A SYSTEM AND METHOD FOR AUTHENTICATING IDENTITIES OVER REMOTE CHANNELS

Field of the Invention

[001] The present invention generally relates to the field of authenticating identities of individuals or organizations. In particular, the invention relates to an apparatus and method for authenticating identities of individuals and organizations over remote channels.

Background of the Invention

[002] Secure communication between 2 parties often starts with each party first establishing and confirming the identity of the opposing party before the exchange of confidential and secure information. Presently, this process is commonly known as Authentication.

[003] With the increased use of remote channels of communications such as the internet and dial-up applications to access or transact confidential information in remote databases and servers, the need for secure and reliable authentication has become an essential element in any organization providing or utilizing such access or transaction.

[004] Single log-in passwords that are still in use today have proven to be far short of the requirements of many organizations desiring higher levels of security and confidentiality. This is especially so when the accessing and transacting of monies is concerned. Such organizations are invariably banks, trading houses and financial institutions. The single log-in passwords were susceptible to hacking by system vulnerability exploits or even simple plain repeated guessing. Tokens were

introduced and in combination with the single-log-in passwords increased security somewhat. Tokens in the form of magnetic cards are still in use by banks all over the world for the withdrawal of cash from ATMs (Automated Teller Machines). This has however been deemed not to be sufficiently secure .

[005] Cryptography was then introduced to encrypt data being accessed and transacted. This prevented the data from being understood even if unintended recipients of the data had somehow hacked through the initial single log-in passwords. However, to decrypt the encrypted data still required a code which many would view simply to be another password for accessing the data. This code similarly faced the problems of being mathematically hacked or repeatedly guessed.

[006] American scientist Gilbert S. Vernam in 1917 developed a cryptographic system "Vernam Cipher" that till today is considered virtually unbreakable. The system required both sending party and receiving party to have the same copy of a code comprising a truly random and unpredictable sequence of random numbers that is used to encrypt and decrypt the data being sent. The code is used by applying an XOR (Exclusive OR) function to encrypt or decrypt the data. Once used, the code is discarded never to be used again. Hence its popularized name the "One-time pad".

[007] The concept of "One-time Pads" have since been actively used in modern day authentication systems. One of the most advanced systems today combine the use of a single log-in password, a smart token and a "One-time Pad" like password. A user would initially access an organization's system by using a single log-in password. The system would then further authenticate the user by sending to the user a randomly generated first password. The user inputs this first password into the smart token which then generates a second password using another mathematical function programmed into the smart token. This second password is

then sent to the system for authentication of the user. The system having generated the first password would also have generated the second password and by comparing the second password from the user and the second password generated by the system, the system can confirm the authentication. The mathematical functions used may further involve the use of several variables including the time of activating the function adding difficulty to the passwords being predicted or mathematically hacked. Such use of smart tokens have also been considered to amount to the usage of "One-time pads" due to the random generation of the first password.

[008] However, these systems may still be hacked as there is disadvantageously a mathematical function involved. By collecting sufficient samples of both the first and second password, the mathematical algorithm used to generate the second password may be still be derived. Furthermore, a disadvantage in using a smart token is the high costs of implementing such systems having such smart tokens. Smart tokens when issued en masse are very expensive and the costs of replacing lost smart tokens are also very high. In addition, lost of a smart token cripples access to the system until another smart token is issued.

[009] Other similar implementations of "One-time pads" have also encountered difficulties when users become out of sync with the system's "One-time pad". It becomes next to impossible for the user to be able to authenticate himself with the system since his passwords from his "One-time pad" do not match the system's "One-time pad".

[0010] It can thus be seen that present authentication systems in use today do still have several disadvantages in terms of security and high costs. Thus, there remains a need for a fully secure system for authentication at reduced costs.

Summary of the Invention

[0011] The present invention seeks to provide a system and method for authenticating identities over remote channels.

[0012] Accordingly, in one aspect, the present invention provides, a method for authenticating the identity of a user having a token and a token reader to an authenticating server having a true random number generator and a storing means, wherein said token reader coupled to a displaying means, said method comprising the steps: generating a sequence of true random numbers by said true random number generator of said authentication server; formatting said sequence of true random numbers to obtain a sequence of formatted true random numbers; storing said sequence of formatted true random numbers on said token; subjecting said sequence of true random numbers to a predetermined one-way function to derive a sequence of server passwords; storing said sequence of server passwords in said storing means of said authentication server; requesting authentication data from a user having said token and said token reader; performing user authenticating process; receiving a first true random number from said user; subjecting said first true random number to said predetermined one-way function to derive a user password; comparing said user password to any of said sequence of said server passwords stored on said storing means of said authenticating server for a match; authenticating of user is negative if said user password does not match any of said sequence of said server passwords; deleting said matching server password and all preceding server passwords if matching server password is not first in said sequence of server passwords; and authenticating of user is positive if said user password matches any of said sequence of server passwords.

[0013] In another aspect, the present invention provides, a system for authenticating identity of a user, comprising: an authentication server having a true

random number generator and a storing means, said authentication server for generating a sequence of true random numbers; said sequence of true random numbers for deriving a sequence of server passwords by subjecting said sequence of true random numbers to a predetermined one-way function, for authenticating identity of said user; a token for storing said sequence of true random numbers for accessing by said user; a token reader coupled to a displaying means for accessing said token; wherein, said token reader upon activation with said token accesses said token for a first of said sequence of true random numbers and deleting said first of said sequence of true random numbers from said token before displaying said first of said sequence of true random numbers on said displaying means; further wherein, said authentication server upon positive authentication of said user by comparing said first of said sequence of true random numbers from said token and any of said sequence of server passwords from said storing means for a matching server password and deleting said matching server password and all preceding server passwords from said sequence of server passwords from said storing means of said authentication server.

[0014] In a further aspect, the present invention provides, a method for authenticating the identity of a user having a token to an authenticating server having a true random number generator and a storing means, said method comprising the steps: generating a sequence of true random numbers by said true random number generator of said authentication server; formatting said sequence of true random numbers to obtain a sequence of formatted true random numbers; storing said sequence of formatted true random numbers on said token; subjecting said sequence of true random numbers to a predetermined one-way function to derive a sequence of server passwords; storing said sequence of server passwords in said storing means of said authentication server; requesting authentication data from a user having said token; performing user authenticating process; receiving a first true random number from said user; subjecting said first true random number to said

predetermined one-way function to derive a user password; comparing said user password to any of said sequence of said server passwords stored on said storing means of said authenticating server for a match; authenticating of user is negative if said user password does not match any of said sequence of said server passwords; deleting said matching server password and all preceding server passwords if matching server password is not first in said sequence of server passwords; and authenticating of user is positive if said user password matches any of said sequence of server passwords.

Brief Description of the Drawings

[0015] A preferred embodiment of the present invention will now be more fully described, with reference to the drawings of which:

[0016] FIG.1 illustrates a block diagram of a system for authenticating identities of users over remote channels in accordance with the present invention;

[0017] FIG.2 illustrates a flowchart of a method of authenticating identities of users over remote channels in accordance with the present invention;

[0018] FIG.3 illustrates a flowchart of the pre-generation process of FIG.2;

[0019] FIG.4 illustrates a flowchart of the server authenticating process of FIG.2; and

[0020] FIG.5 illustrates a flowchart of the user authenticating process of FIG. 4.

Detailed description of the Drawings

[0021] A system and method for authenticating identities over a remote channel with a preferred embodiment and an alternate embodiment are described. In the following description, details are provided to describe the preferred and the alternate embodiment. It shall be apparent to one skilled in the art, however that the invention may be practiced without such details. Some of the details may not be described at length so as not to obscure the invention.

[0022] Referring to Fig. 1, a system 10 in accordance with the present invention is shown which comprises of an Authentication server 12 and a plurality of users 20, 20a, 20b. The system 10 in accordance with the present invention allows a user 20 or the plurality of users 20, 20a, 20b to communicate with the Authentication server 12 over a remote channel 30 for authentication purposes. The remote channel 30 may be by way of internet access, intranet access, via modem remote access, via wireless access, via ATM or via voice communication over the phone.

[0023] The Authentication server 12 further comprises a true random number generator (TRNG) 14 and a storing means such as a hard disk 16 for storing data and information. The user 20 in accordance to the present invention may be an individual or a party of individuals or an organization in possession of a token 22 and a token reader 24. The token reader 24 is further coupled to a displaying means for displaying data accessed from the token 22. The token 22 in the preferred embodiment of the present invention is a smartcard with a non-volatile memory and the token reader 24 would be a smartcard reader. The displaying means coupled to the token reader 24 could be a display device such as an LCD mounted on or coupled to the token reader 24. The displaying means can also be the monitor of a computer, where the monitor is coupled to the token reader via the computer.

[0024] A sequence of true random numbers 17 are pre-generated by the TRNG 14 of the Authentication server 12 and are pre-stored in the token 22 before being issued to the user 20. The same sequence of true random numbers 17 is then subjected to a predetermined one way function 18 in the Authentication server 12 to derive a sequence of server passwords 19. The sequence of server passwords 19 are then stored in the hard disk 16 of the Authentication server 12. In the alternate embodiment, the token 22 is any storage media from simply a sheet of paper with the sequence of true random numbers 17 written or printed on it, to the memory of a PDA or the hard disk of a PC. The token reader 24 would then be the PDA and the PC. However, in the case of the token 22 being a sheet of paper with the sequence of true random numbers 17 on it, a token reader 24 would not be necessary as the user would simply read the data off the sheet.

[0025] Examples of conventional one-way functions which are commonly used in the industry are the Hash function and the Salt/Hash function. The sequence of true random numbers 17 can be subjected to a Hash function such as the MD5 and SHA1 to derive the server passwords 19. In a Salt/Hash function, an additional 2 character string is appended to each of the sequence of true random numbers 17 before performing the Hash function. The 2 character string is unique to each user and generally not kept a secret. These one way functions are deemed adequate but not fully secure and can still be overcomed.

[0026] In the preferred embodiment of the present invention, the predetermined one-way function 18 comprises diversification of a root symmetric encryption key to obtain a diversified symmetric encryption key and an encryption using this diversified symmetric encryption key. A root symmetric encryption (e.g. 3DES) key is securely stored in a tamper-proof Hardware Security Module in the authentication server 12. A diversified symmetric encryption (e.g. 3DES) key is obtained by performing a symmetric encryption using the root symmetric

encryption key on a result of a Hash function performed on a character string unique to each user. This is known as the diversification of root symmetric encryption key. Following which, a symmetric encryption using this diversified symmetric encryption key is performed on the sequence of true random numbers 17 to derive the sequence of server passwords 19.

[0027] Referring to Fig.2, a method 200 for authenticating identities over a remote channel in accordance with the present invention comprises a pre-generation 300 process and a server authenticating 400 process.

[0028] Before the system 10 is able to begin authenticating identities, there is a process of pre-generation 300 that ensures that data on the Authentication server 12 and the token 22 are pre-stored properly.

[0029] Referring to Fig.2, the process for pre-generation 300 starts with the generating 310 of a sequence of true random numbers 17. The total number of true random numbers in the sequence is predetermined and a preferred number is 1000. Each of the true random numbers comprise a predetermined number of decimal digits and a preferred true random number comprises 6 decimal digits and can be any number between 000001 to 999999. Organizations can use this on a per-login basis, and/or prompt the users to re-authenticate after a period of in-activity or to authorize more sensitive transactions.

[0030] Next, the step of formatting 315 the sequence of true random numbers 17 is carried out to ensure proper storage on the token 22. The step of formatting 315 comprises converting the sequence of true random numbers 17 from binary format to decimal format to obtain a sequence of formatted true random numbers and digitally signing the formatted true random numbers before storing into the token.

[0031] The TRNG 14 of the authentication server 12 generates the true random numbers in a byte stream. To avoid the token performing any additional conversion activities, the sequence of true random numbers 17 are first formatted by the authentication server 12 to convert the sequence of true random numbers 17 from byte stream which is binary (base-2) based to decimal (base-10) based. Further, in order to ensure that only a valid authentication server 12 can store the formatted true random numbers into the token 22, the authentication server 12 is required to digitally sign the formatted true random numbers before storing into the token 22 and the token 22 is required to verify the digital signatures before accepting the sequence of formatted true random numbers 17. It would also be possible to format the true random numbers into other numbering formats such as hexadecimal based numbering.

[0032] Upon completion of the step of formatting 315, the sequence of formatted true random numbers 17 is then stored 330 in the token. Following the formatting 315 step, the step of subjecting 320 the sequence of true random numbers 17 to a predetermined one-way function 18 to derive the sequence of server passwords 19. The sequence of server passwords 19 are then stored 325 in the hard disk 16 or storing means of the Authentication server 12.

[0033] With the completion of the pre-generation step 300, the system 10 can then be used to authenticate the user 20 who is issued with the token 22. The Authentication server 12 in the preferred embodiment is likely to be the gateway to a main system or database. Upon the user 20 attempting to access the main system or database, the Authentication server 12 then begins a server authenticating process 400 and the user responds by initiating a user authenticating process 500.

[0034] The server authentication process 400 serves to receive the authentication data from the user 20. Referring to Fig.4, The server authentication process 400

starts with the authentication server 12 requesting 410 authentication data from the user 20. The authentication data required is the first of the sequence of formatted true random numbers on the token 22. This is followed by the user authenticating 500 process where a first true random number from the token 22 is sent to the authentication server. Upon receiving 415 the first true random number, the next step comprises subjecting 420 the first true random number to the predetermined one way function 18 to derive a user password. The Authentication server 12 then compares 425 the user password to the sequence of server passwords 19 on the hard disk 16. If the user password does not match 430 any one of the sequence of server passwords 19, the authenticating of the user 20 is negative 435 and the server authentication process 400 ends. If the user password does match 430 one of the sequence of the server passwords 19, it is further required to determine whether the matching 440 server password is first in the sequence of the server passwords. If the matching server password is the first in the sequence of the server passwords, the matching server password is deleted 445 from the hard disk 16 of the authentication server 12. If the matching server password is not the first in the sequence of the server passwords 19, all server passwords preceding and including the matching server password are deleted 455 from the hard disk 16 of the authentication server 12. Either deleting steps 445 and 455 result in authenticating the user as positive 450. Upon positive authentification of the user 20, the user 20 will be allowed access into the main system or database.

[0035] Referring to Fig.5, the user authentication process 500 starts with the user 20 receiving 510 an authentication request from the Authentication server 12. Next, the step of activating 515 the token reader 24 is carried out to access the token 22 for a first true random number from the sequence of formatted true random numbers 17 stored in the token 22. The requested first true random number is then deleted 520 from the token 22 before the step of presenting 525 the requested first true random number from the token 22 onto the displaying means coupled to the token

reader 24. The sending 530 step sends the first true random number to the Authentication server 12 for authentication purposes.

[0036] The user authenticating process 500 sends or transmits authenticating data which in the preferred embodiment is the first of the sequence of formatted true random numbers on the token 22 issued to the user 20. With the first of the sequence of formatted true random numbers being deleted from the token 22, the subsequent true random number of the remaining sequence of formatted true random numbers on the token 22 is now the first true random number. With every activation 515 of the token reader 24, the first of the remaining sequence of true random numbers is deleted from the token 22.

[0037] The present invention advantageously provides a method of authenticating identities over remote channels without the authenticating server 12 constantly tracking the first true random number on the user's token for authenticating the user 20. The user 20 may misplace or misuse any number of the true random numbers on the token 22 yet still be authenticated by the authentication server 12.

[0038] Further, the user 20 may advantageously consider not carrying the token 22 when traveling and merely activate 515 the token 22 a predetermined number of times to receive a sequence of first true random numbers. This sequence of first true random numbers can then be stored by merely writing onto paper or recorded into a PDA or even the user's computer laptop. When authentication is required, the sequence of first true random numbers are then used sequentially for authentication.

[0039] The present invention further advantageously obviates the problem of having smart tokens for complex computations or functions and thus reduces the problem of high costs of implementing a token based authentication system.

[0040] The present invention also advantageously allows for reduced token management. This is because much of the activities relating to the management of the tokens 22 can be delegated to the user without compromising security. If the user loses the token (by theft/carelessness), conventional systems require the user 20 to contact the organization to disable the token 22 and to arrange for re-issuance of a new token 22. In the present invention, the user 20 may still advantageously authenticate himself to the authentication server 12 if he has an unused first true random number from the token 22. As a temporary measure, the user 20 may further obtain another sequence of first true random numbers from an alternate destination provided for by the authentication server 12 such as an ATM and by using this sequence of first true random numbers, automatically disabling the lost token. If the user 20 finds the token 22 subsequently, he can go to the ATM to reset the token 22 and continue using it.

[0041] The present invention allows organizations to have an increased number of options in terms of tokens for issuing to users. Organizations may issue different tokens to different users depending on the user's requirements and usage. High-value users may be issued with tokens such as smartcards, while low-value users can use paper-based tokens as in the alternate embodiment. Users also have the option of storing the authentication data in their tokens in the media of their choice, e.g. handphone, PDA, PC, etc.

[0042] It will be appreciated that various modifications and improvements can be made by a person skilled in the art without departing from the scope of the present invention.

Claims

1. A method for authenticating the identity of a user having a token and a token reader to an authenticating server having a true random number generator and a storing means, wherein said token reader coupled to a displaying means, said method comprising the steps:

i) generating a sequence of true random numbers by said true random number generator of said authentication server;

ii) formatting said sequence of true random numbers to obtain a sequence of formatted true random numbers;

iii) storing said sequence of formatted true random numbers on said token;

iv) subjecting said sequence of true random numbers to a predetermined one-way function to derive a sequence of server passwords;

v) storing said sequence of server passwords in said storing means of said authentication server;

vi) requesting authentication data from a user having said token and said token reader;

vii) performing user authenticating process;

viii) receiving a first true random number from said user;

ix) subjecting said first true random number to said predetermined one-way function to derive a user password;

x) comparing said user password to any of said sequence of said server passwords stored on said storing means of said authenticating server for a match;

xi) authenticating of user is negative if said user password does not match any of said sequence of said server passwords;

xii) deleting said matching server password and all preceding server passwords if matching server password is not first in said sequence of server passwords; and

xiii) authenticating of user is positive if said user password matches any of said sequence of server passwords.

2. The method in accordance with claim 1, wherein step ii) further comprises the steps:

a. converting said sequence of true random numbers from binary base to decimal base to obtain a sequence of formatted true random numbers;

b. digitally signing said sequence of formatted true random numbers; and

c. verifying said sequence of formatted true random numbers by said token before storing into said token.

3. The method in accordance with claim 1, wherein said step (vii) further comprises the steps:

a. receiving authentication data request from said authentication server;

b. activating said token reader to access said token for a first true random number from said sequence of true random numbers from said token;

c. deleting said first true random number from said sequence of said true random numbers from said token;

d. presenting said first true random number on said displaying means; and

e. sending said first true random number to said authentication server.

4. The method in accordance with claim 1, wherein said predetermined one-way function comprises the steps: diversification of a root symmetric encryption key to obtain a diversified symmetric encryption key and an encryption using said diversified symmetric encryption key.

5. The method in accordance with claim 4, wherein said diversification step further comprises performing a symmetric encryption using said root symmetric encryption key on a result of a Hash function performed on a character string unique to said user.

6. The method in accordance with claim 5, wherein said root symmetric encryption key is securely stored in a tamper-proof hardware security module.

7. The method in accordance with claim 1, wherein said predetermined one-way function comprises a Hash function based on MD5.

8. The method in accordance with claim 1, wherein said predetermined one-way function comprises a Hash function based on SHA1.

9. The method in accordance with claim 1, wherein said token is a smartcard having a non-volatile memory.

10. The method in accordance with claim 1, wherein said token reader is a smartcard reader.

11. A system for authenticating identity of a user, comprising:

an authentication server having a true random number generator and a storing means, said authentication server for generating a sequence of true random numbers; said sequence of true random numbers for deriving a sequence of server passwords by subjecting said sequence of true random numbers to a predetermined one-way function, for authenticating identity of said user;

a token for storing said sequence of true random numbers for accessing by said user;

a token reader coupled to a displaying means for accessing said token;

wherein, said token reader upon activation with said token accesses said token for a first of said sequence of true random numbers and deleting said first of said sequence of true random numbers from said token before displaying said first of said sequence of true random numbers on said displaying means;

further wherein, said authentication server upon positive authentication of said user by comparing said first of said sequence of true random numbers from said token

and any of said sequence of server passwords from said storing means for a matching server password and deleting said matching server password and all preceding server passwords from said sequence of server passwords from said storing means of said authentication server.

12. The system in accordance to claim 11, wherein said predetermined one-way function comprises: diversification of a root symmetric encryption key to obtain a diversified symmetric encryption key and an encryption using said diversified symmetric encryption key.

13. The system in accordance to claim 12, wherein said root symmetric encryption key is securely stored in a tamper-proof hardware security module.

14. The system in accordance to claim 11, wherein said predetermined one-way function comprises a Hash function based on MD5.

15. The system in accordance to claim 11, wherein said predetermined one-way function comprises a Hash function based on SHA1.

16. The system in accordance to claim 11, wherein said token is a smartcard having a non-volatile memory.

17. The system in accordance to claim 11, wherein said token reader is a smartcard reader.

18. The system in accordance to claim 11, wherein said displaying means is an LCD display.

19. The system in accordance to claim 11, wherein said displaying means is a monitor of a PC.

20. A method for authenticating the identity of a user having a token to an authenticating server having a true random number generator and a storing means, said method comprising:

i) generating a sequence of true random numbers by said true random number generator of said authentication server;

ii) formatting said sequence of true random numbers to obtain a sequence of formatted true random numbers;

iii) storing said sequence of formatted true random numbers on said token;

iv) subjecting said sequence of true random numbers to a predetermined one-way function to derive a sequence of server passwords;

v) storing said sequence of server passwords in said storing means of said authentication server;

vi) requesting authentication data from a user having said token;

vii) performing user authenticating process;

viii) receiving a first true random number from said user;

ix) subjecting said first true random number to said predetermined one-way function to derive a user password;

x) comparing said user password to any of said sequence of said server passwords stored on said storing means of said authenticating server for a match;

xi) authenticating of user is negative if said user password does not match any of said sequence of said server passwords;

xii) deleting said matching server password and all preceding server passwords if matching server password is not first in said sequence of server passwords; and

xiii) authenticating of user is positive if said user password matches any of said sequence of server passwords.

21. The method in accordance with claim 20, wherein step ii) further comprises the steps:

a. converting said sequence of true random numbers from binary base to decimal base to obtain a sequence of formatted true random numbers;

b. digitally signing said sequence of formatted true random numbers; and

c. verifying said sequence of formatted true random numbers by said token before storing into said token.

22. The method in accordance with claim 20, wherein said step (vii) further comprises the steps:

a. receiving authentication data request from said authentication server;

b. accessing said token for a first true random number from said sequence of true random numbers from said token;

c. deleting said first true random number from said sequence of said true random numbers from said token; and

d. sending said first true random number to said authentication server.

23. The method in accordance with claim 20, wherein said predetermined one-way function comprises the steps: diversification of a root symmetric encryption key to obtain a diversified symmetric encryption key and an encryption using said diversified symmetric encryption key.

24. The method in accordance with claim 23, wherein said diversification step further comprises performing a symmetric encryption using said root symmetric encryption key on a result of a Hash function performed on a character string unique to said user.

25. The method in accordance with claim 24, wherein said root symmetric encryption key is securely stored in a tamper-proof hardware security module.

26. The method in accordance with claim 20, wherein said predetermined one-way function comprises a Hash function based on MD5.

27. The method in accordance with claim 20, wherein said predetermined one-way function comprises a Hash function based on SHA1.