International Journal of Computer Networks and Communications Security

VOL. 3, NO. 9, SEPTEMBER 2015, 367–372
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

Privacy Issues in Access Control of Web Services: An Appraisal

REKHA BHATIA[1] and MANPREET SINGH[2]

[1] Punjabi University Regional Centre, Mohali

[2] Punjabi University, Patiala

E-mail: [1]r.bhatia71@gmail.com, [2]msgchd@gmail.com

ABSTRACT

Privacy is the right of individuals to determine for themselves when, how and to what extent information about them is communicated to others. Due to the rapid growth in popularity of web services, the complexity of their access control policies is also rising, thus, increasing the likelihood of inadvertent privacy disclosures. Anyone involved in e-business transactions would believe that it is axiomatic that privacy is a building block of effective collaborations of web services. Most of the stakeholders are reluctant to use web services as they are not confident about the privacy preservation of their credentials and this attitude is hampering the growth of web based businesses. These web services collect, store, process and share information about lakhs of citizens, who have different notions and preferences related to their Privacy. This promotes a number of ethical, legal and technical issues that must be addressed at a global level to preserve online privacy of e-Citizens. This paper provides an appraisal of privacy related works in web services access control process.

Keywords: *Access Control, Trust, Web Services, Privacy, Service Collaborations.*

1 INTRODUCTION

Access control is a mean to protect information. It aims to control access to information within the information systems. The access control process is established with the two main security goals: Protecting the information and resources of the system from unauthorized access and preventing unauthorized alterations of the data and resources. A definition of access control is given by Samarati et al. [1]: "The access control process is a process which enforces protection of information by controlling all access to a system and its resources and ensuring that all and only, authorized access can take place". There are three components of Access Control:

- 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).

The purpose of access control in a computer system is to control whether a subject, like a process or a user is able to perform an operation e.g., read, write, execute or delete etc. on an object like, a row in a table, a file, a service, or any other resource of the system according to a pre-defined access-policy. The right to perform an operation on an object is called permission. Access control policies define the subject's permissions in a system to enforce the security of an organization. These policies are organized based on an access control model. The model may add middleware concepts between subjects and permissions to organize policies. These middleware concepts are selected from tasks, groups, roles, attributes or labels etc. The aim of this is to make policies, management, and definitions easier, fitting in as best as possible with the internal structure and needs of the protected system [2]. Informally, access control means to decide "who can do what." Access control is the most basic and most pervasive security mechanism in computer systems. In access control, the major tasks involved are: allowing access, denying access, limiting access and

revoking access. Among these tasks, most access control issues can be described.

This paper provides an appraisal of various works reported in the literature related to privacy issues in web services access control.

2 PRIVACY IN WEB SERVICES ACCESS CONTROL

The recent popularity of online web services has changed our notions about how information is exchanged among clients and business enterprises. Due to this penetration of web services in all aspects of our lives, trust in these services is a must.

It can be achieved only when the network and service providers can guarantee the security and privacy of all the involved parties. Due to the ever increasing number of web services available through the Internet, the privacy as a fundamental human right is endangered. In collaborative web services scenarios, different access control policies of certain services may result in processes which do not run smoothly. Bryans et al. [3] [4] evolved a concept of development of access control policies in such situations. In this concept a process with certain access control requirements is generated through a common consensus thereby being able to detect and prevent errors or contradictions.

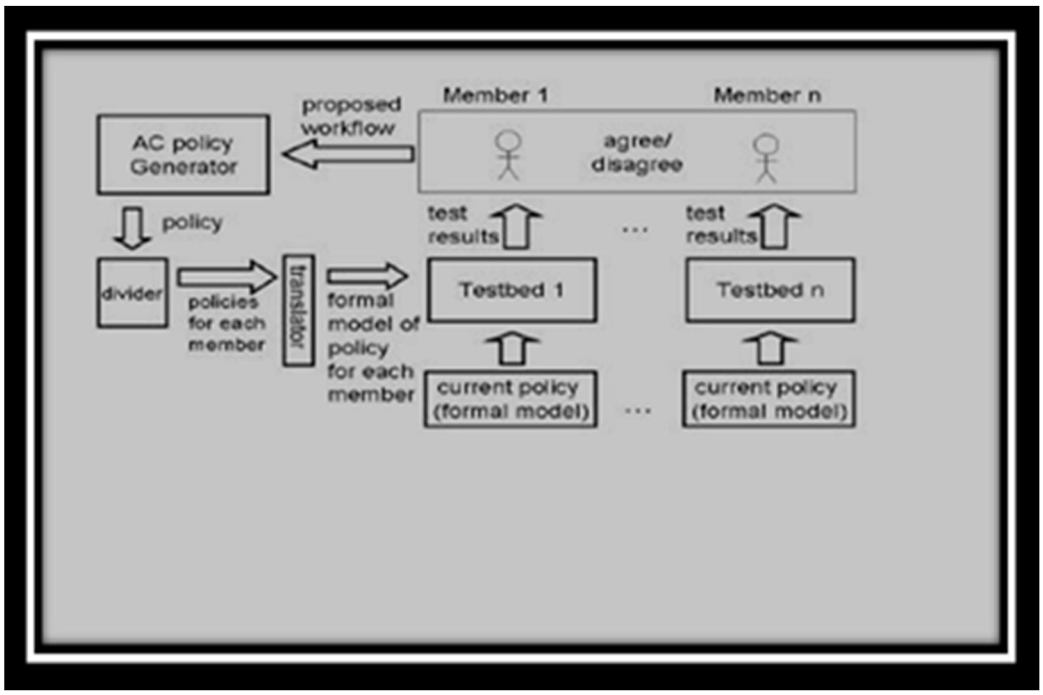

Fig. 1. Evolution of Access Control Policies in Dynamic Coalitions (adapted from: [5])

The same authors in [5] [6] used specification language VDM to create a basic formal model of dynamic collaborations. Their models consist of data types as well as operations and invariants over these types. They replicated the structure of the XACML model (a de facto standard for access control systems) in their formal representation of the model and provided for a faithful semantic interpretation.

The authors also demonstrated the practicability of their modelling approach.

The work presented in [7] extended this approach to cover both structure and process properties in a single formalism, i.e. Abstract State Machines (ASM) and there by created the means to formally analyse dynamic coalitions. We have listed down a few general privacy aware access control models and their contributions as reported in literature.

Table 1: Privacy Aware Access Control Models.

Research Work	Key Features	Contributions
Multi-domain and privacy-aware role based access control in e-health [8].	Provides support for multiple domains and meta information. Extends core- P-RBAC with automatic user to role assignments driven by preconditions on roles, that is, role provisioning and a flexible data specification through the use of data profiles.	The Privacy-Sensitive Data Permission (PDP) binds together the access purpose and the obligation consequential to the access.
Purpose based access control for privacy protection in relational database systems [9].	Proposed an approach for representing purpose information, which results in low storage overhead, and exploited query modification techniques to support access control based on purpose information.	Addressed the issue of granularity of data labelling, that is, the units of data with which purposes can be associated.
PuRBAC: Purpose-aware role-based access control [10].	Defined purpose as an intermediary entity between role and permission. Users can only exercise permissions assigned to an asserted purpose, which itself should be authorized through assignment to the user's active roles.	Supports constraints and obligations with clear semantics for enforcement and leverages hybrid hierarchies for roles and purposes for enforcing fine grained purpose and role based access control to ensure privacy protection.
A conditional role-involved purpose-based access control model [11].	Defined conditional purpose as the intention of data accesses or usages under certain conditions. Allows users using some data for a certain purpose with Conditions.	More information from data providers can be extracted while at the same time assuring privacy that maximizes the usability of consumers' data.
A privacy-aware access control model for distributed network monitoring [12].	Defined access control rules at any level of abstraction and in enabling a verification procedure, which results in inherently privacy-aware workflows, thus fostering the realisation of the Privacy by Design vision.	Enables the specification of contextual authorisation policies and expressive separation and binding of duty constraints.
Privacy Analysis in Mobile Social Networks: the Influential Factors for Disclosure of Personal Data [13].	Focussed on the influential factors: inquirer, purpose of disclosure ,access & control of the disclosed information, location familiarity and current activity of the user.	Provided insight into influential factors of human data disclosure decisions, by presenting and analysing results of an empirical investigation comprising of two online surveys.
A privacy-aware access control system [14].	Categorized privacy-aware policies into access control, release and data handling policies.	Presented a privacy control module in charge of managing, integrating, and evaluating access control, release, and data handling policies.
Exploiting cryptography for privacy-enhanced access control: A result of the prime project [15].	Describes two key elements of the PRIME identity management systems i.e. anonymous credentials and policy languages that fully exploit the advanced functionality offered by anonymous credentials.	Motivates the need for privacy enhancing identity management solutions and gives concrete requirements for such a system.

Since in web services paradigm, various distributed heterogeneous web services collaborate to serve user's request, privacy preserving access control is a much more tedious job in such environments. We have listed down a few prominent works in this domain as reported in literature.

Table 2: Prominent Access Control Models for Distributed Collaborative Environment

Research Work	Highlights	Contributions
Building access control policy model for Privacy Preserving and Testing Policy Conflicting Problems [16].	Proposes a purpose-based access control model in distributed computing environment for privacy preserving policies and mechanisms and describes algorithms for policy conflicting problems.	Provides efficient conflict checking algorithms and their implementation.
Trustbac: integrating trust relationships into the RBAC model for access control in open systems [17].	Extends the conventional role based access control model with notion of trust levels. Users are assigned to trust levels instead of roles based on a number of factors like user credentials, user behaviour history, user recommendation etc. Trust levels are assigned to roles which are assigned to permissions as in role based access control.	Incorporates the advantages of both the role based access control model and credential based access control models.
Access control enforcement for conversation-based web services [18].	Introduces a novel concept of k-trustworthiness where k can be seen as the level of trust that a web service has on a client at any point of their interaction. The greater the level of trust associated with a client, the greater is the disclosure.	Proposes a conversation-based access control model that enables service providers to retain some control on the disclosure of their access control policies while giving clients some guarantees on the termination of their interactions.
A role based access control for web services [19].	Deals with two types of access control: SWS-RBAC (for single services) and CWS-RBAC (for global services).	Proposes an efficient role-mapping mechanism to maintain the autonomy of roles between providers.
An Access Control System for Web Service Compositions [20].	Proposes a policy composition framework that integrates the RBAC policies of multiple domains.	Facilitates secure information and resource sharing in a collaborative environment.
Access control for collaborative systems: A web services based approach [21].	Specifies local as well as collaboration access control rules and enforces security policies by applying Web services mechanisms (XML, SOAP, UDDI and WSDL).	Discusses the most important approaches that emphasize access control in collaborative environments.
Delegation in role-based access control [22].	Shows that the use of administrative scope for authorizing delegations is more efficient than using relations. Also discusses the enforcement and revocation of delegations.	Applies delegation in the context of workflow systems.
A delegation model for extended RBAC [23].	Uses contextual permissions the administrator and users define complex conditions to deal with delegation and revocation features and to restrict the delegation scope.	Provides means to express various delegation and revocation dimensions in a simple manner.
Verification of privacy requirements in Web services composition [24].	Uses privacy policies to specify the privacy privileges of a services composition and models the interface behaviours of services by extending the interface automata to support privacy semantics.	Formally verifies whether the behaviours of a services composition satisfy the privacy policy constraints.

3 CONCLUSION

The focus of this paper was to introduce the preliminary concepts of privacy issues in access control process for web services to establish concretely the various aspects of the paper's objectives and how to achieve a practical, effective and rigorous developmentframework for creating access control model for web services with confidence. A comprehensive study of various works of this arena, reported in literature, is

provided as a bird's eyeview. To the best of our knowledge, no such appraisal as a collective work is available till date. This work will help the researchers of this area to have a look at various models available in order to easily identify the research gaps and get a single point of focus.

4 REFERENCES

[1] P. Samarati and S. de Vimercati. Access control: Policies, models, and mechanisms, Foundations of Security Analysis and Design, 2001, pp. 137–196.

[2] David F. Ferraiolo, and D. Richard Kuhn, "Role –Based Access Control (RBAC): Proceeding of 15th NIST –NSA National Computer Security Conference, Baltimore, Maryland, October 13-16, 1992, pp. 554-563.

[3] J. W. Bryans, J. S. Fitzgerald, D. Greathead, C. B. Jones & R. J. Payne, 'A Dynamic Coalitions Workbench: Final Report', 2008, Technical Report, Newcastle University.

[4] J. W. Bryans, J. S. Fitzgerald, C. B. Jones, I. Mozolevsky, Jeremy W. Bryans, John S. Fitzgerald, Cliff B. Jones & Igor Mozolevsky, ' Dimensions of dynamic coalitions', 2006, Technical Report.

[5] Jeremy Bryans & John Fitzgerald, 'Formal Engineering of XACML Access Control Policies in VDM++. In Michael Butler, Michael Hinchey &Mar´ıaLarrondo-Petrie, editors: Formal Methods and Software Engineering, Lecture Notes in Computer Science 4789, Springer Berlin / Heidelberg, 2007, pp. 37–56. Available at http://dx.doi.org/10.1007/978-3-540-76650-6_4.

[6] Jeremy Bryans, John S. Fitzgerald, Cliff B. Jones & Igor Mozolevsky, 'Formal Modelling of Dynamic Coalitions, with an Application in Chemical Engineering', 2006, Technical Report. Available at http://dx.doi.org/10.1109/ISoLA.2006.21.

[7] Bab, Sebastian, and NadimSarrouh. "Towards a Formal Model of Privacy-Sensitive Dynamic Coalitions." arXiv preprint arXiv:1204.6090, 2012.

[8] L. D. Martino, Q. Ni, D. Lin, and E. Bertino, 'Multi-domain and privacy-aware role based access control in ehealth," in International Conference on Pervasive Computing Technologies for Healthcare, 2008, pp. 131–134.

[9] Byun, Ji-Won, and Ninghui Li, 'Purpose based access control for privacy protection in relational database systems', The VLDB Journal 17, 4 (2008), pp. 603--619.

[10] Masoumzadeh, Amirreza, and James BD Joshi, 'PuRBAC: Purpose-aware role-based access control', On the Move to Meaningful Internet Systems: OTM 2008. Springer Berlin Heidelberg, 2008, pp. 1104-1121.

[11] M. Kabir, H. Wang, E. Bertino, 'A conditional role-involved purpose-based access control model', Journal of Organizational Computing and Electronic Commerce, 21 (1) (2011), pp. 71–91.

[12] Papagiannakopoulou, Eugenia I., Maria N. Koukovini, Georgios V. Lioudakis, Joaquin Garcia-Alfaro, Dimitra I. Kaklamani, Iakovos S. Venieris, FrédéricCuppens, and Nora Cuppens-Boulahia, 'A privacy-aware access control model for distributed network monitoring', Computers & Electrical Engineering 39, no. 7 (2013): pp. 2263-2281.

[13] Sapuppo, A., 'Privacy Analysis in Mobile Social Networks: the Influential Factors for Disclosure of Personal Data', International Journal of Wireless and Mobile Computing, 5(4), 2012, pp. 315-326.

[14] C.A. Ardagna, M. Cremonini, S. De Capitani di Vimercati, and P. Samarati, 'A privacy-aware access control system', Journal of Computer Security 16, 4 (September 2008), pp. 369--392.

[15] Claudio A Ardagna, Jan Camenisch, MarkulfKohlweiss, Ronald Leenes, Gregory Neven, Bart Priem, PierangelaSamarati, Dieter Sommer, Mario Verdicchio ,'Exploiting cryptography for privacy-enhanced access control: A result of the prime project', Journal of Computer Security 18, 1 (2010), pp. 123--160.

[16] Bertino, Elisa; Wang, Hua; and Sun, Li, 'Build7ing access control policy model for Privacy Preserving and Testing Policy Conflicting Problems' (2014). Cyber Center Technical Reports.Paper 11.Available at http://docs.lib.purdue.edu/cctech/11.

[17] Chakarborty, S. and Ray, I., 'Trustbac: integrating trust relationships into the RBAC model for access control in open systems' In SACMAT '06: Proceedings of the 11th ACM symposium on Access control models and technologies (New York, NY, USA, 2006), ACM, pp. 49--58.

[18] Mecella, M., Ouzzani, M., Pacci, F. and Bertino, E., 'Access control enforcement for conversation-based web services', In Proceedings of the 15th international conference on World Wide Web (New York,

NY, USA, 2006), WWW '06, ACM, pp. 257--266.

[19] Wonohoesodo, R. and Tari, Z., 'A role based access control for web services', In Services Computing, 2004 (SCC 2004), Proceedings, 2004 IEEE International Conference (September 2004), pp. 49 -- 56.

[20] Srivatsa, M., Iyengar, A., Mikalsen, T., Rouvellou, I., Jian Yin, 'An Access Control System for Web Service Compositions', ICWS, IEEE International Conference 2007, pp. 1-8.

[21] EL Kalam, A., Deswarte, Y., Baina, A. and Kaaniche, M., 'Access control for collaborative systems: A web services based approach', In Web Services, 2007, ICWS 2007, IEEE International Conference (July 2007), pp. 1064--1071.

[22] Crampton, J. and Khambhammettu, H., 'Delegation in role-based access control', International Journal of Information Security 7 (2008), pp. 123--136.

[23] Ben-Ghorbel-Talbi, M., Cuppens, F., Cuppens-Boulahia, N. and Bouhoula, A., 'A delegation model for extended RBAC', International Journal of Information Security 9 (2010), pp. 209 -- 236.

[24] L. Liu, Z. Huang, F. Xiao and G. Shen, 'Verification of privacy requirements in Web services composition', 2010 Second International Symposium on Data, Privacy, and ECommerce, 2010, pp. 117-122.

[25] L. Zhao, Z. Huang and L. Liu, 'Research on privacy disclosure analysis for Web services composition', Journal of Frontiers of Computer Science and Technology, vol. 6, no. 4, 2012, pp. 319-326.

[26] G. M. Kapitsaki, 'Reflecting user privacy preferences in context-aware Web Services', Department of Computer Science University of Cyprus Nicosia, Cyprus, In proceedings of the IEEE 20th International Conference on Web Services, 2013, pp. 123-130.

[27] Salah-EddineTbahriti, ChirineGhedira, BrahimMedjahed, Michael Mrissa, Djamal Benslimane, 'How to Enhance Privacy Within DaaS Service Composition?', IEEE Systems Journal 7(3), 2013, pp. 442-454.

[28] Lu, Jiajun, Zhiqiu Huang, and ChangboKe., 'Verification of Behavior-aware Privacy Requirements in Web Services Composition', Journal of Software 9, no. 4, 2014, pp. 944-951.

[29] Giannakakis, Konstantinos, 'Adopting Existing Communication Platforms for Security Enabling Technologies', In Secure and Trustworthy Service Composition, Springer International Publishing, 2014, pp. 36-4[35] J. W. Bryans, J. S. Fitzgerald, D. Greathead, C. B. Jones & R. J. Payne, 'A Dynamic Coalitions Workbench: Final Report', 2008, Technical Report, Newcastle University.