J. Lopez, J. A. Montenegro, R. Oppliger, and G. Pernul, "On a Taxonomy of Systems for Authentication and/or Authorization Services", *TERENA Networking Conference*, 2004.
NICS Lab. Publications: https://www.nics.uma.es/publications

On a Taxonomy of Systems for Authentication and/or Authorization Services

Javier Lopez[1], Jose A.Montenegro[1], Rolf Oppliger[2], Guenther Pernul[3]

[1] Computer Science Department, University of Malaga, Spain
{jlm, monte}@ lcc.uma.es
[2]eSECURITY Technologies, Gümligen, Switzerland
rolf.oppliger@esecurity.ch
[3]Department of Information Systems, University of Regensburg, Germany
guenther.pernul@wiwi.uni-regensburg.de

An *authentication service* allows a user to prove who he/she is. Nowadays, the relevance of this service is very clear since applications that have been developed for wide environments, like the Internet, do not allow that trust among transacting parties is based on traditional aspects, like physical proximity or previous knowledge among parties. On the other hand, new applications, especially those that can be placed in the area of e-commerce, need to make use of a service that helps to describe what the user is allowed to do. This is the *authorization service*.

In the Computer Science arena, in general, and specifically, in the Information Security field, the need for authorization services can be considered as old as the need for authentication services. We can find in the literature many solutions that discuss and solve these problems independently, and for the case of authorization services special focus has been made on the *access control* area. However, it is also clear that many times these problems have been discussed together for the cases in which both services are used in conjunction to solve global authorization plus authentication problems. In fact, from the user perspective, the line that divides the world of authentication and authorization seems to be not very clearly defined for some types of applications.

In this work we elaborate on a taxonomy of systems that provide either joint solutions for both authentication and authorization problems, or solutions for only one of the problems. Basically, we do not focus our work on theoretical systems that have been proposed only in the literature. On the other hand, we focus on: (i) systems that are already developed; (ii) systems that are under development or deployment; and (iii) systems that are still in the initial stages of design but are supported by international working groups or bodies. More precisely, we elaborate on a taxonomy of systems that are (or will be soon) available to final users.

This extended abstract just briefly describe those systems in alphabetic order. Limited space does not allow at this moment to present a more detailed description including their advantages and drawbacks, together with a comparative table that analyzes their main features. An eventual final version of this paper will include these issues. However, we can state that the list of features that we have considered for the comparison is the following one: security, efficiency, scalability, interoperability, delegation, revocation, privacy, mobility, suitability for mobile computing, implementation, scope of use, and difficulty of use for final users.

AAAARCH (Authentication, Authorization and Accounting Architecture) [1]

A number of Internet services require Authentication, Authorization, Accounting and Audit Support. The *IETF AAA Working Group* is chartered with defining short term requirements for a protocol that will support such services for NASREQ and MobileIP. The work of the AAA group has shown that there are a number of areas where an AAA Architecture would be helpful.

Akenti [2]

Akenti have developed and deployed an authorization service based on X.509 identified users and access policy contained in certificates signed by X.509 identified stakeholders [TEM03]. A policy language has been deployed also. The Akenti model consists of resources that are being accessed via a resource gateway by users. These users connect to the resource gateway using the SSL handshake protocol to present authenticated X.509 *identity certificates*.

Kerberos [3]

The *Kerberos* authentication system was originally developed at MIT [SNS88, Sch94]. Kerberos is based on authentication and key distribution protocols originally in [NS78, NS87] and modified to use timestamps [DS81]. The aim of Kerberos is to allow a client acting on behalf of a user to authenticate to a service (i.e., an application server) without having to send credentials (e.g., username and password) in the clear. Therefore, Kerberos implements a ticketing system. This basically means that principals request tickets from a trusted *Key Distribution Center* (KDC), and that these tickets are sent together with the service requests to authenticate the requesting principal.

Liberty Alliance [4]

This project is viewed as competitor of *Microsoft .Net Passport* (see below). The principal idea is to create an open, federated, single sign-on identity solution for the digital economy via any device connected to the Internet. Liberty architecture distinguishes between identity providers and service providers. Identity providers provide identification and authentication services, whereas service providers make use of these services to provide commercial services to users. Each participant may have several identities and identity federation and defederation are the basic building blocks in the Liberty Project [Lib03]

PAPI [5]

PAPI is a system for providing access control to restricted information resources across the Internet. The authentication mechanisms are designed to be as flexible as possible, allowing each organization to use its own authentication schema, keeping user privacy, and offering information providers data enough for statistics. Authorization mechanisms

[1] http://www.aaaarch.org
[2] http://dsd.lbl.gov/security/Akenti/
[3] http://web.mit.edu/kerberos/www/
[4] http:// www.projectliberty.org/
[5] http://papi.rediris.es

are transparent to the user and compatible with the most commonly employed Web browsers and any operating system. Since PAPI uses standard HTTP procedures, PAPI authentication and authorization does not require any specific hardware or software. It intends to keep authentication as an issue local to the organization the user belongs to, while leaving the information providers full control over the resources they offer.

PERMIS [6]

PERMIS Project has developed a role based access control infrastructure that uses X.509 *attribute certificates* (ACs) to store the users' roles. All access control decisions are driven by an authorization policy, which is itself stored in an X.509 attribute certificate, thus guaranteeing its integrity. All the ACs can be stored in one or more LDAP directories, thus making them widely available. Authorization policies are written in XML according to a DTD.

Microsoft .NET Passport [7]

As part of its .NET initiative, Microsoft has introduced a set of Web services that implement a so-called "user-centric" application model, and that are collectively referred to as *.NET My Services*. At the core of Microsoft .NET My Services is a password-based user authentication and Single Sign-On service called *Microsoft .NET Passport* [Mic02][Mic03]. Microsoft .NET Passport users are uniquely identified with an e-mail address and all participating sites are uniquely identified with their DNS name. Also, Microsoft .NET Passport requires a shared secret for each principal or registered entity. For users the secret is a password, whereas for participating sites the secret is a cryptographic key. In either case, the secrets are centrally stored in a database. The central database also hosts the sign-in/sign-out pages.

SESAME [8]

The *Secure European System for Applications in a Multi-vendor Environment* (SESAME) was a European research and development project aimed at developing a security infrastructure for distributed computing and networking environments [AV99]. It achieved this by including and combining an extended Kerberos authentication service and a privilege attribute service that can be used to provide authorization and corresponding access control services. The privilege attribute service, in turn, is provided by a *Privilege Attribute Server* (PAS) that issues digitally signed *Privilege Attribute Certificates* (PACs).

Shibboleth [9]

Shibboleth, a project of Internet2/MACE, is developing architectures, policy structures, practical technologies, and an open source implementation to support inter-institutional sharing of web resources subject to access controls. In addition, Shibboleth will develop a policy framework that will allow inter-operation within the higher education community. The purpose of the exchange is typically to determine if a person using a

[6] http://www.permis.org/
[7] http://www.passport.net
[8] https://www.cosic.esat.kuleuven.ac.be/sesame/
[9] http://shibboleth.internet2.edu/

web browser (e.g., Internet Explorer, Netscape Navigator, Mozilla) has the permissions to access a target resource based on information such as being a member of an institution or a particular class. The system is privacy preserving in that it leads with this information, not with an identity, and allows users to determine whether to release additional information about themselves.

ITU-T PMIs [10]

An X.509v3 public key certificate can convey authorization information about its owner. The information can, for example, be encoded in one of the X.509v3 standard or extension fields. However, that there are several reasons why caution should be taken in using X.509v3 public key certificates for conveying authorization information. The latest version of the X.509 ITU-T Recommendation [ITU00] specifies the format of an attribute certificate to solve this problem. This certificate is a separate data structure from the public key certificate of the subject, although ITU proposes the binding of both certificates.

SDSI/SPKI [11]

This project have evolved from the argument that a globally unique namespace is not appropriate for the global Internet, and that logically linked local namespaces provide a simpler and more realistic model [Aba97]. As such, work on SDSI also inspired the establishment of a *Simple Public Key Infrastructure* (SPKI) WG within the IETF. The WG was tasked with producing a certificate infrastructure and operating procedure to meet the needs of the Internet community for trust management in as easy, simple, and extensible way as possible.

References

[Aba97] M. Abadi, *On SDSI's Linked Local Name Spaces*, Proceedings of 10th IEEE Computer Security Foundations Workshop, pp. 98-108, June 1997.

[AV99] P. Ashley and M. Vandenwauver, *Practical Intranet Security: Overview of the State of the Art and Available Technologies*, Kluwer Academic Publishers, 1999.

[DS81] D.E. Denning and G. Sacco, *Timestamps in Key Distribution Protocols, Communications of the ACM*, Vol. 24, 1981, pp. 533-536.

[ITU00] ITU-T Recommendation X.509, *Information Technology. Open systems interconnection. The Directory: Public-key and attribute certificate frameworks*, March 2000.

[Lib03] *Liberty ID-FF Architecture Overview*, Version 1.2, 2003

[Mic02] Microsoft, *.NET Passport: Balanced Authentication Solutions*, December 2002.

[Mic03] Microsoft, *Microsoft .NET Passport Review Guide*, March 2003.

[NS78] R.M. Needham and M.D. Schroeder, *Using Encryption for Authentication in Large Networks of Computers*, Communications of the ACM, Vol. 21, pp. 993- 999, December 1978.

[NS87] R.M. Needham and M.D. Schroeder, *Authentication Revisited*, ACM Operating Systems Review, Vol. 21, 1987, p. 7.

[TEM03] M. Thompson, A. Essiari, S. Mudumbai, *Certificate-based Authorization Policy in a PKI Environment*, ACM Transactions on Infomation and System Security, Aug 2003.

[Sch94] J.I. Schiller, *Secure Distributed Computing*, Scientific American, November 1994, pp.72-76.

[SNS88] J.G. Steiner, B.C. Neuman, and J.I. Schiller, *Kerberos: An Authentication Service for Open Network Systems*, Position Paper, Proceedings of the USENIX UNIX Security Symposium, August 1988.

[10] http://www.itu.int/

[11] http://world.std.com/~cme/html/spki.html