A COLLABORATIVE SECURITY MECHANISM BASED ON REPUTATION AND TRUST LEVEL IN PERVASIVE SYSTEMS

Mohammed Nadir Djedid
Department of Computing, University of Sciences and Technology of Oran, Oran, Algeria

Keywords: Pervasive Systems, Identity Protection, Identification/Authentication, Collaborative Security Mechanism.

Abstract: The emergence of network technologies and the appearance of new varied applications in terms of services and resources, has created new security problems for which existing solutions and mechanisms are inadequate, especially problems of identification and authentication. In a highly distributed and pervasive system, a uniform and centralized security management is not an option. It then becomes necessary to give more autonomy to security systems by providing them with mechanisms that allows a dynamic and flexible cooperation and collaboration between the actors in the system.

1 INTRODUCTION

The rapid development of mobile computing has given rise to ubiquitous information systems: the user has at any time, access to the global network regardless of location or time ("anywhere - anytime" access).

The challenge of pervasive systems is in this perspective, to provide methodological frameworks and protocols to permit the reliable, relevant and efficient use of these systems. (Girma, 2006).

But this new trend reveals new security problems for which solutions and existing mechanisms are inadequate, especially for the problems of identification and authentication. In a highly distributed and pervasive system, a centralized and homogenous security management is not conceivable. It then becomes necessary to give more autonomy to security systems, providing them with mechanisms allowing a dynamic and flexible cooperation and collaboration between the actors in the system.

This paper will be an overview of the main existing security systems and compare their effectiveness and their ability to meet the major identified security constraints of pervasive systems like: Decentralization, Interoperability and Interaction, Autonomy, Transpareancy and Proactivity, Trust management, Scaling, and Privacy protection. Finally, a generic architecture of a security mechanism based on reputation and trust level will be proposed.

2 IDENTITY AND PRIVILEGES MANAGEMENT SYSTEMS

2.1 Systems based on Identity Management

2.1.1 Radius

In Radius (Rigney and Al., 1997) the user sends an Access-Request containing his/her authentication information, and sends it to the server. The server processes the request locally if it recognizes the user, otherwise, it acts as a RADIUS Proxy "or intermediate" by transmitting it to another server.

2.1.2 LemonLDAP

Two connection modes exist in LemonLDAP approach (Wiki.LemonLDAP, 2007). In the pull mode, when a user wants to access a protected application, the system asks the user's name and password. Thus, after a successful authentication, the user is redirected to the resource that he/she seeks. In agent mode, the authenticated user accesses a menu containing all the applications on which he has access permissions.

Djedid M..
A COLLABORATIVE SECURITY MECHANISM BASED ON REPUTATION AND TRUST LEVEL IN PERVASIVE SYSTEMS.
DOI: 10.5220/0003837902580261
In *Proceedings of the 2nd International Conference on Pervasive Embedded Computing and Communication Systems* (PECCS-2012), pages 258-261
ISBN: 978-989-8565-00-6

2.1.3 OpenID

Open ID (Recordon and Reed, 2006) permits to federate unique authentications and share attributes. It provides the ability to authenticate to multiple sites using a unique identifier OpenID.

2.1.4 Liberty Alliance

Liberty Alliance (Alsaleh and Adams, 2006) proposes to combine the requirements of strong authentication (authentication of multiple attributes) by respecting the user's privacy.

Just like OpenID, Liberty Alliance allows the users with a single account to access multiple services from different providers, but under the condition that they must belong to the same "circle of trust".

2.1.5 Shibboleth

Shibboleth (Shibboleth Development Team, 2009) is an authentication mechanism, which permits to federate the identification and supply, as the mechanisms presented above, two possible applications: authentication delegation and sharing attributes.

2.1.6 Ws-security

WS-Security (OASIS, 2004) is a security protocol called "point to point", which is dedicated to the message exchange of information between web services. Based on a mechanism of security tokens, it is associated with digital signatures to authenticate messages. Security tokens provide the identity of the message sender, which is proved by an authentication mechanism.

2.2 Systems based on Privilege Management

2.2.1 Akenti

Akenti (Thompson and Al., 1999) is an architecture designed to provide security services in a completely distributed environnement.

The strength of Akenti is the autonomy offered to the user who has the right to negotiates access to a resource, by using authorization certificates.

2.2.2 Permis

Permis (Chadwick and Otenko, 2003) includes a mechanism of static authority delegation. Thus, each actor defines trust authorities having the right to assign roles. In addition, a new version of Permis (2006), can delegate authority dynamically, by creating a chain of delegation.

The spread of trust by the chain of delegation is considered as a breakthrough in the Permis project. It allows the extension of security policies, but obliges the authorities delegated to describe manually the trusted entities who can take advantage of privileges by the delegation.

2.2.3 Cas

CAS (Pearlman and Al., 2002) is a protocol dedicated to control management in virtual organizations (VO) like grid computing. CAS assumes the role of supreme authority of a virtual organization and allows to manage resources and users between organizations working together in a common project.

2.2.4 Voms

Virtual Organization Management Service (Alferi and Al. 2004) closely resembles the CAS. The major difference lies in the authorization mechanism. Indeed, like if in CAS, the attributes concerning the list of roles and groups members of the VO are stored in the voms server, the authorization rules are presented in the resource, which obtains the power to decide the user's right.

2.2.5 O2O

O2O (Cuppens and Nora cuppens-Boulahia, 2006) is a security system for building a VO from several VPOs (Virtual Private Organizations). Like a VPN (Virtual Private Network), an VPO creates a bridge between two organizations.

The policy of access control uses the same federation mechanism as Liberty Aliance, so that a unique profile can be attributed to each member an organization and can thereby take advantages of the privileges with the organizations linked to this VPO gateway.

2.2.6 Sygn

In sygn (Seitz, Pierson and Brunie, 2005) permissions are defined in the form of certificates stored at the owner. For the creation of such permissions, no interaction with a centralized system is necessary, which makes it one of the Sygn's strengths. Sygn also offers the possibility to define a permission on a set of resources.

2.2.7 Gaia Os

Gaia OS Security (Roman and Al., 2002) authenticates the user through different devices and protocols. A number between 0-1 is assigned to each device after authentication, which represents a measure of trust in the device or protocol.

The advantage of GAIA OS, and in contrast to the mechanisms seen previously, is that the entity is measured digitally and not binary.

2.2.8 Tacp

TACP (Giang and Al., 2007) (Trust-Based Access Control Policy) uses the concept of reputation evoked earlier. The proposed approach begins by estimating the value of trust that can be given to the request sent by the user. In practice, each user is assigned a confidence value between 0-1. Similarly, each resource is a confidence level also included in the interval [0,1]. Thus, if a user has a confidence level higher than the confidence level of the resource requested, he/she will be allowed, otherwise the application will be rejected.

3 SYNTHESIS

This section will be dedicated to the comparison between the different approaches presented above, in relation to the major security needs of pervasive systems. The result of the comparison is summarized in two tables. The following two mentions are used:

- Y: Yes the need is supported by the solution.
- N: No the solution is not adapted for this need.

Table 1: Comparison of systems based on identity management.

Constraints	Systems based on identity management.					
	RADIUS	**Lemon.**	**OPENID**	**Liber.**	**Shib.**	**WS**
Decentralization	Y	N	Y	Y	Y	Y
Interoperability	Y	N	Y	Y	Y	Y
Trust spread	Y	N	N	N	N	Y
Traceability	Y	Y	Y	Y	Y	Y
Autonomy	Y	N	Y	Y	Y	Y
Transparency and proactivity	Y	Y	Y	Y	Y	Y
Flexibility	N	N	N	N	N	Y
Privacy Protection	N	N	Y	Y	Y	N
Scaling	Y	N	Y	N	N	Y

Table 2: Comparison of systems based on privilege management.

Constraints	Systems based on privilege management.							
	Akenti	Permis	CAS	Voms	O2o	Sygn	GAIA.	TACP
Decentral.	Y	N	Y	N	Y	Y	Y	Y
Interoperab.	Y	Y	Y	Y	Y	Y	N	N
Trust spread	N	Y	Y	N	N	Y	Y	Y
Traceability	N	Y	N	N	N	Y	Y	N
Autonomy	Y	Y	Y	Y	Y	Y	N	Y
Transparen./ proactivity	N	N	N	N	N	N	Y	N
Flexibility	N	N	N	N	N	N	Y	N
Privacy Protection	N	N	N	N	N	N	N	N
Scaling	N	Y	Y	Y	Y	Y	N	Y

4 A COLLABORATIVE SECURITY MECHANISM BASED ON REPUTATION AND TRUST LEVEL

In order to fully exploit the concept of spreading the trust to interconnect security systems of various domains, we propose a generic architecture in which different modules are shown in Figure 1:

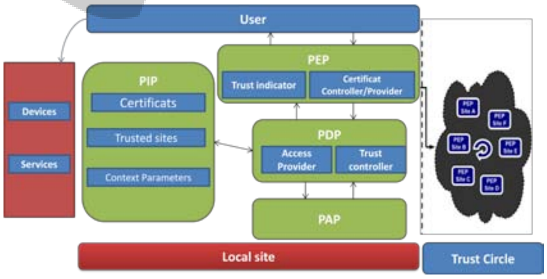

Figure 1: A collaborative security mechanism based on reputation and trust level.

PEP: Is the external interface of the architecture through which pass all the information in the form of certificates, it has a particular module called "Trust indicator" and reflects the reliability level of the site, the site's reputation, the number of links of trust with other sites etc. All these information are used to assign a trust level to the site. The interface can also verify the veracity of the certificates exchanged between the system and the outside thanks to the controller of certificates, and provide certificates commanded by the PDP, to be sent to entities (user, device).

PDP: Allows filtering access to the system via the trust controller, and deciding to establish or revoke the trust with the sites. It also allows applying the security policy defined in the PAP module.

PAP: Is the module where the access control policy is defined.

PIP: Allows the capture of the user's context (device used, connection type etc.). It also maintains a table of trusted sites updated by the trust controller module of PDP.

5 CONCLUSIONS

Through this study we came to the conclusions that the concept of the propagation of trust in a dynamic way is not fully exploited to interconnect the security policies in various fields. Reply to this lack could bring us closer to our goal of protecting the identity of the users, and this in "globalizing" the SSO system across domains: a single sign-on (SSO) would not only provide access to several domain resources belonging to the user, but also the resources of the areas of trust where the user goes, without being forced to decline again its identity. This would avoid to re-circulate the information of identification / authentication at the risk that it would be intercepted by a third party.

Therefore, we proposed a generic architecture, setting up a collaborative security mechanism based on reputation and trust level accumulated by each domain towards its peers. This work is a first step on designing our architecture, and the future works will be focused on calculating the value of the trust level by providing a function that calculates this value.

REFERENCES

Girma, B., 2006. *Thesis: Accès et adaptation de contenus multimédia pour les systèmes pervasifs*. INSA Lyon.

Rigney, C., Rubens, A., Simpson, W., Willens, S., 1997. RFC 2138*: Remote Authentication Dial In User Service (RADIUS).*

Wiki.LemonLDAP,2007 *http://wiki.lemonldap.objectweb.org.*

Recordon, D., Reed D., 2006. OpenID 2.0: a platform for user-centric identity management. In *The 2nd ACM workshop on digital identity management, pp.11-16,* ACM Press, Virginia, USA.

Alsaleh, M., Adams, C., 2006. Enhancing Consumer Privacy in the Liberty Alliance identity Federation and Web Services Frameworks *Workshop on Privacy Enhancing Technologies, pp. 59-77*, Cambridge, UK.

Shibboleth Development Team, 2009. Shibboleth Project, *http://shibboleth.internet2.edu/.*

OASIS, 2004. Web Services Security Specification. *http://www.oasis-open.org/.*

Thompson, M., Johnston, W., Mudumbai, S., Hoo, G., Jackson, K., Essiari, A., 1999. Certificate-based access control for widely distributed resources. In *SSYM 08': 8th Conference on USENIX Security Symposium, p.17,* USENIX Association Berkeley, USA.

Chadwick, D., Otenko, A., 2003. The PERMIS X.509 role based privilege management infrastructure. *Future Generation Computer Systems Journal, Vol 19, No 2, pp.277-289.*

Pearlman, L., welch, V., Foster, I., Kasselman, C., Tuecke, S., 2002. A Community Authorization Service for Group Collaboration. In *POLICY 02': 3rd International workshop on policies for Distributed Sustems and Networks, pp.50-59,* IEEE Computer Society, Washington, USA.

Alferi, R., Cecchini, R., Ciaschini, V., Dell'Agnello, L., Frohner, A., Gianoli, A., Lörentey, K., Spataro., F., 2004. VOMS, an Authorization Systemm fort Virtual Organizations. In *European Across Grids Conference, pp.33-40,* Verlag, Spain.

Cuppens, F., Nora cuppens-Boulahia C., 2006. O2O: Managing Security policy Interoperability with Virtual Private Organizations. In *ICISS 06'. 2nd International Conference on Information Systems Security, pp. 101-115,* Kolkata, India.

Seitz, L., Pierson, J., Brunie, L., 2005. Sygn : A certificate based access control in Grid environnements. Tech Rep. INSA Lyon, France.

Roman, M., Hess, C., Cerqueira, R., Ranganathan, A., Campbel, R., Nahrstedt, K., 2002. Gaia: A Middleware Infrastructure for Active Spaces. In *IEEE Pervasive Computing Vol.1, No 4, pp. 74-83*.

Giang, P., Hung, L., Lee, S., Lee, Y., Lee, H., 2007. A flexible Trust-based Access Control mechanism For Security and Privacy Enhancement in Ubiquitous Systems. In *MUE 07', International Conference on Multimedia and Ubiquitous Engineering, pp.698-703,* IEEE Computer Society, Washington, USA.