Account Password Security: Advanced Edition

Feb 12th, 2014

Just the Steps

What follows is a discussion on how to use file sync software like Dropbox and encryption software like TrueCrypt to securely and conveniently access an offline password database like those created through KeePassX on every device. The idea is to create a small encrypted file container with TrueCrypt, place the password database inside of it, and sync the file container using Dropbox. Then on any device access the file container in Dropbox, decrypt and mount it with TrueCrypt, and load the password database with KeePassX; this only has to be done once until a device is shut down. The result is a highly secure and convenient way of managing online account credentials.

A thorough look with all the details follows.

I Have a Local Password Database, Now What?

Suppose you followed my advice in the Basic Edition and have created an encrypted KeePassX password database that now contains all the credentials and security questions for your online accounts in one easy-to-use bucket. This is a local solution so the password database resides on your computer, but maybe you have multiple computers and mobile devices. Also, as I mentioned there this does place all your eggs in one basket so to speak so securing that basket is critical. There's a nice and secure way to fix these problems without resorting to trusting a closed source platform like LastPass to manage both their and your security. I propose using two applications to help accomplish this task: Dropbox and TrueCrypt.

Dropbox

Dropbox is a cloud storage and file sync service. For the uninitiated, you download the client software, create an account, and a special folder called Dropbox will be placed in your computer's home folder. All files placed in here will be synced and stored online on Dropbox's servers (Dropbox claims to encrypt the transfers and storage), and any other devices you install Dropbox on will have access to these same files.

Dropbox was the first such service to really catch on due to its simplicity, and I believe it's still the best for a few reasons:

- It's fully cross-platform (they even support installation on a headless server)
- Its sync times are faster than the other cross-platform alternatives
- It's a very hands-off solution; all the magic happens without your intervention

That being said some alternatives are Google Drive, Microsoft SkyDrive, and Box. None of these meet all three points I listed above in my experience.

Whatever your choice (I'll assume Dropbox for the remainder but the procedures are the same), these sorts of services will clearly solve our problem of having a local password database on only one device in the easiest manner possible; just use the service to sync the database and use KeePassX to load it wherever you go. However, since Dropbox requires trusting your data to Dropbox's servers there is a degree of risk and concern for privacy despite their use of server-side encryption; there have been a few snafus but no reports of data theft. Regardless, it would be ideal not to have to trust your collection of online account credentials to a third party's security; as we've seen before perfect security doesn't exist, and the more layers we can add without sacrificing much convenience, the better. This leads us to…

TrueCrypt

TrueCrypt is open source cross-platform encryption software that can be used to, among other things, create strongly encrypted file containers. These containers appear as a regular file with size equal to the storage space allocated to the container and, once mounted and decrypted, allow the user to store and access any data inside. In case you're unfamiliar with the software you may consult the official documentation or my overview of TrueCrypt; while it's reasonably straightforward there are some considerations such as choosing between standard volumes and hidden volumes that employ plausible deniability methods.

Immediately it's clear how TrueCrypt can be used to alleviate the problem of placing all of our trust in the hands of Dropbox. Instead of syncing the encrypted password database which, if stolen due to a Dropbox security lapse, might be subject to some vulnerability in KeePassX encryption or a brute force attack if you used a weak password (memorize a strong password instead!), one can sync an encrypted TrueCrypt file container which holds the KeePassX database.

Putting it Together

Now we've seen all the pieces of this scheme for conveniently securing your online account credentials without needing to completely trust a single third party: KeePassX, Dropbox, and TrueCrypt (or your preferred equivalents). This is how it all fits together:

Setup

1. Gather all of your online account credentials into an encrypted password database using software like KeePassX, ideally using it to create maximum length random passwords for each account.
2. Create an account for Dropbox or a similar file sync service and install the client software on all of your devices.
3. Create a small encrypted file container with TrueCrypt or equivalent software, place the KeePassX database inside of it, and move the file container to Dropbox to be synced.

Every Day Use

1. Any time a particular device is rebooted, mount the TrueCrypt file container.
2. Open the password database found inside the mounted file container using KeePassX.
3. Any time you need to log into an account, copy and paste the credentials using KeePassX (by default

these credentials are cleared from the clipboard after 20 seconds).

By the Numbers

- Number of one-time steps each time a device is rebooted: 2
- Number of passwords to remember: 2
- Effort to take to log into any of your accounts: click (to copy username), paste, click (to copy password), paste

Concluding Remarks

When most people hear words like encryption and security they think of things that get in the way of doing what needs to be done — things that complicate their life. I would simply ask whether the reality laid out in the **By the Numbers** section above is more or less complicated than memorizing any number of usernames, passwords, and security questions, sometimes being required to change them frequently, and possibly resorting to sharing credentials between accounts.

It's not often one can enhance both security and convenience at the same time but I suggest this is one of those times.

Posted by Isaac Velando Feb 12th, 2014 encryption, infosec, passwords

« Not Just the NSA: Privacy Breaches Closer to Home What's Different About Linux: Programs »

Comments

 ("shell scripting" or most commonly "bash scripting" if you'd like to Google). I think whether it's for OS  manager I use - Sticky Password - http://www.stickypassword.com

Recent Posts

- What's Different About Linux: Programs
- Account Password Security: Advanced Edition
- Not Just the NSA: Privacy Breaches Closer to Home
- Password Security Failure: When Websites Don't Get It
- The @N Hack: Why Absolute Security is a Myth

GitHub Repos

- twitter-blog-broadcaster

  A Twitter bot written in Python meant to broadcast a site's blog posts or similar resources through nicely hashtagged posts (not designed to be followed)

- dotfiles-general

  A collection of assorted dotfiles not directly tied to the desktop environment or window manager

- btrfs-backup-scripts

  A collection of scripts intended for both periodic and manual use for creating backups with a btrfs filesystem

@iwvelando on GitHub