(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111641610 B
(45)授权公告日 2023.04.07

(21)申请号 202010426368.X

(22)申请日 2020.05.19

(65)同一申请的已公布的文献号
申请公布号 CN 111641610 A

(43)申请公布日 2020.09.08

(73)专利权人 深信服科技股份有限公司
地址 518055 广东省深圳市南山区学苑大道1001号南山智园A1栋

(72)发明人 吕晓滨

(74)专利代理机构 北京派特恩知识产权代理有限公司 11270
专利代理师 刘星雨 张颖玲

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 67/125(2022.01)

(56)对比文件
CN 108490914 A,2018.09.04
CN 110851253 A,2020.02.28
US 2003033599 A1,2003.02.13
JP 2006277752 A,2006.10.12
CN 110609480 A,2019.12.24
CN 110022294 A,2019.07.16
CN 110245004 A,2019.09.17

审查员 吴超

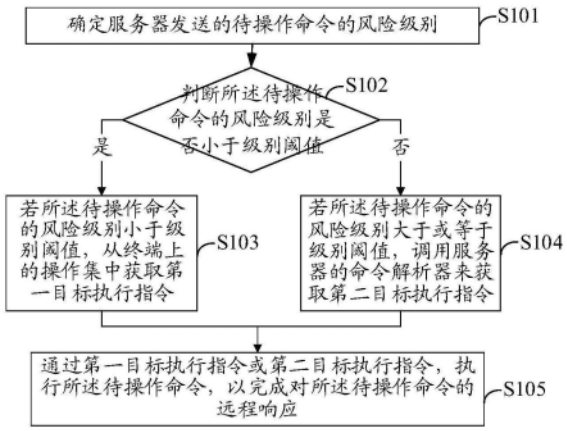
权利要求书3页 说明书19页 附图8页

(54)发明名称

远程响应和远程控制方法、装置、设备及存储介质

(57)摘要

本申请实施例提供一种远程响应和远程控制方法、装置、设备及计算机可读存储介质，其中，远程响应方法包括：确定服务器发送的待操作命令的风险级别；若所述待操作命令的风险级别小于级别阈值，从终端上的操作集中获取第一目标执行指令；若所述待操作命令的风险级别大于或等于所述级别阈值，调用所述服务器的命令解析器来获取第二目标执行指令；通过所述第一目标执行指令或所述第二目标执行指令，执行所述待操作命令，以完成对所述待操作命令的远程响应。



CN 111641610 B

1.一种远程响应方法,其特征在于,包括:

确定服务器发送的待操作命令的风险级别;

若所述待操作命令的风险级别小于级别阈值,获取所述风险级别小于所述级别阈值的至少一操作命令、和每一所述操作命令对应的执行指令,将所述操作命令、所述操作命令对应的执行指令、和所述操作命令与所述执行指令之间的映射关系,封装在终端上的操作集中,从所述终端上的操作集中获取第一目标执行指令;

若所述待操作命令的风险级别大于或等于所述级别阈值,调用所述服务器的命令解析器来获取第二目标执行指令;所述第二目标执行指令为运维人员输入命令解析器的命令;

通过所述第一目标执行指令或所述第二目标执行指令,执行所述待操作命令,以完成对所述待操作命令的远程响应。

2.根据权利要求1所述的方法,其特征在于,所述调用所述服务器的命令解析器来获取第二目标执行指令,包括:

向所述服务器发送命令解析器调用请求,以使所述服务器响应于所述命令解析器调用请求,向终端发送所述第二目标执行指令。

3.根据权利要求1所述的方法,其特征在于,所述终端上部署有第一代理程序,所述服务器上部署有第二代理程序;所述方法还包括:

调用终端上的第一代理程序和所述服务器上的第二代理程序;

通过所述第一代理程序和所述第二代理程序,建立所述终端与所述服务器之间的数据传输通道;

通过所述数据传输通道,接收所述第二代理程序发送的所述待操作命令。

4.根据权利要求3所述的方法,其特征在于,所述通过所述第一目标执行指令或所述第二目标执行指令,执行所述待操作命令,以完成对所述待操作命令的远程响应,包括:

确定所述第一目标执行指令中对应于所述待操作命令的第一目标操作,或者,确定所述第二目标执行指令中对应于所述待操作命令的第二目标操作;

对应执行所述第一目标操作或所述第二目标操作,实现对所述待操作命令的响应,得到命令执行结果;

通过所述数据传输通道,将所述命令执行结果发送给所述服务器,以完成对所述待操作命令的远程响应。

5.根据权利要求4所述的方法,其特征在于,所述方法还包括:

获取预设时间段内所接收到的至少一待操作命令、和每一所述待操作命令对应的命令执行结果;

建立每一所述命令执行结果与对应待操作命令之间的映射关系;

将所述映射关系存储于待审计列表中;

输出所述待审计列表,以实现对所述待审计列表中的至少一所述命令执行结果和/或至少一所述待操作命令进行审计。

6.一种远程控制方法,其特征在于,包括:

确定待操作命令的风险级别;

若所述待操作命令的风险级别小于级别阈值,向终端发送所述待操作命令,以使得终端从操作集中获取第一目标执行指令;所述操作集是通过获取所述风险级别小于所述级别

阈值的至少一操作命令、和每一所述操作命令对应的执行指令，将所述操作命令、所述操作命令对应的执行指令、和所述操作命令与所述执行指令之间的映射关系进行封装构成的；

若所述待操作命令的风险级别大于或等于所述级别阈值，向终端发送所述待操作命令，并基于所述终端的命令解析器调用请求，调用服务器的命令解析器来获取第二目标执行指令；所述第二目标执行指令为运维人员输入命令解析器的命令；

接收所述终端返回的命令执行结果，以完成对所述终端的远程控制，其中，所述命令执行结果是所述终端通过所述第一目标执行指令或所述第二目标执行指令执行所述待操作命令得到的。

7.根据权利要求6所述的方法，其特征在于，所述方法还包括：

接收所述终端发送的命令解析器调用请求；

响应于所述命令解析器调用请求，调用所述命令解析器来获取所述第二目标执行指令；

将所述第二目标执行指令发送给所述终端。

8.根据权利要求6所述的方法，其特征在于，所述终端上部署有第一代理程序，所述服务器上部署有第二代理程序；所述方法还包括：

调用服务器上的第二代理程序和所述终端上的第一代理程序；

通过所述第二代理程序和所述第一代理程序，建立所述服务器与所述终端之间的数据传输通道；

通过所述数据传输通道，向所述第一代理程序发送所述待操作命令。

9.根据权利要求6所述的方法，其特征在于，所述方法还包括：

获取预设时间段内发送的至少一待操作命令、和每一所述待操作命令对应的命令执行结果；

建立每一所述待操作命令与对应命令执行结果之间的映射关系；

将所述映射关系存储于待审计列表中；

输出所述待审计列表，以实现对所述待审计列表中的至少一所述命令执行结果和/或至少一所述待操作命令进行审计。

10.一种远程响应装置，其特征在于，所述装置包括：

第一确定模块，用于确定服务器发送的待操作命令的风险级别；

第一获取模块，用于若所述待操作命令的风险级别小于级别阈值，获取所述风险级别小于所述级别阈值的至少一操作命令、和每一所述操作命令对应的执行指令，将所述操作命令、所述操作命令对应的执行指令、和所述操作命令与所述执行指令之间的映射关系，封装在终端上的操作集中，从所述终端上的操作集中获取第一目标执行指令；

第一调用模块，用于若所述待操作命令的风险级别大于或等于所述级别阈值，调用所述服务器的命令解析器来获取第二目标执行指令；所述第二目标执行指令为运维人员输入命令解析器的命令；

第一执行模块，用于通过所述第一目标执行指令或所述第二目标执行指令，执行所述待操作命令，以完成对所述待操作命令的远程响应。

11.一种远程控制装置，其特征在于，所述装置包括：

第二确定模块，用于确定待操作命令的风险级别；

第一发送模块，用于若所述待操作命令的风险级别小于级别阈值，向终端发送所述待操作命令，以使得终端从操作集中获取第一目标执行指令；所述操作集是通过获取所述风险级别小于所述级别阈值的至少一操作命令、和每一所述操作命令对应的执行指令，将所述操作命令、所述操作命令对应的执行指令、和所述操作命令与所述执行指令之间的映射关系进行封装构成的；

第二发送模块，用于若所述待操作命令的风险级别大于或等于所述级别阈值，向终端发送所述待操作命令，并基于所述终端的命令解析器调用请求，调用服务器的命令解析器来获取第二目标执行指令；所述第二目标执行指令为运维人员输入命令解析器的命令；

第二接收模块，用于接收所述终端返回的命令执行结果，以完成对所述终端的远程控制，其中，所述命令执行结果是所述终端通过所述第一目标执行指令或所述第二目标执行指令执行所述待操作命令得到的。

12.一种远程响应设备，其特征在于，所述设备包括：

存储器，用于存储可执行指令；处理器，用于执行所述存储器中存储的可执行指令时，实现权利要求1至5任一项所述的方法。

13.一种远程控制设备，其特征在于，所述设备包括：

存储器，用于存储可执行指令；处理器，用于执行所述存储器中存储的可执行指令时，实现权利要求6至9任一项所述的方法。

14.一种存储介质，其特征在于，存储有可执行指令，用于引起处理器执行时，实现权利要求1至5任一项，或者，6至9任一项所述的方法。

远程响应和远程控制方法、装置、设备及存储介质

技术领域

[0001] 本申请涉及网络安全领域，涉及但不限于一种远程响应和远程控制方法、装置、设备及存储介质。

背景技术

[0002] 目前，安全托管服务(Managed Security Service，MSS)已逐渐流行，但MMS在实际使用过程中存在较多问题，比如当发生安全事件时，缺少远程响应工具。另外，互联网技术(Internet Technology，IT)安全运维人员在响应企业中发现的安全问题时也会进行远程响应，来加快应急速度。

[0003] 然而，远程桌面、远程访问等方式一般都是管理员登录，管理员具有较大的权限，会允许运维人员在重要资产上进行任意操作，包括无限制浏览或修改重要数据等，造成数据泄密或损失风险。因此，需要一种能够对运维人员的操作命令进行审核的机制，使得运维人员的操作更加精细化，也使得远程响应更容易管控，降低或避免远程管控过程中引入新风险。

发明内容

[0004] 有鉴于此，本申请实施例提供一种远程响应和远程控制方法、装置、设备及存储介质。

[0005] 本申请的技术方案是这样实现的：

[0006] 第一方面，本申请实施例提供一种远程响应方法，包括：

[0007] 确定服务器发送的待操作命令的风险级别；

[0008] 若所述待操作命令的风险级别小于级别阈值，从终端上的操作集中获取第一目标执行指令；

[0009] 若所述待操作命令的风险级别大于或等于所述级别阈值，调用所述服务器的命令解析器来获取第二目标执行指令；

[0010] 通过所述第一目标执行指令或所述第二目标执行指令，执行所述待操作命令，以完成对所述待操作命令的远程响应。

[0011] 第二方面，本申请实施例提供一种远程控制方法，包括：

[0012] 确定待操作命令的风险级别；

[0013] 若所述待操作命令的风险级别小于级别阈值，向终端发送所述待操作命令，以使得终端从操作集中获取第一目标执行指令；

[0014] 若所述待操作命令的风险级别大于或等于所述级别阈值，向终端发送所述待操作命令，并基于所述终端的命令解析器调用请求，调用服务器的命令解析器来获取第二目标执行指令；

[0015] 接收所述终端返回的命令执行结果，以完成对所述终端的远程控制，其中，所述命令执行结果是所述终端通过所述第一目标执行指令和所述第二目标执行指令执行所述待

操作命令得到的。

[0016] 第三方面，本申请实施例提供一种远程响应装置，包括：

[0017] 第一确定模块，用于确定服务器发送的待操作命令的风险级别；

[0018] 第一获取模块，用于若所述待操作命令的风险级别小于级别阈值，从终端上的操作集中获取第一目标执行指令；

[0019] 第一调用模块，用于若所述待操作命令的风险级别大于或等于所述级别阈值，调用所述服务器的命令解析器来获取第二目标执行指令；

[0020] 第一执行模块，用于通过所述第一目标执行指令或所述第二目标执行指令，执行所述待操作命令，以完成对所述待操作命令的远程响应。

[0021] 第四方面，本申请实施例提供一种远程控制装置，包括：

[0022] 第二确定模块，用于确定待操作命令的风险级别；

[0023] 第一发送模块，用于若所述待操作命令的风险级别小于级别阈值，向终端发送所述待操作命令，以使得终端从操作集中获取第一目标执行指令；

[0024] 第二发送模块，用于若所述待操作命令的风险级别大于或等于所述级别阈值，向终端发送所述待操作命令，并基于所述终端的命令解析器调用请求，调用服务器的命令解析器来获取第二目标执行指令；

[0025] 第一接收模块，用于接收所述终端返回的命令执行结果，以完成对所述终端的远程控制，其中，所述命令执行结果是所述终端通过所述第一目标执行指令或所述第二目标执行指令执行所述待操作命令得到的。

[0026] 第五方面，本申请实施例提供一种远程响应设备，包括：

[0027] 存储器，用于存储可执行指令；处理器，用于执行所述存储器中存储的可执行指令时，实现上述的远程响应方法。

[0028] 第六方面，本申请实施例提供一种远程控制设备，包括：

[0029] 存储器，用于存储可执行指令；处理器，用于执行所述存储器中存储的可执行指令时，实现上述的远程控制方法。

[0030] 第七方面，本申请实施例提供一种存储介质，存储有可执行指令，用于引起处理器执行时，实现上述的方法。

[0031] 本申请实施例提供的远程响应和远程控制方法、装置、设备及存储介质，由于可以确定待操作命令的风险级别，当所述待操作命令的风险级别小于级别阈值时，从终端上的操作集中获取执行所述待操作命令的第一目标执行指令；当所述待操作命令的风险级别大于或等于所述级别阈值时，调用所述服务器的命令解析器来获取执行所述待操作命令的第二目标执行指令；如此，通过对待操作命令的审核，并基于不同风险级别的待操作命令以不同方式进行响应，这样，使得运维人员的操作和被控端的响应过程更加精细化，很大程度上避免了在远程管控过程中引入新风险。

附图说明

[0032] 在附图(其不一定是按比例绘制的)中，相似的附图标记可在不同的视图中描述相似的部件。具有不同字母后缀的相似附图标记可表示相似部件的不同示例。附图以示例而非限制的方式大体示出了本文中所讨论的各个实施例。

[0033] 图1A为本申请实施例提供的远程响应方法的一种可选的实现流程示意图；

[0034] 图1B为本申请实施例提供的远程响应方法的一个可选的应用场景示意图；

[0035] 图2为本申请实施例提供的远程响应和远程控制方法的一种可选的实现流程示意图；

[0036] 图3为本申请实施例提供的远程响应和远程控制方法的一种可选的实现流程示意图；

[0037] 图4为本申请实施例提供的远程响应和远程控制方法的一种可选的实现流程示意图；

[0038] 图5A为本申请实施例提供的远程控制方法的一种可选的实现流程示意图；

[0039] 图5B为本申请实施例提供的终端代理与服务器代理建立通道的一种可选的实现流程示意图；

[0040] 图5C为本申请实施例提供的一次命令执行的逻辑流程图；

[0041] 图6为本申请实施例提供的远程响应装置的一个可选的组成结构示意图；

[0042] 图7为本申请实施例提供的远程控制装置的一个可选的组成结构示意图；

[0043] 图8为本申请实施例提供的远程响应设备的一个可选的组成结构示意图；

[0044] 图9为本申请实施例提供的远程控制设备的一个可选的组成结构示意图。

具体实施方式

[0045] 为了使本申请的目的、技术方案和优点更加清楚，下面将结合附图对本申请作进一步地详细描述，所描述的实施例不应视为对本申请的限制，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例，都属于本申请保护的范围。

[0046] 在以下的描述中，涉及到“一些实施例”，其描述了所有可能实施例的子集，但是可以理解，“一些实施例”可以是所有可能实施例的相同子集或不同子集，并且可以在不冲突的情况下相互结合。除非另有定义，本申请实施例所使用的所有的技术和科学术语与属于本申请实施例的技术领域的技术人员通常理解的含义相同。本申请实施例所使用的术语只是为了描述本申请实施例的目的，不是旨在限制本申请。

[0047] 对本申请实施例进行进一步详细说明之前，对本申请实施例中涉及的名词和术语进行说明，本申请实施例中涉及的名词和术语适用于如下的解释。

[0048] 1、终端代理(agent，即第一代理程序和第二代理程序)：终端代理程序，是以软件代理形式，在终端，如个人计算机(Personal Computer，PC)或服务器主机上安装的特定开发的软件，以便做些需要的工作。如以杀毒软件、终端检测与响应(Endpoint Detection and Response，EDR)等终端安全产品为例，其软件代理就是这些产品的客户端代理。

[0049] 2、安全托管服务(Managed Security Service，MMS)：MMS安全托管服务是一种另类的安全运维服务，是将自己业务系统的安全运维工作外包给外部专业的安全服务供应商，自己不再承担系统的安全运维工作。

[0050] 3、远程响应：远程响应指互联网技术(Internet Technology，IT)运维人员在发现问题后需要到问题资产上进行排查和处置的过程。通过远程的形式可避免运维人员必须要到现场的问题，也加快了应急的响应速度。另外，部分企业的安全运维工作往往会以外包的形式，并将安全数据接入云安全运营中心(Security Operations Center，SOC)之类的MSS

安全运维服务平台。当外包人员发现安全问题时，也可以通过远程的形式，从MSS安全运维服务平台直接远程响应，无需到现场。

[0051] 相关技术中的远程响应和远程控制方法存在以下问题：

[0052] MSS拖管服务在使用过程中，当发生安全事件时，经常需要派人到现场导致无法及时响应，若现场处置的人缺乏高级安全能力，在遇到更高级的威胁时响应也无法及时应对，导致即时安全服务托管出去了，企业仍然会在遭受重要威胁时因无法快速响应而造成损失。

[0053] 因此大部分MSS服务厂商或IT运维人员采用了类似远程桌面、远程访问等方式来应对，但都会遇到如下问题而对企业造成了二次打击：

[0054] 1、无响应远程执行权限审核机制。

[0055] 远程桌面类方式一般都是管理员登录，管理员具有较大的权限，会允许运维人员在重要资产上进行任意操作，包括无限制浏览/修改重要数据等，造成数据泄密/损失风险。同时，运维人员执行的任何命令都无法进行审计和权限控制，若MSS托管厂商存在内鬼，在执行恶意命令并删除痕迹后，将导致事后难以追溯和评估影响。

[0056] 2、需要开放对应的风险端口及应用，引入暴露面风险。

[0057] 类似远程桌面和远程访问，如安全外壳协议(Secure Shell，SSH)等都需要开放对应的端口才能实现远程访问，而这些端口通常为黑客常用的风险端口，因此这些方式给攻击者带来了新的利用点。

[0058] 进一步地，MSS托管商或安全运维人员利用远程桌面或远程访问进行运维时都需要进行精细化的远程操作，如查看进程、启动项、注册表、关键系统位置等，并进行处置操作，如删除文件、关闭进程、关闭端口、恢复启动项等，甚至会执行一些脚本命令，来达成目的。

[0059] 基于相关技术所存在的上述至少一个问题，本申请实施例提供一个难度较为简单又可精细化响应的方案，旨在解决上述问题的同时又能支持运维时的精细化操作，让远程响应更容易管控，降低或避免引入新风险。

[0060] 实施例一

[0061] 本申请实施例提供一种远程响应方法，本实施例的远程响应方法所实现的功能可以通过远程响应设备中的处理器调用程序代码来实现，当然程序代码可以保存在计算机可读存储介质中，可见，该远程响应设备至少包括处理器和计算机可读存储介质。

[0062] 图1A为本申请实施例提供的远程响应方法的一种可选的实现流程示意图，如图1A所示，所述方法包括以下步骤：

[0063] 步骤S101、终端确定服务器发送的待操作命令的风险级别。

[0064] 在一些实施例中，终端接收服务器发送的待操作命令，所述待操作命令可以是运维人员输入的命令；例如，运维人员在远程控制时向被控终端发送查看任务列表的命令。

[0065] 在一些实施例中，所述待操作命令也可以是服务器基于预设的周期自动发送的命令；例如，长期处于远程控制下的终端需要12小时清空一次回收站，那么，一种可能的实现方式是：在服务器上设定12小时发送一次回收站的清空命令，以使得被控终端12小时清空一次回收站。

[0066] 在一些实施例中，所述待操作命令的风险级别是执行所述待操作命令产生的结

果,对原服务器系统或原终端系统产生的影响的程度大小。

[0067] 举例来说,所述待操作命令是查看A文件或者删除B文件,那么,查看A文件对所述终端产生的影响和删除B文件对所述终端产生的影响是不同的,因此,查看A文件和删除B文件的风险级别就是不同的。

[0068] 在一些实施例中,所述级别阈值的数值或等级大小视发生安全事故时事故的情况不同而不同,因此,本申请实施例不作限制。

[0069] 步骤S102、终端判断所述待操作命令的风险级别是否小于级别阈值。

[0070] 在一些实施例中,可以由终端判断接收到的待操作命令的风险级别,也可以由服务器判断发送的待操作命令的风险级别。

[0071] 在一些实施例中,终端或者服务器上存储着一个通用命令集合,所述通用命令集合用于判定所述待操作命令的风险级别。

[0072] 这里,所述通用命令集合中保留有至少一种常用的命令;当在所述通用命令集合中能查找出与所述待操作命令对应的命令时,确定所述待操作命令的风险级别小于所述级别阈值;当在所述通用命令集合中不能查找出与所述待操作命令对应的命令时,确定所述待操作命令的风险级别大于或等于所述级别阈值。

[0073] 举例来说,所述通用命令集合中存储着读取数据的命令和写入数据的命令等,当所述待操作命令为读取进程列表时,读取进程列表对应于所述通用命令集合中读取数据的命令,因此,确定所述待操作命令(即读取进程列表)的风险级别小于所述级别阈值。

[0074] 在一些实施例中,当所述待操作命令的风险级别小于级别阈值时,执行步骤S103,当所述待操作命令的风险级别大于等于级别阈值时,执行步骤S104。

[0075] 步骤S103、若所述待操作命令的风险级别小于级别阈值,从终端上的操作集中获取第一目标执行指令。

[0076] 在一些实施例中,所述操作集中保留有至少一常用命令的读或写等执行指令,所述操作集用于确定所述风险级别小于级别阈值的待操作命令的第一目标执行指令。

[0077] 在一些实施例中,所述第一目标执行指令是对应于所述待操作命令的执行指令,所述第一目标执行指令用于执行所述待操作命令。

[0078] 举例来说,所述待操作命令为查看系统启动项,所述操作集中对应于所述查看系统启动项的执行指令是C,那么,将执行指令C确定为所述查看系统启动项的第一目标执行指令。

[0079] 步骤S104、若所述待操作命令的风险级别大于或等于所述级别阈值,调用所述服务器的命令解析器来获取第二目标执行指令。

[0080] 在一些实施例中,若所述待操作命令的风险级别大于或等于所述级别阈值,那么,执行这些指令就需要更高级且灵活的操作,此时,终端调用服务器系统的命令解析器来获取运维人员指定的操作命令来控制执行。

[0081] 这里,运维人员指定的操作命令就对应于执行所述待操作命令的第二目标执行指令,通过所述运维人员指定的操作命令去执行所述待操作命令。

[0082] 步骤S105、终端通过所述第一目标执行指令或所述第二目标执行指令,执行所述待操作命令,以完成对所述待操作命令的远程响应。

[0083] 在一些实施例中,通过执行所述第一目标执行指令或者所述第二目标执行指令,

就可以实现对所述待操作命令的远程响应。

[0084] 举例来说，当终端A接收到服务器B发送的待操作命令为读取系统日志时，终端A判断读取系统日志对应于所述通用命令集合中读取数据的命令，因此，终端A确定所述读取系统日志的待操作命令的风险级别小于级别阈值；此时，终端A从操作集中确定出与所述读取系统日志对应的第一目标执行指令为C，因此，终端A通过所述第一目标执行指令C，执行所述读取系统日志的待操作命令，以完成对所述读取系统日志待操作命令的远程响应。

[0085] 图1B为本申请实施例提供的远程响应方法的一个可选的应用场景示意图，如图1B所示，远程响应系统10至少包含服务器100、网络200和终端300，服务器100接收到运维人员的待操作命令后，通过网络200向终端300发送待操作命令，终端300接收到待操作命令后确定所述待操作命令的风险级别，当所述待操作命名的风险级别小于级别阈值，从终端300上的操作集中获取第一目标执行指令；当所述待操作命令的风险级别大于或等于所述级别阈值，终端300调用所述服务器100的命令解析器100-1来获取第二目标执行指令；终端300通过获取到的第一目标执行指令或第二目标执行指令，来执行服务器100发送的待操作命令，以完成对所述待操作命令的远程响应。

[0086] 本申请实施例提供的远程响应方法，由于可以确定待操作命令的风险级别，当所述待操作命令的风险级别小于级别阈值时，从终端上的操作集中获取执行所述待操作命令的第一目标执行指令；当所述待操作命令的风险级别大于或等于所述级别阈值时，调用所述服务器的命令解析器来获取执行所述待操作命令的第二目标执行指令；如此，通过对待操作命令的审核，并基于不同风险级别的待操作命令以不同方式进行响应，这样，使得运维人员的操作和被控端的响应过程更加精细化，很大程度上避免了在远程管控过程中引入新风险。

[0087] 实施例二

[0088] 本申请实施例提供一种远程响应和远程控制方法，本实施例的远程响应和远程控制方法所实现的功能可以通过远程响应设备和远程控制设备中的处理器调用程序代码来实现，当然程序代码可以保存在计算机可读存储介质中，可见，该远程响应设备和远程控制设备至少包括处理器和计算机可读存储介质。

[0089] 图2为本申请实施例提供的远程响应和远程控制方法的一种可选的实现流程示意图，如图2所示，所述方法包括以下步骤：

[0090] 步骤S201、服务器确定待操作命令的风险级别。

[0091] 在一些实施例中，确定待操作命令的风险级别的操作可以由服务器来执行，也可以在服务器把待操作命令发送给终端之后，由终端来执行，不论是由服务器或是由终端来确定待操作命令的风险级别，确定方法都是一样的，如上述实施例一中记载的确定方法，本实施例不再赘述。

[0092] 本申请实施例中，以服务器来确定待操作命令的风险级别为例进行说明。

[0093] 步骤S202、服务器判断所述待操作命令的风险级别是否小于级别阈值。

[0094] 在一些实施例中，当所述待操作命令的风险级别小于级别阈值时，执行步骤S203，当所述待操作命令的风险级别大于等于级别阈值时，执行步骤S204。

[0095] 步骤S203、若所述待操作命令的风险级别小于级别阈值，向终端发送所述待操作命令，以使得终端从操作集中获取第一目标执行指令。

[0096] 步骤S204、若所述待操作命令的风险级别大于或等于所述级别阈值，向终端发送所述待操作命令，并基于所述终端的命令解析器调用请求，调用服务器的命令解析器来获取第二目标执行指令。

[0097] 在一些实施例中，在服务器确定出待操作命令的风险级别后，服务器将所述待操作命令和所述待操作命令对应的风险级别信息发送给所述终端，终端基于接收到的所述操作命令和所述待操作命令对应的风险级别信息进行响应。

[0098] 步骤S203和步骤S204的实现过程和实现的功能与上述实施例中步骤S103和步骤S104的实现过程和实现的功能相同。

[0099] 步骤S205、服务器将所述第一目标执行指令或所述第二目标执行指令发送给终端。

[0100] 步骤S206、终端通过所述第一目标执行指令或所述第二目标执行指令，执行所述待操作命令，得到命令执行结果。

[0101] 在一些实施例中，所述命令执行结果是所述终端通过所述第一目标执行指令或所述第二目标执行指令执行所述待操作命令得到的。

[0102] 举例来说，终端接收的待操作命令为查看进程信息，基于所述查看进程信息的风险级别，终端获取到的第一目标执行指令为X；终端通过所述第一目标执行指令X，执行查看进程信息的命令，得到的返回结果是进程信息列表，这里，进程信息列表即为查看进程信息的命令执行结果。

[0103] 步骤S207、终端将所述命令执行结果发送给服务器。

[0104] 在一些实施例中，终端将获取的命令执行结果发送给服务器，以实现对所述待操作命令的远程响应。

[0105] 相应地，服务器接收所述终端返回的命令执行结果，以完成对所述终端的远程控制。

[0106] 本申请实施例提供的远程响应和远程控制方法，由于可以确定待操作命令的风险级别，当所述待操作命令的风险级别小于级别阈值时，从终端上的操作集中获取执行所述待操作命令的第一目标执行指令；当所述待操作命令的风险级别大于或等于所述级别阈值时，调用所述服务器的命令解析器来获取执行所述待操作命令的第二目标执行指令；如此，通过对待操作命令的风险级别进行审核，并基于不同风险级别的待操作命令以不同方式进行响应，这样，使得运维人员的操作和被控端的响应更加精细化，很大程度上避免了在远程管控过程中引入新风险。

[0107] 实施例三

[0108] 本申请实施例提供一种远程响应和远程控制方法，本实施例的远程响应和远程控制方法所实现的功能可以通过远程响应设备和远程控制设备中的处理器调用程序代码来实现，当然程序代码可以保存在计算机可读存储介质中，可见，该远程响应设备和远程控制设备至少包括处理器和计算机可读存储介质。

[0109] 图3为本申请实施例提供的远程响应和远程控制方法的一种可选的实现流程示意图，如图3所示，所述方法包括以下步骤：

[0110] 步骤S301、服务器发送待操作命令给终端。

[0111] 步骤S302、终端判断所述待操作命令的风险级别是否小于预设的阈值。

[0112] 步骤S302的实现过程和实现的功能与上述实施例中步骤S102的实现过程和实现的功能相同。

[0113] 在一些实施例中，当所述待操作命令的风险级别小于级别阈值时，执行步骤S303，当所述待操作命令的风险级别大于等于级别阈值时，执行步骤S306。

[0114] 步骤S303、终端获取所述风险级别小于所述级别阈值的至少一操作命令、和每一所述操作命令对应的执行指令。

[0115] 在一些实施例中，所述执行指令用于执行所述操作命令。

[0116] 步骤S304、终端将所述操作命令、所述操作命令对应的执行指令、和所述操作命令与所述执行指令之间的映射关系，封装在所述操作集中。

[0117] 在一些实施例中，建立所述操作命令和所述操作命令对应的执行指令之间的映射关系，并将所述映射关系预先封装在所述操作集中。

[0118] 举例来说，所述操作命令包括以下至少之一，如针对进程信息、注册表、启动项、系统盘目录/文件、资源占用信息、内存DUMP(进程的内存镜像)信息、任务计划、系统日志、内核钩子注册情况、网络会话等的相关读、写操作。这里，将上述操作命令和对应的执行指令预先封装成操作集，形成远程响应工作中的基础固化操作。

[0119] 步骤S305、若所述待操作命令的风险级别小于级别阈值，从终端上的操作集中获取第一目标执行指令。

[0120] 步骤S306、若所述待操作命令的风险级别大于或等于所述级别阈值，终端向所述服务器发送命令解析器调用请求。

[0121] 步骤S305和步骤S306的实现过程和实现的功能与上述实施例中步骤S103和步骤S104的实现过程和实现的功能相同。

[0122] 步骤S307、服务器响应于所述命令解析器调用请求，调用所述命令解析器来获取第二目标执行指令。

[0123] 在一些实施例中，服务器接收所述终端发送的命令解析器调用请求，并响应所述命令解析器的调用请求，通过所述命令解析器来获取运维人员输入命令解析器的命令，即第二目标执行指令。

[0124] 在一些实施例中，从所述服务器的命令解析器中获取的第二目标执行指令用于执行所述风险级别大于或等于所述级别阈值的待操作命令。

[0125] 步骤S308、服务器将所述第二目标执行指令发送给所述终端。

[0126] 步骤S309、终端通过所述第一目标执行指令或所述第二目标执行指令，执行所述待操作命令，得到命令执行结果。

[0127] 步骤S309的实现过程与上述实施例中步骤S206的实现过程和实现的功能相同。

[0128] 步骤S310、终端将所述命令执行结果发送给服务器。

[0129] 本申请实施例提供的远程响应和远程控制方法，由于可以当待操作命令的风险级别小于级别阈值时，预先在在终端上设置操作集，并从操作集中获取第一目标执行指令；当所述待操作命令的风险级别大于或等于所述级别阈值时，向所述服务器发送命令解析器调用请求，调用所述服务器的命令解析器来获取执行所述待操作命令的第二目标执行指令；如此，通过对不同风险级别的待操作命令以不同方式进行响应，这样，使得被控端的响应更加精细化，很大程度上避免了在远程管控过程中引入新风险。

[0130] 实施例四

[0131] 本申请实施例提供一种远程响应和远程控制方法，本实施例的远程响应和远程控制方法所实现的功能可以通过远程响应设备和远程控制设备中的处理器调用程序代码来实现，当然程序代码可以保存在计算机可读存储介质中，可见，该远程响应设备和远程控制设备至少包括处理器和计算机可读存储介质。

[0132] 图4为本申请实施例提供的远程响应和远程控制方法的一种可选的实现流程示意图，如图4所示，所述方法包括以下步骤：

[0133] 步骤S401、服务器获取运维人员发送的待操作命令。

[0134] 在一些实施例中，服务器获取运维人员或者其它IT技术人员发送的待操作命令，所述运维人员或者其它IT技术人员在发送所述待操作命令之前，服务器会对他们进行权限验证，若运维人员或者其它IT技术人员的权限验证通过，即可发送所述待操作命令；若运维人员或者其它IT技术人员的权限验证没有通过，则运维人员或者其它IT技术人员就不能向服务器发送所述待操作命令。

[0135] 在一些实施例中，所述权限验证可以通过账号、密码等方式验证，也可以通过其他权限验证方法来验证，本申请实施例中，对所述权限验证方法，不做限制，任何可以实现身份验证功能的权限验证方法都在本申请实施例保护的范围之内。

[0136] 步骤S402、调用终端上的第一代理程序和所述服务器上的第二代理程序。

[0137] 步骤S403、通过所述第一代理程序和所述第二代理程序，建立所述终端与所述服务器之间的数据传输通道。

[0138] 本申请实施例中，终端上部署有第一代理程序，所述服务器上部署有第二代理程序。

[0139] 在一些实施例中，终端获取所述第一代理程序和服务器获取所述第二代理程序均可以是从特定网站下载第一代理程序和第二代理程序，也可以是在使用时编程得到第一代理程序/第二代理程序，或者也可以采用其它方式获取第一代理程序和第二代理程序，本申请实施例对获取第一代理程序和第二代理程序的方法不做限制，任何可以实现获取第一代理程序和第二代理程序的方法都属于本申请实施例保护的范畴。

[0140] 在一些实施例中，终端/服务器根据用户实施的安装、拷贝或者运行等操作方式，将获取的第一代理程序部署在终端上，将获取的第二代理程序部署在服务器上。

[0141] 在一些实施例中，在终端上部署第一代理程序的实现过程和在服务器上部署第二代理程序的实现过程没有先后关系，可以是同时进行，也可以是任意的顺序。

[0142] 本申请实施例中，可以是终端调用服务器第二代理程序，并通过自身的第一代理程序和所述服务器的第二代理程序建立所述终端与所述服务器之间的数据传输通道；也可以是服务器调用终端的第一代理程序，并通过自身的第二代理程序和所述服务器的第一代理程序建立所述服务器与所述终端之间的数据传输通道。

[0143] 在一些实施例中，在建立所述服务器与所述终端之间的数据传输通道之后，服务器还需要判断所述数据传输通道是否建立成功。

[0144] 在一些实施例中，当所述第一代理程序和所述第二代理程序之间的网络连接成功，即可认为所述数据传输通道建立成功。

[0145] 当所述数据传输通道建立成功时，执行所述步骤S404，当所述数据传输通道没有

建立成功时，返回执行所述步骤S403。

[0146] 步骤S404、服务器上的第二代理程序通过所述数据传输通道，向所述终端的第一代理程序发送待操作命令。

[0147] 对应地，终端上的第一代理程序通过所述数据传输通道，接收所述第二代理程序发送的所述待操作命令。

[0148] 步骤S405、终端判断所述待操作命令的风险级别是否小于预设的阈值。

[0149] 步骤S405的实现过程和实现的功能与上述实施例中步骤S302的实现过程和实现的功能相同。

[0150] 在一些实施例中，当所述待操作命令的风险级别小于级别阈值时，执行步骤S406，当所述待操作命令的风险级别大于等于级别阈值时，执行步骤S407。

[0151] 步骤S406、若所述待操作命令的风险级别小于级别阈值，从终端上的操作集中获取第一目标执行指令。

[0152] 步骤S407、若所述待操作命令的风险级别大于或等于所述级别阈值，调用所述服务器的命令解析器来获取第二目标执行指令。

[0153] 步骤S406和步骤S407的实现过程和实现的功能与上述实施例中步骤S103和步骤S104的实现过程和实现的功能相同。

[0154] 步骤S408、确定所述第一目标执行指令中对应于所述待操作命令的第一目标操作，或者，所述第二目标执行指令中对应于所述待操作命令的第二目标操作。

[0155] 步骤S409、对应执行所述第一目标操作或者所述第二目标操作，实现对所述待操作命令的响应，得到命令执行结果。

[0156] 举例来说，当所述待操作命令为查看系统启动项时，所述操作集中对应于所述查看系统启动项的第一目标执行指令是C(Windows+R)，所述第一目标执行指令C对应的第一目标操作是输入msconfig+enter；那么，通过执行所述第一目标操作msconfig+enter实现对所述查看系统启动项的操作命令的响应。

[0157] 步骤S410、通过所述数据传输通道，终端将所述命令执行结果发送给所述服务器，以完成对所述待操作命令的远程响应。

[0158] 在一些实施例中，终端通过第一代理程序将所述命令执行结果发送给所述服务器的第二代理程序，以完成对所述待操作命令的远程响应。

[0159] 对应地，通过所述数据传输通道，服务器的第二代理程序接收所述命令执行结果，以完成对所述终端的远程控制。

[0160] 在一些实施例中，所述方法还可以包括以下步骤：

[0161] 步骤S411、服务器获取预设时间段内发送的至少一待操作命令、和每一所述待操作命令对应的命令执行结果。

[0162] 在一些实施例中，所述预设时间可以由运维人员或操作人员任意给定合理地时间，本申请实施例中对预设时间不做限制。

[0163] 步骤S412、建立每一所述待操作命令与对应命令执行结果之间的映射关系。

[0164] 步骤S413、将所述映射关系存储于待审计列表中。

[0165] 步骤S414、输出所述待审计列表，以实现对所述待审计列表中的至少一所述命令执行结果和/或至少一所述待操作命令进行审计。

[0166] 在一些实施例中，审计人员通过服务器输出的待审计列表查看终端执行的待操作命令和相应的命令执行结果，通过对所述执行结果和/或所述待操作命令进行审计，可以实现企业对待操作命令的监控，避免远程控制过程中出现数据泄密等风险时，无法追溯的问题。

[0167] 在一些实施例中，当所述待操作命令中包含删除(delete)等能导致数据变化/丢失的风险的命令时，对所述待操作命令进行阻止或以弹窗提醒等方式进行预警，以便运维人员或IT技术人员能够根据提醒框进行警示，避免出现误操作的情况。

[0168] 在一些实施例中，上述待审计列表也可以由终端统计完成。

[0169] 终端可以通过以下步骤来实现对所述待操作命令和/或所述命令执行结果进行审计：

[0170] 步骤S415、终端获取预设时间段内所接收到的至少一待操作命令、和每一所述待操作命令对应的命令执行结果。

[0171] 步骤S416、终端建立每一所述命令执行结果与对应待操作命令之间的映射关系。

[0172] 步骤S417、终端将所述映射关系存储于待审计列表中。

[0173] 步骤S418、输出所述待审计列表，以实现对所述待审计列表中的至少一所述命令执行结果和/或至少一所述待操作命令进行审计。

[0174] 在一些实施例中，终端通过所述第一代理程序将所述待审计列表发送给服务器的第二代理程序，通过服务器的第二代理程序输出所述待审计列表，以使得审计人员基于所述待审计列表实现对所述命令执行结果和/或至少一所述待操作命令进行审计。

[0175] 本申请实施例提供的远程响应和远程控制方法，由于可以通过终端的第一代理程序和服务器的第二代理程序建立数据传输通道，并通过所述数据传输通道实现所述服务器对所述终端的远程控制和所述终端对所述服务器的远程控制的远程响应，可以降低远程控制过程中数据泄密的风险；并在远程控制和响应的过程中记录待操作命令和命令执行结果之间的对应关系，如此，可以实现对远程控制和相应过程中的命令进行监控，大大提高了远程管控过程中的安全性。

[0176] 实施例五

[0177] 本申请实施例提供一种远程响应和远程控制方法，本实施例的远程响应和远程控制方法所实现的功能可以通过远程响应设备和远程控制设备中的处理器调用程序代码来实现，当然程序代码可以保存在计算机可读存储介质中，可见，该远程响应设备和远程控制设备至少包括处理器和计算机可读存储介质。

[0178] 图5A为本申请实施例提供的远程控制方法的一种可选的实现流程示意图，如图5A所示，所述方法包括以下步骤：

[0179] 步骤S501、运维人员发起远程控制请求。

[0180] 在一些实施例中，当出现安全问题时，IT运维人员通过远程响应平台发起远程控制请求。

[0181] 步骤S502、服务器判断运维人员是否具有远程响应权限。

[0182] 在一些实施例中，当运维人员发起远程响应后，服务器首先判断远程操作的运维人员是否具有远程响应权限，当远程操作的运维人员具有远程响应权限时，执行步骤S503，当远程操作的运维人员不具备远程响应权限时，说明服务器不支持该运维人员的操作，返

回执行步骤S501。

[0183] 在一些实施例中，可以通过账号、密码等方式判断运维人员是否具有远程响应权限，也可以通过其他权限验证方法来判断运维人员是否具有远程响应权限，本申请实施例中，对判断运维人员是否具有远程响应权限的方法，不做限制。

[0184] 步骤S503、服务器判断运维人员是否需要执行高级命令(对应上述实施例中风险级别大于或等于级别阈值的待操作命令)。

[0185] 在一些实施例中，当运维人员具有远程响应权限时，服务器继续判断运维人员是否需要执行高级命令，本申请实施例中，可以在远程操作界面中直接做一个“执行命令”的按钮或入口，运维人员点击后可直接输入命令行，若运维人员选择点击了所述“执行命令”的按钮，则认为运维人员需要执行高级命令，那么，运维人员就不用再选择已封装的操作。

[0186] 本申请实施例中，当运维人员不需要执行高级命令时，执行步骤S504，当运维人员需要执行高级命令时，执行步骤S505。

[0187] 步骤S504、运维人员打开基础信息操作集(对应上述操作集)。

[0188] 在一些实施例中，封装一些安全运维工作中常用的低风险操作(对应上述实施例中风险级别小于级别阈值的待操作命令)，如针对进程信息、注册表、启动项、系统盘目录/文件、资源占用信息、内存DUMP(进程的内存镜像)信息、任务计划、系统日志、内核钩子注册情况、网络会话等的相关读、写操作封装成通用的操作集，形成远程响应工作中的基础固化操作，并认为这些操作造成的影响较小，权限审核可降低要求。

[0189] 在安全运维人员进行远程运维时，由终端代理在对应要响应的主机上实现上述封装的操作，并限定操作范围。这些封装后的操作，不需要接受运维人员带特定的参数即可呈现结果，并接受特定处置操作。如需要查看主机进程时，只需点击查看进程即可下发指令，并以可视化的形式展示进程列表和可进行的操作，这样也适用于不熟悉命令执行的运维人员，简单快捷的运维。

[0190] 举例来说，查看进程在视窗操作系统的命令行是“tasklist”，而这个命令可以带很多参数来达成不同的命令效果，这对运维人员的要求很高，要懂命令。因此，若能封装固定几个命令形成固定的操作，终端代理(对应上述实施例中的第一代理程序)直接执行封装的固定的操并反馈结果，就可以大大便捷所有远程人员。

[0191] 对应的处置也是，如查看进程后，可通过结束进程操作，跟据想要结束的进程，自动执行“taskkill/f/t/im指定进程名”，这样远程人员就无需自己输入命令。

[0192] 步骤S505、服务器判断运维人员是否有高级命令权限。

[0193] 在一些实施例中，当运维人员需要进行高级命令操作时，服务器首先判断运维人员是否具有高级命令操作权限，当运维人员具有高级命令操作权限时，执行步骤S506，当运维人员不具备高级命令操作权限时，则意味着运维人员只能操作基础信息操作窗口，即当运维人员不具备高级命令操作权限时，返回执行步骤S504。

[0194] 步骤S506、运维人员打开高级命令窗口。

[0195] 在一些实施例中，打开高级命令窗口的方式可以是通过同时按Windows键和Space键，即采用输入法输入终端的打开方式，也可以是其它打开方式，本申请实施例中，对打开高级命令窗口的方式不作限制。

[0196] 在一些实施例中，一般基础信息操作的范围足够大部分安全响应操作了，但对于

高级长期威胁(Advanced Persistent Threat,APT)等的分析需要深入到主机的各个环节，需要更高级且灵活的操作,如直接执行指定命令等,这些难以由基础信息操作集完成的操作,将由终端代理接管服务器的命令解析器(SHELL)来执行安全运维人员指定的操作命令行,并将命令行运行结果(对应上述实施例中的命令执行结果)反馈回去。通常也是由较为熟悉命令执行的安全运维人员使用,呈现方式可以命令行窗口形式。

[0197] 运维人员接管命令解析器来执行指定命令的实现方式比较简单,如LINUX下的C编码就有几种函数集支持命令执行,如exec()函数、system()函数、popen()函数。例如,以popen()函数执行“ls”命令来查看当前目录下的文件列表,其中,fp=popen(“ls”,“r”)代表执行的“ls”命令,printf(“%s”,data)中的data结果为执行ls命令的结果,popen()函数执行代码如下所示：

[0198]
```
#include<stdio.h>
```

[0199]
```
int main ()
```

[0200]
```
{
```

[0201]
```
        FILE *fp = NULL;
```

[0202]
```
       char data[100]={'0'};
```

[0203]
```
        fp=popen("ls","r");
```

[0204]
```
        if(fp==NULL)
```

[0205]
```
        {
```

[0206]
```
              Printf("popen error!\n");
```

[0207]
```
              Return 1;
```

[0208]
```
        }
```

[0209]
```
        while (fgets(data,sizeof(data,fp)!=NULL)
```

[0210]
```
        {
```

[0211]
```
printf("%s",data)
```

[0212]
```
}
```

[0213]
```
pclose(fp);
```

[0214]
```
return 0;
```

[0215]
```
}
```

[0216] 步骤S507、服务器判断运维人员输入的高级命令是否存在风险。

[0217] 在一些实施例中,当运维人员输入的高级命令中包含删除(delete)等能导致数据变化/丢失的风险的命令时,服务器则认为该高级命令存在风险。

[0218] 如果运维人员输入的高级命令存在风险,执行步骤S510,如果运维人员输入的高级命令不存在风险,执行步骤S508。

[0219] 步骤S508、下发并执行上述高级命令,返回结果。

[0220] 本申请实施例中,在下发并执行命令之前首先建立命令执行通道。本申请实施例的技术方案设计为客户机-服务器(Client-Server,C/S)模式,终端代理作为客户端,并在远程运维平台上建立服务器端程序,使得服务器端程序与终端代理建立命令和数据通道,这样才能顺利将命令传到终端代理,并接收执行结果,通过Server传递给远程运维平台(如MSS的远程平台)。

[0221] 本申请实施例中，由终端代理启动后主动链接服务器端，并建立通道，用于接收命令，并传输命令结果给服务器端。图5B为本申请实施例提供的终端代理与服务器代理建立通道的一种可选的实现流程示意图，其中，终端代理和服务器代理(对应上述实施例中的第二代理程序)建立通道过程包括以下步骤：

[0222] 步骤S51、终端代理和/或服务器代理启动。

[0223] 在一些实施例中，服务器代理或者终端代理，在部署好以后，可以设置成开机自动启动模式。

[0224] 步骤S52、建立终端代理与服务器代理之间的远程响应双向通道链接(对应上述实施例中数据传输通道)。

[0225] 在一些实施例中，通过终端代理和服务器代理建立终端与服务器之间的远程响应双向通道链接，通过所述远程响应双向通道链接可以发送或接受命令或者结果。

[0226] 步骤S53、判断远程响应双向通道链接是否建立成功。

[0227] 在一些实施例中，当所述终端代理与所述服务器代理之间的网络连接成功，即认为所述远程响应双向通道链接建立成功，如此，终端即可接受服务器发送的操作命令，服务器也可以接收到终端基于所述操作命令返回的结果。

[0228] 当终端代理与服务器代理之间的远程响应双向通道建立成功时，执行步骤S54，当终端代理与服务器代理之间的远程响应双向通道未建立成功时，返回执行步骤S52，继续建立远程响应双向通道链接。

[0229] 步骤S54、运维人员持续监听远程响应操作过程。

[0230] 在一些实施例中，所述持续监听远程响应操作过程是指，运维人员持续地或者周期性地查看所述服务器发送的操作命令或接受的命令执行结果。

[0231] 步骤S509、运维人员审计所有的待操作命令和命令执行结果。

[0232] 在一些实施例中，终端或者服务器记录每一次发送/接收的待操作命令及基于所述待操作命令返回的结果，建立所述待操作命令与所述返回结果之间的映射关系，将所有待操作命令对应的映射关系保存在映射关系列表中，审计人员通过观察输出的映射关系列表即可实现对所述操作命令的审计。

[0233] 在一些实施例中，终端或服务器记录待操作命令和返回结果的时间、内容等其它信息。

[0234] 在一些实施例中，当运维人员输入的高级命令存在风险时，服务器可以通过弹窗等方式告警运维人员该命令存在风险，在某些特定的情况下，服务器直接拒绝执行所述风险命令。

[0235] 在一些实施例中，通过以上步骤S501至步骤S510即完成了一次完整的远程控制过程，后续需要执行其他的命令时，返回执行步骤S503及其之后的步骤。

[0236] 图5C为本申请实施例提供的一次命令执行的逻辑流程图，如图5C所示，所述一次命令执行过程包括以下步骤：

[0237] 步骤S510、运维人员输入待操作命令(对应上述实施例中的待操作命令)。

[0238] 在一些实施例中，可以在运维平台上做一个可视化界面，远程运维人员通过可视化界面在服务器上的前台操作区输入操作命令。

[0239] 步骤S511、运维人员发送待操作命令给服务器。

[0240] 步骤S512、服务器代理下发待操作命令。

[0241] 在一些实施例中，服务器代理接收到操作命令后，将所述操作命令通过建立的远程响应双向通道链接下发给终端代理。

[0242] 步骤S513、终端代理返回命令执行结果。

[0243] 在一些实施例中，终端代理响应所述操作命令并返回命令结果。

[0244] 步骤S514、服务器代理返回命令执行结果。

[0245] 在一些实施例中，服务器代理接收终端代理返回的命令执行结果，并把所述命令执行结果发送到远程运维平台的可视化界面上。

[0246] 步骤S515、呈现命令执行结果。

[0247] 在一些实施例中，服务器将接收的命令执行结果呈现给运维人员以便运维人员进行查看，如此，便实现了一次完整的命令执行过程。

[0248] MSS托管商或安全运维人员一般利用远程桌面或远程访问进行运维时都需要进行精细化的远程操作，如查看进程、启动项、注册表、关键系统位置等，并进行处置操作，如删除文件、关闭进程、关闭端口、恢复启动项等，甚至会执行一些shell命令来达成目的。

[0249] 本申请实施例提供一个难度较为简单，又可精细化响应的方案，解决如上问题的同时又能支持运维时的精细化操作，让远程响应更容易管控，降低或避免引入新风险。

[0250] 本申请实施例提供一种远程响应和远程控制方法，通过在终端资产上部署软件代理的形式，以软件代理采集终端数据和处置响应操作来实现通用远程响应的需要，并通过接管命令解析器来执行安全运维人员的高级操作(例如，直接以命令行的方式执行)。此方式再配合良好的权限管理和审计，如在进行远程运维前进行权限认证；在运维过程中进行操作和结果的审计；对高危行为(会导致不良结果的操作)进行及时预警等，来完成此方案。

[0251] 本申请实施例中，通过终端代理执行基础信息操作和接管命令解析器进行高级操作的好处在于：不会开放常用的风险端口，并且可在执行命令前对命令进行权限审核，在执行结果后可对结果进行审计。

[0252] 本申请实施例保护的关键点在于：在MSS安全托管服务或SOC/安全信息和事件管理(Security Information and Event Management，SIEM)/态势感知类平台通过终端代理技术进行远程响应；在EDR、端点防护平台(Endpoint Protection Platform，EPP)等具备管理平台的终端安全品类产品上提供基于终端代理的精细化远程响应能力。

[0253] 实施例六

[0254] 本实施例提供一种远程响应装置，该装置包括所包括的各模块、以及各模块所包括的各子模块，可以通过远程响应装置中的处理器来实现；当然也可通过逻辑电路实现；在实施的过程中，处理器可以为中央处理器(Central Processing Unit，CPU)、微处理器(Microprocessor Unit，MPU)、数字信号处理器(Digital Signal Process，DSP)或现场可编程门阵列(Field Programmable Gate Array，FPGA)等。

[0255] 图6为本申请实施例提供的远程响应装置的一个可选的组成结构示意图，如图6所示，所述远程响应装置60包括：

[0256] 第一确定模块61，用于确定服务器发送的待操作命令的风险级别。

[0257] 第一获取模块62，用于若所述待操作命令的风险级别小于级别阈值，从终端上的操作集中获取第一目标执行指令。

[0258] 第一调用模块63，用于若所述待操作命令的风险级别大于或等于所述级别阈值，调用所述服务器的命令解析器来获取第二目标执行指令。

[0259] 第一执行模块64，用于通过所述第一目标执行指令或所述第二目标执行指令，执行所述待操作命令，以完成对所述待操作命令的远程响应。

[0260] 在一些实施例中，所述装置还包括：第二获取模块，用于在从终端上的操作集中获取第一目标执行指令之前，获取所述风险级别小于所述级别阈值的至少一操作命令、和每一所述操作命令对应的执行指令；封装模块，用于将所述操作命令、所述操作命令对应的执行指令、和所述操作命令与所述执行指令之间的映射关系，封装在所述操作集中。

[0261] 在一些实施例中，所述第一调用模块还用于：向所述服务器发送命令解析器调用请求，以使所述服务器响应于所述命令解析器调用请求，向终端发送所述第二目标执行指令。

[0262] 在一些实施例中，所述终端上部署有第一代理程序，所述服务器上部署有第二代理程序；所述装置还包括：第二调用模块，用于调用终端上的第一代理程序和所述服务器上的第二代理程序；第一建立模块，用于通过所述第一代理程序和所述第二代理程序，建立所述终端与所述服务器之间的数据传输通道；第一接收模块，用于通过所述数据传输通道，接收所述第二代理程序发送的所述待操作命令。

[0263] 在一些实施例中，所述执行模块还包括：第一确定子模块，用于确定所述第一目标执行指令中对应于所述待操作命令的第一目标操作，或者，所述第二目标执行指令中对应于所述待操作命令的第二目标操作；执行子模块，用于执行所述第一目标操作或所述第二目标操作，实现对所述待操作命令的响应，得到命令执行结果；发送子模块，用于通过所述数据传输通道，将所述命令执行结果发送给所述服务器，以完成对所述待操作命令的远程响应。

[0264] 在一些实施例中，所述装置还包括：第三获取模块，用于获取预设时间段内所接收到的至少一待操作命令、和每一所述待操作命令对应的命令执行结果；第二建立模块，用于建立每一所述命令执行结果与对应待操作命令之间的映射关系；第一存储模块，用于将所述映射关系存储于待审计列表中；第一输出模块，用于输出所述待审计列表，以实现对所述待审计列表中的至少一所述命令执行结果和/或至少一所述待操作命令进行审计。

[0265] 需要说明的是，本申请实施例装置的描述，与上述方法实施例的描述是类似的，具有同方法实施例相似的有益效果，因此不做赘述。对于本装置实施例中未披露的技术细节，请参照本申请实施例方法实施例的描述而理解。

[0266] 实施例七

[0267] 本实施例提供一种远程控制装置，该装置包括所包括的各模块、以及各模块所包括的各子模块，可以通过远程控制装置中的处理器来实现；当然也可通过逻辑电路实现；在实施的过程中，处理器可以为中央处理器(Central Processing Unit，CPU)、微处理器(Microprocessor Unit，MPU)、数字信号处理器(Digital Signal Process，DSP)或现场可编程门阵列(Field Programmable Gate Array，FPGA)等。

[0268] 图7为本申请实施例提供的远程控制装置的一个可选的组成结构示意图，如图7所示，所述远程控制装置70包括：

[0269] 第二确定模块71，用于确定待操作命令的风险级别。

[0270] 第一发送模块72,用于若所述待操作命令的风险级别小于级别阈值,向终端发送所述待操作命令,以使得终端从操作集中获取第一目标执行指令。

[0271] 第二发送模块73,用于若所述待操作命令的风险级别大于或等于所述级别阈值,向终端发送所述待操作命令,并基于所述终端的命令解析器调用请求,调用服务器的命令解析器来获取第二目标执行指令。

[0272] 第二接收模块74,用于接收所述终端返回的命令执行结果,以完成对所述终端的远程控制,其中,所述命令执行结果是所述终端通过所述第一目标执行指令或第二目标执行指令执行所述待操作命令得到的。

[0273] 在一些实施例中,所述装置还包括:第三接收模块,用于接收所述终端发送的命令解析器调用请求;响应模块,用于响应于所述命令解析器调用请求,调用所述命令解析器来获取所述第二目标执行指令;第三发送模块,用于将所述第二目标执行指令发送给所述终端。

[0274] 在一些实施例中,所述终端上部署有第一代理程序,所述服务器上部署有第二代理程序;所述装置还包括:第三调用模块,用于调用服务器上的第二代理程序和所述终端上的第一代理程序;第三建立模块,用于通过所述第二代理程序和所述第一代理程序,建立所述服务器与所述终端之间的数据传输通道;所述第一发送模块还用于,通过所述数据传输通道,向所述第一代理程序发送所述待操作命令。

[0275] 在一些实施例中,所述装置还包括:第四获取模块,用于获取预设时间段内发送的至少一待操作命令、和每一所述待操作命令对应的命令执行结果;第四建立模块,用于建立每一所述待操作命令与对应命令执行结果之间的映射关系;第二存储模块,用于将所述映射关系存储于待审计列表中;第二输出模块,用于输出所述待审计列表,以实现对所述待审计列表中的至少一所述命令执行结果和/或至少一所述待操作命令进行审计。

[0276] 需要说明的是,本申请实施例装置的描述,与上述方法实施例的描述是类似的,具有同方法实施例相似的有益效果,因此不做赘述。对于本装置实施例中未披露的技术细节,请参照本申请实施例方法实施例的描述而理解。

[0277] 实施例八

[0278] 本申请实施例中,如果以软件功能模块的形式实现上述的远程响应方法,并作为独立的产品销售或使用时,也可以存储在一个计算机可读取存储介质中。基于这样的理解,本发明实施例的技术方案本质上或者说对相关技术做出贡献的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计算机可读存储介质中,包括若干指令用以使得一台终端执行本发明各个实施例所述方法的全部或部分。而前述的计算机可读存储介质包括:U盘、移动硬盘、只读存储器(Read Only Memory,ROM)、磁碟或者光盘等各种可以存储程序代码的介质。这样,本发明实施例不限制于任何特定的硬件和软件结合。

[0279] 对应的,本申请实施例提供一种远程响应设备,包括:存储器,用于存储可执行指令;处理器,用于执行所述存储器中存储的可执行指令时,实现上述实施例提供的远程响应方法。

[0280] 本申请实施例提供一种存储介质,所述存储介质为计算机可读存储介质,存储有可执行指令,用于引起处理器执行时,实现上述实施例提供的远程响应方法。

[0281] 图8为本申请实施例提供的远程响应设备的一个可选的组成结构示意图,如图8所

示,所述远程响应设备80至少包括:处理器81、远程控制接口82和配置为存储可执行指令的计算机可读存储介质83,其中:处理器81通常控制远程响应设备80的总体操作。

[0282] 远程控制接口82可以使远程响应设备通过网络与其他设备远程控制。

[0283] 计算机可读存储介质83配置为存储有处理器81可执行的指令和应用,还可以缓存待处理器81和远程控制设备80中各模块待处理或已处理的数据,可以通过闪存(FLASH)或随机访问存储器(Random Access Memory,RAM)实现。

[0284] 实施例九

[0285] 本申请实施例中,如果以软件功能模块的形式实现上述的远程控制方法,并作为独立的产品销售或使用时,也可以存储在一个计算机可读取存储介质中。基于这样的理解,本发明实施例的技术方案本质上或者说对相关技术做出贡献的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计算机可读存储介质中,包括若干指令用以使得一台终端执行本发明各个实施例所述方法的全部或部分。而前述的计算机可读存储介质包括:U盘、移动硬盘、只读存储器(Read Only Memory,ROM)、磁碟或者光盘等各种可以存储程序代码的介质。这样,本发明实施例不限制于任何特定的硬件和软件结合。

[0286] 对应的,本申请实施例提供一种远程控制设备,包括:存储器,用于存储可执行指令;处理器,用于执行所述存储器中存储的可执行指令时,实现上述实施例提供的远程控制方法。

[0287] 本申请实施例提供一种存储介质,所述存储介质为计算机可读存储介质,存储有可执行指令,用于引起处理器执行时,实现上述实施例提供的远程控制方法。

[0288] 图9为本申请实施例提供的远程控制设备的一个可选的组成结构示意图,如图9所示,所述远程控制设备90至少包括:处理器91、远程控制接口92和配置为存储可执行指令的计算机可读存储介质93,其中:处理器91通常控制远程控制设备90的总体操作。

[0289] 远程控制接口92可以使远程控制设备通过网络与其他设备远程控制。

[0290] 计算机可读存储介质93配置为存储有处理器91可执行的指令和应用,还可以缓存待处理器91和远程控制设备90中各模块待处理或已处理的数据,可以通过闪存(FLASH)或随机访问存储器(Random Access Memory,RAM)实现。

[0291] 应理解,说明书通篇中提到的“一个实施例”或“一实施例”意味着与实施例有关的特定特征、结构或特性包括在本发明的至少一个实施例中。因此,在整个说明书各处出现的“在一个实施例中”或“在一实施例中”未必一定指相同的实施例。此外,这些特定的特征、结构或特性可以任意适合的方式结合在一个或多个实施例中。应理解,在本发明的各种实施例中,上述各过程的序号的大小并不意味着执行顺序的先后,各过程的执行顺序应以其功能和内在逻辑确定,而不应对本发明实施例的实施过程构成任何限定。上述本发明实施例序号仅仅为了描述,不代表实施例的优劣。

[0292] 需要说明的是,在本文中,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法或者装置不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法或者装置所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。在本申请实施例所提供的几个实施例中,应该理解到,所揭露的设备和方法,可以通过其它的方式实现。以上所描述的设备实施例仅仅

是示意性的，例如，所述单元的划分，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，如：多个单元或组件可以结合，或可以集成到另一个系统，或一些特征可以忽略，或不执行。

[0293] 上述作为分离部件说明的单元可以是、或也可以不是物理上分开的，作为单元显示的部件可以是、或也可以不是物理单元；既可以位于一个地方，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全部单元来实现本实施例方案的目的。本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成，前述的程序可以存储于计算机可读取存储介质中，该程序在执行时，执行包括上述方法实施例的步骤；而前述的计算机可读存储介质包括：移动存储设备、只读存储器、磁碟或者光盘等各种可以存储程序代码的介质。或者，本发明上述集成的单元如果以软件功能模块的形式实现并作为独立的产品销售或使用时，也可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明实施例的技术方案本质上或者说对相关技术做出贡献的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计算机可读存储介质中，包括若干指令用以使得一台终端执行本发明各个实施例所述方法的全部或部分。而前述的计算机可读存储介质包括：移动存储设备、ROM、磁碟或者光盘等各种可以存储程序代码的介质。

[0294] 在本申请所提供的几个实施例中，应该理解到，所揭露的设备和方法，可以通过其它的方式实现。以上所描述的设备实施例仅仅是示意性的，例如，所述单元的划分，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，如：多个单元或组件可以结合，或可以集成到另一个系统，或一些特征可以忽略，或不执行。另外，所显示或讨论的各组成部分相互之间的耦合、或直接耦合、或通信连接可以是通过一些接口，设备或单元的间接耦合或通信连接，可以是电性的、机械的或其它形式的。

[0295] 另外，在本发明各实施例中的各功能单元可以全部集成在一个处理模块中，也可以是各单元分别单独作为一个单元，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，也可以采用硬件加软件功能单元的形式实现。本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成，前述的程序可以存储于一计算机可读取存储介质中，该程序在执行时，执行包括上述方法实施例的步骤；而前述的存储介质包括：移动存储设备、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0296] 本申请所提供的几个方法或设备实施例中所揭露的特征，在不冲突的情况下可以任意组合，得到新的方法实施例或设备实施例。

[0297] 以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应以所述权利要求的保护范围为准。

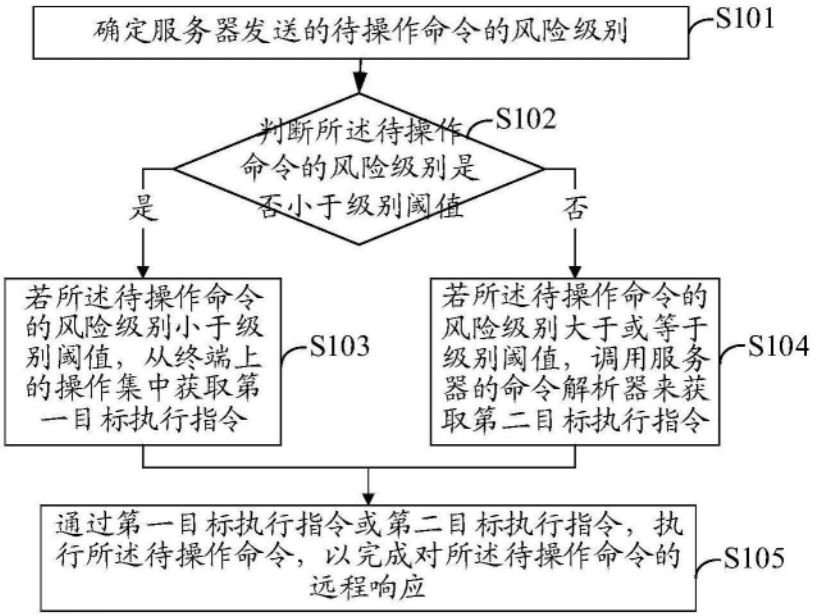

确定服务器发送的待操作命令的风险级别
S101
判断所述待操作命令的风险级别是否小于级别阈值
S102
是
否
若所述待操作命令的风险级别小于级别阈值，从终端上的操作集中获取第一目标执行指令
S103
若所述待操作命令的风险级别大于或等于级别阈值，调用服务器的命令解析器来获取第二目标执行指令
S104
通过第一目标执行指令或第二目标执行指令，执行所述待操作命令，以完成对所述待操作命令的远程响应
S105

图1A

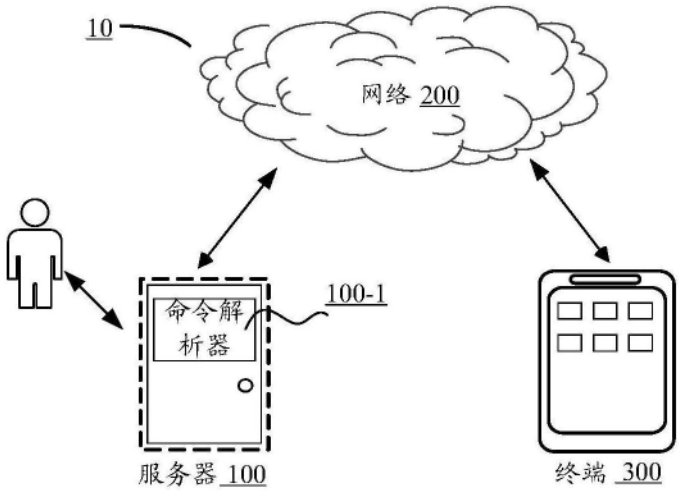

10
网络 200
命令解析器
100-1
服务器 100
终端 300

图1B

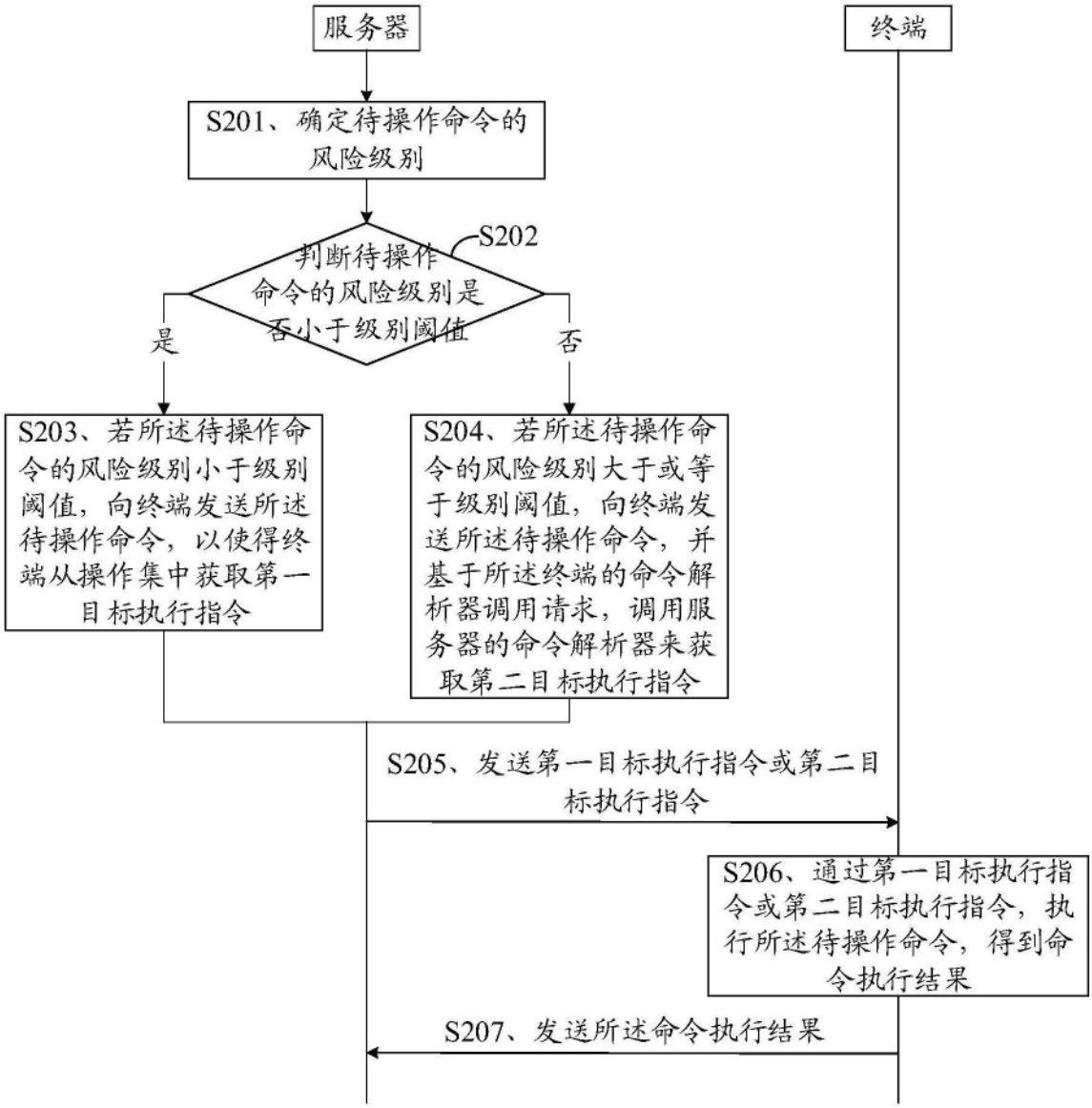

服务器
终端
S201、确定待操作命令的风险级别
S202
判断待操作命令的风险级别是否小于级别阈值
是
否
S203、若所述待操作命令的风险级别小于级别阈值，向终端发送所述待操作命令，以使得终端从操作集中获取第一目标执行指令
S204、若所述待操作命令的风险级别大于或等于级别阈值，向终端发送所述待操作命令，并基于所述终端的命令解析器调用请求，调用服务器的命令解析器来获取第二目标执行指令
S205、发送第一目标执行指令或第二目标执行指令
S206、通过第一目标执行指令或第二目标执行指令，执行所述待操作命令，得到命令执行结果
S207、发送所述命令执行结果

图2

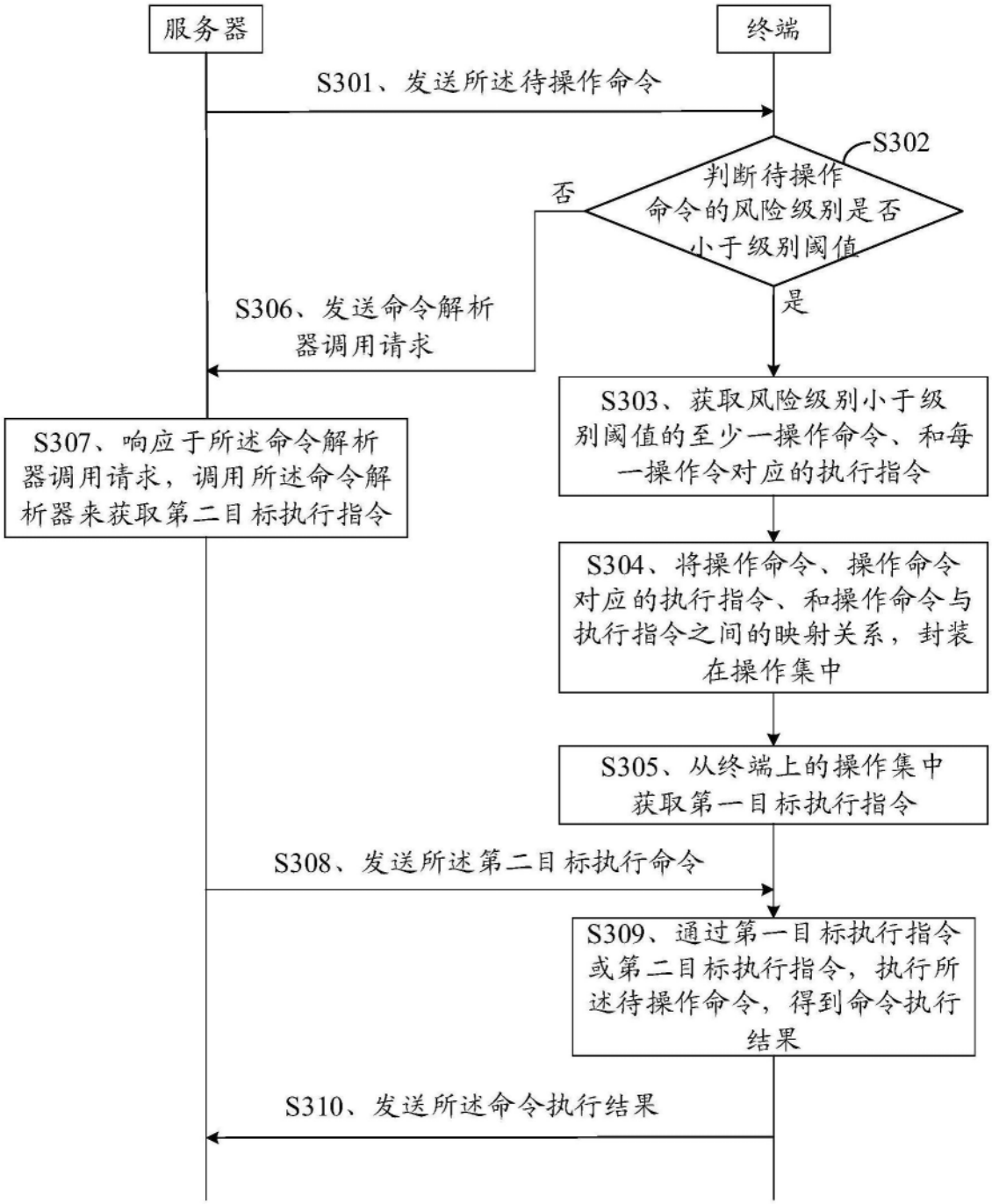

服务器
终端
S301、发送所述待操作命令
S302
判断待操作命令的风险级别是否小于级别阈值
否
是
S306、发送命令解析器调用请求
S303、获取风险级别小于级别阈值的至少一操作命令、和每一操作令对应的执行指令
S307、响应于所述命令解析器调用请求，调用所述命令解析器来获取第二目标执行指令
S304、将操作命令、操作命令对应的执行指令、和操作命令与执行指令之间的映射关系，封装在操作集中
S305、从终端上的操作集中获取第一目标执行指令
S308、发送所述第二目标执行命令
S309、通过第一目标执行指令或第二目标执行指令，执行所述待操作命令，得到命令执行结果
S310、发送所述命令执行结果

图3

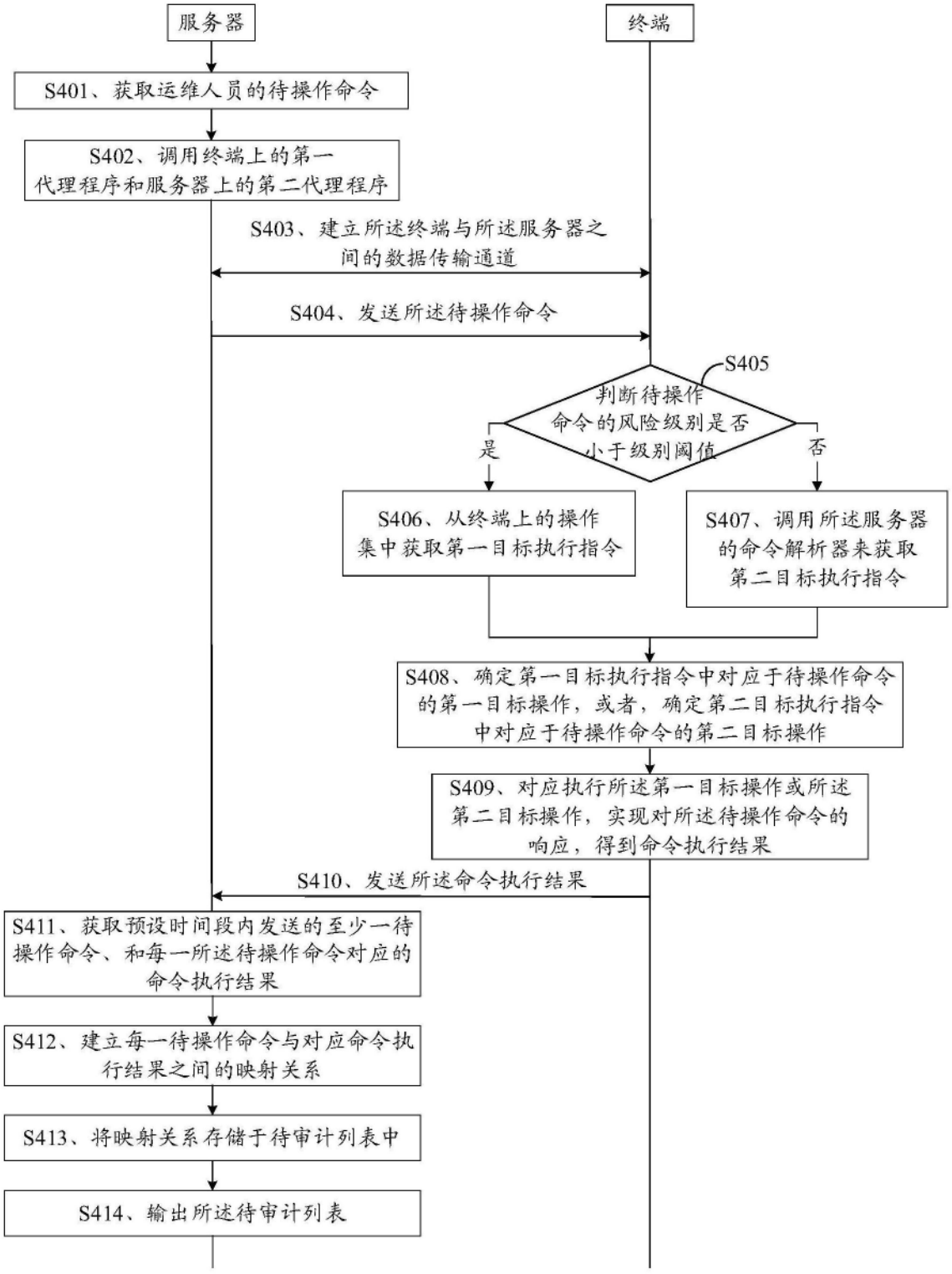

服务器
终端
S401、获取运维人员的待操作命令
S402、调用终端上的第一代理程序和服务器上的第二代理程序
S403、建立所述终端与所述服务器之间的数据传输通道
S404、发送所述待操作命令
S405
判断待操作命令的风险级别是否小于级别阈值
是
否
S406、从终端上的操作集中获取第一目标执行指令
S407、调用所述服务器的命令解析器来获取第二目标执行指令
S408、确定第一目标执行指令中对应于待操作命令的第一目标操作，或者，确定第二目标执行指令中对应于待操作命令的第二目标操作
S409、对应执行所述第一目标操作或所述第二目标操作，实现对所述待操作命令的响应，得到命令执行结果
S410、发送所述命令执行结果
S411、获取预设时间段内发送的至少一待操作命令、和每一所述待操作命令对应的命令执行结果
S412、建立每一待操作命令与对应命令执行结果之间的映射关系
S413、将映射关系存储于待审计列表中
S414、输出所述待审计列表

图4

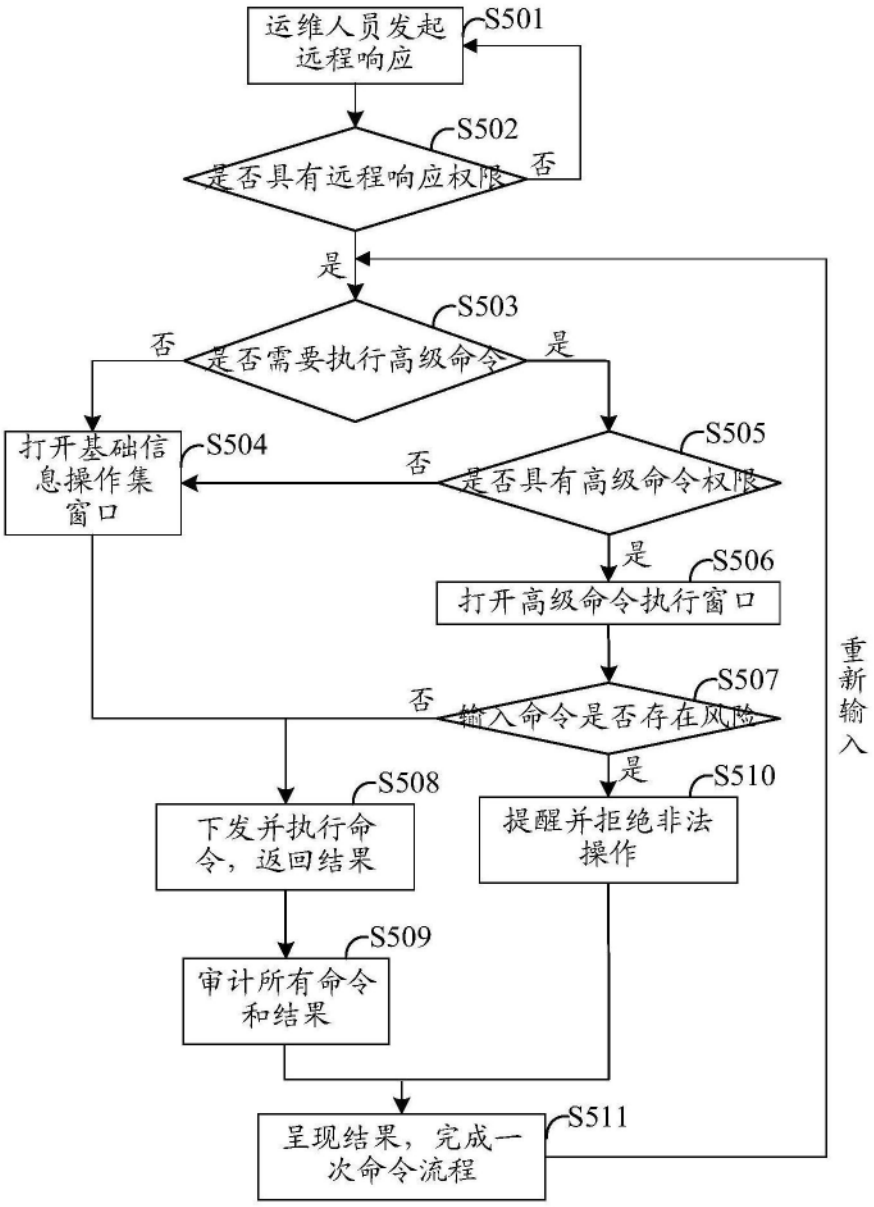

运维人员发起远程响应
S501
S502
是否具有远程响应权限
否
是
S503
是否需要执行高级命令
否
是
打开基础信息操作集窗口
S504
S505
否
是否具有高级命令权限
是
S506
打开高级命令执行窗口
S507
否
输入命令是否存在风险
是
S508
下发并执行命令，返回结果
S510
提醒并拒绝非法操作
S509
审计所有命令和结果
S511
呈现结果，完成一次命令流程
重新输入

图5A

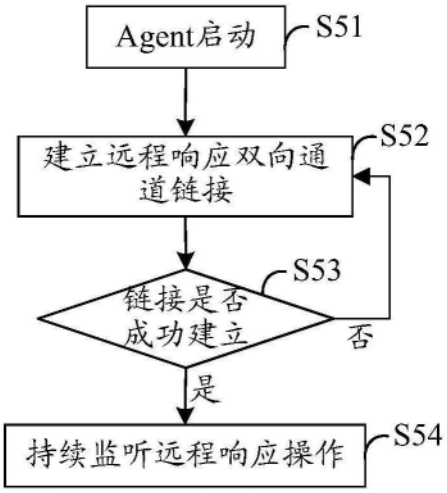

Agent启动
S51
建立远程响应双向通道链接
S52
链接是否成功建立
S53
否
是
持续监听远程响应操作
S54

图5B

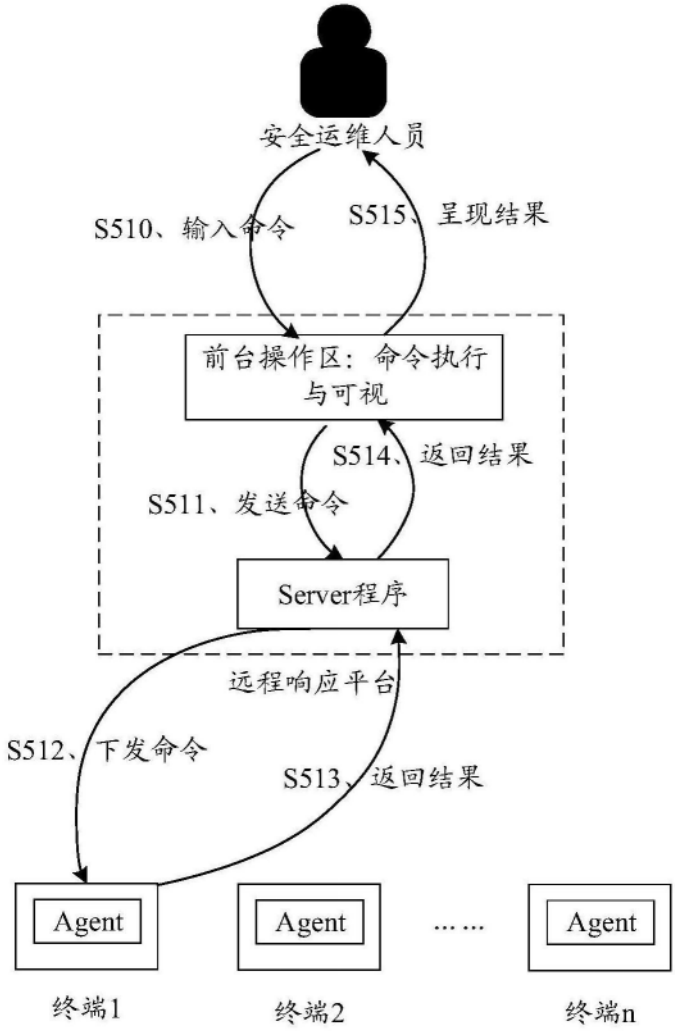

安全运维人员
S510、输入命令
S515、呈现结果
前台操作区：命令执行与可视
S514、返回结果
S511、发送命令
Server程序
远程响应平台
S512、下发命令
S513、返回结果
Agent
Agent
……
Agent
终端1
终端2
终端n

图5C

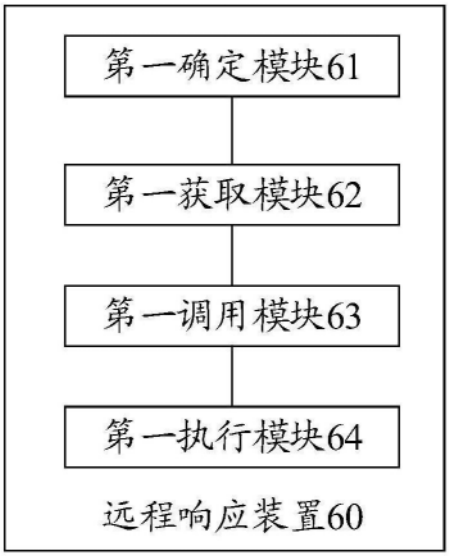

第一确定模块61
第一获取模块62
第一调用模块63
第一执行模块64
远程响应装置60

图6

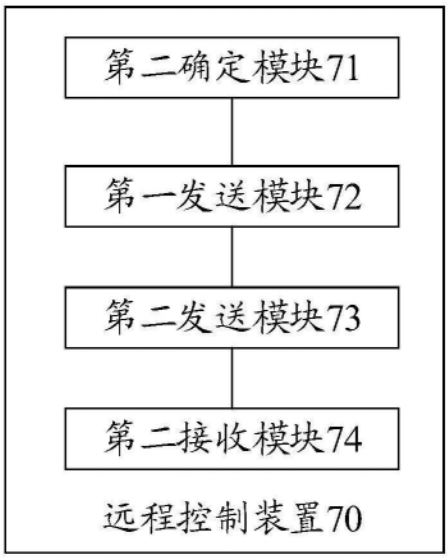

第二确定模块71
第一发送模块72
第二发送模块73
第二接收模块74
远程控制装置70

图7

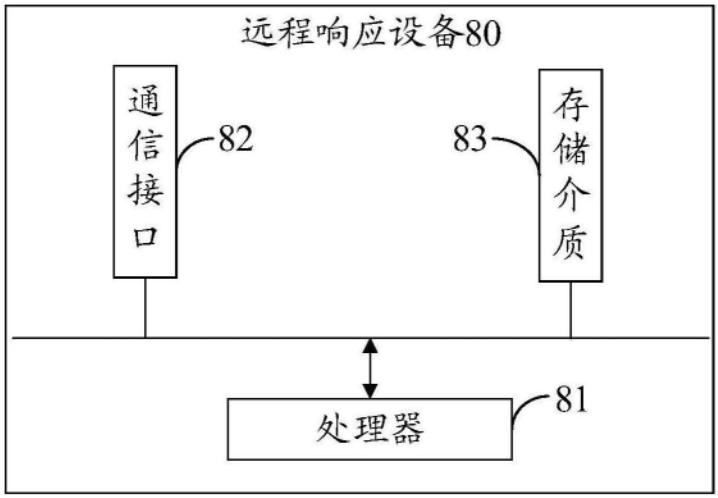

远程响应设备80
通信接口
82
83
存储介质
处理器
81

图8

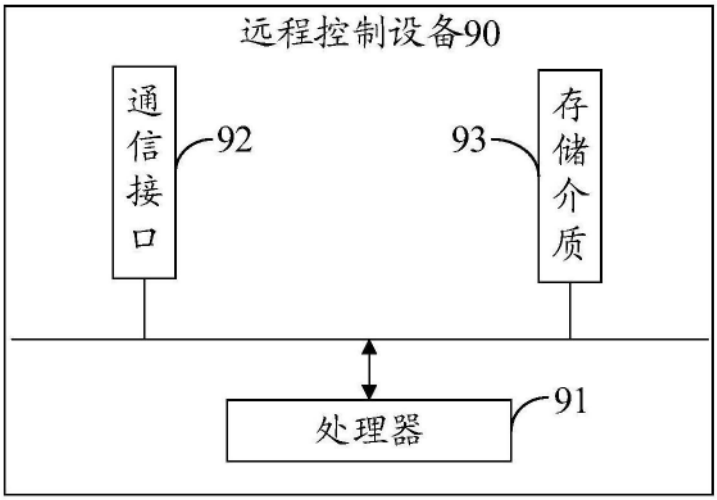

远程控制设备90
通信接口
92
93
存储介质
处理器
91

图9