

MAINBOARDS FOR SECURITY VERIFICATION, SECURITY VERIFICATION METHODS AND APPARATUSES, AND MEDIA

TECHNICAL FIELD

[0001] This specification relates to the field of computer technologies, and in particular, to
5 mainboards for security verification, security verification methods and apparatuses, and media.

BACKGROUND

[0002] At present, with the rapid development of information security technologies and people's increasing concern about their private data, as well as the help of trusted computing in solving security risks of information security and other aspects, trusted computing technology has
10 become an important application and research branch in the field of information security.

SUMMARY

[0003] This specification provides mainboards for security verification, security verification methods and apparatuses, and media, so as to partially alleviate the previous problems existing in a related technology.

[0004] This specification uses the following technical solutions: This specification provides a
15 mainboard for security verification. The mainboard for security verification is deployed in an electronic device, a device to be verified is disposed inside and/or a device to be verified is externally connected to the electronic device, the mainboard for security verification includes a verification unit and a channel management unit, the verification unit is connected to the channel
20 management unit, and the channel management unit is connected to each device to be verified, where the verification unit is configured to: after the electronic device is powered on, send a verification instruction for the device to be verified to the channel management unit; and receive configuration information, of the device to be verified, returned by the channel management unit, verify the configuration information according to verification information, of each device to be
25 verified, stored by the verification unit, and control the electronic device to start after it is

determined that the device to be verified is verified; and the channel management unit is configured to: determine the device to be verified according to the received verification instruction, obtain the configuration information of the device to be verified, and return the configuration information to the verification unit.

5 **[0005]** This specification provides a security verification method, used by a verification unit to perform security verification, where a mainboard for security verification is deployed in an electronic device, a device to be verified is disposed inside and/or a device to be verified is externally connected to the electronic device, the mainboard for security verification includes the verification unit and a channel management unit, the verification unit is connected to the channel
10 management unit, and the channel management unit is connected to each device to be verified; and the method includes: after the electronic device is powered on, sending a verification instruction for the device to be verified to the channel management unit; receiving configuration information, of the device to be verified, returned by the channel management unit; verifying the configuration information according to stored verification information of each device to be verified;
15 and after it is determined that the device to be verified is verified, controlling the electronic device to start.

[0006] This specification provides a security verification method, used by a channel management unit to perform security verification, where a mainboard for security verification is deployed in an electronic device, a device to be verified is disposed inside and/or a device to be
20 verified is externally connected to the electronic device, the mainboard for security verification includes a verification unit and the channel management unit, the verification unit is connected to the channel management unit, and the channel management unit is connected to each device to be verified; and the method includes: after the electronic device is powered on, receiving a verification instruction sent by the verification unit; determining the device to be verified
25 according to the verification instruction; and obtaining configuration information of the device to be verified, and returning the configuration information to the verification unit.

[0007] This specification provides a security verification apparatus, used by a verification unit to perform security verification, where a mainboard for security verification is deployed in an electronic device, a device to be verified is disposed inside and/or a device to be verified is
30 externally connected to the electronic device, the mainboard for security verification includes the verification unit and a channel management unit, the verification unit is connected to the channel

management unit, and the channel management unit is connected to each device to be verified; and the apparatus includes: a sending module, configured to: after the electronic device is powered on, send a verification instruction for the device to be verified to the channel management unit; a receiving module, configured to receive configuration information, of the device to be verified, returned by the channel management unit; a verification module, configured to verify the configuration information according to stored verification information of each device to be verified; and a starting module, configured to: after it is determined that the device to be verified is verified, control the electronic device to start.

[0008] This specification provides a security verification apparatus, used by a channel management unit to perform security verification, where a mainboard for security verification is deployed in an electronic device, a device to be verified is disposed inside and/or a device to be verified is externally connected to the electronic device, the mainboard for security verification includes a verification unit and the channel management unit, the verification unit is connected to the channel management unit, and the channel management unit is connected to each device to be verified; and the apparatus includes: a receiving module, configured to: after the electronic device is powered on, receive a verification instruction sent by the verification unit; a determining module, configured to determine the device to be verified according to the verification instruction; and a forwarding module, configured to: obtain configuration information of the device to be verified, and return the configuration information to the verification unit.

[0009] This specification provides a computer-readable storage medium, where the storage medium stores a computer program, and the computer program is executed by a processor to implement the above-mentioned security verification method.

[0010] The previous at least one technical solution used in this specification can achieve the following beneficial effects: This specification discloses a mainboard for security verification, a security verification method and apparatus, and a medium. A verification unit connected to a channel management unit and a channel management unit connected to each device to be verified are disposed. After an electronic device is powered on, the verification unit is controlled to send a verification instruction for the device to be verified to the channel management unit, configuration information of the device to be verified is obtained according to the received verification instruction by using the channel management unit, and the configuration information is returned to the verification unit. Then the verification unit verifies the received configuration information

according to stored verification information. After verification succeeds, the electronic device is controlled to start.

[0011] The configuration information of the device to be verified is sent by using the channel management unit to the verification unit for verification, so as to implement security verification on a device to be verified disposed inside the electronic device and/or a device to be verified externally connected to the electronic device in a start process of the electronic device, thereby ensuring information security.

BRIEF DESCRIPTION OF DRAWINGS

[0012] The accompanying drawings described here are used to provide a further understanding of this specification, and constitute a part of this specification. Example embodiments of this specification and descriptions of the embodiments are used to explain this specification, and do not constitute an inappropriate limitation on this specification. In the accompanying drawings:

[0013] FIG. 1 is a schematic structural diagram illustrating a mainboard for security verification, according to this specification;

[0014] FIG. 2A is a schematic structural diagram illustrating a mainboard for security verification, according to this specification;

[0015] FIG. 2B is a schematic structural diagram illustrating a mainboard for security verification, according to this specification;

[0016] FIG. 3 is a schematic flowchart illustrating a security verification method, according to this specification;

[0017] FIG. 4 is a schematic flowchart illustrating a security verification method, according to this specification;

[0018] FIG. 5 is a schematic structural diagram illustrating a security verification apparatus, according to this specification; and

[0019] FIG. 6 is a schematic structural diagram illustrating a security verification apparatus, according to this specification.

DESCRIPTION OF EMBODIMENTS

[0020] To make the objectives, technical solutions, and advantages of this specification clearer,

the following clearly and comprehensively describes the technical solutions of this specification with reference to specific embodiments of this specification and corresponding accompanying drawings. It is clear that the described embodiments are merely some but not all of embodiments of this specification. Based on embodiments of this specification, all other embodiments obtained
5 by a person of ordinary skill in the art without creative efforts fall within the protection scope of this specification.

[0021] At present, with development of computer technologies, peripherals, such as a network adapter, that can interact with a device in a network and/or can process data gradually increase, and deploying chips for data processing in the peripherals has become relatively universal. In this
10 case, it is becoming more common for attackers to use peripherals connected to electronic devices to attack the electronic devices to steal information. Therefore, when an electronic device is powered on and started, security verification on a peripheral connected to the electronic device has become one of problems that need to be solved in the information security field.

[0022] The technical solutions provided in the embodiments of this specification are described
15 in detail below with reference to the accompanying drawings. Embodiments of this specification will perform security verification on a peripheral of an electronic device based on a mainboard for security verification.

[0023] FIG. 1 is a schematic structural diagram illustrating a mainboard for security verification, according to this specification. The mainboard for security verification includes a
20 verification unit and a channel management unit.

[0024] In terms of hardware, in one or more embodiments provided in this specification, the verification unit and the channel management unit in the mainboard for security verification can be specifically a chip, a logic control circuit, etc. The verification unit is a TPM chip that can receive configuration information and verify the configuration information. After an electronic
25 device is powered on, the verification unit, that is, the TPM chip, is started. The verification unit obtains configuration information of each device to be verified from the channel management unit, and verifies each piece of configuration information.

[0025] The channel management unit can be a programmable digital logic chip, such as a field-programmable gate array (FPGA) chip or a complex programmable logic device (CPLD) chip.
30 The channel management unit can be connected to the verification unit for data transmission, and the channel management unit can be further connected to the device to be verified for data

transmission.

[0026] The device to be verified contains a target memory for storing host configuration information of the electronic device. The host configuration information is the most basic configuration information of the electronic device that contains a BIOS and/or a BMC. The device to be verified can be externally connected to the electronic device, for example, a printer or a network adapter, or can be disposed inside the electronic device, for example, a coprocessor such as a graphic processing unit (GPU) or a fan configured to dissipate heat.

[0027] Certainly, the previous mainboard for security verification can be deployed on a separate circuit board, or can be deployed on the same circuit board as another electronic component of the electronic device. The another electronic component can be a CPU, a GPU, a memory bank, etc. The device to be verified can be disposed on the same circuit board as the verification unit and the channel management unit, or can be disposed on a different circuit board from that of the verification unit and the channel management unit, and is connected to each other by using a busbar, an I/O bus, etc., to implement data transmission between the channel management unit and the device to be verified. Specifically, how to dispose the mainboard for security verification, a position of the mainboard for security verification in the electronic device, how to specifically connect the mainboard for security verification to the device to be verified in the electronic device, etc. can be set as needed, which is not limited in this specification.

[0028] In terms of software, in one or more embodiments provided in this specification, the verification unit can be a program that runs on a TPM chip and performs security verification on received data. The channel management unit can be a program that runs on a compilable chip and receives data and parses or forwards the data. The mainboard for security verification implements functions of each unit by running code of each unit. In addition, code of different units in this specification is mutually independent, and each unit can perform communication or data transmission with another unit or device through a predetermined data interface. Through mutually independent units, code of each unit can be iteratively updated and tested separately.

[0029] In one or more embodiments provided in this specification, the basis for implementing security verification on multiple devices to be verified by the mainboard for security verification is as follows: The verification unit is not directly connected to the device to be verified to obtain configuration information of the device to be verified, but is connected to the channel management unit, the channel management unit is connected to each device to be verified to obtain the

configuration information, and forwards the configuration information to the verification unit, and the verification unit verifies the configuration information. The channel management unit reserves multiple channels for connecting to the device to be verified. Therefore, security verification can be implemented for multiple devices to be verified when the electronic device is powered on, so as to ensure information security.

[0030] Based on this, the verification unit can obtain the configuration information of each device to be verified by using the channel management unit.

[0031] Specifically, after the electronic device is powered on, the verification unit can be awakened.

[0032] The verification unit can send a verification instruction for the device to be verified to the channel management unit after being awakened, that is, after being powered on.

[0033] The verification instruction can be sent for all devices to be verified connected to the channel management unit, or can be sent for at least a part of devices to be verified connected to the channel management unit.

[0034] Therefore, after receiving the verification instruction, the channel management unit can determine the device to be verified according to the verification instruction, obtain configuration information of the device to be verified from the device to be verified, and return the configuration information to the verification unit.

[0035] The verification unit can receive configuration information, of the at least a part of the devices to be verified, sent by the channel management unit. Each device to be verified corresponding to the received configuration information is the same as each device to be verified targeted by the previous verification instruction.

[0036] After receiving the configuration information, the verification unit can verify the received configuration information according to verification information, of each device to be verified, prestored in the verification unit.

[0037] Obtaining the host configuration information of the electronic device is used as an example. Assume that the host configuration information is a BIOS program, the verification unit can send a verification instruction for the target memory to the channel management unit. The channel management unit can determine, according to the verification instruction, the target memory for storing the BIOS program, obtain the BIOS program from the target memory, and forward the BIOS program to the verification unit.

[0038] After receiving the BIOS program, the verification unit can run the BIOS program, and determine, based on whether a running result matches a root of trust for measurement stored in the verification unit, whether verification succeeds.

[0039] Certainly, the configuration information received by the channel management unit can be the running result of the BIOS program in the target memory, the channel management unit can send the running result to the verification unit, and the verification unit verifies the running result of the BIOS program. The type and form of specific configuration information and how to measure the configuration information are relatively mature technologies currently and are not limited in this specification.

[0040] After the configuration information returned for the verification instruction is verified by the verification unit, the verification unit can control the electronic device to start.

[0041] Further, the verification unit can store a device identifier of each device to be verified, and the device to be verified can send, based on the stored device identifier, a verification instruction carrying the device identifier to the channel management unit.

[0042] After receiving the verification instruction, the channel management unit can determine, according to the device identifier carried in the verification instruction, the device to be verified corresponding to the device identifier, and send an obtaining instruction to the device to be verified.

[0043] After receiving the obtaining instruction, the device to be verified can send configuration information thereof to the channel management unit. The device to be verified can alternatively be a non-volatile memory storing the configuration information of the device to be verified. Specifically, the type of the device to be verified, how to store the configuration information, and how to obtain the configuration information from the device to be verified can be set as needed, which is not limited in this specification.

[0044] For configuration information of each device to be verified, after receiving the configuration information, the channel management unit can forward the configuration information to the verification unit according to the device identifier of the device to be verified.

[0045] The verification unit can receive the configuration information, determine, according to the device identifier corresponding to the configuration information, verification information corresponding to the device identifier from verification information separately corresponding to each piece of prestored configuration information, and then verify the device identifier based on the determined verification information.

[0046] The verification information can be a string, can be a key, or can be a predetermined rule. Specifically, the type and form of the verification information and how to verify the configuration information based on the verification information can be set as needed, which is not limited in this specification.

5 **[0047]** Further, if the electronic device itself is not trustworthy, it would be pointless to verify security of the other device to be verified, that is, it would be necessary to measure security of the other device to be verified only if the electronic device is trustworthy.

[0048] Based on this, the verification unit can first verify the host configuration information of the electronic device, and then after verification succeeds, verify configuration information of
10 the other device to be verified.

[0049] Specifically, after being powered on, the verification unit can send a first verification instruction for the target memory to the channel management unit.

[0050] The channel management unit can determine the target memory according to a device identifier in the first verification unit, obtain the host configuration information of the electronic
15 device from the target memory, and forward the host configuration information to the verification unit.

[0051] After receiving the host configuration information, the verification unit can verify the host configuration information according to stored verification information corresponding to the electronic device.

20 **[0052]** If verification fails, the verification unit can consider that the electronic device itself is not trustworthy. Therefore, in this scenario, to ensure information security and avoid further expansion of a risk, the verification unit can send warning information used to prompt that a fault exists in the host, and control the electronic device to power off and shut down.

[0053] If verification succeeds, it can be considered that the electronic device is in a trusted
25 execution environment, and security verification continues to be performed on the other device to be verified. Therefore, the verification unit can send a second verification instruction to the channel management unit according to a device identifier of the other device to be verified different from the target memory.

[0054] The channel management unit can determine, according to a device identifier in the
30 second verification instruction, a device to be verified corresponding to the device identifier. Therefore, the channel management unit can obtain peripheral configuration information of the

device to be verified, and after obtaining the peripheral information, returns the peripheral configuration information to the verification unit according to the device identifier in the second verification instruction.

[0055] The verification unit can determine, according to the device identifier carried in the peripheral configuration information, verification information corresponding to the device identifier from prestored verification information separately corresponding to each device to be verified, and verify the peripheral configuration information based on the determined verification information.

[0056] If verification fails, the verification unit can consider that the device to be verified is not trustworthy. Similarly, in this scenario, to ensure information security and avoid further expansion of a risk, the verification unit can send warning information used to prompt that a fault exists in the device to be verified, and control the electronic device to power off and shut down.

[0057] If verification succeeds, the verification unit can consider that the device to be verified is trustworthy. In this scenario, the verification unit can separately perform security verification on each of other devices to be verified, and after verification succeeds according to peripheral configuration information of each device to be verified, the electronic device can be controlled to start.

[0058] FIG. 1 describes an example in which the mainboard for security verification performs security verification on only one device to be verified disposed inside the electronic device and one device to be verified externally connected to the mainboard for security verification. Actually, there can be multiple devices to be verified disposed inside the electronic device and multiple devices to be verified externally connected to the electronic device, as shown in FIG. 2A.

[0059] FIG. 2A is a schematic structural diagram illustrating a mainboard for security verification, according to this specification. In the figure, n devices to be verified are disposed inside the electronic device, and $m-k+1$ devices to be verified are externally connected to the electronic device. Therefore, the channel management unit can be connected to a device to be verified 1 to a device to be verified n disposed inside the electronic device. Similarly, the channel management unit can be connected to a device to be verified k to a device to be verified m disposed outside the electronic device. Therefore, the verification unit can verify, by using the channel management unit, each device to be verified connected to the channel management unit.

[0060] In addition, in this specification, there may be a device to be verified that is connected

to the channel management unit through a physical interface. In an example in which the device to be verified is a network adapter and the physical interface is an Open Core Protocol (OCP) interface that satisfies the OCP standard, at least an interface unit and a peripheral memory are disposed in the network adapter, the interface unit is configured to connect to the channel management unit through the physical interface to perform data transmission, and the peripheral memory is configured to store peripheral configuration information of the device to be verified.

[0061] Therefore, when obtaining the peripheral configuration information of the device to be verified, the channel management unit needs to obtain the peripheral configuration information by using the interface unit of the device to be verified.

[0062] Further, for each interface unit, a data type transmitted in the interface unit is predefined. If an attacker obtains sensitive information from the electronic device or injects untrusted data by using the interface unit during or after starting of the electronic device, it is also impossible to ensure information security.

[0063] Based on this, before the peripheral configuration information of the device to be verified is verified, security verification needs to be further performed on the interface unit of the device to be verified.

[0064] Specifically, after the host configuration information is verified, the verification unit can send a third verification instruction for the interface unit of the device to be verified to the channel management unit.

[0065] After receiving the third verification instruction, the channel management unit can determine the interface unit in the device to be verified according to a device identifier in the third verification instruction, obtain interface configuration information of the interface unit from the interface unit, and forward the interface configuration information to the verification unit.

[0066] A memory for storing the interface configuration information corresponding to the interface unit can be disposed in the interface unit, so the interface unit can obtain the interface configuration information stored in the memory, and forward the interface configuration information to the verification unit. The memory for storing the interface configuration information of the interface unit can be connected to the interface unit, and the interface configuration information can be an execution standard corresponding to the interface, that is, a data type transmitted by each pin in the interface unit, a time for transmitting data by each pin, etc.

[0067] The verification unit can verify the interface configuration information according to

verification information, for the interface unit, stored in the verification unit, and after the interface configuration information is verified, send, to the channel management unit, a second verification instruction for a peripheral memory of the device to be verified.

[0068] The channel management unit can obtain peripheral configuration information from the peripheral memory of the device to be verified according to the second verification instruction by using the interface unit, and return the peripheral configuration information to the verification unit, so the verification unit verifies the peripheral configuration information, as shown in FIG. 2B.

[0069] FIG. 2B is a schematic structural diagram illustrating a mainboard for security verification, according to this specification. In the figure, security measurement, that is, verification, needs to be performed on a device to be verified a disposed inside the electronic device, a device to be verified b externally connected to the electronic device, and a target memory for storing the host configuration information of the electronic device. The channel management unit and the interface unit are connected by using a predetermined physical interface. The device to be verified disposed inside the electronic device, the target memory, and the channel management unit are deployed in the mainboard for security verification, and are connected by using a serial bus.

[0070] After the electronic device is powered on, the verification unit can send a first verification instruction to the channel management unit. The channel management unit can obtain the host configuration information of the electronic device from the target memory according to the first verification instruction, and send the host configuration information to the verification unit for verification.

[0071] After the host configuration information is verified, if the device to be verified b connected by using the predetermined physical interface needs to be verified, the verification unit needs to send a third verification instruction for an interface unit of the device to be verified b. The channel management unit can obtain interface configuration information of the interface unit from the interface unit according to the third verification instruction, and send the interface configuration information to the verification unit for verification. After verification succeeds, the verification unit can send a second verification instruction to the channel management unit for a peripheral memory of the device to be verified b. The channel management unit can obtain the peripheral configuration information of the device to be verified from the peripheral memory

according to the second verification instruction by using the interface unit, and return the peripheral configuration information to the verification unit for verification.

[0072] After the host configuration information is verified, if the device to be verified a connected by using the predetermined physical interface needs to be verified, the verification unit
5 can directly send a second verification instruction for the device to be verified a to the channel management unit. The channel management unit obtains peripheral configuration information of the device to be verified a according to the second verification instruction, sends the peripheral configuration information to the verification unit, and the verification unit verifies the peripheral configuration information.

[0073] Certainly, the peripheral memory in FIG. 2B can alternatively be considered as a device
10 to be verified that is connected to the channel management unit by using a predetermined interface unit. That is, the interface unit is not inside the device to be verified, but the device to be verified is connected to the channel management unit by using a peripheral interface unit. Specifically, how the device to be verified defines and connects to the interface unit can be set as needed, which is
15 not limited in this specification.

[0074] In addition, after any chip is produced, data transmission standards corresponding to its pins have been predefined. For each pin, a data transmission standard of the pin contains at least a time period for transmitting a signal by the pin. In a case in which the channel management unit uses a programmable logic chip, if the programmable logic chip still needs to perform data
20 processing after the electronic device is started, the channel management unit needs to transmit configuration information without affecting an original transmission signal of each pin.

[0075] Specifically, for each pin, the channel management unit can determine an idle time period of the pin according to a data transmission standard of the pin. Therefore, the channel management unit can transmit configuration information in the idle time period. The idle time
25 period is a predefined time period for data transmission by the pin.

[0076] Further, in this specification, each pin corresponding to the channel management unit can be multiplexed in a time division multiplexing manner to transmit configuration data. For example, the channel management unit is a chip that satisfies the Open Compute Project (OCP) standard, as shown in Table 1:

Table 1

Pins	Original signals	Multiplexed signals	I/O
OCP_A1	DATA_N	SPI_CS	I
OCP_A2	CLK	SPI1_MISO	0
OCP_A3	SLOT_ID1	CLK	I
...	...	...	...

[0077] Table 1 is a schematic table of signal multiplexing of the channel management unit provided in this specification. OCP_A1, OCP_A2, OCP_A3, and ... are different pins of the channel management unit, and the original signal is a signal type transmitted when data transmission is performed based on a data transmission standard predefined for each pin, where DATA_IN is an input signal, CLK is a clock signal, and SLOT_ID1 is an interface sequence number of the previous physical interface. One channel management device can be connected to multiple devices to be verified by using multiple physical interfaces. The multiplexed signal is a type of a signal transmitted by the channel management unit in an idle time period of the pin. SPI_CS is a chip select signal, and is used to control the channel management unit to gate a device to be verified. I/O indicates whether the pin is specifically used to receive data or send data.

[0078] Certainly, for each pin, a standard or definition manner that an original signal and a multiplexed signal of the pin conform and a specific defined type can be set as needed, which is not limited in this specification.

[0079] Further, in this specification, a channel between the channel management unit and the device to be verified generates a random signal after the electronic device is powered on, to avoid interference of the random signal to the configuration information transmitted by the channel management unit, the channel management unit can further gate, after determining a device to be verified, a channel thereof connected to the device to be verified, and obtain configuration information of the device to be verified through the channel.

[0080] Certainly, after determining a device to be verified, the channel management unit can further gate a channel thereof connected to the device to be verified, and supply power to the device to be verified, so as to wake the device to be verified, and obtain configuration information of the device to be verified through the channel after the device to be verified wakes up. As such,

impact of the random signal is avoided, and resources are saved.

[0081] In addition, currently, after the host configuration information is verified, the verification unit verifies an operating system deployed in the electronic device, and starts the operating system after verification succeeds. After the host configuration information is verified, the verification unit in this specification further needs to verify security of the other device to be verified.

[0082] Therefore, after the host configuration information is verified, the verification unit can send a suspend instruction to a control unit of the electronic device, disconnect a connection to a non-volatile storage unit storing the host configuration information, so as to delay starting of the electronic device, and send verification information to the channel management unit according to a device identifier of the device to be verified, so as to determine, according to a verification result, that both the electronic device and the device to be verified are in a trusted environment.

[0083] Therefore, after peripheral configuration information of each device to be verified is verified by the verification unit, the verification unit can determine that the electronic device and the device to be verified are in a trusted environment, and the verification unit can control the electronic device to continue to start. Then, the verification unit can send an execution instruction to the control unit of the electronic device, and connect the non-volatile storage unit storing the host configuration information, so as to continue a startup procedure of the electronic device.

[0084] Further, the electronic device can contain and/or connect to multiple devices to be verified, and priorities of the devices to be verified are not completely the same. For example, a network adapter can be preferentially verified because the network adapter can process data in the electronic device, and verification on a printer can be suspended because the printer can only perform an operation such as printing data. In addition, if verification on the network adapter fails, the verification unit can consider that a network environment of the electronic device is not trustworthy, and control the electronic device to power off and shut down. If verification on the printer fails, the verification unit can consider that the printer is not trustworthy, continue to start the electronic device, and send warning information used to prompt that the printer is abnormal.

[0085] Therefore, after the host configuration information is verified, according to predetermined priorities of devices to be verified, sequentially for each device to be verified, the verification unit can send a second verification instruction for the device to be verified to the channel management unit, and receive configuration information returned for the second

verification instruction.

[0086] When it is determined, according to the received configuration information, that the device to be verified is in a trusted environment, the verification unit can send a verification instruction to the channel management unit according to a device identifier of the next device to be verified until verification on each device to be verified is completed.

[0087] Further, when the verification unit verifies peripheral configuration information of the device to be verified, a case in which verification fails may occur because the peripheral configuration information is affected by a status of the device to be verified.

[0088] Therefore, for each device to be verified, the verification unit can send a reset instruction to the channel management unit according to a device identifier of the device to be verified.

[0089] The channel management unit can forward the reset instruction to the device to be verified.

[0090] The device to be verified restores an initial state according to the reset instruction, after restoring the initial state, the device to be verified sends peripheral configuration information thereof to the channel management unit.

[0091] The channel management unit can send the peripheral configuration information to the verification unit according to the reset instruction, and the verification unit performs security verification on the device to be verified.

[0092] The reset instruction can alternatively be sent by the verification unit according to the device identifier of the device to be verified when verification by the verification unit fails according to the peripheral configuration information. A specific sending occasion of the reset instruction can be set as needed, which is not limited in this specification.

[0093] In the mainboard for security verification as shown in FIG. 1, a verification unit connected to a channel management unit and a channel management unit connected to each device to be verified are disposed. After an electronic device is powered on, the verification unit is controlled to send a verification instruction for the device to be verified to the channel management unit, the device to be verified is determined according to the received verification instruction by using the channel management unit, configuration information of the device to be verified is obtained, and the configuration information is returned to the verification unit. Then the verification unit verifies the received configuration information according to stored verification

information. After verification succeeds, the electronic device is controlled to start. In the mainboard for security verification, the configuration information of the device to be verified is sent by using the channel management unit to the verification unit for verification, so as to implement security verification on a device to be verified disposed inside the electronic device and/or a device to be verified externally connected to the electronic device in a start process of the electronic device, thereby ensuring information security.

[0094] In addition, to ensure resource utilization, the verification unit and the channel management unit can further transmit data in a data transmission channel in a form of time division multiplexing and/or frequency division multiplexing.

[0095] Specifically, the verification unit and the channel management unit transmit first data on a first data transmission channel to implement data transmission.

[0096] Therefore, the verification unit can determine a first transmission channel used for data transmission with the channel management unit, and determine a time-frequency resource corresponding to the first transmission channel.

[0097] Then, the verification unit can determine first data for data transmission with the channel management unit, and divide the time-frequency resource of the first transmission channel according to the first data.

[0098] Finally, the verification unit can transmit each piece of first data according to the divided time-frequency resource.

[0099] When the time-frequency resource is divided according to the first data, the time-frequency resource can be divided according to a data amount included in the first data, or the time-frequency resource can be divided according to a data type included in the first data. Specifically, how to transmit data based on the form of time division multiplexing and/or frequency division multiplexing is a relatively mature technology currently. This is not limited in this specification.

[0100] Certainly, the channel management unit and each device to be verified further transmit data on a data transmission channel in the form of time division multiplexing and/or frequency division multiplexing.

[0101] Specifically, the channel management unit and each device to be verified transmit second data on a second data transmission channel, so as to implement data transmission.

[0102] Therefore, for each device to be verified, the device management unit can determine a

second transmission channel used for data transmission with the device to be verified, and determine a time-frequency resource corresponding to the second transmission channel.

[0103] Then, the device management unit can determine second data for data transmission with the device to be verified, and divide the time-frequency resource of the second transmission channel according to the second data.

[0104] Finally, the verification unit can transmit each piece of second data according to the divided time-frequency resource.

[0105] Similarly, when the time-frequency resource is divided according to the second data, the time-frequency resource can be divided according to a data amount included in the second data, or the time-frequency resource can be divided according to a data type included in the second data. Specifically, how to transmit data based on the form of time division multiplexing and/or frequency division multiplexing is a relatively mature technology currently. This is not limited in this specification.

[0106] The previous description uses a time division multiplexing/frequency division multiplexing manner to perform data transmission, so as to transmit the host configuration information and the peripheral configuration information of each device to be verified to the verification unit in less time, and complete verification on the host itself and the device to be verified in the host in a relatively short time. This ensures service execution efficiency, and avoids cases in which user satisfaction decreases and resource utilization decreases due to too long time required for starting of the electronic device.

[0107] Based on the same idea, this specification further provides a schematic flowchart of a security verification method, specifically as shown in FIG. 3.

[0108] FIG. 3 is a schematic flowchart illustrating a security verification method, according to this specification. The security verification method is used by a verification unit to perform security verification, where a mainboard for security verification is deployed in an electronic device, a device to be verified is disposed inside and/or a device to be verified is externally connected to the electronic device, the mainboard for security verification includes the verification unit and a channel management unit, the verification unit is connected to the channel management unit, and the channel management unit is connected to each device to be verified.

[0109] S100. After the electronic device is powered on, send a verification instruction for the device to be verified to the channel management unit.

[0110] S102. Receive configuration information, of the device to be verified, returned by the channel management unit.

[0111] S104. Verify the configuration information according to stored verification information of each device to be verified.

5 **[0112]** S106. After it is determined that the device to be verified is verified, control the electronic device to start.

[0113] In one or more embodiments of this specification, the security verification method can be performed by the verification unit in the mainboard for security verification. For a specific process, refer to the previous description of the verification unit in the mainboard used for security
10 verification. Details are not described in this specification.

[0114] Based on the same idea, this specification further provides a schematic flowchart of a security verification method, specifically as shown in FIG. 4.

[0115] FIG. 4 is a schematic flowchart illustrating a security verification method, according to this specification. The method is used by a channel management unit to perform security
15 verification, where a mainboard for security verification is deployed in an electronic device, a device to be verified is disposed inside and/or a device to be verified is externally connected to the electronic device, the mainboard for security verification includes the verification unit and a channel management unit, the verification unit is connected to the channel management unit, and the channel management unit is connected to each device to be verified.

20 **[0116]** S200. After the electronic device is powered on, receive a verification instruction sent by the verification unit.

[0117] S202. Determine the device to be verified according to the verification instruction.

[0118] S204. Obtain configuration information of the device to be verified, and return the configuration information to the verification unit.

25 **[0119]** In one or more embodiments of this specification, the security verification method can be performed by the channel management unit in the mainboard for security verification. For a specific process, refer to the previous description of the channel management unit in the mainboard used for security verification. Details are not described in this specification.

[0120] Based on the same idea, this specification further provides a structural diagram of a security verification apparatus, as shown in FIG. 5.
30

[0121] FIG. 5 is a schematic structural diagram illustrating a security verification apparatus,

according to this specification. The apparatus is used by a verification unit to perform security verification, where a mainboard for security verification is deployed in an electronic device, a device to be verified is disposed inside and/or a device to be verified is externally connected to the electronic device, the mainboard for security verification includes the verification unit and a channel management unit, the verification unit is connected to the channel management unit, and the channel management unit is connected to each device to be verified. The apparatus includes the following modules:

[0122] a sending module 300, configured to: after the electronic device is powered on, send a verification instruction for the device to be verified to the channel management unit;

[0123] a receiving module 302, configured to receive configuration information, of the device to be verified, returned by the channel management unit;

[0124] a verification module 304, configured to verify the configuration information according to stored verification information of each device to be verified;

[0125] and a starting module 306, configured to: after it is determined that the device to be verified is verified, control the electronic device to start.

[0126] Based on the same idea, this specification further provides a structural diagram of a security verification apparatus, as shown in FIG. 6.

[0127] FIG. 6 is a schematic structural diagram illustrating a security verification apparatus, according to this specification. The apparatus is used by a channel management unit to perform security verification, where a mainboard for security verification is deployed in an electronic device, a device to be verified is disposed inside and/or a device to be verified is externally connected to the electronic device, the mainboard for security verification includes the verification unit and a channel management unit, the verification unit is connected to the channel management unit, and the channel management unit is connected to each device to be verified. The apparatus includes the following modules:

[0128] a receiving module 400, configured to: after the electronic device is powered on, receive a verification instruction sent by the verification unit;

[0129] a determining module 402, configured to determine the device to be verified according to the verification instruction;

[0130] and a forwarding module 404, configured to: obtain configuration information of the device to be verified, and return the configuration information to the verification unit.

[0131] In the 1990s, whether improvement to a technology is hardware improvement (for example, improvement to a circuit structure like a diode, a transistor, or a switch) or software improvement (improvement to a method procedure) can be clearly identified. However, with development of technologies, improvement to many existing method procedures can be considered as direct improvement to hardware circuit structures. A designer usually programs an improved method procedure to a hardware circuit, to obtain a corresponding hardware circuit structure. Therefore, a method procedure can be improved by using a hardware entity module. For example, a programmable logic device (PLD) (for example, a field programmable gate array (FPGA)) is such an integrated circuit, and a logical function of the programmable logic device is determined by programming a component by a user. A designer autonomously performs programming to "integrate" a digital system onto a PLD, without requesting a chip manufacturer to design and manufacture a dedicated integrated circuit chip. In addition, at present, instead of manually manufacturing an integrated circuit chip, such programming is mostly implemented by using "logic compiler" software. The "logic compiler" software is similar to a software compiler used to develop and write a program. Original code needs to be written in a particular programming language before being compiled. The language is referred to as a hardware description language (HDL). There are many HDLs, such as the Advanced Boolean Expression Language (ABEL), the Altera Hardware Description Language (AHDL), Confluence, the Cornell University Programming Language (CUPL), HDCal, the Java Hardware Description Language (JHDL), Lava, Lola, MyHDL, PALASM, and the Ruby Hardware Description Language (RHDL). At present, the Very-High-Speed Integrated Circuit Hardware Description Language (VHDL) and Verilog are most commonly used. It should also be clear to a person skilled in the art that a hardware circuit for implementing a logical method procedure can be easily obtained by performing slight logic programming on the method procedure by using the previous several hardware description languages and programming the method procedure into an integrated circuit.

[0132] The controller can be implemented in any suitable manner. For example, the controller can be in a form of a microprocessor or a processor and a computer-readable medium storing computer-readable program code (for example, software or firmware) that can be executed by the (micro) processor, a logic gate, a switch, an application-specific integrated circuit (ASIC), a programmable logic controller, and an embedded microcontroller. Examples of the controller include but are not limited to the following microcontrollers: ARC 625D, Atmel AT91SAM,

Microchip PIC18F26K20, and Silicone Labs C8051F320. A storage controller can further be implemented as a part of control logic of a storage. A person skilled in the art also knows that, in addition to implementing the controller by using only computer-readable program code, logic programming can be performed on a method step, so the controller implements a same function in a form of a logic gate, a switch, an application-specific integrated circuit, a programmable logic controller, an embedded microcontroller, etc. Therefore, the controller can be considered as a hardware component, and an apparatus included in the controller for implementing various functions can also be considered as a structure in the hardware component. Or the apparatus configured to implement various functions can even be considered as both a software module implementing the method and a structure in the hardware component.

[0133] The system, apparatus, module, or unit illustrated in the previous embodiments can be implemented by using a computer chip or an entity, or can be implemented by using a product having a certain function. A typical implementation device is a computer. Specifically, the computer can be, for example, a personal computer, a laptop computer, a cellular phone, a camera phone, a smartphone, a personal digital assistant, a media player, a navigation device, an email device, a game console, a tablet computer, a wearable device, or a combination of any of these devices.

[0134] For ease of description, the above-mentioned apparatus is described by dividing functions into various units. Certainly, during implementation of this specification, functions of units can be implemented in the same or more software or hardware.

[0135] A person skilled in the art should understand that some embodiments of this specification can be provided as methods, systems, or computer program products. Therefore, this specification can use a form of hardware only embodiments, software only embodiments, or embodiments with a combination of software and hardware. In addition, a form of a computer program product that is implemented on one or more computer-usable storage media (including but not limited to a disk memory, a CD-ROM, an optical memory, etc.) that include computer-usable program code can be used in this specification.

[0136] This specification is described with reference to the flowcharts and/or block diagrams of the method, the device (system), and the computer program product based on the embodiments of this specification. It should be understood that computer program instructions can be used to implement each procedure and/or each block in the flowcharts and/or the block diagrams and a

combination of a procedure and/or a block in the flowcharts and/or the block diagrams. These computer program instructions can be provided to a processor of a general-purpose computer, a dedicated computer, an embedded processor, or other programmable data processing device to produce a machine, such that instructions executed by a processor of a computer or other programmable data processing device produce an apparatus for implementing a function specified in one or more processes of the flowchart and/or one or more blocks of the block diagram.

[0137] These computer program instructions can be stored in a computer readable memory that can instruct the computer or the another programmable data processing device to work in a specific way, so the instructions stored in the computer readable memory generate an artifact that includes an instruction apparatus. The instruction apparatus implements a specific function in one or more processes in the flowcharts and/or in one or more blocks in the block diagrams.

[0138] These computer program instructions can be loaded onto the computer or another programmable data processing device, so a series of operations and steps are performed on the computer or the another programmable device, thereby generating computer-implemented processing. Therefore, the instructions executed on the computer or the another programmable device provide steps for implementing a specific function in one or more processes in the flowcharts and/or in one or more blocks in the block diagrams.

[0139] In a typical configuration, the computing device includes one or more processors (CPU), input/output interfaces, network interfaces, and memory.

[0140] The memory may include a form such as a non-permanent memory, a random access memory (RAM), or a non-volatile memory in a computer-readable medium, for example, a read-only memory (ROM) or a flash memory (flash RAM). The memory is an example of the computer-readable medium.

[0141] The computer-readable medium includes persistent, non-persistent, movable, and unmovable media that can store information by using any method or technology. The information can be a computer readable instruction, a data structure, a program module, or other data. Examples of the storage medium of the computer include but are not limited to a phase-change memory (PRAM), a static random access memory (SRAM), a dynamic random access memory (DRAM), another type of random access memory (RAM), a read-only memory (ROM), an electrically erasable programmable read-only memory (EEPROM), a flash memory or another memory technology, a compact disc read-only memory (CD-ROM), a digital versatile disk (DVD) or

another optical storage, a magnetic cassette tape, a magnetic disk storage or another magnetic storage device, or any other non-transmission medium, which can be configured to store information accessible to a computing device. As specified in this specification, the computer-readable medium does not include transitory computer-readable media (transitory media), such as a modulated data signal and a carrier.

[0142] It should also be noted that the term "include" or any other variant thereof is intended to cover a non-exclusive inclusion, so a process, a method, a product, or a device that includes a list of elements not only includes those elements but also includes other elements that are not expressly listed, or further includes elements inherent to such a process, method, product, or device.

In a case without more restrictions, for an element limited by the statement "include a...", a process, method, product, or device that includes the element can further include another same element.

[0143] A person skilled in the art should understand that some embodiments of this specification can be provided as methods, systems, or computer program products. Therefore, a form of hardware only embodiments, software only embodiments, or embodiments with a combination of software and hardware can be used in this specification. In addition, a form of a computer program product that is implemented on one or more computer-usable storage media (including but not limited to a disk memory, a CD-ROM, an optical memory, etc.) that include computer-usable program code can be used in this specification.

[0144] This specification can be described in a general context of a computer-executable instruction executed by a computer, for example, a program module. Typically, program modules include routines, programs, objects, components, data structures, etc. that perform specific tasks or implement specific abstract data types. This specification can also be practiced in a distributed computing environment in which tasks are performed by remote processing devices connected via a communication network. In the distributed computing environment, a program module can be located in local and remote computer storage media including a storage device.

[0145] Embodiments in this specification are all described in a progressive manner, for same or similar parts in embodiments, mutual reference can be made to these embodiments, and each embodiment focuses on a difference from other embodiments. Particularly, the system embodiments are basically similar to the method embodiments, and therefore are described briefly.

For related parts, references can be made to some descriptions in the method embodiments.

[0146] The above-mentioned descriptions are merely some embodiments of this specification

and are not intended to limit this specification. A person skilled in the art can make various changes and variations to this specification. Any modification, equivalent replacement, or improvement made without departing from the spirit and principle of this specification shall fall within the scope of the claims in this specification.

CLAIMS

What is claimed is:

1. A mainboard for security verification, wherein the mainboard for security verification is deployed in an electronic device, a device to be verified is disposed inside and/or a device to be verified is externally connected to the electronic device, the mainboard for security verification comprises a verification unit and a channel management unit, the verification unit is connected to the channel management unit, and the channel management unit is connected to each device to be verified, wherein

the verification unit is configured to: after the electronic device is powered on, send a verification instruction for the device to be verified to the channel management unit; and receive configuration information, of the device to be verified, returned by the channel management unit, verify the configuration information according to verification information, of each device to be verified, stored by the verification unit, and control the electronic device to start after it is determined that the device to be verified is verified; and

the channel management unit is configured to: determine the device to be verified according to the received verification instruction, obtain the configuration information of the device to be verified, and return the configuration information to the verification unit.

2. The mainboard for security verification according to claim 1, wherein the device to be verified disposed inside the electronic device contains at least a target memory for storing host configuration information of the electronic device; and

the verification unit is configured to: after the electronic device is powered on, send, to the channel management unit, a first verification instruction carrying a device identifier of the target memory; and receive and verify host configuration information returned by the channel management unit, and send a second verification instruction to the channel management unit according to a device identifier of the other device to be verified different from the target memory after it is determined that the host configuration information is verified, until verification on each device to be verified is completed; and

the channel management unit is configured to: determine the target memory according to the device identifier carried in the first verification instruction, obtain the host configuration information from the target memory, and return the host configuration information to the

verification unit; and determine, according to a device identifier carried in the second verification instruction, a device to be verified corresponding to the device identifier, obtain peripheral configuration information from the device to be verified, and return the peripheral configuration information to the verification unit according to the second verification instruction.

5 3. The mainboard for security verification according to claim 2, wherein the device to be verified contains at least an interface unit and a peripheral memory; and the interface unit and the channel management unit are connected through a predetermined physical interface; and

the channel management unit is configured to obtain peripheral configuration information of the device to be verified from the peripheral memory by using the interface unit.

10 4. The mainboard for security verification according to claim 3, wherein the verification unit is configured to send a third verification instruction for the interface unit of the device to be verified to the channel management unit; and receive and verify interface configuration information returned by the channel management unit, and send a second verification instruction for the peripheral memory of the device to be verified to the channel management unit after it is
15 determined, according to the interface configuration information, that verification succeeds; and

the channel management unit is configured to: determine the interface unit according to the third verification instruction, obtain the interface configuration information of the interface unit, and return the interface configuration information to the verification unit; and obtain the peripheral configuration information from the peripheral memory according to the second verification
20 instruction by using the interface unit, and return the peripheral configuration information to the verification unit.

5. The mainboard for security verification according to claim 1, wherein the channel management unit is a chip predefining a data transmission standard of each pin; and

the channel management unit is configured to: for at least a part of pins, determine an idle
25 time period of the pin according to a data transmission standard of the pin, and transmit the configuration information in the idle time period, wherein the idle time period is a time period not predefined for data transmission by the pin.

6. The mainboard for security verification according to claim 2, wherein priorities of other devices to be verified than the target memory are not completely the same; and

30 the verification unit is configured to: after the host configuration information is verified, according to predetermined priorities of the other devices to be verified than the target memory,

send a second verification instruction to the channel management unit sequentially for each device to be verified according to a device identifier of the device to be verified, until verification on each device to be verified is completed.

5 7. The mainboard for security verification according to claim 1, wherein the verification unit is configured to: when it is determined, according to the received configuration information, that verification fails, determine that the electronic device is unreliable, and control the electronic device to power off and shut down.

10 8. The mainboard for security verification according to claim 1, wherein a control unit is further deployed in the electronic device, and the control unit is connected to the channel management unit;

the verification unit is configured to: after the electronic device is powered on, send, to the channel management unit, a suspend instruction used to pause starting of the electronic device; and send, to the channel management unit, a start instruction used to continue to start the electronic device after it is determined that the device to be verified is verified; and

15 the channel management unit is configured to connect to the control unit in the electronic device according to the received suspend instruction, and send the suspend instruction to the control unit, so as to pause starting of an operating system predeployed in the control unit; and send the received start instruction to the control unit, so as to start the operating system in the control unit.

20 9. The mainboard for security verification according to claim 1, wherein the verification unit is configured to send a reset instruction carrying a device identifier to the channel management unit; and

the channel management unit is configured to forward the reset instruction to a device to be verified corresponding to the device identifier according to the device identifier, so the device to be verified restores an initial state according to the reset instruction, obtains configuration information of the device to be verified after the initial state is restored, and returns the configuration information to the verification unit.

25 10. The mainboard for security verification according to claim 1, wherein the channel management unit is configured to: after the device to be verified is determined, gate a channel connected to the device to be verified, and obtain the configuration information of the device to be verified through the channel.

11. A security verification method, used by a verification unit to perform security verification, wherein a mainboard for security verification is deployed in an electronic device, a device to be verified is disposed inside and/or a device to be verified is externally connected to the electronic device, the mainboard for security verification comprises the verification unit and a channel management unit, the verification unit is connected to the channel management unit, and the channel management unit is connected to each device to be verified; and the method comprises:

after the electronic device is powered on, sending a verification instruction for the device to be verified to the channel management unit;

receiving configuration information, of the device to be verified, returned by the channel management unit;

verifying the configuration information according to stored verification information of each device to be verified; and

after it is determined that the device to be verified is verified, controlling the electronic device to start.

12. A security verification method, used by a channel management unit to perform security verification, wherein a mainboard for security verification is deployed in an electronic device, a device to be verified is disposed inside and/or a device to be verified is externally connected to the electronic device, the mainboard for security verification comprises a verification unit and the channel management unit, the verification unit is connected to the channel management unit, and the channel management unit is connected to each device to be verified; and the method comprises:

after the electronic device is powered on, receiving a verification instruction sent by the verification unit;

determining the device to be verified according to the verification instruction; and

obtaining configuration information of the device to be verified, and returning the configuration information to the verification unit.

13. A security verification apparatus, used by a verification unit to perform security verification, wherein a mainboard for security verification is deployed in an electronic device, a device to be verified is disposed inside and/or a device to be verified is externally connected to the electronic device, the mainboard for security verification comprises the verification unit and a channel management unit, the verification unit is connected to the channel management unit, and the channel management unit is connected to each device to be verified; and the apparatus

comprises:

a sending module, configured to: after the electronic device is powered on, send a verification instruction for the device to be verified to the channel management unit;

5 a receiving module, configured to receive configuration information, of the device to be verified, returned by the channel management unit;

a verification module, configured to verify the configuration information according to stored verification information of each device to be verified; and

a starting module, configured to: after it is determined that the device to be verified is verified, control the electronic device to start.

10 14. A security verification apparatus, used by a channel management unit to perform security verification, wherein a mainboard for security verification is deployed in an electronic device, a device to be verified is disposed inside and/or a device to be verified is externally connected to the electronic device, the mainboard for security verification comprises a verification unit and the channel management unit, the verification unit is connected to the channel management unit, and
15 the channel management unit is connected to each device to be verified; and the apparatus comprises:

a receiving module, configured to: after the electronic device is powered on, receive a verification instruction sent by the verification unit;

20 a determining module, configured to determine the device to be verified according to the verification instruction; and

a forwarding module, configured to: obtain configuration information of the device to be verified, and return the configuration information to the verification unit.

15 15. A computer-readable storage medium, wherein the storage medium stores a computer program, and the computer program is executed by a processor to implement the method according to claim 11 or 12.