

(12) 发明专利申请

(10) 申请公布号 CN 103279708 A

(43) 申请公布日 2013. 09. 04

(21) 申请号 201210580960. 0

(22) 申请日 2012. 12. 28

(71) 申请人 武汉安天信息技术有限责任公司

地址 430000 湖北省武汉市东湖开发区光谷
创业街 6 栋 2 楼

(72) 发明人 刘汭祥 潘宣辰 乔伟

(51) Int. Cl.

G06F 21/56 (2013. 01)

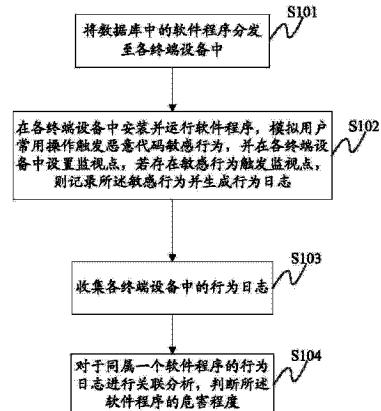
权利要求书1页 说明书4页 附图1页

(54) 发明名称

一种移动终端恶意代码行为监控和分析的方法及系统

(57) 摘要

本发明公开了一种移动终端恶意代码行为监控和分析的方法及系统，首先，将数据库中的软件程序分发至各终端设备中；在各终端设备中安装并运行软件程序，模拟用户常用操作触发恶意代码敏感行为，并在各终端设备中设置监视点，若存在敏感行为触发监视点，则记录所述敏感行为并生成行为日志；收集各终端设备中的行为日志；对于同属一个软件程序的行为日志进行关联分析，判断所述软件程序的危害程度。从而，可以快速处理海量的软件程序样本，进行动态行为监控和分析。



1. 一种移动终端恶意代码行为监控和分析的方法,其特征在于,包括:

将数据库中的软件程序分发至各终端设备中;

在各终端设备中安装并运行软件程序,模拟用户常用操作触发恶意代码敏感行为,并在各终端设备中设置监视点,若存在敏感行为触发监视点,则记录所述敏感行为并生成行为日志;

收集各终端设备中的行为日志;

对于同属一个软件程序的行为日志进行关联分析,判断所述软件程序的危害程度。

2. 如权利要求1所述的方法,其特征在于,所述将数据库中的软件程序分发至各终端设备中包括,根据终端设备的负载情况进行软件程序的分发。

3. 如权利要求1所述的方法,其特征在于,所述安装并运行软件程序包括:手动运行或者自动运行软件程序。

4. 如权利要求1所述的方法,其特征在于,所述监视点包括:短信/wap推送信息监控,数据库操作监控,定位信息监控,网络连接监控,底层操作监控,敏感文件监控。

5. 一种移动终端恶意代码行为监控和分析的系统,其特征在于,包括:

分发模块,用于将数据库中的软件程序分发至各终端设备中;

控制模块,在各终端设备中安装并运行软件程序,模拟用户常用操作触发恶意代码敏感行为,并在各终端设备中设置监视点,若存在敏感行为触发监视点,则记录所述敏感行为并生成行为日志;

回收模块,用于收集各终端设备中的行为日志;

检测模块,对于同属一个软件程序的行为日志进行关联分析,判断所述软件程序的危害程度。

6. 如权利要求5所述的系统,其特征在于,所述分发模块根据终端设备的负载情况进行软件程序的分发。

7. 如权利要求5所述的系统,其特征在于,控制模块中所述安装并运行软件程序包括:手动运行或者自动运行软件程序。

8. 如权利要求5所述的系统,其特征在于,控制模块中所述监视点包括:短信/wap推送信息监控,数据库操作监控,定位信息监控,网络连接监控,底层操作监控,敏感文件监控。

一种移动终端恶意代码行为监控和分析的方法及系统

技术领域

[0001] 本发明涉及移动终端安全技术领域，尤其涉及一种移动终端恶意代码行为监控和分析的方法及系统。

背景技术

[0002] 随着移动终端的日趋复杂化、智能化和联网化，移动终端在信息安全上所面临的问题也逐渐凸现出来。目前，移动终端结构比较松散，没有提供措施对内部器件进行统一管理和认证，并且，在操作系统设计上缺乏有效的安全策略。移动终端在进行业务应用时将面临多种形式的威胁，例如：病毒、机密信息的泄露、代码的非法篡改、关键器件的恶意替换等。

[0003] 由于移动终端具备极强的可移动性、硬件和操作系统的封闭性，当突发的移动终端安全事件或新的恶意代码家族出现时，现有的恶意代码分析技术和系统难以快速确定恶意程序的主要恶意行为，同时难以自动筛选包含恶意代码的软件程序。

发明内容

[0004] 针对上述技术问题，本发明提供了一种移动终端恶意代码行为监控和分析的方法及系统，该方法通过将海量软件程序同时分发至各终端设备中，通过运行各软件程序，并监控软件程序的动态行为，快速判断软件程序是否是恶意代码程序。

[0005] 本发明采用如下方法来实现：一种移动终端恶意代码行为监控和分析的方法，包括：

[0006] 将数据库中的软件程序分发至各终端设备中；

[0007] 在各终端设备中安装并运行软件程序，模拟用户常用操作触发恶意代码敏感行为，并在各终端设备中设置监视点，若存在敏感行为触发监视点，则记录所述敏感行为并生成行为日志；

[0008] 收集各终端设备中的行为日志；

[0009] 对于同属一个软件程序的行为日志进行关联分析，判断所述软件程序的危害程度。

[0010] 方法中，各终端设备依照设定的流程同时处理软件程序。

[0011] 方法中，所述将数据库中的软件程序分发至各终端设备中包括，根据终端设备的负载情况进行软件程序的分发。

[0012] 方法中，所述安装并运行软件程序包括：手动运行或者自动运行软件程序，触发软件程序的恶意行为。

[0013] 方法中，所述监视点包括：短信/wap 推送信息监控，数据库操作监控，定位信息监控，网络连接监控，底层操作监控，敏感文件监控；

[0014] 其中，短信/wap 推送信息监控为：若软件程序存在拦截短息或 wap 推送信息行为，则记录，并同时记录被拦截信息或者短信号码或者短信内容；

- [0015] 数据库操作监控为：若软件程序存在对短信数据库、联系人数据库等个人隐私信息数据库的查询、删除等操作，则记录该行为；
- [0016] 定位信息监控为：若软件程序存在获取移动设备当前定位信息，更新当前定位信息和获取历史定位信息的操作时，则记录该行为；
- [0017] 网络连接监控为：若软件程序存在联网行为，则记录相关 URL 连接及连接参数等网络行为；
- [0018] 底层操作监控为：若软件程序存在调用底层命令，实现更底层、更隐蔽的操作，则记录该行为；
- [0019] 敏感文件操作为：若软件程序存在在敏感目录下进行文件的创建、删除、修改或者执行等操作，则记录该行为；
- [0020] 其他监控包括：若软件程序存在获取设备硬件信息，账号信息等操作，则记录该行为。
- [0021] 方法中，所述终端设备包括：真实移动终端设备或者设备模拟器。
- [0022] 一种移动终端恶意代码行为监控和分析的系统，包括：
- [0023] 分发模块，用于将数据库中的软件程序分发至各终端设备中；
- [0024] 控制模块，在各终端设备中安装并运行软件程序，模拟用户常用操作触发恶意代码敏感行为，并在各终端设备中设置监视点，若存在敏感行为触发监视点，则记录所述敏感行为并生成行为日志；
- [0025] 回收模块，用于收集各终端设备中的行为日志；
- [0026] 检测模块，对于同属一个软件程序的行为日志进行关联分析，判断所述软件程序的危害程度。
- [0027] 系统中，所述分发模块根据终端设备的负载情况进行软件程序的分发。
- [0028] 系统中，控制模块中所述安装并运行软件程序包括：手动运行或者自动运行软件程序，触发软件程序的恶意行为。
- [0029] 系统中，控制模块中所述监视点包括：短信 /wap 推送信息监控，数据库操作监控，定位信息监控，网络连接监控，底层操作监控，敏感文件监控；
- [0030] 其中，短信 /wap 推送信息监控为：若软件程序存在拦截短息或 wap 推送信息行为，则记录，并同时记录被拦截信息或者短信号码或者短信内容；
- [0031] 数据库操作监控为：若软件程序存在对短信数据库、联系人数据库等个人隐私信息数据库的查询、删除等操作，则记录该行为；
- [0032] 定位信息监控为：若软件程序存在获取移动设备当前定位信息，更新当前定位信息和获取历史定位信息的操作时，则记录该行为；
- [0033] 网络连接监控为：若软件程序存在联网行为，则记录相关 URL 连接及连接参数等网络行为；
- [0034] 底层操作监控为：若软件程序存在调用底层命令，实现更底层、更隐蔽的操作，则记录该行为；
- [0035] 敏感文件操作为：若软件程序存在在敏感目录下进行文件的创建、删除、修改或者执行等操作，则记录该行为；
- [0036] 其他监控包括：若软件程序存在获取设备硬件信息，账号信息等操作，则记录该行

为。

[0037] 系统中,所述终端设备包括:真实移动终端设备或者设备模拟器。

[0038] 综上所述,本发明提供了一种移动终端恶意代码行为监控和分析的方法及系统,首先将海量待检测软件程序分发至各终端设备中,安装并运行软件程序,通过在敏感文件或者敏感位置设置监视点的方法,对于软件程序进行动态行为监控,若出现敏感行为则记录,根据各终端设备返回的行为日志,判断软件程序的危害程度。上述方案可以快速完成海量软件程序的行为监控和是否恶意代码程序的定性,使得移动终端恶意代码检测效率大幅提高。

附图说明

[0039] 为了更清楚地说明本发明的技术方案,下面将对实施例中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明中记载的一些实施例,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。

[0040] 图1为本发明提供的一种移动终端恶意代码行为监控和分析的方法流程图;

[0041] 图2为本发明提供的一种移动终端恶意代码行为监控和分析的系统结构图。

具体实施方式

[0042] 本发明给出了一种移动终端恶意代码行为监控和分析的方法及系统,为了使本技术领域的人员更好地理解本发明实施例中的技术方案,并使本发明的上述目的、特征和优点能够更加明显易懂,下面结合附图对本发明中技术方案作进一步详细的说明:

[0043] 本发明首先提供了一种移动终端恶意代码行为监控和分析的方法,如图1所示,包括:

[0044] S101 将数据库中的软件程序分发至各终端设备中;

[0045] S102 在各终端设备中安装并运行软件程序,模拟用户常用操作触发恶意代码敏感行为,并在各终端设备中设置监视点,若存在敏感行为触发监视点,则记录所述敏感行为并生成行为日志;

[0046] S103 收集各终端设备中的行为日志;

[0047] S104 对于同属一个软件程序的行为日志进行关联分析,判断所述软件程序的危害程度;例如,采用代价敏感的贝叶斯决策算法分析行为序列,最终判断软件程序是否恶意。

[0048] 优选地,所述将数据库中的软件程序分发至各终端设备中为,根据终端设备的负载情况进行软件程序的分发。

[0049] 优选地,所述安装并运行软件程序包括:手动运行或者自动运行软件程序,触发软件程序的恶意行为。

[0050] 其中,触发恶意行为的方式包括:模拟系统广播消息、模拟短信接收或者模拟用户常用操作。

[0051] 优选地,所述监视点包括:短信/wap推送信息监控,数据库操作监控,定位信息监控,网络连接监控,底层操作监控,敏感文件监控。

[0052] 优选地,所述终端设备包括:真实移动终端设备或者设备模拟器;例如,移动通信设备(手持电话,智能电话)、便携式娱乐设备(ipad、GALAXY、PS等)、或者相关的设备模拟器

等。

[0053] 本发明还提供了一种移动终端恶意代码行为监控和分析的系统，如图 2 所示，包括：

[0054] 分发模块 201，用于将数据库中的软件程序分发至各终端设备中；

[0055] 控制模块 202，在各终端设备中安装并运行软件程序，模拟用户常用操作触发恶意代码敏感行为，并在各终端设备中设置监视点，若存在敏感行为触发监视点，则记录所述敏感行为并生成行为日志；

[0056] 回收模块 203，用于收集各终端设备中的行为日志；

[0057] 检测模块 204，对于同属一个软件程序的行为日志进行关联分析，判断所述软件程序的危害程度；例如，采用代价敏感的贝叶斯决策算法分析行为序列，最终判断软件程序是否恶意。

[0058] 优选地，所述分发模块根据终端设备的负载情况进行软件程序的分发。

[0059] 优选地，控制模块中所述安装并运行软件程序包括：手动运行或者自动运行软件程序，触发软件程序的恶意行为。

[0060] 其中，触发恶意行为的方式包括：模拟系统广播消息、模拟短信接收或者模拟用户常用操作。

[0061] 优选地，控制模块中所述监视点包括：短信 /wap 推送信息监控，数据库操作监控，定位信息监控，网络连接监控，底层操作监控，敏感文件监控。

[0062] 优选地，所述终端设备包括：真实移动终端设备或者设备模拟器；例如，移动通信设备（手持电话，智能电话）、便携式娱乐设备（ipad、GALAXY、PS 等）、或者相关的设备模拟器等。

[0063] 如上所述，本发明给出了一种移动终端恶意代码行为监控和分析的方法及系统，其与传统方法的区别在于，对于传统方法来说，其对于移动终端恶意代码检测存在很大的滞后性，检测速度过慢，而本发明所提供的技术方案，通过将海量的软件程序同时分发至各终端设备中，安装并运行，同时模拟用户常用操作，对敏感行为进行动态行为监控，存在敏感行为则记录并分析，从而快速完成软件程序的养殖和行为监控，生成行为日志供专业人员使用。

[0064] 以上实施例用以说明而非限制本发明的技术方案。不脱离本发明精神和范围的任何修改或局部替换，均应涵盖在本发明的权利要求范围当中。

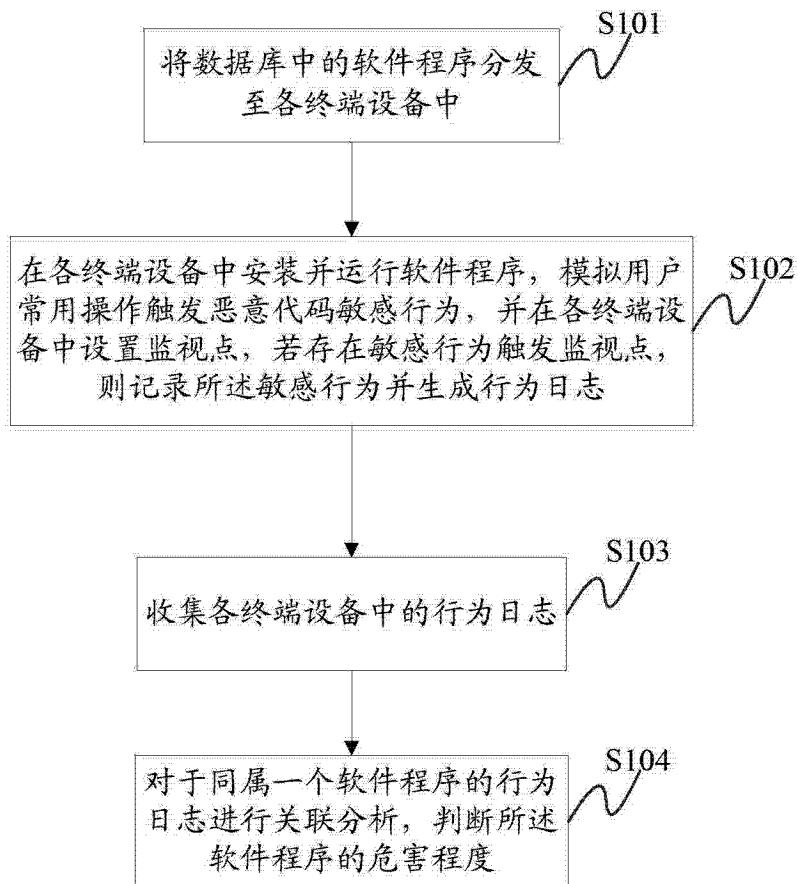


图 1

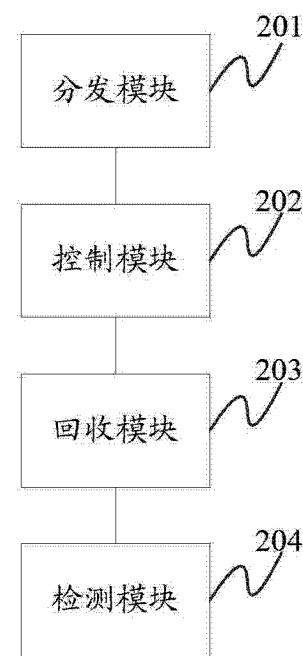


图 2