PHYS.ORG

Be whoever you want to be: Single sign-on systems can be improved

August 15 2012

Web shops, Cloud Computing, Online CRM systems: Each day many IT systems require the user to identify himself. Single Sign-On (SSO) systems were introduced to circumvent this problem, and to establish structured Identity Management (IDM) systems in industry: Here the user only has to identify once, all subsequent authentications are done automatically. However, SSO systems based on the industry standard SAML have huge vulnerabilities: Roughly 80 percent of these systems could be broken by the researchers from Ruhr-Universität Bochum.

Single Sign-On (SSO) can be compared to a well guarded door, which protects sensitive company data: Once you have passed this door, you can access all data. Many industry SSO systems are built on the basis of the Security Assertion Markup Language (SAML). Identity information is stored in a SAML message, protected by a digital signature. Researchers from Bochum were able to circumvent this protection completely in 12 out of 14 SAML systems.

"With novel XML Signature Wrapping techniques we were able to circumvent these digital signatures completely", says Prof. Jörg Schwenk from Ruhr-Universität. "Thus we could impersonate any user, even system administrators." Amongst the 12 affected systems were the SaaS Cloud provider Salesforce, the IBM Datapower security gateway, Onelogin (could e.g. be used as an optional module in Joomla, Wordpress, SugarCRM, or Drupal) and OpenSAML (used e.g. in Shibboleth, and SuisseID, and OpenSAML).

"After we found the attacks, we immediately informed the affected companies, and proposed ways to mitigate the attacks", states security expert and external PhD student Andreas Mayer (Adolf Würth GmbH & Co. KG). "Through the close cooperation with the responsible security teams, the vulnerabilities are now fixed", Juraj Somorovsky adds.

More information: On August 10th, 2012 Juraj Somorovsky presented the results at the 21st USENIX Security Symposium in Bellevue, Washington.
www.nds.rub.de/research/publications/BreakingSAML

Provided by Ruhr-Universitaet-Bochum

Citation: Be whoever you want to be: Single sign-on systems can be improved (2012, August 15) retrieved 6 May 2024 from https://phys.org/news/2012-08-sign-on.html