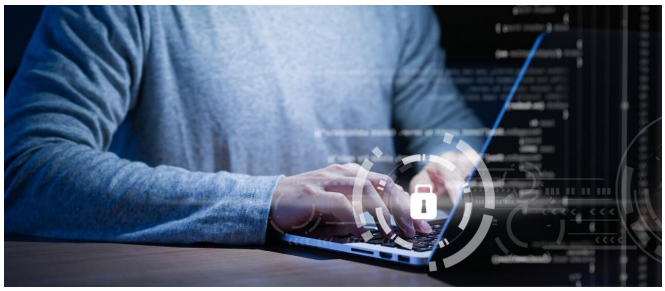
No keys to the kingdom: New single sign-on algorithm provides superior privacy

29 June 2020



A new and secure single sign-on algorithm that eliminates all chances of gathering and leaking personal information without user consent. Credit: Tokyo University of Science

Over the last few decades, as the information era has matured, it has shaped the world of cryptography and made it a varied landscape. Amongst the myriad encoding methods and cryptosystems currently available for ensuring secure data transfers and user identification, some have become quite popular because of their safety or practicality. For example, if you have ever been given the option to log onto a website using your Facebook or Gmail ID and password, you have encountered a single sign-on (SSO) system at work. The same goes for most smartphones, where signing in with a single username and password combination allows access to many different services and applications.

SSO schemes give users the option to access multiple systems by signing in to just one specific system. This specific system is called the 'identity provider' and is regarded as a trusted entity that can verify and store the identity of the user. When the user attempts to access a service via the SSO, the 'service provider' asks this identity provider to authenticate the user.

The advantages of SSO systems are many. For one, users need not remember several username and password combinations for each website or application. This translates into fewer people forgetting their passwords and, in turn, fewer telephone calls to IT support centers. Moreover, SSO reduces the hassle of logging in, which can, for example, encourage employees to use their company's security-oriented tools for tasks such as secure file transfer.

But with these advantages come some grave concerns. SSO systems are often run by Big Tech companies, who have, in the past, been reported to gather people's personal information from apps and websites (service providers) without their consent, for targeted advertising and other marketing purposes. Some people are also concerned that their ID and password could be stored locally by third parties when they provide them to the SSO mechanism.

In an effort to address these problems, Associate Professor Satoshi Iriyama from Tokyo University of Science and his colleague Dr. Maki Kihara have recently developed a new SSO algorithm that on principle prevents such holistic information exchange. In their paper, published in *Cryptography*, they describe the new algorithm in great detail after going over their motivations for developing it. Dr. Iriyama states: "We aimed to develop an SSO algorithm that does not disclose the user's identity and sensitive personal information to the service provider. In this way, our SSO algorithm uses personal information only for authentication of the user, as originally intended when SSO systems were introduced."

Because of the way this SSO algorithm is designed, it is impossible in essence for user information to be disclosed without authorization. This is achieved, as explained by Dr. Iriyama, by applying the principle of 'handling information while it is still encrypted.' In their SSO algorithm, all parties exchange encrypted messages but never

exchange decryption keys, and no one is ever in possession of all the pieces of the puzzle because no one has the keys to all the information. While the service provider (not the identity provider) gets to know whether a user was successfully authenticated, they do not get access to the user's identity and any of their sensitive personal information. This in turn breaks the link that allows identity providers to draw specific user information from service providers.

The proposed scheme offers many other advantages. In terms of security, it is impervious by design to all typical forms of attack by which information or passwords are stolen. For instance, as Dr. Iriyama explains, "Our algorithm can be used not only with an ID and a password, but also with any other type of identity information, such as biometrics, credit card data, and unique numbers known by the user." This also means that users can only provide identity information that they wish to disclose, reducing the risk of Big Tech companies or other third parties siphoning off personal information. In addition, the algorithm runs remarkably fast, an essential quality to ensure that the computational burden does not hinder its implementation.

This study will hopefully bring about positive changes in current SSO systems, so that more users are encouraged to use them and reap their many benefits.

More information: Maki Kihara et al, Security and Performance of Single Sign-On Based on One-Time Pad Algorithm, *Cryptography* (2020). DOI: 10.3390/cryptography4020016