A Federated Authorization and Authentication Infrastructure for Unified Single Sign On

Sascha Neinert

Computing Centre
University of Stuttgart
Allmandring 30a
70550 Stuttgart
sascha.neinert@rus.uni-stuttgart.de

Abstract: Currently federated authorization and authentication infrastructures are deployed to offer services to large groups of users while increasing the usability and scalability of the security architecture. Connection of domains using a variety of technologies brings new challenges and requires the utilization of standardized communication languages between these components. The presented architecture aims to unify types of federations previously separate by using these languages with generic security architecture, able to provide a unified Single Sign On.

Introduction

Over the last years the number of services available on the web has continually grown. The role of the user is changing from a passive consumer of information towards an active participant. Everyone now can publish his personal beliefs, discuss them with others, and participate in online communities. At the same time the need for controlling the access to these services has increased. Internal information shall be accessible only by members of the organization; private data shall only be viewed by friends, and commercial services are provided only for paying customers.

Active users are no longer anonymous but get identities; they register, create accounts and provide information about themselves. The process of identifying a previously registered user is called Authentication. To grant or deny access to services for authenticated users is a process called Authorization. These security aspects are decoupled from the logic of single applications and developed as a generic, reusable authentication and authorization infrastructure (AAI).

Usually users have one account at each provider of a service. This has two disadvantages. From the service provider's view, it is an effort to manage lots of accounts. A trade-off has to be found to get sufficiently detailed, reliable and up-to-date user information on the one hand, and not to discourage users with time-consuming registration and account management procedures on the other hand. From the user's view it is hard to remember multiple logins and passwords, so often they are reused at the cost of security. A federated identity management allows using identity information across security domains, so providers of service can work together with providers of identities. Users can use one login with one password for multiple services now. They can also login once, at one service provider, and need not login again at the next service provider. This is called Single Sign On (SSO).

Not only the number of services but also the number of users is increasing, particularly those users with mobile devices, expecting connectivity everywhere. More and more wireless access points become available at academic institutions, but still they cannot be utilized by visiting students and scientists without administrative effort. By federating the academic institutions and forming an international AA infrastructure the goal of network connectivity everywhere is within reach.

Scenario

Peter studies computer sciences at the University of Stuttgart, in Germany. Currently he works as an exchange student at the University of Murcia, in Spain. As he knows Murcia is part of the eduroam federation, he does not have register for a new account for the crowded students' computer lab. He just opens his laptop anywhere on the campus, and his wireless supplicant tells him about a well-known SSID "eduroam". He enters his credentials "peter@uni-stuttgart.de" and gains network access. Then he goes to the Universities e-learning portal to look up his new schedule and sees he is already logged in as "peter@uni-stuttgart.de". Also the page is displayed in German, but of course he switches to Spanish to better learn the new language. His schedule also lists a programming tutorial. A link gets him to the download page of the needed development environment. Being a computer science student, he is allowed to download and use this commercial software for free. Unfortunately the download as fast as he would like – as a student he is only given a limited bandwidth.

The important thing about this scenario is what the user does not do: he does not use a Spanish guest account, and he does not log in a second time for access to the e-learning portal application. He only needs his account at his home institution where he has registered once. He can use this one account to access any service provider within the federation.

Federation Technologies

Currently a variety of technologies is used to build federated authentication and authorization infrastructures. The European eduroam [2] federation provides network services to roaming academic users. Following the idea "open your laptop and be online" user visiting a participating institution see an SSID "eduroam", connect to the local network, input their username@homedomain and get access to the internet. This is based on a hierarchical setup of RADIUS [3] servers that proxy authentication requests to each user's home domain. Access points enforce users to login using the 802.1x standard. The users' credentials are securely transmitted across multiple RADIUS servers inside an encrypted tunnel (often using EAP-TTLS or Protected EAP).

Shibboleth [4] is a middleware which provides federated Single Sign On for Web Services. It implements and extends the OASIS SAML specification (v1.1). Several national federations have successfully been built with this middleware (SWITCHaai) or are in the process of being built (DFN-AAI). Users accessing a Shibboleth protected Web Service are redirected to an Identity Provider at their home domain. They enter username and password there, and then are redirected back to the Web Service. Transport of messages is done using SOAP over HTTP, or HTTPS.

eduGAIN [5] is the GÉANT Authorisation Infrastructure for the research and education community. Many national federations already have been established, but are based on differing AAI solutions as Shibboleth, PAPI, A-select or Liberty Alliance, for example. With eduGAIN these federations can be connected to form a higher-level federation, a confederation. Users accessing resources in foreign federations are redirected to a "What Federation Are You From" (WFAYF) service, that redirects them to the Identity Provider of their home domain next. eduGAIN is currently based on SAML 1.1.

All of these federations have in common the separation between providers of services and providers of identities. Each of them has the typical use case involving three entities, user, service- and identity provider. Information about users is managed by the home institutions, the rules controlling access to services are managed by the providers of the services. Mutual trust between all providers within a federation is a requirement, this trust is often realised in form of a public key infrastructure based on certificates.

Nevertheless each of these federations only supports one type of service, being either access to the network or access to web services. The proposed system would unify these types of federations, to result in one multi-purpose federation. This unified federation looks more uniform to users while providing more types of services. Usage of a reduced set of technologies based on well-defined and well-known standards simplifies the deployment of such a federation. Furthermore concepts as attribute-based access control can be reused for other type of services, network access for example, to provide greater flexibility.

Standardized Languages for Communication

SAML [6] is an acronym for "Security Assertion Markup Language". It is a standardized way to express security assertions, encoded in XML. Syntax and semantics are defined for statements describing authentication, authorization and attributes of certain subjects. An authentication statement contains information about a subject, the method used for authentication, and the time the authentication took place. An authorization statement describes on which resource a certain subject may perform a certain action. An attribute statement contains a sequence of attributes that are associated with the given subject. These parts are generic enough to be applied to any kind of service or resource, web or non-web.

SAML also defines "bindings". A binding is an underlying transport and communication protocol; this is usually SOAP over HTTP as SAML is mostly used with Web Services. Nevertheless it is designed to be generic and flexible, to be of use in more scenarios than the Web only. "Profiles" define a flow of messages for a scenario – the Browser/POST profile for example provides Single Sign On for browser users requesting access to Web Services.

XACML [7] stands for "eXtensible Access Control Markup Language", and it is a standardized way to express security policies. Like SAML it is encoded in XML. A policy describes a set of rules that apply if a certain subject wants to access a certain service. These rules may permit or deny the access, or permit only under some conditions. If more than one rule applies the combining-algorithm of the policy is used.

Policies can be used for two things in the scenario described above. First, the Provider of a Service wants to ensure that only the intended users can access his service. He defines rules and policies describing what users shall get a "permit", and what users shall get a "deny". Second, a user wants to publish only some of the information describing him, and consider the rest as private. He would define a policy describing which attributes can be released, possibly specific for certain services.

Again, these policies and rules are generic, and can be applied to any resource or service, regardless of the other, supplementing technologies that are involved.

Both SAML and XACML are well-defined and stable standards, produced by OASIS. Using these languages ensures interoperability of different systems. It also simplifies the analysis of important parts of a security infrastructure if analysts already understand the syntax and semantics. Finally it allows harmonizing the view and treatment of services that previously were considered as of different type, and required different technologies for each type of service.

Architecture

The architecture of the proposed system will build upon the existing eduroam [2] infrastructure. The goal is to extend this infrastructure, not to replace it. Authentication will be performed in the same way as in current eduroam, via proxying through a hierarchy of RADIUS servers. The RADIUS servers at both ends of the proxy-chain will be extended with additional modules. The RADIUS server from the home institution will be enabled to create a token, containing a SAML authentication statement, which is sent to the user's client during the network authentication phase. The RADIUS server at the visited institution will have two added functionalities. First, it will be enabled to request user attributes with a SAML attribute request. Second, the resulting SAML attribute statements will be given to a policy decision point that can apply the local security policies to it. These policies will be described in XACML.

The token will be received and securely stored by a piece of middleware on the user's device. If the user accesses a protected web service at some later point in time, the provider of this service has two options: he can send an interface to the user, so he can select his home institution, be redirected, and enter his credentials (again). This is currently the usual way for shibboleth-based federations. But he can also contact the client middleware and get the token that was received during the network authentication phase. Possession of the token proves that the client has already been authenticated by a trusted member of the federation. Then the user does not need to give his credentials a second time. As long as his token is valid, he is logged in.

It is crucial that tokens are digitally signed by the entity that issues them; else malevolent users can change the contents. To prevent theft of tokens, they are encrypted before storing them on the client device. Only service providers that can authenticate themselves and prove they are part of the federation can request the token from the client middleware.

To allow deployment of this system in federations based on a number of technologies, the functionality to request, receive and verify the tokens will not be implemented directly into the service providers. Rather the service providers will refer to their corresponding eduGAIN aware entities, the bridging elements, to provide this functionality. This new system will then be usable within federations based on SAML, but also within such that are based on other technologies.

Conclusions

The proposed architecture enhances the existing eduroam roaming infrastructure. Authorization capabilities are added to the existing authentication facilities. Policies can be described in a standardized way to control access to the network based on characteristics of the users, rather than on their identities alone.

The token acquired during the network authentication phase can be given to web service providers, thereby connecting both worlds. This allows the user to sign on only once, as long as the token is valid. A unified Single Sign On for network access as well as web services is realised.

A prototype for this system is currently being implemented. Tests using SAML authentication and attribute statements in combination with XACML policies were successfully executed to control access to the network. The architecture as described above is currently being refined, to fulfil the requirements of a European-wide unified federation. Such a unified federation is expected to encourage the development of currently separated federations, reducing the complexity while increasing the usefulness and utilization of existing infrastructures that are gradually extended.

Outlook

The bringing together of the web service federations and the network federations combines only two types of services. The integration of access control to Grid services into the described architecture has been addressed in other projects already. The new architecture of this system will be tested for it's suitability to also be used in the Grid context. The network federation suggest examination of a further new concept, location-awareness. In contrast to web services the physical location of a user becomes important for access to the network. A printer service could only be sensibly be included if user get access to printers that are nearby. As the number of possibilities and ways to access the network access increases constantly, mechanisms for dynamic discovery of such services will be needed. The clients need to be able to learn the properties of each available network to make a decision which to use best. The basic architecture as described above is expected to be generic enough to remain unchanged, and also the standardized languages for communications between components, SAML and XACML, will continue to be central parts.

Acknowledgement

The results published in this paper were developed in the DAMe [1] project, a sub project of the GÉANT2 joint research activity 5 that is co-funded by the European Commission within the Sixth R&D Framework Programme (FP6). The DAMe project is developed together with the University of Murcia, Spain, DFN, Germany, and RedIRIS, Spain. The author would like to thank all the partners involved in that project.

References

[1] Deploying Authorization Mechanisms for Federated Services in the eduroam Architecture (DAMe)
http://dame.inf.um.es/

[2] Licia Florio, Klaas Wierenga: Eduroam, providing mobility for roaming users. In: Proceedings of EUNIS, Manchester 2005

[3] C. Rigney et al.: Remote Authentication Dial In User Service (RADIUS). RFC 2865, June 2000

[4] Tom Scavo, Scott Cantor: Shibboleth Architecture Technical Overview. June 2005

[5] D. R. Lopez et al.: GÉANT2 Authorisation and Authentication Infrastructure (AAI) Architecture – second edition. April 2007

[6] Eve Maler, Prateek Mishra, Rob Philpott et al.: Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1. September 2003

[7] Simon Godik, Tim Moses et al.: eXtensible Access Control Markup Language (XACML) Version 1.1. August 2003