computer security

LastPass password manager

a short guide

Tom Gijselinck
tomgijselinck@gmail.com

1st August 2014

Often you have to use a username and a password to use a website. Examples are dropbox, hotmail, facebook, etc. For security reasons it is necessary to use a different password for each website. And although not always required, it is best to use strong passwords. Of course it is an impracticable task to remember all those complex passwords. And that's where LastPass can help us. With LastPass you can save all your passwords in a vault. Each time you have to log into a website, you can use LastPass to fill in the form. The only thing you need to remember is your master password.

This document describes how to install and use the LastPass password manager on PC.

Contents

Abstract 1

How to use this guide 2

1 An introduction to LastPass 2

2 Installation 3

3 Usage 3

3.1 Adding website login forms to your vault 3

3.2 Using LastPass to log into a website 4

3.3 Adding passwords to your vault 5
3.4 Generate random secure passwords 5
3.5 View and edit your passwords 6

4 Limitations **6**

5 Backup your LastPass vault **7**
5.1 Exporting your LastPass vault 7
5.2 Encrypting your LastPass backup 8
5.3 Using your backup 8

6 Epilogue **8**

References **10**

How to use this guide

Not every reader needs all information presented in this guide. Therefore we suggest some guidelines how to read this document.

An introduction to LastPass can be found in section 1. If you are only interested in installing and using LastPass straight out of the box, you only need to read section 2, subsection 3.1 and subsection 3.2. If you are also interested in security and strength of passwords, read subsection 3.4. Should you need to add to or edit manually passwords in your vault, see subsection 3.3 and subsection 3.5. In section 4 the limitations of LastPass are covered. To backup your LastPass vault, you can find instructions in section 5. Finally, section 6 concludes this document.

1 An introduction to LastPass

LastPass is a *password manager*. LastPass remembers your passwords for you by storing them securely on the internet in your *LastPass vault*. Your vault is encrypted with one *master password*. This is the only password you'll ever have to remember.

You can access your vault on the internet. You only have to fill in your master password and then you have access to all your passwords. LastPass automatically detects website login forms. Once a password is saved, the next time you have to log into that website you can use LastPass to fill in the login form. In short, LastPass is a very handy tool that remembers your passwords so you don't have to. In the following sections we will explain how to install LastPass and how you can use it on your computer.

2 Installation

For downloading and installing LastPass we refer to the user manual found at https://helpdesk.lastpass.com/getting-started/downloading-and-installing/ which contains all the necessary steps.

3 Usage

Once LastPass is installed, we can begin using it. We will explain the following applications of LastPass

- adding website login forms to your vault
- using LastPass to log into a website
- adding passwords to your vault
- generate random secure passwords
- view and edit your passwords

We will now cover each of these topics individually.

3.1 Adding website login forms to your vault

Introduction Often you have to use a username and a password to use a website. Examples are dropbox, hotmail, facebook, etc. For security reasons it is necessary to use a *different password for each website*. And although not always required, it is best to use *strong passwords*. These are passwords you wont find in a dictionary, have a length of 13 characters or more and contain lower case characters, upper case characters, numbers and special characters. An example of a good password would be `79!&amXzf6R&@`. [4]

Of course it is nearly an impracticable task to remember all those complex passwords. And that's where LastPass can help us. With LastPass you can save all your passwords in a vault. This vault is protected with a master password chosen by you so that only you can access it.[1] Each time you have to log into a website, you can use LastPass to fill in the form. The only thing you need to remember is your master password.

In the previous sections we've already set up your LastPass account protected with your master password. Now we will add a website login form. First we will explain how to add a website login form and then we will illustrate this with an example.

[1] Consequently, it is of utmost importance to choose a good master password that you can store in a safe place (your memory would be best).

Adding a website First you need to be logged in your LastPass account. For this to be true, you only need to have installed LastPass and filled in your master password. Navigate to the website you need to log into. Access the page where you usually fill in your username and password, and fill in the required fields (username and password). Hit the enter key or Login button to log into the website. Once logged in, LastPass will suggest to save this new website login form. Accept this by saving it to your LastPass vault. From now on you'll never have to manually fill in this password and username again because LastPass will do this for you.

Example As an example we will create a Dropbox account for a fictional person named John Doe [johndoe@mailinator.com]. First we navigate to the Dropbox homepage, `https://www.dropbox.com`. There we hit the sign up button to create our new dropbox account. We use John as first name, Doe as last name, johndoe@mailinator.com as email and `79!&amXzf6R&@` as our random secure password. Once filled in, we hit the sign up button. If everything went all right, LastPass detects our new login credentials and suggests to save it to the LastPass vault. Hit save new website to save your username and password to your vault. A new window will appear where you can modify the name of this login form and if you want you can add this form to an existing or new group[2]. Finally hit save and your website will be added to your vault. The next time you need to fill in the login form of this website (in our example, www.dropbox.com), you can let LastPass fill in the username and password. For more details on logging into websites using LastPass , see subsection 3.2.

3.2 Using LastPass to log into a website

Once we've saved a login form of a website to our LastPass vault, we never need to manually fill in that form again. We can just use LastPass for filling it in for us. We will now explain how you can use LastPass for logging into websites.

First you need to be logged in your LastPass account. For this to be true, you only need to have installed LastPass and filled in your master password. Once logged in, it is very easy to let LastPass fill in login forms for you. Just navigate to the website you need to log into. Access the page where you usually fill in your username and password, but instead of filling it in yourself, you can let LastPass do that for you. Possibly LastPass already filled in your credentials, but in case not, just hit the grey star-like LastPass logo in one of the form fields and select your saved login form. LastPass will then fill in your username and password and you only have to hit enter or the login button to log into the website.

However unlikely, it is possible that LastPass wont recognize the website login form. In that case you need to access you LastPass vault, search for the saved website form and

[2] Groups are user defined collections of login forms.

copy the password of that form and paste it in the required field. This is cumbersome, but it will not often be necessary to use this method. Accessing your LastPass vault and viewing your saved login forms is explained in subsection 3.5.

3.3 Adding passwords to your vault

In subsection 3.1 we've explained how to add website login credentials to your LastPass vault. We let LastPass automatically detect our (new) account. But in case you yourself want to add a password to your vault (e.g. you want to add a password of a non-website application), you need to add it manually. We will explain how to do that in this subsection.

First hit the red LastPass logo in the top right corner of your browser. In the menu that appeared, select Tools and Add Site. Then you get a warning which tells you that LastPass automatically detects and saves login forms. But because we're not dealing with website login forms here, we just hit yes to dismiss the warning. In the new window that appears, we can fill in the username and password, and if you want you can add some notes. Hit ok to save the password to your vault. Next time if you need those credentials, you can access your LastPass vault and view your newly saved password to use them. See subsection 3.5 for more info.

3.4 Generate random secure passwords

We already mentioned that it is important to use different and difficult passwords for each website. Next to the fact that it is difficult to remember those passwords, it's also not an easy job to forge such good passwords. For both problems LastPass offers the solution. In LastPass it is possible to generate secure and random passwords. In this subsection we will explain how you can do that.

To generate a secure random password with LastPass , first hit the red LastPass logo in the top right corner of your browser. In the menu that appeared, select Generate Secure Password. In the new window that appears we can generate a random password. By default the random generated passwords are pretty good. But if you want to have truly secure passwords, you'll have to fine-tune the password generator. For this you'll have to tick the check-box Show Advanced Options which let you modify the settings of the generator. For the necessary password strength tick the following check-boxes only: A-Z, a-z, 0-9, Special.[3] Subsequently set Password Length to 13 or higher. This will generate passwords that fulfil the minimum requirements for password strength. [4]

You can use the generated passwords for new accounts or use it as a replacement for old, bad passwords. It is recommended to use different and secure passwords for all your

[3] The best result is when the number of possible characters is greatest and each character has the same chance to be chosen. For more information about password strength, see the excellent wikipedia article at https://en.wikipedia.org/wiki/Password_strength.

accounts on the internet. If you have old passwords that don't fulfil the requirements for a secure password, you are encouraged to use the LastPass password generator to replace the bad passwords with good passwords. With LastPass this is easily done.

3.5 View and edit your passwords

If you're logged into your LastPass account, you can view and edit all your saved login forms in your LastPass vault. To do this, you need to hit the red LastPass logo in the top right corner of your browser. In the menu that appeared, select My LastPass Vault. A new tab will be opened in your browser showing your LastPass vault.

To search a website, type the website in the Search Vault field at the top of the page. For example, if you want to view your Dropbox username and password, you type in dropbox. The results are shown below the search field. Hit the grey pencil logo of the website you need to view and edit it. A new window will appear where you can view all the saved information. To view your password you have to hit the grey eye icon. If you only need your password, you can just right-click the website in the result list and select Copy Password. Then you need to right-click again in the field where you want to fill in the password and select Paste. Your password will be filled in that field.

4 Limitations

Like most security systems, LastPass is not flawless.

- On may 3, 2011, LastPass discovered an anomaly in their incoming and outgoing traffic which could have been a potential security breach. However, administrators could not determine the root cause of the anomalies and there have been no verified reports of user data loss or password leaks. To adress the situation, LastPass decommissioned the potentially breached servers so they could be rebuilt. [2]

- In february 2011, a security hole was discovered by researcher Mike Cardwell. LastPass solved it within hours but there was disagreement over the severity. Cardwell stated that people should be very concerned but LastPass reported that there was no evidence of exploitation. LastPass however implemented in addition some extra security features. [2]

- In the summer of 2013 researchers at the university of Berkely discovered multiple vulnerabilities in diverse features in web-based password managers like LastPass , RoboForm, My1login, ... They stated that an attacker can learn a user's credentials for arbitrary websites because of those vulnerabilities. The root causes are diverse and their study suggests that it remains to be a challenge for the password managers to be secure. The researchers first revealed their discoveries to companies of the password managers for giving them a chance to solve the vulnerabilities. Most of them, including LastPass , reacted quickly and closed the security holes. [3] [5]

As you can see, LastPass is not perfect and there have been issues. Although possible, there's never been a prove that user data was stolen from the LastPass database. Also, because password managers like LastPass store all your passwords at one location, they are a good target for hackers. One vulnerability is enough to lose all your passwords. The bottom line is that you should take into account that LastPass is not perfectly secure, but the chances of data theft are rather small. For the average user LastPass offers enough security. However, to prevent yourself from losing all your passwords in your LastPass vault you should create a backup. This is explained in the next section, Backup your LastPass vault.

5 Backup your LastPass vault

There are multiple reasons why you should backup your LastPass vault

- you forget/lose your LastPass master password
- your data on the LastPass servers is lost (security breach, fire, natural disaster, ...)
- you have no internet access but you need your passwords

Creating a secure backup of your LastPass vault consists of two steps

1. export your LastPass vault as a CVS file (unprotected)
2. encrypt the unprotected CVS file with a password

The second step is very important because otherwise your passwords can be read by everyone who has access to your backup.

5.1 Exporting your LastPass vault

The first step is downloading all your passwords from the LastPass server to your computer. To do that you need to log into your LastPass account. Once logged in, hit the red LastPass logo in the top right corner of your browser. In the menu that appeared, select Tools, Advanced Tools, Export To and select LasPass CVS File. LastPass asks your master password and after you've entered it the CVS file will be downloaded.

5.2 Encrypting your LastPass backup

Once you've stored your backup on disk, **it is very important to protect this data**. Otherwise everyone who can lay their hands on your backup, has full access to all your passwords. If you use the pgp encryption program, you can use this to encrypt your backup. Otherwise we recommend using an encryption program which implements the AES/Rijndael[4] encryption algorithm. One such a program is AES Crypt[5], which is free and open source. We refer to the documentation for explanation on using these programs.[6] Note that PGP is a bit difficult to master but has very powerful capabilities. AES Crypt is an easy to use program and thus recommended for the average user.

5.3 Using your backup

You can use your backup for offline access to your passwords or to recover from data loss on the LastPass server. Reading you LastPass backup is easy, you can simply open the CVS file in a spreadsheet program like MS Office Excel. You could also use a text editor like notepad to read the file, but using a spreadsheet program gives you the advantage of an easy to read presentation. See http://office.microsoft.com/en-us/excel-help/text-import-wizard-HP010102244.aspx?CTT=5&origin=HP010099725 for importing a CVS file in Microsoft Excel. If you use other programs, search the accompanied documentation for *importing SVS files* for the necessary steps.

In case of data loss on the LastPass server, you can import your backup into your LastPass vault. Just follow the import wizard in LastPass . To start this wizard, hit the red LastPass logo in the top right corner of your browser. In the menu that appeared, select Tools, Import From, LastPass and select Import. Then you select your backup on diska dn hit Open.

6 Epilogue

In this document we've explained how to install and use the LastPass password manager. We've only included the essential elements. Of course LastPass offers a lot more functionality. If you are interested in additional information, we recommend the LastPass user manual which you can find at https://helpdesk.lastpass.com/ (the print version can be found at https://helpdesk.lastpass.com/full.pdf).

[4] AES (Advanced Encryption Standard) is the current industry standard for encryption. It is based on the Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, both graduates at Katholieke Universiteit Leuven, faculty of Engineering. [1]

[5] http://www.aescrypt.com/

[6] Gpg4win (pgp implementation for windows): http://www.gpg4win.org/doc/en/gpg4win-compendium.html,
AES Crypt: http://www.aescrypt.com/documentation/

We hope everything is explained in a clear and not to detailed manner so you can quickly begin using LastPass without any hassle. We strongly encourage to begin using LastPass for creating and storing strong passwords for your different internet accounts. In these days of modern society where almost everything is connected to the internet, we think it is very important to be conscious about our privacy which is ultimately determined by how secure we protect our online information. In the first place it is very important to use difficult and different passwords for your online accounts. The LastPass password manager can help you with this task.

References

[1] *Advanced Encryption Standard.* URL: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard (visited on 15/07/2014).

[2] *LastPass. Security breach.* URL: https://en.wikipedia.org/wiki/Password%5C_strength%5C#Bit%5C_strength%5C_threshold (visited on 12/07/2014).

[3] Z. Li et al. *The Emperor's New Password Manager: Security Analysis of Web-based Password Manag.* Paper. University of California, Berkely, 2013. URL: http://devd.me/papers/pwdmgr-usenix14.pdf (visited on 12/07/2014).

[4] *Password strength. Bit strength threshold.* URL: https://en.wikipedia.org/wiki/Password%5C_strength%5C#Bit%5C_strength%5C_threshold (visited on 29/06/2014).

[5] *Wachtwoordmanagers als LastPass maandenlang kwetsbaar geweest voor hackers.* Dutch. URL: http://www.pcmweb.nl/nieuws/wachtwoordmanagers-als-lastpass-maandenlang-kwetsbaar-geweest-voor-hackers.html (visited on 12/07/2014).