(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112925754 B
(45)授权公告日 2023.04.07

(21)申请号 202110346372.X

(22)申请日 2021.03.31

(65)同一申请的已公布的文献号
申请公布号 CN 112925754 A

(43)申请公布日 2021.06.08

(73)专利权人 四川虹美智能科技有限公司
地址 621050 四川省绵阳市涪城区九州大道303号

(72)发明人 康弦 刘皓

(74)专利代理机构 济南信达专利事务所有限公司 37100
专利代理师 李世喆

(51)Int.Cl.
G06F 16/17(2019.01)
G06F 11/07(2006.01)

(56)对比文件
CN 112346927 A,2021.02.09
CN 107423213 A,2017.12.01
CN 108628740 A,2018.10.09
CN 109947732 A,2019.06.28
CN 111723244 A,2020.09.29
CN 1527978 A,2004.09.08
CN 111400125 A,2020.07.10
CN 111897666 A,2020.11.06
CN 107608852 A,2018.01.19
US 2020249844 A1,2020.08.06
杨朝龙 等.嵌入式系统安全中缓冲区溢出防止技术的研究与实现.《微计算机信息》.2005,第 21 卷(第 12-2 期),
Adolfo Guzmán.The file descriptor: Use of a descriptive tool to retrieve general queries to files.《SIGDOC ″84: Proceedings of the 3rd annual international conference on Systems》.1984,

审查员 杨春颖

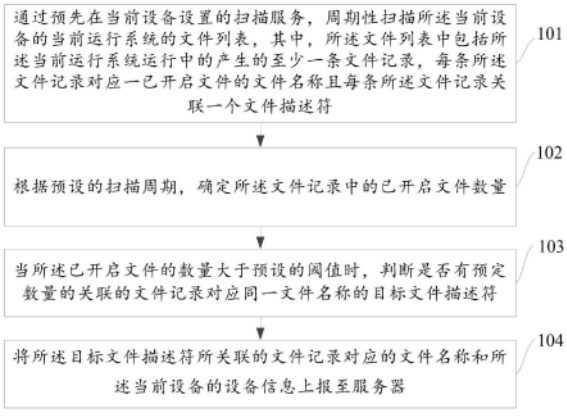
权利要求书3页 说明书8页 附图1页

(54)发明名称

文件描述符溢出上报方法、装置及计算机可读介质

(57)摘要

本发明提供了文件描述符溢出上报方法、装置及计算机可读介质。通过预先在当前设备设置的扫描服务，周期性扫描所述当前设备的当前运行系统的文件列表，其中，所述文件列表中包括所述当前运行系统运行中的产生的至少一条文件记录，每条所述文件记录对应一已开启文件的文件名称且每条所述文件记录关联一个文件描述符；根据预设的扫描周期，确定所述文件记录中的已开启文件数量；当所述已开启文件的数量大于预设的阈值时，判断是否有预定数量的关联的文件记录对应同一文件名称的目标文件描述符；将所述目标文件描述符所关联的文件记录对应的文件名称和所述当前设备的设备信息上报至服务器。本发明的方案能够有效的保证程序的正常运行。



CN 112925754 B

1.文件描述符溢出上报方法,其特征在于,包括:

通过预先在当前设备设置的扫描服务,周期性扫描所述当前设备的当前运行系统的文件列表,其中,所述文件列表中包括所述当前运行系统在运行中产生的至少一条文件记录,每条所述文件记录对应一已开启文件的文件名称且每条所述文件记录关联一个文件描述符;

根据预设的扫描周期,确定所述文件记录对应的已开启文件的数量;

当所述已开启文件的数量大于预设的阈值时,判断是否有预定数量的目标文件描述符;所述预定数量的目标文件描述符所关联的各文件记录均对应同一文件名称;

如果是,将所述目标文件描述符所关联的文件记录对应的文件名称和所述当前设备的设备信息上报至服务器。

2.根据权利要求1所述的方法,其特征在于,

当所述文件名称为套接字socket信息时,将所述目标文件描述符所关联的文件记录对应的文件名称和所述当前设备的设备信息上报至服务器,包括:

确定所述socket信息中包括的端口号;

将所述端口号转换为IP地址;

将所述IP地址和所述当前设备的设备信息上报至服务器。

3.根据权利要求2所述的方法,其特征在于,

所述将所述端口号转换为IP地址,包括:

遍历该socket信息对应的开启文件的传输控制协议tcp目录或用户数据报协议udp目录,获得该已开启文件的端口号,所述端口号中包括通过16进制表示IP地址的in_addr结构体;

确定所述in_addr结构体中的16进制IP地址,将所述16进制IP地址转换为10进制,得到所述IP地址。

4.根据权利要求1所述的方法,其特征在于,

所述设备信息,包括所述当前设备的序列号;

所述将所述目标文件描述符所关联的文件记录对应的文件名称和所述当前设备的设备信息上报至服务器,包括:

访问外部的销售数据库,其中,所述销售数据库中包括至少一台已销售设备的序列号与表征该设备销往地的地址信息;

根据所述当前设备的序列号,确定所述当前设备的销往地对应的目标地址信息;

将所述目标地址信息、所述当前设备的序列号和所述目标文件描述符所关联的文件记录对应的文件名称上报至所述服务器。

5.根据权利要求1所述的方法,其特征在于,

当所述当前运行系统为Linux时,进一步包括:

收集当前运行系统的日志;

针对收集到的日志与预先根据日志建立的关键词类型的故障知识库、汉语语言模型n-gram类型的故障知识库进行扫描以识别故障;

所述收集当前运行系统的日志,包括:当前运行系统中指定的系统服务单元的日志,所述系统服务单元为Linux操作系统中路径及名称为/usr/lib/systemd/system、/run/

systemd/system和/etc/systemd/system三个文件包含系统服务单元的一项或多项。

6.根据权利要求5所述的方法,其特征在于,

所述关键词类型的故障知识库,包括:基于操作系统的日志构建的关键词类型故障知识条目,所述关键词类型故障知识条目包含多个表项,每个表项包括故障类型、故障关键词,故障帮助信息、故障修复方案、故障优先级、故障修复过程中是否需要重启中的一项或多项。

7.基于权利要求1至6中任一所述的文件描述符溢出上报方法的文件描述符溢出上报装置,其特征在于,包括:

扫描模块,用于通过预先在当前设备设置的扫描服务,周期性扫描所述当前设备的当前运行系统的文件列表,其中,所述文件列表中包括所述当前运行系统在运行中产生的至少一条文件记录,每条所述文件记录对应一已开启文件的文件名称且每条所述文件记录关联一个文件描述符;

确定模块,用于根据预设的扫描周期,确定所述文件记录对应的已开启文件的数量;

判断模块,用于当所述已开启文件的数量大于预设的阈值时,判断是否有预定数量的目标文件描述符;所述预定数量的目标文件描述符所关联的各文件记录均对应同一文件名称;

上报模块,用于在有预定数量的目标文件描述符时,将所述目标文件描述符所关联的文件记录对应的文件名称和所述当前设备的设备信息上报至服务器。

8.根据权利要求7所述的装置,其特征在于,

当所述文件名称为套接字socket信息时,所述上报模块,在执行将所述目标文件描述符所关联的文件记录对应的文件名称和所述当前设备的设备信息上报至服务器时,执行:

确定所述socket信息中包括的端口号;

将所述端口号转换为IP地址;

将所述IP地址和所述当前设备的设备信息上报至服务器;

所述将所述端口号转换为IP地址,包括:

遍历该socket信息对应的开启文件的传输控制协议tcp目录或用户数据报协议udp目录,获得该已开启文件的端口号,所述端口号中包括通过16进制表示IP地址的in_addr结构体;

确定所述in_addr结构体中的16进制IP地址,将所述16进制IP地址转换为10进制,得到所述IP地址;

和/或,

当所述设备信息,包括所述当前设备的序列号时,所述上报模块,用于:

访问外部的销售数据库,其中,所述销售数据库中包括至少一台已销售设备的序列号与表征该设备销往地的地址信息;

根据所述当前设备的序列号,确定所述当前设备的销往地对应的目标地址信息;

将所述目标地址信息、所述当前设备的序列号和所述目标文件描述符所关联的文件记录对应的文件名称上报至所述服务器。

9.文件描述符溢出上报装置,其特征在于,包括:至少一个存储器和至少一个处理器;

所述至少一个存储器,用于存储机器可读程序;

所述至少一个处理器，用于调用所述机器可读程序，执行权利要求1至6中任一所述的方法。

10.计算机可读介质，其特征在于，所述计算机可读介质上存储有计算机指令，所述计算机指令在被处理器执行时，使所述处理器执行权利要求1至6中任一所述的方法。

文件描述符溢出上报方法、装置及计算机可读介质

技术领域

[0001] 本发明涉及数据处理领域，特别涉及文件描述符溢出上报方法、装置及计算机可读介质。

背景技术

[0002] 通常Linux系统或安卓系统能够同时打开的文件数量有一个上限值，若同时打开的文件超过该上限值，会导致系统的运行崩溃。

[0003] 目前，为了防止系统在运行时崩溃，需要监控系统内同时打开文件的数量，一旦超过上限值及时进行上报。然而，一些软件释放文件描述符的次数较低，可能在较长的一段时间后才会发生溢出的现象，由于文件描述符数量一直未超过上限值而不会被被检测到，现有的方案也无法发现系统的文件描述符的溢出趋势，因此无法防止突如其来的程序崩溃，无法有效的保证系统的正常运行。

[0004] 申请号CN201610167800.1的专利申请提供了一种DPI系统中数据并发上报的方法及装置，该方案能够提高了DPI的上报性能，实现数据高效并发上报，而且提升了大数据解析的性能，降低了服务器的负荷，但未涉及如何保证程序正常运行的方案。

发明内容

[0005] 本发明实施例提供了文件描述符溢出上报方法、装置及计算机可读介质，能够有效的保证程序正常运行。

[0006] 第一方面，本发明实施例提供了文件描述符溢出上报方法，包括：

[0007] 通过预先在当前设备设置的扫描服务，周期性扫描所述当前设备的当前运行系统的文件列表，其中，所述文件列表中包括所述当前运行系统运行中的产生的至少一条文件记录，每条所述文件记录对应一已开启文件的文件名称且每条所述文件记录关联一个文件描述符；

[0008] 根据预设的扫描周期，确定所述文件记录中的已开启文件数量；

[0009] 当所述已开启文件的数量大于预设的阈值时，判断是否有预定数量的关联的文件记录对应同一文件名称的目标文件描述符；

[0010] 将所述目标文件描述符所关联的文件记录对应的文件名称和所述当前设备的设备信息上报至服务器。

[0011] 优选地，

[0012] 当所述文件名称为套接字socket信息时，将所述目标文件描述符所关联的文件记录对应的文件名称和所述当前设备的设备信息上报至服务器，包括：

[0013] 确定所述socket信息中包括的端口号；

[0014] 将所述端口号转换为IP地址；

[0015] 将所述IP地址和所述当前设备的设备信息上报至服务器。

[0016] 优选地，

[0017] 所述将所述端口号转换为IP地址,包括:

[0018] 遍历该socket信息对应的开启文件的传输控制协议tcp目录或用户数据报协议udp目录,获得该已开启文件的端口号,所述端口号中包括通过16进制表示IP地址的in_addr结构体;

[0019] 确定所述in_addr结构体中的16进制IP地址,将所述16进制IP地址转换为10进制,得到所述IP地址。

[0020] 优选地,

[0021] 所述设备信息,包括所述当前设备的序列号;

[0022] 所述将所述目标文件描述符所关联的文件记录对应的文件名称和所述当前设备的设备信息上报至服务器,包括:

[0023] 访问外部的销售数据库,其中,所述销售数据库中包括至少一台已销售设备的序列号与表征该设备销往地的地址信息;

[0024] 根据所述当前设备的序列号,确定所述当前设备的销往地对应的目标地址信息;

[0025] 将所述目标地址信息、所述当前设备的序列号和所述目标文件描述符所关联的文件记录对应的文件名称上报至所述服务器。

[0026] 优选地,

[0027] 当所述当前运行系统为Linux时,还包括:

[0028] 收集当前运行系统的日志;

[0029] 针对收集到的日志与预先根据日志建立的关键词类型的故障知识库、汉语语言模型n-gram类型的故障知识库进行扫描以识别故障;

[0030] 所述收集当前运行系统的日志,包括:当前运行系统中指定的系统服务单元的日志,所述系统服务单元为Linux操作系统中路径及名称为/usr/lib/systemd/system、/run/systemd/system和/etc/systemd/system三个文件包含系统服务单元的一项或多项。

[0031] 优选地,

[0032] 所述关键词类型的故障知识库,包括:基于操作系统的日志构建的关键词类型故障知识条目,所述关键词类型故障知识条目包含多个表项,每个表项包括故障类型、故障关键词,故障帮助信息、故障修复方案、故障优先级、故障修复过程中是否需要重启中的一项或多项。

[0033] 第二方面,本发明实施例体提供了基于上述第一方面中任一所述的文件描述符溢出上报方法的文件描述符溢出上报装置,包括:

[0034] 扫描模块,用于通过预先在当前设备设置的扫描服务,周期性扫描所述当前设备的当前运行系统的文件列表,其中,所述文件列表中包括所述当前运行系统运行中的产生的至少一条文件记录,每条所述文件记录对应一已开启文件的文件名称且每条所述文件记录关联一个文件描述符;

[0035] 确定模块,用于根据预设的扫描周期,确定所述文件记录中的已开启文件数量;

[0036] 判断模块,用于当所述已开启文件的数量大于预设的阈值时,判断是否有预定数量的关联的文件记录对应同一文件名称的目标文件描述符;

[0037] 上报模块,用于将所述目标文件描述符所关联的文件记录对应的文件名称和所述当前设备的设备信息上报至服务器。

[0038] 优选地，

[0039] 当所述文件名称为套接字socket信息时，所述上报模块，在执行将所述目标文件描述符所关联的文件记录对应的文件名称和所述当前设备的设备信息上报至服务器时，执行：

[0040] 确定所述socket信息中包括的端口号；

[0041] 将所述端口号转换为IP地址；

[0042] 将所述IP地址和所述当前设备的设备信息上报至服务器；

[0043] 所述将所述端口号转换为IP地址，包括：

[0044] 遍历该socket信息对应的开启文件的传输控制协议tcp目录或用户数据报协议udp目录，获得该已开启文件的端口号，所述端口号中包括通过16进制表示IP地址的in_addr结构体；

[0045] 确定所述in_addr结构体中的16进制IP地址，将所述16进制IP地址转换为10进制，得到所述IP地址；

[0046] 优选地，

[0047] 当所述设备信息，包括所述当前设备的序列号时，所述上报模块，用于：

[0048] 访问外部的销售数据库，其中，所述销售数据库中包括至少一台已销售设备的序列号与表征该设备销往地的地址信息；

[0049] 根据所述当前设备的序列号，确定所述当前设备的销往地对应的目标地址信息；

[0050] 将所述目标地址信息、所述当前设备的序列号和所述目标文件描述符所关联的文件记录对应的文件名称上报至所述服务器。

[0051] 第三方面，本发明实施例提供了文件描述符溢出上报装置，包括：至少一个存储器和至少一个处理器；

[0052] 所述至少一个存储器，用于存储机器可读程序；

[0053] 所述至少一个处理器，用于调用所述机器可读程序，执行上述第一方面中任一所述的方法。

[0054] 10、计算机可读介质，其特征在于，所述计算机可读介质上存储有计算机指令，所述计算机指令在被处理器执行时，使所述处理器执行上述第一方面中任一所述的方法。

[0055] 本发明实施例提供了文件描述符溢出上报方法、装置及计算机可读介质。在需要执行文件描述符溢出上报的当前设备中预先设置扫描服务，根据预设的扫描周期扫描当前设备当前运行系统的文件列表，文件列表中包括所述当前运行系统运行中的产生的至少一条文件记录，每条所述文件记录对应一已开启文件的文件名称且每条所述文件记录关联一个文件描述符。根据预设的扫描周期，通过扫描服务确定文件记录中的已开启的文件数量，当已开启文件的数量大于预设的阈值时，则标识文件描述符有溢出的趋势，判断是否有判断是否有预定数量的关联的文件记录对应同一文件名称的目标文件描述符，则目标文件描述符发生了溢出，将目标文件描述符所关联的文件记录对应的文件名称和当前设备的设备信息上报至服务器，技术人员查看到上报的相关信息后，就知道系统出现了问题，再通过技术手段排查，防止系统崩溃。本发明提供的方案通过设置已开启文件数量的阈值，来周期性的确定已开启的文件数量是否超过阈值，判断是否有文件描述符溢出的趋势，找出关联目标文件描述符最多的文件，即打开次数最多，且每次都未被关闭的文件，将该文件的文件名

称和设备信息上报至服务器，开发人员可以及时进行修复，从而能够保证系统的正常运行。

附图说明

[0056] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术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。

[0057] 图1是本发明一实施例提供的一种文件描述符溢出上报方法的流程图；

[0058] 图2是本发明一实施例提供的一种文件列表的示意图；

[0059] 图3是本发明一实施例提供的一种文件描述符溢出上报装置的示意图。

具体实施方式

[0060] 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、完整地描述，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的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。

[0061] 如前所述，通常Linux系统或安卓系统能够同时打开的文件数量有一个上限值，若同时打开的文件超过该上限值，会导致系统的运行崩溃。目前，为了防止系统在运行时崩溃，需要监控系统内同时打开文件的数量，一旦超过上限值及时进行上报。然而，一些软件释放文件描述符的次数较低，可能在较长的一段时间后才会发生溢出的现象，由于文件描述符数量一直未超过上限值而不会被被检测到，现有的方案也无法发现系统的文件描述符的溢出趋势，因此无法防止突如其来的程序崩溃，无法有效的保证系统的正常运行。

[0062] 下面结合附图对本发明各个实施例提供的文件描述符溢出上报方法、装置及计算机可读介质作详细说明。

[0063] 如图1所示，本发明一实施例提供了文件描述符溢出上报方法，该方法包括以下步骤：

[0064] 步骤101：通过预先在当前设备设置的扫描服务，周期性扫描所述当前设备的当前运行系统的文件列表，其中，所述文件列表中包括所述当前运行系统运行中的产生的至少一条文件记录，每条所述文件记录对应一已开启文件的文件名称且每条所述文件记录关联一个文件描述符；

[0065] 步骤102：根据预设的扫描周期，确定所述文件记录中的已开启文件数量；

[0066] 步骤103：当所述已开启文件的数量大于预设的阈值时，判断是否有预定数量的关联的文件记录对应同一文件名称的目标文件描述符；

[0067] 步骤104：将所述目标文件描述符所关联的文件记录对应的文件名称和所述当前设备的设备信息上报至服务器。

[0068] 在本发明实施例中，在需要执行文件描述符溢出上报的当前设备中预先设置扫描服务，根据预设的扫描周期扫描当前设备当前运行系统的文件列表，文件列表中包括所述当前运行系统运行中的产生的至少一条文件记录，每条所述文件记录对应一已开启文件的文件名称且每条所述文件记录关联一个文件描述符。根据预设的扫描周期，通过扫描服务

确定文件记录中的已开启的文件数量，当已开启文件的数量大于预设的阈值时，则标识文件描述符有溢出的趋势，判断是否有判断是否有预定数量的关联的文件记录对应同一文件名称的目标文件描述符，则目标文件描述符发生了溢出，将目标文件描述符所关联的文件记录对应的文件名称和当前设备的设备信息上报至服务器，技术人员查看到上报的相关信息后，就知道系统出现了问题，再通过技术手段排查，防止系统崩溃。本发明提供的方案通过设置已开启文件数量的阈值，来周期性的确定已开启的文件数量是否超过阈值，判断是否有文件描述符溢出的趋势，找出关联目标文件描述符最多的文件，即打开次数最多，且每次都未被关闭的文件，将该文件的文件名称和设备信息上报至服务器，开发人员可以及时进行修复，从而能够保证系统的正常运行。

[0069] 具体地，当前运行系统中的某个程序不断的访问一个网址，但未释放该文件描述符，如果该程序访问该网址的频率很低，可能半年或一年及更长时间才会溢出一次，导致程序退出。在某些应用中，程序退出会导致严重的问题。该例子中的问题很难被测试出来。通过本发明实施例提供的方案，能够提前发现问题，如发现该程序文件描述符有溢出趋势，则上报到服务器，开发人员可以及时修复。

[0070] 在本发明一实施例中，当所述文件名称为套接字socket信息时，将所述目标文件描述符所关联的文件记录对应的文件名称和所述当前设备的设备信息上报至服务器，包括：

[0071] 确定所述socket信息中包括的端口号；

[0072] 将所述端口号转换为IP地址；

[0073] 将所述IP地址和所述当前设备的设备信息上报至服务器。

[0074] 在本发明实施例中，若非socket存在溢出，则直接将文件名称和设备信息上报至服务器即可，因为非socket的文件名称能够直观的体现该文件记录对应的文件名称，但socket比较特殊，需要将socket中包括的端口号转换为IP地址后再进行上报。

[0075] 在本发明实施例中，所述将所述端口号转换为IP地址，包括：

[0076] 遍历该socket信息对应的开启文件的传输控制协议tcp目录或用户数据报协议udp目录，获得该已开启文件的端口号，所述端口号中包括通过16进制表示IP地址的in_addr结构体；

[0077] 确定所述in_addr结构体中的16进制IP地址，将所述16进制IP地址转换为10进制，得到所述IP地址。

[0078] 举例来说，当系统启动时，设置根据预设间隔进行扫描的扫描服务，比如每10秒扫描一次目录/proc/(当前应用程序进程号)/fd，如果该目录下的已开启文件数量大于阀值，如300个，则文件描述符有溢出趋势。

[0079] 若文件描述符有溢出趋势，则找出关联文件描述符最多的文件或socket，方法如下：

[0080] 一种文件列表的示意图如图2所示，根据图2可知，socket:[251044]关联了45到48共4个目标文件描述符，其他文件都只关联了一个文件描述符，则该socket可能存在泄露。

[0081] 通过socket端口号查找对应IP地址的方法：通过在以下文件中查找，直到找到为止，/proc/net/tcp或/proc/net/udp或/proc/当前应用程序进程号/net/tcp或/proc/当前应用程序进程号/net/udp。找到后的数据类似以下格式：

[0082] 434:6600A8C0:8148 7258B276:1F9A 08 00000000:00000001 00:0000000000000000 1000 0 58044 1 0000000000000000 28 3 30 10-1

[0083] 其中7258B276:1F9A为16进制的远程IP地址和端口，转换为10进制后，为118.178.88.114:8090，将该IP地址和当前设备的序列号上报到服务器即可。

[0084] 在本发明实施例中，还可以系统发生故障时进行故障的识别。具体地，当当前运行系统未Linux时，收集当前运行系统的日志；

[0085] 针对收集到的日志与预先根据日志建立的关键词类型的故障知识库、汉语语言模型n-gram类型的故障知识库进行扫描以识别故障；

[0086] 所述收集当前运行系统的日志，包括：当前运行系统中指定的系统服务单元的日志，所述系统服务单元为Linux操作系统中路径及名称为/usr/lib/systemd/system、/run/systemd/system和/etc/systemd/system三个文件包含系统服务单元的一项或多项。

[0087] 在本发明实施例中，所述关键词类型的故障知识库，包括：基于操作系统的日志构建的关键词类型故障知识条目，所述关键词类型故障知识条目包含多个表项，每个表项包括故障类型、故障关键词，故障帮助信息、故障修复方案、故障优先级、故障修复过程中是否需要重启中的一项或多项。

[0088] 综上所述，本发明各个实施例提供的方案中，监测系统中被打开次数最多且没被关闭的文件，该文件随着时间的推移，会造成系统崩溃。通过提前发现该文件并上报到服务器，技术人员收到该信息后，就知道系统出了问题，再通过技术手段排查，防止系统崩溃。

[0089] 具体地，定时监测系统中目前未被关闭的文件描述符数量(文件被打开一次，就会产生一个不同的文件描述符，文件关闭了，所有与该文件相关的文件描述符都会回收)，当数量达到一个阀值后，找出那个关联文件描述符最多的文件(即被打开次数最多，且未关闭的文件)，上报到服务器。如果文件描述符对应的是一个socket，则指的是某个网址被打开次数最多且未关闭(网址打开一次也会产生一个不同的文件描述符)，则通过分析/proc/net/tcp或/proc/net/udp或/proc/当前应用程序进程号/net/tcp或/proc/当前应用程序进程号/net/udp，计算出socket对应的IP地址，和设备的序列号一起上报的服务器。然后邮件自动通知售后人员。该邮件里内容包含了某台设备的序列号，所在地址，出问题的原因等信息。

[0090] 如图3所示，本发明一实施例提供了上述图1中任一所述的文件描述符溢出上报方法的文件描述符溢出上报装置，包括：

[0091] 扫描模块301，用于通过预先在当前设备设置的扫描服务，周期性扫描所述当前设备的当前运行系统的文件列表，其中，所述文件列表中包括所述当前运行系统运行中的产生的至少一条文件记录，每条所述文件记录对应一已开启文件的文件名称且每条所述文件记录关联一个文件描述符；

[0092] 确定模块302，用于根据预设的扫描周期，确定所述文件记录中的已开启文件数量；

[0093] 判断模块303，用于当所述已开启文件的数量大于预设的阈值时，判断是否有预定数量的关联的文件记录对应同一文件名称的目标文件描述符；

[0094] 上报模块304，用于将所述目标文件描述符所关联的文件记录对应的文件名称和所述当前设备的设备信息上报至服务器。

[0095] 在本发明一实施例中，当所述文件名称为套接字socket信息时，所述上报模块304，在执行将所述目标文件描述符所关联的文件记录对应的文件名称和所述当前设备的设备信息上报至服务器时，执行：

[0096] 确定所述socket信息中包括的端口号；

[0097] 将所述端口号转换为IP地址；

[0098] 将所述IP地址和所述当前设备的设备信息上报至服务器；

[0099] 所述将所述端口号转换为IP地址，包括：

[0100] 遍历该socket信息对应的开启文件的传输控制协议tcp目录或用户数据报协议udp目录，获得该已开启文件的端口号，所述端口号中包括通过16进制表示IP地址的in_addr结构体；

[0101] 确定所述in_addr结构体中的16进制IP地址，将所述16进制IP地址转换为10进制，得到所述IP地址；

[0102] 在本发明一实施例中，当所述设备信息，包括所述当前设备的序列号时，所述上报模块304，用于：

[0103] 访问外部的销售数据库，其中，所述销售数据库中包括至少一台已销售设备的序列号与表征该设备销往地的地址信息；

[0104] 根据所述当前设备的序列号，确定所述当前设备的销往地对应的目标地址信息；

[0105] 将所述目标地址信息、所述当前设备的序列号和所述目标文件描述符所关联的文件记录对应的文件名称上报至所述服务器。

[0106] 可以理解的是，本发明实施例示意的结构并不构成对文件描述符溢出上报装置的具体限定。在本发明的另一些实施例中，文件描述符溢出上报装置可以包括比图示更多或者更少的部件，或者组合某些部件，或者拆分某些部件，或者不同的部件布置。图示的部件可以以硬件、软件或者软件和硬件的组合来实现。

[0107] 上述装置内的各单元之间的信息交互、执行过程等内容，由于与本发明方法实施例基于同一构思，具体内容可参见本发明方法实施例中的叙述，此处不再赘述。

[0108] 本发明还提供了一种计算机可读介质，存储用于使一计算机执行如本文所述的文件描述符溢出上报方法的指令。具体地，可以提供配有存储介质的系统或者装置，在该存储介质上存储着实现上述实施例中任一实施例的功能的软件程序代码，且使该系统或者装置的计算机(或CPU或MPU)读出并执行存储在存储介质中的程序代码。

[0109] 在这种情况下，从存储介质读取的程序代码本身可实现上述实施例中任何一项实施例的功能，因此程序代码和存储程序代码的存储介质构成了本发明的一部分。

[0110] 用于提供程序代码的存储介质实施例包括软盘、硬盘、磁光盘、光盘(如CD-ROM、CD-R、CD-RW、DVD-ROM、DVD-RAM、DVD-RW、DVD+RW)、磁带、非易失性存储卡和ROM。可选择地，可以由通信网络从服务器计算机上下载程序代码。

[0111] 此外，应该清楚的是，不仅可以通过执行计算机所读出的程序代码，而且可以通过基于程序代码的指令使计算机上操作的操作系统等来完成部分或者全部的实际操作，从而实现上述实施例中任意一项实施例的功能。

[0112] 此外，可以理解的是，将由存储介质读出的程序代码写到插入计算机内的扩展板中所设置的存储器中或者写到与计算机相连接的扩展单元中设置的存储器中，随后基于程

序代码的指令使安装在扩展板或者扩展单元上的CPU等来执行部分和全部实际操作，从而实现上述实施例中任一实施例的功能。

[0113] 需要说明的是，上述各流程和各系统结构图中不是所有的步骤和模块都是必须的，可以根据实际的需要忽略某些步骤或模块。各步骤的执行顺序不是固定的，可以根据需要进行调整。上述各实施例中描述的系统结构可以是物理结构，也可以是逻辑结构，即，有些模块可能由同一物理实体实现，或者，有些模块可能分由多个物理实体实现，或者，可以由多个独立设备中的某些部件共同实现。

[0114] 以上各实施例中，硬件单元可以通过机械方式或电气方式实现。例如，一个硬件单元可以包括永久性专用的电路或逻辑(如专门的处理器，FPGA或ASIC)来完成相应操作。硬件单元还可以包括可编程逻辑或电路(如通用处理器或其它可编程处理器)，可以由软件进行临时的设置以完成相应操作。具体的实现方式(机械方式、或专用的永久性电路、或者临时设置的电路)可以基于成本和时间上的考虑来确定。

[0115] 上文通过附图和优选实施例对本发明进行了详细展示和说明，然而本发明不限于这些已揭示的实施例，基于上述多个实施例本领域技术人员可以知晓，可以组合上述不同实施例中的代码审核手段得到本发明更多的实施例，这些实施例也在本发明的保护范围之内。

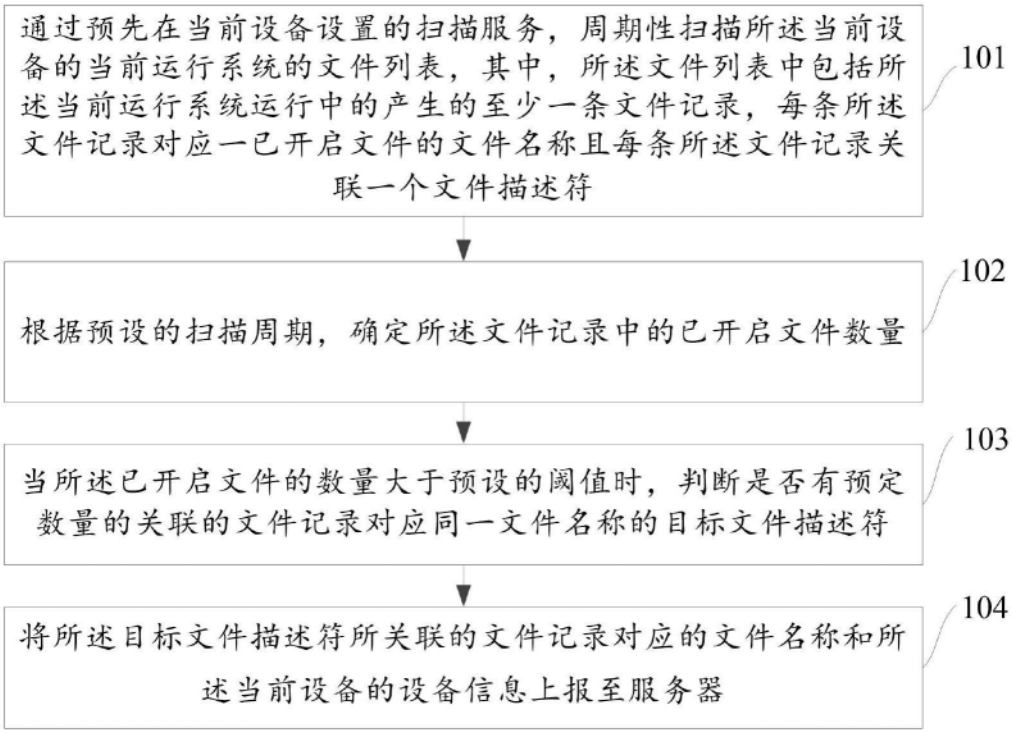

通过预先在当前设备设置的扫描服务，周期性扫描所述当前设备的当前运行系统的文件列表，其中，所述文件列表中包括所述当前运行系统运行中的产生的至少一条文件记录，每条所述文件记录对应一已开启文件的文件名称且每条所述文件记录关联一个文件描述符
101
根据预设的扫描周期，确定所述文件记录中的已开启文件数量
102
当所述已开启文件的数量大于预设的阈值时，判断是否有预定数量的关联的文件记录对应同一文件名称的目标文件描述符
103
将所述目标文件描述符所关联的文件记录对应的文件名称和所述当前设备的设备信息上报至服务器
104

图1


38 -> /system/framework/okhttp.jar
40 -> /system/framework/bouncycastle.jar
41 -> /system/framework/apache-xml.jar
42 -> /system/framework/legacy-test.jar
43 -> /system/framework/ext.jar
44 -> /system/framework/framework.jar
45 -> socket:[251044]
46 -> socket:[251044]
47 -> socket:[251044]
48 -> socket:[251044]

图2


301
扫描模块
302
确定模块
303
判断模块
304
上报模块

图3