(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 November 2012 (01.11.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/148426 A1

(51) International Patent Classification:
G06F 9/06 (2006.01) *G06F 9/44* (2006.01)

(21) International Application Number:
PCT/US2011/034673

(22) International Filing Date:
29 April 2011 (29.04.2011)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.** [US/US]; 11445 Compaq Center Drive W., Houston, Texas 77070 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **KNAPTON, Edward D.** [US/US]; 11445 Compaq Center Dr W., Houston, Texas 77070 (US).

(74) Agents: **ORTEGA, Arthur** et al.; Hewlett-Packard Comapny, Intellectual Property Administration, 3404 East Harmony Road Mail Stop 35, Fort Collins, Colorado 80528 (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, 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, PE, PG, PH, PL, PT, RO, RS, RU, 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.

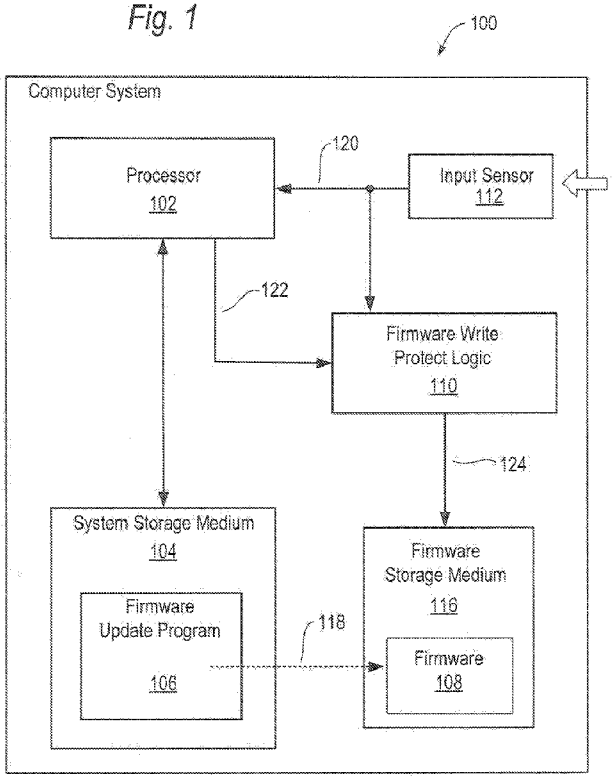
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, 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: COMPUTER SYSTEM FIRMWARE UPDATE

(57) Abstract: Techniques to update firmware include an input sensor to provide a signal and a processor to execute an update program to initiate update of firmware, if the signal is provided from the input sensor and the processor does not provide the signal from execution of the instructions of the update program.

Fig. 1



WO 2012/148426 A1

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

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i))*

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

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

COMPUTER SYSTEM FIRMWARE UPDATE

BACKGROUND

[0001] Some computer systems, such as laptop or notebook computers, may contain firmware which refers to software instructions for controlling the operation of hardware components associated with the computer systems. For example, some computer systems may include non-volatile storage medium for storing a basic input/output system (BIOS) which includes software instructions to check that hardware components within the computer systems are working properly. There are occasions in which it may be desirable to update firmware such as when a new version of the firmware is released to correct problems or improve operation.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] Figure 1 is a block diagram of an example computer system to update firmware.

[0003] Figure 2 is a perspective view of an example computer system to update firmware.

[0004] Figure 3 is a perspective view of another example computer system to update firmware.

[0005] Figure 4 is an example of a flow diagram illustrating a method to update firmware on a computer system.

DETAILED DESCRIPTION

[0006] As explained above, some computer systems, such as laptop or notebook computers, may contain firmware. Such firmware can be referred to as software instructions for controlling the operation of hardware components associated with the computer systems. For example, some computer systems may include non-volatile storage medium for storing a basic input/output system (BIOS) which can include software instructions to check that hardware components within the computer systems are working properly. There are occasions in which it may be desirable to update firmware such as when a new version of the firmware is released to correct problems or improve operation.

[0007] However, problems may be encountered when updating firmware on computer systems. For example, a user may receive a firmware update program to update firmware on computer systems. However, it may be difficult to verify the authenticity of the source of the update program and the program may proceed to update the firmware even though it was not authorized to perform the update. This update program may be an unauthorized program and may introduce undesirable code into the firmware such as a virus which may destroy data on the computer systems or otherwise render the computer systems inoperable. Therefore, it may be desirable to develop techniques for improving the authentication and verification process of updating firmware on computer systems.

[0008] The present application in some examples may provide techniques to help address problems related to authentication and verification of updating firmware on computer systems. For example, the present application describes a computer system with a means of requiring user input to enable a firmware update program to proceed to update firmware on the computer system. In one example, a computer system can be configured with a processor to execute a firmware update program, if a signal is provided from an input sensor, to initiate update of firmware wherein the processor does not provide the signal from execution of the update program. In other words, the firmware is updated if the user causes the input sensor to generate a signal as a result of the user activating the sensor. The input signal is generated by hardware and not by software by the processor executing software instructions; because a signal generated by execution of software could be generated by unauthorized software. The input sensor can detect the presence of the user and the computer can check this signal before it proceeds to update the firmware.

[0009] In one example, the computer system can be a laptop computer with a display member rotatably coupled to a base member. The computer system can include an input sensor that can detect the relative position of the display member to the base member and can detect when the computer system is in the closed position, that is, when the computer display member and the base member are in close proximity or in a predefined position to each other. The computer system can prompt the user to place the computer system in the closed position which can

allow the computer system to proceed to update the firmware. The computer system will not update firmware while the computer system is in the open position; it requires the user to place the computer system in the closed position. That is, it requires the user to take some action before the computer system can proceed to update the firmware. Therefore, these techniques require input from a user before updating the firmware which may help reduce the likelihood of unauthorized firmware updates.

[0010] Figure 1 is a block diagram of an example computer system 100 to update firmware 108 on the computer system based on input from an input sensor 112. The computer system 100 includes firmware storage medium 116 can store firmware 108 which may include software instructions executable by processor 102 to manage hardware components of the computer system. The computer system 100 includes system storage medium 104 to store a firmware update program 106 which can include software instructions executable by processor 102 to update firmware 108 with firmware from the update program as shown by dashed arrow 118.

[0011] The input sensor 112 can be any sensor device that can generate an input signal 120 in response to detection of the physical presence of a user. For example, input sensor can be any sensor device that requires a user to take some action to activate the sensor. In one example, computer system 100 can be a laptop computer with a display member rotatably coupled to a base member. In this case, the input sensor 112 can be a switch which can detect the position of the

display member relative to the base member. The input sensor 112 can generate input signal 120 indicating when the laptop has been placed in a closed position (or a predetermined relative position) by a user. As explained in further detail below, computer system can be configured to update firmware 108 when the computer system 100 is placed in the closed position by the user. The computer system 100 can be prevented from updating firmware 108 when the computer system is in the open position.

[0012] The input signal 120 is shown as being fed to both processor 102 and firmware write protect logic 110. The processor 102 generates a write signal 122 directed to write protect logic 110 indicating that the processor desires to write to firmware storage medium 116 and firmware 108. The firmware write protect logic 110 generates a write enable signal 124 directed to firmware storage 116 to enable processor 102 to initiate update of firmware 108. The write enable signal 124 can be generated based on input signal 120 (which indicates the presence of a user or activation of the sensor by a user) and write signal 122 (which indicates that processor 102 desires writing to firmware storage medium 116).

[0013] As explained below in further detail, processor 102 can execute instructions of update program 106 to initiate update of firmware 108 if input sensor 112 generates input signal 120 based on user activation of the input sensor. That is, input signal 120 can be generated as a result of the physical presence of the user and not by the processor executing instructions of a program. The update program 106 can check for the presence of input signal 120 before proceeding to

initiate the update of firmware 108. In other words, computer system 100 initiates update of firmware 108 when a user causes a signal to be generated from the input sensor and not as result of the processor executing the instructions of update program, as explained below in further detail. These techniques require user input before the update of firmware can occur which may reduce likelihood of unauthorized firmware updates.

[0014] As explained above, update program 106 can check for the presence of input signal 120 before proceeding to initiate the update of firmware 108. In another example, update program 106 can initiate update of firmware without checking for the presence of input signal 120. In this case, update program 106 can initiate the update of firmware 108 by starting to copy or write a portion of the new firmware from the update program 106 to firmware 108. The update program 106 can check whether the update was successful by verifying whether firmware 108 was updated by reading back the portion that was written. This example relies on using write protect logic 110 and whether input signal 120 has been generated. If input signal 120 was not generated, then write enable signal 124 is not enabled which prevents computer system 100 from performing a write operation to firmware 108 and therefore prevent an update to firmware 108. On the other hand if input signal 120 was generated, then write enable signal 124 is enabled which allows computer system 100 to perform a write operation to firmware 108 and therefore update firmware 108.

[0015] Although not shown, computer system 100 can include other hardware components such as a keyboard, a hard disk drive, a graphics video controller, a audio controller, a display device, a communication system and other components for operation of the computer system.

[0016] Although not shown, system storage medium 104 may include other programs or applications having instructions executable by processor 102 to control the operation of computer system 100. For example, system storage 104 may store an operating system (OS) which can include instructions when executed by the processor to control the operation of computer system 100. The OS (not shown) may include software (programs and data) that can manage computer hardware components and provide common services for execution of various application programs. In one example, the OS can be stored on a hard disk drive or other storage device and then loaded into system storage 104 after the completion of the execution of firmware 108. Although a single storage medium component 104 is shown, it should be understood that more than one memory component may be employed by computer system 100.

[0017] The firmware 108 can include software instructions for controlling the operation of hardware components, such as a display device, associated with computer system 100. For example, firmware 108 can be a basic input/output system (BIOS) which can include software instructions to check that hardware components within the computer system are working properly. Likewise, although a single firmware storage medium component 116 is shown, it should be

understood that more than one memory component may be employed by computer system 100. The memory components 104 and 116 can comprise computer-readable medium such as volatile memory (e.g., random access memory, etc.), non-volatile storage (e.g., read only memory, Flash memory, CD ROM, etc.), and combinations thereof.

[0018] The processor 102 can be any hardware or logic configured to execute software instructions. Although a single processor 102 is shown, it should be understood that more than one processor may be employed by computer system 100. For example, computer system 100 may include a processor for controlling the overall operation of the device and a keyboard controller for controlling the operation of the keyboard. The keyboard controller can be a device which interfaces a keyboard to the computer system.

[0019] Figure 2 shows a perspective view of an example computer system 100 of Figure 1. In the example illustrated in Figure 2, computer system 100 comprises a laptop or notebook computer. However, it should be understood that computer system 100 may comprise other types of computer devices such as, but not limited to, tablet personal computers, mobile phones and other types of portable and/or handheld computing devices. In the example illustrated in Figure 1, computer system 100 comprises a display member 130 rotatably coupled to a base member 132 by hinges 128. The components of computer system 100 shown in Figure 1 can be disposed in base member 132, display member 130 or a combination thereof.

[0020] In the example illustrated in Figure 2, computer system 100 shows an input sensor 112 which can be used to detect the presence of a user and to generate input signal 120 (Figure 1) in response thereto. The input sensor 112 requires a user to some take action to activate the sensor for the sensor to generate signal 120. As explained below, to allow computer system 100 to update firmware, a user can rotate display member 130 relative to base member 132 to activate input sensor 112. The input sensor 112 comprises a switch 140 for detecting a position of display member 130 relative to base member 132. The switch 140 comprises a depressable button 142 biased to extend at least partially upward through an opening 138 on a working surface 144 of base member 132 and retract at least partially into base member 132 in response to contact therewith by display member 130 (e.g., contact resulting from display member 130 being moved from an open position as illustrated in Figure 2 toward and/or into a closed position relative to base member 132 as generally shown by arrow 136). However, it should be understood that button 142 may be otherwise located (e.g., elsewhere on working surface 144, a reversed position where button 142 is located on display member 130, etc.). Further, it should be understood that other devices and/or mechanisms may be used instead of button 142 (e.g., a contact element, mechanical toggle, etc.).

[0021] The computer system 100 can employ input sensor 112 to detect the presence of a user and, in response, to allow firmware to be updated. For example, in operation, computer system 100 can execute instructions of firmware

update program 106 which can provide a prompt to a display of display member 130 to request whether a user desires to update firmware 108. The prompt may instruct the user to place the laptop in the closed position as explained below. Figure 2 shows the computer system 100 in the open position. The user can respond to the prompt by rotating display member 130 in the direction indicated by arrow 136 toward base member 132 to a closed and/or predetermined position or arrangement relative to base member, display member 130 approaches base member 132 and engages button 142, thereby actuating switch 140. Actuation of switch 140 causes input signal 120 to be generated which computer system 100 uses to enable or permit the update of firmware 108. In other examples, actuation of switch 140 can cause an interrupt and/or other type of signal to be generated and/or otherwise processed via hardware, software and/or a combination thereof of computer system 100.

[0022] Thus, in operation, once computer system 100 is closed (e.g., display member 130 is brought within a predetermined arrangement, distance and/or position relative to base member 132), computer system 100 can allow the update of firmware 108 to proceed. The computer system 100 can generate an alert or prompt when firmware 108 has completed being updated. At this point, the user can place computer system 100 back to the open position by rotating the display member 130 in the direction indicated by arrow 134 away from base member 132 to an opened and/or predetermined position or arrangement relative to base

member, display member 130 moving away from base member 132 and disengages button 140.

[0023] Figure 3 shows a perspective view of another example of computer system 100 of Figure 1. In the example illustrated in Figure 3, computer system 100 comprises another example input sensor 112. The input sensor 112 is shown to include a switch 164 having a sensor element 166 disposed in base member 132 and a sensor element 168 disposed in display member 130. In operation, input sensor 112 can generate input signal 120 (Figure 1) to allow computer system 100 to update firmware 108. In other examples, input sensor 112 can generate an interrupt and/or transmit a signal generated and/or otherwise processed via hardware, software and/or a combination thereof of computer system 100 to allow firmware updates in response to sensor elements 166 and 168 being positioned within a predetermined distance and/or in close proximity to each other. Computer system 100 does not generate input signal 120 when in an opened position as shown in Figure 1. The computer system 100 generates input signal 120 when computer system is in the closed position. Accordingly, computer system 100 can be in a closed position, that is, when display member 130 is in the closed and/or in another predetermined arrangement or position relative to base member 132, computer system 100 can allow firmware updates to proceed on the computer system.

[0024] In the example illustrated in Figure 3, sensor element 166 comprises a reed switch 160 and sensor element 168 comprises a magnet 162 such that reed

switch 160 is actuated in response to a magnetic field generated by magnet 162. Accordingly, actuation of reed switch 160 causes input signal 120 to be generated to allow computer system to update firmware 108. It should also be understood that the location and/or position of reed switch 160 and magnet 162 may be otherwise reversed (e.g., reed switch 160 located in display member 130 and magnet 162 located in base member 132). Additionally, it should be understood that other types of non-mechanical sensor elements may be used in input sensor 112 for detecting the positioning of display member 130 relative to base member 132.

[0025] Although the above has described input sensor 112 in the context of a sensor that can detect the position of a display member relative to a base member, it should be understood that input sensor 112 can take other forms and functions. For example, input sensor 112 can be a biometric sensor which can receive biometric information from a user and verify the identity of the user before allowing computer system 100 to update firmware 108

[0026] Figure 4 is an embodiment of a flow diagram 400 illustrating a method to update firmware 108 on computer system 100. The computer system 100 can begin the method at block 402 by generating a prompt to a user to inquire whether the user desires to update firmware 108. For example, computer system 100 can execute instructions of update program 106 to generate a prompt on a display of computer system inquiring whether a user desires to update firmware 102. However, it should be understood that other means of prompting the user can be

employed such as an audio indicator (e.g., sound pattern), visual indicator (e.g., light pattern) or the like.

[0027] At block 404, computer system 100 can check whether the user desires to update firmware 108 in response to the prompt. The user can respond to the prompt using any input means such as entering input through a keyboard of the computer system. If the user does not desire to proceed with an update to firmware 108, then processing can terminate by proceeding to the exit block. On the other hand, if the user desires to proceed with an update of firmware 108 then processing proceeds to block 406.

[0028] At block 406, computer system 100 can generate a prompt to the user requesting that the user activate input sensor 112 to proceed with the update of firmware 108. For example, computer system 100 can execute instructions of update program 106 to generate a prompt on a display instructing that the user place computer system 100 in the closed position by rotating display member 130 towards base member 132.

[0029] Processing proceeds to block 408 which may include having computer system 100 check whether the user has activated input sensor 112. For example, update program 106 can check whether the user placed computer system in the closed position by checking for the occurrence of input signal 120. If input signal 120 has not been generated, then processing can proceed back to block 406 to keep checking for the generation of the input signal. A timeout period can be employed to handle a condition when the signal is not generated within the timeout

period. On the other hand, if input signal 120 has been generated, then processing can proceed to block 410.

[0030] In another example, computer system 100 can initiate update of firmware without checking input signal. In this case, computer system 100 can execute instructions of update program 106 to initiate the update of firmware 108 by starting to copy or write a portion of the new firmware from the update program to firmware 108. The update program 106 can check whether the update was successful by verifying whether firmware 108 was updated by reading back the portion that was written. This example relies on using write protect logic 110 and whether input signal 120 has been generated. If input signal 120 was not generated, then write enable signal 124 is not enabled which prevents computer system 100 from performing a write operation to firmware 108. On the other hand, if input signal 120 was generated, then write enable signal 124 is enabled which allows computer system 100 to perform a write operation to firmware 108.

[0031] At block 410, computer system 100 can proceed to initiate update of firmware 108. For example, update program 106 can begin to initiate the update of firmware 108 by updating one or more portions of firmware 108 as necessary. In some examples, update program 106 can verify whether the update of firmware 108 was successful by reading back the portion that was written and comparing the two portions to each other.

[0032] The components of computer system 100 can be implemented with machine-readable instructions that are loaded for execution on processor(s). A

processor can include a microprocessor, microcontroller, processor module or subsystem, programmable integrated circuit, programmable gate array, or another control or computing device.

[0033] Data and instructions can be stored in respective storage devices, which are implemented as one or more computer-readable or machine-readable storage media. The storage media include different forms of memory including semiconductor memory devices such as dynamic or static random access memories (DRAMs or SRAMs), erasable and programmable read-only memories (EPROMs), electrically erasable and programmable read-only memories (EEPROMs) and flash memories; magnetic disks such as fixed, floppy and removable disks; other magnetic media including tape; optical media such as compact disks (CDs) or digital video disks (DVDs); or other types of storage devices. Note that the instructions discussed above can be provided on one computer-readable or machine-readable storage medium, or alternatively, can be provided on multiple computer-readable or machine-readable storage media distributed in a large system having possibly plural nodes. Such computer-readable or machine-readable storage medium or media is (are) considered to be part of an article (or article of manufacture). An article or article of manufacture can refer to any manufactured single component or multiple components.

[0034] Further, the components shown and described in this application may also be implemented in program code (e.g., firmware and/or software and/or other logic instructions) stored on one or more computer readable medium and

executable by one or more processors to perform the operations described in this application. The components are merely examples of various functionality that may be provided, and are not intended to be limiting. The embodiments shown and described are provided for purposes of illustration and are not intended to be limiting.

CLAIMS

1. A computer system comprising:

a input sensor to provide a signal;

a firmware storage medium; and

a processor to execute instructions of an update program if the signal is provided from the input sensor to initiate update of firmware on the firmware storage medium, wherein the processor does not provide the signal from execution of the instructions of the update program.

2. The computer system of claim 1, wherein the processor is configured to execute instructions of the update program to check whether the signal is provided by the input sensor before the processor initiates update of the firmware on the firmware storage medium.

3. The computer system of claim 1, wherein the processor is configured to execute instructions of the update program to initiate update of the firmware on the firmware storage medium without checking whether the signal is provided by the input sensor.

4. The computer system of claim 1, wherein the processor is configured to execute instructions of the update program to verify whether at least a portion of the firmware was updated on the firmware storage medium after the processor initiated update of the firmware on the firmware storage medium.

5. The computer system of claim 1, further comprising a display member coupled to a base member to enable variable positioning of the display member relative to the base member; and wherein the input sensor is configured to generate an input signal based on a position of the display member relative to the base member.

6. The computer system of claim 1, wherein the processor is configured to execute instructions of the update program to provide a user prompt for activation of the input sensor.

7. The computer system of claim 1, wherein the firmware storage medium comprises non-volatile memory.

8. The computer system of claim 1, wherein the firmware comprises instructions that include a basic input output system (BIOS).

9. A method of a processor executing instructions of an update program to update firmware on firmware storage medium of a computer system, the method comprising:

receiving an input signal from an input sensor;

determining whether the input signal is from the input sensor and not from execution of instructions of the update program by the processor of the computer system; and

executing instructions of the update program by the processor to initiate update of the firmware on the firmware storage of the computer system if it is determined that the input signal is from the input sensor and not from execution of instructions of the update program.

10. The method of claim 9, further comprising the processor executing instructions of the update program for providing a prompt to activate the input sensor.

11. The method of claim 9, further comprising the processor executing instructions of the update program for checking whether the signal is provided by the input sensor before the processor initiates update of the firmware on the firmware storage.

12. The method of claim 9, further comprising the processor executing instructions of the update program for initiating update of the firmware on the firmware storage without checking whether the signal is provided by the input sensor.

13. An article comprising at least one computer-readable storage medium storing instructions of an update program that upon execution by a processor cause a computer system to:

determine whether a signal from an input sensor is generated by execution of instructions of the update program by the processor; and

initiate update of firmware on a firmware storage medium of the computer system if it is determined that the input signal is from the input sensor but not from execution of instructions of the update program.

14. The article of claim 13, further comprising executing instructions of the update program that cause the computer system to provide a prompt to activate the input sensor.

15. The article of claim 13, further comprising executing instructions of the update program that cause the computer system to check whether the signal is provided by the input sensor before the processor initiates update of the firmware on the firmware storage.

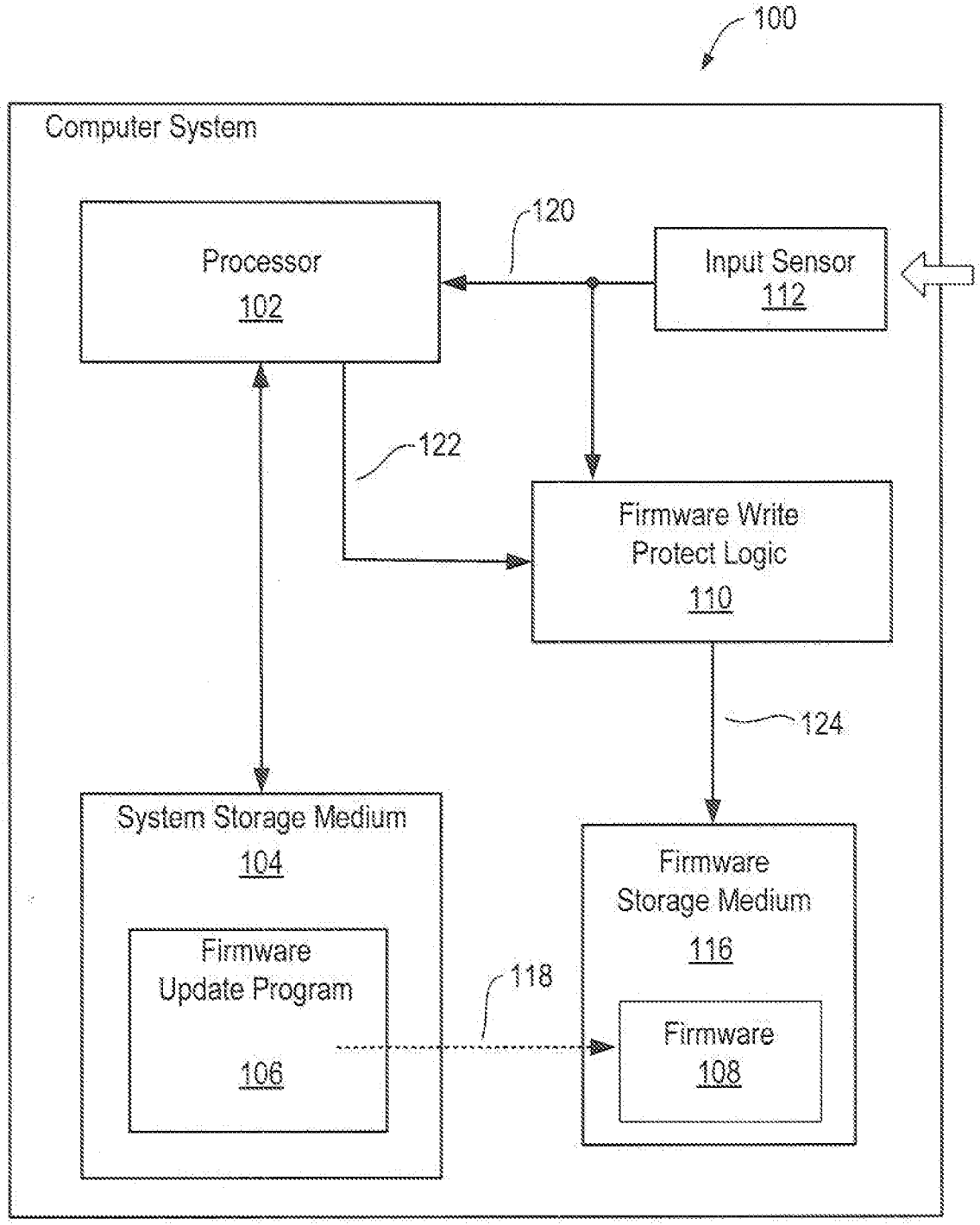

100
Computer System
Processor
102
120
Input Sensor
112
122
Firmware Write
Protect Logic
110
124
System Storage Medium
104
Firmware
Update Program
106
118
Firmware
Storage Medium
116
Firmware
108

Fig. 1

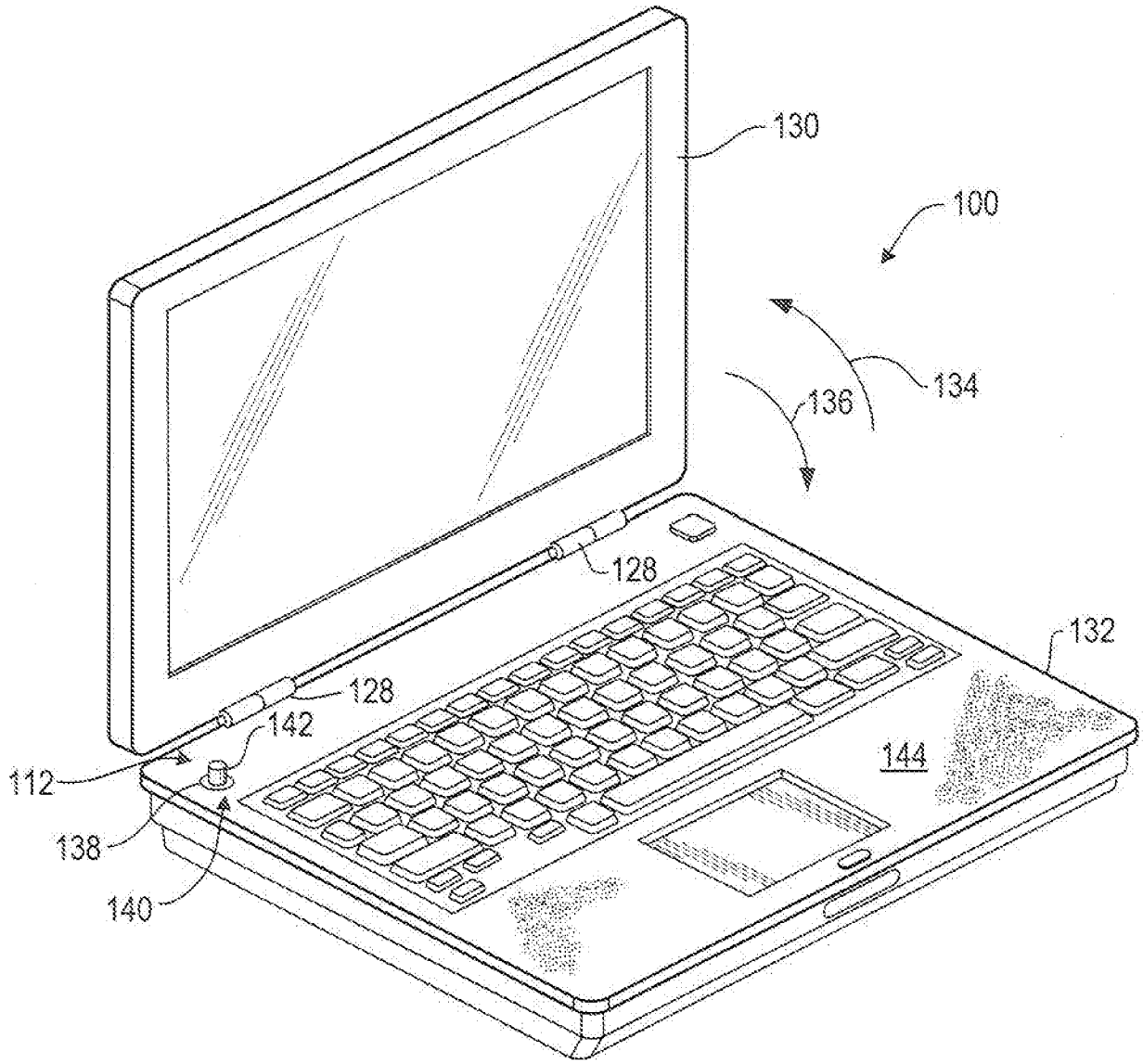


Fig. 2

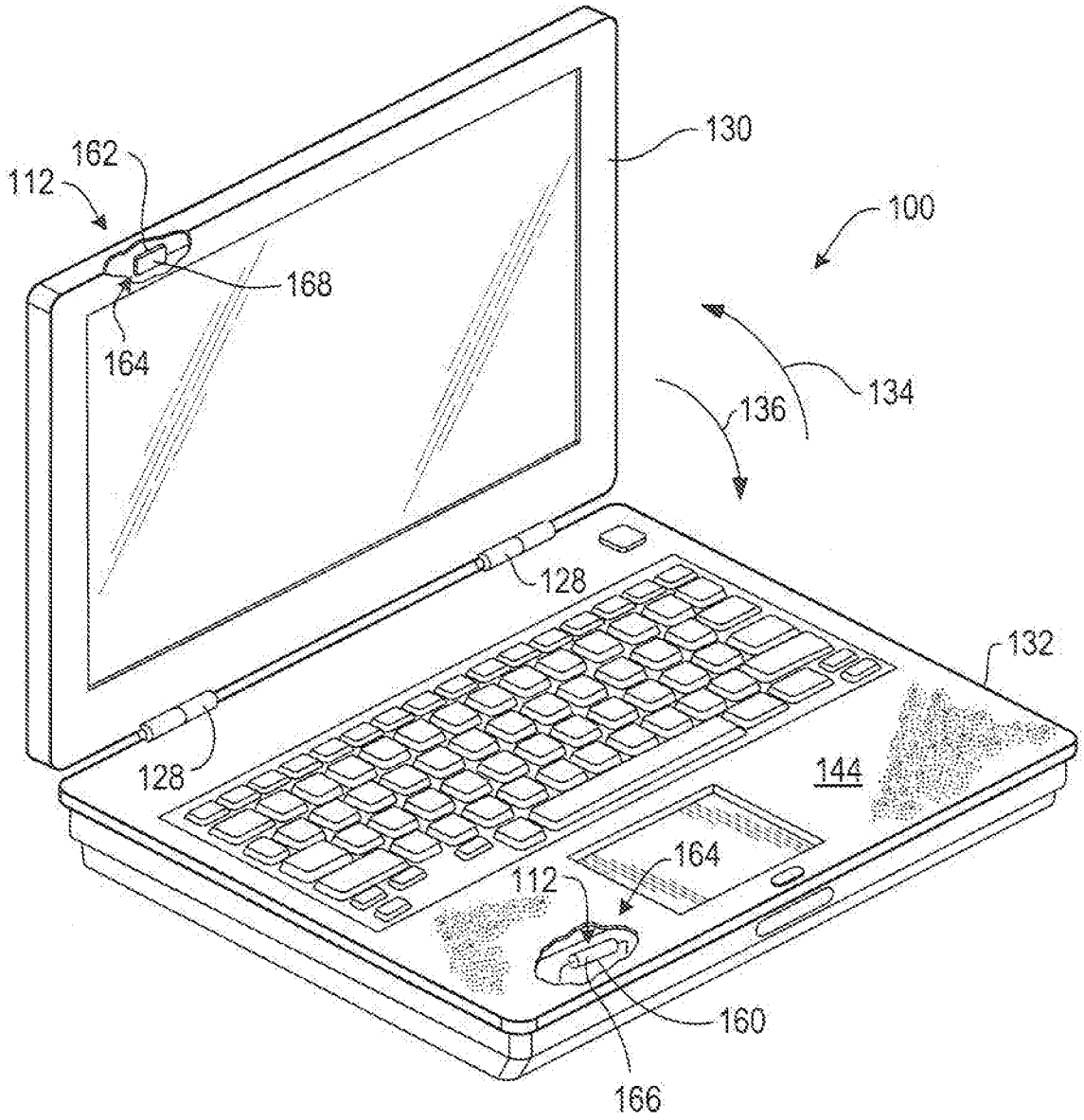


Fig. 3

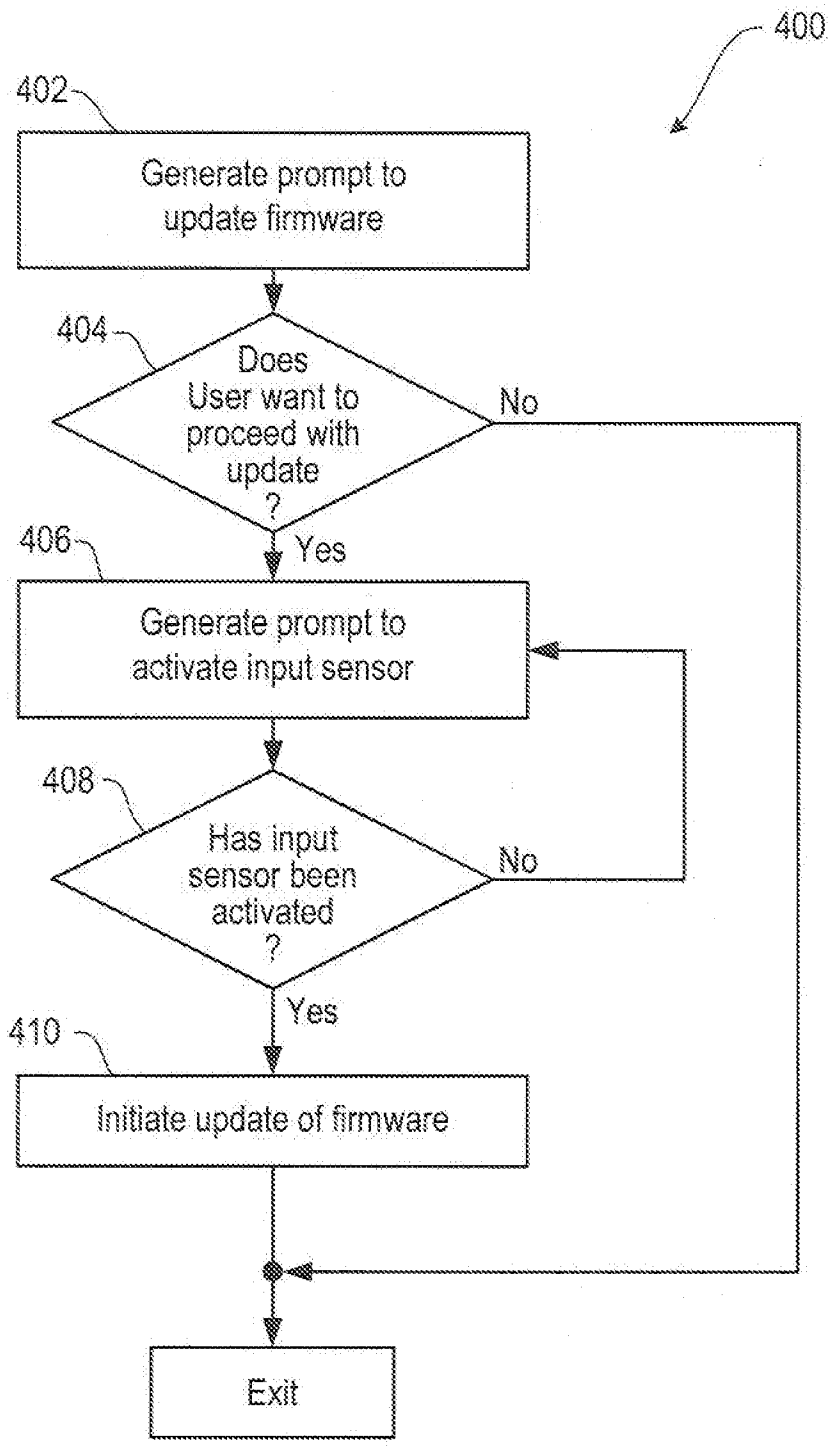

400
402
Generate prompt to update firmware
404
Does User want to proceed with update ?
No
Yes
406
Generate prompt to activate input sensor
408
Has input sensor been activated ?
No
Yes
410
Initiate update of firmware
Exit

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2011/034673

A. CLASSIFICATION OF SUBJECT MATTER

G06F 9/06(2006.01)i, G06F 9/44(2006.01)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 9/06; G06F 9/44; G06F 12/00; G06F 9/00

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: firmware update, firmware storage medium, update program;

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2006-0059300 A1 (CHI-CHUN HSU et al.) 16 March 2006 See the abstract, claims 1-20 and figures 1-5.	1-15
A	US 2004-0255286 A1 (ROTHMAN MICHAEL A. et al.) 16 December 2004 See the abstract, claims 1-30 and figures 1-7.	1-15
A	US 2006-0150177 A1 (HUNG-PING LIU et al.) 06 July 2006 See the abstract, claims 1-18 and figures 1-5.	1-15
A	US 2005-0216753 A1 (JAMES DAILEY et al.) 29 September 2005 See the abstract, claims 1-21 and figures 1-5.	1-15

☐ 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 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	Date of mailing of the international search report
26 DECEMBER 2011 (26.12.2011)	**26 DECEMBER 2011 (26.12.2011)**

Name and mailing address of the ISA/KR

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

Facsimile No. 82-42-472-7140

Authorized officer

BOK, Jin Yo

Telephone No. 82-42-481-5113

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2011/034673

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006-0059300 A1	16.03.2006	TW 259974 B	11.08.2006
		US 2009-0094414 A1	09.04.2009
		US 7480904 B2	20.01.2009
US 2004-0255286 A1	16.12.2004	US 7222339 B2	22.05.2007
US 2006-0150177 A1	06.07.2006	None	
US 2005-0216753 A1	29.09.2005	None	