state attesting method, where the method is applied to a network device. The network device is connected between an upstream device and a downstream network device, the upstream device is an upstream network device of the network device or an attestation server, and the method includes: first, measuring a first trusted attestation proxy for the network device to obtain a first proxy measured value, where the first proxy measured value is used to attest a trusted state of the first trusted attestation proxy; subsequently, sending the first proxy measured value to the upstream device; and finally, receiving at least one baseline value from the upstream device, where at least a part of the at least one baseline value is used to attest a trusted state of the downstream network device.

[0007] In this implementation, the first trusted attestation proxy in the trusted state is used to undertake attestation of the trusted state of the downstream network device, to effectively reduce an amount of information processed by the attestation server. In addition, in the method, when the attestation server is illegally tampered with or damaged, the first trusted attestation proxy can independently attest the trusted state of the downstream network device, to improve reliability.

[0008] In an optional implementation, the network device includes at least one first to-be-attested object connected to the first trusted attestation proxy, and the method further includes: obtaining a first measured value of each of the at least one first to-be-attested object, where the first measured value is used to attest a trusted state of the first to-be-attested object; and the at least one baseline value includes a first baseline value corresponding to the first to-be-attested object, and after the receiving at least one baseline value from the upstream device, the method further includes: attesting the trusted state of the first to-be-attested object based on the first baseline value corresponding to the first to-be-attested object and the first measured value.

[0009] In this implementation, the first trusted attestation proxy is responsible for attesting the trusted state of the first to-be-attested object. The amount of information processed by the attestation server is effectively reduced because attestation of the trusted state of each first to-be-attested object does not need to rely on the attestation server. In addition, when the attestation server is attacked, the first trusted attestation proxy can independently attest the trusted state of the first to-be-attested object, to improve reliability.

[0010] In an optional implementation, after the obtaining a first measured value of each of the first at least to-be-attested object, the method further includes: sending the first measured value to the upstream device. In this implementation, the first trusted attestation proxy in the trusted state sends the first

measured value to the upstream device. The upstream device is responsible for attesting the first to-be-attested object, to effectively reduce an amount of information processed by the first trusted attestation proxy and a burden of the first to-be-attested object.

[0011] In an optional implementation, the at least one baseline value includes a second baseline value, the second baseline value corresponds to a second trusted attestation proxy for the downstream network device, and after the receiving at least one baseline value from the upstream device, the method further includes: receiving a second proxy measured value from the downstream network device, where the second proxy measured value is used to attest a trusted state of the second trusted attestation proxy; and attesting the trusted state of the second trusted attestation proxy based on the second baseline value and the second proxy measured value.

[0012] In this implementation, the first trusted attestation proxy is responsible for attesting the second trusted attestation proxy, to effectively reduce the amount of information processed by the attestation server and the burden of the attestation server.

[0013] In an optional implementation, the method further includes: receiving a second proxy measured value from the downstream network device, where the second proxy measured value is used to attest a trusted state of a second trusted attestation proxy; and sending the second proxy measured value to the upstream device. In this implementation, the upstream device is responsible for attesting the second trusted attestation proxy, to effectively reduce the amount of information processed by the first trusted attestation proxy and the burden of the attestation server.

[0014] In an optional implementation, the at least one baseline value includes a third baseline value, the third baseline value corresponds to a second to-be-attested object of the downstream network device, and after the receiving at least one baseline value from the upstream device, the method further includes: receiving a second measured value from the downstream network device, where the second measured value is used to attest a trusted state of the second to-be-attested object; and attesting the trusted state of the second to-be-attested object based on the third baseline value corresponding to the second to-be-attested object and the second measured value.

[0015] In this implementation, the first trusted attestation proxy in the trusted state undertakes attestation of the trusted state of the second to-be-attested object, to effectively reduce the amount of information processed by the attestation server and the burden of the attestation server. In addition, efficiency in attesting the second to-be-attested object is effectively improved. A risk of

attesting method according to the present invention;

[0040] FIG. 9A and FIG. 9B are a flowchart of steps in a fourth embodiment of a trusted-state attesting method according to the present invention; and

[0041] FIG. 10 is a structural diagram of an embodiment of an attestation server according to the present invention.

DESCRIPTION OF EMBODIMENTS

[0042] First, an architecture of a communication system to which a trusted-state attesting method provided in this application is applied is described. FIG. 1 is a schematic diagram of a communication architecture to which a trusted-state attesting method is applied. As shown in FIG. 1, the communication system includes an attestation server 101 and a network device cluster 102. The network device cluster 102 includes a plurality of network devices. The attestation server 101 is connected to each network device. The attestation server 101 and each network device that are interconnected exchange information, to attest a trusted state of the network device. The following describes a connection manner between the attestation server 101 and each network device with reference to a specific example.

[0043] For example, a network device 1021 included in the network device cluster 102 is directly connected to the attestation server 101. Specifically, the network device 1021 directly creates a transmission control protocol (transmission control protocol, TCP) connection to the attestation server 101. Alternatively, another connection such as an Internet Protocol (internet protocol, IP) connection may be created between the attestation server 101 and the network device 1021. This is not limited in this application.

[0044] For another example, a network device 1022 included in the network device cluster 102 is indirectly connected to the attestation server 101. The attestation server 101 and the network device 1022 that are indirectly connected are separated by one or more other network devices. Specifically, the network device 1022 is indirectly connected to the attestation server 101 via the network device 1021. For a description of a connection relationship between the attestation server 101 and another network device included in the network device cluster 102, refer to the description of the network device 1021 or the network device 1022. Details are not described again.

[0045] The following describes an internal structure of each network device.

included in the NFVI 302. The NFVI 302 provides the virtualized resource for the virtual machine 303. The to-be-attested object may be all or a part of all the virtual machines 303, the NFV MANO 301, and the NFVI 302.

[0050] FIG. 4 is a flowchart of steps in a first embodiment of a trusted-state attesting method according to the present invention. With reference to FIG. 4, the following describes a specific execution process of the trusted-state attesting method provided in this application.

[0051] Step 401: A first trusted attestation proxy obtains a first proxy measured value.

[0052] The first trusted attestation proxy shown in this embodiment is located in a target network device. The first trusted attestation proxy is configured to perform trusted-state attesting. The following first describes a connection location of the target network device in a communication network:

[0053] The target network device shown in this embodiment is connected between an upstream device and a downstream network device. The upstream device may be any one of one or more network devices connected between the target network device and an attestation server. Alternatively, the upstream device may be an attestation server. As shown in FIG. 1, an upstream device of a target network device 1023 may be any one of the network device 1022, the network device 1021, and the attestation server 101.

[0054] The downstream network device is any one of one or more network devices that need to be indirectly connected to the attestation server via the target network device. For a description of the indirect connection, refer to FIG. 1. Details are not described again. For another example, a downstream network device of the target network device 1023 is a network device 1024.

[0055] In a specific implementation, the first trusted attestation proxy may be a service card shown in FIG. 2. In addition, the first trusted attestation proxy and a to-be-attested object are different service cards. For example, the to-be-attested object is the service card 2011 or the service card 2012, while the first trusted attestation proxy is the service card 201N. In this example, alternatively, the to-be-attested object may be the system control card 202 and the system clock card 203.

[0056] The first trusted attestation proxy may be a code segment running in the system control card 202. The to-be-attested object is all service cards and the system clock card 203 included in the target network device 200. Alternatively, the first trusted attestation proxy may be a code segment running in the system clock card 203. The to-be-attested object is all service cards and

trusted attestation proxy is in a trusted state. Specifically, the upstream device may prestore a first proxy baseline value. The upstream device determines whether the first proxy measured value is consistent with the first proxy baseline value.

[0064] If the first proxy measured value is not consistent with the first proxy baseline value, the upstream device determines that the first trusted attestation proxy is in an untrusted state. In an example, the upstream device may send re-attestation information to the first trusted attestation proxy. The re-attestation information is used to indicate the first trusted attestation proxy to re-perform step 401. In another example, the upstream device may generate result indication information, where the result indication information is used to indicate that the first trusted attestation proxy is in an untrusted state. The first trusted attestation proxy is analyzed and processed based on the indication information. If the first proxy measured value is consistent with the first proxy baseline value, the upstream device determines that the first trusted attestation proxy is in a trusted state, and then execution of step 404 is triggered.

[0065] Step 404: The upstream device sends at least one baseline value to the first trusted attestation proxy.

[0066] At least a part of the at least one baseline value shown in this embodiment is used to attest the trusted state of the downstream network device. Specifically, the at least one baseline value includes a baseline value corresponding to a second trusted attestation proxy for the downstream network device; and/or the at least one baseline value includes a baseline value corresponding to a to-be-attested object of the downstream network device. For a specific description of the second trusted attestation proxy, refer to the description of the first trusted attestation proxy shown in step 401. Details are not described again.

[0067] Step 405: The first trusted attestation proxy receives the at least one baseline value.

[0068] The first trusted attestation proxy determines, based on the at least one baseline value, that the first trusted attestation proxy is in a trusted state.

[0069] Step 406: The first trusted attestation proxy attests the trusted state of the downstream network device.

[0070] The first trusted attestation proxy in the trusted state attests the trusted state of the downstream network device. Specifically, the first trusted attestation proxy attests a trusted state of the second trusted attestation proxy based on the at least one baseline value; and/or the first trusted attestation proxy attests a trusted state of the to-be-attested object of the downstream network device based on the at least one baseline value.

[0071] By using the method shown in this embodiment, the first trusted attestation proxy in

the trusted state undertakes attestation of the trusted state of the downstream network device, to effectively reduce an amount of information processed by the attestation server. When the attestation server is illegally tampered with or damaged, the first trusted attestation proxy independently attests the trusted state of the downstream network device, to effectively improve reliability of the downstream network device and accuracy of attesting the trusted state of the downstream network device. In addition, the method avoids a risk of tampering with the downstream network device when the attestation server is illegally tampered with, to effectively improve reliability of the downstream network device.

[0072] FIG. 5A and FIG. 5B are a flowchart of steps in a second embodiment of a trusted-state attesting method according to the present invention. With reference to FIG. 5A and FIG. 5B, the following describes an example of a process of attesting a trusted state of a to-be-attested object of a target network device. As shown in this embodiment, a first trusted attestation proxy is responsible for attesting the trusted state of the to-be-attested object of the target network device.

[0073] Step 501: The first trusted attestation proxy and an upstream device create a first secure channel.

[0074] For a description of the upstream device, refer to FIG. 4. Details are not described again. FIG. 6 is a second schematic diagram of a communication architecture to which trusted-state attesting is applied. FIG. 6 is used as an example. The first trusted attestation proxy is a trusted attestation proxy 641 that belongs to a target network device 64. The trusted attestation proxy 641 and a trusted attestation proxy 621 that belongs to an upstream network device 62 create a first secure channel. For another example, the first trusted attestation proxy is a trusted attestation proxy 621 that belongs to a target network device 62. The trusted attestation proxy 621 and an attestation server 61 create a first secure channel.

[0075] Security of information exchanged between the first trusted attestation proxy and the upstream device is implemented based on the first secure channel. Specifically, the first trusted attestation proxy and the upstream device perform identity authentication and key agreement with each other based on transport layer security (transport layer security, TLS), Internet Protocol security (internet protocol security, IPsec), key sharing, or the like. The first secure channel is successfully created after identity authentication and key agreement are performed. It can be learned that the first secure channel is an encrypted secure channel.

[0076] Step 502: The first trusted attestation proxy receives a measurement proxy request from

[0088] When the first trusted attestation proxy is in a trusted state, the first trusted attestation proxy obtains a first measured value of each first to-be-attested object by using the measurement request. The first trusted attestation proxy may periodically send the measurement request to the first to-be-attested object, so as to periodically attest a trusted state of the first to-be-attested object. Alternatively, the first trusted attestation proxy may send the measurement request to the first to-be-attested object based on a trigger event. The trigger event may be reset or initial power-on of the first to-be-attested object, or a command entered by network management personnel.

[0089] A time sequence of performing step 508 and step 509 shown in this embodiment is not limited.

[0090] Step 510: The first to-be-attested object generates a first measured value based on the measurement request.

[0091] To attest a trusted state of each first to-be-attested object, each first to-be-attested object needs to generate a first measured value. A specific quantity of first measured values generated by the first to-be-attested object is not limited in this embodiment. Specifically, the first to-be-attested object may include a plurality of subobjects. The first to-be-attested object generates a corresponding first measured value for each subobject. The first measured value corresponding to each subobject is used to attest a trusted state of the subobject. It can be learned that, in this embodiment, the trusted state of the first to-be-attested object is attested by attesting the trusted state of each subobject.

[0092] Specifically, the trusted state is attested by statically measuring the first to-be-attested object in a system startup phase. The subobject included in the first to-be-attested object may be a basic input output system (basic input output system, BIOS), an operating system loader (operating system loader, OSLoader), an operating system (operating system, OS), an application started by the OS, and the like.

[0093] Then static measurement is performed to attest that the first to-be-attested object is in the trusted state in the system startup phase. Subsequently, the first to-be-attested object is dynamically measured in a system running phase. The subobject included in the first to-be-attested object is a process that is running on the first to-be-attested object.

[0094] FIG. 7 shows an example of a system architecture of a first to-be-attested object according to the present invention. With reference to FIG. 7, the following describes a process of statically measuring the first to-be-attested object.

[00119] Step 803: The first trusted attestation proxy sends a downstream measurement proxy request to the second trusted attestation proxy through the second secure channel.

[00120] The downstream measurement proxy request is used to request to obtain a second proxy measured value of the second trusted attestation proxy. The second proxy measured value is used to attest the trusted state of the second trusted attestation proxy.

[00121] Step 804: The second trusted attestation proxy obtains a second proxy measured value based on the downstream measurement proxy request.

[00122] For step 804 shown in this embodiment, refer to step 503 shown in FIG. 5A and FIG. 5B. Details are not described again.

[00123] Step 805: The second trusted attestation proxy sends the second proxy measured value to the first trusted attestation proxy through the second secure channel.

[00124] Step 806: The first trusted attestation proxy receives the second proxy measured value through the second secure channel.

[00125] Step 807: The first trusted attestation proxy attests the trusted state of the second trusted attestation proxy.

[00126] It can be learned from step 801 that the first trusted attestation proxy has received the second baseline value. In this case, the first trusted attestation proxy determines whether the second proxy measured value is consistent with the second baseline value.

[00127] If yes, it indicates that the second proxy measured value is in a trusted state. If no, it indicates that the second proxy measured value is in an untrusted state. For a description that the second proxy measured value is in an untrusted state, refer to the description that the first trusted attestation proxy is in an untrusted state shown in step 403. Details are not described again.

[00128] Step 808: The first trusted attestation proxy sends a fourth baseline value to the second trusted attestation proxy through the second secure channel.

[00129] For better understanding, the following provides a description with reference to FIG. 6. The plurality of baseline values received by the first trusted attestation proxy 621 for the target network device 62 from the upstream device (the attestation server 61) may further include a fourth baseline value. The fourth baseline value is used to attest trusted states of the to-be-attested objects (662 and 663) subordinate to the downstream network device 64.

[00130] Specifically, the first trusted attestation proxy 621 determines that a second trusted attestation proxy 641 for the downstream network device 64 is in a trusted state. The first trusted

attestation proxy 621 may send the fourth baseline value to the second trusted attestation proxy 641.

[00131] The second trusted attestation proxy 641 may attest, based on the fourth baseline value, the trusted states of the to-be-attested objects (662 and 663) subordinate to the downstream network device 64. Alternatively, the second trusted attestation proxy may further send the fourth baseline value to the trusted attestation proxy 661 subordinate to the downstream network device 64. The trusted attestation proxy 661 subordinate to the downstream network device 64 attests, based on the fourth baseline value, the to-be-attested objects (662 and 663) subordinate to the downstream network device 64.

[00132] In this embodiment, for example, the first trusted attestation proxy is responsible for attesting the trusted state of the second trusted attestation proxy. In another example, alternatively, the upstream device may be responsible for attesting the trusted state of the second trusted attestation proxy. In this example, the first trusted attestation proxy may send the second proxy measured value to the upstream device through a first secure channel. For a description of a process in which the upstream device attests the second trusted attestation proxy, refer to the process in which the first trusted attestation proxy attests the second trusted attestation proxy. Details are not described again. Because the upstream device is responsible for attesting the second trusted attestation proxy, the plurality of baseline values sent by the upstream device to the first trusted attestation proxy do not include the second baseline value.

[00133] Step 809: The first trusted attestation proxy sends a downstream measurement request to the second trusted attestation proxy through the second secure channel.

[00134] The downstream measurement request is used to obtain a second measured value of each second to-be-attested object. The second trusted attestation proxy forwards the obtained downstream measurement request to each second to-be-attested object. Each second to-be-attested object may perform measurement based on the downstream measurement request to obtain the second measured value. For a specific process in which the second to-be-attested object obtains the second measured value, refer to the process in which the first to-be-attested object obtains the first measured value shown in step 510 shown in FIG. 5A and FIG. 5B. Details are not described again.

[00135] A time sequence of performing step 808 and step 809 shown in this embodiment is not limited.

CLAIMS

What is claimed is:

1. A trusted-state attesting method, wherein the method is applied to a network device, the network device is connected between an upstream device and a downstream network device, the upstream device is an upstream network device of the network device or an attestation server, and the method comprises:

measuring a first trusted attestation proxy for the network device to obtain a first proxy measured value, wherein the first proxy measured value is used to attest a trusted state of the first trusted attestation proxy;

sending the first proxy measured value to the upstream device; and

receiving at least one baseline value from the upstream device, wherein at least a part of the at least one baseline value is used to attest a trusted state of the downstream network device.

2. The method according to claim 1, wherein the network device comprises at least one first to-be-attested object connected to the first trusted attestation proxy, and the method further comprises:

obtaining a first measured value of each of the at least one first to-be-attested object, wherein the first measured value is used to attest a trusted state of the first to-be-attested object; and

the at least one baseline value comprises a first baseline value corresponding to the first to-be-attested object, and after the receiving at least one baseline value from the upstream device, the method further comprises:

attesting the trusted state of the first to-be-attested object based on the first baseline value corresponding to the first to-be-attested object and the first measured value.

3. The method according to claim 2, wherein after the obtaining a first measured value of each of the at least first to-be-attested object, the method further comprises:

sending the first measured value to the upstream device.

4. The method according to any one of claims 1 to 3, wherein the at least one baseline value comprises a second baseline value, the second baseline value corresponds to a second trusted attestation proxy for the downstream network device, and after the receiving at least one baseline value from the upstream device, the method further comprises:

receiving a second proxy measured value from the downstream network device, wherein the

second proxy measured value is used to attest a trusted state of the second trusted attestation proxy; and

attesting the trusted state of the second trusted attestation proxy based on the second baseline value and the second proxy measured value.

5. The method according to any one of claims 1 to 3, wherein the method further comprises:

receiving a second proxy measured value from the downstream network device, wherein the second proxy measured value is used to attest a trusted state of a second trusted attestation proxy; and

sending the second proxy measured value to the upstream device.

6. The method according to any one of claims 1 to 5, wherein the at least one baseline value comprises a third baseline value, the third baseline value corresponds to a second to-be-attested object of the downstream network device, and after the receiving at least one baseline value from the upstream device, the method further comprises:

receiving a second measured value from the downstream network device, wherein the second measured value is used to attest a trusted state of the second to-be-attested object; and

attesting the trusted state of the second to-be-attested object based on the third baseline value corresponding to the second to-be-attested object and the second measured value.

7. The method according to any one of claims 1 to 5, wherein the at least one baseline value comprises a third baseline value, the third baseline value corresponds to a second to-be-attested object of the downstream network device, and after the receiving at least one baseline value from the upstream device, the method further comprises:

sending the third baseline value to the downstream network device.

8. The method according to claim 2 or 3, wherein the first to-be-attested object and the first trusted attestation proxy are two cards; or the first to-be-attested object and the first trusted attestation proxy are two virtual machines; or the first to-be-attested object and the first trusted attestation proxy are any two of a virtual machine, a network functions virtualization management and orchestration system, or a network functions virtualization infrastructure layer.

9. A trusted-state attesting method, wherein the method is applied to an upstream device, the upstream device, a network device, and a downstream network device are sequentially connected, the upstream device is an upstream network device of the network device or an attestation server, and the method comprises:

receiving a first proxy measured value from the network device, wherein the first proxy measured value is used to attest a trusted state of a first trusted attestation proxy for the network device;

attesting, based on the first proxy measured value, that the first trusted attestation proxy is in the trusted state; and

sending at least one baseline value to the network device, wherein at least a part of the at least one baseline value is used to attest a trusted state of the downstream network device.

10. The method according to claim 9, wherein the at least one baseline value comprises a first baseline value corresponding to a first to-be-attested object of the network device.

11. The method according to claim 9 or 10, wherein after the sending at least one baseline value to the network device, the method further comprises:

receiving a first measured value from the network device, wherein the first measured value is used to attest a trusted state of the first to-be-attested object of the network device; and

attesting the trusted state of the first to-be-attested object based on the first baseline value corresponding to the first to-be-attested object and the first measured value.

12. The method according to any one of claims 9 to 11, wherein the at least one baseline value comprises a second baseline value, and the second baseline value corresponds to a second trusted attestation proxy for the downstream network device.

13. The method according to any one of claims 9 to 11, wherein after the sending at least one baseline value to the network device, the method further comprises:

receiving a second proxy measured value from the network device, wherein the second proxy measured value is used to attest a trusted state of a second trusted attestation proxy for the downstream network device; and

attesting the trusted state of the second trusted attestation proxy based on a second baseline value corresponding to the second trusted attestation proxy and the second proxy measured value.

14. The method according to any one of claims 9 to 13, wherein the at least one baseline value comprises a third baseline value, and the third baseline value corresponds to a second to-be-attested object of the downstream network device.

15. A network device, wherein the network device is connected between an upstream device and a downstream network device, the upstream device is an upstream network device of the network device or an attestation server, the network device comprises a first trusted attestation

proxy, and the first trusted attestation proxy is configured to perform the trusted-state attesting method according to any one of claims 1 to 8.

16. An upstream network device, wherein the upstream network device, a network device, and a downstream network device are sequentially connected, and a trusted attestation proxy for the upstream network device is configured to perform the trusted-state attesting method according to any one of claims 9 to 14.

17. An attestation server, wherein the attestation server, a network device, and a downstream network device are sequentially connected, the attestation server comprises a processor, a memory, and an optical transceiver, and the processor is separately interconnected with the memory and the optical transceiver by using a line;

the optical transceiver is configured to receive a first proxy measured value from the network device, wherein the first proxy measured value is used to attest a trusted state of a first trusted attestation proxy for the network device;

the processor invokes program code in the memory to perform the following step:

attesting, based on the first proxy measured value, that the first trusted attestation proxy is in the trusted state; and

the optical transceiver is further configured to send at least one baseline value to the network device, wherein at least a part of the at least one baseline value is used to attest a trusted state of the downstream network device.

18. A computer-readable storage medium, comprising instructions, wherein when the instructions are run on a computer, the computer is enabled to perform the trusted-state attesting method according to any one of claims 1 to 14.

19. A computer program product comprising instructions, wherein when the computer program product runs on a computer, the computer is enabled to perform the trusted-state attesting method according to any one of claims 1 to 14.