4

System Models, e-Risks and e-Trust
Towards bridging the gap?

Theo Dimitrakos
Central Laboratory of the Research Councils, Rutherford Appleton Laboratoy, Oxon, UK

Abstract: Motivated by an industrial application, we introduce a working model of trust in e-commerce, and offer a classification of trust in e-services. Emphasis is also placed on the combination of risk analysis and role-based modelling to support trust management solutions.

1. INTRODUCTION

The issue of trust in e-commerce is central for businesses as electronic services based on ubiquitous media (e.g. Internet, WWW, mobile phones) proliferate. The UK is the largest e-commerce market in Europe [1], and although smaller than the US, it has been closing the gap relative to the size of the economy. The e-service market is predicted to rise to between 4% and 7% of GDP by 2003 for the countries shown in *Figure 1.* However, there is still major concern about user confidence in e-services. Year 2000 started with high hopes and many promising e-commerce start-ups but the bubble soon burst with many of them going out of business by the fourth quarter. In addition to well-thought business plans, if e-business ventures are to prosper, there is a prominent need to improve consumer confidence in e-services.

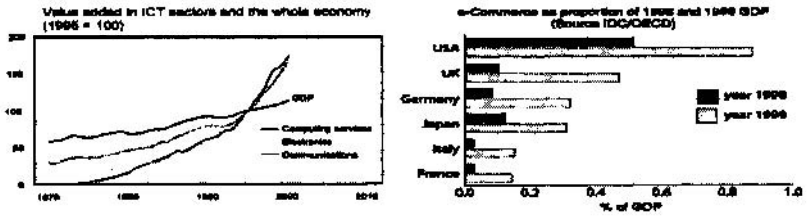

Figure 1. Sources: IDC/OECD (left) and “Success in 2005”, UK ESRC (right)

Differing trust relationships can be found among the parties involved in a contract, and the emerging virtual communities require richer models of trust, in order to distinguish between them, and accommodate them in the context of a specific service. To build consumer confidence, e-commerce platform providers need to improve the existing technology in order to capture, measure and manage the trusting relationships that underlie such services. If e-commerce is to achieve the same levels of acceptance as traditional commerce, trust management has to become an intrinsic part of it.

Current solutions fail to incorporate in their decision making evidence or opinions collected by an agent through the agent's own experience, or via communication with other agents who cohabit the system. This makes the evolution of e-commerce systems harder and impedes their ability to adapt to changes in trust and to set up new relationships. In order to be able to handle trust dynamics, future solutions will have to incorporate methods to simulate learning, reasoning and analysing transactional and environmental risks with respect to the agents' view of the system they inhabit.

Motivated by an industrial application (section 2), this paper introduces a working model of trust in e-commerce (section 3) and a trust management scheme (section 4) including a classification of the basic types of trust underlying e-services. We suggest that the needs for flexibility and scalability are better addressed by separating the trust management framework from the purpose of the application, and we emphasise that risk management and role-based modelling can be combined to support trust management solutions. More specifically, we find roles to be well suited for modelling service-specific aspects of trust and particularly helpful for identifying and analysing cases where trust may be transferable. We also anticipate that risk management can guide an agent through transforming a mere *inclination* to trust into a carefully considered *intention* to trust, and through endorsing dependable *behaviour* as a realisation of the agent's dependable *intentions* to trust.

2. MOTIVATING EXAMPLE

As a motivating example, we summarise the Home Shopping Tool (HST) component of the ACTIVE platform[10] , which will be used as one of the test-beds in the CORAS project[11].

[10] Developed in the ESPRIT EP 27046 project which aimed to introduce an e-commerce platform for integrated retail services, providing an intelligent interface upon which the trading parties (retailers, suppliers and consumers) establish a tied and trusted relationship.

[11] CORAS (IST-2000-25031) is an industry lead European project developing a framework for precise, unambiguous, and efficient risk analysis of security critical systems. The framework will be evaluated in major user trials in e-commerce and e-medicine.

HST delivers a personalised, targeted marketing experience through the realisation of a variety of services including personalised shopping, catalogue information, product search and recommendations, sales negotiation, e-payment, and user management facilities. Specific consumer information is gathered for the purpose of behaviour analysis and can be made available to the platform operator.

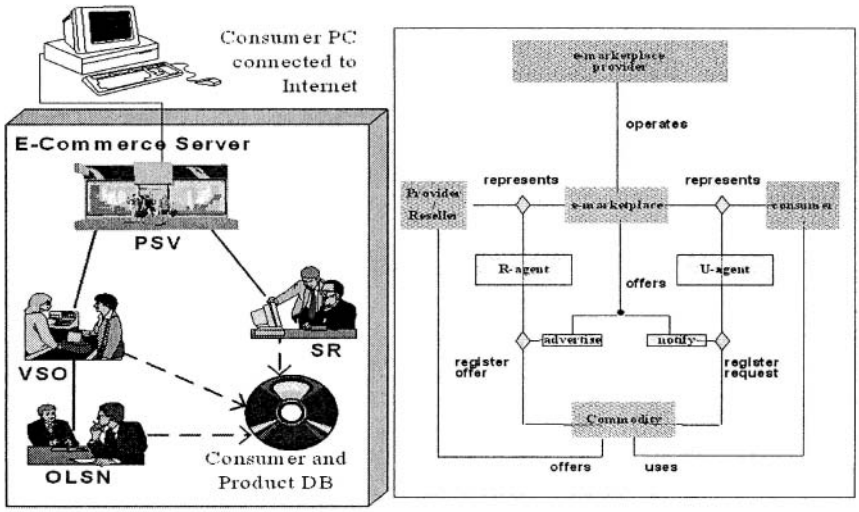

Figure 2. HSP components and basic business entities & relationships underlying OSLN

Notably, consumers and suppliers are provided with an agent-based automated bargaining mechanism that allows customers to find and negotiate products with various suppliers, and suppliers to promote their products and attract consumers. The agents get involved in a negotiation process and try to reach a mutual agreement according to the mandates given by their creators.

These services are offered to the users with the help of the following software modules depicted in *Figure 2*: The Virtual Shopping Operator (VSO), the Shopping Recommender (SR), the On-line Sales Negotiator (OLSN) and the Personalised Store Visualiser (PSV).

In the course of the CORAS project, this platform will be modelled in order to perform security risk analysis. We will further analyse these models (in parallel to CORAS) and use them as indicative examples to relate basic security and fairness properties to trust. During this analysis we will assess the effectiveness of, and further develop, the model of trust outlined in this paper. The results of the security risk analysis being conducted in CORAS will be used as input to our working model of trust management.

3. TRUST IN E-COMMERCE

In the physical world, we derive much of our notions of trust from the tangible nature of the entities in our environment. Our trust relies on personal contact, the tangibility of the objects and services, the difficulty of fraudulence and a clearly defined legal framework. Personal contact in virtual communities is limited, the legal framework is vague and the objects and services under negotiation are less tangible. The traditional notions of trust need to be rethought, and suitable models of trust in e-commerce have to be developed.

In this section we provide a rigorous definition of trust in e-commerce and analyse some general properties of trust proposed following surveys of recent attempts to formalise this concept [2],[3].

3.1 A working definition of Trust in e-Commerce

Although the importance of trust has been recognised, there is no consensus in the literature on what trust is. On the other hand, as it is elaborated in [3], many researchers assume an (unprovided) definition of trust and use the term in a specific way related to access control or to paying for purchases. In [2] we survey various attempts to provide some definition of trust that is suitable for e-commerce. Some aspects of these definitions are common, other are complementary. For example, [8] emphasises that trust is a belief in the competence of an entity within a specified context, while [3] lay stress on that the entity that manifests trust (the "trustor") is the human - not the system. They also emphasise that trust is in part subjective. A somewhat similar view is expressed in [4] where entities are distinguished into *passionate,* who have free will, and *rational,* who don't. According to [3],[4] trustors are *passionate* entities. The definition in [6] focuses on another aspect of trust: in commerce, *trust is relative to a business relationship.* One entity may trust another entity for one specific business and not in general. This diversity of the purpose of trust is also mentioned in [4] but not incorporated into a definition. Finally, none of the above emphasises that trust is not only inherently measurable but also it exists and evolves in time. We define trust as follows.

Definition 1: *Trust of a party A in a party B for a service X is the measurable belief of A in that B will behave dependably for a specified period within a specified context.*

Remarks:

- A party can be an individual entity, a collective of humans or processes, or a system; (obviously, the trustor must be an entity that can form a belief).
- The term service is used in a deliberately broad sense to include transactions, recommendations, issuing certificates, underwriting, etc.

- The above mentioned period may be in the past, the duration of the service, future (a scheduled or forecasted critical time slot), or always.
- Dependability is used broadly to include *security, safety, reliability, timeliness, and maintainabiliy* (following [7]).
- The term context refers to the relevant service agreements, service history, technology infrastructure, legislative and regulatory frameworks that may apply.
- Trust may combine objective information with subjective opinion formed on the basis of factual evidence and recommendation by a mediating authority.
- Trust allows one agent to reasonably rely for a critical period on behaviour or on information communicated by another agent. Its value relates to the subjective probability that an agent will perform a particular action (which the trustor may not be able to monitor) within a context that affects the trustor's own actions.

Notably, our definition differs from [4],[5] with respect to the trusting subjects. Intelligent agents who negotiate can be either humans or programs and in both cases they need to manifest trust intentions and establish trusting relationships. Intelligent software agents are adaptive autonomous programs featuring the ability to acquire knowledge and to alter their behaviour through learning and exercise. Their decision making can be enhanced so that they form trust intentions and make decisions relying on trust. Our definition differs from [3],[6],[10] with respect to the inherent measurability and the subjective nature of trust. It also differs from [3],[4],[7],[8] in that trust differentiates between services and it is active for critical periods of time.

We also note that distrust, accounting to what extent we can ignore one's claims about her own or a third party's trustworthiness and their proclaimed actions or commitments, is modelled as a measurable belief in that a party will behave *non-dependably* for a critical period within a specified context. Distrust is useful in order to revoke previously agreed trust, obstruct the propagation of trust, ignore recommendations, and communicate that a party is "blacklisted" for a class of potential business transactions.

3.2 Properties of Trust and Distrust

The particular characteristics of trust may differ from business to business. Nevertheless, there are some common delimiters that indicate the existence of general principles governing trust in e-commerce.

Proposition 2: The following are general properties of trust and distrust.

P1. *Trust is relativised to some business transaction.* A may trust B to drive her car but not to baby-sit.

P2. *Trust is a measurable belief.* A may trust B more than A trusts C for the same business.

P3. *Trust is directed.* A may trust B to be a profitable customer but B may distrust A to be a retailer worth buying from.

P4. *Trust exists in time.* The fact that A trusted B in the past does not in itself guarantee that A will trust B in the future. B's performance and other relevant information may lead A to re-evaluate her trust in B.

P5. *Trust evolves in time, even within the same transaction.* During a business transaction, the more A realises she can depend on B the more A trusts B. On the other hand, A's trust in B may decrease if B proves to be less dependable than A anticipated.

P6. *Trust between collectives does not necessarily distribute to trust between their members.* On the assumption that A trusts a group of contractors to deliver (as a group) in a collaborative project, one cannot conclude that A trusts each member of the team to deliver independently.

P7. *Trust is reflexive, yet trust in oneself is measurable.* A may trust her lawyer to win a case in court more than she trusts herself to do it. Self-assessment underlies the ability of an agent to delegate or offer a task to another agent in order to improve efficiency or reduce risk.

3.2.1 Propagation of trust

As we elaborate in the sequel, at least unintentional transferability of trust within a locus may be acceptable in specific contexts. *Note that "transferability" in our case corresponds to influencing the level of trust rather than relational transitivity.* We distinguish three special *roles* that entities mediating in a trust relationship can play. These roles are *guarantors, intermediaries,* and *advisors.* Note that an entity may play more than one mediating role in a business relationship.

Guarantor is a party taking the responsibility that the obligations of the parties she guarantees for are fulfilled at an agreed standard. Guarantors assist the establishment or facilitate the increase of trust for a specific transaction by underwriting (a part of) the risk associated with the transaction. A typical example is a credit card company.

Intermediary is a party that intervenes between other parties in a business transaction and mediates so that they establish a business relationship with or without their knowledge. We distinguish the following types of intermediary:

– *Transparent:* an intermediary that identifies the parties she is mediating between to each other. An example is `Lloydstsb. com,` a bank, who offer to their on-line customers a comprehensive car rental and flight booking service powered by `Expedia. co. uk,` an on-line travel agency. A trivial example is an entity that simply redirects to another entity.

– *Translucent:* an intermediary that identifies the existence of the parties she mediates between but not their identity. An example is a retailer advertising product delivery by courier without identifying which delivery company is responsible for this.

– *Overcast:* an intermediary that hides the existence of the parties she is mediating between from each other. Examples include virtual enterprises, and ventures selectively outsourcing tasks to unidentified strategic allies.
– *Proxy:* an intermediary who is authorised to act as a substitute of another entity.

Advisor is a party that offers recommendations about the dependability of another party. Advisors include the authorities maintaining blacklists for a community. Examples include, credit scoring authorities and reputation systems.

Proposition 3: Trust and distrust propagate according to the following rules:

P8. *(Dis)trust is not transferred along an overcast intermediary.* Assume that A (dis)trusts an overcast intermediary T for a service X provided by B. Since A is not aware that B provides the service, her (dis)trust is placed in T.

P9. *Trust is transferred along transparent intermediaries – distrust is not.* Assume that, for a service X, A trusts a transparent intermediary T mediating for B. By agreeing to the service, A expresses trust in B for X instigated by T's mediation.

P10. *(Dis)trust in a subcontractor of a transparent intermediary is transferred to (dis)trust in the intermediary.* If a party A (dis)trusts a subcontractor of a transparent intermediary T for a service X, then A is inclined to (dis)trust T for this particular service.

P11. *Trust is transferred anonymously along translucent intermediaries – distrust is not.* Assume that A trusts a translucent intermediary T for X and T trusts B to subserve for X. By agreeing to the service, A effectively expresses trust in a third party to subserve for X without necessarily knowing identity of that party.

P12. *Trust in an advisor is transferred to the recommended party - distrust is not.* The more A trusts T the more she relies on her recommendation.

P13. *Distrust in a recommended party is transferred to the advisor – trust is not.* A's distrust in a party B recommended by T for a service X prompts A to question T's competence as an advisor for X.

P14. *Advisors distinguish between recommendation based on "first hand" and "second hand" evidence. In the latter case they ought to identify their sources.* If T_1 and T_2 both pass to A advise by T as their own observations then T gains an unfair advantage in influencing A. See section 4.2 of [9] for further analysis.

P15. *Distrust propagates through trust and it obstructs the propagation of trust.* If A distrusts an intermediary T for a service X then A will ignore T's mediation to the extent of the distrust.

Note that P9, P10 and P12, P13 allow for trust and distrust to be transferred in opposite directions. This does not necessarily result in a conflict. The opposite initial values will affect each other and the final decision will depend on the resulting balance between trust and distrust in each party, and the tendencies of the trustor. This would not have been possible, had trust been viewed as a binary operator, because transitivity of trust would have lead to inconsistency.

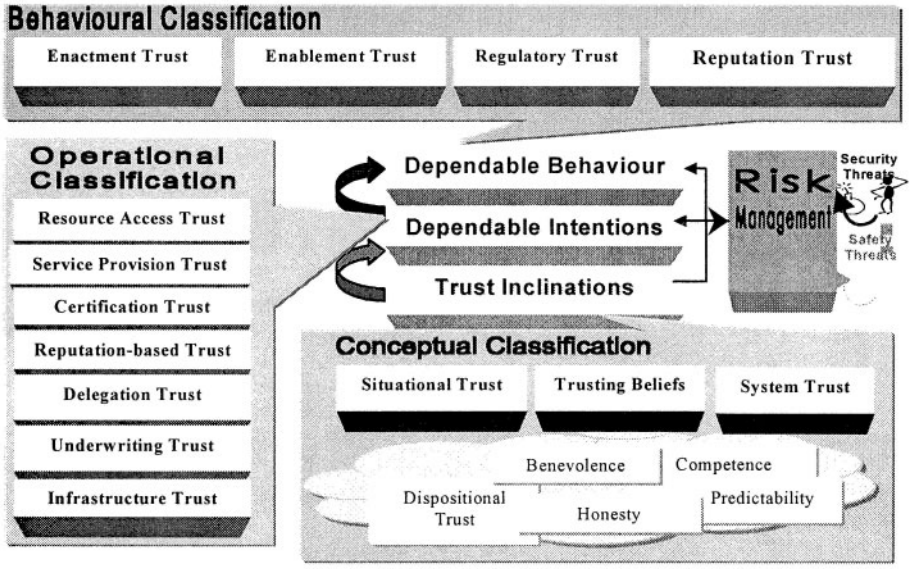

Figure 3. A pictorial overview of the proposed trust-management scheme

4. TRUST MANAGEMENT

The term *trust management* was introduced in [10] addressing the problem of developing a *"coherent intellectual framework... for the study of security policies, security credentials and trust relationships"*. It was the first time that issues such as *providing a unified mechanism, locality of control,* and most importantly, *separating mechanism from policy* were paid enough attention. Indeed, solutions to the shortcomings of existing trust management systems can be better addressed by separating the trust management framework from the purpose of the application. To achieve this, we need to systematise the development of control mechanisms and trust-based policies across all aspects of dependability, including security.

Trust management aims to provide a coherent framework for determining the conditions under which a party A takes the risk to depend on a party B with respect to a service X for a specific period within a specific context, and even though negative consequences are possible. Increasing the levels of trust facilitates processes to become more efficient but also increases the risk of allowing for the exploitation of vulnerabilities. One would consequently aim, in principle, to *maximise trust while minimising risk.* Hence, trust management subsumes and relies on risk management:

1. One may employ tailored risk analysis in order to analyse environmental risks and assess the most tangible aspects of trust (e.g. the dependability of the information technology infrastructure).

2. Risk management allows us to weight transaction risk against trust, evaluate the impact of a failure in trust and help device countermeasures.

Note that the above two analyse different types of risk (cf. section 4.1.4).

4.1 Classifications of trust

Trust management becomes more tractable in the presence of a conceptual classification of the different aspects of trust and the different ways they influence behaviour. For this purpose, we have adapted the conceptual framework proposed in [7]. Our adaptation extends the approach proposed in [11] and includes the following concepts summarised in *Figure 3.*

4.1.1 Trust inclinations

Trust inclinations is an intentionally broad term referring to the tendencies of an agent. These are typically influenced by the agent's own view of the environment it inhabits, by the extent it is willing to depend on another potentially unknown agent in a given circumstance, and by the extent it perceives the known institutions and infrastructure to be dependable.

The following classification focuses on trust inclinations inherent in an agent or acquired through the agent's exposure to an environment. (See also *Figure 3.*)

Situational trust measures the extent to which a party is willing to depend on an unspecified party in a specific role and a given circumstance.

Beliefs describe an agent's schema about the environment it inhabits. Four categories of primitives contribute to belief formation [7]:

– *benevolence,* i.e. the belief that one cares about the others welfare;
– *honesty,* i.e. that one makes an agreement in good faith;
– *competence,* i.e. that one is able to perform a specific task;
– *predictability,* i.e. that one's behaviour is predictable in a given situation.

Dispositional trust is a fifth primitive referring to an agent's persistent tendency to trust oneself and others across a wide spectrum of situations.

System trust measures the extent to which an agent believes that it can depend on the known institutional structures such as legislative, regulatory, reputation systems and the underlying technology infrastructure.

4.1.2 Dependable intentions

Dependable Intentions describe the extent to which a party is willing to depend on other parties (including oneself) for a specified period, within a specified context and in relation to a specific service. Dependable intentions can be modelled within policies, where a **policy** is viewed as *"a rule that can be used to change the behaviour of a system"* (following [12]). In decentralised open distributed systems,

policies apply *within a locus,* i.e., a subsystem. As perception and knowledge evolve, an agent may find herself in a position where, according to one policy, pursuing a business relationship with another agent is to her interest, but according to another policy, the same business relationship with the same agent has to be avoided. **Meta-policies** (i.e., policies *"about which policies can coexist in the system or what are permitted attribute values for a valid policy"* [12]) are particularly useful for resolving such conflicts [13].

An operational classification of trust relates to this viewpoint (*Figure 3*), focusing on how the intention to trust is controlled and exercised.

- **Resource Access Trust:** for the purposes of a service X, A trusts B to access resources that A controls. This type of trust forms the basis for authorisation policies that specify actions the trusted party can perform on the resources, and constraints that apply such as time periods for when the access is permitted.
- **Provision of Service Trust:** A trusts B to for a service X that does not involve access to A's resources. Application service providers (ASPs) are typical examples of entities that would require service provision trust to be established.
- **Certification-based Trust:** A trusts a B for a service X on the basis of criteria relating to the set of certificates presented to A by B and provided by a third party C. Certificates are commonly used to authenticate identity or membership of a group.
- **Reputation-based Trust:** A trusts B for a service X on the basis of criteria relating to the opinions of other parties who have considered interacting with B in the past for similar services. Examples include reputation systems in e-auctions such as `eBay.com`. This type of trust is often complementary to certification-based trust.
- **Delegation Trust:** For a service X, A trusts B to make decisions on A's behalf about resources that A owns or controls. Examples include the delegation of decisions regarding investment to one's financial advisor.
- **Underwriting Trust:** A trusts B for a service X based on criteria related to the reduction of risk caused by the intervention of a third party C underwriting X. Examples include insurance companies underwriting loss or damage, and credit-card companies guaranteeing payment for a purchase.
- **Infrastructure Trust:** For the purposes of a service X, party A trusts the base infrastructure (subsystem B) upon which the provision of a service will take place.

4.1.3 Dependable behaviour

Dependable behaviour describes the extent to which a party behaves dependably. It implies acceptance of risks (potential of negative consequences) and their effect. At this level, the agent's inclinations and intentions have been analysed and endorsed resulting in patterns of behaviour.

The following classes of trust relate to this viewpoint (*Figure 3*), focusing on the roles of the stakeholders as they engage in a business relationship.

- **Enactment trust** is the trust between parties that engage in a business relationship through e-services, including customers and retailers.
- **Enablement trust** is the trust in those who enable or mediate in the provision of e-services including the technology and platform providers.
- **Regulatory trust** is the trust in the legislative, regulatory, standardisation and advisory bodies for e-business at a local or a global level.
- **Reputation trust** is the trust in reputation systems or the recommendation of arbitrary agents.

4.1.4 Risk management

Risk management is the *"total process of identifying, controlling and minimising the impact of uncertain events"* [14]. Risk management often involves a form of risk analysis. The latter is *"the process of identifying risks, determining their magnitude, and identifying areas needing safeguards"* [14]. Risk analysis is critical for achieving the right means of abstracting information from reality into a formal model. Its importance has been recognised in the process industry and finance – business areas where elegant methods for risk management have been developed. As is depicted in *Figure 3,* we see risk management supporting the analysis of trust inclinations leading to the formation of trust intentions, and the analysis of trust intentions leading to the endorsement of dependable behaviour. We anticipate different kinds of risks to be analysed in these two phases. The focus in the former case is on analysing the effect that an agent's persistent tendencies and risks from the environment have on the formation of this agent's trust for a specific service. The focus in the latter case is on balancing intentions to trust against interaction risks in order to endorse an informed and dependable behaviour.

Ideally, risk management should be applied across all aspects of dependability. However, the increasing complexity of today's systems urges the improvement of existing methods of analysing systems and their specification in order to increase the likelihood that all possible threats are taken into consideration. There is therefore a need for combining different risk analysis methodologies with respect to the system architecture. For example, qualitative methodologies for analysing risk lack the ability to account for the dependencies between events, but are effective in identifying potential hazards and failures in trust within the system, whereas tree-based techniques take into consideration the dependencies between each event. We are not aware of an already developed integrated approach to system modelling and risk analysis, where the architecture of the information system model is used to guide the combined application of risk analysis techniques. This need is being addressed in CORAS [15],[16] for the area of security risk analysis. We aim to build

on the work of CORAS extending the integrated risk analysis and system-modelling framework to support analysing trust in e-services.

5. CONCLUSION

The pliability of the emerging communication media, the complexity of plausible interactions in virtual communities and the frequency of critical interactions among people who are relative strangers lead to problems that may not arise in traditional social settings. Yet, the same pliability abides an unprecedented degree of engineering and allows for solutions to many of these problems. However, effective solutions require interdisciplinary approaches requiring the integration of tools from cognitive sciences and economics in addition to telecommunications and computing.

In this paper, we introduced a rigorous model of trust in e-commerce and presented general properties of trust that underlie e-services, highlighting a role-based approach to the analysis of (unintentional) transfer of trust. We proceeded by proposing a trust management scheme, which included *(i).* an hierarchical decomposition of trust into inclinations, intentions and behaviour; *(ii).* a classification of the basic types of trust in each viewpoint. We suggested that risk analysis and role-based modelling can be combined to support the formation of trust intentions and the endorsement of dependable behaviour based on trust.

Concluding, we provided evidence of emerging methods, formalisms and conceptual frameworks which, if appropriately integrated, can bridge the gap between systems modelling, trust and risk management in e-commerce. However, there is still a long way to go. Further work and foreseen research challenges include:

– *To formalise and evaluate the proposed role-based model of trust in e-commerce.* (Preliminary results have been reported in [17] and [18]).

– *To extend on-going work* [15] *on integrating systems modelling and security risk analysis by correlating risks with trust.* This also involves understanding how to combine suitable risk analysis methods across different areas of dependability.

– *To develop risk management techniques supporting the transition between trust inclinations, intentions and dependable behaviour.* An output is to produce practical guidelines for the attention of regulators and technology providers on how to maximise trust and minimise risk in different e-service scenarios.

– *To embody trust-based decision making in the policy-based management of decentralised open distributed systems.* This involves enhancing the management of decentralised distributed systems with methods to simulate learning, reasoning and analysing transactional and environmental risks, and enabling the *dynamic evaluation* of the trust associated with each transaction.

– *To embody trust elements in contract negotiation, execution monitoring, re-negotiation and arbitration.* This involves modelling legal issues concerning the status of electronic agents as participants in the process of contract formation.
– *To experiment with developing a virtual marketplace from scratch, taking trust issues into account throughout the development lifecycle.*

6. ACKNOWLEDGEMENT

Motivating and fruitful discussions with the CORAS partners and the participants of the CLRC/CORAS workshop on *"Semi-formal Modelling, e-Risk and e-Trust"* [12] contributed to the improvement of this paper.

7. REFERENCES

[1] UK-online Annual Report, year 2000, http://wwww.ukonline.gov.uk
[2] T. Dimitrakos. System-models, e-Risks and e-Trust. CLRC working paper. http://www.itd.clrc.ac.uk/PublicationAbstract/1331
[3] T. Grandison and M. Sloman. *A Survey of Trust in Internet Applications* IEEE Communications Surveys and Tutorials, Fourth Quarter 2000.
[4] A. Kini and J. Choobineh, *Trust in Electronic Commerce: Definition and Theoretical Consideration.* Proc. 31st International Conference on System Sciences, IEEE, 1998.
[5] A. Jøsang, *The right type of trust for distributed systems.* Proc. of the New Security Paradigms Workshop, ACM, 1996.
[6] S. Jones, TRUST-EC: requirements for Trust and Confidence in E-Commerce, European Commission, Joint Research Centre, 1999.
[7] J.C. Laprie, *Dependability: Basic Concepts and Terminology,* Springer-Verlag, 1992. D.H. McKnight and N.L. Chervany. *The Meanings of Trust.* Technical Report MISRC Working Paper Series 96-04, University of Minnesota, 1996. See also [19]
[8] A. Jøsang and N. Tran. *Trust Management for E-Commerce.* Virtual Banking 2000.
[9] A. Jøsang. *An Algebra for Assessing Trust in Certification Chains.* In Proc. Network and Distributed Systems Security Symposium. The Internet Society, 1999.
[10] M. Blaze, J. Feigenbaum and J. Lacy, *Decentralized Trust Management.* Proc. IEEE Conference on Security and Privacy, Oakland, CA. May 1996
[11] D. Povey, *Developing Electronic Trust Policies Using a Risk Management Model.* In LNCS, Vol. 1740, Springer-Verlag, 1999.
[12] N. Damianou, N. Dulay, E Lupu and M. Sloman. *The Ponder Policy Specification Language* Proc. Policy 2001: Workshop on Policies for Distributed Systems and Networks, Bristol, UK, 29-31 Jan. 2001, Springer-Verlag LNCS 1995, pp. 18-39
[13] E.C. Lupu and M. Sloman, *Conflicts in Policy-Based Distributed Systems Management.* IEEE Trans. on Software Engineering, 25(6): 852-869 Nov. 1999.

[12] Workshop hosted at Rutherford Appleton Laboratory in conjunction to the 2nd CORAS meeting. See http://www.itd.clrc.ac.uk/Activity/CORAS+1087 for contributed talks.

[14] *Information technology-Security techniques-Guidelines for the management of IT Security (GMITS)Part1: Concepts and models for IT Security.* ISO/IEC TR13335-1:1996

[15] K. Stølen. CORAS: A Platform for Risk Analysis of Security Critical Systems. Proc. The International Conference on Dependable Systems and Networks, 2001 (To appear)

[16] *CORAS Web* http://www.nr.no/coras See also http://www.itd.clrc.ac.uk/Activity/CORAS

[17] T. Dimitrakos, *Modelling Trust in e-Commerce.* Proc. AI 2001 workshop: Novel E-Commerce Applications of Agents. Ottawa, Canada, NRC-44883, June 2001.

[18] T. Dimitrakos and J.C. Bicarregui. *Towards modelling e-trust.* Proc. 3rd Panhellenic Symposium on Logic, Anogia academic village, Crete, Greece, July 2001.

[19] D.H. McKnight and N.L. Chervany. *What is Trust? A Conceptual Analysis and an Interdisciplinary Model.* Proc. The 2000 Americas Conference on Information Systems (AMCIS2000). AIS, Long Beach, CA, August 2000