(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 102591696 A
(43)申请公布日 2012.07.18

(21)申请号 201110008473.2

(22)申请日 2011.01.14

(71)申请人 中国科学院软件研究所
地址 100190 北京市海淀区中关村南四街 4 号

(72)发明人 应凌云 冯登国 杨轶 苏璞睿

(74)专利代理机构 北京君尚知识产权代理事务所（普通合伙） 11200
代理人 冯艺东

(51)Int.Cl.
G06F 9/45(2006.01)
G06F 21/00(2006.01)
H04M 1/725(2006.01)

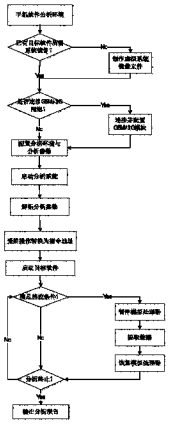
权利要求书 2 页 说明书 8 页 附图 2 页

(54)发明名称

一种手机软件行为数据提取方法及系统

(57)摘要

本发明公开了一种手机软件行为数据提取方法及系统，属于信息安全技术领域。本方法为：1）虚拟目标手机软件所需的硬件设备，构建手机模拟器；2）建立该目标手机软件的配置文件；3）解析配置文件并初始化手机模拟器，加载手机操作系统镜像；4）启动操作系统，将设定需拦截的系统调用操作转换为手机模拟器内手机操作系统对应的系统调用的指令起始地址；5）启动目标手机软件，在手机模拟器的虚拟处理器执行任一指令之前，判断当前执行指令地址是否为步骤 4）所得的指令起始地址，如果是，则暂停该操作系统的运行，记录当前指令并收集该系统调用相关的数据，然后恢复该操作系统的运行。本发明可提取到真实环境中的手机软件的各种行为数据。



CN 102591696 A

1. 一种手机软件行为数据提取方法，其步骤为：

1) 虚拟目标手机软件所需的硬件设备，构建手机模拟器并提供手机操作系统镜像；

2) 建立该目标手机软件的配置文件，所述配置文件包括分析环境信息和分析参数信息；

3) 解析所述配置文件并根据解析的配置信息初始化所述手机模拟器，加载所述手机操作系统镜像到所述手机模拟器；

4) 启动该操作系统，数据采集模块将设定需拦截的系统调用操作转换为手机模拟器内手机操作系统对应的系统调用的指令起始地址；

5) 启动所述目标手机软件，所述数据采集模块在所述手机模拟器的虚拟处理器执行任一指令之前，判断当前执行指令地址是否为步骤 4) 所得的指令起始地址，如果是，则暂停该操作系统的运行，记录当前指令的内容和对应的系统调用，同时从手机模拟器中收集该系统调用相关的数据，然后恢复该操作系统的运行。

2. 如权利要求 1 所述的方法，其特征在于如果目标手机软件需要网络环境，则将所述手机模拟器与一通讯网络模块建立数据连接。

3. 如权利要求 2 所述的方法，其特征在于所述分析环境信息包括：手机操作系统镜像文件、存储卡镜像文件、虚拟内存大小、屏幕分辨率大小和颜色精度、虚拟系统时间、虚拟键盘类型、虚拟传感器类型和精度、虚拟 GPS 类型和精度、虚拟摄像头类型和像素解析度、虚拟触摸屏类型和精度、虚拟轨迹球类型、虚拟电池类型、网络接入类型；所述分析参数信息包括：要监控的系统资源、系统调用名称、系统调用的含义、系统调用参数的结构和含义、系统调用返回值的结构和含义、手机软件文件名。

4. 如权利要求 1 或 2 或 3 所述的方法，其特征在于所述配置文件还包括数据分析模块参数、数据展现模块参数、用户控制模块参数；其中，所述数据分析模块参数包括：历史数据保存时间、分析结果输出形式，所述数据展现模块参数包括：虚拟系统实时运行状态信息与手机软件运行信息是否自动刷新、刷新时间间隔，所述用户控制模块参数包括：分析过程的终止条件设置、分析日志记录和操作监控项目选择。

5. 如权利要求 4 所述的方法，其特征在于所述配置文件为一 XML 格式的配置文件。

6. 如权利要求 1 或 2 或 3 所述的方法，其特征在于启动该操作系统时，拦截操作系统的动态链接库加载操作，将动态链接库中与设定需拦截的系统调用操作相同的操作也转换为手机模拟器内手机操作系统的系统调用的指令起始地址。

7. 如权利要求 6 所述的方法，其特征在于所述暂停该操作系统的运行，记录当前指令的内容和对应的系统调用，同时从手机模拟器中收集该系统调用相关的数据，然后恢复该操作系统的运行的方法为：数据采集模块暂停该操作系统的运行，将当前步骤 5) 中判断为真的指令的后继指令的地址加入一指令监控列表，并根据该指令对应的系统调用声明的参数个数和结构，从虚拟系统运行栈中获取参数的值，对于指针类型的参数值，还需要获取指针对应的内存区域的值；然后恢复该操作系统的运行，判断当前执行指令地址是否为所述指令监控列表中的指令地址，如果是，则再次暂停该操作系统的运行，数据采集模块从虚拟系统运行栈中获取该返回操作对应的系统调用的返回值，并从所述指令监控列表中删除该返回操作对应的指令，最后恢复该操作系统的运行。

8. 一种手机软件行为数据提取系统，其特征在于包括运行在宿主主机上的硬件虚拟模

块、数据采集模块、一用户控制模块；宿主主机通过网络与所述用户控制模块连接；其中：

所述硬件虚拟模块，用于虚拟实现物理手机具备的各种硬件设备，构建手机模拟器，加载手机软件运行所需的手机操作系统镜像；

所述数据采集模块，用于拦截手机操作系统的系统调用和虚拟硬件的访问操作，收集并记录相关操作的数据；

所述用户控制模块，用于配置分析环境和分析目标参数信息，控制分析过程。

9. 如权利要求 8 所述的系统，其特征在于还包括一通讯模块、一数据展现模块，手机模拟器所在的物理计算机通过数据线与所述通讯模块连接；所述数据展现模块，用于将解析的数据以可视化的方式动态显示分析系统状态信息和手机软件运行信息。

一种手机软件行为数据提取方法及系统

技术领域

[0001] 本发明属于信息安全技术领域，尤其涉及一种手机软件行为数据提取方法及系统。

背景技术

[0002] 随着手机技术的不断发展以及智能手机终端价格的不断下降，以智能手机为代表的手机终端日益普及，摩根斯坦利估计全球智能手机出货量将在2012年超过PC，2010年预期智能手机出货4亿台。随着智能手机用户的迅速增长，智能手机上的应用软件也越来越多。由于手机软件行为数据提取困难，用户、应用商店提供商、运营商都难以对手机软件的真实行为进行分析，从而无法对手机软件的安全性进行评估，导致恶意扣费软件、信息窃取软件等恶意手机软件层出不穷。而随着手机银行、手机支付等应用的普及，手机软件的安全问题会变得越来越重要，对手机软件行为数据采集工具的需求也越来越迫切。手机出现信息安全问题的最大根源是手机终端本身的技术发展，使手机不再是一个简单的话音通信设备，而是成了一个功能强大的可进行数据通信和处理的智能终端，同时，移动互联网正在形成中，互联网上存在的种种信息安全问题都可能在手机移动网络上出现。因此，手机软件行为数据提取方法及工具的研发，对于手机软件行为分析和安全性分析，都具有重要意义。

[0003] 由于现有的软件行为数据提取方法主要通过静态反编译人工分析方法提取数据进行安全性分析。

[0004] 利用静态反编译技术开展手机软件安全性分析，主要是利用IDA Pro等工具静态反编译手机软件，对软件的二进制文件进行静态分析，通过分析反编译出的汇编指令，还原代码的执行流程，检查其中包含的各种操作，查找是否存在安全问题。这种方式的主要缺陷是需要大量人工参与，分析速度和效率很低，并且，由于手机软件运作在ARM等平台上，其指令集等与计算机的x86平台相差很大，对分析人员的要求很高。

发明内容

[0005] 针对现有技术中的技术问题，本发明的目的在于提供一种手机软件行为数据提取方法及系统。本发明通过在硬件模拟器的基础之上构建手机模拟器，创建目标手机软件所需的运行环境，手机模拟器再配合GSM/3G模块接入通讯网络，构建目标手机软件所需的网络环境，然后通过操纵和控制手机操作系统中目标软件对各种资源的访问操作，收集目标软件的各种操作信息，控制目标软件的运行过程。通过分析收集到的各种数据，动态显示模拟器中的手机操作系统状态信息和目标软件的运行信息。由于分析环境通过模拟器构造，数据采集过程在模拟器中实现，运行目标软件的手机操作系统与真实手机上的操作系统没有差别，目标软件无法感知自身是否运行在分析环境中，也无法分辨自身是否被跟踪，从而实现对手机软件的透明分析。

[0006] 为实现以上目的，本发明的构思是：分析人员通过用户控制模块配置分析环境和分析目标的参数，并根据分析需求选择是否搭配GSM/3G网络通讯模块，然后启动硬件虚拟

模块，加载目标软件运行所需的手机操作系统镜像，启动该操作系统，解析分析配置参数，将相关的受控操作解析为目标操作系统中对应的指令地址，并运行待分析的手机软件。数据采集模块根据分析配置参数，监视目标软件的运行过程，拦截虚拟处理器的内存及寄存器读写、执行流程跳转指令，收集并记录指令相关的数据，并可根据需要，通过修改跳转指令的目标地址、寄存器的标志位来更改目标软件指令的执行流程。数据采集模块还拦截目标软件对各种虚拟硬件和网络通讯模块的访问操作，收集并记录相关操作的数据，并根据访问请求和用户配置返回不同的数据，如对存储卡文件的读请求，用户可以配置系统每次都返回一个预先生成的文件，对摄像头的拍摄请求，用户可以配置系统一直返回预先配置的图像作为摄像头输出数据。数据分析模块综合数据采集模块收集的各种数据，通过数据展现模块实时显示最新的目标软件运行信息，并在数据采集过程终止后，分析工具根据指令涉及的数据是否相同、不同系统调用的参数之间是否相关、以及对同一个虚拟硬件资源的访问顺序等关系，对不同时刻采集的数据开展关联分析，自动输出分析结果。

[0007] 基于以上构思，本发明的技术方案为：

[0008] 一种手机软件行为数据提取方法，其步骤为：

[0009] 1）虚拟目标手机软件所需的硬件设备，构建手机模拟器并提供手机操作系统镜像；

[0010] 2）建立该目标手机软件的配置文件，所述配置文件包括分析环境信息和分析参数信息；

[0011] 3）解析所述配置文件并根据解析的配置信息初始化所述手机模拟器，加载所述手机操作系统镜像到所述手机模拟器；

[0012] 4）启动该操作系统，数据采集模块将设定需拦截的系统调用操作转换为手机模拟器内手机操作系统对应的系统调用的指令起始地址；

[0013] 5）启动所述目标手机软件，所述数据采集模块在所述手机模拟器的虚拟处理器执行任一指令之前，判断当前执行指令地址是否为步骤 4）所得的指令起始地址，如果是，则暂停该操作系统的运行，记录当前指令的内容和对应的系统调用，同时从手机模拟器中收集该系统调用相关的数据，然后恢复该操作系统的运行。

[0014] 进一步的，如果目标手机软件需要网络环境，则将所述手机模拟器与一通讯网络模块建立数据连接。

[0015] 进一步的，所述分析环境信息包括：手机操作系统镜像文件、存储卡镜像文件、虚拟内存大小、屏幕分辨率大小和颜色精度、虚拟系统时间、虚拟键盘类型、虚拟传感器类型和精度、虚拟 GPS 类型和精度、虚拟摄像头类型和像素解析度、虚拟触摸屏类型和精度、虚拟轨迹球类型、虚拟电池类型、网络接入类型；所述分析参数信息包括：要监控的系统资源、系统调用名称、系统调用的含义、系统调用参数的结构和含义、系统调用返回值的结构和含义、手机软件文件名。

[0016] 进一步的，所述配置文件还包括数据分析模块参数、数据展现模块参数、用户控制模块参数；其中，所述数据分析模块参数包括：历史数据保存时间、分析结果输出形式，所述数据展现模块参数包括：虚拟系统实时运行状态信息与手机软件运行信息是否自动刷新、刷新时间间隔，所述用户控制模块参数包括：分析过程的终止条件设置、分析日志记录和操作监控项目选择。

[0017] 进一步的，所述配置文件为一 XML 格式的配置文件。

[0018] 进一步的，启动该操作系统时，拦截操作系统的动态链接库加载操作，将动态链接库中与设定需拦截的系统调用操作相同的操作也转换为手机模拟器内手机操作系统的系统调用的指令起始地址。

[0019] 进一步的，所述暂停该操作系统的运行，记录当前指令的内容和对应的系统调用，同时从手机模拟器中收集该系统调用相关的数据，然后恢复该操作系统的运行的方法为：数据采集模块暂停该操作系统的运行，将当前步骤 5) 中判断为真的指令的后继指令的地址加入一指令监控列表，并根据该指令对应的系统调用声明的参数个数和结构，从虚拟系统运行栈中获取参数的值，对于指针类型的参数值，还需要获取指针对应的内存区域的值；然后恢复该操作系统的运行，判断当前执行指令地址是否为所述指令监控列表中的指令地址，如果是，则再次暂停该操作系统的运行，数据采集模块从虚拟系统运行栈中获取该返回操作对应的系统调用的返回值，并从所述指令监控列表中删除该返回操作对应的指令，最后恢复该操作系统的运行。

[0020] 一种手机软件行为数据提取系统，其特征在于包括运行在宿主主机上的硬件虚拟模块、数据采集模块、一用户控制模块；宿主主机通过网络与所述用户控制模块连接；其中：

[0021] 所述硬件虚拟模块，用于虚拟实现物理手机具备的各种硬件设备，构建手机模拟器，加载手机软件运行所需的手机操作系统镜像；

[0022] 所述数据采集模块，用于拦截手机操作系统的系统调用和虚拟硬件的访问操作，收集并记录相关操作的数据；

[0023] 所述用户控制模块，用于配置分析环境和分析目标参数信息，控制分析过程。

[0024] 进一步的，还包括一通讯模块、一数据展现模块，手机模拟器所在的物理计算机通过数据线与所述通讯模块连接；所述数据展现模块，用于将解析的数据以可视化的方式动态显示分析系统状态信息和手机软件运行信息。

[0025] 本方法主要包括：

[0026] 1) 搭建手机软件运行环境，包括根据手机软件运行环境的要求，虚拟所需的硬件设备，构建手机模拟器，准备相关的手机操作系统镜像；

[0027] 2) 根据手机软件和分析目的的不同，可选地，手机模拟器可再配合 GSM/3G 模块接入通讯网络，构建目标手机软件所需的网络环境；

[0028] 3) 配置分析环境与分析参数，包括手机软件运行所需的操作系统镜像所在位置，手机模拟器中各种虚拟硬件的参数，如虚拟内存大小，外部存储卡容量大小，屏幕分辨率，虚拟系统时间等，以及需要收集的手机软件运行数据和需要监控的手机软件操作，如号码簿读写操作，外部存储卡文件访问，网络连接操作等；

[0029] 4) 分析系统启动后，解析配置参数，启动手机模拟器，并根据配置完成各种虚拟设备初始化，加载手机软件运行所需的手机操作系统镜像，启动该操作系统，并在操作系统启动过程中将所有需要拦截的系统调用操作转换为对应系统调用的指令起始地址；

[0030] 5) 在手机模拟器中运行待分析的手机软件，在虚拟处理器执行任何指令之前，判断即将执行的指令地址是否为需要监控的操作的指令起始地址，并在匹配为真时暂停手机操作系统的运行，记录当前匹配指令对应的操作名、操作类型，同时，数据采集模块还从手

机模拟器的模拟处理器、模拟内存中收集该操作相关的数据，如 CPU 寄存器的值、手机系统调用栈中的参数，并根据操作类型及参数含义，提取操作相关的其他数据，如访问的文件名，连接的网络地址，短信息发送的目标号码等信息，然后再恢复手机操作系统的运行；同时，对于读取操作，还可根据需要提供特定的输入数据，改变手机软件的执行流程；

[0031] 解析收集到的各种数据，比如根据指令集规范和不同数据结构的定义、以及不同系统调用的原型及其参数、返回值定义进行数据解析，根据解析的数据，在控制端动态显示手机操作系统状态信息和手机软件运行信息，并在手机软件退出，自动终止数据采集过程；用户也可以根据分析进展，手动终止手机软件的运行，结束数据采集过程；数据采集过程结束后，分析工具根据指令涉及的数据是否相同、不同系统调用的参数之间是否相关、以及对同一个虚拟硬件资源的访问顺序等关系，对不同时刻采集的数据开展关联分析，输出最终分析结果。

[0032] 本系统主要包括一硬件虚拟模块，一 GSM/3G 通讯模块，一数据采集模块，一数据展现模块和一用户控制模块；硬件虚拟模块运行在宿主主机上，宿主主机通过数据线和 GSM/3G 通讯模块连接；硬件虚拟模块和用户控制模块通过网络连接相互通讯其中：

[0033] 硬件虚拟模块虚拟实现物理手机具备的各种硬件设备，加载手机软件运行所需的手机操作系统镜像；

[0034] 数据采集模块拦截各种手机操作系统的系统调用和虚拟硬件的访问操作，收集并记录相关操作的数据；

[0035] 数据展现模块将数据以可视化的方式展现给分析人员，动态显示分析系统状态信息和手机软件运行信息；

[0036] 用户控制模块供分析人员配置分析环境和分析目标参数，控制分析过程。

[0037] 根据手机软件运行所需的手机操作系统的不同，可以包含多个不同的数据采集模块，如图 2 所示。

[0038] 对于采集到的数据可以采用数据分析模块进行解析，并根据指令涉及的数据是否相同、不同系统调用的参数之间是否相关、以及对同一个虚拟硬件资源的访问顺序等关系，对不同时刻采集的数据开展关联分析；

[0039] 本发明的配置信息，可以 XML 结构化方式组织并存储。

[0040] 进一步配置信息的分析环境信息可包括：手机操作系统镜像文件，存储卡镜像文件，虚拟内存大小，屏幕分辨率大小和颜色精度，虚拟系统时间，虚拟键盘类型，虚拟传感器类型和精度，虚拟 GPS 类型和精度，虚拟摄像头类型和像素解析度，虚拟触摸屏类型和精度，虚拟轨迹球类型，虚拟电池类型，以及网络接入类型。

[0041] 进一步配置信息的分析参数信息可包括：要监控的系统资源，系统调用名称，系统调用的含义，系统调用参数的结构和含义，系统调用返回值的结构和含义，以及可选的待分析的手机软件文件名。

[0042] 本发明的硬件虚拟模块和数据采集模块，与数据分析模块、数据展现模块和用户控制模块可以运行在不同的体系结构和操作系统上，可以通过网络通信实现交互。

[0043] 与现有技术相比，本发明的优点在于：

[0044] 整个分析过程对被分析的手机软件完全透明，手机软件无法识别是否运行在虚拟环境中还是真实环境中，也无法察觉指令执行过程是否被监控，从而能够观察到真实环境

中的手机软件的各种可能行为。并且，由于分析人员能够控制模拟器中所有虚拟硬件和资源，本发明还能够在手机软件运行过程中，根据手机软件对虚拟硬件资源的访问请求和用户配置，动态返回指定的数据，如对存储卡文件的读请求，用户可以配置系统每次都返回一个预先生成的文件，对摄像头的拍摄请求，用户可以配置系统一直返回预先配置的图像作为摄像头输出数据，触发被分析手机软件中依赖于特定外部输入的隐蔽行为，提高分析数据的全面性。

附图说明

[0045] 图 1 为本发明的系统工作过程流程图。

[0046] 图 2 为本发明的系统组成与模块间详细关系示意图。

具体实施方式

[0047] 下面结合附图和具体实施方式对本发明作进一步详细描述：

[0048] 分析人员根据被分析手机软件所属的手机平台类型，搭建手机软件运行环境，并根据是否需要接入网络选择配置 GSM/3G 网络模块，然后根据分析目标配置分析环境和分析参数，启动分析系统，加载并启动手机软件运行所需的手机操作系统镜像，并运行待分析的手机软件。数据采集模块根据分析参数设置，在分析系统启动时将需要拦截的操作系统调用转换为对应的指令起始地址，并在这些指令被执行时，收集并记录相关操作的数据。

[0049] 数据分析模块解析数据采集模块收集的各种数据，综合分析数据之间的关系，然后通过数据展现模块实时显示手机软件的运行信息，并在分析过程终止后，关联分析所有的搜集到的数据，输出分析结果。分析人员利用用户控制模块配置分析环境和分析目标参数，控制分析过程。分析人员也可以根据分析进展，手动终止手机软件的运行，结束分析过程。

[0050] 参考附图 1，下面给出详细过程。

[0051] 第一步：搭建手机软件运行环境

[0052] 利用硬件虚拟模块，虚拟实现物理手机具有的处理器，内存，存储卡等部件以及传感器，键盘，轨迹球等外设。由于本发明的手机模拟器通过硬件虚拟模块实现，手机模拟器上运行的手机操作系统，其所有数据以虚拟系统镜像文件的形式存在。根据手机软件针对的运行平台和操作系统要求，利用已有的虚拟系统镜像文件，或是运行相应的手机模拟器配置所需的手机操作系统，制作新的虚拟系统镜像文件。如 ARM 平台上的 Android 手机操作系统上的手机软件，则可以通过手机模拟器加载所需版本的 Android 系统镜像文件作为手机软件的运行环境。

[0053] 第二步：搭建手机软件网络环境

[0054] 对于需要联网下载，与远程服务器进行交互，或是需要分析软件的网络访问及行为的软件，手机模拟器通过宿主主机的数据线与 GSM/3G 通讯网络模块连接。GSM/3G 通讯网络模块是物理板卡，手机模拟器通过桥接接口使用该模块提供的通讯网络接入功能，使手机模拟器具有与物理手机完全一致的网络接入能力。

[0055] 第三步：配置分析环境和分析参数

[0056] 进一步配置信息的分析环境信息可包括：手机操作系统镜像文件，存储卡镜像文

件，虚拟内存大小，屏幕分辨率大小和颜色精度，虚拟系统时间，虚拟键盘类型，虚拟传感器类型和精度，虚拟 GPS 类型和精度，虚拟摄像头类型和像素解析度，虚拟触摸屏类型和精度，虚拟轨迹球类型，虚拟电池类型，以及网络接入类型。

[0057] 进一步配置信息的分析参数信息可包括 :要监控的系统资源，系统调用名称，系统调用的含义，系统调用参数的结构和含义，系统调用返回值的结构和含义，以及可选的待分析的手机软件文件名。

[0058] 本发明的参数配置用户控制模块的图形用户界面完成，并存储为 XML 格式的配置文件，也可以通过其他工具直接修改 XML 格式的配置文件实现。

[0059] XML 配置文件包含各种分析环境设置信息，以及数据采集模块支持拦截和监控的系统调用，各个系统调用的参数以及返回值的数据结构和含义。如对一个 Android 平台系统，配置文件的主要内容包括各种手机部件的属性，数据采集模块支持监控的网络操作，文件操作和系统服务操作接口等，形式如下 :

[0060] <Platform>

[0061] <Name>Android</Name>

[0062] <Version>2.2</Version>

[0063] <Image>\usr\analysis\platform\android\v2_2.img</Image>

[0064] <Card>

[0065] <Type>SD</Type>

[0066] <Size>256M</Size>

[0067] </Card>

[0068] ......

[0069] </Platform>

[0070] ......

[0071] <Action>

[0072] <ID>0001</ID>

[0073] <Name>connect</Name>

[0074] <Monitor>false</Monitor>

[0075] <Catalog>network</Catalog>

[0076] <Detail>

[0077] <Signature>

[0078] int connect(int sockfd,struct sockaddr*serv_addr,int addrlen) ;

[0079] </Signature>

[0080] <Remark> 与远端服务器建立一个 TCP 连接 </Remark>

[0081] <Return> 出现错误时返回 -1，并且设置 errno 为相应的错误码。</Return>

[0082] <Parameter>

[0083] Sockfd 是 socket 函数返回的 socket 描述符 ;

[0084] serv_addr 是包含远端主机 IP 地址和端口号的指针 ;

[0085] addrlen 是远端地址结构的长度。

[0086] </Parameter>

[0087] </Detail>

[0088] .....

[0089] </Action>

[0090] 各种参数的配置通过用户控制模块的图形用户界面完成（也可以用命令行），具体包括硬件虚拟模块参数，数据分析模块参数，数据展现模块参数和用户控制模块参数。

[0091] 硬件虚拟模块参数包括：手机操作系统镜像文件，存储卡镜像文件，虚拟内存大小，屏幕分辨率大小和颜色精度，虚拟系统时间，虚拟键盘类型，虚拟传感器类型和精度，虚拟 GPS 类型和精度，虚拟摄像头类型和像素解析度，虚拟触摸屏类型和精度，虚拟轨迹球类型，虚拟电池类型等。

[0092] 数据分析模块参数包括：历史数据保存时间，分析结果输出形式等。

[0093] 数据展现模块参数包括：虚拟系统实时运行状态信息与手机软件运行信息是否自动刷新，刷新时间间隔等。

[0094] 用户控制模块参数包括：分析过程的终止条件设置，分析日志记录和操作监控项目选择等。

[0095] 第四步：启动分析系统，分析恶意代码

[0096] 完成相关配置后，用户启动硬件虚拟模块，硬件虚拟模块完成相关的初始化之后，手机模拟器自动加载指定的虚拟系统镜像文件，之后开始手机操作系统的正常启动过程。当系统启动完成后，利用控制接口向手机操作系统上传并安装目标手机软件，并根据设置启动该软件。

[0097] 在虚拟系统启动的同时，数据采集模块拦截操作系统内核模块的加载过程，并将所有支持拦截的内核系统调用操作转换为虚拟系统对应的系统调用的指令起始地址。在手机软件启动和运行过程中，数据采集模块还拦截操作系统的动态链接库加载操作，将所有动态加载的链接库中的、数据采集模块支持拦截的系统调用操作也转换为虚拟系统对应的系统调用的指令起始地址。数据采集模块指示虚拟处理器在执行指令之前，比较和判断即将执行的指令是否在监控范围之内。当指令满足监控条件时（即在当前执行的指令的地址等于上面的拦截操作转换过来的系统调用的指令起始地址时），数据采集模块指示虚拟处理器暂停，从而暂停虚拟系统的运行，在数据采集模块提取并保存相关的数据之后再恢复虚拟系统的运行。

[0098] 例如针对 Android 系统，监控手机软件的网络连接操作 connect，在虚拟处理器执行下一条指令之前，判断当前进程是否为受监控的目标软件进程，当前指令地址是否与 connect 系统调用的指令起始地址相等，从而决定是否中断当前执行流程。当满足条件时，数据采集模块指示虚拟处理器暂停，将返回地址对应的指令加入指令监控列表，并根据 connect 调用声明的参数个数和结构，从虚拟系统运行栈中获取参数 sockfd、serv addr 和 addrlen 的值，进而根据 sockaddr 结构获取远端主机 IP 地址和端口号。数据提取完成后，数据获取模块指示虚拟处理器恢复执行。当虚拟系统从 connect 系统调用中返回时，由于当前当前进程为受监控的目标软件进程，当前指令地址与先前保存的返回地址对应的指令相等，数据采集模块再次指示虚拟处理器暂停，从指令监控列表中删除原先保存的返回地址对应的指令，并从虚拟系统运行栈中获取 connect 的返回值，最后再指示虚拟处理器恢

复运行。通过这种方式，在不利用任何操作系统和硬件调试功能的情况下，完成对一个完整的系统调用的截获以及所有参数以及返回值的收集。

[0099] 对于获取数据的操作，如获取系统时间的系统调用，数据采集模块还可以根据配置的指示，在该系统调用返回时，根据系统调用参数、返回值的结构和含义，通过硬件模拟器接口直接修改虚拟 CPU 寄存器和虚拟内存中调用堆栈并填充相关数据，为目标手机软件提供特定的输入数据。

[0100] 数据分析模块接收、解析并存储数据采集模块收集到的数据，并通过数据展现模块实时显示手机模拟器中的操作系统状态和目标软件运行信息。动态显示的操作系统状态信息，主要包括虚拟系统内部正运行的进程的详细信息，具体包括 :进程名称，进程标识，可执行文件名，当前调度状态，进程环境信息，内存占用大小。动态显示的目标软件运行信息，包括恶意代码的进程详细信息，具体包括 :进程名称，进程标识，可执行文件名，当前调度状态，进程环境信息，内存占用大小。目标软件的系统调用信息，具体包括 :系统调用发生的时间，执行系统调用的进程名字，执行系统调用的进程标识符，系统调用类型，系统调用名，系统调用结果，系统调用参数内容，系统调用的安全级别，以及其他能够提供额外帮助的系统调用信息。

[0101] 当数据采集过程终止时，数据分析模块通过数据的时序关系，控制依赖关系和数据依赖关系对收集到的数据进行分析，具体包括数据采集时间的先后关系，手机软件加载的模块之间的加载先后顺序关系，不同进程间的父子关系，进程的线程创建 / 终止关系，不同系统调用的参数是否相同，以及一个系统调用的返回值是否作为另一个系统调用的参数等关系，标识相互关联的数据。数据分析模块完成分析后，输出自动分析结果。用户通过分析目标软件访问的资源，执行的操作，以及访问的各种数据项目之间的关系，了解目标软件的功能，找到目标软件的隐藏行为和实现机制。

[0102] 尽管为说明目的公开了本发明的具体实施例和附图，其目的在于帮助理解本发明的内容并据以实施，但是本领域的技术人员可以理解 :在不脱离本发明及所附的权利要求的精神和范围内，各种替换、变化和修改都是可能的。因此，本发明不应局限于最佳实施例和附图所公开的内容，本发明要求保护的范围以权利要求书界定的范围为准。

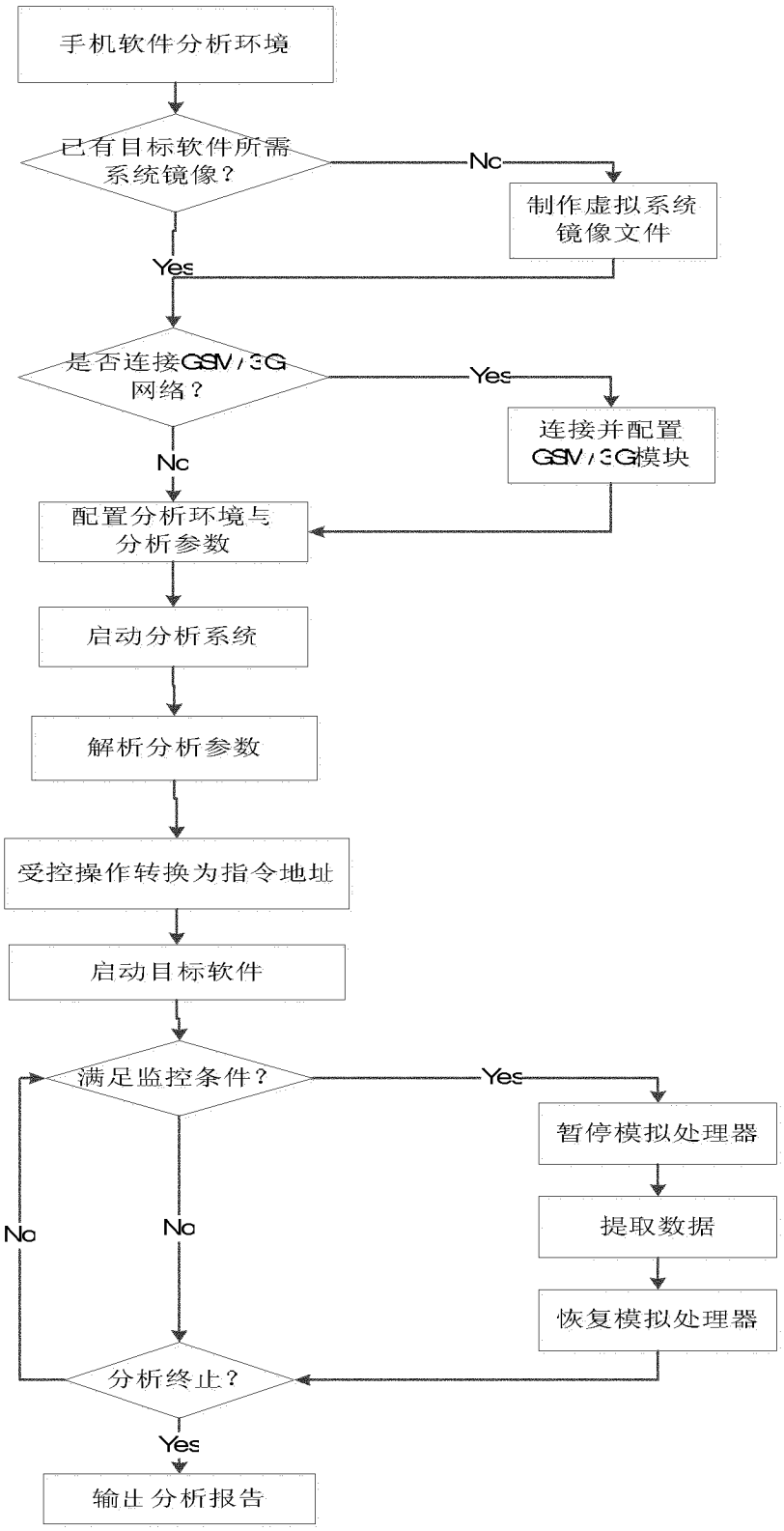

手机软件分析环境
已有目标软件所需系统镜像？
No
制作虚拟系统镜像文件
Yes
是否连接GSM/3G网络？
Yes
连接并配置GSM/3G模块
No
配置分析环境与分析参数
启动分析系统
解析分析参数
受控操作转换为指令地址
启动目标软件
满足监控条件？
Yes
暂停模拟处理器
提取数据
恢复模拟处理器
No
No
分析终止？
Yes
输出分析报告

图 1

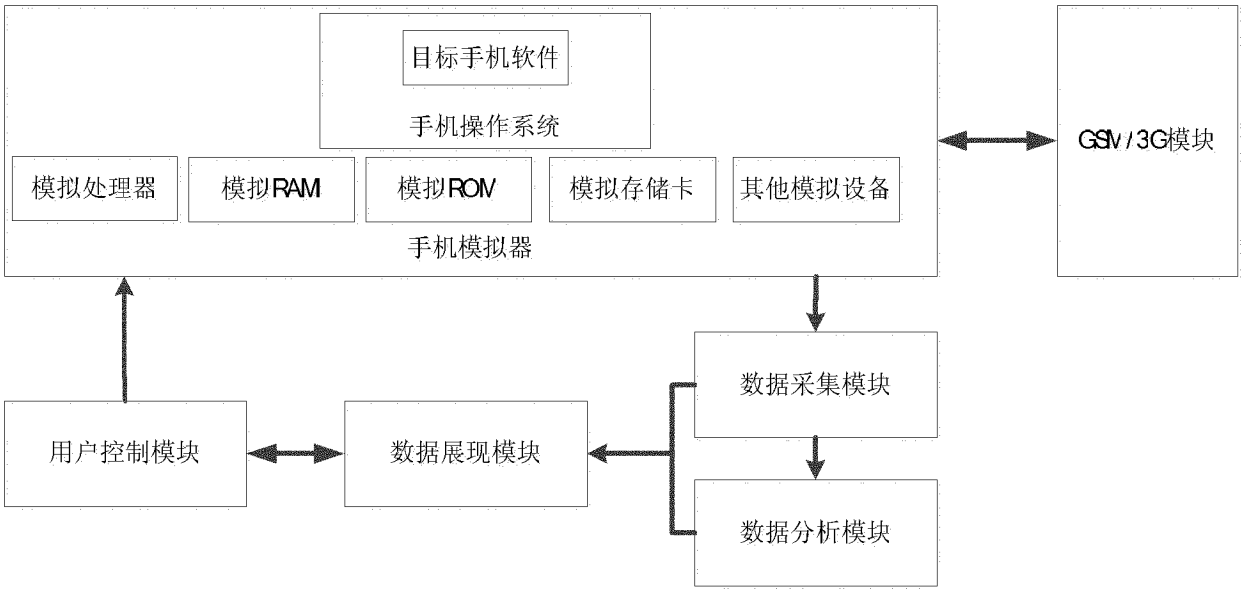

目标手机软件
手机操作系统
模拟处理器
模拟RAM
模拟ROM
模拟存储卡
其他模拟设备
手机模拟器
GSM/3G模块
数据采集模块
用户控制模块
数据展现模块
数据分析模块

图 2