2010 IEEE 24th International Conference on Advanced Information Networking and Applications Workshops

A High-level Semiotic Trust Agent Scoring Model for Collaborative Virtual Organisations

Tim French
Department of Computer Science and Technology/ Informatics Research Centre, University of Reading
University of Bedfordshire
Park square, Luton, LU1 3JU, UK
0044 (0) 1582 489101
tim.french@beds.ac.uk

Nik Bessis
Department of Science and Technology
University of Bedfordshire
Park square, Luton, LU1 3JU, UK
0044 (0) 1582 743476
nik.bessis@beds.ac.uk

Carsten Maple
Department of Science and Technology
University of Bedfordshire
Park square, Luton, LU1 3JU, UK
0044 (0) 1582 489164
carsten.maple@beds.ac.uk

ABSTRACT
In this paper, we describe how a semiotic ladder, together with a supportive trust agent, can be used to address "soft" trust issues in the context of collaborative Virtual Organisations (VO). The intention is to offer all parties better support for trust (as reputation) management including the reduction of risk and improved reliability of VO e-services. The semiotic ladder is intended to support the VO e-service lifecycle through the articulation of e-trust at various levels of system abstraction, including trust as measurable confidence. At the social level, reputation and reliability measures of e-trust are the relevant dimensions as regards choice of VO partner and are also relevant to the negotiation of service level agreements between the VO partners. By contrast, at the lower levels of the trust ladder, e-trust measures typically address the degree to which secure sign on and message level security conforms to various tangible technological security protocols. The novel trust agent provides the e-service consumer with an objective measure of the trustworthiness of the e-service at run-time, just prior to its actual consumption. Specifically, VO e-service consumer confidence level is informed, by leveraging third party objective evidence. This evidence comprises a set of Corporate Governance (CG) scores. These scores are used as a trust proxy for the "real" owner of the VO. There are also inherent limitations associated with the use of CG scores. These are duly acknowledged.

Categories and Subject Descriptors
B.4.4, C.2.4, D.4.3, D.4.4, D.4.5, D.4.6, D.4.8, H.1.2, I.6.5, I.6.8

General Terms
Management, Measurement, Reliability, Security.

Keywords
Semiotic ladder; light-weight trust agent; scoring system; corporate governance score; past performance history.

1. INTRODUCTION
Whilst tangible VO e-services are relatively well understood, intangible "soft" trust issues, particularly with respect to trust measurement amongst VO e-partners is a much less well-developed area. Most VO collaborations are mainly concerned with the verification and exchange of security tokens [1] using a mixture of SSL (Secure Sockets Layer) certificates for user authentication and virtual X.509 digital certificate credentials. For example, initiatives such as the SECURE project [2] seek to develop and enable trust agents with the power to exchange and verify electronic credentials, to gather local evidence, and to verify local data security access rights. In turn, a distributed agent or entity seeks to partially mimic human trust or mistrust formation in respect of its own predetermined trust orientation (mistrustful, trustful or neutral), a set of trust criteria, and the evidence gathered during a trust even.

Computational models of trust mechanisms based on explicating notion of trust in the context of VO e-services have only recently emerged [3]. One need for this is that traditional security mechanisms are being increasingly challenged by open, large scale and decentralised environments. This situation naturally leads to a highly decentralised model of security, risk and trust as between VO partners in some pre-determined orchestrated manner. Several works are currently examining relevant trust issues at the VO level of abstraction, including work from the TrustCOM project [4]. These works claim to deal with high-level "reputation" issues. However, much of these works actually seek merely to address tangible security aspects and performance aspects [5]. Among the first works to establish the need to examine "soft" trust issues is described in Song. Their trust index is calculated using a mixture of inputs including the site's defence capabilities and site reputation, defined as a performance track record. Their solution is relatively "heavy-weight". A large number of inputs are used to calculate the trust index, via the use of neural network based techniques. In contrast, our contribution seeks to support both the design of VO partnership lifecycle via a semiotic trust ladder as well as the runtime execution of "light-weight" agent. Our model is designed to quantify VO "reputation" using two relatively simple measures: corporate governance scores and past performance history.

With this in mind, the paper's aim is multifold: firstly, to briefly present our rationale; secondly, to introduce the semiotic e-trust viewpoint by presenting the trust ladder role as well as the role of trust agents and semiotics; thirdly, discuss in full our proposed high-level semiotic trust agent model and its limitations.

2. SEMIOTIC E-TRUST VIEWPOINT
We suggest that a semiotic e-trust viewpoint offers a unifying conceptual framework within which to model and conceptualise

978-0-7695-4019-1/10 $26.00 © 2010 IEEE
DOI 10.1109/WAINA.2010.173

trust. The aim is to make e-trust issues transparent throughout the VO collaborative partnership "lifecycle" using a viewpoint that is not itself necessarily tied to any particular platform or XML standard.

A collaborative e-service consumer needs a method of secure single sign-on authentication, followed by access to single multiple VO resources. A VO consumer needs to be assured that only authorized parties can gain access to sensitive data. It is of course essential that local security measures and standards work seamlessly with global VO level trust and security measures. A VO consumer also needs to be assured that the reputation of the VO provider and also its "real" corporate owner is adequate, hence the risk of e-service failure or interruption is minimized. Adequate support for VO e-service delegation is required (i.e. a program initiated on a consumer's behalf may need the ability to delegate a task to another program), located elsewhere amongst the VO partners. The use of a trust ladder [6] is intended to make some of these complex issues more transparent, hence aiding the VO e-trust lifecycle.

We argue that within VO collaborative partnerships wider organizational and cultural factors influence human trust formation, not merely local contextual cues. In particular, human trust formation involves wider trust contexts: organizational, social, and human cultural factors pre-determine human trust formation and expectations and beliefs. Furthermore, human trust is also ultimately not merely a rational cognitive construct but has a strong emotional component [6]. For this reason, we propose that current models and approaches to autonomic trust formation should seek to endow agents and entities with wider more subtle "soft" contexts, hence seek to more closely mimic human-to-human trust formation.

In the "real" corporate world third party scores (such as credit rating agencies) are used by businesses to assess the risks of engaging with other businesses via partnerships of various kinds. Though such scoring systems have recently been criticized recently in relation to the so-called "credit crunch", their use is ubiquitous and is often supplemented by other measures, with respect to UK banks for example such as Corporate Governance scores, measures of Capital Ratios *et al.* [7]. Hence, the use of Corporate Governance (CG) scores to support a trust agent model is at least partially justified by the current usage of third party objective corporate trust metrics within "real" corporate business partnerships. Previously, the general assumption has been that merely enabling a set of tangible security technological mediators will be a necessary and sufficient condition to invoke 'trusted' VO services. Our work explicitly seeks to questions this assumption as will be seen.

2.1 Role of the Trust Ladder

Human trust is an elusive and subtle concept that involves reference to local as well as wider organizational social settings within which e-service transactions occur [8]. Existing approaches to trusted VO e-services have over emphasized the value of establishing secure communications between autonomic entities, at the expense of addressing these wider dimensions. Liu [9] has previously called for a wider examination of so-called "soft" issues within VO collaborative contexts and identifies the semiotic paradigm as being central to address these wider concerns.

Table 1. Macro-dimensions of the VO lifecycle and the semiotic trust ladder

Exemplar Grid Service Trust Issues	*Semiotic Trust Ladder*	*Applic-ability (VO Lifecycle)*	*Signs*
Does the Service conform to desired VO cultural norms? Are there any legal safeguards?	***Social world***: trust beliefs and expectations.	Planning stage.	Cultural/ Social trust; Policy signs.
Reputation of grid- service consumer or provider? Any ethical conflicts?	***Pragmatics***: goals, intentions, trusted negotiations, comms.	Planning, build and run time.	Reputation signs.
How reliable, valid are the services and will they meet quality norms?	***Semantics***: meanings, truth/ falsehood, validity.	Build and run time.	Authentication/ validity signs.
Secure agents: how trusted are they?	***Syntactics***: formalisms, trusted access to data.	Build and run time.	Trusted access signs.
Are the intrusion detection/ prevention controls adequate?	***Empirics***: entropy, channel capacity.	Run time.	Messaging/ traffic management signs.

In response to this suggestion, we map "soft" and "hard" VO e-trust concerns to a novel semiotic ladder, as shown within Table 1 above. The trust ladder currently functions as a kind of meta-model, within which VO partners can conceptualize e-trust issues within a typical partnership, from its earliest inception to design and implementation. By attempting to identify and map trust issues to the trust ladder, it is hoped that previously implicit or poorly understood or articulated trust issues may be more clearly revealed to VO partners at an earlier stage in the VO lifecycle than hitherto. The intention is for the VO partners to use the high-level model as a reference point for e-trust issues at each stage of the evolution of a VO partnership, thus making the issues fully explicit. It is expected that for any given e-service VO

partnership, the ladder will become refined and indeed tailored by the partners themselves, so as to best meet their needs.

For example, at the planning and building stages of a grid, partners need to address and collect various sources of top-level organizational reputation. Furthermore, legal agreements of various kinds will need to be entered into and perhaps automated by standards such as WS-Agreement. Any mismatches between partners (in terms of trust thresholds, expectations or e-service level policies) will need to be resolved through negotiation. During run-time execution, partners will need to continuously check with one another that the agreements previously entered into are being implemented in the expected manner. Typically, validation of security aspects will be a major concern. One recommended method of validating the agreements entered into during the earlier stages of the ladder, may well take the form of trust agents. These agents need to be enabled with sufficient knowledge so as to check high-level norms and policies as well as low-level access rights. In a sense therefore these agents will act as the self-validators of the agreements and policies identified in the earlier stages of the ladder itself. An open question at present is the detection of intrusion via vulnerabilities of various kinds. Little is known about intrusion at the present time. To validate this part of the ladder, VO partners will however, need to anticipate intrusion (hence vulnerabilities) and will need to carry out a vulnerability analysis that is relevant to the particular security standard chosen (e.g. SSL/TLS, proxy X.509 certificates, Shibboleth). Whilst little has been published thus far, intrusion detection is likely to become a more important issue, as VO's increasingly form academic-business partnerships.

Whilst the layers of the ladder are clearly invariant, and the use of trust agents is also pre-supposed, the exact methods, tools and techniques used at each level of the trust ladder to verify e-trust signs remain open. The main idea therefore is to use the ladder as a generic framework within which the partners themselves can seek to validate and negotiate agreements, with each other, rather than a set of prescriptive set of tools and techniques. That is to say the ladder is designed to be self-tailored by the VO partners.

2.2 Role of the Trust Agents and Semiotics

A means of enabling an agent with human like rational reasoning concerning trust and irrational (emotional) human like trust responses to trust is ideally needed to fully simulate human trust formation. Pioneering work has already been carried out by researchers in developing and applying various mathematical formalisms that can be used to design and implement trust models within autonomic systems. Many of these formalisms [10] rely on the calculation of local trust thresholds of various kinds and their subsequent propagation across nodes via graph-theoretic models [11]. This approach is currently being extended so as to seek to enable MAS (Multi-agent Systems) with the power to investigate trust credentials, provenance and reputation. Thus far however, progress appears to be limited to various high-level models and proposed prototype solutions. Readers seeking a full review of the relevant MAS literature are directed to the EU 6th Framework Project "eRep" website. Traditional work in Artificial Intelligence research enables the probing of the mental states of other agents with respect to their state of mind (intentions, beliefs, and goals). This and other work will perhaps in the future enable a MAS (Multi-Agent Systems) to fully simulate human trust formation in all its richness, including emotional and cognitive aspects. In the meantime, we believe that a somewhat less ambitious yet rigorous approach is needed to assess VO high-level reputation using a computationally and analytically lightweight methodology. In the longer term a richer model and approach will inevitably be needed, but as yet the whole area of "soft" trust is still an emergent one within e-systems, with many conflicting models and solutions [12].

The contribution described here is to be regarded as a lightweight, pragmatic model that does not seek to be fully comprehensive. Rather, the model though simplistic, is intended to offer an exemplar pragmatic means to leverage current technologies to address VO "soft" trust using one (exemplar) third party measure: namely Corporate Governance (CG) scores.

3. A HIGH-LEVEL SEMIOTIC TRUST AGENT MODEL

The key issues that an agent based approach should seek to satisfy is related to the extent to which a requested e-service should (or should not) trust in the ability, of a service provider to fulfill a particular request to a given level of service quality. From the preceding discussion it is clear that some kind of dynamic VO trust verification process is required.

Our approach provides information about the service provider's "real" organizational reputation to the VO consumer whilst also leveraging any previous service history (reliability) data, in order to (at least partially) fill the VO trust "gap". Our approach takes the form of a design (a set of requirements) for an agent-based solution is presented. The intention is to show from a top-level viewpoint, that VO agent-to-agent mediated systems (such as grid and web-services) can be supported using a semiotically informed trust model. The following working trust definition from [13] is used as the starting point for the agent design, where measurable "belief" means in this case a trust metric that combines and reflects both top-level organizational reputation and any previous e-service history:

"*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"* p.5

The following stages of local and global trust management in the context of a VO seeking to check trust credentials just prior to invoking a request for a generic e-service is given below. Two agents working co-operatively are assigned to support the task: Agent-1 ["Local trust agent"] and Agent-2 ["Global trust agent"]:

1. A service request is made originating within a given VO, named service requestor, which seeks to request and invoke a given service originating from outside that VO. The request is sent to Agent-1 in the form of a message.

2. Agent-1 responds to the request by looking up the service in a "Registry Yellow Page" (such as a UDDI registry) of VO's and their services that are accessible by all existing VO's in the grid environment.

3. Agent-1 finds the service (if not found or not available a suitable error message is sent back to the requestor). Every available service is mapped to at least one VO, named service provider.

4. Agent-1 passes the name of the service provider to Agent-2. Agent-2 then looks up a global VO Trust Table for their

rating details by calculating a global trust score for that VO. The global VO Trust Table contains a series of ratings that, when combines, are used to calculate a trust rating based on various "Corporate Governance" (CG) scores.

5. Agent-2 calculates the sum of the scores and returns a single integer value to Agent-1.

6. Agent-1 compares the received global trust rating to see if it lies within the acceptable range of the VO e-service requestor. The global trust score is defined as a real number normalized in the range [0-1] wherein a low value or range of values (such as 0-0.1 for example) indicates a very low level of trust and where high values (for example 0.9 - 1) represents a highly trusted VO. An acceptable range represents the minimum score that falls within a particular consumer's own individual preferred trust confidence level. For example, a VO consumer might typically specify that they only wish to consume a particular VO e-service, if Agent-1 returns a global trust rating > 0.5. If the global trust score lies below the minimum level (or minimum range of values) deemed by a particular VO e-service consumer to be acceptable then, the service request is terminated with a suitable diagnostic message sent to the service requestor. The procedure can go to Stage 3 to check if the requested service can be available by another VO. If not, the procedure is terminated. If the trust rating is acceptable (within the acceptable range of the service requestor), Agent-1 proceeds with Stage 7 by sending a message to Agent-2.

7. Agent-2 looks up the VO Previous Performance table, which shows recent real time performance (Previous Performance Measure) of the VO e-service provider and passes the value back to Agent-1. If minimal acceptable performance criteria are met (e.g. history of node failures is within a pre-defined acceptable boundary value) then Agent-1 flag's the service request as "low-risk" so as to allow the service request to continue. If not, the service request is terminated.

8. Finally, Agent-1 checks the service requestor's access rights and privileges, to see if the requestor has the necessary permissions (as defined by role, security and time delimiters) to access the required service and hence local data sets residing outside the current VO.

3.1 Role of Global Trust Table

Marsh, [10] made an early attempt to formalize the notion of the trust for computational use in interactions between two autonomous agents. This approach takes into account many of the widely accepted aspects of trust in the relevant literature, i.e. defining basic or dispositional trust, general trust in another entity and situational trust in another entity, combined with the notions of utility, risk and importance. From this, simple linear equations allow the formation of trust values, which are represented in the range [-1, 1] to allow for reasoning about distrust. Trust information (values representing payoff) from past interactions of an agent is stored, allowing evolution of trust, albeit in a rather arbitrary manner.

The concept of a threshold for trusting behaviour based on the perceived risk and competence in the situation, demonstrates the inherent relationship between trust and risk. One of the basic requirements of a computational trust model is that it should provide a metric for comparing the relative trustworthiness of different agents. An agent is deemed trustworthy if it has a high probability of performing a particular action, which in our context, is to fulfill its obligations during an e-service interaction. This probability can be related to a wide variety of inputs. The function of the GTT (Global Trust Table) is to provide a set of inputs that serve to increase the confidence level (the probability whether subjectively or objectively determined) that a VO will perform a task successfully, and reliably. The approach adopted here is inspired by Marsh, in that he advocated the use of trust scores, which although simplistic, are computationally lightweight enough to be used within realistic dynamic VO contexts. The lightweight approach advocated here, is ideally suited to reduce latency time within demanding high-performance environments.

The main assumption made is that of the availability of data for VO high-level reputation. Organizations such as the Investors Shareholder Services (ISS) now publish data for CG (Corporate Governance) scores for major corporations, so it would seem reasonable to assume that such data can be readily accessed. Our lightweight scoring model takes its inspiration from large-scale collaborative funded projects such as the TrustCOM consortium in its treatment of high-level VO reputation management issues. That is to say we propose a scoring system provided by a trusted third party in which it is assumed that "reputation" can be scored using one or more CG metrics. This approach to quantifying reputation (hence trust by proxy) and associating this with company valuations appears to be already widely accepted in the relevant literature [14]. Some of the more obvious limitations are briefly outlined in (i) - (iv) below, where the scope of the present model is also clearly stated:

i) Our suggested method is only applicable to VO partnerships formed from parent organizations that come within the scope of the UK Combined Code on Corporate Governance. It is acknowledged that the Combined Code is mandatory only for certain classes of corporate entity, and only then within the UK. One example of a VO collaboration that would fall within the Combined Code and regulatory remit of the FRC (Financial Reporting Council) being a collaborative VO e-service partnership between several high-street UK banks. Similarly, collaborative VO partnerships between UK listed companies would also come under direct scope of the Combined Code.

ii) Private businesses within the UK and some public bodies (such as NHS foundation trusts) would not be formally covered by the code. Hence CG scores might either typically unavailable, or else be available on a voluntary, hence un-audited (unreliable) basis. Partnerships arising from VO collaborations outside the UK would fall outside the stated scope of the method entirely.

iii) VO partnerships may often involve parent company/ organizations that are based anywhere in the world. Such partnerships might also often involve partnerships between VO parent bodies and organizations that lie entirely outside the scope of CG metrics. One significant example is the e-science initiative, in which academic bodies worldwide collaborate amongst themselves and with large PLC's to engage in novel drug research via the grid. The use of CG scores in such a situation would be one of a VO trust asymmetry amongst the other VO collaborators.

iv) Almost certainly CG scores would be available to the agent model (in some usable form at least), in the case of the large PLC drug companies, whether based in the UK or not. However, CG scores would not be available in the case of their University partners, or other public bodies that were owners of VO's.

Within the limitations expressed here, the role of the GTT is to verify the trustworthiness of the owner of the VO e-service provider (expressed as a set of CG scores) as a proxy for trust in the VO e-service itself. In the human world it is a commonplace observation that we invest our trust in entities that are known to us through brand identity and reputation. In order to design an agent-to-agent solution it is necessary to use a proxy for trust that reflects high-level organizational reputation that is objectively measurable (so as to satisfy the earlier definition). CG scores are one such measure. CG indexes and scores are both publicly available and have been shown to correlate well with firm performance [14]. Similar indexes have been generated for e-government. Thus, they are potentially valid as a trust proxy, though is has already been noted they are necessarily limited in their present scope.

The solution outlined above assumes that the requestor passes a trust threshold value to Agent-2. This value can be assumed to be normalized to a value within the range 0 to 1. Agent-2 then looks up the service provider's originator (the real organization that owns the VO) to see if an entry exists in the GTT. If an entry exists then a set of individual scores ($x_1,x_2...x_n$) pertaining to a particular companies entry are summed and scaled to a real-value in the range [0-1]. Agent-1 then simply compares the values to see if according to the service originator the trust value (reputation) lies within an acceptable range.

If the value does lie within an acceptable range then a check is then made of any relevant service history. If this check indicates that the service history lies within an e-service consumer's acceptable tolerance range then the service is enabled. An exemplar is presented in the next section so as to show how the lightweight model might operate in practice. The process is essentially a two-stage model: VO reputation trust is measured and compared to a threshold value (Trust Threshold Score), followed by any known previous service performance history (Previous Performance Measure). If no-history is available a service log is then generated accordingly in real-time.

3.2 Agent Scoring Model

In the following illustrative example Basepoint Bank (UK) is the (fictional) owner of a VO that provides a publishable e-service to VO consumers. In this case the consumer is another UK bank (let us say Barclay's Capital PLC). This particular e-service is needed by Barclay's Capital on demand to determine the forward pricing of a complex financial derivative instrument, known as a "quant99". Barclay's needs a result within 20 ms thus very low system latency is required. Note that the service may be provided by more than one VO. Thus Barclay's Capital potentially has a choice of provider. Barclay's Capital has previously agreed to use CG scores as a trust proxy since the various alternative VO e-service providers of the "quant99" pricing e-service are all owned by UK Banks, hence come within the remit of the Combined Code. Let us further assume that Barclay's Capital has previously used the e-service owned and operated by Basepoint and provided by a VO, so there is (for simplicity) both an existing TTS Trust Threshold Score and PPM Previous Performance Measure for the "quant99" e-service as published by Basepoint Bank.

i) The service requestor (Barclay's Capital) sends Agent-1 two values: a TTS (i.e. trust as measurable "reputation") and a PPM that quantifies trust as past history (trust as measurable "reliability"). Both TTS and PPM are scaled for convenience to a real number in the range [0..1]. The TTS is defined wherein a low value (for example, 0.11) or range of values (such as 0-0.1, for example) indicates a relatively "low" consumer trust threshold. A high value (for example 0.99) or a high-range of values (for example 0.97 - 1.0) represents a relatively "high" trust threshold.

ii) An "acceptable" range represents the minimum TTS and / or PPM score that falls within a particular VO consumer's own individual preferred and previously defined measurable trust confidence threshold level. Thus, Barclay's Capital will only "trust", hence invoke the VO e-service from the service provider (e.g. Basepoint Bank) if both the TTS and PPM both fall within the previously identified confidence range deemed as acceptable for that particular e-service.

iii) In this case, Barclay's Capital has previously set a minimum TTS for the consumption of the "quant99" e-service as being >= 0.8; they have set the minimum acceptable PPM for this particular e-service as being >= 0.9; (*these being two arbitrary values used for illustrative purposes only*). Clearly, every e-service must be given a TTS and PPM trust threshold score by the e-service consumer so as to enable the agent.

iv) Barclay's Capital checks during run-time (just prior to e-service consumption) whether or not the "quant99" VO e-service owned by Basepoint Bank global trust score (GTS) lies within its previously defined acceptable range (>= .8). It is assumed that the following five relevant CG metrics (shown in Table 4.3) are made available to Agent-2 at run time via a third party publisher (these being a sub-set derived from a larger potential "universe" of CG scores). Within Table 2 that follows, the following terms are used:

$\boldsymbol{S_1 \ldots S_n}$ = A set of individual CG metrics in compliance with the Combined Code. In this instance (Table 2) five exemplar CG scores are listed for simplicity. (In practice up to 60+ or so available CG scores might be used to calculate a GTS.)

$\boldsymbol{Sc_1 \ldots Sc_n}$ = A set of CG scores provided by a trusted third party for each of the available CG Metrics in respect of the VO owner.. These scores are normalized within the range [0-1]. An entry of "1" within the 2nd column of Table 2 shows that the listed CG metric is known (i.e. is available). An entry of "0" shows that the metric though potentially relevant to the calculation of the TTS is not available, hence is unknown to the agent (not all relevant CG scores are likely to be available in a real working system).

Table 2, also presents five exemplar CG values that are used by Agent-2, to calculate the GTS for the "*quant99*" the e-service owned and operated by *Basepoint Bank Ltd*, as requested by *Barclay's Capital* (the e-service consumer), from the VO.

v) Agent-2 sums up the available values so as to calculate the GTS as follows:

$$\text{GTS} = \sum_{i=1}^{n} S_i \bullet Sc_i \,/\, \sum_{i=1}^{n} S_i$$

Agent-2 sums up the values for entry "Basepoint Ltd" for every non-null value. In this instance since the resultant GTS is 0.8, this particular e-service lies within Barclay's Capital stated acceptable TTS. Agent-2 sends a suitable message back to Agent-1 and proceeds to calculate the PPM for the "quant99" e-service (note: if the TTS lies outside the stated threshold range then Agent-2 would terminate any further calculation, sending a suitable message to Agent-1). In Table 2 only five values are

shown for illustrative purposes. In practice up to 60+ CG values might be potentially be available to the agent so as to generate a given GTS for any given corporation. [14] have previously shown that the use of "lean" (i.e. 7-10 key CG measures) can be as effective as the use of complete data sets in the context of CG reputation scores. Thus, the proposed system is not therefore overly dependant for its reliability on large or complete data sets being available. Rather, values for key indicators are needed. Where complete data sets (60+) CG values and associated indices are deemed to be valid they are increasingly being made available on-line in the public domain and are hence available to both human and software agents. Various organizations update and freely publish CG measures and indices on a regular basis. In this illustrative example the (fairly commonplace) case of a VO being owned by more than one "real" organizations is not considered here for reasons of clarity, but the model supports this case by simple extension.

Table 2. Agent Scores: An exemplar

Corporate Governance Criteria/Metrics (Derived from Brown and Caylor (2004)	**CG Metric Availability for "Basepoint Bank Ltd" (S)** **(The owner of "quant99"** **VO e-service.)**	**Score [0..1] – supplied by trusted third party (Sc)**
All directors > 1 year of service own shares in Basepoint Ltd.	$S_1 = 1$	$S_{c1} = 0.4$
> 1 member of the Board has participated in an accredited director education program.	$S_2 = 0$	$S_{c2} = 0$
Basepoint audit committee comprises solely of independent outside directors.	$S_3 = 1$	$S_{c3} = 0.1$
CEO[(2)] of Basepoint serves on < 2 additional boards.	$S_4 = 1$	$S_{c4} = 0.1$
All directors have attended > 75% of board meetings.	$S_5 = 1$	$S_{c5} = 0.2$

vi) Agent-2 now attempts to establish any previous experience (service invocation history) for the requested e-service by examining a history log of previous consumption of the "quant99" e-service by Barclay's Capital. The service history log contains a service history (analogous to a "credit check" for a human agent) that records failure points or service non-availability per unit time. This is made available to Agent-2 by the e-service consumer (i.e. Barclays Capital) as the log is regarded to be specific to that consumer, given their own particular platform configuration and own particular pattern of e-service consumption. If no previous service log exists (hence the PPM value cannot be calculated) the service is only invoked, if the GTS exceeds TTS specified by the consumer. Essentially, the history log in our example needs to be "mined" using well established approaches to the intelligent data mining of consumer credit transactions such as regression analysis, statistical analysis and the use of neural network methods. As a result of these mining activities the "quant99" e-service provided by Basepoint Bank may be regarded as being "low" or "high" risk and a variety of actions could be taken in response to this categorization, depending on the expressed preferences of the service requestor. In this example we assume for simplicity and brevity the simple case in which these activities result in a calculation of a PPM that is above the specified TTS as defined by Barclays Capital (i.e.>= 0.9). Thus, since both the GTS and PPM are both above the minimum trust thresholds set by Barclays in connection with the consumption of the "quant99" e-service, Agent-2 sends a message to Agent-1 to indicate that consumption can proceed.

4. CONCLUSIONS

We have demonstrated that the "soft" trust 'gap' can be partially filled through using the combination of a semiotic trust ladder and a CG scoring agent model to aid better conceptualization of trust issues. By using one unified paradigm to describe VO level trust issues, e-service level trust, will be considerably better clarified. We also used an example to illustrate our model functioning.

A severe limitation of our model, (which may in time be lessened) is the limited scope of formal CG regulation and scope. For example under the Companies Act 2006 compliance with CG regulations and codes of conduct are limited only to "listed" UK companies. Also, there is as yet in the UK no specific regulator to oversee CG. It has recently been suggested that several reputation metrics can be combined (triangulated) so as to provide for internationalization [15], i.e. the development of a multi-valued reputation metric index. The index (would speculatively) comprises nine categories further decomposed into numerous individual metrics. The categories offered by [15] are as follows: products and services, employees, external relationships, innovation, value creation, financial strength, strategy, culture and intangible liabilities. These categories are weighted so as to generate an overall reputation index value in the range [1 - 9.] A value of 1 indicates that a "corporate reputation has little or no value", whilst a maximal value of 9 indicates "an ideal level - rarely achievable". It should be stressed that these metrics have not been discusses by [15] within a computational setting, merely as a set of generic potential corporate reputation metrics.

Thus whilst such relatively heavyweight sets of reputation metrics clearly an approach that holds promise for the future, much more basic research is needed before these can enable an agent in high-performance VO settings. As yet, for example, there appears to be a lack of third party rating agencies for such a set of metrics, were a consensus to emerge, as to their viability. Without internationalization efforts, CG scores can only inform about corporate entities that fall within the Combined Code (i.e. are UK based). This limitation is severe, but perhaps with increased international efforts, a small sub-set of suitable metrics will eventually emerge that can be used as trust (reputation) proxies. Clearly, if it were possible to enable a VO trust agent with a wider

set of metrics and to combine these to form a composite trust index, of the type proposed by [15] many of the limitations of the present model (CG scores) would be ameliorated.

The recent "credit crunch" and the first anniversary of the failure of Lehman Bros., should serve as a warning to us all that "better" systems are needed to avoid potentially catastrophic losses (high risk). Indeed the failure of Lehman also serves to illustrate two pertinent aspects of "real-world" business collaboration: *contagion* (one failure leads to others due to service delegation, distributed risk and hasty reactions) and *qausi-independent third party* rating agencies, that may not prove to be reliable or timely in flagging measures of high risk (low trust). Both these issues need further thought before we can fully replace "blind" VO trust collaborations with "trusted" agent mediated partnerships collaborations.

Nevertheless, we do now believe that "soft" VO trust issues need to be raised. There would seem to be a trust 'gap' in existing XML architectures and XML certificate based systems. These merely support tangible security *not* high-level reputation. It is difficult to see at this stage exactly how to fully meet this trust gap; other than to encourage more fundamental research in the area of reputation trust metrics. Also to call for more the development of suitable test beds that can be used to trial the use of a sub-set of reputation metrics (such as CG scored) that exhibit the necessary low latency, high objectivity characteristics that are needed for demanding collaborative VO settings.

5. REFERENCES

[1] Platzer, C. 2004. Trust based Security in Web-Services. MSc Thesis, Technical University of Vienna.

[2] Cahill, V., Gray, E., Seigneur, J.M., Jensen, C.D., Chen, Y., Shand, B., Dimmock, N., Twigg, A., Bacon, J., English, C., Wagealla, W., Terzis, S., Nixon, P., Serugendo, G., Bryce, C., Carbone, M., Krukow, K., and Nielsen, M., 2006. Pervasive Computing, July-Sept 2003, 52-61.

[3] Song, S., Hwang, K., and Kwok, Y., 2005. Trusted Grid Computing with Security Binding and Trust Integration. Journal of Grid Computing, 3(1-2), June, 2005, 53-73.

[4] Wilson, M., Arenas, A., & Schubert, L., 2007. TrustCOM Framework Version 4. Available as a PDF download from http://www.eu-trustcom.com.

[5] Song, S., Hwang, K., and Kwok, Y. 2005. Trusted Grid Computing with Security Binding and Trust Integration. Journal of Grid Computing, 3,1-2, June, 2005, 53-73.

[6] French, T., Liu, K., & Springett, M. 2007. A Card-Sorting Probe of E-Banking Trust Perceptions, Proceedings HCI 2007, (Full paper), Lancaster University, UK, 3rd-7th September 2007,1, 45-53.

[7] Turner, A. 2009. The Turner Review: a regulatory response to the current banking crisis, FSA (Financial Services Authority), Technical Report March 2009. Available from: http://www.fsa.gov.uk/pubs/other/turner_review.pdf

[8] Gambetta, D., and Hamill, H. 2005. Streetwise: How Taxi Drivers Establish Customers' Trustworthiness. Russell Sage Publications.

[9] Liu, K., 2003. Incorporating Human aspects into Grid Computing for Collaborative Work. Keynote at the ACM International Workshop on Grid Computing and eScience,21st June 2003, San Francisco, USA.

[10] Marsh, S.P. 1994. Formalising Trust as a Computational Concept. PhD Thesis, Stirling University, UK.

[11] Bistarelli, S., and Santini, F. 2008. Propagating Multitrust within Trust Networks. Procs. SIG on Applied Computing 2008, Track: Trust, Recommendations, Evidence and other Collaboration Know-how, March 16-20th, Fortaleza, Ceara, Brazil, ACM.

[12] Josang, A., Ismail R., & Boyd, C. 2007. A Survey of Trust and Reputation Systems for on-line Service Provision, Decision Support Systems, 43,2, 618-644.

[13] Olmedilla, D., Rana, O., Matthews, B & Nejdi, W., 2006. Security and Trust Issues in Semantic Grids. Proceedings Semantic Grid: The Convergence of Technologies. Available from: http://drops.dagstuhl.de/popus/volltexte/2006/408

[14] Brown, L., and Caylor, M. 2006. Corporate Governance and Firm Valuation, Journal of Accounting Policy, 25, 409-434.

[15] Cravens, K., Goad-Oliver, F., Ramamoorti, S. 2003. The Reputation Index: measuring and managing corporate reputation. European Journal, 21, 2, 201-212.