(19) Japan Patent Office (JP)

(12) Published Unexamined Patent Application (A)

(11)	Publication No. of Unexamined Application:	**Kokai No. 2000-10927** **(P2000-10927A)**
(43)	Date of Publication of Unexamined Application:	**January 14, 2000**

(51) Int. Cl.7	ID	FI		Theme Code (Reference)
G06F 15/00	330	G06F 15/00	330 B	5B085
H04Q 7/38		H04M 1/66	B	5J104
H04L 9/32		11/00	303	5K027
12/28		H04B 7/26	109 S	5K033
H04M 1/66		H04L 9/00	673 A	5K067

Request for Examination:	Requested
Number of Claims:	**6**
Method of Filing:	OL (Online)
Total Number of Pages:	**7**

Continued on last page

(21)	Patent Application No.:	H10-178410
(22)	Filing Date:	June 25, 1998
(71)	Applicant:	000240617 NEC Yonezawa Ltd. 6-80, Shimohanazawa 2-chome, Yonezawa-shi, Yamagata Prefecture
(72)	Inventor:	Masaru KATOU c/o NEC Yonezawa Ltd. 6-80, Shimohanazawa 2-chome, Yonezawa-shi, Yamagata Prefecture
(74)	Agent:	100085235 Patent Attorney Kaneyuki MATSUURA

Continued on last page

(54) Title of Invention

AUTHENTICATION SYSTEM AND
AUTHENTICATION DEVICE

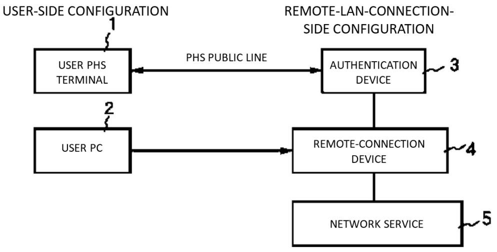
(57) Abstract

Problem

Conventional authentication systems have not reached large-scale usage because devices (one-time-password generating cards and authentication devices) that generate and manage changing passwords are very expensive.

Solution

An authentication device 3 performs: management of a "user-password request/notification function" of the user; issuance of a "temporary password" in response to a connection request from the user; and notification of the "temporary password" to a PHS terminal 1 and to a remote-connection device 4. Based on the "temporary password," the remote-connection device 4 accepts the connection request from a user PC 2 and remotely connects a proper user or an inquiring user to the authentication device 3. Based on the "temporary password," the user PC 2 connects to the remote-connection device 4. A network service 5 is a network resource wherein each user receives service.



CLAIMS

1. An authentication system, which, after verifying the validity of a user, permits usage of a resource of a network service from the user personal computer, comprising:

the user simplified, mobile-telephone terminal;

an authentication device that: preregisters a telephone number, a password, and a remote-connection ID of the simplified, mobile-telephone terminal; notifies the user of the password and the remote-connection ID; receives the telephone number and the password from the user simplified, mobile-telephone terminal; compares such with the preregistered telephone number and password; and, when they match, issues a temporary password to the user simplified, mobile-telephone terminal; and

a remote-connection device that: receives a connection request, which, owing to the simplified, mobile-telephone terminal being notified of the temporary password, is performed by the user using the personal computer; inquires with the authentication device as to whether the password and the remote-connection ID are correct; and connects the personal computer and the network service only when being notified by the authentication device that they are correct.

2. The authentication system according to claim 1, wherein the user uses the personal computer to make a connection request to the remote-connection device using the remote-connection ID and the temporary password for which notification was given by the authentication device.

3. The authentication system according to claim 1, wherein, in response to the inquiry from the remote-connection device, the authentication device determines whether the information issued to the user and the information from the remote-connection device match and notifies the remote-connection device of the determination result thereof.

4. The authentication system according to claim 1, wherein the power of the mobile-telephone terminal is turned off prior to the notification of the temporary password from the authentication device.

5. An authentication device used in an authentication system, which, after verifying the validity of a user, permits usage of a resource of a network service from the user personal computer, wherein:

a telephone number, a password, and a remote-connection ID of the user simplified, mobile-telephone terminal are preregistered; the user is notified of the password and the remote-connection ID; the telephone number and the password are received from the user simplified, mobile-telephone terminal; such is compared with the preregistered telephone number and password; and, when they match, a temporary password is issued to the user simplified, mobile-telephone terminal; and when it has been determined that it is proper with respect to the inquiry from a remote-connection device, the personal computer and the network service are connected using the remote-connection device.

6. The authentication device according to claim 5, wherein, in response to the inquiry from the remote-connection device, determines whether the information issued to the user and the information from the remote-connection device match and notifies the remote-connection device of the determination result thereof.

DETAILED DESCRIPTION OF THE INVENTION

[0001]

FIELD OF THE INVENTION

The present invention relates to an authentication system and an authentication device, and particularly relates to an authentication system and an authentication device that permits the provision of a local area network (LAN) service only to proper users.

[0002]

RELATED ART

As an example of a network-service function that uses services among computers in a LAN, there is an authentication function that checks the usage rights of a remote resource, generally, using a transmitted user identifier (ID, password) of a logged-in computer. In a network-connected computer system, when usage of each computer is started, a user identifier is provided by system software, which runs on each computer, using a user-registration list of all computers that constitutes the network-computer system. In addition, in an international telephone utilization system in which Personal Handy-phone System (PHS) terminals are used, a system is also known (Japanese Laid-open Patent Publication H9-135295) in which the system is called using an ID number and a password, and a callback function is used from the system side after validity verification.

[0003] However, with this method, there is a risk that, if a user ID or a password is stolen by a third party, the unauthorized third party can penetrate the network service. Accordingly, in recent years, authentication systems in which passwords that change at fixed time intervals are used have been proposed and are already in practical use. In these conventional authentication systems, misappropriation of a password by a third party can be made difficult because the password changes at fixed time intervals.

[0004]

PROBLEMS SOLVED BY THE INVENTION

Nevertheless, the above-mentioned conventional authentication systems have a problem in that they have not reached large-scale diffusion because devices (one-time-password generating cards and authentication devices) that generate and manage changing passwords are very expensive.

[0005] The present invention was conceived considering the above problem, and an object of the present invention is to provide a high-speed, high-reliability authentication system and a low-cost authentication device.

[0006] In addition, another object of the present invention is to provide an authentication system and an authentication device that excels in manufacturability, maintainability, and resource reusability.

[0007] Furthermore, another object of the present invention is to provide an authentication device that is compact and lightweight.

[0008]

MEANS FOR SOLVING THE PROBLEMS

To achieve the above-mentioned objects, an authentication system of the present invention, which, after verifying the validity of a user, permits usage of a resource of a network service from the user personal computer, comprises: the user number, a password, and a remote-connection ID of the simplified, mobile-telephone terminal; notifies the user of the password and the remote-connection ID; receives the telephone number and the password from the user simplified, mobile-telephone terminal; compares such with the preregistered telephone number and password; and, when they match, issues a temporary password to the user simplified, mobile-telephone terminal; and a remote-connection device that: receives a connection request, which, owing to the simplified, mobile-telephone terminal being notified of the temporary password, is performed by the user using the personal computer; inquires with the authentication device as to whether the password and the remote-connection ID are correct; and connects the personal computer and the network service only when being notified by the authentication device that they are correct.

[0009] In addition, regarding the authentication system of the present invention, to achieve the above-mentioned objects, in an authentication device used in an authentication system, which, after verifying the validity of a user, permits usage of a resource of a network service from the user personal computer: a telephone number, a password, and a remote-connection ID of the user simplified, mobile-telephone terminal are preregistered; the user is notified of the password and the remote-connection ID; the telephone number and the password are received from the user simplified, mobile-telephone terminal; such is compared with the preregistered telephone number and password; and, when they match, a temporary password is issued to the user simplified, mobile-telephone terminal; and when it has been determined that it is proper with respect to the inquiry from a remote-connection device, the personal computer and the network service are connected using the remote-connection device.

[0010] According to the present invention, it is possible to provide security that combines: security whereby the authentication device has only registered mobile-telephone terminals; security wherein the user manages their password to their mobile-telephone terminal; and security wherein the authentication device sends a temporary password to a determined mobile-telephone terminal of a user.

[0011] In addition, according to the present invention, authentication permission is obtained using a commercially available simplified, mobile-telephone terminal, such as a PHS terminal.

[0012]

EMBODIMENTS OF THE INVENTION

Next, embodiments of the present invention will be explained, together with the drawings. FIG. 1 is a block diagram of one embodiment of an authentication system that constitutes the present invention. In the same drawing are configured: a user Personal Handy-phone System (PHS) terminal 1; a user personal computer (PC) 2; an authentication device 3, which is connected to the PHS terminal 1 via a PHS public line; a remote-connection device 4, which is connected to the user PC 2 and the authentication device 3; and a network service 5, which is provided by the remote-connection device 4. The configuration on the remote-LAN connection side comprises the authentication device 3, the remote-connection device 4, and the network 5.

[0013] The authentication device 3 is a device that verifies the validity of a user and performs: management of a "user-password request/notification function" of the user; issuance of a "temporary password" in response to a connection request from the user; and notification of the "temporary password" to the user PHS terminal 1, which has the user-password request/notification function, and to the remote-connection device 4, which has a remote-connection function.

[0014] Based on the "temporary password" issued by the authentication device 3, the remote-connection device 4 accepts the connection request from the user PC 2, which is a computer system for user connection, and remotely connects a proper user or an inquiring user to the authentication device 3. The user PHS terminal 1 is a commercially available simplified mobile telephone having a user-password request/notification function; if a user makes a request to the authentication device 3 for a "temporary password" and the user is properly authenticated, then the authentication device gives notification of a "temporary password." A "temporary password" is not a predetermined specific password but rather is a password that is set as appropriate for each request.

[0015] Based on a "temporary password" for which the authentication device has given notification to the user PHS terminal 1, the user PC 2, which is the computer system for user connection, connects to the remote-connection device 4. The network service 5 is a network resource wherein each user receives service.

[0016] Next, the operation of this embodiment will be explained, with reference to the flowchart in FIG. 2. First, the PHS number, the authentication-device password, and the remote-connection ID of the user PHS terminal 1 are registered in the authentication device 3 (step 11). Continuing, the user is notified in advance of the authentication-device password and the remote-connection ID (step 12). Continuing, the user places a call (TEL) from the user PHS terminal 1 to the authentication device 3 (step 13). The method of placing a call is, for example, the numeric string: "authentication-device telephone number#authentication-device password." For example, 0238211234#ABCD.

[0017] Next, the authentication device 3 receives the call from the user PHS terminal 1 and verifies the user PHS number and the authentication-device password (step 14), determines whether those values match the registration information in step 11, and, if they do match, replies to the user PHS terminal 1 with a voice message such as "A password will now be issued. Please disconnect power and wait." (step 15). It is noted that, other than a voice message, a character message and other methods are also possible.

[0018] Next, in accordance with the above-mentioned voice message, the user turns off the power to the user PHS terminal 1 (step 16). Continuing, the authentication device 3 issues a "temporary password" to the user PHS terminal 1 and notifies the user PHS terminal 1 of the character message (step 17). In this situation, a service, such as Chara-Mail, is used. It is assumed that the temporary password is, for example, VWXYZ.

[0019] The user PHS terminal 1 is notified of the above-mentioned temporary password VWXYZ (step 18), and the user issues a network-connection request to the remote-connection device 4 (step 19). That is, the user PC 2 is used to dial up the remote-connection device 4. In this situation, the ID obtained in step 11 is used as the ID, and the "temporary password" obtained in step 18 is used as the password. For example, the ID is "SUZUKI," and the temporary password is "VWXYZ."

[0020] Continuing, when the remote-connection device 4 receives the connection request from the user PC 2 (step 20), an inquiry is made to the authentication device 3 regarding whether the user ID and the password are correct (step 21). Thereupon, in response to the inquiry from the remote-connection device 4, the authentication device 3 determines whether they match the information issued to the user (step 22). In the situation in which the authentication device 3 has determined in step 22 that they do match, the remote-connection device 4 is notified of the determination result thereof, and thereby the remote-connection device 4 gives permission to the user for usage of the network service 5 and connects the user PC 2 and the network service 5 (step 23).

[0021] Thereby, the resource of the network service 5 becomes available from the user PC 2 (step 24). It is noted that, in the situation in which the authentication device 3 has obtained a mismatched determination result in step 22, the remote-connection device 4 receives that determination result and denies the provision of the network service 5 to the user.

[0022] Thus, in this embodiment, by authenticating only the PHS terminal 1, which the user has registered in the authentication device 3 utilizing the fact that the PHS terminal 1 has a function that gives notification of its own PHS number, it is possible to make it extremely difficult for a third party to improperly use the network service 5 because it has extremely strong security through the combination of: security in that it is difficult for another PHS terminal to masquerade as the PHS terminal 1; security in that, even in an unfortunate situation such as, for example, the theft of the user PHS terminal 1, the PHS terminal 1 cannot connect to the authentication device 3 without knowing the password, and consequently the user can manage their password on the PHS terminal 1; and security in that the authentication device 3 issues a temporary password to the proper PHS terminal 1.

[0023] In addition, the user PHS terminal 1 is a

commercially available PHS terminal; a terminal that is compact, lightweight, and has low power consumption can be used for the user PHS terminal 1; operation is easy; in addition, in this embodiment, because the infrastructure of the PHS public line is used, it is high speed, the transmission efficiency is increased, and data transfer can be performed with high reliability; and, furthermore, the cost of the overall system can also be reduced. In addition, a service in which a PHS high-speed communication function (PIAFS) is used also becomes possible. Furthermore, in this embodiment, by utilizing a commercially available PHS terminal, it also becomes possible to set the price low because of the mass-production effect; manufacturability and maintainability are also excellent; and it also becomes possible to reuse resources by utilizing unused PHS terminals.

[0024]

EFFECTS OF THE INVENTION

As explained above, according to the present invention, it is possible to improve security such that it is extremely strong compared with conventional security because it has been provided with security that combines: security whereby the authentication device has only registered mobile-telephone terminals; security wherein the user manages their password to their mobile-telephone terminal; and security wherein the authentication device sends a temporary password to a determined mobile-telephone terminal of a user.

[0025] In addition, according to the present invention, because authentication permission is obtained using a commercially available simplified, mobile-telephone terminal, such as a PHS terminal, the infrastructure of a PHS public line can be used, and thereby it is high speed, transmission efficiency is improved, and data can be transferred with high reliability. Furthermore, according to the present invention, because commercially available simplified, mobile-telephone terminals, such as PHS terminals, are used: terminals that are compact, lightweight, and have low power consumption, terminals having excellent manufacturability and maintainability and that are also easy to use, or the like can be used as the terminals; resources are also reusable owing to the use of unused PHS terminals; and, in turn, the cost of the overall system can be reduced and services that utilize high-speed communication functions can be accepted.

BRIEF DESCRIPTION OF THE DRAWINGS

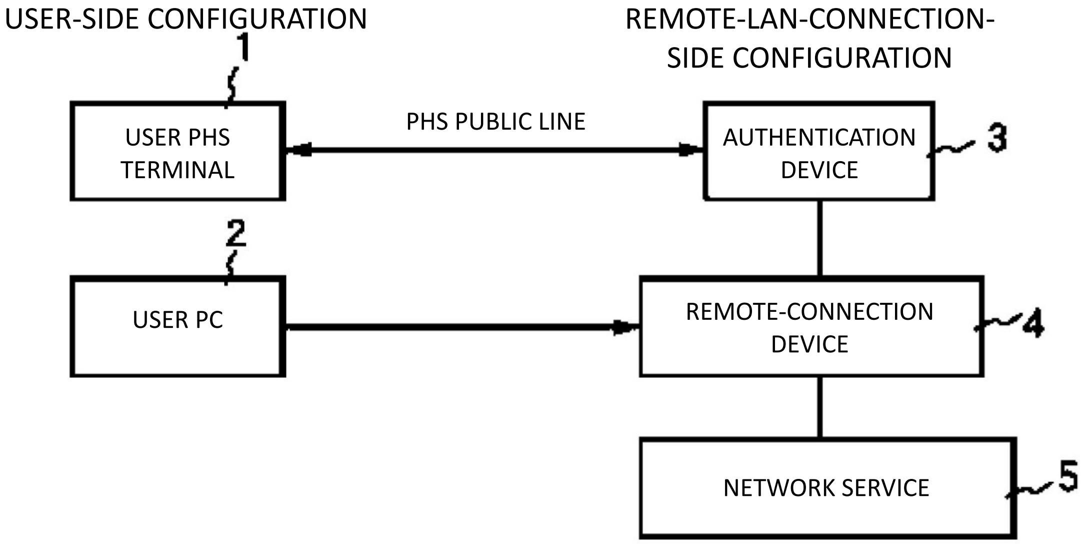
FIG. 1 is a block diagram of one embodiment of the present invention.

FIG. 2 is a flowchart of one embodiment of the present invention.

EXPLANATION OF SYMBOLS

1	User PHS terminal
2	User personal computer (PC)
3	Authentication device
4	Remote-connection device
5	Network service

FIG. 1


USER-SIDE CONFIGURATION
REMOTE-LAN-CONNECTION-SIDE CONFIGURATION
1
USER PHS TERMINAL
PHS PUBLIC LINE
AUTHENTICATION DEVICE
3
2
USER PC
REMOTE-CONNECTION DEVICE
4
NETWORK SERVICE
5

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE

fastcase®
Smarter legal research.