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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 April 2011 (21.04.2011)

PCT

(10) International Publication Number
WO 2011/046567 A1

(51) International Patent Classification:
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/US2009/061060

(22) International Filing Date:
16 October 2009 (16.10.2009)

(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 TX 77070, Houston, TX 77070 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **ERICKSON, John S.** [US/US]; Mail Stop 707 Rt. 132, Norwich, VT 05055 (US).

(74) Agents: **DAKIN, JR., Lloyd, E.** et al.; Hewlett-Packard Company, Intellectual Property Administration, 3404 E. Harmony Road, Mail Stop 35, Fort Collins, CO 80527-2400 (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, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM,

[Continued on next page]

(54) Title: RESOURCE ACCESS CONTROL MANAGEMENT

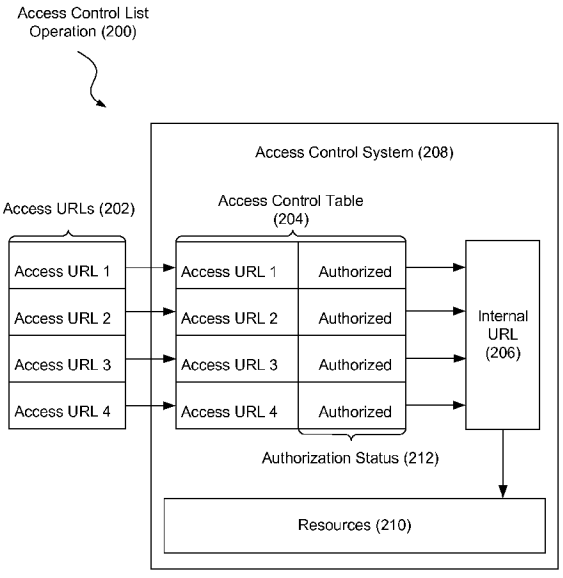

Fig. 2

(57) Abstract: A method for managing access to resources (106) over a network (102) includes issuing a unique access Uniform Resource Locator (URL) (202) with an access control system (208) to a user (116), maintaining a record of the unique access URL (202) in an access control table (204) associated with the access control system (208), associating an authorization status (212) with the unique access URL (202) in the access control table (204) with the access control system (208), and resolving the unique access URL (202) to an internal URL (206) if allowed by the authorization status (212) with the access control system (208), the internal URL (206) providing access to a resource (210).

WO 2011/046567 A1

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

Declarations under Rule 4.17:

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

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

Published:

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

RESOURCE ACCESS CONTROL MANAGEMENT

BACKGROUND

[0001] Several security methods have been developed to limit access to particular resources on a network to authorized individuals. One such method is that of a capability-based security method. In its simplest form, capability-based security involves an access control system providing "locators" to users who are authorized to access particular resources. The access control system assumes that because a user knows the location of particular resources, the user is authorized to access the resources. No other form of authorization, such as a password, is required. However, authentication may, in some cases, be required to receive the locator.

[0002] One form of a simple capabilities-based security system is an access control system providing access Uniform Resource Locators (URLs). An access URL may provide the location of resources available over a network. The fact that a user has the access URL may signify that the user has authorization to access the resources to which the access URL points. Many users may choose to bookmark their access URL in a web-browser. Additionally or alternatively, users may have other computer applications which rely on the access URL to access particular resources on the Internet. One challenge inherent in such systems is that of maintaining a record of which users are currently authorized to access which resources. Another challenge is revoking access privileges to users who are no longer allowed to access certain resources. In a typical capabilities based security system, revoking privileges of less than all users involves making all issued access URLs null and reissuing valid access URLs to all currently authorized users.

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] The accompanying drawings illustrate various embodiments of the principles described herein and are a part of the specification. The illustrated embodiments are merely examples and do not limit the scope of the claims.

[0004] Fig. 1 is a block diagram showing an illustrative access control system, according to one embodiment of principles described herein.

[0005] Fig. 2 is a diagram showing an illustrative access control process for allowing a user from an access control table to access resources, according to one embodiment of principles described herein.

[0006] Fig. 3 is a diagram showing an illustrative access control process for handling access attempts from unauthorized access URLs, according to one embodiment of principles described herein.

[0007] Fig. 4 is a diagram showing an illustrative access control table used by an access control system, according to one embodiment of principles described herein.

[0008] Fig. 5 is a flowchart showing an illustrative method for managing access to resources over a network, according to one embodiment of principles described herein.

[0009] Throughout the drawings, identical reference numbers designate similar, but not necessarily identical, elements.

DETAILED DESCRIPTION

[0010] As mentioned above, several security methods have been developed to limit access to particular resources on a network to authorized individuals. While capability-based security is useful for many applications, difficulties can arise when revoking access to a previously authorized user of such an application. Particularly, updating an access URL for an application whenever access is revoked from a user of the application may be inconvenient

for other authorized users of the application, since these users may have to update any programs or applications that use the old access URL. This inconvenience can be exacerbated in systems where access is routinely withdrawn from users, as the time expended by authorized users to update their files and/or program settings may cause a substantial loss of productivity by the authorized users. Moreover, frequent changes to access URLs may also lead to a greater incidence of technical difficulties in accessing a protected application due to an increased likelihood of errors resulting from implementing the changes. The resolution of such technical difficulties may also expend resources.

[0011] It may, therefore, be desirable to provide a system of capability-based security that reduces or eliminates these difficulties. Specifically, it may be desirable to extend the benefits of capability-based security to applications for which authorized access is at times revoked while eliminating the detrimental effects caused by changing access URLs.

[0012] In light of these and other considerations, the present specification relates to an access control management system which makes use of access control tables to determine which users are currently authorized to access particular resources on a network. According to one illustrative embodiment, a unique access URL is issued to each user authorized to access particular resources. An access control table is used to maintain a record of which users are currently authorized to access which resources. The access control table may also maintain a record of all users who were authorized at one time, but have since had their access rights revoked. In one embodiment, the access control table may maintain an authorization status for each user. This may allow an administrator to easily revoke or reinstate access privileges to users in the system.

[0013] If a user is authorized, the access control system may resolve the access URLs given to valid users to an internal URL specifying the location of a protected resource. The access control table may also maintain a record of which users are currently authorized to access which resources. Additionally or alternatively, the access control system may log any attempts to access

resources using an unauthorized access URL. In some embodiments, a selective response may be provided to those attempting to access resources using unauthorized access URLs. Additionally or alternatively, further authentication may be requested.

[0014] Through use of an access control system embodying principles described herein, users having authorization to access resources or services do not need to use a new access URL each time access is revoked to one of the users on the access control table. In addition, if a user who has had his or her access privileges revoked and subsequently reinstated a new access URL may not be necessary. The access control system may simply change the authorization status of the user.

[0015] In the following description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present systems and methods. It will be apparent, however, to one skilled in the art that the present apparatus, systems and methods may be practiced without these specific details. Reference in the specification to "an embodiment," "an example" or similar language means that a particular feature, structure, or characteristic described in connection with the embodiment or example is included in at least that one embodiment, but not necessarily in other embodiments. The various instances of the phrase "in one embodiment" or similar phrases in various places in the specification are not necessarily all referring to the same embodiment.

[0016] Throughout this specification and in the appended claims, the term "resource" may refer to an electronic file which may be an electronic document, an image file, an audio, file, a video file, etc. A resource may also refer to an application or service provided over a network.

[0017] Throughout this specification and in the appended claims, the term "access URL" refers to a uniform resource locator used to access resources over a network. An access URL does not necessarily reference a resource directly. An "internal access URL" refers to a URL which directly points to resources.

[0018] Throughout the present specification and in the appended claims, the term "access control table" refers to a table of unique access URLs which have been issued to allow access to a resource. An access control table may also maintain a record of other information associated with issued access URLs.

[0019] Throughout the present specification and in the appended claims, the term "user" refers broadly to any person or process able to request access to resources.

[0020] Throughout this specification and in the appended claims, the term "access control system" refers to a system capable of controlling access to resources based on a list of authorized users.

[0021] Throughout this specification and in the appended claims, the term "resolve" refers to the process of referencing a resource and allowing access to the resource.

[0022] Referring now to the figures, Fig. 1 is a block diagram showing an illustrative access control system (100). According to one illustrative embodiment, an access control system (100) may include resources (106) stored on storage medium (104) of a computer network (102). The access control system may further include an access control table (108). The access control table (108) may allow a user (116) to access the resources (106) through use of an issued unique access URL (114). The access control system may also include a processor (110) and computer readable code (112).

[0023] Many resources (106) may be made available to users over the Internet. These resources (106) may be stored on storage servers connected to the Internet. These resources (106) may be intended for the use of an exclusive group of authorized individuals. For example, a text document may have private information that only a few people are authorized to access. In a further example, resources (106) such as a video file may be provided to a consumer for a limited amount of time. Resources may also be services or applications which are available over a network. Access to these resources may be managed by an access control system (100). In some cases, a resource may be assembled and delivered upon request from a user. Additionally or

alternatively, a resource may perform a function that is not delivered in any human-readable form. For example, the resource may update a program stored on a user's computer.

[0024] An access control system (100) may maintain an access control table (108) for particular resources (106) or a group of resources (106). In one embodiment, the access control table (108) may include a list of access URLs given to various users which have been given authorization to access particular resources (106). Each access URL may be uniquely keyed for each authorized user.

[0025] The access control table (108) may maintain a record of the internal URLs which resolve to resources a user is authorized to access. If a user is authorized to access a particular resource, the access control system (100) may resolve the issued unique access URL to an internal access URL (118) which references the appropriate resource.

[0026] An access URL may include a string of characters which denote the location of the resources to which the access URL provides access. The string of characters is often encoded and obfuscated to provide additional security. The access URL may also contain additional information which may be relevant. One such piece of additional information may be a unique user identification (ID). Thus each access URL is unique to the user, and the resource for which it provides access. The user ID may allow the access control system (100) to record in the access control table when and how often a user (116) uses his or her unique access URL to access particular resources (108).

[0027] Fig. 2 is a diagram of an illustrative access control process (200) for allowing a user from an access control table (204) to access a resource (210). Fig. 2 shows a list of access URLs (202) which have been given to users to access various resources (210). The access URLs which have been given out are maintained in an access control table (204). According to one illustrative embodiment, an access control system (208) resolves the access URLs (202) in the access control table (204) to an internal access URL (206) if allowed by an authorization status (212).

[0028] Access URLs (202) may be given to users through a variety of methods. In one embodiment, when the access control system (208) grants access to a user, the user is given the access URL (202) through an email or some other means of communication. The access URL (202) may be generated as it is given to the user. When an access URL (202) is generated and given to a user, a copy is maintained by the access control table (204).

[0029] The access control table (204) may include a list of all users who have been given access to a particular resources (210) as well as the access URL they were given. In one embodiment, the access control table (204) may be created and managed manually by a system administrator. The system administrator may provide the access control system (208) with the users who have access to particular resources (210). In one embodiment, the access control table (204) may also be completely automated. The access control system (208) may obtain a list of users through a query of a database.

[0030] The access control system (208) may resolve the access URLs (202) given to the authorized users to an internal access URL (206). The internal access URL (206) may give the location of the resources (210). By having access URLs (202) resolved to an internal URL, an additional level of security is provided. This is because the user is prevented from viewing the internal URL and thus the actual location of the resources (210).

[0031] As mentioned above, at any point, it may be necessary to revoke the privileges of one or a subset of the users. Fig. 3 is a diagram of an illustrative access control process (300) for handling access attempts from unauthorized access URLs (308). According to one illustrative embodiment, it may be desired that at least one user's access privileges be revoked. In this case, the access control system (208) may change the authorization status of a user. When this is done, the access URL (202) issued to the new user will no longer resolve to the internal URL (206) which references the appropriate resource (210). If an attempt is made to access a resource (210) using an unauthorized access URL (308), the access control system (208) may provide a selective alternative response (302). Additionally or alternatively, further authentication (304) may be requested.

[0032] The authorization status associated with a unique access URL (202) may be updated either by a system administrator or an automated process. In one embodiment, an automated process may make use of a corporate user directory which contains metadata associated with each user which may determine an authorization or revocation status for particular users. A user may have access privileges revoked for a variety of reasons. One reason may be that the user has failed to fulfill a part of a contract. For example, access to a resource (210) may be provided as a service for which a user is charged. If a user fails to pay a periodic fee, access may be revoked. Another reason may be that there is suspicion that an access URL (202) may have been compromised. For example, a third party has intercepted the access URL (202). As no authentication is required, the third party may gain access to a resource (210) for which they are not authorized to access.

[0033] A selective response (302) may be provided to a user who attempts to access a resource (210) using an unauthorized access URL (202). The selective response (302) may be a webpage explaining why access is not allowed. The selective response (302) may be based on information maintained in the access control table (204). For example, the selective response (302) may contain information specific to the user who was originally issued the access URL (202) or the resource (210) for which the access URL allows access.

[0034] In one embodiment, when an attempt to access a resource (210) using an unauthorized access URL (308), the access control system (208) may request further authentication (304). This authentication may require a password, an employee or student code, or some other form of authentication. If the appropriate authentication is provided by the user, access to the resource (210) may be reauthorized. The reauthorization may either be a one time allowance to access or may permanently change the authorization status associated with the access URL (202).

[0035] In one embodiment, the access control system (208) may maintain a record of any attempts made to access a resource (210) using an unauthorized access URL (308). This record may be kept in an access log

(306). The access log (306) may be made available to a system administrator. The system administrator may then take appropriate action if desired. For example, the system administrator may contact a user who persistently attempts to use an unauthorized access URL (308).

[0036] An access control table may contain a variety of information which may be relevant to the management of access control. Fig. 4 is a diagram showing an illustrative access control table (400). According to one illustrative embodiment, an access control table (400) may include an access URL column (402), a user ID column (404), an internal URL column (406), an authorization status column (408), a log column (410), and an alternate URL column (412).

[0037] An entry in the access control table (400) may include an issued unique access URL (402). An entry may also include a user ID (404). The user ID (404) may be a string of characters which uniquely identifies a user. By associating a user ID (404) with each issued access URL (402), the access control system may keep track of which users are authorized for which resources and what access URLs (402) they have been given.

[0038] An entry in the access control table (400) may also include an internal URL (406). As mentioned above, the internal URL directly references a resource. The access control system may resolve an issued access URL to an internal URL if access is authorized. Whether access is authorized may be indicated by an authorization status (408).

[0039] In one embodiment, an access control table may contain a log column (410). The log column (410) may indicate that there are entries in a log which indicate when access attempts have been made using the associated access URL (402). The log may be stored at the same or a separate location as the access control table. The log may maintain a record of authorized access attempts, unauthorized access attempts, or both.

[0040] In one embodiment, the access control table may contain an alternate URL column (412). An alternate URL (412) may be used to direct a user who attempts to access a resource using an unauthorized access URL. For example, the alternate URL (412) may provide a location where a selective

response is generated. The alternate URL (412) may also provide a location where further authentication is requested.

[0041] In some embodiments, an access control table (400) may have more than one entry per user. A user may have one entry for each resource they are authorized to access. In the example shown in Fig. 4, there are two unique access URLs assigned to user 1. Both access URLs resolve to a different internal URL. Access URL 1 which resolves to internal URL 1 is currently not authorized. However, access URL 2 which resolves to internal URL 2 is currently authorized.

[0042] In some embodiments, an access URL may expire or become no longer valid for any reason and a new access URL may be issued. This may be done, for example, if an organization's security policy dictates that access URLs should expire after a predetermined amount of time. If this is the case, it may be inconvenient for the user to change user a different access URL if the original access URL is already embedded into browser bookmarks or other applications. A user may have the option to have an old access URL resolve to a new access URL. In the example shown in the figure, access URL 3 which has been issued to user 2 is no longer authorized. However, access URL 4 which is also given to user 2 and resolves to the same internal URL is authorized. If user 2 chooses to have access URL 3 resolved (414) to access URL 4, the user may still access the appropriate resource using access URL 3.

[0043] In one embodiment, an access URL may be given an "expiry" status. In this case, the access URL's authorization status may disallow access to the appropriate resource when the current date passes the expiry date.

[0044] Fig. 5 is a flowchart showing an illustrative method for managing access to resources over a network. According to one illustrative embodiment, the method may include issuing (step 502) a unique access URL with an access control system to a user, maintaining (step 504) a record of the unique access URL in an access control table associated with the access control system, associating (step 506) an authorization status with the unique access URL in the access control table, and resolving (step 508) the unique access URL to an internal URL if allowed by the authorization status, the

internal URL providing access to a resource. The method may further include disallowing (step 510) access to the resource if an authorization status disallows access to the resource using the unique access URL.

[0045] In sum, a system and method for managing access to resources on a network involves issuing and maintaining a record of access URLs. The access URLs are completely unique to each user for each resource. The access URLs are accompanied with an authorization status. If allowed by the authorization status, an access control system will resolve the issued access URLs to an internal URL. The internal URL will reference the location of the resource desired to be accessed. The access control system may maintain a record of each attempt to access resources using both authorized and unauthorized access URLs.

[0046] An advantage of an access control system embodying principles described herein is that no authentication is required. The fact that a user has an access URL is evidence enough that the user is authorized. Furthermore, the access control system described herein allows easy revocation of access privileges without affecting other users. Additionally, if opted by a user, expired URLs may be resolved to currently valid URLs which resolve to the same internal URL. This will eliminate the need for the user to change any bookmarks or applications which use the expired URL.

[0047] The preceding description has been presented only to illustrate and describe embodiments and examples of the principles described. This description is not intended to be exhaustive or to limit these principles to any precise form disclosed. Many modifications and variations are possible in light of the above teaching.

CLAIMS

WHAT IS CLAIMED IS:

1. A method for managing access to resources (106) over a network (102), the method comprising:

issuing a unique access Uniform Resource Locator (URL) (202) with an access control system (208) to a user (116);

maintaining a record of said unique access URL (114) in an access control table (204) stored on a computer readable storage medium (104) associated with said access control system (208);

associating an authorization status (212) with said unique access URL (202) in said access control table (204) with said access control system (208);

resolving said unique access URL (202) to an internal URL (206) if allowed by said authorization status (212) with said access control system (208), said internal URL (206) providing access to a resource (210).

2. The method of claim 1, further comprising disallowing access to said resource (210) through said unique access URL (202) with said access control system (208) if said authorization status (212) indicates that said unique access URL (202) is not authorized to access said resource (210).

3. The method of any preceding claim, further comprising allowing an administrator to change said authorization status (212) with said access control system (208).

4. The method of any preceding claim, further comprising:

issuing a new unique access URL with said access control system (208) to replace said unique access URL (202); and

resolving said new unique access URL to said internal URL (206) if allowed by an authorization status (212) associated with said new unique access URL.

5. The method of any preceding claim, further comprising changing said authorization status (212) associated with any unique access URL (202) preceding said new unique access URL to disallow access to said resource (210) using any of said preceding unique access URLs (202).

6. The method of any preceding claim, further comprising recording with said access control system (208) an attempt to access said resource (210) using said issued unique access URL (202) when said authorization status (212) disallows access to said resource (210).

7. The method of any preceding claim, further comprising, requesting with said access control system (208) a further measure of authentication (304) when an attempt is made to access said resource (210) using said issued unique access URL (202) and said authorization status (212) disallows access to said resource (210).

8. The method of any preceding claim, further comprising returning a selective response (302) to a user attempting to access said resource (210) using said unique access URL (202) when said authorization status (212) disallows access to said resource (210).

9. The method of any preceding claim, further comprising, responsive to said authorization status (212) disallowing access to said resource (210), resolving said issued unique access URL (202) to a new unique access URL having an authorization status (212) that allows access to said resource (210).

10. A system for managing access to resources (106) over a network (102), the system comprising:

at least one processor (110);

at least one computer readable storage medium (104) having an access control table (204) stored thereon, said access control table (204) being

configured to maintain a record of a plurality of issued unique access Uniform Resource Locators (URLs) (202) for a resource (210), each said unique access URL being associated with an internal access URL (206) referencing said resource (210);

in which said processor (110) is configured to resolve each said issued unique access URL (202) to said internal access URL (206) if permitted by an authorization status (212) associated with said issued unique access URL (202).

11. The system of claim 10, in which said processor (110) is further configured to disallow access to said resource (210) through said unique access URL (202)with said access control system (208) if said authorization status (212) indicates that said unique access URL (202) is not authorized to access said resource (210).

12. The system of any of claims 10 – 11, in which said processor (110) is further configured to allow an administrator to change said authorization status (212) with said access control system (208).

13. The system of any of claims 11 – 12, in which said processor (110) is further configured to:

issue a new unique access URL with said access control system (208) to replace said unique access URL (202); and

resolve said new unique access URL to said internal URL (206) if allowed by an authorization status (212) associated with said new unique access URL.

14. The system of any of claims 11 – 13, in which said processor (110) is further configured to record with said access control system (208) an attempt to access said resource (210) using said issued unique access URL (202) when said authorization status (212) disallows access to said resource (210).

15. A method for managing access to resources (106) over a computer network (102), the method comprising:

issuing a first unique access URL (202) to a user (116) who is authorized to access a resource (210);

associating with said first unique access URL (202), an internal access URL (206), and a first authorization status (212), said internal access URL (206) providing access to said resource if allowed by said first authorization status (212);

issuing a second unique access URL to said user (116);

associating said second unique access URL with said internal access URL (206), and a second authorization status (212);

setting said first authorization status (212) to indicate that said first unique access URL (202) is disallowed from accessing resource (210); and

logging an attempt to access said resource (210) using said first unique access URL (202).

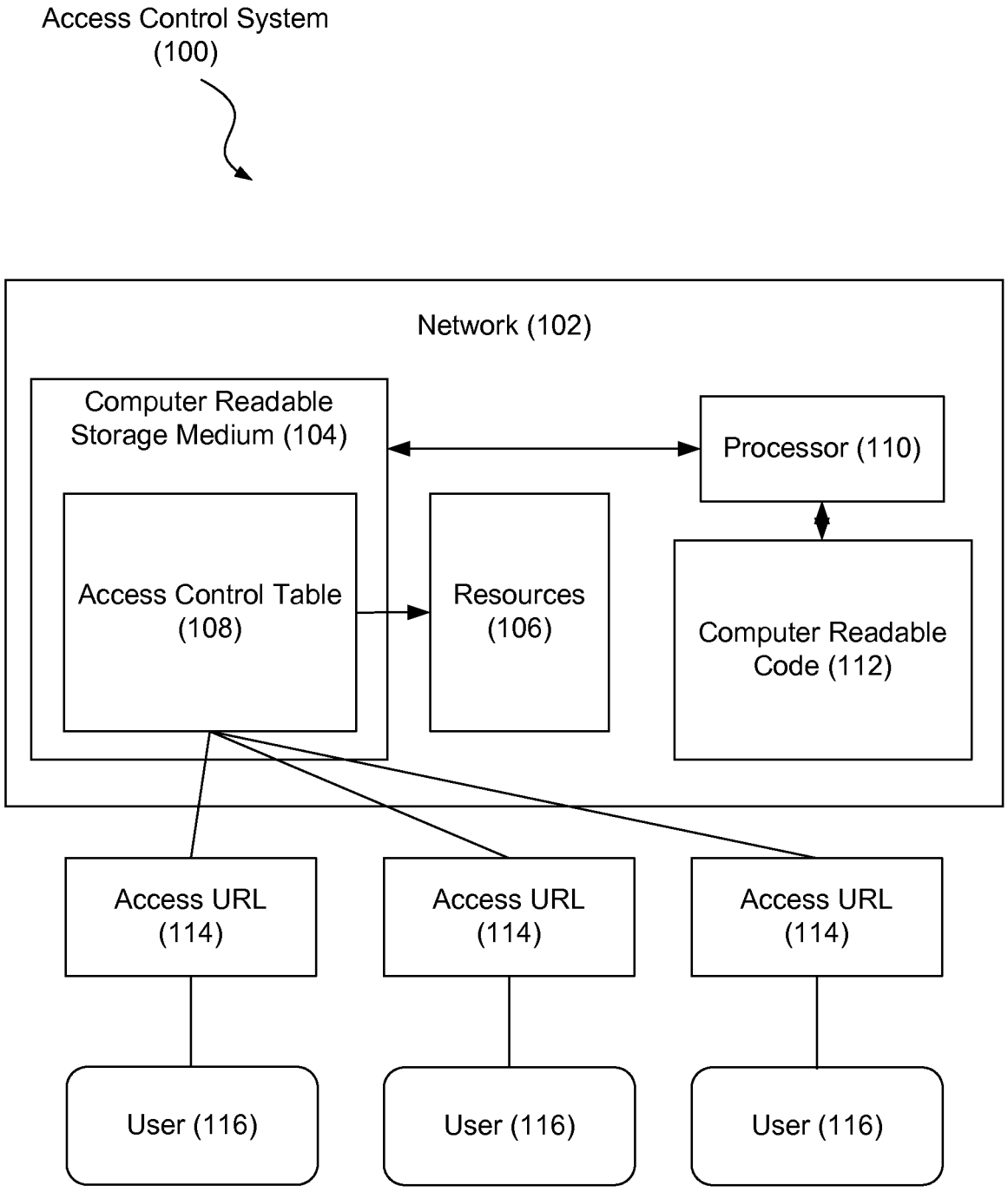
Access Control System
(100)
Network (102)
Computer Readable
Storage Medium (104)
Processor (110)
Access Control Table
(108)
Resources
(106)
Computer Readable
Code (112)
Access URL
(114)
Access URL
(114)
Access URL
(114)
User (116)
User (116)
User (116)

Fig. 1

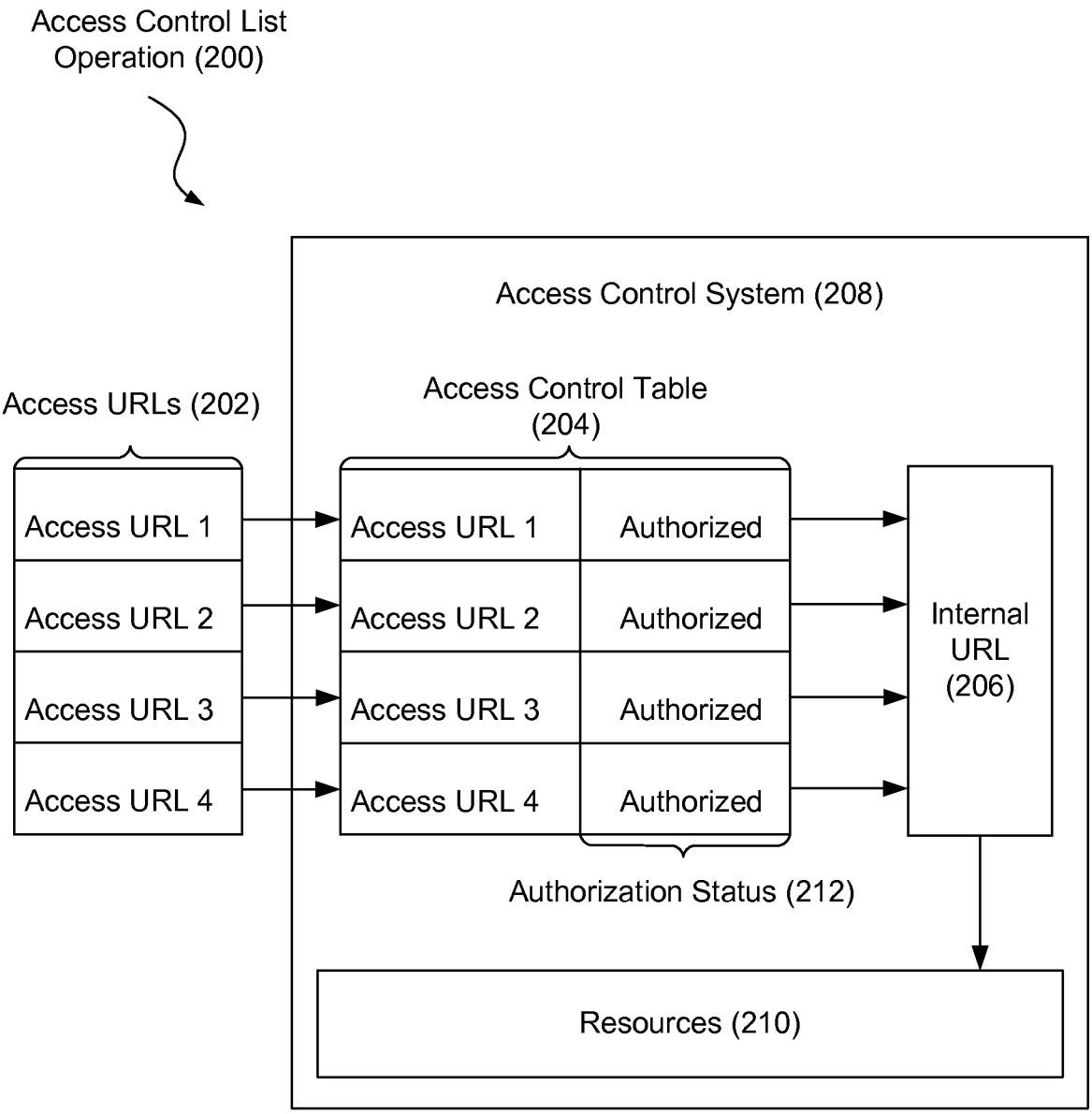
Access Control List
Operation (200)
Access Control System (208)
Access URLs (202)
Access Control Table
(204)
Access URL 1
Access URL 2
Access URL 3
Access URL 4
Access URL 1
Authorized
Access URL 2
Authorized
Access URL 3
Authorized
Access URL 4
Authorized
Internal
URL
(206)
Authorization Status (212)
Resources (210)

Fig. 2

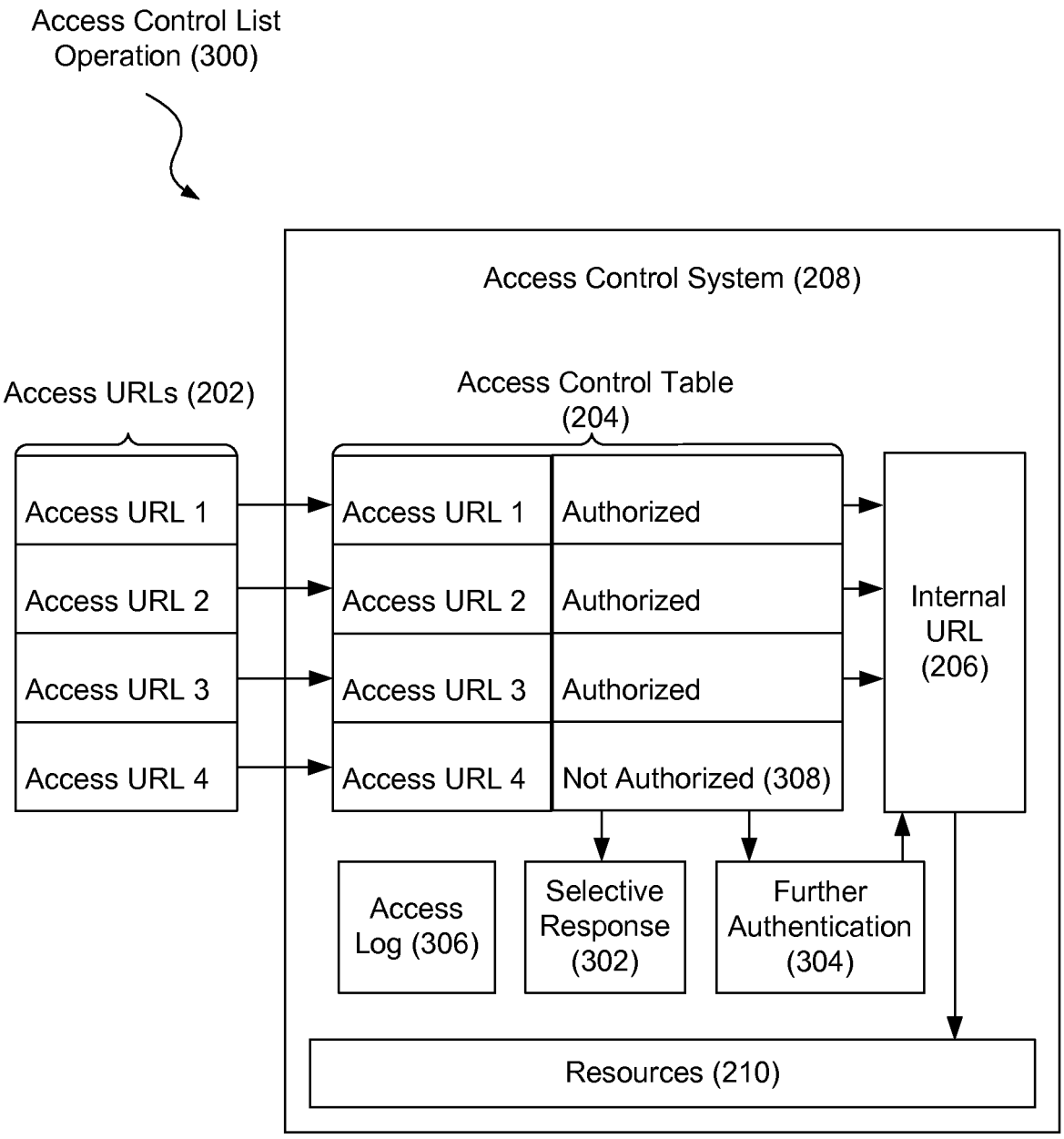
Access Control List Operation (300)
Access Control System (208)
Access URLs (202)
Access Control Table (204)
Access URL 1
Access URL 2
Access URL 3
Access URL 4
Access URL 1
Authorized
Access URL 2
Authorized
Access URL 3
Authorized
Access URL 4
Not Authorized (308)
Internal URL (206)
Access Log (306)
Selective Response (302)
Further Authentication (304)
Resources (210)

Fig. 3

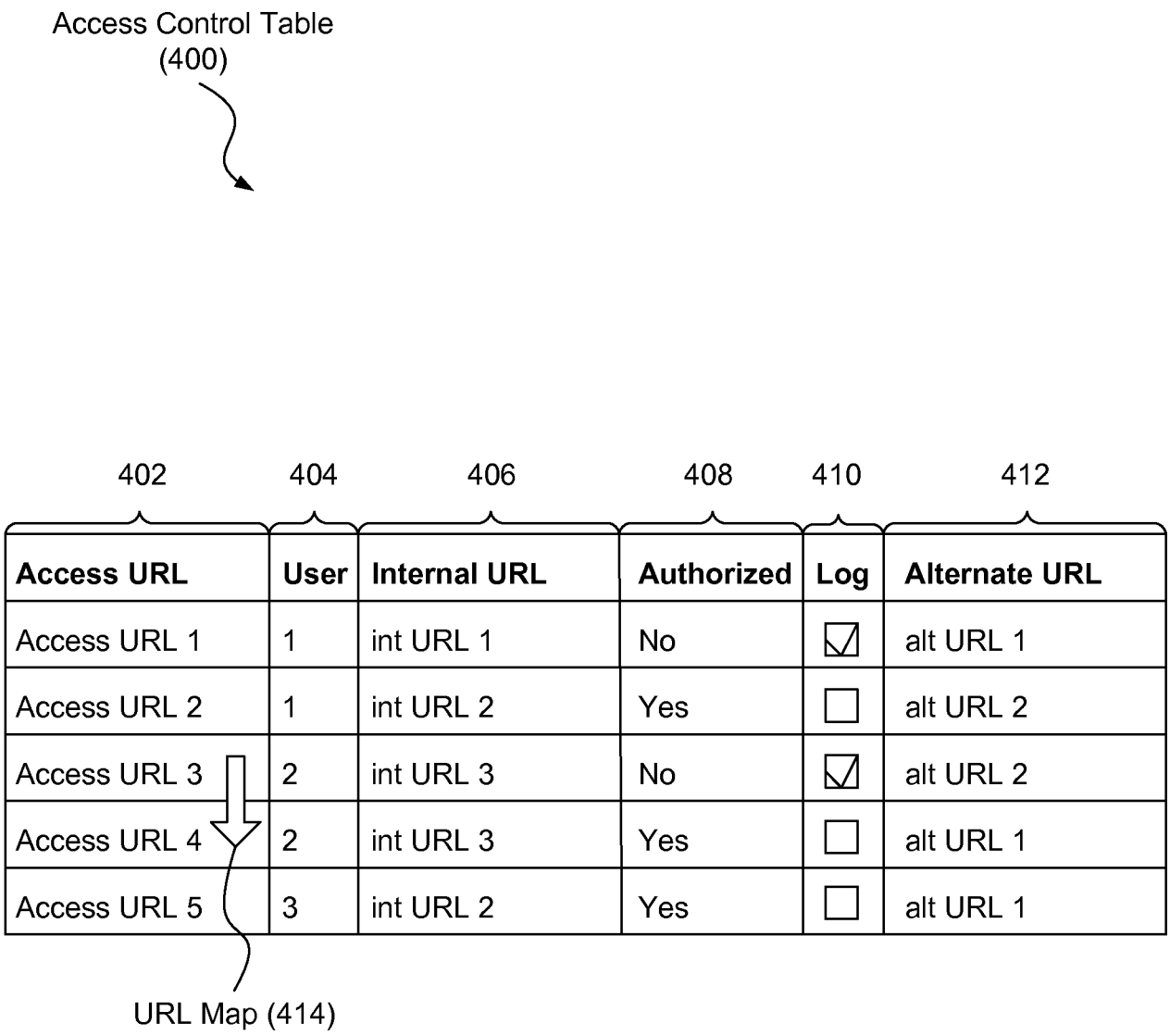
Access Control Table
(400)
402
404
406
408
410
412
Access URL
User
Internal URL
Authorized
Log
Alternate URL
Access URL 1
1
int URL 1
No
alt URL 1
Access URL 2
1
int URL 2
Yes
alt URL 2
Access URL 3
2
int URL 3
No
alt URL 2
Access URL 4
2
int URL 3
Yes
alt URL 1
Access URL 5
3
int URL 2
Yes
alt URL 1
URL Map (414)

Fig. 4

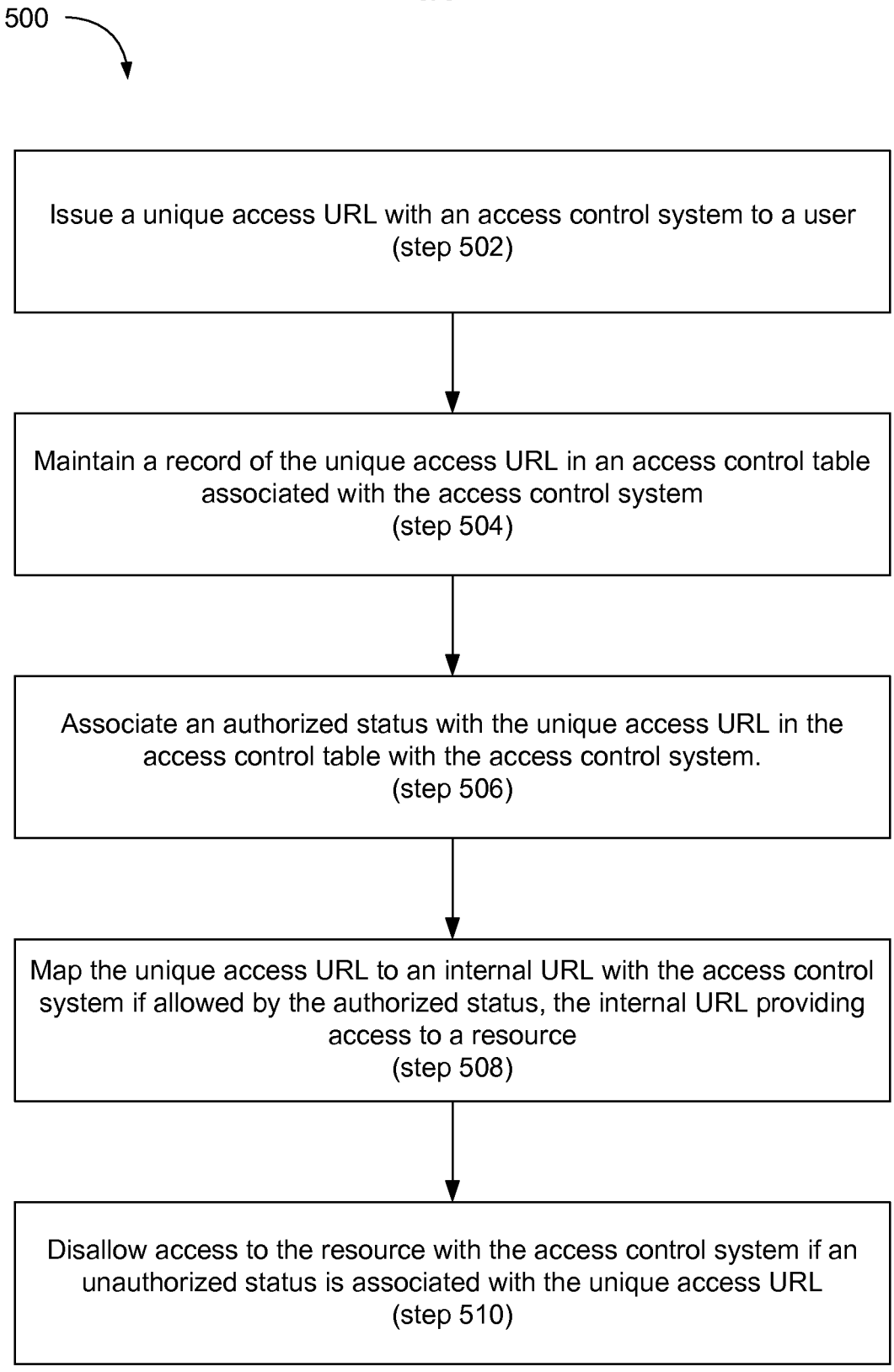
500
Issue a unique access URL with an access control system to a user (step 502)
Maintain a record of the unique access URL in an access control table associated with the access control system (step 504)
Associate an authorized status with the unique access URL in the access control table with the access control system. (step 506)
Map the unique access URL to an internal URL with the access control system if allowed by the authorized status, the internal URL providing access to a resource (step 508)
Disallow access to the resource with the access control system if an unauthorized status is associated with the unique access URL (step 510)

Fig. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2009/061060

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(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)

H04L 9/32; G06F 15/16; H04L 9/00

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

Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: URL, access control, authorization & status

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2002-0147929 A1 (MARK E. ROSE) 10 October 2002. See abstract, figs.2-6, paragraphs [0039]-[0041],[0046]-[0051],[0061]-[0063] and claims 1,2,6,10.	1-15
A	US 6240455 B1 (HITOSHI KAMASAKA et al.) 29 May 2001. See abstract, figs.1,6,10-11 and claims 4-6,7,9.	1-15
A	US 2006-0095779 A9 (SHIVARAM BHAT et al.) 04 May 2006. See abstract, figs.3,5-6, paragraphs [0053]-[0057],[0073]-[0082],[0090]-[0093] and claims 1,4-11.	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
29 JUNE 2010 (29.06.2010)	**30 JUNE 2010 (30.06.2010)**

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon, 139 Seonsa-ro, Seo-gu, Daejeon 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

Yang, Jong Phil

Telephone No. 82-42-481-8595

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2009/061060

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002-0147929 A1	10.10.2002	None	
US 6240455 B1	29.05.2001	JP 11-161672 A	18.06.1999
		JP 2996937 B2	11.01.2000
US 2006-0095779 A9	04.05.2006	US 2003-200442 A1	23.10.2003
		US 7243369 B2	10.07.2007