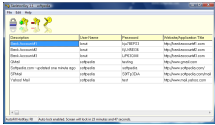


6 January 2009

By: Ionut Ilascu, Editor, Software Reviews



SkeletonKey main application window

Password Reminder

No need to remember passwords anymore

We live in a time where passwords are an active component of our lives. They protect the access to everything we do not want to share with others. Email accounts, computer access, online bank accounts, forum logins, program logins, they all are defended by passwords. To keep them all out of reach of prying eyes it is generally recommended to change access credentials as often as possible. And it is a rule of thumb never to have the same password for multiple accounts.

The trouble rising from all this is remembering which countersign goes with which account. It is comfort that pushes us to assigning the same password, and sometimes username, to multiple online accounts, but comfort can also step in under the form of a software app and help us place all passwords under a single roof and instead of bothering with remembering complicated, senseless sequences of letters, symbols and numbers, keep in mind only one master password and a single username.

SkeletonKey is a password manager with the right structure for the task at hand and it comes at \$4.99. The trial available for testing lets you store only 3 entries. Despite the fact that this should not be an impediment for testing the application, we were given for evaluation a full version of the application.

Installing SkeletonKey is as easy as can be and the only interruption occurs at the creation of a new user and at the end when a master password has to be set. Careful with this though, as once lost there is no way to retrieve stored information.

The program is nothing like what you are used to seeing in Vista because the looks of the interface don't fit with the shiny shell of the operating system. Actually, it hardly accommodates Windows XP as everything seems displaced from another time. Everything is kept to the most Spartan build possible and there is absolutely nothing more and nothing less than a password manager. From a first look one would definitely not be attracted to SkeletonKey.

The main application window is composed of the list of passwords and usernames added by the user and the website or application title they are for. The first drawback of the software consists in the fact that the passwords are not at all hidden but in plain view. An option for hiding and revealing the passphrases at your command would have been a great compromise.

The toolbar is in tone with the menus and comprises only functions for locking the software, adding a new entry, deleting one or accessing the master password change panel.

The same scarcity of options welcomes us when getting at the configuration section of the application. Here you can enable/disable the autolock feature, set the autolock time or the auto-fill key. Indeed, SkeletonKey is more than meets the eye and the auto-fill function is by all means the most important feature that distinguishes it among other password managers on the market.

The AutoLock function can be set to be enforced after a period of time from one minute to

an entire hour. This means that after the set time, the application will reflexively lock the password screen cutting all access to stored entries. The action occurs independently of the system activity and even if you are currently handling the software. Fortunately, the time to lock down is displayed at the bottom of the interface giving the remaining minutes and seconds. The only time when auto-lock can be paused is when the Settings panel is open.

Unlike in other password managers with a similar feature, the AutoFill function does not prompt you automatically when a certain login page/window is detected. It is activated by the function key (default is F7) and the popping screen permits choosing the credentials to be completed. I would call this behavior semi-automatic because it can't do the job by itself and requires a little more than minimum user input.

SkeletonKey seems to be limited when it comes to selecting the auto-fill key as you cannot choose just any key combination but you are limited to only five alternatives: F5, F6, F7, F8, F9 and F11. Also, the application needs restarting for the change to take effect. From this point of view the program proves its inflexibility as these keys may stand for different actions in a web browser that you might actually need.

If all the options in the application have not been too persuasive, security details are definitely something else. All data in SkeletonKey is encrypted with a symmetric key algorithm (AES). The master password is stored using a cryptographic hash function (basically the input can be of any length with the output having the same length).

To enforce even more security to your data, once the software is locked up brute-force attacks are pretty useless even if a pretty weak password is selected. This is due to the 5 attempt limit for the passphrase entering. However, this does not mean that after five screw-ups the data is lost without recovery as after 5 incorrect tries the application lets you try again in 30 seconds' time.

Also, passwords will never stay in the clipboard for more than 20 seconds if copied from SkeletonKey (this goes for the username, website/application title and description as well). The AutoFill function does not use the clipboard either since the program sends the keystrokes directly to the input fields just like they have been typed by the user (a keylogger on your computer will record the username and password).

SkeletonKey is a simple password manager that needs few resources, brings only the essential on the table and runs on extremely low system resources. An uncomplicated application set to relieve you of the effort of remembering complex countersigns, offering in return the comfort of automatically filling in the credential fields.

A brush-up of the interface is in order as well as for several other aspects, but the low price and the high security provided make for a great starting point.

The Good

The simple interface makes it extremely easy to handle. It comes with sharp security for both stored data as well as the master password.

SkeletonKey can be used by multiple users, each with its own set of credentials and separate database. The AutoFill feature works great and saves you from memorizing complicated countersigns.

The Bad

Flexibility is not a strong point here. When setting the auto-lock time you cannot type in the value by yourself but instead click on them or use the up/down arrows of the keyboard. Also, the choices for the AutoFill key are limited to six and you cannot set them to your liking.

Passwords are visible in the main application window and there is no option to hide them from view.

The interface is much too old-school and fails to integrate in the modern shell provided by Windows Vista and even XP.

The Truth

Security is the best thought of feature of SkeletonKey. AutoFill plays an important role as well but its access is restricted by the few options in setting the hotkey.

The interface may not be shiny and pretty but it is just a means to an end and can be handled with little to no effort at all on your part. If by any chance you fail to get around the few options SkeletonKey provides, an extensive help file is available explaining each feature and function of the software.

There is certainly plenty to fix and modify but it is a low-cost password manager that boasts an auto-fill function, extraordinary security measures for your data and multi-user support.

Here are some snapshots of the application in action: