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 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. They make it easier for you to have a different, strong password for every site while making it convenient to change a password when necessary. 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 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.

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. Instead, it puts the metadata in bookmarks, which virtually all browsers synchronize across machines. The security aspects of this choice are covered in Section 4.

Using bookmarks makes the settings available on machines that cannot install the extension, such as mobile devices. In addition, there is only a small risk attached to printing the settings, since they only contain data of limited security value.

2 SitePassword Overview

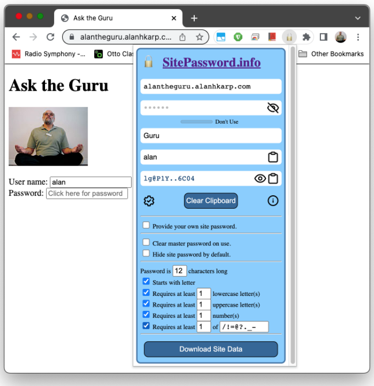
SitePassword is an extension that runs in Chromium browsers.[1] It has three components. A popup, with the user interface shown in Figure 1, is where the user provides the necessary metadata. A content script is responsible for finding the userid and password fields on the page and filling them in on 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.

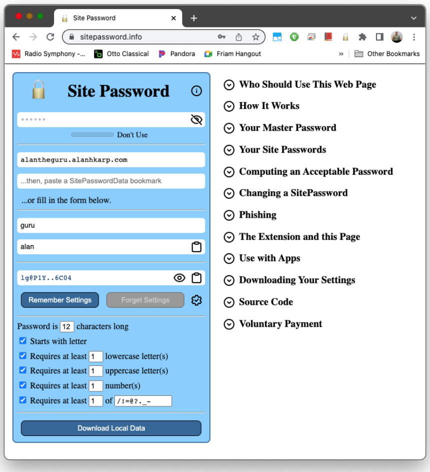
Figure 3 shows the warning you get if you are at a potential phishing site. The detailed message is described in the section on usability.

3 Usability Considerations

People who adopt and then abandon password managers often site 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 you should fill 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 remember the settings without this information. Instead, the *Remember Settings* button is only enabled after that information is available.

Another way to help the user is to provide meaningful labels and tooltips.



••••••

alantheguru.alanhkarp.com

...then, paste a SitePasswordData bookmark

...or fill in the form below.

guru

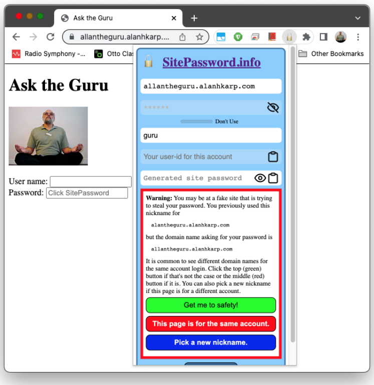
alan

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 /!=@?._-

- Who Should Use This Web Page
- How It Works
- Your Master Password
- Your Site Passwords
- Computing an Acceptable Password
- Changing a SitePassword
- Phishing
- The Extension and this Page
- Use with Apps
- Downloading Your Settings
- Source Code
- Voluntary Payment

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.

4 Security Considerations

5 Future Work

6 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.

7 Footnotes, Verbatim, and Citations

Footnotes should be places after punctuation characters, without any spaces between said characters and footnotes, like so.[2] 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 8, 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.

8 Floating Figures and Lists

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

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.

8.1 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.

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