Juan Zepeda

May 01, 2014

COMP 424

Professor Noga

LastPass Security

Introduction

I have been using LastPass for over three years now. LastPass is a password manager that stores user's passwords for all the users' log-in sites. This avoids the need to have to remember all your passwords. Initially, I used RoboForm, another password manager, because I was becoming informed that it was not a good idea to have one password for many sites. It was the first product I had encountered that could store my data offline. Before I started to use any password manger, about five years ago, I had one or two simple passwords for all my sites. One password I had was actually "123456". Today I now know is really weak.

The Problem

In today's world, we are all dependent on passwords. This is how we authenticate with a bank, social media, and entertainment website. This dependency on a password relies on something we "know" for security. The problem with the password is that every security dependent website asks for one. They have their own rules on the length, uppercase or not, at least one number, etc. A user must create a secure password with a size length greater than 10 with mix of uppercase lowercase and include numbers and symbols. Also to mention the obvious, the user must remember it! But there is a problem with having a strong password through all the users' sites.

When having one password for every site, the user trusts the website server to hold and securely store the password and not share it. This trust can be violated in many ways. First, should the user trust the past, present, and future employees that maintain the website server? How does the user know that they won't look at the user's data, steal it or sell it? Second, if the user does trust the employees, who says the server will never get hacked? A perfect and recent example is the Heart Bleed bug that leaked server RAM in 64KB chunks of data, potentially revealing the user's website account password. We can see it is not a good idea to have a common password for all the websites.

To avoid having a common password on all websites, have a unique strong password for every website. Can one remember all these passwords though? Generally, the answer is no. That is where LastPass solved my problem, of having strong unique passwords for every website that I login into. LastPass remembers them, I don't.

What is LastPass?

LastPass is a password manager that synchronizes across multiple browsers and computers. LastPass securely stores and manages all the users' usernames and passwords locally. It provides a Trust No One (TNO) solution. TNO is end-to-end encryption where trust is not given to a third party with the user's data. The user's data gets encrypted locally on the client side and a big "blob" of data is stored on the server. This avoids the third party from snooping or accounts getting hacked with the user's sensitive data. If a hacker gains access to the "blob" of data, the hacker must still decrypt the data. LastPass simplifies the whole process from generating new strong unique passwords, storing passwords, and auto filling a login after authenticating the user. The only thing the user needs to remember is one strong master password. That is it.

How the encryption works client side

LastPass does the majority of its work on the client side. It stores all the users' username and password locally before sending it off to their server. All the encryption is done locally so what LastPass servers receive what looks like random noise. In reality, it is the user's encrypted data. This noise is produced by encrypting data using the AES-256 cipher with a key and transmitting the "pseudo random noise" to their servers over SSL. LastPass cannot decrypt the data on their servers because they never store, or have they decryption key at any point in time.

The AES-256 decryption key is generated by concatenation of the email and master password of the user for the LastPass account. They salt the previous concatenated string of the username and password and run through a one-way function, a SHA-256 hash. This outputs a 256-bit key. This key is non-reversible. Nobody can take the key and get back the user's username and password. This key encrypts and decrypts data that LastPass stores for the user. LastPass holds the user's encrypted results on their servers.

User Authenticating to LastPass

Since LastPass does not store the key to decrypt data and only stores a blob of encrypted data, how does it authenticate the user as the owner of that data? LastPass takes the key, generated by the SHA-256 key and concatenates it again with the user's password. This concatenated string is then passed into SHA-256 to produce another key. This key is then used as unique ID of the user, which does not reveal the original key to decrypt the data nor the user's password. Once the new key has been generated the username and the unique id is sent to LastPass to authenticate the user.

How the encryption works Server Side

On LastPass's servers the user's encrypted data is stored. Since they don't have the key to decrypt the "blob" no employee or malicious hacker can steal any sensitive information. If they manage to steal anything they cannot decrypt it nor make sense of it since LastPass has no key. Simply, LastPass acts like a cloud sync storage provider for the users encrypted data.

Since LastPass only stores encrypted data, it does not store the user's unique id that was generated to authenticate the user. The unique id is sent over but only to be concatenated with another previous 256-bit string that was uniquely made for the user, by the user at the creation of the LastPass account. The concatenation of this 256-bit string is then passed through another SHA-256 hash that outputs a user key. This user key is compared to their stored key of the user and allows them to authenticate the user.

What if LastPass disappears?

LastPass is storing and syncing all your encrypted password data on their servers, which can bring up scary thoughts because of the danger of them going bankrupt or any other reason. Can we rely and depend on them? What is great about LastPass is that if they do go away a user may still grab their data. LastPass stores and syncs a local cache of the encrypted data with the browser and platform plug-ins. The user can locally decrypt the data and access their username and passwords.

Conclusion

LastPass through its technology has proved to be a flexible and secure source for their users to store their usernames and passwords. Users can easily generate a strong unique password for every website without having to remember all of their passwords. A user can simply remember one strong master password for their LastPass account. When signing into any website that requires the user login LastPass auto fills the fields and logs them in.

References

1. http://blog.lastpass.com/2010/07/lastpass-gets-green-light-from-security.html
2. https://lastpass.com/whylastpass_technology.php
3. http://twit.tv/sn256
4. http://www.techrepublic.com/blog/it-security/lastpass-is-it-the-password-manager-for-you/3291/
5. https://www.grc.com/sn/sn-256.htm