THIS IS AN EARLY VERSION OF PAPER PUBLISHED IN
Mathematical and Computer Modelling 49 (2009) 226–233, Elsevier
(this early version is made available due to copyright reasons)

A Formal Apparatus for Modeling Trust in Computing Environments

Denis Trček
Faculty of computer and information science
Laboratory for e-media
Tržaška cesta 25, 1000 Ljubljana, Slovenia
Tel.: +386 1 4768 918 / Fax: +386 1 4264 647
E-mail: denis.trcek@fri.uni-lj.si

Abstract

Recent research in computer systems security has evolved into trust issues, which are now becoming an important topic. Majority of approaches for trust modeling addressed trust by actually focusing on security, and some of them addressed also trust as such. This paper presents a formal apparatus that concentrates on trust as such. It is flexible enough to accommodate the driving factors behind trust and consequently different trust-focused methodologies and technologies. The basic goal of work presented in this paper is definition of qualitative trust modeling methodology for trust management in contemporary computing environments that efficiently complements existing quantitative methodologies. Further, an open conceptual model for trust management is presented that accommodates various qualitative and quantitative trust management methodologies. This model has also been implemented in web services environment, and it is discussed in this paper as well.

Keywords: services oriented architectures, security, trust management, human behavior, modeling and simulation.

---

1. INTRODUCTION

Research of trust is a multi-disciplinary area that has roots in psychology, but is strongly related to sociology, economy, and computer and information sciences. Thus various paths to investigation of this topic can be taken. The approach in this paper will be based on the evolution of security research in computer information systems that have recently evolved to research of trust.

Security in computer networks environment became important in the mid-nineties with the proliferation of e-business. During the last years it is gaining even more importance due to events of 9/11. Trust is related to security in distributed systems and this fact has been recognized already some twenty years ago (DoD, 1985). Later, it has played a fundamental role in formal methods for analysis of cryptographic services (Burrows et al., 1990). But the problem of trust in computer networks based information systems, including its appropriate analysis and formalization, became a major research issue only a few years ago.

Extensive survey on trust in computing environments done by Grandison and Sloman (Grandison, 2000) defines trust as the firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context. Authors studied trust in order to be able to model it for use in automated systems, so they did not consider the interactive, i.e. social component of trust. However, this component is vital and has to be taken into account. Authors have likely excluded it because of concentrating on technological issues (that could be called trust enabling technologies) and not the trust phenomenon itself. They analyzed some trust enabling solutions like

- PICS of W3C (Miller, 1996) – this is a standardized platform, which defines formats and distribution of labels that are meta-data for description of Web documents;
- AT&T's PolicyMaker (Blaze, 1996) – this is a technology that binds access rights to an owner of a public key, whose identity is bound to this key through a certificate;
- IBM's Trust Establishment Module (Herzberg, 2000) – this is Java based solution with appropriate language, similar to PolicyMaker.

An opposite approach to those above, which rests almost exclusively on social component of trust, and that is intended to promote on-line business, is TRUSTe (TRUSTe, 2005). TRUSTe services allow companies to communicate their commitment to privacy, and let consumers know which businesses they can trust. Similar is approach given in (Osterwalder, 2001), where trust is supposed to be a matter of accreditation and certification of IT technology, which certainly is true to a certain degree.

Among other trust related initiatives, one should mention EU project TrustCoM, which is a trust management framework for enabling secure business processing in Virtual organizations (TrustCoM, 2005). In addition, also within services oriented architectures trust is becoming intensively addressed (Nadalin, 2005).

All these mentioned works present two different approaches to trust modeling and management. The rest of approaches can be positioned in-between, meaning that they address technological and social component. Despite of this, the very functioning and modeling of trust phenomenon still needs to be addressed. ¸

Fifteen years ago Denning analyzed the concept of trust and came to conclusion that trust is not a property of an entity or a system, but is an assessment (Denning, 1993). Such assessment is driven by experience, it is shared through a network of people interactions and it is continually remade each time the system is used. This definition effectively covers both approaches and will be the basis for modeling approach in this paper. It is now clear that proper modeling of trust is vital for its management to assure security and privacy in contemporary information systems (Trček, 2006).

2. AN OVERVIEW OF SOME TRUST MODELING METHODOLOGIES

An entity using modern information services has "to sense" the computing environment and has to permanently value his / her decisions to assure security of sensitive business transactions and processes. In fact, risk analysis is taking place in the background of trust. In case of positive decision, a corresponding level of trust is established and vice versa.

With regard to risk assessment processes, it was common in the past to assume that human agents behave rationally. Such cases can be found in economy (e.g. a consumer is assumed to make choices by maximizing the utility function in the choice set (Varian, 1999)), psychology (e.g. agents are assumed to function according to Bayesian theorem when it comes to risk judgment (Edwards, 2001)), etc. As far as we know today, the real problem with agents' behavior is their irrational component in decision making processes and this has to be taken into account.

In the area of computer science, an often used methodology for trust management is Dampster - Shafer theory of evidence (Shafer, 1996). This theory defines a set of possible states as *a frame of discernment* Θ. Within this frame of discernment, exactly one state is assumed to be true at any time. For example, let a frame of discernment be given by atomic states x_1, x_2, x_3 and a compound state $x_4 = \{x_1, x_3\}$, which means that $\Theta = \{x_1, x_2, x_3, \{x_1, x_3\}\}$. Then the *belief mass* is assigned to every state. In case of, e.g. x_4 it is interpreted as the belief that either x_1 or x_3 is true, but the observer cannot determine the exact sub-state, which is true. Belief mass serves as a basis for *belief function*, which is interpreted as a total belief that a particular state is true, be it atomic or compound.

This theory has been further used as a basis for Jøsang's subjective algebra (Jøsang, 2001), and an example of its early practical implementation can be found in (Dimitrakos, 2001). The main contribution of subjective algebra is preservation of a mathematically sound basis, while introducing various operators for trust. Subjective algebra contains equivalents to traditional logical operators, and also introduces new ones like recommendation and consensus. An opinion ω is modeled with a triplet (b, d, u), where b stands for belief, d for disbelief and u for uncertainty. Each of those elements gets its continuous values from a closed interval [0, 1], such that $b + d + u = 1$. For example, an agent's opinion can be expressed as $\omega = (0.6, 0.2, 0.2)$. The problem with the latter methodology is assumption of rational behavior of agents.

This overview is not intended to imply that rational approaches are useless. Rather, it implies that due to facts that have been brought to scientific light during recent decades, it is vital to address all relevant factors when it comes to trust management.

3. DEFINING TRUST FACTORS

To obtain a formal basis with generic elements, the basis will present research done by Piaget (Piaget, 1999). Trust is a manifestation of reasoning and judgment processes that have origins in psychology. These processes are of a developmental nature and Piaget is famous for his work on developmental psychology.

It should be noted that it is not the intention of our work to present a new methodology that would supersede that above mentioned methodologies for trust phenomenon analysis and its management. On the contrary, Piaget's work will serve to identify basic ingredients, i.e. factors that drive trust. Next, these factors will be used to enable qualitative and quantitative, computer based research and management of trust regardless of a particular law behind trust phenomenon.

When talking about developmental psychology, the following facts have to be taken into account. Firstly, the mind is in perpetual movement and it is not static. Secondly, when an agent fails to analyze an object, whether on account of its novelty or its complexity, juxtaposition and syncretism appear. Juxtaposition leads to an absence of implication and reciprocal justification between successive judgments; syncretism creates a tendency to bind everything together and to justify by means of the most ingenious or the most facetious devices. Thirdly, the mind gets conscious of itself only when it is in contact with physical objects or with other subjects. Fourthly, a subject often forgets the reasons for believing a certain fact (he / she can no longer enter into a past state of mind). This phenomenon leads to contradictory beliefs.

Based on the above premises, the following trust forming factors can be identified:

- *Time dynamics*. An agent's relation towards object / subject being trusted is a dynamic relation, where time should be treated as an intrinsic variable.
- *Rationality / irrationality*. An agent's trust is driven by rational or irrational factors.
- *Action binding*. Trust presents a potential (a basis) for an agent's deeds or, better said, ways of interaction with the environment.
- *Feed-back dependence*. Trust is not a product of independent mind, but is influenced by agent's environment. In the first place, this are reported trust values of other agents. Further, being forced to adopt a certain kind of behavior may change the agent's opinion about this behavior. Trust influences a certain action, but it is also adjusted based on the feedback of the action.
- *Trust differentiation*. Trust evolves into various forms. The reasons are linguistic capabilities of an entity expressing trust and perceiving capabilities of a targeting entity. Additionally, trust can be mediated in an intentionally modified form. Thus trust should be divided into minor trust (denoted by $\underline{\omega}$), that is expressed and communicated, and major trust, that is personal, intimate trust (denoted by ϖ).

A computational model of trust is given in Fig. 1. T denotes the set of time values t, Δ denotes the set of observed facts δ (e.g. deeds), and Ω denotes the set of other agents' opinions. The context Γ is thus defined as $\Gamma = T \times \Delta \times \Omega$.

Let $\underline{\omega}^{\bullet}$ denote the sequence $\underline{\omega}_1, \ldots, \underline{\omega}_n$, and let $\underline{\delta}^{\bullet}$ denote the sequence $\underline{\delta}_1, \ldots, \underline{\delta}_n$. Thus $\varpi = \varphi\ (t, \underline{\omega}^{\bullet}, \underline{\delta}^{\bullet})$ results in agent's major trust.

The relationship between the space of minor, expressed opinions and deeds is defined by function η, such that $\underline{\delta}^{\bullet} = \eta\ (\varpi)$. Further, particular expressed opinion influences the rest of opinions by function μ, such that $\underline{\omega}^{\bullet} = \mu\ (\underline{\omega})$ (this bullet notation is used intentionally to emphasize the multiform nature of η and μ mapping). And finally, the expressed opinion $\underline{\omega}$ is given by function ζ, i.e. $\underline{\omega} = \zeta\ (\varpi)$.

Summing up, rationality and irrationality are modeled by trust forming function φ, action binding by function η, and trust differentiation by function ζ. Further, feedback dependence is modeled by μ and also η. Finally, temporal dynamics is covered by function φ.

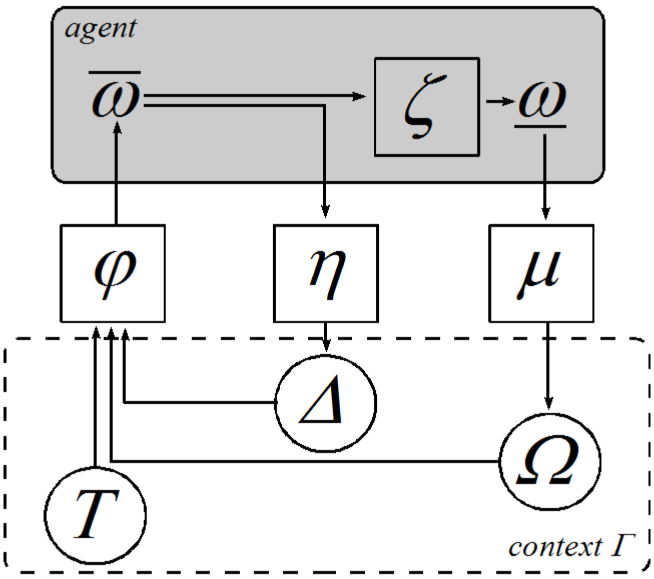

Figure 1: Modeling trust in agents' environment

It can be observed that this formal framework is independent of the exact mechanism that drives trust. To simplify subsequent analysis, only the context $\Gamma = \Omega$ will be considered. Further, it will be assumed that $\zeta(\varpi) = \underline{\omega}$ is such that $\varpi = \underline{\omega}$.

4. TRUST ALGEBRA

This section presents trust algebra that fits in the model given in Fig. 1. Its basic premise is that humans hardly perceive trust on the basis of sophisticated quantitative methodologies that were discussed in the first section, which is also proven by our experiments. Thus one natural starting point is to think about trust in qualitative terms of trusted, untrusted and undecided relations.

Definition 1*. Trust is a relationship between agents A and B, which may be trusted, untrusted or undecided. Trust relationship is denoted by* $\omega_{A,B}$*, which means agent' s A attitude towards agent B.*

By focusing on actual trust within a certain context the following can be observed:

- Trust relation is generally not reflexive - an agent can trust itself in a certain context, however, in another context this may not be the case.
- Trust relation is generally not symmetric $\omega_{A,B} \neq \omega_{B,A}$. One agent's trust towards the other agent often differs from the trust of the other agent related to the first one.
- Trust relation is generally non-transitive, i.e. $\omega_{A,B}$ and $\omega_{B,C}$ does not imply $\omega_{A,C}$. There might exist a different emotional attitude between the first and the third agent, which prevents transitive propagation of trust.

When considering trust, it is hard for an ordinary person to evaluate it in quantitative terms. Suppose person *C* is fully trusted by persons *A* and *B*. Now asking *A* and *B* to define how much money they are willing to lend to person *C*, the answers will rarely be the same. It is much more comfortable for a human being to think about trust in qualitative terms. Therefore this will be the basis for our approach.

To study propagation of trust in social interactions trust graphs are introduced. The links of trust graphs are directed and weighted accordingly. If a link denotes trust attitude of agent *A* towards agent *B*, the link is directed from *A* to *B*. Because graphs can be equally presented with matrices (Harary, 1972), the next basic definition can be given:

Definition 2. *Propagated trust in social interactions within a context* Γ *is represented with trust matrix* M_Γ*, where elements* $\omega_{i,j}$ *denote trust relationships of i-th agent towards j-th agent, and have values* 1*, or* 0 *or* -1 *to denote trusted, undecided and untrusted relationships. If a relation is not defined, it is denoted by "-", meaning that an agent is either not aware of existence of another agent, or does not want to disclose its trust.*

Note that $\omega_{i,j}$ = "-" does not imply $\omega_{j,i}$ = "-".

A general form of trust matrix M of a certain society with *n* agents in a given context Γ is as follows:

$$\begin{bmatrix} \omega_{1,1} & \omega_{1,2} & \cdots & \omega_{1,n} \\ \omega_{2,1} & \omega_{2,2} & \cdots & \omega_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \omega_{n,1} & \omega_{n,2} & \cdots & \omega_{n,n} \end{bmatrix}$$

It should be emphasized that trust matrices operations are not the same as those in ordinary linear algebra. Rows represent certain agent's trust towards other agents, while columns (trust vectors) represent trust of community related to a particular agent. Further, an interesting case with this algebra for computing environments is a possibility to include trust about technological components or services. Such component or service is treated as a dumb agent, which is not aware of itself nor its surroundings. These dumb agents can be recognized in a trust matrix through a row that consists exclusively of "-".

***Defintion 3**. Trust operation is denoted by expression $\omega_{i,k}^{+} = op_l(\omega_{i,k}^{-}, \omega_{j,k}^{-})$, where op_l is the prefix operator that models trust of i-th agent, while $\omega_{i,k}$ and $\omega_{j,k}$ denote trust values of i-th and j-th agent towards k-th agent. If $\omega_{i,k}$ equals "-", then the result of trust operation is also "-".*

In the above definition, "$^{-}$" denotes pre-operation value, and "$^{+}$" denotes the resulting value of operation.

To model the most simplified situations, and in line with above definitions, trust will be based on three-valued algebra with operators for optimistic assessment, pessimistic assessment, and balanced assessment.

***Definition 4**. Let ↑ denote optimistic assessment operator, ↓ pessimistic assessment operator, and ↔ balanced assessment operator that are applied as prefix operators to opinions $\omega_{i,k}^{-}$, $\omega_{j,k}^{-}$, where the results of calculations $\omega_{i,k}^{+}$ are given in table* 1.

$\omega_{i,k}^{-}$	$\omega_{j,k}^{-}$	$\omega_{i,k}^{+}, \uparrow_i$	$\omega_{i,k}^{+}, \downarrow_i$	$\omega_{i,k}^{+}, \leftrightarrow_i$
1	1	1	1	1
1	0	1	0	0
1	-1	1	-1	0
1	-	1	1	1
0	1	1	0	0
0	0	0	0	0
0	-1	0	-1	0
0	-	0	0	0
-1	1	1	-1	0
-1	0	0	-1	0
-1	-1	-1	-1	-1
-1	-	-1	-1	-1
-	1	-	-	-
-	0	-	-	-
-	-1	-	-	-
-	-	-	-	-

Table 1*: The definition of trust assessment operators*

It should be added that the simplified notation ($\omega_{i,k}^{+}$, op_i) is equivalent to the following notation: $\omega_{i,k}^{+} = op_l(\omega_{i,k}^{-}, \omega_{j,k}^{-})$.

Regarding the precedence of operators - they are equal, thus any particular precedence has to be enforced by use of parentheses. This requires precise definition of operations for particular trust vector.

Definition 5*. A new trust value* $\omega_{i,j}^{+}$ *in a certain trust vector* $\omega_{i,j=const}$ *is computed according to the following rule:* $op_I\,(\ldots\,(op_I\,(\,op_I\,(\omega_{i,j}^{-},\ \omega_{1,j}^{-}),\ \omega_{2,j}^{-}),\ \ldots\ ,\ \omega_{n,j}^{-})$*.*

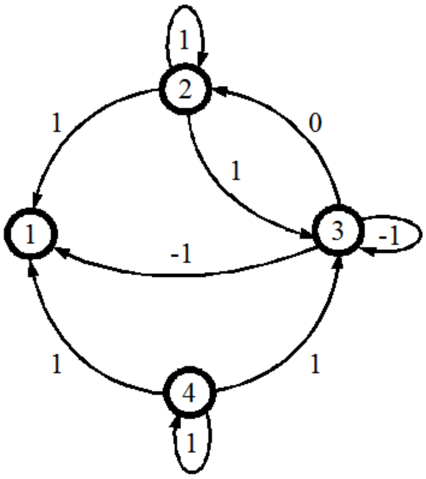

Figure 2: A model of trust for agents' environment

Let' s introduce three notions that will be used in the rest of the paper: homogeneous society, fully connected society and trust cluster.

- Homogeneous society denotes a society that consists of agents, which all evaluate trust using the same operator, but their initial trust values may be different.
- Fully connected society denotes society where all agents disclose their trust relations (no "-" values).
- Trusted / untrusted / undecided cluster denotes connected sub-graph of a trust graph that consists of only trusted / untrusted / undecided arcs.

Theorem 1*. For any value of* $\omega_{j,k}$ *the following holds true:*

$$\uparrow_i (1, \omega_{j,k}) = 1, \quad \downarrow_i (-1, \omega_{j,k}) = -1, \quad \leftrightarrow_i (0, \omega_{j,k}) = 0, \quad op_i\,(\omega_{i,j}, -) = \omega_{i,j}$$

Proof. The above rules follow trivially from the definition of trust operators. ∎

Lemma 1*. Assume a homogeneous and fully connected society with optimistic impact operator. If there exists at least one* $\omega_{i,j} = 1$ *in a trust vector* $\omega_{i,j=const}$*, then all resulting values in this trust vector equal* 1*.*

Proof. Each value in a trust vector is calculated according to definition 5. If at least one trust value in this trust vector equals 1, and all operators are $\uparrow$, then using table 1 the proof is obtained. ∎

The proof for the following two lemmas is analogous to the above proof.

Lemma 2. *Assume a homogeneous and fully connected society with pessimistic impact operator. If there exists at least one* $\omega_{i,j}$ = -1 *in a trust vector, then all resulting values in this trust vector equal* -1*.*

Lemma 3. *Assume a homogeneous and fully connected society with balanced impact operator. If there exists at least one* $\omega_{i,j}$ = 0 *in a trust vector, then all resulting values in this trust vector equal* 0*.*

Similar lemmas about the largest / the smallest / different trust values can be proved to derive the following corollaries.

Corollary 1. *In every homogeneous and fully connected society with optimistic / pessimistic impact operator the resulting values in each trust vector equal to the largest / the smallest value of this particular trust vector.*

Corollary 2. *In every homogeneous and fully connected society with balanced impact operator the resulting values in each trust vector equal to* 0 *(undecided relation), if at least two values in this particular trust vector differ.*

Theorem 2. *In any fully connected society,* $\omega_{i,k}^{+} = op_i\ (\omega_{i,k}^{-},\ \omega_{j,k}^{-}) = op_i\ (\omega_{j,k}^{-},\ \omega_{i,k}^{-})$, *meaning that arguments are commutative.*

Proof. On the basis of notion of fully connected society, the proof of the theorem follows by using table 1. $\blacksquare$

Fig. 2 gives an example of trust graph of a certain society in a context Γ. The corresponding matrix is given below:

$$\begin{bmatrix} - & - & - & - \\ 1 & 1 & 1 & - \\ -1 & 0 & -1 & - \\ 1 & - & 1 & 1 \end{bmatrix}$$

The general functioning of trust engine, or the general procedure for simulation of trust dynamics in a certain agents society, goes as follows:

- Define initial trust matrix M_Γ.
- Define functions φ, η, μ, ζ that model agents' behavior (as each row in trust matrix describes particular agent's trust attitude towards the society, this *n*-tuple φ, η, μ, ζ is a characteristic of row *i*).
- For every trust vector $\omega_{i,j}$, where *i* =1, …, *n* and *j* = *const*, use *n*-tuple, defined for particular *j*, i.e. all operands $\omega_{i,j}$ in a trust vector, to obtain the new resulting value $\omega_{i,j}$ by using definition 5.
- If the resulting trust matrix differs from the previous one, increment time ($t \leftarrow t + 1$), and go to the previous step. Otherwise end the procedure.

The following example illustrates the process. Let us assign optimistic impact operator to agent A_2, and pessimistic impact operator to agents A_3 and A_4 (see Fig. 2). Then performing the first loop of the above-described procedure results in

$$\begin{bmatrix} - & - & - & - \\ 1 & 1 & 1 & - \\ -1 & 0 & -1 & - \\ -1 & - & -1 & 1 \end{bmatrix}$$

For example, the calculation of $\omega_{2,3}^{+}$ goes as follows:

$$\uparrow_I(\uparrow_I(\uparrow_I(\uparrow_I(1, -), 1), -1), 1) = 1$$

The above matrix describes a stable state for the given society and further loops do not change it.

5. APPLICABILITY AND REAL WORLD ISSUES

To prove our assumptions about the need for qualitative algebra for computerized trust management, we have conducted an experiment that is described in detail in this section.

This experiment has been conducted in a form of a survey, which has been anonymous and where we have firstly shortly described the general problem area of computer supported trust management. Next, we have asked participants whether they would be willing to completely leave a computer system to manage trust on their behalf. Next, we have given an example and asked participants to evaluate trust in quantitative terms, which are basically tied to understanding of probability related concepts. Therefore we have at the same time checked indirectly participants' understanding of these concepts. It is questionable whether it makes sense for a person to decide for a quantitative methodology to model trust, when this very person has problems with perceiving trust on the basis of probability. Finally, in the last question, we have asked participants, which way of expressing trust they have preferred, quantitative or qualitative one.

We have initially planned to get statistically relevant sample for our experiment. But it has turned out that random samples in this area are currently hard to obtain - many of involved persons have not felt competent enough for participation because of their unfamiliarity with computers. Computer illiteracy is still a serious issue within EU, where approximately half of population has no computer skills, while in some member states this can be as high as 65% (Eurostat, 2006). This illiteracy is growing with age: for ages between 55 and 64 it is almost 60%, and for ages above, it is almost 80%.

Therefore we have decided to concentrate on one narrow segment of the whole population. The population should not be from mathematics, natural sciences or technology domain, but it should certainly have enough experiences with computers. This would quite well reflect the general population in the EU, which at tertiary level consists almost 80% of social science, business, law, agriculture, veterinary, health, welfare, services education, humanities and art (Andren and Schmidt, 2005). Further, the total population having completed at least upper secondary education in the EU was 69,1% in 2005 (Eurostat, 2005). So in order to roughly reflect this structure, students population is a good choice.

Therefore the chosen population has been students of restoration studies at Academy of fine arts and design at University of Ljubljana. This population has consisted of *n* = 45 students, and the number of participants that completed the survey has been 35 - the response rate was 77.8%, there have been eight no show-ups, and two students have refused to take part on the spot. Further, sex proportion has been 86% females and 14% males, while the average age of the whole population has been 24.55, and its standard deviation has been 5.35.

The results of this experiment have confirmed our expectations. Firstly, the majority of users have opted for direct trust modeling, i.e. 82.9 %. Put another way, more than 80% of users have not been willing to let computer system to manage trust on their behalf – users simply want to directly intervene with the systems when trust is an issue. Secondly, based on the fact that significant number of papers on trust methodologies deploys quantitative methodologies (e.g. Jøsang's algebra), this implies that such methodologies are supposed to be of a general application. Our experiment has proved that this has not been the case with our population, because 74.3% of students have opted for qualitative assessment of trust. And finally, there has existed a high percentage of those that that have had troubles with understanding of probabilities - their rate has been 20%. This further justifies the need for qualitative methodologies for computerized trust management.

Based on above research and the concept, presented in the third section, trust management application, called trustGuard, has been implemented, which deploys the conceptual model from Fig. 1. trustGuard can be accessed through browser, or web services. It enables trustors' and trustees' identifications through Uniform Resource Identifiers (URIs), e-mail addresses and aliases. It currently supports qualitative algebra and Jøsang's algebra, but because of its open conceptual model, new methodologies that will be the result of future research, can be easily added.

6. CONCLUSIONS AND FURTHER WORK

Trust in contemporary information systems is an area with growing importance - not only within academic community, but also industry. Although trust is closely related to security, it should not be messed up with it. Trust is a socio-cognitive phenomenon and has to be adequately modeled to enable its management in contemporary information systems.

The modeling methodology presented in this paper takes the socio-cognitive nature of trust phenomenon into account. It is open and not tied to particular methodology for trust management, thus it can accommodate existing various methodologies that were described in this paper. The methodology presented in this paper starts with taxonomy, continuous with the definition of a generic model, and ends with the definition of a qualitative algebra. The main premises of this algebra have been subject to an experiment that has proved the need for such algebra, and has been described in detail in this paper. This qualitative algebra complements other modeling methodologies like Jøsang's algebra to fully support trust management in contemporary information systems. In addition, trust management application, called trustGuard, has been implemented that currently supports the above mentioned two methodologies, Jøsang's algebra and qualitative algebra.

Future work will be concentrated on experiments to derive the necessary additional inference rules for qualitative algebra to expand the set of those most intuitive operators that are presented in this paper. Last but not least, the developed apparatus is anticipated to serve as a useful input for research of trust itself through computer simulations by deploying agents technologies, e.g. Zeus toolkit (Collis, 2001), or Repast toolkit (Collier, 2003).

7. REFERENCES

Andren B., Schmidt P. (2005). Statistics in focus - Education in Europe. *KS-NK-05-010-EN-N*, European Communities, Luxembourg.

Blaze M., Feigenbaum J., Lacy J. (1996). The Role of Trust Management in Distributed Systems Security. *Proc. of the IEEE Conf. on Security and Privacy*, Oakland.

Burrows M., Abadi M., Needham R. (1990). A Logic of Authentication. *ACM Transactions on Computer Systems*, 8(1), 18-36.

Collier, N., Howe, T., North, M. (2003). Onward and Upward - The Transition to Repast 2.0. *Proceedings of the First Annual North American Association for Computational Social and Organizational Science Conference,* Pittsburgh.

Collis J., Ndumu D., van Buskirk C. (2000). *The Zeus Technical Manual*. British Telecom, London, http://labs.bt.com/projects/agents/zeus/techmanual/.

Denning D. (1993). A new Paradigm for Trusted Systems. *Proc. of ACM SIGSAC New Security Paradigms Workshop*, ACM, New York, pp. 36-41.

Department of Defense-DoD (1985). *Trusted Computer System Evaluation Criteria*. DoD Standard 5200-28.STD, Washington D.C:, 1985.

Dimitrakos T., Bicarregui J. (2001). Towards a Framework for Managing Trust in e-Services. *Proc. of Fourth Int. Conference on e-Commerce Research*, pp. 360-381, Dallas.

Edwards W. (2001). Conservativism in Human Information Processing. *Judgement under Uncertainty*, editors Kahneman D., Slovic P., Tversky A., Cambridge University Press, Cambridge.

Eurostat (2005). Eurostat Year Book 2005. *KS-CD-05-001-EN-C*, European Communities, Luxembourg.

Eurostat (2006). More than a third of EU25 population have no basic computer skills - Large differences between the generations. *ES news release No. 83/06*, Brussels.

Grandison T., Sloman M. (2000). A Survey of Trust in Internet Applications. *IEEE Communications Surveys*, IEEE Society Press, pp. 2-13.

Harary F. (1972). *A Graph Theory*. Menlo Park: Addison Wesley.

Herzberg A. et al. (2000). Access Control Meets Public Key Infrastructure. *Proc. of the IEEE Conf. on Security and Privacy*, Oakland.

Jøsang A. (2001). A Logic for Uncertain Probabilities. *Int. Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 9(3), 279-311.

Miller J., Resnick P., Singer D. (1996). *PICS Rating Services and Rating Systems*. http://www.w3c.org/TR/REC-PICS-services.

Nadalin A. (ed.) (2005). *Web Services Trust Language (WS-Trust)*. Actional Corporation, BEA Systems, Inc., Computer Associates International, Inc., IBM Corporation, Layer 7 Technologies, Microsoft Corporation, Oblix Inc., OpenNetwork

Technologies Inc., Ping Identity Corporation, Reactivity Inc., RSA Security Inc., and VeriSign Inc., http://msdn.microsoft.com/library/en-us/dnglobspec/html/WS-trust.pdf

Osterwalder D. (2001). Trust Through Evaluation and Certification? *Social Science Computer Review*, 19(1), 32-46, Sage Publications.

Piaget J. (1999). *Judgment and Reasoning in the Child.* London: Routledge.

Shafer G. (1976). *A Mathematical Theory of Evidence*. Princeton: Princeton University Press.

Trček D. (2006). *Managing Information Systems Security & Privacy*. New York / Heidelberg: Springer.

TrustCoM Consortium (2005). TrusCoM Project - Executive Summary. EU 6.th FW Programme IST/2002/2.3.1.9, http://www.eu-trustcom.com/DownDocumentation.php.

TRUSTe (2005). *TRUSTe Security Guidelines*. TRUSTe, San Francisco, http://www.truste.org/pdf/SecurityGuidelines.pdf.

Varian H. (1999). *Intermediate Microeconomics - A Modern Approach.* Norton: New York.

Denis Trček is a professor of computer and information sciences at University of Ljubljana. His area of research includes information systems and electronic business with emphasis on security and trust. He has taken part in various European research projects. He has been involved in application projects in the banking and insurance sector. His bibliography includes approx. 100 titles, including scientific monograph published by Springer and contributions to monographs published by John Wiley, and Idea Inc. He is a member of program committees of international conferences (IASTED SE, WAWC, IS), and a member of IEEE.