Passwords, and how to look after them

by Andy Pepperdine

Introduction

Passwords are like keys; they identify the user, they are used to determine whether someone is authorised to access a function, file, or site, in much the same way as a physical key does in the physical world. Possession of a key will enable you to open a lock. “Possession” (i.e. knowledge) of a password enables you to access the feature.

In the same way that keys are kept on keyrings, passwords can be kept on virtual keyrings, or wallets, or lockers – the terminology varies from program to program. Of course, in the electronic world, access to the locker also need to be authorised.

This paper will describe some of the methods in use to help you organise your passwords, and givve some reasons why they are needed in some case, but not others.

User accounts

A user account is where you keep your data, files, mail, and other information on a computer. To access that data you should say who you are.

All systems can be set up so that when you switch the machine on, it will present you with a challenge screen asking for name and password to identify the account you want to access. This is the traditional way of checking who you are and putting you in touch with your data. Supplying the name and password is known as logging on or logging in.

As machines became more personal, it became apparent that this was annoying when the device was never out of your physical control. Consequently, there is usually a way of setting it up so that it will log in to a particular account automatically when the device is switched on, and is the commonest method for computing machinery these days. This will be acceptable so long as access to the device is controlled.

Networks

Networks can either be wired or wireless. There is an assumption among the vast majority of common devices that a wired connection is already authorised, simply because you have access to the physical hardware that makes the connection. There are ways of making a new wired connection ask for authentication, but so far as I know, they are used only in extremely sensitive locations of a military or delicately commercial nature.

For wireless connections, however, you might see the network from outside the control of the owner of the network, by standing outside in the road, for example. So in these cases, it is much more common to insist on a password before obtaining access to the network. Some systems, like Ubuntu, ***may*** use a wireless manager that saves its passwords in the Gnome keyring. This means that it will be accessible so long as a password has been given. If it was used when you logged in, then it should not ask again. However, if you have set the account to automatically log in when the system boots up, then it will ask for the password to access the keyring.

There are some disadvantages to this scheme. If you change your login password, at some time you may find that wireless connections ask for the password that the keyring still expects, which will be the old login password. The recommended method to fix this is to delete the *.gnome2/keyrings* directory and set up all the passwords again. When it is recreated, it will reset access to it.

Websites

Websites can contain personal information, like your bank, for instance. In order to control access to these, they will request some authorisation, usually a password and some other data. Since almost all sites these days use standard types of forms to ask for the password, modern browsers can keep the contents for you and fill them in automatically. However, you will have to ask yourself where it keeps them, and how safe it is.

Firefox allows you to set a master password under Edit → Preferences → Security tab → Set master password and then set it, to prevent accidental access by anyone who can use the device. However, once used, it stays active indefinitely. If you may leave your device unattended, then make sure you close Firefox first.

For Chrome, and possibly Chromium, there are some add-ons that can save your passwords under a master password. The browser does not seem to offer the feature.

E-mail

E-mail messages do not magically arrive at your machine, but have to be fetched from the mail server that supplies your e-mail address. To access this also needs a password. If you access your e-mail via a website, then the browser sees this is just any other website, and can keep your password for you. Like browsers, if you may leave your device unattended, then ensure the mail client is closed.

But if you use an e-mail client (Thunderbird, for example) then it can keep them all for you for the purpose of contacting the servers and downloading the messages. But you would need to enter all the passwords for each machine you are running the client on.

How to keep your passwords

With so many passwords, and it is ***not*** a good idea to use the same one for everything, the question arises as to how you can keep them. Remembering them is not an option unless you have an exceptional memory. There are various methods, choose one that suits your circumstances.

It is worth pointing out here that if you save all your strong passwords in some sort of safe, then it is not necessary to use a really strong password on the safe, since it is used only by you, and any person wishing to obtain the passwords, must get physical access to it. So choose an easily remembered password as your master to the keyring, or safe, where all the others are. This obviously does not apply if you store them in a more publicly accessible place, like the cloud.

Remote access

If you have several devices, or you want to access your data from remote locations, then you will need your list of passwords in some form accessible to you each time. You can either do this by taking a mobile memory stick with you and looking them up each time. Or you can use some cloud storage to access them. There are now a number of synchronisation services that will automatically

transfer details of passwords and many other things (like address books) that you could use, provided that you are satisfied with the security of the service. Do you trust the service provider, whether it be Apple, Ubuntu, Google, Amazon, or any of a number of other places? Is the data encrypted when you place it there? Can the service provider decrypt it?

But you need to bear in mind that any device may be lost or stolen. Does the finder have access to all your keys? In other words, it is preferable to choose a method that requires a password to unlock access to the keys every time a key is used, which is tedious, but necessary if you have security in mind.

Programs that promise to keep them safe

These are known as wallets, vaults, or keyrings. Some programs (like Google's Chrome or Chromium browser) will seek out an existing keyring program you may have installed, and will use that. Others, like Firefox and Thunderbird will keep them locally within their own data. Other programs can link to browsers automatically, like Lastpass.

Among the specialised wallets, the free ones generally only work on a local machine, and the data has to be carried on a separate device, like a USB stick, when moving to another device. Several companies provide services that can be accessed remotely, or can synchronise between devices, but these features are generally available only to subscribers.

There is a fairly recent list of reviewed password managers at :
http://www.techradar.com/news/software/applications/8-of-the-best-linux-password-managers-916152

Some of these are available for non-Linux systems as well.

But I disagree with the order of their recommendations; in any case, these four look worth further investigation if you want to pursue it:

KeePassX: https://www.keepassx.org/
GPassword Manager: http://sourceforge.net/projects/gpasswordman/
Password Safe: http://sourceforge.net/projects/passwordsafe/ or http://pwsafe.org/
MyPasswords: http://sourceforge.net/projects/mypasswords7/ or http://www.mypasswords7.com/

All of these claim to be cross platform and will run on Windows. For Linux users, some, but not all, may be available in your distro's repository.

Conclusion

When considering how you manage your passwords, you have to think how important it is, and who you trust.