Security Whitepaper

February 2014

SpeedyPassword
1837 Fort Street
Victoria, BC
support@speedypassword.com

SpeedyPassword makes it easy to manage passwords. Utilizing a password generator, military-grade encryption, SSL connections, and other security measures, SpeedyPassword protects your passwords, accounts, and information. This document provides a technical overview of the security practices and principles SpeedyPassword uses to protect your passwords.

Key Features

- The Master Password is a key to SpeedyPassword's success in protecting passwords. Used to encrypt all of other passwords, the Master Password is so important that SpeedyPassword team does not know it or store it.

- To assist in situations when users just cannot remember their Master Password, SpeedyPassword employs a Recovery Image. When setting up an account, users can upload an image to be used in case the Master Password is forgotten. If you need to recover your Master Password, you just upload that exact same image.

- All data is encrypted and decrypted on the user's computer (Client-Side Encryption). This means no unencrypted data is sent to the SpeedyPassword servers.

- Encryption is done using AES-256 encryption. AES is considered unbreakable with modern computing powers.

Storage of User Data

SpeedyPassword does not store unencrypted user information on its servers. All information sent to the SpeedyPassword servers is encrypted using AES-256 encryption. The Advanced Encryption Standard is an encryption algorithm that is trusted by banks, the U.S. government, and the military. AES-256 uses a key size of 256 bits to encrypt data.

Passwords and data are only decrypted on the user's computer. All data stored locally, on the user's machine, is encrypted.

For the use of a Recovery Image, a hash (basically a value) is generated using SHA1. This value is stored on the SpeedyPassword server with a thumbnail of the Recovery Image. When you login, the recovery information is stored on the client. If you forget your password, you can recover on a client that you have logged in on, and only one you have logged in on previously. All recovery is done client side. No one can try to recover an account unless they are physically on a computer the account has been used on previously. When the user chooses the exact Recovery Image, the previously created hash is utilized as an encryption key to recover the Master Password.

User Sign In and Authentication

Users sign in to SpeedyPassword using their Master Password. The Master Password is never transmitted over the Internet. Instead, authentication is done using advanced security methods.

Hashes are created from the Master Password for authentication. The cryptographic hashes are generated using the industry standard Password-Based Key Derivation Function 2 (PBKDF2) with thousands of iterations. A salt is used during hashing to make it even tougher for hackers to crack. A salt is additional data that is applied during hashing. A 16-byte salt is the server salt length, which uses SHA256 server side for the hashing.

The first hash is never stored anywhere. The second hash is sent to our servers to verify the the users credentials). When received by our servers, it is hashed again, using SHA256, and that is what is stored.

When a user signs into a SpeedyPassword account, the Master Password is authenticated using the second hash. Once the Master Password has been authenticated, the first hash is used to decrypt passwords on the client side.

Password Recovery

If a user forgets their password, they can use a Recovery Image to retrieve their Master Password. The image they use must match exactly the Recovery Image the user uploaded previously.

A SHA1 hash is generated from the Recovery Image. This hash is used as an encryption key to recover the Master Password. In regards to the Recovery Image, SHA hash is created by an algorithm that creates a string out of the image's data. SHA1 is a cryptographic hash function, meaning it is one way, and the original data is not retrievable from the hash.

As the Recovery Image is the only way to retrieve the Master Password if it is forgotten, it is highly recommended that you back up the Recovery Image. No matter where it is stored, it needs to be easily accessible if needed to recover the Master Password.

Communication

As stated previously, all data sent to and from the SpeedyPassword servers is encrypted using the AES-256 encryption. The AES algorithm uses the Stanford Javascript Crypto Library, which was designed to be a fast, secure, powerful cross-browser library for cryptography.

In addition to AES-256 encryption, communication between the user's computer and SpeedyPassword is done with yet another layer of encryption – SSL. All of your passwords and information are sent using the Hypertext Transfer Protocol Secure. HTTPS (indicating SSL) is often seen at the top of web browsers when on banking or shopping site. This means the website is using the standard for secure Internet transactions.

In addition to all of safeguards, SpeedyPassword locks out users if failed login attempts are made. This prevents brute force attacks. After someone tries five times to login, the account is locked for 15 minutes. To stop password theft attempts, a user can only try five times in 20 minutes to recover their password. After that, the SpeedyPassword account is locked for 15 minutes.

Server Hosting/Network Architecture

All SpeedyPassword servers are located in highly-secure data centres. These centres are protected 24 hours a day, seven days a week by trained security guards and electronic surveillance. SpeedyPassword proudly using Amazon Web Sevices. For more on security of this service, please see http://aws.amazon.com/security/

In addition, the SpeedyPassword database is only accessible internally.

Accessible User Experience

While SpeedyPassword has strived to create an extremely secure password manager, the team also has focused on usability. Users want programs like SpeeyPassword that are secure, but also easy to use. Because of its intuitive interface and easy-to-follow workflow, users will likely not even be aware of all the processes and cutting-edge security methods previously described going on in the background. It is this meshing of convenience and security that SpeedyPassword has been designed for.