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.
While web services have indeed reduced the overhead needed to integrate functionality from multiple providers, extensive human interaction is still required in the process. Semantically enabled web services are forming the research area known as semantic web services (SWS). Semantic web services (Payne, 2004) can be defined as web services whose descriptions are annotated by machine-interpretable ontologies, so that other software agents can use them without having any prior ‘built-in’ knowledge about how to invoke them. Semantic web services complement standards around WSDL, SOAP and UDDI which aim to enable total or partial automation of tasks such as discovery, selection, composition, mediation, invocation, and monitoring of services. The research on semantic web services addresses definition and development of concepts, ontologies, languages, and technologies for SWSs. With the development of the semantic web and semantic web services, interoperation and service sharing are widely adopted to support collaboration across different enterprise systems (Park, 2001). Semantic interoperation and service sharing have been accepted as efficient means to facilitate collaboration among heterogenous system applications.

**Ontologies and Their Representation Languages**

As an important technique to represent knowledge and information, so-called ontologies allow to incorporate semantics into data to drastically enhance information exchange. The term ontology is borrowed from philosophy, where it refers to a systematic account of what can exist or ‘be’ in the world. In the fields of artificial intelligence and knowledge representation, ontologies are used to construct knowledge models that specify sets of concepts, their attributes, and the relationships between them. Ontologies are defined as “explicit conceptualisation(s) of a domain” (Gruber, 1993), and are seen as a key to realise the vision of the semantic web.

Ontologies play a prominent role in the concept of the semantic web to provide semantic information in assisting communication among heterogeneous information repositories (Fonseca, 2001). There are many formal languages proposed to represent ontologies, such as XML (eXtensible Markup Language), RDF (Resource Description Framework), and OWL (Web Ontology Language) (Dean, 2002).

As stated by Fensel (Fensel, 2000), XML can be used to define arbitrary domain- and task-specific extensions. RDF took the first step towards defining the web in XML terms. It does so by a syntactical convention and a simple data model for representing machine-processable semantics of data. The RDF metadata model is based upon the idea of making statements about web resources in the form of subject-predicate-object expressions, called *triples* in RDF terminology. The subject denotes the resource, and the predicate denotes traits or aspects of the resource expressing a relationship between the subject and the object.

OWL (Web Ontology Language) (Dean, 2002) has been developed inspired by description logics. It builds upon the Resource Description Framework. An OWL ontology consists of a set of axioms which place constraints on sets of individuals (classes) and the types of relationships permitted between them. These axioms provide semantics by allowing systems to infer additional information based on the data explicitly provided.

**Security Requirements**

To guarantee semantic interoperation, security measures must be considered to protect against unauthorised disclosure, transfer, modification, or destruction, whether accidental or intentional. To realise them, proper identity must reliably be established by employing authentication techniques, and confidential data must be encrypted
The requirements of security include authentication, authorisation, integrity, confidentiality, privacy, trust and reputation. Some of the security requirements are briefly summarised below:

- **Authentication** determines the identity or role of a party attempting to perform some action such as accessing a resource or participating in a transaction.
- **Confidentiality** is generally associated with encryption technologies. It ensures shared content to be viewed by legitimate parties, only.
- **Privacy** is closely related to security. Some portions of a document (XML, RDF, or ontology) may set to be private, so that they are invisible during interoperation, while certain other portions may set to be public or semi-private, which causes a question, that is how one can take advantage of the semantic web and still maintain privacy at the same time?
- **Trust and reputation** are also related to security. Trust exerts an enormous impact on decisions whether to believe or disbelieve information asserted by peers (Ziegler, 2004). Trust and reputation are defined as the “subjective expectation an agent has about another’s future behavior based on the history of their encounters” (Mui, 2002).

**MAIN FOCUS OF THE CHAPTER**

As stated in (Thuraisingham, 2003), to secure the semantic web we must protect all its layers, including XML, RDF, ontologies, and information interoperation processes. In this section, we aim to investigate the security, privacy, and trust-preserving methods in semantic interoperation of semantic web services.

By combining conventional security technologies with semantic web technologies, we may be able to provide network security. Some currently used security-preserving methods are classified into:

- XML and RDF security
- Ontological security
- Secure access control
- Privacy-preservation in semantic interoperation
- Trust- and reputation-enhanced semantic interoperation

**XML and RDF Security**

In the case of XML and RDF representation languages, the security challenges include specifying security policies with XML and RDF, ensuring access control for XML and RDF documents, and investigating the secure interoperability of resources and services on the web. Access control policies are rules regulating how access control should take place.

The XML Encryption Working Group of the World Wide Web Consortium (W3C) (http://www.w3.org/Encryption/2001/) has proposed as W3C Recommendations an XML encryption syntax, processing specification, and the decryption transform for encrypting or decrypting digital content in XML documents. Though there are technologies that allow people to secure a data object, only W3C XML Signature, when paired with the W3C XML Encryption Recommendation, permits users to sign and encrypt portions of XML data.

Another XML-based security method is proposed in (Lee, 2002). Here, an agent can dynamically exchange its authentication and authorisation information using SAML (Security Assertion Markup Language, based on XML) during the interoperation process. As SAML does not need to share the same security infrastructure and allows applications to exchange authentication and authorisation information, the agent can play various roles in heterogeneous platforms, can dy-
namically change their requirements and, finally, act on behalf of users with diverse permissions to access the semantic web.

Giereth (Giereth, 2005) has studied hiding a fragment of an RDF document by encrypting it while the rest of the document remains publicly readable. The encrypted fragments are included as XML literals which are represented using the XML-Encryption and XML-Signature Recommendations. The access control policies and encryption techniques either allow or prohibit access to sensitive information: They do not allow the use of private knowledge to answer queries that can safely be answered using private knowledge without revealing it.

Jain et al. (Jain, 2006) have proposed an RDF authorisation model based on RDF-patterns. An RDF-pattern is associated with an RDF instance, schema, and a security classification. RDF-patterns are mapped to the statements in RDF-instances and schemas to determine security classifications for the statements. The method can selectively control access to stored RDF triples, assign security classification to inferred RDF triples, and check for unauthorised inferences. The focus of the design is to allow the use of hidden knowledge to answer queries without revealing hidden knowledge.

In (Kagal, 2003), a security framework for the semantic web employing the distributed policy language based on Resource Description Framework Schema (RDF-S) has been proposed to mark up security information, since it is important for web entities to be able to express their security information in a clear and concise manner for its meaning not to be ambiguous. The policy language is modeled on concepts of rights, prohibitions, obligations, and dispensations.

**Ontological Security**

Ontological security means to formulate security information based on ontology representation. In the current applications of semantic web services, some efforts have been made to facilitate ontological security:

An ontology-based rights expression language (OREL) (Qu, 2004) built on top of OWL has been presented to express access rights to resources. OWL ontologies can be imported by OREL users to write their own licenses by using instantiation or inheritance to fulfill their application-specific requirements. Qin and Atluri (Qin, 2003) have introduced concept-level security polices represented in an OWL-based access control language. This access control model is to specify access authorisations based on concepts and the relationships between these concepts, and to enforce these authorisations upon the data annotated by these concepts. Each concept is defined in an OWL ontology. This work deals with how terms naming resources (whose access is being controlled) can be re-written using other terms subject to logical rules expressed in the Web Ontology Language (OWL).

A fine-grain security mark-up of semantic web service parameters in OWL-S (Kagal, 2004) has been proposed to enforce the privacy and authorisation constraints that cryptographic techniques (using encryption and digital signatures) can implement. It aims to provide security and policy annotations for OWL-S service descriptions and enforcements by extending the OWL-S Matchmaker for policy matching and the OWL-S Virtual Machine (VM) with policy enforcement and security mechanisms. By using the security mechanisms proposed, web services implementing the OWL-S VM are guaranteed to maintain secure communication with their partners.

**Secure Access Control**

To make semantic interoperation secure, secure access control policies must be established. Security and confidentiality are the key points for the success of electronic commerce. Suppose two organisations want to carry out a transaction, they may both log into their semantic webs
and use a variety of information interoperation tools to exchange data and information. Various access control and usage control policies must be applied to ensure that the users can carry out the operations and access the data. Safeguarding multiagent systems also requires the development of access control models for agents.

Access control is the mechanism that allows resource owners to define, manage, and enforce the access conditions for each resource (Samarati, 2001). The Role-Based Access Control model (RBAC), the mediator-based access control model, and the dynamic access control model are considered as the most appropriate paradigms for access control in complex scenarios. In RBAC (Sandhu, 1996), role is an abstract description of behaviour and collaborative relation with others in an organisation, and permission is an access authorisation to an object, which is assigned to role instead as to an individual user to simplify security administration. In the mediator-based model, the mediator performs access control checks to early reject the queries that should be denied access. In dynamic access control, there is neither role nor mediator to assist in the process of access control.

Role-Based Access Control

The Semantic Access Control model (SAC) (Yague, 2005) extends RBAC by considering the semantics of objects and associating permission with concepts instead of objects. It is built on the basis of separating the responsibilities for authorisation and access control management, and provides adequate solutions to the problems of access control in distributed and dynamic systems with heterogeneous security requirements. SAC is characterised by its flexibility for accommodating dissimilar security policies, but also by the ease of management and control over a large number of distributed elements and the support for interoperability of authorisation mechanisms.

Another modified RBAC model, Ontology-based Hybrid Access Control (OHAC) (Sun, 2007) is designed based on a coalition, which stands for an association of representative enterprises in a specific application domain. By defining a common ontology of the domain, the coalition provides a platform for members to share, federate, and collaborate with each other, as well as serves as a portal to provide common services for the public. The authors declare that by mapping local authorisations to the common ontology. Enterprises can efficiently support automatic interoperation across heterogeneous member systems in the coalition, as well as general requests from dynamically changing exterior collaborators not belonging to the coalition.

Secure e-business between multiple organisations requires intra-organisational and inter-organisational perspectives on security and access control issues. There is paucity in research on information assurance of distributed inter-organisational e-business processes from a business process perspective. Some security measures for e-business applications have been reported in (Hassler, 2000). The challenges of secure electronic commerce (Thuraisingham, 2005) include identifying and authenticating consumers as well as businesses, and tracing all transactions and purchases. The proposed solution is for consumers and businesses to have some credentials when they execute transactions. These credentials, which may be some random numbers, could vary with any transaction. This way a malicious process that pretends to be a business may not have the correct credentials. Moreover, there will be a problem if the credentials are stolen.

Mediator-Based Access Control

The mediator in the model performs access control checks to reject as early as possible the queries that should be denied. Agarwal (Agarwal, 2004) has introduced policy algebras as a means to specify and handle complex access control policies, and
Security in Semantic Interoperation

has shown how Access Control Lists (ACLs) and certificates generated by the credential-based public key infrastructure resulting from the merge of the Simple Distributed Security Infrastructure (SDSI) with the Simple Public Key Infrastructure (SPKI) can be integrated with DAML-S to specify access control policies of web services, where DAML-S is a DAML+OIL ontology for web service descriptions aiming to make web services interpretable and to enable tasks like discovery, composition, and interoperation of web services.

In the ARTEMIS project (Boniface, 2005) a semantic web service-based Peer-to-Peer interoperability infrastructure has been developed for healthcare information systems. The ARTEMIS mediator uses the semantic web service descriptions as broker between organisational policies by reasoning about security and clinical concept ontologies. Each health information system is represented as an ARTEMIS Peer node that communicates directly with an ARTEMIS Mediator. The web service descriptions are held at the mediator using standard web service repositories. The service descriptions are annotated with semantics so that service operation, meaning of data, and non-functional requirements can be understood by the infrastructure. In detail, when a web service is invoked, the ARTEMIS mediators act as brokers between requester and provider. ARTEMIS allows requester and provider to support different encryption mechanisms by allowing compatibility between algorithms to be expressed using ontologies. When a web service is invoked, the mediator translates the role of the healthcare professional in the requesting organisation to the equivalent role in the providing organisation.

As the mediator-based access control has the disadvantage that the mediator has to obtain the access control tables of the participating information sources, a modified model called Semantic Access Control Toolkit (SACE) (Pan, 2006) has been proposed to interoperate among semantically heterogeneous information sources, and to handle the corresponding confidentiality concerns of the organisations involved in information sharing. The objective of SACE is to enable users of organisation A to access organisation B’s data using queries written against A’s database schema without violating any security policy. The architecture of the SACE model has two aspects: the on-line aspect shows how an inter-organisation query is processed at run-time, and the off-line aspect shows how the initial processing is prepared for the on-line processes.

Dynamic Access Control

The Semantic Mapping Framework Security Policy (SPDM) proposed in (Muthaiyah, 2006) aims to dynamically map security policies of real organisations (RO) and virtual organisations (VO), and to update a global policy stored in a knowledge base for future use. Dynamic mappings of local and global policies help to maintain the consistency of mapped global policies in the knowledge base storage. The model functions in five steps: (1) security policy ontologies RO and VO are created and exported to OWL; (2) a reasoning process is carried out to check for consistency, classify the taxonomy, and compute the inferences; (3) consistency checks on RO and VO are performed; (4) the SPDM and via merging a global security policy are generated, and similar instances are merged; and (5) output results are generated and the mapping process is completed.

Privacy Preserving in Semantic Interoperation

Although many tools have been developed to enable different organisations to share information, most of these tools have not taken into account the necessity of maintaining the privacy and confidentiality of the organisations’ data and metadata. Actually, some organisations do not want to publish their metadata or even share them with external users. At the same time, however,
they want to enable interoperation. Therefore, the privacy of the metadata (the ontologies of information sources or the schemas of databases) must be preserved.

The semantic web has brought about new challenges for privacy management. The privacy-preserving semantic web allows users to employ agents to carry out sophisticated tasks while being confident that personal information is being managed in the fashion desired. Most semantic interoperation approaches rely on the fact that both schemas and ontologies are completely visible by both parties. Clearly, this approach disregards security and privacy considerations. Even within the same organisation, different users have access to different database views.

In this section, the currently used technologies to preserve privacy by ontology representation, by mediators, or just automatically are discussed.

Privacy by an Ontology

Currently proposed policy languages (Tonti, 2003) for information hiding on the semantic web rely on complete denial of access to the hidden parts of an ontology. Such approaches are overly restrictive in that they prohibit the use of hidden knowledge in answering queries where it is possible to do so without disclosing the hidden knowledge. In (Kim, 2002), the idea of a privacy ontology has been proposed to enable agents to exchange privacy-related information using a common language. The privacy ontology should be able to clearly define the various dimensions of privacy (e.g., privacy of personal behaviour vs. privacy of communications), and contain sufficient parameters and index terms to enable specification of a privacy policy in a standard machine-understandable format. It should be descriptive enough to specify the highest known standards of data protection and privacy. It should not only allow specification of a user’s privacy preferences to a web-site, but also allow users to collect and store certain information about web-sites and other agents they interact with.

Privacy by a Mediator

Clifton et al. (Clifton, 2004) have discussed issues and identified research directions in privacy-preserving data integration, including those that arise in schema-matching. In their approach, terms in the ontologies and in the matching rules (which define the mappings) are encrypted, so that the mediator does not see the actual terms. During the process of ontology interoperation, however, a human expert has access to both ontologies in clear text with a session key.

Two frameworks (automatic and semi-automatic) for privacy-preserving interoperation have been presented in (Mitra, 2005), especially highlighting their privacy-preserving ontology matching components. These frameworks achieve ontology matching with minimum “privacy leak” of the ontologies being matched. The interoperation system does not assume a trusted mediator. Ideally, organisations want a mediator to gain minimum information about the data and the metadata stored in their information sources. In this system, the mediator operates over encrypted queries, encrypted ontologies, and encrypted data.

Automatic Privacy-Preserving Technologies

The Privacy-preserving Access Control Toolkit (PACT) has been put forward in (Mitra, 2006) to enable privacy-preserving secure semantic access control, and to allow sharing of data among heterogeneous databases without having to share metadata. PACT uses encrypted ontologies, encrypted ontology mapping tables as well as conversion functions, encrypted role hierarchies, and encrypted queries. The encrypted results of queries are sent directly from the responding
system to the requesting one, bypassing the mediator to further improve system security. PACT provides semantic access control using ontologies and semantically expanded authorisation tables at the mediator. One of the distinguishing features of PACT is that it requires very little changes to underlying databases.

An automatic privacy-preserving protocol for schema matching using mutual information of pair-wise attributes has been proposed in (Cruz, 2007). The protocol is executed by two entities, each having a private schema. The output of the protocol is a set of mappings between the matching attributes of the two schemas. This privacy-preserving schema matching protocol is proved secure against malicious adversaries for all mapping types, the authors argue.

In (Bao, 2007), a framework has been designed for privacy-preserving reasoning, in which an agent can safely answer queries against its knowledge base using inferences based on both the hidden and the visible part of the knowledge base, without revealing the hidden knowledge.

**Trust- and Reputation-Enhanced Semantic Interoperation**

Trust is a type of social knowledge and encodes evaluations about which agents can be taken as reliable sources of information or services (Ding, 2003). It is an important aspect of social interaction in human society and potentially in agent societies as well. Trust management and negotiations play an important role in semantic security. The semantic web has created new opportunities and challenges to trust: on one hand, the machine-understandable knowledge resources freely available on the semantic web make it easy to build trust relationships, on the other hand, the vast amount of information, including inconsistent and contradictory information, demands trust in managing the interoperation problem. As shown in Figure 1, trust is an integral part of the semantic web architecture.

Reputation-based trust management (Resnick, 2000) has been identified as a viable solution to the problem of trust in multiagent systems and peer-to-peer networks as well. The main goal of a reputation mechanism is to take the reputation information that is locally generated as a result of an interaction between agents, and spread it throughout the network to produce a global reputation.

Problems of trust and reputation on the web in general, and the semantic web in particular, are topics of significant interest. A satisfactory and robust trust model is important in a situation of information overload, and to help users to collect reliable information in on-line communities. The currently used trust measures can be classified as follows:

**Figure 1. Architecture of the Semantic Web**
Trust is built on an agent’s direct experience with an interaction partner. Current research on trust prediction strongly relies on a web of trust, which is directly collected from users based on previous experience. However, the web of trust is not always available in on-line communities, and even when it is available, it is often too sparse to predict the trust value between two unacquainted people with high accuracy (Kim, 2008). In order to overcome the sparseness of a web of trust, another trust measurement has been proposed (Kim, 2008) (Figure 2) to consider a user’s reputation (i.e., expertise) and affiliation with contexts as main factors to derive trust connectivity and the degree of trust value. The main idea is that a user would trust an expert in the area of interest that matters greatly to her/him.

Trust information is provided by other agents. Agents should be able to reliably acquire and reason about the transmitted information. Sabater (Sabater, 2003) has proposed a decentralised trust model called Regret. It uses an evaluation technique not only based on an agent’s direct experience of its partners’ reliability, but also on a witness reputation component. In addition, trust values (called ratings) are dealt with according to their recent relevance. Regret does not deal, however, with the possibility that an agent may lie about its rating of another agent. Since the ratings are simply equally summed, the technique can be sensitive to noise. The approach in (Venkatraman, 2000) uses a social network to enable a user to leverage the knowledge of several users and their personal agents to find services of the desired type and of high quality without causing excessive communication. A social network (Freeman, 2006) is a social structure made of nodes (which are generally individuals or organisations) that are tied by one or more specific types of interdependency, such as values, visions, or friends.

In a service-oriented environment, trust can be visualised in at least three domains (Hussain, 2006), namely, agent trust, service trust, and product trust. The agent trust ontology is defined as the conceptualisation of agent trust. The interoperation is measured by criteria that are mutually agreed by both the trusting agent and the trusted agent during the negotiation phase.

In (Bentaha, 2007) an agent-based securing system has been developed, where agents are equipped with reasoning capabilities to interact with each other. The agents can reason about the reputation of each other using their argumentation systems. Reputation is computed using a set of parameters based on the interaction histories and the notion of social networks. The model has gathered four most important factors: the reputation of confidence agents; the target’s reputation according to the point of view of confidence agents; the number of interactions between confidence agents and the target agent; and the timely relevance of information transmitted by confidence agents. The author claims that this model can produce a comprehensive assessment of the agents’ credibility.

Certified trust information is provided by

Figure 2. A framework for deriving degrees of trust
Agents should provide third-party referees to witness about their previous performance. In (Yu, 2003) an approach based on social networks has been proposed, where agents can transmit information as witnesses using referrals. Referrals are pointers to other sources of information similar to links that a search engine would plough through to obtain a web page. In this model, agents do not use any particular reasoning, however, and all witnesses are assumed to be totally honest. Timely relevance information is not treated and all ratings are dealt with equally. Consequently, this approach cannot manage the situation where the agents’ behaviour changes.

The trust value of an agent is assessed by collecting the required information of its target agents assuming that they are willing to share their experiences. For this reason, an approach called certified reputation has been put forward in (Huynh, 2006), based not only on direct and indirect experiences, but also on third-party references provided by the target agent itself. The idea is that the target agent can present arguments about its reputation. These arguments are references produced by the agents that have interacted with the target agent certifying its credibility. This approach has the advantage of quickly producing an assessment of the target’s trust, because it only needs a small number of interactions and it does not require the construction of a trust graph. However, this approach has some serious limitations. As the referees are proposed by the target agent, this agent can provide only referees that will give positive ratings about it and avoid other referees, probably more credible than the provided ones. Even if the provided agents are credible, their witnesses could not reflect the real picture of the target’s honesty. This approach can privilege opportunistic agents, which are agents only credible with potential referees.

(4) Trust information is obtained based on semantic similarity between agents. Jiang et al. (Jiang, 2005) have presented a trust construction model to achieve autonomy of trust management in multiagent systems. The presented model adopts graphs to describe trust information, and uses graph combination and path searching to construct trust relations. Any agent can implement trust management autonomously. An agent system can construct a global trust concept by combining trust information among agents. An agent can achieve a trust relation with another agent by trust path searching or trust negotiation.

Gupta et al. (Gupta, 2003) have designed a partially centralised mechanism using reputation computation agents and a public-key-based mechanism that periodically updates peer reputations in a secure and light-weight manner. The PeerTrust (Xiong, 2002) reputation mechanism has been presented to evaluate the trustworthiness of peers by incorporating feedback context such as the total number of transactions and the credibility of feedback sources, where a scalar trust value for a peer is computed based on a figure of the satisfaction received by other peers. A reputation multiagent system, SemTrust, (Wang, 2006) has been introduced to enable the semantic web to utilise reputation mechanisms based on semantic similarity between agents. The main component in Figure 3 is the trust management with the support of the reputation database which stores the agents’ reputation data. The main goal of the reputation

Figure 3. Architectural model of SemTrust Agent

![SemTrust Agent Diagram]
mechanism is to take the reputation information that is locally generated as result of interactions between agents, and to spread it throughout the network to produce a global reputation rating for the network nodes.

(5) Trust information is exchanged using security tokens. In (Wu, 2007), security tokens have been designed to convey various types of trust information exchanged in federated systems. A security token includes claims representing a name, password, identity, key, certificate, group, privilege, and so on. The authors have introduced a hybrid approach (Figure 4) with intermediary- and query-based mechanisms to resolve semantic gaps and incompatibilities for different types of trust information exchanged by security tokens, and then have proposed different exchange models for different types of information.

FUTURE TRENDS

The above overview of the security measures in semantic interoperation shows that there is still a lot of research work to be done. New security levels must be attached to ontologies: certain parts of ontologies could be secret while certain other parts may be open. So, the coming challenge is the interoperation of these ontologies with different security levels, which is the key problem in the application areas of semantic web services.

Current work on ontology security aims to describe security information based on a specified ontology representation language, whereas there are only few papers on how to deal with the security problem of ontologies themselves. This is also worth studying to maintain security and confidentiality of different enterprise ontologies.

Up to now, security research has been separated from trust and reputation. Attention must be given to both security research and privacy research, i.e., we need to protect the privacy of individuals and, at the same time, ensure that they have the information needed to carry out their functions. The adoption of security tokens makes identity, privileges, and trust-related knowledge interoperable across security domains, which eliminates a barrier to inter-domain business transactions, collaborations, and trust-knowledge management. Our future work will focus on managing privacy, trust, and reputation simultaneously during semantic interoperation.

CONCLUSION

This chapter has given a snapshot of the security issues in the semantic web and of web services. After reviewing the background of the security problem in the semantic web, we have provided details of various security methods in semantic interoperation like XML security, RDF security,
ontology security, security and privacy in semantic interoperation, and trust (including reputation) enhanced semantic interoperation, where secure access control policies and secure knowledge management techniques have been addressed. Various methods of security, privacy, and trust management during semantic interoperation have been mentioned in the chapter. Significant work is still required, however, to focus on security, privacy, and trust at the same time.

REFERENCES


KEY TERMS AND DEFINITIONS

Access Control: Access control is a mechanism that allows resource owners to define, manage, and enforce the access conditions for any resource.

Ontology: Ontologies are defined as “explicit conceptualisation(s) of a domain” (Gruber, 1993), and are seen as a key to realise the vision of the semantic web.

Privacy: Portions of a document can be set to private, so that they are invisible during the interoperation process.

Security: Syntax for encrypting or decrypting digital content in XML documents, in RDF triples, or in ontology representation languages.

Semantic Interoperation: Semantic interoperation and service sharing are used to support collaboration across different enterprise systems.

Semantic Web: Envisioned by Tim Berners-Lee, the semantic web is a universal medium for data, information, and knowledge exchange. It suggests to annotate web resources with machine-processable metadata.

Semantic Web Services: Semantic Web services can be defined as web services whose descriptions are annotated by machine-interpretable ontologies so that other software agents can use them without having any prior ‘built-in’ knowledge about how to invoke them.

Trust and Reputation: Trust and reputation is defined as the “subjective expectation an agent has about another’s future behavior based on the history of their encounters”.