Keeping passwords secure with KeePassX

SECRET STASH

For optimum security, a password has to be too long and complex for normal humans to remember. If you want to wield effective passwords without hurting your brain, manage your online logins with the KeePassX password manager. **BY JAN RÄHM**

Most users have no trouble remembering the password for their web mailer, and they can usually remember how to access a frequently used online forum or web store. But if you don't visit a site very often, you might not remember the spontaneous password you typed in when you joined the site. Some people work around this issue by using the same password every time. Needless to say, this approach isn't very secure. Once an attacker has discovered a password combination, other accounts are totally open.

A password manager like KeePassX [1] provides a solution to the password problem (Figure 1). KeePassX saves credentials in a secure manner – no matter how rarely you visit a website or how complex the password combination might be.

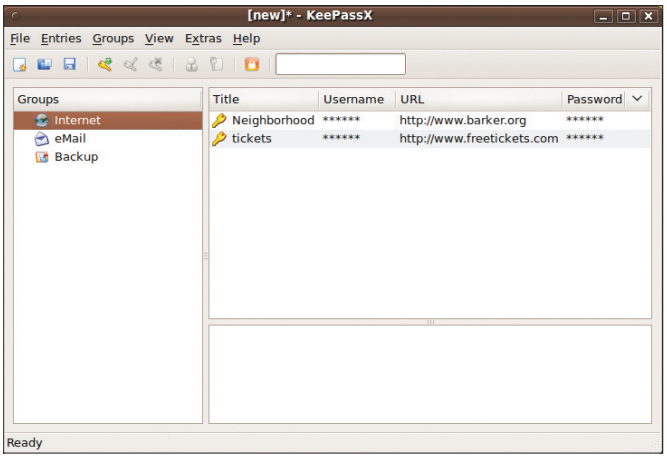

Figure 1: KeePassX keeps track of your online passwords.

The KeePassX password manager is a Linux and Mac OS port of the KeePass program [2]. Both projects aim to secure and manage user credentials. Besides usernames and their corresponding passwords, KeePassX additionally stores URLs, notices, and file attachments in its database. It uses the AES or Twofish algorithms with a 256-bit key to secure the database.

To install KeePassX, use the Ubuntu Synaptic package manager. See the box titled "Installation" for alternative approaches to installing the software on your system. The program launcher is listed in the *Applications* | *Accessories* menu section. Clicking the icon launches the password safe, which comes up with a three-panel main window and menu and taskbars at the top.

To populate KeePassX, either import a database or create a new one yourself. Importing a database makes sense if you worked with the program's predecessor, KeePass or if you already use KeePassX on another system. KeePassX will also import the KWallet or PwManager databases.

Populating the Keyring

To create a new database, begin by clicking on the *New Database* icon. This takes you to a dialog box in which the program prompts you for the initial password for the database. Your password should be long and secure (see the "Secure Passwords" box).

Alternatively, you can protect the database with a Key File. To do so, select a file, or let KeePassX create it for you by checking the *Key Pass* box and clicking *Generate Key File*. If you only protect the database with a key file, anybody who possesses the key will be able to access any data you store.

A combination of a long and complex password and a key file is your best bet, although this does make it difficult to recreate the passwords if you accidentally delete or damage the key file and don't have a backup.

After choosing a key, press *OK* to confirm and create the new, almost totally empty database. In fact, the database only contains two empty groups at this point. You can create a new entry by selecting *Entries* | *Add New Entry* in the menu or by pressing Ctrl + Y. The entries appear in a box top right.

A dialog box asks you for details of the entry. The drop-down menu lets you assign the entry to a group. KeePassX will

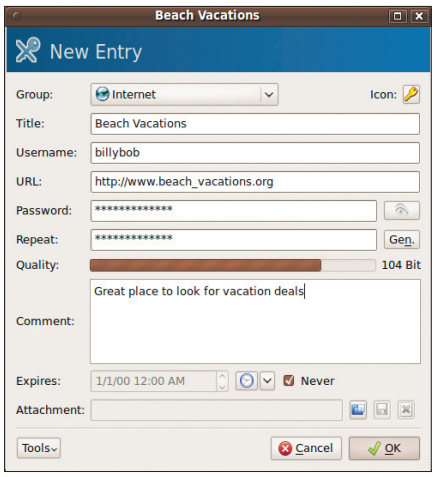

Figure 2: KeePassX asks for information to add a new password entry.

Figure 3: KeePassX can generate a password for you automatically.

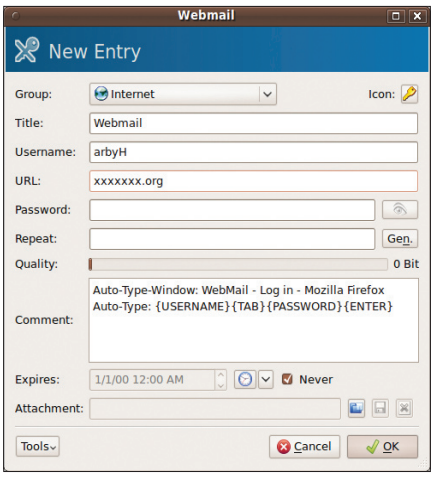

Figure 4: The Auto-Type feature removes the need for typing usernames and passwords.

then ask you for a title, the username, the matching URL, and the password (Figure 2). Or, you can create the password automatically by pressing the *Generate* button (Figure 3).

After retyping the password, you can add a comment to the entry and even attach a file if necessary. This feature means that KeePassX can quickly encrypt small files such as text or images.

Auto-Type

The *Tools* drop-down (bottom of Figure 2) provides an option that will help you configure the KeyPassX Auto-Type function. According to the documentation, Auto-Type only works on Linux systems right now. The feature reduces the need for typing and lets you associate the login with a keyboard shortcut. The advantage of Auto-Type is that you are never exposed to keyloggers.

To use the Auto-Type feature, open the website on which you want to log. Now toggle back to KeePassX and the open dialog box. Click *Tools* and *Auto-Type: Select target window* to open a window with a drop-down menu containing multiple entries.

Clicking the entry copies the target window information to the comment box. This selects the window for automatic input. Another click on *Tools* and *Auto-Type: Customize Sequence* tells KeePassX to add the *Auto-Type: {USERNAME}{TAB}{PASSWORD}{ENTER}* line to the comment field (Figure 4). Then you then click OK to save the entry.

The next step is to define a global keyboard shortcut for the Auto-Type function. To do so, go to *Settings* and select *Preferences Advanced*. This dialog includes a *Global Auto-Type Shortcut* text box. Click the box and then press your preferred keyboard shortcut.

After entering the shortcut, you can simply press the keyboard shortcut in a web browser, or any other program that prompts you for a username and password, to supply the credentials. Just make sure you don't use a shortcut that you have already assigned, or one that you use frequently in some other program.

Now, when you press the keyboard shortcut in your browser or program, you can watch the fields for both the username and password automatically fill, allowing you to log in without too much typing.

Conclusions

KeePassX patiently waits as an icon in the system tray until you need it for something. We didn't hear a single word from KeePassX, apart from the request to authenticate against the database.

The KeePassX password manager makes logging into websites and applications safe and enjoyable – with no need for distress over long and complex passwords.

An auto-login feature that didn't require a password shortcut keyboard would be the icing on the cake, but the shortcut key is easy to manage now that all of my credentials are stored centrally and available for cross-platform use. ■

Installation

Prebuilt installation packages for KeePassX are available from the project website for a variety of Linux flavors, Apple Mac OS X, and Microsoft Windows. You can download the source code for the software from the same place. Also, you can use the Ubuntu package manager to install the program.

Secure Passwords

Secure passwords tend to be fairly long and include a variety of different characters. However, they also tend to be less than intuitive, and that makes them easy to forget. Thankfully, there is a workaround for this.

You will definitely want to avoid passwords that contain dictionary words. One practical approach is to start with a sentence you are familiar with, write the sentence down, and create a string from it by using the first letter of each word, including upper- and lower-case characters.

Add non-standard characters and numbers at the beginning and end – and other easily remembered locations in the middle of the sentence. The longer your password is, the more secure it is and the more time an attacker will need to brute force it.

INFO

[1] KeePassX project: *http://www.keepassx.org/*

[2] Keepass: *http://keepass.info/*

AUTHOR

Science journalist Jan Rähm writes articles and broadcasts shows on Linux, IT, and technology.