Journal of Information Systems and Communication
ISSN: 0976-8742 & E-ISSN: 0976-8750, Volume 3, Issue 1, 2012, pp.- 207-209.
Available online at http://www.bioinfo.in/contents.php?id=45

CONCEPTUALIZATION OF PRIVACY AWARE ACCESS CONTROL IN WEB SERVICES PARADIGM

REKHA BHATIA[1] AND MANPREET SINGH[2]

[1]GTBIT, Rajouri Garden, New Delhi, India
[2]Punjabi University, Patiala, India
*Corresponding Author: Email-

Received: January 12, 2012; Accepted: February 15, 2012

Abstract- The conveniences offered by the latest era of dynamic web services technology, its ability to make our lives easier by performing an endless number of tasks at a faster pace and in a more efficient manner, we have given it free rein in our lives, with little thought about privacy implications. These days, massive data about individuals is available in government e-databases as well as other web databases, which can be readily accessed by persons with malicious intentions and privacy as a fundamental human right is endangered. The reason behind this is the open nature of web and ever increasing number of web services which make it easier to share information among databases and applications. This ease of web is giving rise to privacy invasion. The goal of privacy aware access control is to automate privacy management for providing better compliance to the needs of the service provider and service requester and ensure that personal data is accessed not only based on security policies but also on privacy policies. In this paper, we have proposed a conceptual model of how privacy parameters can be introduced in prevailing access control mechanisms
Keywords- Access Control, Privacy, Web Services, Security policy, P3P

Citation: Rekha Bhatia and Manpreet Singh (2012) Conceptualization of Privacy Aware Access Control in Web Services Paradigm. Journal of Information Systems and Communication, ISSN: 0976-8742 & E-ISSN: 0976-8750, Volume 3, Issue 1, pp.-207-209.

Introduction

Web services are a part and parcel of our daily life in modern society. These are a platform independent way to establish communication between two applications connected through a network. The world is overwhelming with web based services and enterprises need to share their databases and applications to work together efficiently.

To fulfill these needs, enterprises are using Service Oriented Architecture (SOA) [2]. In spite of the many benefits offered by SOA, designing an SOA based application involves many issues and the most daunting issue is the security. A web service may expose a company's secure back office and business logic for transactions to the public, potentially opening up a large security hole for hackers.

Many transactions cannot be completed without revealing personal information (PI). This disclosure of PI is leading to growing concerns about privacy.

Now a days, millions of web users have two identities, one actual and the other digital. In the real world, disclosure of personal data is controllable by the user but the same is not true in the web based digital world. Access control is about making sure that only those who are entitled to something can get to it.

The lock on a table's drawer is an example of access control. If it is functioning properly, it ensures that only the authorized user can get access to the items placed in drawer. But if the drawer is accidentally left open, then unauthorized users can get an access to the items placed inside it. A similar concept exists in context of access control to web services covering three aspects: authentication, authorization and audit, which correspond respectively to the questions such as `whether the user is what he claims to be', `whether the user is allowed to get an access of something' and `how the user is accessing or has already accessed the resource'.

There are three components of traditional access control systems

- Security Policies (what is allowed & what is not allowed).
- Model of Access Control (Formal representation of Security Policies).
- Mechanism of Access Control (Procedure for enforcing the

Access Control).

Access control systems are of generally of two types

- Discretionary Access Control System (DAC): Resource owners specify the policies about who has access to the resource.
- Non Discretionary Access Control (NDAC): Policies are not specified at the discretion of the user. Some of the common NDAC techniques are Mandatory Access Control (MAC), Role Based Access Control (RBAC) and Context Based Access Control (CBAC) [6, 8, 11].

This paper is organized as follows:

a. In the next section, privacy issues in web services paradigm are discussed.
b. In section 3, generic components of a privacy aware access control model are described.
c. In section 4, a novel privacy aware access control model is proposed based on granularity, purpose, visibility and retention.
d. In section 5, this paper is concluded with the finding that there is an urgent requirement to develop formal methods based techniques for automating the checking mechanisms for privacy policies matching.

Privacy Issues In Web Services Paradigm

In web services paradigm, no matter the service is simple or complex, the requester as well as provider of the service has to disclose some personal information in order to utilize the service. So the privacy issues will always exist. The problem becomes serious when the disclosed personal information is shared with a third party without the user consent. Further, in dynamic web scenarios, such as web services, a data provider can change his mind during the course of transaction due to change in trust level with the data recipient based on his interaction upto that point in time. So suitably representing desired privacy levels in such highly dynamic web scenarios is a complex challenge.

According to Barker et al [5], data privacy has four major aspects, i.e., purpose, visibility, granularity and retention. Purpose stands for the motivation behind providing personal information to the data collector, for example, a patient may provide detailed description about his disease to a doctor for the treatment purpose. Visibility defines the persons who are authorized to access the personal information provided by a service user, for example, the patient has given consent to the doctor to view his personal data and not to any third party like his insurance company resulting into financial loss.

This aspect of privacy is of utmost importance in Web Services context as personal information can potentially be made available to third parties, the data provider has not imagined. The granularity defines the generalization level of precise details of user data to be made available in response to a query, for example, information that a person's name is 'R.B' is more generalized as compared to the name 'Rekha Bhatia' and is disclosing minimum information about a person. Retention defines the period after which the collected data for a specific purpose should be removed from the service data store, for example, personal information collected for a particular purpose should not be retained after the 'expiry date' of that purpose fulfillment by the service provider.

The traditional access control models cannot preserve privacy due to the lack of considering these important aspects of privacy in access control decisions. Thus purpose of access, granularity of access as well as environment conditions prevailing during the access are the core additional elements in our privacy aware access control model.

Components Of Privacy Aware Access Control

General components of a privacy aware access control model are:

a. Subjects (S): Entities that want to access the resources provided by the service.
b. Objects (O): Targetted resource provided by the service for which access is required.
c. Permissions (PERM): Actions performed by the Subjects on the Objects, for example, who can do what?
d. Granularity (G): It represents privacy sensitivity value of Objects, i.e, exposure level of resource allowed to the user based on his clearance level, for example, depending upon the permissions, we can set the exposure level of a data resource for some role as one of these three values: FINE_DETAILS, FINER_DETAILS, FINEST_DETAILS.
e. Purpose of Access (P): It specifies how the collected data is going to be used? Data collected for one purpose should not be used for another purpose.
f. Environmental Conditions (E): Environmental conditions prevailing at the time of access, for example, an accountant in a bank can view the A/C information of a depositer from, say, 9 a.m to 7 p.m but a doctor can view the patient records at any time depending upon how critical his condition is?

Conceptual Model For Privacy Aware Access Control In Web Services Paradigm

Even though various standards for securing Web Services currently exist, but none of them is based on strong theoretical foundations. There is a need of an access control mechanism which can check and validate consistency of security policies. Secondly, the implementation mechanisms for access control policies should be independent of the underlying technology. Apart from this, there is a lack of consistent methodology based on sound theoretical grounds for integrating privacy considerations into access control mechanism. We have outlined the motivation for defining privacy aware access control mechanism in Web Services environment as follows:

a. Business Enterprises involved in Web based transactions don't want to lose control of their critical resources and disclose their confidential information. They want their access control systems to be extensible and adaptable to fast changing business scenarios.
b. Access control policies should not be dependent on underlying platform and technologies.
c. Access control security policies should not assign permissions for executing Web Services operations to individuals rather permissions should be assigned to roles.
d. Access control policies should provide integrated support for incorporating privacy into traditional access control systems.

We have developed our model based on the observations made by Cassasa Mont [1] and Li et al [12]. This model is also based on W3C standards like P3P, EPAL and XACML [3] [4] [7]. In our privacy aware conceptual access control model, the access decision

is arrived in the following steps:

i. The requester application sends its credentials/identification information to the privacy aware policy enforcement point (PEP).
ii. This PEP software sends the credentials for verification to the policy decision point (PDP).
iii. The privacy information like sensitivity value of data, the granularty of access to be allowed and the purpose and context of access along with general access control policies are provided to the policy decision point.
iv. The policy decision point sends the access decision to the privacy aware policy enforcement point.
v. Based on the access decision, the requested information is rtrieved from the data store.
vi. The retrieved information is then provided to the policy enforcement point.
vii. Based on the privacy policy, the policy enforcement point filters the information and provides the required data to the requesting application.

Conclusions

Web Services pose several challenges for keeping personal information private. The reason behind this is the open nature of Web and Web Services which make it easier to share information among databases and applications. This ease of web is giving rise to privacy invasion. The goal of privacy aware access control is to automate privacy management for providing better compliance to the needs of the service provider and service requester and ensure that personal data is accessed not only based on security policies but also on privacy policies. The proposed access control framework will ensure that personal information is accessed by two or more communicating parties if agreed privacy policies and preferences are satisfied. Secondly, the purpose aware access control mechanism, proposed in this paper, integrates privacy & purpose in traditional Role Based Access Control Mechanism. To enable information sharing across Web Services, policies of all the involved services that receive information pertaining to a given service requester should comply with privacy preferences of the requester. To achieve this goal, formal methods based techniques for automating the checking mechanisms for privacy policies matching and privacy preference compliance need to be developed.

References

[1] Casassa Mont M., Thyne R., Chan K., Bramhall P. (2005) *http://www.hpl.hp.com/techreports/2005/HPL-2005-110.pdf* .
[2] Nina Godbole, *Information Systems Security, Wiley India Pvt Ltd*, ISBN -978-81-265-1692-6, 680-712.
[3] World Wide Web Consortium (2007) *Platform for Privacy Preference (P3P) Project*.
[4] IBM, (2004) *The Enterprise Privacy Authorization Language*.
[5] Barker K., Askari M., Banerjee M., Ghazinour K., Mackas B., Majedi M., Pun S. and Williams A. (2009) *BNCOD*, 42-54.
[6] Min Wu, Jiaxun Chen and Yongsheng Ding (2006) 5*th WSEAS International Conference on Telecommunications and Informatics*, 41-45.
[7] OASIS,(2011) *eXtensible access control markup language* 2.0.
[8] David F. Ferraiolo and Richard Kuhn D. (1992) *15th NIST-NSA National Computer Security Conference, Baltimore, Maryland*.
[9] Bell E., La Padula L.J., *Technical Report MTR-2997, The Mitre Corporation, Burlington Road, Bedford, MA* 01730, USA.
[10] Samarati P. (2002) *32 Jahrestagung der Gesellschaft f¨ur Informatik*, 114-119.
[11] Department of Defense (1985) *Trusted Computer Security Evaluation Criteria, DOD* 5200.28-STD.
[12] Li M., Wang H. and Plank A. (2009) *Thirty-Second Australasian Computer Science Conference*, 93-100.