Proceedings of the IASTED International Conference
Software Engineering (SE 2009)
February 17 - 19, 2009 Innsbruck, Austria

REQUIREMENTS OF A SECURITY FRAMEWORK FOR THE SEMANTIC WEB

Ibrahim R. Mbaya[1], Aurona J. Gerber[1,2], Alta J. Van der Merwe[1,2]
1) University of South Africa (UNISA), School of Computing
2) Meraka Institute, CSIR
Pretoria, South Africa
ibrahimm@infosys.co.tz, aurona.gerber@meraka.org.za, vdmeraj@unisa.ac.za

ABSTRACT
The vision of the Semantic Web is to provide the World Wide Web the ability to automate, interoperate, and reason about resources and services on the Web. However, the autonomous, dynamic, open, distributed and heterogeneous nature of the Semantic Web introduce new security challenges. Consequently, security becomes a crucial factor for the adoption of the Semantic Web. There are existing suggested security frameworks for the Semantic Web, however none of these address all issues related to the Semantic Web, neither have any requirements for such frameworks been established. Common criteria are therefore required to evaluate existing security frameworks. In this paper, we suggest a set of evaluation criteria that can be used to evaluate existing Semantic Web security frameworks.

KEY WORDS
Requirements, security framework, Semantic Web

1. Introduction

In the late 1990s, the inadequacy of existing Web technologies to automate processing of Web resources was realised [1], and the need for machine understandable Web pages and the use of ontologies for information integration was formulated. To address this need, the concept of the Semantic Web was introduced by Tim Berners-Lee in 2001 [1]. The Semantic Web can been seen as an extension of the current World Wide Web (WWW) where resources are enriched with machine-understandable metadata that describe their meaning to enable easy processing of information by machines and software agents.

At present the ultimate vision of the Semantic Web as formulated by Berners-Lee et al. [1] remains largely a research initiative. However, the vision initiated significant interest with regards to the required technologies for the enabling of the Semantic Web [2, 3, 4, 5]. Notably, the W3C recommended a number of standards for languages of increasing expressivity as depicted by the Semantic Web layered architecture [1, 6, 7, 8]. The Semantic Web architecture depicts a hierarchy of languages that exploit the features and extend the capabilities of the layer below it [9]. Languages that have been adopted by the World Wide Web Consortium (W3C)1 for the Semantic Web include Unicode, Uniform Resource Identifier (URI), extensible mark-up language (XML), Resource Description Framework (RDF), RDF-Schema (RDF-S) and ontology Web language (OWL) [10].

At present the W3C technologies are used in various prototype applications demonstrating Semantic Web functionality such as proposed by, for instance, the participants in the Semantic Web Challenge (Golbeck and Mika, 2008). Quoting from the Semantic Web Challenge web site [11], "The Semantic Web Challenge offers participants the chance to show the best of the Semantic Web". For 2007, Challenge Co-Chair, Peter Mika added "this was by far the most competitive year, with the highest number of participants ever, and a significant improvement in the quality of the entrants" [11]. Revyu [12] was selected as the challenge winner from a record 23 entries of which 18 made the first round and five were shortlisted. Revyu is an application that allows anybody to review and rate anything on the Web.

Another interesting and recent application of Semantic Web technologies is the CHIP (Cultural Heritage Information Presentation) site winning third prize at the 2007 Semantic Web Challenge [13]. The stated goal of the CHIP project is to demonstrate (i) how Semantic Web technologies can be deployed to enrich the Rijksmuseum vocabularies and providing semantic browsing, searching and semantic recommendations; and (ii) how personalization and user modeling techniques can be explored to enhance users' experiences both on the museum Web site and in the physical museum space. Based on a semantically-enriched data model, the team members have implemented three different tools in the CHIP demonstrator naemly Artwork Recommender, a web-based virtual Tour Wizard and a PDA-based Mobile Tour. *Artwork Recommender* is a Web-based rating dialog for artworks/topics to build a user profile, based on semantics-driven recommendations. *Tour Wizard* is a Web-based tool using the user prole to generate (semi)automatically personalization virtual museum tours for each user. *Mobile Tour* is a PDA-based tool to map

virtual tours into the physical museum space with constraints; to give guidance to users and to synchronize the user profile on the web and in the PDA.

From the above evidence and related activities, it is possible to argue that Semantic Web applications are moving from being mainly research activities to the commercial space. This is mainly due to the level of maturity reached by the Semantic Web technologies and standards as proposed by the W3C.

The Semantic Web creates new security challenges due to its completely decentralised nature, the meta-data descriptions, the extremely large number of users, agents, and services, and their heterogeneity. Security challenges associated with the Semantic Web involves the ability to handle security and to automate security mechanism to a more autonomous system that support complex and dynamic relationships between data, clients and service providers [14].

Various attempts have been made to develop security mechanisms or frameworks for the Semantic Web [15, 16, 17]. The problem with most of these suggested frameworks is that none was developed from a set of basic requirements as design criteria. In addition, we could not find any criteria that could be used to evaluate or validate existing frameworks. In order to develop a holistic and comprehensive security framework for the Semantic Web, a set of design criteria is a prerequisite. This indicates an identified gap in the literature that is one of the focus areas of this paper.

In this research we propose a set of requirements for a security framework for the Semantic Web extracted from the existing theory. In addition, some of the recent proposed security frameworks for the Semantic Web will be evaluated against the requirements of a security framework for the Semantic Web in order to establish the usefulness thereof.

In section 2, an overview on the Semantic Web, as well as existing security frameworks for the Semantic Web are given. In section 3 we give a short discussion on how the characteristics were derived followed by a discussion on the characteristics itself in section 4. In section 5 we evaluate the security frameworks discussed in section 2.2 and add some concluding remarks in section 6.

2. Background

2.1 The Semantic Web

In 2001, a vision of a Web called the Semantic Web was presented by Tim Berners-Lee [1]. The Semantic Web was envisioned as an information space usable by machines i.e computers, PDAs, cell phones and computer programs that can perform tasks on the World Wide Web. In the Semantic Web, a user could have, for example, personal software agents that would search Web resources and Web services, process information from multiple sources, exchange results with other software agents on behalf of users and present the results to the user, who would only have access to the results presented by his or her software agent.

The Semantic Web is an extended Web of machine-readable information and automated services that extends beyond current capabilities of the World Wide Web. According to Berners-Lee [8], the Semantic Web is a mechanism that assists data interoperability across applications and organisations. It is a set of interoperable standards for data, information, and knowledge exchange, and for integration between applications and communities. The main use of the Semantic Web is to integrate diverse data sources intelligently into modern Information systems. The Semantic Web enables software agents and search engines to find and interpret Web content quicker and with more accuracy than is possible with current keyword-searching or data-mining techniques [18].

The Semantic Web is specified by means of various interoperable technologies that perform different functions within the context of the Semantic Web namely data interoperability using meta-data descriptions. In order to understand the purpose and functions of these technologies, one needs to investigate the architecture of the Tim Bernesrs-Lee 2005 Semantic Web [7]. The Semantic Web architecture is generally presented as a layered architecture in which semantic language functionalities and technologies are layered into an increasingly expressive stack. Different versions (Figure 1-4) of the Semantic Web architecture were released by Tim Berners-Lee in order to organise the existing Semantic Web technologies and to identify functionalities of metadata languages used on the Semantic Web [1, 6, 7, 8]

Table 1
Summary of the Semantic Web architecture as adopted [19]

	Functionality	**Technologies**
1	Unique Identification	Unicode and URI
2	Syntax Description Language	XML, XML-Schema, and Namespaces
3a	Metadata Data Modelling	RDF
3b and 4a	Ontology	RDF-Schema and OWL
4b	Rules	SWRL?
5	Logic Framework	
6	Proof	
7	Trust	
Vertical Layers	Security mechanisms	XMLDSig and XMLEnc

Layer functionalities that make up the Semantic Web stack includes unique identification layer, syntax description layer, metadata data modelling, ontology, rules, logic framework, proof, and trust. The Semantic Web stack also includes two vertical layers namely signature and encryption. The vertical layers provide security mechanisms to support the language architecture.

The purpose of the Semantic Web layered architecture is to depict the languages necessary for data interoperability between applications. Unicode, Uniform

Resource Identifier (URI), extensible mark-up language (XML), Resource Description Framework (RDF), RDF-Schema (RDF-S) and ontology Web language (OWL) are at present W3C Recommendations or standards for the Semantic Web [10]. The original layered architecture as presented by Berners-Lee has been the subject of numerous academic discussions, for example, the status discussions and an extraction of the Semantic Web layer functionality by Gerber et.al [19] summarised in Table 1.

From the discussion above it is clear that the current standardisation efforts with regards to the Semantic Web focus on the data interoperability and meta-data description functionality. There is no clear distinguishable effort in determining the security needs for the Semantic Web. The need for a security framework for the Semantic Web is evident due to the current activity within the Semantic Web domain. Some work has been published in an attempt to address various security issues related to the Semantic Web as is summarised in the next section.

2.2 Existing security frameworks for the Semantic Web

From the literature studied, different authors use different terms such as models, method, technique, approach, infrastructure etc referring to frameworks. For the purpose of this discussion, a security framework refers to frameworks, models, approaches, methods and techniques that provide one or more security services such as integrity, authentication, authorisation, confidentiality and non-repudiation.

In order to compile a security framework for the Semantic Web, it is essential to study existing security frameworks, and establish their applicability to the Semantic Web. Studying the existing security frameworks will assist with the identification of requirements for such a framework, as well as assist with the justification of the need to establish a comprehensive security framework for the Semantic Web. By understanding how existing security frameworks were compiled will assist in this study to establish similar or better method of compiling a security framework and to decide on features and components to be included in the framework.

The following security frameworks are considered:

- Kagal et al. [20] proposed a policy-based security approach for the Semantic Web (PBSASW). The security framework is based on a policy language, which addresses security issues for Web resources, agents and Web services in the Semantic Web. The framework provides access control to entities without necessarily authenticating the requesters completely. Furthermore, it provides flexibility in specifying security requirements and gives every entity certain autonomy in making its own security decisions.
- Qin and Atluri [21] proposed a concept-level access control model for the Semantic Web (CLACSW). The model is used to specify access authorisations based on concepts and their relationships. Access authorisations are stated on concepts specified by ontologies. The model consists of concepts and their relationships, propagation policies, authorisation conflict resolution, and a semantic access control language.
- Ashri et al. [17] proposed a Semantic Web security infrastructure (SWSI) that uses Semantic Web technologies to improve security in service-oriented, open heterogeneous environments. The infrastructure makes use of conventional security solutions, together with the ability to reason about security at the semantic level, by using appropriate security policies. The infrastructure also makes use of a semantic firewall for the enforcement of security policies.
- Tan and Poslad [22] proposed a profile-based security model for the Semantic Web (PBSMSW) that supports policy-type constraints and a profile-based security information interchange for multi-domain services. A profile describes relationships among safeguards, assets and threats. Profiles can also express policy rules, defining security instantiations and preconditions supported.
- Carminati, Ferrari and Thuraisingham [23] proposed a security framework that uses RDF for policy specification and enforcement (RDF-PSE). The framework utilises the semantic richness of RDF for expressing security information and hence making policy specification and enforcement easier. The framework is capable of automatically entailing all the authorisations implied by the application of the high-level policies to a specific scenario.

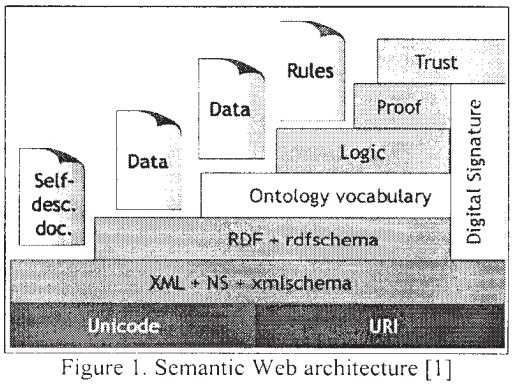


Figure 1. Semantic Web architecture [1]

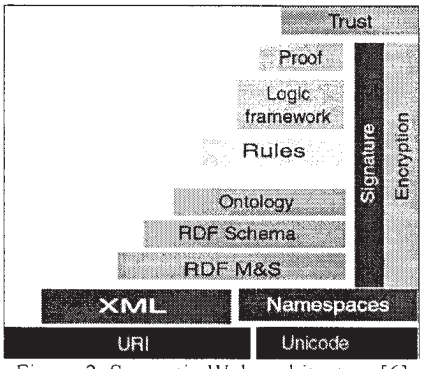


Figure 2. Semantic Web architecture [6]

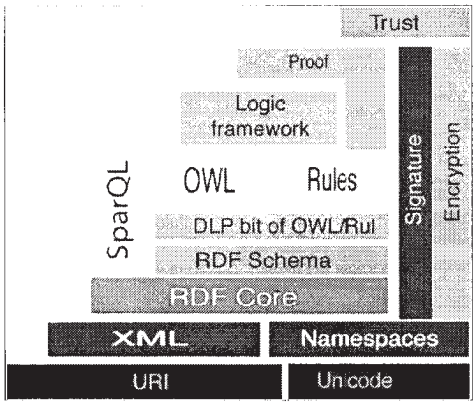


Figure 3. Semantic Web architecture [7]

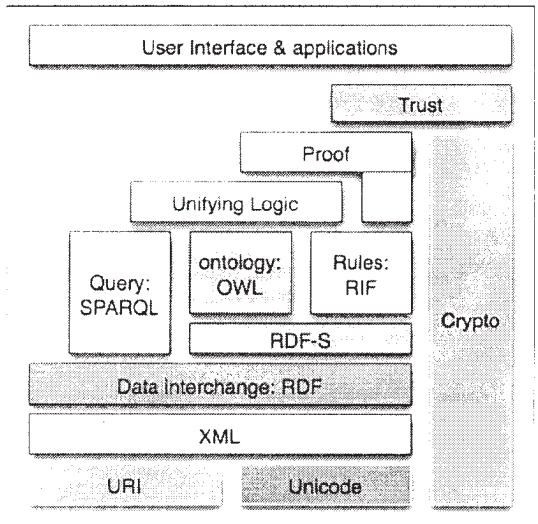


Figure 4. Semantic Web architecture [8]

From the literature presented, it is evident that existing security frameworks were developed to address different security aspects of the Semantic Web. There is a clear need to have a security framework that integrates these disparate security frameworks to provide a holistic, comprehensive, secure environment for the Semantic Web. This paper addresses the first step in developing such a security framework by outlining the requirements of a security framework for the Semantic Web.

3. Research Approach

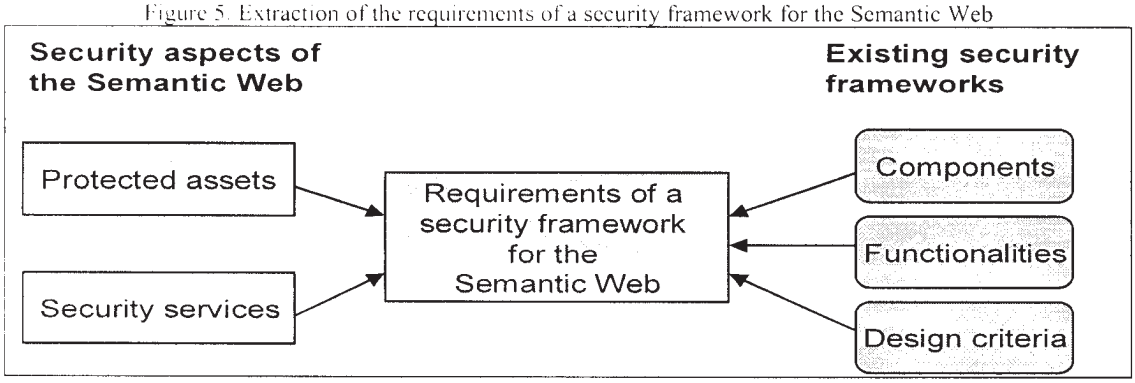
The requirements of a security framework for the Semantic Web were derived from the literature surveyed. In the research we used documentary sources, which involve existing textual documents available in electronic and printed media. The data sources used in this research include databases available in the University of South Africa's (UNISA's) online library catalogue, as well as academic articles published in peer-reviewed, academic journals, applicable textbooks, and the Internet.

In this research project, textual analysis is used as a means of data collection. Textual analysis involves both content analysis and textual interpretations. Based on the research departure points, namely the Semantic Web and security frameworks, the contents of the referenced publications were analysed to find their applicability to the study. Furthermore, textual interpretation of a relevant publication led to the identification of additional publications relevant to the study. Textual data are rich in meaning and difficult to capture in a short and structured manner. Relevant publications were summarised to capture the information provided by the reference. Similar information from different publications were categorised and grouped to simplify and obtain a coherent understanding of a particular domain.

The requirements were extracted from existing security frameworks (overview in section 2) and other surveyed literature on security aspects of the Semantic Web (Figure 5).

Security aspects of the Semantic Web include protected assets and security services. The protected assets for the Semantic Web include entities that interact with the Semantic Web i.e. agents, Web resources, and Web services [20]. Security services associated with the Semantic Web include security requirements for network access defined by the International Organisation for Standardisation (ISO7498-2, [24]) i.e. authentication, authorisation, integrity, confidentiality, availability, and non-repudiation.

Figure 5. Extraction of the requirements of a security framework for the Semantic Web



Different authors have indicated different aspects that should be considered when developing a security framework for the Semantic Web [20, 24, 17]. These aspects range from technologies to be used, security functionalities to be provided, and design criteria, to implementation issues.

4. Requirements of a Security Framework for the Semantic Web

The existing body of knowledge indicates that there are various attributes and features that may be used as design criteria for a security framework for the Semantic Web. The requirements of a security framework for the Semantic Web are presented in this section without following a particular order in terms of importance, complexity, or whatsoever. All the requirements are considered important and need to be satisfied by a security framework for the Semantic Web.

4.1 Decoupling of security functionalities from core service functionalities

According to the discussion of infrastructure capabilities for the Semantic Web Security Infrastructure by Ashri et al. [17] 'the security infrastructure should take into account the possibility that not all services will be able to individually reason about security requirements'.

Since not all Web Services will be able to reason individually about security requirements, such Web Services should be supported by other components that are able to reason about security. The inability of other entities to reason about security requires decoupling of the capability to reason about security from the core service capability. The advantage of decoupling of security functionality from core service functionalities lies in the increased efficiency of the Web service and the reusability of the security components.

4.2 Layered security support

According to Ashri et al. [17], 'If an individual Web Service defines and is able to reason about its own security requirements, these may still need to be aligned with the security requirements of the larger domain within which the service operates'. This argument carries with it the need for a layered security framework with security requirements that are Web Service-specific, application-specific, domain-specific and inter-domain-specific.

To facilitate collaboration, groups of software components, people, resources, and other entities are structured into organisations of domains and sub-domains [25]. Securing entities in these multi-domain environments needs generic security functionalities as well as application-specific security functionalities. A layered security framework will enable interoperability of Web services between organisations without compromising the security of the service providers.

4.3 Flexible, dynamic and adaptive

The set of entities that need to access an information source or interact with a given Semantic Web entity cannot be enumerated a priori [14, 20, 16]. Entities can also join or leave the Semantic Web without prior notification. The framework must be flexible enough to be applicable in different scenarios with few or no changes [26].

Interactions within the Semantic Web entities can be secured depending on aspects such as the current context, interaction type, and so on. The security framework should be able to adapt to these aspects in order to allow the sending and receiving of appropriate messages [17]. The framework must be capable of adapting itself to frequent changes in parameters such as access criteria, client attributes, environment conditions, resources available, and the like [26].

4.4 Semantically rich

The problem of semantic meaning of the security information where it is not feasible to expect all entities to use the same terminology to represent security protocols and information necessitates the security framework for the Semantic Web to be semantically rich [14, 20].

There is an increasing need to be able to describe and reason about security requirements at the semantic level [16, 17]. Security should be preserved at the semantic level in order to provide access control at the finest granularity and to ensure that RDF documents are secured [16]. A semantically rich representation allows description of contexts at a high level of abstraction, which is essential in both reasoning and conflict resolution for policies [27].

4.5 Simple enough to automate

The need for machines to access and process information securely on the Semantic Web requires the automation of the Semantic Web security framework [14]. According to Kagal et al. [20], the ability to handle security and privacy and the ability to automate security protocols for the use of all Web entities are the key needs for the vision of the Semantic Web to succeed. Complex and static security mechanisms that will need the intervention of system administrators will not scale well with the Semantic Web. Too sophisticated security mechanisms to implement security requirements in open environments can result in complex systems that are impractical for large-scale interoperable deployments [22].

Automatic computing is necessary for systems that need to interoperate securely in open environments, where real-time applications need automatic security mechanisms to interoperate, mediate and self-manage [22].

4.6 Impervious to common network security problems

The Semantic Web as the extension of the current Web shares the inherent common characteristics and problems of the current Web technologies such as network partitioning [14]. Issues of secure communication channels, user and server authentication, and end-to-end network security are common in network environments.

Security from the above-mentioned common network security problems is not specified on the Semantic Web but needs to be addressed by the security framework for the Semantic Web. The security framework for the Semantic Web therefore needs to include mechanisms such as SSL, X.509, etc. that will address common security problems on networks.

4.7 Implementable on the current Semantic Web technologies

The Semantic Web is built upon layers of expressive languages of increasing powers. These languages enable the automation of the retrieval and usage of Web resources. Languages that have been adopted by W3C include Unicode/URI, XML, RDF, and OWL [1, 19, 10].

Since the study focuses on compiling the security framework for the Semantic Web and not on developing or improving the current enabling technologies, the security framework for the Semantic Web needs to be implementable on existing technologies.

4.8 Provides protection to all Semantic Web entities

In order to enforce security on a computer system, one needs to identify computing assets that need to be protected [28]. In the context of the Semantic Web, the assets that need protection are the entities that interact with the Semantic Web. These entities include agents, Web services and Web resources.

Web services need to be protected from session-hijacking, eavesdropping, wire-tapping, impersonation, spoofing, masquerading, and denial-of-services. Web resources need to be protected from eavesdropping, wire-tapping, impersonation, deletion of resources, illegal inferences and denial of services. Software agents need to be protected from eavesdropping, information modification, masquerading, cloning and denial of service.

4.9 Provides a complete set of security services

According to a computer security principle, i.e., the principle of easiest penetration, an intruder must be expected to use any available means of penetration. This principle teaches us that to attain the goal of security one needs to consider every possible means of protection [28]. To achieve security, the framework should provide all security services outlined by International Standards organisation (ISO 7498-2, [24]), i.e. authentication, authorisation, integrity, confidentiality, availability and non-repudiation.

5. Evaluation of existing security frameworks

In this section, existing security frameworks are evaluated against the requirements of a security framework for the Semantic Web. The evaluation is intended to establish the gap between the existing security frameworks and the security requirements for the Semantic Web. In Table 2 we list the security frameworks discussed in section 2.2 for reference purposes.

Table 2
Abbreviations for existing security frameworks, refer to section 2.2

Abbreviation	Security framework
SWSI	Semantic Web Security Infrastructure.
PBSASW	Policy-Based Security Approach for the Semantic Web.
PBSMSW	Policy-Based Security Model for the Semantic Web.
CLACSW	Concept-Level Access Control for the Semantic Web.
RDF-PSE	RDF for Policy Specification and Enforcement.

Using the requirements identified it was found that there is no security framework that satisfies all the requirements, although all security frameworks satisfied at least four requirements (Table 2). Few security frameworks satisfy more than five requirements. Those frameworks that do satisfy more than five requirements have the potential to be adapted to a security framework for the Semantic Web.

Table 3
Requirements satisfied by existing security frameworks

Framework	Requirement number								
	1	2	3	4	5	6	7	8	9
SWSI	x	x	x	x	x	x	x		
PBSASW	x	x	x	x	x	x	x	x	
PBSMSW	x	x	x	x		x	x	x	
CLACSW		x		x	x		x		
RDF-PSE		x	x	x	x		x		

The following summarize how each requirement is addressed in the specified framework:

- For requirement 1, decoupling of security functionalities from core service functionalities, the decoupling of security functionalities from core service functionalities increases the efficiency of Web services and reusability of security components. The various

security frameworks discussed indicate the importance of decoupling security functionalities from core service functionalities. Security frameworks such as SWSI, PBSASW, and PBSMSW incorporate this requirement in their design principles.

- For requirement 2, a layered security framework enables interoperability of Web services in a multi-agent multi-domain environment (Tan and Poslad, 2004). Security frameworks that support layered security include SWSI, PBSASW, PBSMSW, CLACSW, and RDF-PSE.
- For requirement 3, security frameworks that are flexible, dynamic and adaptive are considered. These included SWSI, PBSASW, PBSMSW, and RDF-PSE. The use of a reasoning model supports dynamic reconfiguration of security services.
- For requirement 4, the semantically richness of the framework is important. Security frameworks that are semantically rich include SWSI, PBSASW, PBSMSW, CLASW, and RDF-PSE. These security frameworks use ontologies to specify security concepts.
- Requirement 5 states that the framework should be simple enough to automate. Security frameworks that are simple enough to automate include SWSI, PBSASW, CLACSW, and RDF-PSE. These are frameworks that are not complex, and use technologies such as RDF, OWL, etc. that are easily automated.
- For rrequirement 6, impervious to common network security problems, the list includes SWSI, PBSASW, and PBSMSW. These security frameworks incorporate conventional security mechanisms to address common network security problems.
- For rrequirement 7, implementable on current Semantic Web technologies, SWSI, PBSASW, PBSMSW, CLACSW, and RDF-PSE are included since these security frameworks use XML, RDF, or OWL for their implementation.
- For requirement 8, provide protection to all Semantic Web entities, we mentioned in section 4 that Semantic Web entities that need protection include agents, Web services, and Web resources. Security frameworks that provide protection to agents include PBSASW and PBSMSW. These frameworks allow agents to specify policies that a requester must satisfy in order to use their services. Security frameworks that provide protection to Web services include SWSI, PBSASW, and PBSMSW. Most of these frameworks make use of policies to specify the security requirements of a Web service for authorised access to the Web service. Security frameworks that provide protection to Web resources include SWSI, PBSASW, PBSMSW, CLACSW, and RDF-PSE. Security for Web resources is mostly provided by cryptographic methods. SSL is commonly used for secure communication of Web resources. From the evaluation of existing security frameworks, it is only PBSASW and PBSMSW that provides protection to all Semantic Web entities.
- For requirement 9, provide a complete set of security services, only SWSI, PBSASW, PBSMSW, and RDF-PSE adheres to this requirement. But, Security frameworks that provide authorisation services include SWSI, PBSASW, PBSMSW, CLACSW, and RDF-PSE. Security frameworks that provide integrity services include SWSI, PBSASW, and PBSMSW. Digital signatures and hash functions are used to ensure integrity of resources on the Web. Security frameworks that provide confidentiality services include SWSI, PBSASW, and PBSMSW. Cryptographic solutions such as encryption are used to ensure confidentiality of Web resources and communication information. The surveyed security frameworks do not provide availability services whereas PBSMSW is the only security framework that provides non-repudiation services.

From the evaluation of existing security frameworks, there is no single security framework that provides all security services required for the Semantic Web.

6. Conclusion

The Semantic Web creates new security challenges due to its completely decentralised nature, the extremely large number of users, agents, and services, and their heterogeneity. Various efforts have been made to develop security infrastructure to support interoperability and secure interchange of information for the Semantic Web. However, there are no clear criteria that can be used to harmonise these disparate efforts into a single security framework for the Semantic Web.

In this paper, requirements of a security framework for the Semantic Web were proposed. The requirements include:

- Decoupling of security functionalities from core service functionalities
- Layered security support
- Flexible, dynamic and adaptive
- Semantically rich
- Simple enough to automate
- Impervious to common network security problems
- Implementable on current Semantic Web technologies
- Provides protection to all Semantic Web entities
- Provides a complete set of security services.

The evaluation of existing security frameworks against the requirements indicates the need to have a security framework for the Semantic Web that satisfies all the requirements.

Establishing the requirements of a security framework for the Semantic Web is a critical milestone in the development of a security framework for the Semantic Web. Developing a security framework for the Semantic Web is crucial for adoption and secure use of the Semantic Web in the multi-agent multi-domain environment.

References

[1] Berners-Lee, T., J. Hendler and O. Lassila (2001). "The Semantic Web." *Scientific American* 285(5): 34-44.

[2] Palmer, S. (2001). "The Semantic Web: An Introduction." Retrieved August, 2005, from http://infomesh.net/2001/swintro/.

[3] Euzenat, J. and A. Napoli (2003). "The Semantic Web: Year One." *IEEE Intelligent Systems* 3: 1094-7167.

[4] Uschold, M. (2003). "Where are the Semantics in the Semantic Web?" *AI Magazine* 24(3): 25-26.

[5] Grau, B. (2004). A Possible Simplification of the Semantic Web Architecture. 13th International Conference on World Wide Web, WWW '04, New York, ACM Press.

[6] Berners-Lee, T. (2003). *Standards, Semantics and Survival.* SHA Upgrade: 6-10.

[7] Berners-Lee, T. (2005). "WWW 2005 Keynote." from http://www.w3.org/2005/Talks/0511-keynote-tbl/.

[8] Berners-Lee, T. (2006). "Artificial Intelligence and the Semantic Web: AAAI2006 Keynote." from http://www.w3.org/2006/Talks/0718-aaai-tbl/Overview.html.

[9] Horrocks, I. and P. F. Patel-Schneider (2003). Three theses of representation in the semantic web. *Proceedings of the 12th International Conference on World Wide Web, WWW '03*, New York, NY, USA, ACM Press.

[10] Horrocks, I., B. Parsia, P. Patel-Schneider, et al. (2005). "Semantic Web Architecture: Stack or Two Towers?" *Lecture Notes in Computer Science: Principles and Practice of Semantic Web Reasoning: Third International Workshop.*

[11] Golbeck, J. and P. Mika. (2008). "Semantic Web Challenge." Retrieved June, 2008, from http://challenge.semanticweb.org/.

[12] Revyu.com (2007). "What is Revyu.com?" Retrieved November, 2007, from http://revyu.com/.

[13] CHIP. (2007). "Cultural Heritage Information Presentation." Retrieved November, 2007, from www.chip-project.org.

[14] Finin, T. and A. Joshi (2002). "Agents, Trust, and Information Access on the Semantic Web." *SIGMOD Record* 31(4): 30-35.

[15] Farkas, C. and M. N. Huhns (2002). "Making Agents Secure on the Semantic Web." *IEEE Internet Computing*: 76-79.

[16] Thuraisingham, B. (2003). "Security Issues for the Semantic Web." *27th Annual International Computer Software and Applications Conference, COMPSAC'03*, IEEE Computer Society.

[17] Ashri, R., T. Payne, D. Marvin, et al. (2004). "Towards a Semantic Web Security Infrastructure." *AAAI Spring Symposium on Semantic Web Services.*

[18] Denker, G., L. Kagal, T. Finin, et al. (2003). "Security for DAML Web Services: Annotation and Matchmaking." *2nd International Semantic Web Conference, ISWC'03*, Springer-Verlag.

[19] Gerber, A., A. Barnard and A. Van der Merwe (2006). "A Semantic Web Status Model." *Ninth World Conference on Integrated Design & Process Technology*, San Diego, California, IEEE.

[20] Kagal, L., T. Finin and A. Joshi (2003). "A Policy-Based Approach to Security for the Semantic Web." *2nd International Semantic Web Conference*. ISWC'03, Springer-Verlag

[21] Qin, L. and V. Atluri (2003). "Concept-Level Access Control for the Semantic Web." *ACM Workshop on XML Security*, Fairfax, VA, USA, ACM.

[22] Tan, J. J. and S. Poslad (2004). "A Profile Based Security Model for the Semantic Web." *ECOWS'04*, Berlin, Germany, Springer-Verlag.

[23] Carminati, B., E. Ferrari and B. Thuraisingham (2004). "Using RDF for policy specification and enforcement." *15th International Workshop on Database and Expert Systems Applications*, Los Alamitos, CA, USA, IEEE Computer Society.

[24] ISO7498-2 (1988). Security Architecture, International Standard Organisation.

[25] Uszok, A., J. M. Bradshaw, M. Johnson, et al. (2004). "KAoS Policy Management for Semantic Web Services." *IEEE Intelligent Systems*: 32-41.

[26] Yague, M. I., A. Mana, J. Lopez, et al. (2003). "Applying the Semantic Web Layers to Access Control." *14th International Workshop on Database and Expert Systems Applications* (DEXA'03).

[27] Toninelli, A., R. Montanari, L. Kagal, et al. (2006). "A Semantic Context-Aware Access Control Framework for Secure Collaborations in Pervasive Computing Environments." *5th International Semantic Web Conference*, ISWC 2006, Berlin, Germany, Springer-Verlag.

[28] Pfleeger, C. P. and S. L. Pfleeger (2003). *Security in Computing.* Upper Saddle River, NJ, Prentice Hall.