Universal Journal of Computer Science and Engineering Technology
1 (2), 99-104, Nov. 2010.

Making secure Semantic Web

Adis Medić
Infosys ltd, Bos. Krupa
Bihać, Bosnia and Herzegovina
adismedic@hotmail.com

Adis Golubović
Primary School "Podzvizd", Podzvizd
Velika Kladuša, Bosnia and Herzegovina
golub_a@hotmail.com

***Abstract* – this paper first describes ways of semantic web security implementation through layers. These layers are presented as a backbone for semantic web architecture and are represented in XML security, RDF security and in an idea of semantic web security standardization.**

Keywords – ontology; XML Schema; RDF Schema; OWL; Proof; Trust;

I. INTRODUCTION

One of the most prized assets in today's world course information. Information, as the foundation of web today, usually appears on the form of documents or data. Name of the document can be any information suitable for use by people (articles, reports, texts, pictures etc.). Data on the web can be considered as calendars, address books, databases and similar instances that can be searched, browsed and combined in various ways. Although today's Internet is a vast information resource, its lack of structure and metadata makes it difficult to extract desired information in a reasonable time. The advent of the World Wide Web (WWW) has resulted in even greater demand for managing data, information and knowledge effectively. There is now so much data on the web that managing it with conventional tools is becoming almost impossible. New tools and techniques are needed to effectively manage this data. Therefore, to provide interoperability as well as warehousing between the multiple data sources and systems, and to extract information from the databases and warehouses on the web, various tools are being developed. Consequently the web is evolving into what is nowcalled the semantic web. The semantic web [1] is a vision of an Internet in which web resources are enriched with machine-processable metadata that describes their meaning. This will enable computers to interpret and extract web content much more effectively and precisely than today's XML-based approaches to allow interoperability. In the semantic web, a web resource's metadata makes it possible to evaluate its appropriateness for a given query, which in turn will lead to greater efficiency of web resource allocation, despite the daily expansion of web space. As in [11], we can see that is provided an overview of some directions in data and applications security research. In this paper, we focus on one of the topics and that is securing the semantic web. While the current web technologies facilitate the integration of information from a syntactic point of view, there is still a lot to be done to integrate the semantics of various systems and applications. That is, current web technologies depend a lot on the human-in-the-loop for information integration. Tim Berners Lee, the father of WWW, realized the inadequacies of current web technologies and subsequently strived to make the web more intelligent. His goal was to have a web that will essentially alleviate humans from the burden of having to integrate disparate information sources as well as to carry out extensive searches. He then came to the conclusion that one needs machine understandable web pages and the use of ontologies for information integration. This resulted in the notion of the semantic web [1].

A semantic web can be thought as a web that is highly intelligent and sophisticated and one needs little or no human intervention to carry out tasks such as scheduling appointments, coordinating activities or nearby devices, searching for complex documents as well as integrating disparate databases and information systems. While much progress has been made toward developing such an intelligent web there is still a lot to be done. For example, technologies such as ontology matching, intelligent agents, trustful information, and markup languages are contributing a lot toward developing the semantic web. Nevertheless one still needs the human to make decisions and take actions.

There have been many developments on the semantic web [12][13]. The World Wide Web Consortium (W3C) has specified several standards for the semantic web [19], organized into different layers (i.e., the semantic web layers cake). These standards include XML and XML Schema for representing the data, RDF and RDF Schema for describing the data by means of vocabularies, and OWL a language for defining and instantiating web Ontologies.

As the web evolves into the semantic web, there are more and more possibilities for security breaches as we introduce new technologies. Therefore, it is critical that security is considered right from the beginning of expansion of the semantic web. For the semantic web to be secure we need to ensure that all of the layers ofthe semantic web are secure. This includes secure XML, secure RDF, secure ontologies, and ensure the secure interoperation of all these technologies.

II. LAYERS FOR THE SEMANTIC WEB

Tim Berners Lee has specified various layers for the semantic web (Figure 1) [1].

Corresponding Author: Adis Medić, Infosys ltd, Bos. Krupa, Bihać, Bosnia and Herzegovina.

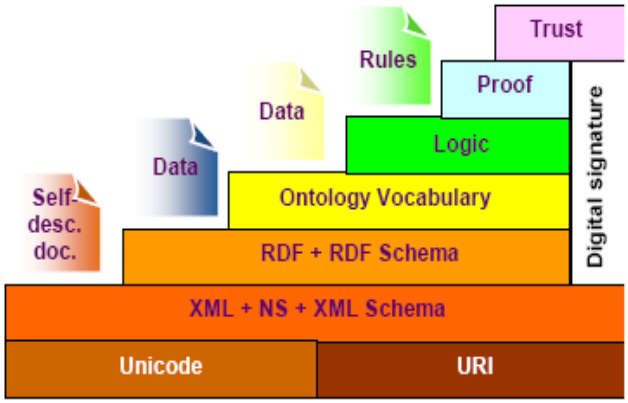

Figure 1. Stack for the semantic web

Layer 1: *URI and Unicode*: Unicode is considered as the universal standard encoding system [21] for computer character representation [22]. Web pages can use a variety of character encoding such as ASCII, Latin-1 or Unicode. Most encoding systems represent only few languages while Unicode represents all languages [23] such as Arabic, English and Chinese. While URI which stands for Uniform Resource Identifier (URI) provides a simple and extensible way for identifying resources. A resource can be anything that has an identity such as a web site, a document, an image and a person [24]. Protocols that exist on this layer are TCP/IP, SSL and HTTP, as the protocols for data transmission. They are built on top of more basic communication layers [32]. With these protocols one can transmit the web pages over the Internet. At this level one does not deal with syntax or the semantics of the documents.

Layer 2: *XML, XML schema and namespaces*: Layer 2 consists of XML, XML Schema and Namespaces. XML is a language used to represent data in a structural way. It describes what is in the document, not what the documents looks like, while XML Schema provides grammars for legal XML documents [5]. On the other hand, Namespaces allows the combination of different vocabularies. For example, if a document is not marked-up, and then each machine may display the documentin its own way. This makes document exchange extremely difficult. XML is a markup language that follows certain rules and if all documents are marked-up using XML then there is uniform representation and presentation of documents. This is one of the significant developments of the WWW. Without some form of common representation of documents, it is impossible to have any sort of meaningful communication on the web. XML schemas essentially describe the structure of the XML documents. Both XML and XML schemas are the invention of Tim Berners Lee and the W3C [3].

Layer 3: *RDF and RDF schema*: Layer 3 consists of the Resource Description Framework (RDF) and the Resource Description Framework Schema (RDF Schema). RDF is a way for representing, exchanging and reusing of metadata [28][29]. RDF uses URIs to identify web resources and uses a graph model for the purpose of describing the relationship between different resources [22]. RDF Schema is a simple modeling language introducing classes of resources, properties and relations between them [22]. In fact, XML focuses only on the syntax of the document. A document could have different interpretations at different sites. This is a major issue for integrating information seamlessly across the web. In order to overcome this significant limitation, W3C started discussions on a language called RDF in the late 1990s. RDF essentially uses XML syntax but has support to express semantics. One needs to use RDF for integrating and exchanging information in a meaningful way on the web. While XML has received widespread acceptance, RDF is only now beginning to get acceptance. So while XML documents are exchanged over protocols such as TCP/IP, HTTP and SSL, RDF documents are built using XML.

Layer 4: *Ontology vocabulary*: Ontology is considered the backbone for the semantic web architecture provides a machine-processable semantics and a sharable domain which can facilitate communication between people and different applications. Next layer is the Ontologies and Interoperability layer. Now RDF is only a specification language for expressing syntax and semantics. The question is what entities do we need to specify? How can the community accept common definitions? To solve this issue, various communities such as the medical community, financial community, defense community, and even the entertainment community have come up with what are called Ontologies. One could use Ontologies to describe the various car models of the world or the different types of aircraft used by the Military. Ontologies can also be used to specify various diseases or financial entities. Once a community has developed ontologies, the community has to publish these ontologies on the web. The idea is that for anyone interested in the ontologies developed by a community to use those ontologies. Now, within a community there could be different factions and each faction could come up with its own ontologies.

Layer 5: *Logic*: There is no specific definition for the Logic layer in the semantic web, not only the Logic layer, but for Trust and Proof layers. There are attempts to reach to their full meaning, status and functions of these layers, because Tim Berners Lee propositions and presentations did not describe these layers in details. The Logic layer is placed above the ontology layer. It is supposed that information will be extracted from the web according to this logic.

Layer 6: *Proof*: Proof is the layer placed above the Logic layer. It is assumed to be a language used in a manner that describes for agents why they should believe the results. This will be a useful semantic web service.

Layer 7: *Trust*: A lot of efforts have been exerted to reach the trusted web, but this is very complicated and difficult task and has not become a reality. Trust has many meanings in the semantic web. Trust is the final layer in the semantic web architecture. It depends on the source of information as well as the policies available on the information source which can

prevent unwanted applications or user from access to these sources. For example, who is allowed to see my medical records? Can my doctor see this information [30]? It depends on the policies available on the information source and the doctor privilege. Web of trust can be found if each user trusts a small number of other users [31]. Confidence will come from the trust between parities [27].

The vertical layer: *Digital signature*: Digital Signature is the only vertical layer in the semantic web architecture. It begins from layer 3 and ends at layer 6. Digital Signature is a step towards a web of trust. By using of XML digital signature, any digital information can be signed [26]. There are specific elements in XML syntax used for this process such as Signed Info, Reference and Digest Value [25]. The final layer is logic, proof and trust. The idea here is how do you trust the information on the web? Obviously it depends on whom it comes from. How do you carry out trust negotiation? That is, interested parties have to communicate with each other and determine how to trust each other and how to trust the information obtained on the web. Closely related to trust issues is security and will be discussed later on. Logic-based approaches and proof theories are being examined for enforcing trust on the semantic web. Note that the layers as evolving as progress is made on the semantic web. For example, more recently a layer in query and rules has been included to support query and rule processing capability. Therefore for more up-to-date information we refer to the work of W3C [20].

III. SECURITY IN SEMANTIC WEB

A. In short about semantic web security

We first provide an overview of security issues for the semantic web and then discuss some details on XML security, RDF security and secure information integration, which are components of the secure semantic web. As more progress is made on investigating these various issues, we hope that appropriate standards would be developed for securing the semantic web. As stated earlier, logic, proof and trust are at the highest layers of the semantic web. That is, how can we trust the information that the web gives us? Closely related to trust is security. However security cannot be considered in isolation. That is, there is no one layer that should focus on security. Security cuts across all layers and this is a challenge. That is, we need security for each of the layers and we must also ensure secure interoperability as illustrated in Table I.

TABLE I. SECURITY LAYERS FOR THE SEMANTIC WEB

Layer 5	Logic, Proof, Trust
Layer 4	Secure Ontologies
Layer 3	RDF Security
Layer 2	XML Security (Secure XML Schemas)
Layer 1	Secure TCP/IP, HTTPS, Secure Sockets

For example, consider the lowest layer. One needs secure TCP/IP, secure sockets, and secure HTTP. There are now security protocols for these various lower layer protocols. One needs end-to-end security. That is, one cannot just have secure TCP/IP built on untrusted communication layers [32]. That is, we need network security. Next layer is XML and XML schemas. One needs secure XML. That is, access must be controlled to various portions of the document for reading, browsing and modifications. There is research on securing XML and XML schemas. The next step is securing RDF. Now with RDF not only do we need secure XML, we also need security for the interpretations and semantics. For example under certain context, portions of the document may be Unclassified while under certain other context the document may be Classified. As an example one could declassify an RDF document, once the war is over. Lot of work has been carried out on security constraints processing for relational databases. One needs to determine whether these results could be applied for the semantic web [7].

Once XML and RDF have been secured the next step is to examine security for ontologies and interoperation. That is, ontologies may have security levels attached to them. Certain parts of the ontologies could be Secret while certain other parts may be Unclassified. The challenge is how does one use these ontologies for secure information integration? Researchers have done some work on the secure interoperability of databases. We need to revisit this research and then determine what else needs to be done so that the information on the web can be managed, integrated and exchanged securely. Closely related to security is privacy. That is, certain portions of the document may be private while certain other portions may be public or semi-private. Privacy has received a lot of attention recently partly due to national security concerns. Privacy for the semantic web may be a critical issue, That is, how does one take advantage of the semantic web and still maintain privacy and sometimes anonymity. Note that W3C is actively examining privacy issues and a good starting point is P3P (Platform for Privacy Preferences) standards, P3P 1.0 Specification [15].

We also need to examine the inference problem for the semantic web. Inference is the process of posing queries and deducing new information. It becomes a problem when the deduced information is something the user is unauthorized to know. With the semantic web, and especially with data mining tools, one can make all kinds of inferences.

That is the semantic web exacerbates the inference problem [9]. Recently there has been some research on controlling unauthorized inferences on the semantic web. We need to continue with such research [1]. Security should not be an afterthought. We have often heard that one needs to insert security into the system right from the beginning. Similarly security cannot be an afterthought for the semantic web [14]. However, we cannot also make the system inefficient if we must guarantee one hundred percent security at all times. What is needed is a flexible security policy. During some situations we may need one hundred percent security while during some

other situations say 30% security (whatever that means) may be sufficient.

B. Security in XML

Various research efforts have been reported on XML security [16]. We briefly discuss some of the key points. XML documents have graph structures. The main challenge is whether to give access to entire XML documents or parts of the documents. Bertino et al. [10] have developed authorization models for XML. They have focused on access control policies as well as on dissemination policies. They also considered push and pull architectures. They specified the policies in XML. The policy specification contains information about which users can access which portions of the documents. As in reference [14] is stated algorithms for access control as well as computing views of the results are also presented. In addition, architectures for securing XML documents are also discussed. Bertino et al. [10] go further and describe how XML documents may be published on the web. The idea is for owners to publish documents, subjects to request access to the documents and untrusted publishers to give the subjects the views of the documents they are authorized to see. W3C (World Wide Web Consortium) is also specifying standards for XML security. The XML security project [16] is focusing on providing the implementation of security standards for XML. The focus is on XML-Signature Syntax and Processing, XML-Encryption Syntax and Processing and XML Key Management. W3C also has a number of working groups including XML-Signature working group [17] and XML-Encryption working group [18]. While the standards are focusing on what can be implemented in the near term lot of research is needed on securing XML documents.

C. Security in RDF

RDF is the foundations of the semantic web. While XML is limited in providing machine understandable documents, RDF handles this limitation. As a result, RDF provides better support for interoperability as well as searching and cataloging. It also describes contents of documents as well as relationships between various entities in the document. While XML provides syntax and notations, RDF supplements this by providing semantic information in a standardized way.

The basic RDF model has three types: they are resources, properties and statements. Resource is anything described by RDF expressions. It could be a web page or a collection of pages. Property is a specific attribute used to describe a resource. RDF statements are resources together with a named property plus the value of the property. Statement components are subject, predicate and object. There are RDF diagrams very much like say ER-diagrams or object diagrams to represent statements. There are various aspects specific to RDF syntax and for more details we refer to the various documentson RDF published by W3C. Also, it is very important that the intended interpretation be used for RDF sentences. This is accomplished by RDF schemas. Schema is sort of a dictionary and has interpretations of various terms used in sentences. RDF- and XML-namespaces resolve conflicts in semantics. More advanced concepts in RDF include the container model and statements about statements. The container model has three types of container objects and they are Bag, Sequence, and Alternative. A bag is an unordered list of resources or literals. It is used to mean that a property has multiple values but the order is not important. A sequence is a list of ordered resources. Here, the order is important. Alternative is a list of resources that represent alternatives for the value of a property. Various tutorials in RDF describe the syntax of containers in more detail. RDF also provides support for making statements about other statements. Again one can use object-like diagrams to represent containers and statements about statements. RDF also has a formal model associated with it. This formal model has a formal grammar. As in the case of any language or model, RDF will continue to evolve. Now to make the semantic web secure, we need to ensure that RDF documents are secure. This would involve securing XML from a syntactic point of view. However with RDF we also need to ensure that security is preserved at the semantic level. The issues include the security implications of the concepts resource, properties and statements. There are many difficult questions and we need to start research to provide answers. XML security is just the beginning. Securing RDF is much more challenging.

D. Standardization of semantic web security

Web resources and services need to be protected from unauthorized access and software agents want to be ensured about the privacy of data they disclose to services. Thus, a broad range of security-related notions, such as authentication, authorization, access control, confidentiality, data integrity, and privacy are relevant for semantic web technology. Currently, low-level encryption, digital signature mechanisms, certification, and public key infrastructures provide a good security infrastructure for web-based interactions. However, providing higher-level security, especially without prior trust relations in dynamic interactions, relies on a variety of ad hoc mechanisms. This heterogeneity of mechanisms leaves security holes with deleterious effects. The proposed industrial standards on security assume a well-established web of trust among business-to-business (B2B) partners. For example, there exists a significant body of standardization efforts for security of XML-based web services, such as WS-Security [4], -Trust [6], and -Policy [8] at W3C, or SAML of the OASIS Security Services Technical Committee, and the Security Specifications of the Liberty Alliance Project. WS-Security provides a layer of security over SOAP, which is an XML-based protocol for exchanging information primarily used for web services. WS-Security describes how to attach signature and encryption headers or security tokens to SOAP messages.

The standards support low-level security or policy markups that concern formats of credentials or supported character sets for encoding. They do not address semantic user- or application-specific trust tokens and their relations, nor do they allow for expressive policies. The standards deliver to the needs of B2B applications where trusted partners and business

relationships have already been established in advance of operation and transactions. However, in a world where more and more public and private services are becoming available online and the vision of cyber-societies is becoming reality, assumptions about pre-established trust relationships do not hold true. The standards are not extensible to more dynamic environments in which simple authentication is not enough, but authentication on user-defined attributes needs to be considered as „foreign" or unknown entities will interoperate with each other across heterogeneous domains and applications using delegation mechanisms.

E. Other viewpoint to semantic web Security

Trust is, usually, the last but not the least thing for people to concern when they build a system. So, why we worry about trust issue at this moment? Especially when the trust layer was declared as the top of layer on the semantic web layer cake. If we agree that proof and trust are applications rather than a new ontology language on the layer stack, then it will not hurt to explore the trust issues at current stage [5]. There are several important results on agent trust based on psychology and security viewpoints [33][34][35][36]. Trust and risk are complementary terms in social relations. An emphasis on risk is generally based on mistrust, whereas trust is associated with less doubts about security. Those who trust others do not look for high security before they act. Trust (or security) is also one of the important issues for web service and grid computing in the semantic web pyramid [37][38].

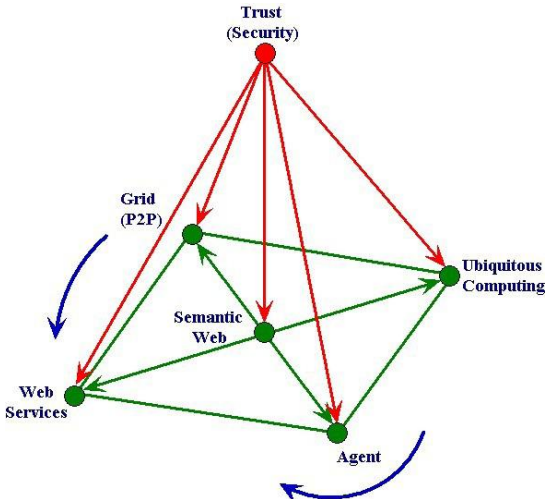

Figure 2. Basis for secure/trustful information [41]

When we compare with other emerging technologies, the research progress for the trusted semantic web is very slow and the results are scarce [39][40]. Trusted semantic web was defined as well-defined trust ontologies and trust rules in the agent interaction protocols so that agent's access control services, such as authentication, authorization, and delegation can be achieved. This approach not only solves the agent's authenticity and authority problems but also provides the possible capacity to resolve information propagation authenticity, ontology and rule integrity issues in the future. In the trust traversing path, *d, b, c* (Figure 2), the Ontology and rule techniques will be leveraged on agent trust control. In another trust traversing path, *e, b, a*, agent technology will be leveraged on the building and verifying of authenticity and integrity of ontology and rule.

IV. CONCLUSIONS AND FURTHER WORK

This paper has provided an overview of the semantic web and discussed security standards. We first discussed the layered framework of the semantic web proposed by Tim Berners Lee. Next we discussed security issues. We discuss that security must cut across all the layers. Furthermore, we need to integrate the information across the layers securely. Next we provided some more details on XML-Security, RDF-Security, secure information integration and trust.

If the semantic web is to be secure we need all of its components to be secure. We also described some of our research on access control and dissemination of XML documents. Finally, we discussed privacy for the semantic web. There is a lot of research that needs to be done. We need to continue with the research on XML-Security. We must start examining security for RDF. This is much more difficult as RDF incorporates semantics. We need to examine the work on security constraint processing and context dependent security constraints and see if we can apply some of the ideas for RDF-Security. Finally, we need to examine the role of ontologies for secure information integration. Standards play an important role in the development of the semantic web. W3C has been very effective in specifying standards for XML, RDF and the semantic web. We need to continue with the developments and try as much as possible to transfer the research to the standards efforts. We also need to transfer the research and standards to commercial products. The next step for the semantic web standards efforts is to examine security, privacy, quality of service, integrity, proof of information, trust and other features such as multimedia processing and query services. As we have stressed security and privacy are critical and must be investigated while the standards are being developed.

Information assurance, security, and privacy have moved from narrow topics of interest to information system designers to become critical issues of fundamental importance to society. As such, they also play an important rule in web-based applications and newer technology such as semantic web applications. These applications need the capability for agents, devices, and services to seamlessly interact while preserving appropriate security, privacy and trust.

Meeting this challenge requires realizing fourhigh-level objectives: (1) to advance the theoryand practice of security, privacy, and trust of webbased interactions by providing technology for trust in the semantic web and trustworthy, semantically annotated web services; (2) to provide declarative policy representation languages, ontologies, and inference algorithms for security, trust and privacy management, enforcement, and negotiation; and (3) to prototype software tools allowing system designers and end users to both specify and verify policies for trust and privacy.

In final words of these paper it must be told that more significant is how obtain a trusted information. And research in „trust area“ in semantic web poses new challenges that can be significant body of work in a way to trust in computer science. But, it is also highly considered that security of information is on a high level and that is proof for well based security model and it is starting point for modeling trust.

REFERENCES

[1] T. Berners Lee, J. Hendler, O. Lassila, The semantic web, Scientific American; May 2001, 34 - 43

[2] E. Bertino, et al., Secure Third Party Publication of XML Documents, to appear in IEEE Transactions on Knowledge and Data Engineering

[3] S. St. Laurent, XML, McGraw Hill, New York, NY, 2000.

[4] B. Atkinson, et al. web services security (WS-Security), http://www-106.ibm.com/developerworks/webservices/library/ws-secure/O; 2002.

[5] D. Fensel, 2002. Layering the semantic web: Problems and Directions. In the Proceeding of 1st International semantic web Conference (ISWC, 2002). Sardinia, Italy, 9-12 June, pp: 476. ISBN: 3540437606, 9783540437604.

[6] G. Della-Libera, et al. web services trust language (WS-Trust). http://www.106.ibm.com/developerworks/library/ws-trust/O, 2003.

[7] B. Thuraisingham,W. Ford, Security constraint processing in a distributed database management system, IEEE Transactions on Knowledge and Data Engineering (1995) 274– 293.

[8] D. Box, et al. web services policy framework (WS-PoIicy), http://www-106.ibm.com/developerworks/library/ws-polfram/O ;

[9] B. Thuraisingham, Data Mining: Technologies, Techniques, Tools and Trends, CRC Press, Boca Raton, FL, 1998.

[10] E. Bertino, et al., Access Control for XML Documents, Data and Knowledge Engineering, North Holland, 2002, pp. 237–260

[11] B. Thuraisingham, bData and applications securityQ developmentsand directions, Proceedings IEEE COMPSAC, 2002.

[12] B. Thuraisingham, XML, Databases and the semantic web, CRC Press, Florida, 2001.

[13] B. Thuraisingham, The semantic web, in: W. Bainbridge (Ed.), Encyclopedia of Human Computer Interaction, Berkshire Publishers, 2003.

[14] B. Thuraisingham, *Secure Sematic web Services*, Technical Report, University of Texas – Department of Computer Science, 2007

[15] L. Cranor, M. Langheinrich, M. Marchiori, M Presler Marshall, J. Reagle, Platform for privacy preferences (P3P); 2002.

[16] http://xml.apache.org/security/.

[17] http://www.w3.org/Signature/.

[18] http://www.w3.org/Encryption/.

[19] www.w3c.org

[20] B.Thuraisingham, Security for the semantic web, Computer Standards and Interfaces 27, 257 – 268, 2005

[21] C. Burleson, 2007. Introduction to the semantic web Vision and Technologies, http://www.semanticfocus.com/blog/entry/title/introduction-to-the-semantic-web-vision-andtechnologies-part-2-foundations

[22] B. Matthews,” semantic web Technologies. JISC Technology and Standards Watch,” 2005. http://www.scribd.com/doc/300024/What-is-web-20-Ideas-technologies-and-implications-Paul-Anderson

[23] M. Davis., 2008. Moving to Unicode 5.1., http://googleblog.blogspot.com/2008/05/movingto-unicode-51.html

[24] T. Berners Lee, 2006. Uniform Resource Identifiers, URI Generic Syntax. IETF. http://www.ietf.org/rfc/rfc2396.txt

[25] T. Haytam, Al-Feel, M. Koutb and H. Suoror, *semantic web on Scope: A New Architectural Model for the semantic web*, Journal of Computer Science 4 (7): 613-624, 2008

[26] R. Cloran and B. Irwin, 2005. XML Digital Signature and RDF, http://icsa.cs.up.ac.za/issa/2005/Proceedings/Poster/026_Article.pdf

[27] B. Matthews and T. Dimitrakos., Deploying Trust Policies on the semantic web, 2004; http://epubs.stfc.ac.uk/bitstream/638/SWADtrust2004.pdf

[28] S. Buraga and G. Ciobanu., 2002. A RDF- based model for expressing spatio-temporal relation between web sites. In The 3rd International Conference on Information Systems Engineering. IEEE Computer Society. pp: 355. IEEE Computer Society Washington, DC, USA., ISBN:0-7695-1766-8

[29] Description Framework”, in D-Lib Magazine, May.1998; http://www.dlib.org/dlib/may98/miller/05miller.html

[30] W. Nejd, D. Olmedillal and M. Winslett, 2004. Peer Trust: Automated Trust Negotiation for Peers on the semantic web. Lecture Notes in Computer Science: Secure Data Management. Springer Berlin/Heidelberg, vol.3178/2004. pp: 118-132. ISBN: 978-3-540-22983- 4.

[31] M. Richardson, R. Agrawal and P. Domingos, *et al*., 2003. Trust management for the semantic web. Lecture Notes Comput. Sci., 2870:351-368. DOI: 10.1007/b14287.

[32] A. Medić, Criptography – Securing web Servers and web Applications, University of Bihać, Technical Faculty Bihać, engineer thesis, Bihać, Bosnia and Herzegovina, February 2008

[33] C. Castelfranchi and R. Falcone, Trust and Control: A Dialectic Link. Applied Artificial Intelligence, 14 (2000), 799-823

[34] Q. He, K. Sycara and T. Finin., Personal Security Agent: KQML-Based PKI. Proceedings of the Second International Conference on Autonomous Agents, (1998).

[35] Hu, Y.-J., Some Thoughts on Agent Trust and Delegation. *The Fifth International Conference on Autonomous Agents*, Montreal, Canada, May 28 - June 1, (2001), 489-496.

[36] H. C. Wong and K. Sycara, Adding Security and Trust to Multi-Agent Systems. *Proceedings of Autonomous Agents '99 (Workshop on Deception, Fraud and Trust in Agent Societies)*, Seattle, Washington, (1999), 149-161

[37] Security in a web Services World: A Proposed Architecture and Roadmap. A joint security white paper from IBM Corp. and Microsoft Corp., Version 1.0, April 7 2002. http://www-106.ibm.com/developworks/library/ws-secmap

[38] N. Nagaratnam et al., The Security Architecture for Open Grid Services. Ver. 1, July 17 2002, http://www.globus.org/ogsa/Security/

[39] G. Jennifer, J. Hendler, and B. Parsia, Trust Networks on the semantic web. *World Wide web Conference*, Budapest, Hungary, May 20-26 2003.

[40] Y. Gil and V. Ratnakar, Trusting Information Sources One Citizen at a Time. *The semantic web - ISWC 2002*, (2002), 162-176

[41] H. Yuh Jong, A Pyramid for the semantic web: Some Issues and Challenges, March 14 2003, http://www.cs.nccu.edu.tw/~jong/TPyramid/TPyramid.html