Generating a Standardized Upper Ontology for Security of Information and Networks

Atilla Elçi

Abstract A usable functional interface between ontology and security integrating related information is needed for security engineering as well as creating secure systems. That in turn necessitates ontologizing security of information and networks to start with and then standardization. Having involved in the fields of semantic technology and information assurance, I have strived to facilitate establishing an interface between them and for this reason SIN Conference Series I created included all interest areas of semantics, metadata and ontology aspects. In a keynote talk and its proceedings paper in SIN 2014, I took up this subject and drove to the point that generic ontology for security of information and networks is timely, and it should better be standardized. In the present paper I investigate through examples where available to drive the point that the standard upper ontology for security may be developed through community sourcing and then standardized through competent agencies.

Keywords Information security · Semantic · Ontology · Secure ontology · Standards

1 Introduction

Realization of security-critical systems involves quality security engineering from analysis to design to development as well as implementation, testing, deployment and maintenance. Sphere of interest is quite large expanding to computers, network, internet and cloud, confidentiality, integrity, availability of data and applications, information flow, access control, privacy, trust, algorithms and protocols, cryptology and so on. The body of knowledge involved is beyond grasp of any individual,

A. Elçi (✉)
Department of Electrical and Electronics Engineering,
Aksaray University, Aksaray 68100, Turkey
e-mail: aelci@acm.org

M. Senthilkumar et al. (eds.), *Computational Intelligence, Cyber Security and Computational Models*, Advances in Intelligent Systems and Computing 412, DOI 10.1007/978-981-10-0251-9_4

extremely detailed and highly parametric, and certainly very complex to keep current in all aspects even for experts. It is thought that semantic technology with existing theory, standardized languages and associated practical tools together with properly configured domain ontologies can provide highly appreciable services in alleviating associated issues. In order to realize such synergy, a functional interface integrating related information between ontology and security is imperative which in turn necessitates ontologizing the domain of security of information and networks. Eventually such ontologies would be standardized.

Having worked in the fields of semantic technology and information assurance, I have strived to facilitate establishing an interface between security and ontology and for this reason SIN Conference Series [1] I created included all pertinent research interest areas of security, semantics, metadata and ontology aspects. In a keynote talk and in the associated paper in the proceedings of SIN 2014, I took up this subject [2]. The contents of that paper was such that the wide span of the interest area was highlighted in a long list of specialized research topics initially, then surveyed the few studies on ontologizing security related works, and standards on security and ontologies. It was shown that although numerous standards existed on either but there were none on the joint topic of information security ontology. It was highlighted that a generic ontology for security of information and networks is needed, earlier the better. Furthermore, it was concluded that a dire need existed for standardization of high-level information security ontology, perhaps an upper ontology for all others to link up to so that a forest of linked ontologies allowing all concerned to link their big data can evolve in time.

In this paper I inquire into how to realize an upper ontology for security domain and eventually standardize it. Next section introduces a vision to develop the security upper ontology. Standardization issue is taken up in section three and conclusions follow in section four.

2 Generating Security Ontology

As reviewed in [2], few studies exist in relation to ontologizing security and standardization. All, inclusive of those by this author, are minor and isolated initiatives studying certain aspects of ontology and security. At the World Wide Web Consortium (W3C), respected standardization body for Web matters, there has been little work with respect to information security ontology; and, hardly any results exist in producing standardized security ontology [3].

The Security Activity at W3C is organized through its subgroups variously named as Web Security Interest, Web Cryptography Working, Web Application Security, Privacy Interest, Technical Architecture Group (TAG), Web Payments Interest and XML Security Working Group. These groups provide a facilitating forum for discussions on how to improve standards, related implementations and extending existing standards in order to further Web security. The WebCrypto group has announced a draft Web Cryptography API [4] featuring message

confidentiality and authentication services as building blocks for improved Web security. The Web Application Security Group "aims to enable secure mash-ups, address click-jacking, and to create a more robust Web security environment through light-weight policy expression that meshes with HTML5's built-in security policies." The XML Security Working Group, XMLSec for short [5], has already produced three W3C Recommendations on XML signature, encryption and signature properties. While TAG is "responsible for the security, sanity, and layering of the overall web platform", Web Security Interest, Privacy Interest and Web Payments Interest Groups appear as advisory.

It is to be concluded that the W3C Security Activity has so far been concerned with instigating secure versions of existing Web standards and applications through extensions. This modus operandi has been the norm for quite some time now in the industry as there have been isolated research studies on aspects of ontology and security. For example as early as 2002, Jürgens [6] proposed extending UML to UMLsec for integrating security related information in UML diagram specifications in the form of UML profiles. Such information provided through standard UML extension mechanism can then be used for model-based security engineering and verification through formal semantics of UML. As would be known, UML is fairly high up in the spectrum of ontology formalism above concept model, RDF/S but just below OWL (see: Fig. 7.5: The ontology spectrum: Weak to strong semantics in [7, 10]). Similarly, Fatemi et al. [8] took up securing ontologies to protect company private information. This work proposed creating a secure flavor of OWL in order to remedy this issue through one of two approaches. In the first, a Secure Web Ontology Language (SOWL) is proposed with extensions that may be non-compliant to OWL Recommendation thus requiring a new version of OWL. In the next, a scheme called OWL + S is proposed whereby OWL is enhanced by implicit attachment of security ontology. Considering the extent and maturity of OWL recommendations, it would not be reasonable to propose extensions requiring modification of its syntax. Doubtless there could be other similar attempts at investigating security of semantic systems, for example references in [9].

In the end, rather than modifying well-established and in-widespread-use existing ontology languages unreasonably, it would be advisable to leave them intact but to develop security ontologies. In that, rather than attempting isolated individual domain ontologies for subareas of security field, it would be pertinent to go for an upper level ontology for all the expanse of information security. (Here again, by information security I mean to cover information technology and information assurance including as well as all associated flavors.) Upper-level ontology, sometimes called variously as top level as well, normally includes domain concepts as generic common knowledge broad and abstract terms and relations in a hierarchical and networked structure. The Suggested Upper Merged Ontology (SUMO), the Descriptive Ontology for Linguistic and Cognitive Engineering (DOLCE), PROTON, UMBEL, Cyc and Basic Formal Ontology (BFO) are examples of upper-level ontology [10]. Upper level ontology is abstract or conceptual; it is meant to alleviate integration of middle-level operational and low-level data base schema ontologies developed by disparate individuals.

Consensus building nature of upper ontology is to be kept in view while attempting to develop one. All stake-holders, those with an interest in using it, should be involved. The crowdsourcing modus operandi suits well. "Crowdsourcing" is defined as the "practice of obtaining needed services, ideas, or content by soliciting contributions from a large group of people and especially from the online community rather than from traditional employees or suppliers" by Merriam-Webster Dictionary [11]. "By definition, crowdsourcing combines the efforts of numerous self-identified volunteers or part-time workers, where each contributor, acting on their own initiative, adds a small contribution that combines with those of others to achieve a greater result [12]". Crowdsourcing should be employed with a twist: considering the specific expertise requirement constricting the likely public audience, the crowd is "the community" composed of concerned, related and professional people of the extended domain. Hence, rather than outsourcing to or commissioning from a specific named group, "community sourcing" and "community curating" leading to collaborative ontology development must be employed. With use of proper tools, such as Collaborative Protegé [13] allowing and managing contributions of multiple contributing editors this scheme is feasible. A recommender system and trust scores among parties would serve here for social harvesting and sourcing up front. At the well advanced stage with reasonably large set of ontology definitions in hand, the touch up then may be affected by a commissioned committee work as it's been done in W3C.

3 Standardizing Security Ontology

International Standards Organization defines a standard as a formal document providing requirements, specifications, guidelines or characteristics of materials, products, processes and services fit for the purpose if used consistently. Standards "ensure that products and services are safe, reliable and of good quality. For business, they are strategic tools that reduce costs by minimizing waste and errors, and increasing productivity. They help companies to access new markets, level the playing field for developing countries and facilitate free and fair global trade" [14]. Standards often elicit compliance. They come in various flavors but in this paper we are interested in "technical standards" or "industry standards" in information security and ontologies domains. A technical standard establishes uniform engineering or technical criteria, methods, processes and practices in reference to technical systems.

Technical standards may be developed unilaterally but their acceptance and enforcement in practice would depend on the pulling power of the entity developed it. A community standard however developed through consensus would carry willing acceptance of its stake-holders thus it becomes a voluntary de facto standard.

Thus we would need a standardization process that secures the formal consensus of the security and ontology communities. Ontolog Community is a good example

of an organization of loosely coupled people of common interests in ontology area. Its weekly virtual working meetings establish a platform to present individual points of views, discussion, consensus building and evolution of resolutions. The case in point is the Ontology-Based Standards Mini Series of virtual meetings [15].

As soon as a reasonably mature draft standard ontology evolves in the process, the product should eventually have to get the consensus of technical experts. Consequently, the development of the standard upper ontology for security would better continue through the joint concerted effort of such standardization organizations operative in the interest area as W3C, IEEE Standards Association, NIST, and ISO. These organizations have practical competence in the processes of standardization. W3C has been active in producing voluntary standards called "recommendation" in Web realm [16]. IEEE SA has produced the Standard Ontologies for Robotics and Automation [17] and for Learning Technology [18].

It is only through such a process of security community harvesting, cooperation and collaboration of field experts, finalization by standardization organizations, standard upper ontology for security will be rendered open, international and authoritative in the field.

4 Conclusions

I will conclude with the same sentence as in [2]: "It should be clear that generic ontology for security of information and networks is needed and that earlier the better." Certainly the outcome will be much more usable if the security ontology gets standardized. Furthermore, for a standardized ontology it is best if it is of high-level, perhaps an information security upper ontology for all others to link up to. Provided all concerned link their big data, this then should come handy in evolving a forest of linked ontologies, eventually helping as well in unifying the terminology.

This paper proposes a social harvesting approach involving community sourcing and volunteer-driven standardization for evolving a standardized upper ontology for security of information and networks.

References

1. International Conference on Security of Information and Networks. www.sinconf.org. Accessed 29 Sept 2015
2. Elci, A.: (Keynote Talk) Isn't the time ripe for a standard ontology on security of information and networks? In: Poet, R., Elci, A., Gaur, M.S., Orgun, M.A., Makarevich, O. (eds.) Proceedings of SIN 2014, the Seventh International Conference on Security of Information and Networks, pp. 1–3 (SIN 2014), 9–11 Sept 2014. Glasgow, UK. Published by ACM, ISBN 978-1-4503-3033-6. doi:10.1145/2659651.2664291 (2014)

3. World Wide Web Consortium. Security Activity. www.w3.org/Security/. Accessed 29 Sept 2015
4. W3C Web Cryptography Working Group. Web Cryptography API. www.w3.org/TR/WebCryptoAPI/. Accessed 29 Sept 2015
5. W3C XML Security Working Group. www.w3.org/2008/xmlsec/. Accessed 29 Sept 2015
6. Jürjens, J.: UMLsec: Extending UML for secure systems development. In: Jezequel, J.-M., Hussmann, H., Cook, S. (eds.) UML 2002—The Unified Modeling Language, pp. 412–425. Dresden, Springer-Verlag. And, for a brief summary of the proposal. https://en.wikipedia.org/wiki/UMLsec (2002)
7. Daconta, M.C., Obrst, L.J., Smith, K.T.: The Semantic Web: A Guide to the Future of XML, Web Services, and Knowledge Management. John Wiley & Sons. ISBN:0471432571 (2003)
8. Fatemi, M.R., Elci, A., Bayram, Z.: A proposal to ontology security standards. In: Proceedings of the 2008 International Conference on Semantic Web and Web Services (SWWS'08), of the 2008 World Congress in Computer Science, Computer Engineering, and Applied Computing (WORLDCOMP'08), pp. 183–186. Las Vegas, USA, July 14–17
9. Sicilia, M.-A., García-Barriocanal, E., Bermejo-Higuera, J., Sánchez-Alonso, S.: What are Information Security Ontologies Useful for? In: Garoufallou, E,. Hartley, E., Richard, J., Gaitanou, P. (eds.) Metadata and Semantics Research, vol. 544, pp. 51–61. Communications in Computer and Information Science, doi:10.1007/978-3-319-24129-6_5. Springer International Publishing. ISBN: 978-3-319-24128-9 (2015)
10. Open Semantic Framework. A Basic Guide to Ontologies. http://wiki.opensemanticframework.org/index.php/A_Basic_Guide_to_Ontologies. Accessed 29 Sept 2015
11. http://www.merriam-webster.com/dictionary/crowdsourcing. Accessed 29 Sept 2015
12. https://en.wikipedia.org/wiki/Crowdsourcing. Accessed 29 Sept 2015
13. Tudorache, T.: Collaborative protege. Available: http://protegewiki.stanford.edu/wiki/CollaborativeProtege. Accessed 29 Sep 2015 (2011)
14. http://www.iso.org/iso/home/standards.htm
15. Ontolog Community. Ontology-based standards. http://ontolog.cim3.net/cgi-bin/wiki.pl?ConferenceCall_2013_11_07. Accessed 29 Sept 2015
16. http://www.w3.org/standards/. Accessed 29 Sept 2015
17. IEEE SA—1872-2015—IEEE Standard Ontologies for Robotics and Automation. http://standards.ieee.org/findstds/standard/1872-2015.html. Accessed 29 Sept 2015
18. IEEE Standard for Learning Technology. http://standards.ieee.org/findstds/standard/1484.13.1-2012.html. Accessed 29 Sept 2015