Towards the Definition of an Ontology for Trust in (Web) Data

Davide Ceolin, Archana Nottamkandath,

Wan Fokkink, and Valentina Maccatrozzo

VU University, Amsterdam, The Netherlands
{d.ceolin,a.nottamkandath,w.j.fokkink,v.maccatrozzo}@vu.nl

Abstract. This paper introduces an ontology for representing trust that extends existing ones by integrating them with recent trust theories. Then, we propose an extension of such an ontology, tailored for representing trust assessments of data, and we outline its specificity and its relevance.

Keywords: Trust, Ontology, Web Data, Resource Definition Framework (RDF)

1 Introduction

In this paper we tackle the problem of modeling and representing trust assertions, in particular about (Web) data. This is an important issue for a variety of reasons. First, trust is an important aspect both of everyday life and of many computational approaches, for similar reasons. In fact, trust is a "leap of faith"[1] that is necessary to be taken whenever we need to rely on third party agents or information. We decide whether or not to take this leap of faith based on the evaluation of the trustworthiness of the agent or information. In general, when trusting, a risk is involved, i.e., the risk of relying on uncertain and possibly unpredictable actions or information. We can soften such a risk, and one way to achieve this result is to share trust and trustworthiness values, along with their provenance, to allow their reuse and increase the probability to correctly place trust thanks to the availability of this information. Therefore, an ontology for trust assessments, in particular of Web data, can indicate the basic elements that are necessary to define a trust value.

This paper aims at introducing an ontology for trust representation, starting from existing ones and extending them to cover aspects indicated by recent trust theories. In Section 2 we present related work, in Section 3 we provide a summary of the trust theory of O'Hara that we use in the rest of the paper, in Section 4 we propose an extended ontology for representing trust and in Section 5 we expose our vision about the issues of trusting (Web) data. Lastly, we conclude in Section 6.

[1] Stephen Marsh, "Trust: Really, Really Trust", IFIP Trust Management Conference 2014 Tutorial

2 Related Work

Trust is a widely explored topic within a variety of computer science areas. Here, we focus on those works directly touching upon the intersection of trust, reputation and the Web. We refer the reader to the work of Sabater and Sierra [19], Artz and Gil [2], and Golbeck [12] for comprehensive reviews about trust in artificial intelligence, Semantic Web and Web respectively. Trust has also been widely addressed in the agent systems community. Pinyol and Sabater-Mir provide an up-to-date review of the literature in this area [18].

We extend the ontology proposed by Alnemr et al. [1]. We choose it because: (1) it focuses on the computational part of trust, rather than on social and agent aspects that are marginal to our scope, and (2) it already presents elements that are useful to represent computational trust elements. Nevertheless, we propose to extend it to cover at least the main elements of the trust theory of O'Hara, that are missing from their original ontology, and we highlight how these extensions can be beneficial to model trust in (Web) data. Viljanen [21] envisions the possibility to define an ontology for trust, but puts a particular emphasis on trust between people or agents. Heath and Motta [14] propose an ontology for representing expertise, thus allowing us to represent an important aspect of trust, but again posing more focus on the agents rather than on the data. A different point of view is taken by Sherchan et al. [20], who propose an ontology for modeling trust in services.

Goldbeck at al. [13], Cesare et al. [5] and Huang et al. [15] propose ontologies for modeling trust in agents. Although these could be combined with the ontology we propose (e.g., to model the trust in the author of a piece of data), for the moment their focus falls outside of the scope of our work, that is trust in data.

Trust has been modeled also in previous works of ours [7,6,8,9] using generic models (e.g., the Open Annotation Model [4] or the RDF Data Cube Vocabulary [10]). Here we aim at providing a specific model for representing trust.

3 A Definition of Trust in Short

We recall here the main elements of "A Definition of Trust" by O'Hara [17], that provide the elements of trust we use to extend the ontology of Alnemr et al.

Tw<Y,Z,R(A),C> (Trustworthiness) agent Y is willing, able and motivated to behave in such a way as to conform to behaviour R, to the benefit of members of audience A, in context C, as claimed by agent Z.

Tr<X,Y,Z,I(R(A),c),Deg,Warr> (Trust attitude) X believes, with confidence Deg on the basis of warrant Warr, that Y's intentions, capacities and motivations conform to I(R[A],c), which X also believes is entailed by R(A), a claim about how Y will pursue the interests of members of A, made about Y by a suitably authorised Z.

X places trust in Y (Trust Action) X performs some action which introduces a vulnerability for X, and which is inexplicable without the truth of **Trust attitude**.

4 Extending a Trust Ontology

We are interested in enabling the sharing of the trust values regarding both trust attitude and actions, along with their provenance. The ontology proposed by Alnemr et al. [1] captures the basic computational aspects of these trust values. However we believe that it lacks some peculiar trust elements that are present in the theory of O'Hara, and thus we extend that ontology as shown in Figure 1[2]. Compared with the ontology of Alnemr et al., we provide some important additions. We clearly identify the parts involved in the trust relation:

Trustor (source): every trust assessment is made by an agent (human or not), that takes his decision based on his policy and on the evidence at his disposal;

Trustee (target): the agent or piece of information that is actually being trusted or not trusted. This class replaces the generic "Entity" class, as it emphasizes its role in the trust relation.

We also distinguish between the attitude and the act of trusting.

Trust Attitude Object: it represents the graded belief held by the trustor in the trustworthiness of the trustee and it is treated as a quality attribute when deciding if to place trust in the trustee or not. It replaces the reputation object defined by Alnemr et al. because it has a similar function to it (quantifying the trust in something), but implements the trust attitude relation defined by O'Hara that is more precise and complete (e.g. warranties are not explicitly modeled by the reputation object);

Trust Action Object: the result of the action of placing trust. Placing trust is an instantaneous action based on an "outright" belief. Therefore the trust value is likely to be a Boolean value.

Role, Context and Warranty: in the original ontology, the criterion is a generic class that contextualizes the trust value. We specialize it, to be able to model the role and the context indicated in the theory of O'Hara, as well as the evidence on which the trust value is based, by means of the warranty.

The trustworthiness relation is not explicitly modeled, since it falls outside our current focus. We discuss this further in the following section. The remaining elements of the model shown in Figure 1 are part of the original trust ontology. These include a criterion for the trust value, and an algorithm that allows combining observations (warranties) into a trust value (an algorithm is used also to determine the value of the trust action). The trust attitude value corresponds to the Deg element of the theory of O'Hara. We model the action both when it is performed and when it is not. Both trust values are modeled uniformly.

5 Modeling Trust in Data

In the previous section we provided an extended ontology that aims at capturing the basic elements that are involved in the process of taking trust decisions. Here we focus on the specificity of trusting (Web) data.

[2] The ontology is available at `http://trustingwebdata.org/ontology`

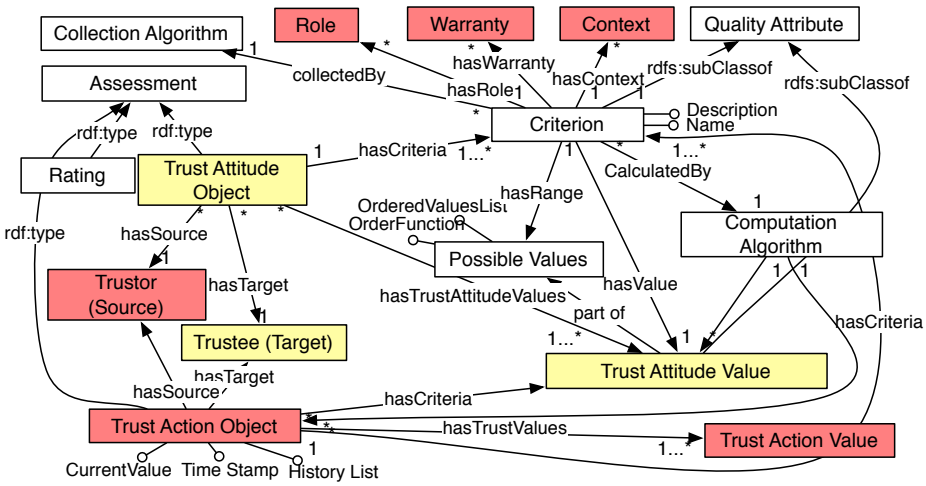

Fig. 1. Extended Trust Ontology. We highlight in red the added elements and in yellow the updated ones.

Data are used as information carriers, so actually trusting data does not mean to place trust in a sequence of symbols. It rather means to place trust in the interpretation of such a sequence of symbols and on the basis of its trustworthiness. For instance, consider a painting reproducing the city "Paris" and its annotation "Paris". To trust the annotation, we must have evidence that the painting actually corresponds to the city Paris. But, to do so, we must: (1) give the right interpretation to the word "Paris" (e.g., there are 26 US cities and towns named "Paris"), and (2) check if one of the possible interpretations is correct. Both in the case the picture represents another city or in the case the picture represents a town named Paris which existence we ignored, we would not place trust in the data, but for completely different reasons. One possible RDF representation of the above example is: `exMuseum:ParisPainting ex:depicts dbpedia:Paris`, where we take for granted the correctness of the subject and of the property and, if we accept the triple, we do so because we believe in the correctness of the object in that context (represented by the subject), and role (represented by the property). We make use of the semantics of RDF 1.1 [22], from which we recall the elements of a simple interpretation I of an RDF graph:

1. A non-empty set IR of resources, called the domain or universe of I.
2. A set IP, called the set of properties of I.
3. A mapping IEXT : IP $\rightarrow \mathcal{P}$ (IR $\times$ IR).
4. A mapping IS: IRIs $\rightarrow$ (IR $\cup$ IP). An IRI (Internationalized Resource Identifier [11]) is a generalization of a URI [3].
5. A partial mapping IL from literals into IR

Also, the following semantic conditions for ground graphs hold:

a. if E is a literal then I(E) = IL(E)
b. if E is an IRI then I(E) = IS(E)
c. if E is a ground triple s p o. then I(E) = true if I(p) ∈ IP and the pair <I(s),I(o)> ∈ IEXT(I(p)) otherwise I(E) = false.
d. if E is a ground RDF graph then I(E) = false if I(E') = false for some triple E' ∈ E, otherwise I(E) = true.

Items 1, 2, 4 and 5 map the URIs, literals and the RDF triples to real-world objects. We are particularly interested in Item 3, that maps the property of an RDF triple to the corresponding real-world relation between subject and object. Trusting a piece of data means to place trust in the information it carries, in a given context. The trust context can be represented by means of the subject and object of an RDF triple, so their semantic interpretation is assumed to be known by the trustor. If the trustor trusts the triple, he believes that the interpretation of the object *o* makes the interpretation of the triple *s p o* true:

$$TrustAttitude_{trustor}(o|s,p) = Belief_{trustor}(\exists I(o) : <\text{I(s)},\text{I(o)}> \in IEXT(I(p))$$

Belief is an operator that maps logical propositions to values that quantify their believed truth, e.g., by means of subjective opinions [16] quantified in the Deg value of the theory of O'Hara and based on evidence expressed by Warranty.

By virtue of items *c* and *d*, we do not model explicitly the trustworthiness relation defined by O'Hara: we consider an object *o* to be trustworthy by virtue of the fact that it is part of an RDF triple that is asserted.

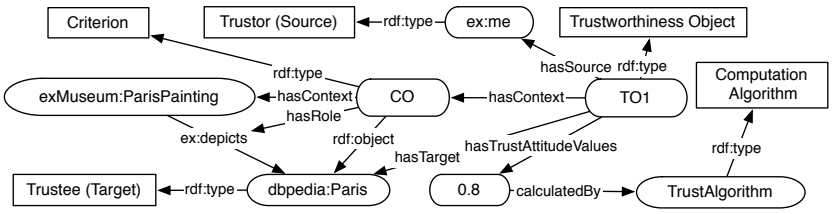

Fig. 2. Snapshot of the trust ontology, specialized for modeling data trustworthiness.

Figure 2 presents a snapshot of the trust ontology modeling the example above and adding a trust attitude value computed with a sample trust algorithm.

6 Conclusion

In this paper we introduce an ontology for trust representation that extends an existing model with recent trust theories. We specialize it in order to model data-related trust aspects, and we motivate our design choices based on standard RDF 1.1 semantics. This model is still at a very early stage, but it emerges from previous research and from standard trust theories. In the future, it will be extended, and evaluated in depth, also by means of concrete applications.

References

1. R. Alnemr, A. Paschke, and C. Meinel. Enabling reputation interoperability through semantic technologies. In *I-SEMANTICS*, pages 1–9. ACM, 2010.
2. D. Artz and Y. Gil. A survey of trust in computer science and the semantic web. *Journal of Semantic Web*, 2007.
3. T. Berners-Lee, R. Fielding, and L. Masinter. Uniform Resource Identifier (URI): Generic Syntax (RFC 3986). Technical report, IETF, 2005. `http://www.ietf.org/rfc/rfc3986.txt`.
4. S. Bradshaw, D. Brickley, L. J. G. Castro, T. Clark, T. Cole, P. Desenne, A. Gerber, A. Isaac, J. Jett, T. Habing, B. Haslhofer, S. Hellmann, J. Hunter, R. Leeds, A. Magliozzi, B. Morris, P. Morris, J. van Ossenbruggen, S. Soiland-Reyes, J. Smith, and D. Whaley. Open Annotation Core Data Model. `http://www.openannotation.org/spec/core`, 2012. W3C Community Draft.
5. S. J. Casare and J. S. Sichman. Towards a functional ontology of reputation. In *AAMAS*, pages 505–511. ACM, 2005.
6. D. Ceolin, A. Nottamkandath, and W. Fokkink. Automated Evaluation of Annotators for Museum Collections using Subjective Logic. In *IFIPTM 2012*, pages 232–239. Springer, May 2012.
7. D. Ceolin, A. Nottamkandath, and W. Fokkink. Semi-automated Assessment of Annotation Trustworthiness. In *PST 2013*. IEEE, 2013.
8. D. Ceolin, A. Nottamkandath, and W. Fokkink. Efficient semi-automated assessment of annotations trustworthiness. *Journal of Trust Management*, 1(1):3, 2014.
9. D. Ceolin, W. R. van Hage, and W. Fokkink. A Trust Model to Estimate the Quality of Annotations using the Web. In *WebSci 2010*. Web Science Trust, 2010.
10. R. Cyganiak, D. Reynolds, and J. Tennison. The rdf data cube vocabulary. Technical report, W3C, 2014.
11. M. Dürst and M. Suignard. Internationalized Resource Identifiers (IRIs) (RFC 3987). Technical report, IETF, 2005. `http://www.ietf.org/rfc/rfc3987.txt`.
12. J. Golbeck. Trust on the World Wide Web: A Survey. *Foundations and Trends in Web Science*, 1(2):131–197, 2006.
13. J. Golbeck, B. Parsia, and J. A. Hendler. Trust networks on the semantic web. In *CIA*, pages 238–249. Springer, 2003.
14. T. Heath and E. Motta. The Hoonoh Ontology for describing Trust Relationships in Information Seeking. In *PICKME 2008*. CEUR-WS.org, 2008.
15. J. Huang and M. S. Fox. An ontology of trust: Formal semantics and transitivity. In *ICEC '06*, pages 259–270. ACM, 2006.
16. A. Jøsang. A logic for uncertain probabilities. *Intl. Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 9(3):279–212, 2001.
17. K. O'Hara. A General Definition of Trust. Technical report, University of Southampton, 2012.
18. I. Pinyol and J. Sabater-Mir. Computational trust and reputation models for open multi-agent systems: A review. *Artif. Intell. Rev.*, 40(1):1–25, June 2013.
19. J. Sabater and C. Sierra. Review on computational trust and reputation models. *Artificial Intelligence Review*, 24:33–60, 2005.
20. W. Sherchan, S. Nepal, J. Hunklinger, and A. Bouguettaya. A trust ontology for semantic services. In *IEEE SCC*, pages 313–320. IEEE Computer Society, 2010.
21. L. Viljanen. Towards an ontology of trust. In *Trust, Privacy, and Security in Digital Business*, pages 175–184. Springer, 2005.
22. W3C. RDF 1.1 Semantics. `http://www.w3.org/TR/2014/REC-rdf11-mt-20140225/`, 2014.