(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111866044 B
(45)授权公告日 2024.09.17

(21)申请号 201910357610.X
(22)申请日 2019.04.29
(65)同一申请的已公布的文献号
申请公布号 CN 111866044 A
(43)申请公布日 2020.10.30
(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
(72)发明人 夏靓 王子韬 史玉林
(74)专利代理机构 北京三高永信知识产权代理有限责任公司 11138
专利代理师 颜晶
(51)Int.Cl.
H04L 67/51(2022.01)
H04L 41/0803(2022.01)

(56)对比文件
CN 103460215 A,2013.12.18
WO 2018140628 A1,2018.08.02
US 2007118642 A1,2007.05.24
US 2012216244 A1,2012.08.23
US 9088509 B1,2015.07.21

审查员 张琦

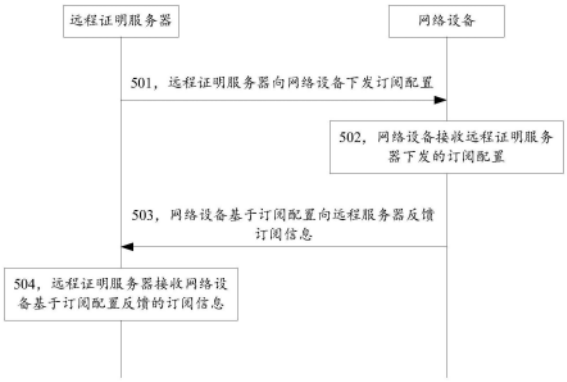
权利要求书5页 说明书23页 附图12页

(54)发明名称

数据采集方法、装置、设备及计算机可读存储介质

(57)摘要

本申请公开了采集数据的方法、装置、设备及计算机可读存储介质。方法应用于远程证明的过程中,方法包括:远程证明服务器向网络设备下发订阅配置,订阅配置用于订阅网络设备进行远程证明的相关信息;远程证明服务器接收网络设备基于订阅配置反馈的订阅信息。通过远程证明服务器向网络设备下发订阅配置,网络设备可据此自动反馈订阅信息,使得远程证明中的数据采集方式更为灵活,及时性较高,进而降低安全风险。此外,由于订阅配置无需远程证明服务器多次下发,因而减少了额外的消息交互,进而提高了数据采集效率。



CN 111866044 B

1.一种数据采集方法,其特征在于,所述方法应用于远程证明的过程中,所述方法包括:

远程证明服务器向网络设备下发订阅配置,所述订阅配置用于订阅所述网络设备进行远程证明的相关信息,所述订阅配置包括事件的订阅配置,订阅信息包括设备启动、设备升级、主备切换、单板拔插/切换、证书生命周期事件中的一种或多种事件触发的相关信息,所述订阅信息用于证明所述网络设备是否可信;

所述远程证明服务器接收所述网络设备基于所述订阅配置反馈的所述订阅信息。

2.根据权利要求1所述的方法,其特征在于,所述订阅配置还包括数据流的订阅配置。

3.根据权利要求2所述的方法,其特征在于,若所述订阅配置包括数据流的订阅配置,则所述订阅信息包括以下信息中的一种或多种:

所述网络设备启动时记录的信任链的各层的软件的完整性信息,

所述网络设备运行时记录的操作系统动态完整性信息,

所述网络设备运行时记录的软件的动态完整性信息,

所述网络设备相关的身份证书,和

所述网络设备相关的远程证明证书。

4.根据权利要求1-3任一所述的方法,其特征在于,所述订阅配置还包括订阅模式,所述订阅模式用于指示反馈所述订阅信息的方式,所述订阅模式包括周期性反馈和事件触发反馈中的一种或组合。

5.根据权利要求4所述的方法,其特征在于,不同类型的信息对应不同的订阅模式。

6.根据权利要求1-3或5任一所述的方法,其特征在于,所述订阅配置还包括过滤器的配置,所述订阅信息包括基于所述过滤器的配置进行过滤之后得到的信息。

7.根据权利要求4所述的方法,其特征在于,所述订阅配置还包括过滤器的配置,所述订阅信息包括基于所述过滤器的配置进行过滤之后得到的信息。

8.根据权利要求1-3、5或7任一所述的方法,其特征在于,所述方法还包括:向所述网络设备下发数据处理参数,所述订阅信息包括基于所述数据处理参数处理之后得到的信息。

9.根据权利要求4所述的方法,其特征在于,所述方法还包括:向所述网络设备下发数据处理参数,所述订阅信息包括基于所述数据处理参数处理之后得到的信息。

10.根据权利要求6所述的方法,其特征在于,所述方法还包括:向所述网络设备下发数据处理参数,所述订阅信息包括基于所述数据处理参数处理之后得到的信息。

11.根据权利要求1-3、5、7、9或10任一所述的方法,其特征在于,所述向网络设备下发订阅配置,包括:

与所述网络设备建立网络配置协议会话,基于所述网络配置协议会话向所述网络设备下发订阅配置。

12.根据权利要求4所述的方法,其特征在于,所述向网络设备下发订阅配置,包括:

与所述网络设备建立网络配置协议会话,基于所述网络配置协议会话向所述网络设备下发订阅配置。

13.根据权利要求6所述的方法,其特征在于,所述向网络设备下发订阅配置,包括:

与所述网络设备建立网络配置协议会话,基于所述网络配置协议会话向所述网络设备下发订阅配置。

14.根据权利要求8所述的方法,其特征在于,所述向网络设备下发订阅配置,包括:

与所述网络设备建立网络配置协议会话,基于所述网络配置协议会话向所述网络设备下发订阅配置。

15.一种数据采集方法,其特征在于,所述方法应用于远程证明的过程中,所述方法包括:

网络设备接收远程证明服务器下发的订阅配置,所述订阅配置用于订阅所述网络设备进行远程证明的相关信息,所述订阅配置包括事件的订阅配置,订阅信息包括设备启动、设备升级、主备切换、单板拔插/切换、证书生命周期事件中的一种或多种事件触发的相关信息,所述订阅信息用于证明所述网络设备是否可信;

所述网络设备基于所述订阅配置向所述远程证明服务器反馈所述订阅信息。

16.根据权利要求15所述的方法,其特征在于,所述订阅配置还包括数据流的订阅配置。

17.根据权利要求16所述的方法,其特征在于,若所述订阅配置包括数据流的订阅配置,所述基于所述订阅配置向所述远程证明服务器反馈所述订阅信息,包括:

基于所述数据流的订阅配置向所述远程证明服务器反馈以下信息中的一种或多种:

所述网络设备启动时记录的信任链的各层的软件的完整性信息,

所述网络设备运行时记录的操作系统动态完整性信息,

所述网络设备运行时记录的软件的动态完整性信息,

所述网络设备相关的身份证书,和

所述网络设备相关的远程证明证书。

18.根据权利要求15-17任一所述的方法,其特征在于,所述订阅配置还包括订阅模式,所述订阅模式用于指示反馈所述订阅信息的方式,所述订阅模式包括周期性反馈和事件触发反馈中的一种或组合;

所述基于所述订阅配置向所述远程证明服务器反馈所述订阅信息,包括:

基于所述订阅配置中包括的订阅模式,向所述远程证明服务器反馈所述订阅信息。

19.根据权利要求18所述的方法,其特征在于,不同类型的信息对应不同的订阅模式。

20.根据权利要求15-17或19任一所述的方法,其特征在于,所述订阅配置还包括过滤器的配置,所述订阅信息包括基于所述过滤器的配置进行过滤之后得到的信息。

21.根据权利要求18所述的方法,其特征在于,所述订阅配置还包括过滤器的配置,所述订阅信息包括基于所述过滤器的配置进行过滤之后得到的信息。

22.根据权利要求15-17、19或21任一所述的方法,其特征在于,所述方法还包括:接收所述远程证明服务器下发的数据处理参数,所述订阅信息包括基于所述数据处理参数处理之后得到的信息。

23.根据权利要求18所述的方法,其特征在于,所述方法还包括:接收所述远程证明服务器下发的数据处理参数,所述订阅信息包括基于所述数据处理参数处理之后得到的信息。

24.根据权利要求20所述的方法,其特征在于,所述方法还包括:接收所述远程证明服务器下发的数据处理参数,所述订阅信息包括基于所述数据处理参数处理之后得到的信息。

25.根据权利要求15-17、19、21、23或24任一所述的方法,其特征在于,所述接收远程证明服务器下发的订阅配置,包括:

与所述远程证明服务器建立网络配置协议会话,基于所述网络配置协议会话接收所述远程证明服务器下发的订阅配置。

26.根据权利要求18所述的方法,其特征在于,所述接收远程证明服务器下发的订阅配置,包括:

与所述远程证明服务器建立网络配置协议会话,基于所述网络配置协议会话接收所述远程证明服务器下发的订阅配置。

27.根据权利要求20所述的方法,其特征在于,所述接收远程证明服务器下发的订阅配置,包括:

与所述远程证明服务器建立网络配置协议会话,基于所述网络配置协议会话接收所述远程证明服务器下发的订阅配置。

28.根据权利要求22所述的方法,其特征在于,所述接收远程证明服务器下发的订阅配置,包括:

与所述远程证明服务器建立网络配置协议会话,基于所述网络配置协议会话接收所述远程证明服务器下发的订阅配置。

29.一种数据采集装置,其特征在于,所述装置应用于远程证明的过程中,所述装置包括:

发送模块,用于向网络设备下发订阅配置,所述订阅配置用于订阅所述网络设备进行远程证明的相关信息,所述订阅配置包括事件的订阅模式,订阅信息包括设备启动、设备升级、主备切换、单板拔插/切换、证书生命周期事件中的一种或多种事件触发的相关信息,所述订阅信息用于证明所述网络设备是否可信;

接收模块,用于接收所述网络设备基于所述订阅配置反馈的所述订阅信息。

30.根据权利要求29所述的装置,其特征在于,所述订阅配置还包括数据流的订阅配置。

31.根据权利要求30所述的装置,其特征在于,若所述订阅配置包括数据流的订阅配置,则所述订阅信息包括以下信息中的一种或多种:

所述网络设备启动时记录的信任链的各层的软件的完整性信息,

所述网络设备运行时记录的操作系统动态完整性信息,

所述网络设备运行时记录的软件的动态完整性信息,

所述网络设备相关的身份证书,和

所述网络设备相关的远程证明证书。

32.根据权利要求29-31任一所述的装置,其特征在于,所述订阅配置还包括订阅模式,所述订阅模式用于指示反馈所述订阅信息的方式,所述订阅模式包括周期性反馈和事件触发反馈中的一种或组合。

33.根据权利要求32所述的装置,其特征在于,不同类型的信息对应不同的订阅模式。

34.根据权利要求29-31或33任一所述的装置,其特征在于,所述订阅配置还包括过滤器的配置,所述订阅信息包括基于所述过滤器的配置进行过滤之后得到的信息。

35.根据权利要求32所述的装置,其特征在于,所述订阅配置还包括过滤器的配置,所

述订阅信息包括基于所述过滤器的配置进行过滤之后得到的信息。

36.根据权利要求29-31、33或35任一所述的装置,其特征在于,所述发送模块,还用于向所述网络设备下发数据处理参数,所述订阅信息包括基于所述数据处理参数处理之后得到的信息。

37.根据权利要求32所述的装置,其特征在于,所述发送模块,还用于向所述网络设备下发数据处理参数,所述订阅信息包括基于所述数据处理参数处理之后得到的信息。

38.根据权利要求34所述的装置,其特征在于,所述发送模块,还用于向所述网络设备下发数据处理参数,所述订阅信息包括基于所述数据处理参数处理之后得到的信息。

39.根据权利要求29-31、33、35、37或38任一所述的装置,其特征在于,所述发送模块,用于与所述网络设备建立网络配置协议会话,基于所述网络配置协议会话向所述网络设备下发订阅配置。

40.根据权利要求32所述的装置,其特征在于,所述发送模块,用于与所述网络设备建立网络配置协议会话,基于所述网络配置协议会话向所述网络设备下发订阅配置。

41.根据权利要求34所述的装置,其特征在于,所述发送模块,用于与所述网络设备建立网络配置协议会话,基于所述网络配置协议会话向所述网络设备下发订阅配置。

42.根据权利要求36所述的装置,其特征在于,所述发送模块,用于与所述网络设备建立网络配置协议会话,基于所述网络配置协议会话向所述网络设备下发订阅配置。

43.一种数据采集装置,其特征在于,所述装置应用于远程证明的过程中,所述装置包括:

接收模块,用于接收远程证明服务器下发的订阅配置,所述订阅配置用于订阅网络设备进行远程证明的相关信息,所述订阅配置包括事件的订阅配置,订阅信息包括设备启动、设备升级、主备切换、单板拔插/切换、证书生命周期事件中的一种或多种事件触发的相关信息,所述订阅信息用于证明所述网络设备是否可信;

发送模块,用于基于所述订阅配置向所述远程证明服务器反馈所述订阅信息。

44.根据权利要求43所述的装置,其特征在于,所述订阅配置还包括数据流的订阅配置。

45.根据权利要求44所述的装置,其特征在于,若所述订阅配置包括数据流的订阅配置,所述发送模块,用于基于所述数据流的订阅配置向所述远程证明服务器反馈以下信息中的一种或多种:

所述网络设备启动时记录的信任链的各层的软件的完整性信息,

所述网络设备运行时记录的操作系统动态完整性信息,

所述网络设备运行时记录的软件的动态完整性信息,

所述网络设备相关的身份证书,和

所述网络设备相关的远程证明证书。

46.根据权利要求43-45任一所述的装置,其特征在于,所述订阅配置还包括订阅模式,所述订阅模式用于指示反馈所述订阅信息的方式,所述订阅模式包括周期性反馈和事件触发反馈中的一种或组合;

所述发送模块,用于基于所述订阅配置中包括的订阅模式,向所述远程证明服务器反馈所述订阅信息。

47.根据权利要求46所述的装置,其特征在于,不同类型的信息对应不同的订阅模式。

48.根据权利要求43-45或47任一所述的装置,其特征在于,所述订阅配置还包括过滤器的配置,所述订阅信息包括基于所述过滤器的配置进行过滤之后得到的信息。

49.根据权利要求46所述的装置,其特征在于,所述订阅配置还包括过滤器的配置,所述订阅信息包括基于所述过滤器的配置进行过滤之后得到的信息。

50.根据权利要求43-45、47或49任一所述的装置,其特征在于,所述接收模块,还用于接收所述远程证明服务器下发的数据处理参数,所述发送模块反馈的所述订阅信息包括基于所述数据处理参数处理之后得到的信息。

51.根据权利要求46所述的装置,其特征在于,所述接收模块,还用于接收所述远程证明服务器下发的数据处理参数,所述发送模块反馈的所述订阅信息包括基于所述数据处理参数处理之后得到的信息。

52.根据权利要求48所述的装置,其特征在于,所述接收模块,还用于接收所述远程证明服务器下发的数据处理参数,所述发送模块反馈的所述订阅信息包括基于所述数据处理参数处理之后得到的信息。

53.根据权利要求43-45、47、49、51或52任一所述的装置,其特征在于,所述接收模块,用于与所述远程证明服务器建立网络配置协议会话,基于所述网络配置协议会话接收所述远程证明服务器下发的订阅配置。

54.根据权利要求46所述的装置,其特征在于,所述接收模块,用于与所述远程证明服务器建立网络配置协议会话,基于所述网络配置协议会话接收所述远程证明服务器下发的订阅配置。

55.根据权利要求48所述的装置,其特征在于,所述接收模块,用于与所述远程证明服务器建立网络配置协议会话,基于所述网络配置协议会话接收所述远程证明服务器下发的订阅配置。

56.根据权利要求50所述的装置,其特征在于,所述接收模块,用于与所述远程证明服务器建立网络配置协议会话,基于所述网络配置协议会话接收所述远程证明服务器下发的订阅配置。

57.一种数据采集设备,其特征在于,所述设备包括存储器及处理器;所述存储器中存储有至少一条指令,所述至少一条指令由所述处理器加载并执行,以实现权利要求1-14中任一所述的数据采集方法,或者实现权利要求15-28中任一所述的数据采集方法。

58.一种计算机可读存储介质,其特征在于,所述存储介质中存储有至少一条指令,所述指令由处理器加载并执行以实现权利要求1-14中任一所述的数据采集方法,或者实现权利要求15-28中任一所述的数据采集方法。

59.一种计算机程序产品,其特征在于,所述计算机程序产品包括:计算机程序代码,当所述计算机程序代码被计算机运行时,使得所述计算机执行权利要求1-14中任一所述的数据采集方法,或者执行权利要求15-28中任一所述的数据采集方法。

数据采集方法、装置、设备及计算机可读存储介质

技术领域

[0001] 本申请涉及计算机安全技术领域，特别涉及数据采集方法、装置、设备及计算机可读存储介质。

背景技术

[0002] 随着计算机安全技术的发展，可信计算的研究越来越受到重视，而远程证明又是可信计算中的重要一环。为了进行远程证明，远程证明服务器需要采集网络设备上的数据，因此，采集数据的方式显得尤为重要。

[0003] 相关技术在采集数据时，提供了一种轮询式挑战响应机制。该种机制下，由远程证明服务器发起请求，网络设备基于该请求答复当前的可信信息和状态。

[0004] 不难看出，轮询式挑战响应机制中，由于每次需要服务器发起请求后，网络设备才进行答复，因而该种数据采集方式不够灵活。

[0005] 申请内容

[0006] 本申请实施例提供了一种数据采集方法、装置、设备及计算机可读存储介质，以解决相关技术中的问题，技术方案如下：

[0007] 第一方面，提供了一种数据采集方法，所述方法应用于远程证明的过程中，根据该方法，远程证明服务器向网络设备下发订阅配置，所述订阅配置用于订阅所述网络设备进行远程证明的相关信息。所述远程证明服务器接收所述网络设备基于所述订阅配置反馈的订阅信息。通过远程证明服务器向网络设备下发订阅配置，网络设备可据远程证明服务器的订阅自动反馈订阅信息，这样，网络设备在远程证明中的数据采集方式较为灵活。而且，由于订阅配置无需远程证明服务器多次下发，可减少额外的消息交互，提高数据采集效率。

[0008] 可选地，所述方法还包括：远程证明服务器向所述网络设备下发数据处理参数，所述订阅信息包括所述网络设备基于所述数据处理参数处理之后得到的信息。通过提前将数据处理参数下发至网络设备，以备网络设备反馈信息时使用，减少了交互次数，提高了数据采集效率。

[0009] 可选地，所述向网络设备下发订阅配置，包括：所述远程证明服务器与所述网络设备建立网络配置协议会话，基于所述网络配置协议会话向所述网络设备下发订阅配置。通过网络配置协议来实现信息订阅，不仅有广泛的使用场景，还可继承网络配置协议的灵活、高效、主动通知、确保时效性等优点。

[0010] 第二方面，提供了一种数据采集方法，所述方法应用于远程证明的过程中，所述方法包括：网络设备接收远程证明服务器下发的订阅配置，所述订阅配置用于订阅所述网络设备进行远程证明的相关信息；所述网络设备基于所述订阅配置向所述远程证明服务器反馈订阅信息。

[0011] 可选地，上述订阅配置包括数据流的订阅配置和事件的订阅配置中的一种或多种。

[0012] 可选地，若所述订阅配置包括数据流的订阅配置，所述基于所述订阅配置向所述

远程证明服务器反馈订阅信息,包括:基于所述数据流的订阅配置向所述远程服务器反馈以下信息中的一种或多种:

[0013] 所述网络设备启动时记录的信任链的各层的软件的完整性信息,

[0014] 所述网络设备运行时记录的操作系统动态完整性信息,

[0015] 所述网络设备运行时记录的软件的动态完整性信息,

[0016] 所述网络设备相关的身份证书,和

[0017] 所述网络设备相关的远程证明证书。

[0018] 可选地,若所述订阅配置包括事件的订阅配置,所述基于所述订阅配置向所述远程证明服务器反馈订阅信息,包括:基于所述事件的订阅配置向所述远程服务器反馈设备启动、设备升级、特定模式攻击事件、主备切换、单板插拔/切换、证书生命周期事件中的一种或多种事件触发后的相关信息。

[0019] 可选地,上述订阅配置还包括订阅模式,所述订阅模式用于指示反馈订阅信息的方式,所述订阅模式包括周期性反馈和事件触发反馈中的一种或组合;

[0020] 所述基于所述订阅配置向所述远程证明服务器反馈订阅信息,包括:

[0021] 基于所述订阅配置中包括的订阅模式,向所述远程证明服务器反馈订阅信息。

[0022] 可选地,上述不同类型的信息对应不同的订阅模式。

[0023] 可选地,上述订阅配置还包括过滤器的配置,所述订阅信息包括基于所述过滤器的配置进行过滤之后得到的信息。

[0024] 可选地,所述方法还包括:接收所述远程证明服务器下发的数据处理参数,所述订阅信息包括基于所述数据处理参数处理之后得到的信息。

[0025] 可选地,所述接收远程证明服务器下发的订阅配置,包括:与所述远程证明服务器建立网络配置协议会话,基于所述网络配置协议会话接收所述远程证明服务器下发的订阅配置。

[0026] 第三方面,提供了一种数据采集装置,所述装置应用于远程证明的过程中,所述装置包括:发送模块,用于向网络设备下发订阅配置,所述订阅配置用于订阅所述网络设备进行远程证明的相关信息;接收模块,用于接收所述网络设备基于所述订阅配置反馈的订阅信息。

[0027] 可选地,所述发送模块,还用于向所述网络设备下发数据处理参数,所述订阅信息包括基于所述数据处理参数处理之后得到的信息。

[0028] 可选地,所述发送模块,用于与所述网络设备建立网络配置协议会话,基于所述网络配置协议会话向所述网络设备下发订阅配置。

[0029] 第四方面,提供了一种数据采集装置,所述装置应用于远程证明的过程中,所述装置包括:接收模块,用于接收远程证明服务器下发的订阅配置,所述订阅配置用于订阅所述网络设备进行远程证明的相关信息;发送模块,用于基于所述订阅配置向所述远程证明服务器反馈订阅信息。

[0030] 可选地,若所述订阅配置包括数据流的订阅配置,所述发送模块,用于基于所述数据流的订阅配置向所述远程服务器反馈以下信息中的一种或多种:

[0031] 所述网络设备启动时记录的信任链的各层的软件的完整性信息,

[0032] 所述网络设备运行时记录的操作系统动态完整性信息,

[0033] 所述网络设备运行时记录的软件的动态完整性信息，

[0034] 所述网络设备相关的身份证书，和

[0035] 所述网络设备相关的远程证明证书。

[0036] 可选地，若所述订阅配置包括事件的订阅配置，所述发送模块，用于基于所述事件的订阅配置向所述远程服务器反馈设备启动、设备升级、特定模式攻击事件、主备切换、单板插拔/切换、证书生命周期事件中的一种或多种事件触发后的相关信息。

[0037] 可选地，所述订阅配置还包括订阅模式，所述订阅模式用于指示反馈订阅信息的方式，所述订阅模式包括周期性反馈和事件触发反馈中的一种或组合；

[0038] 所述发送模块，用于基于所述订阅配置中包括的订阅模式，向所述远程证明服务器反馈订阅信息。

[0039] 可选地，所述接收模块，还用于接收所述远程证明服务器下发的数据处理参数，所述发送模块反馈的订阅信息包括基于所述数据处理参数处理之后得到的信息。

[0040] 可选地，所述接收模块，用于与所述远程证明服务器建立网络配置协议会话，基于所述网络配置协议会话接收所述远程证明服务器下发的订阅配置。

[0041] 第五方面，提供了一种采集数据的设备，所述设备包括存储器及处理器；所述存储器中存储有至少一条指令，所述至少一条指令由所述处理器加载并执行，以实现本申请第一方面或第二方面的任一种可能的实施方式中的方法。

[0042] 第六方面，提供了一种通信装置，该装置包括：收发器、存储器和处理器。其中，该收发器、该存储器和该处理器通过内部连接通路互相通信，该存储器用于存储指令，该处理器用于执行该存储器存储的指令，以控制收发器接收信号，并控制收发器发送信号，并且当该处理器执行该存储器存储的指令时，使得该处理器执行第一方面或第二方面的任一种可能的实施方式中的方法。

[0043] 可选地，所述处理器为一个或多个，所述存储器为一个或多个。

[0044] 可选地，所述存储器可以与所述处理器集成在一起，或者所述存储器与处理器分离设置。

[0045] 在具体实现过程中，存储器可以为非瞬时性(non-transitory)存储器，例如只读存储器(read only memory，ROM)，其可以与处理器集成在同一块芯片上，也可以分别设置在不同的芯片上，本申请实施例对存储器的类型以及存储器与处理器的设置方式不做限定。

[0046] 第七方面，提供了一种通信系统，该系统包括上述第三方面或第三方面的任一种可能实施方式中的装置，以及上述第四方面或第四方面的任一种可能实施方式中的装置。

[0047] 第八方面，提供了一种计算机程序(产品)，所述计算机程序(产品)包括：计算机程序代码，当所述计算机程序代码被计算机运行时，使得所述计算机执行上述第一方面或第二方面的任一种可能的实施方式中的方法。

[0048] 第九方面，提供了一种可读存储介质，可读存储介质存储程序或指令，当所述程序或指令在计算机上运行时，上述第一方面或第二方面的任一种可能的实施方式中的方法被执行。

[0049] 第十方面，提供了一种芯片，包括处理器，处理器用于从存储器中调用并运行所述存储器中存储的指令，使得安装有所述芯片的通信设备执行上述第一方面或第二方面的任

一种可能的实施方式中的方法。

[0050] 第十一方面,提供另一种芯片,包括:输入接口、输出接口、处理器和存储器,所述输入接口、输出接口、所述处理器以及所述存储器之间通过内部连接通路相连,所述处理器用于执行所述存储器中的代码,当所述代码被执行时,所述处理器用于执行上述第一方面或第二方面的任一种可能的实施方式中的方法。

[0051] 根据本申请实施例的技术方案,通过远程证明服务器向网络设备下发订阅配置,网络设备可据此自动反馈订阅信息,使得远程证明中的数据采集方式更为灵活,及时性较高,进而降低安全风险。此外,由于订阅配置无需远程证明服务器多次下发,因而减少了额外的消息交互,进而提高了数据采集效率。

附图说明

[0052] 图1A为本申请实施例提供的远程认证过程示意图;

[0053] 图1B为本申请实施例提供的实施环境示意图;

[0054] 图2为本申请实施例提供的启动过程示意图;

[0055] 图3为本申请实施例提供的启动过程示意图;

[0056] 图4为本申请实施例提供的远程证明过程示意图;

[0057] 图5为本申请实施例提供的采集数据的方法流程图;

[0058] 图6为本申请实施例提供的配置订阅数据模型树形结构示意图;

[0059] 图7为本申请实施例提供的会话交互示意图;

[0060] 图8为本申请实施例提供的会话交互示意图;

[0061] 图9为本申请实施例提供的动态订阅数据模型树形结构示意图;

[0062] 图10为本申请实施例提供的动态订阅数据模型树形结构示意图;

[0063] 图11为本申请实施例提供的会话交互示意图;

[0064] 图12为本申请实施例提供的会话交互示意图;

[0065] 图13为本申请实施例提供的动态订阅数据模型树形结构示意图;

[0066] 图14为本申请实施例提供的采集数据的装置结构示意图;

[0067] 图15为本申请实施例提供的采集数据的装置结构示意图;

[0068] 图16为本申请实施例提供的采集数据的设备结构示意图;

[0069] 图17为本申请实施例提供的通信装置结构示意图。

具体实施方式

[0070] 本申请的实施方式部分使用的术语仅用于对本申请的实施例进行解释,而非旨在限定本申请。

[0071] 在可信计算体系中,建立可信网络系统需要先拥有可信根(root-of-trust,RoT),然后建立一条可信链(Chain of Trust),再将可信传递到网络系统的各个模块,之后就能建立整个网络系统的可信。由此可见,可信根需要是一个能够被信任的组件。由于一般可以认为可信平台模块(trusted platform module,TPM)和基本输入输出系统(basic input output system,BIOS)是绝对可信的,因而可信根可存在于每个网络设备的TPM和BIOS中。

[0072] 一个可信网络设备包括三个可信根:度量可信根(root of trust for

measurement,RTM)、存储可信根(root of trust for storage,RTS)和报告可信根(root of trust for reporting,RTR)。其中,RTM被用来完成完整性度量,通常使用度量可信根的核心(core root of trust for measurement,CRTM)所控制的计算引擎来完成完整性度量。CRTM包括网络设备执行RTM时的执行代码,CRTM一般存在BIOS中。RTM也是信任传递的原点。RTS是维护完整性摘要的值和摘要序列的引擎,RTS一般包括对存储的信息加密的引擎和加密密钥。RTR是计算引擎,能够可靠地报告RTS持有的数据,这个可靠性一般由签名来保证。

[0073] 远程证明(remote attestation,RA)是可信计算整体解决方案中的技术之一,RA用于判断可信服务器的可信性状态。如图1A所示,远程证明系统包括RA服务器(RA server)、RA客户端(RA client)和隐私证书颁发中心(privacy certificate authority,PCA)。RA服务器保存有RA客户端的平台配置寄存器(platform configure register,PCR)的参考值,负责接收RA客户端发送的PCR值,并给出RA客户端的可信状态。RA客户端是带有TPM并支持可信启动功能的设备。RA客户端向PCA申请并获得PCA分配的证明标识密钥(attestation identity key,AIK)证书。当某些场景下,RA服务器会发起对RA客户端的远程认证,RA服务器向RA客户端发起挑战请求,RA客户端收集PCR值,使用AIK私钥签名后,将使用AIK私钥签名的PCR值以及AIK证书一起发送给RA服务器,RA服务器向PCA验证RA客户端发送的AIK证书的有效性。PCA向RA服务器返回对应该RA客户端的PCR参考值,RA服务器将RA客户端发送的PCR值与所述RA客户端的PCR参考值比较,根据比较结果确定RA客户端的可信性状态,即确定RA客户端是否可信。

[0074] 以图1B所示的实施环境中,可信计算组织(trusted computing group,TCG)提出的可信根存在于TPM为例,网络管理系统(network management system,NMS)和/或运行支持系统(operations supporting system,OSS)作为RA服务器,网络设备作为RA客户端,网络设备包括TPM。从网络设备上电开始,到网络设备的BIOS启动、网络设备上的多重操作系统启动管理器(grand unified bootloader,GRUB)及网络设备的系统核心程序加载的整个过程中,每个过程都需要NMS/OSS进行远程认证,以便逐级建立信任链。网络设备将度量得到的动态度量及静态度量等度量值存储在TPM的PCR中。网络设备的远程证明模块将这些度量值发送给作为RA服务器的NMS/OSS。而NMS/OSS可以根据PCR值与度量日志计算获取网络设备的当前状态。之后,再与预期值对比判断网络设备的可信性。图1B中的高安全区可以包括系统核心程序或信任区或因特尔软件保护扩展(intel software guard extensions,SGX)等。图1B中的终端具有设备身份组合引擎(device identity combination engine,DICE)。

[0075] 由于网络设备的安全性严重依赖于设备上运行的软件的完整性,通常使用信任链模型确保软件完整性,启动期间每个阶段在执行前检查下一个阶段。如图2所示,可信根(RoT)要确保绝对安全,然后在设备启动过程中,系统固件(firmware)初始化整个硬件系统,并对下一阶段要运行的系统载入程序(loader)进行检查,即,对下一阶段要运行的系统载入程序(loader)进行HASH签名对比。如果系统载入程序通过检查,则启动系统载入程序,并由系统载入程序对下一阶段要运行的系统核心程序(kernal)进行检查。如果系统核心程序通过检查,则启动系统核心程序。以上从检查到启动的过程一直重复,直到启动过程全部完成。其中,启动包括安全启动(Secure BOOT)和可信启动(Trusted BOOT)。

[0076] 安全启动是统一的可扩展固件接口(unified extensible firmware interface,UEFI)的一个部分(子规则),两者是局部与整体的关系。UEFI是一种详细描述类型接口的标准,这种接口用于操作系统自动从预启动的操作环境,加载到一种操作系统上。可扩展固件接口(extensible firmware interface,EFI)是Intel为个人计算机(personal computer,PC)固件的体系结构、接口和服务提出的建议标准,其主要目的是为了提供一组在操作系统(operating system,OS)加载之前(启动前)在所有平台上一致的、正确指定的启动服务。而Secure BOOT采用密钥的方式来防止恶意软件侵入。UEFI规定,主板出厂的时候,可以内置一些可靠的公钥。然后,任何想要在这块主板上加载的操作系统或者硬件驱动程序,都必须通过这些公钥的认证。也就是说,这些软件必须用对应的私钥签署过,否则主板拒绝加载。由于恶意软件不可能通过认证,因此就没有办法感染BOOT。

[0077] 可信启动包括:在设备的系统启动过程中,设备的TPM记录设备的关键系统状态,在设备的系统启动完成后,设备向远程服务器发送报告,进行远程证明和认证,由使用者根据远程证明和认证的结果来确定整个系统环境的状态是否可信。在本申请的一些实施例中,设备的远程证明功能模块向远程服务器发送报告,进行远程证明和认证。在本申请的一些实施例中,网络管理系统或网络控制器可以基于预先配置或通过某种方式获取的策略,根据远程证明和认证的结果来确定整个系统环境的状态是否可信,比如,对于是否允许设备接入、是否允许设备承载某业务等,都可以由所述网络管理系统或网络控制器基于预先配置或获得去的策略以及远程证明和认证的结果来确定。

[0078] 如图3所示,可结合使用启动文件校验和启动文件度量,如果文件校验失败则停止启动,而文件度量只记录对启动过程或启动过程相关信息的度量值而不干涉启动。如图3所示,启动文件校验时,系统固件(firmware)初始化整个硬件系统,并对下一阶段要运行的系统载入程序(loader)进行检查,即,对下一阶段要运行的系统载入程序(loader)进行HASH签名对比。如果系统载入程序未通过检查,则停止启动系统载入程序。如果系统载入程序通过检查,则启动系统载入程序,并由系统载入程序对下一阶段要运行的系统核心程序(kernal)进行检查。如果系统核心程序未通过检查,则停止启动系统核心程序。如果系统核心程序通过检查,则启动系统核心程序。如图3所示,启动文件度量时,也会对系统载入程序及系统核心程序进行检查,但该检查并不干涉系统载入程序及系统核心程序的启动,只将启动过程或启动过程相关信息的度量值记录在TPM中。

[0079] 进一步地,如图4所示,远程证明服务器可以通过网络收集网络设备或节点通过一定格式和交互流程发送的网络设备或节点的安全属性,然后通过挑战-响应的交互机制安全发送给远程证明服务器,并按照一定策略进行验证,最终证明设备的是否可信。另外,为了保证整个远程证明协议交互过程中设备和通信的安全性,包括证书申请和吊销等证书机制必须预先部署好,以支持协议交互过程中的证书的校验和查看等必要操作。所述网络设备或节点可以是服务器、物联网(internet of things,IoT)网关或终端。所述网络设备或节点的安全属性包括软硬件完整性值、配置信息、节点状态等。所述网络设备或节点可以从中央处理器(central processing unit,CPU)&TPM、到BIOS,再到Grub,再到系统核心程序(kernal),最后到应用程序(application,App)的信任链进行完整性值的计算和记录。如图4所示,在终端、网关、云终端可以实现可信移动、远程证明、端到端的保证设备层、通信层、管理层的可信执行环境。

[0080] 其中,上述远程证明过程中,采集数据的方式是通过挑战-响应的交互机制来实现。该种方式中,需要远程证明服务器先向网络设备发送请求,网络设备再将自身安全属性等数据反馈给远程证明服务器。因此,该种数据采集方式不够灵活,且及时性不高,导致具有一定的安全风险。此外,由于需要服务器发起请求,因而具有额外的消息交互,导致效率不高。

[0081] 对此,本申请实施例提供了一种应用于远程证明过程中的采集数据的方法,该方法以基于网络配置协议(network configuration protocol,NETCONF)的订阅/发布和推送机制实现数据采集为例。其中,NETCONF是一种应用在网络配置管理工具中的网络配置协议,它提供了一个对网络设备的配置文件进行安装、查询、读写以及删除操作的机制,相对于命令行界面)(command-line interface,CLI)和简单网络管理协议(simple network management protocol,SNMP),NETCONF在灵活性和可扩展性上更有优势。此外,NETCONF通过可扩展标记语言(extensible markup language,XML)数据格式,基于远程过程调用(remote procedure call,RPC)层之上,提供网络设备配置的安装、操作、删除机制。

[0082] NETCONF协议分成如下四层:

[0083] 内容层:表示的是被管对象的集合。

[0084] 操作层:定义了一系列在RPC中应用的基本的原语操作集,这些操作将组成NETCONF的基本能力。

[0085] RPC层:为RPC模块的编码提供了一个简单的、传输协议无关的机制。

[0086] 通信协议层:与SNMP使用无连接的用户数据报协议(user datagram protocol,UDP)作为传输协议不同,NETCONF是面向连接的,它要求通信端口之间永久性的连接,而且这种连接必须提供可靠的,顺序的数据传输。目前支持安全壳协议(secure shell,SSH),安全传输层协议(transport layer security,TLS)等。

[0087] 此外,本申请实施例提供的方法采用Yang push提供了一种标准的机制,使得可以订阅系统内以Yang模型描述的任何数据。指定要订阅的路径和订阅模式后,当选择周期性反馈的订阅模式时,系统会在指定的时间周期到达之后,将指定的数据推送给订阅用户。当选择on change模式(即事件触发反馈的订阅模式)时,系统会在订阅的数据发生改变时就将这些数据推送给订阅用户。

[0088] 接下来,对本申请实施例提供的采集数据的方法进行举例说明。如图5所示,该方法包括如下几个步骤。

[0089] 在步骤501中,远程证明服务器向网络设备下发订阅配置,订阅配置用于订阅网络设备进行远程证明的相关信息。

[0090] 本申请采用订阅的方式,由远程证明服务器向网络设备下发订阅配置,从而订阅网络设备进行远程证明的相关信息。可选地,订阅配置包括数据流的订阅配置和事件的订阅配置中的一种或多种。例如,远程证明服务器向网络设备下发数据流的订阅配置,从而订阅网络设备进行远程证明的数据流的相关信息。或者,远程证明服务器向网络设备下发事件的订阅配置,从而订阅网络设备进行远程证明的事件的相关信息。又或者,远程证明服务器向网络设备下发数据流的订阅配置和事件的订阅配置,从而订阅网络设备进行远程证明的数据流和事件的相关信息。远程证明服务器向网络设备下发数据流的订阅配置和事件的订阅配置时,可以同时下发,也可以不同时下发,本申请实施例对此不加以限定。

[0091] 其中,数据流的相关信息可以是网络设备可信相关的各类信息,包括但不限于以下信息中的一种或多种:网络设备启动时记录的信任链的各层的软件的完整性信息,网络设备运行时记录的操作系统动态完整性信息,网络设备运行时记录的软件的动态完整性信息,网络设备相关的身份证书和网络设备相关的远程证明证书。

[0092] 事件包括但不限于设备启动、设备升级、特定模式攻击事件、主备切换、单板插拔/切换、证书生命周期事件中的一种或多种事件。其中,单板切换事件包括业务所在单板进行切换的事件。远程证明服务器订阅哪种数据流以及哪种事件可以依据应用场景来定,本申请实施例对此不加以限定。

[0093] 可选地,订阅配置还可以包括订阅模式,该订阅模式用于指示反馈订阅信息的方式,该订阅模式包括周期性反馈和事件触发反馈中的一种或组合。可选地,不同类型的信息对应不同的订阅模式。例如,对于一些关键安全数据流,可以配置事件触发反馈的订阅模式,从而在订阅的数据发生改变时,立即由网络设备反馈至远程证明服务器。而对于一般安全数据,可以配置周期性反馈的订阅模式,从而在达到周期后,由网络设备反馈至远程证明服务器。当然,还可以采用其他策略来确定订阅模式,例如依据应用场景确定订阅模式等,本申请实施例对此不加以限定。

[0094] 可选地,订阅配置还可以包括过滤器的配置。过滤器的配置用于对数据流或事件的相关信息进行过滤。应当理解的是,数据流及事件的订阅配置是一个较宽范围的信息订阅,而过滤器可以理解为一种限制条件,即在较宽范围的信息中筛选出更为细化的信息,从而使得采集的数据更具针对性。

[0095] 在本申请实施例的可选实施方式中,无论订阅配置是对哪些内容进行订阅的配置,为了将订阅配置下发至网络设备,远程证明服务器向网络设备下发订阅配置的方式,包括但不限于以下方式中的一种或多种:与网络设备建立网络配置协议会话,基于网络配置协议会话向网络设备下发订阅配置。

[0096] 可选地,本申请实施例提供的方法还可以将订阅配置的时效与网络配置协议会话的时效绑定。订阅配置基于网络配置协议会话下发之后,后续依赖于网络配置协议会话,即可以实现动态订阅。也就是说,在网络配置协议会话有效的情况下,可以基于该订阅配置继续订阅。一旦网络配置协议会话断开,则该订阅配置时效,无法再基于该订阅配置继续订阅,从而可以动态的监控网络设备的状态。该种方式下,可以定义相应的动态订阅RPC,减少额外信息交互。

[0097] 当然,还可以将订阅配置的时效与网络配置协议会话的时效不绑定。订阅配置基于网络配置协议会话下发后,后续不依赖于网络配置协议会话,即实现配置订阅。也就是说,无论网络配置协议会话是否断开,基于该订阅配置仍然可以继续订阅,可以始终监控网络设备的状态。

[0098] 订阅配置的时效与网络配置协议会话的时效是否绑定可以基于采集数据的类型来确定,例如,对于一些关键安全数据,可以采用二者不绑定的方式,利用on-change模式始终监控。对于一般安全数据,可以采用二者绑定的方式,在开启NETCONF会话期间周期性读取相关信息。

[0099] 在步骤502中,网络设备接收远程证明服务器下发的订阅配置。

[0100] 可选地,若网络设备与远程证明服务器建立了网络配置协议会话,在远程证明服

务器基于网络配置协议会话下发订阅配置之后,网络设备基于网络配置协议会话接收远程证明服务器下发的订阅配置。

[0101] 在步骤503中,网络设备基于订阅配置向远程证明服务器反馈订阅信息。

[0102] 网络设备接收到远程证明服务器下发的订阅配置后,可基于订阅配置获取需要向远程证明服务器反馈的订阅信息。

[0103] 可选地,若订阅配置包括数据流的订阅配置,基于订阅配置向远程证明服务器反馈订阅信息,包括:基于数据流的订阅配置向远程服务器反馈以下信息中的一种或多种:网络设备启动时记录的信任链的各层的软件的完整性信息,网络设备运行时记录的操作系统动态完整性信息,网络设备运行时记录的软件的动态完整性信息,网络设备相关的身份证书和网络设备相关的远程证明证书。具体反馈哪种订阅信息,可根据订阅配置中的订阅要求来确定。例如,若订阅配置要求订阅网络设备启动时记录的信任链的各层的软件的完整性信息,则网络设备基于订阅配置将启动时记录的信任链的各层的软件的完整性信息作为订阅信息反馈至远程证明服务器。

[0104] 可选地,若订阅配置包括事件的订阅配置,基于订阅配置向远程证明服务器反馈订阅信息,包括:基于事件的订阅配置向远程服务器反馈设备启动、设备升级、特定模式攻击事件、主备切换、单板插拔/切换、证书生命周期事件中的一种或多种事件触发后的相关信息。具体反馈哪种订阅信息,可根据订阅配置中的订阅要求来确定。例如,若订阅配置要求订阅设备启动的相关信息,则网络设备基于订阅配置在网络设备启动完成后,将网络设备启动完成后的信息作为订阅信息反馈至远程证明服务器。

[0105] 可选地,若订阅配置还包括订阅模式,订阅模式用于指示反馈订阅信息的方式,该订阅模式包括周期性反馈或事件触发反馈或周期性反馈和事件触发反馈的组合。可选地,不同类型的信息对应不同的反馈订阅信息的方式;则网络设备基于订阅配置中包括的订阅模式,向远程证明服务器反馈订阅信息。具体采用哪种订阅模式反馈订阅信息,可基于订阅配置中的订阅要求来确定。例如,若订阅配置要求的订阅模式为周期性反馈,则网络设备在达到周期后,将获取的订阅信息反馈至远程证明服务器。

[0106] 若订阅配置还包括过滤器的配置,则网络设备在采集订阅配置中订阅的数据流和事件的信息后,基于过滤器的配置对采集的信息进行过滤,之后得到满足订阅需求的订阅信息。

[0107] 在步骤504中,远程证明服务器接收网络设备基于订阅配置反馈的订阅信息。

[0108] 远程证明服务器接收网络设备反馈的订阅信息后,完成数据采集,可基于该订阅信息进行远程证明。例如,按照一定策略进行验证,最终证明网络设备是否可信。由此可见,远程证明可以动态监控网络设备的安全属性,防止网络设备被篡改、替换、复制等。

[0109] 本申请实施例通过远程证明服务器向网络设备下发订阅配置,网络设备可据此自动反馈订阅信息,使得远程证明中的数据采集方式更为灵活,及时性较高,进而降低安全风险。此外,由于订阅配置无需远程证明服务器多次下发,因而减少了额外的消息交互,进而提高了数据采集效率。

[0110] 进一步地,本申请实施例提供的方法还包括:远程证明服务器向网络设备下发数据处理参数,网络设备接收远程证明服务器下发的数据处理参数。在此基础上,网络设备向远程证明服务器反馈的订阅信息为基于数据处理参数处理之后得到的信息。通过该种方

式,远程证明服务器将nonce、hash签名算法、指定TPM名称等数据处理参数提前发送至网络设备,以备后续使用。

[0111] 例如,如果为了获取tpm的PCR值,数据处理参数包括Nonce、PCR-list数组、完整消息的签名算法标识和可使用的公钥编号(public-key-identifier)。其中,各个参数的内容:

[0112] Nonce:每次不同即可,使用时间戳或者计数增加均可。远程证明服务器和网络设备可基于Nonce来确认收到的消息的时效性和非重复性。除了采用Nonce来确认消息的时效性和非重复性之外,在本申请的一些实施例中,远程证明服务器也可以发送一个种子和一个持续计算的hash算法标识,由网络设备及远程证明服务器同步运算,从而共同确认收到的远程证明消息的时效性和非重复性;或者,也可以使用基于时间的单向认证(time-based uni-directional attestation,RATS TUDA)机制,实现Nonce类似的功能。RATS TUDA机制本质上是一个单向的远程证明协议,即:attester(网络设备)单向给verifier(远程证明服务器)发送其完整性证据,verifier完成验证功能。它主要通过引入一个信任的第三方:可信的时间戳颁发机构(a trusted time stamp authority,TSA)。在verifier利用收到的远程证明消息中携带的attester的时间戳信息,以及TSA提供的时间戳令牌(time stamp token,TST),共同确认收到的远程证明消息的时效性和非重复性。

[0113] PCR-list数组:包括多个PCR信息,PCR信息包括PCR寄存器编号,以及其使用的特定的签名算法。例如:数字签名算法(digital signature algorithm,DSA)、椭圆曲线数字签名算法(elliptic curve digital signature algorithm,ECDSA)或爱德华兹曲线数字签名算法(edwards-curve digital signature algorithm,EDDSA)等;

[0114] 完整消息的签名算法:包括DSA、ECDSA或EDDSA等。本申请实施例中,该参数为一组可选的签名算法,attester可自主随机选择,并在返回的消息中指明选择了哪种签名算法;

[0115] 可使用的公钥编号(public-key-identifier):指定应该使用哪一个公钥/私钥对进行签名和验证;本申请实施例中,该参数为一组可选的公钥编号。attester可自主随机选择,并在返回的消息中指明选择了哪个公钥;

[0116] 目标TPM名称/编号:一组TPM名称,attester可以根据一些策略做决策,例如,1)选择哪个TPM进行收集,2)哪个TPM的PCR值发生变化了,就发送;3)按一定顺序依次发送每个TPM的PCR值等。

[0117] 又例如,如果Verifier为了获取attester(网络设备)上存储的管理日志(stored management log,SML)的PCR值,发送的数据处理参数包括节点名称、SML中日志记录选择方式、日志类型和PCR-list数值。其中,各个参数的内容如下:

[0118] 节点名称:本申请实施例中,该参数为一组节点名称。Verifier将节点名称下发给attester后,attester可以根据一些策略做决策,例如:1)attester选择哪个节点进行收集,2)哪个节点的SML日志文件发生变化了,就发送;3)按一定顺序依次发送每个节点的SML全部/更新值等;

[0119] SML中日志记录选择方式:上次取完后的下一个/指定编号/指定时间的。Verifier将SML中日志记录选择方式下发给attester后,attester可自主随机选择,并在返回的消息中指明选择了哪种选择方式;

[0120] 日志类型:bios或者完整性度量结构(integrity measurement architecture,

IMA)。

[0121] PCR-list数组:由多个PCR信息组成,PCR信息包括PCR寄存器编号,以及其使用的特定的签名算法。例如:DSA、ECDSA或EDDSA等。

[0122] 应当理解,上述两个数据处理参数的实例只是本申请实施例所提供的方法的示例性实施例,根据应用场景不同,还可以下发其他类型或其他内容的数据处理参数,本申请实施例对此不加以限定。无论针对哪种数据处理参数,网络设备在获取到用于进行远程证明的相关信息后,可基于该数据处理参数对获取到的信息进行处理,之后再将处理后的信息反馈至远程证明服务器。例如,基于数据处理参数中的加密算法对获取到的信息进行加密。

[0123] 综上所述,本申请实施例通过使用netconf的pub/sub和push机制,不仅在现有固定网络中有广泛使用场景,且还继承了其灵活、高效、主动通知、确保时效性等优点;并且,通过网络设备主动反馈订阅信息,实现了设备侧事件触发的远程证明的机制;另外,通过nonce的随机性和同步性,使得信息可在本申请实施例提供的交互机制中使用。

[0124] 为了便于理解,接下来以如下两个实例进行举例说明。

[0125] (一)针对配置订阅远程证明事件

[0126] 1、以订阅配置包括数据流的订阅配置、事件的订阅配置、过滤器的订阅配置和订阅模式,远程证明服务器还下发了数据处理参数为例,各个内容如下:

[0127] 数据流的订阅配置内容包括:

[0128] 数据流:pcr-trust-evidence(PCR信任证据);

[0129] bios-log-trust-evidence(BIOS日志信任证据);

[0130] ima-log-trust-evidence(IMA日志信任证据)。

[0131] 事件的订阅配置内容包括:

[0132] 事件名:1001;

[0133] 事件类型:设备启动完成。

[0134] 数据流的数据处理参数包括:

[0135] 远程证明类型:tpm2-attestation-challenge;

[0136] pcr库:aaa;

[0137] pcr-indices:6;

[0138] 哈希算法id:14;nonce-value:0x564ac291;

[0139] signature-identifer-type使用TPM_ALG-ID:2;

[0140] Key-id使用价格public-key:0x784a22bf。

[0141] 过滤器的订阅设置包括:

[0142] 某厂家设备yang模型:xxx-vendor-device;

[0143] 某设备的设备id:030DLA106C0522221111。

[0144] 订阅模式包括:

[0145] 周期性反馈:periodic;

[0146] 订阅周期为:500;

[0147] 推送安全数据流为:1001(与事件的订阅配置中设备启动事件id相同)。基于上述订阅配置,配置信息如下:

```
<rpcnetconf:message-id="101"
  xmlns:netconf="urn:ietf:params:xml:ns:netconf:base:1.0">
 <edit-config>
  <streams>
   <stream>
    <name>pcr-trust-evidence</name>
   </stream>
   <stream>
    <name>bios-log-trust-evidence</name>
   </stream>
```

[0148]

```
   <stream>
    <name>ima-log-trust-evidence</name>
   </stream>
  </streams>
  <subscriptions
    xmlns="urn:ietf:params:xml:ns:yang:ietf-subscribed-notifications">
   <events>
    <event>
     <name>1001</name>
     <type>device-startup-ok</type>
    </event>
```

[0149]

```
</events>
<subscription>
  <subscription-id>100</subscription-id>
  <rats-type>
   <tpm2-attestation-challenge>
    <pcr-list>
     <id>aaa</id>
     <pcr-indices>6</pcr-indices>
     <algo-registry-type>
      <ietf-ni-hash-algo-id>14</ietf-ni-hash-algo-id>
     </algo-registry-type>
    </pcr-list>
    <nonce-value>0x564ac291</nonce-value>
    <signature-identifer-typ>
     <TPM_ALG-ID>2</TPM_ALG-ID>
    </signature-identifer-typ>
    <key-identifier>
     <public-key>0x784a22bf</public-key>
      </key-identifier>
    </tpm2-attestation-challenge>
  </rats-type>
  <stream-subtree-filter>
      <xxx-vendor-device
       xmlns="urn:xxx:params:xml:ns:yang:xxx-vendor-device ">
      <device-id>030DLA106C0522221111</device-id>
     </xxx-vendor-device>
  </stream-subtree-filter>
  <periodic xmlns="urn:ietf:params:xml:ns:yang:ietf-yang-push:1.0">
     <sub-rats-event xmlns="urn:ietf:params:xml:ns:yang:ietf-rats-sub-push:1.0">
      1001</sub-rats-event>
     <period>500</period>
  </periodic>
 </subscription>
</subscriptions>
</edit-config>
</rpc>
```

[0150] 定义yang数据模型,描述订阅数据流类型,订阅事件类型,实现配置订阅。相关配置订阅数据模型树形结构如图6所示,树形结构撰写例依据IETF RFC8340。

[0151] 对于下层的传输协议NETCONF而言,远程证明服务器为NETCONF客户端(NETCONF client),而网络设备为NETCONF服务端(NETCONF server)。如图7所示,NETCONF client(远程证明服务器)与NETCONF server(网络设备)首先建立netconf session,并通过上述yang数据模型将所关注的远程证明的订阅配置下发给NETCONF server。NETCONF server通过定期发送notification(通知),周期性的将相关数据即订阅信息推送给NETCONF client。配置订阅不依赖于netconf session,session down(会话断开)后配置订阅仍然存在,NETCONF server依旧向NETCONF client定期发送notification。

[0152] 2、以订阅配置包括数据流的订阅配置、事件的订阅配置、过滤器的订阅配置和订阅模式,远程证明服务器还下发了数据处理参数为例,各个内容如下:

[0153] 数据流的订阅配置内容包括:数据流:pcr-trust-evidence(PCR信任证据),bios-log-trust-evidence(BIOS日志信任证据)和ima-log-trust-evidence(IMA日志信任证据)。

[0154] 事件的订阅配置内容包括:

[0155] 事件名:1002;

[0156] 事件类型:设备主备切换。

[0157] 数据流的数据处理参数包括:

[0158] 远程证明类型:log-retrieval;

[0159] log-selector配置:node-name:aaa;

[0160] node-physical-index:77;

[0161] index-type选择为last-entry-value:010101;

[0162] log-type为bios;pcr库:aaa;pcr-indices:7;

[0163] 哈希算法id:14;log-entry-quantity:69。

[0164] 过滤器的订阅设置包括:

[0165] 某厂家设备yang模型:xxx-vendor-device;

[0166] 某设备的设备id:xxxx。

[0167] 订阅模式包括:

[0168] on-change上报:on-change;

[0169] 推送安全数据流为:1002(与设备主备切换事件id相同)。

[0170] 基于上述订阅配置,配置信息如下:

```
<rpcnetconf:message-id="101"
  xmlns:netconf="urn:ietf:params:xml:ns:netconf:base:1.0">
  <edit-config>
  <streams>
   <stream>
    <name>pcr-trust-evidence</name>
   </stream>
```

[0171]

```
  <stream>
    <name>bios-log-trust-evidence</name>
  </stream>
  <stream>
    <name>ima-log-trust-evidence</name>
  </stream>
  </streams>
  <subscriptions
```

```
xmlns="urn:ietf:params:xml:ns:yang:ietf-subscribed-notifications">
<events>
 <event>
  <name>1002</name>
    <type>master-slave-swithover</type>
 </event>
</events>
<subscription>
  <subscription-id>100</subscription-id>
 <rats-type>
  <log-retrieval>
    <log-selector>
    <node-name>linkcard-2</node-name>
    <node-physical-index>77</node-physical-index>
     <index-type>
     <last-entry-value>67</last-entry-value>
     <index-type>
     </log-selector>
      <log-type>bios</log-type>
      <pcr-list>
[0172]  <id>aaa</id>
      <pcr-indices>7</pcr-indices>
      <algo-registry-type>
      <ietf-ni-hash-algo-id>5</ietf-ni-hash-algo-id>
      </algo-registry-type>
      </pcr-list>
     <log-entry-quantity>69</log-entry-quantity>
  </log-retrieval>
 </rats-type>

<stream-subtree-filter>
  <xxx-vendor-device
        xmlns="urn:xxx:params:xml:ns:yang:xxx-vendor-device ">
    <device-id>030DLA106C0522221111</device-id>
 </xxx-vendor-device>
</stream-subtree-filter>
<on-change xmlns="urn:ietf:params:xml:ns:yang:ietf-yang-push:1.0">
  <sub-rats-event xmlns="urn:ietf:params:xml:ns:yang:ietf-rats-sub-push:1.0">
    1001</sub-rats-event>
</on-change>
</subscription>
```

```
        </subscriptions>
      </edit-config>
    </rpc>
```

[0174] 如图8所示,NETCONF client与NETCONF server建立netconf session,并通过上述yang数据模型将所关注的远程证明的订阅配置下发给NETCONF server。当订阅的关键数据发生改变时,NETCONF Server发送notification将相关数据即订阅信息推送给NETCONF client。配置订阅可以不依赖于netconf session,session down后配置订阅仍然存在,NETCONF server依旧向client定期发送notification。

[0175] 当订阅事件触发时,NETCONF server向NETCONF client发送如下格式的notification。相关动态订阅数据模型树形结构如图9所示,树形结构撰写例依据IETF RFC8340。

[0176] (二)针对动态订阅远程证明事件

[0177] 1、以订阅配置包括数据流的订阅配置、过滤器的订阅配置和订阅模式为例,各个内容如下:

[0178] 数据流的订阅配置内容包括:

[0179] 远程证明类型为:tpm2-attestation-challenge;

[0180] pcr库:aaa;pcr-indices:7;

[0181] 哈希算法id:5;

[0182] nonce-value:0xa45668b1;

[0183] signature-identifer-type使用TPM_ALG-ID:2;

[0184] Key-id使用价格public-key:0xad3567c3。

[0185] 过滤器的订阅配置内容包括:

[0186] 某厂家设备yang模型:xxx-vendor-device;

[0187] 某设备的设备id:xxxx。

[0188] 订阅模式包括:

[0189] 周期性上报:periodic;

[0190] 订阅周期为:500;

[0191] 推送安全数据流为:1001(与设备启动事件id相同)。

[0192] 基于上述订阅配置,配置信息如下:

```
<rpcnetconf:message-id="101"
 xmlns:netconf="urn:ietf:params:xml:ns:netconf:base:1.0">
  <establish-subscription
  xmlns="urn:ietf:params:xml:ns:yang:ietf-subscribed-notifications">
  <rats-type>
  <tpm2-attestation-challenge>
```

[0193]

```
                <pcr-list>
            <id>aaa</id>
                <pcr-indices>7</pcr-indices>
                <algo-registry-type>
                <ietf-ni-hash-algo-id>5</ietf-ni-hash-algo-id>
              </algo-registry-type>
              </pcr-list>
              <nonce-value>0xa45668b1</nonce-value>
              <signature-identifer-typ>
               <TPM_ALG-ID>2</TPM_ALG-ID>
               </signature-identifer-typ>
              <key-identifier>
                <public-key>0xad3567c3</public-key>
              </key-identifier>
             </tpm2-attestation-challenge>
              </rats-type>
```

[0194]

```
                <stream-subtree-filter>
                    <xxx-vendor-device xmlns="urn:xxx:params:xml:ns:yang:xxx-vendor-device ">
                    device-id>xxxxx</device-id>
                    </xxx-vendor-device>
              </stream-subtree-filter>
              <periodic xmlns="urn:ietf:params:xml:ns:yang:ietf-yang-push:1.0">
              <sub-rats-event xmlns="urn:ietf:params:xml:ns:yang:ietf-rats-sub-push:1.0">1001</sub-rats-event>
              <period>500</period>
            </periodic>
      </establish-subscription>
</rpc>
```

[0195] 定义yang数据模型,描述订阅数据流类型,订阅事件类型,实现动态订阅。相关动态订阅数据模型树形结构如图10所示,树形结构撰写例依据IETF RFC8340。

[0196] 动态订阅由NETCONF client在netconf session开启时向NETCONF server发送订阅RPC,NETCONF server在netconf session存在的时间段内向NETCONF client周期性或者on-change式的推送所订阅的订阅信息。例如,如图11所示。NETCONF client与NETCONF

server建立netconf session,并通过上述RPC将自己所关注的远程证明的订阅配置下发给NETCONF server。NETCONF server通过定期发送notification,周期性的将相关数据即订阅信息推送给NETCONF client。动态订阅依赖于netconf session,session down订阅消失。

[0197] 2、以订阅配置包括数据流的订阅配置、事件的订阅配置、过滤器的订阅配置和订阅模式为例,各个内容如下:

[0198] 数据流的订阅配置内容包括:

[0199] 远程证明类型为:log-retrieval;

[0200] log-selector配置:node-name:linecard-2;

[0201] node-physical-index:77;

[0202] index-type选择为last-entry-value:28;

[0203] log-type为bios;pcr库:aaa;pcr-indices:7;

[0204] 哈希算法id:5;

[0205] log-entry-quantity:69。

[0206] 事件的订阅配置内容包括:

[0207] 事件名:1008;

[0208] 事件类型:设备更新。

[0209] 过滤器的订阅配置内容包括:

[0210] 某厂家设备yang模型:xxx-vendor-device;

[0211] 某设备的设备id:xxxx。

[0212] 订阅模式包括:

[0213] on-change上报:on-change;

[0214] 推送安全数据流为:1008(与设备更新事件id相同)。基于上述订阅配置,配置信息如下:

[0215]

```
<rpcnetconf:message-id="101"
  xmlns:netconf="urn:ietf:params:xml:ns:netconf:base:1.0">
    <establish-subscription
      xmlns="urn:ietf:params:xml:ns:yang:ietf-subscribed-notifications">
     <rats-type>
      <log-retrieval>
      <log-selector>
       <node-name>aaa</node-name>
       <node-physical-index>77</node-physical-index>
       <index-type>
         <last-entry-value>010101</last-entry-value>
         <index-type>
      </log-selector>
      <log-type>bios</log-type>
            <pcr-list>
            <id>aaa</id>
            <pcr-indices>73</pcr-indices>
            <algo-registry-type>
            <ietf-ni-hash-algo-id>14</ietf-ni-hash-algo-id>
            </algo-registry-type>
            </pcr-list>
            <log-entry-quantity>69</log-entry-quantity>
        </log-retrieval>
       </rats-type>
      <stream-subtree-filter>
       <xxx-vendor-device xmlns="urn:xxx:params:xml:ns:yang:xxx-vendor-device ">
       device-id>xxxxx</device-id>
       </xxx-vendor-device>
       </stream-subtree-filter>
     <on-change xmlns="urn:ietf:params:xml:ns:yang:ietf-yang-push:1.0">
     <sub-rats-event xmlns="urn:ietf:params:xml:ns:yang:ietf-rats-sub-push:1.0">1008</sub-rats-event>
     </on-change>
     </establish-subscription>
</rpc>
```

[0216]

[0217] 如图12所示,NETCONF client与NETCONF server首先建立netconf session,并通过上述RPC将所关注的远程证明的订阅配置下发给NETCONF server。当订阅的关键数据发生改变时,NETCONF Server发送notification将相关数据即订阅信息推送给NETCONF client。动态订阅依赖于netconf session,session down订阅消失。

[0218] 当订阅事件触发时,NETCONF server向NETCONF client发送如下格式的

notification。相关动态订阅数据模型树形结构如图13所示,树形结构撰写例依据国际标准RFC8340。

[0219] 综上所示,本申请实施例提供的方法使用了最新的netconf/表述性状态转移配置协议(representational state transfer configuration protocol,RESCONF)pub(发布)/sub(订阅)和push(推送)机制,在现有固定网络中有广泛使用场景。应当理解的是,该机制可以非常容易地转换成其他协议和消息编码格式,如:RESCONF+JS对象简谱(javascript object notation,JSON)/可扩展标记语言(extensible markup language,XML),受限应用协议(constrained application protocol,CoAP)+简明二进制对象展现(concise binary object representation,CBOR),从而可以很容易地移植到web(互联网)、IoT、移动设备等场景中。其他协议的数据采集方式与NETCONF的原理相同,此处不再一一赘述。

[0220] 基于相同技术构思,本申请实施例还提供了一种数据采集装置,该装置应用于远程证明的过程中,参见图14,该装置包括:

[0221] 发送模块141,用于向网络设备下发订阅配置,订阅配置用于订阅网络设备进行远程证明的相关信息;

[0222] 接收模块142,用于接收网络设备基于订阅配置反馈的订阅信息。

[0223] 可选地,发送模块141,还用于向网络设备下发数据处理参数,订阅信息包括基于数据处理参数处理之后得到的信息。

[0224] 可选地,发送模块141,用于与网络设备建立网络配置协议会话,基于网络配置协议会话向网络设备下发订阅配置。

[0225] 基于相同技术构思,本申请实施例还一种数据采集装置,该装置应用于远程证明的过程中,参见图15,该装置包括:

[0226] 接收模块151,用于接收远程证明服务器下发的订阅配置,订阅配置用于订阅网络设备进行远程证明的相关信息;

[0227] 发送模块152,用于基于订阅配置向远程证明服务器反馈订阅信息。

[0228] 可选地,若订阅配置包括数据流的订阅配置,发送模块152,用于基于数据流的订阅配置向远程服务器反馈以下信息中的一种或多种:

[0229] 网络设备启动时记录的信任链的各层的软件的完整性信息,

[0230] 网络设备运行时记录的操作系统动态完整性信息,

[0231] 网络设备运行时记录的软件的动态完整性信息,

[0232] 网络设备相关的身份证书,和

[0233] 网络设备相关的远程证明证书。

[0234] 可选地,若订阅配置包括事件的订阅配置,发送模块152,用于基于事件的订阅配置向远程服务器反馈设备启动、设备升级、特定模式攻击事件、主备切换、单板插拔/切换、证书生命周期事件中的一种或多种事件触发后的相关信息。

[0235] 可选地,订阅配置还包括订阅模式,订阅模式用于指示反馈订阅信息的方式,订阅模式包括周期性反馈和事件触发反馈中的一种或组合;

[0236] 发送模块152,用于基于订阅配置中包括的订阅模式,向远程证明服务器反馈订阅信息。

[0237] 可选地,接收模块151,还用于接收远程证明服务器下发的数据处理参数,发送模块反馈的订阅信息包括基于数据处理参数处理之后得到的信息。

[0238] 可选地,接收模块151,用于与远程证明服务器建立网络配置协议会话,基于网络配置协议会话接收远程证明服务器下发的订阅配置。

[0239] 应理解的是,上述提供的装置在实现其功能时,仅以上述各功能模块的划分进行举例说明,实际应用中,可以根据需要而将上述功能分配由不同的功能模块完成,即将设备的内部结构划分成不同的功能模块,以完成以上描述的全部或者部分功能。另外,上述实施例提供的装置与方法实施例属于同一构思,其具体实现过程详见方法实施例,这里不再赘述。

[0240] 基于相同构思,本申请实施例还提供了一种采集数据的设备,参见图16,该设备包括存储161及处理器162;存储器161中存储有至少一条指令,至少一条指令由处理器162加载并执行,以实现本申请实施例提供的上述任一种采集数据的方法。

[0241] 本申请实施例还提供了一种通信装置,参见图17,该装置包括:收发器171、存储器172和处理器173。其中,该收发器171、该存储器172和该处理器173通过内部连接通路互相通信,该存储器172用于存储指令,该处理器173用于执行该存储器存储的指令,以控制收发器171接收信号,并控制收发器171发送信号,并且当该处理器173执行该存储器172存储的指令时,使得该处理器173执行上述任一种采集数据的方法。

[0242] 本申请实施例还提供了一种通信系统,该系统包括上述图14所示的装置,以及上述图15所示的装置。

[0243] 本申请的采集数据的设备可以是个人电脑(personal computer,PC)或服务器或网络设备。例如,采集数据的设备可以是路由器、交换机、服务器等。

[0244] 基于相同构思,本申请实施例还提供了一种计算机可读存储介质,存储介质中存储有至少一条指令,指令由处理器加载并执行以实现本申请实施例提供的上述任一种采集数据的方法。

[0245] 本申请实施例还提供了一种芯片,包括处理器,处理器用于从存储器中调用并运行存储器中存储的指令,使得安装有芯片的通信设备执行上述任一种的采集数据的方法。

[0246] 本申请实施例还提供了一种芯片,包括:输入接口、输出接口、处理器和存储器,输入接口、输出接口、处理器以及存储器之间通过内部连接通路相连,处理器用于执行存储器中的代码,当代码被执行时,处理器用于执行上述任一种的采集数据的方法。

[0247] 应理解的是,上述处理器可以是中央处理器(Central Processing Unit,CPU),还可以是其他通用处理器、数字信号处理器(digital signal processing,DSP)、专用集成电路(application specific integrated circuit,ASIC)、现场可编程门阵列(field-programmable gate array,FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者是任何常规的处理器等。值得说明的是,处理器可以是支持进阶精简指令集机器(advanced RISC machines,ARM)架构的处理器。

[0248] 进一步地,在一种可选的实施例中,上述处理器为一个或多个,存储器为一个或多个。可选地,存储器可以与处理器集成在一起,或者存储器与处理器分离设置。上述存储器可以包括只读存储器和随机存取存储器,并向处理器提供指令和数据。存储器还可以包括非易失性随机存取存储器。例如,存储器还可以存储设备类型的信息。

[0249] 该存储器可以是易失性存储器或非易失性存储器,或可包括易失性和非易失性存储器两者。其中,非易失性存储器可以是只读存储器(read-only memory,ROM)、可编程只读存储器(programmable ROM,PROM)、可擦除可编程只读存储器(erasable PROM,EPROM)、电可擦除可编程只读存储器(electrically EPROM,EEPROM)或闪存。易失性存储器可以是随机存取存储器(random access memory,RAM),其用作外部高速缓存。通过示例性但不是限制性说明,许多形式的RAM可用。例如,静态随机存取存储器(static RAM,SRAM)、动态随机存取存储器(dynamic random access memory,DRAM)、同步动态随机存取存储器(synchronous DRAM,SDRAM)、双倍数据速率同步动态随机存取存储器(double data date SDRAM,DDR SDRAM)、增强型同步动态随机存取存储器(enhanced SDRAM,ESDRAM)、同步连接动态随机存取存储器(synchlink DRAM,SLDRAM)和直接内存总线随机存取存储器(direct rambus RAM,DR RAM)。

[0250] 本申请提供了一种计算机程序,当计算机程序被计算机执行时,可以使得处理器或计算机执行上述方法实施例中对应的各个步骤和/或流程。

[0251] 在上述实施例中,可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时,可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时,全部或部分地产生按照本申请所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中,或者从一个计算机可读存储介质向另一个计算机可读存储介质传输,例如,所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线(例如同轴电缆、光纤、数字用户线)或无线(例如红外、无线、微波等)方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质,(例如,软盘、硬盘、磁带)、光介质(例如,DVD)、或者半导体介质(例如固态硬盘Solid State Disk)等。

[0252] 以上所述仅为本申请的实施例,并不用以限制本申请,凡在本申请的精神和原则之内,所作的任何修改、等同替换、改进等,均应包含在本申请的保护范围之内。

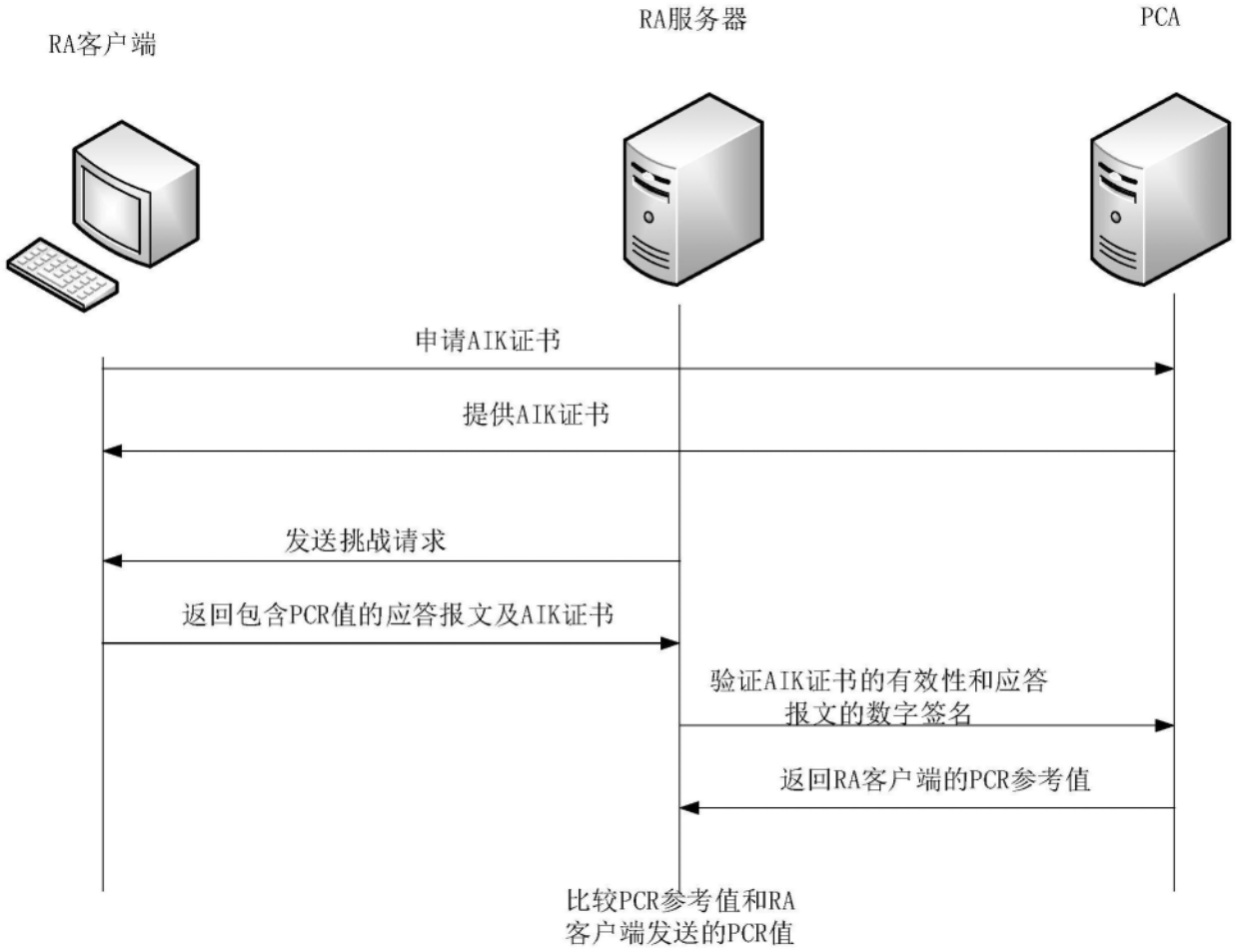

RA客户端
RA服务器
PCA
申请AIK证书
提供AIK证书
发送挑战请求
返回包含PCR值的应答报文及AIK证书
验证AIK证书的有效性和应答报文的数字签名
返回RA客户端的PCR参考值
比较PCR参考值和RA客户端发送的PCR值

图1A

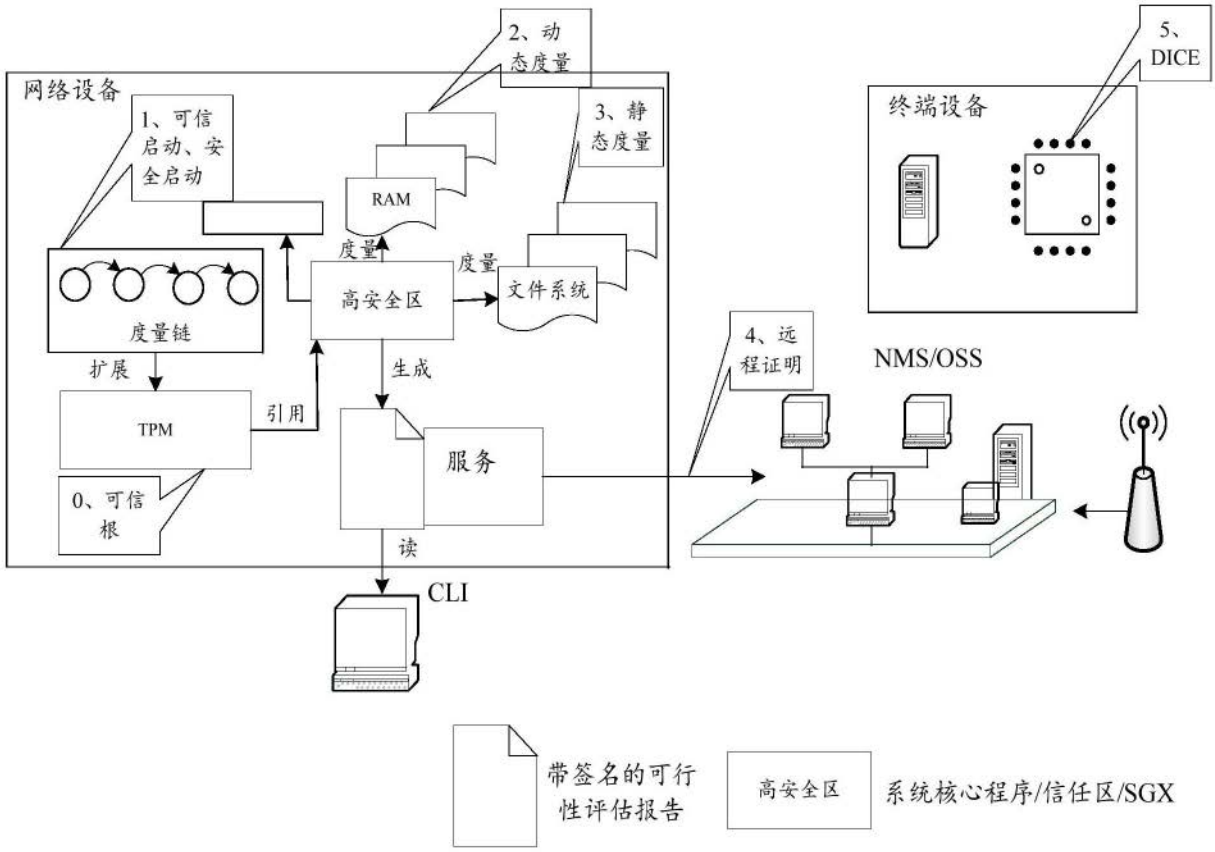

网络设备
1、可信启动、安全启动
2、动态度量
3、静态度量
RAM
度量
度量
高安全区
文件系统
度量链
扩展
TPM
引用
生成
服务
0、可信根
读
CLI
终端设备
5、DICE
4、远程证明
NMS/OSS
带签名的可行性评估报告
高安全区
系统核心程序/信任区/SGX

图1B

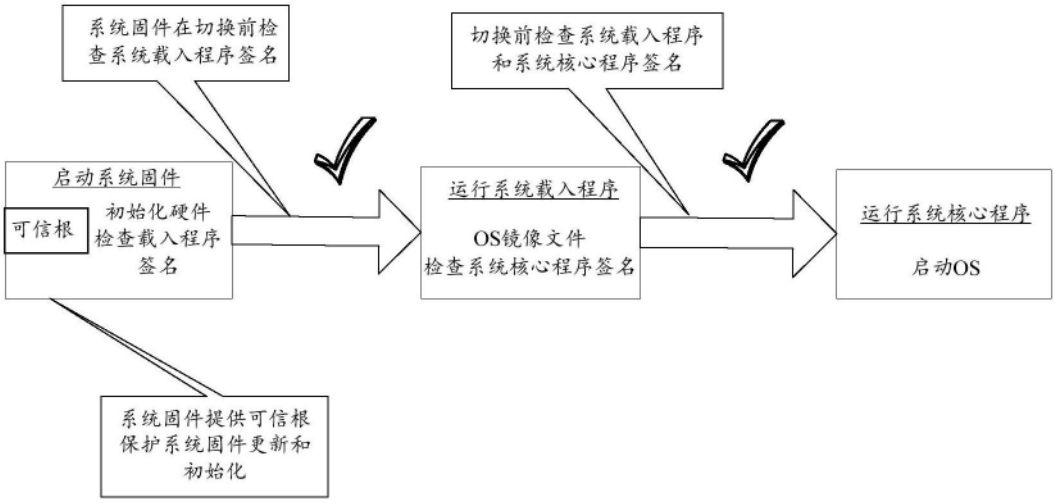

系统固件在切换前检查系统载入程序签名
切换前检查系统载入程序和系统核心程序签名
启动系统固件
可信根
初始化硬件
检查载入程序签名
运行系统载入程序
OS镜像文件
检查系统核心程序签名
运行系统核心程序
启动OS
系统固件提供可信根保护系统固件更新和初始化

图2

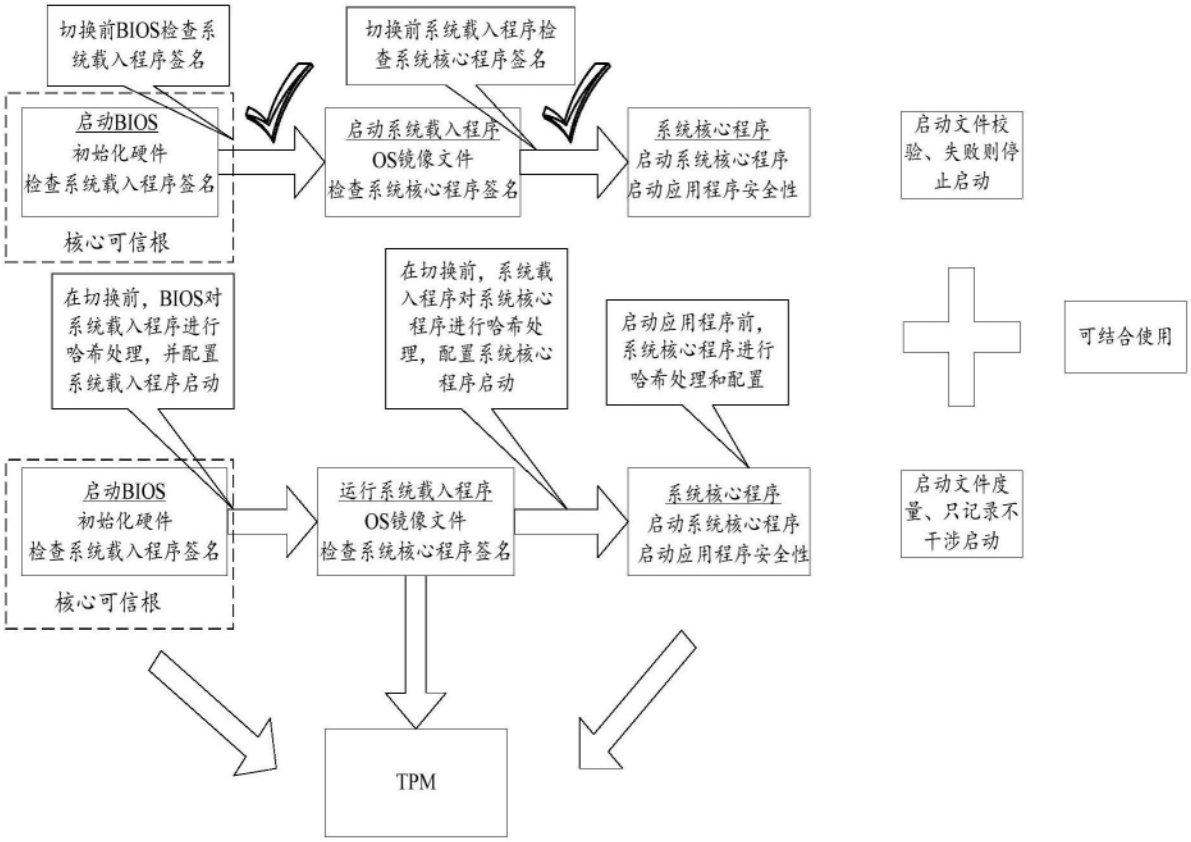

切换前BIOS检查系统载入程序签名
切换前系统载入程序检查系统核心程序签名
启动BIOS
初始化硬件
检查系统载入程序签名
核心可信根
启动系统载入程序
OS镜像文件
检查系统核心程序签名
系统核心程序
启动系统核心程序
启动应用程序安全性
启动文件校验、失败则停止启动
在切换前，BIOS对系统载入程序进行哈希处理，并配置系统载入程序启动
在切换前，系统载入程序对系统核心程序进行哈希处理，配置系统核心程序启动
启动应用程序前，系统核心程序进行哈希处理和配置
可结合使用
启动BIOS
初始化硬件
检查系统载入程序签名
核心可信根
运行系统载入程序
OS镜像文件
检查系统核心程序签名
系统核心程序
启动系统核心程序
启动应用程序安全性
启动文件度量、只记录不干涉启动
TPM

图3

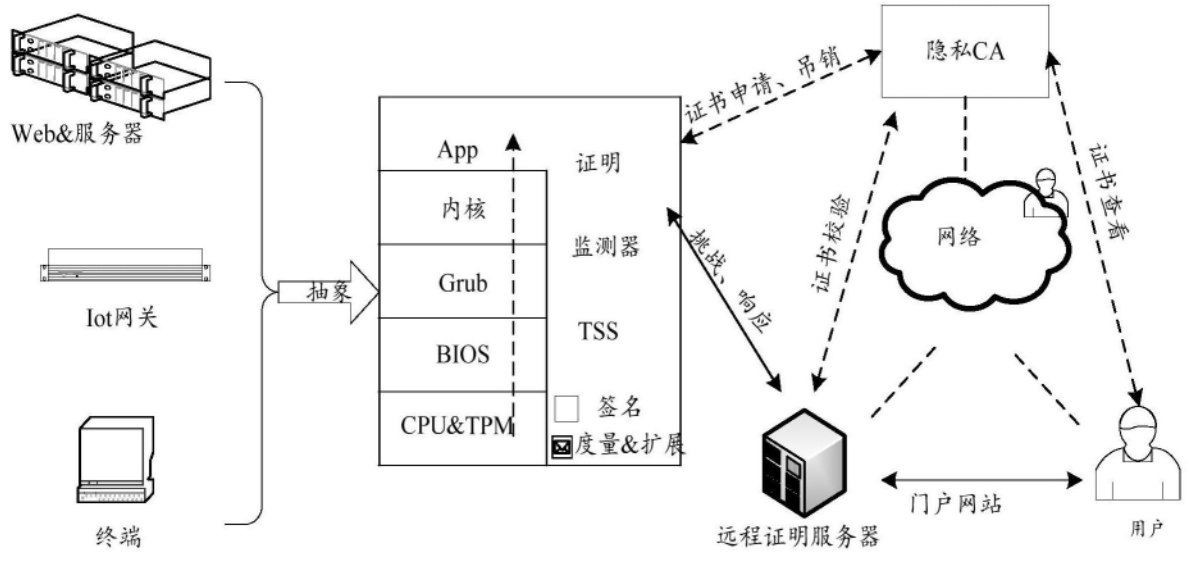

Web&服务器
Iot网关
终端
抽象
App
内核
Grub
BIOS
CPU&TPM
证明
监测器
TSS
签名
度量&扩展
隐私CA
证书申请、吊销
证书校验
证书查看
挑战、响应
网络
远程证明服务器
门户网站
用户

图4

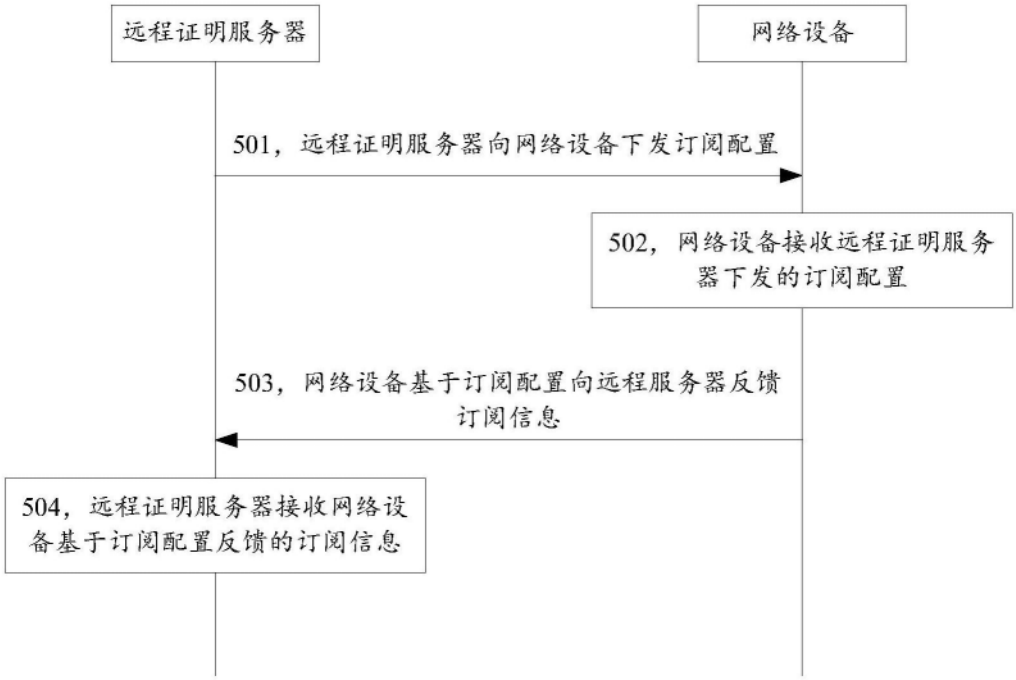

远程证明服务器
网络设备
501，远程证明服务器向网络设备下发订阅配置
502，网络设备接收远程证明服务器下发的订阅配置
503，网络设备基于订阅配置向远程服务器反馈订阅信息
504，远程证明服务器接收网络设备基于订阅配置反馈的订阅信息

图5

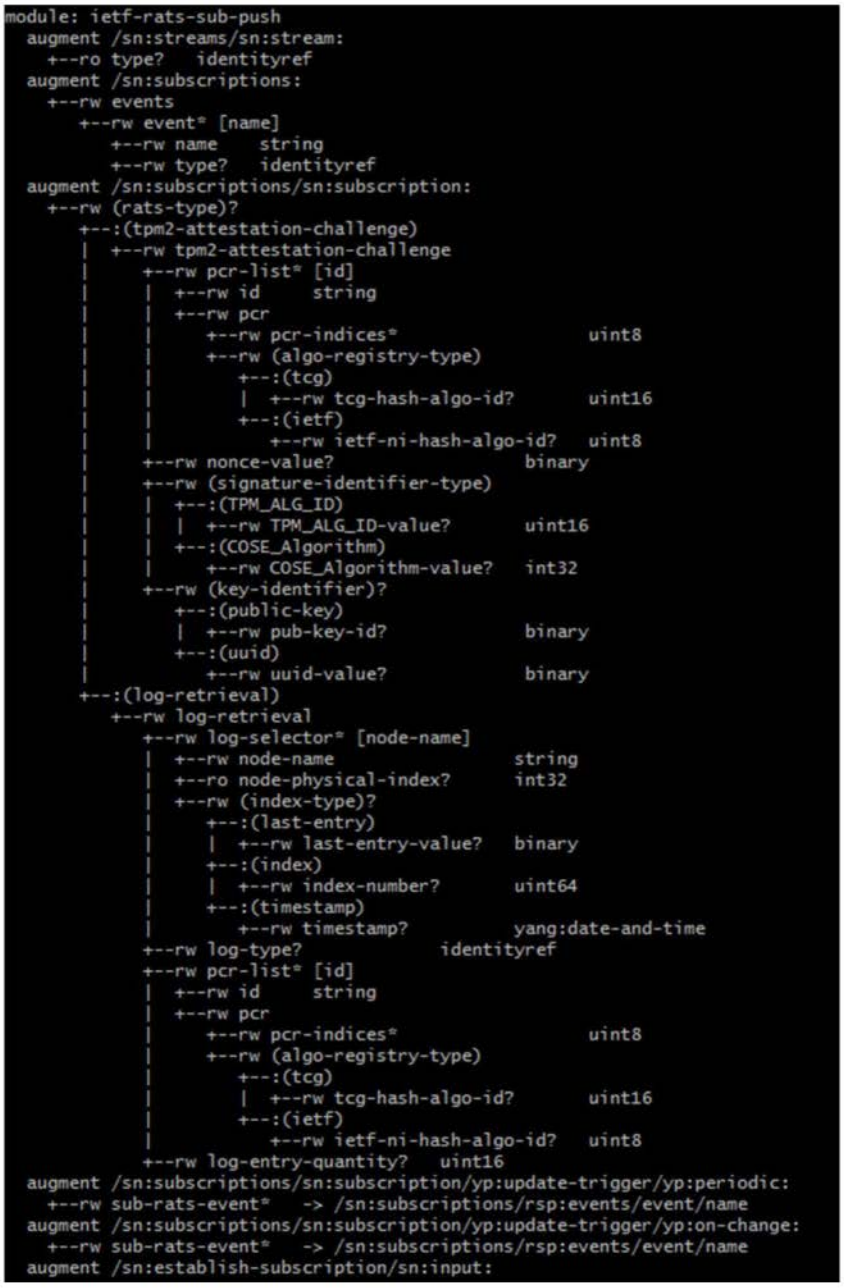

module: ietf-rats-sub-push
augment /sn:streams/sn:stream:
+--ro type? identityref
augment /sn:subscriptions:
+--rw events
+--rw event* [name]
+--rw name string
+--rw type? identityref
augment /sn:subscriptions/sn:subscription:
+--rw (rats-type)?
+--:(tpm2-attestation-challenge)
+--rw tpm2-attestation-challenge
+--rw pcr-list* [id]
+--rw id string
+--rw pcr
+--rw pcr-indices* uint8
+--rw (algo-registry-type)
+--:(tcg)
+--rw tcg-hash-algo-id? uint16
+--:(ietf)
+--rw ietf-ni-hash-algo-id? uint8
+--rw nonce-value? binary
+--rw (signature-identifier-type)
+--:(TPM_ALG_ID)
+--rw TPM_ALG_ID-value? uint16
+--:(COSE_Algorithm)
+--rw COSE_Algorithm-value? int32
+--rw (key-identifier)?
+--:(public-key)
+--rw pub-key-id? binary
+--:(uuid)
+--rw uuid-value? binary
+--:(log-retrieval)
+--rw log-retrieval
+--rw log-selector* [node-name]
+--rw node-name string
+--ro node-physical-index? int32
+--rw (index-type)?
+--:(last-entry)
+--rw last-entry-value? binary
+--:(index)
+--rw index-number? uint64
+--:(timestamp)
+--rw timestamp? yang:date-and-time
+--rw log-type? identityref
+--rw pcr-list* [id]
+--rw id string
+--rw pcr
+--rw pcr-indices* uint8
+--rw (algo-registry-type)
+--:(tcg)
+--rw tcg-hash-algo-id? uint16
+--:(ietf)
+--rw ietf-ni-hash-algo-id? uint8
+--rw log-entry-quantity? uint16
augment /sn:subscriptions/sn:subscription/yp:update-trigger/yp:periodic:
+--rw sub-rats-event* -> /sn:subscriptions/rsp:events/event/name
augment /sn:subscriptions/sn:subscription/yp:update-trigger/yp:on-change:
+--rw sub-rats-event* -> /sn:subscriptions/rsp:events/event/name
augment /sn:establish-subscription/sn:input:

图6

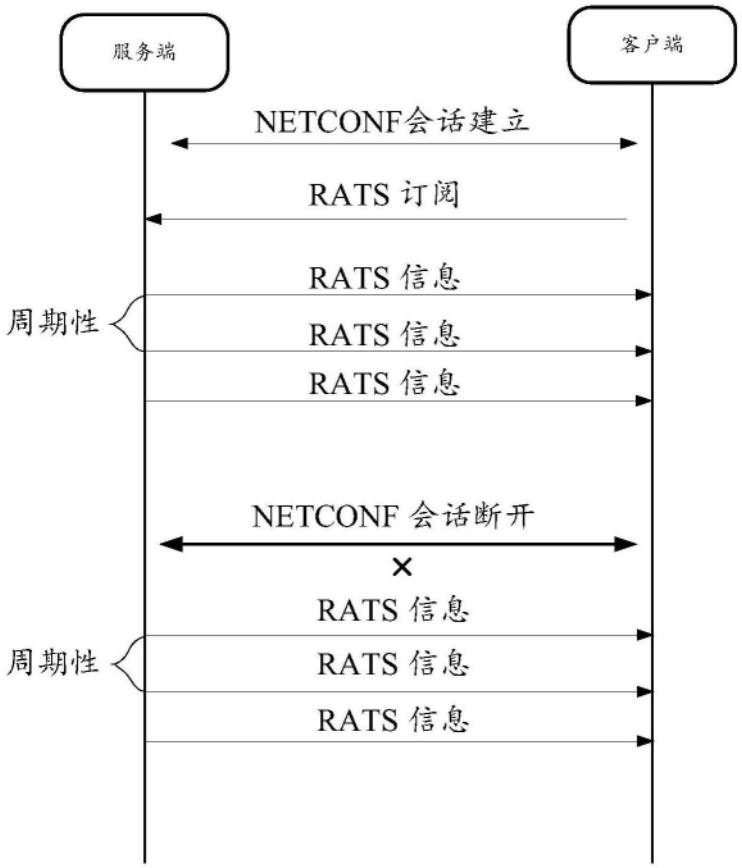

服务端
客户端
NETCONF会话建立
RATS 订阅
RATS 信息
周期性
RATS 信息
RATS 信息
NETCONF 会话断开
RATS 信息
周期性
RATS 信息
RATS 信息

图7

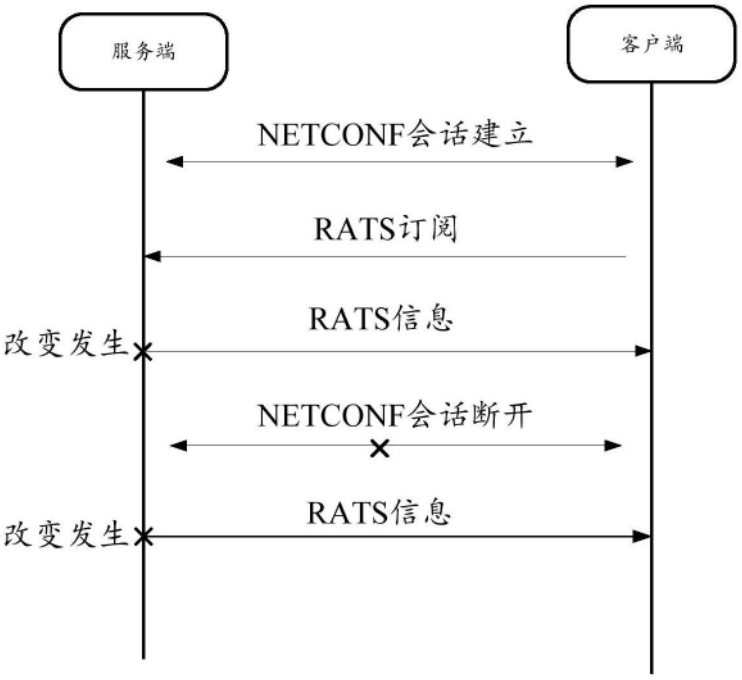

服务端
客户端
NETCONF会话建立
RATS订阅
RATS信息
改变发生
NETCONF会话断开
RATS信息
改变发生

图8

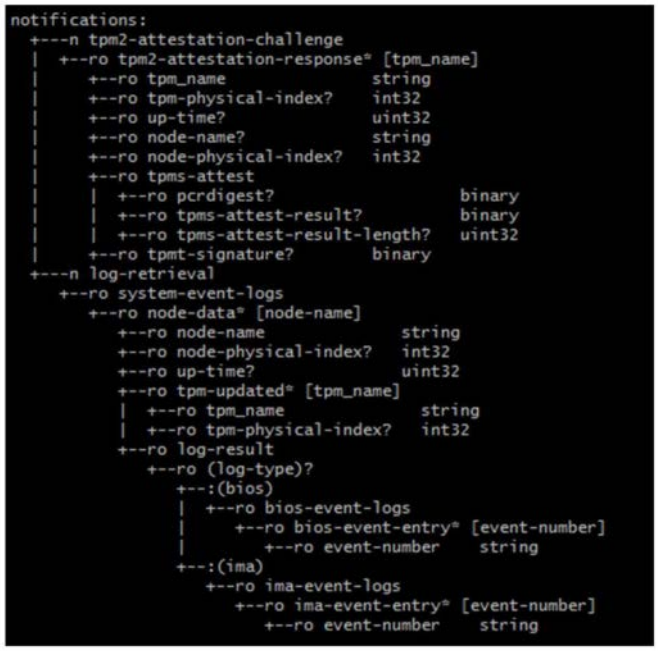

notifications:
+---n tpm2-attestation-challenge
| +--ro tpm2-attestation-response* [tpm_name]
| +--ro tpm_name string
| +--ro tpm-physical-index? int32
| +--ro up-time? uint32
| +--ro node-name? string
| +--ro node-physical-index? int32
| +--ro tpms-attest
| | +--ro pcrdigest? binary
| | +--ro tpms-attest-result? binary
| | +--ro tpms-attest-result-length? uint32
| +--ro tpmt-signature? binary
+---n log-retrieval
+--ro system-event-logs
+--ro node-data* [node-name]
+--ro node-name string
+--ro node-physical-index? int32
+--ro up-time? uint32
+--ro tpm-updated* [tpm_name]
| +--ro tpm_name string
| +--ro tpm-physical-index? int32
+--ro log-result
+--ro (log-type)?
+--:(bios)
| +--ro bios-event-logs
| +--ro bios-event-entry* [event-number]
| +--ro event-number string
+--:(ima)
+--ro ima-event-logs
+--ro ima-event-entry* [event-number]
+--ro event-number string

图9

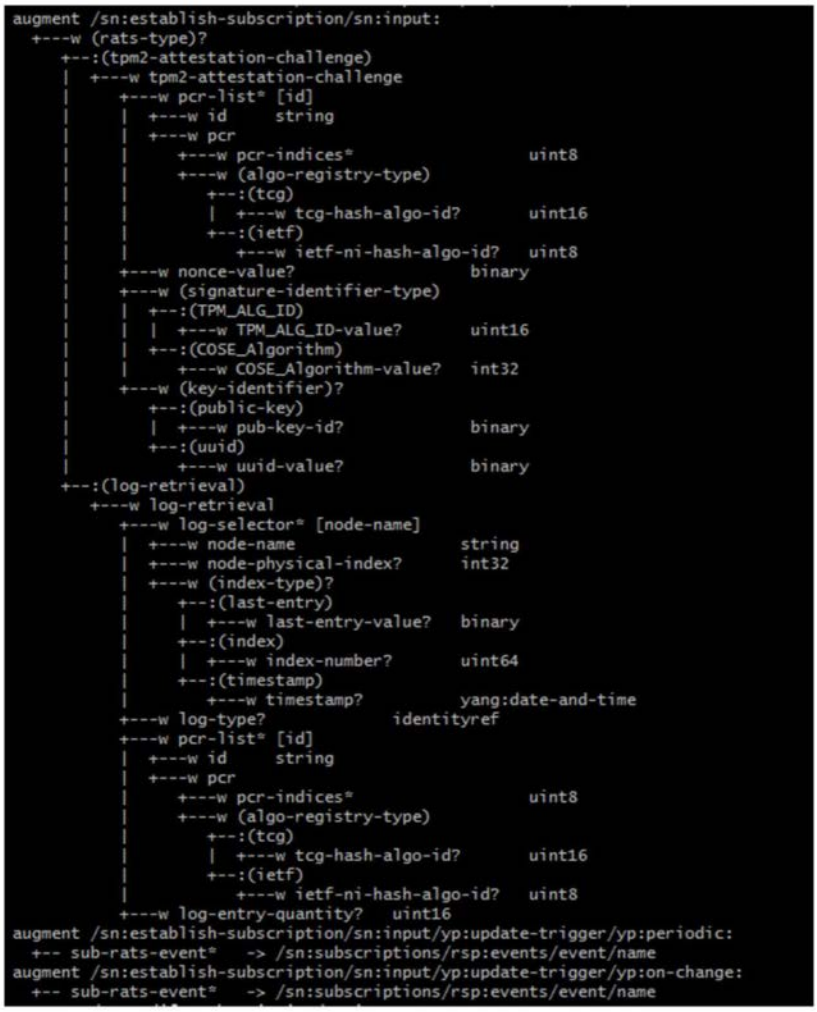

augment /sn:establish-subscription/sn:input:
+---w (rats-type)?
+--:(tpm2-attestation-challenge)
+---w tpm2-attestation-challenge
+---w pcr-list* [id]
+---w id string
+---w pcr
+---w pcr-indices* uint8
+---w (algo-registry-type)
+--:(tcg)
+---w tcg-hash-algo-id? uint16
+--:(ietf)
+---w ietf-ni-hash-algo-id? uint8
+---w nonce-value? binary
+---w (signature-identifier-type)
+--:(TPM_ALG_ID)
+---w TPM_ALG_ID-value? uint16
+--:(COSE_Algorithm)
+---w COSE_Algorithm-value? int32
+---w (key-identifier)?
+--:(public-key)
+---w pub-key-id? binary
+--:(uuid)
+---w uuid-value? binary
+--:(log-retrieval)
+---w log-retrieval
+---w log-selector* [node-name]
+---w node-name string
+---w node-physical-index? int32
+---w (index-type)?
+--:(last-entry)
+---w last-entry-value? binary
+--:(index)
+---w index-number? uint64
+--:(timestamp)
+---w timestamp? yang:date-and-time
+---w log-type? identityref
+---w pcr-list* [id]
+---w id string
+---w pcr
+---w pcr-indices* uint8
+---w (algo-registry-type)
+--:(tcg)
+---w tcg-hash-algo-id? uint16
+--:(ietf)
+---w ietf-ni-hash-algo-id? uint8
+---w log-entry-quantity? uint16
augment /sn:establish-subscription/sn:input/yp:update-trigger/yp:periodic:
+-- sub-rats-event* -> /sn:subscriptions/rsp:events/event/name
augment /sn:establish-subscription/sn:input/yp:update-trigger/yp:on-change:
+-- sub-rats-event* -> /sn:subscriptions/rsp:events/event/name

图10

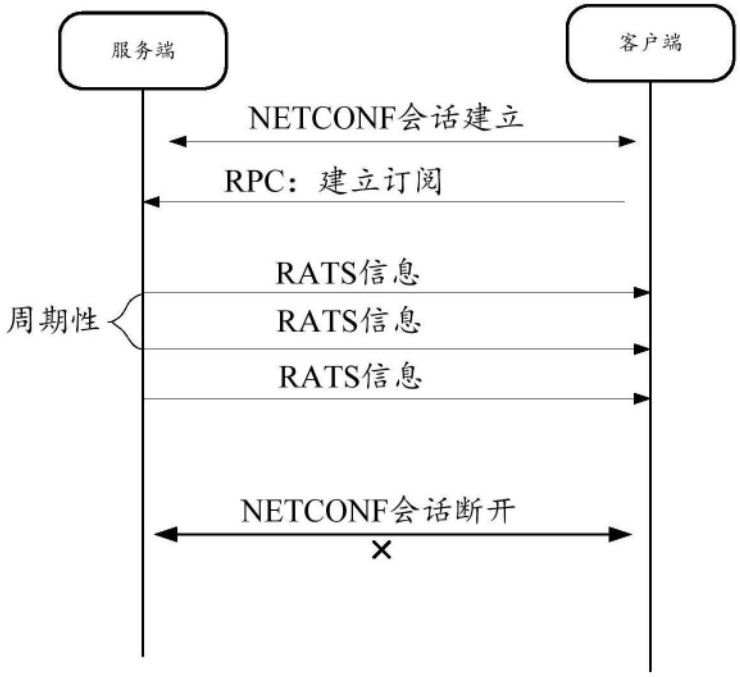

服务端
客户端
NETCONF会话建立
RPC：建立订阅
RATS信息
周期性
RATS信息
RATS信息
NETCONF会话断开

图11

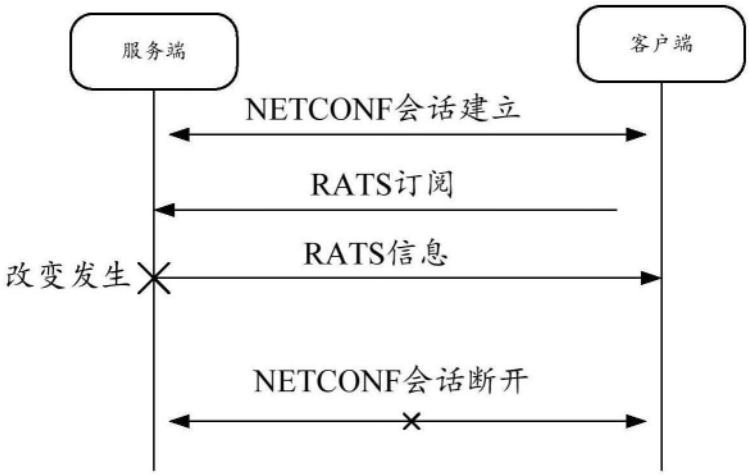

服务端
客户端
NETCONF会话建立
RATS订阅
改变发生
RATS信息
NETCONF会话断开

图12

```
notifications:
  +---n tpm2-attestation-challenge
  |  +--ro tpm2-attestation-response* [tpm_name]
  |     +--ro tpm_name                string
  |     +--ro tpm-physical-index?     int32
  |     +--ro up-time?                uint32
  |     +--ro node-name?              string
  |     +--ro node-physical-index?    int32
  |     +--ro tpms-attest
  |     |  +--ro pcrdigest?                      binary
  |     |  +--ro tpms-attest-result?             binary
  |     |  +--ro tpms-attest-result-length?      uint32
  |     +--ro tpmt-signature?         binary
  +---n log-retrieval
     +--ro system-event-logs
        +--ro node-data* [node-name]
           +--ro node-name              string
           +--ro node-physical-index?   int32
           +--ro up-time?               uint32
           +--ro tpm-updated* [tpm_name]
           |  +--ro tpm_name            string
           |  +--ro tpm-physical-index? int32
           +--ro log-result
              +--ro (log-type)?
                 +--:(bios)
                 |  +--ro bios-event-logs
                 |     +--ro bios-event-entry* [event-number]
                 |        +--ro event-number    string
                 +--:(ima)
                    +--ro ima-event-logs
                       +--ro ima-event-entry* [event-number]
                          +--ro event-number    string
```

图13

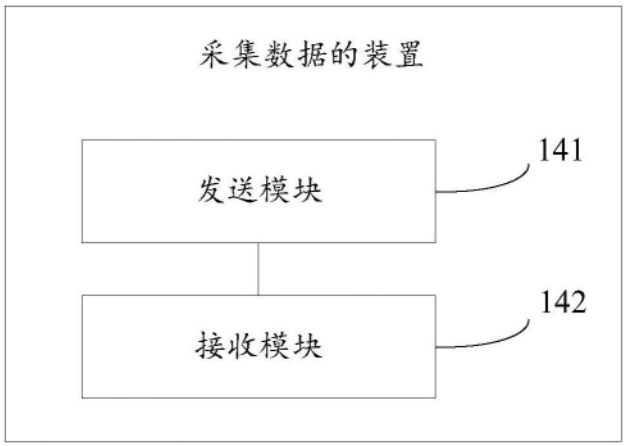


图14

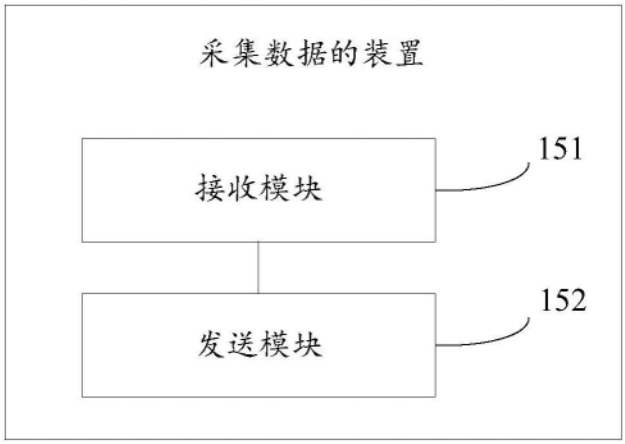


图15

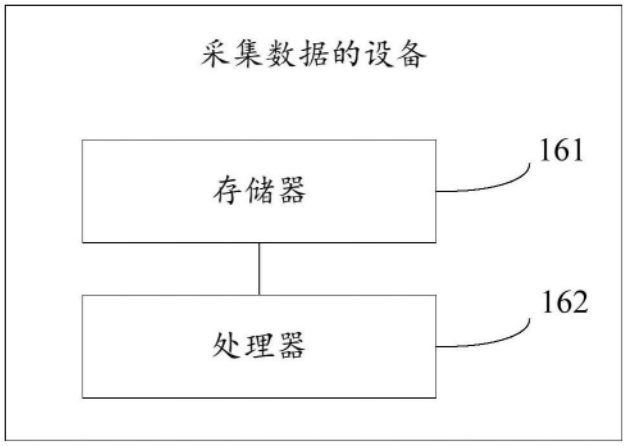


图16

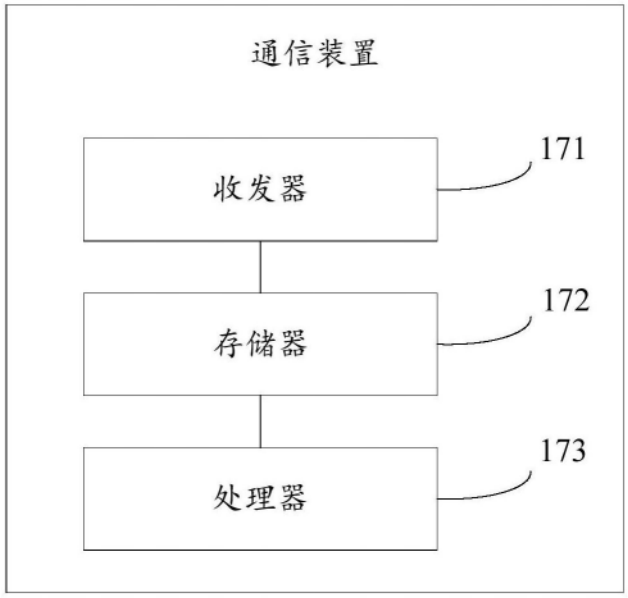


图17