**EMCS2020: Advanced Topics in Computer Security**

Post-Work Assignment: Auto-Fill in Password Managers

Brian Russel Davis, [brian\_davis@brown.edu](mailto:brian_davis@brown.edu)

***What are the two types of password autofill mentioned in the papers and how do they differ?***

One type is “automatic autofill” or basically autofill that ***does not wait*** for user interaction.

Another type is “manual autofill”, in this case, the password manager waits for the user to interact with the page before filling in the password. Since the “automatic autofill” doesn’t wait for user interaction as soon as the site is loaded in the browser the password manager fills in the user’s password in clear plain text that javascript can read. Manual fill, on the other hand, waits for the user to choose from a list of saved sites.

***Which type of autofill is vulnerable to various sweep attacks described in the paper and why?***

While both types of autofill are vulnerable to attacks, autofill that does **not** wait for the user interaction is more vulnerable because it may expose the user’s password in clear text to a site that the user does not intend without the user’s knowledge. In the examples provided by the researchers showed how an attacker could intercept a user request for a site, redirect to site that would contain valuable credentials, use automatic autofill to steal the credentials, and then serve up the site that the user was expecting, all in a matter of seconds without much interruption to the user. The reason this attack works is because the password manager doesn’t require the user’s interaction to fill in the password. When the password managers require the user to select the account the attack fails.

**How do the two types of autofill compare in terms of usability?**

In terms of usability, the two versions of autofill are very close. According to the study, the “automatic autofill” takes one click ( ie click the submit button ) and the “manual autofill” takes 2 clicks ( ie one to select the correct account and another to submit the credentials ). For people that are accustomed to not having to do anything, that extra click may seem like a lot of work, until they realize the risk associated with this feature.

**How would you summarize the conclusions of the paper?**

One very sad conclusion is that most companies that make password managers are not very careful with our passwords. If their job was only to give convenience then we would have very little reason to complain, but that is not the extent of their job. Passwords, in some instances, could be worth more than the money sitting in our bank accounts. Depending on the context and the user, stolen credentials can help an attacker do tremendous permanent damage. In my opinion companies like Google should be doing more to prevent these types of attacks, and they could by simply changing the way their products work.