CLAIMS

What is claimed is:

1. A method for validating a user's authenticity to access a secure system, the method comprising:

receiving an authentication request from the user;

generating a security matrix based on a user ID and user preference data and sending said matrix to the user;

receiving a one-time code from the user in response to the security matrix;

validating the one-time code based on the security matrix, the user ID, at least one user keyword, and user preference data;

after validating the one-time code, sending an authentication result to the user, said authentication result being based on the one-time code, the security matrix, the user ID, the user keyword, and user preferences; and

sending a success or fail message, distinct from the authentication result, to the secure system based on the authentication result.

2. The method of claim 1, wherein the user keyword is stored in encrypted form.

3. The method of claim 1, generating a security matrix based on a user ID and user preference data includes generating a randomly arranged security matrix as specified by the user preference data.

4. The method of claim 1, generating a security matrix based on a user ID and user preference data includes generating an alphabetically arranged security matrix as specified by the user preference data.

5. The method of claim 1,

wherein the authentication request includes a system ID; and

wherein the matrix generation is based on the user preference data, the user ID, and the system ID.

6. The method of claim 1, wherein the step of generating a security matrix based on the user ID and user preference data includes constructing a custom representation of the security matrix.

7. The method of claim 1,

wherein the system has system preference data; and

wherein the step of generating a security matrix is based on the user ID, user preference data, and system preference data.

8. The method of claim 1, wherein the step of generating a security matrix includes generating a matrix that is different from any previously generated matrix.

9. The method of claim 1, wherein the authentication result includes a session ID to be used by the secure system.

10. The method of claim 1, wherein the step of receiving the one-time code includes receiving the user ID, and system ID.

11. The method of claim 1,

wherein the user keyword consists of a plurality of characters; and

wherein the security matrix maps each character of the keyword to a corresponding number.

12. The method of claim 11, wherein the user-preference data includes an indication to form the one-time code by modifying with an offset each number to which a character of the user keyword is mapped.

13. The method of claim 11, wherein the user-preference data includes an indication to form the one-time code by modifying with a crawl each number to which a character of the user keyword is mapped.

14. The method of claim 11, wherein the user-preference data includes an indication to form the one-time code by modifying with a jump each number to which a character of the user keyword is mapped.

15. The method of claim 11, wherein the user-preference data includes an indication to form the one-time code by modifying with a mask each number to which a character of the user keyword is mapped.

16. The method of claim 11, wherein the user-preference data includes an indication to form the one-time code by modifying with a user-chosen letter each number to which a character of the user keyword is mapped.

17. The method of claim 11, wherein the user-preference data includes an indication to form the one-time code by modifying with a user-chosen word having a size equal to the keyword each number to which a character of the user keyword is mapped.

18. The method of claim 1,

wherein the step of receiving a one-time code from the user in response to the security matrix includes generating the one-time code based on an alternative keyword;

wherein validating the one-time code includes validating the one-time code based on the alternative keyword; and

wherein sending the success or fail message includes a panic indication to the secure system such that the secure system protects the user.

19. A security system for validating a user's authenticity to access a secure system, the security system comprising:

a security computer that is programmed

to store a user keyword and user preference data,

to receive an authentication request including a user ID from the user to access the secure system and to generate a security matrix in response to said authentication request based on stored user preference data and the user ID;

to send the security matrix to the user and to receive from the user a one-time code,

to validate the one-time code using the generated security matrix, the user keyword, and user preference data, and to send an authentication result based on the validation to the user, and

to send a success or fail message, distinct from the authentication result, to the secure system based on the authentication result; and

a client interface that enables the user to transmit to the security system an authentication request to access the secure system, receives and displays the security matrix, and enables the user to send the one-time code to the security system.

20. The security system of claim 19, wherein the security system receives the authentication request via the secure system.

21. The security system of claim 19, wherein the security system sends the security matrix to the user via the secure system.

22. The security system of claim 19,

wherein the security system sends the security matrix to the secure system; and

wherein the secure system generates a custom representation of the security matrix and sends it to the user.

23. The security system of claim 19, wherein the security system receives the one-time code via the secure system.

24. The security system of claim 19, wherein the security system sends the authentication result via the secure system.

25. The security system of claim 19, wherein the client interface is a browser that runs on a client computer system.

~~26. The security system of claim 19, wherein the client interface is an ATM machine.~~

~~27. The security system of claim 19, wherein the client interface is a point of sale terminal.~~

~~28. The security system of claim 19, wherein the client interface is a browser of a computer system operated by a customer representative of the system for which access is requested.~~

CLAIMS:

1. A user authentication method comprising execution, by a processing system (30), of the steps of:

receiving (160) a request from a user to initiate an authentication session, the request comprising a unique identifier of the user;

accessing, using the unique identifier, a record stored in memory associated with the user, the stored record comprising at least code value complexity preference data (40) and a user-defined keyword (41) consisting of an ordered sequence of symbols comprising members of a predetermined symbol set selected from one or more symbol sets supported by the processing system, wherein the symbols of the ordered sequence have been previously selected by the user independently of other users' selections;

generating (162) a one-time security matrix which is valid only for the user during the authentication session, and which comprises a mapping between each symbol within the symbol set and a code value which is specific to the authentication session and randomly selected from a code set which is distinct from the symbol set;

transmitting (164a) the one-time security matrix for presentation to the user;

receiving an ordered sequence of code values (12) selected from the one-time security matrix and input by the user, based upon the user-defined keyword and the code value complexity preference data, in response to presentation of the one-time security matrix;

validating (174) the received ordered sequence of code values by comparison with a corresponding sequence of code values generated, but not transmitted, by the processing system based upon the user-defined keyword in the stored record, the code value complexity preference data and the one-time security matrix; and

generating (178) an authentication result of the authentication session based upon the comparison.

2. The method of claim 1 wherein the step of generating the one-time security matrix comprises arranging the symbols within the symbol set in a random order.

3. The method of claim 1 wherein the step of generating the one-time security matrix comprises arranging the symbols within the symbol set in an alphabetical order.

4. The method of claim 1 wherein:

the step of receiving the request from the user comprises receiving the request from a secure system distinct from the processing system, the secure system having a corresponding secure system identifier;

the request further comprises the secure system identifier; and

the step of generating the one-time security matrix is based upon preferences associated with the secure system identifier.

5. The method of claim 4 wherein the step of transmitting the one-time security matrix for presentation to the user comprises:

transmitting the one-time security matrix to the secure system;

the secure system constructing a custom representation of the one-time security matrix; and

the secure system presenting the custom representation of the one-time security matrix to the user.

6. The method of claim 4 wherein the step of generating the one-time security matrix includes randomly selecting code values from a code set determined in accordance with preferences associated with the secure system identifier.

7. The method of claim 1 wherein the predetermined symbol set comprises alphabetical characters, and wherein the code set is a set of numerical values.

8. The method of claim 7 wherein the stored record associated with the user comprises user preferences including an offset value, and wherein the step of validating the received ordered sequence of code values comprises generating a corresponding sequence of code values based upon the user-defined keyword in the stored record, the one-time security matrix mapping of symbols to the numerical values of the code set, and calculation of modified code values based upon the offset value.

9. The method of claim 7 wherein the stored record associated with the user comprises user preferences including a crawl value, and wherein the step of validating the received ordered sequence of code values comprises generating a corresponding sequence of code values based upon the user-defined keyword in the stored record, the one-time security matrix mapping of symbols to the numerical values of the code set, and calculation of modified code values based upon the crawl value.

10. The method of claim 7 wherein the stored record associated with the user comprises user preferences including a jump value, and wherein the step of validating the received ordered sequence of code values comprises generating a corresponding sequence of code values based upon the user-defined keyword in the stored record, the one-time security matrix mapping of symbols to the numerical values of the code set, and calculation of modified code values based upon the jump value.

11. The method of claim 7 wherein the stored record associated with the user comprises user preferences including a mask value, and wherein the step of validating the received ordered sequence of code values comprises generating a corresponding sequence of code values based upon the user-defined keyword in the stored record, the one-time security matrix mapping of symbols to the numerical values of the code set, and calculation of modified code values based upon the mask value.

12. The method of claim 7 wherein the stored record associated with a user comprises an alternative user-defined keyword consisting of an ordered sequence of symbols selected from the predetermined symbol set, and wherein:

the step of validating the received ordered sequence of code values further comprises performing a comparison with a corresponding sequence of code values generated, but not transmitted, by the processing system based upon the alternative user-defined keyword in the stored record, the code value complexity preference data and the one-time security matrix; and

in the event that the comparison results in a match, generating the authentication result of the authentication session comprising a panic indication.

13. A user authentication apparatus (30) comprising:

a data store containing one or more records, each of which is associated with a user by a unique identifier and comprises at least code value complexity preference data (40) and a user-defined keyword (41) consisting of an ordered sequence of symbols comprising members of a predetermined symbol set selected from one or more symbol sets supported by the processing system, wherein the symbols of the ordered sequence have been previously selected by the user independently of other users' selections; and

a processor comprising a processing unit and stored program instructions which, when executed, cause the processing unit to:

receive (160) a request from a user to initiate an authentication session, the request comprising the unique identifier associated with the user;

access in the data store, using the unique identifier, the stored record associated with the user;

generate (162) a one-time security matrix which is valid only for the user during the authentication session, and which comprises a mapping between each symbol within the symbol set and a code value which is specific to the authentication session and randomly selected from a code set which is distinct from the symbol set;

transmit (164a) the one-time security matrix for presentation to the user;

receive an ordered sequence of code values (12) selected from the one-time security matrix and input by the user, based upon the user-defined keyword and the code value complexity preference data, in response to presentation of the one-time security matrix;

validate (174) the received ordered sequence of code values by comparison with a corresponding sequence of code values generated, but not transmitted, by the processing system based upon the user-defined keyword in the stored record, the code value complexity preference data and the one-time security matrix; and

generate (178) an authentication result of the authentication session based upon the comparison.

14. A security system comprising:

a user-authentication apparatus according to claim 13;

a secure system (20) for which a user requires authentication, and which is configured to:

receive a unique identifier of the user;

transmit a request to initiate an authentication session to the user-authentication apparatus, the request comprising the unique identifier of the user;

receive, from the user-authentication apparatus, the one-time security matrix;

present the one-time security matrix to the user;

receive, from the user, the ordered sequence of code values selected from the one-time security matrix;

transmit the ordered sequence of code values to the user-authentication apparatus; and

receive, from the user-authentication apparatus, the authentication result.

15. The security system of claim 14 wherein the secure system comprises one of:

a web server interface, wherein input is received from the user and the one-time security matrix is presented to the user via a web browser (110, 112) operated by the user;

an automatic teller machine (102a, 102b); or

a point-of-sale terminal (104).