International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
©2016 INPRESSCO®, All Rights Reserved
Available at http://inpressco.com/category/ijcet

Research Article

Identity Management in Scholars

Arturo Elías_Ramírez†* and Guillermo Domínguez_Aguilar†

†Electronics System Department, Universidad Autónoma de Aguascalientes, Aguascalientes, México

Accepted 05 Jan 2016, Available online 22 Jan 2016, **Vol.6, No.1 (Feb 2016)**

Abstract

There are many benefits of having an online profile as an academic, thus the use of academic profiling sites is becoming more common, and emerging technologies boost researchers' visibility and exchange of ideas. However researchers are reluctant to maintain multiple profiles, this is due to little overlap between different services and the management of individual identities for each one. So, the integration of online profiling services through an identity mechanism that defines a domain, with servers and clients that share centrally-managed services, where users, machines, services, and polices are all configured in one place, using the same tools and multiple machines can all use the same configuration and the same resources simply by joining the domain. Users only have to sign into services once, and administrators only have to manage a single user account. is the proposal in which our work is supported.

Keywords: *Online Profile, Identity Access Management, Authentication, Authorization, LDAP*

1. Introduction

The benefits for academics using social media (Cragg, 2015):

- Make connections and collaborate with researchers across the globe
- Reach and engage with new audiences
- Disseminate your research, ideas and skills
- Build your reputation outside your own field and institution
- Track the impact of your research

A main finality of online presence are collaborative platforms that allow several institutions hosting their resources, including processes, data, or services. Thus, the complexity of this heterogeneous systems such as Cloud systems has made security issues and enforcement one of the most challenging task (Bouchami and Perrin, 2014). Security models should lay on identity management and identity must become persistent through any given process spanning multiple applications and organizations (Windley, 2005). Besides considering digital identity management as one of the security pillar, it is also considered as one of the major enablers of e-business (Ben Ayed, 2014). The question is what identity actually is in the aspect of digital technology. Identification actually establishes unique digital identities (Bogicevic *et al.*, 2014). There are numerous definitions, but we can say that identity is something that describes an individual person with a set of attributes such as naming, credentials, privileges; identification is a key to establish relations with other objects. In other way authentication is the act of identifying one actor to another.

Currently, the university's authentication system mainly in the following questions:

1. Management of individual identities, as a user to enter different applications, you need to input each different account number and password. Users may find their need to remember that the application system account and password is also increasing. This is easy to generate the password that is forgotten, it could cause some users account and password for the convenience of the memory, in a number of applications use the same account and password.
2. Authentication and authorization, the application systems have a separate authentication and access control policy. Additional applications, as useless unified authentication and access control policy specification constraints, resulting in authentication and access control code duplication and development, and independent, is not conducive to cross-system integration.
3. Privileges, permissions and within or across systems, when each application for their users to add, delete, and modify the permissions, in order to maintain different user roles and permissions application consistency and integrity, and only on the relevant application system interoperability,

*Corresponding author: **Arturo Elías_Ramírez**

this operation is complex and error-prone, easily leads to different application systems that are having inconsistent user roles and permissions.

In order to solve the current campus network, the application of existing authentication systems and access control issues, the establishment of a unified service for all applications authentication and access control platform, unified identity authentication, user rights, and reasonable access control is necessary.

2. LDAP and Identity Access Management

2.1 Lightweight Directory Access Protocol (LDAP)

LDAP stands for Lightweight Directory Access Protocol. As the name suggests, it is a lightweight client-server protocol for accessing directory services, specifically X.500-based directory services. LDAP runs over TCP/IP or other connection oriented transfer services. LDAP is defined in RFC2251 "The Lightweight Directory Access Protocol (v3). There are many different ways to provide a directory service. Different methods allow different kinds of information to be stored in the directory, place different requirements on how that information can be referenced, queried and updated, how it is protected from unauthorized access, etc. Some directory services are local, providing service to a restricted context (e.g., the finger service on a single machine). Other services are global, providing service to a much broader context (Sermersheim, 2006).

LDAP directory service is based on a client-server model. One or more LDAP servers contain the data making up the LDAP directory tree or LDAP backend database. An LDAP client connects to an LDAP server and asks it a question. The server responds with the answer or with a pointer to where the client can get more information (typically, another LDAP server). No matter what LDAP server a client connects to, it sees the same view of the directory; a name presented to one LDAP server references the same entry it would at another LDAP server. This is an important feature of a global directory service, like LDAP.

2.2 Identity Access Management

The only way to control identity is by identity management. That is the system and framework used in computer or communication systems, and it is an integrated system of business processes, policies, and technologies. An identity management system provides the tools for managing these partial identities in the digital world. Each identity consists of different attributes and relationships with other entities. The identity provider is responsible for the processes associated with giving a subject some role and establishing and maintaining the electronic identity (Senk and Dotzler, 2011).

Identity access management (IAM) can be divided into four major areas: Authentication, Authorization, User Management and Central User Repository. The IAM components are grouped under these four areas. The ultimate goal of the IAM is to provide the right people with the right access at the right time (see the Figure 1 below What is Identity & Access Management?).

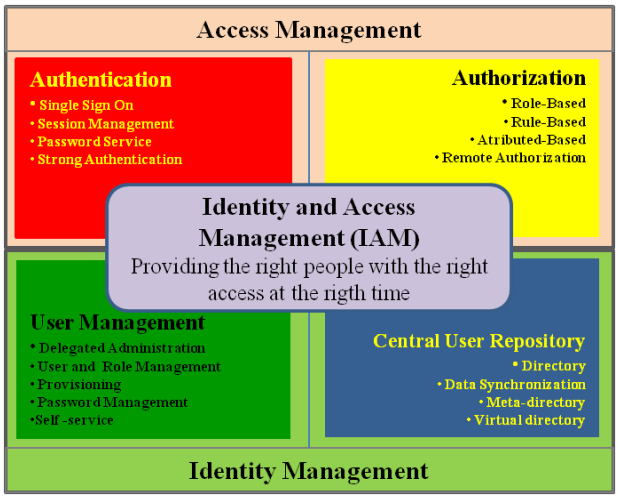

Fig.1 What is Identity & Access Management?

The task of assuring authorized access to services in distributed environments is performed by an identity and access management system. The distinctive feature of IAM systems to other distributed systems is the handling of sensitive user data that raises privacy concerns (Schell *et al*., 2009).

Identity Management is as a set of technical models, which are classified into four categories based on identity's scope. The identity management paradigms in computing are analogous to real-life practices. In fact, the scope of an individual identity varies from one person to another. A person may be known only to his or her family, immediate neighbors, or a workplace; another person can be known throughout his or her locality or a much bigger geography; while another person is known over the globe. The scope of identity in computing follows the same logic: (1) local identity model such as local registry management of users; (2) network identity model such as cross-domain Kerberos and PKI cross-certification implementations; (3) federated identity in which cross organizational trust or circle of trust is a foundation; and (4) global Web identity such as meta-directory, virtual-directory, and OASIS Extensible Resource Identifier (XRI) and Extensible Data Interchange (XDI) infrastructure implementations (Benantar, 2006).

There are different approaches for realizing access control like discretionary access control (DAC), mandatory access control (MAC) or more sophisticated ones like role-based access control (RBAC) (Sandhu *et al*., 1996) or attribute-based access control (ABAC) (Yuan and Tong, 2005) that are more likely to be used in a distributed environment (Benantar, 2006). The basic principle behind ABAC is to use attributes for making authorization decisions to achieve more scalability than identity-based access control (Schell *et*

al., 2009). The eXtensible Access Control Markup Language (XACML) is an XML-based standard for specifying access control policies, which can be processed to determine authorization decisions (IETF, 2013).

Authentication and authorization infrastructures support service providers to outsource security services to 3rd party providers (Schlaeger and Pernul, 2005). This raises the overall level of security, provides a flexible access control model like ABAC, and eases the usability through, e.g., single sign-on (SSO) mechanisms (Schlager *et al*., 2006). Furthermore specific user data, e.g., user profiles, buying patterns, and earned privileges, can be gathered and transferred federation-wide for authorizing access to service providers based on actual data of federation members.
So, every networked machine needs accounts and authentication services. From small startups to big enterprises, from cloud deployments to on-premise, every system admin or develop environment faces the problem of managing users, administrators, systems, their credentials and keys, and control and coordinate access. Purpose built Identity Management systems reduce errors, and improve productivity of both administrators and users by simplifying management.

3. Implementation of IAM

An ideal solution to implement an IAM should have the following features: central location (but with redundancy), secure but easy to use, based on industry standards, SSO mechanisms, allow access control (and self-service) on data, privilege delegation and separation. These features are a way to create identity stores, centralized authentication, domain control for Kerberos and DNS services, and authorization policies.
The goal of IAM is to simplify that administrative overhead. Users, machines, services, and polices are all configured in one place, using the same tools. Because IAM creates a domain, multiple machines can all use the same configuration and the same resources simply by joining the domain. Users only have to sign into services once, and administrators only have to manage a single user account.

The closest relative to Identity Management is a standard Lightweight Directory Access Protocol (LDAP) directory. In LDAP, authentication is supplied in the "bind" operation. Ldapv3 supports three types of authentication: anonymous, simple and *Simple Authentication and Security Layer* (SASL) authentication. A client that sends a LDAP request without doing a "bind" is treated as an anonymous client. Simple authentication consists of sending the LDAP server the fully qualified Domain Name of the client (user) and the client's clear-text password. This mechanism has security problems because the password can be read from the network. To avoid exposing the password in this way, you can use the simple authentication mechanism within an encrypted channel (such as SSL), provided that this is supported by the LDAP server.

LDAP server is the base stone of the whole IAM solution. It serves as a data backend for all identity, authentication and authorization services and other policies, but there are some intrinsic differences between what they do and what they're intended to do. The primary feature of an LDAP directory is its generality. It can be made to fit into a variety of applications.

Identity Management, on the other hand, has a very specific purpose and fits a very specific application. It is not a general LDAP directory, it is not a backend, and it is not a general policy server. It is not generic. A solution to provide integrated infrastructure catering for the requirements outlined above comprises of directory, identity management, provisioning and presentation services, illustrated in architecture as outlined in the diagram below.

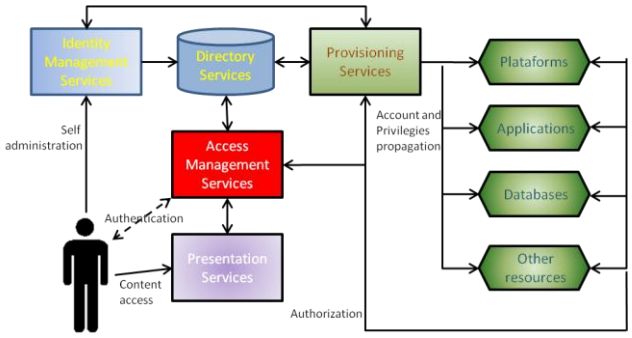

Fig.1 Identity and Access Management Infraestructure Adapted from (Lewis, 2002)

4. Results and Discussions

In this paper, the basic rule is to maintain a concept of identity of reference for scholar community members with information only about their recovery with it. Identity is administered in a single point of control, creating login credentials for those services that integrate this identity. Thus, if the identified personnel required access a particular service, they should present their unique credentials (usually an account and password) and if they have the appropriate permissions, they can manipulate the services according to their convenience, improving the productive impact and their collaborative teaching and research activities.

The information is managed under the rules of operation defined by the academic institution, balancing the standards of information transparency, but under the standby arrangements privacy thereof that is sensitive to each of its members. At the moment, digital presence services that are active and available depending on the level of integration of each, for every member when processing digital integrity scheme are shown in Table 1.

The identity management service, as already mentioned, is the engine that integrates the rest of the available platforms, besides being the supplier of unique authentication credentials based on a reliable

scheme. Likewise manages the information of members of the institution with respect thereto.

Table 1 Experimental procedure parameters

Service	Access Mode		
	Digital Identity	Registration process	Other
Teaching process	✓		
Web hosting	✓		
Social academic Networking	✓	✓	
Cloud services	✓		✓
Chat	✓	VoIP	XMPP
Virtual classrooms	✓		
Digital meetings	✓		
E-mail	✓		
Calendar and Event scheduling	✓		
Survey application	✓	✓	
Electronic library	✓	✓	
Management and monitoring projects	✓	✓	
Storage and media publishing		Local registration process	
Applications services and remote desktops in Windows		✓	Digital identity sincronization

From the table it is clear that all platforms are linked through a single identification service, where although you need to enter credentials for each independently, these credentials are the same for all platforms.

Conclusions

Identification of the function is repeated in the design and implementation, distributed in various application systems, resulting in substantial waste of time and money. In this paper, a unified authentication system to achieve the specific technology used, the key question is described in detail.

Key applied to this project is the integration, the need for multiple integrated and secure modern digital services advanced, who being used by the academic community provide it substantial benefits, whether in service quality or in streamlining their daily activities, thereby presenting a concurrent and ubiquitous access to all the information generated and controlled by an integrated digital identity.

At the time have been configured several service platforms, which support authentication and authorization policies for identities, creating mutual trust with other Identity Management systems like Microsoft Active Directory.

The next stage of this project is to achieve the academic exploit the potential of this set of integrated services through a unified identity scheme

References

Ben Ayed G. (2014) Digital Identity Management, Architecting User-Centric Privacy-as-a-Set-of-Services, Springer International Publishing. pp. 57-95.

Benantar M. (2006) Foundations of Security and Access Control in Computing, Access Control Systems, Springer US. pp. 1-39.

Bogicevic M., Milenkovic I., Simic D. (2014) Identity Management–A Survey. Innovative Management and Firm Performance: An Interdisciplinary Approach and Cases:370.

Bouchami A., Perrin O. (2014) Access Control Framework Within a Collaborative PaaS Platform, in: K. Mertins, *et al*. (Eds.), Enterprise Interoperability VI, Springer International Publishing. pp. 465-476.

Cragg E. (2015) Benefits and concerns of using social media as an academic, in: Piirus (Ed.), Warwick, UK.

IETF. (2013) eXtensible Access Control Markup Language (XACML) XML Media Type, Request for Comments: 7061.

Lewis J. (2002) The Emerging Infrastructure for Identity and Access Management, Security Forum in Anaheim: 23 January 2002, The Open Group, Anaheim, Cal.

Sandhu R.S., Coyne E.J., Feinstein H.L., Youman C.E. (1996) Role-based access control models. Computer:38-47.

Schell F., Dinger J., Hartenstein H. (2009) Performance Evaluation of Identity and Access Management Systems in Federated Environments, in: P. Mueller, *et al*. (Eds.), Scalable Information Systems, Springer Berlin Heidelberg. pp. 90-107.

Schlaeger C., Pernul G. (2005) Authentication and Authorisation Infrastructures in b2c e-Commerce, in: K. Bauknecht, *et al*. (Eds.), E-Commerce and Web Technologies, Springer Berlin Heidelberg. pp. 306-315.

Schlager C., Nowey T., Montenegro J.A. (2006) A reference model for Authentication and Authorisation Infrastructures respecting privacy and flexibility in b2c eCommerce, Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on. pp. 8 pp.

Senk C., Dotzler F. (2011) Biometric authentication as a service for enterprise identity management deployment: a data protection perspective, Availability, Reliability and Security (ARES), 2011 Sixth International Conference on. pp. 43-50.

Sermersheim J. (2006) Lightweight Directory Access Protocol (LDAP): The Protocol, in: IETF (Ed.), RFC 4511, Network Working Group.

Windley P.J. (2005) Digital identity " O'Reilly Media, Inc.".

Yuan E., Tong J. (2005) Attributed based access control (ABAC) for web services, Web Services, 2005. ICWS 2005. Proceedings. 2005 IEEE International Conference on, IEEE.