A Different Kind of Password Manager

Alan H. Karp
Independent

Abstract

Most password managers store passwords so you don't have to remember them. That choice imposes costs on the company providing the password manager and risks on its users. Another option is to calculate passwords as they are needed. SitePassword is such a calculator that provides all the key features that users want in their password manager – remembering of metadata, synchronization across machines, and autofill capability.

1 Introduction

"Dealing with passwords is awful" is a statement few would disagree with. Password managers make the situation less awful, improving both security and usability. Basically, they make it easier for you to have a different, strong password for every site. Of course, users care at least as much about ease of use, trust in the the password manager, and the ability to get their passwords from any of their machines or when using a friend's machine as they do the strength of their passwords.

There are two kinds of password managers. The vast majority of them remember passwords and other metadata, such as userids. They make the stored passwords available from any machine by using encrypted databases and cloud storage.

Remembering passwords adds cost for the company providing the password manager for it to manage user accounts and to pay for the necessary cloud storage. It imposes risks on the user because the stored passwords can be stolen. It has also happened that companies have dropped support for their password databases, leaving users in the lurch.

The second kind, password calculators, don't need to store passwords. They combine a master password with other data to calculate a strong password for a website when you need to login. SitePassword is a password calculator designed for usability and security that supports all the features users want. Usability features are discussed in Section 3.

SitePassword remembers your settings for each site and synchronizes them across your machines without the need for user accounts or cloud storage. It does that by putting the metadata in bookmarks, which virtually all browsers synchronize across machines. Using bookmarks makes the settings available on machines that cannot install the extension, such as mobile devices. The security aspects of this choice are covered in Section 4.

2 SitePassword Overview

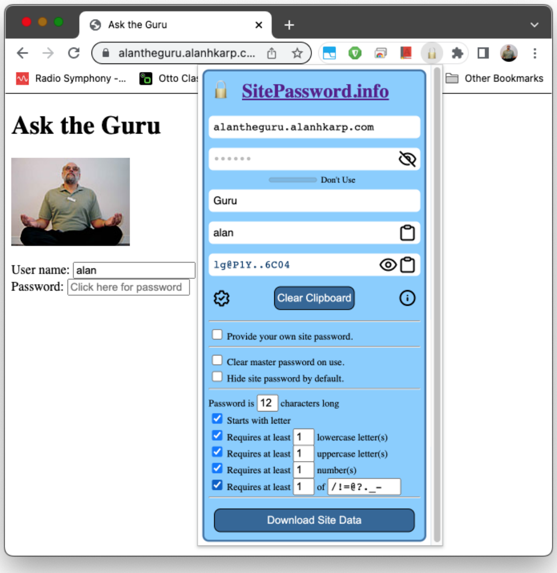
SitePassword is an extension that runs in Chromium browsers.[1] It has three components. A popup, with the user interface shown in Figure 1, is where the user provides the necessary metadata. A content script running on the page with the login form is responsible for finding the userid and password fields on the page and filling them in on request. A service worker manages the metadata and calculates the site password when the content script asks for it.

When the user first encounters a page with a login form at a given domain, the password field contains a placeholder *Click SitePassword*. Clicking the SitePassword icon opens the popup. As you fill out the form the site password field updates on every keystroke, making it clear how uncorrelated the passwords are.

As you mouse over to the password field, the userid gets filled in and the placeholder changes to say *Click here for password*. Click and the password gets filled in. When returning to that login page on any machine that synchronizes your bookmarks and has the extension installed, you only need to

USENIX Symposium on Usable Privacy and Security (SOUPS) 2022.
August 7–9, 2022, Boston, MA, United States.

[1] Brave, Chrome, Edge, and Opera. Firefox is not a pure Chomium Browser.



Ask the Guru

User name: alan
Password: Click here for password

alantheguru.alanhkarp.com

••••••

Guru

alan

1g@P1Y..6C04

□ Provide your own site password.

□ Clear master password on use.
□ Hide site password by default.

Password is 12 characters long
☑ Starts with letter
☑ Requires at least 1 lowercase letter(s)
☑ Requires at least 1 uppercase letter(s)
☑ Requires at least 1 number(s)
☑ Requires at least 1 of /!=@?._-

Figure 1: The SitePassword popup showing all available options.

click on the password field. The result is that using SitePassword is easier than even typing the same, weak password for every site.

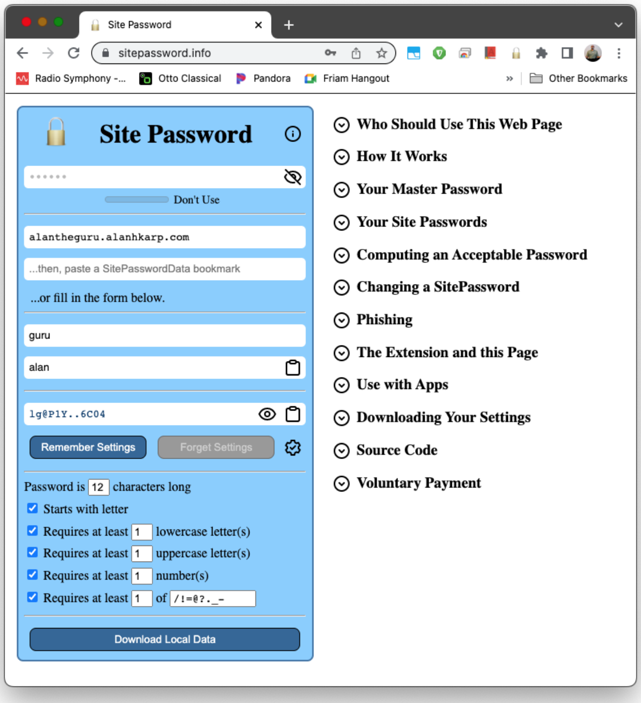
SitePassword also includes a web page, shown in Figure 2, that can be used to get your passwords when the extension is not available, such as on your mobile devices. You don't even have to remember your settings if you synchronize bookmarks to the device. You can paste the corresponding bookmark into the form.

SitePassword includes an anti-phishing feature shown in Figure 3, which.is described in Section 3.

3 Usability Considerations

People who adopt and then abandon password managers often give usability as the main reason. SitePassword was designed to be as usable as a simple game. Each step should be obvious; you should be able to experiment without worrying about breaking something; warnings make clear what next steps to take. Although SitePassword comes with extensive instructions, as shown in Figure 2, the hope is that they won't be needed.

A very simple way to guide the user is to focus on the field that should be filled in next. Another is to disable fields until they are ready for user interaction. For example, the settings that get stored are indexed by the domain name and associated with the nickname for the site. One choice would be to present an error message to the user when trying to



••••••

alantheguru.alanhkarp.com

...then, paste a SitePasswordData bookmark

...or fill in the form below.

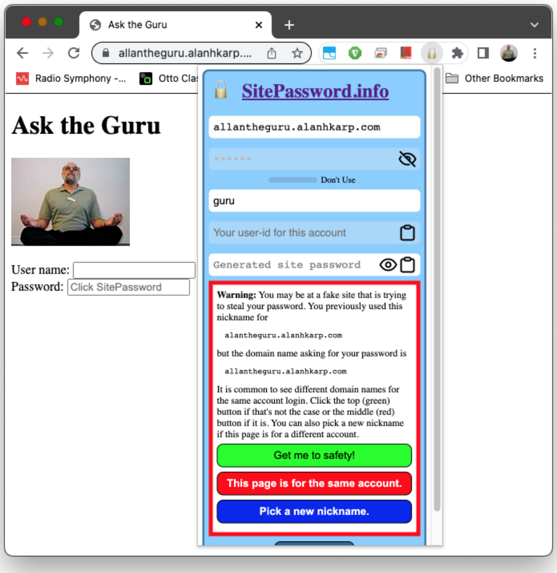
guru

alan

1g@P1Y..6C04

Password is 12 characters long
☑ Starts with letter
☑ Requires at least 1 lowercase letter(s)
☑ Requires at least 1 uppercase letter(s)
☑ Requires at least 1 number(s)
☑ Requires at least 1 of /!=@?._-

Figure 2: The SitePassword web page showing all available options and the table of contents of the instructions. Note that the calculated password is the same as in Figure 1.



Ask the Guru

User name:
Password: Click SitePassword

allantheguru.alanhkarp.com

••••••

guru

Your user-id for this account

Generated site password

Warning: You may be at a fake site that is trying to steal your password. You previously used this nickname for

alantheguru.alanhkarp.com

but the domain name asking for your password is

allantheguru.alanhkarp.com

It is common to see different domain names for the same account login. Click the top (green) button if that's not the case or the middle (red) button if it is. You can also pick a new nickname if this page is for a different account.

Figure 3: The SitePassword phishing warning.

remember the settings without this information. Instead, the *Remember Settings* button on the web version is only enabled after that information is available.

Another way to help the user is to put the information the user needs where the user is looking. An example is the placeholder put in the password field of the login form. More extensive information is provided by tooltips, which also serve as a backup in cases when the placeholder isn't visible.

Websites often have rather specific password rules, such as how many upper case letters, numbers, and special case characters are needed and even which ones are acceptable. The users only involvement in getting a valid site password is in filling out the form in the popup to specify the rules. SitePassword automatically finds a suitable password by continually hashing until one is found, stopping after 1,000 tries. While that could happen by chance, the most frequent cause is incompatible settings, such as asking for more numbers than the specified length of the password. If that's not the case, trying again with a different nickname for the site will find a valid password with high probability.

There are times when you need to type the site password manually. The most common case is logging into an app on a smart TV. In addition, it is possible that SitePassword won't find the password field on a page that has disabled pasting. Hence, it is important to choose a readable font that doesn't make, for example, lower case l (ell) look like upper case I (eye).[2]

Phishing is a threat that SitePassword is in a position to warn about, but too many websites make it ambiguous by using different domain names for logging into the same account. Unfortunately, it is virtually impossible to use the domain name to distinguish phishing from a legitimate use of a different domain name. Checking the TLS certificate would solve the problem, but that information is not available to extension developers. The fact is that most phishing warnings are spurious leaves two choices. Either ignore them or explain them. SitePassword made the latter choice in the hope that the explanation shown in Figure 3 suffices.

One question is how are you going to remember the URL to use when you're visiting a friend's house and you want your Netfilx password if you don't use the web page on a regular basis? One thing that might help you remember is the title on the popup, which shows the URL and is a link to the page. Whether or not that's sufficient is an open questions.

4 Security Considerations

A guiding principle is that a system cannot be secure if users are not aware of the implications of their actions. To that end, the SitePassword user experience is based on 10 Principles for a Secure UX. For one, it makes the easy way the secure way. It also requires a click on the password field both to avoid a family of attacks, but also to give the user a sense of control. Leaving a password on the clipboard is not good practice, so SitePassword indicates when that might be the case. Finally, potential phishing results in a warning as shown in Figure 3.

Of course, that's not enough. It's also necessary to keep the user informed. To that end, SitePassword provides a strength meter for the master password and uses the same colors for the site password in case a generated one is weak.

Other protections aren't visible to the user. The user's master password is never stored. It is kept in session memory, a transient space only available to the extension for the duration of the browser session. The callback that fills in the password is only registered on visible password elements, making clickjacking more difficult. If that element is in an iframe, the domain name of that iframe is used to select the metadata used to calculate the site password. Using the userid and site's nickname in the computation provides salt to protect the master password from pre-image attacks.

Some decisions slightly weaken security to give a big gain in usability. For example, the site password is visible by default to increase the user's trust in the generated passwords.[3] While users have the option to change the default, any risk is mitigated by the fact that you only open the popup to set up a new password and to enter your master password at the start of a browser session. Another decision was choosing a default site password length of 12, because some websites did not accept longer ones, although that has become less of an issue in recent years.

The main decision that weakens security is using unencrypted bookmarks to store your settings.[4] The benefits are huge in that there's no need for user accounts or cloud storage, the settings are available on your mobile devices that can't install the extension, and the risk is low. All an attacker gains is the sites you log into and your userids at those sites. That's not nothing, but knowing that gives no hint of either your master or site passwords.

There are also mitigating factors. It is very hard to get to the bookmarks from a web page, so malware on your machine is the main threat. Such malware is likely to cause bigger problems than exposing your SitePassword settings.

The biggest threat you face is an offline attack against your master password. Say that you create an account at a rogue site. The site owner knows your userid and site password and can probably guess your nickname for the site. The site owner can now mount an offline guessing attack against your master password.

There are three mitigations. First is choosing a strong master password. According to zxcvbn, which is used for the password strength meter, it would take 30 days to guess a 12-character password at a 10^6 guesses per second. The second is

[2] An earlier version did not follow this advice, resulting in the author needing several tries to log into Netflix on his new smart TV.

[3] Besides, it's cool watching it change as you type.

[4] The user can have more than one master password, making it impractical to encrypt the bookmarks.

that SitePassword hashes a minimum of 100 times before producing a site password, increasing the attackers work factor by that amount. The third is up to the user. Nothing says you can have only one master password. You could have one for banking and health accounts, a second for subscriptions, and a third for sketchy sites. This choice is not readily available for password managers that store your passwords.

5 Related Work

There are a number of reviews of the kind of password manager that stores passwords, so this section only reviews password calculators.

An early very simple calculator (https://www.hpl.hp.com/techreports/2002/HPL-2002-39R1.html) hashed the user's master password with a user selected nickname for the site to produce a password that the user would copy and paste into the password field. It was later adapted into the HP Antiphishing Toolbar for Internet Explorer, which added many of the features of a modern password manager.

PwdHash (https://www.usenix.org/legacy/events/sec05/tech/full_papers/ross/ross.pdf) combines the user's master password with the domain name of the page.

6 Future Work

There is still work to be done. A user study would identify any glitches in the user experience. A comprehensive security review of both the design and the code should also be done. Unfortunately, there is no funding to support either of them. In lieu of a user study, SitePassword is only available to those who know its URL in the Chrome Store. The hope is that early users will provide sufficient feedback. Informal discussions with a number of security experts has confirmed the validity of several aspects of the design.

Work has started on porting SitePassword to both Firefox and Safari, but there is no plan to create an app for mobile devices because of existing security problems on those platforms.

7 Conclusions

SitePassword is a full-featured password manager that includes the features people want most – ease of use, trustworthiness, remembering of metadata, and availability of passwords across devices. Because it doesn't require user accounts or cloud storage, it is free. It is also open source, allowing a company to produce a version with corporate branding.

8 Acknowledgements

The author would like to thank Dale Schumacher for both providing a professional look and feel to the user interface, significant code improvements to the web version, and generally useful discussion. Douglas Crockford provided significant feedback as an early adopter, and Jasvir Nagra provided guidance needed to make the content script work properly. Useful input came from the Friam security group.

9 Footnotes, Verbatim, and Citations

Footnotes should be places after punctuation characters, without any spaces between said characters and footnotes, like so.[5] And some embedded literal code may look as follows.

```
int main(int argc, char *argv[])
{
    return 0;
}
```

Now we're going to cite somebody. Watch for the cite tag. Here it comes. Arpachi-Dusseau and Arpachi-Dusseau co-authored an excellent OS book, which is also really funny [**?**], and Waldspurger got into the SIGOPS hall-of-fame due to his seminal paper about resource management in the ESX hypervisor [**?**].

The tilde character (˜) in the tex source means a non-breaking space. This way, your reference will always be attached to the word that preceded it, instead of going to the next line.

And the 'cite' package sorts your citations by their numerical order of the corresponding references at the end of the paper, ridding you from the need to notice that, e.g, "Waldspurger" appears after "Arpachi-Dusseau" when sorting references alphabetically [**?**, **?**].

It'd be nice and thoughtful of you to include a suitable link in each and every bibtex entry that you use in your submission, to allow reviewers (and other readers) to easily get to the cited work, as is done in all entries found in the References section of this document.

Now we're going take a look at Section 10, but not before observing that refs to sections and citations and such are colored and clickable in the PDF because of the packages we've included.

10 Floating Figures and Lists

Lists are sometimes quite handy. If you want to itemize things, feel free:

[5] Remember that USENIX format stopped using endnotes and is now using regular footnotes.

fread a function that reads from a `stream` into the array `ptr` at most `nobj` objects of size `size`, returning returns the number of objects read.

Fred a person's name, e.g., there once was a dude named Fred who separated usenix.sty from this file to allow for easy inclusion.

The noindent at the start of this paragraph in its tex version makes it clear that it's a continuation of the preceding paragraph, as opposed to a new paragraph in its own right.

10.1 LaTeX-ing Your TeX File

People often use `pdflatex` these days for creating pdf-s from tex files via the shell. And `bibtex`, of course. Works for us.

Acknowledgments

The USENIX latex style is old and very tired, which is why there's no \acks command for you to use when acknowledging. Sorry.