SYSTEM AND METHOD FOR SINGLE OR MULTI-PARTY ON-SCREEN AUTHENTICATION USING VISUAL CODES

FIELD OF THE INVENTION

This invention relates generally to authentication or verification of a person's identity for security purposes, and more particularly to a system and method for on-screen authentication using a visual overlay.

BACKGROUND

An authentication factor is a piece of information and process used to authenticate or verify a person's identity for security purposes. Two-factor authentication is a system wherein two different methods are used to authenticate. Using two factors as opposed to one delivers a higher level of authentication assurance. Using more than one factor is sometimes called strong authentication.

Currently, there are a number of ways to achieve two-factor authentication:

1) Biometric – Using the unique physical features in human being as an authentication factor. The main draw back for biometric authentication is the privacy issue with the end-users. As an end-user, they might not be willing and comfortable to allow banks and merchants to capture their biometric data such as retina scan and fingerprint.

2) Security tokens – Smart cards, USB tokens, one-time-password (OTP) tokens are just a few examples. Specifically, Some manufacturers also offer a One Time Password (OTP) token. These have an LCD screen which displays a pseudo-random number consisting of 6 or more alphanumeric characters (sometimes numbers, sometimes combinations of letters and numbers,

depending upon vendor and model). This pseudo-random number changes at pre-determined intervals, usually every 60 seconds, but they can also change at other time intervals or after a user event, such as the user pushing a button on the token. Tokens that change after a pre-determined time are called time-based, and tokens that require a user event are referred to as sequence-based (since the interval value is the current sequence number of the user events, i.e. 1, 2, 3, 4, etc.). When this pseudo-random number is combined with a PIN or password, the resulting passcode is considered two factors of authentication (something you know with the PIN/password, and something you have from the OTP token). There are also hybrid-tokens that provide a combination of the capabilities of smartcards, USB tokens, and OTP tokens.

3) Hand Phones - a new category of two-factor authentication tools transforms the PC user's mobile phone into a token device using SMS messaging or an interactive telephone call. Since the user now communicates over two channels, the mobile phone becomes a two-factor, two-channel authentication mechanism.

However, there is a lack of pervasive use of these two-factor authentication forms and the main reason is because of cost effectiveness. Adding a second factor in the authentication mechanism could lead to increase in costs for implementation and maintenance. Most systems are proprietary and charge an annual fee per user in the $50-100 USD range. Deployment of hardware tokens is logistically challenging. Hardware tokens may get damaged or lost and issuance of tokens in large industries such as banking or even within large enterprises needs to be managed. Therefore, an analysis on the cost and benefit should be made before deciding on a stronger authentication mechanism.

There is a need for a method or system that is cost effective and easy to manage two-factor authentication using on-screen authentication methods.

SUMMARY

An embodiment of the invention is a method and/or system for providing authentication of users by first distributing a physical, secret visual overlay/key to all users and thereafter, each user could use their respective overlay/key as a means of two-factor authentication to access online resources. As part of a challenge-response scheme, the authentic authority offers an on-screen visual challenge for each of its user and by overlaying the users' own visual key to display a secret message or image which is required for login.

An aspect of the invention is a method for verification of an identity of a user comprising, assigning a user key corresponding to an identity of a user, generating a visual matrix pattern corresponding to the key, the visual matrix pattern arranged to overlie a user's screen, displaying a pseudo-random share on the user's screen based on a secret message and the user key share, and revealing the secret message to the user when the user views the share displayed on the screen through the visual matrix pattern that overlies the pseudo-random share.

BRIEF DESCRIPTION OF THE DRAWINGS

In order that embodiments of the invention may be fully and more clearly understood by way of non-limitative examples, the following description is taken in conjunction with the accompanying drawings in which like reference numerals designate similar or corresponding elements, regions and portions, and in which:

FIG. 1 illustrates a block diagram of a registration and key distribution process in accordance with an embodiment of the invention;

FIG. 2 illustrates a block diagram of a user login process in accordance with an embodiment of the invention;

FIG. 3 illustrates a block diagram of a password reset process in accordance with an embodiment of the invention;

FIG. 4 illustrates a block diagram of a registration and mobile key distribution process in accordance with an embodiment of the invention;

FIG. 5 illustrates a block diagram of a user login process in accordance with an embodiment of the invention; and

FIG. 6 illustrates a mobile key reset process in accordance with an embodiment of the invention.

DETAILED DESCRIPTION

Embodiments of the invention propose a method and system that are cost effective and easy to manage two-factor authentication using the enclosed on-screen authentication methods where the "token" is essentially a pseudo-random visual matrix pattern printed on normal transparency paper using normal printing devices. FIG. 1-3 show block diagrams illustrating the registration and key distribution (FIG. 1), the user login process (FIG. 2), and the password reset process (FIG. 3) in accordance with an embodiment of the invention. An embodiment of the invention is a technique that is different from typical tokens solution in that it can be use for secure multi-party login.

Secret sharing scheme is a well researched area in cryptography proposed by Naor, M. and Shamir, A., "Visual cryptography", In: LNCS, vol. 950, Springer-Verlag. pp. 1-12, incorporated herein by reference. The motivation for secret sharing is secure key management. In some situations, there is usually one secret key that provides access to many important files. If such a key is lost (e.g., the person who knows the key becomes unavailable, or the computer which stores the key is destroyed), then all the important files become inaccessible. The basic idea in secret sharing is to divide the secret key

into pieces and distribute the pieces to different persons so that certain subsets of the persons can get together to recover the key.

The general model for secret sharing is called an m-out-of-n scheme (or (m, n)-threshold scheme) for integers 1, m, and n. In the scheme, there is a sender (or dealer) and n participants. The sender divides the secret into n parts and gives each participant one part so that any m parts can be put together to recover the secret, but any m - 1 parts reveal no information about the secret. The pieces are usually called shares or shadows. Different choices for the values of m and n reflect the tradeoff between security and reliability. A secret sharing scheme is perfect if any group of at most m - 1 participant (insiders) has no advantage in guessing the secret over the outsiders. Therefore in a single party authentication mode, it is a (2, 2)-threshold scheme. In practice, the hidden secret could be any colored image which contains any graphics or characters from any language. This secret will be required as a second factor authentication during user login.

With the reduction of cost in flat-screen display devices like LCD, Plasma TV, flat-screen CRT, and even mobile devices, it is becoming more pervasive items.

Embodiments of the invention may include different schemes for effective and secured T-FA, for example by visual codes overlay, mobile token authentication, or the like.

In an embodiment, the proposed scheme by visual codes overlay can be described in main phases: 1) registration and key distribution to users, 2) online user login and 3) password reset.

For phase 1 as shown in FIG. 1, the authority 4 for online resources, for example a bank which provides internet banking services, first needs to register and distribute a random key share to a user 2. Typically, the user will be given a generated user ID and password generated by a key generator 6 and on top of that, the secret key shares printed on a transparent, physical medium (transparency) 50. This key could be sent to the user through registered mail or even by electronic form for self-printing. The

authority will keep a database 8 of all the user information: user ID | Password | key share.

For phase 2, as shown in system 10 of FIG. 2, when a user 2 tries to access online resources, the authority 4 will prompt the user for user ID and password. Once this information is verified be correct, the system from the authority will generate a pseudo-random share, S, based on a secret message and the user key share so that when the user overlays 50 his/her share on-screen 52 on top of S, the secret message will be revealed. The user then needs to key in this secret message and if it is correct, the user can gain access to the online resource. For multi-party login, at least n users need to be present with their key shares to overlay 50 and reveal the secret message before they can login.

For Phase 3, as shown in FIG. 3, in the case of compromise or loss of the end-user secret token, the end-user could easily do a password reset with the authority. Basically, the end-user 2 will registered with the authority and ask for a new token. Authority system 4 will process the request and re-generate by the key generator 6 a new visual key and update the user ID | Password| key share entry in the database 8. The new key can be convenient distributed to the end user via registered mail, email etc.

Due to the variants of display devices at the user's end, it may be difficult for end-user to align and overlay lens against the display screen to correctly display the secret message during authentication. To tackle this, an embodiment of the invention includes a few proposed techniques for easy on-screen authentication.

Technique 1: Easily adjustable on-screen lens size for end users
Technique 2: Redundancy in secret message structure
Technique 3: Dynamic screen size matching program
Technique 4: Pre-printed multi-size lens key

By using the lens key as a token, there are several advantages over traditional tokens solution:

1) Each lens key cost much less than a physical token
2) Lens key could be easy distributed to the end-user for self printing.
3) In case of any compromise to the lens key, a renewal key could be easily generated and distributed to the affected user.

In an embodiment, the proposed scheme by mobile token authentication can be described in main phases: 1) User registration and mobile key distribution, 2) User login and authentication and 3) Mobile key reset. FIG. 4-6 provide similar and self-explanatory process for mobile token authentication.

In order for the Mobile Key to be transmitted securely (either via SMS, GPRS or any form of transportation protocol), it will be encrypted prior to the transmission. The encryption can be done either via a symmetric key algorithm or based on Public Key Infrastructure (PKI) key-pairs. When a PKI system is used, the contents embedded in the Visual Code may be encrypted and digitally signed using the public and private keys of the Authority System. In this way, a 2-way verification of the service provider and service requestor can be ascertained securely, thereby increasing the security of the whole system.

Similarly, the Mobile Key generated can either be based on a symmetric key algorithm or based on Public Key Infrastructure (PKI) key-pairs.

In cases where the user needs to authenticate with more than one Authority Systems, the same mobile application installed on his mobile phone can be used. In this case, multiple Mobile Keys specific to each of the Authority Systems would be stored securely on the mobile phone.

Visual lens 50 is comparatively easier to replicate than physical tokens but it will be appreciated that the visual lens is more cost effective.

An embodiment of the invention could be used as authentication means for scenario with these important characteristics: cross-order and mass authentication.

Market segments and/or applications of embodiments of the invention in regards to two-factor authentication may include enterprise applications such as secure remote access, enterprise authentication, business to business (B2B) transactions, or the like; consumer applications such as online banking, electronic commerce, ISPs, or the like; government applications such as common authentication or the like.

While embodiments of the invention have been described and illustrated, it will be understood by those skilled in the technology concerned that many variations or modifications in details of design or construction may be made without departing from the present invention.

CLAIMS:

1. A method for verification of an identity of a user comprising:
assigning a user key corresponding to an identity of a user;
generating a visual matrix pattern corresponding to the key, the visual matrix pattern arranged to overlie a user's screen;
displaying a pseudo-random share on the user's screen based on a secret message and the user key share; and
revealing the secret message to the user when the user views the share displayed on the screen through the visual matrix pattern that overlies the pseudo-random share.