Once usability becomes secure

Eurekalert!

Risk increases with comfort: "Single Sign-On" permits users to access all their protected Web resources, replacing repeated sign-ins with passwords. However, attackers also know about the advantages such a single point of attack offers to them. Andreas Mayer, who is writing his PhD thesis as an external doctoral candidate at the Chair for Network and Data Security (Prof. Dr. Jörg Schwenk) at Ruhr-Universität Bochum, has now been able to significantly increase the security of this central interface for the simpleSAMLphp framework.

In the past, no protection against targeted Web attacks

The "Single sign-on" system, in short SSO, seems to be a wonderful solution for any user: "Once authenticated, the information and services are immediately available,without repeated inconvenient password input", says Mayer. However, this concept significantly increases the possible damage, which could harm the user through a "single point of attack". The researchers in Bochum recently showed that the single sign-on is not as safe as assumed: They broke 12 of 14 SSO systems that had critical security flaws. "In the near future, we expect an increasing number of attacks on browser based SSO solutions such as Facebook Connect, SAML, OpenID and Microsoft Cardspace", explains Mayer. "It is very alarming that none of the currently used SSO protocols, developed during the last twelve years, provides effective protection against targeted attacks".

Highly efficient open source SSO solution

In the past, the many threatening scenarios, such as phishing, man-in-the-middle attacks, cross site scripting or Web malware, did not negatively affect the increasing popularity of SSO offerings. The "single sign-on, access everywhere" model is too comfortable and the users are too unsuspecting. Andreas Mayer addresses this risk with his own results: He implemented the OASIS-standardized "SAML Holder-of-Key Web Browser SSO Profile" in the popular open source framework "SimpleSAMLphp". "This profile binds the critical authentication and authorization information – the so-called security tokens – cryptographically to the browser of the legitimate user", explains Mayer. "The result is a highly effective, open source solution that is supported by all established browsers".

Andreas Mayer works at Adolf Würth GmbH & Co. KG and works in his free time at his doctoral thesis at the Chair for Network and Data Security of the RUB.