Chapter 11
Access Control and Information Flow Control for Web Services Security

Saadia Kedjar
University of Bejaia, Algeria

Abdelkamel Tari
University of Bejaia, Algeria

Peter Bertok
RMIT University, Australia

ABSTRACT

With the advancement of web services technology, security has become an increasingly important issue. Various security standards have been developed to secure web services at the transport and message level, but application level has received less attention. The security solutions at the application level focus on access control which cannot alone ensure the confidentiality and integrity of information. The solution proposed in this paper consists on a hybrid model that combines access control (AC) and information flow control (IFC). The AC mechanism uses the concept of roles and attributes to control user access to web services' methods. The IFC mechanism uses labels to control how the roles access to the system's objects and verify the information flows between them to ensure the information confidentiality and integrity. This manuscript describes the model, gives the demonstration of the IFC model safety, presents the modeling and implementation of the model and a case study.

INTRODUCTION

Several companies have adopted the Web services technology to implement their distributed systems, because they offer cooperation and interoperability (Cantara et al., 2003; Chen, 2003). However, the opening and accessibility of the web services on Internet make them vulnerable to various attacks. Con-

DOI: 10.4018/978-1-7998-0417-8.ch011

sequently, web services security remains a significant issue which motivates many researchers to develop various security solutions (Bertino et al., 2010). Access control is the most used security mechanism at the application level.

Traditional access control models (LBAC: Lattice-based access control, RBAC: Role-based access control, etc.) are designed for the LAN-based applications such as banking applications, which are closed systems. These models are not suitable for open systems like the web services considering their distributed and decentralized aspect. Indeed, the application of these controls is based mainly on known users' identities and attributes. However, the opened, distributed and dynamic environments are confronted with a great number of unknown users. Furthermore, AC models for the web services must be decentralized and must be able to manage the trust relationships between service providers and requesters. Moreover, these models must be able to control the accesses to heterogeneous resources i.e. the methods of the web services and data which they handle.

Access control (AC) models proposed for web services are distinguished by the concepts, which are used for authentication and authorization policies definition. We can find the role-based models which adapt the RBAC model such as the models suggested by (Tari and Wonohoesodo, 2004) and (Bhatti et al., 2003). Attribute-based models for the trust management such as the models of (Hai-bo and Fan, 2006) and (Bertino et al., 2004). Hybrid models use various concepts (e.g. the role and the attribute) to fulfil the requirements of the web services such as the models suggested by (Chakraborty and Ray, 2006) and (Liu et al., 2005). (Alipour et al., 2012) proposed another type of models, which use dynamic separation of duty rules.

Absence of information flow control (IFC) between the objects of a web services system constitutes the limit of the majority of the AC models found in the literature. Indeed, these models control the direct accesses to the resources of a system but they do not perform control over the information after their dissemination or distribution (Gondara, 2011) (Esfandi and Sabbari, 2012).

The IFC was introduced for the programming languages by (Myers and Liskov, 1997) and is used in other field as the data bases (Ferrari et al., 1997). The IFC models for web services must take into account the highly dynamic and distributed aspect of web services and they must take into account the composite web services (Bryce et al., 1995).

Tari (Tari et al., 2006) proposed IFC model for the web services based on the dynamic label checking of objects handled by the web services. This model consists of an adaptation of the model of Myers and Liskov (Myers and Liskov, 1997). The model aims to ensure data confidentiality handled by a web services system by preventing the information disclosure.

This model is improved in (Bertok et al., 2009) by modifying the operation joins to ensure information confidentiality. Moreover, the label is extended to allow not only information confidentiality but also their integrity by considering writing operation in the control policies.

In (Kedjar and Tari, 2013), a new approach of web services security has been proposed which combine access control and information flow control.

In this paper, the authors propose a hybrid model for web services security, theoretical proofs of safety, its modeling and some details of its implementation. The model adopts two concepts: "role" to control user access to web services methods and, "labels" to control the role's access to system's objects and IFC between them. The model is extended to exploit the relation of hierarchy of XML data.

This paper is structured as follows. First, the model is presented and its basic components are detailed. Then, the modeling with UML diagrams is described. It is followed by a brief overview of implementation methodology. After, a case study and software validation are presented.