# Towards an Ontology of Trust

Lea Viljanen

University of Helsinki, Department of Computer Science
Lea.Viljanen@cs.helsinki.fi

**Abstract.** Trust is a fundamental factor when people are interacting with each other, hence it is natural that trust has been researched also in relation to applications and agents. However, there is no single definition of trust that everybody would share. This, in turn, has caused a multitude of formal or computational trust models to emerge to enable trust use and dependence in applications. Since the field is so diverse, there also exists a confusion of terminology, where similar concepts have different names and, what is more disturbing, same terms are also used for different concepts. To organize the research models in a new and more structured way, this paper surveys and classifies thirteen computational trust models by the trust decision input factors. This analysis is used to create a new comprehensive ontology for trust to facilitate interaction between business systems.

## 1 Introduction

Trust, trust models and trust management systems have been under a lot of research in recent years. In the field of computing it is not sufficient to just define trust: for automation the concept of trust must be represented by a trust model, which can be utilized by systems enabling business interaction. Here we define a trust model to be the formal or computational realization of a trust definition, verbal or implicit. The word computational is used here loosely, meaning a model that can be utilized by computer applications. It is important to note that the models are by necessity simplifications of the complexity of trust and different models simplify differently.

Since there is no universal definition of trust, the developed models and systems relying on those models are very different in both verbal and formal trust definitions, and also in the used vocabulary. Therefore, it is beneficial to survey recent work in this area, classify the models according to their trust input factors and to develop a partial ontology. A trust ontology enables systems with different trust models to share trust relationship information and information on how this trust relationship has been formed. This is crucial in today's digital business, where different organizations with differing infrastructure must co-operate to utilize networked services.

This analysis focuses on only one aspect of trust, information to be utilized by the trust decision process. However, there are three distinct problem areas around trust. The first one is to define the facts that support trust, the second is how to find the appropriate rules to derive consequences of a set of assumptions about trust, and the third is how to use information about trust to take decisions [9]. This analysis focuses clearly on the first problem, i.e. finding a maximal set of support facts. Therefore many important trust research areas, for example reasoning logics or negotiation protocols, are not part of this analysis.

S. Katsikas, J. López, G. Pernul (Eds.): TrustBus 2005, LNCS 3592, pp. 175–184, 2005.

## 2 On Trust and Trust Research

Trust has been a very awkward concept in computer science since it is silently embedded in many aspects of human behaviour and it is in its very nature quite subjective. However, since trust is a part of the basic decision making framework for humans, it has also some interest from the computer systems point of view.

### 2.1 Trust Characteristics

There have been many definitions of trust, below are examples from Diego Gambetta and Audun Jøsang:

> trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action [12].
>
> Trust in a passionate entity is the belief that it will behave without malicious intent ... Trust in a rational entity is the belief that it will resist malicious manipulation by a passionate entity [15].

These definitions are very different and use widely different vocabulary. How can the models built on these definitions interact in any way? Before we can attempt an answer, some characteristics of trust need to be explored. Since trust is subjective, we must assume a role of some subject and evaluate the trust from that particular perspective. From this the lack of global trust is evident, i.e. there are no entities everybody trusts. From this basic property, other natural characteristics follow:

- Trust is not symmetric. If ”Alice trusts Bob”, it does not follow that ”Bob trusts Alice”.
- Trust is not distributive. If “Alice trusts (Bob and Carol)”, it does not follow that “(Alice trusts Bob) and (Alice trusts Carol)”.
- Trust is not associative, since the trust-operator does not map from entities to entities. Therefore “(Alice trusts Bob) trusts Carol” is not a valid trust expression. However, “Alice trusts (Bob trusts Carol)” is a possibility.
- Trust is not inherently transitive. If “Alice trusts Bob” and “Bob trusts Carol”, it does not automatically follow that “Alice trusts Carol”.

### 2.2 Trust Model Research

Early attempts to formalise trust for computer use have been in the context of authentication. Yahalom et al. developed a trust model to be used in authentication scenarios [20]. One of the earliest attempts to define trust from the general and computational point of view was Stephen Marsh’s thesis [16], which drew input from the sociological trust research. After that several interesting trust models and also systems, such as PolicyMaker [4], KeyNote [3] and REFEREE [8] have emerged. Around that time also

Abdul-Rahman et al. [1], Daniel Essin [11] and Audun Jøsang [15] described their trust concepts and models.

In recent years the focus has been on more comprehensive and concrete systems having wider trust management elements, such as Poblano [7], Free Haven [10], SULTAN [14], TERM [2] and SECURE [5,6]. But since the applicability of trust has been widened to cover more than authentication and authorization, they do not necessarily use the same terminology or basic components. Additionally, some models do not focus on general trust management, but have tried to explore trust in various application domains, such as peer-to-peer networking or web applications.

These thirteen models span a time frame of ten years of trust model research and form a comprehensive set of research models. Thus this set is used for the actual factor analysis.

## 3 Taxonomy of Trust Models

One of the key differentiating elements in trust models is the list of factors required or used in the trust evaluation. Because of this factor diversity, it is impossible to give a simple taxonomy where each model sits squarely only in one classification box along this axis. Instead, a classification of factors has been developed and each model can be desribed by what set of factors it is using or, in our terminology, is aware of. A summary is shown in Figure 1.

### 3.1 Identity-Aware Models

All reviewed systems are identity-aware, i.e. they assume to have some identifying information on the target of the trust evaluation. This identity awareness does not require knowing the real name or other globally unique information of the communicating principal. In some models it is quite sufficient that the identity is only locally unique and temporally sufficiently stable so that it aids in recognizing the same entity in this system over time. There are models that use globally unique identities or locally unique

| MODEL | Identity | Action | Business value | Capability | Competence | Confidence | Context | History | 3rd party |
|---|---|---|---|---|---|---|---|---|---|
| Abdul-Rahman | X | X | | | | | | | X |
| Essin | X | X | X | X | X | | X | X | X |
| Free Haven | X | | | | X | X | | | X |
| Jøsang | X | | | | | X | | | |
| KeyNote | X | X | | | | | | | X |
| Marsh | X | X | X | | X | | | X | |
| Poblano | X | | X | | X | X | | | |
| PolicyMaker | X | X | | | | | X | | X |
| REFEREE | X | X | | | | | | | X |
| Sultan | X | X | | | | | | | X |
| TERM | X | X | | | | X | | X | X |
| Secure | X | X | | | | | | X | X |
| Yahalom et al | X | X | | | | | | | X |

**Fig. 1.** Trust model input factor summary

identities. For example, the Poblano system uses *peerID*, which needs to be unique across the universe of peers. An example of local identities can be found in the work of Abdul-Rahman et al.

### 3.2 Action-Aware Models

Most trust models have noticed that there is an action component to trust. That is, the actual trust evaluation and decision depends on what the target of our trust is trying to do in or with our system or for what purpose we are trusting the target. This is very intuitive, as we may trust one party to relay our messages but not to transfer any money. This is also reflected in the definition by Gambetta in Chapter 2 above. On the other hand, the action component is not always necessary, since there is a concept called *general trust* which is an unqualified trust towards a principal [16].

In action-aware models the set of actions can be closed or open. A closed set is a set of pre-defined actions the model supports and no others can be defined by organizations using the model. An open set of actions means that the model offers a way of defining at least some of the actions or does not restrict them to a particular set.

This concept has many names in the actual models. PolicyMaker, REFEREE and KeyNote call this *action* and Abdul-Rahman et al. have a *trust category*. Yahalom et al. use a closed set of *trust classes* for which they trust a certain principal. SULTAN uses the name *context*, but in its core the the definition is about actions and action sets. Similarly, the SECURE project uses context in the meaning of action. Essin has the concept of *activity*, although it is not used in the trust evaluation directly, but as a subcomponent in determining the capability of trust subject and subject reputation.

However, not all models use the action factor explicitly. Some specialized systems, for example Poblano and Free Haven, use the trust valuation in relation to data content received from a network peer. There the actions are implicit in the system definition, but since there is only the one basic action type and the action set is closed, Poblano or Free Haven systems are not considered action-aware.

Marsh describes a *situation*, which is a point of time relative to a specific agent, i.e. the principal evaluating trust. This definition includes the actions the other principals are attempting, therefore Marsh's model is action-aware. The TERM system has no action concept as such, but trust calculations are related to *roles* in role-based access control. There are two roles, an access role and a testifying role, so the system has two predefined actions. Hence it is action-aware, although the action set is closed.

### 3.3 Business Value Awareness

Between people trust implies potential loss and also potential benefit. In several models there are concepts called *risk*, *benefit* or *value*. These are all associated with a particular action and try to give impression on how the action can help us or how the misplaced trust can hurt us. Risk is the most commonly modeled business value element. However, to understand the full impact of the attempted action, risk needs to be balanced against the potential benefits or value of the action. We combine these under the common concept of *business value*, since all these concepts try to model the potential impact, positive or negative, of the attempted operation.

Marsh is using three separate business value concepts: utility, importance and risk. Utility is a measurable benefit, importance a subjective valuation of the importance of the action. These both are used in evaluating situational trust, i.e. trust in a specific situation or action. Risk is used in determining the co-operation threshold, i.e. whether to actually engage in the action in a particular situation.

The model by Essin also uses several business value factors. He uses the concept of *valuation* as the cost of the resources or assets affected by the action. He also uses *stake* which is the degree to which the entity(s) proposing to engage in the activity has a vested interest in the outcome. Stake tries to measure the level of commitment for this action and thus it is quite close to the concept of importance. He also uses the concepts of risk and benefit, although his model combines these to a single risk/benefit set.

In the Poblano P2P system, risk is a statistically computed metric of peer accessibility and performance, both viewed technically. Here the considered risk is of the type "risk of not getting the information" instead of any loss of data or money. This is however, well within the defined use of "risk", so Poblano is business value aware. Poblano also uses *importance*, which is the importance in engaging in the activity, when calculating the co-operation threshold.

The SECURE model does not have risk as part of the formal trust model, although the resulting system has an added risk and cost/benefit analysis as part of the trust evaluation. Therefore the model itself is not business-value aware.

### 3.4 Competence-Aware Models

One type of trust decision factor is information on the competence of the subject with regard to performing a particular action. When human clients are considered, this is an important decision factor, but with automated clients at least some degree of technical competence in following the specification should be assumed. Therefore this factor is not very common in the reviewed models.

Competence is considered by Marsh in calculating the co-operation threshold based on trust. The SULTAN model uses competence as a factor in their verbal trust definition, but surprisingly does not include it in the computational model. This concept of ability to perform a task is called *capability* by Essin. He defines capability as measurable expertise that the entity possesses about the activity, i.e. competence in this common vocabulary.

One interesting variant of this is lifting the competence evaluation from the technical to the semantic level. The Poblano model has a concept of *CodatConfidence*, which is a measure of semantic experience, i.e. the system's competence in providing us with relevant information. Similarly, the Free Haven system has a concept of *metatrust*, which signals that the data received from a node is indeed valuable information. For example, if the Free Haven system agrees with a recommendation from a third party, the third party metatrust is incremented.

### 3.5 Capability-Aware Models

Capability has a dual meaning in the security and trust research. On one hand, capability is considered synonymous with competence, i.e. evaluating the peer's ability to perform

a certain task. On the other hand, a capability has a very specialized meaning in the field of security as a token given to a peer to access a resource. We differentiate between these two concepts and here define capability as a form of an access granting token.

This latter form is also used by Essin. In addition to the capability as competence definition, he defines capability also as demonstrable access and authority necessary to act [11]. This is capability in this second sense.

### 3.6 Confidence-Aware Models

As input for the trust calculation can be received from multiple sources, sometimes also as external recommendations or reputation, we may also have uncertainty associated with trust or the trust input factors. The concept of *confidence* reflects this uncertainty, although in the actual models this concept has many names.

The TERM model uses the concept of an *opinion*, meaning how much the calculating TERM server believes the trust statement. The Poblano system also uses a confidence value, *PeerConfidence*, in determining whether the trust subject is able to co-operate and thus being trustworthy.

Confidence can also relate to only one of the trust input factors. Essin uses the term *certainty* that the true identity of the trust subject is known. The Free Haven system uses the concept of *confidence rating*, which is used as a measure of how fast or slow external recommendations change our trust value in regards of that particular entity.

### 3.7 Context-Aware Models

The trust evaluation may depend on the evaluating system internal or external status at that particular point of time, i.e. context. If, for example, the organization firewall is experiencing heavy port scanning activity, it may be sensible to lower the trust valuation on all or some principals to limit exposure to potentially malicious activity.

Interestingly enough, this is not a very widely used factor. Essin uses it as a subfactor in determining the action valuation and subject stake in the action. In PolicyMaker, the policy is defined in an interpreted programming language and it thus can obtain some context information. The set of local policies are considered the context under which the trust is evaluated.

The SECURE model also defines trust via a policy construct. Theoretically it may be possible to include context information in the policy, but since this option is not explored in their work, SECURE is not classified here as context-aware. Neither is the SULTAN model since it uses context to mean the action to be performed (see Chapter 3.2).

### 3.8 History Awareness

When people interact, one of the key components in our trust evaluation is the trustee past behaviour or track record. This can be modeled using vocabulary like *experience* or *evidence* or *local reputation*.

Reputation is opinion or view of one about something [18]. There can be two types of reputation: subjective reputation is reputation calculated directly from the trustor

direct experiences and external reputation is reputation received from third parties. The former type of subjective reputation is considered in this history awareness category.

Essin uses the word *reputation* but does not differentiate between subjective and external reputation. The Marsh model also includes past history data by including the trust values in all previous similar situations in the situational trust evaluation.

The TERM model includes a concept called *direct experience*. It is used by the system to evaluate trust opinions, although it is not formally defined. The SECURE model is very flexible so that it can also use history information if required by making history part of the local trust policy.

### 3.9 Third Party Awareness

A trust model can be open or closed. A closed model does not take into account any input from outside the actors involved in the trust evaluation. Open trust models accept information from third parties. This information can be in the form of external reputation, recommendations or even delegated decision making.

In addition to subjective reputation discussed above with regards to history-awareness, we also have external reputation. For example, we may belong to a community, which has a common reputation service with shared ontology and receive reputation information from that external source. This external type of reputation is also considered in this third party awareness category. This is not a widely used feature. In the Essin model there is reputation, either generally or bound to a specific action, as a component in the trust evaluation [11].

Recommendations are conceptually somewhat difficult. Since trust is not transitive, recommendations should not be taken directly as trust. However, third party recommendations can be an influencing factor when deciding about trust. Recommendations are considered by many models. For example the models by Yahalom et al. and Abdul-Rahman et al. use them. The SULTAN model and system also uses recommendations as a basis for new trust relationships. The Free Haven system uses the word of *referral* instead of a recommendation. The TERM model also uses recommendations, although it is said that they are used indirectly because of the transitivity issue.

Delegated decision making is not very common. The SECURE model is third party aware because it can handle *delegation* where a principal can refer to another principal's trust information.

External information can be carried in the form of a credential, which is simply a statement, purportedly made by some speaker [8]. Thus a credential is not a semantic information category, but a technical one. A credential can carry identity information, subject properties, reputation data or even capabilities. Therefore we do not categorize models as credential-aware, but the classifying factor is the semantic category such as identity or a particular property. The TERM model calls these credentials *evidence*. In some systems credentials can also be executable programs. This is true in the Keynote and PolicyMaker systems, where these programs are called *assertions*. In the REFEREE system a credential is also a program that examines the inital statements passed to it and derives additional statements.

## 4 Towards an Ontology of Trust

The trust model analysis above gives us a wide view on how trust has been modeled in previous research. This information makes it possible to create a domain ontology, i.e. a description of the concepts and relationships in the trust domain. Trust ontologies have been made before [13], but not based on a comprehensive analysis. This background analysis makes this new ontology widely usable and compatible with previous research models. Therefore this ontology can facilitate not only discussion across trust models, but also interoperability across different trust systems in autonomous applications.

Because different trust models emphasize different features in the concept and abstract away others, it is assumed that a union of these emphasized features across all models provides us with a maximal list of trust input factors. Based on this maximal list we formulate the following ontological structure.

First of all, trust is a relationship between two principals, the subject, trustor, and the target, trustee. The trust between trustor and trustee may depend on the the action trustor is attempting. The action may have a score of business value properties attached to it. The trustor also may use context information or history data to help in the trust

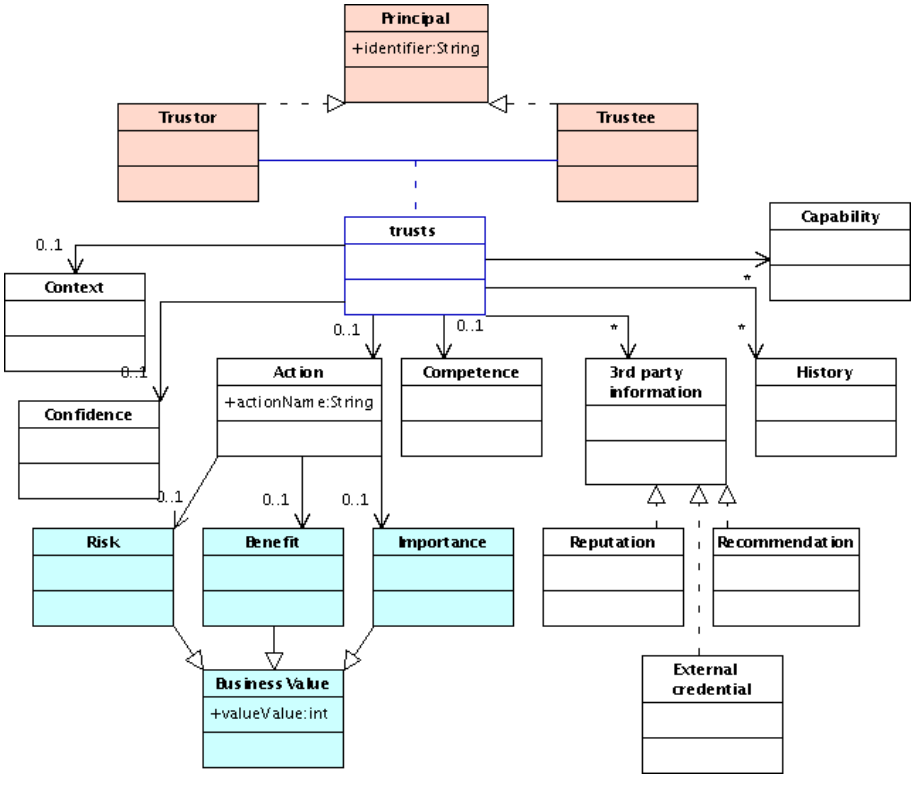


**Fig. 2.** Trust as a UML diagram

evaluation. The trust can also depend on the peer competence. Additionally, there can be an element of confidence attached to the trust relationship. There can also be a set of third party opinions in the form of reputation information, recommendations or credentials that influence the trust evaluation.

A UML diagram modeling these relationships in trust is presented in Figure 2. The model in the picture is a level 1 metamodel, i.e. it models a particular application domain, trust, which is represented in a UML modeling system [17]. An actual population of this model, such as defining trust relationships between concrete principals, is a level 0 metamodel and can be created utilizing this level 1 model.

The conceptualization can also be described in the OWL Web Ontology language [19]. Trust can easily be described as a trustor property used to list all trusted principals. This is a good option for describing general trust, i.e. trust not linked to a specific action. As can be seen from the general characteristics of trust discussed in Chapter 2, this property can not be a transitive or symmetric property in the OWL model. However, this is not enough for situational trust, i.e. trust which is linked to a particular action. Therefore we transform the UML model in Figure 2 to an ontology expressed in the OWL language using to ontology definition metamodel guidelines [17]. The resulting OWL file can be obtained from the URL `http://tinyurl.com/4pw5p`.

## 5 Conclusion

Thirteen very different computational trust models were analyzed on what information they require for the trust decision. This has accomplished two important goals. First, a common vocabulary for describing facts that are considered for trust calculation in the reviewed trust models was created. The models can be classified as identity-aware, action-aware, business value aware, capability-aware, competence-aware, confidence-aware, context-aware, history-aware and third-party aware in their input factors. This new vocabulary facilitates communication when models use different terminology for similar concepts.

Secondly, based on this analysis, the paper presents a new level 1 UML metamodel for the trust concept and link to the corresponding OWL ontology. This ontology can be utilized in digital business in several ways. First of all, it supports trust model sharing between organizations, although the sharing of the trust relationship data may be restricted because of privacy or security reasons. Secondly, new business applications may emerge that automatically process and integrate trust information to be usable in business scenarios. One key area could be single sign on systems or Web Services business communities, which require trust to offer services.

## Acknowledgements

This article is based on work performed in the TuBE project (Trust based on evidence) at the Department of Computer Science at the University of Helsinki. The TuBE project is funded by TEKES, Nixu Oy and StoneSoft Oyj.

## References


1. A. Abdul-Rahman and S. Hailes. A distributed trust model. In *Proceedings of the 1997 New Security Paradigms Workshop*, pages 48–60. ACM, 1997.
2. B. Bhargava and Y. Zhong. Authorization based on evidence and trust. In *Proceedings of the Data Warehouse and Knowledge Management Conference (DaWak), France*, 2002.
3. M. Blaze, J. Feigenbaum, and A. D. Keromytis. KeyNote: Trust management for public-key infrastructures (position paper). In *Proceedings of the 6th International Workshop on Security Protocols*, volume LNCS 1550/1998, pages 59 – 63. Springer-Verlag, Apr. 1998.
4. M. Blaze, J. Feigenbaum, and J. Lacy. Decentralized trust management. In *Proceedings of the IEEE Symposium on Security and Privacy*. IEEE, May 1996.
5. V. Cahill, E. Gray, J.-M. Seigneur, C. Jensen, Y. Chen, B. Shand, N. Dimmock, A. Twigg, J. Bacon, C. English, W. Wagealla, S. Terzis, P. Nixon, G. D. M. Serugendo, C. Bryce, M. Carbone, K. Krukow, and M. Nielsen. Using trust for secure collaboration in uncertain environments. *Pervasive Computing*, 2(3):52–61, Aug. 2003.
6. M. Carbone, M. Nielsen, and V. Sassone. A formal model for trust in dynamic networks. In *Proceedings of the First International Conference on Software Engineering and Formal Methods*, pages 54–61. IEEE Computer Society, Sept. 2003.
7. R. Chen and W. Yeager. Poblano a distributed trust model for peer-to-peer networks. Technical paper, Sun Microsystems, 2000.
8. Y.-H. Chu, J. Feigenbaum, B. LaMacchia, P. Resnick, and M. Strauss. REFEREE: Trust management for Web applications. *Computer Networks and ISDN Systems*, 29(8–13):953–964, 1997.
9. R. Demolombe. Reasoning about trust: A formal logical framework. In *Proceedings of the Second International Conference on Trust Management, iTrust 2004, LNCS 2995*, pages 291–303. Springer-Verlag, 2004.
10. R. Dingledine. The Free Haven project: Design and deployment of an anonymous secure data haven. Master's thesis, MIT, 2000.
11. D. J. Essin. Patterns of trust and policy. In *Proceedings of the 1997 New Security Paradigms Workshop*. ACM Press, 1997.
12. D. Gambetta. Can we trust trust? *Trust: Making and Breaking Cooperative Relations*, pages 213–237, 2000. Electronic edition.
13. J. Golbeck, B. Parsia, and J. Hendler. Trust networks on the semantic web. In *Proceedings of Seventh International Workshop on Cooperative Intelligent Agents CIA'03*, Helsinki, Finland, August 2003.
14. T. Grandison and M. Sloman. Specifying and analysing trust for internet applications. In *Proceedings of the 2nd IFIP Conference on e-Commerce, e-Business, e-Government I3e2002, Lisbon, Portugal*, Oct. 2002.
15. A. Jøsang. The right type of trust for computer networks. In *Proceedings of the ACM New Security Paradigms Workshop*. ACM, 1996.
16. S. Marsh. *Formalising Trust as a Computational Concept*. PhD thesis, Department of Mathematics and Computer Science, University of Stirling, 1994.
17. OMG. OWL full and UML 2.0 compared, 2004.
18. J. Sabater and C. Sierra. REGRET: A reputation model for gregarious societies. Research Report 2000-06, Institut d'Investigacio i Intelligencia Artificial, 2000.
19. W3C. OWL web ontology language overview, 2004. W3C Recommendation.
20. R. Yahalom, B. Klein, and T. Beth. Trust relationships in secure systems - a distributed authentication perspective. In *Proceedings of the 1993 IEEE Symposium on Research in Security and Privacy*, pages 150–164. IEEE Computer Society, 1993.