

## Authentication Information Processing

### Filed of the Invention

[0001] The present invention generally relates to a method and system for processing data, more particularly, the present invention relates to a method and system for processing authentication information.

### Description of the Related Art

[0002] Authentication technologies are used for determining whether a user or other entity is permitted to access a specific system or resource. Authentication technologies have been widely applied in various computer applications. Password-based authentication is a most common technology. In password authentication, the user will send a login request including a user account and password, and the sever end will transfer the login request to an authentication node, which authenticates the authentication information in the login request according to the authentication information stored on the node.

[0003] Authentication information in the prior art is usually stored in one or more fixed authentication nodes. An authentication system with only one authentication node has poor security, since the authentication node is prone to be attacked by hackers. The Lightweight Directory Access Protocol (LDAP) is a protocol for accessing an online directory service. Distributed LDAP systems have been widely applied in authentication, so as to allow a plurality of authentication nodes to interconnect with each other to form an authentication cluster. For performance optimization and disaster recovery considerations, authentication information will be distributed among multiple authentication nodes. For example, assuming a company has 100 employees, with the employee numbers from No.1-No.100. The authentication information for a user to log in the company's intranet is distributed among 5 authentication nodes. In order to enable a login request to get a timely response and prevent data loss due to disasters or machine malfunctions, the authentication information of the 100 employees may be stored on 5 authentication nodes redundantly. The distribution result of the authentication information may be as in the following Table 1:

| Authentication node                     | Node1                     | Node 2                     | Node 3                     | Node 4                                    | Node 5                      |
|-----------------------------------------|---------------------------|----------------------------|----------------------------|-------------------------------------------|-----------------------------|
| Authentication information of employees | No.1-No.20<br>No.31-No.50 | No.21-No.40<br>No.51-No.70 | No.41-No.60<br>No.71-No.90 | No.61-No.80<br>No.1-No.10<br>No.91-No.100 | No.81-No.100<br>No.11-No.30 |

Table 1

[0004] As can be seen from Table 1, the authentication information of each employee is stored on two different authentication nodes.

### Summary of the Invention

[0005] The inventor of the present invention finds that each authentication information in the prior art is stored on one or more authentication nodes. However, once the authentication information is stored on the one or more authentication nodes, it will not be updated, and is stored on the original authentication node(s) all the time. Therefore, this manner of storing authentication information fixedly will bring some potential security risks. Once a hacker breaks the one or more authentication nodes, he/she will get the corresponding authentication information. If the authentication information of a company's intranet is centralized on one authentication node, the hacker can obtain the authentication information of all the employees permanently once he/she breaks the authentication node. If the authentication information of a company's intranet is stored among a plurality of authentication nodes in a plurality of countries in a distributed manner, then the hacker may permanently obtain the authentication information of the company's senior executives by attacking the authentication node at the place where the company's headquarter is located. That is to say, the manner of storing authentication information fixedly will enable hackers to have greater possibility to obtain the authentication information and permanently use the obtained authentication information.

[0006] In order to solve the above problem, the present invention proposes an authentication information processing technology, which will make authentication information to rotate among multiple authentication nodes, so that hackers will be unable to obtain the authentication information permanently.

[0007] Specifically, the present invention provides a method for processing authentication information, wherein the authentication information is stored on a first authentication node, the method comprising: determining a rotation sequence of the authentication information, determining a rotation trigger condition of the authentication information, and in response to satisfaction of the rotation trigger condition, transmitting at least part of the authentication information to a second authentication node according to the rotation sequence.

[0008] The present invention further provides a system for processing authentication information, wherein the authentication information is stored on a first authentication node, the system comprises: a rotation sequence determining means configured to determine a rotation sequence of the authentication information, a rotation trigger condition determining means configured to determine a rotation trigger condition of the authentication information, and a transmitting means configured to, in response to satisfaction of the rotation trigger condition, transmit at least part of the authentication

information to a second authentication node according to the rotation sequence.

[0009] According to an aspect of the present invention, the authentication information includes account information and authentication module information, wherein the rotation sequence includes rotation sequence of the account information and rotation sequence of the authentication module information, and the transmitting at least part of the authentication information to a second authentication node according to the rotation information comprises: transmitting the account information to the second authentication node according to the rotation information of the account information; the method further comprises transmitting the authentication module information to a third authentication node according to the rotation sequence of the authentication module information.

[0010] According to one aspect of the present invention, the authentication information comprises timestamp information to indicate a period of validity of the authentication information.

#### Brief Description of the Accompanying Drawings

[0011] The accompanying drawings referred to by the present invention are only for exemplifying typical embodiments of the present invention, and shall not be construed as limitation to the scope of the present invention.

[0012] Fig. 1 shows a block diagram of an exemplary computing system suitable for realizing an implementation of the present invention.

[0013] Fig. 2 shows a flowchart of the authentication information processing method of the present invention.

[0014] Fig. 3 shows a flowchart for determining a rotation sequence of authentication information according to an embodiment of the present invention.

[0015] Fig. 4A shows a schematic diagram of authentication information according to an embodiment of the present invention.

[0016] Fig. 4B shows a schematic diagram of authentication information according to another embodiment of the present invention.

[0017] Fig. 5 shows a flowchart of dispatching an authentication request according to an embodiment of the present invention.

[0018] Fig. 6 shows a flowchart of dispatching an authentication request according to another embodiment of the present invention.

[0019] Fig. 7 shows a flowchart of processing an authentication request according to an embodiment of the present invention.

[0020] Fig. 8A shows a schematic diagram of an authentication system before authentication information is rotated according to an embodiment of the present invention.

[0021] Fig. 8B shows a schematic diagram of an authentication system after authentication information is rotated according to an embodiment of the present invention.

[0022] Fig. 9A shows a schematic diagram of an authentication system before authentication information is rotated according to another embodiment of the present invention.

[0023] Fig. 9B shows a schematic diagram of an authentication system after authentication information is rotated according to another embodiment of the present invention.

[0024] Fig. 10 shows a flowchart of an authentication information processing system of the present invention.

#### Best Modes for Carrying out the Invention

[0025] The terms used herein are only for describing specific embodiments, rather than intended to limit the present invention. The singular forms used herein, “a”, “an” and “the”, are intended also to cover the plural forms, unless the context explicitly points out otherwise. It should also be known that when the word “comprise”, as used in this specification, means the existence of the stated features, integers, steps, operations, units and/or components, but does not exclude the presence or addition of one or more other features, integers, steps, operations, units and/or components, and/or a combination thereof.

[0026] The corresponding structures, materials, operations and all the equivalent replacements of the functionally defined means or steps in the claims are intended to include any structures, materials or operations for executing the functions in combination with the other units as specifically stated out in the claims. The objective of the presented description of the present invention is illustration and description, and it is non-exhaustive, nor limits the present invention to the described forms. It is obvious to those of ordinary skill in the art that many modifications and variants can be made without departing from the scope and sprits of the present invention. The selection and description of the embodiments are intended to better interpret the principles and practical applications of the present invention, so that those of ordinary skill in the art know that the present invention may have various implementations

with various changes suitable for the desired specific purposes.

[0027] Those skilled in the art know that many aspects of the present invention may be embodied as systems, methods or computer program products. Therefore, many aspects of the present invention may specifically take the following forms, i.e., entirely hardware, entirely software (including firmware, resident software, microcode, etc.), or a combination of software portion and hardware portion generally called “circuit”, “module” or “system” herein. In addition, many aspects of the present invention can take the form of a computer program product embodied in one or more computer readable mediums, in which computer readable program code is included.

[0028] Any combination of one or more computer readable mediums may be utilized. The computer readable medium may be a computer readable signal medium or computer readable storage medium. The computer readable storage medium, may be, for example, but not limited to, an electronic, magnetic, optical, electromagnetic, infrared or semiconductor system, apparatus, device, or any combination thereof. More specific examples (a non-exhaustive list) of computer readable medium include the following: an electrical connection having one or more wires, a portable computer diskette, a hard disc, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage device, a magnetic storage device, or any suitable combination of thereof. In the context of this document, the computer readable storage medium may be any tangible medium that contain or store a program for use by or in connection with an instruction execution system, apparatus or device.

[0029] The computer readable signal medium may include a data signal with computer readable program code embodied therein and propagated in a baseband or as part of a carrier wave. The propagated signal may take various forms, including but not limited to, an electromagnetic signal, an optical signal or any suitable combination thereof. The computer readable signal medium may be any computer readable medium that is not a computer readable storage medium, but can transmit, propagate or transport a program used by or in connection with an instruction execution system, apparatus or device. The computer program code contained in the computer readable medium may be transmitted by any appropriate mediums, including but not limited to, wireless, cable, optical fiber cable, RF, or any suitable combination thereof.

[0030] The computer program code contained in the computer readable medium may be transmitted by any appropriate mediums, including but not limited to, wireless, cable, optical fiber cable, RF, or any suitable combination thereof.

[0031] The computer program code for carrying out the operations of the present invention may be written in any combination of one or more programming languages,

including an object oriented programming language such as Java, Smalltalk, C++, or the like, and conventional procedural programming languages, such as "C" programming language or similar programming languages. The program code may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer, or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet service provider).

[0032] In the following various aspects of the present invention are described by referring to the flowcharts and/or block diagrams of the method, apparatus (system) and computer program products according to embodiments of the present invention. It should be understood that each block of the flowcharts and/or block diagrams and combinations of the blocks in the flowcharts and/or block diagrams can be implemented by computer program instructions. These computer program instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions, which are executed via the computer or other programmable data processing apparatus, create means for implementing the functions/actions specified in the blocks in the flowcharts and/or block diagrams.

[0033] These computer program instructions may also be stored in a computer readable medium that can direct a computer or other programmable data processing apparatus to function in a particular manner, such that the instructions stored in the computer readable medium produce a manufactured article including instruction means that implement the functions/actions specified in the blocks in flowcharts and/or block diagrams.

[0034] The computer program instructions may also be loaded onto a computer or other programmable data processing apparatus, to cause a series of operation steps to be performed on the computer or the other programmable apparatus, to produce a computer implemented process such that the instructions which are executed on the computer or other programmable apparatus provide processes for implementing the functions/actions specified in the blocks of flowchart and/or block diagrams.

[0035] The flowcharts and block diagrams in the drawings of the present invention illustrate the architecture, functionality and operations of possible implementations of systems, methods and computer program products according to various embodiments of the present invention. In this regard, each block in the flowcharts or block diagrams may represent a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specific logic function(s). It should also be noted that, in some alternative implementations, the functions noted in the blocks

may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams and/or flowcharts, and combinations of blocks in the block diagrams and/or flowcharts, can be implemented by special purpose hardware-based systems that perform the specified functions or actions, or a combination of the special purpose hardware and computer instructions.

[0036] Fig. 1 shows a block diagram of an exemplary computing system suitable for realizing an implementation of the present invention. As shown, the computer system 100 comprises: a CPU (central processing unit) 101, a RAM (random access memory) 102, a ROM (read-only memory) 103, a system bus 104, a hard disk controller 105, a keyboard controller 106, a serial interface bus 107, a parallel interface bus 108, a display controller 109, a hard disk 110, a keyboard 111, a serial peripheral 112, a parallel peripheral 113 and a display 114. Among these components, what are coupled with the system bus 104 are CPU 101, RAM 102, ROM 103, the hard disk controller 105, the keyboard controller 106, the serial interface controller 107, the parallel interface controller 108 and the display controller 109. The hard disk 110 is coupled with the hard disk controller 105; the keyboard 111 is coupled with the keyboard controller 106; the serial peripheral 112 is coupled with the serial interface controller 107; the parallel peripheral 113 is coupled with the parallel interface controller 108, and the display 114 is coupled with the display controller 109. It should be understood that the structural block diagram of Fig. 1 is shown only for the illustrative purpose, rather than limiting the scope of the present invention. In some cases, some devices may be added or removed depending on the specific circumstances.

[0037] Fig. 2 shows a flowchart of an authentication information processing method of the present invention. The authentication information in the authentication information processing method shown in Fig. 2 is stored on a first authentication node. According to an embodiment of the present invention, the authentication information includes account information, e.g., account ID, personal identification number PIN, etc. The account ID may be any account ID like a user name, an email, a license plate number, and the identification number may be any identification number like a password and an ID number. Fig. 4A shows a schematic diagram of authentication information according to an embodiment of the present invention, in which the authentication information includes account information Acc A. If the account information is stored as a list, it can be shown as follows:

| ID     | PIN    |
|--------|--------|
| James  | XXXXXX |
| Thomas | XXXXXX |
| .....  | .....  |

Table 2

[0038] According another embodiment of the present invention, the authentication information includes account information and authentication module information. Fig. 4B shows a schematic diagram of authentication information according to another embodiment of the present invention, in which the authentication information includes account information Acc A and authentication module information Mod A. Besides information like ID and PIN, the account information further includes an authentication module tag. The authentication module information includes the authentication module tag and an encryption algorithm. The authentication module tag is a bridge between the account information and the encryption algorithm. Those skilled in the art know that generally, a PIN is stored in ciphertext on an authentication node, and an ID can either be stored in cipher text on an authentication node, or stored in plain text on an authentication node. Conversion from plain text to cipher text is realized by the encryption algorithm. Different account information may use a uniform encryption algorithm, or use different encryption algorithms. If different account information uses a uniform encryption algorithm, there is no need to store an authentication module tag on the authentication node. If different account information uses different encryption algorithms, it is needed to differentiate different encryption algorithms in the authentication information. One simple implementation is to store an authentication module tag corresponding to an account ID in the authentication node to identify the corresponding encryption algorithm. If there are two encryption algorithms, Tag=0 indicates that first encryption algorithm is applied, while Tag=1 indicates that the second encryption algorithm is applied, then the account information in this embodiment can be shown as in the following Table 3:

| ID     | PIN    | Tag   |
|--------|--------|-------|
| James  | XXXXXX | 0     |
| Thomas | XXXXXX | 1     |
| .....  | .....  | ..... |

Table 3

[0039] The authentication module information in the present embodiment may be shown as the following Table 4:

| Tag | Encryption algorithm            |
|-----|---------------------------------|
| 0   | The first encryption algorithm  |
| 1   | The second encryption algorithm |

Table 4

[0040] From tables 3 and 4, the encryption algorithm that is applicable to an account can be determined.

[0041] As a variant of the above embodiment, it may be set that the number of the Tags is greater than the number of the encryption algorithms, which can increase system security, such that even if an authentication node is attacked by a hacker, it is difficult for the hacker to infer which encryption algorithm is used. The account

information may be shown as in the following Table 5, and the authentication module information may be shown as in the following Table 6:

| ID     | PIN    | Tag   |
|--------|--------|-------|
| James  | XXXXXX | 0     |
| Thomas | XXXXXX | 1     |
| Anna   | XXXXXX | 2     |
| Rose   | XXXXXX | 3     |
| Marry  | XXXXXX | 4     |
| .....  | .....  | ..... |

Table 5

| Tag   | Encryption algorithm            |
|-------|---------------------------------|
| 0、2、4 | The first encryption algorithm  |
| 1、3   | The second encryption algorithm |

Table 6

[0042] Similar to the mechanism that account information can be distributed among different nodes, the authentication module information can also be distributed among different authentication nodes.

[0043] The present invention does not have any specific limitation on the storage format of the authentication information. It may be a plain text file (like a CVS file), a database, a list or a directory tree (like LDAP and NIS (Network Information Service) directory tree, etc).

[0044] Returning to Fig. 1, the rotation sequence of the authentication information is determined at step 201. The rotation sequence at least describes to which authentication node an authentication node will transmit the authentication information stored thereon. According to an embodiment of the present invention, the rotation sequence is temporally determined before the rotation (e.g., one day or one hour before the rotation, etc.). Determining the rotation sequence temporally may increase system security, since hackers will be unable to determine where the authentication information on a node will be rotated to.

[0045] According another embodiment of the present invention, the rotation sequence is determined within a certain time period before the rotation (e.g., one week, one month before the rotation or even the rotation sequence of a next rotation is determined right after the last rotation). In such an embodiment, since the rotation sequence is determined a period of time in advance, the overhead brought by determining the rotation sequence before the rotation is saved.

[0046] If the authentication information includes account information and authentication module information, then the rotation sequence may further include a rotation sequence of the account information and a rotation sequence of the

authentication module information. The rotation sequence of the account information and the rotation sequence of the authentication module information may be the same or different. In the case that the rotation sequence of the account information and the rotation sequence of the authentication module information are different, the authentication node to which the account information is rotated may be different from the authentication node to which the authentication module information is rotated; for example, the account information may be transmitted to a second authentication node while the authentication module information may be transmitted to a third authentication node.

[0047] At step 203, the rotation trigger condition of the authentication information is determined. The rotation trigger condition describes when or under what condition the rotation starts. From a general perspective, the rotation trigger condition may be either a static trigger condition or a dynamic trigger condition. A static trigger condition may be reaching a predetermined time (e.g., after three months), that is to say, the rotation of the authentication information is performed every predetermined time period. According to an embodiment of the present invention, the predetermined time period may be a fixed period (e.g., always be three months). According to another embodiment of the present invention, the specific time period may be continuously adjusted (e.g., the interval between the first rotation and second rotation is 3 months, while the interval between the second rotation and third rotation is 2 months). The management cost of using a static trigger condition is low, since so long as the clocks on the authentication nodes are accurate and stable, the rotation of the authentication information can be performed according to the static trigger condition.

[0048] In another embodiment, the rotation trigger condition is a dynamic trigger condition. For example, the rotation of the authentication information may be triggered when an authentication node is attacked by hackers. Still for example, the system administrator may trigger the rotation of the authentication information at any time according to specific conditions. In addition, if an authentication node is frequently accessed, then the rotation of the authentication information may also be triggered when the number of accesses to the authentication node reaches a certain number. Further, if an authentication node does not participate in rotation for many times since it is always busy, this authentication node may trigger the rotation of the authentication information by itself. The present invention may further include other dynamic trigger conditions. Furthermore, a dynamic condition in the present invention can be used at the same time with a static trigger condition. For example, the static trigger condition is to rotate once every three months; however, an authentication node triggers the rotation of the authentication information on some day in the second month since it is attacked by a hacker.

[0049] From a specific perspective, the rotation trigger condition includes starting the rotation of the authentication information when the node is idle. For example, the authentication node usually will not be accessed frequently at night, and it can be

selected to perform rotation of the authentication information at night. Or, for example, if an authentication node is still busy at the predetermined rotation time, then the node can be skipped to not participate in the rotation process. Still for example, the busy state of each authentication node may be queried before the due rotation time; if a node is busy, the rotation start time may be delayed until all the authentication nodes are in an idle state.

[0050] At step 205, in response to that the rotation trigger condition is satisfied, at least part of the authentication information is transmitted according to the rotation sequence; for example, a first authentication node transmits the authentication information stored thereon to a second authentication node such that the second authentication node processes the authentication request related to the authentication information.

[0051] The order of steps 201 and 203 in Fig. 2 is not fixed; step 201 may be performed either prior to or subsequent to step 203; or, steps 201 and 203 may be performed concurrently.

[0052] Fig. 3 shows a flowchart of determining the rotation sequence of authentication information according to an embodiment of the present invention. Fig. 3 is a further description of step 201 in Fig. 2. At step 301, each authentication node generates a random number. At step 303, a commander node is determined according to the generated random numbers. At step 305, the commander node determines the rotation sequence.

[0053] In the following the process of determining the rotation sequence of authentication information is described in conjunction with Figs. 8A and 8B.

[0054] Fig. 8A shows a schematic diagram of an authentication system before authentication information is rotated according to an embodiment of the present invention. The authentication system shown in Fig. 8A has 5 authentication nodes, Node 1-Node 5, respectively. In this embodiment, assume the encryption algorithm of each authentication information is the same, and thus the authentication information stored on the authentication nodes only includes account information and does not include authentication module information. In this embodiment, assume the current Node 1 stores authentication information Acc A, Node 2 stores authentication information Acc B, and Node 4 stores authentication information Acc C.

[0055] At step 301, each authentication node generates a random number ranging from 0 to 99, and the results of each authentication node generating a random number is shown as in the following Table 7:

| Node 1 | Node 2 | Node 3 | Node 4 | Node 5 |
|--------|--------|--------|--------|--------|
| 1      | 50     | 79     | 44     | 32     |

Table 7

[0056] At step 303, a commander node is determined according to the random numbers generated by each authentication node. For example, the node generating the biggest random number may be used as the commander node. In Table 7, Node 3 generates the biggest random number, and hence Node 3 becomes the commander node.

[0057] Next, at step 305, the commander node Node 3 determines the rotation sequence. Node 3 may temporarily generate an integer sequence consisting of numbers 1-5, e.g., 5->3->4->1->2->5. The integer sequence describes the rotation sequence of the next rotation process, that is, if there is authentication information on Node 5, it is transmitted to Node 3; if there is authentication information on Node 3, it is transmitted to Node 4; if there is authentication information on Node 4, it is transmitted to Node 1; if there is authentication information on Node 1, it is transmitted to Node 2; if there is authentication information on Node 2, it is transmitted to Node 5. As can be determined from the above rule, the Acc A in Fig. 8A will be transmitted to Node 2, Acc B will be transmitted to Node 5, Acc C will be transmitted to Node 1. Fig. 8B shows a schematic diagram of an authentication system after authentication information is rotated according to an embodiment of the present invention. After the rotation, the authentication information is stored by a new authentication node, and the authentication request related to the authentication information will also be processed by the new authentication node. The rotation sequence in the present invention may either refer to the sequence of transmitting, from one authentication node the authentication information thereon to another authentication node, e.g., 5->3, or refer to the rotation sequence of authentication information among a plurality of authentication nodes, e.g., 5->3->4->1->2->5.

[0058] According to another embodiment of the present invention, there is no need to set a commander node. First, each authentication node generates a random number, e.g., as in Table 7. Then the rotation sequence is determined according to the order of the sizes of the generated random numbers, e.g., 3->2->4->5->1. If there is authentication information on Node 3, it is transmitted to Node 2; if there is authentication information on Node 2, it is transmitted to Node 4; if there is authentication information on Node 4, it is transmitted to Node 5; if there is authentication information on Node 5, it is transmitted to Node 1; if there is authentication information on Node 1, it is transmitted to Node 3.

[0059] According to another embodiment of the present invention, there is no need to set a commander node. First, each authentication node generates a random number, then a modulus operation is performed on the generated random numbers, and the rotation sequence is determined according to the order of the sizes of the remainders of the modulus operation.

[0060] According to a further embodiment of the present invention, a random

sequence is generated by the authentication node initiating the rotation of the authentication information, e.g., the random sequence is formed by 5 numbers of 1-5 (e.g., 31245), and the rotation sequence is determined to be 3->1->2->4->5->3 according to the generated random sequence. Thus it can be seen that the determination of the rotation sequence in the present invention may be associated with the determination of the rotation trigger condition; for different rotation trigger conditions, there may be different rotation sequence generation manners. In the above example in this paragraph, when the rotation trigger condition is a dynamic trigger condition, the rotation sequence may be determined dynamically by a certain authentication node.

[0061] The present invention is not limited to the above described rotation sequence generation manners, and can be extended to more rotation sequence generation manners. In order to further reduce the possibility that the generated rotation sequence be obtained by hackers, the rotation sequence of the authentication information may be determined through random numbers, and the random numbers may be a random sequence generated by an authentication node, or random numbers generated by a plurality of nodes.

[0062] Fig. 9A shows a schematic diagram of an authentication system before authentication information is rotated according to another embodiment of the present invention. In the embodiment shown in Fig. 9A, the account information and the corresponding authentication module information in the authentication information are stored in the same authentication node before rotation (the account information Acc A and the authentication module information Mod A are both stored in the authentication node Node 1, the account information Acc B and the authentication module information Mod B are both stored in the authentication node Node 2, and the account information Acc C and the authentication module information Mod C are both stored in the authentication node Node 4), while after rotation, the account information and the corresponding authentication module information are stored in different authentication nodes. Fig. 9B shows a schematic diagram of an authentication system after authentication information is rotated according to another embodiment of the present invention. In the embodiment shown in Fig. 9B, the authentication node Node 1 stores the account information Acc C and the authentication module information Mod A, the authentication node Node 2 stores the account information Acc A, the authentication node Node 3 stores the authentication module information Mod B, the authentication node Node 4 stores the authentication module information Mod C, and the authentication node Node 5 stores the account information Acc B.

[0063] As mentioned in above, if different account information applies different encryption algorithms, then the different algorithms should be differentiated in the authentication information. A simple implementation is to store an authentication module tag corresponding to an account in an authentication node, so as to identify a

corresponding encryption algorithm; wherein the rotation sequence of the authentication module information may be either the same as or different from the rotation sequence of the account information. If the rotation sequence of the authentication module information is the same as the rotation sequence of the account information, the authentication module information will be bound to the corresponding account information permanently. If the rotation sequence of the authentication module information is different from that of the account information, the two may be stored on different authentication nodes, and the account information and the authentication module information may go through subsequent rotations in their respective separate manners.

[0064] According to an embodiment of the present invention, only the account information may be rotated while the authentication module information may not be rotated. According to another embodiment, only the authentication module information may be rotated while the account information may not be rotated.

[0065] Optionally, when the authentication module information is rotated, the authentication module tag Tag may be modified to further increase system security. For example, the Tags in Table 3 and Table 4 may be modified, Tag=0 being changed into Tag=3, Tag=1 being changed to Tag=4. The modified account information and authentication module information are shown as in the following Tables 8 and 9:

| ID     | PIN    | Tag   |
|--------|--------|-------|
| James  | XXXXXX | 3     |
| Thomas | XXXXXX | 4     |
| .....  | .....  | ..... |

Table 8

| Tag | Encryption algorithm            |
|-----|---------------------------------|
| 3   | The first encryption algorithm  |
| 4   | The second encryption algorithm |

Table 9

[0066] According to an embodiment of the present invention, the authentication information may further include timestamp information to indicate the period of validity of the authentication information. In one example, the timestamp information is “20110417, 3”, indicating that the authentication information was rotated to the local authentication node on April 17, 2011, and its period of validity is 3 months. That is to say, the next rotation needs to be performed after three months. In another example, the timestamp information is “20110717”, indicating that the authentication information is valid before July 17, 2011. In still another example, the timestamp information is “20110417, valid”, indicating that the authentication information was rotated to the local authentication node on April 17, 2011, and the “valid” status bit of the authentication information is “valid”. Once rotation of the authentication

information is started, the “valid” status bit will be set as “invalid”. This example is suitable for a solution using a dynamic trigger condition to trigger rotation. Of course, the present invention is not limited in respect of using other expressions to denote timestamp information. Authentication information using timestamp information may further increase system security. Once a hacker attacks an authentication node, he/she can not always use the authentication information in the node.

[0067] According to an embodiment of the present invention, only partial rotation of the authenticating nodes is performed during a rotation period. For example, the originally set rotation time is 2:00 am; however, before the rotation time, the real performance of the second authentication node is evaluated. If the second authentication node is found to be busy through the evaluation, this rotation process may skip the second authentication node and perform the rotation of authentication information among other nodes. Further, in order to avoid an authentication node from being skipped in multiple rotation processes, the real performance of the authentication node may be revised to prevent that the authentication node cannot participate in rotation forever. For example, the value of the real performance is a score ranging from 0 to 100, with a higher score indicating that the authentication node is busier, while a lower score indicating that the authentication node is idler. Then the revised performance after the real performance is revised may be as follows:

$$CP = RP - (W * T)$$

Equation 1

[0068] Therein CP denotes the performance score after the revision, RP denotes the real performance score of the authentication node, W denotes a weight, and T denotes the number of times that the authentication node did not participate in rotation. From Equation 1, it can be seen that with the increase of the number of times that an authentication node did not participate in rotation, the performance score after the revision will be reduced. If the performance score after the revision is lower than a certain threshold, the authentication node should participate in the rotation of the authentication information. Equation 1 prevents an authentication node from being always unable to participate in the rotation of the authentication information due to its being always busy.

[0069] Of course, the present invention does not exclude using other ways to avoid that some authentication node is always ignored in a rotation process, e.g., it may be specified that any authentication node is not allowed to not participate in a rotation process of the authentication information for two consecutive times.

[0070] Fig. 5 shows a flowchart of dispatching an authentication request according to an embodiment of the present invention. Fig. 5 is corresponding to Figs. 8A and 8B. In the embodiment shown in Fig. 5, assume the authentication information includes account information and does not include authentication module information, that is to say, the same encryption algorithm is applied to all the account information. At step 501, an authentication request is received. The authentication request may be from a

client, e.g., the authentication request may be from a login request sent by an employee when he/she logs in the company's intranet.

[0071] At step 503, the authentication request is dispatched to corresponding authentication nodes. There are many ways for dispatching an authentication request to corresponding authentication nodes. According to an embodiment of the present invention, multicasting can be used to broadcast the authentication request in the authentication network consisting of authentication nodes. The addresses of the authentication nodes in the authentication network form a multicast address set. Once a new authentication node joins the authentication network, the network address of the new authentication node also joins the multicast address set. The authentication node receiving an authentication request in the authentication network will check whether there is information satisfying the authentication request on the node. If there is not, no response is made. If there is, then the subsequent steps are performed. In one example, assume the user inputs an account ID and a password PIN on the client, the ID and PIN (or a variant of the PIN) are sent to an authentication node, which checks the IDs stored thereon to determine whether there is information satisfying the authentication request thereon. After that, the authentication node will authenticate the user according to the PIN input by the user.

[0072] In another example, assume the user inputs an account ID and a password PIN at the client, only the ID is sent to an authentication node, and when the authentication node checks the ID information stored thereon to determine that there is information satisfying the authentication request thereon, the authentication node will further contact the client to obtain the PIN, so as to perform subsequent process steps. In a more complex example, the authentication node not only needs to contact the client to get the PIN, but also needs to contact a special authentication node to perform subsequent processing of the authentication request, e.g, it needs to contact a server of a government department to determine whether the ID card number input by the user is correct.

[0073] Above has been described the details of dispatching an authentication request to the authentication nodes by multicasting. In the following will be described a process of using a node router to dispatch an authentication request to corresponding authentication nodes. The node router is responsible for dispatching an authentication request to corresponding authentication nodes to be processed. The node router can be undertaken by a special node, or undertaken by one of a plurality of authentication nodes. The node router can store a dispatch table thereon, which is shown as in the following Table 10:

| User ID ( ID ) | Authentication node |
|----------------|---------------------|
| James          | Node 1              |
| .....          | .....               |

Table 10

[0074] The contents in Table 10 indicate that the authentication information of the user name James is stored on the first node. Therefore, the node router may transmit an authentication request related to James to the first node. If the authentication information on the authentication node is rotated, then after the rotation, the dispatch table will be updated to reflect the latest authentication information storage status. For example, if the authentication information on Node 1 is rotated to Node 2, then the dispatch table may be modified as shown in the following Table 11:

| User ID ( ID ) | Authentication node |
|----------------|---------------------|
| James          | Node 2              |
| .....          | .....               |

Table 11

[0075] Now returning to Fig. 5, the authentication request is processed at step 505. The detailed contents of step 505 will be further described in detail below. At step 507, the authentication result is returned to indicate whether the authentication request passes or fails the authentication.

[0076] Fig. 6 shows a flowchart of dispatching an authentication request according to another embodiment of the present invention. The embodiment of Fig. 6 corresponds to that of Figs. 9A and 9B. In the embodiment shown in Fig. 6, assume the authentication information includes account information and authentication module information, that is to say, different encryption algorithms are applied to different account information. At step 601, receive an authentication request. At step 603, obtain account information corresponding to the authentication request according to the authentication request. At step 605, check the authentication module tag in the authentication request and determine the authentication node where the authentication module information (e.g., the encryption algorithm) corresponding to the authentication module tag resides. At step 607, dispatch the account information and the authentication request to the authentication node including the authentication module information, so that the authentication node including the authentication module information processes the authentication request. At step 609, process the authentication request. The details of step 609 will be described in detail below. At step 611, return the authentication result to determine whether the authentication request is successful.

[0077] Fig. 7 shows a flowchart of processing an authentication request according to an embodiment of the present invention. The flowchart in Fig. 7 is a further description of step 505 in Fig. 5 and step 609 in Fig. 6. No matter in the embodiments shown in Figs. 8A and 8B or in the embodiments shown in Figs. 9A and 9B, processing of the authentication request may be either paused or not paused during transmitting the authentication information. If the processing of the authentication request is paused, the authentication request will be forwarded to a new authentication node to be processed after the rotation ends, that is to say, the authentication information can be transmitted from the original authentication node to the new

authentication node by means of cut, and the original authentication node will no longer save the copy of the original authentication information. If the processing of the authentication request is not paused, the authentication request can still be processed by the original authentication node during transmitting the authentication information, and after all the authentication information has been copied from the original authentication node to the new authentication node, the new authentication node processes the authentication request. In this embodiment, the authentication information can be transmitted from the original authentication node to the new authentication node by means of copy and paste.

[0078] Specifically, it is determined whether the authentication node is in the time period of transmitting authentication information at step 701. If the authentication node is right in the time period of transmitting the authentication information, then at step 703 it is further determined whether the processing of the authentication request needs to be paused. If the processing of the authentication request needs to be paused, then at step 705, the authentication request is dispatched to another authentication node after the time period of transmitting the authentication information ends, and the other authentication node processes the authentication request. The action of dispatching to the other authentication node may be accomplished in the above-described multicast manner, or assisted by the above-described node router, or the authentication node may directly forward the authentication request to be solved to another authentication node. If at step 703 it is determined that the process to the authentication node needs not to be paused, then at step 707, the authentication node accomplishes the processing of the authentication request. If at step 701, it is determined that the authentication node is not in the time period of transmitting the authentication information, then the flow directly proceeds to step 707, at which the authentication node processes the authentication request.

[0079] Fig. 10 shows a flowchart of an authentication information processing system of the present invention. The authentication information processing system in Fig. 10 comprise rotation sequence determining means, rotation trigger condition determining means and transmitting means. In the authentication information processing system in Fig. 10, the authentication information is stored in a first authentication node. The rotation sequence determining means in Fig. 10 is configured to determine a rotation sequence of the authentication information. The rotation trigger condition determining means is configured to determine a rotation trigger condition of the authentication information. The transmitting means is configured to transmit at least part of the authentication information to a second authentication node so that the second authentication node, in response to satisfaction of the rotation trigger condition, processes the authentication request related to the authentication information according to the rotation sequence.

[0080] According to an embodiment of the present invention, the authentication information in Fig. 10 includes account information.

[0081] According to another embodiment of the present invention, the authentication information in Fig. 10 further includes authentication module information besides the account information.

[0082] According to an embodiment of the present invention, the rotation sequence in Fig. 10 includes a rotation sequence of the account information and a rotation sequence of the authentication module information. And the transmitting means is further configured to: transmit the account information to a second authentication node and transmit the authentication module information to a third authentication node.

[0083] According to an embodiment of the present invention, the rotation trigger condition comprises starting rotation of the authentication information after a certain time period interval.

[0084] According to another embodiment of the present invention, the rotation trigger condition is a dynamic trigger condition.

[0085] According to still another embodiment of the present invention, the rotation trigger condition comprises starting rotation of the authentication information when the node is idle.

[0086] According to another embodiment, the authentication information includes timestamp to indicate the period of validity of the authentication information.

[0087] The functions of the modules in the authentication information processing system shown in Fig. 10 have been described in detail in the above description of the authentication information processing method, and are not repeated here.

[0088] Various embodiments of the present invention can provide many advantages, including what are stated in the summary of the invention and what may be deduced from the technical solution per se. However, whether an embodiment achieves all the advantages, and whether such advantages are thought to constitute a substantive improvement, are not limitation to the present invention. In the meantime, the various implementations mentioned above are only for illustrative purpose, and those of ordinary skill in the art can make various modifications and changes to the above implementations without departing from the substance of the present invention. The scope of the present invention is totally defined by the appended claims.

## CLAIMS

1. A method for processing authentication information, the authentication information being stored on a first authentication node, the method comprising:  
determining a rotation sequence of the authentication information,  
determining a rotation trigger condition for the authentication information, and  
in response to satisfaction of the rotation trigger condition, transmitting at least part of the authentication information to a second authentication node according to the rotation sequence.
2. The method of claim 1, wherein the authentication information includes account information and authentication module information.
3. The method of claim 2, wherein the rotation sequence information includes a rotation sequence of the account information and a rotation sequence of the authentication module information, and  
transmitting at least part of the authentication information to a second authentication node according to the rotation sequence comprises:  
transmitting the account information to the second authentication node according to the rotation sequence of the account information;  
and the method further comprises:  
transmitting the authentication module information to a third authentication node according to the rotation sequence of the authentication module information.
4. The method of claim 1, wherein the rotation trigger condition comprises reaching a predetermined time.
5. The method of claim 1, wherein the rotation trigger condition is a dynamic trigger condition.
6. The method of any one of claims 1-5, wherein the rotation trigger condition comprises starting rotation of the authentication information when the first authentication node is idle.
7. The method of claim 1, wherein determining the rotation sequence of the authentication information further comprises determining the rotation sequence of the authentication information randomly.
8. The method of claim 1, wherein the first authentication node pauses the processing of an authentication request related to the authentication information during transmission of the authentication information.
9. The method of claim 1, wherein the first authentication node does not pause the processing of an authentication request related to the authentication information

during transmission of the authentication information.

10. The method of claim 1, wherein the authentication information includes timestamp information to indicate the period of validity of the authentication information.

11. The method of claim 1, wherein the authentication request is dispatched to a plurality of authentication nodes by multicasting.

12. The method of claim 1, wherein the authentication request is dispatched to a second authentication node through a node router, wherein the node router stores a dispatch table for the authentication information.

13. A system for processing authentication information, wherein the authentication information is stored on a first authentication node, the system comprising:

a rotation sequence determining means configured to determine a rotation sequence of the authentication information,

a rotation trigger condition determining means configured to determine a rotation trigger condition of the authentication information, and

a transmitting means configured to, in response to satisfaction of the rotation trigger condition, transmit at least part of the authentication information to a second authentication node according to the rotation sequence.

14. The system of claim 13, wherein the authentication information includes account information and authentication module information.

15. The system of claim 14, wherein the rotation sequence includes a rotation sequence of the account information and a rotation sequence of the authentication module information, and

the transmitting device is further configured to transmit the account information to the second authentication node according to the rotation sequence of the account information and transmit the authentication module information to a third authentication node according to the rotation sequence of the authentication module information.

16. The system of claim 13, wherein the rotation trigger condition comprises reaching a predetermined time.

17. The system of claim 13, wherein the rotation trigger condition is a dynamic trigger condition.

18. The system of any one of claims 13 to 17, wherein the rotation trigger condition comprises starting rotation of the authentication information when the first authentication node is idle.

19. The system of claim 13, wherein the authentication information includes timestamp information to indicate the period of validity of the authentication information.

20. A computer program comprising program code adapted to perform the method steps of any of claims 1 to 12 when said program is run on a computer.