BMC Software Inc.

Technical Disclosure Publication Document

Author

Myron Warach

Posted: June 2009

Overview

This document describes a solution called “User-friendly password switch”. The solution is designed to eliminate a user’s apprehension of losing control of an account because of password change.

Background

Best practices for password management require that users change their passwords periodically (e.g. every three months).

Users may be reluctant to change an account password for an operating system, home or enterprise application, or web-based application because of an apprehension of losing control of the account; that is, being unable to log into the account after the password is changed.

This may be especially true in mandatory password change environments such as online banking or financial trading where it may be difficult to get help from remotely located IT support. A mandatory password change environment is one where the user is instructed to change his or her password immediately, or within “X” number (e.g. 5 or 10) of days.

Apprehension of changing an account password may also be the case in non-mandatory password change environments, such as Gmail or social-networking sites, where users may decide that it is not ever worthwhile risking a password change.

Solution

The “User-friendly password switch” solution provides that a user’s password is changed only after the user successfully enters it in the login screen for the first time. Until the new password is actually used to log in, the user’s old password remains valid.

The solution is implemented by storing the user’s new password hash value in a “User-friendly new passwords” table – not in a standard table of current hashed passwords. After password change, when a user logs out and tries to log in again the following occurs:

The user’s password hash value is compared in the “User-friendly new passwords” table. If the user’s password hash value matches a password hash value in the “User-friendly new passwords” table then 1) the user’s old password hash value in the table of current passwords is deleted and replaced by the new password hash value and 2) the new password hash value is deleted from the “User-friendly new passwords” table. The user has logged in using the new password and the user’s password change is completed.

If the password change has not yet occurred, the user’s password hash value will not match a password hash value in the “User-friendly new passwords” table. The application then tries to find a match for it in the table of current hashed passwords. If a match is found, the user has logged in with his or her old password.

Password change takes place when the user successfully uses his or her new password to log in for the first time. Until the user correctly enters the new password the old password is valid.

Note: In mandatory password change environments the old password will become invalid after the stated expiration period if the user has not by then completed password change.

The advantage of the “User-friendly password switch” is that the user effects the actual password change only when the new password is successfully used thereby assuring the user that he or she will retain control of the account during password change.

These are examples of user-friendly instructions that may be given to users to explain the password change scenarios.

Non-mandatory password change regime (sample instructions).

It is good security policy to change your password occasionally because someone may have discovered it or a computer virus or spyware may have intercepted it.

To change your password:

1. Enter your old password.

2. Enter your new password then confirm it.

3. Click OK.

Your old password will expire as soon as you log in using your new password. It is recommended that you log out now and log in again with your new password to complete the password change.

Mandatory password change regime (sample instructions).

It is good security policy to change your password because someone may have discovered it or a computer virus or spyware may have intercepted it.

You must change your password within X days or you will not be able to log in.

To change your password:

1. Enter your old password.

2. Enter your new password then confirm it.

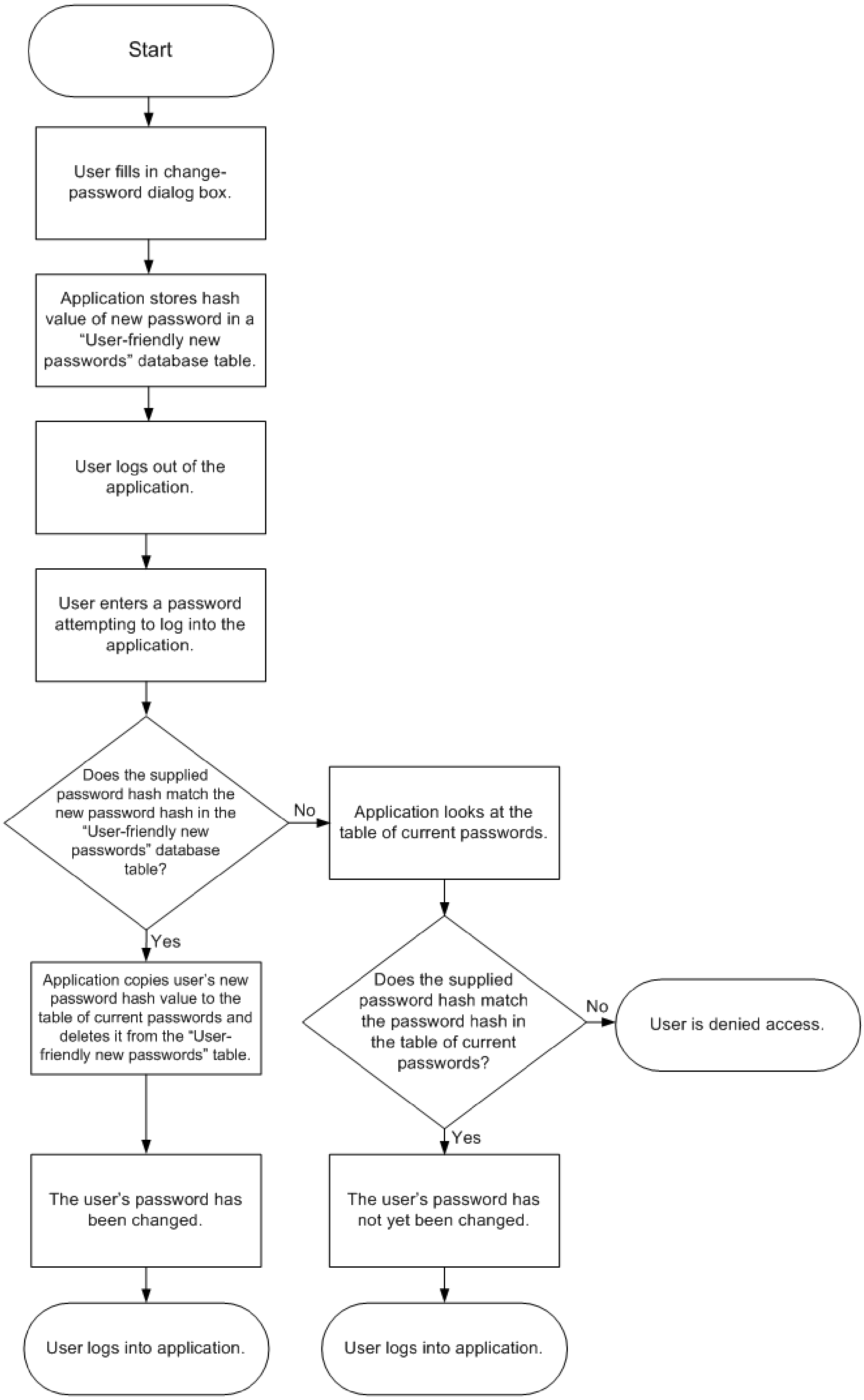
3. Click OK.

Your old password will expire whichever occurs sooner:

- It expires in X days from now.

  Or

- As soon as you log in using your new password.


Start
User fills in change-password dialog box.
Application stores hash value of new password in a "User-friendly new passwords" database table.
User logs out of the application.
User enters a password attempting to log into the application.
Does the supplied password hash match the new password hash in the "User-friendly new passwords" database table?
No
Application looks at the table of current passwords.
Yes
Application copies user's new password hash value to the table of current passwords and deletes it from the "User-friendly new passwords" table.
Does the supplied password hash match the password hash in the table of current passwords?
No
User is denied access.
Yes
The user's password has been changed.
The user's password has not yet been changed.
User logs into application.
User logs into application.