Web Application Security using SAML2 and oAuth2

Martin Haase, Peter Gietz
DAASI International GmbH
Tübingen, Germany
martin.haase@daasi.de, peter.gietz@daasi.de

Abstract—The OASIS standard SAML (Security Assertion Markup Language) is being used for securing Web applications both in academic and enterprise contexts. SAML allows for distributing authentication and authorization information within a trust federation and provides the feature Single Sign On. In the academic world, already a majority of higher education institutions are connected to so-called SAML federations, enabling their users access to on-line Web resources of all institutions connected to the federation. In the enterprise context, SAML frequently serves as the "contract" between companies in order to outsource Web resource development.

The first part of this talk will present an introduction to SAML version 2[1] and deal with the different use cases in academia and industry, focusing on the most frequently used SAML profile, Web Browser Single Sign-On.

The second part will concentrate on how to secure non browser based application, i.e. SOAP and RESTlike web services. There are many possible and standard approaches using core SAML2, SAML2 extensions like the STS profile, the IETF standard oAuth2 [2], and various combinations of SAML2 and oAuth2. The talk will give an introduction to oAuth2 and then demonstrate several flows, their requirements and which situations are appropriate for which approach. Finally actual deployments of the SAML2/oAuth2 combination approach based on Open Source software will be reported.

Keywords—Web security, SAML, oAuth2

REFERENCES