INTERCEPTION-PROOF AUTHENTICATION AND ENCRYPTION SYSTEM AND METHOD

This application is a continuation of U.S. patent application Ser. No. 14/925,769, filed Oct. 28, 2015. The disclosure of U.S. patent application Ser. No. 14/925,769 is incorporated herein by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to authentication and encryption systems and methods and, more particularly, to interception-proof authentication and encryption systems and methods.

2. Background of the Related Art

In modern society, daily life requires the use of a wide variety of information devices, such as mobile phones, PCs, notebooks, and ATMs to name a few. The information devices may keep users' personal data. Due to the importance of protecting this personal data, there are methods to securely lock and unlock these devices.

At present, the most commonly used method to lock and unlock these devices is a password-based challenge authentication procedure, whereby a device typically requires that, before accessing its services, users enter a user id and a password for identity recognition. This is known as a login. This login process is designed to prevent users' personal data from being stolen or fraudulently changed.

With the rapid daily increase of network coverage and accessibility, hackers are more likely to target users' passwords to gain access to their private information. In addition, hackers are getting more and more sophisticated at guessing and cracking users' passwords. Therefore, simple passwords no longer provide adequate protection from cyber threats and espionage.

In view of this, various mechanisms have been implemented to provide better protection. For example, users are required to create a password that meets the requirements of password length, complexity, and unpredictability, such that the strength of the password is, in theory, sufficient enough to fend off brute-force search attacks and dictionary attacks. Furthermore, users are required to change their passwords regularly to invalidate old passwords, thereby reducing the chance that their passwords will be cracked. These mechanisms do enhance security to a certain degree and thus help users protect their accounts.

However, each organization may have a different set of password rules. Some require the password length to be at least 6 or 8 characters. Some require the use of mixed uppercase and lowercase letters, as well as numbers. Some require at least one special character, yet some do not allow special characters, so when you think you have just created a very strong golden password which you can use in all places, there will be a next place which has a different set of requirements that will make your golden password invalid.

As a result of these different password rules, it may be difficult, if not impossible, for users to remember the multitude of passwords they have set up with different sites/organizations. Thus, users will typically store their passwords, such as in a file that is stored on their information device and/or in a password storage application that runs on their information device. The stored passwords can be targeted by hackers, and if they gain access to the device on which the passwords are stored, they will gain access to all the passwords and have access to all of the user's password protected accounts/sites. Therefore, implementing strict rules for passwords to avoid passwords that are too weak can have the opposite of the intended effect (an increased risk of exposing more information).

In view of these problems with traditional passwords, new methods have been developed to try to solve these problems. These methods may include, but are not limited to, using photos, graphic images, or different shapes and shades to make it harder for hackers to peek or steal. Some techniques even use gestures and positioning of information in certain locations of the input screen to validate user access. However, none of these methods can defeat a hidden camera which can record users' every move every time they log into a device. If a hacker can play back all the recordings and analyze a user's every move, the hacker will eventually gain access.

The primary problems with existing authentication methods are:

(1) Traditional passwords and security questions (the most commonly used method) are not peek-proof;

(2) Graphic images and photo-based methods may require users to upload an image or photo file, and the system must save and maintain the images and/or photos. This increases user and system burden, and if hackers record and playback the login process, the images can still be recognized;

(3) New graphic and gesture and/or location-based authentication methods can only be used between human and computer, and thus cannot be used machine to machine.

Thus, there is a need for authentication and encryption systems and methods that do not exhibit the above-described problems.

SUMMARY OF THE INVENTION

An object of the invention is to solve at least the above problems and/or disadvantages and to provide at least the advantages described hereinafter.

Therefore, an object of the present invention is to provide a system and method for authentication of a user.

Another object of the present invention is to provide a system and method for authentication of a user attempting to access an electronic device.

Another object of the present invention is to provide a system and method for authentication of a user that is requesting access to electronically stored information.

Another object of the present invention is to provide a system and method for authentication of a user that is requesting access to a device on a network.

Another object of the present invention is to provide a system and method for authentication of a user that utilizes passcodes that contain a predetermined number of symbols.

Another object of the present invention is to provide a system and method for authentication of a user that utilizes multiple tokens, where each token is a group of at least two symbols from a set of symbols used to create a user passcode.

Another object of the present invention is to provide a system and method for encryption and decryption of electronic information.

Another object of the present invention is to provide a system and method for encryption and decryption of electronic information that utilize a passcode that contains a predetermined number of symbols for encrypting and decrypting the electronic information.

Another object of the present invention is to provide a system and method for encryption and decryption of elec-