How to store SSH passphrases in LastPass

W. Adam Koszek

Koszek ORG

wojciech@koszek.com

2022-10-05T17:48:24Z

Passwords are a terrible authentication mechanism. Even though this mechanism exists in computer systems for years, frankly there aren't too many solutions to address the password problem. If you've dealt with more than three different APIs I bet you must have committed confidential data to GitHub at least once. SSH with its keys isn't any better, and is used in more critical places.

Below I attempt to address the SSH passphrase problem. My setup is based on LastPass. LastPass stores a binary bundle with all your passwords in the cloud. Bundle is fetched on your machine, and you decrypt it with a master password. During decrypting phone-based 2-factor authentication is used for increased security. If your master password is weak, you're baked. Upon decryption you have an access to all your passwords, including SSH passphrases. The script automates the management of ssh-agent and key adding.

Quickstart

Visit the: https://github.com/wkoszek/lastpass-ssh

How to use it?

Before we start, full disclosure: LastPass has had 2 security incidents that I know about, plus they've been acquired recently, so it's up to you to decide if you're willing to invest your time in this solution. I just haven't found anything better than that. Reports about how LastPass handled the incidents made me feel they know what they're doing. Described in this article is a open-source command line client which they published and support.

How to install?

Install `lastpass-ssh` and `lpass` client:

```
sudo brew install lastpass-cli
sudo gem install lastpass-ssh
```

Setup

You make yourself an "SSH" subfolder in the LastPass "Secure Notes" and add secure notes there. Each note has a name and a passphrase. The name corresponds to the filename of the SSH key file, and the passphrase is its key's passphrase.

Example: if you have a key like myrepos in `~/.ssh/`, then the name of the Secure Note would be `myrepos`.

How to run

Type:

```
lastpass-ssh
```

It will poll the "Secure Notes/SSH" folder and for each note of name "A", it'll try to perform `ssh-add ~/.ssh/A` with an appropriate passphrase.

You can change the location of keys by passing `--keys-path=<where-you-have-keys>`. By default all keys are added. You can change this behavior by passing `--key=KEYNAME` option, where `KEYNAME` is the name of the key file you want to add.

Details

Internally the lastpass-ssh script is based on the lpass command line tool provided by LastPass guy themselves.