Salt Management

A unique take on making passwords more secure.

We developed this project because we believe that is more secure to remember passwords than having a password manager to do all the work for you. In addition, it has been proven that people suck at making up passwords. This security project addresses that issue by making any password much more secure.

This project will generate an 8 character string that includes random characters(0-9,a-z,A-Z,special characters) for every username you want with any site. You can have the option to append this randomly generated salt to your password to make it more secure. Ideally, service providers should salt your passwords for you already (*cough* Yahoo *cough*), but it won't hurt to have your password double salted if they do already!

All the passwords and according usernames are encrypted using SHA3 and AES and stored locally. For each pair of username, domain name, and salt, we will store three objects with a key and a value locally on the browser. We append username,string and domain as a string and use SHA3 to hash it to a 256-bit hex string as the keys where the string is "IV", "KEY", or "salt". We store a randomly generated hex string IV, a generated AES key, and the encrypted salt as the values. All the keys and values inside the database have the same length, so it's impossible to distinguish IV, AES-key and the salt. Therefore, if the database is breached, and there are enough pairs stored, the hacker will have a hard time bruteforcing to figure out the salts.

Compared to other password managers like LastPass, we believe this is more secure because one isn't bounded by a single, master password that grants access to all passwords one adds to the manager. If the master password is spoofed, hackers can get all the password information easily. However, our password salt manager will not have that risk. Hackers will have to gain access to the user's local machine because everything is encrypted and stored locally, and guess the username and the domain name correctly in order to get the salt. This salt management software is all local; we do understand it will be a pain to log into multiple

devices. But there's a similar inconvenience with 2FA (mobile) applications. Perhaps in the future we will develop a mobile application that serves this purpose.

This is also secure because this manager has no way of knowing what your password really is, and even if they somehow find out the salt for the users, the users still have the other half of the password only he knows, thus making it much harder for the hackers to find out the complete password.

How to use this

This project is an add-on and is tested to work on FireFox. To add this, type in "about:debugging" without quotes in the url bar. Then click "Load Temporary Add-On", navigate to the .json file and open that up. You will see a key icon show up in the top right corner. Navigate to any website and you will see a field to put a username and three options "New Password", "Show Password", and "Delete Password" when you expand the add-on window. The popup will output error message if the username is empty or more than 30 characters. If you press new password, the password salt manager will generate a 8-bit random salt paired with the username you put in and the domain you are on right now and encrypt it and store it locally. You can then copy and paste the salt to your password. If there is already a password salt associated with the same domain and username, the salt manager will prompt to ask you if you want to replace the existing salt. You should only do that when you are changing your password because the old salt can not be recovered. Click "Show Password" will fetch the data stored locally and decrypt the salt to show the password salt associated the input username and domain, and output error message if there isn't one. Click "Delete Password" will delete the salt associated with the input username and the domain, so use it with caution.