



- (51) **International Patent Classification:**
G06F 21/50 (2013.01) *G06F 21/30* (2013.01)
- (21) **International Application Number:**
PCT/US2013/032569
- (22) **International Filing Date:**
15 March 2013 (15.03.2013)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (71) **Applicant:** INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, 95052 (US).
- (72) **Inventors:** PRAKASH, Gyan; 1525 NW Amberglen Court, Beaverton, Oregon 97006 (US). SHAHIDZADEH, Shahrokh; 16036 SW Waxwint Way, Beaverton, Oregon 97007 (US). RAMAMURTHY, Venkatesh; 3758 SE Twelve Oaks Street, Hillsboro, Oregon 97123 (US). LI, Hong; 245 Kinhead Ct, El Dorado Hills, Oregon 95762 (US). KUMAR, Mohan J.; 18680 SW Marko Lane, Aloha, Oregon 97007 (US).
- (74) **Agent:** THREADGILL, Greg Michael; International IP Law Group, P.C., C/o CPA GLOBAL, P.O. Box 52050, Minneapolis, Minnesota 52050 (US).
- (81) **Designated States** (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) **Designated States** (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,

[Continued on next page]

(54) Title: COMPUTING DEVICE SECURITY

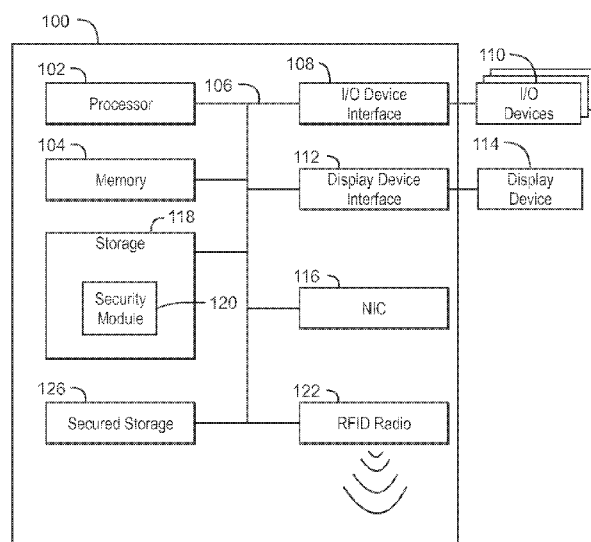


FIG. 1

(57) **Abstract:** Techniques for providing security for a computing device are described herein. In one example, a maintenance issue for the computing device is detected. Additionally, a maintenance credential proximate the computing device can be detected. Furthermore, an alarm system within the computing device can be disabled in response to detecting an authorized maintenance credential.

WO 2014/143047 A1



TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, **Published:**
ML, MR, NE, SN, TD, TG).

— *with international search report (Art. 21(3))*

COMPUTING DEVICE SECURITY

Background

Field

[0001] This disclosure relates generally to computing device security and more specifically, but not exclusively, to providing security during computing device maintenance.

Description

[0002] Data centers continue to grow in size as an increasing number of services are provided through cloud computing and other large scale networks. As a result, data centers include an increasing number of computing devices, such as servers, among others. At times, the computing devices in the data centers are physically accessed to provide maintenance such as hardware replacement, visual inspection of cables, and operating system installation.

Brief Description of the Drawings

[0003] The following detailed description may be better understood by referencing the accompanying drawings, which contain specific examples of numerous features of the disclosed subject matter.

[0004] Fig. 1 is a block diagram of an example of a computing device that can provide security during maintenance on a computing system;

[0005] Fig. 2 is a process flow diagram illustrating an example of a method for providing security during maintenance on a computing system;

[0006] Fig. 3 is a process flow diagram illustrating an example of a method for operating a security alarm during maintenance on a computing system; and

[0007] Fig. 4 is a block diagram depicting an example of a tangible, non-transitory computer-readable medium that can provide security during maintenance on a computing system.

Description of the Embodiments

[0008] According to embodiments of the subject matter described herein, a computing device can include a security module that provides security during maintenance. In some embodiments, the security module can provide security during maintenance by activating an alarm system if an unauthorized individual performs the maintenance. For example, maintenance may be performed on a computing device for any suitable maintenance issue such as routine maintenance, replacing hardware components, replacing cables, or installing new components, among others. In one embodiment, a security module can detect maintenance credentials, which verify that an authorized user is performing the maintenance on a computing device. A maintenance credential, as referred to herein, can include any suitable credential that authenticates an authorized individual such as a password, authentication token, or radio-frequency identification tag, among others.

[0009] Reference in the specification to “one embodiment” or “an embodiment” of the disclosed subject matter means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the disclosed subject matter. Thus, the phrase “in one embodiment” may appear in various places throughout the specification, but the phrase may not necessarily refer to the same embodiment.

[00010] Fig. 1 is a block diagram of an example of a computing device that can provide security during maintenance on a computing system. The computing device 100 may be, for example, a mobile phone, laptop computer, desktop computer, or tablet computer, among others. The computing device 100 may include a processor 102 that is adapted to execute stored instructions, as well as a memory device 104 that stores instructions that are executable by the processor 102. The processor 102 can be a single core processor, a multi-core processor, a computing cluster, or any number of other configurations. The memory device 104 can include random access memory, read only memory, flash memory, or any other suitable memory systems. The instructions that are executed by the processor 102 may be used to implement a method that can provide security during maintenance on a computing system.

[00011] The processor 102 may be connected through a system interconnect 106 (e.g., PCI®, PCI-Express®, HyperTransport®, NuBus, etc.) to an input/output (I/O) device interface 108 adapted to connect the computing device 100 to one or more I/O devices 110. The I/O devices 110 may include, for example, a keyboard and a pointing device, wherein the pointing device may include a touchpad or a touchscreen, among others. The I/O devices 110 may be built-in components of the computing device 100, or may be devices that are externally connected to the computing device 100.

[00012] The processor 102 may also be linked through the system interconnect 106 to a display interface 112 adapted to connect the computing device 100 to a display device 114. The display device 114 may include a display screen that is a built-in component of the computing device 100. The display device 114 may also include a computer monitor, television, or projector, among others, that is externally connected to the computing device 100. In addition, a network interface card 116, also referred to herein as NIC, may be adapted to connect the computing device 100 through the system interconnect 106 to a network (not depicted). The network (not depicted) may be a wide area network (WAN), a local area network (LAN), or the Internet, among others.

[00013] The processor 102 may also be linked through the system interconnect 106 to a storage device 118, which can include a hard drive, an optical drive, a USB flash drive, an array of drives, or any combinations thereof. The storage device 118 may include a security module 120 that can provide security while maintenance is performed on the computing device 100. For example, the security module 120 can detect information received by a radio-frequency identification radio, also referred to herein as an RFID radio 122. In one embodiment, the RFID radio 122 can detect authentication data from an RFID device 124. Authentication data, as referred to herein, can include any suitable encryption key, encryption method, or authentication credentials, among others. For example, an RFID device 124 may transmit authentication data with a particular frequency which allows maintenance to be performed on the computing device 100. In some embodiments, the security module 120 can verify that the authentication data received from the RFID device 124 through the RFID radio 122 is correct by accessing secured storage 126. The secured storage 126 can store authentication data that, when detected, prompts the security module 120 to disable an

alarm system. In some embodiments, the secured storage 126 includes non-volatile, read-only memory.

[00014] It is to be understood that the block diagram of Fig. 1 is not intended to indicate that the mobile device 100 is to include all of the components shown in Fig. 1. Rather, the computing device 100 can include fewer or additional components not illustrated in Fig. 1 (e.g., a board management controller, additional memory components, additional modules, additional network interfaces, etc.). Furthermore, any of the functionalities of the security module 120 may be partially, or entirely, implemented in hardware and/or in the processor 102. For example, the functionality may be implemented with an application specific integrated circuit, or in logic implemented in the processor 102, or in a board management controller, among others.

[00015] Fig. 2 is a process flow diagram illustrating an example of a method for providing security during maintenance on a computing system. The method 200 can be implemented with any suitable computing device, such as the computing device 100 of Fig. 1.

[00016] At block 202, the security module 120 can detect a maintenance issue for the computing device. As discussed above, a maintenance issue can include periodic maintenance such as repairing components, replacing cables or wires, or installing operating systems, among others. In some embodiments, the security module 120 may send an electronic notification, such as an email notification, among others, in response to a maintenance issue. For example, the security module 120 may detect that a hardware component is not functioning properly and the security module 120 may send a communication to another computing system or administrator that monitors the performance of the computing system.

[00017] At block 204, the security module 120 can detect a maintenance credential proximate the computing device. As discussed above, a maintenance credential can include any suitable credential that authenticates an authorized user such as a password, authentication data, or a radio-frequency identifier, among others. In some embodiments, the maintenance credential can be transmitted to the security module 120 from an RFID device through an RFID radio in the computing device. For example, a technician that is authorized to perform maintenance on the computing device may

have an RFID device, such as a badge, that can emit authentication data to the security module 120. In some embodiments, the security module 120 can verify that the authentication data received from an RFID device is accurate by accessing a secured storage device in the computing device. The secured storage device can enable the security module 120 to retrieve stored authentication data such as encryption keys, among others. In one embodiment, the secured storage may be a read-only device. Therefore, in some examples, the secured storage device may allow one write operation containing authentication data to be performed on the secured storage device. The security module 120 may then read authentication data from the secured storage device any suitable number of times.

[00018] At block 206, the security module 120 can disable an alarm system within the computing device based on an authorized maintenance credential. In some embodiments, an alarm system can alert additional computing systems, or administrators, among others of unauthorized maintenance or access to a computing device. For example, an alarm system may include sending an email or any other suitable electronic communication to an administrator that indicates an unauthorized user has accessed a computing device. In one embodiment, disabling the alarm system can prevent the security module 120 from sending a communication regarding unauthorized access of a computing device. In some embodiments, the security module 120 can also provide power to lights, such as light-emitting diodes, in response to disabling the alarm system. In one example, the lights can indicate that the computing device is to receive maintenance.

[00019] The process flow diagram of Fig. 2 is not intended to indicate that the operations of the method 200 are to be executed in any particular order, or that all of the operations of the method 200 are to be included in every case. For example, the security module 120 may detect a maintenance credential proximate the computing device before detecting a maintenance issue.

[00020] Fig. 3 is a process flow diagram illustrating an example of a method for operating a security alarm during maintenance on a computing system. The method 300 can be implemented with a computing system, such as the computing device 100 of Fig. 1.

[00021] At block 302, a security module 120 can activate an RFID radio after detecting a maintenance issue. As discussed above, a maintenance issue can include any suitable periodic maintenance on a computing device such as replacing components, or replacing cables, among others. In some embodiments, the RFID radio is activated in response to a technician entering a data center in which a computing device is stored. The RFID radio may also be activated according to a time scheduled for maintenance.

[00022] At block 304, a security module 120 detects an RFID device. An RFID device can include any device capable of emitting a radio frequency identifier. For example, an RFID device can include RFID badges, or mobile devices, among others. In some embodiments, the security module 120 may detect RFID devices within any suitable proximity of a computing device. For example, the security module 120 may detect RFID devices that are within a predetermined distance from the computing device.

[00023] At block 306, the security module 120 can determine if the RFID device includes authentication data that authorizes maintenance on a computing device. In some embodiments, the security module 120 can validate authentication data received from the RFID device. For example, the security module 120 can compare authentication data received from the RFID device to authentication data stored in secured memory in the computing device. Authentication data, as referred to herein, can include any suitable encryption key, encryption method, or authentication credentials, among others. In some examples, authentication data can be written once to the secured memory. The secured memory may not allow any additional writes to the secured memory, which can prevent modification to the stored authentication data. In some embodiments, the authentication data can include a technician personal identifier, a company identifier, and computing device identity information, among others. In one example, the computing device identity information can include any suitable alphanumeric string that identifies a computing device.

[00024] If the authentication data stored in the secured memory matches the authentication data received from the RFID device, the process flow continues at block 308. If the authentication data stored in the secured memory does not match the

authentication data received from the RFID device, the process flow continues at block 310.

[00025] At block 308, the security module 120 can activate an alarm switch. In some embodiments, the alarm switch can include a general purpose input output pin that can trigger an alarm system in response to a condition such as a computing device losing power, among others. For example, if an unauthorized user removes the power from a computing system, an alarm system may be activated. In some embodiments, a computing device may include a second power source, such as a battery, that can provide power to the security module 120. In one embodiment, the alarm switch may also trigger an alarm system if a cover is removed from a computing device, if the computing device is removed from a rack of computing devices, or if any number of cables are detached from the computing device, among others.

[00026] At block 312, the security module 120 determines if a condition has occurred that triggers the alarm system. If a condition to activate the alarm system has not occurred, the process flow returns to block 306. If a condition to activate the alarm system has occurred, the process flow continues at block 314.

[00027] At block 314, the security module 120 can activate the alarm system. In some embodiments, the alarm system can include generating an audio alarm or a haptic alarm such as a vibration. In one embodiment, the security module 120 can also transmit an electronic communication to a separate computing device or an administrator, among others. For example, the security module 120 may send an electronic communication to an administrator that includes the time of unauthorized access of a computing system and any additional information such as the hardware components or software components that are modified.

[00028] If the security module determines that an RFID device is authorized at block 306, the process flow continues at block 310. At block 310, the security module 120 can activate a maintenance signal. A maintenance signal, as referred to herein, can include any suitable display that indicates to a technician that a computing device is to receive maintenance. For example, a maintenance signal may include providing power to a light source, such as a light-emitting diode. In some embodiments, the maintenance signal can indicate to a technician which computing device is to receive

maintenance. The maintenance signal can assist the technician in locating the computing system to receive maintenance within a rack of computing systems.

[00029] At block 316, the security module 120 can deactivate the alarm switch. For example, the security module can prevent the alarm system from emitting an audio sound, or transmitting an electronic communication to another computing device, or administrator.

[00030] At block 318, the security module 120 can store a service repair log that includes maintenance details. In some embodiments, the security module 120 generates the service repair log as maintenance is performed on the computing device. The maintenance details, as referred to herein, can include the length of time to perform maintenance, the technician's personal identification, and the time of the maintenance, among others. In one embodiment, the maintenance details can also be transmitted to another computing device or an administrator, among others, after the maintenance is complete. The security module 120 can also store the order that maintenance is performed for the software and hardware components of a computing device.

[00031] At block 320, the security module 120 can disable the RFID radio in response to completed maintenance that resolves a maintenance issue. In some embodiments, disabling the RFID radio can provide additional security for the computing system because the computing system may not enable the RFID radio unless the computing system detects a maintenance issue. In one example, the alarm system may remain activated unless a maintenance issue is detected and an authorized maintenance credential is detected proximate the computing system.

[00032] The process flow diagram of Fig. 3 is not intended to indicate that the operations of the method 300 are to be executed in any particular order, or that all of the operations of the method 300 are to be included in every case. For example, the security module 120 may deactivate the alarm switch before activating the maintenance signal. Additionally, the security module 120 may also use the maintenance signal to indicate that maintenance is not performed according to a maintenance policy. For example, a maintenance policy stored in the computing device may indicate that software maintenance issues are to be repaired before hardware maintenance issues. In one embodiment, the security module 120 may notify the technician that the

maintenance policy has been violated by emitting an audio signal, changing the color of lights that display the maintenance signal, or flashing the lights that display the maintenance signal, among others.

[00033] Fig. 4 is a block diagram depicting an example of a tangible, non-transitory computer-readable medium that can provide security during maintenance on a computing system. The tangible, non-transitory, computer-readable medium 400 may be accessed by a processor 402 over a computer interconnect 404. Furthermore, the tangible, non-transitory, computer-readable medium 400 may include code to direct the processor 402 to perform the operations of the current method.

[00034] The various software components discussed herein may be stored on the tangible, non-transitory, computer-readable medium 400, as indicated in Fig. 4. For example, a security module 406 may be adapted to direct the processor 402 to provide security during maintenance on a computing system. It is to be understood that any number of additional software components not shown in Fig. 4 may be included within the tangible, non-transitory, computer-readable medium 400, depending on the specific application.

EXAMPLE 1

[00035] A method for providing security for a computing device is described herein. The method includes detecting a maintenance issue for the computing device. The method also includes detecting a maintenance credential proximate the computing device. Furthermore, the method includes disabling an alarm system within the computing device in response to detecting an authorized maintenance credential.

[00036] In some embodiments, detecting a maintenance credential proximate the computing device can include detecting a radio frequency identification device proximate the computing device, detecting the maintenance credential from the radio frequency identification device, and determining the maintenance credential authorizes maintenance to be performed on the computing device. In some examples, the maintenance credential is stored in a secured non-volatile, read-only memory in the computing device. In one embodiment, the method can include using a maintenance signal to indicate that a maintenance policy has been violated.

EXAMPLE 2

[00037] A computing device for providing security for a computing device is described herein. The computing device can include a radio-frequency identification radio to receive a maintenance credential, a processor to execute stored computer-readable instructions, and a storage device that stores computer-readable instructions. The computer-readable instructions, when executed by the processor, direct the processor to detect a maintenance issue for the computing device and detect the maintenance credential proximate the computing device. The computer-readable instructions, when executed by the processor, can also direct the processor to disable an alarm system within the computing device in response to detecting an authorized maintenance credential and deactivate the radio-frequency identification radio.

[00038] In some embodiments, the alarm system comprises sending an electronic notification to an administrator. In one example, the alarm system comprises emitting a sound indicative of unauthorized access to the computing device. Additionally, in one embodiment, the computing device can also include a secured non-volatile, read-only memory to store the maintenance credential and a light that indicates maintenance is to be performed on the computing device.

EXAMPLE 3

[00039] A non-transitory, computer-readable medium comprising a plurality of instructions for providing security for a computing device is described herein. The plurality of instructions, in response to being executed on a computing device, can cause the computing device to detect a maintenance issue for the computing device and detect the maintenance credential from a radio-frequency identification device proximate the computing device. The plurality of instructions, in response to being executed on a computing device, can also cause the computing device to disable an alarm system within the computing device in response to detecting an authorized maintenance credential. Furthermore, the plurality of instructions, in response to being executed on a computing device, can cause the computing device to deactivate a radio-frequency identification radio.

[00040] In some embodiments, the instructions cause the computing device to determine the maintenance issue is resolved, and deactivate the radio-frequency

identification radio. In one example, the instructions can also cause the computing device to store a service repair log in response to detecting the authorized maintenance credential proximate the computing device.

EXAMPLE 4

[00041] An apparatus for providing security for a computing device is described herein. The apparatus includes means for detecting a maintenance issue for the computing device and means for detecting the maintenance credential from a radio-frequency identification device proximate the computing device. The apparatus also includes means for disabling an alarm system within the computing device in response to detecting an authorized maintenance credential. Furthermore, the apparatus includes means for deactivating a radio-frequency identification radio.

[00042] In some embodiments, the apparatus includes means for determining the maintenance issue is resolved, and means for deactivating the radio-frequency identification radio. In one example, the apparatus includes means for storing a service repair log in response to detecting the authorized maintenance credential proximate the computing device.

[00043] Although an example embodiment of the disclosed subject matter is described with reference to block and flow diagrams in Figs. 1-4, persons of ordinary skill in the art will readily appreciate that many other methods of implementing the disclosed subject matter may alternatively be used. For example, the order of execution of the blocks in flow diagrams may be changed, and/or some of the blocks in block/flow diagrams described may be changed, eliminated, or combined.

[00044] In the preceding description, various aspects of the disclosed subject matter have been described. For purposes of explanation, specific numbers, systems and configurations were set forth in order to provide a thorough understanding of the subject matter. However, it is apparent to one skilled in the art having the benefit of this disclosure that the subject matter may be practiced without the specific details. In other instances, well-known features, components, or modules were omitted, simplified, combined, or split in order not to obscure the disclosed subject matter.

[00045] Various embodiments of the disclosed subject matter may be implemented in hardware, firmware, software, or combination thereof, and may be described by

reference to or in conjunction with program code, such as instructions, functions, procedures, data structures, logic, application programs, design representations or formats for simulation, emulation, and fabrication of a design, which when accessed by a machine results in the machine performing tasks, defining abstract data types or low-level hardware contexts, or producing a result.

[00046] Program code may represent hardware using a hardware description language or another functional description language which essentially provides a model of how designed hardware is expected to perform. Program code may be assembly or machine language or hardware-definition languages, or data that may be compiled and/or interpreted. Furthermore, it is common in the art to speak of software, in one form or another as taking an action or causing a result. Such expressions are merely a shorthand way of stating execution of program code by a processing system which causes a processor to perform an action or produce a result.

[00047] Program code may be stored in, for example, volatile and/or non-volatile memory, such as storage devices and/or an associated machine readable or machine accessible medium including solid-state memory, hard-drives, floppy-disks, optical storage, tapes, flash memory, memory sticks, digital video disks, digital versatile discs (DVDs), etc., as well as more exotic mediums such as machine-accessible biological state preserving storage. A machine readable medium may include any tangible mechanism for storing, transmitting, or receiving information in a form readable by a machine, such as antennas, optical fibers, communication interfaces, etc. Program code may be transmitted in the form of packets, serial data, parallel data, etc., and may be used in a compressed or encrypted format.

[00048] Program code may be implemented in programs executing on programmable machines such as mobile or stationary computers, personal digital assistants, set top boxes, cellular telephones and pagers, and other electronic devices, each including a processor, volatile and/or non-volatile memory readable by the processor, at least one input device and/or one or more output devices. Program code may be applied to the data entered using the input device to perform the described embodiments and to generate output information. The output information may be applied to one or more output devices. One of ordinary skill in the art may appreciate that embodiments of the

disclosed subject matter can be practiced with various computer system configurations, including multiprocessor or multiple-core processor systems, minicomputers, mainframe computers, as well as pervasive or miniature computers or processors that may be embedded into virtually any device. Embodiments of the disclosed subject matter can also be practiced in distributed computing environments where tasks may be performed by remote processing devices that are linked through a communications network.

[00049] Although operations may be described as a sequential process, some of the operations may in fact be performed in parallel, concurrently, and/or in a distributed environment, and with program code stored locally and/or remotely for access by single or multi-processor machines. In addition, in some embodiments the order of operations may be rearranged without departing from the spirit of the disclosed subject matter. Program code may be used by or in conjunction with embedded controllers.

[00050] While the disclosed subject matter has been described with reference to illustrative embodiments, this description is not intended to be construed in a limiting sense. Various modifications of the illustrative embodiments, as well as other embodiments of the subject matter, which are apparent to persons skilled in the art to which the disclosed subject matter pertains are deemed to lie within the scope of the disclosed subject matter.

Claims

What is claimed is:

1. A method for providing security for a computing device comprising:
detecting a maintenance issue for the computing device;
detecting a maintenance credential proximate the computing device; and
disabling an alarm system within the computing device in response to detecting an authorized maintenance credential.
2. The method of claim 1, wherein detecting a maintenance credential proximate the computing device comprises:
detecting a radio frequency identification device proximate the computing device;
detecting the maintenance credential from the radio frequency identification device; and
determining the maintenance credential authorizes maintenance to be performed on the computing device.
3. The method of claims 1 or 2, wherein the alarm system comprises sending an electronic notification to an administrator.
4. The method of claims 1 or 2, wherein the alarm system comprises emitting a sound indicative of unauthorized access to the computing device.
5. The method of claims 1 or 2 comprising storing a service repair log in response to detecting the authorized maintenance credential proximate the computing device.
6. The method of claims 1 or 2, wherein the maintenance credential is stored in a secured non-volatile, read-only memory in the computing device.

7. The method of claims 1 or 2 comprising displaying a light that indicates maintenance is to be performed on the computing device.

8. The method of claims 1 or 2 comprising:
determining the maintenance issue is resolved; and
deactivating a radio frequency identification radio.

9. The method of claims 1 or 2 comprising using a maintenance signal to indicate that a maintenance policy has been violated.

10. A computing device for providing security for a computing device comprising:
a radio-frequency identification radio to receive a maintenance credential;
a processor to execute stored computer-readable instructions; and
a storage device that stores computer-readable instructions that, when executed by the processor, direct the processor to:
detect a maintenance issue for the computing device;
detect the maintenance credential proximate the computing device;
disable an alarm system within the computing device in response to detecting an authorized maintenance credential; and
deactivate the radio-frequency identification radio.

11. The computing device of claim 10, wherein the computer-readable instructions direct the processor to:
detect a radio frequency identification device proximate the computing device;
detect the maintenance credential from the radio frequency identification device;
and
determine the maintenance credential authorizes maintenance to be performed on the computing device.

12. The computing device of claims 10 or 11, wherein the alarm system comprises sending an electronic notification to an administrator.

13. The computing device of claims 10 or 11, wherein the alarm system comprises emitting a sound indicative of unauthorized access to the computing device.

14. The computing device of claims 10 or 11, wherein the computer-readable instructions direct the processor to store a service repair log in response to detecting the authorized maintenance credential proximate the computing device.

15. The computing device of claims 10 or 11 comprising a secured non-volatile, read-only memory to store the maintenance credential.

16. The computing device of claims 10 or 11 comprising a light that indicates maintenance is to be performed on the computing device.

17. The computing device of claims 10 or 11, wherein the computer-readable instructions direct the processor to:

determine the maintenance issue is resolved; and
deactivate the radio-frequency identification radio.

18. An apparatus for providing security for a computing device comprising:

means for detecting a maintenance issue for the computing device;
means for detecting the maintenance credential from a radio-frequency
identification device proximate the computing device;
means for disabling an alarm system within the computing device in response to
detecting an authorized maintenance credential; and
means for deactivating a radio-frequency identification radio.

19. The apparatus of claim 18, comprising:
means for detecting a radio frequency identification device proximate the
computing device;
means for detecting the maintenance credential from the radio frequency
identification device; and
means for determining the maintenance credential authorizes maintenance to be
performed on the computing device.
20. The apparatus of claims 18 or 19, comprising means for sending an
electronic notification to an administrator.
21. The apparatus of claims 18 or 19, comprising means for storing a service
repair log in response to detecting the authorized maintenance credential proximate the
computing device.
22. The apparatus of claims 18 or 19, comprising:
means for determining the maintenance issue is resolved; and
means for deactivating the radio-frequency identification radio.

1/4

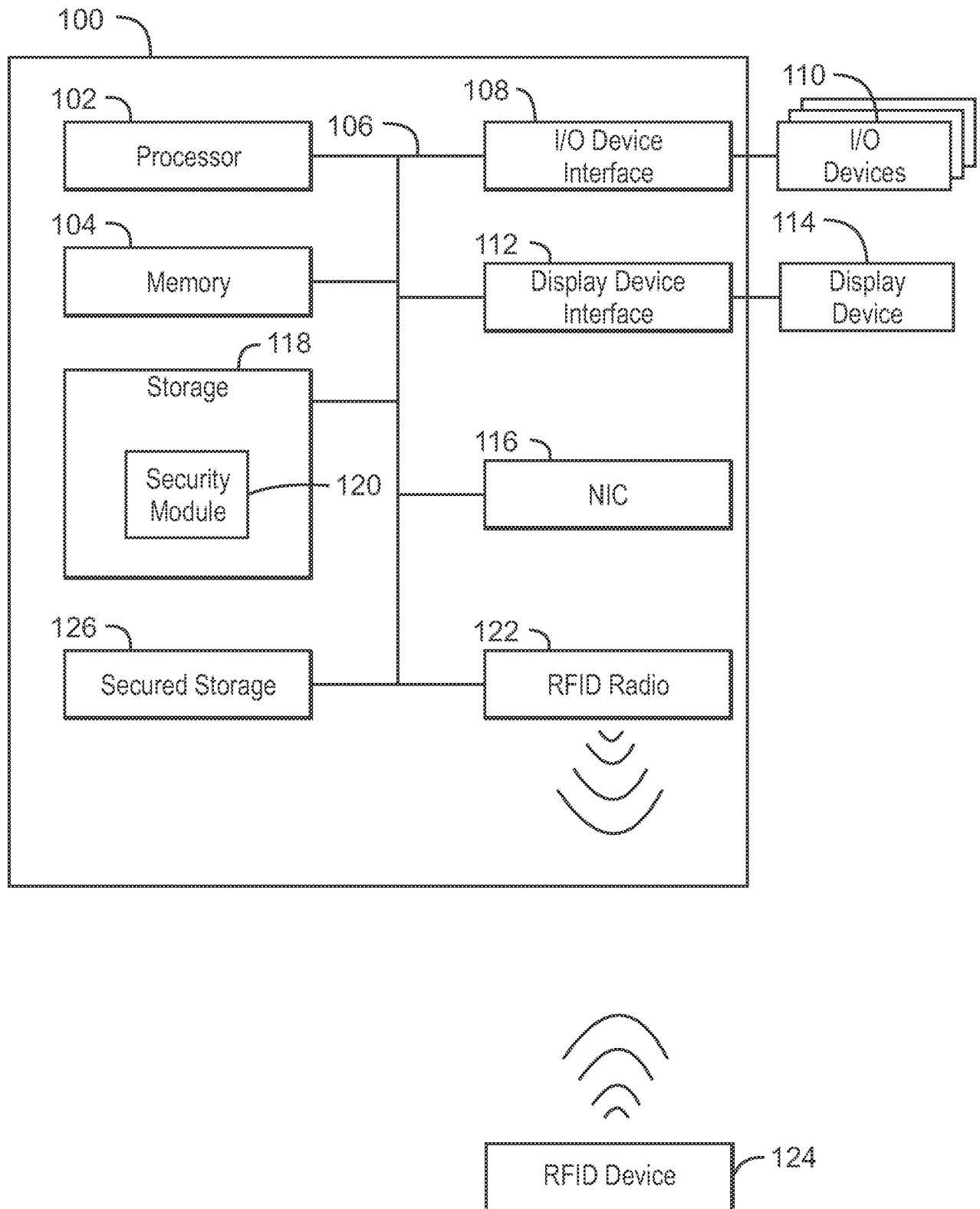
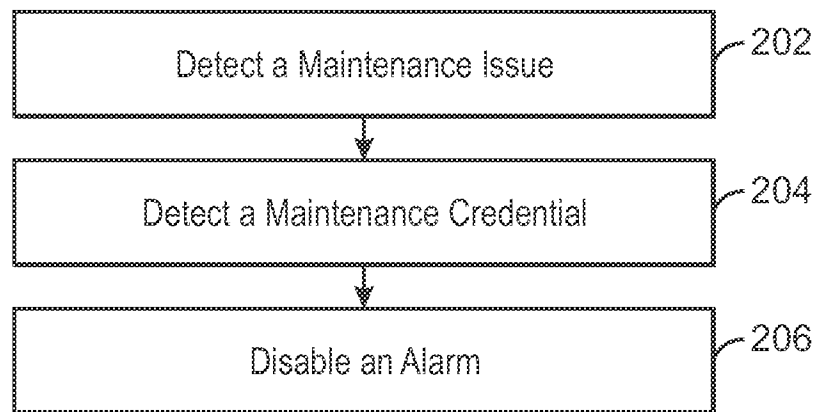


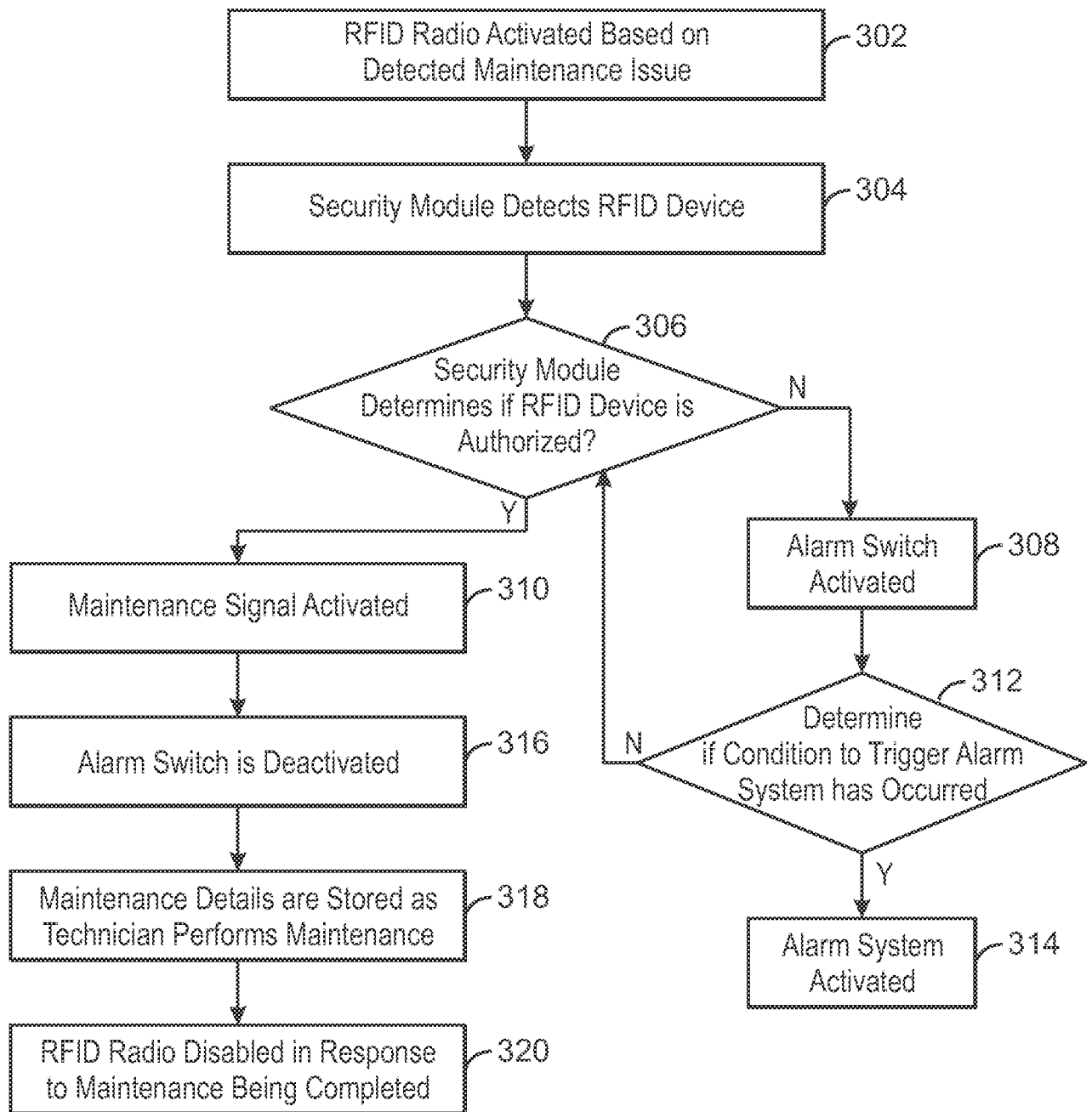
FIG. 1

2/4



200
FIG. 2

3/4



300
FIG. 3



4/4

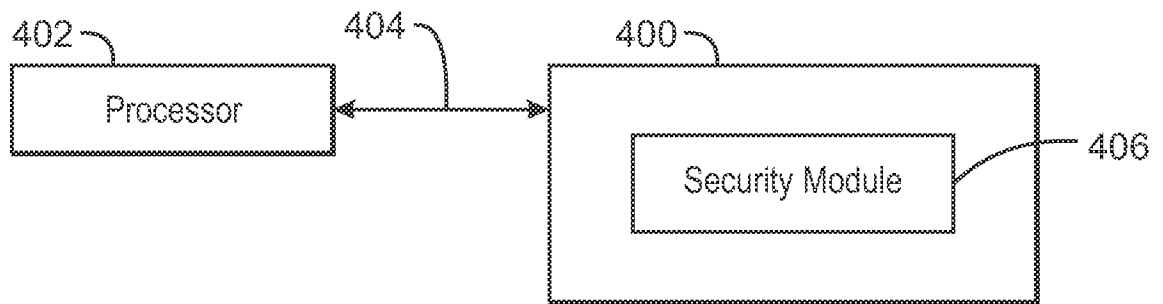


FIG. 4



INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2013/032569**A. CLASSIFICATION OF SUBJECT MATTER****G06F 21/50(2013.01)i, G06F 21/30(2013.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/50; G06F 17/00; H04M 11/04; H04L 29/06; H04L 9/32; G06K 17/00; G06K 19/07; B66B 5/00; G08B 25/00; G06F 7/04; G06F 21/00; G06F 21/30

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: security, computing device, maintenance credential, alarm system, RFID

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 7607014 B2 (THANE MICHAEL LARSON et al.) 20 October 2009 See column 5, line 47 - column 8, line 42; and figures 3-4.	1-6, 8, 10-15, 17-22
A		7, 9, 16
Y	KR 10-0813288 B1 (KONKUK UNIVERSITY INDUSTRIAL COOPERATION CORP.) 13 March 2008 See paragraphs 21-54; and figures 1, 3.	1-6, 8, 10-15, 17-22
A	US 2008-0283342 A1 (ROMEO DEPLAZES et al.) 20 November 2008 See paragraphs 4-12, 18-63; and figure 2.	1-22
A	KR 10-2009-0001248 A (E.M.W. ANTENNA CO., LTD.) 08 January 2009 See paragraphs 29-50; and figures 3-4.	1-22
A	KR 10-2011-0101601 A (JI YONG DO) 16 September 2011 See paragraphs 15-28; and figures 1-3.	1-22



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

13 December 2013 (13.12.2013)

Date of mailing of the international search report

13 December 2013 (13.12.2013)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City,
302-701, Republic of Korea

Facsimile No. +82-42-472-7140

Authorized officer

BYUN, Sung Cheal

Telephone No. +82-42-481-8262



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2013/032569

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 7607014 B2	20/10/2009	GB 0611342 D0 GB 2427951 A GB 2427951 B JP 04461119 B2 JP 2007-012050 A US 2007-0004381 A1	19/07/2006 10/01/2007 06/01/2010 12/05/2010 18/01/2007 04/01/2007
KR 10-0813288 B1	13/03/2008	CN 101437723 A CN 101437723 B EP 2013082 A1 JP 2009-535728 A KR 10-0673249 B1 US 2009-0184452 A1 WO 2007-129836 A1	20/05/2009 06/07/2011 14/01/2009 01/10/2009 22/01/2007 23/07/2009 15/11/2007
US 2008-0283342 A1	20/11/2008	AU 2005-304247 A1 AU 2005-304247 B2 BR PI0518023 A CA 2583131 A1 CN 101048330 A CN 101048330 B EP 1814813 A1 EP 1814813 B1 JP 2008-518863 A MX 2007005538 A US 8028807 B2 WO 2006-050626 A1	18/05/2006 14/07/2011 28/10/2008 18/05/2006 03/10/2007 31/08/2011 08/08/2007 28/08/2013 05/06/2008 21/05/2007 04/10/2011 18/05/2006
KR 10-2009-0001248 A	08/01/2009	None	
KR 10-2011-0101601 A	16/09/2011	KR 10-1080522 B1	04/11/2011