(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 105721542 B
(45)授权公告日 2018.12.28

(21)申请号 201610029437.7

(22)申请日 2016.01.15

(65)同一申请的已公布的文献号
申请公布号 CN 105721542 A

(43)申请公布日 2016.06.29

(73)专利权人 南京熊猫电子股份有限公司
地址 210002 江苏省南京市中山东路301号
专利权人 南京熊猫信息产业有限公司

(72)发明人 周春健 谢晋 李杨

(74)专利代理机构 南京瑞弘专利商标事务所（普通合伙）32249
代理人 陈琛

(51)Int.Cl.
H04L 29/08(2006.01)
H04L 29/06(2006.01)
H04N 21/436(2011.01)
H04N 21/422(2011.01)
H04N 21/643(2011.01)
H04N 21/443(2011.01)

(56)对比文件
CN 104202666 A,2014.12.10,
CN 103684872 A,2014.03.26,
US 2013086577 A1,2013.04.04,

审查员 丁筱

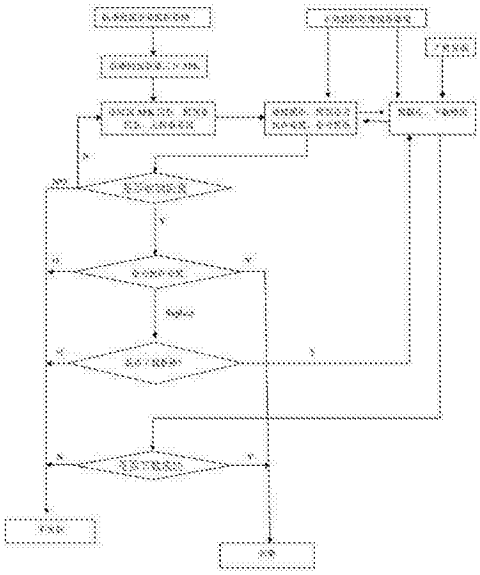
权利要求书1页 说明书3页 附图2页

(54)发明名称

一种基于网络安全监控安装智能机顶盒应用程序的方法

(57)摘要

本发明涉及一种基于网络安全监控安装智能机顶盒应用程序的方法，由安装监控管理服务器端强权决定，客户端忠实执行。客户端在该智能设备上拥有最高权限，可以读取任何文件、终止进程、封堵端口、删除文件、恢复出厂设置等，配合服务器端，共同管理好每一台受控安卓智能设备的软件环境。本发明能在保证一定人权、自由的前提下最大限度的保障安卓网络的安全，带给用户更好更健康更正确的体验。



CN 105721542 B

1.一种基于网络安全监控安装智能机顶盒应用程序的方法，其特征在于，包括以下步骤：

步骤一、智能机顶盒客户端安装APK应用程序启动时，首先由智能机顶盒客户端安装的后台监控模块截取APK应用程序的安全信息，协同智能机顶盒本身安全信息一同上传至安装监控管理服务器，请求权限；

步骤二、安装监控管理服务器将步骤一中接受到的信息与数据库中存储的允许安装的安全信息对比，如果所有信息都与数据库中存储的信息相符，则安装监控管理服务器回复后台监控模块允许安装；如果有任一项在数据库中未找到，则安装监控管理服务器回复后台监控模块不允许安装；

(1)安装监控管理服务器回复后台监控模块允许安装，则提示后台监控模块请权结束，放开权限，继续正常安装流程；

(2)安装监控管理服务器回复后台监控模块不允许安装，则提示后台监控模块请权失败，强制终止安装流程；之后安装监控管理服务器回复后台监控模块需要换成安装监控管理服务器中的安全版本才可安装，后台监控模块在确认后，弹出选择框提示用户是否下载安装监控管理服务器版本并安装，用户选择是则自动切换到下载界面从安装监控管理服务器下载并安装，选择否则终止安装流程。

2.根据权利要求1所述的一种基于网络安全监控安装智能机顶盒应用程序的方法，其特征在于，步骤二中后台监控模块若多次在规定时限内未确认到安装监控管理服务器回复，则提示请权失败，并终止安装流程。

3.根据权利要求1所述的一种基于网络安全监控安装智能机顶盒应用程序的方法，其特征在于，当所待安装的APK应用程序属于安装监控管理服务器中存储的需要替换的APK应用程序时，安装监控管理服务器发送命令要求后台监控模块静默替换APK应用程序，下载安装监控管理服务器版本并安装。

4.根据权利要求1所述的一种基于网络安全监控安装智能机顶盒应用程序的方法，其特征在于，对于已安装的APK应用程序，利用后台监控模块协同安装监控管理服务器实时监控，若智能机顶盒在运行过程中，发现所述APK应用程序有安全漏洞，后台监控模块提交所述APK应用程序的安全信息至安装监控管理服务器，安装监控管理服务器将接受到的信息与数据库中存储的安全信息对比，如果所有信息都与数据库中存储的信息相符，则安装监控管理服务器回复后台监控模块程序安全；如果有任一项在数据库中未找到，则安装监控管理服务器发布命令提示后台监控模块全网删除所述APK应用程序并将APK应用程序加入黑名单；后台监控模块无条件最高优先级第一时间处理安装监控管理服务器发来的命令。

5.根据权利要求1所述的一种基于网络安全监控安装智能机顶盒应用程序的方法，其特征在于，所述APK安全信息包括签名、大小、包名和APK文件校验MD5信息。

6.根据权利要求1所述的一种基于网络安全监控安装智能机顶盒应用程序的方法，其特征在于，所述智能机顶盒本身安全信息包括序列号、账户信息、地址信息。

7.根据权利要求1所述的一种基于网络安全监控安装智能机顶盒应用程序的方法，其特征在于，所述后台监控模块截取APK安全信息，协同智能机顶盒本身安全信息一同以加密方式上传至安装监控管理服务器。

一种基于网络安全监控安装智能机顶盒应用程序的方法

技术领域

[0001] 本发明涉及智能家居领域，尤其涉及一种基于网络安全监控安装智能机顶盒应用程序的方法。

背景技术

[0002] 近年来，安卓系统的智能设备发展的突飞猛进，带给人们丰富多彩的生活资讯和便捷体验，但也带来了各种各样的网络安全问题，如恶意广告、违法行为、反动言论等，给人民生活和社会治安带来负面的影响。

[0003] 在广电机顶盒领域，兹事体大，所以研发厂商关闭自动安装功能，删除手动安装的引导程序，只能通过特定途径安装广电规定的APK(Android安装包)，以保证机顶盒软件生态环境的稳定和可控。

[0004] 任何系统和软件都有漏洞，这些在市场上不受监控的安卓机顶盒、电视如果被黑客或商家恶意劫持，用以发布反动言论提供违法服务时，若没有及时有效的处理手段，必会给网络安全和社会安全带来挑战。

发明内容

[0005] 针对现有技术存在的问题，本发明提供一种基于网络安全监控安装智能机顶盒应用程序的方法，是为控制安卓智能机顶盒安装私有程序的权限并提供应急处理的方法，提供安装前后的监控、紧急情况下的应急处理机制。

[0006] 本发明的技术方案是：一种基于网络安全监控安装智能机顶盒应用程序的方法，包括以下步骤：

[0007] 步骤一、智能机顶盒客户端安装APK应用程序启动时，首先由智能机顶盒客户端安装的后台监控模块截取APK应用程序的安全信息，协同智能机顶盒本身安全信息一同上传至安装监控管理服务器，请求权限；

[0008] 步骤二、安装监控管理服务器将步骤一中接受到的信息与数据库中存储的允许安装的安全信息对比，如果所有信息都与数据库中存储的信息相符，则安装监控管理服务器回复后台监控模块允许安装；如果有任一项在数据库中未找到，则安装监控管理服务器回复后台监控模块不允许安装；

[0009] (1)安装监控管理服务器回复后台监控模块允许安装，则提示后台监控模块请权结束，放开权限，继续正常安装流程；

[0010] (2)安装监控管理服务器回复后台监控模块不允许安装，则提示后台监控模块请权失败，强制终止安装流程；之后安装监控管理服务器回复后台监控模块需要换成安装监控管理服务器中的安全版本才可安装，后台监控模块在确认后，弹出选择框提示用户是否下载安装监控管理服务器版本并安装，用户选择是则自动切换到下载界面从安装监控管理服务器下载并安装，选择否则终止安装流程。

[0011] 进一步的，步骤二中后台监控模块若多次在规定时限内未确认到安装监控管理服

务器回复，则提示请权失败，并终止安装流程。

[0012] 进一步的，当所待安装的APK应用程序属于安装监控管理服务器中存储的需要替换的APK应用程序时，安装监控管理服务器发送命令要求后台监控模块静默替换APK应用程序，下载安装监控管理服务器版本并安装。

[0013] 进一步的，对于已安装的APK应用程序，利用后台监控模块协同安装监控管理服务器实时监控，若智能机顶盒在运行过程中，发现所述APK应用程序有安全漏洞，后台监控模块提交所述APK应用程序的安全信息至安装监控管理服务器，安装监控管理服务器将接受到的信息与数据库中存储的安全信息对比，如果所有信息都与数据库中存储的信息相符，则安装监控管理服务器回复后台监控模块程序安全；如果有任一项在数据库中未找到，则安装监控管理服务器发布命令提示后台监控模块全网删除所述APK应用程序并将APK应用程序加入黑名单；后台监控模块无条件最高优先级第一时间处理安装监控管理服务器发来的命令。

[0014] 进一步的，APK安全信息包括签名、大小、包名和APK文件校验MD5信息。

[0015] 进一步的，本机信息包括序列号、账户信息、地址信息。

[0016] 进一步的，所述后台监控模块截取APK安全信息，协同本机信息一同以加密方式上传至安装监控管理服务器。

[0017] 本发明的效果：本发明涉及一种维护安卓智能设备软件安装和管理的方法，由安装监控管理服务器端强权决定，客户端忠实执行。客户端在该智能设备上拥有最高权限，可以读取任何文件、终止进程、封堵端口、删除文件、恢复出厂设置等，配合服务器端，共同管理好每一台受控安卓智能设备的软件环境。本发明能在保证一定人权、自由的前提下最大限度的保障安卓网络的安全，带给用户更好更健康更正确的体验。

附图说明

[0018] 图1为智能机顶盒安全安装和安装监控管理服务器端响应结构示意图。

[0019] 图2为安装监控管理服务器端紧急处理和智能机顶盒端受理结构示意图。

具体实施方式

[0020] 下面结合附图对本发明做进一步的说明。

[0021] 本发明实施例提供了智能机顶盒基于网络安全安装应用程序，它分为两部分，1为待安装APK应用程序的智能机顶盒客户端程序，2为安装监控管理服务器程序。

[0022] 待安装APK应用程序的智能机顶盒客户端程序放入智能机顶盒系统区，无法删除，拥有root权限；监控管理安装应用的服务器端程序24小时待命，随时监控。

[0023] 图1为本智能机顶盒安全安装和安装监控管理服务器端响应结构示意图，智能机顶盒客户端安装有监控模块，一旦发现有APK应用程序安装，启动安装界面，在安装界面上给出正在检验信息，等待授权。具体的，基于网络安全监控安装智能机顶盒应用程序的方法，包括以下步骤：

[0024] 步骤一、智能机顶盒客户端安装APK应用程序启动时，首先由智能机顶盒客户端安装的后台监控模块截取APK应用程序的安全信息(包括签名、大小、包名和APK文件校验MD5信息)，协同智能机顶盒本身安全信息(包括序列号、账户信息、地址信息)一同以加密方式

上传至安装监控管理服务器，请求权限；

[0025] 步骤二、安装监控管理服务器将步骤一中接受到的信息与数据库中存储的允许安装的安全信息对比，如果所有信息都与数据库中存储的信息相符，则安装监控管理服务器回复后台监控模块允许安装；如果有任一项在数据库中未找到，则安装监控管理服务器回复后台监控模块不允许安装；

[0026] (1)安装监控管理服务器回复后台监控模块允许安装，则提示后台监控模块请权结束，放开权限，继续正常安装流程；

[0027] (2)安装监控管理服务器回复后台监控模块不允许安装，则提示后台监控模块请权失败，强制终止安装流程；之后安装监控管理服务器回复后台监控模块需要换成安装监控管理服务器中的安全版本才可安装，后台监控模块在确认后，弹出选择框提示用户是否下载安装监控管理服务器版本并安装，用户选择是则自动切换到下载界面从安装监控管理服务器下载并安装，选择否则终止安装流程。

[0028] 其中，步骤二中后台监控模块若多次在规定时限内未确认到安装监控管理服务器回复，则提示请权失败，并终止安装流程。且步骤(2)中当所待安装的APK应用程序属于安装监控管理服务器中存储的需要替换的APK应用程序时，安装监控管理服务器发送命令要求后台监控模块静默替换APK应用程序，下载安装监控管理服务器版本并安装。

[0029] 图2安装监控管理服务器端紧急处理和智能机顶盒端受理结构示意图，对于已安装的APK应用程序，利用后台监控模块协同安装监控管理服务器实时监控，若智能机顶盒在运行过程中，发现所述APK应用程序有安全漏洞，后台监控模块提交所述APK应用程序的安全信息至安装监控管理服务器，安装监控管理服务器将接受到的信息与数据库中存储的安全信息对比，如果所有信息都与数据库中存储的信息相符，则安装监控管理服务器回复后台监控模块程序安全；如果有任一项在数据库中未找到，则安装监控管理服务器发布命令提示后台监控模块全网删除所述APK应用程序并将APK应用程序加入黑名单；后台监控模块无条件最高优先级第一时间处理安装监控管理服务器发来的命令，包括重启机顶盒、卸载某应用程序，重新下载安装制定APK等。

[0030] 上述机顶盒实施例中，通过智能机顶盒网络安装和管理安装服务器联动的方法，提供给用户另外一种智能机顶盒安装APK应用程序的方法，保证智能机顶盒安全观看。

[0031] 本说明书中公开的所有特征，或公开的所有方法或过程中的步骤，除了互相排斥的特征和/或步骤以外，均可以以任何方式组合。

[0032] 本说明书(包括任何附加权利要求、摘要和附图)中公开的任一特征，除非特别叙述，均可被其他等效或具有类似目的的替代特征加以替换。即，除非特别叙述，每个特征只是一系列等效或类似特征中的一个例子而已。

[0033] 本发明不局限于安卓智能机顶盒，智能手机、平板、智能电视都可以以类似协议定制维护前端和终端。

[0034] 本发明并不局限于前述的具体实施方式。本发明扩展到任何在本说明书中披露的新特征或任何新的组合，以及披露的任一新的方法或过程的步骤或任何新的组合。

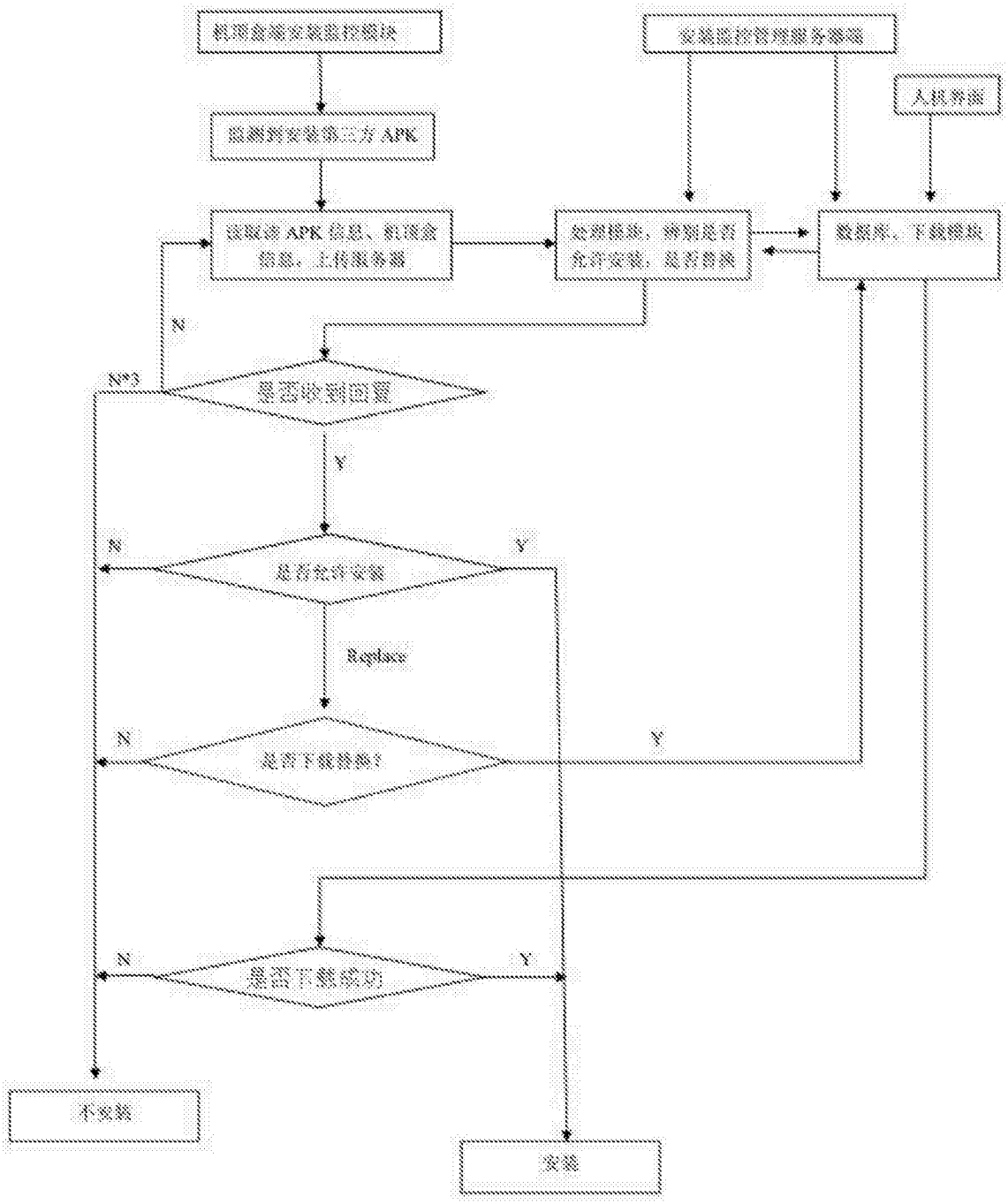

机顶盒端安装监控模块
监测到安装第三方 APK
获取该 APK 信息、机顶盒信息，上传服务器
安装监控管理服务器端
人机界面
处理结果，控制是否允许安装，是否替换
数据库、下载模板
N
N*3
是否收到回复
Y
N
是否允许安装
Y
Replace
N
是否下载替换?
Y
N
是否下载成功
Y
不安装
安装

图1

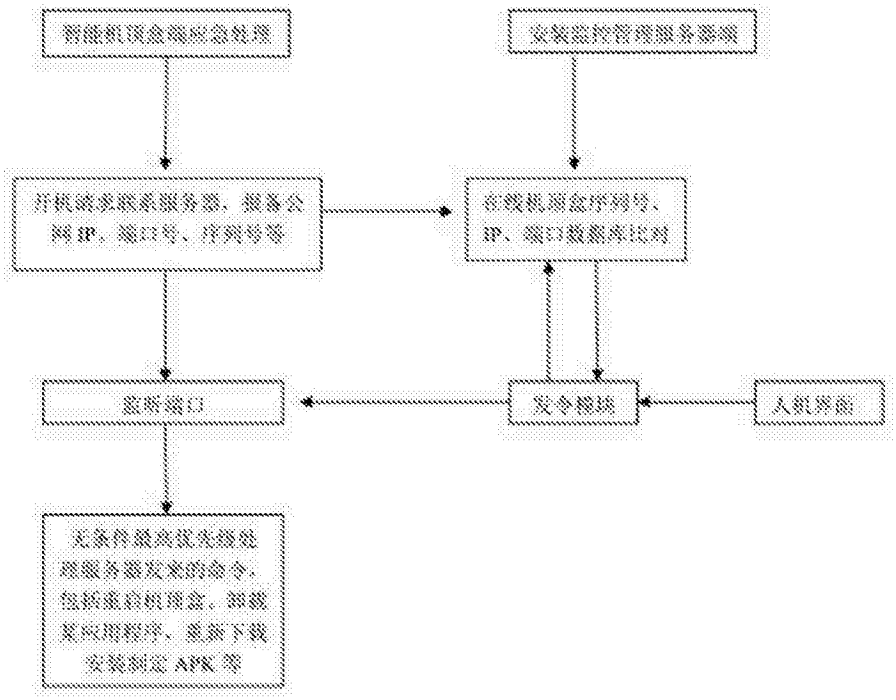

智能机顶盒响应急处理
安装监控管理服务器端
开机请求联系服务器，报备公网IP、端口号、序列号等
在线机顶盒序列号、IP、端口数据库比对
监听端口
发令模块
人机界面
无条件最高级先响应处理服务器发来的命令，包括重启机顶盒、卸载某应用程序、重新下载安装制定APK等

图2