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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 November 2016 (03.11.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/175772 A1

(51) International Patent Classification:
G06F 21/60 (2013.01) *G06F 21/62* (2013.01)

(21) International Application Number:
PCT/US2015/028110

(22) International Filing Date:
29 April 2015 (29.04.2015)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **HEWLETT PACKARD ENTERPRISE DEVELOPMENT LP** [US/US]; 11445 Compaq Center Drive West, Houston, TX 77070 (US).

(72) Inventors: **BUTT, John**; Longdown Avenue & Stoke, Gifford Bristol BS34 8QZ (GB). **SIMPSON, Ben**; Longdown Avenue & Stoke, Gifford Bristol BS34 8QZ (GB). **DONAGHY, Dave**; Longdown Avenue & Stoke, Gifford Bristol BS34 8QZ (GB).

(74) Agents: **SORENSEN, C. Blake** et al.; Hewlett Packard Enterprise, 3404 E. Harmony Road, Mail Stop 79, Fort Collins, CO 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, 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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, 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, SA, 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, ST, 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, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

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

Published:

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

(54) Title: DATA PROTECTION

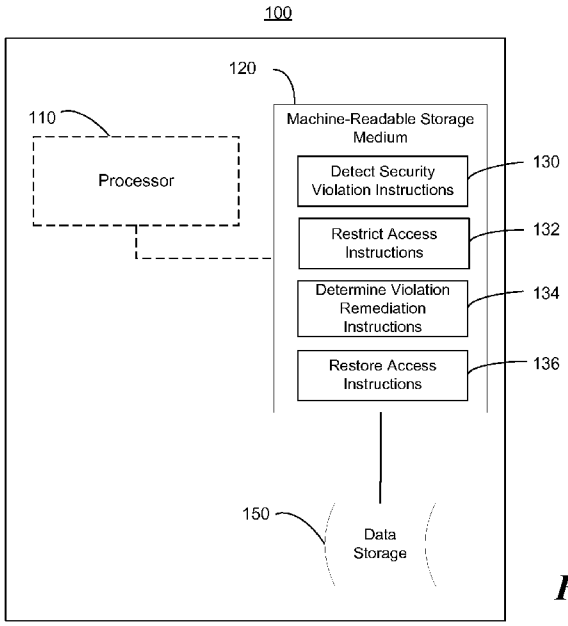

FIG. 1

(57) Abstract: Examples disclosed herein relate to data protection instructions to detect, according to a command execution, that a security violation associated with a data storage has occurred. In response to detecting that the security violation has occurred, data protection instructions may restrict access to the data storage, determine whether the security violation has been remediated, and in response to determining that the security violation has been remediated, restore access to the data storage.

WO 2016/175772 A1

DATA PROTECTION

BACKGROUND

[0001] Data protection allows for preventing changes to data that may have been compromised. In some situations, active processes and/or sessions may be reading and writing to a data storage device after a security violation has occurred.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] In the accompanying drawings, like numerals refer to like components or blocks. The following detailed description references the drawings, wherein:

[0003] FIG. 1 is a block diagram of an example data protection device;

[0004] FIG. 2 is a flowchart of an example of a method for data protection; and

[0005] FIG. 3 is a block diagram of an example system for data protection.

DETAILED DESCRIPTION

[0006] As described above, data protection may identify when a security violation has occurred on a data storage device. After identifying such a violation, active processes and/or network sessions may be blocked from reading and/or writing to the storage device in order to prevent access to corrupted data and/or to prevent adding data to the compromised storage device.

[0007] In the description that follows, reference is made to the term, "machine-readable storage medium." As used herein, the term "machine-readable storage medium" refers to any electronic, magnetic, optical, or other physical storage device that stores executable instructions or other data (e.g., a hard disk drive, random access memory, flash memory, etc.).

[0008] Referring now to the drawings, FIG. 1 is a block diagram of an example data protection device 100 consistent with disclosed implementations. Data

protection device 100 may comprise a processor 110 and a non-transitory machine-readable storage medium 120. Data protection device 100 may comprise a computing device such as a server computer, a desktop computer, a laptop computer, a handheld computing device, a smart phone, a tablet computing device, a mobile phone, or the like. Device 100 may further comprise a data storage 150.

[0009] Processor 110 may comprise a central processing unit (CPU), a semiconductor-based microprocessor, or any other hardware device suitable for retrieval and execution of instructions stored in machine-readable storage medium 120. In particular, processor 110 may fetch, decode, and execute a plurality of detect security violation instructions 130, restrict access instructions 132, determine violation remediation instructions 134, and restore access instructions 136 to implement the functionality described in detail below.

[0010] Executable instructions may be stored in any portion and/or component of machine-readable storage medium 120. The machine-readable storage medium 120 may comprise both volatile and/or nonvolatile memory and data storage components. Volatile components are those that do not retain data values upon loss of power. Nonvolatile components are those that retain data upon a loss of power.

[0011] The machine-readable storage medium 120 and data storage 150 may comprise, for example, random access memory (RAM), read-only memory (ROM), hard disk drives, solid-state drives, USB flash drives, memory cards accessed via a memory card reader, floppy disks accessed via an associated floppy disk drive, optical discs accessed via an optical disc drive, magnetic tapes accessed via an appropriate tape drive, and/or other memory components, and/or a combination of any two and/or more of these memory components. In addition, the RAM may comprise, for example, static random access memory (SRAM), dynamic random access memory (DRAM), and/or magnetic random access memory (MRAM) and other such devices. The ROM may comprise, for example, a programmable read-only memory (PROM), an erasable programmable read-only memory (EPROM), an

electrically erasable programmable read-only memory (EEPROM), and/or other like memory device.

[0012] Data storage 150 may comprise a physical storage device, such as a hard disk drive and/or a solid state drive, and/or a logical storage device, such as a database, a user-based logical data storage (e.g., a user's home directory and associated files), a network-attached storage, and a logical partition. A logical storage device may comprise data stored on part of and/or across a plurality of physical storage devices.

[0013] Detect security violation instructions 130 may detect, according to a command execution, that a security violation associated with a data storage has occurred. The executed commands may be associated with assessing and/or remediating unauthorized access to data storage 150, such as by securing and/or removing data in data storage 150.

[0014] For example, detect security violation instructions 130 may comprise a list of secure commands associated with addressing suspected security breaches on data storage 150. Such commands may comprise, for example, secure delete commands for files in data storage 150, encryption commands, network configuration commands such as firewall adjustments and/or commands to disconnect users, applications, and/or communication sessions, and/or audit commands for security information such as access logs for device 100 and/or data storage 150. A secure delete command, for example, erases the data specified in the command and then overwrites the memory and storage location with random bits of data to prevent recovery. In some implementations, any command run with elevated permissions, such as those performed via a SUDO operation, may comprise a command associated with addressing a security breach.

[0015] Restrict access instructions 132 may, in response to detecting that the security violation has occurred, restrict access to data storage 150. For example, user sessions interacting with data storage 150 may be blocked from reading and/or writing to data storage 150.

[0016] Different types and/or levels of restriction may be used, such as restricting non-administrative/super users, only restricting non-secure commands on data storage 150, and/or blocking only reads from data storage 150 or writes to data storage 150. In some implementations, users may be notified of the security violation and/or may receive an error message regarding the block on reading/writing to data storage 150. In some implementations, read and/or write requests may be paused and/or the read/write processes may be placed in an idle state. In some implementations, user sessions interacting with data storage 150 may be closed and/or disconnected, and/or processes associated with such sessions may be terminated.

[0017] Determine violation remediation instructions 134 may determine whether the security violation has been remediated. For example, the security violation may be determined to have been remediated after the command associated with detecting the violation has been completed. For another example, the security violation may be determined to have been remediated after the session in which the command was detected has disconnected and/or exited a privileged state (e.g., a user of the session switches to a non-administrator user).

[0018] Restore access instructions 136 may, in response to determining that the security violation has been remediated, restore access to the data storage. For example, idled read/write processes may be permitted to complete execution and/or new sessions may be permitted to connect to data storage 150.

[0019] FIG. 2 is a flowchart of a method 200 for data protection consistent with disclosed implementations. Although execution of method 200 is described below with reference to the components of data protection device 100, other suitable components for execution of method 200 may be used.

[0020] Method 200 may start in stage 205 and proceed to stage 210 where device 100 may detect, according to a first command performed on a data storage, that a security violation has occurred. In some implementations, the first command may comprise a secure command. For example, detect security violation instructions 130 may detect, according to a command execution, that a security

violation associated with a data storage has occurred. The executed commands may be associated with assessing and/or remediating unauthorized access to data storage 150, such as by securing and/or removing data in data storage 150.

[0021] For example, detect security violation instructions 130 may comprise a list of secure commands associated with addressing suspected security breaches on data storage 150. Such commands may comprise, for example, secure delete commands for files in data storage 150, encryption commands, network configuration commands such as firewall adjustments and/or commands to disconnect users, applications, and/or communication sessions, and/or audit commands for security information such as access logs for device 100 and/or data storage 150. A secure delete command, for example, erases the data specified in the command and then overwrites the memory and storage location with random bits of data to prevent recovery. In some implementations, any command run with elevated permissions, such as those performed via a SUDO operation, may comprise a command associated with addressing a security breach.

[0022] Method 200 may then advance to stage 215 where device 100 may restrict access to the data storage for a user session. A user session may comprise a local and/or network communication session with a computer such as device 100, such as may occur when a user has logged into device 100 and/or an application or service executing on device 100. For example, a user session may be associated with a user of a web-based application wherein the user's web browser is accessing device 100 and data storage 150 via a network. In some implementations, the user session may be associated with a second command comprising a non-secure command, such as a standard data read and/or write command.

[0023] In some implementations, restrict access instructions 132 may, in response to detecting that the security violation has occurred, restrict access to data storage 150. For example, user sessions interacting with data storage 150 may be blocked from reading and/or writing to data storage 150 entirely, blocked

writing while permitted to read, or vice versa, and/or blocked from executing non-secure commands while permitting other, secure commands to still be executed.

[0024] Different types and/or levels of restriction may be used, such as restricting non-administrative/super users, only restricting non-secure commands on data storage 150, and/or blocking only reads from data storage 150 or writes to data storage 150. For example, in response to determining that the second user session is associated with an administrator user, continued access to the data storage may be permitted. In such an example, the administrator user may be notified of the detected security violation.

[0025] In some implementations, users may be notified of the security violation and/or may receive an error message regarding the block on reading/writing to data storage 150. In some implementations, read and/or write requests may be paused and/or the read/write processes may be placed in an idle state. In some implementations, user sessions interacting with data storage 150 may be closed and/or disconnected, and/or processes associated with such sessions may be terminated. In some implementations, restricting access to data storage 150 may comprise preventing a new user session from connecting to the data storage.

[0026] Method 200 may then advance to stage 220 where device 100 may determine whether the security violation has been remediated. For example, determine violation remediation instructions 134 may determine whether the security violation has been remediated. For example, the security violation may be determined to have been remediated after the command associated with detecting the violation has been completed. For another example, the security violation may be determined to have been remediated after the session in which the command was detected has disconnected and/or exited a privileged state (e.g., a user of the session switches to a non-administrator user).

[0027] If the security violation has not been remediated, then method 200 may return to stage 215 and device 100 may maintain the restriction on access to the data storage. Otherwise, method 200 may advance to stage 240 where device 100 may restore access to the data storage for the user session. For example, restore

access instructions 136 may, in response to determining that the security violation has been remediated, restore access to the data storage. For example, idled read/write processes may be permitted to complete execution and/or new sessions may be permitted to connect to data storage 150.

[0028] After restoring access to the data storage at stage 240, method 200 may then end at stage 250.

[0029] FIG. 3 is a block diagram of a system 300 for data protection. System 300 may comprise a computing device 310 comprising a command engine 315, a security engine 320, and a session engine 325. Session engine 325 may manage and control a plurality of user sessions 330(A)-(C) and an administrator user session 335. System 300 may further comprise a data storage 340.

[0030] Computing device 310 may comprise, for example, a general and/or special purpose computer, server, mainframe, desktop, laptop, tablet, smart phone, game console, and/or any other system capable of providing computing capability consistent with providing the implementations described herein. Data storage 340 may comprise a physical storage device, such as a hard disk drive and/or a solid state drive, and/or a logical storage device, such as a database, a user-based logical data storage (e.g., a user's home directory and associated files), a network-attached storage, and a logical partition. A logical storage device may comprise data stored on part of and/or across a plurality of physical storage devices.

[0031] Each of engines 315, 320, and 325 may comprise any combination of hardware and programming to implement the functionalities of the respective engine. In examples described herein, such combinations of hardware and programming may be implemented in a number of different ways. For example, the programming for the engines may be processor executable instructions stored on a non-transitory machine-readable storage medium and the hardware for the engines may include a processing resource to execute those instructions. In such examples, the machine-readable storage medium may store instructions that, when executed by the processing resource, implement engines 315, 320, and 325. In such examples, system 300 may comprise the machine-readable storage medium storing the

instructions and the processing resource to execute the instructions, or the machine-readable storage medium may be separate but accessible to system 300 and the processing resource.

[0032] Command engine 315 may detect, according to a secure command performed on a data storage, that a security violation has occurred. For example, detect security violation instructions 130 may detect, according to a command execution, that a security violation associated with a data storage has occurred. The executed commands may be associated with assessing and/or remediating unauthorized access to data storage 150, such as by securing and/or removing data in data storage 150.

[0033] For example, detect security violation instructions 130 may comprise a list of secure commands associated with addressing suspected security breaches on data storage 150. Such commands may comprise, for example, secure delete commands for files in data storage 150, encryption commands, network configuration commands such as firewall adjustments and/or commands to disconnect users, applications, and/or communication sessions, and/or audit commands for security information such as access logs for device 100 and/or data storage 150. A secure delete command, for example, erases the data specified in the command and then overwrites the memory and storage location with random bits of data to prevent recovery. In some implementations, any command run with elevated permissions, such as those performed via a SUDO operation, may comprise a command associated with addressing a security breach.

[0034] Session engine 325 may determine, for at least one of a plurality of user sessions, whether the at least one of the plurality of user sessions is associated with an administrator user. For example, session engine 325 may identify user sessions 330(A)-(C) as not associated with administrators while administrator session 335 is associated with an administrator user.

[0035] A user session may comprise a local and/or network communication session with a computer such as device 310, such as may occur when a user has logged into device 310 and/or an application or service executing on device 310.

For example, a user session may be associated with a user of a web-based application wherein the user's web browser is accessing device 310 and data storage 340 via a network. In some implementations, the user session may be associated with a second command comprising a non-secure command, such as a standard data read and/or write command.

[0036] An administrator user may comprise a higher privileged user account than a non-administrator user. Such an account may be permitted to execute commands and/or applications, such as those that may affect an operating system of computing device 310. An administrator user may also be permitted to make changes that will affect other users. Administrators may change security settings, install software and hardware, and/or access all files on computing device 310.

[0037] In response to determining that the at least one of the plurality of user sessions is not associated with the administrator user, session engine 325 apply a restriction on access to the data storage for the at least one of the plurality of user sessions. In some implementations, the restriction may comprise a disconnection from the data storage, a blocking of an executing command associated with the data storage, a write restriction for the data storage, and/or a read restriction for the data storage.

[0038] For example, restrict access instructions 132 may, in response to detecting that the security violation has occurred, restrict access to data storage 340. For example, user sessions interacting with data storage 340 may be blocked from reading and/or writing to data storage 340 entirely, blocked writing while permitted to read, or vice versa, and/or blocked from executing non-secure commands while permitting other, secure commands to still be executed.

[0039] Different types and/or levels of restriction may be used, such as restricting non-administrative/super users, only restricting non-secure commands on data storage 340, and/or blocking only reads from data storage 340 or writes to data storage 340. For example, in response to determining that the second user session is associated with an administrator user, continued access to the data

storage may be permitted. In such an example, the administrator user may be notified of the detected security violation.

[0040] In some implementations, user sessions 330(A)-(C) and/or administrator session 335 may be notified of the security violation and/or may receive an error message regarding the block on reading/writing to data storage 340. In some implementations, read and/or write requests may be paused and/or the read/write processes may be placed in an idle state. In some implementations, user sessions interacting with data storage 340 may be closed and/or disconnected, and/or processes associated with such sessions may be terminated. In some implementations, restricting access to data storage 340 may comprise preventing a new user session from connecting to the data storage.

[0041] Security engine 320 may determine whether the security violation has been remediated according to whether the secure command has completed executing. For example, determine violation remediation instructions 134 may determine whether the security violation has been remediated. In some implementations, the security violation may be determined to have been remediated after the command associated with detecting the violation has been completed. For another example, the security violation may be determined to have been remediated after the session in which the command was detected has disconnected and/or exited a privileged state (e.g., a user of the session switches to a non-administrator user).

[0042] In response to determining that the security violation has been remediated, security engine 320 may cause session engine 325 to remove the restriction applied to the at least one of the plurality of user sessions. For example, restore access instructions 136 may, in response to determining that the security violation has been remediated, restore access to data storage 340 for user sessions 330(A)-(C). For example, idled read/write processes may be permitted to complete execution and/or new sessions may be permitted to connect to data storage 150.

[0043] The disclosed examples may include systems, devices, computer-readable storage media, and methods for data protection. For purposes of explanation, certain examples are described with reference to the components illustrated in the Figures. The functionality of the illustrated components may overlap, however, and may be present in a fewer or greater number of elements and components. Further, all or part of the functionality of illustrated elements may co-exist or be distributed among several geographically dispersed locations. Moreover, the disclosed examples may be implemented in various environments and are not limited to the illustrated examples.

[0044] Moreover, as used in the specification and the appended claims, the singular forms “a,” “an,” and “the” are intended to include the plural forms as well, unless the context indicates otherwise. Additionally, although the terms first, second, etc. may be used herein to describe various elements, these elements should not be limited by these terms. Instead, these terms are only used to distinguish one element from another.

[0045] Further, the sequence of operations described in connection with the Figures are examples and are not intended to be limiting. Additional or fewer operations or combinations of operations may be used or may vary without departing from the scope of the disclosed examples. Thus, the present disclosure merely sets forth possible examples of implementations, and many variations and modifications may be made to the described examples. All such modifications and variations are intended to be included within the scope of this disclosure and protected by the following claims.

CLAIMS

We claim:

1. A non-transitory machine-readable storage medium comprising instructions for data protection which, when executed by a processor, cause the processor to:

detect, according to a command execution, that a security violation associated with a data storage has occurred; and

in response to detecting that the security violation has occurred:

restrict access to the data storage,

determine whether the security violation has been remediated, and

in response to determining that the security violation has been remediated, restore access to the data storage.

2. The non-transitory machine-readable medium of claim 1, wherein the instructions to restrict access to the data storage comprise instructions to restrict access to a physical storage device.

3. The non-transitory machine-readable medium of claim 1, wherein the instructions to restrict access to the data storage comprise instructions to restrict access to a logical data storage.

4. The non-transitory machine-readable medium of claim 3, wherein the logical data storage comprises at least one of the following: a database, a user-based logical data storage, a network-attached storage, and a logical partition.

5. The non-transitory machine-readable medium of claim 1, wherein the command execution comprises a secure delete command.

6. The non-transitory machine-readable medium of claim 5, wherein the instructions to determine whether the security violation has been remediated

comprise instructions to determine whether the secure delete command has completed.

7. The non-transitory machine-readable medium of claim 1, wherein the instructions to restrict access to the data storage comprise instructions to block performance of at least one of the following: a non-secure data read command and a non-secure data write command.

8. A computer-implemented method for data protection comprising:

detecting, according to a first command performed on a data storage, that a security violation has occurred, wherein the first command comprises a secure command;

restricting access to the data storage for a user session, wherein the user session is associated with a second command comprising a non-secure command;

determining whether the security violation has been remediated; and

in response to determining that the security violation has been remediated, restoring access to the data storage for the user session.

9. The computer-implemented method of claim 8, wherein restricting access to the data storage for the user session comprises disconnecting the user session.

10. The computer-implemented method of claim 8, wherein restricting access to the data storage for the user session comprises permitting a third command to be executed.

11. The computer-implemented method of claim 10, wherein the third command comprises a read command associated with the data storage.

12. The computer-implemented method of claim 8, wherein restricting access to the data storage for the user session further comprises preventing a new user session from connecting to the data storage.

13. The computer implemented method of claim 8, wherein restricting access to the data storage for the user session further comprises determining whether a second user session is associated with an administrator user; and

in response to determining that the second user session is associated with the administrator user, permitting continued access to the data storage for the

second user session.

14. The computer implemented method of claim 13, further comprising, in response to determining that the second user session is associated with the administrator user, notifying the administrator user of the security violation.

15. A system for data protection, comprising:

a command engine to:

detect, according to a secure command performed on a data storage, that a security violation has occurred;

a session engine to:

determine, for at least one of a plurality of user sessions, whether the at least one of the plurality of user sessions is associated with an administrator user;

in response to determining that the at least one of the plurality of user sessions is not associated with the administrator user, apply a restriction on access to the data storage for the at least one of the plurality of user sessions, wherein the restriction comprises at least one of the following: a disconnection from the data storage, a blocking of an executing command associated with the data storage, a write restriction for the data storage, and a read restriction for the data storage; and

a security engine to:

determine whether the security violation has been remediated according to whether the secure command has completed executing; and

in response to determining that the security violation has been remediated, cause the session engine to remove the restriction applied to the at least one of the plurality of user sessions.

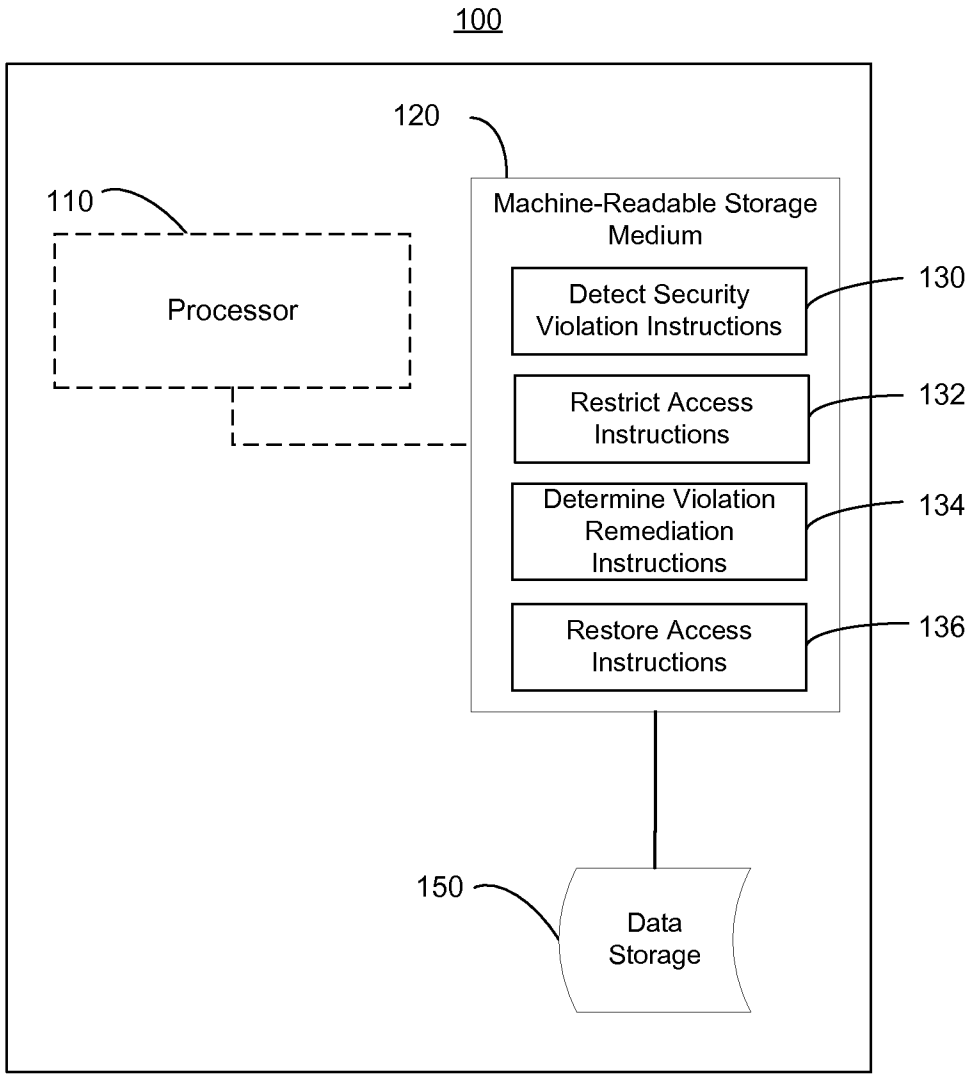
100
120
110
Machine-Readable Storage Medium
Processor
Detect Security Violation Instructions
130
Restrict Access Instructions
132
Determine Violation Remediation Instructions
134
Restore Access Instructions
136
150
Data Storage

FIG. 1

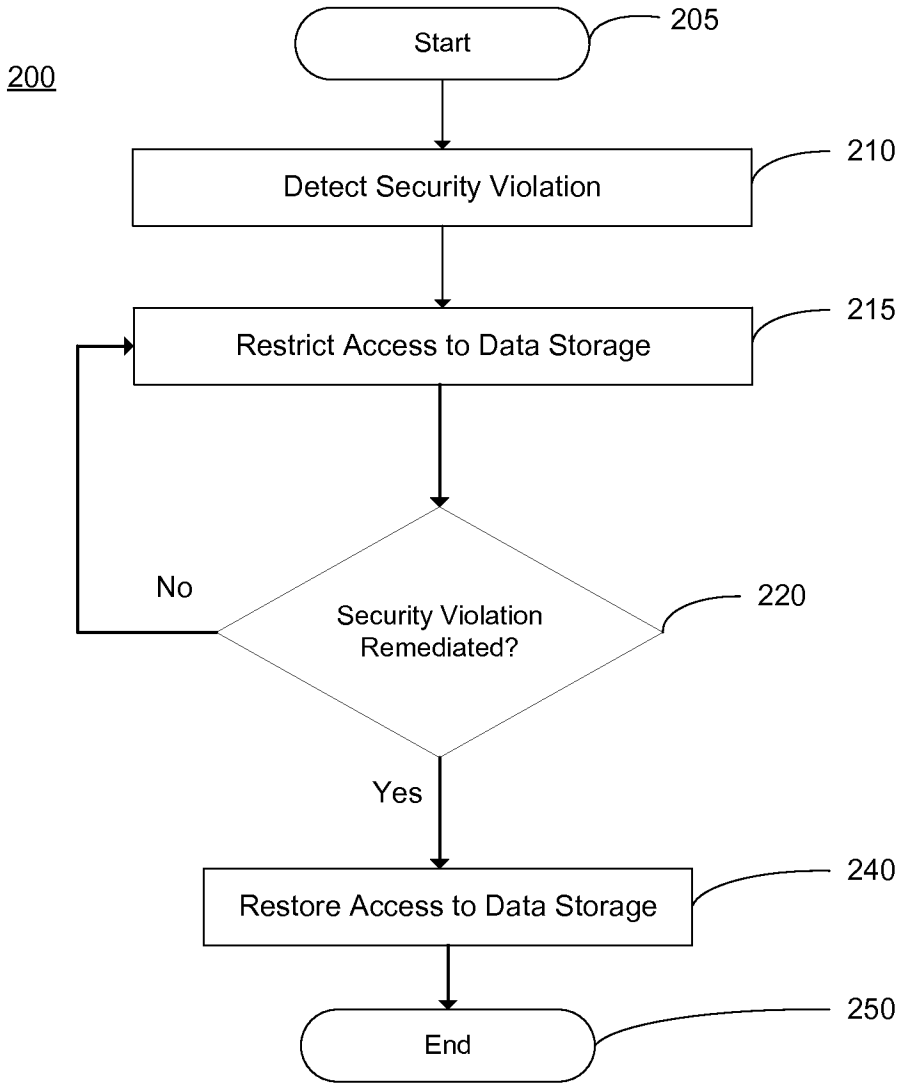
200
Start
205
Detect Security Violation
210
Restrict Access to Data Storage
215
Security Violation Remediated?
220
No
Yes
Restore Access to Data Storage
240
End
250

FIG. 2

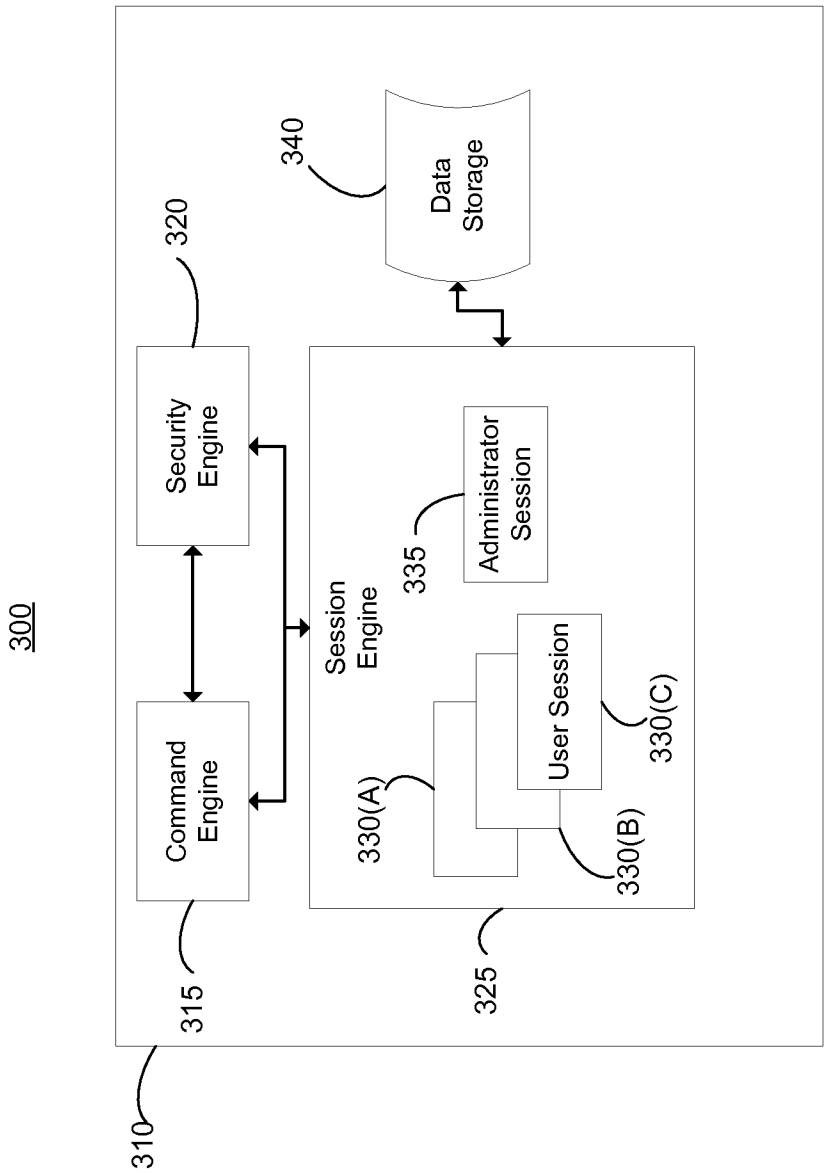
300
310
315
320
325
330(A)
330(B)
330(C)
335
340
Command Engine
Security Engine
Session Engine
User Session
Administrator Session
Data Storage

FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2015/028110

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/60(2013.01)i, G06F 21/62(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 21/60; G06F 12/02; G06F 17/30; G06F 12/14; G06F 12/00; G06K 19/07; H04L 9/00; G06F 21/00; G06F 21/62

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: data storage, access right, security violation, remediation, command, integrity

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2008-0162784 A1 (WILLY OBEREINER et al.) 03 July 2008 See paragraphs [0001], [0022], [0026]-[0027], [0039]-[0041], [0047], [0057]-[0059], [0063]; and figures 2, 7-8.	1-8,10-11,13-15
Y		9,12
Y	US 2010-0242082 A1 (DAVID P. KEENE et al.) 23 September 2010 See paragraphs [0059], [0062]-[0064]; and figure 1.	9,12
A		1-8,10-11,13-15
A	US 2002-0112131 A1 (ANTHONY S. FONG) 15 August 2002 See paragraphs [0024]-[0026]; and figure 4.	1-15
A	US 8255370 B1 (MICHEL ZOPPAS et al.) 28 August 2012 See column 10, lines 35-67; and figure 3A.	1-15
A	JP 2015-052950 A (NATIONAL INSTITUTE OF ADVANCED INDUSTRIAL & TECHNOLOGY et al.) 19 March 2015 See paragraphs [0005], [0008]-[0011]; and figure 1.	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 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
25 February 2016 (25.02.2016)	**25 February 2016 (25.02.2016)**

Name and mailing address of the ISA/KR
International Application Division
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
COMMISSIONER
Telephone No. +82-42-481-3578

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2015/028110

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008-0162784 A1	03/07/2008	US 7836269 B2	16/11/2010
US 2010-0242082 A1	23/09/2010	None	
US 2002-0112131 A1	15/08/2002	US 2003-0028739 A1	06/02/2003
		US 2006-0015780 A1	19/01/2006
		US 6292879 B1	18/09/2001
		US 6941444 B2	06/09/2005
		US 7146479 B2	05/12/2006
		US 7487507 B1	03/02/2009
US 8255370 B1	28/08/2012	US 7996373 B1	09/08/2011
JP 2015-052950 A	19/03/2015	US 2015-0074824 A1	12/03/2015