TOWARDS A CONTEXT-AWARE ACCESS CONTROL FRAMEWORK IN WEB SERVICE TRANSACTIONS

Carina K Wangwe, Mariki M Eloff, Lucas M Venter

University of South Africa

carina.wangwe@gmail.com, +255 754 600512, Box 60049 Dar es Salaam
eloffmm@unisa.ac.za, +27 12 4296330, Box 392 UNISA 0003 SA
ventelm@unisa.ac.za, +27 12 4296330, Box 392 UNISA 0003 SA

ABSTRACT

Interoperability across heterogeneous domains has become a reality through technologies such as Service Oriented Architectures and Web Services. These technologies have been put to use in e-Government and e-Business, enabling services to transact without human intervention. Such transactions, however, raise security concerns, as a human response to an authorization or access request can take into consideration semantics and the context in which the request is being made, while a machine to machine decision to grant access would rely on how well the XML based security policies have captured all semantic and contextual considerations.

This paper proposes a context-aware access control framework in a web services environment. The framework is based on the Organization for Advancement of Structured Information Standards (OASIS) for web services security and access control and extends these to include semantic interpretation of security attributes. Furthermore, the framework addresses contextual information that would affect an access control decision, in a web service transaction, such as legal or regulatory requirements.

KEY WORDS

Access Control

A CONTEXT – AWARE FRAMEWORK FOR ACCESS CONTROL ASSERTIONS IN WEB SERVICE TRANSACTIONS

1 INTRODUCTION

With any collaboration, it is crucial to have unambiguous communications between the collaborators, to ensure that no information is either wrongly withheld or provided based on an ambiguous request.

For Web Service transactions, one way to achieve such communication is the use of a semantic framework to provide a basis for interpretation of access control requests depending on the context of the transaction within a given domain. Furthermore, where laws and regulations exist that govern the transaction, these have to be taken into consideration when applying the access control or authorisation policy. The framework would thus include an access control mechanism, semantic interpretation of access requests, a context service and a repository of relevant laws and regulations.

The Organisation of Advancement of Structured Information Standards (OASIS) has adopted standards such as the Extensible Access Control Markup Language (Oasis 2005a) and the Security Assertion Markup Language (Oasis 2005b) to address access control across heterogeneous domains. The Extensible Access Control Markup Language (XACML) is a policy language which uses XML statements to present access control policies while the Security Assertion Markup Language (SAML) is an XML-based security specification schema for exchanging authentication and authorization information. XACML and SAML both have extensibility mechanisms which allow them to be used for different implementation. Use of these standards alone does not however ensure the

correct access control decisions in interacting web services. There is a need to ensure that those XML tags passed to request access are correctly interpreted in the context of the transaction.

The use of ontologies in web services has been promoted by the World Wide Web Consortium (W3C) which has recommended the Web Ontology Language (OWL) as a general ontology for the semantic web (W3C, 2004). OWL is based on the Resource Description Framework (RDF) schema which was an earlier specification from W3C. The ontology serves the purpose of clearly defining terms that are used in a transaction, and enables a semantic evaluation of terms to determine similar meaning. Specific ontologies based on OWL or RDF have been proposed by Ceravolo (2003), Domingue et.al. (2004), and Dritsas et.al. (2005) for the e-Government domain.

For a specific ontology to be used, the context of the transaction must be taken into consideration. Context defines the conditions that must or must not hold in order for an authorisation policy to apply (McDaniel, 2003). Contextual information may include the location of the requester and the provider of the service or the time when the transaction is taking place. For transactions that are taking place in an E-Government or E-Business environment, the legal context may also be necessary. All contextual information needs to be captured and combined so as to act as input into the access control decision.

This paper presents a framework that comprises of a context service, ontological mapping mechanism and a legal repository which together with extended markup languages, support correct access control decisions in interacting web services. The remainder of the paper is structured as follows: Section 2 describes existing access control models for web services. Section 3 proposes a context –aware framework while section 4 looks at related work in this area and we conclude and look at further work in Section 6.

2 ACCESS CONTROL IN WEB SERVICE TRANSACTIONS

A major requirement of an access control model for web services is the handling of the dynamic nature of the transactions. Web services interact across disparate computing platforms, in different geographical locations and with different regulatory compliance requirements. In subsequent sub

sections, we describe some access control models that have been proposed or implemented for web services.

2.1 Role Based Access Control (RBAC)

RBAC uses roles as a basis for access control decisions and was designed specifically with enterprise organisation structure in mind. RBAC allows the specification of security roles that map naturally to an organisation's authorisation structures. However RBAC does not entirely suit web service transactions and its weakness in open environments were identified by De Capitani di Vimercati and Samarati (2005). Several studies have subsequently been done to extend the RBAC model in order to address some of the weaknesses (Demchenko et.al, 2007).

2.2 Attribute Based Access Control ABAC

In recent years, there has been a shift to looking at attributes as a basis for access control in a web services environment. (Coetzee and Eloff, 2007; Damaini et. al, 2005; Shen and Hong, 2006; Yuan and Tong, 2005). Attributes describe the characteristics of the requester, and may be a combination of identity and role. Attributes may be subject attributes, resource attributes or environment attributes. The ABAC model comprises of an Attribute Authority, Policy Enforcement Point, Policy Decision Point and Policy Authority.

It has been recognized that there is still a need for the usage of semantics and or ontologies to ensure correct access control decisions with the ABAC model, and some research to that end has been done. (Preibe et.al; 2006; Warner et.al, 2007).

2.3 Context Aware Access Control

Both RBAC and ABAC paradigms do provide ways to include contextual information (Bacon et.al, 2002; Huselboch et.al., 2005; Strembeck and Neumann, 2004). However other access control models that focus primarily on context have been proposed. These include:

2.3.1 Governance Based Access Control

The idea as presented by the Centre for Governance Institute (2005) is that transactions in which information is shared must be governed by the relevant legislation to which the organizations sharing the information are accountable. Thus any request for information is checked against the exiting laws or regulations before it is granted.

2.3.2 Session Based Access Control (SBAC)

In session based access control, the context of a transaction is limited to a session. Access to resources is based on the attributes of the subjects and the properties of the objects but the rights that can be applied at a given time are limited based on the context defined by the access session (Fernandez and Pernul, 2006)

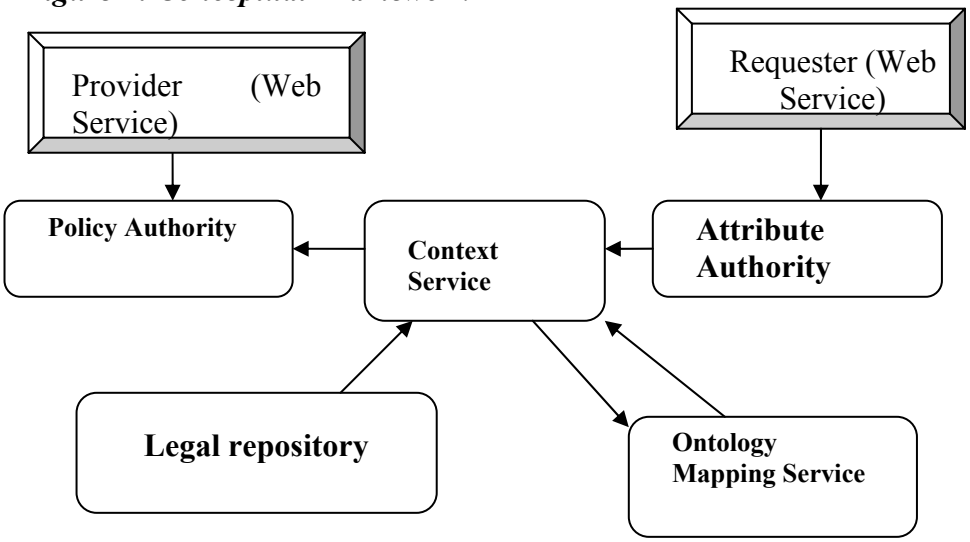
2.3.3. Location-Based Access Control (LBAC)

LBAC takes requester's physical location into account when determining their access privileges. The physical location may be combined with other attributes related to identity or role of the requester. Ardagna et.al (2006) propose combining location with user credentials to support access control decisions.

3 PROPOSED FRAMEWORK

In order to achieve correct access control decisions in the context of a web service transaction, we propose a framework based on the ABAC model. The proposed framework is illustrated in Figure 1 below:

Figure 1: Conceptual Framework



Each of the components of the framework works as follows:

i) Policy Authority

The policy authority contains the Policy Decision Point (PDP) and Policy enforcement points that evaluate the requester's attributes against the providers XACML policy. In order to evaluate the compliance with legal requirements XACML is extended to include a function that accepts environment attributes and compares against relevant laws and regulations within the legal repository. This operation will be stated as a XACML obligation in the Provider's policy. If there is no legal requirement for a particular transaction, then the request is granted provided the other requirements of the policy are met.

ii) Attribute Authority

The attribute authority issues SAML assertions to the requester. The attribute assertions correspond to the subject, resource and environmental attributes of the requester. If there is a legal requirement on the requester's

side that has to be complied with, this requirement is passed in a SAML condition statement.

iii) Ontological mapping service

The ontological mapping services checks the semantics of the requester's attributes match with those in the provider's policy. A mechanism to conduct such a mapping has been described by Patil et.al (2007). If unknown vocabularies are used, ontology mediators may be used (Kolter, et.al, 2007).

iv) Legal repository

The legal repository contains laws and regulations that apply to different transactions. The legal repository contains the conditions in which a transaction is considered legal or illegal. The legal repository is a database which with several indexes to allow multiple matching by the Context Service.

v) Context Service

The context service is a key element of the framework and is adapted from Lei et.al. (2002). The role of the context service is to combine the results from the ontological mapping mechanism and the legal repository into an environmental attribute that is then passed to the attribute authority for authorisation and access control decisions to be made. To illustrate how the framework could be applied, consider the following illustrative example:

A request for information is made in a criminal investigation where a national of Country A is suspected of committing a crime in Country B; and the suspected criminal is now in resident in Country C. In order for the service in Country C to decide whether to authorise access to the information the following requirements must be met:

- The penalty for the crime in Country C must be evaluated against the penalty for the crime in country A. If conviction may result in a death penalty, then Country C must refuse to provide information.
- The crime committed in Country B must be interpreted in the context of the laws of country C.

- Laws of country A must be examined to see if they have any relevance in the crime and or penalty for the crime

Thus for this example the service provider would need access to a legal repository of the countries' laws and also to the ontological mapping mechanism to make semantic comparisons as to whether or not all necessary conditions to grant the requested information hold.

4. RELATED WORK

There are various studies that have been done in relation to context – aware and or semantic – aware authorisation and access control. The studies that are pointed out below are those that address context in access control decisions with some reference to semantics.

Demchenko et al. (2007) use XACML to handle policy and base on RBAC with a Domain Resource Management model. The study argues that domain based access control provides several benefits including dynamic context management. However interpretation of attributes is not addressed by the study. Toninelli et.al (2006) also draw inspiration from the RBAC model and associate the context in which a subject transacts directly with the role that the subject plays in that transaction.

Hu and Weaver (2006) look at the healthcare domain and provide a formal definition of context and context constraints. The definition of context is restricted to time, location, user type, object type and object ID. Context is built into the policy language and WS policy is used for the implementation.

Kolter et al. (2007) describe a semantic aware security architecture which includes an ontological mapping mechanism. The architecture is based on the ABAC model, but does not specifically address how contextual attributes would be handled.

Our work, as presented in Section 3 above, takes into consideration both semantics and contextual information with emphasis on legal requirements.

5. CONCLUSION AND FURTHER WORK

We have presented a framework that comprises of a context service, ontological mapping mechanism and a legal repository which together with extended markup languages support corrects access control decisions in interacting web services. The inclusion of a legal repository make the framework especially useful for e-Government or e-Business transactions that take place across two or more legal domains where different regulations may apply to the transaction. Thus combine with the ontologically mapping mechanism that address semantic interpretation of attributes, the framework lays a basis for correct access control decisions based on the context of the transaction.

Future work shall include formalising a model based on the proposed framework and evaluating the framework in against requirements for access control architectures (Keromytis and Smith, 2007) when the framework is implemented in a practical setting.

6. REFERENCES

Ardagna, C.A., Cremonini, M. & Damiani, E. (2006). *Supporting Location – Based Conditions in Access Control Policies.* Proceedings of ASIACCS'06 held in Taipei. ACM.

Bacon, J., Moody, K. & Yao, W. (2002). A Model of OASIS Role-Based Access Control and Its Support for Active Security. *ACM Transactions on Information Security and Systems Security*, 5(4): 492:540.

Centre for Governance Institute (CGI). (2005). Governance Based Access Control (GBAC): Enabling improved information sharing that meets compliance requirements. Available from http://www.cgi.com/cgi/pdf/cgi_whpr_63_gbac_e.pdf. (Accessed 1 April 2008).

Ceravolo, P. (2003). *Managing identities via interactions between ontologies.* Proceedings of the OTM Workshop held in Catania.

Coetzee, M & Eloff, JHP. (2007). A Trust and Context Aware Access Control Model for Web Service Conversations. *Lecture Notes in Computer Science*, 4657:115:124

Damiani, E., de Capitani di Vimercati, S., & Samarati, P. (2005). *New Paradigms for Access Control in Open Environments*, Proceedings of the fifth IEEE International Symposium on Signal Processing and Information Technology. IEEE.

De Capitani di Vimercati, S. & Samarati, P. (2005). New Directions in Access Control. In Cyberspace *Security and Defense: Research Issues*. Edited by Kowalik, J & A Sachenko, A. Kluwer Academic Publisher.

Demchenko, Y., Gommans, L., & de Laat, C. (2007). Role Based Access Control Model for Distributed Multidomain Applications. In *New Approaches for Security, Privacy and Trust in Complex Environments*. Edited by Venter, H. Eloff, M., Labuschagne, I.., Eloff, J., & von Solms, R. IFIP International Federation for Information Processing.

Domingue, J., Gutierrez, L., Cabral, L., Rowlatt, M., Davies, R., & Galizia, S. (2004,). WP9: Case Study eGovernment D9.3 e-Government Ontology. Available from http://www.dip.deri.org/documents/D9-3-improved-eGovernment.pdf (Accessed 14th March 2008)

Dritsas, S., Gymnopoulos L., Karyda M., Balopoulos, T., Kokolakis, S., Lambriniudakis C., & Gritzalis S. (2005). *Employing Ontologies for the Development of Security Critical Applications: The secure e-poll paradigm*. Proceedings of the International Conference on eBusiness, eCommerce and EGovernment held at Turku. IFIP.

Fernandez & Pernul, (2006) *Patterns for Session Based Access Control.* Proceedings of Pattern Languages of Programming Conference held at Portland.

Keromytis, A.D & Smith J.M. (2007). Requirements for Scalable Access Control and Security Management Architectures. *ACM transactions on Internet Technology (* 7) 2.

Hu, J. & Weaver A.C. (2006) Dynamic , Context – Aware Access Control for Distributed HealthCare Applications . Available at http://www. cs.virginia.edu/papers/p1-hu-dynamic.pdf

Huselbosch, R.J., Salden, A.H., Bargh, M.S., Ebben, P.W.G, & Reitsma, J. (2005) *Context Sensitive Access Control*. Proceedings of SACMAT'05 held in Stockholm. ACM.

Lei, H., Sow, D.M. Davis, J.H., Banavar, G. & Ebling, M.R. (2002). The Design and Applications of a Context Service. *ACM SIGMOBILE Mobile Computing and Communications Review* (6) 4: 45:55.

McDaniel, P. (2003). *On Context in Authorization Policy.* Proceedings of SACMAT 2003 held at Como, Italy. ACM.

OASIS, (2005 a), XACML v2.0 Documentation. Available at http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml (Accessed 15th March, 2008)

OASIS, (2005 b) SAML v2.0 Documentation. Available at http://docs.oasis-open.org/security/saml/v2.0/ (Accessed 15th March 2008).

Patil, V., Mei, A. & and Mancini, L. (2007). *Addressing Interoperability issues in access control models.* Proceedings of ASIACCS'07 held at Singapore. ACM.

Priebe, T., Dobmeier, W. & Kamprath, N (2006), *Supporting Attribute-based Access Control with Ontologies.* Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06) held at Vienna. IEEE Computer Society.

Shen, H & Hong, F (2006). *An Attribute – Based Access Control Model for Web Services*. Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06) held at Taipei.

Strembeck, M. & Neumann, G, (2004). An Integrated Approach to Engineer and Enforce Context Constraints in RBAC Environments. *ACM Transactions on Information and System Security*, (7) 3: 392:427.

Toninelli, A., Montanari, R., Kagal, L., & Lassila, O. (2006). A Semantic Context – Aware Framework for Secure Collaborations in Pervasive Computing Environments. *Lecture Notes in Computer Science*, (4273): 473-486

Warner, J., Atluri, V., Mukkamala, R., &Vaidya, J. (2007). *Using semantics for automatic enforcement of access control policies among dynamic coalitions*, In Proceedings of SACMAT 2007.

W3C (2004). OWL Web Ontology Language Overview. Available from http://www.w3.org/TR/owl-features (Accessed 2nd May 2008)

Yuan, E. & Tong, J. (2005). *Attribute Based Access Control (ABAC) for Web Services.* In Proceedings of the IEEE International Conference on Web Services (ICWS'05) held at Orlando. IEEE Computer Society.