

DESCRIPTION

Title of the Invention

COMMUNICATION APPARATUS, REMINDER APPARATUS, AND
INFORMATION RECORDING MEDIUM

5 Technical Field

[0001] The present invention relates generally to a communication apparatus and a reminder apparatus which are suitable for securely managing private information, such as a password for utilizing a server apparatus, and a nontransitory information recording medium recording a program for allowing a computer to
10 realize the apparatuses.

Background Art

[0002] Heretofore, various server apparatuses that users can start using by inputting their passwords have been proposed. In case of utilizing a plurality of such server apparatuses, it is desirable to use different passwords for respective
15 services in order to enhance security. It is however troublesome for a user to memorize multiple passwords himself or herself; according to the technique disclosed in Patent Literature 1, a storage medium from which passwords for individual services becomes available with a single master password input.

Prior Art Literature

20 Patent Literature

[0003] Patent Literature 1: Unexamined Japanese Patent Application Kokai
Publication No. 2004-280245

Problems to be Solved by the Invention

[0004] Because such a storage medium permits passwords for individual
25 services to be read out, however, the use of the storage medium in an Internet Cafe or

the like would lower security. There arises another problem such that if the storage medium is lost, the passwords for individual services may not be remembered.

[0005] Meanwhile, various communication apparatuses accessible over the Internet, such as a router unit to realize a home LAN (Local Area Network), are set up in individual homes at present. Further, a lot of multifarious communication apparatuses including personal computers as well as cellular phones, smartphones and the like, which are connectable to the Internet are provided. Many of those communication apparatuses have communication capabilities and computation capabilities which match the capability of home routers.

10 [0006] In this respect, there is a strong demand to use those communication apparatuses to securely provide a server apparatus with individual passwords of a user and to enable password management to permit the user to use the passwords without carrying a storage medium storing the passwords.

[0007] Accordingly, in order to solve the above problems, it is an object of the present invention to provide a communication apparatus and a reminder apparatus which are suitable for securely managing private information, such as a password for utilizing a server apparatus, and a nontransitory information recording medium recording a program for allowing a computer to realize the apparatuses.

Means for Solving the Problem

20 [0008] In order to solve the above problems, the following subject matters are disclosed according to the principle of the invention.

[0009] A communication apparatus according to a first aspect of the invention is configured to include:

a storage that stores server names and a password table having a
25 predetermined number of rows and a predetermined number of columns in

association with each other;

a receiver that receives an authentication request specifying a server name;

a generator that generates a random table having the predetermined number of rows and the predetermined number of columns;

5 a presenter that presents the generated random table to a user;

an acceptor that accepts from the user a key obtained by selecting and arranging elements in the presented random table in a selection order associated with the user;

an identification unit that identifies the selection order associated with the user
10 base on the accepted key and the generated random table;

an acquirer that acquires a password from a column of elements obtained by selecting elements included in the password table, stored in the storage in association with the server name specified in the authentication request, from the password table in the identified selection order, and arranging the elements in the identified selection

15 order; and

an output unit that outputs the acquired password as a password for allowing the user to use a server apparatus with the server name specified in the authentication request.

[0010] In the communication apparatus according to the invention,

20 the server apparatus with the server name specified in the authentication request may be configured to determine whether the server apparatus is available to the user based on a time-synchronous one-time password, and

the acquirer may be configured to acquire, as the password, a result of applying a predetermined one-way function to a seed including the obtained column
25 of elements and a current time.

[0011] In the communication apparatus according to the invention, the acquirer may be configured to acquire the obtained column of elements as the password.

[0012] In the communication apparatus according to the invention, the output unit may be configured to output the acquired password by displaying the acquired
5 password to the user.

[0013] In the communication apparatus according to the invention, the output unit may be configured to output the acquired password by sending a use request specifying the acquired password to the server apparatus with the server name specified in the authentication request.

10 [0014] In the communication apparatus according to the invention,
the receiver may be configured to receive the authentication request from a first terminal used by the user,
the presenter may be configured to present the generated random table to a second terminal used by the user,
15 the acceptor may be configured to accept the key from the first terminal, and
the output unit may be configured to send the use request to permit the user to use the server apparatus through the first terminal.

[0015] In the communication apparatus according to the invention,
the receiver may be configured to receive the authentication request from a
20 first terminal used by the user,
the presenter may be configured to present the generated random table to the first terminal used by the user,
the acceptor may be configured to accept the key from a second terminal, and
the output unit may be configured to send the use request to permit the user to
25 use the server apparatus through the first terminal.

[0016] The communication apparatus according to the invention may be configured to further include an updater that, when the password table associated with the server name specified in the authentication request is not stored in the storage, updates the storage by generating a new password table having the
5 predetermined number of rows and the predetermined number of columns, setting individual elements in the new password table, and storing the new password table in the storage in association with the server name,

the output unit may be configured to send the use request to the server apparatus with the server name specified in the authentication request to register the
10 user in the server apparatus.

[0017] The communication apparatus may be configured to further include an updater that, when the password table associated with the server name specified in the authentication request is not stored in the storage, updates the storage by generating a new password table having the predetermined number of rows and the
15 predetermined number of columns, accepting an input of a password from the user, dividing the accepted password into segments to be stored in elements in the identified selection order in the new password table, setting other elements at random, and storing the new password table in the storage in association with the server name.

20 [0018] The communication apparatus according to the invention from which components associated with a server name and components associated with communications are omitted serve as a reminder apparatus that reminds various kinds of private information including a password and a seed.

[0019] In a computer readable nontransitory information recording medium
25 according to another aspect of the invention, a program which is recorded on the

information recording medium is configured to permit a computer to function as the individual components of the communication apparatus or the reminder apparatus.

[0020] More generally, the key used in the foregoing communication apparatus or reminder apparatus can be considered to be information which is associated with
5 the user's selection order of selecting elements in a password table or a private information table. That is, if the selection order can be uniquely derived from the key, the random table should not necessarily be used.

[0021] The program may be recorded on a computer readable nontransitory information recording medium such as a compact disk, a flexible disk, a hard disk, a
10 magneto-optical disk, a digital video disk, a magnetic tape, a semiconductor memory or a RAM (Random Access Memory) in operation.

[0022] The program may be distributed and sold over a signal line in a computer communication network, that is, a temporary signal medium,
independently of a computer on which the program is run. In addition, the
15 information recording medium may be distributed and sold independently of a computer.

Effects of the Invention

[0023] The invention can provide a communication apparatus and a reminder apparatus which are suitable for securely managing private information, such as a
20 password for utilizing a server apparatus, and a nontransitory information recording medium recording a program for allowing a computer to realize the apparatuses.

Brief Description of Drawings

[0024] FIG. 1 is an explanatory diagram illustrating the schematic configurations of a communication apparatus according to an embodiment of the
25 invention and various devices which are connected thereto;

FIG. 2 is an explanatory diagram illustrating the schematic configurations of the communication apparatus according to the embodiment;

FIG. 3 is an explanatory diagram illustrating an example of a password table for a server name of a user;

5 FIG. 4 is an explanatory diagram illustrating an example of a random table for a server name of a user;

FIG. 5 is an explanatory diagram illustrating how communication according to one example of the embodiment is carried out; and

FIG. 6 is an explanatory diagram illustrating how communication according to
10 another example of the embodiment is carried out.

Mode for Carrying Out the Invention

[0025] While the following describes an embodiment according to the present invention, the embodiment to be described below is given by way of illustration only, and does not limit the scope of the invention. Therefore, those skilled in the art can
15 employ embodiments in which the individual components or all the components are replaced with equivalent ones, and which are also encompassed in the scope of the invention.

First Embodiment

[0026] FIG. 1 is an explanatory diagram illustrating the schematic
20 configuration of a communication system including a communication apparatus according to an embodiment of the invention. A description is given below referring to FIG. 1.

[0027] In a communication system 101, a communication apparatus 121
functions as a router that relays communication between a LAN 141 and an the
25 Internet 161.

[0028] A user can access the Internet 161 via the communication apparatus 121 from a computer 151 in the LAN 141, and can access the communication apparatus 121 from the Internet 161.

[0029] Schemes of accessing the communication apparatus 121 from the

5 Internet 161 include a scheme of using a terminal apparatus 181 which is installed in such as an Internet Cafe other than the LAN 141, and used by unspecified multiple users, as well as a scheme of using a mobile terminal 171 such as a cellular phone or a smartphone owned by a user.

[0030] The Internet 161 is connected with various kinds of server apparatuses

10 191. According to the embodiment, when a user tries to use the server apparatus 191 through a computer 151 in the LAN 141 or a terminal apparatus 181 within an external network such as an Internet Cafe, a password of the user is transferred to the server apparatus 191 using the communication apparatus 121.

[0031] The communication apparatus 121 according to the embodiment is

15 realized by a computer for a router on which a predetermined program runs.

[0032] A typical computer for a router uses, under control of a CPU (Central Processing Unit), a RAM as a temporary memory area and an EEPROM (Electrically Erasable Programmable Read Only Memory) or HD (Hard Disk) as a non-volatile memory area, and uses two NICs (Network Interface Cards) to communicate with the

20 Internet 161 or the computer 151 within the LAN 141. The CPU refers to the RAM and EEPROM, HD or the like, or uses the NICs to perform processes such as acquisition and provision of various kinds of data, and computations.

[0033] When the computer for a router has a capability of a wireless router, one of the two NICs serves as an access point of a wireless LAN to relay communication

25 with the computer 151 within the LAN 141 and the Internet 161.

[0034] At the time of accessing the computer for a router from the Internet 161, it is possible to use a fixed host name and a fixed global IP (Internet Protocol) address that are assigned to the computer for a router, or a fixed host name and a dynamic global IP address that are provided by a DDNS (Dynamic Domain Name System).

[0035] The computer for a router is accessed via a browser or the like on another computer within the LAN 141 or receives an instruction via a keyboard, a mouse or the like which is connected to the computer for a router to execute various maintenances.

10 [0036] The program is recorded on the HD or EEPROM and is read out into the RAM to be executed. The distribution of the program is realized by downloading the program via the NIC from another device in the Internet or by using a DVD-ROM (Digital Versatile Disk ROM).

[0037] (Fundamental Configuration of Communication Apparatus)

15 FIG. 2 is an explanatory diagram illustrating the schematic configurations of the communication apparatus 121 according to the embodiment. The following description is given referring to FIG. 2.

[0038] The communication apparatus 121 includes a storage 201, a receiver 202, a generator 203, a presenter 204, an acceptor 205, an identification unit 206, an acquirer 207, an output unit 208, and an updater 209.

[0039] While the communication apparatus 121 generally manages passwords of a plurality of users, the following describes management of information on a specific single user for the ease of understanding. By way of executing similar processing for each of a plurality of users, the communication apparatus 121 can manage the passwords of those users. In a case where a plurality of users use the

communication apparatus 121, identification information such as server names of the users and unique ID numbers of the computers 151 or the mobile terminals 171 that are used by the users are specified in exchanging various kinds of information.

[0040] An selection order for selecting a predetermined number of elements from elements in a table having a predetermined number of rows and a predetermined number of columns is assigned to a user whose password is managed by the communication apparatus 121. This selection order is used in authenticating the user.

[0041] (Password Table)

10 A server name and a password table having a predetermined number of rows and a predetermined number of columns are stored in the storage 201 in association with each other. The storage 201 is realized by an EEPROM or HD according to the embodiment.

[0042] The server name is the name of the server apparatus 191 available to the user, and the domain name or IP address of the server apparatus 191 is used as such according to the embodiment.

[0043] FIG. 3 is an explanatory diagram illustrating an example of a password table for a server name of a user. The following description is given referring to FIG. 3.

20 [0044] A password table 301 illustrated in FIG. 3 includes twenty-five elements 302 in five rows by five columns. Three random alphanumeric characters are embedded in each of the elements 302 in the password table 301. To express each element in the password table 301, a lower-case alphabet is suffixed to the end of numeral "302," and a numeral without such a suffix means a generic name.

25 [0045] As mentioned above, a selection order of sequentially selecting a certain

number of elements from the 5 by 5 table is assigned to the user of the password table 301. It is assumed herein that a selection order of "first selecting the first row and the first column, then selecting the second row and the fifth column, and finally selecting the fourth row and the second column" is assigned to the user.

5 [0046] According to the embodiment, an actual password for the server name of the user is obtained as "Lmja8i6zh" by coupling three characters "Lmj" of an element 302a of the first row and the first column in the password table 301, three characters "a8i" of an element 302 of the second row and the fifth column in the password table 301, and three characters "6zh" of an element 302c of the fourth row
10 and the second column in the password table 301.

[0047] Random alphanumeric characters are embedded in the elements 302 in the password table 301 which are not included in the selection order. Even if the communication apparatus 121 is cracked or hacked and the password table 301 is entirely leaked, the actual password of the user for the server name is not
15 immediately detected by the cracker or hacker. This is one of the features of the embodiment.

[0048] According to the embodiment, when a user attempts to use the server apparatus 191, the user sends an authentication request specifying the server name of the server apparatus 191 from a computer 151 within the LAN 141 or a terminal
20 apparatus 181 or the like outside the LAN 141, which is involved in the use of the server apparatus 191.

[0049] Then, the receiver 202 receives the authentication request specifying the server name. Therefore, the NIC serves as the receiver 202 under control of the CPU.

25 [0050] (Random Table)

Upon reception of the authentication request, the generator 203 generates a random table having the same number of rows and the same number of columns as the password table 301 stored in the storage 201 for the server name specified in the authentication request of the user. According to the embodiment, the CPU executes
 5 this generation process.

[0051] FIG. 4 is an explanatory diagram illustrating an example of a random table for a server name of a user.

[0052] A random table 401 illustrated in FIG. 4 has the same number of rows and the same number of columns as the password table 301, i.e., a 5 by 5 table, and
 10 two random numerals are embedded in each of elements 402 in the random table 401. The numerals embedded in the individual elements 402 differ from one another.

[0053] The random table 401 generated by this way is presented to the user by the presenter 204. For example, the CPU in the computer for a router carries out this presentation process by instructing the computer 151 within the LAN 141 or the
 15 terminal apparatus 181 outside the LAN 141, which the user attempts to use in accessing the server apparatus 191, by means of the NIC to display the random table 401 on the monitor screen.

[0054] The user presented with the random table 401 makes selection from the elements 402 in the random table 401 according to the user's own selection order.
 20 According to the above example, a two-digit numeral "13" in an element 402a of the first row and the first column in the random table 401, a two-digit numeral "02" in an element 402b of the second row and the fifth column in the random table 401 and a two-digit numeral "31" in an element 402c of the fourth row and the second column in the random table 401.

25 [0055] Then, the user sends a key comprised of a six-digit numeral "130231"

obtained by coupling those numerals to the communication apparatus 121 from the mobile terminal 171 or the like the user owns.

[0056] The acceptor 205 in the communication apparatus 121 accepts this key "130231" from the user. Therefore, the NIC serves as the acceptor 205 under
5 control of the CPU.

[0057] Further, the identification unit 206 identifies the selection order associated with the user from the accepted key and the generated random table 401.

[0058] In this example, the accepted key is separated two digits by two digits to obtain "13", "02" and "31". Since the individual elements 402 in the random table
10 401 differ from one another, the user's selection order is identified as "first selecting the first row and the first column, then selecting the second row and the fifth column, and finally selecting the fourth row and the second column" by searching the individual elements 402 in the random table 401 for those three two-digit numerals.

[0059] As another possible mode, a graphical image may be put in each
15 element in the random table 401 or each element may be set blank. In this mode, a user may be permitted to input a row number and a column number of each element in the random table 401.

[0060] Moreover, another mode may be taken such that pictures are displayed in the individual elements in the random table 401, and random numerals which are
20 not displayed are assigned to the respective elements, so that when a user specifies a picture, the numeral assigned to the element for the picture is selected.

[0061] That is, a table having the same number of rows and the same number of columns as the random table 401 and having various pictures, symbols or illustrations disposed in the elements, not the random table 401 as shown in FIG. 4,
25 is displayed on the screen.

[0062] Then, when the user specifies an element having a graphical image or the like drawn therein (for example, when the screen is structured as a touch screen, the user should directly touch the element with a finger; alternatively, a scheme of moving a cursor on the screen using a keyboard or mouse and then operating a Set
 5 key or a mouse button to specify an element may be employed), the numeral in the random table 401 in FIG. 4 which is arranged at the same row and the same column as that element is selected.

[0063] This mode uses pictures or the like familiar with a user and thus brings about an effect of facilitating the user's selection in the random table 401.

10 [0064] Then, the acquirer 207 acquires the password of the user who wants to access the server apparatus 191 with the server name specified in the authentication request. That is, the acquirer 207 selects from the password table 301 three characters "Lmj" of the element 302a of the first row and the first column in the password table 301, three characters "a8i" of the element 302 of the second row and
 15 the fifth column in the password table 301, and three characters "6zh" of the element 302c of the fourth row and the second column in the password table 301 in the selection order identified in the foregoing manner, and coupling the characters to acquire the password "Lmja8i6zh." Therefore, the CPU cooperates with the EEPROM or HD to serve as the acquirer 207.

20 [0065] As apparent from the above, according to the embodiment, the selection order itself is not recorded in the communication apparatus 121. Even if the communication apparatus 121 is cracked and thus the entire password table 301 is leaked, the actual password of the user for the server name is not immediately detected by the cracker or hacker. This is one of the features of the embodiment.

25 [0066] The output unit 208 sends a use request specifying the acquired

password to the server apparatus 191 with the server name specified in the authentication request, so that the user can utilize the server apparatus 191.

[0067] That is, the communication apparatus 121 serves as a proxy server for log-in to the server apparatus 191.

5 [0068] Even after the password is sent to the server apparatus 191 via the communication apparatus 121 from the computer 151 within the LAN 141 or the mobile terminal 171 such as a cellular phone, which is used by the user, and log-in is made successfully, the communication apparatus 121 for the server apparatus 191 may be continuously used as a proxy server, or the proxy of the communication
10 apparatus 121 may be removed and communication may be carried out between the computer 151 within the LAN 141 or the mobile terminal 171 such as a cellular phone, and the server apparatus 191 as done according to the authentication technique of OpenID or the like.

[0069] FIG. 5 is an explanatory diagram illustrating how communication
15 according to one example of the embodiment is carried out. The following description is given referring to FIG. 5.

[0070] As described above, according to the example,

(1) the computer 151 within the LAN 141 or the terminal apparatus 181 outside the LAN 141 is adopted as a first terminal, and is used as a sender for
20 transmission of an authentication request (501), a destination for presentation of the random table 401 (502) and one which uses the server apparatus 191 (503), and

(2) the mobile terminal 171 is adopted as a second terminal, and is used as a sender of sending a key (504),
so that a device on which the random table 401 is displayed is separated from a
25 device for inputting the key.

[0071] According to the embodiment, the simplest mode is to input the user name of the user and the server name besides the key through the mobile terminal 171 such as a cellular phone.

[0072] In addition, it is possible to adopt a mode of managing the email address or short-message address of the mobile terminal 171 such as a cellular phone of the user in the storage 201, and informing URL (Universal Resource Locator) representing an input form to input a key to this session to permit the user to gain access using the browser of the mobile terminal 171 such as a cellular phone.

[0073] In addition, the presentation destination of the random table 401 and the sender of the key may be interchanged with each other. FIG. 6 is an explanatory diagram illustrating how communication according to another example of the embodiment is carried out. The following description is given referring to FIG. 6.

[0074] Specifically,

(1) the computer 151 within the LAN 141 or the terminal apparatus 181 outside the LAN 141 is adopted as a first terminal, and is used as a sender for transmission of an authentication request (501), a sender of sending the key (504), and one which uses the server apparatus 191 (503), and

(2) the mobile terminal 171 is adopted as a second terminal, and is used as a destination for presentation of the random table 401, so that a device on which the random table 401 is displayed is separated from a device for inputting the key.

[0075] According to the mode, a mode of managing the email address or short-message address of the mobile terminal 171 such as a cellular phone of the user may be managed in the storage 201, and the random table 401 may be presented in the form of description in the text of an email or a short message for this session this

session, or a URL (Universal Resource Locator) representing an input form to display the random table 401 may be informed to permit the user to gain access using the browser of the mobile terminal 171 such as a cellular phone.

[0076] With those modes adopted, even if a cracker or hacker traces the display
5 on the monitor screen of the terminal apparatus 181 or the history of operations on the keyboard for the terminal apparatus 181, the password for the server apparatus 191 is not leaked. Therefore, security can be improved significantly.

[0077] In addition, when and only when the server apparatus 191 is accessed through the communication apparatus 121 from the computer 151 within the LAN
10 141, the computer 151 within the LAN 141 may be allowed to serve as the sender of the authentication request, the presentation destination of the random table 401 and one which uses the server apparatus 191 sending the key.

[0078] This is because with the communication apparatus 121 serving as a router for a home LAN, it is considered that the computer 151 within the LAN 141
15 has a high reliability even when those pieces of information are exchanged thereover.

[0079] Of course, even the computer 151 within the LAN 141 accesses the server apparatus 191 through the communication apparatus 121, a mode of separating the first terminal from the second terminal as mentioned above may be adopted.

20 [0080] Further, at the time of making the authentication, the communication apparatus 121 may also check information for identifying a user, such as a user name and the ID number of the mobile terminal 171 such as a cellular phone.

[0081] The number of rows and the number of columns in the password table 301, and the length of a string of characters included in each element 302 are not
25 limited to those mentioned above, and may be changed variously. In general, a

plurality of password tables 301 for various server apparatuses 191 are prepared for a single user, so that the number of rows and the number of columns are common in those password tables 301. Moreover, the length of a character string in each element 302 is determined by the length of a password needed for the server apparatus 191 for the password table 301, and the number of elements 302 to be selected based on the user's selection order.

[0082] While the number of rows and the number of columns of the random table 401 should be common to those of the password table 301, the type and length of a character string included in each element 402 may be varied as needed. In order to permit a user's selection order to be obtained from the random table 401 and the key, the random table 401 is generally structured so that each character string in every element 402 has a common length and the elements 402 differ from one another.

[0083] A character string included in each element 302 in the password table 301 and a character string included in each element 402 in the random table 401 may be used as prefix codes, so that those character strings may have variable lengths. That is, those tables should be structured at random in such a way that each character string in an element in the table has such a property as not to be a prefix of the character string in any one of the other elements in the table. The use of prefix codes permits the selection order to be uniquely restored from the key.

[0084] According to the embodiment, the output unit 208 outputs a password by sending a use request specifying the password to the server apparatus 191.

[0085] In addition, when the first terminal (computer 151 or terminal apparatus 181) and the second terminal (mobile terminal 171) are configured integral with the communication apparatus 121, the communication apparatus 121 serves as a

password reminder.

[0086] Typically, the communication apparatus 121 in this mode includes an input unit such as a keyboard or touch panel, and a display unit such as a display, and is realized by a cellular phone, smartphone or the like which has a communication
5 capability to be connectable to the Internet 161.

[0087] According to the mode, the authentication request is given by the user via the input unit of the communication apparatus 121 (501).

[0088] The random table is displayed on the display unit (502) to be presented to the user.

10 [0089] The user performs conversion on the displayed random table to provide the communication apparatus 121 with a key via the input unit (504).

[0090] Then, the output unit 208 of the communication apparatus 121 displays the acquired password on the display unit to inform the user of the password for the desired server apparatus.

15 [0091] According to the password reminder of the mode, a password is not directly stored in the storage 201, so that even if a smartphone or the like constituting the communication apparatus 121 is stolen, the password is not immediately leaked.

[0092] Because a rule for conversion by a user is not recorded in the communication apparatus 121, when a third party has obtained the smartphone or the
20 like and attempts an illegal use thereof, the risk is low of making the "password" displayed on the display unit actually available on the server apparatus.

[0093] Various modes of the password reminder based on the principle of the invention will be further described in the description of a third embodiment to be discussed later.

25 [0094] (New Registration in Server Apparatus)

Although the foregoing description is premised on a situation where the password table 301 is already stored in the storage 201, the following describes a scheme to newly generate a password table 301 for a user for a server apparatus 191 with a certain server name.

5 [0095] That is, when a password table which is associated with the server name specified in the authentication request is not stored in the storage 201, the updater 209 generates a new password table having a predetermined number of rows and a predetermined number of columns, and stores the new password table in the storage 201 so as to update the storage 201.

10 [0096] The length of a character string (the number of characters) determined for each element 302 of the new password table 301 and the type of the characters are determined according to specification data of the user's selection order and the type of a password which is allowed by the corresponding server apparatus 191.

[0097] When N elements 302 are selected according to the user's selection
15 order, and the length of the password for the server apparatus 191 is M characters, the length, L, of a character string to be stored in each element 302 is determined to satisfy

$$L \times (N-1) < M \leq L \times N.$$

[0098] In a system in which the length of a password should be required to be
20 within a certain range, it is desirable to set M and L so that the equality holds in the inequality expression.

[0099] When the length of a password is fixed and the expression with the equality in the inequality expression is not fulfilled, the following scheme may be adopted.

25 (1) A scheme of storing the length, M, of a password in addition to the

password table 301 in association with the server name. According to the scheme, any M characters are regularly extracted from a character string of L×N characters obtained according to the selection order, and are used as a password. A specific rule is to extract top an M characters or extract a last M characters. There is another
 5 scheme of adopting the Bresenham's line algorithm to draw a line with a slope of M over L×N using only addition and subtraction of integers to thereby extract a single character every time an error counter is carried up.

(2) A scheme of obtaining a password when a character which cannot be used by the server apparatus 191 is inserted as appropriate, and deleting this unusable
 10 character from a character string of L×N characters. For example, in general, ASCII characters with character codes 32 to 127 are available for an ordinary password, and a Tab character and a line feed character may not be available. According to this scheme, therefore, those unavailable characters are inserted in the individual elements 302 at random. It is desirable that the individual elements 302
 15 should be set at random in such a way that the ratio of the number of characters in the entire elements 302 in the password table 301 to the number of available characters which appear in the entire elements 302 in the password table 301 matches with $M/L \times N$ as much as possible.

[0100] After a new password table 301 for the user for the server name is
 20 generated and then stored in the storage 201 this way, the output unit 208 sends a use request to the server apparatus 191 with the server name specified in the authentication request to register the user in the server apparatus 191.

[0101] That is, when obtaining a password from the stored password table 301 in the above manner, the output unit 208 sends this password to the server apparatus
 25 191 as a "password for a user registered as a user for the server apparatus 191 to log

in."

[0102] When obtaining a password from the password table 301 which has been newly generated by the updater 209 and has just been stored in the storage 201, on the other hand, the output unit 208 sends this password to the server apparatus 191 as a "log-in password for newly registering a user who is not registered as a user for the server apparatus 191".

[0103] This mode is useful even when a password in the server apparatus 191 has an expiration period and needs to be changed. That is, the acquirer 207 obtains an old password from an existing password table 301 and obtains a new password from a newly generated password table 301, and the output unit 208 sends both passwords to the server apparatus 191 to update the password.

[0104] According to the mode, a user need not consider a password which is hardly imaginable by a third party and is easy to remember. This is because the password of the user for the server apparatus 191 is generated at random, and is hardly imaginable by any one. Therefore, security of a password for the server apparatus 191 can be enhanced more as compared with the case where a user selects a password himself/herself.

[0105] Although the communication apparatus 121 according to the embodiment is installed on a computer for a router most typically, the communication apparatus 121 should not necessarily function as a router. For example, the communication apparatus 121 can be realized by a computer that serves as a proxy for the server apparatus 191 in some mode, which is encompassed in the scope of the invention.

Second Embodiment

[0106] The foregoing embodiment may be carried out on the assumption that a

user registration is newly made to the server apparatus 191, whereas the embodiment set forth below may cope with a case where a user registration has been made to the server apparatus 191 and further a his/her password has already been set.

[0107] In this case, a password table associated with the server name specified
5 in the authentication request is not stored in the storage 201.

[0108] Thus, as in the first embodiment, the updater 209 generates a new password table 301 having a predetermined number of rows and a predetermined number of columns, and stores the new password table 301 in the storage 201 in association with the server name, thereby updating the storage 201.

10 [0109] It is noted however that the embodiments slightly differ from each other in how a character string to be embedded in each element 302 in the password table 301 is formed.

[0110] Specifically, the updater 209 accepts an input of a password from the user to the server apparatus 191. From the viewpoint of enhancing security, it is
15 desirable that the device the user uses to input the password be limited to a computer 151 within the LAN 141.

[0111] The user inputs a user name and a server name via the computer 151 within the LAN 141, and an authentication request specifying the user name and the server name is sent to the server apparatus 191 via the computer 151. Then, the
20 updater 209 of the communication apparatus 121 requests the computer 151 to cause the user to input the password for the server apparatus 191, and accepts the password sent from the computer 151.

[0112] There is another mode in which a user inputs a password in addition to a user name and a server name. In this case, the password for the server apparatus
25 191 is added as additional information for an authentication request. The updater

209 accepts the password added to the authentication request.

[0113] Then, generation and presentation of the random table 401, input of a key by the user, and identification of the user's selection order are carried out in the same way as the first embodiment.

5 [0114] When an existing password for the server apparatus 191 is obtained this way, the existing password is separated into segments equal in number to the elements to be selected according to the selection order. When the lengths of segments are not constant, the length of the password itself is saved in the storage 201 or a line feed character or the like is embedded in the password to adjust the
10 length.

[0115] Then, the updater 209 sequentially stores the segments, obtained by separating the password, into the elements in the password table 301 according to the identified selection order.

[0116] Thereafter, random character strings equal in length to the segments of
15 the password are generated and embedded in those individual elements 302 in the password table 301 which are not associated with the selection order. In this case, random character strings are generated according to the frequencies of appearance of the types of characters appearing in the password, such as an alphabet letter, numeral or symbol, and an inserted line feed character or the like, so that even if the password
20 table 301 is leaked, it is possible to prevent a third party from predicting the password.

Third Embodiment

[0117] The aforementioned communication apparatus 121 manages the password table 301 associated with a user and a server name. In addition, even
25 when the password table 301 is directly displayed on the screen, the password of the

user for the server apparatus 191 is not immediately recognized. The password for the password table 301 is not obtained unless the user's selection order and the password table 301 are both acquired.

[0118] Therefore, when the user accesses the communication apparatus 121 via the computer 151 within the LAN 141 and requests a password table 301 to be associated with the user and the server name, the communication apparatus 121

(a) displays the password table 301 on the screen of the computer 151 within the LAN 141 in response to the computer 151 within the LAN 141, or

(b) sends an email describing the password table 301 to the email address of the mobile terminal 171 such as a cellular phone, or the like, which has been set for the user in advance, so that a so-called password reminder can be realized.

[0119] In addition, there may be a mode in which when a mobile terminal 171 such as a cellular phone request a password table 301 to be associated with a user and a server name, the communication apparatus 121 checks the ID number of the mobile terminal 171 such as a cellular phone, and sends an email describing the password table 301 to an email address associated with the mobile terminal 171 such as a cellular phone.

[0120] That is, although the communication apparatus 121 sends the random table 401 to the mobile terminal 171 according to the above embodiment, the communication apparatus 121 can be allowed to send the password table 301 to the mobile terminal 171 upon successful authentication of the communication apparatus 121 (normal password-based authentication may be adopted, or authentication using a random table and a selection order may be adopted, as in the foregoing example, so that the selection order itself serves as a password).

[0121] Some general browsers store a password for a certain site to be prepared for a next log-in. The browser with such a capability often provides a function of displaying a password itself on the screen, whereas a password itself is not directly displayed on the screen according to the embodiment.

- 5 [0122] Therefore, a temperature reminder safer than the conventional type can be realized.

Fourth Embodiment

[0123] According to the embodiment, a string of elements obtained by arranging the elements 302 in a password table 301 is used directly as a password for
10 utilizing the server apparatus 191.

[0124] According to the embodiment, a string of elements obtained by arranging elements 302 selected from a password table 301 based on a rule assigned to the user is used as a seed for a one-time password. The following first describes a conventional time-synchronous one-time password system.

- 15 [0125] In the conventional system, each user is provided with an electronic device called "token."

[0126] A seed assigned to the user is recorded in the token in a non-volatile manner. In general, a seed is a string of characters and/or a string of numerals.

- [0127] With regard to a token, a current time (typically expressed in terms of
20 an elapsed time from a specific reference time) is acquired by referring to a real-time clock or the like, a predetermined one-way function is applied to the acquired current time and the seed stored in a non-volatile manner to compute a string of characters or a string of numerals (6-digit numeral string in a system which is popular today),
thereby providing a one-time password, which is in turn displayed on a liquid crystal
25 display.

[0128] On the other hand, the server apparatus is designed to be able to compute a one-time password for each user from the seed assigned to each user and the current time by applying the predetermined one-way function thereto.

[0129] Accordingly, the server apparatus carries out authentication by checking
5 if the combination of the user name and the one-time password both sent from a terminal apparatus matches with one-time password which is computed from the combination of the seed for the user and the current time.

[0130] According to the embodiment, in such a one-time password system, a user does not carry around an exclusive token, but the invention is used to prevent a
10 seed from being leaked at the time of using a cellular phone, a smartphone, a mobile computer or the like as a token.

[0131] According to the embodiment, the seed for the user is divided into segments based on the user's rule, the segments are embedded into elements in the password table 301 to be stored in the storage 201 which are based on the user's rule,
15 and random strings with substantially the same lengths are embedded in the other elements.

[0132] The receiver 202 of the communication apparatus 121 accepts an authentication request issued based on a keyboard operation or a touch-panel operation by the user via a signal line of an electronic circuit of this hardware.

20 [0133] The generator 203 generates a random table 401 as done in the foregoing embodiment. The presenter 204 displays the generated random table 401 on the display provided on the communication apparatus 121.

[0134] The acceptor 205 accepts a key input based on a keyboard operation or a touch-panel operation by the use, and the identification unit 206 identifies the user's
25 conversion rule based on the random table 401 and the key.

[0135] The acquirer 207 sequentially extracts elements in the password table 301 and arranging the elements based on the user's conversion rule, thereby acquiring a seed. Further, the acquirer 207 refers to the real-time clock or the like to acquire a current time. Then, the acquirer 207 applies a predetermined one-way
5 function to the seed and the current time to compute a one-time password for the user.

[0136] The output unit 208 displays the computed one-time password on the display. The other structures can be set the same as those of the foregoing embodiment.

10 [0137] The invention can likewise be adapted to such a time-synchronous one-time password system even when the router or the like of the LAN 141 is used as the communication apparatus 121 according to the invention.

[0138] This embodiment may be reckoned as the foregoing embodiment in which a one-time password seed is used as the password for a user. According to
15 the embodiment, as in the foregoing embodiment, the server apparatus of the conventional one-time password system can be used directly.

Fifth Embodiment

[0139] Although each of the communication apparatuses 121 can be realized by a computer having a communication capability, the communication apparatus 121
20 should not necessarily have the communication capability when the communication apparatus 121 is permitted to serve as a password reminder. That is, even under a situation where connection to the Internet 161 is not possible, the communication apparatus 121 can be permitted to serve as a password reminder by running a predetermined program on the computer 151, the mobile terminal 171, the terminal
25 apparatus 181 or the like.

[0140] A password and a seed are information which should be confidential to a third party. Therefore, more generally speaking, the password reminder according to the embodiment can be regarded as a reminder for private information.

[0141] That is, with private information divided into a predetermined segments
5 which are stored in the password table 301, the password reminder can serve as a reminder apparatus for various kinds of private information. Although the password table 301 according to this mode has a structure similar to that of the foregoing mode, the password table 301 serves as a private information table in which segments of various kinds of private information including a password are
10 embedded.

[0142] To store plural kinds of private information in the reminder apparatus according to the embodiment, the type of necessary private information is identified based on information from the user accepted by the receiver 202. That is, the reminder apparatus according to the mode causes a user to input a name of the type
15 of private information instead of a server name by means of the receiver 202.

[0143] When private information is limited to one type, the receiver 202 can be omitted. In this case, the generator 203 generates a random table regularly or based on an instruction from the user.

[0144] The output unit 208 may automatically provide private information as a
20 password for various kinds of authentication functions on a computer which serves as the reminder apparatus, or may provide an external server apparatus with private information using the communication capability, besides the output to be displayed on the liquid crystal display.

[0145] As private information, various kinds of information such as the social
25 security number, insurance number, credit card number and bank account number of

a user, besides a password and a seed, can be stored in the reminder apparatus.

Those pieces of private information may be simply divided into segments to be stored in the a private information table (password table 301), or another mode may be adopted in which private information may be encrypted and stored separately and
 5 a key for decrypting the encrypted private information is stored in the private information table (password table 301).

[0146] Note that more generally, the key in the communication apparatus 121 or the reminder apparatus can be considered as information to be associated with the user's selection order of selecting elements in the password table 301 or private
 10 information table. That is, if the selection order can be uniquely derived from the key, the random table 401 should not necessarily used.

[0147] For example, a mode in which the password table 301 is directly displayed on the screen may be adopted. Further, a mode in which the individual elements in the random table 401 are always fixed may be adopted.

15 [0148] This application claims priority based on Japanese Patent Application No. 2010-194234 filed on August 31, 2010, the entire disclosure of which is incorporated herein by reference in its entirety as much as is permitted by the law of the designated country.

Industrial Applicability

20 [0149] The present invention can provide a communication apparatus and a reminder apparatus which are suitable for securely managing private information, such as a password for utilizing a server apparatus, and a nontransitory information recording medium recording a program for allowing a computer to realize the apparatuses.

Description of Reference Numerals

[0150]	101	Communication system
	121	Communication apparatus
	141	LAN
5	151	Computer
	161	Internet
	171	Mobile terminal
	181	Terminal apparatus
	191	Server apparatus
10	201	Storage
	202	Receiver
	203	Generator
	204	Presenter
	205	Acceptor
15	206	Identification unit
	207	Acquirer
	208	Output unit
	209	Updater
	301	Password table
20	302	Elements in password table
	401	Random table
	402	Elements in random table

CLAIMS

1. A communication apparatus comprising:
 - a storage that stores server names and a password table in association with each other, the password table having a predetermined number of rows and a
 - 5 predetermined number of columns;
 - a receiver that receives an authentication request specifying a server name;
 - a generator that generates a random table having the predetermined number of rows and the predetermined number of columns;
 - a presenter that presents the generated random table to a user;
 - 10 an acceptor that accepts from the user a key obtained by selecting and arranging elements in the presented random table in a selection order associated with the user;
 - an identification unit that identifies the selection order associated with the user from the accepted key and the generated random table;
 - 15 an acquirer that acquires a password from a column of elements obtained by selecting elements included in the password table, stored in the storage in association with the server name specified in the authentication request, from the password table in the identified selection order, and arranging the elements in the identified selection order; and
 - 20 an output unit that outputs the acquired password as a password for allowing the user to use a server apparatus with the server name specified in the authentication request.
2. The communication apparatus according to Claim 1, wherein
 - the server apparatus with the server name specified in the authentication
 - 25 request determines whether the server apparatus is available to the user based on a

time-synchronous one-time password, and

the acquirer acquires, as the password, a result of applying a predetermined one-way function to a seed including the obtained column of elements and a current time.

5 3. The communication apparatus according to Claim 1, wherein
the acquirer acquires the obtained column of elements as the password.

4. The communication apparatus according to Claim 1, wherein
the output unit outputs the acquired password by displaying the acquired
password to the user.

10 5. The communication apparatus according to Claim 1, wherein
the output unit outputs the acquired password by sending a use request
specifying the acquired password to the server apparatus with the server name
specified in the authentication request.

6. The communication apparatus according to Claim 5, wherein
15 the receiver receives the authentication request from a first terminal which is
used by the user,

the presenter presents the generated random table to a second terminal which
is used by the user,

the acceptor accepts the key from the first terminal, and
20 the output unit sends the use request to permit the user to use the server
apparatus through the first terminal.

7. The communication apparatus according to Claim 5, wherein
the receiver receives the authentication request from a first terminal which is
used by the user,
25 the presenter presents the generated random table to the first terminal which is

used by the user,

the acceptor accepts the key from a second terminal, and

the output unit sends the use request to permit the user to use the server apparatus through the first terminal.

- 5 8. The communication apparatus according to Claim 5, further comprising an updater that, when the password table associated with the server name specified in the authentication request is not stored in the storage, updates the storage by generating a new password table having the predetermined number of rows and the predetermined number of columns, setting individual elements in the new password
10 table, and storing the new password table in the storage in association with the server name,

wherein the output unit sends the use request to the server apparatus with the server name specified in the authentication request to register the user in the server apparatus.

- 15 9. The communication apparatus according to Claim 1, further comprising an updater that, when the password table associated with the server name specified in the authentication request is not stored in the storage, updates the storage by generating a new password table having the predetermined number of rows and the predetermined number of columns, accepting an input of a password from the user,
20 dividing the accepted password into segments to be stored in elements in the identified selection order in the new password table, setting other elements at random, and storing the new password table in the storage in association with the server name.

10. A computer readable nontransitory information recording medium
25 recording a program that permits a computer to function as individual components of

the communication apparatus of Claim 1.

11. A reminder apparatus comprising:

a storage that stores a private information table having a predetermined number of rows and a predetermined number of columns;

5 a generator that generates a random table having the predetermined number of rows and the predetermined number of columns;

a presenter that presents the generated random table to a user;

an acceptor that accepts from the user a key obtained by selecting and arranging elements in the presented random table in a selection order associated with
10 the user;

an identification unit that identifies the selection order associated with the user from the accepted key and the generated random table;

an acquirer that acquires private information from a column of elements obtained by selecting elements included in the private information table stored in the
15 storage from the private information table in the identified selection order, and arranging the elements in the identified selection order; and

an output unit that outputs the acquired private information.

12. A reminder apparatus comprising:

a storage that stores a private information table having a predetermined
20 number of rows and a predetermined number of columns;

an acceptor that accepts from a user a key associated with a selection order of selecting elements in the private information;

an identification unit that identifies the selection order associated with the user from the accepted key;

25 an acquirer that acquires private information from a column of elements

obtained by selecting elements included in the private information table stored in the storage from the private information table in the identified selection order, and arranging the elements in the identified selection order; and
an output unit that outputs the acquired private information.