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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 July 2009 (16.07.2009)

PCT

(10) International Publication Number
WO 2009/088362 A1

(51) International Patent Classification:
G06F 21/00 (2006.01) *H04L 9/00* (2006.01)

(21) International Application Number:
PCT/SG2008/000450

(22) International Filing Date:
27 November 2008 (27.11.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
200800249-5 9 January 2008 (09.01.2008) SG

(71) Applicant *(for all designated States except US)*: **DAL-LAB(S) PTE LTD** [SG/SG]; 519 Balestier Road, #02.03/04, Le Shantier, Singapore 329852 (SG).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LO KHIAM, Foh** [SG/SG]; 519 Balestier Road, #02-03/04, Le Shantier, Singapore 329852 (SG). **LUO, Jianlin** [CN/SG]; 519 Balestier Road, #02-03/04, Le Shantier, Singapore 329852 (SG).

(74) Agent: **LAWRENCE Y D HO & ASSOCIATES PTE LTD**; 30 Bideford Road, #02-02, Thongsia Building, Singapore 229922 (SG).

(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, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL,

[Continued on next page]

(54) Title: LIMITING ACCESS TO FILE AND FOLDER ON A STORAGE DEVICE

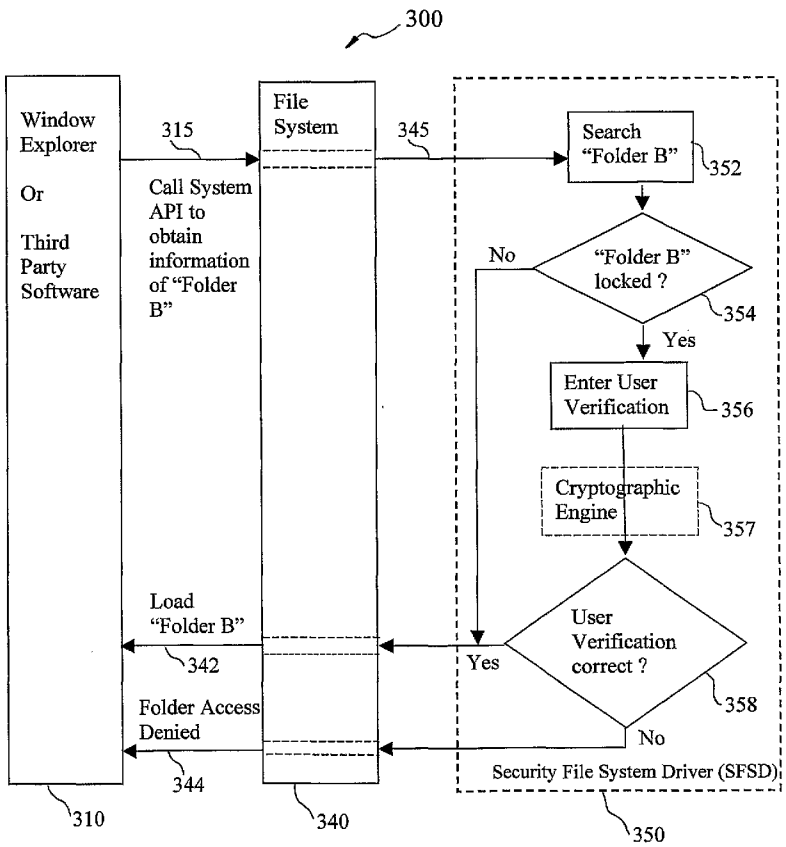

FIG. 3B

(57) Abstract: The present invention provides a modified operating system (OS) (100) operable on a portable computing device, such as, a mobile telephone, a mobile computer, an electronic organizer and a data storage device. The modified OS includes a file filter system (146), associated security file system driver (SFSD) (148) and a security user interface (152). The SFSD is loaded prior to final OS initialization/ configuration and loading of user security/data registry. A security user interface (152) associated with the SFSD then generates a dialogue box to allow the user to create a confidential file A or folder B and options for locking and/or encrypting. User identity is verified (258,358) before access to the file/folder is allowed; the file A/folder B remains secure even when security setting data created by the SFSD dialogue box is altered/removed or after the computing device undergoes a clean boot-up.

WO 2009/088362 A1

NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

Limiting Access To File And Folder On A Storage Device

Field of Invention

[0001] The present invention relates to system and method of limiting unauthorized access to data file and folder on a storage device of an electronic device.

Background

[0002] Computers, such as notebooks, personal digital assistant (PDA) and some mobile telephones, are now relatively affordable and are used widely; one can retrieve and send emails while traveling; another can perform electronic banking or commerce wirelessly. Coupled with the propensity of losing one's portable electronic devices, data security in such devices is imperative, and access to confidential files and folder is desired to be restricted or limited to the owner; in other words, it is desirable to prevent unauthorized reading or copying of confidential or sensitive data on one's computing or communication devices, especially if one's device has relatively large data storage and is also used for business activities.

[0003] Confidential or sensitive data can be made secure by the following approach:

(a) contents are accessible only after verification by passwords or other biometrics;
(b) contents are encrypted with passwords or passphrases;
(c) contents remain encrypted when copied out of a device;
(d) contents are not allowed to be copied out of a device;
(e) contents are protected and encrypted automatically when security setting is damaged or deleted; or
(f) contents are deleted after a lapse of predefined time interval.

[0004] Associated with security of data, there are two separate aspects of data security: confidentiality and integrity. Confidentiality refers to the reversible transformation of data into a form which has little or no resemblance to the original data, thereby making the transformed data non-intelligible to those without the knowledge to reverse the

transformation. Thus, confidentiality is associated with cryptography or encryption and decryption of data. Integrity of data refers to the assurance that data has not been tampered with. Integrity of data is often provided by digital signatures; a cryptographic checksum of the original data is calculated and stored somewhere; a verifier then calculates the checksum of the data and compares it with the stored pre-calculated checksum to ensure that the data is not tampered with.

[0005] To ensure data security, a user may either encrypt and decrypt a file or folder selectively or manually, or run a third party application to carry out these tasks automatically. One drawback of these approaches is that the encrypted file and folder and their security settings can be removed after the computing device undergoes a clean boot-up. It can thus be seen that there exists a need for another approach to ensuring data security that can overcome the disadvantage of the existing prior art.

[0006] FIG. 1 shows a simplified boot up process 1 of a conventional personal computer system. When a personal computer is turned on 10, a microprocessor in the computer passes control over to a basic input/output system (BIOS). The BIOS boots up the computer, checks whether all the input/output (I/O) and peripheral devices are connected and operational, initializes 20 all the operable peripheral devices before the BIOS invokes the operating system (OS) to load the OS from a bootable drive into the computer's random access memory (RAM).

[0007] When the OS is invoked, the kernel or core of the OS is loaded into the RAM. The kernel then starts system initialization and configuration 40. After OS initialization, a file system (FS) 42 is built up, as shown in FIG. 1. A file filter system (FFS) 44 and its associated window file filter driver (FFD) 46 are then loaded into the RAM. Loading of the OS then continues with loading 50 of all the required drivers and software applications predefined by the user. After the OS or computer is booted up 60, a directory of files and folders is created. The file directory can then be viewed by the user, and data files and folders can then be created, changed or removed by the user.

Summary

[0008] The following presents a simplified summary to provide a basic understanding of the present invention. This summary is not an extensive overview of the invention, and is not intended to identify key features of the invention. Rather, it is to present some of the inventive concepts of this invention in a generalised form as a prelude to the detailed description that is to follow.

[0009] In one embodiment, the present invention provides a file security system operable at boot up in a portable computing device. The file security system comprises: a file filter system and associated security file system driver (SFSD) to extend or replace functionality of a file system that is configurable with an original window operating system; wherein the file filter system is operable to interrupt the file system and the associated security file system driver (SFSD) is operable to boot up from a read-only memory (ROM).

[0010] In another embodiment, the file security system further comprises a security interface driver. The security interface driver generates a dialogue box for the user to create a confidential file or folder and to lock the file/folder to deny unauthorized access to confidential data or application stored therein.

[0011] In another embodiment, the present invention provides a method for preventing unauthorized electronic file access in a computing device. The method comprises: interrupting the file system during booting up of the computing device; replacing the file filter system that is configurable with an original window operating system with a modified file filter system; installing a security file system driver (SFSD) associated with the modified file filter system; and installing a security user interface driver, which generates a dialogue box to allow the user to create a confidential file or folder whilst loading user installable software and drivers, before completing the booting up process.

[0012] In another embodiment, the SFSD in the above method further comprises a cryptographic engine. In addition, the SFSD is loaded prior to loading of user data and

the confidential file/folder thus created on a computing device remains secure until it is unlocked with a correct user verification.

[0013] The present invention also discloses a computer readable medium containing a file security system according to any one of claims 1-5 or containing a method of preventing unauthorized electronic file access according to any one of claims 6-10

Brief Description of the Drawings

[0014] This invention will be described by way of non-limiting embodiments of the present invention, with reference to the accompanying drawings, in which:

[0015] FIG. 1 illustrates a boot up process of a conventional personal computer system;

[0016] FIG. 2 illustrates a boot up process of a portable computing device according to one embodiment of the present invention; and

[0017] FIG. 3A illustrates a security system for accessing a file according to another embodiment of the present invention; and FIG. 3B illustrates a security system for accessing a folder according to yet another embodiment of the present invention.

Detailed Description

[0018] One or more specific and alternative embodiments of the present invention will now be described with reference to the attached drawings. It shall be apparent to one skilled in the art, however that this invention may be practised without such specific details. Some of the details may not be described at length so as not to obscure the invention. For ease of reference, common reference numerals or series of numerals will be used throughout the figures when referring to the same or similar features common to the figures.

[0019] FIG. 2 shows a boot up process 100 of a portable computing device according to one embodiment of the present invention. As shown in FIG. 2, a power up step 110 is followed by a basic hardware initialization step 120. The basic hardware initialization step 120 involves passing control over to a basic input/output system (BIOS). The BIOS boots up the portable computing device, checks whether all the input/output (I/O) and peripheral devices are connected and operational, and initializes 120 all the operable peripheral devices.

[0020] Step 120 is followed by step 130. In step 30, the BIOS invokes the operating system (OS) to load the OS from a bootable drive into the computer's random access memory (RAM). After the OS is invoked, the kernel of the OS is loaded into the RAM; this is then followed by OS initialization and configuration in step 140.

[0021] As shown in FIG. 2, part of the OS initialization and configuration in step 140 involves building up a file system in step 142 and a file filter system in step 144, loading of a window filter driver in step 146 and loading of a security file system driver (SFSD) from a read-only memory (ROM) in step 148; the following description of the present invention deals with this aspect of configuring the system files. This approach builds the file system in layers comprising the file filter and file system drivers and allows interrupts to the system files that would be built up by an original window OS; in this way, this approach allows security of the system files to be extended or modified. In other words, security of the file system is managed at the OS level and bootable in ROM instead of a user installable application level.

[0022] In one embodiment of building the file system drivers, FIG. 2 shows the step of loading a security file system driver (SFSD) in step 148. For tighter security, the SFSD is loaded from a read-only memory (ROM). Such reading from a ROM may be reading from a protected disc during which read-write operation is denied by a separate disk filter system. After all the file system drivers are loaded, including the SFSD in step 148, the booting up process reverts to step 140 to finalise the OS initialization and configuration prior to loading of user security or data registry. Once the OS initialization and configuration processes are finalized, the booting up process involves loading the user installed software and associated drivers into the RAM in step 150 and

loading in step 152 of a security interface driver associated with the SFSD. In one embodiment, the security interface driver associated with the SFSD generates a dialogue box to allow a user to create a confidential file A for storing sensitive information; in another embodiment, the dialogue box allows a user to create a confidential folder B for storing files containing sensitive information or applications which the user can launch. In addition, the dialogue box also allows the user to lock or unlock the confidential file A or folder B.

[0023] After all the user installed software and associated drivers predefined for launching during boot up are loaded in step 150, including the process in step 152, the OS boot up process is completed in step 160. The SFSD dialogue box can then be called out after the computing device has booted up to allow the user create additional confidential files or folders and to lock/unlock the confidential files/folders as and when required. For example, a user may lock a confidential file A/folder B before lending the computing device, such as a mobile phone or a PDA, to another user so that the other user can use the computing device without having access to the locked confidential file A/folder B; in addition, the user may lock selected applications, for example by storing email or short message (SMS) applications in the confidential folder B.

[0024] In one embodiment of locking or unlocking the confidential file A/folder B, the user enters a password or passphrase; in another embodiment, the user signs in with a digital signature; in yet another embodiment, the user signs in with a biometric signature.

[0025] FIG. 3A shows the system file's security process 200 according to the confidential file A embodiment of the present invention. As shown in FIG. 3A, process box 210 illustrates execution of a window explorer or a third party software application. Execution of a request from the window explorer to open a locked file A sends a system call 215 to the file system 240 to obtain file A's information. The file information 245 is then sent to the SFSD 250. Within the SFSD, a search for file A in the storage disk is conducted in step 252. Following execution of step 252, a decision is made in step 254 whether the requested file A is locked or not.

[0026] If the decision in box 254 is no, the SFSD 250 passes control over to the file system 240 and the requested file information is sent, in step 242, to the window explorer or requestor application. If the decision in box 254 is yes, the SFSD 250 proceeds to step 256. In step 256, the SFSD 250 prompts the user to enter a user verification.

[0027] After the user enters a user verification in step 256, the SFSD 250 checks, in step 258, whether the user verification is correct. If the user is correctly verified, the SFSD 250 passes control over to the file system 240 and the requested file information is sent, also in step 242, to the window explorer or requestor application. If the decision in box 258 is no, the SFSD 250 informs the file system 240, which then sends a "no file" response in step 244 to the file explorer 210. The file explorer or requestor application 210 in turn informs the user that access to file A is denied.

[0028] FIG. 3B shows the system file's security process 300 according to the confidential folder B embodiment of the present invention. Security process 300 is similar to security process 200 in substantially the same manner. Execution of the file explorer 310 or requestor application sends a system call 315 to the file system 340 to obtain folder B's information. The folder B information 345 is then sent to the SFSD 350. Within the SFSD 350, a search for folder B in the storage disk is conducted in step 352. Following search step 352, a decision is made in step 354 whether the requested folder B is locked or not.

[0029] If the decision in box 354 is no, the SFSD 350 passes control over to the file system 340 and the requested folder information is sent, in step 342, to the window explorer or requestor application. If the decision in box 354 is yes, the SFSD 350 proceeds to step 356. In step 356, the SFSD 350 prompts the user to enter a user verification.

[0030] After the user enters a user verification in step 356, the SFSD 350 checks, in step 358, whether the user verification is correct. If the user is correctly verified, the SFSD 350 passes control over to the file system 340 and the requested folder B

information is sent, also in step 342, to the window explorer or requestor application. If the decision in box 358 is no, the SFSD 350 informs the file system 240, which then sends a "no content" response in step 344 to the file explorer 310. The file explorer or requestor application 310 in turn informs the user that access to folder B is denied.

[0031] In another embodiment of security process 200, the SFSD 250 includes an addition cryptographic engine 257 after step 256. Similarly, in another embodiment of security process 300, the SFSD 350 includes an additional cryptographic engine 357 after step 356. The additional cryptographic engine 257,357 may employ a symmetric key algorithm, such as an Advanced Encryption System (AES). The cryptographic engine 257,357 may be used to encrypt owner's verification, which is stored in the computing device. In addition, the cryptographic engine 257,357 may be used to decrypt the owner's verification which is stored in the computing device by comparing it with the user verification. The cryptographic engine 257,357 may be supplied to a user on a ROM, a protected ROM disk or on a separate processor.

[0032] An advantage of the present system is that a confidential file/folder created on an electronic device with an operating system of the present invention remains secure until it is unlocked with a correct user verification. This is because the SFSD of the present invention is loaded by the file system before the system file is fully initialized, i.e,. before user data and any third party installable security software are loaded; in other words, the SFSD is executed prior to entry of user data or execution of any third party installable security software. The confidential file A/folder B is denied even when security setting data entered through the SFSD dialogue box is altered or removed, or even when the computing device undergoes a clean boot-up. In this way, all user data and system or user installable applications can be made secure, that is, in terms of confidentiality and integrity; in general, use of a mobile or portable electronic device operable with an operating system according to the present invention can be restricted by an owner or with permission from the owner.

[0033] As can be appreciated from the above description, the present invention provides data security to a computing device without much trouble to the user or with no difference from a third party installable application; a user need only to create the

confidential file A or confidential folder B and to install/migrate all applications that contain confidential information into the confidential folder B. Another advantage is that a computing device incorporating the security process or processes 100,200,300 of the present invention can be used by another user with no access to the confidential file A or folder B or applications installed in the confidential folder B.

[0034] While specific embodiments have been described and illustrated, it is understood that many changes, modifications, variations and combinations thereof could be made to the present invention without departing from the scope of the invention. For example, whilst the OS was illustrated with a personal portable computing device, the principle underlying its security at a system level is applicable to an operating system that is operable in a mobile phone, a portable electronic organizer or data storage device.

CLAIMS:

1. A file security system operable at boot up in a portable computing device, said file security system comprising:

a file filter system and associated security file system driver (SFSD) to extend or replace functionality of a file system that is configurable with an original window operating system;

wherein the file filter system is operable to interrupt the file system and the associated security file system driver (SFSD) is operable to boot up from a read-only memory (ROM).

2. A file security system according to claim 1, further comprising a security interface driver, which generates a dialogue box for the user to create a confidential file or folder and to lock the file/folder to deny unauthorized access to confidential data or application stored therein.

3. A file security system according to claim 2, wherein access to the file/folder is verified via a password, a passphrase or sign-in signature.

4. A file security system according to any one of claims 1-3, wherein the security file system driver (SFSD) further comprises a cryptographic engine.

5. A file security system according to any one of claims 2-4, wherein the file/folder remains locked even when security setting data entered by the SFSD dialogue box is altered/removed or even after the computing device undergoes a clean boot-up.

6. A method for preventing unauthorized electronic file access in a computing device, the method comprising:

interrupting the file system during booting up of the computing device;

replacing the file filter system that is configurable with an original window operating system with a modified file filter system;

installing a security file system driver (SFSD) associated with the modified file filter system; and

installing a security user interface driver associated with the SFSD whilst loading user installable software and drivers before completing the booting up process, wherein the SFSD security interface driver generates a SFSD dialogue box to allow the user to create a confidential file or folder and to lock/unlock the confidential file/folder.

7. A method according to claim 6, wherein the SFSD further comprises a cryptographic engine.

8. A method according to claim 6 or 7, wherein the modified file filter system and its associated security file system driver (SFSD) are loaded prior to loading of user data or any user installable security application.

9. A method according to any one of claims 6-8, wherein the confidential file or folder created with the modified file filter system remains locked even when security setting data entered by the SFSD dialogue box is altered/removed or even after the computing device undergoes a clean boot-up.

10. A method according to any one of claims 6-9, wherein the computing device is a mobile telephone, a mobile personal computer, an electronic organizer or a data storage apparatus.

11. A computer readable medium containing a file security system according to any one of claims 1-5.

12. A computer readable medium containing a method of preventing unauthorized electronic file/folder access according to any one of claims 6-10.

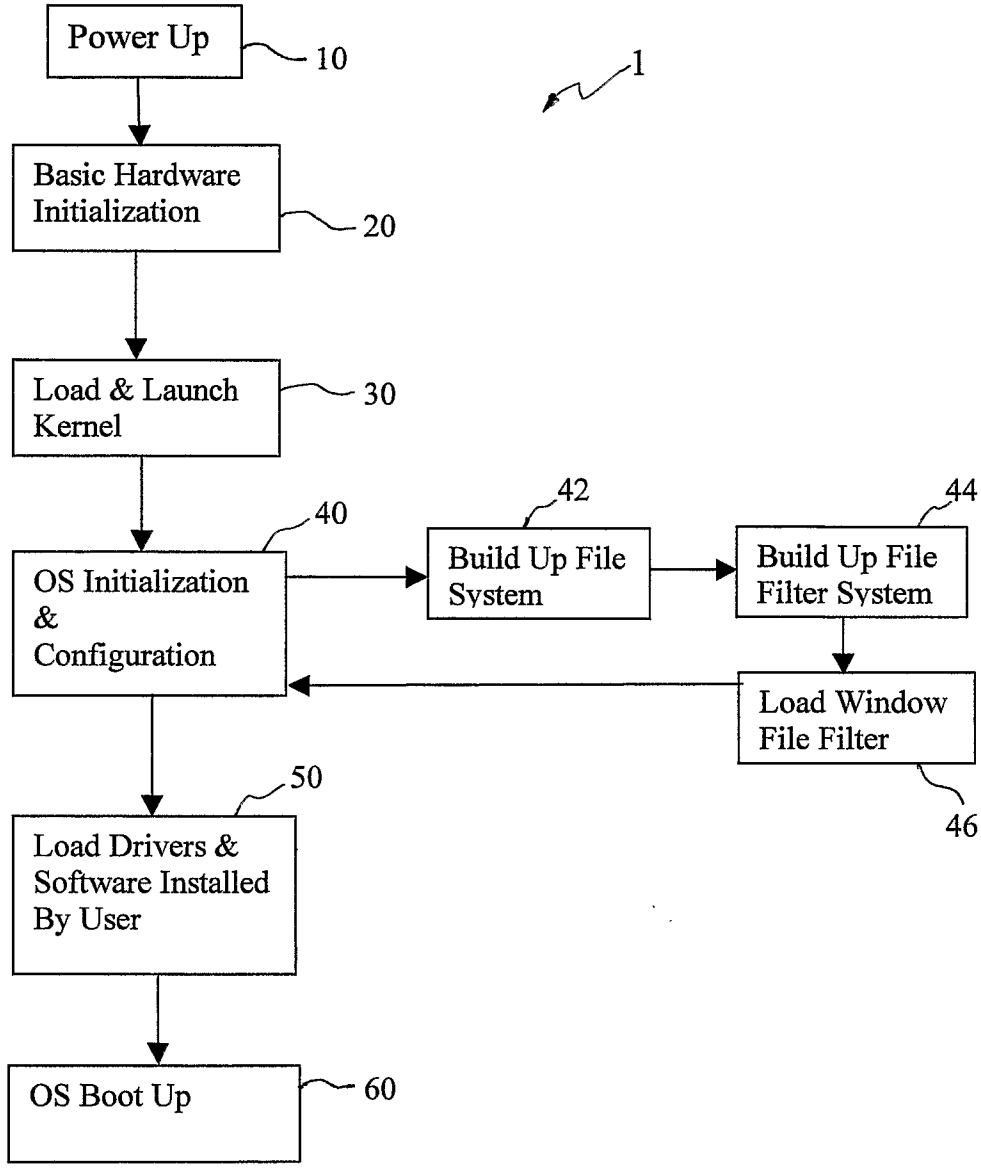
Power Up
10
1
Basic Hardware Initialization
20
Load & Launch Kernel
30
42
44
40
OS Initialization & Configuration
Build Up File System
Build Up File Filter System
Load Window File Filter
46
50
Load Drivers & Software Installed By User
OS Boot Up
60

FIG. 1

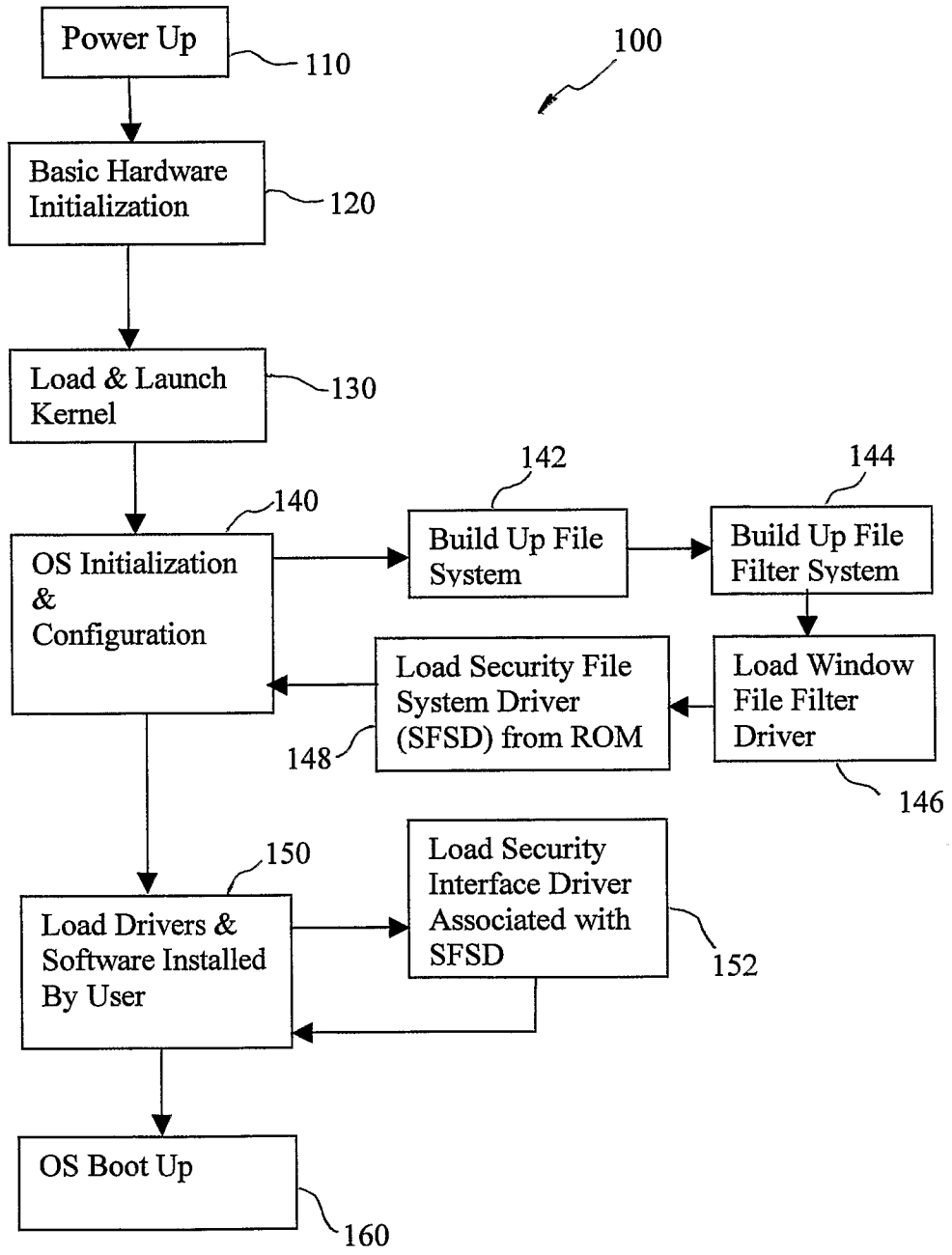
Power Up
110
100
Basic Hardware Initialization
120
Load & Launch Kernel
130
142
144
140
OS Initialization & Configuration
Build Up File System
Build Up File Filter System
Load Security File System Driver (SFSD) from ROM
148
Load Window File Filter Driver
146
150
Load Drivers & Software Installed By User
Load Security Interface Driver Associated with SFSD
152
OS Boot Up
160

FIG. 2

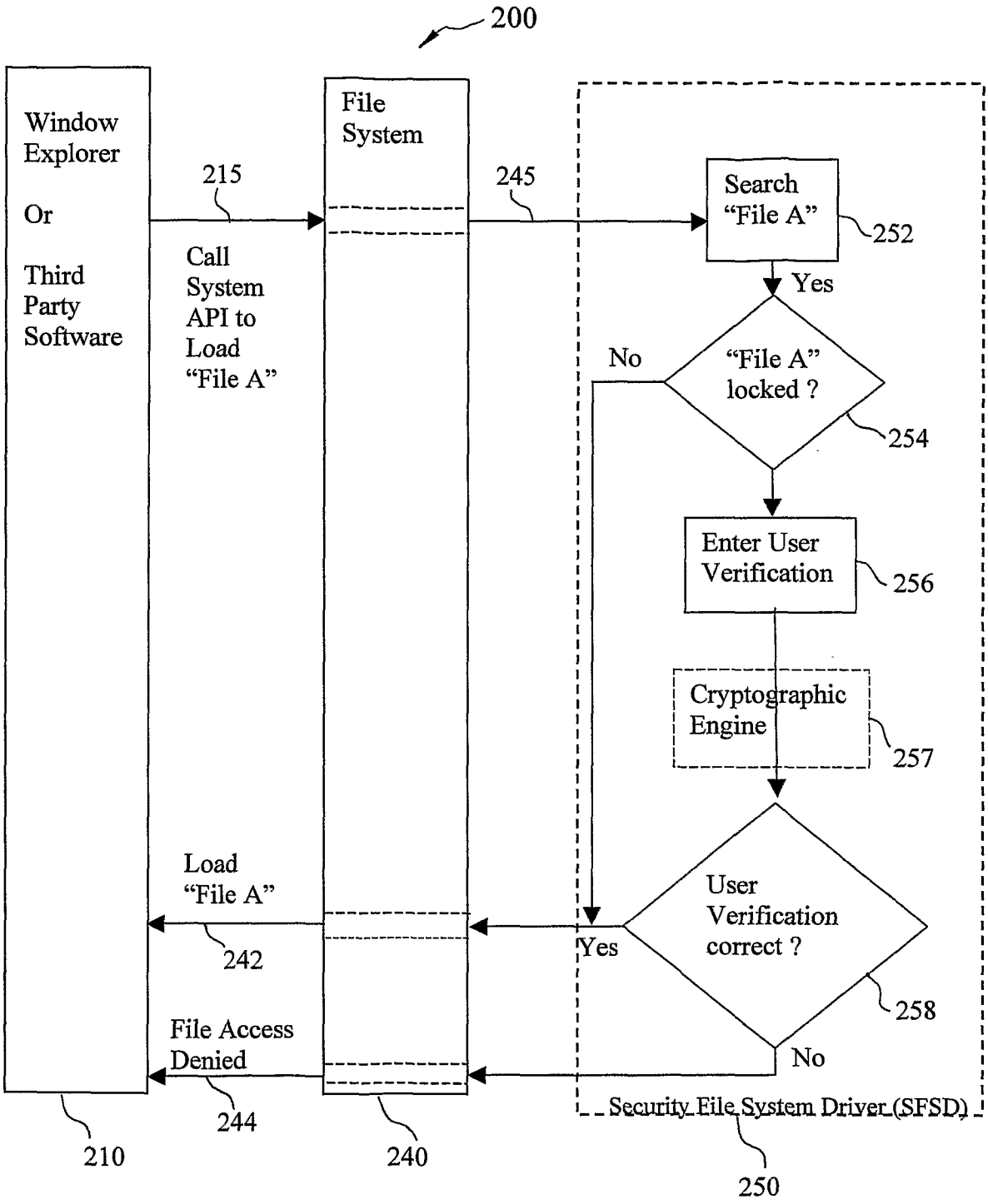
200
Window Explorer
Or
Third Party Software
210
215
Call System API to Load "File A"
File System
240
245
Search "File A"
252
Yes
No
"File A" locked ?
254
Enter User Verification
256
Cryptographic Engine
257
User Verification correct ?
258
Yes
No
Load "File A"
242
File Access Denied
244
Security File System Driver (SFSD)
250

FIG. 3A

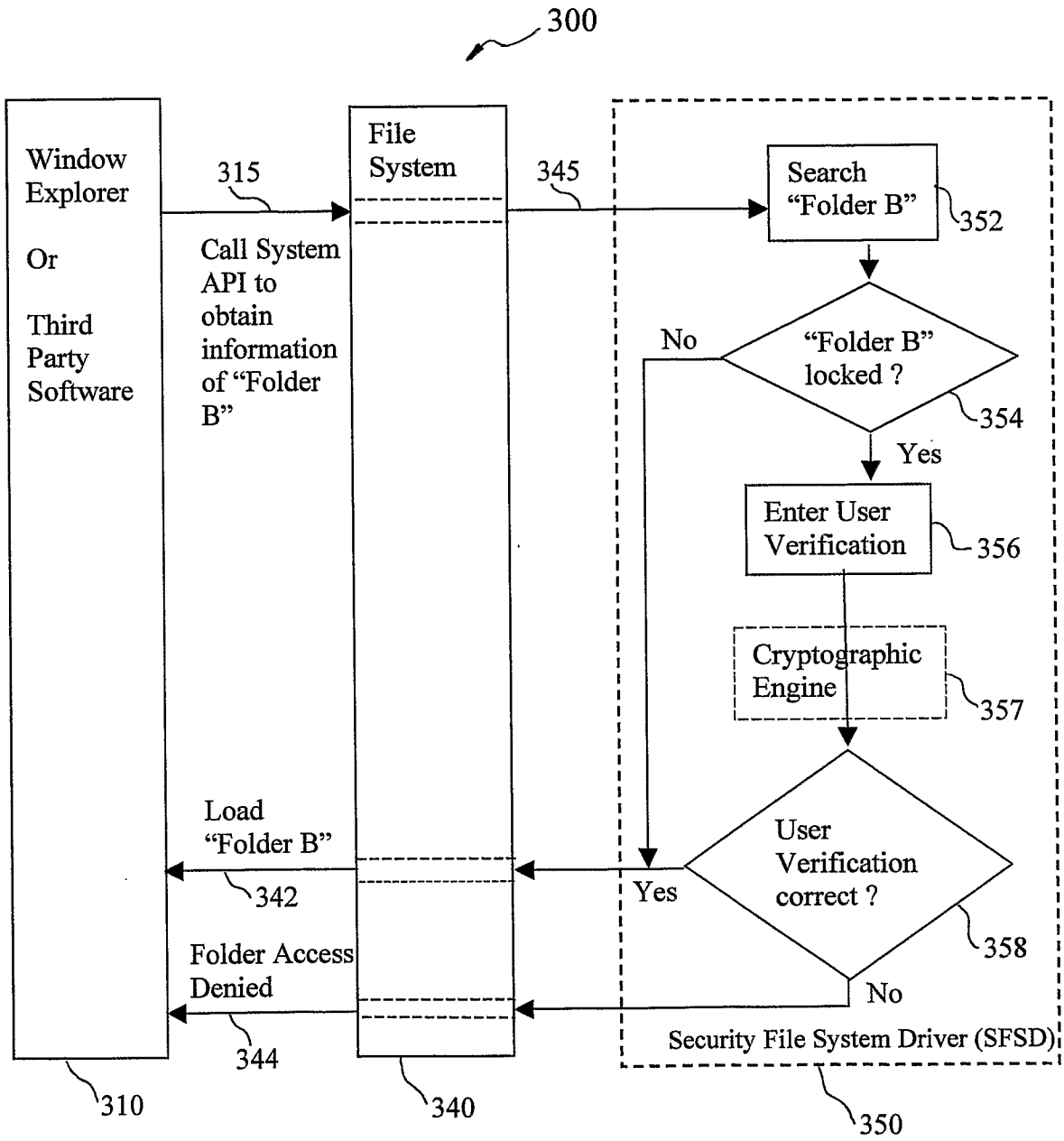
300
Window Explorer
Or
Third Party Software
315
Call System API to obtain information of "Folder B"
File System
345
Search "Folder B"
352
No
"Folder B" locked ?
354
Yes
Enter User Verification
356
Cryptographic Engine
357
User Verification correct ?
358
Yes
No
Load "Folder B"
342
Folder Access Denied
344
Security File System Driver (SFSD)
310
340
350

FIG. 3B

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG2008/000450

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.

G06F 21/00 (2006.01) ***H04L 9/00*** (2006.01)

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)

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPODOC, WPI with keywords (SECUR+ FILE+ SYSTEM) and like terms

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 1999/014652 (BRUNDRETT et al.) 25 March 1999 Pg 7, 8 , 15, 20, 25, Fig 1)	1-12
Y	US 2003/0065875 (Van Cleve et al.) 3 April 2003 (Abstract, Para 0010)	1-4, 6-8, 10-12
Y	US 2007/0050620 A1 (PHAM et al.) 1 March 2007 (Abstract, Para 0014,Para 0033-0034, Fig 2)	5, 9
A	US 7178165 B2 (ABRAMS) 13 February 2007 See whole document	1-12

☐ 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	Date of mailing of the international search report
23 December 2008	03 FEB 2009

Name and mailing address of the ISA/AU

AUSTRALIAN PATENT OFFICE
PO BOX 200, WODEN ACT 2606, AUSTRALIA
E-mail address: pct@ipaustralia.gov.au
Facsimile No. +61 2 6283 7999

Authorized officer
KANWAL PAHWA
AUSTRALIAN PATENT OFFICE
(ISO 9001 Quality Certified Service)
Telephone No : +61 2 6283 2644

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/SG2008/000450

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
WO	9914652	EP	1012691	US	6249866	US	6986043
		US	2002019935				
US	2003065875	US	7299345				
US	2007050620	AU	2003279767	EP	1552643	US	7143288
		US	2004078568	WO	2004036350		
US	7178165	US	2003037252				

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

END OF ANNEX