Two-step authentication that provides highly secure access to secure areas or resources

Victor Solovyev
victorsolo@gmail.com

Abstract

A two-step authentication system and method are provided for secure authentication that implements highly secure access to secure areas or resources with disabling the access when the main passcode is compromised. A user, after successfully passing through the passcode of the first-step verification stage, is asked to input an additional secret and presumably easy memorezible code (a pin, second password), or recognize an image for authentication (from a generated set). If during this second-step the user entered information fails to match the correct secret code, then the system sends signal message on intrusion to the user or other designated authorities through a communication device (e.g., email or telephone message) and the access is disabled immediately or after a few permitted attempts. Such authentication, while providing better security and user experience, does not require the usual practice of disabling the access, when the first-step access required information (such as complex alphanumeric password) is entered with errors in repeated access attempts.

Keywords

Authentication system, secure acsess, two-step authentication, image passcode

Introduction

Today in order to control access to most of electronic or computer-based resources, identification and authentication steps require providing a login name and a password associated with the user and known to the accessed resource [1-2].

The problem is complicated by possibility of unauthorized access when the password is compromised due to the password theft or cyber attacks or other activities of unauthorized user. Such access can result in significant material or other damages to the account owner such as manipulation with his money (intrusion to the bank system) or usage of expensive resources (running some CPU-intensive tasks with intrusion to Amazon cloud) and etc. Important that in typical (login name/password) setting (depicted in FIG.1) an unauthorized intrusion with compromised password usually is unnoticed for a time period sometimes long enough to inflict irreparable damages.

A popular measure to prevent unauthorized access is requesting the system to block access to the account (FIG.1: 106) after a small number of failed attempts to

enter the passcode (FIG. 1: 105). However if the account has a strong (and hard-to-remember) passcode, in many cases it would be a waste of time to initiate procedures of unlocking the account that is blocked due to errors in entering the password when the passcode is not actually compromised. Unlocking procedures sometimes can prevent the resource access for a long time (if you need to call to the resource administration, for example) and it might be harmful for businesses that require a quick response in their operations. It would be especially relevant to

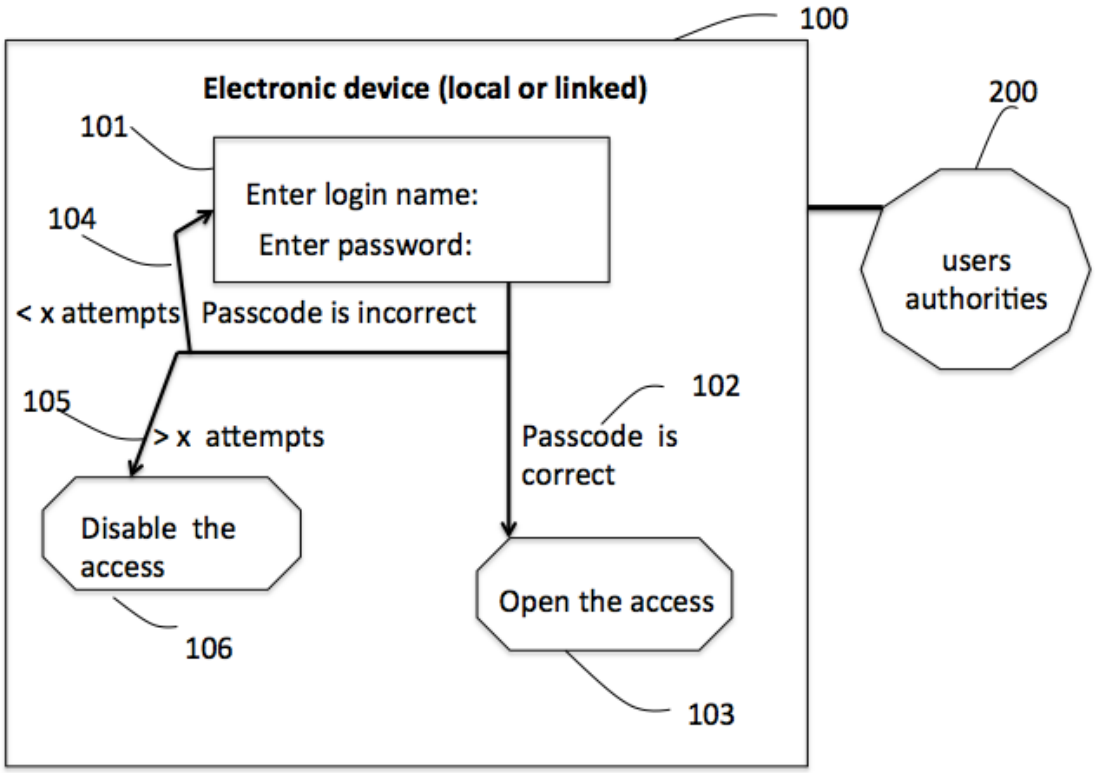

FIG. 1 is a flowchart illustrating typical implementation of system secure access (100) by providing a login name and a password (101) by users (200). If the passcode pair (login name and password) is correct (102) the access is open; if the password associated with a particular login name is wrong then the system permit to repeat the entry of password a few times (104); and if the password entry is fail more than a few (x) times (105), then the access to the resource is disabled (blocked) (106).

multiuser accounts where the frequency of password entering errors is usually higher and account-unlocking procedure is more tedious, especially for users without the administrative rights.

Highly secure logins using multi-factored authentication require remembering

many passcodes that increase frequency of account blocking due to passwords entering errors. It has negative effects on users experience. The complex multi-factored authentication would not be necessary in most typical settings when we apply the two-step authentication method described in this paper.

Two-step authentication sytem

It is an object of the paper to provide a system and method to enable secure access to some resource that would not be a burden to authorized users and deliver highly secure authentication by notifying a user and blocking the access only when main passcode is compromised. It is resistant to the entering errors in the main passcode and includes the access blocking when the main passcode is compromised with reporting the intrusion to the user or other delegated authority by sending signal to their communication devices.

The details of implementation are set forth in the accompanying drawings and the description below. Other features and advantages will be apparent from the description and drawings.

Below, the system will be explained in greater detail based on two embodiments that are depicted in the drawings. The first one covers a general implementation of two-step authentication system for secure access. Such implementation can be applied in systems to control secure access by mechanical or electro-mechanical devices (e.g., digital locks) that require providing some passcode to unlock the access to a secure area and communication devices that notify the intrusion may be as simple as sound or light alarms. The second exemplary embodiment covers an implementation of the two-step authentication system for typical computer or other electronic systems. Such implementation can be applied in systems with local or remote access to a linked resource through their web page or other user interfaces.

The exemplary of general embodiment is depicted in FIG. 2 in a flowchart illustrating implementation of two-step authentication system for secure access. The access control device 100 includes the system of entering and verification of passcodes that is represented by two consequent stages 101 and 102. When access required information is entered incorrectly at the first-step (103), then the user 200 is requested to enter this step's access required information again (101), otherwise (104) the user is requested to enter the second-step's access required information (102); if the second-step entry data fails to match this stage secret code (105), the access to the resource is disabled (blocked) immediately or after a few permitted attempts (106) and the notification on intrusion (107) is sent to the user's or other delegated authority's communication device 300; the access is open(108) if the second stage passcode is correct (109).

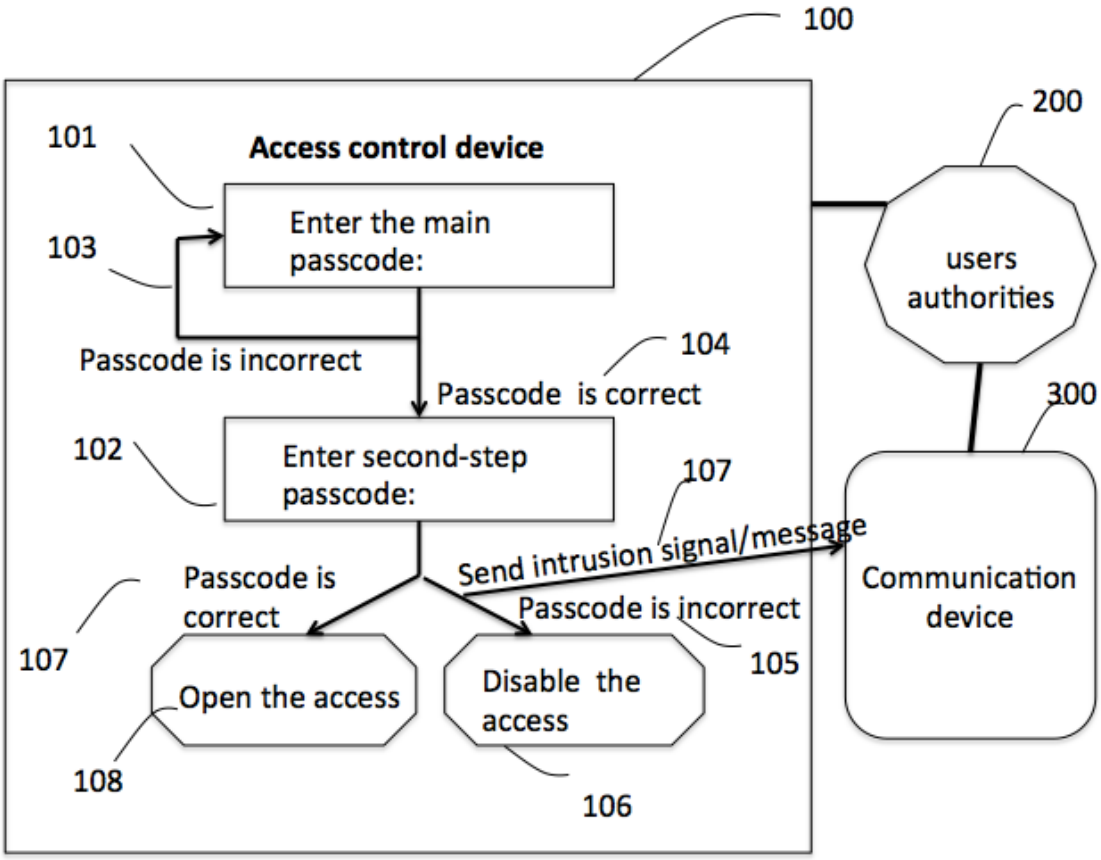

FIG. 2 is a flowchart illustrating general implementation of two-step authentication system for secure access (see detailed explanations in the text).

The second exemplary of embodiment depicted in FIG. 3 is a flowchart illustrating the two-step authentication system for secure access to computer or other electronic systems. The electronic device 100 includes a typical access control login system that includes login name and password (first-step: 101). If login name and password pair is entered incorrectly (103), then the user 200 is requested to enter this information again (101), otherwise (104) the user is requested to enter the second-step's access required information that may be in the form of pin or additional password (that pre-selected by the owner of the computer or electronic system account), alternatively the user may be required to recognize the pre-selected image from a set of displayed images (102) (that would be more secure against typical cyber attacks). If the second-step entry data fails to match the secret code or select the right image (105), the access to the resource is disabled (blocked)

immediately or after a few permitted attempts (106) and a notification on intrusion (107) is sent to the users or other delegated authorities (200) to their communication devices 300 (such as telephone or computer) by email, telephone call or message; the access is open (108) if the second stage passcode is correct (109).

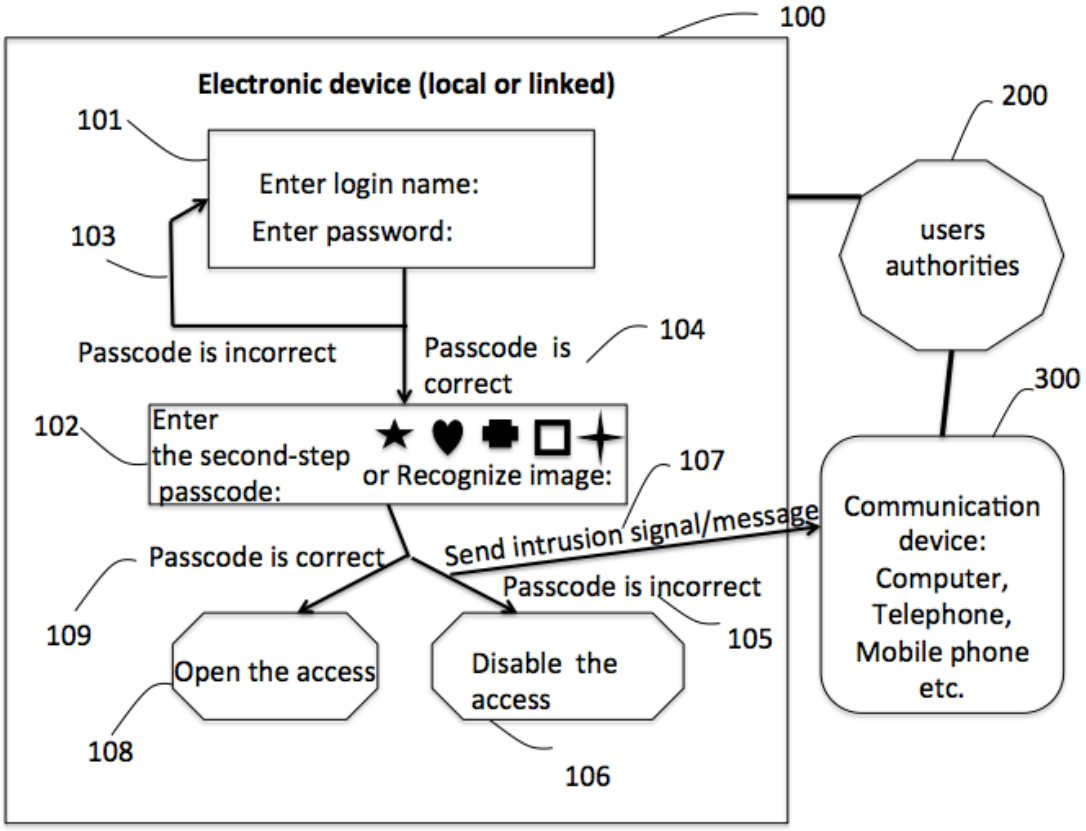

FIG. 3 is a flowchart illustrating the two-step authentication system for secure access to computer or other electronic systems (see detailed explanations in the text).

The method can be applied to on-line passport changing procedures: if the second-step entered information fails to match the secret code or recognize the owner's pre-selected image, the system generates and send notification on intrusion to the owner of the account by email, telephone call or message and the password change operation is disabled.

It is presumed that the first-step passcode is strong (i.e. hard to compromise). In view of the fact that possible errors during the passcode entering will not block the

system, the system will be available to users most of the time. It will provide much better user experience than, for example, a typical access system that block the resource access (login) after a few failed attempts to enter the correct passcode. The second-step passcode should be reasonable simple with a small probability to enter it with error (such as pin or recognition an image). In such case the whole access process will not be a burden to the users. To increase security the set of presented images at each access/login attempt can be generated randomly from a big arhive or some image generating procedure. The set just should include the secod-step passcode image. All images of the set can be presented at the same time or it might be short time separated a few series of showing one or several images where the user shoud select the correct one.

It would be beneficial to always memorize the simpler second-step passcode to guarantee better security of resources in case their access controlling main passport is compromised (e.g., stolen from electronic or paper records). Image-based second-step passcodes are easier to remember than complex alphanumeric passwords and they are more resistant to phishing and other forms of password theft.

References

[1] https://en.wikipedia.org/wiki/Authentication and references in it.
[2] Schneier, B., 1996. Applied cryptography, John Wiley & Sons, Inc., 758 p.