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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 December 2012 (20.12.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/173599 A1

(51) International Patent Classification:
G06F 21/20 (2006.01) *G06F 9/44* (2006.01)

(21) International Application Number:
PCT/US2011/040304

(22) International Filing Date:
14 June 2011 (14.06.2011)

(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) Inventors; and

(75) Inventors/Applicants *(for US only)*: **PEARSON, Siani** [GB/GB]; HP Ltd., Bristol Filton B3 (BUK03) M M215, Mail Stop M21, Longdown Avenue, Stoke Gifford Bristol BS34 8QZ (GB). **MONT, Marco Casassa** [IT/GB]; HP Ltd., Bristol Filton B3 (BUK03) M M215, Mail Stop M21, Longdown Avenue, Stoke Gifford Bristol BS34 8QZ (GB). **REID, Peter J.** [GB/US]; Hewlett-Packard Co., M/S H4-1A-37, 5400 Legacy, Plano, Texas 75024 (US).

(74) Agents: **FOY, Andrew T.** et al.; Hewlett-Packard Company, Intellectual Property Administration, 3404 E. 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, 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))*

(54) Title: SYSTEM AND METHOD FOR CONTROLLING ACCESS

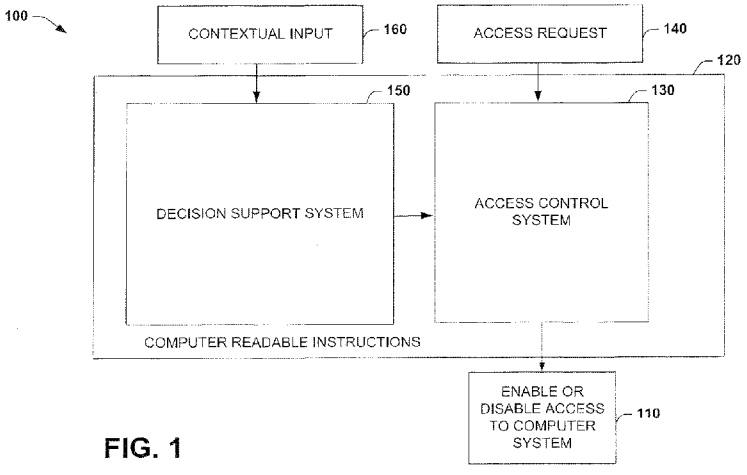

FIG. 1

(57) Abstract: One example provides an access control system to enable or disable admittance to a computer system based on an access request. A decision support system is provided to augment control decisions determined by the access control system, wherein the decision support system analyzes a contextual input to enable or disable the admittance to the computer system.

WO 2012/173599 A1

SYSTEM AND METHOD FOR CONTROLLING ACCESS

BACKGROUND

[0001] Access control is a system which enables an authority (e.g., computer) to control access to areas and resources in a given physical facility or computer-based information system. An access control system, within the field of physical security, is generally observed as the second layer in the security of a physical structure.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] FIG. 1 illustrates an example of a decision support access control system.

[0003] FIG. 2 illustrates an example of a system for decision support access control and associated databases.

[0004] FIG. 3 illustrates an example of a decision support system.

[0005] FIG. 4 illustrates an example of an access control system.

[0006] FIG. 5 illustrates a flowchart of an example method for decision support access control.

[0007] FIG. 6 illustrates an example of a computer system that can be employed to implement the systems and methods illustrated in FIGS. 1-5.

DETAILED DESCRIPTION

[0008] FIG. 1 illustrates an example of a decision support access control system 100. The system 100 includes computer readable instructions that provide functionality for enabling or disabling access to a computer system 110. In one example, this includes a computer readable medium 120 comprising computer readable instructions. Such instructions can include an access control system 130 to enable or disable admittance to a computer system 110 based on an access request 140 (or requests) from a requestor. A decision support system 150 is provided to

augment control decisions determined by the access control system 130, where the decision support system analyzes a current contextual input 160 (or inputs) associated with the requestor to enable or disable the admittance to the computer system 110. For example, the access control system 130 may analyze items such as passwords that are submitted via the access request 140 and submitted by the requestor or user of the system. The decision support system 150 may further analyze the contextual input 160 to determine whether or not access can be granted to the computer 110. In this example, contextual input 160 refers to a user's current situation or circumstances as they relate at the time of the request. Thus, a question relating to a requestor's mother's maiden name does not relate to current context or circumstance but rather a past event, where a question relating to the requestor's current country, citizenship, age, ID numbers such as passport or license numbers, or other current information, for example, help to establish relevant context for the decision support system 150 that can be employed to enable or disable entry to the computer at 110.

[0009] As will be described in more detail below with respect to FIG. 2, the access control system 130 can employ a policy to enable or disable admittance to the computer system 110. Also, the decision support system 150 can employ a decision support database (See FIG. 2) that stores rules and questionnaires, for example, to analyze the contextual input 160. The decision support database can include legal or legislative data, business constraint data, or security constraint data, for example. Other components of the access control system 130 include a policy enforcement point to generate the contextual input 160 for the decision support system 150. This can also include a policy decision point to facilitate redirection of the decision support system 150 in case of failure to the access request 140. As will be described in more detail below, other components may include an audit log to facilitate context determinations for the decision support system 150 which can also access a personal database to store confidential information of a user, wherein the confidential information is further processed to determine context for the decision support system. In another example, the decision support system 150 can generate questions or requests for information to further analyze a user's context. The

decision support system 150 can also analyze a user's access purposes, contractual terms, or contractual conditions in order to enable or disable admittance to the computer system 110.

[0010] In general, there is a desire to enhance traditional access control mechanisms within a range of service delivery models to facilitate that individual user needs and context-dependent legal and business requirements are taken into account. Furthermore, some of the required information utilized for access control decisions may not be immediately available or known or contemplated beforehand. The system 100 addresses these issues by introducing real-time accountability and complementing access control solutions with a decision support system 150.

[0011] For purposes of simplification of explanation, in the present example, different components of the system 100 are illustrated and described as performing different functions. However, one of ordinary skill in the art will understand and appreciate that the functions of the described components can be performed by different components, and the functionality of several components can be combined and executed on a single component. The components can be implemented, for example, as software (e.g., computer executable instructions), hardware (e.g., an application specific integrated circuit), or as a combination of both (e.g., firmware). In other examples, the components could be distributing among remote devices across a network as describe in more detail below with respect to FIG. 2.

[0012] FIG. 2 illustrates an example of a system 200 for decision support access control and associated databases. The system 200 includes a processing unit 210 (or processor) that executes instructions from a memory 214 that includes firmware or other storage media for storing computer executable instructions associated with a computer. The processing unit 210 and memory 214 can be provided as part of a hybrid tool that includes a decision support system 220 that is associated with components of an access control system as described in more detail below. For data access requests where there is 'missing information' or information that requires additional validation, the decision support system (DSS) 220 can be triggered to gather additional context that is utilized before an automated decision can be performed. As described previously, context is related to a user or

requestor's current condition or circumstance or situation, where automated questions can be queried by the decision support system 220 to determine such current conditions.

[0013] The DSS 220 can be used in order to allow (e.g., strongly) authenticated people to access protected resources by holding them accountable for statements and information they provide in order to access such resources. An end user at interface 224 requests access at 226 to a resource via a Policy Enforcement Point (PEP) 230. The PEP 230 intercepts this access request 226 and redirects it to a Policy Decision Point (PDP) 234. By making an access control decision that may also consider current business, contractual and regulatory rules, an automated result (e.g., access granted or denied) can be reached.

[0014] The overall process flow is shown in the system 200 where administrators or managers at 240 may vouch for credentials/assertions, where these statements and the end users' statements can be audited at 244 to facilitate accuracy and enterprise compliance. The DSS 220 can create awareness of what needs to be satisfied to receive access and can require the user to make statements (e.g., regarding current context), in addition to collecting credentials or other information from various sources.

[0015] The DSS 220 can be driven by a set of rules 250 with exception management and strong tracking of authenticated users' statements by means of auditing and checking at the audit log 244. A context 260 can be output by the PDP 234 to the DSS 220 for further interactions, where exception management can involve discretionary statements made by users or by administrators. The circumstances where these can occur can be covered by policies 270. Also, shown is a personal data and confidential information store 280 that can be processed by the PEP 230 to further determine current contextual conditions of the user or requestor.

[0016] In one aspect, the system 200 includes the memory 214 for storing computer executable instructions associated with a computer. This includes the processing unit 210 for accessing the memory 214 and executing the computer executable instructions. The computer executable instructions can include the

decision support system 220 to process a current contextual input to determine access to a computer system. The policy enforcement point 230 is provided to process access requests 226 to the computer system and to issue grants or to deny access to the computer system based on the current contextual input. The policy decision point 234 is provided to redirect control to the decision support system in the event of a denial of access to the computer system. The decision support database 250 stores rules and questionnaires to analyze the current contextual input, wherein the decision support database includes legal or legislative data, business constraint data, or security constraint data. The audit log 244 is employed to facilitate context determinations for the decision support system 220. The personal database 280 is provided to store confidential information of a user, wherein the confidential information is further processed to determine current context for the decision support system 220, wherein the decision support system generates questions or requests for information to further analyze a user's current context.

[0017] FIGS. 3 and 4 are now provided to illustrate example details of the decision support system 150 and access control system 130 depicted in FIG. 1. FIG. 3 illustrates an example of a decision support system 300 and is related to the decision support system 150 depicted in FIG. 1. As shown, contextual input 310 is processed by a decision support system 320 (DSS). Such input 310 can include answers to questions that are generated by the decision support system 320 to determine a requestor's current context or condition. After processing the contextual input 310, the decision support system 320 generates an automated decision 330 that is applied to augment access control decisions of a decision support system that is described in more detail below with respect to FIG. 4.

[0018] In general, the decision support system (DSS) 320 is a computer-based information system that supports business or organizational decision-making activities. The DSS 320 serves the management, operations, and planning levels of an organization and helps to make decisions, which may be rapidly changing and not easily specified in advance via policy or hard-coded rules. Thus, in this example, the DSS 320 can be associated with an access control system (described in FIG. 4) in order to grant or deny access to a computer system based on a user's present

context. The DSS 320 also includes knowledge-based systems. Thus, the DSS 320 can be an interactive software-based system to help decision makers compile useful information from a combination of raw data, documents, personal knowledge, or business models to identify and solve problems and make decisions regarding access and current context. As noted, in the example, the acquired knowledge of the DSS 320 can be employed to augment or assist access control decisions at 330.

[0019] FIG. 4 illustrates an example of an access control system 400 such as related to the access control system depicted at 130 of FIG. 1. In this example, the access control system 400 is illustrated with two main functional blocks. A policy enforcement point 410 (PEP) and a policy decision point 420 (PDP) may be provided as previously described with respect to FIG. 2. As noted previously, other components that are not illustrated may also be provided and these may include policy and personal data stores in addition to interfaces for accessing the access control system 400, for example. Access control systems 400 provide the essential services of identification and authentication (I&A), authorization, and accountability where: identification and authentication determine who can log on to a system, and the association of users with the software subjects that they are able to control as a result of logging in; authorization determines what a subject can do; accountability identifies what a subject (or all subjects associated with a user) did. As can be appreciated, other functions can also be served by the access control system 400 (e.g., coordinating with decision support system to perform joint security or access decision based on determined current contextual conditions).

[0020] FIG. 5 illustrates an example method 500 for decision support access control. It is noted that such method 500 can be automatically executed by one or more computer systems. At 510, the method 500 includes processing a request to access a computer system. As described previously, such initial processing can be provided by an access control system where initial authentication or authorization may occur (e.g., password exchange). At 520, the method includes analyzing a policy to access the computer system in conjunction with the request. Such policy analysis could occur at a policy decision point, where further data may be employed to gather other data from the requestor such as current contextual data, for example.

At 530, the method includes requesting a current user context associated with the policy before granting the access to the computer system. As described previously, such current context can be determined by a decision support system for example, where queries are sent to the requestor and analyzed in substantially real-time to enable or deny access to the requestor.

[0021] FIG. 6 is a schematic block diagram illustrating an example system 600 of hardware components capable of implementing examples disclosed in FIGS. 1-5. The system 600 can include various systems and subsystems. The system 600 can be a personal computer, a laptop computer, a workstation, a computer system, an appliance, an application-specific integrated circuit (ASIC), a server, a server blade center, a server farm, a mobile device, such as a smart phone, a personal digital assistant, and so forth.

[0022] The system 600 can include a system bus 602, a processing unit 604, a system memory 606, memory devices 608 and 610, a communication interface 612 (e.g., a network interface), a communication link 614, a display 616 (e.g., a video screen), and an input device 618 (e.g., a keyboard and/or a mouse). The system bus 602 can be in communication with the processing unit 604 and the system memory 606. The additional memory devices 608 and 610, such as a hard disk drive, server, stand alone database, or other non-volatile memory, can also be in communication with the system bus 602. The system bus 602 operably interconnects the processing unit 604, the memory devices 606-610, the communication interface 612, the display 616, and the input device 618. In some examples, the system bus 602 also operably interconnects an additional port (not shown), such as a universal serial bus (USB) port.

[0023] The processing unit 604 can be a computing device and can include an application-specific integrated circuit (ASIC). The processing unit 604 executes a set of instructions to implement the operations of examples disclosed herein. The processing unit can include a processor core.

[0024] The additional memory devices 606, 608 and 610 can store data, programs, instructions, database queries in text or compiled form, and any other information that can be needed to operate a computer. The memories 606, 608 and

610 can be implemented as computer-readable media (integrated or removable) such as a memory card, disk drive, compact disk (CD), or server accessible over a network. In certain examples, the memories 606, 608 and 610 can comprise text, images, video, and/or audio.

[0025] Additionally, the memory devices 608 and 610 can serve as databases or data storage. Additionally or alternatively, the system 600 can access an external system (e.g., a web service) through the communication interface 612, which can communicate with the system bus 602 and the communication link 614.

[0026] In operation, the system 600 can be used to implement, for example, a client computer, a printer server, and at least some components of printers the can be employed in a system that manages a print job. Computer executable logic for implementing the system 600 can reside in the system memory 606, and/or in the memory devices 608 and/or 610 in accordance with certain examples. The processing unit 604 executes one or more computer executable instructions originating from the system memory 606 and the memory devices 608 and 610. The term "computer readable medium" as used herein refers to a medium that participates in providing instructions to the processing unit 604 for execution.

[0027] What have been described above are examples. It is, of course, not possible to describe every conceivable combination of components or methods, but one of ordinary skill in the art will recognize that many further combinations and permutations are possible. Accordingly, this disclosure is intended to embrace all such alterations, modifications, and variations that fall within the scope of this application, including the appended claims.

CLAIMS

What is claimed is:

1. A computer readable medium comprising computer readable instructions comprising:

an access control system to enable or disable admittance to a computer system based on an access request from a requestor; and

a decision support system to augment control decisions determined by the access control system, wherein the decision support system analyzes a current contextual input associated with the requestor to enable or disable the admittance to the computer system.

2. The computer readable medium of claim 1, wherein the access control system employs a policy to enable or disable admittance to the computer system.

3. The computer readable medium of claim 1, wherein the decision support system employs a decision support database that stores rules and questionnaires to analyze the current contextual input.

4. The computer readable medium of claim 3, wherein the decision support database includes legal or legislative data, business constraint data, or security constraint data.

5. The computer readable medium of claim 3, further comprising a policy enforcement point to generate the contextual input for the decision support system.

6. The computer readable medium of claim 5, further comprising a policy decision point to facilitate redirection of the decision support system in case of failure to the access request.

7. The computer readable medium of claim 6, further comprising an audit log to facilitate context determinations for the decision support system.

8. The computer readable medium of claim 6, further comprising a personal database to store confidential information of a user, wherein the confidential information is further processed to determine current context for the decision support system.

9. The computer readable medium of claim 6, wherein the decision support system generates questions or requests for information to further analyze a user's current context.

10. The computer readable medium of claim 9, wherein the decision support system analyzes access purposes, contractual terms, or contractual conditions in order to enable or disable admittance to the computer system.

11. A method, comprising:

processing, by a computer, a request to access a computer system;

analyzing, by the computer, a policy to access the computer system in conjunction with the request; and

requesting, by the computer, a current user context associated with the policy before granting the access to the computer system.

12. The method of claim 11, further comprising granting or denying access to the computer system, by the computer, based on the current user context and the policy.

13. The method of claim 11, further comprising analyzing, by the computer, answered questions received from a user to determine the current user context.

14. The method of claim 13, further comprising processing, by the computer, a policy enforcement point or a policy decision point to determine the current user context.

15. A system, comprising:

a memory for storing computer executable instructions associated with a computer; and

a processing unit for accessing the memory and executing the computer executable instructions, the computer executable instructions comprising:

a decision support system to process a current contextual input to determine access to a computer system;

a policy enforcement point to process access requests to the computer system and to issue grants or to deny access to the computer system based on the current contextual input;

a policy decision point to redirect control to the decision support system in the event of a denial of access to the computer system;

a decision support database that stores rules and questionnaires to analyze the current contextual input, wherein the decision support database includes legal or legislative data, business constraint data, or security constraint data;

an audit log to facilitate context determinations for the decision support system; and

a personal database to store confidential information of a user, wherein the confidential information is further processed to determine current context for the decision support system, wherein the decision support system generates questions or requests for information to further analyze a user's current context.

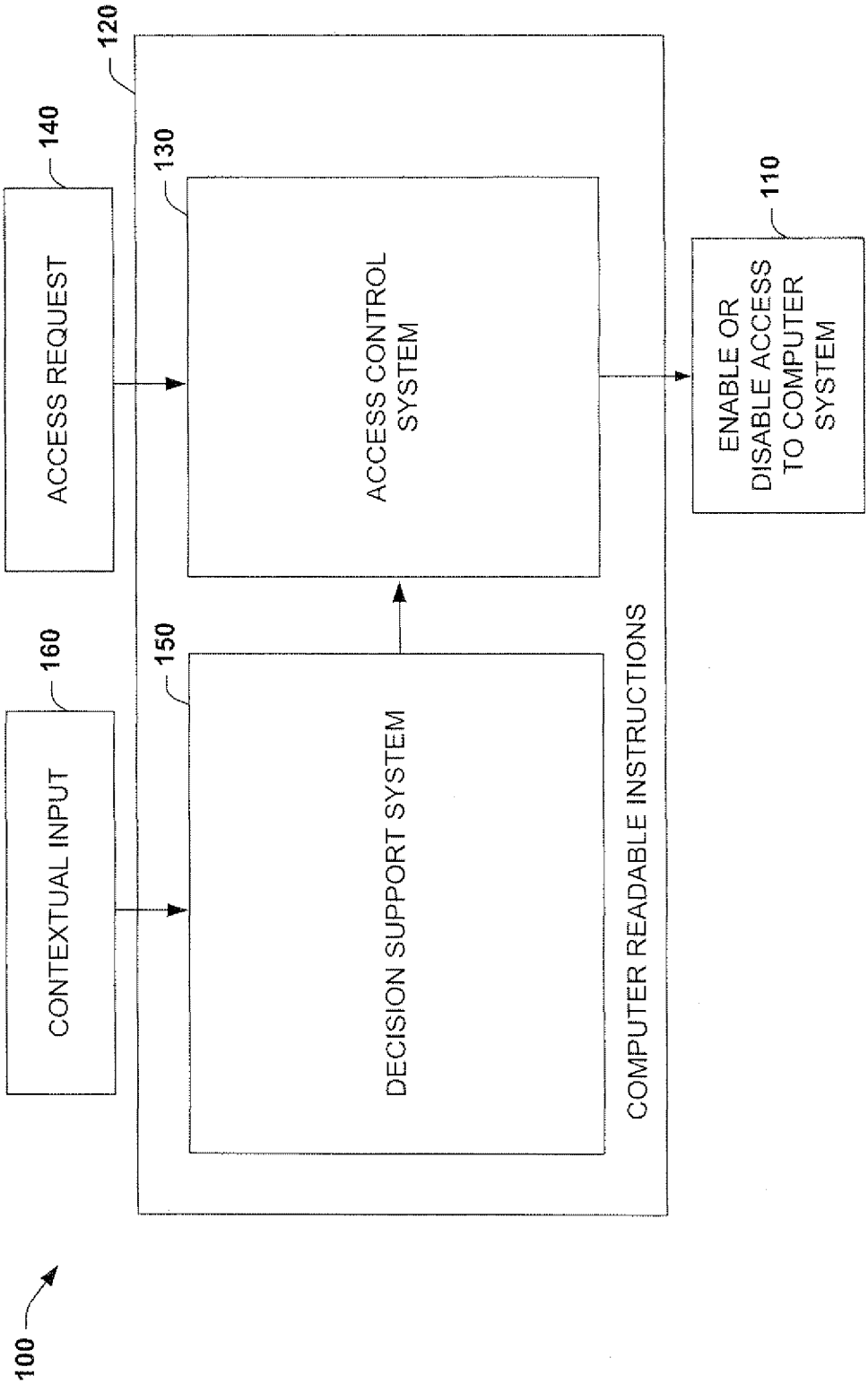
100
120
140
ACCESS REQUEST
130
ACCESS CONTROL SYSTEM
110
ENABLE OR DISABLE ACCESS TO COMPUTER SYSTEM
160
CONTEXTUAL INPUT
150
DECISION SUPPORT SYSTEM
COMPUTER READABLE INSTRUCTIONS

FIG. 1

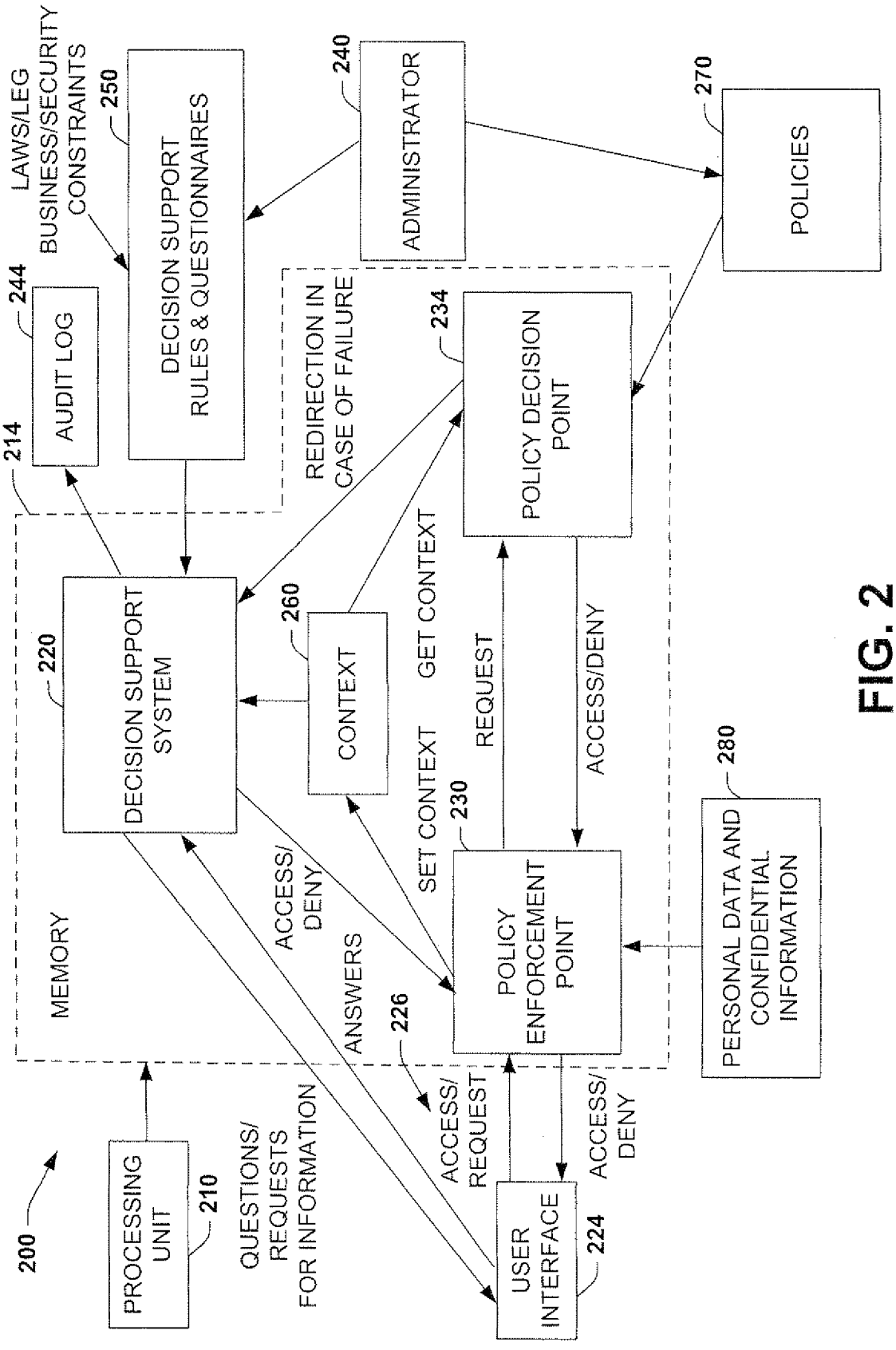
200
PROCESSING UNIT
210
QUESTIONS/ REQUESTS FOR INFORMATION
USER INTERFACE
224
ACCESS/ REQUEST
ACCESS/ DENY
MEMORY
214
DECISION SUPPORT SYSTEM
220
ACCESS/ DENY
ANSWERS
226
CONTEXT
260
SET CONTEXT
GET CONTEXT
POLICY ENFORCEMENT POINT
230
REQUEST
ACCESS/DENY
POLICY DECISION POINT
234
REDIRECTION IN CASE OF FAILURE
AUDIT LOG
244
DECISION SUPPORT RULES & QUESTIONNAIRES
250
LAWS/LEG BUSINESS/SECURITY CONSTRAINTS
ADMINISTRATOR
240
POLICIES
270
PERSONAL DATA AND CONFIDENTIAL INFORMATION
280

FIG. 2

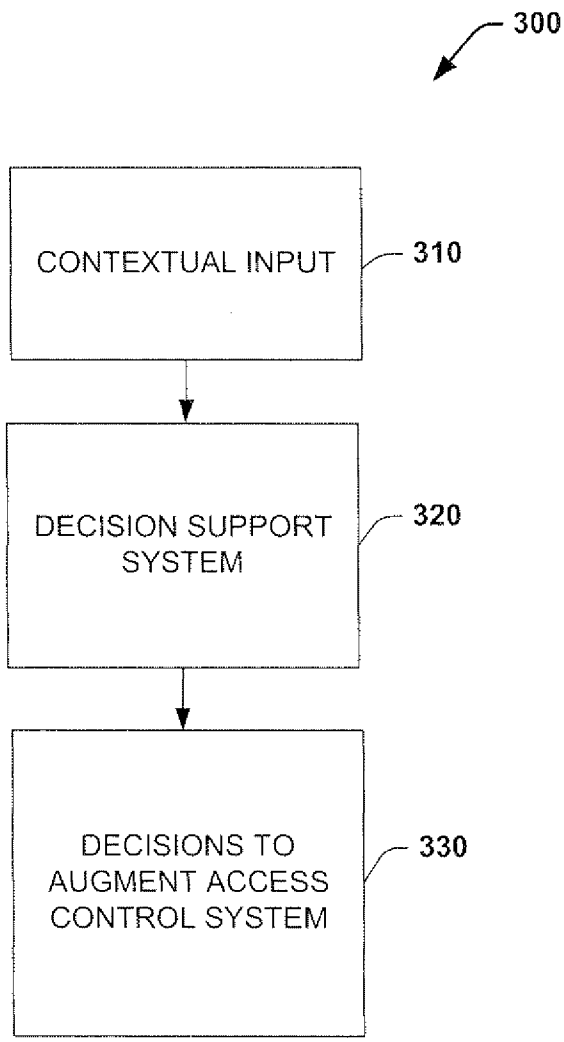
300
CONTEXTUAL INPUT
310
DECISION SUPPORT SYSTEM
320
DECISIONS TO AUGMENT ACCESS CONTROL SYSTEM
330

FIG. 3

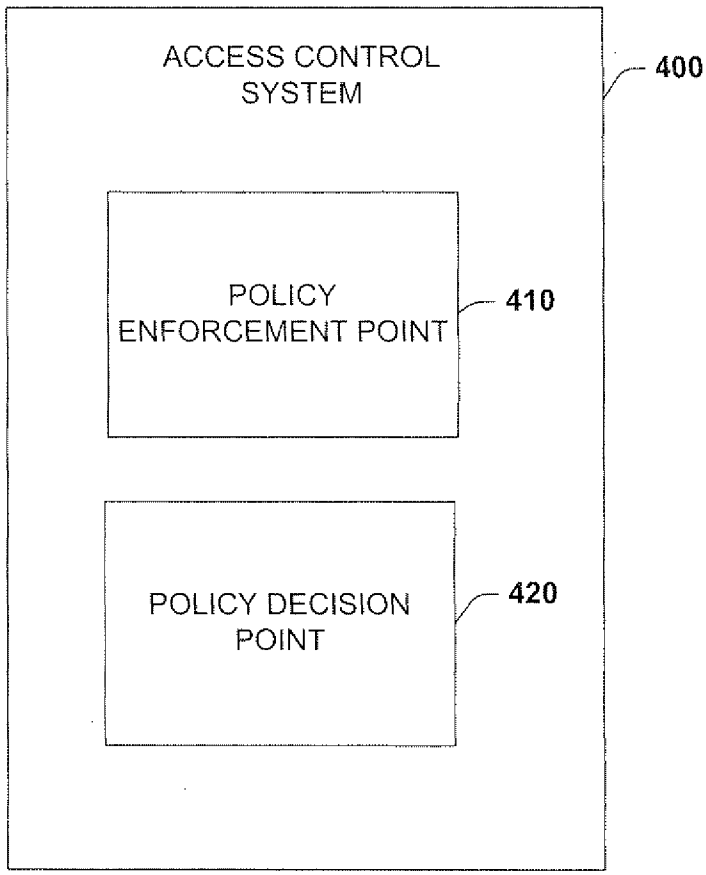
ACCESS CONTROL SYSTEM
400
POLICY ENFORCEMENT POINT
410
POLICY DECISION POINT
420

FIG. 4

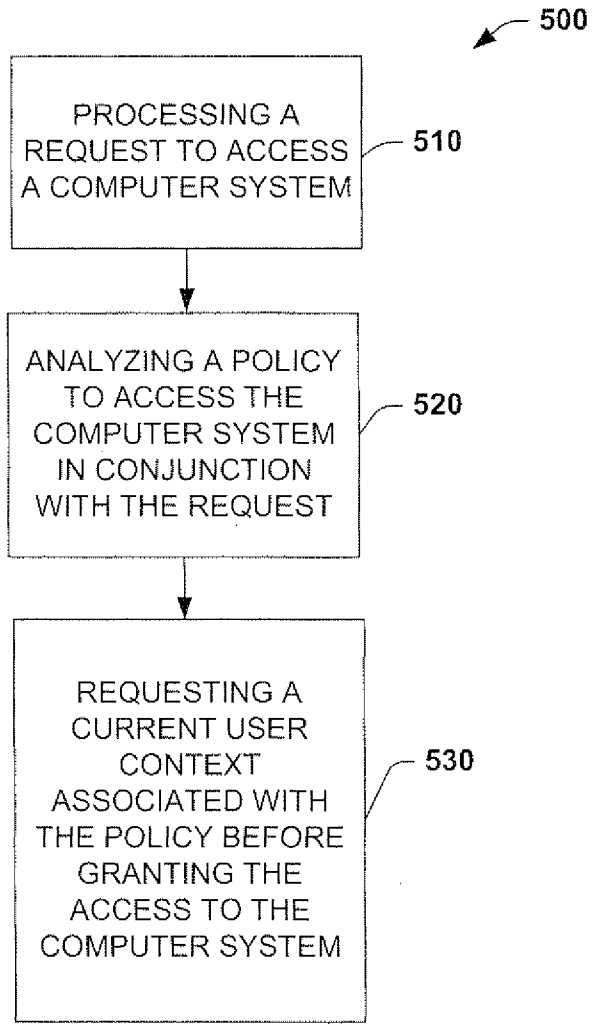
500
PROCESSING A REQUEST TO ACCESS A COMPUTER SYSTEM
510
ANALYZING A POLICY TO ACCESS THE COMPUTER SYSTEM IN CONJUNCTION WITH THE REQUEST
520
REQUESTING A CURRENT USER CONTEXT ASSOCIATED WITH THE POLICY BEFORE GRANTING THE ACCESS TO THE COMPUTER SYSTEM
530

FIG. 5

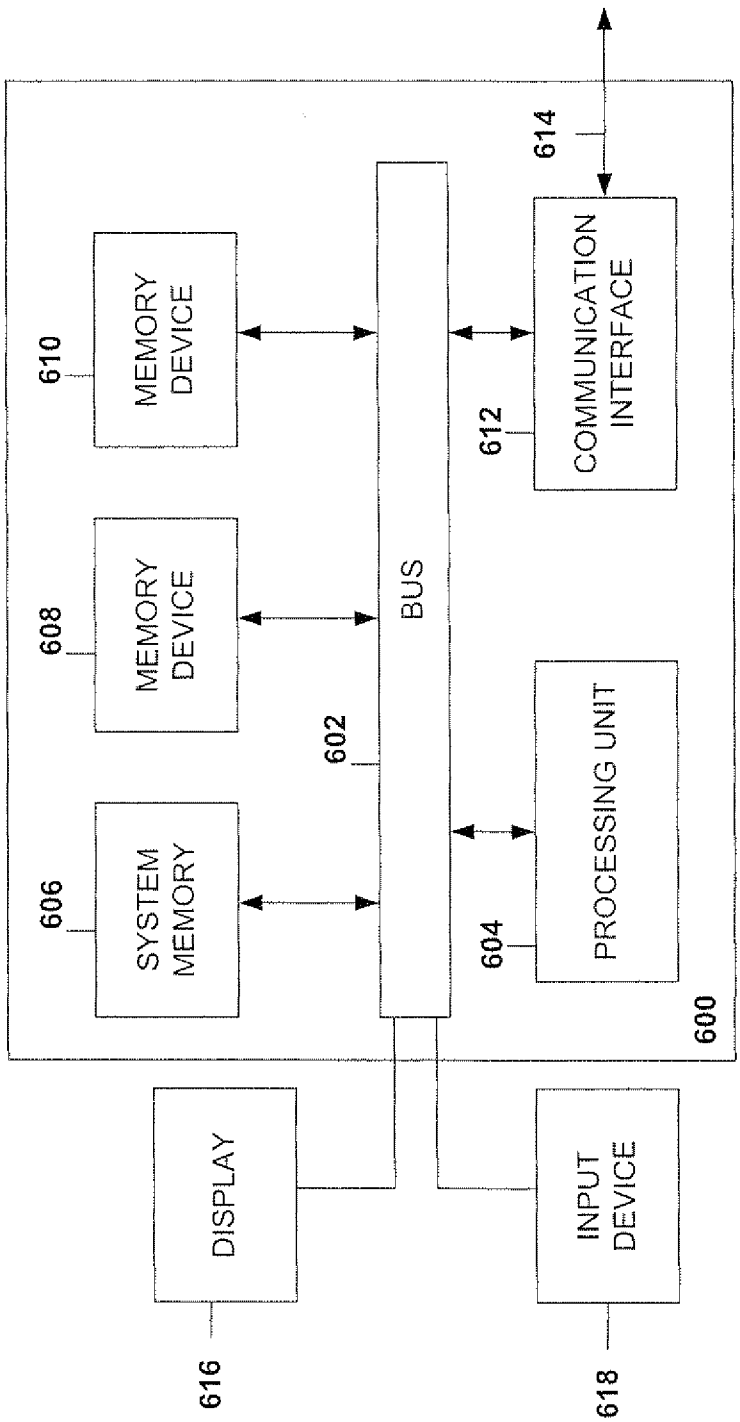
614
610
MEMORY DEVICE
612
COMMUNICATION INTERFACE
608
MEMORY DEVICE
BUS
602
606
SYSTEM MEMORY
604
PROCESSING UNIT
600
DISPLAY
INPUT DEVICE
616
618

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2011/040304

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/20(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 21/20; H04L 9/08; G06F 15/173; H04N 7/16; G06F 7/04

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:

(access*,login*,approv*,permi*,allow*,author*,secur*,authenti*,authorit*,verif*,authenticat*,valid*,invalid*,AUTHENTICAT*,VALID AT* CERTIFICAT* SECURIT* CERTIFY*)+(control* manag* monitor*)+(text* passport* licens* age* locati* positi* area* address*)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No
X	US 2011-0055905 A1 (SAKURAMOTO KENTARO) 03 March 2011 See abstract, paragraphs [0113]-[0116],[0163], claim 1 and figures 1-18.	1-15
A	US 2007-0276944 A1 (Kerry Samovar et al.) 29 November 2007 See abstract, paragraphs [0107]-[0110] and figures 1,2,5,6.	1-15
A	US 2010-0287584 A1 (STARIKOV YURI et al.) 11 November 2010 See abstract, paragraphs [0022]-[0026] and figure 2.	1-15
A	US 2008-0107274 A1 (WORTHY DAVID) 08 May 2008 See abstract, paragraphs [0021]-[0024] 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 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
27 FEBRUARY 2012 (27.02.2012)	**28 FEBRUARY 2012 (28.02.2012)**

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

UHM, In Kwon

Telephone No. 82-42-481-5712

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2011/040304

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011-0055905 A1	03.03.2011	CN 102004869 A	06.04.2011
		JP 2011-053821 A	17.03.2011
		JP 2011-053822 A	17.03.2011
US 2007-0276944 A1	29.11.2007	AU 2007-282165 A1	14.02.2008
		CA 2651543 A1	14.02.2008
		CN 101467173 A	24.06.2009
		EP 2016553 A2	21.01.2009
		EP 2016553 A4	29.06.2011
		MX 2008014302 A	09.12.2008
		WO 2008-018934 A2	14.02.2008
		WO 2008-018934 A3	12.06.2008
US 2010-0287584 A1	11.11.2010	None	
US 2008-0107274 A1	08.05.2008	WO 2007-149977 A2	27.12.2007
		WO 2007-149977 A3	03.04.2008