F. Moyano, C. Fernandez-Gago, and J. Lopez, "A Conceptual Framework for Trust Models", *9th International Conference on Trust, Privacy & Security in Digital Business (TrustBus 2012)*, LNCS vol. 7449, pp. 93-104, 2012.
http://doi.org/10.1007/978-3-642-32287-7
NICS Lab. Publications: https://www.nics.uma.es/publications

# A Conceptual Framework for Trust Models*

Francisco Moyano, Carmen Fernandez-Gago, Javier Lopez
NICS
www.nics.uma.es
University of Malaga,
Spain
{moyano,mcgago,jlm}@lcc.uma.es

**Abstract**

During the last twenty years, a huge amount of trust and reputation models have been proposed, each of them with their own particularities and targeting different domains. While much effort has been made in defining ever-increasing complex models, little attention has been paid to abstract away the particularities of these models into a common set of easily understandable concepts. We propose a conceptual framework for computational trust models that will be used for analyzing their features and for comparing heterogeneous and relevant trust models.

## 1 Introduction

The concept of trust in Computer Science derives from the concept in sociological, psychological and economical environments. The definition of trust is not unique. It may vary depending on the context and the purpose where it is going to be used. Despite it is admitted of paramount importance when considering systems security, a standard definition of trust has not been provided yet. However, it is wide accepted that trust might assist decision-making processes such as those involved in access control schemes.

Reputation and trust are related concepts, although they have different meanings. Reputation is defined by the Concise Oxford Dictionary as 'what is generally said or believed about a person or the character or standing of a thing' while trust is defined as 'the firm belief in the reliability or truth or strength of an entity'. From these definitions we can infer that the concept of reputation is more objective compared to the concept of trust. Actually, both

*This work has been partially funded by the European Commission through the FP7/2007-2013 project NESSoS (www.nessos-project.eu) under grant agreement number 256980, and by the Spanish Ministry of Science and Innovation through the research project ARES (CSD2007-00004) and SPRINT (TIN2009-09237). The first author is funded by the Spanish Ministry of Education through the National F.P.U. Program.

Table 1: Contributions mainly considered while the elaboration of the conceptual framework for trust

| | 2000 | 2005 | 2006 | 2007 | 2008 | 2009 | 2011 |
|---|---|---|---|---|---|---|---|
| Surveys | [7] | [24] [19] [21] | | [10] [2] | [27] | | [28] |
| Others | | | [25] | | | [11] | [22] |

concepts are strongly related as reputation can be used as a means to determine whether an entity can trust another entity [10]. Trust and reputation services assure the trustworthiness on the entities that take part of any system, reducing the uncertainty during the interactions of such entities.

The origins of computational trust date back to the nineties, when Marsh [13] analyzed social and psychological factors that have an influence on trust and replicated this concept in a computational setting. A few years later, Blaze [3] identified trust management as a way to leverage and unify authentication and access control in distributed settings. These two early contributions show that trust can be conceived in different ways and for different purposes. From these seminal works onwards, different types of trust models have been proposed, with different purposes and targeting different settings. A trust model comprises the set of rules and languages for deriving trust among entities in an automatic or semi-automatic way.

This heterogeneity often leads to confusion as one might easily lose the most relevant concepts that underlie these trust models. This is precisely the motivation for this work. We aim to shed light on computational trust concepts and how they relate to each other. By trust concept or trust-related concept, we refer to any notion that has a high relevance, according to how frequently the notion arises in existing trust models. Our intention is to build the foundations towards the design of a development framework that supports the acommodation of heterogeneous trust and reputation models. We advocate that the identification of the main trust-related concepts can help in the design of such a framework.

Note that, due to space limitations, it is out of the scope of this paper to provide details on existing trust models. For this, the reader is advised to read the surveys considered in this work (see Table 1). We intend to provide the main concepts that are common in most trust management models. In order to achieve this, we have reviewed some of the most relevant surveys that have been written during the last years in the area of trust management. We also considered other relevant works that abstract away from the particularities of different trust models in order to elicitate their commonalities. These works have assisted us in making the following contributions: (i) identification of trust concepts and how they relate to each other; (ii) categorization of trust models into different types; (iii) and elaboration of a conceptual framework onto which it is possible to compare different types of trust models, building on the concepts and relations previously identified.

The rest of the paper is organized as follows. Section 2 explores several definitions of trust provided during the last years, and it extracts the most important concepts related to it. In Section 3, we categorize trust models and raise their most relevant concepts. We elaborate on these concepts in Section 4 in order to build a conceptual framework onto which to compare some relevant trust models. Finally, Section 5 concludes the paper and provides lines of future research.

## 2 Trust Definitions Concepts

Many definitions of trust have been provided along the years. This is due to the complexity of this concept, which spans across several areas such as psychology, sociology, economics, law, and more recently, computer science. The vagueness of this term is well represented by the statement "trust is less confident than know, but also more confident than hope" [16]. In this section, we plan to revise the definitions that have been mostly considered in the literature when designing computational trust and reputation models. We advocate that making an effort to understand this term and its implications is crucial if we want to implement meaningful models. On the other hand, understanding trust and reputation allows for a better trust-related concepts identification as well as for building a more comprehensive conceptual framework for trust models comparison. Definitions are presented in chronological order.

Gambetta [6] defines trust as "a particular level of the subjective probability with which an agent will perform a particular action [...] in a context in which it affects our own action". McKnight and Chervany [15] explain that trust is "the extent to which one party is willing to depend on the other party in a given situation with a feeling of relative security, even though negative consequences are possible". For Olmedilla et al. [18], "trust of a party A to a party B for a service X is the measurable belief of A in that B behaves dependably for a specified period within a specified context (in relation to service X)". Ruohomaa and Kutvonen [21] state that trust is "the extent to which one party is willing to participate in a given action with a given partner, considering the risks and incentives involved". Finally, Har Yew [8] defines trust as "a particular level of subjective assessment of whether a trustee will exhibit characteristics consistent with the role of the trustee, both before the trustor can monitor such characteristics (or independently of the trustor's capacity ever to be able to monitor it) and in a context in which it affects the trustor's own behavior".

These definitions are used as an input to build the concepts cloud depicted in Figure 1. There are other relevant definitions, apart from those written above, which contributed to this cloud, althought they have not been included due to space limitations. Yet Table 2 summarizes all the definitions considered, which were processed following several rules. A word that appears several times in the same definition is counted just once. We only take into consideration words that mean something by themselves and do not require surrounding words to mean something (e.g. *particular level* does not make sense separatedly). If two words

Table 2: Trust Definitions

| 1988 | 1991 | 1995 | 1996 | 2000 | 2002 | 2005 | 2011 |
|---|---|---|---|---|---|---|---|
| [6] | [4] | [14] | [15] | [7] | [17] | [19] [18] [21] | [28] [8] |

with the same meaning appear either in plural and singular, it is expressed in singular. Dependability is splitted into security and reliability. Party, agent, entity, trustor and trustee are named as entity. Most words are adjectives and nouns, since they are more meaningful without a context than verbs, but some relevant verbs are considered as well. Assessment is used in place of *quantifiable*, *measurable*, *describable* and alike terms. The resulting concepts were introduced in Wordle [1].


Figure 1: Concepts Cloud for Trust Definitions

In a glimpse, the figure reveals that entity is the main concept, and this is obvious, given that trust has no sense if there are neither entities that trust nor entities in which to trust. Context appears as the other big concept since trust is very context-dependent. Other important concepts include imprecise concepts such as subjective, belief, willingness or expectation. They show that trust is strongly related to *uncertainty* about an entity's behaviour. Finally, it is important to note that even though the concept of risk is not explicitly present in all the definitions, a careful reading reveals that it is indeed implicitly considered in almost all of them. As a wrap-up, trust is beneficial in the presence of uncertainty and risk during the interaction of two entities, which are willing to collaborate and to depend on each other.

# 3 Trust Models Concepts

Trust models are very hetereogeneous. This heterogeneity depends on many factors such as the trust definition they use or their application domain. In order to provide a conceptual framework for trust models we first establish a

[1] `http://www.wordle.net/` is a free online tool to generate words clouds

classification of them. However, this task is not straightforward and there are many ways to tackle it. We propose the following classification:

- *Decision Models.* Trust management has its origins in these models [3]. They aim to make more flexible access control decisions, simplifying the two-step authentication and authorization process into a one-step trust decision. *Policy models* and *negotiation models* fall into this category. They build on the notions of policies and credentials, restricting the access to resources by means of policies that specify which credentials are required to access them.

- *Evaluation Models.* These models are often referred to as *computational trust*, which has its origin in the work of Marsh [13]. Their intent is to evaluate the reliability (or other similar attribute) of an entity by measuring certain factors that have an influence on trust in the case of *behaviour models*, or by disseminating trust information along trust chains, as it is the case in *propagation models*. An important sub-type of the former are *reputation models*, in which entities use other entities' opinions about a given entity to evaluate their trust on the latter.

Making a classification is important as it eases the extraction of common features between different classes of models. It is not possible (or better said, it is not useful) to compare policy models such as PolicyMaker [3] with a behaviour model such as eBay's reputation system [20], because their nature and workings are very different. However, it makes sense to extract some common features for all types of models. Each type of model exhibits its own features which allow us to identify the most meaningful ones. This leads in turn to a more consistent comparison framework. For the sake of simplicity, we divide our conceptual framework into three concepts blocks. The first block contains concepts that are applicable to any trust model, independently from its type. The next two blocks gather concepts specific to the types of models identified above.

## 3.1 Common Features

A trust model aims to capture how trust is perceived, computed and transmitted in a computational setting. This setting must have, at least, two entities which have to interact in some way. In any trust setting, an entity plays a role, or even several ones. In the simplest case, these roles are trustor, the entity which places trust, and trustee, the entity on which trust is placed. However, depending on the context and complexity of the model, other roles are possible. For example, an entity can be a witness that informs about its opinion of an entity based on observations or its own experience. Some specializations of trustors and trustees include a requester of a service or resource, the provider of a service or resource, or a trusted third party that issues credentials or gathers feedbacks to compute a centralized reputation score. Once there exist a trustor and a trustee, we say that a trust relationship has been established. In the case of evaluation

models, this relationship is tagged by a trust value. This is further discussed in Sections 3.3.

In any trust model, establishing a trust relationship has a purpose. According to Jøsang et al. [10], a trust purpose is an instantiation of any of the following trust classes identified by Grandison and Sloman [7]: access trust, provision trust, identity trust, and infrastructure trust (considering delegation a sub-class of provision trust). The instantiation is due to the fact that trust is context-dependent, one of the most important properties of trust, since it influences all the other concepts, such as the purpose, the type of entities and the role that they can play. Other factors, in addition to the context, that have an influence on trust are the trustee's subjective and objective properties, and the trustor's subjective and objective properties. The reader is advised to read [27] for examples on these properties.

Note that trust can be also conceived as a strong belief about a given property of the trustee. From a theoretical perspective, there would be no purpose under this trust conception. Yet we are interested in trust models from a more pragmatic perspective. Thus, trust in a given property would eventually assist in making a decision for some purpose. For instance, if an entity believes that another entity is competent to encrypt files, it would select the latter among other candidates less qualified (according to the entity's belief). In this example, the purpose will therefore be the provision of an encryption service (i.e. provision trust).

A trust model also makes some assumptions, such as "entities will provide only fair ratings" or "initial trust values are assumed to exist", and might follow different modeling methods, including mathematic, linguistic and graphic. The resulting conceptual model that gathers these concepts is depicted in Figure 2.

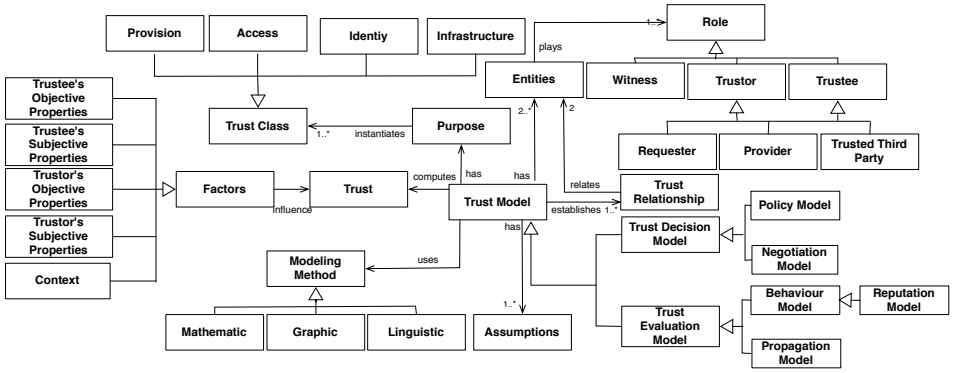


Figure 2: Common Concepts for Trust Models

## 3.2 Concepts for Trust Decision Models

As their name suggests, policy models (e.g. PolicyMaker [3]) use policies, which specify the conditions under which access to a resource is granted. These conditions are usually expressed in terms of credentials, signed logical statements that assert that an entity is which it claims to be, or that it is member of a group. Credentials might have different formats, including X.509 certificates and XML. Another concept of policy models is the compliance checker, in charge of checking whether the credentials satisfy the policies. Policies are written in a policy language. Policy languages used by these models might consider policy conflicts resolution. Likewise, the model might also support the search for a credential through credential chains. Some models also include the required components to verify that a credential is valid.

The other type of trust decision models are negotiation models, being TrustBuilder [26] the first representative implementation of them. Trust negotiation models add a protocol, called *negotiation strategy*, during which two entities perform a step-by-step, negotiation-driven exchange of credentials and policies until they decide whether to trust each other or not. This strategy allows protecting the privacy of the entities as policies and credentials are only revealed when required. A later work [11] supports the implementation of different trust negotiation models. Here the authors state that trust negotiation can use evidence types, which represent information about the negotiation process (e.g. certain steps of the negotiation were already accomplished) and have a purpose (e.g. optimization of the negotiation).

The conceptual model for decision models is depicted in Figure 3.

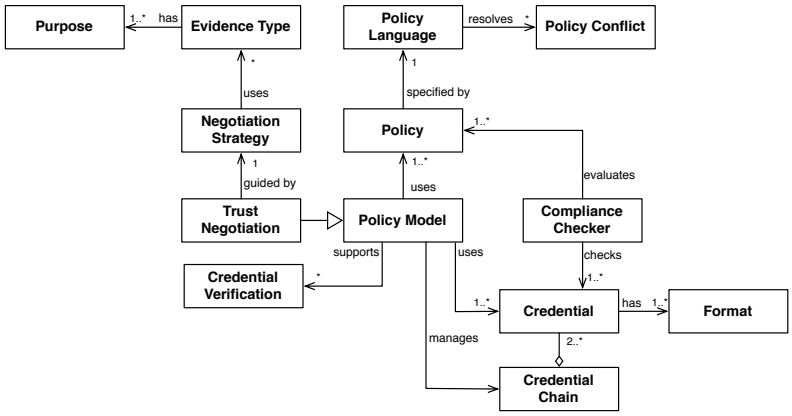


Figure 3: Concepts for Decision Models

## 3.3 Concepts for Trust Evaluation Models

### 3.3.1 Concepts for Behaviour Models

Behaviour models often follow a trust lifecycle with three phases. First, a bootstrapping phase might be required to assign initial trust values to the entities of the system; some other times initial values are assigned. Trust propensity is a concept related to the bootstrapping phase and it refers to the propensity of the model towards high or low trust values in the beginning. Second, monitoring is performed to observe an attribute or set of attributes. Finally, an assessment process is done in order to assign values to the monitored qualities and to aggregate them into a final trust or reputation score.

In behaviour trust, each trust relationship is tagged with a trust value that indicates to what extent the trustor trusts the trustee. This value can be unidimensional or multi-dimensional, and according to Jøsang [10], might have different degrees of objectivity and scope. The former refers to whether the measure comes from an entity's subjective judgement or from assessing the trusted party against some formal criteria. The latter specifies whether the measure is done against one factor or against an average of factors.

Trust values are assigned to relations using a trust assessment process, where trust metrics are used to compute them. Trust metrics use variables, such as risk or utility, and combine them in order to yield a final score for the measured attribute(s). Basic examples of attributes are trust and reputation. Attributes can be more specific, such as "quality of service provider" or "reliability of a seller". Trust metrics use computation engines, which may include simple summation or average engines, continous engines, discrete engines, belief engines, bayesian engines, fuzzy engines or flow engines. Jøsang [10] provides a summary of their features.

The source of information that feeds the metric might come from direct experience (either direct interaction or direct observation), sociological and psychological factors. Reputation models use public trust information from other entities to compose a trust evaluation. Reputation models can be centralized, where there is an entity in charge of collecting and distributing reputation information; or distributed, when there is no such an entity and each one has to maintain a record of trust values for other entities, and send this information to the rest of entities. Regardless of which information source is used to compute the trust value, the model might consider how certain or reliable this information is (e.g. credibility of witnesses), and might also consider the concept of time (e.g. how fresh the trust information is).

Finally, a behaviour model might use a game-theoretic approach (as most existing trust models do), where relationships between entities is emphasized in terms of direct experience, feedbacks, utility, risk, and so forth; or it might be socio-cognitive, where mental models of entities are built to consider beliefs in properties. All the concepts discussed in this section are depicted in Figure 4, together with propagation models concepts, which are described next.

### 3.3.2 Concepts for Propagation Models

Propagation models often assume that several trust relationships have already been established and quantified, although this is not always the case. They aim to create new trust relationships by disseminating the trust values information to other entities. Some models assume that trust is transitive and exploit this property, although transitivity is not, in general, considered as a property that holds for trust [5].

Some behaviour models implement propagation mechanisms. For example, Advocato [12] is a reputation model that allows users of the community to provide a ranking for other users. However, it is also a propagation model, since it allows computing a reputation flow through a network where members are nodes and edges are referrals between nodes.

New trust values are often computed by means of operators, and in several models, we find two of them: a concatenator and an aggregator. The former is used to compute trust along a trust path or chain, whereas the latter aggregates the trust values computed for each path into a final trust value. For example, in [1] the authors use a sequential and a parallel operator in order to compute trust along a path. Subjective logic [9] uses a discounting operator to compute opinions along different trust paths, and a consensus operator to combine them into a final opinion. All the concepts discussed are shown in Figure 4.

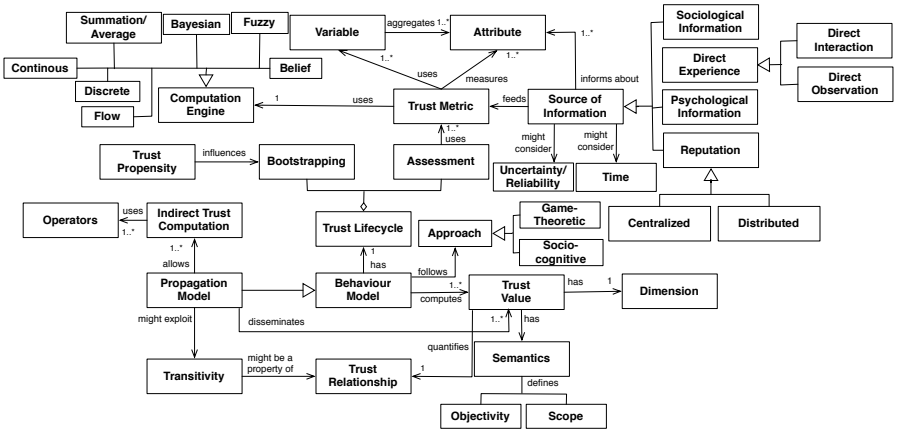


Figure 4: Concepts for Evaluation Models

# 4 Conceptual Framework

The concepts identified in the previous section constitute a conceptual framework for the comparison of trust models. As a way to validate our framework, we have chosen a set of relevant trust models that represent the types discussed earlier, namely PolicyMaker [3], TrustBuilder [26], Marsh's model [13], Jøsang's

belief model [9], Agudo et al. [1], eBay reputation model [20] and REGRET [23]. Table 3 shows the comparison among these models under the lens of their common features. In Table 4 we compare the trust decision models, whereas trust evaluation models are compared in Table 5. Note that the classification has been made according to the features explicitly presented by the corresponding authors, and that due to the diversity of the models, in some circumstances the classification for some concepts is subjective according to our own intepretation.

Table 3: Common Features Comparison. (*T=trustor/trustee, R/P=requester/provider, W=Witness, TTP = Trusted Third Party, AT=Access Trust, IT=Identity Trust, PT=Provision Trust, PM=Policy Model, NM=Negotiation Model, BM=Behaviour Model, PrM=Propagation Model, RM=Reputation Model*)

| Model | Role | Purpose | Type | Method |
|---|---|---|---|---|
| PolicyMaker | R, P | AT, IT | PM | Linguistic |
| TrustBuilder | R, P | AT, IT | NM | Linguistic |
| Marsh's | T, W | AT, PT | BM, PrM | Mathematic |
| Jøsang's | T, W | AT, PT | RM, PrM | Mathematic |
| Agudo et al. | T, W | AT, PT | PrM | Graphic, Mathematic |
| eBay | R, P, W, TTP | PT | RM | Mathematic |
| REGRET | R, P, W | PT | RM | Mathematic |

Table 4: Decision Models Comparison. (*PC=Policy Conflict detection, CC=Credential Chaining support, CV=Credential Verification support, ET=Evidence Type, -=undefined or not explicitly mentioned*)

| | | | | | | Trust Negotiation | |
|---|---|---|---|---|---|---|---|
| Model | P. Language | C. Format | PC | CC | CV | Strategy | ET |
| PolicyMaker | PolicyMaker | PGP's sig, X.509 cert | - | - | - | - | - |
| TrustBuilder | XML, IBM's TPL | X.509 cert | - | ✓ | ✓ | ✓ | - |

## 4.1 Discussion

By observing Table 3, the reader can see that decision models follow a linguistic modeling method, embodied in the policy and credential languages. The purpose of decision models is often either access trust (a provider wants to protect a resource from malicious requesters) or identity trust (trust in a requester is based on its identity). Regarding evaluation models, their purpose might be either to protect a requester from malicious providers (provision trust), or protect providers from malicious requesters (access trust). The only pure propagation model is Agudo et al. Since it is based on graph theory, it uses a graphic and

Table 5: Evaluation Models Comparison. (*DI=Direct Interaction, DO=Direct Observation, SI=Sociological Information, PI=Psychological Information, R=Reputation, C=Centralized, D=Distributed, GT=Game-Theoretic, I.Trust=Indirect Trust, -=undefined or not explicitly mentioned*)

| | | | | Source of Information | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Model | Approach | Dimension | C.Engine | DI | DO | SI | PI | R | I. Trust | Uncertainty | Time |
| Marsh's | GT | 1 | Continuous | ✓ | - | - | - | - | ✓ | - | ✓ |
| Jøsang's | GT | 3 | Belief | ✓ | - | - | - | D | ✓ | ✓ | - |
| Agudo et al. | - | 1 | Flow | - | - | - | - | D | ✓ | - | - |
| eBay | GT | 1 | Summation | - | - | - | - | C | - | - | - |
| REGRET | GT | 1 | Fuzzy | ✓ | - | ✓ | ✓ | D | - | ✓ | ✓ |

mathematic modeling method. The rest of models are based on reputation, except for Marsh's, which does not consider this concept.

As the reader might notice from the inspection of Table 5, most existing evaluation models follow a game-theoretic approach, except for Agudo et al., the only pure propagation model. Also, most models provide a single-dimension value, except for Jøsang's, which provides a vector of values that represent belief, disbelief and uncertainty. Semantics have been omitted as all trust models consider trust under some sort of *subjective* judgement (and not as formal measurements) and take into account *general* properties (and not specific ones). Indirect trust indicates whether the model proposes ways to create indirect trust relationships from direct ones by disseminating trust information. Uncertainty specifies whether the model considers uncertainty or reliability in the trust information, whereas time refers to whether the model takes into account this parameter when computing trust values. Note that there is not any model that accommodates all these factors. Also, few models consider sociological factors, such as the role played by the entities in the system or their location. In terms of sources of information, REGRET is one of the most complete models. However, as far as we know, no current models exploit direct observation as a source of information.

# 5 Conclusion and Future Work

In this paper, we propose a conceptual framework for trust. The purpose of this framework is twofold: (i) the identification of trust concepts that are often present in very heterogeneous types of models, as well as the relationships among these concepts; and (ii) the provision of a foundation onto which to compare different types of trust models.

Given the high heterogeneity of trust models, it is challenging to provide a general framework. We first identify and relate concepts that are general enough to be common to every trust model. After classifying trust models into different

types, we then identify and relate a set of concepts that are more closely related to each type of model. Thus, we suggest a two-dimensional framework in which we make a explicit differentiation between common and specific concepts.

As future work, we are interested in exploiting the conceptual framework in order to build a development framework that supports the flexible acommodation of different trust models. We think that the conceptual framework presented in this work can simplify the design of this development framework, by mapping the trust concepts into classes and components. Finding this mapping, in turn, might also assist in refining our conceptual framework.

The development framework will allow designers and developers to implement applications on top of a huge heterogeneity of trust models, according to the application needs. This provides support for the natural inclusion of trust requirements at design time, instead of adding trust as an after-the-fact property, which is the standard nowadays.

# References


[1] Isaac Agudo, Carmen Fernandez-Gago, and Javier Lopez. A model for trust metrics analysis. In *5th International Conference on Trust, Privacy and Security in Digital Business (TrustBus'08)*, volume 5185 of *LNCS*, pages 28–37. Springer, 2008.

[2] Donovan Artz and Yolanda Gil. A survey of trust in computer science and the Semantic Web. *Web Semantics: Science, Services and Agents on the World Wide Web*, 5:58–71, 2007.

[3] Matt Blaze, Joan Feigenbaum, and Jack Lacy. Decentralized trust management. In *IEEE Symposium on Security and Privacy*, pages 164–173, 1996.

[4] S. Boon and J. Holmes. The dynamics of interpersonal trust: Resolving uncertainty in the face of risk. pages 190–211, 1991.

[5] Bruce Christianson and William S. Harbison. Why isn't trust transitive? In *Proceedings of the International Workshop on Security Protocols*, pages 171–176, London, UK, UK, 1997. Springer-Verlag.

[6] Diego Gambetta. Can we trust trust? In *Trust: Making and Breaking Cooperative Relations*, pages 213–237. Basil Blackwell, 1988.

[7] Tyrone Grandison and Morris Sloman. A survey of trust in internet applications. *Communications Surveys & Tutorials, IEEE*, 3(4):2–16, 2000.

[8] Chern Har Yew. *Architecture Supporting Computational Trust Formation.* PhD thesis, University of Western Ontario, London, Ontario, 2011.

[9] Audun Jøsang. A logic for uncertain probabilities. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 9(3):279–311, June 2001.

[10] Audun Jøsang, Roslan Ismail, and Colin Boyd. A survey of trust and reputation systems for online service provision. *Decision Support Systems*, 43(2):618–644, March 2007.

[11] Adam J. Lee, Marianne Winslett, and Kenneth J. Perano. Trustbuilder2: A reconfigurable framework for trust negotiation. In Elena Ferrari, Ninghui Li, Elisa Bertino, and YÃ$\frac{1}{4}$cel Karabulut, editors, *IFIPTM*, volume 300 of *IFIP Conference Proceedings*, pages 176–195. Springer, 2009.

[12] Raph Levien. *Attack Resistant Trust Metrics*. PhD thesis, University of California at Berkeley, 2004.

[13] Stephen Marsh. *Formalising Trust as a Computational Concept*. PhD thesis, University of Stirling, April 1994.

[14] Roger C Mayer, James H Davis, and F David Schoorman. An integrative model of organizational trust. *Academy of Management Review*, 20(3):709–734, 1995.

[15] D. Harrison McKnight and Norman L. Chervany. The meanings of trust. Technical report, University of Minnesota, Management Information Systems Research Center, 1996.

[16] Keith W Miller, Jeffrey Voas, and Phil Laplante. In Trust We Trust. *Computer*, 43:85–87, 2010.

[17] L. Mui, M. Mohtashemi, and A. Halberstadt. A computational model of trust and reputation. pages 280–287, 2002.

[18] D. Olmedilla, O.F. Rana, B. Matthews, and W. Nejdl. Security and trust issues in semantic grids. In *Proceedings of the Dagsthul Seminar, Semantic Grid: The Convergence of Technologies*, volume 5271, 2005.

[19] Sarvapali D Ramchurn, Dong Huynh, and Nicholas R Jennings. Trust in multi-agent systems. *The Knowledge Engineering Review*, 19(01):1–25, April 2005.

[20] Paul Resnick and Richard Zeckhauser. Trust among strangers in Internet transactions: Empirical analysis of eBay's reputation system. In Michael R. Baye, editor, *The Economics of the Internet and E-Commerce*, volume 11 of *Advances in Applied Microeconomics*, pages 127–157. Elsevier Science, 2002.

[21] Sini Ruohomaa and Lea Kutvonen. Trust management survey. In *Proceedings of the Third international conference on Trust Management*, iTrust'05, pages 77–92, Berlin, Heidelberg, 2005. Springer-Verlag.

[22] Rachid Saadi, Mohammad Ashiqur Rahaman, ValÃ©rie Issarny, and Alessandra Toninelli. Composing trust models towards interoperable trust management. In Ian Wakeman, Ehud Gudes, Christian Damsgaard Jensen,

and Jason Crampton, editors, *IFIPTM*, volume 358 of *IFIP Publications*, pages 51–66. Springer, 2011.

[23] Jordi Sabater and Carles Sierra. Regret: reputation in gregarious societies. In *Proceedings of the fifth international conference on Autonomous agents*, AGENTS '01, pages 194–195, New York, NY, USA, 2001. ACM.

[24] Jordi Sabater and Carles Sierra. Review on Computational Trust and Reputation Models. *Artificial Intelligence Review*, 24:33–60, 2005.

[25] Girish Suryanarayana, Mamadou H. Diallo, Justin R. Erenkrantz, and Richard N. Taylor. Architectural Support for Trust Models in Decentralized Applications. In *Proceeding of the 28th international conference*, pages 52–61, New York, New York, USA, 2006. ACM Press.

[26] M Winslett, T Yu, K.E Seamons, A Hess, J Jacobson, R Jarvis, B Smith, and L Yu. Negotiating trust in the Web. *Internet Computing, IEEE*, 6(6):30–37, 2002.

[27] Zheng Yan and Silke Holtmanns. Trust Modeling and Management: from Social Trust to Digital Trust. *Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions*, January 2008.

[28] Ping Zhang, A Durresi, and L Barolli. Survey of Trust Management on Various Networks. In *Complex, Intelligent and Software Intensive Systems (CISIS), 2011 International Conference on*, pages 219–226, 2011.