(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 117453456 A
(43)申请公布日 2024.01.26

(21)申请号 202311423401.3

(22)申请日 2023.10.28

(71)申请人 深圳市凯迪仕智能科技股份有限公司

地址 518000 广东省深圳市南山区西丽街道西丽社区仙洞路创智云城二期项目B2栋11层写字楼02办公室

(72)发明人 苏祺云 邹伟 李显 周雪春

(74)专利代理机构 广州三环专利商标代理有限公司 44202

专利代理师 赖妙旋

(51)Int.Cl.

G06F 11/14(2006.01)
G06F 11/08(2006.01)
G06F 8/65(2018.01)
G06F 8/71(2018.01)

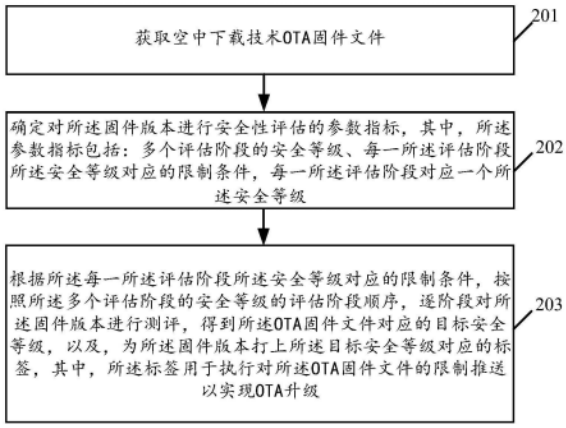
权利要求书2页 说明书17页 附图3页

(54)发明名称

固件版本安全性评估方法及相关装置

(57)摘要

本申请实施例公开了一种固件版本安全性评估方法及相关装置,方法包括:获取空中下载技术OTA固件文件,其中,OTA固件文件对应固件版本;确定对固件版本进行安全性评估的参数指标,其中,参数指标包括:多个评估阶段的安全等级、每一评估阶段安全等级对应的限制条件;根据每一评估阶段安全等级对应的限制条件,按照多个评估阶段的安全等级的评估阶段顺序,逐评估阶段对固件版本进行测评,得到OTA固件文件对应的目标安全等级,以及,为固件版本打上目标安全等级对应的标签,其中,标签用于执行对OTA固件文件的限制推送以实现OTA升级。采用本申请实施例有利于保证OTA升级时的固件安全性,并有利于提高用户使用体验。



CN 117453456 A

1.一种固件版本安全性评估方法,其特征在于,包括:

获取空中下载技术OTA固件文件,其中,所述OTA固件文件对应固件版本;

确定对所述固件版本进行安全性评估的参数指标,其中,所述参数指标包括:多个评估阶段的安全等级、每一所述评估阶段所述安全等级对应的限制条件,每一所述评估阶段对应一个所述安全等级;

根据所述每一所述评估阶段所述安全等级对应的限制条件,按照所述多个评估阶段的安全等级的评估阶段顺序,逐评估阶段对所述固件版本进行测评,得到所述OTA固件文件对应的目标安全等级,以及,为所述固件版本打上所述目标安全等级对应的标签,其中,所述标签用于执行对所述OTA固件文件的限制推送以实现OTA升级。

2.根据权利要求1所述的方法,其特征在于,若所述多个评估阶段的安全等级包括第i评估阶段的安全等级,i为大于或等于2的正整数;

所述根据所述每一所述评估阶段所述安全等级对应的限制条件,按照所述多个评估阶段的安全等级的评估阶段顺序,逐评估阶段对所述固件版本进行测评,得到所述OTA固件文件对应的目标安全等级,包括:

若所述固件版本满足第i-1评估阶段的安全等级对应的限制条件,则确定所述固件版本通过所述第i-1评估阶段的测评,并根据所述第i评估阶段的安全等级对应的所述限制条件,对所述固件版本进行测评;

若所述固件版本未满足所述第i评估阶段的安全等级对应的所述限制条件,则确定所述OTA固件文件对应的所述目标安全等级为所述第i-1评估阶段的安全等级;

若所述固件版本满足所述第i评估阶段的安全等级对应的所述限制条件,则确定所述OTA固件文件对应的所述目标安全等级为所述第i评估阶段的安全等级,或继续根据第i+1评估阶段的安全等级的限制条件,对所述固件版本进行测评。

3.根据权利要求2所述的方法,其特征在于,若所述固件版本满足所述第i评估阶段的安全等级对应的所述限制条件,所述方法还包括:

若所述第i评估阶段为所述多个评估阶段中最高评估阶段,则确定所述OTA固件文件对应的所述目标安全等级为所述第i评估阶段的安全等级;

若所述第i评估阶段不为所述多个评估阶段中所述最高评估阶段,则根据所述第i+1评估阶段的安全等级的限制条件,对所述固件版本进行测评。

4.根据权利要求2或3所述的方法,其特征在于,若所述第i评估阶段的安全等级对应的所述限制条件包括以下至少一种:所述第i评估阶段的评估对象、所述第i评估阶段的评估周期、所述第i评估阶段的限制参数、所述评估周期内所述限制参数对应的阈值;所述根据所述第i评估阶段的安全等级对应的所述限制条件,对所述固件版本进行测评,包括:

将所述第i评估阶段的所述评估对象均分为实验组和参照组,其中,所述实验组和所述参照组对应有相同数量的多个所述评估对象;

向所述实验组内每一所述评估对象推送所述OTA固件文件;

在所述第i评估阶段的评估周期内,监控所述实验组中每一所述评估对象的限制参数和所述参照组中每一所述评估对象的限制参数;

确定所述实验组中所述多个评估对象的限制参数的第一均值,以及参照组中所述多个评估对象的限制参数的第二均值;

根据所述第一均值、第二均值和所述限制参数对应的阈值,对所述固件版本进行测评。

5.根据权利要求4所述的方法,其特征在于,所述根据所述第一均值、第二均值和所述限制参数对应的阈值,对所述固件版本进行测评,包括:

确定所述第一均值和所述第二均值的差值;

若所述差值小于或等于所述限制参数对应的阈值,则确定所述固件版本满足所述第i评估阶段的安全等级对应的所述限制条件;

若所述差值大于所述限制参数对应的阈值,则确定所述固件版本不满足所述第i评估阶段的安全等级对应的所述限制条件,并停止所述第i评估阶段后续所述评估阶段的所述测评。

6.根据权利要求1所述的方法,其特征在于,在所述为所述固件版本打上所述目标安全等级对应的标签之后,所述方法还包括:

根据所述固件版本的标签,确定所述OTA固件文件在OTA任务中的安全推送范围;

根据所述安全推送范围,完成针对所述OTA固件文件的OTA任务推送。

7.根据权利要求1或6所述的方法,其特征在于,所述方法还包括:

若所述固件版本的标签指示所述目标安全等级为所述多个评估阶段的安全等级中最高评估阶段,则停止对所述OTA固件文件对应固件版本的安全性评估,并在后续的OTA任务中不针对所述OTA固件文件进行所述安全性评估。

8.一种固件版本安全性评估装置,其特征在于,所述装置包括:获取单元、确定单元和测评单元,其中,

所述获取单元,用于获取空中下载技术OTA固件文件,其中,所述OTA固件文件对应固件版本;

所述确定单元,用于确定对所述固件版本进行安全性评估的参数指标,其中,所述参数指标包括:多个评估阶段的安全等级、每一所述评估阶段所述安全等级对应的限制条件,每一所述评估阶段对应一个所述安全等级;

所述测评单元,用于根据所述每一所述评估阶段所述安全等级对应的限制条件,按照所述多个评估阶段的安全等级的评估阶段顺序,逐评估阶段对所述固件版本进行测评,得到所述OTA固件文件对应的目标安全等级,以及,为所述固件版本打上所述目标安全等级对应的标签,其中,所述标签用于执行对所述OTA固件文件的限制推送以实现OTA升级。

9.一种服务器,其特征在于,包括处理器、存储器,所述存储器用于存储一个或多个程序,并且被配置由所述处理器执行,所述程序包括用于执行如权利要求1-7任一项所述的方法中的步骤的指令。

10.一种计算机可读存储介质,其特征在于,存储用于电子数据交换的计算机程序,其中,所述计算机程序使得计算机执行如权利要求1-7任一项所述的方法。

固件版本安全性评估方法及相关装置

技术领域

[0001] 本申请涉及固件升级技术领域,具体涉及一种固件版本安全性评估方法及相关装置。

背景技术

[0002] 在物联网时代,能够进行空中下载技术(Over The Air,OTA)升级已经成为电子设备的标准能力。通过物联网OTA升级技术可以实现对于物联网产品的功能和特性的更新,但是,在OTA升级过程中,任何一个小到某功能的升级异常会使得用户体验变差,大到升级固件出现问题可能会直接导致电子设备彻底宕机且不可恢复,因此,确保OTA升级时固件的安全性已经成为亟需解决的问题。

发明内容

[0003] 本申请实施例提供了一种固件版本安全性评估方法及相关装置,有利于保证功能的正常使用,能够保证OTA升级时的固件安全性,并有利于提高用户使用体验。

[0004] 第一方面,本申请实施例提供一种固件版本安全性评估方法,包括:

[0005] 获取空中下载技术OTA固件文件,其中,所述OTA固件文件对应固件版本;

[0006] 确定对所述固件版本进行安全性评估的参数指标,其中,所述参数指标包括:多个评估阶段的安全等级、每一所述评估阶段所述安全等级对应的限制条件,每一所述评估阶段对应一个所述安全等级;

[0007] 根据所述每一所述评估阶段所述安全等级对应的限制条件,按照所述多个评估阶段的安全等级的评估阶段顺序,逐评估阶段对所述固件版本进行测评,得到所述OTA固件文件对应的目标安全等级,以及,为所述固件版本打上所述目标安全等级对应的标签,其中,所述标签用于执行对所述OTA固件文件的限制推送以实现OTA升级。

[0008] 第二方面,本申请实施例提供了一种固件版本安全性评估装置,所述装置包括:获取单元、确定单元和测评单元,其中,

[0009] 所述获取单元,用于获取空中下载技术OTA固件文件,其中,所述OTA固件文件对应固件版本;

[0010] 所述确定单元,用于确定对所述固件版本进行安全性评估的参数指标,其中,所述参数指标包括:多个评估阶段的安全等级、每一所述评估阶段所述安全等级对应的限制条件,每一所述评估阶段对应一个所述安全等级;

[0011] 所述测评单元,用于根据所述每一所述评估阶段所述安全等级对应的限制条件,按照所述多个评估阶段的安全等级的评估阶段顺序,逐评估阶段对所述固件版本进行测评,得到所述OTA固件文件对应的目标安全等级,以及,为所述固件版本打上所述目标安全等级对应的标签,其中,所述标签用于执行对所述OTA固件文件的限制推送以实现OTA升级。

[0012] 第三方面,本申请实施例提供一种服务器,包括处理器、存储器、通信接口以及一个或多个程序,其中,上述一个或多个程序被存储在上述存储器中,并且被配置由上述处理

器执行,上述程序包括用于执行本申请实施例第一方面中所描述的部分或全部步骤的指令。

[0013] 第四方面,本申请实施例提供了一种计算机可读存储介质,其中,上述计算机可读存储介质存储用于电子数据交换的计算机程序,其中,上述计算机程序使得计算机执行如本申请实施例第一方面中所描述的部分或全部步骤。

[0014] 第五方面,本申请实施例提供了一种计算机程序产品,其中,上述计算机程序产品包括存储了计算机程序的非瞬时性计算机可读存储介质,上述计算机程序可操作来使计算机执行如本申请实施例第一方面中所描述的部分或全部步骤。该计算机程序产品可以为一个软件安装包。

[0015] 实施本申请实施例,具备如下有益效果:

[0016] 可以看出,本申请实施例中所描述的固件版本安全性评估方法及相关装置,获取空中下载技术OTA固件文件,其中,所述OTA固件文件对应固件版本;确定对所述固件版本进行安全性评估的参数指标,其中,所述参数指标包括:多个评估阶段的安全等级、每一所述评估阶段所述安全等级对应的限制条件,每一所述评估阶段对应一个所述安全等级;根据所述每一所述评估阶段所述安全等级对应的限制条件,按照所述多个评估阶段的安全等级的评估阶段顺序,逐评估阶段对所述固件版本进行测评,得到所述OTA固件文件对应的目标安全等级,以及,为所述固件版本打上所述目标安全等级对应的标签,其中,所述标签用于执行对所述OTA固件文件的限制推送以实现OTA升级。如此,可在OTA升级之前,实现对于OTA固件文件的安全性评估,能够保证OTA升级时的固件安全性;并且,在确定该OTA固件文件的目标安全等级以后,根据该目标安全等级的标签确定推送范围,以避免在未安全性评估的情况下直接推送有问题OTA固件文件而带来的电子设备功能无法使用等风险,有利于保证功能的正常使用,有利于降低OTA升级带来的风险,并有利于提高用户使用体验。

附图说明

[0017] 为了更清楚地说明本申请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,下面描述中的附图仅仅是本申请的一些实施例,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。

[0018] 图1是本申请实施例提供的一种固件版本安全性评估系统的架构示意图;

[0019] 图2是本申请实施例提供的一种固件版本安全性评估方法的流程示意图;

[0020] 图3是本申请实施例提供的一种服务器的结构示意图;

[0021] 图4A是本申请实施例提供的一种固件版本安全性评估装置的功能单元组成框图;

[0022] 图4B是本申请实施例提供的一种固件版本安全性评估装置的功能单元组成框图。

具体实施方式

[0023] 为了使本技术领域的人员更好地理解本申请方案,下面将结合本申请实施例中的附图,对本申请实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本申请一部分实施例,而不是全部的实施例。基于本申请中的实施例,本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例,都属于本申请保护的范围。

[0024] 本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别不同对象,而不是用于描述特定顺序。此外,术语“包括”和“具有”以及它们任何变形,意图在于覆盖不排他的包含。例如包含了一系列步骤或单元的过程、方法、系统、产品或电子设备没有限定于已列出的步骤或单元,而是可选地还包括没有列出的步骤或单元,或可选地还包括对于这些过程、方法、产品或电子设备固有的其他步骤或单元。

[0025] 在本文中提及“实施例”意味着,结合实施例描述的特定特征、结构或特性可以包含在本申请的至少一个实施例中。在说明书中的各个位置出现该短语并不一定均是指相同的实施例,也不是与其它实施例互斥的独立的或备选的实施例。本领域技术人员显式地和隐式地理解的是,本文所描述的实施例可以与其它实施例相结合。

[0026] 请参见图1,图1为本申请实施例提供的一种固件版本安全性评估系统的架构示意图。如图1所示,该固件版本安全性评估系统包括:电子设备100a、电子设备100b、电子设备100c和服务器200a。

[0027] 其中,本申请实施例中的电子设备100a和/或电子设备100b和/或电子设备100c可以包括智能手机(如Android手机、iOS手机、Windows Phone手机等)、平板电脑、掌上电脑、行车记录仪、车载电子设备、服务器、笔记本电脑、移动互联网电子设备(MID,Mobile Internet Devices)或穿戴式电子设备(如智能手表、蓝牙耳机)等,上述仅是举例,而非穷举,包含但不限于上述电子设备。

[0028] 其中,上述服务器200a可以包括但不限于后台服务器、组件服务器、固件版本安全性评估系统服务器、固件版本安全性评估软件服务器或OTA升级服务器等,服务器可以通过互联网与多个上述电子设备进行通信。服务器将客服推送结果发送到用户对应的电子设备,可通过该服务器建立用户与客服之间的通信连接。

[0029] 示例的,在一次安全性评估过程中,测试人员或者电子设备运维人员可以向服务器200a中固件版本安全性评估系统上传空中下载技术OTA固件文件,服务器200a可获取上述OTA固件文件,该OTA固件文件对应固件版本,并确定对固件版本进行安全性评估的参数指标,其中,该参数指标包括:多个评估阶段的安全等级、每一所述评估阶段所述安全等级对应的限制条件,每一所述评估阶段对应一个所述安全等级;服务器200a还可根据每一所述评估阶段所述安全等级对应的限制条件,按照多个评估阶段的安全等级的评估阶段顺序,逐评估阶段对固件版本进行测评,得到OTA固件文件对应的目标安全等级,以及,为固件版本打上目标安全等级对应的标签,其中,标签用于执行向多个电子设备100a和/或电子设备100b和/或电子设备100c限制推送OTA固件文件,以实现OTA升级。

[0030] 进一步地,在每一次安全等级评估过程中,服务器200a可向测试人员或者电子设备运维人员推送最终得到的该OTA固件文件对应的目标安全等级的标签,以告知测试人员或者电子设备运维人员该OTA固件文件版本的推送限制。

[0031] 请参阅图2,图2是本申请实施例提供的一种固件版本安全性评估方法的流程示意图;该方法包括:

[0032] 201、获取空中下载技术OTA固件文件,其中,所述OTA固件文件对应固件版本。

[0033] 202、确定对所述固件版本进行安全性评估的参数指标,其中,所述参数指标包括:多个评估阶段的安全等级、每一所述评估阶段所述安全等级对应的限制条件,每一所述评估阶段对应一个所述安全等级。

[0034] 其中,本申请实施例可应用于服务器,具体可包括如图1所示的固件版本安全性评估系统中的服务器200a。

[0035] 其中,上述固件版本用于表征在本次根据OTA固件文件执行OTA升级的版本号。OTA固件文件用于推送到如图1中的电子设备100a和/或电子设备100b和/或电子设备100c,以实现对于客户端的固件版本的OTA升级。

[0036] 其中,服务器可响应于测试人员或运维人员在对应显示器中的操作选项的选择,自动调度多个安全评估阶段对应的安全性评估模型,完成本次安全性评估。上述操作选项可以包括“立即评估”或“手动评估”;若服务器识别到“立即评估”的操作选项,则自动调度安全性评估模型。

[0037] 进一步地,若服务器识别到“手动评估”的操作选项,则默认OTA固件文件的安全等级为最低级,即最小或最低评估阶段的安全等级,测试人员或运维人员可在后续的任意时间手动操作服务器中程序自动化固件安全等级评估模块以启动本申请实施例所描述的固件版本安全性评估方法,以实现对于OTA固件文件的安全性评估。

[0038] 其中,上述参数指标包括以下至少一种:多个评估阶段的安全等级、每一所述评估阶段所述安全等级对应的限制条件等等,在此不作限定。上述多个评估阶段存在评估阶段顺序,即先后顺序,可逐评估阶段对OTA固件文件对应固件版本进行测评。

[0039] 其中,服务器可预设多个安全等级评估模型,用于对OTA固件文件的安全等级进行数据建模,每一安全等级评估模型可对应一个上述安全等级;并且每一评估阶段可对应一个上述安全等级,上述多个评估阶段可以是连续设置的,服务器可根据每一评估阶段的安全等级对应的限制条件设置上述安全等级评估模型,并且每一评估阶段的安全等级对应的限制条件是存在关联关系的。

[0040] 示例的,在针对上述每一评估阶段的安全等级的安全性评估或者测评过程中,服务器可以针对该评估阶段的安全等级评估模型选择至少两套样本数据,实际参考样本可以是多个参照组,一套样本数据可作为安全性评估或者测评过程中的实验对象,其数量可根据实际需要或者条件设定;另外一套样本数据可以作为参照组,形成对上述实验对象的观察参照和数据对比的基准对象。

[0041] 需要说明的是,多个可指两个或两个以上,后续不再赘述。

[0042] 203、根据所述每一所述评估阶段所述安全等级对应的限制条件,按照所述多个评估阶段的安全等级的评估阶段顺序,逐评估阶段对所述固件版本进行测评,得到所述OTA固件文件对应的目标安全等级,以及,为所述固件版本打上所述目标安全等级对应的标签,其中,所述标签用于执行对所述OTA固件文件的限制推送以实现OTA升级。

[0043] 其中,服务器可以根据实际业务的特征或者需求拆分,以将其拆分为多个评估阶段的安全等级对应的多个限制条件,且每一评估阶段的安全等级可对应一个限制条件,因此,上述多个评估阶段的安全等级对应的多个限制条件之间存在逻辑关系或者业务特征关系。例如,针对评估阶段1-评估阶段4的安全等级,评估阶段2的安全等级对应限制条件,默认满足其前面顺序的评估阶段1的安全等级对应的限制条件,评估阶段3的安全等级对应的限制条件,也默认满足其前面顺序的评估阶段1和评估阶段2的限制条件。

[0044] 其中,上述限制条件可用于限制测试人员或者电子设备运维人员推送OTA固件文件。上述限制条件可为用户自行设置或者系统默认,在此不作限定。

[0045] 其中,不同的评估阶段的限制条件是不同的,上述限制条件可包括以下至少一种:每一评估阶段对应的评估对象、评估对象的数量、每一评估阶段对应的评估周期、每一评估阶段对应的限制参数、每一评估阶段对应评估周期内该限制参数对应的阈值等等,在此不作限定。

[0046] 其中,上述评估阶段顺序可指多个评估阶段的评估顺序。例如,针对S0-S4评估阶段,越小的评估阶段越靠前评估,S0的评估顺序优先于S1评估阶段,S1评估阶段的评估顺序优先于S2评估阶段,以此类推。

[0047] 其中,上述评估对象可以是电子设备,可指符合OTA升级条件的电子设备。

[0048] 其中,不同评估阶段的评估对象的数量可以按需配置,由于实际的业务中,不同的物联网产品的销售情况并不是平均分布的,多数情况下也遵循二八定律,即80%的销量集中到20%的产品型号,在产品长尾的销售数据的数据量会出现断崖式跳跃,这时候,不同的评估阶段的限制条件中的评估对象的数量,可以根据服务器推送的推荐模型和用户自定义条件模型组合方式,以形成该安全等级对应的安全等级模型,以实现评估对象的数据抽样。

[0049] 其中,在上述推荐模型中,服务器可以设置不同的数据梯度模型,例如,可以是相对比例与绝对数量组合条件模型、系统自动数据梯度模型,且该推荐模型应该满足最低数量与最高数量的数据抽取的边界条件。

[0050] 示例的,针对评估阶段1来说,其对应的评估对象应该最低满足5台电子设备,最高50台电子设备的抽样边界数值条件,以及,再叠加用户自定义筛选条件,但是其自定义抽样条件影响抽样的随机性或者抽样特征,但是不影响抽样的数值边界模型,例如最终得到的评估阶段1的安全等级模型的评估对象仍旧最低满足5台电子设备,最高50台抽样的边界条件。

[0051] 示例的,上述评估对象的数量可以是10台、100台、1000台、10000台等等,在此不作限定;不同评估阶段的安全等级的评估对象的数量可以不同,例如,针对评估阶段1-评估阶段4的安全等级,评估阶段越高,其对应的评估对象的数量可以越多。

[0052] 示例的,上述评估对象的数量还可以是指符合OTA升级条件的评估对象总量的0.5%、2%、80%等。例如,针对评估阶段1-评估阶段4的安全等级,评估阶段越高,其对应的评估对象的数量的占比越大。

[0053] 其中,上述评估周期可以是按小时观测,连续24小时、36小时、72小时等、或者按天观测,连续7天、15天、30天等。

[0054] 其中,上述每一评估阶段的限制参数可不同,该限制参数可以是实时在线电子设备数量占比、低功耗电子设备剩余电量、用户完成配网使用时长、电子设备是否处于活跃时间窗口等等,在此不限定。上述活跃时间窗口可以是夜晚是人的睡眠时间、或者根据使用场景与人的睡觉时间形成电子设备是否可能处于活跃的窗口的时间段。

[0055] 其中,上述标签可用于标记OTA固件文件在本次安全性评估过程中的安全等级,即目标安全等级,该标签可用于提示电子设备运维人员当前OTA固件文件的限制条件,以根据限制条件实现限制推送,例如,针对评估阶段S0-评估阶段S4的安全等级,评估阶段越高或越大,则对应的限制推送范围越大。

[0056] 其中,针对任意一个评估阶段,若进入下一评估阶段评估时,服务器会自动给OTA固件文件打上通过该评估阶段的安全等级测评的标签,例如,若多个评估阶段为S0-S4评估

阶段,通过了S1评估阶段的安全测试,那么服务器则自动给OTA固件文件打上安全等级为S1的标签。

[0057] 其中,服务器在执行对所述OTA固件文件的限制推送时,可以根据该目标安全等级对应的安全推送范围确定。

[0058] 可选地,若所述多个评估阶段的安全等级包括第i评估阶段的安全等级,i为大于或等于2的正整数;上述步骤203,所述根据所述每一所述评估阶段所述安全等级对应的限制条件,按照所述多个评估阶段的安全等级的评估阶段顺序,逐评估阶段对所述固件版本进行测评,得到所述OTA固件文件对应的目标安全等级,可包括如下步骤:

[0059] A1、若所述固件版本满足第i-1评估阶段的安全等级对应的限制条件,则确定所述固件版本通过所述第i-1评估阶段的测评,并根据所述第i评估阶段的安全等级对应的所述限制条件,对所述固件版本进行测评;

[0060] A2、若所述固件版本未满足所述第i评估阶段的安全等级对应的所述限制条件,则确定所述OTA固件文件对应的所述目标安全等级为所述第i-1评估阶段的安全等级;

[0061] A3、若所述固件版本满足所述第i评估阶段的安全等级对应的所述限制条件,则确定所述OTA固件文件对应的所述目标安全等级为所述第i评估阶段的安全等级,或继续根据第i+1评估阶段的安全等级的限制条件,对所述固件版本进行测评。

[0062] 其中,上述第i评估阶段可指多个评估阶段的中间评估阶段,i为大于或等于2的正整数。

[0063] 其中,每相邻的两个测评评估阶段的限制条件是可以继承的,例如,若i为2,进入第i+1评估阶段的OTA固件文件默认是满足第i评估阶段(第2评估阶段)和第i-1评估阶段(第1评估阶段)分别对应的限制条件的。

[0064] 其中,每一评估阶段的限制条件,可用于评估该OTA固件文件是否能够进入下一评估阶段的安全等级的测评。

[0065] 示例的,服务器可设置多个评估阶段的安全等级,分别对应S0评估阶段、S1评估阶段、S2评估阶段、S3评估阶段和S4评估阶段,如下所示,每一评估阶段的安全等级的定义以及每一评估阶段的具体目标或者安全等级评估模型的用途如下:

[0066] S0评估阶段:安全性未知,表示未进行固件安全评估版本,若目标安全等级为S0评估阶段,可认为OTA固件文件在OTA升级时存在升级风险;

[0067] S1评估阶段:完成基本安全测试;在该评估阶段中可抽样OTA升级过程中的验证流程以验证或确认该OTA固件文件的安全性,确保不会出现OTA固件文件OTA升级事故,例如:升级固件错误造成电子设备变砖无法使用需要返厂维修才能恢复、电子设备OTA升级之后无法联网等情况。

[0068] S2评估阶段:完成抽样批次电子设备OTA升级之后的基于发布/订阅模式的轻量级消息传输协议(Message Queuing Telemetry Transport,MQTT)长连接稳定性监测;

[0069] S3评估阶段:完成抽样电子设备OTA升级之后低功耗电子设备耗电异常监测;

[0070] S4评估阶段:完成评估数量(例如,可以是绝对数量,可动态设定例如1000台、10000台等)的评估对象对应电子设备的OTA推送,并且能够OTA升级完成,以及通过上述S1-S3评估阶段的安全性评估或测评。

[0071] 其中,可以通过不同安全等级的限制条件实现上述不同的评估阶段的测评。

[0072] 举例来说,若针对OTA固件文件,若i＝3,即第i评估阶段对应上述S3评估阶段。服务器评估OTA固件文件对应的固件版本时,若该固件版本满足S2评估阶段(第i-1评估阶段)的限制条件,即该固件版本完成抽样批次电子设备OTA升级,且监测得到的MQTT长连接稳定性的限制参数满足其对应的阈值条件,则可确定该固件版本通过S2评估阶段的测评,则可进入S3评估阶段的测评,并确定OTA固件文件对应的目标安全等级为S2评估阶段的安全等级。

[0073] 进一步地,若固件版本满足S3评估阶段的测评,即完成OTA升级之后电子设备的耗电异常监测,且监控到的耗电异常情况对应的限制参数满足其对应的阈值条件,则可确定OTA固件文件满足S3评估阶段对应的限制条件,则确定该固件版本进入S4评估阶段(第i+1评估阶段)的测评,则进一步可确定此时OTA固件文件对应的目标安全等级为S3评估阶段的安全等级。

[0074] 进一步地,在上述过程中,在进入S3评估阶段的测评时,若该固件版本不满足S3评估阶段的限制条件,即未完成抽样批次电子设备OTA升级,和/或监控到MQTT长连接稳定性的限制参数不满足其对应的阈值条件,则可以停止S3评估阶段的测评,并最终确定OTA固件文件对应的目标安全等级为S2评估阶段的安全等级。

[0075] 再进一步地,在确定该固件版本进入S4评估阶段的测评之后,可继续对该OTA固件文件的固件版本的测评,即可进入S4评估阶段的测评,若OTA固件文件的固件版本满足S4评估阶段的安全等级对应的限制条件,即在大规模的评估数量下,能够完成90％-100％比例的电子设备的OTA升级,则可确定OTA固件文件的固件版本满足S4评估阶段的安全等级对应的限制条件,则可将OTA固件文件对应的目标安全等级更新为S4评估阶段对应的安全等级,并停止对OTA固件文件的固件版本的安全性评估或者测评。

[0076] 因此,服务器可在确定OTA固件文件的固件版本进入到任意一个中间的评估阶段的安全性评估或测评过程时,则可确定OTA固件文件的固件版本对应的目标安全等级为该中间的评估阶段上一评估阶段的评估阶段对应的安全等级,并在OTA固件文件的固件版本通过该中间的评估阶段的测评,即满足该中间的评估阶段的安全等级的限制条件以后,更新OTA固件文件的固件版本对应的目标安全等级为该中间的评估阶段的安全等级,以此类推,直到确定最终的其不满足的评估阶段的安全等级的限制条件,或者直到进入最后评估阶段或最高评估阶段的安全等级的测评,则终止对于该OTA固件文件的固件版本的安全性测评。

[0077] 需要说明的是,在上述步骤中,每一次确定OTA固件文件对应的目标安全等级之后,均可为该OTA固件文件或对应的固件版本打上该目标安全等级对应的标签,在通过后续评估阶段的测评以后,可实时更新上述OTA固件文件或对应的固件版本的目标安全等级的标签。

[0078] 可选地,若i＝1,即在多个评估阶段的第一评估阶段,若固件版本满足第一评估阶段的安全等级对应的限制条件,则继续对该OTA固件文件进行固件版本安全性的测评,即进入测评第二评估阶段,若固件版本不满足第一评估阶段的安全等级对应的限制条件,则终止对于OTA固件文件的测评。

[0079] 可见,本示例中,服务器可以自动化完成OTA固件文件或固件等级的安全性评估,无需电子设备运维人员手动分评估阶段测评,有利于提高人力成本和时间成本。并且,服务

器在每一次中间评估阶段的安全性评估时,需要满足该中间评估阶段之前评估阶段的限制条件,可以将风险范围控制在可控范围内,有利于提高后续通过OTA固件文件实现OTA升级的安全性。可选地,在上述步骤A1之后,上述方法还可包括如下步骤:

[0080] A4、若所述固件版本不满足第i-1评估阶段的安全等级对应的限制条件,则终止进入第i评估阶段的测评。

[0081] 可见,本示例中,在任意一个评估阶段,若固件版本不满足该评估阶段的安全等级对应的限制条件,则终止下一评估阶段的安全性评估,并且在任意一个评估阶段,若固件版本满足该评估阶段的安全等级对应的限制条件,则自动进入下一评估阶段的安全性评估,如此,可以实现中间安全等级的控制,有利于实现中间评估阶段控制整体的OTA升级风险,并有利于减少OTA升级风险。

[0082] 可选地,若所述固件版本满足所述第i评估阶段的安全等级对应的所述限制条件,上述步骤A2,还可包括如下步骤:

[0083] A21、若所述第i评估阶段为所述多个评估阶段中最高评估阶段,则确定所述OTA固件文件对应的所述目标安全等级为所述第i评估阶段的安全等级;

[0084] A22、若所述第i评估阶段不为所述多个评估阶段中所述最高评估阶段,则根据所述第i+1评估阶段的安全等级的限制条件,对所述固件版本进行测评。

[0085] 可见,本示例中,在逐评估阶段对所述固件版本进行测评时,如果测评到了最后一个评估阶段,即最高评估阶段,且固件版本满足最高评估阶段的安全等级对应的限制条件,则确定测评结束;若当前测评的评估阶段未到最后一个评估阶段,则进入下一评估阶段的所述OTA固件文件安全性的测评;如此,可以实现本次固件版本安全性评估流程,有利于体现固件版本安全性评估的整体性。

[0086] 可选地,若所述第i评估阶段的安全等级对应的所述限制条件包括以下至少一种:所述第i评估阶段的评估对象、所述第i评估阶段的评估周期、所述第i评估阶段的限制参数、所述评估周期内所述限制参数对应的阈值;在上述步骤A1中,所述根据所述第i评估阶段的安全等级对应的所述限制条件,对所述固件版本进行测评,上述方法可包括如下步骤:

[0087] A11、将所述第i评估阶段的所述评估对象均分为实验组和参照组,其中,所述实验组和所述参照组对应有相同数量的多个所述评估对象;

[0088] A12、向所述实验组内每一所述评估对象推送所述OTA固件文件;

[0089] A13、在所述第i评估阶段的评估周期内,监控所述实验组中每一所述评估对象的限制参数和所述参照组中每一所述评估对象的限制参数;

[0090] A14、确定所述实验组中所述多个评估对象的限制参数的第一均值,以及参照组中所述多个评估对象的限制参数的第二均值;

[0091] A15、根据所述第一均值、第二均值和所述限制参数对应的阈值,对所述固件版本进行测评。

[0092] 其中,服务器可以通过每一评估阶段对应的限制条件,设置其对应的安全评估模型,并在该安全评估模型内,根据安全等级对应的限制条件,对固件版本或OTA固件文件进行安全性的测评。

[0093] 在本示例中,仅以其中的第i评估阶段作为示例,第i评估阶段可以是下述S0-S4评估阶段的中间评估阶段,例如,可以是S2-S3评估阶段中任意一个评估阶段,当然,第i评估

阶段也可以是最后一个评估阶段,即S4评估阶段。

[0094] 其中,服务器可以向第i评估阶段中评估对象为实验组内每一电子设备推送OTA固件文件,服务器还可监控实验组中每一评估对象的限制参数和参照组中每一所述评估对象的限制参数,以收集实验组与参照组对应电子设备在执行OTA升级过程中的升级的数据分析指标,以用于评估是否能够通过第i评估阶段的测评,以及是否进入第i+1评估阶段的测评。

[0095] 示例的,第i评估阶段的限制参数可以是在线电子设备数量占比或者MQTT电子设备掉线与重连次数占比,限制参数对应的具体数据可以作为数据分析指标。

[0096] 举例来说,针对上述S0-S4评估阶段,更具体地,服务器可根据每一评估阶段对应的限制条件中限制参数,设置其对应的安全等级模型,以用于实现对应评估阶段的安全性的测评:

[0097] S0安全评估模型:针对未进行安全性评估的OTA固件文件,可指测试人员或者电子设备运维人员通过电子设备管理后台上传的OTA固件文件,默认其对应的固件安全等级为S0。

[0098] S1安全评估模型:选取少量评估对象(例如10台、20台等数量电子设备)进行OTA升级,在对应的评估周期内监控得到评估对象对应的OTA升级的成功率、重新上线率,进而判断OTA固件文件的正确性。并通过设定的S1测评评估阶段对应的阈值来判断是否自动进入下一评估阶段,或者自动终止安全性评估或测评,服务器可针对自动终止的OTA固件文件生成并输出评估报告。

[0099] S2安全评估模型:抽取S2评估阶段的评估数量(该评估数量的选取可以参考电子设备OTA因素条件)的评估对象作为S2评估模型的评估对象;同时,将评估对象分割成为实验组和参照组;例如,根据设定的电子设备OTA因素条件抽取200台电子设备作为S2评估对象,其中100台作为实验组,另外100台作为参照组;实验组进行OTA固件文件的自动推送,参照组则不推送OTA固件文件,只作为观测对象。

[0100] 其中,S2评估模型需要满足S1评估模型的限制条件,同时,叠加该S2评估阶段的限制条件,与参照组对比MQTT长连接稳定的监测,例如,服务器可设定连续24小时、或者连续7天或30天等测评周期(涉及到时间因素,时间越长评估越准,实际要参考业务因素来设置评估时间,服务器可以参数化动态配置该评估周期),并在测评周期内监测MQTT长连接稳定性,即该S2评估阶段的限制参数,例如,可以是实验组中多个评估对象的限制参数的第一均值,以及参照组中多个评估对象的限制参数的第二均值,并根据第一均值、第二均值和该评估阶段对应的阈值,判断是否自动进入S3评估阶段。

[0101] S3安全评估模型:S3评估阶段的评估对象和评估数量可以继承S2评估阶段,也可以单独抽取样本作为评估对象。

[0102] 其中,该评估阶段的评估方法与S2评估阶段基本一致,S3评估模型需要满足S2评估模型的限制条件。S3评估模型或S3评估阶段对应的限制条件可以是:在评估周期内上报的电子设备剩余电量,服务器可以根据电子设备剩余电量构建耗电量异常监控数据分析模型,并通过该评估阶段对应的阈值判断是否终止或者进入S4评估阶段的安全性评估;对于通过S3评估阶段的OTA固件文件,则自动化进入S4评估阶段,如果未通过S3评估阶段的安全性评估或者测评,即确定耗电存在异常的情况下,则自动终止下一评估阶段的评估,生成并

输出用于警告用电异常的测评报告,以便于电子设备运维人员查看。

[0103] S4安全评估模型:S4评估阶段评估对应的评估对象的评估数量是最大的,这个评估阶段需要将电子设备推送和监控的范围扩大一个较大数量的范围,例如最多1000台、或者最少1%比例条件执行OTA升级,并对其进行自动OTA升级推送。

[0104] 其中,S4自动化安全评估模型需要满足S1-S3的评估模型对应的限制条件;并通过扩大测评对象的测评数量的范围来自动化完成有规模的数据量的OTA安全性推送测试。

[0105] 其中,针对通过S4评估阶段评估的OTA固件文件,电子设备运维人员可以自由的进行任意数量(最多全量电子设备)的电子设备OTA升级。

[0106] 可见,本示例中,服务器可以根据第i评估阶段的安全评估模型实现对于OTA固件文件的评估阶段性安全性评估,以确定其是否满足第i评估阶段的测评,有利于实现评估阶段性的安全性测评;并且,能够在测评过程中输出评估报告,有利于测评人员非常直观的判断OTA升级固件的安全性,有利于帮助测评人员及时了解到测评评估阶段的测评结果,有利于在后续评估阶段实现问题的复现,从而,有利于提高安全性评估效率。

[0107] 可选地,上述步骤A15中,所述根据所述第一均值、第二均值和所述限制参数对应的阈值,对所述固件版本进行测评,上述方法可包括如下步骤:

[0108] A151、确定所述第一均值和所述第二均值的差值;

[0109] A152、若所述差值小于或等于所述限制参数对应的阈值,则确定所述固件版本满足所述第i评估阶段的安全等级对应的所述限制条件;

[0110] A153、若所述差值大于所述限制参数对应的阈值,则确定所述固件版本不满足所述第i评估阶段的安全等级对应的所述限制条件,并停止所述第i评估阶段后续所述评估阶段的所述测评。

[0111] 其中,上述阈值可为用户自行设置或者系统默认,在此不作限定。

[0112] 其中,在每一评估阶段中,如果在评估周期结束仍未达到进入下一评估阶段的测评,即确定固件版本不满足第i评估阶段的安全等级对应的限制条件,则服务器可以终止测评,生成并输出测评报告,该测评报告中可以指示在该第i评估阶段测评失败或者安全性评估失败,且在测评报告中还可以指示该OTA固件文件的目标安全等级为第i-1评估阶段的安全等级。

[0113] 需要说明的是,若测试人员上传错误固件等级,那么可能会在第一个评估阶段(例如,上述S0评估阶段)就不满足其对应安全等级,则也可以认为评估失败,可以终止测评,并输出用于指示安全性评估失败的测评报告,那么在OTA推送时,可以选择一个电子设备执行OTA推送,或者不执行OTA推送。

[0114] 示例的,由于在不同的评估阶段,均可能出现评估失败的情况,实际情况针对安全测评的固件从S1评估阶段到S4评估阶段任意一个安全测评评估阶段都可能会失败,并且失败的原因会存在多种复杂的情况,不能单纯的使用测评失败就是固件存在问题的结论,有可能是样本数据的问题、固件本身存在问题影响了监控指标结果、电子设备网络问题等各种复杂的情况。因此,针对未测试通过安全性测试的OTA固件文件,服务器对应系统允许重复性提交固件安全性等级测试。

[0115] 进一步地,针对测试未通过的OTA固件文件对应的测评报告,也用于指示电子设备运维人员或者测试人员判断是否存在必要进行重复安全性测试,针对非常明确的固件安全

性问题的情况应该重新回到OTA固件文件问题修复以及OTA固件文件测试流程,服务器可针对OTA固件文件执行新一轮的安全性评估,并重复执行上述步骤A1-A3及其相关步骤。

[0116] 需要说明的是,在本示例中,是通过阈值判断OTA固件文件或其对应固件版本不满足第i评估阶段的安全等级对应的限制条件,其他方法也适用于本方法。

[0117] 可见,本示例中,服务器可以在多个评估阶段的中间评估阶段,通过限制参数对应的阈值,实现对于OTA固件文件的安全性评估,即安全等级测评,并在第i评估阶段的安全等级不满足该评估阶段的限制参数时,停止后续评估阶段的测评,考虑到随着测评评估阶段的提高,其对应的安全推送范围是越大的,因此,服务器可以在中间评估阶段规避大规模或大范围推送带来的风险和损失,用最小的代价避免因为上传错误OTA固件文件的固件版本等人为问题造成的OTA升级,有利于提高OTA升级的安全性,有利于规避规模化的OTA升级带来的风险。

[0118] 可选地,上述步骤203之后,在所述为所述固件版本打上所述目标安全等级对应的标签之后,上述方法还可包括如下步骤:

[0119] B1、根据所述固件版本的标签,确定所述OTA固件文件在OTA任务中的安全推送范围;

[0120] B2、根据所述安全推送范围,完成针对所述OTA固件文件的OTA任务推送。

[0121] 其中,每一目标安全等级或标签可对应有一个安全推送范围,该安全推送范围可用于限制OTA推送的范围,目标安全等级的等级越高,则设定其对应的安全推送范围越大。

[0122] 举例来说,可以将安全推送范围设置为递增方式,针对S0评估阶段的目标安全等级,其对应的安全推送范围可以是1-10台或不推送;针对S1评估阶段的目标安全等级,其对应的安全推送范围可以是100台;针对S2评估阶段的目标安全等级,其对应的安全推送范围可以是1000台;针对S3评估阶段的目标安全等级,其对应的安全推送范围可以是5000台;针对S4评估阶段的目标安全等级,其对应的安全推送范围可以不限制,例如,可以是10000台等等。

[0123] 可选地,在完成针对所述OTA固件文件的OTA任务推送的执行过程中,或者推送完成后,若标签指示未达到多个评估阶段的安全等级的最高等级,服务器还可以自动化执行继续对该固件版本进行安全性评估,并更新该标签,安全性评估的方式如上步骤202及其相关步骤所示,那么,在该OTA固件文件的下一次OTA任务过程中,可以直接根据该标签,确定新的安全推送范围,以实现对于OTA固件文件的OTA升级。

[0124] 可见,本示例中,服务器可以根据标签,直接确定其对应的安全推送范围,以完成该目标安全等级的限制推送,有利于实现OTA升级的安全推送,有利于降低OTA大规模升级风险。

[0125] 可选地,上述步骤203之后或步骤B1之后,上述方法还可包括如下步骤:

[0126] C1、若所述固件版本的标签指示所述目标安全等级为所述多个评估阶段的安全等级中最高评估阶段,则停止对所述OTA固件文件对应固件版本的安全性评估,并在后续的OTA任务中不针对所述OTA固件文件进行所述安全性评估。

[0127] 其中,例如,通过S4评估阶段的OTA固件文件,服务器不再对其的OTA升级的规模数量或者范围进行限制,同时,通过S4评估阶段的安全性评估的OTA固件文件,后续OTA任务的执行过程中也可以不再参与本申请实施例中所描述的固件版本安全性评估,不属于安全性

监控的范围。

[0128] 可见,本示例中,服务器可以针对未通过最高评估阶段的OTA固件文件进行限制推送,即OTA限制升级,有利于从关键路径上通过程序化的设定避免运维人员不按照流程操作的管理风险。并针对通过最高评估阶段的OTA固件文件的不限制其推送范围,设置不限制其参与固件版本安全性评估,可以让设备运维人员在大规模推送OTA升级任务时不再关心OTA升级固件的安全性问题,而且,有利于防止出现规模化OTA升级造成风险给企业和用户带来的损失。

[0129] 可以看出,本申请实施例中所描述的固件版本安全性评估方法,获取空中下载技术OTA固件文件,其中,所述OTA固件文件对应固件版本;确定对所述固件版本进行安全性评估的参数指标,其中,所述参数指标包括:多个评估阶段的安全等级、每一所述评估阶段所述安全等级对应的限制条件,每一所述评估阶段对应一个所述安全等级;根据所述每一所述评估阶段所述安全等级对应的限制条件,按照所述多个评估阶段的安全等级的评估阶段顺序,逐评估阶段对所述固件版本进行测评,得到所述OTA固件文件对应的目标安全等级,以及,为所述固件版本打上所述目标安全等级对应的标签,其中,所述标签用于执行对所述OTA固件文件的限制推送以实现OTA升级。如此,可在OTA升级之前,实现对于OTA固件文件的安全性评估,能够保证OTA升级时的固件安全性;并且,在确定该OTA固件文件的目标安全等级以后,根据该目标安全等级的标签确定推送范围,以避免在未安全性评估的情况下直接推送有问题OTA固件文件而带来的电子设备功能无法使用等风险,有利于保证功能的正常使用,有利于降低OTA升级带来的风险,并有利于提高用户使用体验。

[0130] 与上述实施例一致地,请参阅图3,图3是本申请实施例提供的一种服务器的结构示意图,如图所示,该服务器包括处理器、存储器、通信接口以及一个或多个程序,上述一个或多个程序被存储在上述存储器中,并且被配置由上述处理器执行,上述程序包括用于执行以下步骤的指令:

[0131] 获取空中下载技术OTA固件文件,其中,所述OTA固件文件对应固件版本;

[0132] 确定对所述固件版本进行安全性评估的参数指标,其中,所述参数指标包括:多个评估阶段的安全等级、每一所述评估阶段所述安全等级对应的限制条件,每一所述评估阶段对应一个所述安全等级;

[0133] 根据所述每一所述评估阶段所述安全等级对应的限制条件,按照所述多个评估阶段的安全等级的评估阶段顺序,逐评估阶段对所述固件版本进行测评,得到所述OTA固件文件对应的目标安全等级,以及,为所述固件版本打上所述目标安全等级对应的标签,其中,所述标签用于执行对所述OTA固件文件的限制推送以实现OTA升级。

[0134] 在一个可能的示例中,若所述多个评估阶段的安全等级包括第i评估阶段的安全等级,i为大于或等于2的正整数;

[0135] 在所述根据所述每一所述评估阶段所述安全等级对应的限制条件,按照所述多个评估阶段的安全等级的评估阶段顺序,逐评估阶段对所述固件版本进行测评,得到所述OTA固件文件对应的目标安全等级方面,上述程序包括用于执行以下步骤的指令:

[0136] 若所述固件版本满足第i-1评估阶段的安全等级对应的限制条件,则确定所述固件版本通过所述第i-1评估阶段的测评,并根据所述第i评估阶段的安全等级对应的所述限制条件,对所述固件版本进行测评;

[0137] 若所述固件版本未满足所述第i评估阶段的安全等级对应的所述限制条件,则确定所述OTA固件文件对应的所述目标安全等级为所述第i-1评估阶段的安全等级;

[0138] 若所述固件版本满足所述第i评估阶段的安全等级对应的所述限制条件,则确定所述OTA固件文件对应的所述目标安全等级为所述第i评估阶段的安全等级,或继续根据第i+1评估阶段的安全等级的限制条件,对所述固件版本进行测评。

[0139] 在一个可能的示例中,若所述固件版本满足所述第i评估阶段的安全等级对应的所述限制条件,上述程序还包括用于执行以下步骤的指令:

[0140] 若所述第i评估阶段为所述多个评估阶段中最高评估阶段,则确定所述OTA固件文件对应的所述目标安全等级为所述第i评估阶段的安全等级;

[0141] 若所述第i评估阶段不为所述多个评估阶段中所述最高评估阶段,则根据所述第i+1评估阶段的安全等级的限制条件,对所述固件版本进行测评。

[0142] 在一个可能的示例中,若所述第i评估阶段的安全等级对应的所述限制条件包括以下至少一种:所述第i评估阶段的评估对象、所述第i评估阶段的评估周期、所述第i评估阶段的限制参数、所述评估周期内所述限制参数对应的阈值;在所述根据所述第i评估阶段的安全等级对应的所述限制条件,对所述固件版本进行测评方面,上述程序包括用于执行以下步骤的指令:

[0143] 将所述第i评估阶段的所述评估对象均分为实验组和参照组,其中,所述实验组和所述参照组对应有相同数量的多个所述评估对象;

[0144] 向所述实验组内每一所述评估对象推送所述OTA固件文件;

[0145] 在所述第i评估阶段的评估周期内,监控所述实验组中每一所述评估对象的限制参数和所述参照组中每一所述评估对象的限制参数;

[0146] 确定所述实验组中所述多个评估对象的限制参数的第一均值,以及参照组中所述多个评估对象的限制参数的第二均值;

[0147] 根据所述第一均值、第二均值和所述限制参数对应的阈值,对所述固件版本进行测评。

[0148] 在一个可能的示例中,在所述根据所述第一均值、第二均值和所述限制参数对应的阈值,对所述固件版本进行测评方面,上述程序包括用于执行以下步骤的指令:

[0149] 确定所述第一均值和所述第二均值的差值;

[0150] 若所述差值小于或等于所述限制参数对应的阈值,则确定所述固件版本满足所述第i评估阶段的安全等级对应的所述限制条件;

[0151] 若所述差值大于所述限制参数对应的阈值,则确定所述固件版本不满足所述第i评估阶段的安全等级对应的所述限制条件,并停止所述第i评估阶段后续所述评估阶段的所述测评。

[0152] 在一个可能的示例中,在所述为所述固件版本打上所述目标安全等级对应的标签之后,上述程序还包括用于执行以下步骤的指令:

[0153] 根据所述固件版本的标签,确定所述OTA固件文件在OTA任务中的安全推送范围;

[0154] 根据所述安全推送范围,完成针对所述OTA固件文件的OTA任务推送。

[0155] 在一个可能的示例中,上述程序还包括用于执行以下步骤的指令:

[0156] 若所述固件版本的标签指示所述目标安全等级为所述多个评估阶段的安全等级

中最高评估阶段,则停止对所述OTA固件文件对应固件版本的安全性评估,并在后续的OTA任务中不针对所述OTA固件文件进行所述安全性评估。

[0157] 可以看出,本申请实施例中所描述的服务器,获取空中下载技术OTA固件文件,其中,所述OTA固件文件对应固件版本;确定对所述固件版本进行安全性评估的参数指标,其中,所述参数指标包括:多个评估阶段的安全等级、每一所述评估阶段所述安全等级对应的限制条件,每一所述评估阶段对应一个所述安全等级;根据所述每一所述评估阶段所述安全等级对应的限制条件,按照所述多个评估阶段的安全等级的评估阶段顺序,逐评估阶段对所述固件版本进行测评,得到所述OTA固件文件对应的目标安全等级,以及,为所述固件版本打上所述目标安全等级对应的标签,其中,所述标签用于执行对所述OTA固件文件的限制推送以实现OTA升级。如此,可在OTA升级之前,实现对于OTA固件文件的安全性评估,能够保证OTA升级时的固件安全性;并且,在确定该OTA固件文件的目标安全等级以后,根据该目标安全等级的标签确定推送范围,以避免在未安全性评估的情况下直接推送有问题OTA固件文件而带来的电子设备功能无法使用等风险,有利于保证功能的正常使用,有利于降低OTA升级带来的风险,并有利于提高用户使用体验。

[0158] 图4A是本申请实施例中所涉及的一种固件版本安全性评估装置400的功能单元组成框图,所述固件版本安全性评估装置400包括:获取单元401、确定单元402和测评单元403,其中,

[0159] 所述获取单元401,用于获取空中下载技术OTA固件文件,其中,所述OTA固件文件对应固件版本;

[0160] 所述确定单元402,用于确定对所述固件版本进行安全性评估的参数指标,其中,所述参数指标包括:多个评估阶段的安全等级、每一所述评估阶段所述安全等级对应的限制条件,每一所述评估阶段对应一个所述安全等级;

[0161] 所述测评单元403,用于根据所述每一所述评估阶段所述安全等级对应的限制条件,按照所述多个评估阶段的安全等级的评估阶段顺序,逐评估阶段对所述固件版本进行测评,得到所述OTA固件文件对应的目标安全等级,以及,为所述固件版本打上所述目标安全等级对应的标签,其中,所述标签用于执行对所述OTA固件文件的限制推送以实现OTA升级。

[0162] 在一个可能的示例中,若所述多个评估阶段的安全等级包括第i评估阶段的安全等级,i为大于或等于2的正整数;

[0163] 在所述根据所述每一所述评估阶段所述安全等级对应的限制条件,按照所述多个评估阶段的安全等级的评估阶段顺序,逐评估阶段对所述固件版本进行测评,得到所述OTA固件文件对应的目标安全等级方面,上述测评单元403具体用于:

[0164] 若所述固件版本满足第i-1评估阶段的安全等级对应的限制条件,则确定所述固件版本通过所述第i-1评估阶段的测评,并根据所述第i评估阶段的安全等级对应的所述限制条件,对所述固件版本进行测评;

[0165] 若所述固件版本未满足所述第i评估阶段的安全等级对应的所述限制条件,则确定所述OTA固件文件对应的所述目标安全等级为所述第i-1评估阶段的安全等级;

[0166] 若所述固件版本满足所述第i评估阶段的安全等级对应的所述限制条件,则确定所述OTA固件文件对应的所述目标安全等级为所述第i评估阶段的安全等级,或继续根据第

i+1评估阶段的安全等级的限制条件,对所述固件版本进行测评。

[0167] 在一个可能的示例中,若所述固件版本满足所述第i评估阶段的安全等级对应的所述限制条件,上述测评单元403具体还用于:

[0168] 若所述第i评估阶段为所述多个评估阶段中最高评估阶段,则确定所述OTA固件文件对应的所述目标安全等级为所述第i评估阶段的安全等级;

[0169] 若所述第i评估阶段不为所述多个评估阶段中所述最高评估阶段,则根据所述第i+1评估阶段的安全等级的限制条件,对所述固件版本进行测评。

[0170] 在一个可能的示例中,若所述第i评估阶段的安全等级对应的所述限制条件包括以下至少一种:所述第i评估阶段的评估对象、所述第i评估阶段的评估周期、所述第i评估阶段的限制参数、所述评估周期内所述限制参数对应的阈值;在所述根据所述第i评估阶段的安全等级对应的所述限制条件,对所述固件版本进行测评方面,上述测评单元403具体用于:

[0171] 将所述第i评估阶段的所述评估对象均分为实验组和参照组,其中,所述实验组和所述参照组对应有相同数量的多个所述评估对象;

[0172] 向所述实验组内每一所述评估对象推送所述OTA固件文件;

[0173] 在所述第i评估阶段的评估周期内,监控所述实验组中每一所述评估对象的限制参数和所述参照组中每一所述评估对象的限制参数;

[0174] 确定所述实验组中所述多个评估对象的限制参数的第一均值,以及参照组中所述多个评估对象的限制参数的第二均值;

[0175] 根据所述第一均值、第二均值和所述限制参数对应的阈值,对所述固件版本进行测评。

[0176] 在一个可能的示例中,在所述根据所述第一均值、第二均值和所述限制参数对应的阈值,对所述固件版本进行测评方面,上述测评单元403具体用于:

[0177] 确定所述第一均值和所述第二均值的差值;

[0178] 若所述差值小于或等于所述限制参数对应的阈值,则确定所述固件版本满足所述第i评估阶段的安全等级对应的所述限制条件;

[0179] 若所述差值大于所述限制参数对应的阈值,则确定所述固件版本不满足所述第i评估阶段的安全等级对应的所述限制条件,并停止所述第i评估阶段后续所述评估阶段的所述测评。

[0180] 在一个可能的示例中,与图4A一致的,如图4B所示,在图4A的基础上,上述固件版本安全性评估装置400还包括:推送单元404,在所述为所述固件版本打上所述目标安全等级对应的标签之后,上述推送单元404用于:

[0181] 根据所述固件版本的标签,确定所述OTA固件文件在OTA任务中的安全推送范围;

[0182] 根据所述安全推送范围,完成针对所述OTA固件文件的OTA任务推送。

[0183] 在一个可能的示例中,上述测评单元403具体用于:

[0184] 若所述固件版本的标签指示所述目标安全等级为所述多个评估阶段的安全等级中最高评估阶段,则停止对所述OTA固件文件对应固件版本的安全性评估,并在后续的OTA任务中不针对所述OTA固件文件进行所述安全性评估。

[0185] 可以看出,本申请实施例中所描述的固件版本安全性评估装置,获取空中下载技

术OTA固件文件,其中,所述OTA固件文件对应固件版本;确定对所述固件版本进行安全性评估的参数指标,其中,所述参数指标包括:多个评估阶段的安全等级、每一所述评估阶段所述安全等级对应的限制条件,每一所述评估阶段对应一个所述安全等级;根据所述每一所述评估阶段所述安全等级对应的限制条件,按照所述多个评估阶段的安全等级的评估阶段顺序,逐评估阶段对所述固件版本进行测评,得到所述OTA固件文件对应的目标安全等级,以及,为所述固件版本打上所述目标安全等级对应的标签,其中,所述标签用于执行对所述OTA固件文件的限制推送以实现OTA升级。如此,可在OTA升级之前,实现对于OTA固件文件的安全性评估,能够保证OTA升级时的固件安全性;并且,在确定该OTA固件文件的目标安全等级以后,根据该目标安全等级的标签确定推送范围,以避免在未安全性评估的情况下直接推送有问题OTA固件文件而带来的电子设备功能无法使用等风险,有利于保证功能的正常使用,有利于降低OTA升级带来的风险,并有利于提高用户使用体验。

[0186] 可以理解的是,本实施例的固件版本安全性评估装置的各程序模块的功能可根据上述方法实施例中的方法具体实现,其具体实现过程可以参照上述方法实施例的相关描述,此处不再赘述。

[0187] 本申请实施例还提供一种计算机存储介质,其中,该计算机存储介质存储用于电子数据交换的计算机程序,该计算机程序使得计算机执行如上述方法实施例中记载的任一方法的部分或全部步骤,上述计算机包括服务器。

[0188] 本申请实施例还提供一种计算机程序产品,上述计算机程序产品包括存储了计算机程序的非瞬时性计算机可读存储介质,上述计算机程序可操作来使计算机执行如上述方法实施例中记载的任一方法的部分或全部步骤。该计算机程序产品可以为一个软件安装包,上述计算机包括服务器。

[0189] 需要说明的是,对于前述的各方法实施例,为了简单描述,故将其都表述为一系列的动作组合,但是本领域技术人员应该知悉,本申请并不受所描述的动作顺序的限制,因为依据本申请,某些步骤可以采用其他顺序或者同时进行。其次,本领域技术人员也应该知悉,说明书中所描述的实施例均属于优选实施例,所涉及的动作和模块并不一定是本申请所必须的。

[0190] 在上述实施例中,对各个实施例的描述都各有侧重,某个实施例中没有详述的部分,可以参见其他实施例的相关描述。

[0191] 在本申请所提供的几个实施例中,应该理解到,所揭露的装置,可通过其它的方式实现。例如,以上所描述的装置实施例仅仅是示意性的,例如上述单元的划分,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,例如多个单元或组件可以结合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。另一点,所显示或讨论的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,装置或单元的间接耦合或通信连接,可以是电性或其它的形式。

[0192] 上述作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者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者全部单元来实现本实施例方案的目的。

[0193] 另外,在本申请各个实施例中的各功能单元可以集成在一个处理单元中,也可以

是各个单元单独物理存在,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,也可以采用软件功能单元的形式实现。

[0194] 上述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时,可以存储在一个计算机可读取存储器中。基于这样的理解,本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或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器中,包括若干指令用以使得一台计算机电子设备(可为个人计算机、服务器或者网络电子设备等)执行本申请各个实施例上述方法的全部或部分步骤。而前述的存储器包括:U盘、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

[0195] 本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成,该程序可以存储于一计算机可读存储器中,存储器可以包括:闪存盘、只读存储器(英文:Read-Only Memory,简称:ROM)、随机存取器(英文:Random Access Memory,简称:RAM)、磁盘或光盘等。

[0196] 以上对本申请实施例进行了详细介绍,本文中应用了具体个例对本申请的原理及实施方式进行了阐述,以上实施例的说明只是用于帮助理解本申请的方法及其核心思想;同时,对于本领域的一般技术人员,依据本申请的思想,在具体实施方式及应用范围上均会有改变之处,综上所述,本说明书内容不应理解为对本申请的限制。

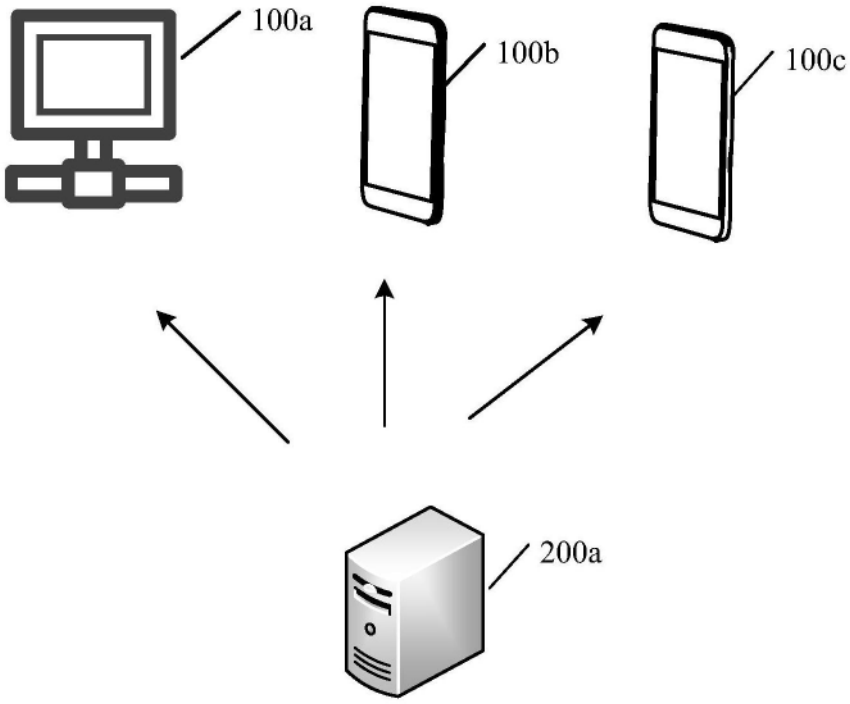

100a
100b
100c
200a

图1

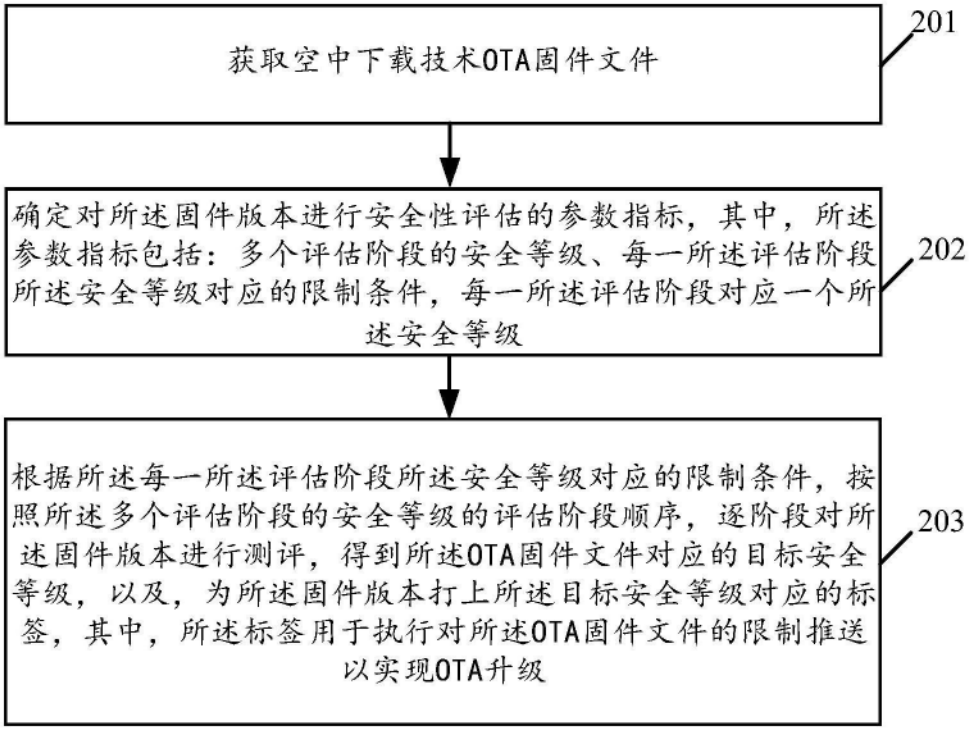

获取空中下载技术OTA固件文件
201
确定对所述固件版本进行安全性评估的参数指标，其中，所述参数指标包括：多个评估阶段的安全等级、每一所述评估阶段所述安全等级对应的限制条件，每一所述评估阶段对应一个所述安全等级
202
根据所述每一所述评估阶段所述安全等级对应的限制条件，按照所述多个评估阶段的安全等级的评估阶段顺序，逐阶段对所述固件版本进行测评，得到所述OTA固件文件对应的目标安全等级，以及，为所述固件版本打上所述目标安全等级对应的标签，其中，所述标签用于执行对所述OTA固件文件的限制推送以实现OTA升级
203

图2

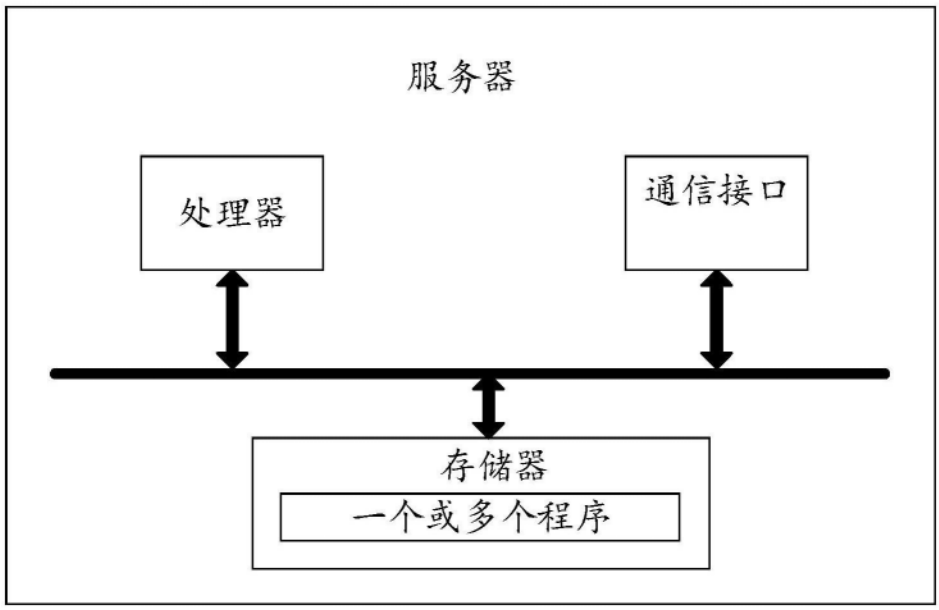

服务器
处理器
通信接口
存储器
一个或多个程序

图3

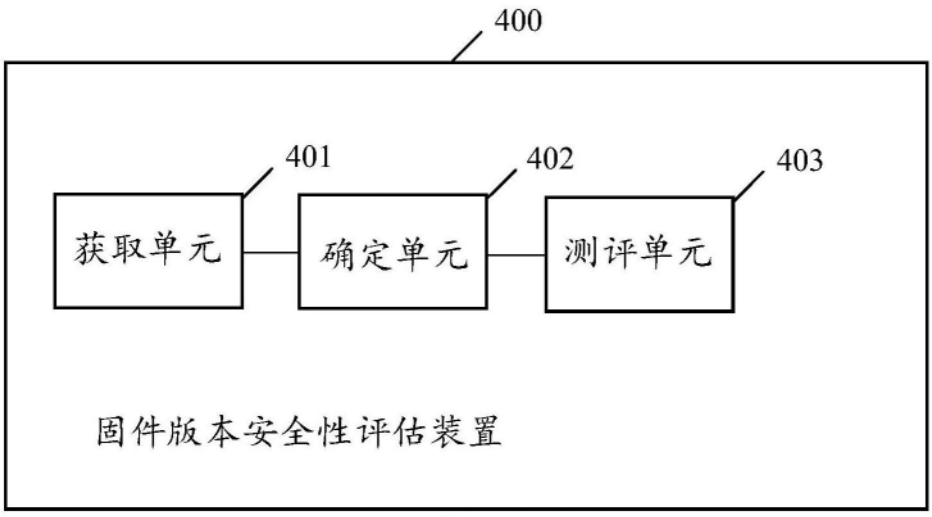

400
401
402
403
获取单元
确定单元
测评单元
固件版本安全性评估装置

图4A

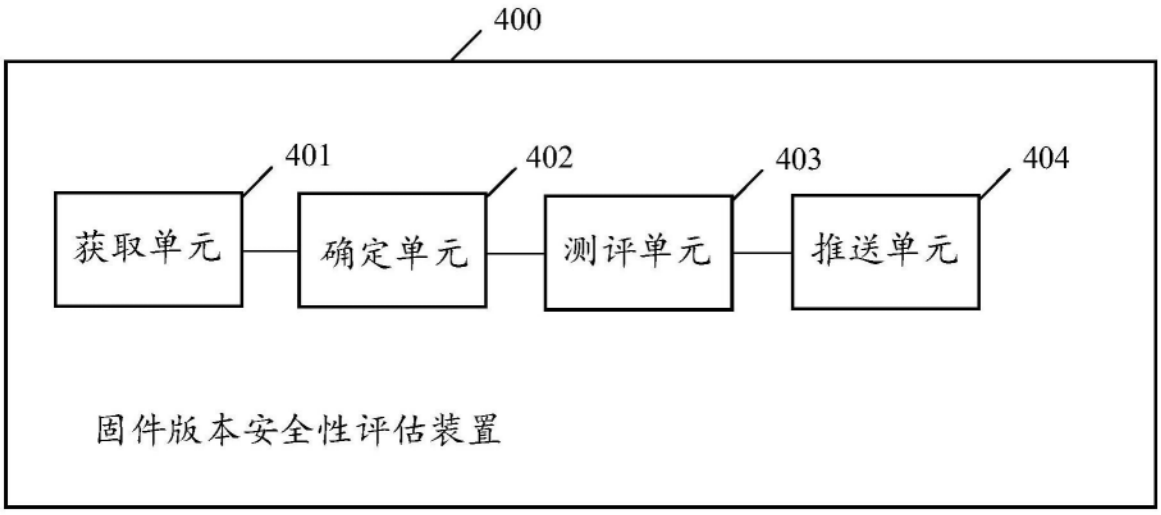


图4B