Improving password managers and multidevice synchronization

Yngve Nysæter Pettersen
Opera Software ASA
yngve@opera.com
http://www.opera.com/

Abstract: This document discuss challenges to using password managers to manage online identities, particularly when synchronizing password on multiple devices, and proposes directions for how to improve this functionality.

Introduction

Password managers have for many years been used to manage users online identities and credentials. All major browsers have such managers today.

Opera's password manager will, after the user submits a form with a password, ask if the password and other details from the page should be stored. If the user decides to store this information, the details, associated with the form, or any similar form on the server (which is useful when the form's URL constantly changes), are stored in an obfuscated form ("encrypted" with a hardcoded password), while the password can optionally be stored encrypted with an encryption key derived from the master password used for the Client Certificate database.

When the user later visits the site the log-in fields will be displayed with a golden border, indicating that the details are known, and users can then use a drop-down menue to select the account name they want to use (multiple entries can be registered).

The benefit of such a tool is that users do not have to remember every password they have. Also, the tool provides more secure storage of the credentials, and it reduces the risk of accidentally leaking the credentials to phishing websites, since the password manager is keyed to provide the credentials to specific forms, thus increasing the user's security.

There are, however, several challenges for the use of password managers:

- Users frequently have multiple computers, clients, or devices, such as phones, tablets, etc., where they need the credentials to be present.
- Consistency for credential submission is an issue
- Managing the identity information at the site and in the manager is an issue.

Synchronization across devices

Users are increasingly accessing websites through multiple computers and devices, such as home and work computers, laptops, web-enabled phones, tablets, and TVs.

Synchronization of passwords across these devices is currently a challenge, as, in many cases, the software used on each of these are from different vendors, with different formats for most files. In many cases, manually entering every credential on each device has been the only option.

Upcoming versions of Opera will be able to do such synchronization between different installations of Opera for desktop, Opera Mobile and Opera Mini browsers through the Opera Link service that already provides such synchronization of bookmarks and notes. At present, passwords will not be available to third-party applications through the Opera Link API.

Credential submission consistency

There is great variation among the log-in systems used by websites.

This variation extends well beyond the names of the fields in the log-in forms, to some fields having to be filled manually by the user (e.g., two factor authentication data or CAPTCHAs) and further to how the forms have to be submitted. Some forms can be submitted through simulating the standard "Submit" button event, while other forms require clicking a specific button or image that triggers further actions that must be performed before the form is submitted.

A possible way forward, to mitigate this issue, might be to develop a system for declaring which fields must be entered by the user, because they change for each login, and which actions are needed to submit the form. Some of this may already be implied by some HTML and ECMAscript APIs, but perhaps some further enhancements are needed.

Managing identity information

At present, when creating an account with a website or updating it, the user must manually enter the necessary information, including the selection of a password, and must later enter the credential information into the password manager separately.

This process makes it more likely that users will select bad passwords, such as weak passwords or ones they already are using for other websites.

It would greatly improve security if websites could inform the client that an account is being created or updated. This would allow the client to help the user by storing the credentials immediately, using information specified by the website to configure the settings for the account (including authentication algorithm requirements). More importantly, it will also be able to assist the choice of password.

Password selection assistance can be accomplished in several ways: yy displaying a selection of generated password, such as the "pwgen" utiliy on Linux, or by constructing a hexadecimal or Base64 encoded pseudo random string that the user stricly speaking never need to know. A special kind of such pseudo random string might be constructed using the RFC 5705 TLS Key material extractor method to derive a shared secret (password) based on the current TLS connection's

MasterSecret key, a method that will be most useful if combined with authentication methods that do not send the password directly to the server.

The password selection assistant can be implemented independently of whether account creation/update forms indicate what action is underway, but such an indication would permit more automation of the process.

Conclusion

Password managers can help improve the security of submitting identity credentials, and standardized APIs for multidevice synchronization can improve the usability of such credentials.

With more assistance from the websites using the credentials, such as by indicating what actions are being performed and what actions are required by the user, the process of creating and submitting credentials can be improved and automated, and more secure credentials can be configured for the accounts.