Chiff: Moving beyond passwords

Summary

Password authentication has been the primary mean of authentication for web applications since the early days of the Internet, but it suffers from both security and usability issues. One of its most promising alternatives – WebAuthn – still lacks instead in adoption from both end-users and website owners.

With NGI_Trust support, Chiff developed a hybrid authenticator supporting a variety of existing authentication methods, such as WebAuthn, in a uniform UI-flow for the user.

Keywords

Authentication, WebAuthn, passwords.

Actors involved in the project

- Chiff BV: https://www.chiff.app (former Keyn BV)
- Content Power: https://www.contentpower.nl

Beyond passwords

Password authentication has been the primary mean of authentication for web applications since the early days of the Internet. However, this method suffers from both security and usability issues.

On average, a person has well over thirty accounts, for instance for online banking, shopping and reading the news. All cybersecurity experts advise to use long, complex and unique passwords for all our online accounts, but obviously it's not possible to remember more than thirty different passwords such as "A'5q."tJ5%kUP*Ai`;Q1".

It's time to move beyond passwords. One of the most promising alternatives for password authentication is the FIDO2 project and the WebAuthn W3C standard it is built upon. It is a strong authentication scheme that provides an API in the browser to communicate with an external authenticator, such as a smartphone. The WebAuthn API is already incorporated in all major browsers.

To realize widespread adoption of the WebAuthn standard, there are two main challenges: adoption by end-users and adoption by website-owners. To make things complicated, these two are interdependent: users will probably not start using a new authentication method if there are only a few websites where it can be used, and website owners will not invest in updating their infrastructure to support an authentication mechanism that almost nobody uses. A current strategy chosen by website owners to break out of this impasse, is to offer WebAuthn as a second factor to password authentication.

The solution

Chiff is a Dutch cybersecurity start-up focusing on secure and easy authentication. Its main objective is to develop a solution to allow people to log in onto websites more easily and with greater security by using their smartphone. Chiff bridges the gap from password authentication to strong authentication on the web, such as WebAuthn, by creating a uniform user experience for a variety of existing authentication methods.

Chiff is a hybrid authenticator that consists of a smartphone application and a browser extension, communicating over an end-to-end encrypted communication channel. All details are stored on the smartphone, with a browser extension sending a request to the smartphone whenever it needs to authenticate. The user authorises these requests by authenticating on the phone.

Chiff supports both password authentication and WebAuthn in a uniform UI-flow. Whenever the user wants to log in, a push message is sent to the app. The user authorizes the request using the phone's biometric functionalities. Then the extension completes the process, when the

browser receives either a signed WebAuthn response or a password - which can be long and complex, as the user doesn't need to remember it.

The project

Chiff got funded twice by NGI_Trust, in both the first and the third open call, with the aim to bridge the gap to WebAuthn and commercialise its solution. Technically, the two projects were closely related, consisting of the following components:

- Mobile authenticator (native iOS and Android apps)
- Browser extension (all major browsers)
- Implementation of the WebAuthn standard
- Back-end for end-to-end encrypted communication
- Admin panel to manage accounts for an organisation

From a business point of view there was instead a clear distinction. The first project was entirely focused on the B2C-market and the second on the B2B-market. In the first project the app was released in the Apple AppStore and in Google Play Store.

Chiff had launched the app with a thorough marketing strategy, resulting in downloads and new users, but the business case proved quite challenging. Therefore, they decided to make the app freely available and use it as a marketing tool for the second project, focusing on businesses, resulting in the first paying customers for their password management tool for Small and Medium Enterprises (SMEs): Chiff for Teams.

Together with project partner Content Power, a Dutch web development company, Chiff also investigated the possibility to pilot WebAuthn projects at SMEs. A reason for this was that during the COVID pandemic SMEs were mainly focusing on surviving the crisis, instead of making their authentication processes more efficient and secure.

The quest on finding the right niche is a continuous process. Recently, Chiff's solution proved very useful for Business Process Outsourcing (BPO) companies, such as contact centres. Since Chiff works entirely client-side, a BPO company can use the solution without the need of their clients implementing things server-side: Chiff works out-of-the-box.

With the help of NGI_Trust, Chiff has explored and discussed different use cases for several target groups. The mentoring support of NGI_Trust coaches helped the project to be completed efficiently and within time, quality and budget. Furthermore, NGI_Trust's technical knowledge and overall guidance were very useful. In a broader perspective, the NGI network resulted in valuable contacts and in many interesting meetings between Chiff, other project applicants and NGI partners, especially regarding intellectual property rights.

Free and open source

One of the project's most important milestones was to make Chiff's core open source and offer it for free for private use. This serves several purposes:

- Chiff is built on a zero-trust model: being transparent about how Chiff is built may help to gain trust and increase adoption;
- This lowers the threshold for end-users to start using WebAuthn and encourages them to start using Chiff.

Since Chiff's core has been made open source only recently, the results of making the code publicly available are still pending. However, having developed a free-to-use password manager for the consumer market, based on a zero-trust model is a huge achievement in itself.

Although the project funded by NGI_Trust has ended, Chiff's project is continuing, by developing additional features and optimally tailoring the solution towards specific target groups.

If you are interested, you are very welcome to give Chiff a try! You can download Chiff from Apple's AppStore and Google's Play Store, or you can visit https://chiff.app for more information.