

CLAIMS

What is claimed is:

1. A trusted computing method, applicable to a server, wherein the server is equipped with a first trusted computing chip and a second trusted computing chip, and the method comprises:

performing, by the first trusted computing chip, a static measurement on the server during startup of the server to obtain a static measurement result, and sending the static measurement result to a verification center; and

performing, by the second trusted computing chip, a dynamic measurement on the server during operations after the startup of the server to obtain a dynamic measurement result, and sending, by the second trusted computing chip to the verification center, the dynamic measurement result and association evidence indicating that the first trusted computing chip and the second trusted computing chip are disposed in the same server, for the verification center to associate the static measurement result with the dynamic measurement result based on the association evidence, and to verify integrity of a software system of the server based on the associated static measurement result and dynamic measurement result.

2. The method according to claim 1, wherein

the first trusted computing chip is inserted into a serial peripheral interface (SPI) interface or a low pin count (LPC) interface on the server, and

the second trusted computing chip is inserted into a peripheral component interconnect express (PCIE) interface, a serial advanced technology attachment (SATA) interface, or a universal serial bus (USB) interface on the server.

3. The method according to claim 1, wherein

before the performing, by the first trusted computing chip, a static measurement on the server, the method further comprises: receiving, by the first trusted computing chip, a first device certificate issued by a certificate authority (CA); and receiving, by the second trusted computing chip, a second device certificate issued by the CA, wherein

when the first trusted computing chip sends the static measurement result to the verification center, the first trusted computing chip further sends the first device certificate to the verification center, for the verification center to verify the first device certificate, and

when the second trusted computing chip sends the dynamic measurement result to the verification center, the second trusted computing chip further sends the second device certificate to the verification center, for the verification center to verify the second device certificate.

4. The method according to claim 3, wherein before the performing, by the first trusted computing chip, a static measurement on the server, the method further comprises:
receiving, by the second trusted computing chip, the association evidence signed by the CA.

5. The method according to claim 1, wherein the association evidence comprises:
identification information of the first trusted computing chip;
identification information of the second trusted computing chip; and
a signature of a certificate authority (CA).

6. The method according to claim 1, wherein the performing, by the first trusted computing chip, a static measurement on the server to obtain a static measurement result comprises:
acquiring, by the first trusted computing chip, program code of a basic input/output system (BIOS), program code of a Bootloader, and program code of an operating system (OS) that are in the server; and
generating, by the first trusted computing chip, the static measurement result based on the program code of the BIOS, the program code of the Bootloader, and the program code of the OS.

7. The method according to claim 1, wherein the performing, by the second trusted computing chip, a dynamic measurement on the server to obtain a dynamic measurement result comprises:
acquiring, by the second trusted computing chip, static executable program code of application programs and program code of the application programs in an internal memory during the operations, wherein the application programs are installed on the server; and
generating, by the second trusted computing chip, the dynamic measurement result based on the static executable program code of the application programs and the program code of the application programs in the internal memory during the operations.

8. The method according to any one of claims 1 to 7, wherein after the sending, by the second trusted computing chip, the dynamic measurement result and association evidence to the verification center, the method further comprises:

receiving, by the first trusted computing chip, a first verification result fed back by the verification center, wherein the first verification result corresponds to the static measurement; and

receiving, by the second trusted computing chip, a second verification result fed back by the verification center, wherein the second verification result corresponds to the dynamic measurement, and the second verification result carries the association evidence.

9. A server, comprising:

a main board;

a first trusted computing chip, disposed on the main board and configured to perform a static measurement on the server during startup of the server to obtain a static measurement result, and send the static measurement result to a verification center; and

a second trusted computing chip, disposed on the main board and configured to perform a dynamic measurement on the server during operations after the startup of the server to obtain a dynamic measurement result, and send, to the verification center, the dynamic measurement result and association evidence indicating that the first trusted computing chip and the second trusted computing chip are disposed in the same server, for the verification center to associate the static measurement result with the dynamic measurement result based on the association evidence, and to verify integrity of a software system of the server based on the associated static measurement result and dynamic measurement result.

10. The server according to claim 9, wherein

the first trusted computing chip is inserted into a serial peripheral interface (SPI) interface or a low pin count (LPC) interface on the server, and

the second trusted computing chip is inserted into a peripheral component interconnect express (PCIE) interface, a serial advanced technology attachment (SATA) interface, or a universal serial bus (USB) interface on the server.

11. The server according to claim 9, wherein

the first trusted computing chip is further configured to:

receive a first device certificate issued by a certificate authority (CA) before performing the static measurement on the server; and further send the first device certificate to the verification center when sending the static measurement result to the verification center, for the verification center to verify the first device certificate; and

the second trusted computing chip is further configured to:

receive a second device certificate issued by the CA before the first trusted computing chip performs the static measurement on the server; and further send the second device certificate to the verification center when sending the dynamic measurement result to the verification center, for the verification center to verify the second device certificate.

12. The server according to claim 11, wherein the second trusted computing chip is further configured to:

receive the association evidence signed by the CA before the first trusted computing chip performs the static measurement on the server.

13. The server according to claim 9, wherein the association evidence comprises:

identification information of the first trusted computing chip;

identification information of the second trusted computing chip; and

a signature of a certificate authority (CA).

14. The server according to claim 9, wherein the first trusted computing chip is further configured to:

acquire program code of a basic input/output system (BIOS), program code of a Bootloader, and program code of an operating system (OS) that are in the server; and generate the static measurement result based on the program code of the BIOS, the program code of the Bootloader, and the program code of the OS.

15. The server according to claim 9, wherein the second trusted computing chip is further configured to:

acquire static executable program code of application programs and program code of the application programs in an internal memory during the operations, wherein the application programs are installed on the server; and generate the dynamic measurement result based on the static executable program code of the application programs and the program code of the application programs in the internal memory during the operations.

16. The server according to any one of claims 9 to 15, wherein

the first trusted computing chip is further configured to: receive a first verification result fed back by the verification center, wherein the first verification result corresponds to the static measurement; and

the second trusted computing chip is further configured to receive a second verification result fed back by the verification center, wherein the second verification result corresponds to the dynamic measurement, and the second verification result carries the association evidence.