Author(s): Bimrah, Kamaljit Kaur; Mouratidis, Haralambos; Preston, David
Title: iTrust: a trust-aware ontology for information systems development
Year of publication: 2008
Citation: Bimrah, K.K., Mouratidis, H., Preston, D. (2008) 'Settling time formulae for the design of control systems with linear closed loop dynamics' Proceedings of Advances in Computing and Technology, (AC&T) The School of Computing and Technology 3rd Annual Conference, University of East London, pp.40-51
Link to published version:
http://www.uel.ac.uk/act/proceedings/documents/ACT08.pdf

iTrust: A TRUST-AWARE ONTOLOGY FOR INFORMATION SYSTEMS DEVELOPMENT

Kamaljit Kaur Bimrah, Haralambos Mouratidis, David Preston
Innovative Informatics, School of Computing and Technology, University of East London, UK
bimrah@uel.ac.uk, haris@uel.ac.uk, david17@uel.ac.uk

Abstract: This paper gives a synopsis of our present state of affairs in modelling an ontology which reflects trust related concepts collectively in information systems development. The main problem is that there is a lack of ontological and methodological support to model and reason about trust with its related concepts in one allied framework. This situation provides the foremost motivation for our research. In particular, our aim is to develop a reasoning and modelling framework that will enable information system developers to consider trust and its related concepts collectively during the development of information systems.

1. Introduction

Trust is a concept, which although difficult to define precisely (Michael, 2002) is very important in various aspects of human society. As information systems play an increasingly important role to every aspect of the human life, 'trust is becoming an increasingly important issue in the design of many kinds of information systems' (Yu, 2001). As research (Chopra, 2003) has shown, if trust is not present, if there is no confidence, expectation, belief and faith in an information system, then there will be no willingness to rely on any such systems. As it is highlighted in (Sutcliffe, 2006) 'design and trust intersect in two ways'. The importance of users having a positive experience from a software system will only happen if software systems are designed so the users trust them (Sutcliffe, 2005).
Moreover, recent research (Chopra, 2003; Sutcliffe, 2006; Mouratidis, 2006) argues not only for the need to consider trust when developing information systems, but to consider it from the early stages of the development process. Such arguments are in line with research on other important, and related to trust, issues for information systems, such as security (Yu, 2001; Mouratidis, 2006). 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).
Nevertheless, and despite the large number of works related to trust models and trust ontologies (see the related work section of this paper), there is an important issue that current state of the art fails to address. This is the lack of a trust ontology that considers not only trust but a number of closely related concepts and the realisation of an information systems development methodology to consider trust as part of its development process.

Our aim is to fill this gap. In this paper we present our effort to develop the much needed trust ontology, which will form the basis for our development methodology. In particular, and differently than other existing works, our trust ontology includes a number

of concepts related to trust such as reputation, privacy and security.

The rest of the paper is structured as follows. Section 2 comprises of work on the ontology. This consists of a discussion on the methodology and the tool used for developing the ontology. The requirements of the ontology are discussed next, pinpointing the specific trust related concepts that form the basis of the ontology, flowing on is description of the structure of the ontology, which includes a portrayal of the ontology. Section 3 discusses the case study which is to be used in the validation of the ontology. The penultimate section is related work, closing with the conclusion and future work.

2. The Ontology

The main novelty of our ontology lies in the fact that it supports a collective treatment of trust, and a number of closely related concepts, in information systems development. This allows any users of the proposed ontology to consider trust in a same way as it would be considered in real life, i.e. not as an isolated concept that needs to be treated in a separate way, but within an appropriate context including concepts such as security.

For the development of the ontology, we have followed a structured ontology development course of action, which was carried out by using a precise methodology that is explained in the subsequent segment.

2.1. The Methodology for the Ontology

During the development of our ontology, the first challenge was the choice of the methodology for the ontological development. To help the selection, a number of requirements were identified including the following: (i) It should be clear and concise. We wanted a methodology that was straightforward to follow, and where the development steps are well defined, and well explained to the new ontology developer; (ii) It should be flexible enough to be adapted to your purpose if needed; (iii) It should have been employed previously in a number of projects, and preferable by novice (with respect to their knowledge of the methodology) developers.

After reviewing a large number of ontology methodologies (Fernandez-Lopez, 2002; Gomez-Perez, 2004; Jomes, 1998; Lau, 2002; No, 2001; Pinto, 2004; Mayer, 2005) and taking into consideration the above requirements, it was decided that the METHONTOLOGY methodology be used for our ontology development. Out of all the methodologies we reviewed, the METHODOLOGY is the most popular choice for ontological development and one of the few methodologies that is accepted by external organizations (Gomez-Perez, 2004). Other pulling factors towards the METHONTOLOGY methodology was that it has been employed widely even by inexperienced users (Pinto, 2004).

It is also worth mentioning that the METHONTOLOGY methodology is recommended by FIPA for ontology development (Gomez-Perez, 2004).

The following figure shows the ontology life cycle which is proposed in the METHONTOLOGY methodology.

The methodology for the ontology development process has been specified and justified, and the same had to be applied for the tool that we were to be developing the ontology in. The foremost feature that we were looking at whilst deciding upon a tool were its usability.

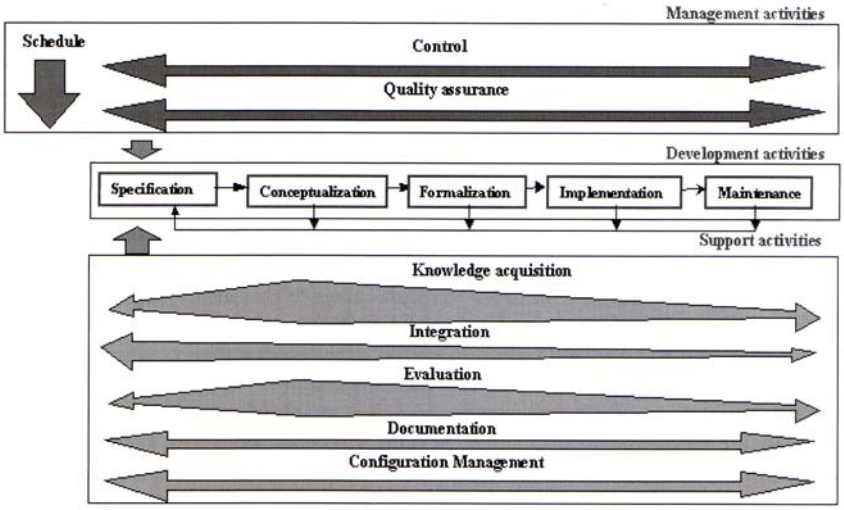


Fig. 1. Development process and lifecyle of METHONTOLOGY (Gomez-Perez et al, 2004)

Due to the fact the ontology needed to be developed in a short span of time, the usability of the tool was considered necessary to be straightforward for a new ontology developer like ourselves. The classes, attributes, instances etc needed to be implemented into the system with not too much botheration.

It is mentioned in (Gomez-Perez, 2004) that in recent years a new generation of ontology-engineering environments ha been developed. Some of which are Protégé-2000; WebODE; OntoEdit; OILEd, or the KAON tool suit. After careful research and analysis we decided to go for Protégé-2000 which was developed at Stanford University, California. (Fernandez-Lopez, 2002). It is mentioned in (Fernandez-Lopez, 2002) paper that Protégé-2000 has thousands of users all over the world who use the system for projects ranging from modeling cancer-protocol guidelines to modeling nuclear-power station. As mentioned previously, a foremost feature that we were looking at whilst deciding upon a tool was the usability factor. Protégé-2000 provides a graphical and interactive ontology-design and knowledge-base–development environment. It helps knowledge engineers and domain experts to perform knowledge-management tasks (Fernandez-Lopez, 2002). The Protégé-2000 tool has a tree hierarchy structure, so in terms of accessing all concepts, attributes and instances, it can be done so promptly and minimally. Protégé-2000 also allows for scalability and extensibility; there is no limit in terms of concepts as well as there being no limit of when the ontology is regarded as being complete, the ontology can keep on growing. Finally, another pulling factor towards Protégé-2000 was the fact that the system is constructed in an open, modular fashion. Its component-based architecture enables system builders to add new functionality by creating appropriate plugins.

2.2. The Requirements of the Ontology

Trust can be thought of in terms of faith or confidence. Borrowing an example from everyday life, if a ladder looks wobbly, one is unlikely to trust it to hold ones weight (Michael, 2002). Similarly in the

information systems world, if a system does not appear to be appropriate users might not trust it. Consider for instance the issue of security. If a system's mechanisms for enforcing authentication, authorization, privacy, integrity and non-repudiation policy do not appear to be sufficiently strong to the users, then users may hesitate to use the system. From this brief discussion, initiated from trust, it can be highlighted that a few terms have taken significance. For example in the case of weak security considerations in a system, as mentioned in the example above, the concept of reputation emerges. In the next section, we discuss a number of trust related concepts and argue for the need to consider them for a trust related ontology.

2.2.1. Trust and its Related Concepts

An important question that was raised as part of the first phase of research was w*hat main concepts are related to trust?* To answer this, a thorough study of trust as it appears in the literature took place. It is stated in (Li, 2004) that 'trust is the extent to which one part is willing to depend on somebody, or something, in a given situation with a feeling of relative security, even though negative consequences are possible'. This definition makes aware that a trusting object is being trusted; however the trusting subject is aware that there are potential consequences which may prove to have negative consequences for him/her. Risk emerges when the value at stake in a transaction is high, or when this transaction has a critical role in the security or the safety of a system (Josang, 2004). '*Risk management is a crucial activity in the development of secure systems'*. (Mayer, 2007). Here, the potential for risk is distinguished, it is known that individuals do trust knowingly when they know that risk could be a potential, however some individuals may decide not to trust due to this risk element. Individuals are aware of the potential risk(s), yet they still wish to trust, however if this risk materialises, then how would this affect the trust aspect? This may cause the user never to use and/or trust the system again, or it may not. If a system has a high risk, then having trust is also unlikely.

Using an example of the electronic commerce industry, Patton & Jøsang says that since trust is based on experience over time, establishing initial trust can be a major challenge to newcomers in e-commerce (Josang, 2004b). Initial trust was defined as trust in an unfamiliar object, dealing with a relationship in which the trustor does not have meaningful experience, knowledge or affecting bonds with the trustee (Li, 2004). Closely tied to initial trust is reputation. It is stated in (Josang, 2007) that reputation is what is generally said or believed about a person's or thing's character or standing.

Relating to that, (Josang, 2004b) said about trust, it seems as though the reputation of a trusting subject is also an extremely important concept. If the trusting subject does not have a good reputation, then they may be discarded and distrusted.

Security has a similar association with trust; if the user is aware of the security aspects being adequately covered then they may feel more confident in using the system, they may have trust, however, if the user is not sure of the security aspects, then they may decide against using the system. '*Few works have tried to directly link trust with security'* (Lo Presti, 2003). It is advocated by (Mayer, 2007) that *'security engineering should begin at early stages of IT system development, including the use of risk analysis'*. It is mentioned in (Yu, 2002) *that 'privacy, security and trust are increasingly*

demanding attention in today's networked based systems, they are frequently demanding tradeoffs to be considered and requirements to be negotiated there, they have to be taken into account at the earliest stages of the software development process'. From the above discussion we conclude that concepts related to trust are risk, initial trust, reputation, security and privacy. Although we do not claim that this is a complete list, we consider these concepts as the minimum set of concepts related to trust.

2.3. The Structure of the Ontology

Following knowledge acquisition, the main development process took place. According to the METHONTOLOGY, the main development takes place in the conceptualisation activity. During that activity, six different tasks are identified as illustrated in Figure 2.

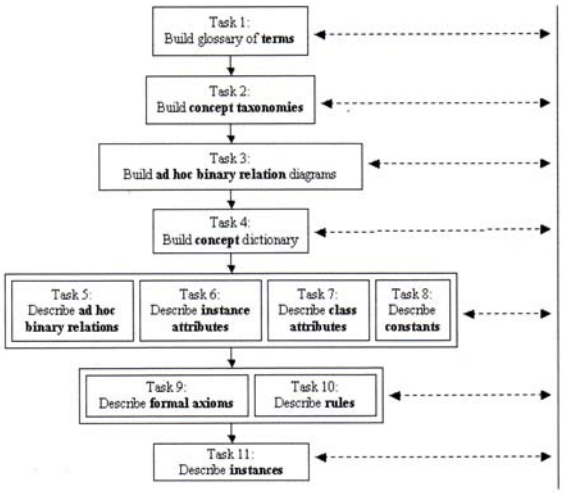


Fig. 2. Tasks of the conceptualization activity according to METHONTOLOGY(Gomez-Perez et al, 2004

Therefore, in demonstrating the development of our ontology we refer to these tasks. It is worth mentioning that due to lack of space, in this paper we demonstrate the development of our ontology focusing only on the concept of initial trust, however work has been carried out on the other trust related concepts such as privacy, security, reputation and risk, which incorporates the aspects of the conceptualization activity from the ontology development process such as building concept taxonomies, specifying the binary relations, building the concept dictionary etc, however these will all be explained for the initial trust concept subsequently.

The foremost task in the development of the ontology involves the building of the glossary of terms that identifies the set of terms to be included on the ontology, their natural language definition (description), their type and their synonyms and acronyms. Considering the concept if Initial Trust, a number of terms can be identified that contribute towards the ontological analysis of the concept. These are illustrated in Table 2. For instance, trusting belief is of type concept and it is described as the trusting subject's perception that the trusting object has attributes that are beneficial to the trusting subject.

Name	Synonyms	Acronyms	Description	Type
Initial Trust	-	-	Trust in an unfamiliar object, dealing with a relationship in which the trusting subject does not have credible, meaningful experience, knowledge, or affective bonds with, the trusting object.	Concept
Experience	-	-	The past experience (if any) that the trustor has of the trustee	Attribute
Personal Judgement	-	-	If the trustor has no experience of the trustee, they can use their personal judgement.|	Attribute
Trusting belief	-	-	The trusting subject's perception that the trusting object has attributes that are beneficial to the trusting subject.	Concept
Competence	-	-	Trusting object's ability to do what the subject needs	Instance Attribute
Benevolence	-	-	Trusting object's caring and motivation to act in the subject's interests	Instance Attribute
Integrity	-	-	Trusting object's honesty and promise keeping	Instance Attribute

Table 1. Glossary of terms related to initial trust

The first column in the above table displays the various names which are included in the ontology, and all these names have a

corresponding type (concept, attribute, and instance). It is mentioned in (Noy, 2001) that an ontology is a formal explicit description of concepts in a domain of discourse and properties of each concept describing various features and attributes of the concept. They also go on to say that concepts in the ontology should be close to objects (physical or logical) and relationships in the domain of interest. These are most likely to be nouns (objects) or verbs (relationships) in sentences that describe the domain. An attribute is an element of the data structure that, together with operations, defines a class. Overall it describes some property of instances of the class (McRobb, 2002). An instance is a single object, usually called nainstnce in the context of its membership of a particular class or type (McRobb, 2002).

It was important to build a glossary of terms that identifies a set of terms to be included on the ontology - which takes Table 1's format - as it acted as a basis for our ontology. The information from Table 1 is able to be extracted for the next stage on the ontology development process, which is building the taxonomy for the ontology.

When the glossary of terms has been finalised, the next task involves building the concept taxonomies to classify the various concepts. The output of this task is one or more taxonomies where concepts are classified. Following our example of initial trust, Figure 3 illustrates part of the taxonomy related to that concept.

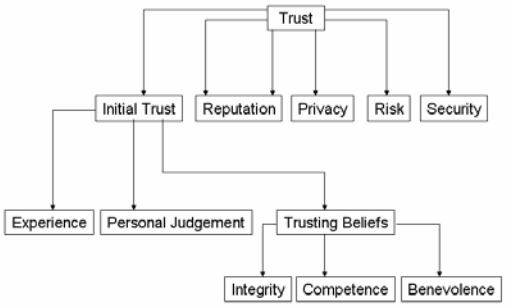
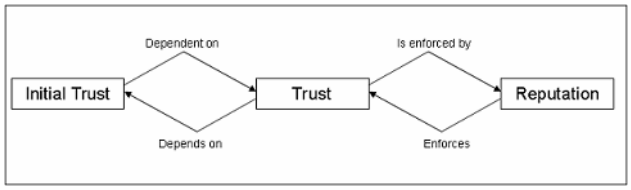


Fig. 3. Partial Taxonomy of initial trust

A taxonomy is considered necessary as when the glossary of terms contains a sizable number of times, we need to build concept taxonomies to define the concept hierarchy (Gomez-Perez, 2004).

The following task involves building an ad-hoc binary relation diagram to specifically identify the relationships between concepts of a particular taxonomy and concepts of other taxonomies. For instance, a binary relation can be identified between the main



concepts of the initial trust taxonomy, the trust taxonomy and the reputation taxonomy as illustrated in Figure 4.

Fig. 4. Partial ad-hoc binary relation diagram

Identifying the relationships between the various taxonomies of the ontology, allows us to build the concept dictionary, which mainly includes the concept instances for each concept, their instance and class attributes, and their ad hoc relations (Gomez-Perez, 2004). A partial representation of the concept dictionary for our trust ontology, focused on the initial trust taxonomy is illustrated in Table 2.

Concept Name	Class attributes	Instance attributes	Relations
Experience	Present?	-	-
Personal judgement	-	-	
Trusting beliefs	What are the trusting beliefs?	Competence Benevolence Integrity	Belief present
Trusting intention	What are the trusting intentions?	Willingness to depend Subjective probability of depending	
Disposition to trust	-	Faith in humanity Trusting stance	Is dependant on Depends on
Institution based trust	-	Structural assurance Situational normality	

Table 2. Partial Concept Dictionary

The below figure demonstrates how Table 2 is displayed in the tool we are using for the ontology development process. The main concepts are displayed on the left hand side, in the form of a tree hierarchy. As the tree whittles down, the attributes and the instances of the respective concepts can be distinguished.

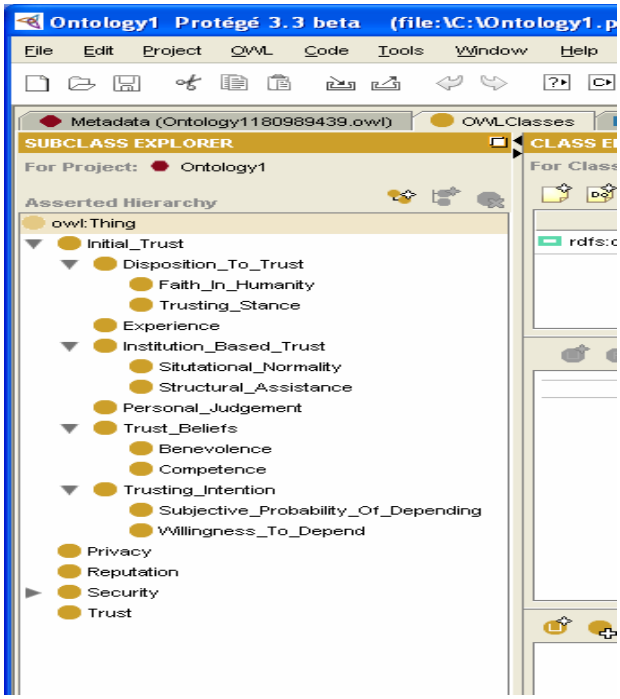


Fig 5. Partial Initial Trust Tree Hierarchy

Once the concept taxonomy and ad hoc binary relation diagrams had been generated we needed to specify which are the properties and relations that describe each concept of the taxonomy in a concept dictionary which is defined next.

An important issue is the exact definition of the various relations as they appear in the binary relation diagram, and on the concept dictionary. It is important to precisely identify what the source concept is, what the source cardinality is, what is the target concept and what is the inverse relation. An illustration of some of the relations of our ontology is shown in Table 3.

Relation name	Source concept	Source cardinality (max)	Target concept	Inverse relation
Dependent on	Initial Trust	N	Trust	Depends on
Depends on	Trust	N	Initial Trust	Dependent on
Is enforced by	Trust	N	Reputation	Enforces
Enforced	Reputation	N	Trust	Is enforced by
Is enhanced by	Trust	N	Security	Enhances
Enhances	Security	N	Trust	Is enhanced by
Is enhanced by	Trust	N	Reputation	Enhances
Enhances	Reputation	N	Trust	Is enhanced by
Needs	Security	N	Authentication	Is needed by
Is needed by	Authentication	N	Security	needs

Table 3. Binary relations definition

For example, we have the concept of Initial Trust (which is the source concept), and this concept has a relationship with Trust (target concept). Initial Trust is dependent on Trust. Now, the inverse relation of this is, Trust depends on Initial Trust.

The below figure exhibits the relationship of the concepts that are displayed in Table 3 in the tool that is used for the ontology.

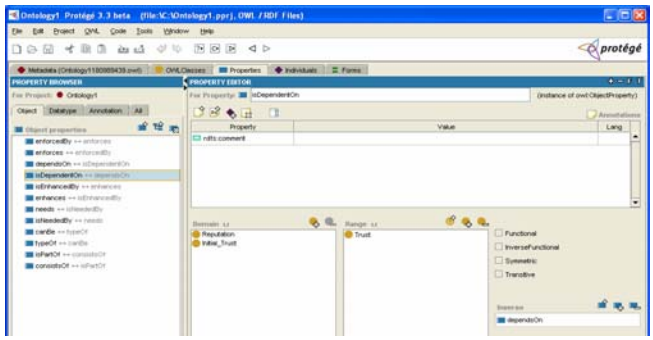


Fig. 6. Sample of relationships

It is also important to describe in detail each instance attribute that appears on the concept dictionary. The output of this task is a table (Table 4) where instance attributes are defined in terms of their value types, value range and cardinality.

Instance attribute name	Concept name	Value type	Value range	Cardinality
Competence	Trusting beliefs	String	-	
Benevolence	Trusting beliefs	String	-	
Integrity	Trusting beliefs	String	-	

Table 4. Instance Attributes

The next step involves the detailed description of each class attribute that appears on the concept dictionary. The output of this step is the description of the class attribute in terms of its defined concept, its value type, its cardinality and its values as shown in Table 5.

Class attribute name	Defined concept	Value type	Cardinality	Values
What are the trusting beliefs?	Trusting beliefs	String		-

Table 5. Description of class attributes

3. Case Study

To validate our ontology, we have used a case study from a domain where trust and its related concepts play an important role, the health care domain. Consider the scenario where a patient is seeing a GP for the first time. The reason for this is because the patient has moved house and has had to change to a nearer practice closer to their new home. Travelling to the previous practice, where the patient has been going for years, was not practical due to the distance. To illustrate our ontology, we illustrate the instantiation of some of the concepts of our ontology in relation to the above case study. Consider for instance the questions related to trust that might be running through the patients head for example; can they trust the GPs information system? For example, how does one know that the information system that is used by the GP has been developed with security in mind? The patients may be apprehensive that so much of their personal information is at effortless access on the information system, hence the patient may be averse to providing information because of such simple access and they are not convinced of the level of security of the information system. They also may be sceptical about the reliability of the system and how their personal details are stored. They may worry that if the information that is held on them is inaccurate, then wrong decisions might be taken by the GP. In order to develop a usable information system is it important to fully understand the environment in which the system will be placed, and most importantly understand all the various implications that might affect the trust not only on the information system but also on its users. Therefore, it is important that an ontological analysis takes place to assist information system developers in understanding the answers to the above questions. Our ontology is able to capture all these issues. For example, for the above simple example, a number of concepts could be employed from our ontology to enable information system developers to introduce a number of features on the system that will that will help to balance the trust related issues that are imposed by the environment of the system.

4. Related Work

There is literature that describes a number of research works related to trust models (Li, 2004; Abdul-Rahman, 2000; Maarof, 2002; Purser, 2001; Carbone, 2003) and methodologies for considering some trust

aspects (Yu, 2001; Mouratidis, 2002; Kethers, 2005; Cams and the Department of Commerce and Trade, 2003; Alberts, 2003; Mayer, 2007; Stolen, 2002). Such works, although important they are not directly related to our efforts to provide an ontological foundation for trust. Closer to our work, is an effort to define trust related ontology. Such efforts have concluded in a number of ontologies focused on security (Kim, 2005; Simmonds, 2004; Mouratidis, 2003) trust (Viljanen, 2005); and risk (Cuske, 2005). Other trust related concepts, such as reputation and privacy, although might have been considered partially in some ontological efforts (Golbeck, 2004; Chang, 2005), they have no corresponding ontologies. However, an important limitation of these ontologies is the fact that they are independent. In other words, they do not consider trust and its related concepts but they are focused on some of the concepts. 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 have not been incorporated, therefore causing the sharing constraint of the trust related data. On the other hand, 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 authors argue for the need for further ontologies to address issues which have not been addressed before such as 'privacy policies, access control and survivability'. It is mentioned in (Cuske, 2005) that 'an extension of the technology risk ontology's scope is feasible, e.g. by including risk measurement'. The following table summarises the various ontologies proposed for trust and its related concepts and it demonstrates what concepts are considered by which ontology.

Ontology	Initial Trust	Trust	Reputation	Security	Risk	Privacy
Ontology of Trust (Viljanen, 2005)		*	*		*	
NRL Security Ontology (Kim *et al*, 2005)				*		
Technology Risk Ontology (Cuske, 2005)					*	
Network Security Attacks Ontology (Simmonds *et al*, 2004)				*		
Functional Ontology of Reputation (Casare, 2004)			*			
Security Incident Ontology (Martimianno)				*	*	
Secure Tropos ontology (Mouratidis, 2003)				*		

Table 6. Ontology Alignment Table

As it can be seen from the above table, we are lacking an ontology that will consider trust and its related concepts in a unified ontological framework. This was described in the previous section titled, The Structure of the Ontology.

It has been mentioned at the start of this section that currently there are many ontologies obtainable to individuals, some have concepts which have a direct link to trust, however they are included in their own independent ontologies, not collectively. It is important to put them into one communal ontology so all the concepts stay in concert. It can be understood that one can put together the related concepts respective ontologies together however, not all the concepts that are in the ontology are to be included within our trust ontology, further proving the originality of our ontology.

5. Conclusion and Future Work

In this paper we have argued for the need to produce a trust ontology that will include a

number of trust related concepts. Our argument is consistent with a number of arguments presented in the literature. We have reviewed a number of related works and we have identified a number of important limitations. To overcome these limitations we have concentrated our efforts in developing a novel ontology that considers trust and its related concepts in one ontological framework. We have also illustrated the development of such ontology by focusing, due to page limitations, to the development of one of the ontology's concept, initial trust. We have also illustrated with the aid of a case study from the health sector how our ontology can assist information systems developers to analyse a number of trust issues related to the environment of a potential information system. However, our work is not complete. We are aiming to formalise our ontological framework and apply it in full to a complex case study that will help to evaluate the formalisation.

6. 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.

7. References

Abdul-Rahman, A., Hailes, S (2000) Supporting Trust in Virtual Communities. *In Proceedings of the Hawaii International Conference on System Sciences 33.* Maui, Hawaii.

Alberts, C., Dorofee, A., Stevens, J., Woody, C (2003) Introduction to the OCTAVE Approach. *Software Engineering Institute.* Pittsburgh, PA, Carnegie Mellon University.

Cams and the Department of Commerce and Trade (2003) A Security Management Framework for Online Services

Carbone, M., Nie;sem, M., Sassone, V (2003) A Formal Model for Trust in Dynamic Networks. *BRICS Report RS-03-4*.

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 (HICSS'03)*. Hawaii.

Cuske, C., Korthaus, A., Seedorf, S., Tomvzyk, 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., Gomez-Perez, A (2002) Deliverable 1.4: A Survey on Methodologies for Developing, Maintaining, Integrating, Evaluating and Reengineering Ontologies.

Fernandez-Lopez, M. (2002) Deliverable 1.3: A Survey on Ontology Tools.

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., Fernandez-Lopez & Corcho, O. (2004) *Ontological Engineering*, Springer-Verlag.

Jomes, D., Bench-Capon, T. & Visser, P (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.

Josang, A., Ismail, R., and Boyd, C (2007) A Survey of Trust and Reputation Systems for Online Service Provision. *Decision Support Systems,* 43(2)**,** pages 618-644.

Josang, A., Presti, SL (2004a) Analysing the Relationship Between Risk and Trust. IN DIMITRAKOS, T. (Ed.) *Proceedings of the Second International Conference on Trust Management.* Oxford.

Josang,, A., Patton, MA (2004b) Technologies for Trust in Electronic Commerce. *Electronic Commerce Research Journal,* 4**,** pp. 9-21.

Kethers, S. E. A. (2005) Modelling Trust Relationships in a Healthcare Network: Experiences with the TCD Framework. *In Proceedings of the Thirteenth European Conference on Information Systems.* Regensburg, Germany.

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

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

Li, X., Valacich, J.S., Hess, T.J. (2004) Predicting User Trust in Information Systems: A Comparison of Competing Trust Models. *The Proceedings of the 37th Hawaii International Conference on Systems Sciences* Hawaii.

Lo Presti, S., Cusack, M., Booth, C (2003) Deliverable WP2-01 - Trust Issues in Pervasive Environments. QinetiQ & the University of Southampton.

Maarof, M. A., Krishna, K (2002) A Hybrid Trust Management Model For MAS Based. Information Security Group, Faculty of Computer Science and Information System University of Technology Malaysia, 81310 Skudai, Johor.

Mayer, N., Heymans, P., Matulevicius, R (2007) Design of a Modelling Language for Information System Security Risk Management. *1st International Conference on Research Challenges in Information Science (RCIS 2007).* Ouarzazate, Morocco.

Mayer, N., Rifaut, A., Dubois, E (2005) Towards a Risk-Based Security Requirements Engineering Framework. *11th International Workshop on Requirements Engineering: Foundation for Software Quality (REFSQ'05), in conjunction with CAiSE'05.* Porto, Portugal.

McRobb, S., Farmer, R (2002) *Object Orientated Systems Analysis and Design Using UML*, McGraw Hill Education.

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

Mouratidis, H., Giorgini, P., Mansoon, G (2005) When Security Meets Software Engineering: A Case Of Modelling Secure Information Systems. *Information Systems,* 30**,** pp. 609-629.

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

Mouratidis, H., Giorgini, P., Manson, G., Philip, I (2002) Using Tropos methodology to Model an Integrated Health Assessment System. *Proceedings of the 4th International Bi-*

Conference Workshop on Agent-Oriented Information Systems (AOIS-2002). Toronto-Ontario.

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

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

Purser, S. (2001) A Simple Graphical Tool for Modelling Trust. *Computers & Security,* 20**,** 479-484.

Simmonds, A., Sandilands, P., Ekert, L.V (2004) An Ontology for Network Security Attacks. IN MANANDHARM S., A., J., DESAI, U., OYANGI, Y., TALUKDER, A. (Ed.) *Lecture Notes in Computer Science.* Kathmandu, Nepal, Springer Berlin / Heidelberg

Stolen, N, K. (2002) Model-Based Risk Assessment - the CORAS Approach. *In proceedings of the First iTrust Workshop*
Sutcliffe, A. (2006) Trust: From Cognition to Conceptual Models and Design. IN DUBOIS, E., POHL, K (Ed.) *18th International Conference, CAiSE 2006, June 5-9, 2006 Proceedings.* Luxembourg, Luxembourg, Springer-Verlag Berlin Heidelberg

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. IN VERLAG, S. (Ed.) *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, LM (2002) Designing for Privacy and Other Computing Requirements. *2nd Symposium on Requirements Engineering for Information Security.* Raleigh, North Carolina.