提供的基于安全策略的入侵防御方法，针对当前存在的几种隐私窃取攻击技术，主要利用隐私窃取攻击在获取隐私数据和发送隐私数据时表现出的时序逻辑关系，设计一系列的入侵防御安全策略。方案设计考虑全面，构建了智能移动终端隐私保护和入侵防御的安全机制，能够在不修改操作系统，不影响手机安全应用正常运行，不需要用户频繁参与决策的情况下，有效地阻断隐私窃取行为并检测隐私窃取应用。

[0095] 本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0096] 本申请是参照根据本申请实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流

程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0097] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0098] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0099] 需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。术语“上”、“下”等指示的方位或位置关系为基于附图所示的方位或位置关系，仅是为了便于描述本发明和简化描述，而不是指示或暗示所指的装置或元件必须具有特定的方位、以特定的方位构造和操作，因此不能理解为对本发明的限制。除非另有明确的规定和限定，术语“安装”、“相连”、“连接”应做广义理解，例如，可以是固定连接，也可以是可拆卸连接，或一体地连接；可以是机械连接，也可以是电连接；可以是直接相连，也可以通过中间媒介间接相连，可以是两个元件内部的连通。对于本领域的普通技术人员而言，可以根据具体情况理解上述术语在本发明中的具体含义。

[0100] 本发明的说明书中，说明了大量具体细节。然而能够理解的是，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。类似地，应当理解，为了精简本发明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呈反映如下意图：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。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。本发明并不局限于任何单一的方面，也不局限于任何单一的实施例，也不局限于这些方面和/或实施例的任意组合和/或置换。而且，可以单独使用本发明的每个方面和/或实施例或者与一个或更多其他方面和/或其实施例结合使用。

[0101] 最后应说明的是：以上各实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述各实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的范围，其均应涵盖在本发明的权利要求和说明书的范围当中。

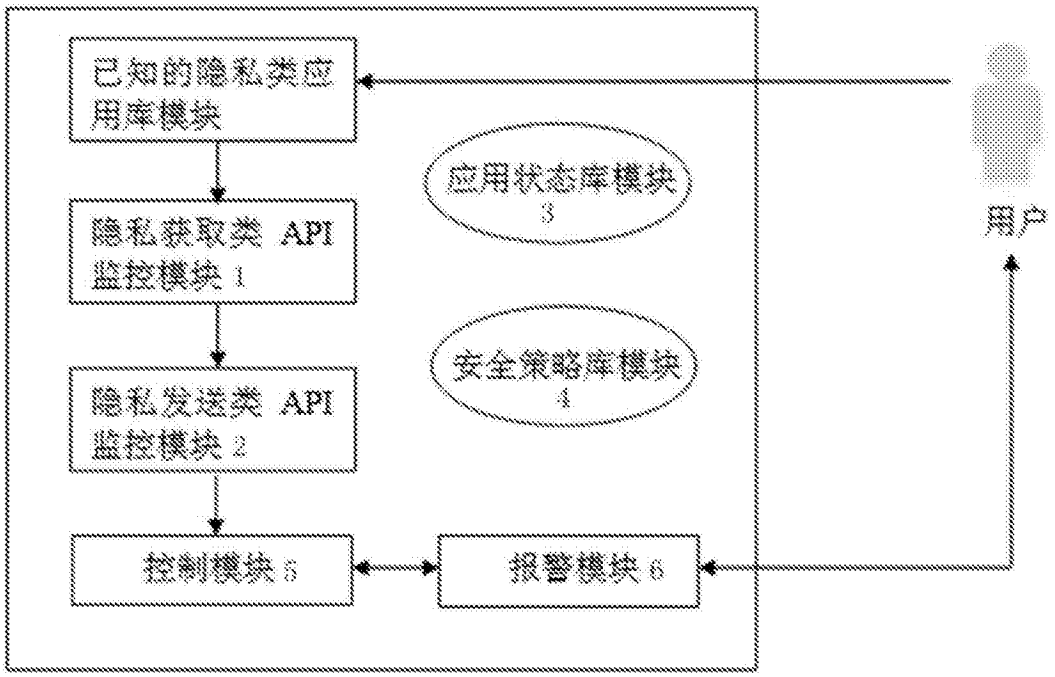

已知的隐私类应用库模块
隐私获取类 API 监控模块 1
隐私发送类 API 监控模块 2
应用状态库模块 3
安全策略库模块 4
控制模块 5
报警模块 6
用户

图1

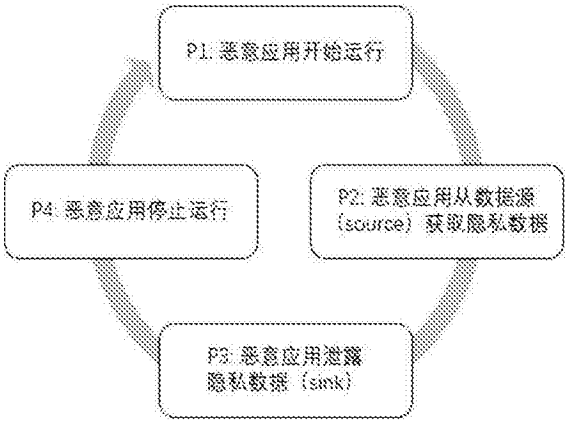

P1: 恶意应用开始运行
P2: 恶意应用从数据源 (source) 获取隐私数据
P3: 恶意应用泄露隐私数据 (sink)
P4: 恶意应用停止运行

图2

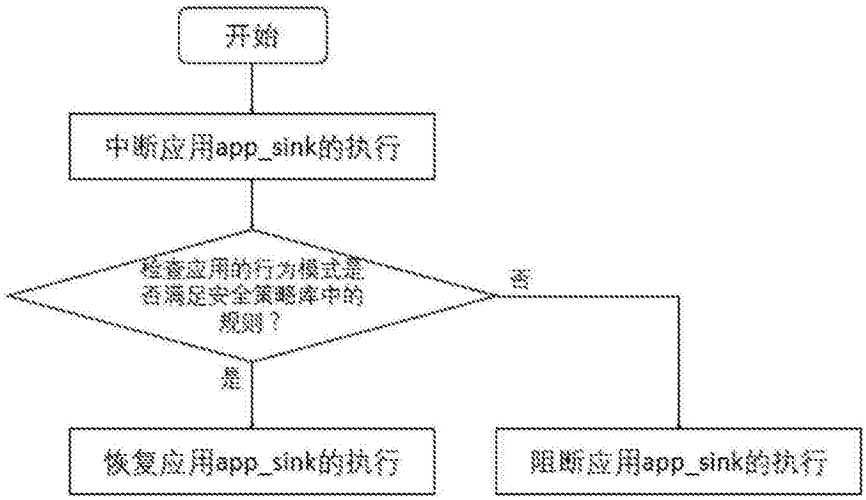

开始
中断应用app_sink的执行
检查应用的行为模式是否满足安全策略库中的规则？
否
是
恢复应用app_sink的执行
阻断应用app_sink的执行

图3

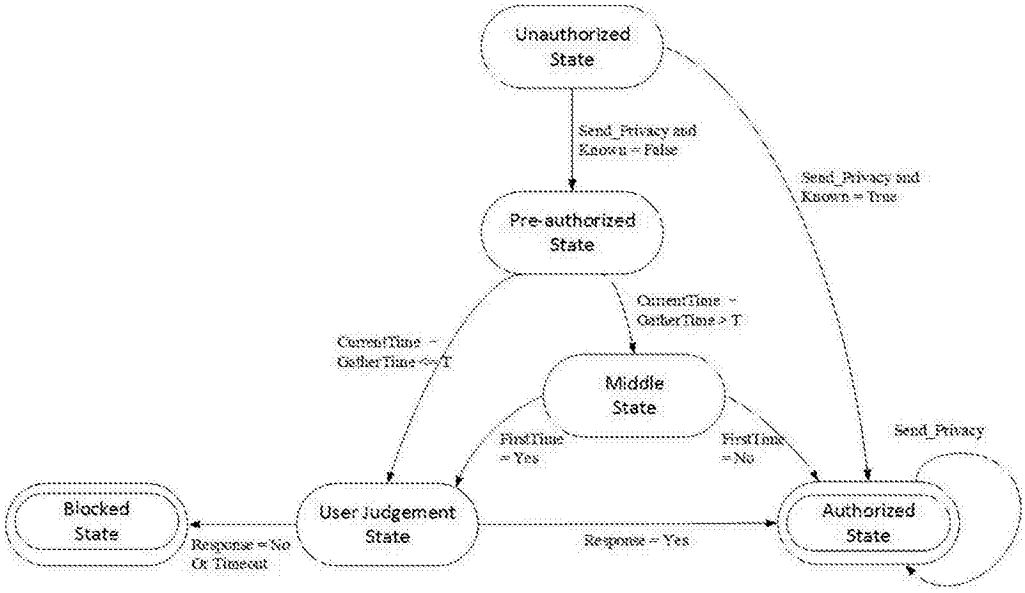

Unauthorized State
Send_Privacy and Known = False
Send_Privacy and Known = True
Pre-authorized State
CurrentTime - GetherTime > T
CurrentTime - GetherTime <= T
Middle State
FirstTime = Yes
FirstTime = No
Send_Privacy
Blocked State
User Judgement State
Authorized State
Response = No Or Timeout
Response = Yes

图4

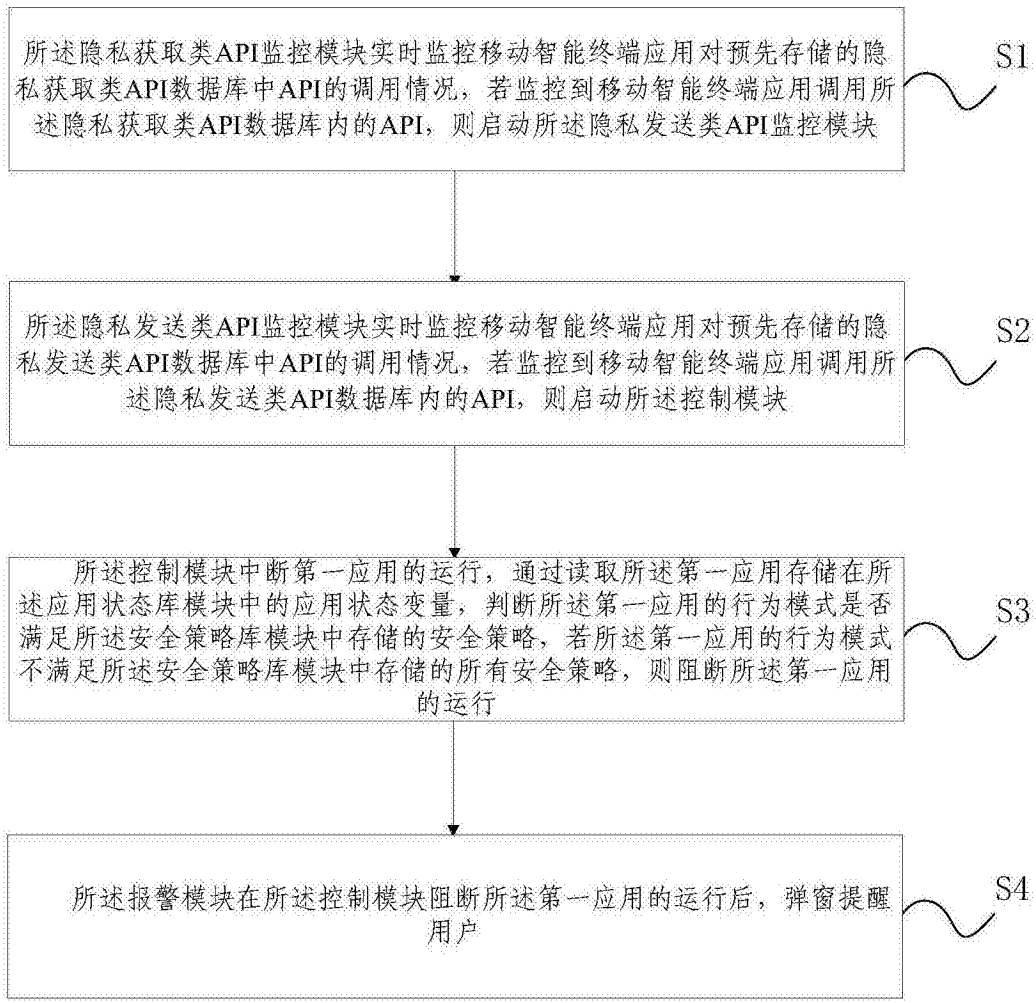

所述隐私获取类API监控模块实时监控移动智能终端应用对预先存储的隐私获取类API数据库中API的调用情况，若监控到移动智能终端应用调用所述隐私获取类API数据库内的API，则启动所述隐私发送类API监控模块
S1
所述隐私发送类API监控模块实时监控移动智能终端应用对预先存储的隐私发送类API数据库中API的调用情况，若监控到移动智能终端应用调用所述隐私发送类API数据库内的API，则启动所述控制模块
S2
所述控制模块中断第一应用的运行，通过读取所述第一应用存储在所述应用状态库模块中的应用状态变量，判断所述第一应用的行为模式是否满足所述安全策略库模块中存储的安全策略，若所述第一应用的行为模式不满足所述安全策略库模块中存储的所有安全策略，则阻断所述第一应用的运行
S3
所述报警模块在所述控制模块阻断所述第一应用的运行后，弹窗提醒用户
S4

图5