A proposal for Ontology Security Standards

Muhammad Reza Fatemi, Atilla Elçi and Zeki Bayram
Department of Computer Engineering, Eastern Mediterranean University,
Gazimagusa, TRNC (Northern Cyprus)
{muhammad.fatemi, atilla.elci, zeki.bayram}@emu.edu.tr

Abstract - *Semantic technologies, such as RDF (Resource Description Framework) and OWL (Web Ontology Language), are being widely used to store information. Ontology is mostly used in semantic platforms or embedded in other applications as a repository system. Data is the most crucial asset of information systems, and ontology can be used as a data repository, so it should be well protected. Trust, proof and security are three major aspects of semantic systems which are less investigated and are mostly afterthoughts of the semantic web. In this paper security problem(s) of ontology, as a layer of the semantic web, is discussed.*

Keywords: security, semantic, ontology, secure ontology.

1 Introduction

The crucial characteristics of security are confidentiality (prevention of unauthorized users from obtaining access to information), integrity (the prevention of the unauthorized modification or deletion of information), and availability (the prevention of the unauthorized withholding of information). Information needs to be granted access, so people can use and improve it. But there is always the risk of information getting into the wrong hands. Security of data transmission is not a new topic and many algorithms and models are proposed to defeat possible attacks and intrusions, and to protect data. The main concern of security is access control managment and risk assessment process, which grants access for read, write and browse based on users qualifications, detects unusual activity and determines risk possibilities [12].

The Semantic Web is well defined as a technology which permits computers to process data, communicate with other computers and make decisions on behalf of humans [1]. It has provided hope for easier daily transactions and trusted, meaningful desicion making of computers without human supervision.

We can imagine a computer agent as our personal secretary which wakes us up on any day of the year according to our specified schedule on that day. It can remind us of any event according to its meaning. For example, one week before our wedding anniversary, it reminds us of buying a gift. If we want to schedule a meeting on that date, it reminds us that we should not have any arrangment on that date beacause of our special arrangements eralier. Although there already is plenty of software with similar functionality, they need to be configured by the user and have no content or context awarness. Semantic based technologies transact with the rest of the web (information repositories) and make desicions based on information available with consideration of meaning of the context.

Semantic computing is really promising, but security concerns must be addressed as well. Without proper security mechanisms, data and its meaning would be at risk. For example, if an unauthorized person could obtain control over one's computer agent, that person's personal data could be exposed and his/her privacy invaded. Security measures are not well specified in the semantic web: to what extent should agents trust each other, or who should be permitted to view some portion of information, or should he/she be permitted to make changes? In the databases area, during past two decades, a lot of advances have been made concerning access control and data privileges management. The same thing should be done in semantic data repositories to avoid security problems.

This paper provides an insight into available secure protocols and standards for the semantic web layers, and proposes ways of providing security in the semantic web. In section 2, we briefly review available semantic web security standards. In section 3, three different approaches are proposed to overcome the lack of security in ontologies as the data repository layer of the semantic web. Section 4 is the summary and future research directions.

2 Semantic web security standards

In this section we briefly visit current security measures of the semantic web. Several layers form the semantic web, which is visualized in Figure 1. It is not possible to say security is need as a whole package; it should be considered separately for each layer. Different measures of security are considered for each layer depending on their characteristics and specification. It is really a better software engineering approach to consider security during design time, but unfortunately for some layers of the semantic web, security was not considered during design. The lowest layer is URI/IRI which is the transport layer. Mostly, this layer is considered to be the web itself. It has been functional for many years now, and there are a lot of simple and complicated security measures considered for it, such as secure sockets. Next layer is XML and RDF which are used in web services and semantic web services. There are some security measures available for it and still people are working to improve them. These measures include XML signature, XML encryption and XML access control management. The next layer is ontology, rules and queries which lacks a lot in security when compared to the above mentioned layers. Security has been left out of consideration for this layer. Ontologies are mostly protected through other layers of the system rather than themselves. The next layer is logic and proof, which is currently less defined than the other layers, and is not that much in use, although there is ongoing research on it. The next layer is trust, which provides confidentiality, integrity and authentication. The most important untouched layer is Crypto, which is the means in which securiy is implemented in the other layers [2, 3, 4, 5, 6, 7].

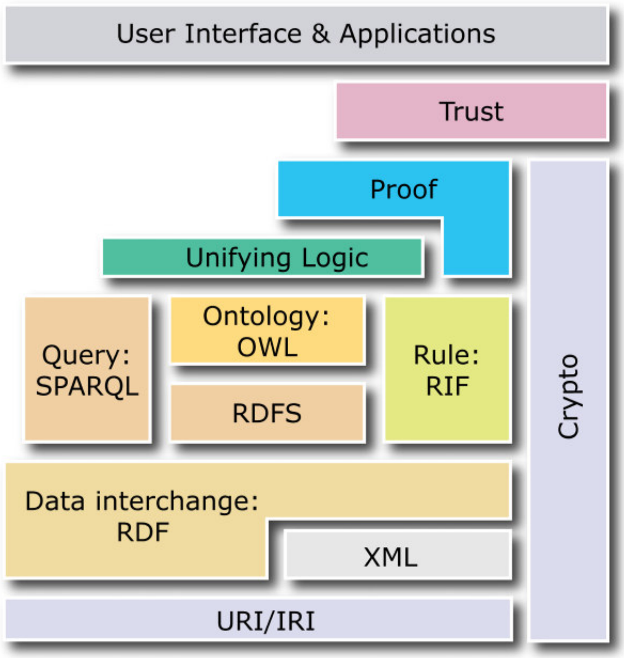

Figure. 1. Semantic Web layers (obtained from http://www.w3.org/2007/03/layerCake.png).

2.1 URI/IRI Security

URI/IRI security concerns mostly the transport or communication layer. It includes secure sockets, secure TCP/IP, secure agents communication and secure HTML. It is usually considered an already built standard because most applications are using available technologies such as http or https which have their own security specifications. But if one decides to work in a personal semantic framework which will not use available technologies for the means of data transportation, he/she must apply at least the same level of security available in hardware and software implementation.

2.2 XML and RDF Security

XML documents are structured graphs. Security standards have been set for them almost completely in means of access control, authentication, digital signatures and encryption methods. XML documents are mostly considered as structured files, so there are no semantic issues in protecting them, and as it was mentioned above they can be heavily protected [5].

RDF documents are basically XML documents which define the meaning of their content in a basic manner. They can be secured using conventional methods which are defined for XML, but there has to be security for semantics as well as the document itself [5]. It is a challenging task, and it is out of scope of this paper.

2.3 Ontology Security

Ontology is the highest level in semantic layers which has been completely designed and well defined. Unfortunatlly, currently there are no means of security available for this layer. It contains the most important part of the system, i.e. the data, meaning of the data and rules and logic for deduction and decision making. Security-related issues that should be addressed, regarding ontologies, include:

- How much or which part of the data should be accessed and by whom?
- Which queries should be answered and till which depth?
- Access Control: Who is going to access the information and which portions of it?
- Authentication: How to know the identity of a person exploring the ontology? Should we use digital signatures?
- Encryption: Should we use encryption? Should it be symmetric or asymmetric?
- SPARQL: If all above are implemented, one tries to run a query which the answer is out of his/her security permissions what should the system do?

These questions and similar security problems of ontologies can be solved using a secure semantic framework which we propose section 3.

2.4 Logic, Proof and Trust

Logic is partly available in previous layers in the form of rules and restrictions. Proof and trust are layers of the semantic web which are not standardized yet. Regarding Trust management, outstanding issues include: How to trust the information? How much to trust the information? How to trust the other party during the communication? Most importantly, with what standards we should negotiate with other party? Currently, Protocols and languages are being defined for trust management, and hopefully security issues will not be left out to be considered later like the ontology layer [9].

3 Ontology security managment

The issues raised in section 2.3, and other similar security problems of ontologies, can be solved using the secure semantic frame work which we propose in this section. Our frame work consists of two tiers, the first of which is from section 3.2 or section 3.3 (both implementing EMLS described in Section 3.1), and the second one from section 3.4. The first tier deals exclusively with OWL files. A framework is needed to recognize and configure the OWL file because of modifications in the OWL-language in 3.2 and joint file structure in 3.4. In section 3.4 a framework is proposed which runs SPARQL queries according to security measures which are applicable with both approaches of 3.2 and 3.3.

3.1 Security rules and regulations

Security rules are taken from the Izadpanahi and Fatemi proposal on Enhanced Multi-Level Security (EMLS) [10], which we review here briefly.

A Multi-Layer Security (MLS) system must properly enforce two rules: (1) the no read-up rule, where reading of an object above the subject's clearance level is prevented, and (2) the no write-down rule, where writing into an object below the subject's clearance level is prevented by the system. Clearance level indicates the level of trust given to a person with a security clearance. Classification level indicates the level of sensitivity associated with some information.

Group Security (GS) is an object oriented perspective of data sharing over a secure system with specific properties. EMLS supports the properties and functionalities of MLS but in this system we have some more features as listed below:

- Owner of a subject can bind access modifiers according to his/her criteria (ownership property)

- Owner can grant divided access levels to each of his/her objects as follows:

  - Read, Write, Delete for owner (private property)

  - Read, Write, Delete for subject with same clearance level (group property)

  - Read, Write, Delete for everyone (public property)

Considering the above security measures, we have to have semantic meaning for our users and objects. For this purpose we have classes in our ontology for our users and groups, and every user should belong to a group. So we will have a group ID for each user inside the system. Objects are individuals in the system; they also have a group ID. These proposed security security measures are considered at really basic levels for the sake of simplicity.

3.2 Secure OWL (SOWL)

This proposal considers a new Web Ontology language which has security measures built in it, which we call Secure Web Ontology Language (SOWL). SOWL will be a really simple language if we want to just consider the security measures in previous section; there will be more realistic and complicated security measures considered in future framework implementation. For now the EMLS framework [11] is considered.

Our Security rules will have the form of Subject, Activity, and Object type (S, A, O). As depicted in Figure 2, security class is a sample class type for security markup rules. Security measures can also be as property types for group id allocations as it is shown in Figure 3.

```
<SecurityClass name= " "  subject="David" >

    <rule name=" "  type="Permission"
    activity="ReadUp"      object=" "/>

    <rule name=" "  type="requirment"
   activity="WriteDown" object=" "/>

</SecurityClass>
```

Figure. 2. Security Class Tags

```
<owl:Class rdf:ID="Person"/>

<Person rdf:ID="David">

    <hasClearancelevel
    rdf:datatype="http://www.w3.org/2001/XMLSchema#i
    nt">3</ hasClearancelevel>

</Person>
```

Figure. 3. Security property Tags

It has to be considered that SOWL is a new syntax proposal, and has a new grammar. We can consider it to be next generation of OWL. Also, for security measures, SOWL files are rendered to be readable in the framework reader or to be text-based if they are in secure environment under the semantic management server protection.

3.3 Ontology Security layer (OWL+S)

OWL+S is considered as extra layer to OWL itself. It is the idea of passing the security ontology along with the

OWL file. It is more applicable than SOWL because already operational services would not need any modifications to secure themselves. By defining the tags inside security ontology as Classes and properties we do not nee the syntax change like SOWL; as it is demonstrated in Figure 4. We should note that since the security ontology itself is a text-based file, it should be protected from being obtained without authentication and appropriate access management (a kind of meta-level security).

```
<owl:Class rdf:ID="Person"/>

<owl:Class rdf:ID="Security"/>

<Person rdf:ID="David>


    <hasClearancelevelrdf:datatype="http://www.w3.org/2
    001/XMLSchema#int">3</ hasClearancelevel>

</Person>

<Security tdf:ID="GeneralSecurity">

     <hasName
    rdf:datatype="http://www.w3.org/2001/XMLSchema#st
    ring">" "</hasName>

      <hasSubject rdf:resource="David " />

.....

</Security>
```

Figure. 4. Security Ontology Example

3.4 Secure Semantic Query Management System (SSQMS)

This is part of our semantic frame-work management system. According to a user's choice for security layer (SOWL/OWL+S), the system is configured to derive the normal SPARQL result, and compare it to the security access level of the Subject, and if user is permitted to have access to the result, then display it. Security policies are defined in our security ontology, where users and objects are related to their security clearence levels. According to the EMLS access management regulations, if the user would be permitted to have access to the results of query, he/she would be permitted to see the results.

4 Summary and directions

Security standards had to be set when OWL was designed, but unfortunately they have been left as afterthoughts. To make up for this deficiency, we designed a new security framework, based on our previous work on EMLS. This involved, in our first method, an extension to OWL in order to incorporate security information directly in the OWL file containing the actual data. Furthermore, we described briefly how SPARQL queries could be executed within this security framework in order to show results to users only if they are authorized to see the results. For future work, we plan to implement the proposed security framework, and see how existing data in semantic repositories can be made to benefit from our approach.

5 References

[1] Berners Lee T., et al.; Semantic Web, Scientific American, may 2001.

[2] Thuraisingham B.; Security standards for the semantic web, Computer Standards & Interfaces, Vol. 27, pp. 257-268, 2005.

[3] Harris D., et al.; Standards for secure data sharing across organizations, Computer Standards & Interfaces, Vol. 29, pp. 86-96, 2007.

[4] Tan J.J., Poslad, S.; Dynamic security reconfiguration for the semantic web, Engineering Applications of Artificial Intelligence, Vol. 17, pp. 783-797, 2004

[5] Thuraisingham B.; Building secure survivable semantic web, IEEE International Conference on Tools with Artificial Intelligence, ICTAI02, 04-06 November 2002, Washington D.C., USA.

[6] Thuraisingham B.; Confidentiality, Privacy and Trust Policy Enforcement for the Semantic Web, IEEE International Workshop on Policies for Distributed Systems and networks, POLICY07, Bologna, Italy, 13-15 June 2007.

[7] Bertino E., et al.; Secure knowledge management: Confidentiality, Trust and Privacy, IEEE Transactions on Systems, Vol. 36, No. 3, May 2006.

[8] Li J., et al.; A Policy language for Adaptive Web Services Security framework, ACIS International Conference on Software Engineering, SNPD07, Qingdao, China, 30 July 30 – 01 Aug 2007.

[9] Kim A., et al.; Building Privacy into the semantic web: An Ontology needed now, International Workshop on the Semantic Web, www02, Hawaii, USA, 7 May 2002.

[10] Izadpanahi S., Fatemi M.R.; Enhanced multi-level security: secure sharing model, The 2007 World Congress in Computer Science, Computer Engineering & Applied Computing, SAM07, Las Vegas, Nevada, USA, 25-28 June, 2007.

[11] Li C., Pahl C.; Security in the web services framework; International. Symposium on Information and Communications Technologies, ISICT03, Dublin, Ireland, 24-26 September, 2003.

[12] Chefranov A.G.; CMPE552 Lecture notes, Computer Engineering, Eastern Mediterranean University, Famagusta, TRNC, Fall 2006.