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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 July 2016 (28.07.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/118621 A1

(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/US2016/014120

(22) International Filing Date:
20 January 2016 (20.01.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201510031127.4 22 January 2015 (22.01.2015) CN

(71) Applicant: **ALIBABA GROUP HOLDING LIMITED** [—/US]; Fourth Floor, One Capital Place, P.O. Box 847, George Town, Grand Cayman (KY).

(72) Inventor: **WANG, Xiaodong**; Alibaba Group Legal Department, 5/f, Building 3, No 969 West Wen Yi Road, Yu Hang District, Hangzhou, 311121 (CN).

(74) Agent: **CHEN, Weiguo**; Finnegan, Henderson, Farabow, Garrett & Dunner LLP, 901 New York Avenue, NW, Washington, DC 20001-4413 (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).

Published:

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

(54) Title: METHODS, APPARATUS, AND SYSTEMS FOR RESOURCE ACCESS PERMISSION MANAGEMENT

(57) Abstract: A resource permission management method is disclosed. The method includes monitoring, by a processor, a sensitivity of a target resource, and when the sensitivity of the target resource changes, adjusting, by the processor, a permission level of the target resource according to the sensitivity of the target resource.

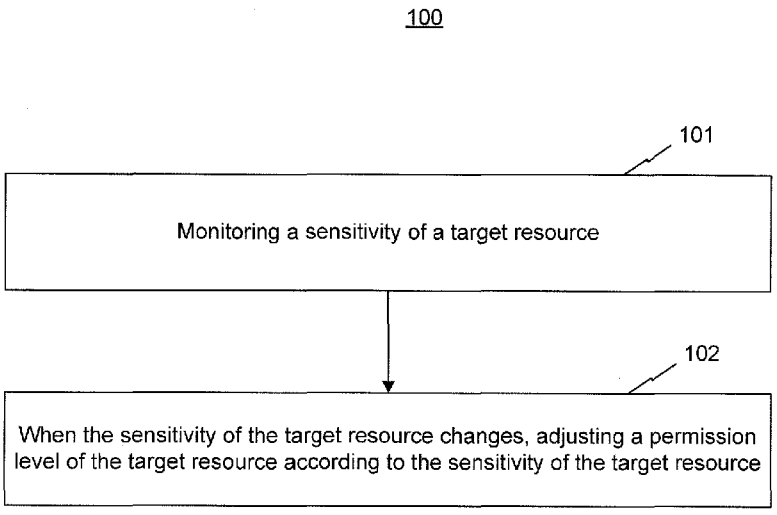


Fig. 1

WO 2016/118621 A1

METHODS, APPARATUS, AND SYSTEMS FOR RESOURCE ACCESS PERMISSION MANAGEMENT

CROSS REFERENCE TO RELATED APPLICATION

[001] The present application is based on and claims the benefits of priority to Chinese Application No. 201510031127.4, filed January 22, 2015, the entire contents of which are incorporated herein by reference.

TECHNICAL FIELD

[002] The present application relates to resource access level controls, and more particularly, to methods, apparatus, and systems for resource access permission management.

BACKGROUND

[003] Online resources open to public access are subjected to different risks such as identity theft. In response, service providers have implemented control methods to restrict the access. For resources containing less sensitive information, such as forum resources, access control is less strict; whereas for resources containing more sensitive information, such as ID numbers, member information and bank accounts, access control is more strict.

[004] Different types of resources have different sensitivities associated with their values. For example, if bank accounts are leaked, it may cost monetary loss to account holders or banks, and thus such resources have a very high sensitivity. For another example, if users are allowed to freely access video and image resources in a server, hackers may attack the server for various purposes, which can be potentially disastrous to server operations. Thus, such resources have a high sensitivity. For yet another example, advertisement information and online forum

information are public-oriented and usually do not involve confidentiality. They are resources with a low sensitivity.

[005] Existing practices of defining access/permission level are usually static and cannot dynamically adjust the access levels, nor have the flexibility to respond to an evolving resource content. It is common that an administrator, in a stage of defining permission, artificially divides permission levels of the resources based on importance of content currently included in the resources, which is a static manner. This manner of dividing permission levels for the resources fails to take dynamic changes of the resources into account, if the content included in the resources changes, it may result in that the permission levels of the resources change, if such a change cannot be done timely, it is likely to result in improper access control. For example, suppose that, in the stage of defining permission, the administrator divides a resource into a higher permission level and forbids users to access the resource at will. As time goes on, the content included in the resource changes, resulting in that the resource can be accessed by most users. However, as the permission level of the resource is not altered, it results in that only a small number of users can access the resource, which limits utilization of the resource. For another example, suppose that, in the stage of defining permission, the administrator divides a resource into a lower permission level and allows most users to access the resource. As time goes on, the content included in the resource changes. At this point, it is necessary to forbid some users to access the resource at will. However, as the permission level of the resource is not altered, it results in that most users can still access the resource, thus causing potential safety hazards to the resource.

SUMMARY

[006] One aspect of the present disclosure is directed to a resource permission management method. The method includes monitoring, by a processor, a sensitivity of a target resource; and when the sensitivity of the target resource changes, adjusting, by the processor, a permission level of the target resource according to the sensitivity of the target resource.

[007] Another aspect of the present disclosure is directed to a resource permission management apparatus. The apparatus includes a monitoring module configured to monitor a sensitivity of a target resource; and an adjustment module configured to, when the sensitivity of the target resource changes, adjust a permission level of the target resource according to the sensitivity of the target resource.

[008] Another aspect of the present disclosure is directed to a webpage resource permission management method. The method includes monitoring, by a web browser, a sensitivity of a webpage resource; and when the sensitivity of the webpage resource changes, adjusting, by a processor on a server, a permission level of the webpage resource according to the sensitivity of the webpage resource.

[009] Another aspect of the present disclosure is directed to a webpage resource permission management apparatus. The method includes a monitoring module configured to monitor a sensitivity of a webpage resource; and an adjustment module configured to, when the sensitivity of the webpage resource changes, adjust a permission level of the webpage resource according to the sensitivity of the webpage resource.

[010] Additional features and advantages of the present disclosure will be set forth in part in the following detailed description, and in part will be obvious from the

description, or may be learned by practice of the present disclosure. The features and advantages of the present disclosure will be realized and attained by means of the elements and combinations particularly pointed out in the appended claims.

[011] It is to be understood that the foregoing general description and the following detailed description are exemplary and explanatory only, and are not restrictive of the invention, as claimed.

BRIEF DESCRIPTION OF THE DRAWINGS

[012] The accompanying drawings, which constitute a part of this specification, illustrate several embodiments and, together with the description, serve to explain the disclosed principles.

[013] Fig. 1 is a flow diagram illustrating a resource access permission management method, according to an exemplary embodiment.

[014] Fig. 2 is a block diagram illustrating a resource access permission management apparatus, according to an exemplary embodiment.

[015] Fig. 3 is a block diagram illustrating a resource access permission management apparatus, according to another exemplary embodiment.

DETAILED DESCRIPTION

[016] Reference will now be made in detail to exemplary embodiments, examples of which are illustrated in the accompanying drawings. The following description refers to the accompanying drawings in which the same numbers in different drawings represent the same or similar elements unless otherwise represented. The implementations set forth in the following description of exemplary embodiments consistent with the present invention do not represent all implementations consistent with the invention. Instead, they are merely examples of

systems and methods consistent with aspects related to the invention as recited in the appended claims.

[017] FIG. 1 is a flow diagram of an embodiment of a resource access permission management method 100. The method may include:

[018] Step 101: monitoring a sensitivity of a target resource. The monitoring can be performed by a processor executing software codes stored on memories.

[019] Step 102: when the sensitivity of the target resource changes, adjusting a permission level of the target resource according to the sensitivity of the target resource. The adjusting can be performed by the processor executing the software codes stored on the memories.

[020] This example provides a resource access permission management method, which can be executed by a resource access permission management apparatus described below. In some embodiments, the resource access permission management apparatus is configured to manage permission levels of resources, so as to perform access control on the resources.

[021] Service systems generally provide some sources for users to access or use. If service systems are different, it is likely that resources which the service systems can provide are also different. Generally, sensitivity of different resources is also different. For the resources with different sensitivity, it is necessary to perform access control in different degrees, so as to improve security of the resources while giving full play to advantages of the resources.

[022] For instance, the service system can be an information management system inside an enterprise, and resources that can be provided mainly include some information type resources, for example, including employee information, enterprise information and the like. The employee information can include account

names, correspondence addresses, mobile phone numbers, and ID numbers of employees, and the like; the enterprise information can include an address of the enterprise, a name of the enterprise, registered assets of the enterprise and an internal BBS opened by the enterprise for the employees, and the like.

[023] For example, once the account names, the correspondence addresses, the mobile phone numbers, and the ID numbers of the employees, and the like are revealed, they can be easily illegally used by offenders, so as to cause inestimable losses to the employees and the enterprise. These resources are resources with higher sensitivity, and users are generally not allowed to access such resources at will. The address of the enterprise, the name of the enterprise, the registered assets of the enterprise and the internal BBS opened by the enterprise for the employees and the like are public-oriented, and thus do not involve confidentiality and are resources with lower sensitivity. For such resources, the more users that access or use them there are, the greater the value of the resources is, and thus, generally, most users are allowed to access the resources.

[024] The service system can include a resource permission management apparatus, for example, a network resource management system. The resources that can be provided can include network resources, for example, advertisement information, BBS information, video resources, image resources, member information and the like. The member information and the like are normally categorized with higher sensitivity. If users are allowed to access the video resources and the image resources above mentioned at will, it is likely that some hackers may attack servers that provide the resources, and thus these resources may be categorized with higher sensitivity. For such resources with higher sensitivity, generally, users are not allowed to access them at will. The

advertisement information, the BBS information and the like are public-oriented, and thus do not involve confidentiality and can be categorized with lower sensitivity. For such resources, the more users that access or use them there are, the greater the value of the resources is, and thus, generally, most users are allowed to access the resources.

[025] In order to facilitate access control on the resources provided by the service system, the resource permission management apparatus can divide permission levels for the resources with different sensitivities. The resource permission management apparatus can also adjust a permission level of a resource timely, so as to facilitate access control on the resource. The resource permission management apparatus can monitor the sensitivity of a target resource, and when the sensitivity of the target resource changes, the resource permission management apparatus can adjust a permission level of the target resource according to the sensitivity of the target resource.

[026] In some embodiments of the present disclosure, the resource permission management apparatus can periodically monitor a sensitivity of a target resource, and when it is found that sensitivity of the target resource in a current cycle is different from that in a previous cycle, adjust a permission level of the target resource according to the sensitivity of the target resource in the current cycle.

[027] In one embodiment, the resource permission management apparatus can monitor a sensitivity of a target resource in real time, and when it is found that the sensitivity of the target resource changes, adjust a permission level of the target resource according to the sensitivity of the target resource.

[028] The sensitivity of the target resource can be embodied through sensitive information included in the target resource. The sensitive information can

be defined differently according to a different application scenario. The sensitive information referred to in this example is information which is generally recognized as having higher requirements for confidentiality in various application scenarios, for example, a user's account number, bank card number, mobile phone number and other similar information.

[029] In some embodiments, the sensitivity of the target resource can be measured through a number of pieces of sensitive information included in the target resource. The resource permission management apparatus can monitor the number of the pieces of sensitive information included in the target resource, and determine the sensitivity of the target resource according to the number of the pieces of sensitive information included in the target resource. The higher the number of the pieces of sensitive information included in the target resource is, the higher the sensitivity of the target resource is; on the contrary, the lower the number of the pieces of sensitive information included in the target resource is, the lower the sensitivity of the target resource is.

[030] Further, in some embodiments, the sensitivity of the target resource can be measured through a type of sensitive information included in the target resource. The resource permission management apparatus can monitor the type of the sensitive information included in the target resource, and determine the sensitivity of the target resource according to the type of the sensitive information included in the target resource. Different types of sensitive information have different requirements for confidentiality. The higher the requirements of the sensitive information included in the target resource for the confidentiality is, the higher the sensitivity of the target resource is; the lower the requirements of the sensitive

information included in the target resource for the confidentiality is, the lower the sensitivity of the target resource is.

[031] Further, in some embodiments, the sensitivity of the target resource can be measured through the number of pieces of sensitive information included in the target resource and/or a type of the sensitive information. The resource permission management apparatus can monitor the number of the pieces of sensitive information included in the target resource and the type of the sensitive information, and determine the sensitivity of the target resource according to the number of the pieces of sensitive information included in the target resource and the type of the sensitive information. The higher the number of the pieces of sensitive information included in the target resource is, the higher the requirements of the sensitive information for confidentiality is, then the higher the sensitivity of the target resource is; on the contrary, the lower the number of the pieces of sensitive information included in the target resource is, the lower the requirements of the sensitive information for confidentiality is, then the lower the sensitivity of the target resource is. For a situation where the same number of pieces of sensitive information is included, the higher the requirements of the sensitive information included for confidentiality is, then the higher the sensitivity of the target resource is. For a situation where the sensitive information included has the same requirement for confidentiality, the higher the number of the pieces of sensitive information included is, then the higher the sensitivity of the target resource is.

[032] In one embodiment, the manner in which the resource permission management apparatus adjusts a permission level of a target resource according to the sensitivity of the target resource includes: determining a sensitivity level corresponding to the sensitivity of the target resource; and setting the permission

level of the target resource to a permission level corresponding to the sensitivity level.

[033] In some embodiments, after the resource permission management apparatus adjusts the permission level of the target resource, the resource permission management apparatus can notify an administrator, for example, by sending a notification message to the administrator in a manner such as a short message or an email, to remind the administrator that the permission level of the target resource changes and further verifying can be carried out.

[034] In some embodiments, the sensitivity level and the permission level can be set according to an application scenario. Illustration is given below, as shown in Table 1, the sensitivity level can be determined according to the number of the pieces of sensitive information, but the sensitivity level is not limited to 1, 2 and 3, and the permission level is not limited to ordinary, important and confidential levels either. A user may use other sensitivity levels and permission levels.

[035] Table 1

Permission level	Sensitivity level	Number of pieces of sensitive information	Description
ordinary	1	0	Calculation is made with a weight value of each piece of sensitive information being 1. The sensitive information includes: ID numbers, mobile phone numbers, bank card numbers, emails, and the like.
important	2	0-N; N is a natural number greater than 1	
confidential	3	>N	

[036] In some embodiments, by monitoring sensitivity of a target resource, a permission level of the target resource is adjusted according to the sensitivity of the target resource when the sensitivity of the target resource changes. The present application can timely adjust the permission level of the target resource according to the change in the sensitivity of the target resource, in a dynamic manner. For example, when sensitivity of a resource becomes from lower to higher, the resource permission management apparatus can adjust the permission level of the resource from the original "ordinary" to "confidential," and the access control on the resource can be changed from the original "allow most of users to access" into "forbid users to access at will", or changed into "allow users at higher levels to access", or the access control can be strengthened in a manner of multi-level examination and approval and verifying, and so on, so as to ensure security of the resource and reduce a safety risk. For another example, when sensitivity of a resource becomes from higher to lower, the resource permission management apparatus can adjust the permission level of the resource from the original "confidential" to "ordinary", and the access control on the resource can be changed from the original "forbid users to access at will" into "allow most of users to access", or changed into "allow users at lower levels to access", or the access control can be loosened in a manner of a single-level examination and approval, and so on, so as to facilitate that the resource is fully used.

[037] In one embodiment, the resource permission management apparatus, in addition to adjusting the permission level of the resource, can also be responsible for an access control process of the resource, so as to achieve access control on the resource. When a user needs to access the target resource, for example, through a terminal device, the terminal device can send a resource access request to the

resource permission management apparatus. The resource access request generally carries user information and identification information of a resource to be accessed. The identification information of the resource to be accessed is used to identify a resource that the user makes a request for accessing, which mainly refers to the target resource in this example; the user information mainly includes identity, permission level, and other information of the user who makes a request for accessing the target resource. The resource permission management apparatus receives the resource access request sent by the terminal device; determines whether the user is an authorized user. That is, for example, determining whether the user is qualified to access the target resource; if the determination result is Yes, allowing the user to access the target resource; and if the determination result is No, refusing the user to access the target resource.

[038] In one embodiment, the resource permission management apparatus can set an authorization code for the target resource, and sends the authorization code to the user who is qualified to access the target resource. Based on this, determining, by the resource permission management apparatus, whether the user who sends the resource access request is an authorized user can include: determining whether the resource access request includes the authorization code of the target resource; if the determination result is Yes, determining that the user is an authorized user; and if the determination result is No, determining that the user is not an authorized user.

[039] In some embodiments, if the user is determined to be an authorized user, the resource permission management apparatus can send the target resource to the user, to allow the user to access the target resource; when the user is not determined to be an authorized user, the resource permission management

apparatus refuses the user to access the target resource by not sending the target resource to the user.

[040] In some other embodiments, if the user is determined to be an authorized user, the resource permission management apparatus can allow the user to log in to a device, e.g., a server, where the target resource is located, to allow the user to access the target resource; when the user is not determined to be an authorized user, the resource permission management apparatus forbids the user to log in to the device where the target resource is located, to refuse the user to access the target resource.

[041] In one embodiment, a user can apply for the authorization code to access the target resource to the resource permission management apparatus. For example, a user can apply for the authorization code to the resource permission management apparatus after being refused to access the target resource by the resource permission management apparatus due to the absence of the authorization code; or a user can also previously apply for the authorization code to the resource permission management apparatus before applying for access to the target resource. When the user needs to apply for the authorization code of the target resource, the user can send an authorization request to the resource permission management apparatus, in which the authorization request can generally include user information and identification information of the target resource. The resource permission management apparatus receives the authorization request sent by the user, verifies the user according to the authorization request and the permission level of the target resource. The resource permission management apparatus can determine the target resource according to the identification information of the target resource in the authorization request, and then verify whether the user is qualified to

access the target resource with the permission level according to the permission level of the target resource and the user information in the authorization request. If the user passes the verification, the resource permission management apparatus can send the authorization code of the target resource to the user, so that the user can access the target resource.

[042] In one embodiment, the above target resource can be a webpage resource. Sensitivity of the webpage resource is monitored, when the sensitivity of the webpage resource changes, a permission level of the webpage resource is adjusted according to the sensitivity of the webpage resource, thereby achieving the purpose of timely adjusting the permission level of the webpage resource, so as to facilitate access control on the webpage resource.

[043] In some embodiments, the resource permission management apparatus can be implemented by embedding software codes in a webpage browser. In some other embodiments, the resource permission management apparatus can be implemented in a distributed deployment manner. For example, a monitoring function is deployed at the browser, while a permission level adjustment function is deployed at a server side. An implementation flow of the distributed resource permission management apparatus is described below in detail.

[044] A browser monitors sensitivity of a webpage resource and sends the sensitivity of the webpage resource to a server, and the server determines whether the sensitivity of the webpage resource changes and, when determining that the sensitivity of the webpage resource changes, adjusts a permission level of the webpage resource according to current sensitivity of the webpage resource.

[045] In some embodiments, the browser can monitor the sensitivity of the webpage resource regularly. Alternatively, the browser can monitor the sensitivity of

the webpage resource when rendering the webpage resource. For example, the user can click a URL of the webpage resource to send a resource access request, and the browser, when receiving the resource access request, renders the webpage resource and monitors the sensitivity of the webpage resource.

[046] Further, in some embodiments, the browser, after receiving the resource access request sent by the user, determines whether the user who sends the resource access request is an authorized user. That is, for example, determining whether the user is qualified to access the webpage resource; if the determination result is Yes, returning the webpage resource to the user; and if the determination result is No, refusing to return the webpage resource to the user.

[047] The foregoing exemplary methods are described as a series of combinations of steps so as to simplify the description. However, those skilled in the art should understand that the present application is not limited by a sequence of the combination of the steps described, because some steps can be performed in other sequences or at the same time in accordance with the present application.

[048] In the foregoing examples, the description about each example has its own focus, and reference can be made to the related description of other examples for the part not detailed in a certain example.

[049] FIG. 2 is a schematic structural diagram of a resource permission management apparatus 200 provided as an example of the present application. As shown in FIG. 2, the apparatus includes a monitoring module 21 and an adjustment module 22. The monitoring module 21 and adjustment module 22 can be implemented by a processor executing software codes stored on memories.

[050] The monitoring module 21 is configured to monitor a sensitivity of a target resource. The adjustment module 22 is configured to, when the monitoring

module 21 monitors that the sensitivity of the target resource changes, adjust a permission level of the target resource according to the sensitivity of the target resource monitored by the monitoring module 21.

[051] In some embodiments, the monitoring module 21 is configured to: periodically monitor the sensitivity of the target resource; or monitor the sensitivity of the target resource in real time.

[052] In one embodiment, the monitoring module 21 is configured to monitor a number of pieces of sensitive information included in the target resource and/or a type of the sensitive information, and determine the sensitivity of the target resource according to the number of the pieces of sensitive information and/or the type of the sensitive information.

[053] In one embodiment, the adjustment module 22 is configured to determine a sensitivity level which the sensitivity of the target resource is at when the sensitivity of the target resource changes, and adjust the permission level of the target resource to a permission level corresponding to the sensitivity level.

[054] In one embodiment, as shown in FIG. 3, the resource permission management apparatus 300 further comprises: a first receiving module 23, a determination module 24 and an access control module 25. The first receiving module 23 is configured to receive a resource access request sent by a user terminal device. The determination module 24 is configured to determine whether the user is an authorized user. The access control module 25 is configured to, when the determination result of the determination module 24 is Yes, allow the user to access the target resource; and if the determination result of the determination module 24 is No, refuse the user to access the target resource. The first receiving module 23,

determination module 24 and access control module 25 can be implemented by a processor executing software codes stored on memories.

[055] In one embodiment, the determination module 24 is configured to determine whether the resource access request includes a permission code of the target resource. If the determination result is Yes, the determination module 24 determines that the user is an authorized user; and if the determination result is No, the determination module 24 determines that the user is not an authorized user.

[056] In one embodiment, as shown in FIG. 3, the resource permission management apparatus further comprises a second receiving module 26, a verifying module 27, and a sending module 28. The second receiving module 26 is configured to receive an authorization request sent by the user terminal device. The verifying module 27 is configured to verify the user according to the authorization request received by the second receiving module 26 and the permission level of the target resource. The sending module 28 is configured to, when the user passes the verification, send the permission code of the target resource to the user. The second receiving module 26, verifying module 27, and sending module 28 can be implemented by a processor executing software codes stored on memories.

[057] The resource permission management apparatus provided in this example, by monitoring sensitivity of a target resource, adjusts a permission level of the target resource according to the sensitivity of the target resource when the sensitivity of the target resource changes. The resource permission management apparatus provided in this example can timely adjust the permission level of the target resource according to the change in the sensitivity of the target resource in a dynamic manner.

[058] The present disclosure also provides a webpage resource permission management apparatus, which may include a monitoring module and an adjustment module. The monitoring module is configured to monitor a sensitivity of a webpage resource. The adjustment module is configured to, when the sensitivity of the webpage resource changes, adjust a permission level of the webpage resource according to the sensitivity of the webpage resource monitored by the monitoring module.

[059] The webpage resource permission management apparatus according to this example can be implemented by embedding software codes in a browser, or can also be implemented through distributed deployment, that is, for example, the monitoring module being deployed at a browser, and the adjustment module is deployed at a server.

[060] The webpage resource permission management apparatus provided in this example can timely adjust the permission level of the webpage resource according to the change in the sensitivity of the webpage resource in a dynamic manner.

[061] Those skilled in the art should understand that, reference can be made to the corresponding process in the foregoing method examples for the working procedures of the system, apparatus and modules described above, and will not be repeated herein in order to make the description convenient and concise.

[062] In the several examples provided in the present application, it should be understood that the system, apparatus and method disclosed may be implemented in other manners. For example, the apparatus examples described above are only exemplary. For example, division of the modules/units is merely division of a logical function and a division in another manner may exist in actual

implementation. For example, a plurality of units or components may be combined or integrated into another system, or some features may be ignored or not performed. In addition, the mutual coupling or direct coupling or communication connections displayed or discussed may be implemented by using some interfaces, and the indirect coupling or communication connections between the apparatus or modules may be implemented electrically or in another form.

[063] The modules/units described as separate parts may be or may not be physically separate, and parts displayed as modules/units may be or may not be physical modules/units, may be located in one position, or may be distributed on a plurality of network units. Some or all of the modules/units may be selected according to actual needs to achieve the objectives of the solutions of the examples.

[064] In addition, each of functional modules/units in each of the examples of the present application may be integrated into one processing unit, or each of the modules/units may exist alone physically, or two or more of the above modules/units may be integrated into one processing unit. The modules/units may be logical modules implemented by software codes, or implemented in the form of hardware, or may be implemented in the form of hardware plus a software functional unit. For example, the modules/units may be implemented by a processor executing software instructions stored in computer readable memories.

[065] The specification has described methods, apparatus, and systems for resource permission management. The illustrated steps are set out to explain the exemplary embodiments shown, and it should be anticipated that ongoing technological development will change the manner in which particular functions are performed. Thus, these examples are presented herein for purposes of illustration, and not limitation. For example, steps or processes disclosed herein are not limited

to being performed in the order described, but may be performed in any order, and some steps may be omitted, consistent with disclosed embodiments. Further, the boundaries of the functional building blocks/modules have been arbitrarily defined herein for the convenience of the description. Alternative boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed. Alternatives (including equivalents, extensions, variations, deviations, etc., of those described herein) will be apparent to persons skilled in the relevant art(s) based on the teachings contained herein. Such alternatives fall within the scope and spirit of the disclosed embodiments.

[066] While examples and features of disclosed principles are described herein, modifications, adaptations, and other implementations are possible without departing from the spirit and scope of the disclosed embodiments. Also, the words "comprising," "having," "containing," and "including," and other similar forms are intended to be equivalent in meaning and be open ended in that an item or items following any one of these words is not meant to be an exhaustive listing of such item or items, or meant to be limited to only the listed item or items. It must also be noted that as used herein and in the appended claims, the singular forms "a," "an," and "the" include plural references unless the context clearly dictates otherwise. It also should be noted that as used herein and in the appended claims, the phrases "by a processor/browser," and the like include partially or fully by a processor/browser, by a processor/browser in combination with other hardware and/or software, by one or more of processor/browser, and the like.

[067] Furthermore, one or more computer-readable storage media may be utilized in implementing embodiments consistent with the present disclosure. A computer-readable storage medium refers to any type of physical memory on which

information or data readable by a processor may be stored. Thus, a computer-readable storage medium may store instructions for execution by one or more processors, including instructions for causing the processor(s) to perform the steps or stages or implement the modules consistent with the embodiments described herein. The term "computer-readable storage medium" should be understood to include tangible items and exclude carrier waves and transient signals, i.e., be non-transitory. Examples include RAM, ROM, volatile memory, nonvolatile memory, hard drives, CD ROMs, DVDs, flash drives, disks, and any other known physical storage media.

[068] It will be appreciated that the present invention is not limited to the exact construction that has been described above and illustrated in the accompanying drawings, and that various modifications and changes can be made without departing from the scope thereof. It is intended that the scope of the invention should only be limited by the appended claims.

WHAT IS CLAIMED IS:

1. A resource permission management method, comprising:

monitoring, by a processor, a sensitivity of a target resource; and

when the sensitivity of the target resource changes, adjusting, by the processor, a permission level of the target resource according to the sensitivity of the target resource.

2. The method of claim 1, wherein monitoring the sensitivity includes:

monitoring a number of pieces and/or a type of the sensitive information of the target resource; and

determining the sensitivity of the target resource according to the number of pieces and/or the type of the sensitive information.

3. The method of claim 1, wherein adjusting the permission level of the target resource according to the sensitivity of the target resource includes:

determining a sensitivity level corresponding to the sensitivity of the target resource; and

setting the permission level of the target resource to a permission level corresponding to the sensitivity level.

4. The method of claim 1, further comprising:

receiving a resource access request from a user terminal device;

determining whether the user is an authorized user;

if the user is determined to be an authorized user, allowing the user to access the target resource; and

if the user is not determined to be an authorized user, refusing the user to access the target resource.

5. The method of claim 4, wherein determining whether the user is an authorized user includes:

determining whether the resource access request includes a permission code of the target resource;

if the resource access request is determined to include a permission code of the target resource, determining that the user is an authorized user; and

if the resource access request is not determined to include a permission code of the target resource, determining that the user is not an authorized user.

6. The method of claim 5, further comprising:

receiving an authorization request from the user terminal device;

verifying the user according to the authorization request and the permission level of the target resource; and

if the user passes the verification, sending the permission code of the target resource to the user.

7. A resource permission management apparatus, comprising:

a monitoring module configured to monitor a sensitivity of a target resource; and

an adjustment module configured to, when the sensitivity of the target resource changes, adjust a permission level of the target resource according to the sensitivity of the target resource.

8. The apparatus of claim 7, wherein the monitoring module is further configured to:

monitor a number of pieces and/or a type of the sensitive information of the target resource; and

determine the sensitivity of the target resource according to the number of pieces and/or the type of the sensitive information.

9. The apparatus of claim 7, wherein the adjustment module is further configured to:

determine a sensitivity level corresponding to the sensitivity of the target resource; and

set the permission level of the target resource to a permission level corresponding to the sensitivity level.

10. The apparatus of claim 7, further comprising:

a first receiving module configured to receive a resource access request from a user terminal device;

a determination module configured to determine whether the user is an authorized user; and

an access control module configured to:

if the user is determined to be an authorized user, allow the user to access the target resource; and

if the user is not determined to be an authorized user, refuse the user to access the target resource.

11. The apparatus of claim 10, wherein the determination module is further configured to:

determine whether the resource access request includes a permission code of the target resource;

if the resource access request is determined to include a permission code of the target resource, determine that the user is an authorized user; and

if the resource access request is not determined to include a permission code of the target resource, determine that the user is not an authorized user.

12. The apparatus of claim 11, further comprising:

a second receiving module configured to receive an authorization request from the user terminal device;

a verifying module configured to verify the user according to the authorization request and the permission level of the target resource; and

a sending module configured to, if the user passes the verification, send the permission code of the target resource to the user.

13. A webpage resource permission management method, comprising:

monitoring a sensitivity of a webpage resource by a web browser on a terminal device; and

when the sensitivity of the webpage resource changes, adjusting, by a server, a permission level of the webpage resource according to the sensitivity of the webpage resource.

14. A webpage resource permission management apparatus, comprising:

a monitoring module configured to monitor a sensitivity of a webpage resource; and

an adjustment module configured to, when the sensitivity of the webpage resource changes, adjust a permission level of the webpage resource according to the sensitivity of the webpage resource.

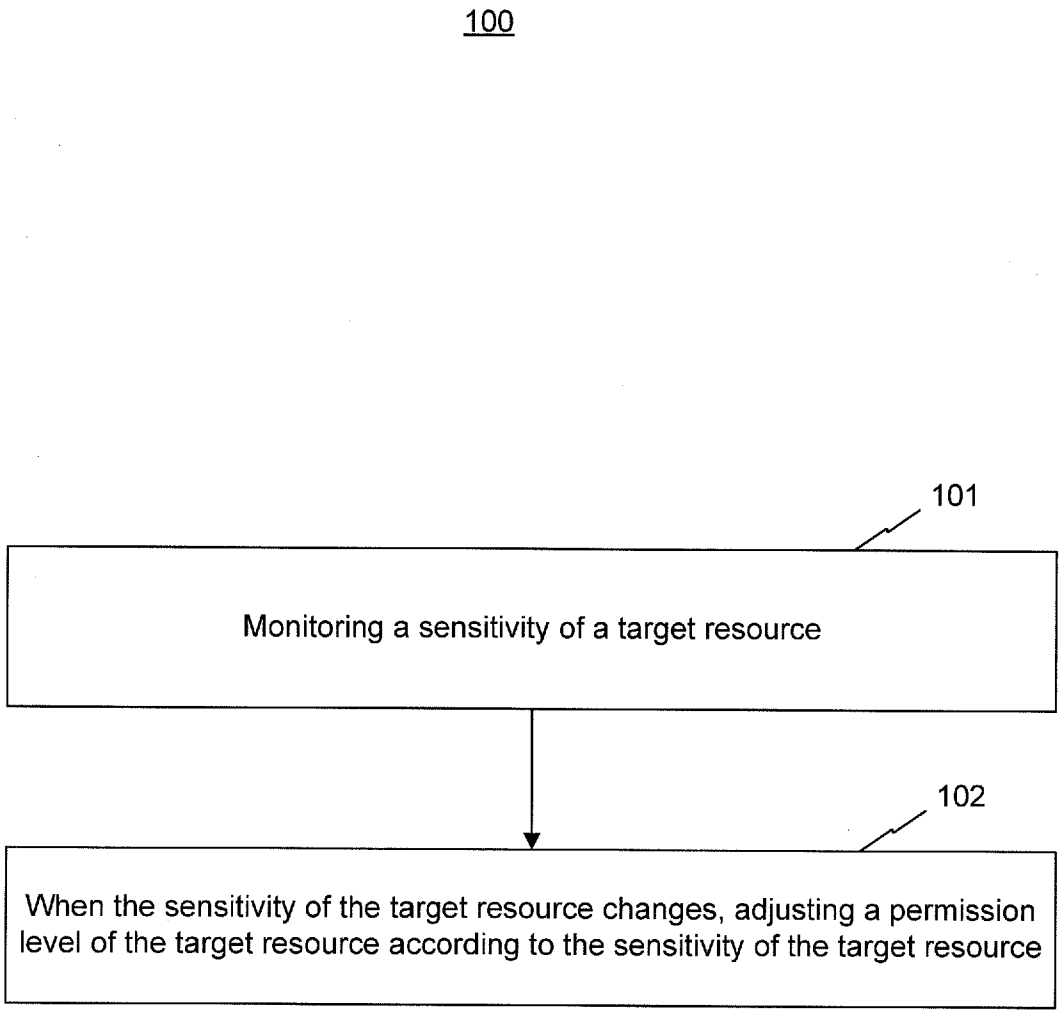

100
101
Monitoring a sensitivity of a target resource
102
When the sensitivity of the target resource changes, adjusting a permission level of the target resource according to the sensitivity of the target resource

Fig. 1

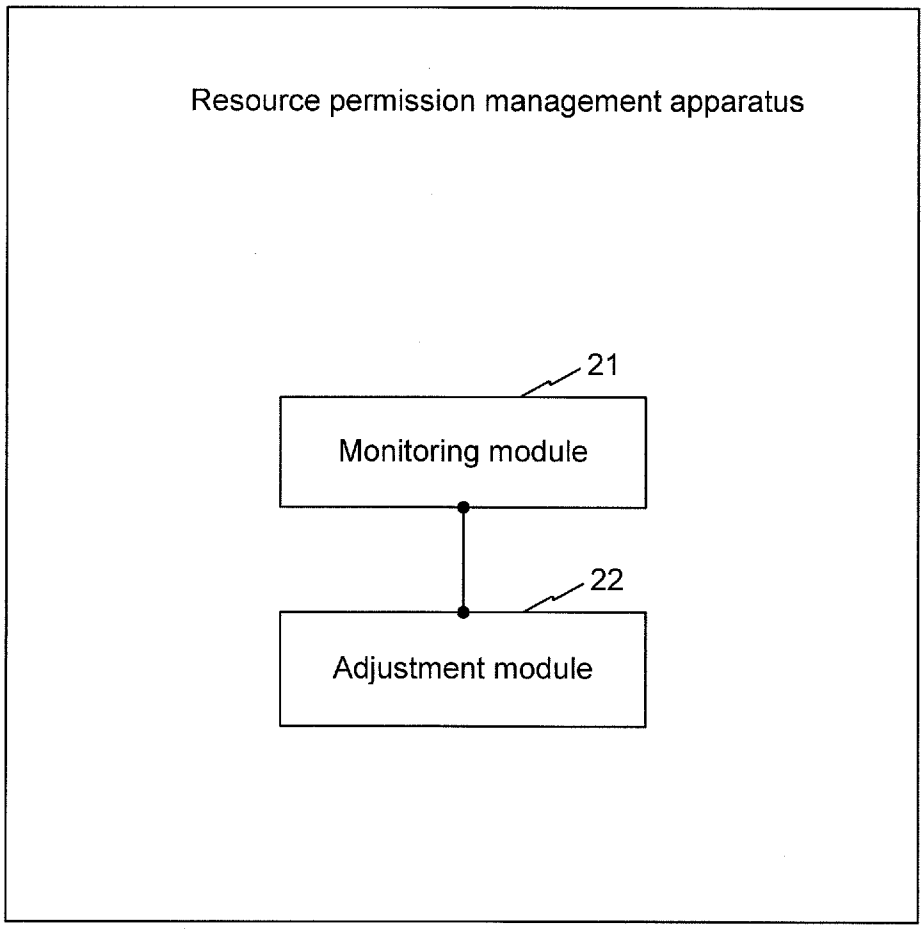

200
Resource permission management apparatus
21
Monitoring module
22
Adjustment module

Fig. 2

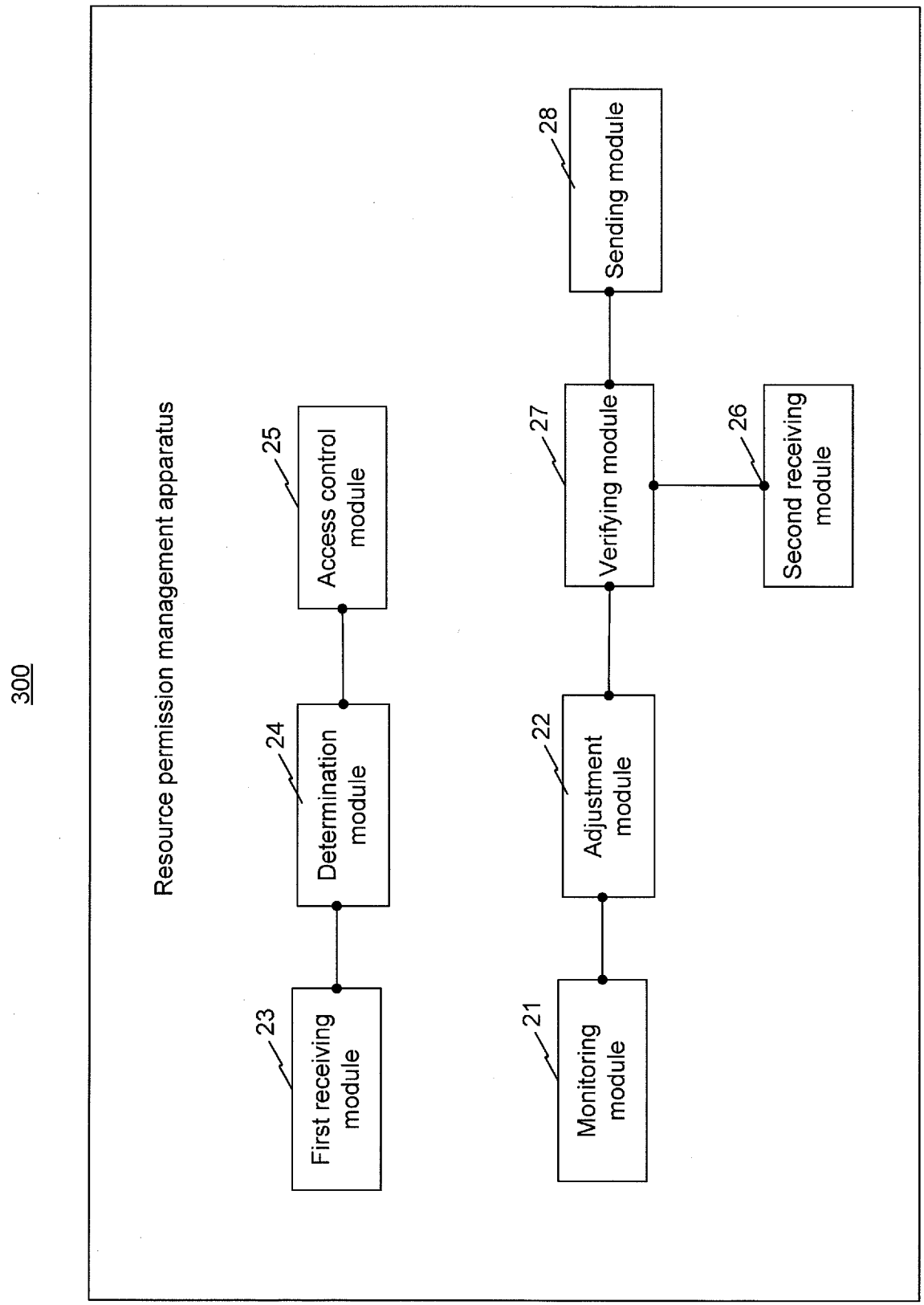

300
Resource permission management apparatus
First receiving module
23
Determination module
24
Access control module
25
Monitoring module
21
Adjustment module
22
Verifying module
27
Second receiving module
26
Sending module
28

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 16/14120

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04L 29/06 (2016.01)
CPC - H04L 63/20; H04L 63/102; G06F 21/6218
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)
CPC: H04L 63/20; H04L 63/102; G06F 21/6218; IPC(8): H04L 29/06 (2016.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 726/1; 726/25; 726/26; CPC: H04L 63/20; H04L 63/102; G06F 21/6218; G06F 21/604, H04L 63/0227; IPC(8): H04L 29/06 (2016.01) (keyword limited, terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PatBase, Google Patents, IEEE; Search Terms: monitoring, reviewing; resource, database, asset, repository; sensitivity, classification, secret, top secret, SCI; permission, access, clearance; level, grade, rank; code, password, key; changing, modifying; user, client; authorizing

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006/0048224 A1 (Duncan et al.) 02 March 2006 (20.03.2006), entire document especially paras [0045], [0046], [0047], [0049], [0056]	1 - 14
A	US 2014/0165167 A1 (Nunn et al.) 12 June 2014 (12.06.2014), entire document	1 - 14
A	US 2014/0196103 A1 (Chari et al.) 10 July 2014 (10.07.2014), entire document	1 - 14
A	US 2007/0143825 A1 (Goffin) 21 June 2007 (21.06.2007), entire document	1 - 14
A	US 2014/0215603 A1 (Giblin et al.) 31 July 2014 (31.07.2014), entire document	1 - 14

☐ Further documents are listed in the continuation of Box C. ☐

* 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
10 March 2016 (10.03.2016)	01 APR 2016
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (January 2015)