Chapter XXV
Security in Semantic Interoperation

Yi Zhao  
FernUniversitaet, Germany

Xia Wang  
FernUniversitaet, Germany

Wolfgang A. Halang  
FernUniversitaet, Germany

ABSTRACT

With the increasing interest in Semantic Web-based applications, researchers have started to build tools enabling organisations to share information. An important aspect in maintaining the Semantic Web is, however, to preserve security during semantic interoperation of different entities. Security and privacy are indispensable to the success of Semantic Web services. Hence, this chapter aims to investigate the currently used security methods in semantic interoperation, including the security methods employing Semantic Web representation languages such as XML, RDF and ontologies, and their application methods in semantic interoperation such as secure access control and secure knowledge management. How to manage privacy, trust and reputation at the same time during semantic interoperation will also be discussed in this chapter. Finally, some directions for our further research will be presented.

INTRODUCTION

With the increasing interest in semantic web-based applications, tools for semantic interoperation have to be built to enable different organisations to share information. The emerging semantic web integrates logical inference, knowledge representation, and technologies of intelligent software agents. Annotation of web resources with machine-processable metadata and ontologies are employed as means to conceptualise and
structure knowledge in order to realise the vision of the semantic web. As the semantic web is composed of web entities like web services, agents and human users, an important aspect in maintaining the semantic web is to preserve security during semantic interoperation of different entities. Hence, for the semantic web to succeed it is essential to maintain the security of the organisations involved and the confidentiality of the data handled, in particular during semantic interoperation of different entities.

The requirements of successful semantic interoperation are arising from three kinds of policies: security policies, privacy policies, and trust and reputation based policies. According to this, this chapter aims to investigate the currently used security methods in semantic interoperation, including the security methods employing semantic web representation languages such as XML, RDF and ontologies, and their application methods in semantic interoperation such as secure access control, secure knowledge management, and secure agent communication. How to manage privacy, trust and reputation during semantic interoperation will also be discussed in this chapter.

The main body of the chapter is organised as follows. The backgrounds and concepts of security and privacy in semantic integration will be introduced in the next section. Then, a comprehensive treatment of different security-preserving methods and architectures will be given. Closely related aspects are XML, RDF security, and security ontology. Secure semantic interoperation architecture and methods such as access control, knowledge management, and agent communication will be addressed, too. Privacy-preserving, trust and reputation-enhanced semantic interoperation will be discussed, since they are closely related to the security requirements. Finally, directions for further research will be indicated.

BACKGROUND

The semantic web (Berners-Lee, 2001) is a universal medium to exchange data, information and knowledge. It suggests annotating web resources with machine-processable metadata. The emerging semantic web integrates logical inference, knowledge representation, and technologies of intelligent software agents. With the increasing interest in web-based applications such as electronic commerce, researchers have started to build tools enabling organisations to share information. Most of these tools have not taken into account, however, the important aspect of maintaining the security of the organisations involved and the confidentiality and privacy of data. Therefore, for the semantic web to succeed it is essential to preserve security and privacy during semantic interoperation of different entities.

Semantic Web Services and Semantic Interoperation

Web services are defined as small units of functionality, which are made available by service providers for use in larger applications. The intention to develop web services was to reduce the overhead needed to integrate functionality from multiple providers. Communication with web services is usually achieved using the SOAP protocol (Gudgin, 2003). SOAP is an XML-based protocol for communication between distributed environments. Descriptions of the interfaces of the web services are formulated using the Web Service Description Language (WSDL) [CCMW01]. WSDL documents are generally stored in a Universal Description Discovery and Integration (UDDI) repository where services can be discovered by end-users.