MODELLING TRUST IN INFORMATION SYSTEMS DEVELOPMENT: Existing Approaches and Limitations

Kamaljit Kaur Bimrah, Haralambos Mouratidis, David Preston
Innovative Informatics, School of Computing and Technology
{bimrah, haris, d.preston}@uel.ac.uk

Abstract: This paper presents the current stage of our research, in respect to modelling and reasoning about trust and its related concepts during information systems development. In particular, it reviews the current state of the art with respect to modelling trust in information systems development and it concludes with the fact that there is no ontology which takes into account trust and all its related concepts. However, before discussing this matter, trust definitions and models are demonstrated, directly moving onto the current treatment of trust in information systems development and why it is important for trust and its related concepts to be modelled collectively in one methodology. It then briefly discusses the foundations for an ontology that advances the current state of the art, concluding with our future work and conclusions

1. Introduction

Nowadays, information systems play a colossal and equally imperative part. The grounds on why individuals are moving towards such systems are because they see optimistic results from the systems' assistance on different everyday activities. Research has shown (Jøsang, 2005a; Jøsang, 2005b; Jøsang, 2005c; Jøsang, 2004a) that individuals are willing to trust information systems, as they trust other humans, knowing that there are potential risks. Once they trust, if they have a good experience, then trust is gained, hence the fabrication of trust, building reputation, which proves beneficial for potential users. On the other hand, if the individuals have a bad experience, then there is no trust for the future, causing a bad reputation for a particular information system. Therefore, the consideration of trust in information systems is not any more an option but rather a necessity for the acceptance of a system. The importance of the issue has also been identified in research (Yu, 2001), where the need to consider trust as part of the development process of an information system is also argued.

Trust, however, is not a concept to be considered in isolation. Initial investigation has shown that trust is related to many other concepts - it should be considered together with security, risk and other related concepts as part of the development process of an information system. In particular, recent research (Sutcliffe, 2006) has shown that trust should be considered from the early stages of the development process of information systems and modelling languages and methodologies should incorporate trust and its related concepts into their ontology and modelling processes. One of the reasons for this need comes from the necessity to identify early in the development process any conflicts between the requirements introduced to the system by trust and security considerations and the system's functional requirements. This is similar to the conclusions reached by a large number of works related to security modelling (Mouratidis, 2005; Mouratidis, 2006).

To assist information systems developers to consider trust during the development process, it is vital to have ontologies and modelling languages, to provide the concepts and notations needed, and methods and methodologies, to provide the structured processes that will guide information system developers in analyzing and modelling trusted information systems. The current state of the art fails to adequately satisfy this need.

The main aim of our research is to advance fill in that gap by developing ontologies, methods and methodologies. This paper reports on our efforts towards the development of an ontology that provides the concepts, notation and formalism to capture trust and its related concepts.

The paper consists of five sections. The next section discusses the trust definition that is to be used for the duration of this project. Section three discusses the current treatment of trust in information systems development. The limitations, with respect to trust, of existing works in ontologies are discussed in section four, leading onto the novelty of the work. Section five states the current situation of the proposed ontology and section six concludes this paper and presents directions for future work.

2. Trust Definitions and Models

According to the current state of art, trust is difficult to define, convey, measure or specify (Michael, 2002) "…Trust is a term with many meanings" (Williamson, 1993). Numerous researchers have put their own viewpoints forward regarding the definition of the word trust. There are many definitions of the word 'trust' (Alford, 2004; Almenarez, 2004; Chopra, 2003; Gambetta, 2000; Jøsang, 1996; Jøsang, 2004a; Jøsang, 2004b; Jøsang, 2005a; Jøsang, 2005c; McKnight, 1996; Maarof, 2002; Numan, 1998; Robinson, 1996; Tang, 2002)

In this research, the following definition is used 'trust is one's expectations, assumptions, or beliefs about the likelihood that another's future actions will be beneficial, favorable, or at least not detrimental to one's interests' (Robinson, 1996). Moreover, this research employs the 'weight of hurt model'. For example, A may trust B o do something if A knows it hurts B not to do it. For example, one trusts MGM to make a movie that doesn't show unimaginably horrific scenes as otherwise they will be hurt more than any viewer's momentary unpleasant feeling and loss of admission fee.

3. Current Treatment of Trust in Information Systems Development

It is mentioned in (Yu, 2001) that 'trust is becoming an increasingly important issue in the design of many kinds of information systems'. The paper brings to light the importance of assessing and establishing trust as part of the development process because 'many new kinds of technologies are being used in new contexts and social-technical configurations that have not been tried before' as well as the fact that 'uncertainties and concerns of various stakeholders and participants need to be considered and addressed'.

Moreover, recent research (Sutcliffe, 2006; Chopra, 2003) has shown that trust should be considered from the early stages of the information systems development process (Chopra, 2003; Mouratidis, 2005; Yu, 2001; Mouratidis, 2006). There are analogous conclusions which have been reached by a large number of works associated to security modelling. One of the reasons for this need comes from the necessity to identify early in the development process any conflicts or inconsistencies between the requirements introduced to the system by trust and security considerations and the system's functional requirements (Chopra, 2003).

In particular, it is highlighted in (Sutcliffe, 2006) 'design and trust intersect in two ways'. (Sutcliffe, 2006).mentions the importance of users having a positive experience from a software product, but this will only happen if the software products are designed so the users trust it. This role is to be fulfilled by good design (Sutcliffe, 2006). If the design is not thought-out prior to the development stage, then there is a possibility that the software product will not be built as per the user's requirements, and when the user actually utilizes the software product, he will be made aware that his requirements haven't been fulfilled, hence causing distrust of the product. A number of examples under the category of good design could be usability and appropriate functionality amongst many other issues found in (Sutcliffe, 2006). Some form of 'ownership' should also be allowed in such products, which allows the user to customize and adapt according to his/her needs; this in turn actually 'facilitates trust'. The second way that (Sutcliffe, 2006) mentions that design and trust are intersected is by having 'technology acting as a mediator of trust between people, organizations or products'. In essence, what the paper is saying is that the uncertainty that is present in relationships should be reduced by technology, this in return will make information more accessible; enhancing trust.

However, to successfully analyze trust issues during the development of information systems, it is extremely important to model trust, along with its related concepts, such as initial trust, reputation, risk, privacy and security.

If there is nothing to start of with initially, then going on to fully trust an object would prove difficult. Flowing on from this would be reputation. If a certain product has no reputation it may prove difficult to trust. Good reputation leads to trust, and bad reputation leads to distrust. However, saying this, it has been shown that even when the reputation of a system or product is poor, then some individuals still take the risk to going onto trusting. It has been made aware that individuals and/or systems are trusted knowingly, even when there is some degree of risk involved. Another concept related to trust is privacy. If one knows that a system cannot guarantee privacy assurance, will the user still use the system willingly? (Yu, 2002). Privacy and trust work in concurrence with each other, and it is important for them to be modeled together also. Similarly to privacy, security plays an important part in the modelling of trust; if a system is not secure, what use is it? Security, as a concept needs to be adequately modeled in conjunction with the above concepts mentioned.

4. Limitations

The current state of the art does not provide an ontology which takes trust and its related concepts into consideration collectively. There are many independent security ontologies (Kim; 2005, Simmonds, 2004; Mouratidis, 2003), trust ontologies (Viljanen, 2005), risk ontologies (Cuske, 2005), currently, however nothing which models all related concepts together. The other trust related concepts which came to light via research (such as reputation and privacy), have no corresponding ontologies. There are reputation ontology related papers (Chang, 2005; Golbeck, 2004); however there is no such ontology for the concept mentioned.

These independent ontologies have limitations. For example, as declared in (Viljanen, 2005) there are problems in the trust ontology '…the sharing of the trust relationship data may be restricted because of privacy or security reasons'. The latter have not been taken into consideration into the building of the ontology. It has been established that privacy and security are trust related concepts, and even though security has its own ontology, this and privacy haven't been incorporated, therefore causing the sharing constraint of the trust related data. There are seven different security ontologies which have been accumulated to form the NRL Security Ontology (Kim, 2005). Saying this, even though seven separate ontologies are combined together to form the NRL Security Ontology, the paper illustrates the need for further ontologies to address issues which haven't been addressed before such as 'privacy policies, access control and survivability'. This is actually a security ontology, however it has been bought to light that supplementary ontologies 'are needed to address the issues such as privacy policies amongst others'. (Kim, 2005).

It is mentioned in (Cuske, 2005) that 'an extension of the technology risk ontology's scope is feasible, e.g. by including risk measurement', however there is no such study or extension point mentioned of introducing other concepts, just to extend the current ontology scope.

5. Initial Ideas for a Complete Trust (with Related Concepts) Ontology

The first challenge during the development of a trust ontology was the choice of the methodology for the ontological development. After reviewing a large number of papers regarding ontology methodologies (Fernandez, 2002; Gomez-Perez, 2003; Gomez-Perez, 2004; Jones, 1998; Lau, 2002; Noy, 2001; Pinto, 2002; Pinto, 2004, Uschold, 1996; Uschold, 1995), it was decided that the METHONTOLOGY be used for our ontology development. There are various reasons for this decision. First of all, the METHONTOLOGY fulfills our criterion which was as the ontology domain was new to us, we wanted a methodology that was straightforward to follow and that the steps of the ontology should be well defined, and well explained to the new ontology developer. Other pulling factors towards the METHONTOLOGY methodology was that it has been employed widely even by inexperienced users (Pinto, 2004); thirdly concrete guidelines are provided to guide developers. It is also worth mentioning that the METHONTOLOGY methodology is recommended by FIPA for ontology development.

In respect to the proposed ontology, individuals or systems may not trust a system because of bad reputation, or may decide to trust the system because of its good reputation, as well as being aware of the risks present. They may decide to progress knowing that the security and privacy policies are in place. Simply, individual will trust. Risk may affect trust. Trust may be dependent on reputation. Security and privacy policies may enhance trust.

As has already been established, the ontology in question is about trust and its related concepts which are most important and which should be taken into consideration during the information systems development stage. The ontology will serve as a guideline for the methodology which will be used in information systems development. Till date, the main scenarios of use which have arisen are that the ontology could be employed with the aid of a methodology which takes into contemplation trust or any of its related concepts, the ontology could be employed by individuals wanting to find out the main trust related concepts, the ontology could be utilized by other ontology developers that are enhancing their current ontology, the ontology could also be exploited by ontology developers that are attempting to design their own ontology and need some direction, the ontology could also be used by developers of information systems who are researching into trust related issues with regards to security for their system. These were the main uses of the potential ontology which have become apparent. From the scenarios, some users came to light that have been initiated from these mentioned scenarios. The users of the potential ontology could be methodology designers; researchers wanting to know about trust related concepts and the relationships, current ontology researchers/developers, new ontology researchers/developers respectively, as well as developers of information systems respectively.

To sum up the proposed ontology, the main classes are trust, risk, reputation, privacy and security. Within each of these classes there are attributes and within these attributes there are sub-attributes. An example would be the security class. Within here we have the security mechanism attribute and the security policy attribute. If we take the security mechanism attribute, we have defined the sub-attributes to be syntax and protocol. These attributes/sub-attributes will need to be modelled successfully in the development stage, in order for their respective class to get a 'tick' to indicate that that trust related concept has been taken into consideration and modelled productively in the proposed information system.

6. Conclusions and Future Work

As mentioned previously in Section 4, the current state of the art does not provide an ontology that takes trust and its related concepts into consideration collectively, although there are many individual ontologies.

Also pointed out earlier, it was declared in (Viljanen, 2005) that there are problems in the trust ontology '…the sharing of the trust relationship data may be restricted because of privacy or security reasons'. The latter concepts have been taken into deliberation hence shown by their inclusion in the proposed ontology.

There was a limitation highlighted by Cuske et al 2005, who said that 'an extension of the technology risk ontology's scope is feasible, e.g. by including risk measurement', however there is no such study or extension point mentioned of introducing other concepts related to risk; the latter is just progressing to extend the current ontology scope.

The Intial Ideas for a Complete Trust (With Related Concepts) Ontology in Section 5, although not complete, does demonstrate an important advantage with respect to existing ontologies. It considers trust along with related concepts and therefore it provides the foundations for a methodology that will allow information systems developers to reason about trust in a coherent and structured way.

In regards to future work, the first step aims to define the concepts of our ontology in more detail and identify their relationships. This will provide the foundations for a graphical modelling language, which in turn will provide the basis for a complete methodology to consider trust during the information systems development process. Moreover, research into various case studies which are related to trust will have to be carried out concluding on to identifying one that is suitable for the validation of the proposed methodology.

7. Acknowledgements

Firstly, we would like to show gratitude to EPSRC for their funding with regards to this project and secondly we would like to express thanks to the staff at St Patrick's College, (London) for their support in our research.

8. References

Alford, J. (2004). Building Trust in Partnerships Between Community Orgnization and Government. Changing the Way Government Works Seminar, Melbourne.

Almenarez, F., et al (2004). PTM: A Pervasive Trust Management Model for Dynamic Open Environments. First Workshop on Pervasive Security, Privacy and Trust, PSPT'04 in conjunction with Mobiquitous. Boston, USA.

Chang, E., Hussain, F.K., Dillon T (2005). "Reputation Ontology for Reputation Systems." International Workshop on Web Semantics (SWWS): pp. 957-966.

Chopra, K., Wallace, WA (2003). Trust in Electronic Environments. Proceedings of the 36th Hawaii Conference on System Sciences, Hawaii.

Cuske, C., Korthaus, A., Seedorf, S., Tomczyk, P (2005). Towards Formal Ontologies for Technology Risk Measurement in the Banking Industry. Proceedings of the 1st Workshop Formal Ontologies Meet Industry, Verona, Italy.

Fernandez-Lopez, M. and A. Gomez-Perez (2002). Deliverable 1.4: A Survey on Methodologies for Developing, Maintaining, Integrating, Evaluating and Reengineering Ontologies Technical Report. M. Fernandez-Lopez, OntoWeb Consortium.

Gambetta, D. (2000). Can We Trust Trust? Making and Breaking Cooperative Relations**:** 213-237.

Golbeck, J., Hendler, J (2004). Accuracy of Metrics for Inferring Trust and Reputation in Semantic Web-Based Social Networks. Engineering Knowledge in the Age of the SemanticWeb: 14th International Conference, EKAW 2004, Proceedings Whittlebury Hall, UK, Springer Berlin / Heidelberg.

Gomez-Perez, A., O. Corcho, et al. (2003). "Methodologies, Tools and Languages For Building Ontologies. Where is Their Meeting Point?" Data and Knowledge Engineering 46(1): pp. 41-64.

Gomez-Perez, A., Fernandez-Lopez, et al. (2004). *Ontological Engineering*, Springer-Verlag.

Jones, D., T. Bench-Capon, et al. (1998). Methodologies for Ontology Development. In Proceedings of IT&KNOWS - Information Technology and Knowledge

Systems - Conference of the 15th IFIP World Computer Congress, Vienna, Austria and Budapest, Bulgaria, 1998., Chapman-Hall.

Jøsang, A. (1996). The right type of trust for distributed systems. In Proceedings of the 1996 New Security Paradigms Workshop.

Jøsang, A., Presti, SL (2004a). Analysing the Relationship Between Risk and Trust. Proceedings of the Second International Conference on Trust Management, Oxford.

Jøsang, A., Patton, MA (2004b). "Technologies for Trust in Electronic Commerce." *Electronic Commerce Research Journal*, l 4(1&2): pp. 9-21.

Jøsang, A., Pope, S (2005a). Semantic Constraints for Trust Transitivity. Second Asia-Pacific Conference on Conceptual Modelling (APCCM2005), Newcastle, Australia.

Jøsang, A., R. Ismail, et al. (2005b). "A Survey of Trust and Reputation Systems for Online Service Provision." Decision Support Systems.

Jøsang, A., C. Keser, et al. (2005c). Can We Manage Trust? Third International Conference on Trust Management (iTrust), Paris.

Kim, A., Luo, J. & Kang, M (2005). Security Ontology for Annotating Resources. Lecture Notes in Computer Science, Agai Napa, Cyprus, Springer-Verlag Berlin / Heidelberg.

Lau, T. and Y. Sure (2002). "Introducing Ontology-based Skills Management at a Large Insurance Company." pp.123-134.

Maarof, M. A., Krishna, K (2002). "An Hybrid Trust Management Model For MAS Based."

McKnight, D., Chervany, NL (1996). The Meanings of Trust. Technical Report MISRC Working Paper Series 96-04, University of Minnesota, Management Information Systems Reseach Centre.

Michael, J. B., Hestad, D.R., Pedersen, C.M., Gaines L.T (2002). "Incorporating the Human Element of Trust into Information Systems." *IAnewsletter* 5(2): pp 4-8.

Mouratidis, H., Giorgini, P., Mansoon, G (2003). An Ontology for Modelling Security: The Tropos Approach. Proceedings of the 7th International Conference on Knowledge-Based Intelligent Information & Engineering Systems, Oxford, England.

Mouratidis, H. and P. Giorgini (2006). Integrating Security and Software Engineering: An Introduction. In Integrating Security and software engineering Advances and Future Vision.

Mouratidis, H., P. Giorgini, et al. (2005). "When Security Meets Software Engineering: A Case Of Modelling Secure Information Systems."

Noy, N. F. and D. L. McGuinness (2001). Ontology Development 101: A Guide to Creating Your First Ontology. Technical Report KSL-01-05, Stanford Knowledge Systems Laboratory.

Numan, J. (1998). Knowledge-Based Systems as Companions: Trust, Human Computer Interaction and Complex

Systems. Faculty of Management and Organization University of Groningen: 142.

Pinto, H. S. and H. Beck (2002). Overview of Approach, Methodologies, Standards, and Tools for Ontologies, University of Florida.

Pinto, H. S. and J. P. Martins (2004). "Ontologies: How can they be built?" *Knowledge and Information Systems* 6(4): pp.441-464.

Robinson, S. L. (1996). "Trust and Breach of the Psychological Contract." *Administrative Science Quarterly* 41(4): pp 574-579.

Simmonds, A., Sandilands, P., Ekert, L.V (2004). An Ontology for Network Security Attacks. Lecture Notes in Computer Science, Kathmandu, Nepal, Springer Berlin / Heidelberg

Sutcliffe, A. (2006). Trust: From Cognition to Conceptual Models and Design. 18th International Conference, CAiSE 2006, June 5-9, 2006 Proceedings, Luxembourg, Luxembourg, Springer-Verlag Berlin Heidelberg

Tang, Y., Winoto, P., Niu, X (2002). Investigating Trust between Users and Agents in a Multi agent Portfolio Management System: a Preliminary Report. In the Workshop on Business Agents and the Semantic Web, Fifteenth Canadian Conference on Artificial Intelligence, Canada.

Uschold, M., King, M (1995). Towards a Methodology for Building Ontologies. . In Workshop on Basic Ontological Issues in Knowledge Sharing, held in conjunction with IJCAI-95. Montreal, Canada

Uschold, M., Gruninger, M (1996). "Ontologies: Principles, Methods, and Applications." *Knowledge Engineering Review* 46(2).

Viljanen, L. (2005). Towards an Ontology of Trust. Lecture Notes in Computer Science. Copenhagen, Denmark, Springer Berlin / Heidelberg.

Williamson, O. (1993). "Calculativeness, Trust, and Economic Organization." *Journal of Law and Economics* 34: 453-502.

Yu, E., Liu, L (2001). Modelling Trust for System Design Using the i* Strategic Actors Framework. Proceedings of the workshop on Deception, Fraud, and Trust in Agent Societies held during the Autonomous Agents Conference: Trust in Cyber-societies, Integrating the Human and Artificial Perspectives.

Yu, E., Cysneiros, L.M. (2002) Designing for Privacy and Other Competing Requirement. 2nd Symposium on Requirements Engineering for Information Security. Raleigh, North Carolina.