(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111782416 B
(45)授权公告日 2024.05.31

(21)申请号 202010515143.1

(22)申请日 2020.06.08

(65)同一申请的已公布的文献号
申请公布号 CN 111782416 A

(43)申请公布日 2020.10.16

(73)专利权人 OPPO广东移动通信有限公司
地址 523860 广东省东莞市长安镇乌沙海滨路18号

(72)发明人 陈勇 陈振明 李擎宇

(74)专利代理机构 北京派特恩知识产权代理有限公司 11270
专利代理师 刘欣 张颖玲

(51)Int.Cl.
G06F 9/54(2006.01)

(56)对比文件
CN 103514030 A,2014.01.15
CN 108121607 A,2018.06.05
CN 110740190 A,2020.01.31

审查员 殷娉

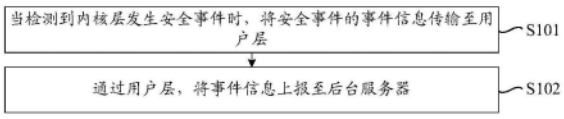
权利要求书4页 说明书19页 附图5页

(54)发明名称

数据上报方法、装置、系统、终端及计算机可读存储介质

(57)摘要

本申请提供了一种数据上报方法、装置、系统、终端及计算机可读存储介质;方法包括:当检测到内核层发生安全事件时,将安全事件的事件信息传输至用户层;通过用户层,将事件信息上报至后台服务器。通过本申请,能够提高终端安全性。



CN 111782416 B

1.一种数据上报方法,其特征在于,包括:

当检测到内核层发生安全事件时,将所述安全事件的事件信息传输至用户层;

通过所述用户层,将所述事件信息上报至后台服务器;

其中,所述通过所述用户层,将所述事件信息上至后台服务器,包括:

通过用户层的用户进程,根据所述事件信息的事件类型,执行对所述事件信息的上报处理,以将所述事件信息上报至所述后台服务器;

其中,所述通过所述用户进程,根据所述事件信息的事件类型,执行对所述事件信息的上报处理,包括:

通过所述用户进程,从所述事件信息中解析出所述事件类型;

当所述事件类型为执行类型时,通过所述用户进程,将所述事件信息保存在预设链表中;并根据预设时间间隔,将所述预设链表中的事件信息保存至本地日志中;

当所述事件类型为提权类型时,通过所述用户进程获取所述事件信息对应的应用包名,将所述应用包名与所述事件信息保存至所述本地日志中,并通过所述用户进程调用弹框在终端界面进行提示;

当所述事件类型为挂载类型时,将所述事件信息保存至所述本地日志中;

通过数据采集服务,将所述本地日志上报至所述后台服务器,以供所述后台服务器进行分析处理。

2.根据权利要求1所述的方法,其特征在于,所述当检测到内核层发生安全事件时,将所述安全事件的事件信息传输至用户层,包括:

当检测到所述内核层发生所述安全事件时,将所述安全事件的事件信息传输至所述内核层的数据上报模块;

通过所述数据上报模块将所述事件信息传入所述内核层与所述用户层之间的预设上报通道;所述事件信息包含所述事件类型;

通过所述用户进程,从所述预设上报通道中获取所述事件信息。

3.根据权利要求2所述的方法,其特征在于,所述将所述安全事件的事件信息传输至所述内核层的数据上报模块之前,所述方法还包括:

在所述内核层的初始化阶段,实现所述数据上报模块中的内核发送子模块和内核接收子模块,并创建所述预设上报通道;

在所述用户层的初始化阶段,实现所述用户层的用户发送模块和用户接收模块,并启动所述用户进程,通过所述用户进程打开所述预设上报通道,完成所述预设上报通道的启动。

4.根据权利要求2或3所述的方法,其特征在于,所述将所述安全事件的事件信息传输至所述内核层的数据上报模块之前,所述方法还包括:

获取所述用户进程的进程标识;

利用所述用户进程调用所述用户发送模块,将所述进程标识通过所述预设上报通道发送给所述数据上报模块;

通过所述数据上报模块的内核接收子模块接收所述进程标识,并保存在所述内核层。

5.根据权利要求4所述的方法,其特征在于,所述通过所述数据上报模块将所述事件信息传入所述内核层与所述用户层之间的预设上报通道,包括:

根据保存的所述进程标识,利用所述数据上报模块的内核发送子模块,将所述事件信息传入所述预设上报通道,以指定所述用户层通过所述进程标识对应的用户进程接收所述事件信息。

6.根据权利要求4所述的方法,其特征在于,所述通过用户层的用户进程,从所述预设上报通道中获取所述事件信息,包括:

结合所述进程标识,通过所述用户进程调用所述用户接收模块,周期性的从所述预设上报通道中读取所述事件信息。

7.根据权利要求2所述的方法,其特征在于,所述当检测到所述内核层发生所述安全事件时,将所述安全事件的事件信息传输至所述内核层的数据上报模块,包括:

当通过所述内核层的第一检测模块,检测到所述内核层中运行的可执行文件的安全上下文不对应时,确定所述内核层发生所述执行类型的安全事件;

获取所述执行类型的安全事件对应的执行类型的事件信息,并通过所述内核发送子模块,将所述执行类型的事件信息发送至所述数据上报模块。

8.根据权利要求2所述的方法,其特征在于,所述当检测到所述内核层发生所述安全事件时,将所述安全事件的事件信息传输至所述内核层的数据上报模块,包括:

当通过所述内核层的第二检测模块,检测到所述内核层的系统调用指令在执行后出现调用权限变化时,确认所述内核层发生所述提权类型的安全事件;

获取所述提权类型的安全事件对应的提权类型的事件信息,并通过所述内核发送子模块,将所述提权类型的事件信息发送至所述数据上报模块。

9.根据权利要求2所述的方法,其特征在于,所述当检测到所述内核层发生所述安全事件时,将所述安全事件的事件信息传输至所述内核层的数据上报模块,包括:

当通过所述内核层的第三检测模块,检测到所述内核层的分区挂载指令在执行后出现预设系统分区读写权限变化时,确认所述内核层发生所述挂载类型的安全事件;

获取所述挂载类型的安全事件对应的挂载类型的事件信息,并通过所述内核发送子模块,将所述挂载类型的事件信息发送至所述数据上报模块。

10.一种数据上报装置,其特征在于,包括:

内核层,用于当检测到内核层发生安全事件时,将所述安全事件的事件信息传输至用户层;

所述用户层,用于将所述事件信息上报至后台服务器;

所述用户层,还用于通过用户进程,根据所述事件信息的事件类型,执行对所述事件信息的上报处理,以将所述事件信息上报至所述后台服务器;

所述用户层,还用于通过所述用户进程,从所述事件信息中解析出所述事件类型;以及当所述事件类型为执行类型时,将所述事件信息保存在预设链表中;并根据预设时间间隔,将所述预设链表中的事件信息保存至本地日志中;以及当所述事件类型为提权类型时,获取所述事件信息对应的应用包名,将所述应用包名与所述事件信息保存至所述本地日志中,并通过所述用户进程调用弹框在终端界面进行提示;以及当所述事件类型为挂载类型时,将所述事件信息保存至所述本地日志中;通过数据采集服务,将所述本地日志上报至后台服务器,以供所述后台服务器进行分析处理。

11.一种数据上报系统,其特征在于,包括:

终端与后台服务器,其中,所述终端包括:内核层与用户层;

所述内核层,用于当检测到所述内核层发生安全事件时,将所述安全事件的事件信息传输至所述用户层;

所述用户层,用于将所述事件信息上报至所述后台服务器;

所述用户层,还用于通过用户进程,对所述事件信息进行解析,得到所述事件信息的事件类型;并根据所述事件类型,将所述事件信息上报至所述后台服务器;

所述用户层还包括弹框模块、数据采集服务、解析模块和保存模块;其中,

所述解析模块,用于从所述事件信息中解析出所述事件类型;

所述保存模块,用于当所述事件类型为执行类型时,将所述事件信息保存在预设链表中;并根据预设时间间隔,将所述预设链表中的事件信息保存至本地日志中;

所述用户进程,还用于当所述事件类型为提权类型时,获取所述事件信息对应的应用包名;

所述保存模块,还用于将所述应用包名与所述事件信息保存至所述本地日志中,并通过所述用户进程调用所述用户层的弹框模块,在终端界面进行提示;

所述保存模块,还用于所述当事件类型为挂载类型时,将所述事件信息保存至所述本地日志中;

所述数据采集服务,用于将所述本地日志上报至所述后台服务器,以供所述后台服务器进行分析处理

所述后台服务器,用于通过所述数据采集服务,根据所述终端上报的所述事件信息,实现对所述内核层安全事件的分析、收集和优化处理。

12.根据权利要求11所述的数据上报系统,其特征在于,

所述内核层,还用于当检测到所述内核层发生所述安全事件时,将所述安全事件的事件信息传输至所述内核层的数据上报模块;以及通过所述数据上报模块将所述事件信息传入所述内核层与所述用户层之间的预设上报通道,所述事件信息包含所述事件类型;

所述用户层,还用于通过所述用户进程,从所述预设上报通道中获取所述事件信息。

13.根据权利要求12所述的数据上报系统,其特征在于,

所述内核层还包括检测模块,所述数据上报模块还包括内核发送子模块与内核接收子模块,所述用户层还包括用户接收模块;其中,

所述检测模块,用于当检测到所述内核层发生所述安全事件时,调用所述内核发送子模块,将所述安全事件的事件信息传输至所述数据上报模块;

所述数据上报模块,用于将所述事件信息传入所述内核层与所述用户层之间的预设上报通道,所述事件信息包含所述事件类型;

所述用户接收模块,用于从所述预设上报通道中获取所述事件信息。

14.根据权利要求12所述的数据上报系统,其特征在于,所述用户层还包括用户发送模块;其中,

所述用户发送模块,用于在所述检测模块调用所述内核发送子模块,将所述安全事件的事件信息传输至所述数据上报模块之前,获取所述用户进程的进程标识;以及将所述进程标识通过所述预设上报通道发送给所述内核接收子模块;

所述内核接收子模块,用于接收所述进程标识,并保存在所述内核层中。

15.根据权利要求14所述的数据上报系统,其特征在于,

所述数据上报模块,还用于根据保存的所述进程标识,将所述事件信息传入所述预设上报通道,以指定所述用户进程根据所述进程标识,通过所述用户接收模块接收所述事件信息。

16.根据权利要求14所述的数据上报系统,其特征在于,

所述用户接收模块,还用于结合所述进程标识,通过所述用户进程的调用,周期性的从所述预设上报通道中读取所述事件信息。

17.一种终端,其特征在于,包括:

存储器,用于存储计算机程序;

处理器,用于执行所述存储器中存储的计算机程序时,实现权利要求1至9任一项所述的方法。

18.一种计算机可读存储介质,其特征在于,存储有计算机程序,用于引起处理器执行时,实现权利要求1至9任一项所述的方法。

数据上报方法、装置、系统、终端及计算机可读存储介质

技术领域

[0001] 本申请涉及终端领域技术,尤其涉及一种数据上报方法、装置、系统、终端及计算机可读存储介质。

背景技术

[0002] Android终端上,埋点是终端数据采集的一种方式,通过埋点上报数据可以追踪与记录终端上一些关键行为,进而用于分析和优化产品体验,也可以为产品的运营提供数据支撑。当前Android终端上通常使用应用自身实现或设备厂商定制的数据采集(Data Collection Server,DCS Service)服务进行应用层、框架层和Native层的埋点上报。然而,由于现有的埋点上报方法只能上报应用层、框架层和Native层中发生的安全事件,上报范围比较局限,从而影响了终端的安全性。

发明内容

[0003] 本申请实施例提供一种数据上报方法、装置、系统、终端及计算机可读存储介质,能够提高终端安全性。

[0004] 本申请实施例的技术方案是这样实现的:

[0005] 本申请实施例提供一种数据上报方法,包括:

[0006] 当检测到内核层发生安全事件时,将所述安全事件的事件信息传输至用户层;

[0007] 通过所述用户层,将所述事件信息上报至后台服务器。

[0008] 本申请实施例提供一种数据上报装置,包括:

[0009] 内核层,用于当检测到内核层发生安全事件时,将所述安全事件的事件信息传输至用户层;

[0010] 用户层,用于将所述事件信息上报至后台服务器。

[0011] 本申请实施例提供一种数据上报系统,包括:

[0012] 终端与后台服务器,其中,所述终端包括:内核层与用户层;

[0013] 所述内核层,用于当检测到内核层发生安全事件时,将所述安全事件的事件信息传输至用户层;

[0014] 所述用户层,用于将所述事件信息上报至所述后台服务器;

[0015] 所述后台服务器,用于通过数据采集服务,根据所述终端上报的所述事件信息,实现对内核层安全事件的分析、收集和优化处理。

[0016] 本申请实施例提供一种终端,包括:

[0017] 存储器,用于存储计算机程序;

[0018] 处理器,用于执行所述存储器中存储的计算机程序时,实现本申请实施例提供的方法。

[0019] 本申请实施例提供一种计算机可读存储介质,存储有计算机程序,用于引起处理器执行时,实现本申请实施例提供的数据上报方法。

[0020] 本申请实施例提供的技术方案带来的有益效果至少包括：

[0021] 本申请实施例所提供的一种数据上报方法、装置、系统、终端及计算机可读存储介质，当内核层发生安全事件时，终端可以将事件信息传递至用户层，并由用户层事件信息的接收和后台服务器的上报，从而实现了内核层的埋点数据上报，使得内核层发生的安全事件可以及时上报至后台服务器进行进一步的分析，提高了终端的安全性。

附图说明

[0022] 图1为本申请实施例提供的数据上报系统架构的一个可选的结构示意图；

[0023] 图2为本申请实施例提供的数据上报方法的一个可选的流程示意图；

[0024] 图3为本申请实施例提供的数据上报方法的一个可选的流程示意图；

[0025] 图4为本申请实施例提供的数据上报方法的一个可选的流程示意图；

[0026] 图5为本申请实施例提供的数据上报方法的一个可选的流程示意图；

[0027] 图6为本申请实施例提供的数据上报方法的一个可选的流程示意图；

[0028] 图7为本申请实施例提供的数据上报方法的一个可选的流程示意图；

[0029] 图8为本申请实施例提供的数据上报方法的一个可选的流程示意图；

[0030] 图9为本申请实施例提供的数据上报方法的一个可选的流程示意图；

[0031] 图10为本申请实施例提供的数据上报方法的一个可选的流程示意图；

[0032] 图11为本申请实施例提供的在数据上报系统中进行内核安全事件上报的一个可选的流程示意图；

[0033] 图12为本申请实施例提供的数据上报方法的一个可选的流程示意图；

[0034] 图13为本申请实施例提供的数据上报装置的一个可选的组成结构示意图；

[0035] 图14为本申请实施例提供的一种终端的硬件实体示意图。

具体实施方式

[0036] 为了使本申请的目的、技术方案和优点更加清楚，下面将结合附图对本申请作进一步地详细描述，所描述的实施例不应视为对本申请的限制，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它实施例，都属于本申请保护的范围。

[0037] 在以下的描述中，涉及到“一些实施例”，其描述了所有可能实施例的子集，但是可以理解，“一些实施例”可以是所有可能实施例的相同子集或不同子集，并且可以在不冲突的情况下相互结合。

[0038] 在以下的描述中，所涉及的术语“第一\第二\第三”仅仅是是区别类似的对象，不代表针对对象的特定排序，可以理解地，“第一\第二\第三”在允许的情况下可以互换特定的顺序或先后次序，以使这里描述的本申请实施例能够以除了在这里图示或描述的以外的顺序实施。

[0039] 除非另有定义，本文所使用的所有的技术和科学术语与属于本申请的技术领域的技术人员通常理解的含义相同。本文中所使用的术语只是为了描述本申请实施例的目的，不是旨在限制本申请。

[0040] 随着社会的进步和技术的发展，人们越来越多地使用移动终端来以无线的方式接入因特网络来获取信息，包括信息浏览和文件下载等。但是，随着网络信息的广泛普及，网

络安全问题也日益严峻,尤其是许多可执行文件,现在的病毒和木马不仅盗取密码帐号让系统变慢,还感染可执行文件删除ghost的备份。

[0041] 由于终端本身硬件资源的限制,在接入网络获得信息或者增加某些附加功能的过程中尤其需要下载许多可执行文件,而所下载的可执行文件的安全性问题就更为严重,如今有越来越多的终端病毒或恶意程序捆绑、或伪装成正规终端应用软件诱骗用户下载安装,如近期利用“手机护士”、“手机管家”之名大肆传播的“手机兽医”病毒,造成了大量用户中招,造成用户通过手机等移动终端中安装的部分软件出现自动发短信、无法卸载、盗取用户通讯录等恶意情况,使用户在执行此类可执行文件的过程中存在极大的安全隐患,随着安全事件越来越频繁地爆发,终端安全问题已经逐渐成为产业乃至社会关注的焦点。

[0042] 对本申请实施例进行进一步详细说明之前,对本申请实施例中涉及的名词和术语进行说明,本申请实施例中涉及的名词和术语适用于如下的解释。

[0043] 1)内核层、用户层:在操作系统中,虚拟内存通常会被分成用户层即使用者空间(User space)与内核层即核心空间(Kernel space)这两个区块。Linux操作系统和驱动程序运行在内核层,应用程序运行在用户层。

[0044] 2)Netlink套接字:Netlink套接字是一种特殊的应用内核层和用户层进行进程间数据传输的进程间通信方法,Netlink套接字在内核层和用户层提供了一种全双工通信方式,使用AF_NETLINK协议族,通过异步通信机制,将在内核层与用户层之间传递的消息保存在套接字(socket)缓存队列中,发送端只是把消息保存在接收端的socket的接收队列中,而不需要等待接收端收到消息,以此实现内核层和用户层的数据交换和相互通信。

[0045] 本申请实施例提供一种数据上报方法、装置、系统、终端和计算机可读存储介质,能够提高终端安全性,下面说明本申请实施例提供的数据上报终端的示例性应用,本申请实施例提供的终端可以实施为智能手机、平板电脑、笔记本电脑等各种类型的用户终端。

[0046] 参见图1,图1为本申请实施例提供的数据上报系统100的一个可选的架构示意图,为实现支撑一个数据上报应用,终端400(示例性示出了终端400-1和终端400-2)通过网络300连接后台服务器200,网络300可以是广域网或者局域网,又或者是二者的组合。

[0047] 终端400包括内核层410与用户层420,其中,内核层410,用于当检测到内核层发生安全事件时,将安全事件的事件信息传输至用户层420;用户层420,用于将事件信息上报至后台服务器200。其中,内核层410还用于当检测到内核层410发生安全事件时,将安全事件的事件信息传输至内核层410的数据上报模块410_1,以及通过数据上报模块410_1将事件信息传入内核层410与用户层420之间的预设上报通道,事件信息包含事件类型;预设上报通道由内核层410在初始化时创建;用户层420还用于通过用户进程,从预设上报通道中获取事件信息;通过用户进程,对事件信息进行解析,得到事件信息的事件类型;并根据事件类型,将事件信息上报至后台服务器200。后台服务器200用于通过数据采集服务,根据终端上报的事件信息,实现对内核层安全事件的分析、收集和优化处理。具体地,终端400会对内核层410进行安全检测,将检测到的安全事件的事件信息通过预设上报通道传输至用户层420,由用户层420对事件信息进行解析,从而可以得到不同事件信息的不同事件类型。这样,用户层420即可根据事件类型,对事件信息进行不同方式处理,如将事件信息存储至用户层420的本地日志中,或是将事件信息进行界面告警提示等等。用户层420通过终端400的数据采集服务,将包含事件信息的本地日志上报至服务器200,从而完成终端400侧对内核

层410中出现的安全事件的数据上报。后台服务器200通过数据采集服务,接收包含事件信息的本地日志,并存储在数据库500中,并根据数据库500中的事件信息,对终端400的内核层发生的安全事件进行分析,这样,后台服务器200通过对多个事件信息的综合分析,可以分析出终端上存在的恶意程序以及安全漏洞,进而可以对终端400的内核层安全问题进行优化处理。

[0048] 基于图1,内核层410还包括检测模块410_2与内核初始化模块410_3,数据上报模块410_1还包括内核发送子模块410_11和内核接收子模块410_12;用户层420还包括用户初始化模块420_2,弹框模块420_3、数据采集服务420_4;用户接收模块420_11、解析模块420_12、保存模块420_13和用户发送模块420_14。

[0049] 在本申请的一些实施例中,基于图1,检测模块410_2,用于当检测到内核层发生安全事件时,调用内核发送子模块410_11,将安全事件的事件信息传输至数据上报模块410_1;数据上报模块410_1,用于将事件信息传入内核层410与用户层420之间的预设上报通道,事件信息包含事件类型;预设上报通道由内核层410在初始化时创建;用户接收模块420_11,用于从预设上报通道中获取事件信息;解析模块420_12,用于对事件信息进行解析,得到事件信息的事件类型;保存模块420_13,用于根据事件类型,将事件信息上报至后台服务器。

[0050] 在本申请的一些实施例中,基于图1,用户发送模块420_14,用于在检测模块410_2调用内核发送子模块410_11,将所述安全事件的事件信息传输至数据上报模块410_1之前,获取用户进程的进程标识;以及将进程标识通过预设上报通道发送给内核接收子模块410_12;内核接收子模块410_12,用于接收进程标识,并保存在内核层410中。

[0051] 在本申请的一些实施例中,基于图1,数据上报模块410_1,还用于根据保存的进程标识,将事件信息传入预设上报通道,以指定用户进程根据进程标识,通过所述用户接收模块420_11接收事件信息。

[0052] 在本申请的一些实施例中,基于图1,用户接收模块420_11,还用于结合进程标识,通过用户进程的调用,周期性的从预设上报通道中读取事件信息。

[0053] 在本申请的一些实施例中,基于图1,内核初始化模块410_3,用于在检测模块410_2调用内核发送子模块410_11,将所述安全事件的事件信息传输至数据上报模块410_1之前,在内核层410的初始化阶段,实现数据上报模块410_1中的内核发送子模块410_11和内核接收子模块410_12,并创建预设上报通道;用户初始化模块420_2,用于在用户层420的初始化阶段,实现用户层420的用户发送模块420_14和用户接收模块420_11,并启动用户进程,通过用户进程打开预设上报通道,完成预设上报通道的启动。

[0054] 在本申请的一些实施例中,基于图1,解析模块420_12,用于从事件信息中解析出事件类型;保存模块420_13,用于当事件类型为执行类型时,将事件信息保存在预设链表中;并根据预设时间间隔,将预设链表中的事件信息保存至本地日志中;用户进程,还用于当事件类型为提权类型时,获取事件信息对应的应用包名;保存模块420_13,还用于将应用包名与事件信息保存至本地日志中,并通过用户进程调用用户层420的弹框模块420_3,在终端界面进行提示;保存模块420_13,还用于当事件类型为挂载类型时,将事件信息保存至本地日志中;数据采集服务420_4,用于将本地日志上报至后台服务器200,以供后台服务器200进行分析处理。

[0055] 在本申请的一些实施例中,基于图1,检测模块410_2还包括第一检测模块,其中,第一检测模块,用于当检测到内核层410中运行的可执行文件的安全上下文不对应时,确定内核层410发生执行类型的安全事件;以及获取执行类型的安全事件对应的执行类型的事件信息,并通过内核发送子模块410_11,将执行类型的事件信息发送至数据上报模块410_1。

[0056] 在本申请的一些实施例中,基于图1,检测模块410_2还包括第二检测模块,其中,第二检测模块,用于当检测到内核层410的系统调用指令在执行后出现调用权限变化时,确认内核层410发生提权类型的安全事件;以及获取提权类型的安全事件对应的提权类型的事件信息,并通过内核发送子模块410_11,将提权类型的事件信息发送至数据上报模块410_1。

[0057] 在本申请的一些实施例中,基于图1,检测模块410_2还包括第三检测模块,其中,第三检测模块,用于当检测到内核层410的分区挂载指令在执行后出现预设系统分区读写权限变化时,确认内核层410发生挂载类型的安全事件;以及获取挂载类型的安全事件对应的挂载类型的事件信息,并通过内核发送子模块410_11,将挂载类型的事件信息发送至数据上报模块410_1。

[0058] 下面将结合本申请实施例提供的终端的示例性应用和实施,说明本申请实施例提供的数据上报方法。

[0059] 本申请实施例提供一种数据上报方法,适用于对终端内核层发生的安全事件以及其他扩展事件进行上报的场景。本申请实施例中的数据上报在应用于终端时,可以适用终端不同的操作系统,例如Windows系统、Linux系统、Android系统、苹果iOS系统等,下面的实施例仅以Linux系统为例进行阐述。

[0060] 参见图2,图2为本申请实施例提供的数据上报方法的一个可选的流程示意图,将结合图2示出的步骤进行说明。

[0061] S101、当检测到内核层发生安全事件时,将安全事件的事件信息传输至用户层。

[0062] 本申请实施例中,当终端检测到内核层发生安全事件时,会对应获取安全事件的事件信息,并将安全事件的事件信息传输至用户层。

[0063] 本申请实施例中,内核层中的检测模块能够对内核层中运行的操作指令和文件程序等进行安全检测,当检测到内核层中运行的操作指令或程序、文件等存在恶意行为,例如非法提取系统最高权限,修改文件关键读写权限、或者可执行文件中的安全上下文不对应时,检测模块认为内核层发生了安全事件,需要及时上报该安全事件以便进一步分析处理。因此,检测模块将安全事件的事件信息传输至内核层的数据上报模块,由数据上报模块开始对内核安全数据进行上报。

[0064] 本申请实施例中,安全事件的事件信息表征所发生的安全事件的事件内容,示例性的,事件信息可以包含该安全事件发起进程的身份信息,当终端检测到第一进程在内核层中发生提权操作时,可以认为内核层发生了安全事件,终端可以获取第一进程的身份信息和第一进程的父进程的身份信息作为该安全事件的事件信息,其中,身份信息可以是实际用户标识(real user ID,UID)、有效用户标识(effective user ID,EUID)和文件系统用户标识(file set user ID,FSUID),还可以包括GUID、设置用户标识(set user ID,SUID)、进程标识符(Process Identification,PID)等。进一步的,安全事件的事件信息还可以包

括安全事件发生的时间、当时的软硬件运行数据,以及当时系统或应用的其他运行数据等,本申请实施例不作限定。

[0065] 在本申请的一些实施例中,检测模块可以通过在内核层中系统调用的预设位置设置插桩函数,并在插桩函数中设置检测逻辑的方式,对内核层中运行的操作指令、可执行文件等的行为特征进行检测判断,以识别出恶意程序以及恶意操作。

[0066] S102、通过用户层,将事件信息上报至后台服务器。

[0067] 本申请实施例中,用户层接收到内核层传来的事件信息之后,可以对事件信息进行解析、存储等一系列处理,之后通过用户层与后台服务器之间的网络通道,将事件信息上报至后台服务器。

[0068] 本申请实施例中,后台服务器端可以从终端上报的本地日志中同步到终端侧所发生的安全事件,并可基于在一段时间内采集的事件信息,对终端的安全情况进行分析,进而可以定位出终端上的高风险恶意程序,以及查找到终端的安全漏洞,以对终端的安全性进行进一步的优化和安全性提升。

[0069] 可以理解的是,本申请实施例中,当内核层发生安全事件时,终端可以将事件信息传递至用户层,并由用户层事件信息的接收和后台服务器的上报,从而实现了内核层的埋点数据上报,使得内核层发生的安全事件可以及时上报至后台服务器进行进一步的分析,提高了终端的安全性。

[0070] 在本申请的一些实施例中,参见图3,图3为本申请实施例提供的数据上报方法的一个可选的流程示意图,图2示出的S101可以通过S1011-S1013实现,将结合各步骤进行说明。

[0071] S1011、当检测到内核层发生安全事件时,将安全事件的事件信息传输至内核层的数据上报模块。

[0072] 本申请实施例中,终端检测到内核层发生安全事件时,先将事件信息传输至内核层的数据上报模块。

[0073] S1012、通过数据上报模块将事件信息传入内核层与用户层之间的预设上报通道;事件信息包含事件类型。

[0074] 本申请实施例中,终端中的数据上报模块在接收到检测模块传输的事件信息时,通过数据上报模块中的内核发送子模块,将事件信息传入内核层与用户层之间的预设上报通道。

[0075] 本申请实施例中,预设上报通道是终端系统在启动后进行初始化时,在内核层的初始化阶段创建的。预设上报通道是内核层与用户层的通信管道,用于在内核层与用户层之间进行数据的传输和通信。预设上报通道可以通过系统调用实现,也可以通过ioctl,或是proc文件系统实现,也可以通过套接字实现,本申请实施例不作限定。

[0076] 本申请实施例中,当预设上报通道为套接字,示例性的,为Netlink套接字时,则在预设上报通道即Netlink套接字被创建后,终端在内核层中分配该Netlink套接字的输入缓冲区,并在用户层中分配该Netlink套接字的输出缓冲区,以对在Netlink套接字中传输的事件信息进行异步收发。

[0077] 本申请实施例中,当预设上报通道为Netlink套接字时,数据上报模块通过将事件信息写入内核层中Netlink套接字的输入缓冲区实现将事件信息传入内核层与用户层之间

的预设上报通道。对于Netlink套接字的传输方式,一旦事件信息被写入到Netlink套接字的输入缓冲区,数据上报模块即可返回发送成功,不管事件信息有没有到达用户层,也不管事件信息何时被发送到用户层,而是由Netlink套接字中的传输协议将事件信息从输入缓冲器发送到用户层的目标接收进程。

[0078] 本申请实施例中,在使用Netlink套接字的传输协议进行事件信息的发送时,一个事件信息可以在刚被写入输入缓冲区就被发送到用户层,也可以在数据缓存区中与其他事件信息进行累积,由传输协议将多次写入的事件信息一次性发送至用户层,具体的取决于当前线程的空闲或忙碌状态,以及预设上报通道的空间或忙碌状态,本申请实施例不作限定。

[0079] 本申请实施例中,事件信息包含事件类型,其中,事件类型可以根据安全事件的事件特征、触发原因或是安全级别等包含不同的类型。示例性的,对于可执行文件安全上下文不对应所引发的安全事件,事件类型可以是执行类型;对于系统调用非法提权所引发的安全事件,事件类型可以是提权类型;对于修改系统分区读写权限的所引发安全事件,事件类型可以是挂载类型等等。事件类型也可以不限于安全事件,包含内核层发生的其他类型的事件,本申请实施例对事件类型的定义不作限定。

[0080] S1013、通过用户层的用户进程,从预设上报通道中获取事件信息。

[0081] 本申请实施例中,终端利用用户层的用户进程,通过预设上报通道进行事件信息的获取,从而实现将内核层中发生的安全事件初步传递至终端的用户层。

[0082] 本申请实施例中,相应地,当预设上报通道为Netlink套接字时,用户进程可以通过用户接收模块定期对用户层中Netlink套接字的输出缓冲区进行检测,当检测到输出缓冲区中存在发送给该用户进程的事件信息时,用户进程通过用户接收模块获取输出缓存区中对应的事件信息。

[0083] 需要说明的是,本申请实施例中,当预设上报通道为Netlink套接字时,由于数据收发模块对事件信息的发送与用户进程对事件信息的获取是异步的,因此在用户进程定期对用户层中Netlink套接字的输出缓冲区进行检测时,可能存在输出缓冲区中还没有传输过来的事件信息,或者输出缓冲区中已有多个事件信息的情况,对于输出缓冲区中已有多个事件信息的情况,用户进程可以根据用户接收模块中可读取数据长度与缓冲区已有事件信息的数据长度的对比情况,对多个事件信息进行一次性或多次读取。

[0084] 在本申请的一些实施例中,参见图4,图4为本申请实施例提供的数据上报方法的一个可选的流程示意图,基于图2或图3,图2示出的S102可以通过S1021实现,将结合各步骤进行说明。

[0085] S1021、通过用户进程,根据事件信息的事件类型,执行对事件信息的上报处理,以将事件信息上报至后台服务器。

[0086] 本申请实施例中,当用户进程获取到内核层传输过来的事件信息,可以通过用户进程调用用户层的解析模块,对事件信息进行解析,从中解析出事件类型,并根据事件类型获知安全事件的特征类型或安全级别等信息,根据不同安全事件的特征类型或安全级别等信息,通过不同的方式将事件信息上报至服务器。

[0087] 本申请实施例中,用户层可以基于事件类型采取多种上报方式,示例性的,终端可以将每次发生的安全事件,尤其是高风险类型的安全事件即时上报至服务器,也可以先通

过用户层的保存模块将事件信息保存在本地日志文件中,然后通过终端上的数据采集服务,定期将本地日志文件上报至服务器。本申请实施例对用户层向后台服务器上报的方式不作限定。

[0088] 在本申请的一些实施例中,对于Android系统的终端,数据采集服务可以是Android系统中的DCS服务,对于Android系统以及其他类型的终端系统,数据采集服务也可以是其他具备数据上报服务器、或数据采集功能的服务,本申请实施例不作限定。

[0089] 可以理解的是,当内核层发生安全事件时,终端可以通过预设上报通道将事件信息传递至用户层,并由用户层的专门的用户进程进行事件信息的接收、解析和服务器上报,从而实现了内核层的埋点数据上报,使得内核层发生的安全事件可以及时上报至服务器进行进一步的分析,提高了终端的安全性。

[0090] 在本申请的一些实施例中,参见图5,图5为本申请实施例提供的数据上报方法的一个可选的流程示意图,基于图3,在S1011之前,还可以执行S201-S202,如下:

[0091] S201、在内核层的初始化阶段,实现数据上报模块中的内核发送子模块和内核接收子模块,并创建预设上报通道。

[0092] 本申请实施例中,终端会在系统启动阶段首先进行内核层的初始化,终端在内核层初始化阶段的主要工作是完成预设上报通道如Netlink套接字的建立,以及对内核发送子模块和内核接收子模块进行初始化,使内核层中的数据上报模块具备内核层数据的发送和接收功能。

[0093] 本申请实施例中,内核发送子模块与内核接收子模块可以分别实现对内核数据的发送功能和接收功能。

[0094] S202、在用户层的初始化阶段,实现用户层的用户发送模块和用户接收模块,并启动用户进程,通过用户进程打开预设上报通道,完成预设上报通道的启动。

[0095] 本申请实施例中,在内核层初始化完成后,终端进入用户层的初始化阶段,终端在用户层初始化阶段的主要工作是启动用户进程,并通过用户进程打开内核层初始化阶段所创建的预设上报通道,如打开内核层创建的Netlink套接字,从而启动预设上报通道,以使后续数据上报模块能够直接利用预设上报通道进行事件信息的传输。

[0096] 本申请实施例中,终端在用户层的初始化阶段还会实现用户层中的用户发送模块和用户接收模块,从而可以通过用户进程对用户发送模块和用户接收模块的调用,实现用户层数据的发送和接收功能。

[0097] 本申请实施例中,用户发送模块与用户接收模块可以分别实现对用户层数据的发送功能和接收功能。

[0098] 可以理解的是,本申请实施例中,终端在系统初始化阶段即可完成预设上报通道的建立以及内核层、用户层相关接收和发送的功能实现,使得终端在初始化完成后即具备了内核层数据的上报功能,并使得内核层发生的安全事件可以得到及时上报,从而提高了终端的安全性。

[0099] 在本申请的一些实施例中,参见图6,图6为本申请实施例提供的数据上报方法的一个可选的流程示意图,基于图3或图5,在S1011之前,还可以执行S301-S303,如下:

[0100] S301、获取用户进程的进程标识。

[0101] 本申请实施例中,在用户层的初始化阶段,终端启动用户进程后,可以获取到系统

为用户进程分配的进程标识。

[0102] 在本申请的一些实施例中,进程标识用于唯一的标识出用户进程,其可以是用户进程的PID,也可以是其他可以唯一表征用户进程的标识形式,本申请实施例不作限定。对于PID形式的进程标识,终端系统中每启动一个进程都会创建该进程对应的PID,PID是终端系统中各进程的代号,每个进程有唯一的PID编号,进程在运行时其PID不会发生变化,进程终止后PID被系统回收。

[0103] S302、利用用户进程调用用户发送模块,将进程标识通过预设上报通道发送给数据上报模块。

[0104] 本申请实施例中,终端利用用户进程调用用户发送模块,将进程标识通过已经启用的预设上报通道发送给内核层的数据上报模块。

[0105] S303、通过数据上报模块的内核接收子模块接收进程标识,并保存在内核层。

[0106] 本申请实施例中,终端通过数据上报模块中的内核接收子模块接收用户进程发送的进程标识,并将进程标识保存在内核层,以备后续发送事件信息时,可以将事件信息发送至进程标识所对应的用户进程。

[0107] 需要说明的是,S201-S202中所述的内核层和用户层的初始化过程,以及S301-S303中所述的进程标识的传递过程都是在S101之前进行的操作,可以根据不同的终端系统初始化流程以对应的顺序结合执行。示例性的,对于linux系统以及以linux系统为内核的Android系统、Tizen系统、Kubuntu系统、Ubuntu系统、Kylin系统等系统,内核层的初始化和用户层的初始化都是在系统启动阶段进行的,且内核层的初始化先于用户层的初始化。因此,用户进程的进程标识的传递可在用户层的初始化后进行,对于其他类型的终端系统,S201-S202以及S301-S303中的步骤可以根据具体系统的初始化流程以相应的顺序结合执行,本申请实施例不作限定。

[0108] 可以理解的是,本申请实施例中,用户进程通过将进程标识发送给内核层的数据上报模块,数据上报模块在进行内核层安全事件的上报时即可对应将事件信息发送至专门的用户进程,并由用户进程继续进行下一步的上报处理,这样不仅实现了事件信息从内核层至用户层的传递,也使得用户层可以通过专门的用户进程对事件信息进行接收、解析和上报,从而提高了终端的安全性。

[0109] 在本申请的一些实施例中,参见图7,图7为本申请实施例提供的数据上报方法的一个可选的流程示意图,基于图3,图3示出的S1011可以通过S10111-S10112实现,将结合各步骤进行说明。

[0110] S10111、当通过内核层的第一检测模块,检测到内核层中运行的可执行文件的安全上下文不对应时,确定内核层发生执行类型的安全事件。

[0111] 本申请实施例中,终端可以通过内核层中的第一检测模块,对内核层中运行的可执行文件进行检测,当可执行文件的安全上下文不对应时,说明该可执行文件的上下文环境不安全,存在恶意程序通过该可执行文件非法调用系统高级权限的风险,因此终端确定内核层发生执行类型的安全事件。

[0112] 本申请实施例中,内核层的检测模块包含第一检测模块,第一检测模块用于对可执行文件的安全上下文进行检测。

[0113] 本申请实施例中,可执行文件(executable file)指的是可以由操作系统进行加

载执行的文件。示例的,在不同的操作系统环境下,可执行程序的呈现方式不一样。在视窗(Windows)操作系统下,可执行程序可以是.exe文件、.sys文件、.com等类型文件。在Linux操作系统下,可执行程序的文件格式为可执行可链接格式(Executable and Linkable Format,ELF)。

[0114] 本申请实施例中,安全上下文指的是一类定义某个进程允许做什么的许可和权限的集合。例如权限、特权、访问令牌、完整性等级等等都会包含在其中。每一个进程或服务都会在操作系统里注册自己的安全上下文,如果某个可执行文件或执行进程没有安全上下文或是安全上下文不对应,表示该可执行文件没有在操作系统注册或是文件内容被非法篡改,为来路不明的文件,极有可能是恶意程序。

[0115] 在本申请的一些实施例中,对于Linux系统,当用户层的可执行文件被调用时,会发起系统调用exec过程,其中,系统调用exec过程会替换原进程上下文的内容,以新的进程去代替原来的进程,但进程的PID保持不变,从而实现在一个进程中启动另一个程序执行的方法。因此,一些恶意程序可能会利用exec的这种调用方式,在正常的可执行文件运行过程中发起对内核层的恶意提权。因此,本申请实施例中的终端可以相应的通过第一检测模块,对可执行文件的安全上下文进行检测,将安全上下文不对应的情况作为执行类型的安全事件进行及时上报。

[0116] S10112、获取执行类型的安全事件对应的执行类型的事件信息,并通过内核发送子模块,将执行类型的事件信息发送至数据上报模块。

[0117] 本申请实施例中,终端在通过第一检测模块,确认内核层发生执行类型的安全事件时,终端获取执行类型的安全事件对应的执行类型的事件信息,并通过第一检测模块调用内核发送子模块,将执行类型的事件信息发送至数据上报模块。

[0118] 在本申请的一些实施例中,参见图8,图8为本申请实施例提供的数据上报方法的一个可选的流程示意图,图3示出的S1011可以通过S10113-S10114实现,将结合各步骤进行说明。

[0119] S10113、当通过内核层的第二检测模块,检测到内核层的系统调用指令在执行后出现调用权限变化时,确认内核层发生提权类型的安全事件。

[0120] 本申请实施例中,终端可以通过内核层中的第二检测模块,对内核层中运行的系统调用指令进行检测,当系统调用指令在执行后出现调用权限变化时,说明该系统调用指令可能在调用过程中提取了原权限之外的高级权限,因此终端可以确认内核层发生提权类型的安全事件。

[0121] 本申请实施例中,检测模块包含第二检测模块,第二检测模块用于对系统调用指令的调用权限进行检测。

[0122] 本申请实施例中,用户层在调用系统调用指令时,实际系统调用会在内核层中执行,在系统调用指令被执行前,第二检测模块可以获取并保存该系统调用指令对应的调用权限,再执行该系统调用指令,并在该系统调用指令被执行后重新获取调用权限,对比调用权限是否已经发生改变。若调用权限发生变化,说明该系统调用指令极有可能曾经参与了提权操作,非法提取了系统的高级权限,具有破坏性,则终端确认内核层发生提权类型的安全事件。

[0123] 在本申请的一些实施例中,对于Linux系统,root权限为系统权限的一种,是整个

系统的最高权限,一般Linux系统中的超级管理员用户帐户拥有root权限,可方便地对于系统中的任何文件(包括系统文件)执行所有增、删、改、查的操作。对于Linux系统的系统调用指令,第二检测模块可以获取该系统调用指令在执行前的进程信息中的UID、EUID、FSUID等,若此时UID的值为非零值,表征终端处于未解锁状态,第二检测模块在该系统调用指令被执行后重新获取进程信息中的UID、EUID、FSUID等,若此时UID的值为零,表征终端已经被root,内核层中的文件处于未被保护的状态,则终端确认内核层发生提权类型的安全事件。

[0124] S10114、获取提权类型的安全事件对应的提权类型的事件信息,并通过内核发送子模块,将提权类型的事件信息发送至数据上报模块。

[0125] 本申请实施例中,终端在通过第二检测模块,确认内核层发生提权类型的安全事件时,终端获取提权类型的安全事件对应的提权类型的事件信息,并通过第二检测模块调用内核发送子模块,将提权类型的事件信息发送至数据上报模块。

[0126] 在本申请的一些实施例中,参见图9,图9为本申请实施例提供的数据上报方法的一个可选的流程示意图,图3示出的S1011可以通过S10115-S10116实现,将结合各步骤进行说明。

[0127] S10115、当通过内核层的第三检测模块,检测到内核层的分区挂载指令在执行后出现预设系统分区读写权限变化时,确认内核层发生挂载类型的安全事件。

[0128] 本申请实施例中,终端可以通过内核层中的第三检测模块,对内核层中运行的分区挂载指令进行检测,当分区挂载指令在执行后出现预设系统分区读写权限变化时,说明该分区挂载指令可能在调用过程中修改了其挂载点的读写权限。示例性的,当挂载点为内核中重要的预设系统分区,如linux系统中的system或vendor分区时,由于system或vendor分区中保存了终端大量应用程序的数据,如果恶意程序将system或vendor分区挂载为可读可写的权限,就可以对终端中的应用程序进行任意操作。因此当内核层的分区挂载指令在执行后出现预设系统分区读写权限变化时,终端可以确认内核层发生挂载类型的安全事件。

[0129] 本申请实施例中,检测模块包含第三检测模块,第三检测模块用于对分区挂载指令对应的分区读写权限进行检测。

[0130] 本申请实施例中,第三检测模块可以对分区挂载指令中传入的参数,如挂载的分区名、挂载的标志位等进行判断,如果挂载的分区名为预设系统分区的分区名,挂载的标志位为可读可写的读写权限,则确定内核层发生挂载类型的安全事件。

[0131] S10116、获取挂载类型的安全事件对应的挂载类型的事件信息,并通过内核发送子模块,将挂载类型的事件信息发送至数据上报模块。

[0132] 本申请实施例中,终端在通过第三检测模块,确认内核层发生挂载类型的安全事件时,终端获取挂载类型的安全事件对应的挂载类型的事件信息,并通过第一检测模块调用内核发送子模块,将挂载类型的事件信息发送至数据上报模块。

[0133] 可以理解的是,本申请实施例中,终端可以通过第一、第二和第三检测模块,对内核层中发生的多种安全事件进行及时有效的检测和上报,从而能够尽快发现内核层中可能存在的恶意程序,提高了终端的安全性。

[0134] 在本申请的一些实施例中,基于图6,图3示出的S1012中通过数据上报模块将事件信息传入内核层与用户层之间的预设上报通道可以通过S10121实现,将结合各步骤进行说

明。

[0135] S10121、根据保存的进程标识,利用数据上报模块的内核发送子模块,将事件信息传入预设上报通道,以指定用户层通过进程标识对应的用户进程接收事件信息。

[0136] 本申请实施例中,基于内核层中保存的进程标识,数据上报模块在将事件信息向用户层发送时,会通过内核发送子模块发出发送指令,并在发送指令中将进程标识作为事件信息的接收方,从而实现将事件信息传入预设上报通道,以指定用户层通过进程标识对应的用户进程接收事件信息。

[0137] 在本申请的一些实施例中,当预设上报通道为Netlink套接字时,内核发送子模块使用事件信息作为发送数据,使用进程标识PID作为目的地址,对Netlink消息结构进行填充,得到一个Netlink消息,并调用sendmsg()函数将该Netlink消息写入Netlink套接字对应在内核层的输入缓冲区,再由Netlink协议将事件信息从输入缓冲区发送至该Netlink套接字在用户层的输出缓冲区,以供用户层的用户进程从输出缓冲区中周期性获取事件信息。

[0138] 在本申请的一些实施例中,基于图6,图3示出的S1013可以通过S10131实现,将结合各步骤进行说明。

[0139] S10131、结合进程标识,通过用户进程调用用户接收模块,周期性的从预设上报通道中读取事件信息。

[0140] 本申请实施例中,终端可以通过用户进程调用用户接收模块,周期性的对预设上报通道中进行读取,当预设上报通道中存在与进程标识对应的事件信息时,说明该事件信息是内核层主动上报给用户进程的,用户进程通过用户接收模块,对该事件信息进行获取。

[0141] 在本申请的一些实施例中,当预设上报通道为Netlink套接字时,用户接收模块通过调用recvmsg()函数,从输出缓冲区中获取事件信息。

[0142] 可以理解的是,本申请实施例中,终端通过进程标识将事件信息指定给用户进程进行获取,从而实现了事件信息的单播传递,提高了终端的安全性。

[0143] 在本申请的一些实施例中,参见图10,图10为本申请实施例提供的数据上报方法的一个可选的流程示意图,图4示出的S1021可以通过S10211-S10215实现,将结合各步骤进行说明。

[0144] S10211、通过用户进程,从事件信息中解析出事件类型。

[0145] 本申请实施例中,用户层的解析模块也是在用户层的初始化阶段完成功能实现的,当终端通过用户接收模块获取到内核层传递的安全事件的事件信息时,终端通过用户进程调用解析模块,从事件信息中解析出每个事件信息对应的事件类型。

[0146] S10212、当事件类型为执行类型时,通过用户进程,将事件信息保存在预设链表中;并根据预设时间间隔,将预设链表中的事件信息保存至本地日志中。

[0147] 本申请实施例中,当事件类型为执行类型时,说明内核层中出现了可执行文件的安全上下文不对应的安全问题,终端通过用户进程调用用户层的保存模块,将事件信息保存在预设链表中。其中,保存模块也是在用户层的初始化阶段完成功能实现的。

[0148] 本申请实施例中,由于终端在正常工作时,可执行文件运行次数较多,因此执行类型的安全事件发生会较为频繁,因此为了避免频繁对本地日志进行写入操作,终端会先将事件信息保存在预设链表中,每隔预设的时间间隔,或是预设链表存储空间已满时,或是出

现其他事件类型的安全事件,如挂载类型的安全事件时,再将预设链表中的事件信息转入本地日志中保存,以便后续将本地日志上传至后台服务器。

[0149] S10213、当事件类型为提权类型时,通过用户进程获取事件信息对应的应用包名,将应用包名与事件信息保存至本地日志中,并通过用户进程调用弹框在终端界面进行提示。

[0150] 本申请实施例中,当事件类型为提权类型时,说明有系统调用指令非法调取了最高系统权限,这类安全事件的安全风险很高,终端会通过用户进程进一步获取该事件信息对应的应用包名,即发起系统调用指令的应用名称,然后通过保存模块,将应用包名与对应的事件信息共同保存在本地日志中。

[0151] 本申请实施例中,提权类型的事件信息对应的应用包名表征可能存在非法获取系统最高权限行为的恶意程序。终端将应用包名与事件信息共同进行保存,以便后续共同上传至后台服务器,并在后台服务器端对此类恶意程序进行追溯。

[0152] 本申请实施例中,由于提权类型的安全事件存在较高的安全风险,因此终端会进一步通过用户进程,调用用户层中负责界面显示的弹框模块,在终端界面进行弹框提示,以向使用者进行告警,提醒使用者当前有高风险程序正在调取系统最高权限。

[0153] S10214、当事件类型为挂载类型时,将事件信息保存至本地日志中。

[0154] 本申请实施例中,当事件类型为挂载类型时,说明有分区挂载指令非法篡改了预设系统分区的读写权限,终端通过保存模块,将挂载类型的事件信息保存在本地日志中。

[0155] S10215、通过数据采集服务,将本地日志上报至后台服务器,以供后台服务器进行分析处理。

[0156] 本申请实施例中,终端会通过数据采集服务,定期将本地日志上报至后台服务器,后台服务器端可以对应有人工或自动的分析机制,对本地日志中包含的安全事件的相关信息进行分析处理,从中定位出终端上的恶意程序,以及终端上的安全漏洞,以对终端的安全性进行进一步的优化和提升。

[0157] 可以理解的是,本申请实施例中,终端通过对不同事件类型的事件信息进行保存和上报处理,实现了对内核层的安全事件内容的并行处理,并且对安全级别高的安全事件可以及时进行界面提示,从而提高了终端的安全性。

[0158] 下面结合一个具体实施例对上述数据上报系统及对应的数据上报方法进行说明,然而值得注意的是,该具体实施例仅是为了更好地说明本申请,并不构成对本申请的不当限定。

[0159] 参见图11,图11为本申请实施例提供的在数据上报系统中进行内核安全事件上报的一个可选的流程示意图,其中数据上报系统包括后台服务器10以及终端20,其中,终端20包含用户层210与内核层220,用户层210中包含弹框模块610、本地日志文件620和数据采集服务630;内核层220中包含检测模块700与数据上报模块800,用户层210和内核层220之间的预设上报通道为Netlink套接字。其中,用户层210还包括用户发送模块600_1、用户接收模块600_2、解析模块600_3和保存模块600_4;数据上报模块800包括内核发送子模块800_1,内核接收子模块800_2;检测模块700包括第一检测模块700_1、第二检测模块700_2以及第三检测模块700_3。在Android系统中,用户发送模块600_1可以为Userspace_send模块;用户接收模块600_2可以为Userspace_receive模块;内核发送子模块800_1可以为

Kernelspace_send模块;解析模块600_3可以为Userspace_parse模块;保存模块600_4可以为Userspace_record模块;本地日志文件620可以是Userspace_log文件;第一检测模块700_1可以为Kernelspace_exec_check模块;第二检测模块700_2可以为Kernelspace_root_check模块;第三检测模块700_3可以为Kernelspace_mount_check模块。下面将结合图11示出的步骤进行说明:

[0160] S401、在内核层220与用户层210初始化完毕,并且Netlink套接字被正常启用后,通过用户进程调用Userspace_send模块,将用户进程的PID发送至数据上报模块800的Userspace_receive模块。

[0161] S402、数据上报模块800通过Userspace_receive模块接收用户进程PID,并保存在数据上报模块800中。

[0162] S403、当检测模块700中的Kernelspace_exec_check模块、Kernelspace_root_check模块以及Kernelspace_mount_check模块检测到内核层220中发生安全事件时,调用Kernelspace_send模块将事件信息上报至数据上报模块800。

[0163] 在本申请的一些实施例中,Kernelspace_exec_check用于对可执行文件安全上下文进行检测;Kernelspace_root_check用于对系统调用指令是否获取了Android系统的root权限进行检测;Kernelspace_mount_check用于对分区挂载指令是否修改了Android系统分区如system、vendor目录的读写权限进行检测。

[0164] S404、Kernelspace_send模块通过Netlink套接字,将事件信息上报至用户层210,指定发送给PID所对应的用户进程。

[0165] S405、通过用户进程调用Userspace_receive模块,从Netlink套接字中接收事件信息。

[0166] S406、Userspace_receive模块将接收到的事件信息传递给Userspace_parse模块。

[0167] S407、通过Userspace_parse模块对事件信息进行解析,得到事件信息对应的事件类型,并将解析后的事件信息传递给Userspace_record模块。

[0168] S408、若事件类型为提权事件类型,调用用户层210中的弹框模块610在终端界面上进行弹框提示。

[0169] S409、通过用户进程调用Userspace_record模块将事件信息保存在Userspace_log中。

[0170] S4010、通过数据采集服务630,定期从Userspace_log中读取事件信息数据。

[0171] S4011、数据采集服务630将从Userspace_log中读取到的事件信息上报至后台服务器10。

[0172] 可以理解的是,本申请实施例中,终端可以通过Kernelspace_exec_check模块、Kernelspace_root_check模块以及Kernelspace_mount_check模块,对内核层中发生的多种安全事件进行检测,并且可以使用Kernelspace_send模块通过Netlink套接字进行及时上报,从而能够尽快发现内核层中可能存在的恶意程序并传递至用户层,进一步的,用户层的Userspace_receive模块在接收到事件信息后,可以通过Userspace_parse模块对事件信息进行解析,对高风险的安全事件可以及时进行界面提示,并可以通过Userspace_record模块对不同事件类型的事件信息进行保存和上报处理,从而实现了内核层的埋点数据上

报,使得内核层发生的安全事件可以及时上报至后台服务器进行进一步的分析,提高了终端的安全性。

[0173] 在本申请的一些实施例中,不同安全事件的事件类型可以对应不同的事件ID,参见图12,图12为本申请实施例提供的数据上报方法的一个可选的流程示意图。基于图11,在S407之后,还可以执行S501-S508来替代S408-S4011,如下:

[0174] S501、通过Userspace_parse模块,根据事件ID判断安全事件的事件类型。

[0175] S502、当事件ID表征事件类型为执行类型时,通过Userspace_record模块,将事件信息保存在预设链表中。

[0176] S503、通过Userspace_record模块,根据预设时间间隔,将预设链表中的事件信息保存至Userspace_log中。

[0177] 本申请实施例中,S502-S503中的方法与S10212描述一致,此处不再赘述。

[0178] S504、当事件ID表征事件类型为提权类型时,通过用户进程获取事件信息对应的应用包名。

[0179] S505、通过Userspace_record模块,将应用包名与事件信息保存至Userspace_log中。

[0180] S506、通过用户进程,调用弹框模块610在终端界面进行弹框提示。

[0181] 本申请实施例中,S504-S505中的方法与S10213描述一致,此处不再赘述。

[0182] S507、当事件ID表征事件类型为挂载类型时,通过Userspace_record模块,将事件信息保存至Userspace_log中。

[0183] 本申请实施例中,S507中的方法与S10214描述一致,此处不再赘述。

[0184] S508、通过数据采集服务630,将Userspace_log上报至后台服务器10,以供后台服务器10进行分析处理。

[0185] 本申请实施例中,S508中的方法与S10215描述一致,此处不再赘述。

[0186] 可以理解的是,本申请实施例中,终端可以根据不同事件类型,对内核层的安全事件进行并行处理,并且,终端可以通过扩展事件类型的事件ID实现对内核上报数据的扩展,不仅可上报安全事件的数据,也可上报其他类型事件的数据,从而提高了数据上报系统的可扩展性和可维护性,使得数据上报系统能够上报更多类型的内核事件,最终提高了终端的安全性。

[0187] 基于前述的实施例,本申请实施例再提供一种数据上报装置,所述数据上报装置包括所包括的各模块、以及各模块所包括的各单元,可以通过终端中的处理器来实现;当然也可通过具体的逻辑电路实现;在实施的过程中,处理器可以为中央处理器(Central Processing Unit,CPU)、微处理器(Micro Processing Unit,MPU)、数字信号处理器(Digital Signal Processor,DSP)或现场可编程门阵列(Field Programmable Gate Array,FPGA)等。

[0188] 参见图13,图13为本申请实施例提供的数据上报装置的一个可选的组成结构示意图,所述数据上报装置900包括内核层910和用户层920,其中:

[0189] 所述内核层910,用于当检测到内核层发生安全事件时,将所述安全事件的事件信息传输至用户层;

[0190] 所述用户层920,用于将所述事件信息上报至后台服务器。

[0191] 在本申请的一些实施例中,所述内核层910,还用于当检测到内核层发生安全事件时,将所述安全事件的事件信息传输至所述内核层的数据上报模块;以及通过所述数据上报模块将所述事件信息传入所述内核层与用户层之间的预设上报通道,所述事件信息包含事件类型;

[0192] 所述用户层920,用于通过用户进程,从所述预设上报通道中获取所述事件信息。

[0193] 在本申请的一些实施例中,所述用户层920,还用于通过所述用户进程,根据所述事件信息的事件类型,执行对所述事件信息的上报处理,以将所述事件信息上报至后台服务器。

[0194] 在本申请的一些实施例中,所述内核层910,还用于在所述内核层的初始化阶段,实现所述数据上报模块中的内核发送子模块和内核接收子模块,并创建所述预设上报通道;

[0195] 所述用户层920,还用于在所述用户层的初始化阶段,实现所述用户层的用户发送模块和用户接收模块,并启动所述用户进程,通过所述用户进程打开所述预设上报通道,完成所述预设上报通道的启动。

[0196] 在本申请的一些实施例中,所述用户层920,还用于获取所述用户进程的进程标识;以及利用所述用户进程调用所述用户发送模块,将所述进程标识通过所述预设上报通道发送给所述数据上报模块;

[0197] 所述内核层910,还用于通过所述数据上报模块的内核接收子模块接收所述进程标识,并保存在所述内核层。

[0198] 在本申请的一些实施例中,所述内核层910,还用于根据保存的所述进程标识,利用所述数据上报模块的内核发送子模块,将所述事件信息传入所述预设上报通道,以指定所述用户层通过所述进程标识对应的用户进程接收所述事件信息。

[0199] 在本申请的一些实施例中,所述用户层920,还用于结合所述进程标识,通过所述用户进程调用所述用户接收模块,周期性的从所述预设上报通道中读取所述事件信息。

[0200] 在本申请的一些实施例中,所述用户层920,还用于通过所述用户进程,从所述事件信息中解析出所述事件类型;以及当所述事件类型为执行类型时,将所述事件信息保存在预设链表中;并根据预设时间间隔,将所述预设链表中的事件信息保存至本地日志中;以及当所述事件类型为提权类型时,获取所述事件信息对应的应用包名,将所述应用包名与所述事件信息保存至所述本地日志中,并通过所述用户进程调用弹框在终端界面进行提示;以及当所述事件类型为挂载类型时,将所述事件信息保存至本地日志中;通过数据采集服务,将所述本地日志上报至后台服务器,以供所述后台服务器进行分析处理。

[0201] 在本申请的一些实施例中,所述内核层910,还用于当通过所述内核层的第一检测模块,检测到所述内核层中运行的可执行文件的安全上下文不对应时,确定所述内核层发生执行类型的安全事件;以及获取所述执行类型的安全事件对应的执行类型的事件信息,并通过所述内核发送子模块,将所述执行类型的事件信息发送至所述数据上报模块。

[0202] 在本申请的一些实施例中,所述内核层910,还用于当通过所述内核层的第二检测模块,检测到所述内核层的系统调用指令在执行后出现调用权限变化时,确认所述内核层发生提权类型的安全事件;以及获取所述提权类型的安全事件对应的提权类型的事件信息,并通过所述内核发送子模块,将所述提权类型的事件信息发送至所述数据上报模块。

[0203] 在本申请的一些实施例中,所述内核层910,还用于当通过所述内核层的第三检测模块,检测到所述内核层的分区挂载指令在执行后出现预设系统分区读写权限变化时,确认所述内核层发生挂载类型的安全事件;以及获取所述挂载类型的安全事件对应的挂载类型的事件信息,并通过所述内核发送子模块,将所述挂载类型的事件信息发送至所述数据上报模块。

[0204] 这里需要指出的是:以上装置实施例的描述,与上述方法实施例的描述是类似的,具有同方法实施例相似的有益效果。对于本申请装置实施例中未披露的技术细节,请参照本申请方法实施例的描述而理解。

[0205] 需要说明的是,本申请实施例中,如果以软件功能模块的形式实现上述数据上报方法,并作为独立的产品销售或使用时,也可以存储在一个计算机可读取存储介质中。基于这样的理解,本申请实施例的技术方案本质上或者说对相关技术做出贡献的部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质中,包括若干指令用以使得终端(可以是具有摄像头的智能手机、平板电脑等)执行本申请各个实施例所述方法的全部或部分。而前述的存储介质包括:U盘、移动硬盘、只读存储器(Read Only Memory,ROM)、磁碟或者光盘等各种可以存储程序代码的介质。这样,本申请实施例不限制于任何特定的硬件和软件结合。

[0206] 对应地,本申请实施例提供一种计算机可读存储介质,其上存储有计算机程序,该计算机程序被处理器执行时实现上述实施例中任一所述数据上报方法中的步骤。

[0207] 在本申请的一些实施例中,计算机可读存储介质可以是FRAM、ROM、PROM、EPROM、EEPROM、闪存、磁表面存储器、光盘、或CD-ROM等存储器;也可以是包括上述存储器之一或任意组合的各种设备。

[0208] 对应地,本申请实施例中,还提供了一种芯片,所述芯片包括可编程逻辑电路和/或程序指令,当所述芯片运行时,用于实现上述实施例中任一所述数据上报方法中的步骤。

[0209] 对应地,本申请实施例中,还提供了一种计算机程序产品,当该计算机程序产品被终端的处理器执行时,其用于实现上述实施例中任一所述数据上报方法中的步骤。

[0210] 对应地,本申请实施例中,还提供了一种芯片,所述芯片包括可编程逻辑电路和/或程序指令,当所述芯片运行时,用于实现上述实施例中任一所述数据上报方法中的步骤。

[0211] 对应地,本申请实施例中,还提供了一种计算机程序产品,当该计算机程序产品被终端的处理器执行时,其用于实现上述实施例中任一所述数据上报方法中的步骤。

[0212] 在本申请的一些实施例中,计算机程序产品可以采用程序、软件、软件模块、脚本或代码的形式,按任意形式的编程语言(包括编译或解释语言,或者声明性或过程性语言)来编写,并且其可按任意形式部署,包括被部署为独立的程序或者被部署为模块、组件、子例程或者适合在计算环境中使用的其它单元。

[0213] 作为示例,计算机程序产品可以但不一定对应于文件系统中的文件,可以可被存储在保存其它程序或数据的文件的一部分,例如,存储在超文本标记语言(HTML,Hyper Text Markup Language)文档中的一个或多个脚本中,存储在专用于所讨论的程序的单个文件中,或者,存储在多个协同文件(例如,存储一个或多个模块、子程序或代码部分的文件)中。

[0214] 作为示例,计算机程序产品可被部署为在一个计算设备上执行,或者在位于一个

地点的多个计算设备上执行,又或者,在分布在多个地点且通过通信网络互连的多个计算设备上执行。

[0215] 基于同一技术构思,本申请实施例提供一种终端,用于实施上述方法实施例记载的数据上报方法。图14为本申请实施例提供的一种终端的硬件实体示意图,如图14所示,所述终端1100包括存储器1110和处理器1120,所述存储器1110存储有可在处理器1120上运行的计算机程序,所述处理器1120执行所述程序时实现本申请实施例任一所述数据上报方法中的步骤。

[0216] 存储器1110配置为存储由处理器1120可执行的指令和应用,还可以缓存待处理器1120以及终端中各模块待处理或已经处理的数据(例如,图像数据、音频数据、语音通信数据和视频通信数据),可以通过闪存(FLASH)或随机访问存储器(Random Access Memory,RAM)实现。

[0217] 处理器1120执行程序时实现上述任一项的会话检测方法的步骤。处理器1120通常控制终端1100的总体操作。

[0218] 上述处理器可以为特定用途集成电路(Application Specific Integrated Circuit,ASIC)、数字信号处理器(Digital Signal Processor,DSP)、数字信号处理装置(Digital Signal Processing Device,DSPD)、可编程逻辑装置(Programmable Logic Device,PLD)、现场可编程门阵列(Field Programmable Gate Array,FPGA)、中央处理器(Central Processing Unit,CPU)、控制器、微控制器、微处理器中的至少一种。可以理解地,实现上述处理器功能的电子器件还可以为其它,本申请实施例不作具体限定。

[0219] 上述计算机存储介质/存储器可以是只读存储器(Read Only Memory,ROM)、可编程只读存储器(Programmable Read-Only Memory,PROM)、可擦除可编程只读存储器(Erasable Programmable Read-Only Memory,EPROM)、电可擦除可编程只读存储器(Electrically Erasable Programmable Read-Only Memory,EEPROM)、磁性随机存取存储器(Ferromagnetic Random Access Memory,FRAM)、快闪存储器(Flash Memory)、磁表面存储器、光盘、或只读光盘(Compact Disc Read-Only Memory,CD-ROM)等存储器;也可以是包括上述存储器之一或任意组合的各种终端,如移动电话、计算机、平板设备、个人数字助理等。

[0220] 这里需要指出的是:以上存储介质和设备实施例的描述,与上述方法实施例的描述是类似的,具有同方法实施例相似的有益效果。对于本申请存储介质和设备实施例中未披露的技术细节,请参照本申请方法实施例的描述而理解。

[0221] 综上所述,通过本申请实施例,终端可以通过第一、第二和第三检测模块,对内核层中发生的多种安全事件进行及时有效的检测和上报,从而能够尽快发现内核层中可能存在的恶意程序,进一步的,终端可以通过预设上报通道将事件信息传递至用户层,并由用户层的专门的用户进程进行事件信息的接收、解析,对不同事件类型的事件信息进行保存和上报处理,实现了对内核层的安全事件内容的并行处理,并且对安全级别高的安全事件可以及时进行界面提示和服务器上报,从而实现了内核层的埋点数据上报,使得内核层发生的安全事件可以及时上报至后台服务器进行进一步的分析,最终提高了终端的安全性。并且,终端可以通过扩展事件类型的事件ID实现对终端安全事件的扩展,从而提高了数据上报系统的可扩展性和可维护性,使得数据上报系统能够上报更多类型的内核事件,进一步

提高了终端的安全性。

[0222] 应理解,说明书通篇中提到的“一个实施例”或“一实施例”意味着与实施例有关的特定特征、结构或特性包括在本申请的至少一个实施例中。因此,在整个说明书各处出现的“在一个实施例中”或“在一实施例中”未必一定指相同的实施例。此外,这些特定的特征、结构或特性可以任意适合的方式结合在一个或多个实施例中。应理解,在本申请的各种实施例中,上述各过程的序号的大小并不意味着执行顺序的先后,各过程的执行顺序应以其功能和内在逻辑确定,而不应对本申请实施例的实施过程构成任何限定。上述本申请实施例序号仅仅为了描述,不代表实施例的优劣。

[0223] 需要说明的是,在本文中,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、物品或者装置不仅包括那些要素,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、物品或者装置所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。

[0224] 在本申请所提供的几个实施例中,应该理解到,所揭露的设备和方法,可以通过其它的方式实现。以上所描述的设备实施例仅仅是示意性的,例如,所述单元的划分,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,如:多个单元或组件可以结合,或可以集成到另一个系统,或一些特征可以忽略,或不执行。另外,所显示或讨论的各组成部分相互之间的耦合、或直接耦合、或通信连接可以是通过一些接口,设备或单元的间接耦合或通信连接,可以是电性的、机械的或其它形式的。

[0225] 上述作为分离部件说明的单元可以是、或也可以不是物理上分开的,作为单元显示的部件可以是、或也可以不是物理单元;既可以位于一个地方,也可以分布到多个网络单元上;可以根据实际的需要选择其中的部分或全部单元来实现本申请实施例方案的目的。

[0226] 另外,在本申请各实施例中的各功能单元可以全部集成在一个处理单元中,也可以是各单元分别单独作为一个单元,也可以两个或两个以上单元集成在一个单元中;上述集成的单元既可以采用硬件的形式实现,也可以采用硬件加软件功能单元的形式实现。

[0227] 或者,本申请上述集成的单元如果以软件功能模块的形式实现并作为独立的产品销售或使用时,也可以存储在一个计算机可读取存储介质中。基于这样的理解,本申请实施例的技术方案本质上或者说对相关技术做出贡献的部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质中,包括若干指令用以使得设备自动测试线执行本申请各个实施例所述方法的全部或部分。而前述的存储介质包括:移动存储设备、ROM、磁碟或者光盘等各种可以存储程序代码的介质。

[0228] 本申请所提供的几个方法实施例中所揭露的方法,在不冲突的情况下可以任意组合,得到新的方法实施例。

[0229] 本申请所提供的几个方法或设备实施例中所揭露的特征,在不冲突的情况下可以任意组合,得到新的方法实施例或设备实施例。

[0230] 以上所述,仅为本申请的实施例而已,并非用于限定本申请的保护范围。凡在本申请的精神和范围之内所作的任何修改、等同替换和改进等,均包含在本申请的保护范围之内。

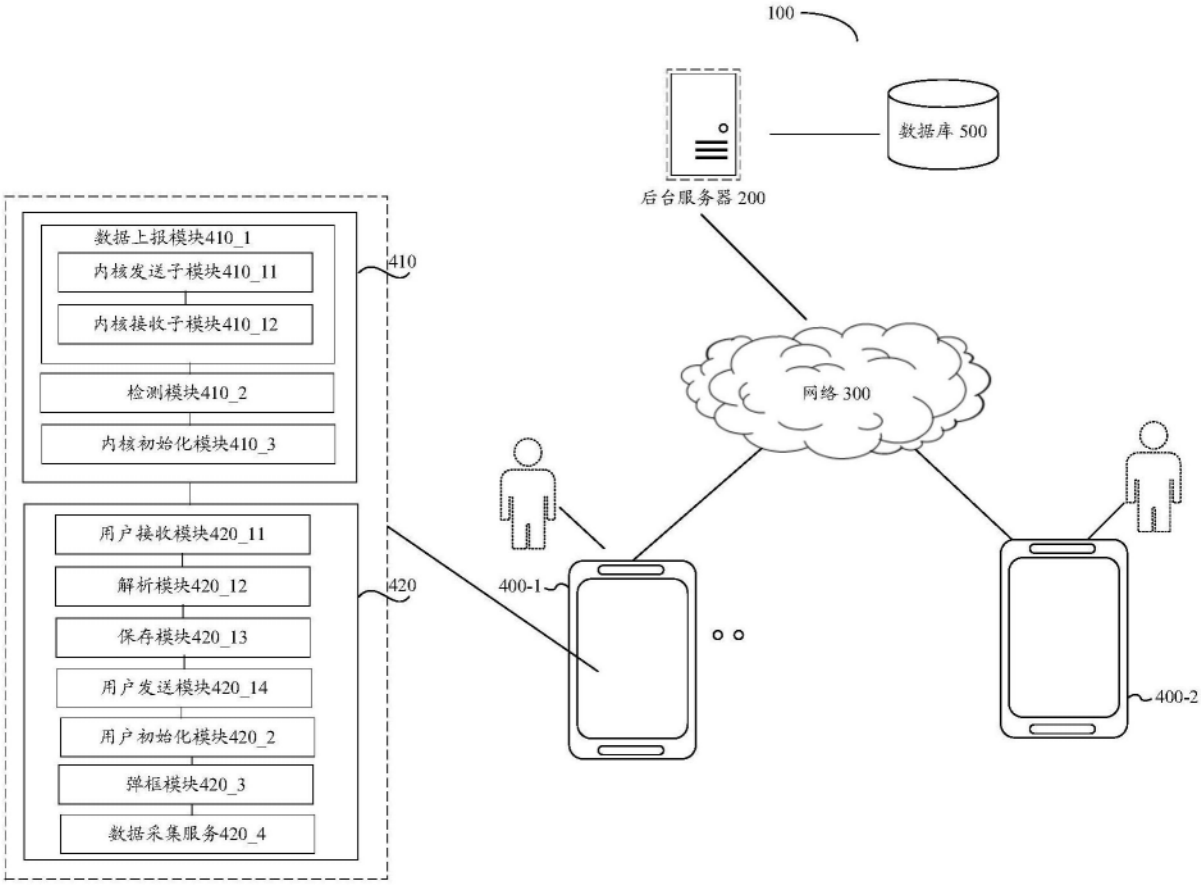

100
数据库 500
后台服务器 200
数据上报模块410_1
内核发送子模块410_11
内核接收子模块410_12
检测模块410_2
内核初始化模块410_3
410
用户接收模块420_11
解析模块420_12
保存模块420_13
用户发送模块420_14
用户初始化模块420_2
弹框模块420_3
数据采集服务420_4
420
网络 300
400-1
400-2

图1

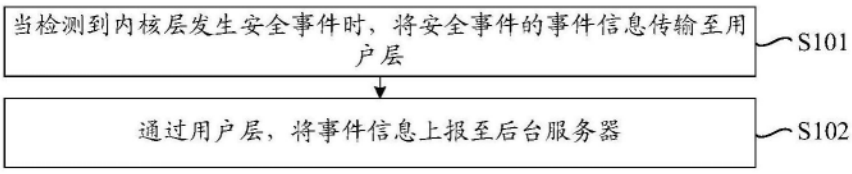

当检测到内核层发生安全事件时，将安全事件的事件信息传输至用户层
S101
通过用户层，将事件信息上报至后台服务器
S102

图2

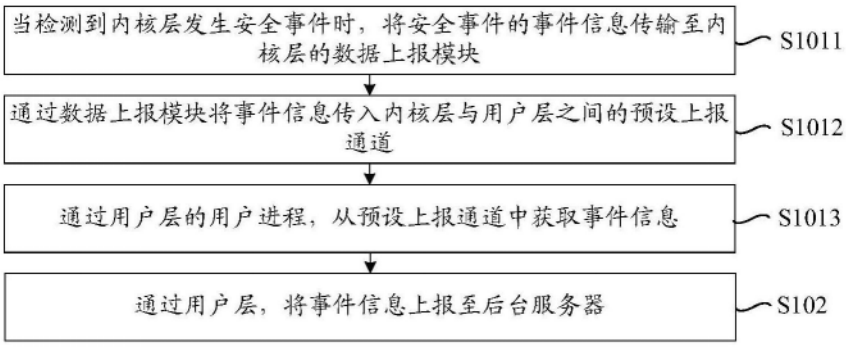

当检测到内核层发生安全事件时，将安全事件的事件信息传输至内核层的数据上报模块
S1011
通过数据上报模块将事件信息传入内核层与用户层之间的预设上报通道
S1012
通过用户层的用户进程，从预设上报通道中获取事件信息
S1013
通过用户层，将事件信息上报至后台服务器
S102

图3

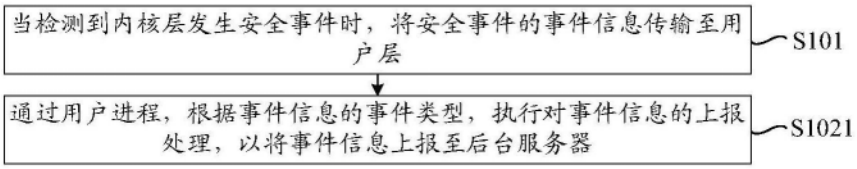

当检测到内核层发生安全事件时，将安全事件的事件信息传输至用户层
S101
通过用户进程，根据事件信息的事件类型，执行对事件信息的上报处理，以将事件信息上报至后台服务器
S1021

图4

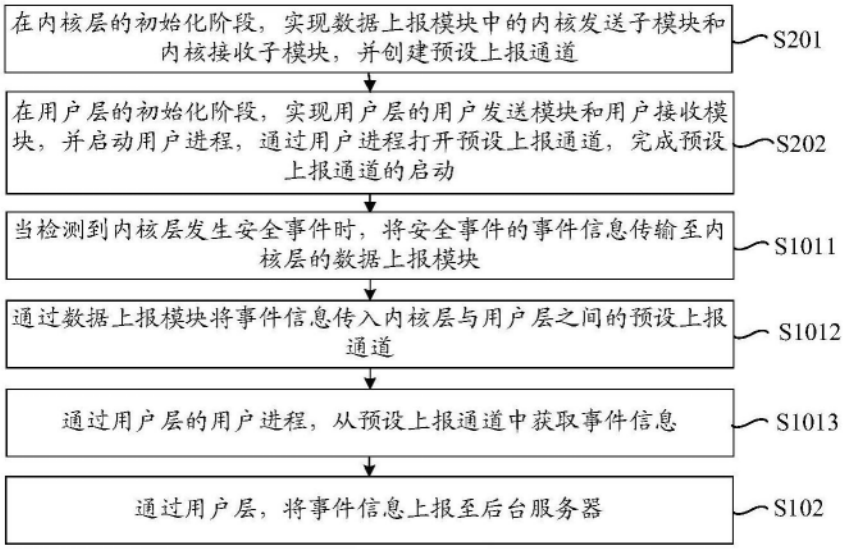

在内核层的初始化阶段，实现数据上报模块中的内核发送子模块和内核接收子模块，并创建预设上报通道
S201
在用户层的初始化阶段，实现用户层的用户发送模块和用户接收模块，并启动用户进程，通过用户进程打开预设上报通道，完成预设上报通道的启动
S202
当检测到内核层发生安全事件时，将安全事件的事件信息传输至内核层的数据上报模块
S1011
通过数据上报模块将事件信息传入内核层与用户层之间的预设上报通道
S1012
通过用户层的用户进程，从预设上报通道中获取事件信息
S1013
通过用户层，将事件信息上报至后台服务器
S102

图5

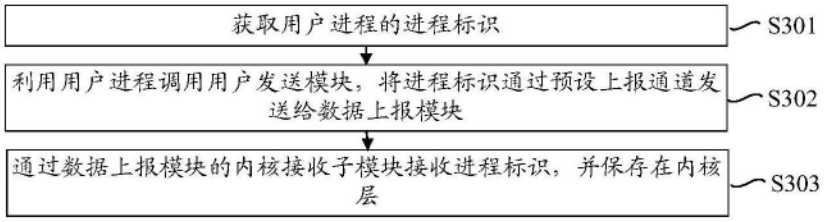

获取用户进程的进程标识
S301
利用用户进程调用用户发送模块，将进程标识通过预设上报通道发送给数据上报模块
S302
通过数据上报模块的内核接收子模块接收进程标识，并保存在内核层
S303

图6

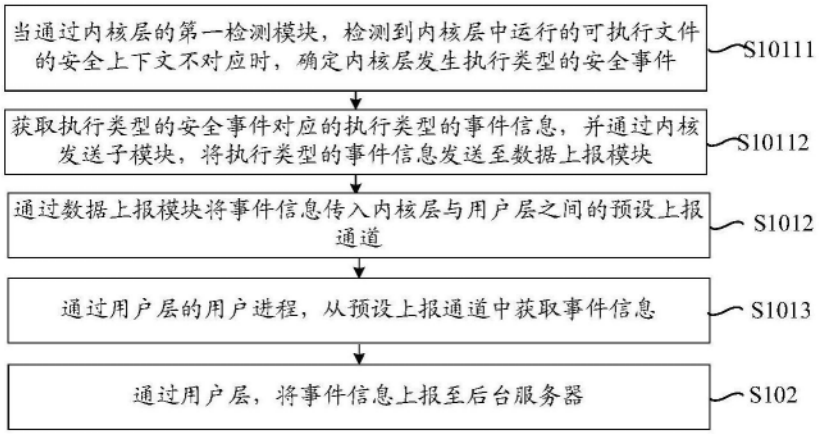

当通过内核层的第一检测模块，检测到内核层中运行的可执行文件的安全上下文不对应时，确定内核层发生执行类型的安全事件
S10111
获取执行类型的安全事件对应的执行类型的事件信息，并通过内核发送子模块，将执行类型的事件信息发送至数据上报模块
S10112
通过数据上报模块将事件信息传入内核层与用户层之间的预设上报通道
S1012
通过用户层的用户进程，从预设上报通道中获取事件信息
S1013
通过用户层，将事件信息上报至后台服务器
S102

图7

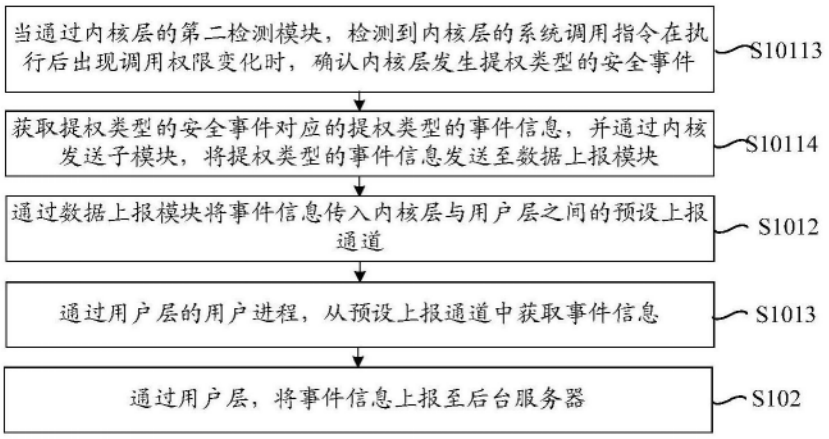

当通过内核层的第二检测模块，检测到内核层的系统调用指令在执行后出现调用权限变化时，确认内核层发生提权类型的安全事件
S10113
获取提权类型的安全事件对应的提权类型的事件信息，并通过内核发送子模块，将提权类型的事件信息发送至数据上报模块
S10114
通过数据上报模块将事件信息传入内核层与用户层之间的预设上报通道
S1012
通过用户层的用户进程，从预设上报通道中获取事件信息
S1013
通过用户层，将事件信息上报至后台服务器
S102

图8

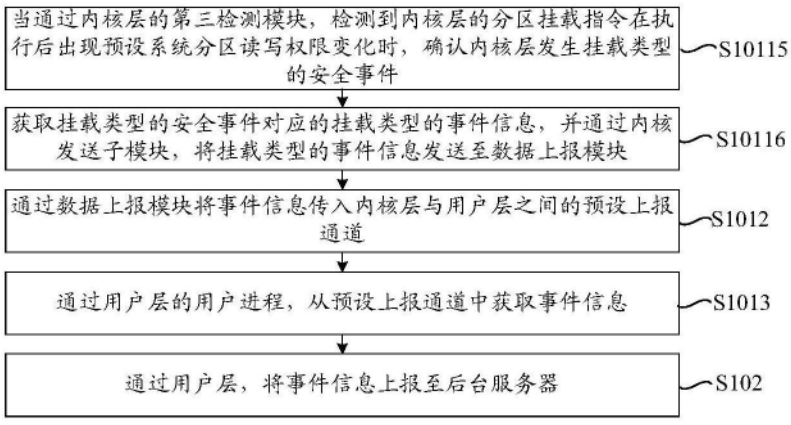

当通过内核层的第三检测模块，检测到内核层的分区挂载指令在执行后出现预设系统分区读写权限变化时，确认内核层发生挂载类型的安全事件
S10115
获取挂载类型的安全事件对应的挂载类型的事件信息，并通过内核发送子模块，将挂载类型的事件信息发送至数据上报模块
S10116
通过数据上报模块将事件信息传入内核层与用户层之间的预设上报通道
S1012
通过用户层的用户进程，从预设上报通道中获取事件信息
S1013
通过用户层，将事件信息上报至后台服务器
S102

图9

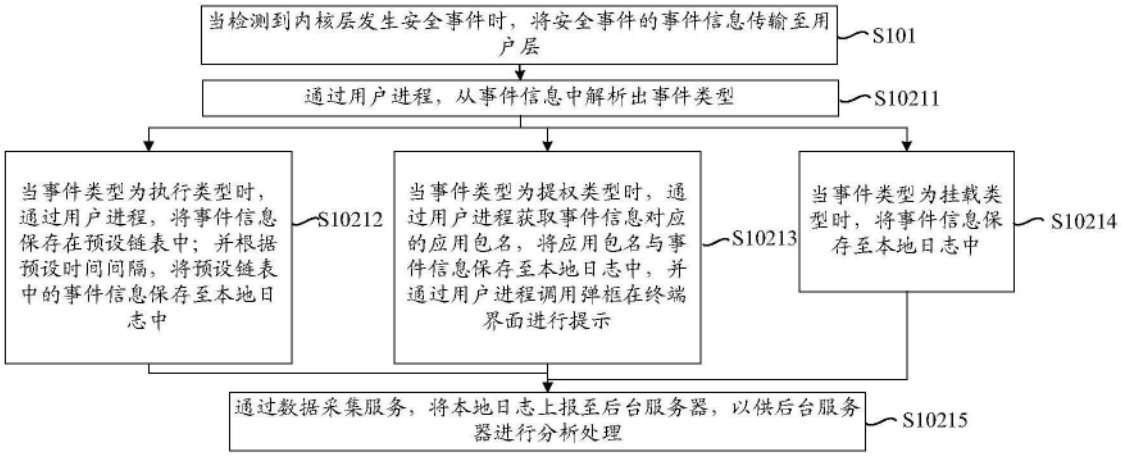

当检测到内核层发生安全事件时，将安全事件的事件信息传输至用户层
S101
通过用户进程，从事件信息中解析出事件类型
S10211
当事件类型为执行类型时，通过用户进程，将事件信息保存在预设链表中；并根据预设时间间隔，将预设链表中的事件信息保存至本地日志中
S10212
当事件类型为提权类型时，通过用户进程获取事件信息对应的应用包名，将应用包名与事件信息保存至本地日志中，并通过用户进程调用弹框在终端界面进行提示
S10213
当事件类型为挂载类型时，将事件信息保存至本地日志中
S10214
通过数据采集服务，将本地日志上报至后台服务器，以供后台服务器进行分析处理
S10215

图10

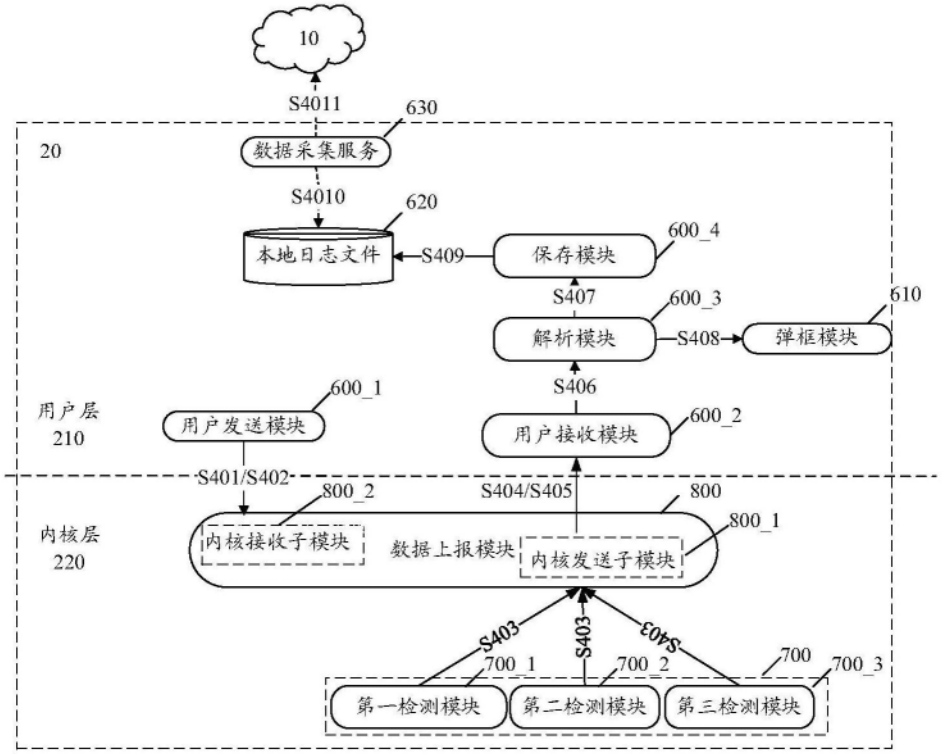

10
S4011
630
20
数据采集服务
S4010
620
本地日志文件
S409
保存模块
600_4
S407
600_3
610
解析模块
S408
弹框模块
S406
600_1
用户层
210
用户发送模块
用户接收模块
600_2
S401/S402
800_2
S404/S405
800
800_1
内核层
220
内核接收子模块
数据上报模块
内核发送子模块
S403
S403
S403
700
700_1
700_2
700_3
第一检测模块
第二检测模块
第三检测模块

图11

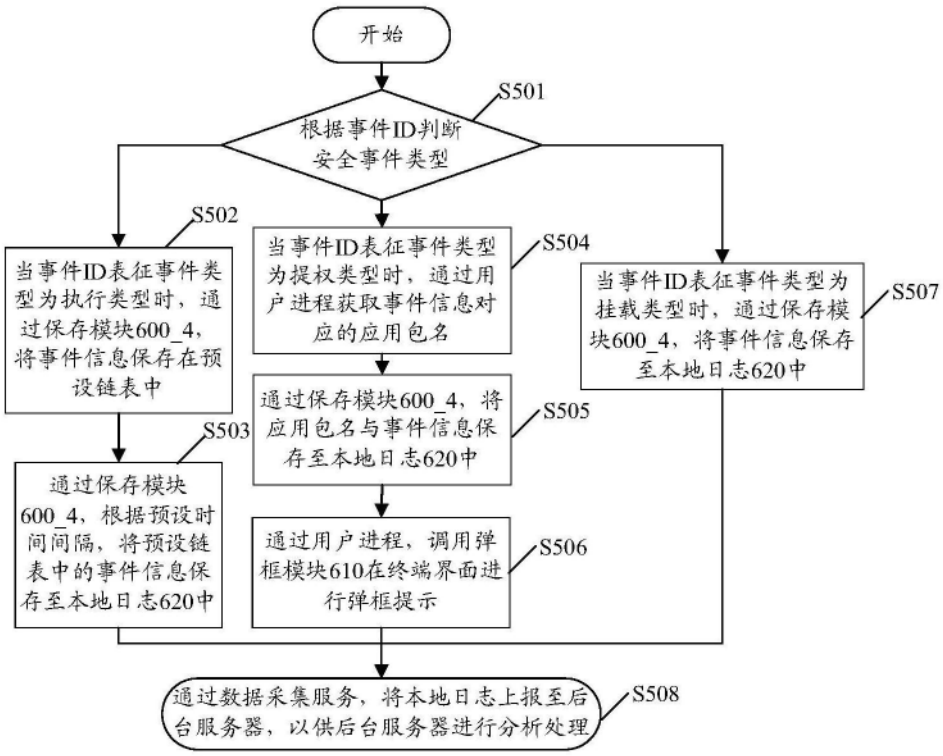

开始
S501
根据事件ID判断安全事件类型
S502
当事件ID表征事件类型为执行类型时，通过保存模块600_4，将事件信息保存在预设链表中
S503
通过保存模块600_4，根据预设时间间隔，将预设链表中的事件信息保存至本地日志620中
S504
当事件ID表征事件类型为提权类型时，通过用户进程获取事件信息对应的应用包名
S505
通过保存模块600_4，将应用包名与事件信息保存至本地日志620中
S506
通过用户进程，调用弹框模块610在终端界面进行弹框提示
S507
当事件ID表征事件类型为挂载类型时，通过保存模块600_4，将事件信息保存至本地日志620中
S508
通过数据采集服务，将本地日志上报至后台服务器，以供后台服务器进行分析处理

图12


900
数据上报装置
910
内核层
920
用户层

图13

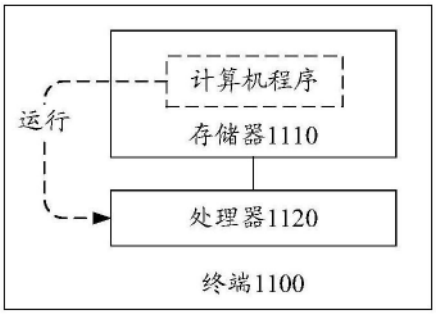

计算机程序
运行
存储器1110
处理器1120
终端1100

图14