December 2004

A Conceptual Trust Framework for Semantic Web Agents

Todd Kowalczyk
The Hartford Insurance

Heidi Ellis
Rensselaer Polytechnic Institute

Gregory Hislop
Drexel University

A Conceptual Trust Framework for Semantic Web Agents

Todd M. Kowalczyk
The Hartford Insurance
Todd.Kowalczyk@thehartford.com

Heidi J. C. Ellis
Rensselaer Polytechnic Institute
heidic@rh.edu

Gregory W. Hislop
Drexel University
hislop@drexel.edu

ABSTRACT

In order for the true potential of Semantic Web agents to be realized, the Semantic Web must contain resources and mechanisms that allow agents to make the same types of qualitative judgments about trust that are intuitively and often unconsciously made by their human counterparts. This paper presents an overview of existing research on trust on the Semantic Web. In this paper, the attributes of trust relevant to Semantic Web applications are identified, defined, and organized into a conceptual framework. Our work uses this framework to describe how these attributes can be used collectively to define an agent's trust-related processes and how the attributes support the ability of agents to make decisions about trust given the unique set of characteristics and challenges associated with the Semantic Web environment.

Keywords

Semantic Web, agents, trust, decision-making

INTRODUCTION

Tim Berners-Lee's (2001) vision of the Semantic Web augments the existing web by adding meta-data and structured information that allows web information to be processed more easily by machines. This vision promises to unleash a new breed of powerful computing agents that can interact with Web Services, other agents, and a diverse set of information sources to make informed decisions. Advances in core Semantic Web technologies such as knowledge representation languages, ontologies, and proof mechanisms are bringing us closer to the creation of a parallel society of automated agents that can work on our behalf. In the not so far off future, it is reasonable to expect that humans will be able to configure agents to engage in well-defined tasks and allow agents to carry out many tasks currently executed by their human counterparts.

For example, imagine an intelligent navigational agent that is included in your vehicle's standard instrumentation. At the onset of your journey, the agent, using your point of origin and intended destination, interacts across a wireless network with other mapping agents to develop a detailed set of directions and displays them on the in-vehicle monitor. While en route, the agent subscribes to traffic services and interacts with these agents to monitor traffic reports, alerting you of alternate routes when significant impediments are identified. If your vehicle's fuel level is low, the navigational agent interacts with travel service agents and determines an alternate route that has several fuel stations that are currently open for business.

The above scenario is an example of the tremendous potential of how agents, known as Semantic Web Agents, can leverage semantics to carry out sophisticated tasks. The example also demonstrates that the day-to-day activities in which humans engage involve a complex decision making process that depends upon resources and information that are obtained from others. Implicit in this process is a set of value judgments about the trustworthiness of each resource and information provider. In order for the promise of Semantic Web agents to be realized, the Semantic Web must contain resources and mechanisms that allow agents to make the same types of qualitative judgments about trust that are intuitively made by their human counterparts.

The ability to make qualitative decisions about the trustworthiness of other agents and information published by foreign sources is a challenging task. Making a trust determination requires that an agent engage in a complex and dynamic decision making process. During this process, an agent must define the scope of the trust aspects being considered, identify the

context in which the trust decision is being made, select the rules and protocols that are most relevant given the scope and context, and apply the rules and protocols to derive a final trust determination.

OBJECTIVES

In this paper, we present an overview of the existing research that has been done on trust as this concept relates to Semantic Web agents. Our work acknowledges the extensive research in this area and identifies from existing research the set of attributes of trust that we believe need to be present in order for Semantic Web agents to make decisions about trust. Our focus is on providing a "forest level" view of existing research.

We examine trust from the perspective of an agent that seeks to make a trust determination about the services offered by another entity. We examine the attributes of trust in the context of the Semantic Web and attempt to illuminate the importance of each attribute as each relates to the unique characteristics that are implicit in this environment. In addition, our work presents a high-level, conceptual framework for the attributes of trust. As noted by Marsh (1994) and Mollering (2001), the concept of trust isn't easily defined. It is our hope that our logical framework will serve as a valuable tool for future research.

Merriam Webster defines the term *attribute* as "an inherent characteristic" and "an object closely associated with or belonging to a specific person, thing, or office" (www.merriamwebster.com). In this paper, we extend the definition provided by Merriam Webster dictionary for the term attribute. A *trust attribute* is *an inherent characteristic that is closely associated with the concept of trust and the process of acquiring and establishing trust between two distinct entities*.

SEMANTIC WEB ENVIRONMENT

The environment in which trust decisions are made plays a key role in shaping the process and protocols that are used to make these decisions. Environmental factors largely define the information and resources that are available, influence how these assets can be used and assembled into meaningful data, and place specific boundaries on each trust-related process. To better understand the attributes of trust that are relevant to the Semantic Web, the characteristics of this environment must be examined. We discuss the characteristics of the Semantic Web environment that have the greatest impact on the decision-making ability of Semantic Web applications below.

Anonymous

Finin and Joshi (2002) note that that the value of identity in a large, open network such as the Semantic Web diminishes significantly. In closed or small networks where entities are well known, a trust determination becomes an authentication problem. Once identity is confirmed, access to a controlled resource is granted. For example, if two individuals work in the sales department, they would likely be willing to share sales data freely. Identity allows each entity to establish trust based on a mutual association, namely the department to which both belong.

In a large environment like the Semantic Web, the increased size of the network reduces the strength and value of the associations that identity can convey as a trust determinant. Knowing that John Smith controls an agent isn't useful to another agent that is unfamiliar with John Smith. In order to leverage Semantic Web resources that are available, agents must be able to interact without knowledge of another entity's identity.

Distributed Control

One of the primary strengths of the Semantic Web is the fact that, as a knowledge repository, it is vast and diverse. Unlike traditional resources, such as libraries and museums that are controlled by a central authority, the Semantic Web isn't managed by any single entity. There is no central authority that can testify to whether a particular information source or interaction partner is trustworthy. In addition, agents don't have knowledge of the security policies and integrity controls that other entities use to administer the resources that the entity controls.

Dynamic

Since its inception, the Web has grown at an astounding rate. As the value of semantics on the Web becomes more widely recognized and increasing numbers of agents are introduced and begin to provide valuable services that utilize these semantics, the pace of change will accelerate. Services, information sources and agents will be introduced and retired continuously. Agents must be capable of making decisions about trust in a landscape that is constantly changing and presenting new interaction opportunities and new risks.

Heterogeneous

The distributed nature and sheer size of the Web guarantees that the Semantic Web will be an environment that is both rich with standards and devoid of them at the same time. It isn't feasible to expect a universal standard for terminologies and protocols to emerge (Finin and Joshi, 2002). Models of trust must accommodate the heterogeneous nature of the Semantic Web, capitalizing on standards when they are present, but at the same time not sacrificing the flexibility that agents need to effectively and efficiently achieve their intended function.

RELATED WORK

Existing researchers are overcoming the challenges associated with establishing and automating trust decisions on the web by embracing the afore-mentioned Semantic Web characteristics. In their architecture, Maximillien and Singh (2002) propose adding a Web Service Agent Proxy (WSAP) to access each service on an agent's behalf. A WSAP monitorins the activities and usage of a service by the client and is responsible for collecting personal experience data that is helpful in assessing future usages.

Reputation and endorsement agencies are mechanisms that agents can use to assess the trustworthiness of an entity with which they are not familiar. Maximillien and Singh's (2002) approach acknowledges that in a large, distributed environment, agents will not always possess sufficient personal experience to make good trust decisions. Agents must rely upon the opinions of trusted agents that share their view of the reputation of another agent. Maximillien and Singh (2002) also offer a method for introducing new agents that don't have an existing reputation. Endorsements allow new services that don't have a reputation to be advertised by trusted agents so that they can begin to build a reputation. Just as Google has emerged as a trusted search engine, one can imagine the agencies that serve as the Better Business Bureau organizations of the Semantic Web.

Abdul-Rahman and Hailes (2000) and Ramchurn, Jennings, Sierra, and Godo (2003) point out that trust is context-dependent. One's reputation as a Computer Scientist has no relation to one's reputation of being a good cook (Mui, Halberstadt and Mohtashemi, 2002). Context allows an agent to distinguish between an entity's reputation for *accuracy* during rush hour versus their reputation for *timeliness* of reporting on a Sunday morning.

Finin and Joshi (2002) use credentials to allow entities to establish credibility with one another in an anonymous environment. Finin and Joshi's (2002) approach acknowledges the decentralized and heterogenous nature of the Web and avoids employing a global trust mechanism in favor of a distributed approach that allows agents to make trust decisions locally. Their approach incorporates policy languages that use ontologies to define concepts for permissions, obligations, and credentials, and establish personal security policies.

Gil and Ratnakar (2002) present the TRELLIS application and annotations as a method of determining whether to trust the content of a web resource. TRELLIS allows users to annotate their analysis of alternate sources of information as they make a decision or reach a conclusion based on their analysis. Once recorded, rationale can be used to help users share and justify analysis results.

McGuiness and Pinheiro da Silva (2003) discuss an infrastructure for web explanations, the Inference Web (IW). The IW contains data used for proof manipulations and tools for building and presenting proofs. Understanding the source of a statement allows agents to base their decisions on the quality of source data, provenance of this data, suitability / quality of the reasoning / retrieval engine, and the context of the situation in which an analysis is occurring.

The existing research that our work is based upon is concentrated in the area of Computer Science. Our conceptual model has drawn from the all of the work cited above. Our framework combines the individual attributes of trust identified by existing researchers into a conceptual model that agents can use to make decisions about trust.

CONCEPTUAL FRAMEWORK OF TRUST

This section presents an overview of our conceptual framework of trust and the trust attributes within our framework. Figure 1 illustrates the elements in our framework. The trust elements must be evaluated within the *context* in which the trust evaluation is being made. The *scope* of a trust decision is the definition of the nature of trust and establishes a specific basis for trusting another entity. *Policies* provide guidance to the trust decision process by describing the social and security guidelines associated with the trust decision. We begin this section by defining the trust attributes that are applicable to Semantic Web agents. We then describe the mediating elements of context, scope, and policies that provide perspective and guidance during the trust decision-making process.

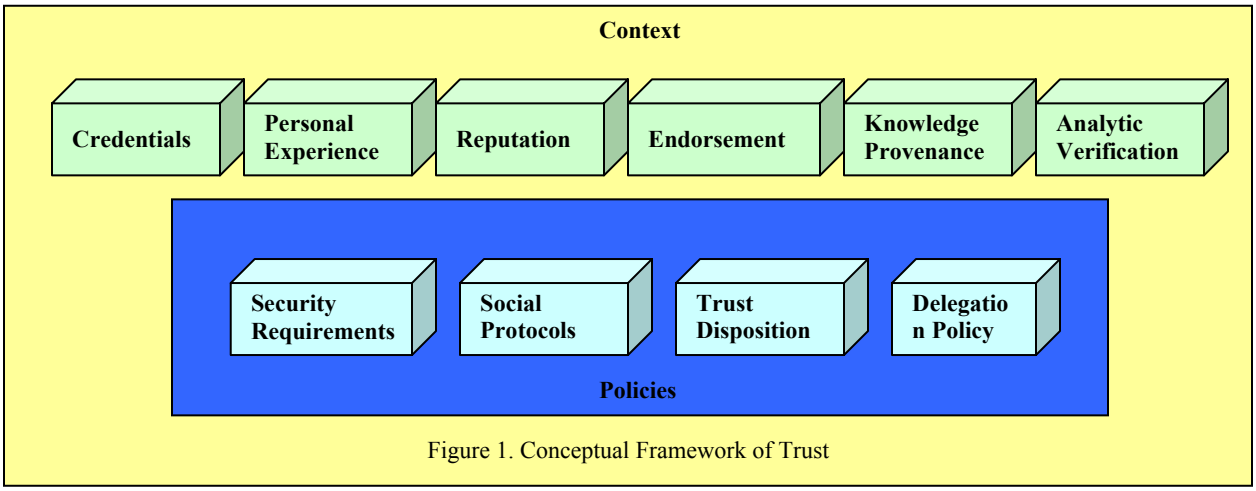

Figure 1. Conceptual Framework of Trust

Our review of the research done to date has identified the following trust attributes: *Personal Experience, Reputation, Endorsement, Credentials Knowledge Provenance*, and *Analytic Verification.* Each attribute represents an individual pathway to trust that an agent can analyze to determine if a sufficient basis for trust exists. Positive personal experiences, reports that an entity has a good reputation or an endorsement of an entity by a trusted party are examples of how each trust attribute helps agents establish trust.

Personal Experience

Personal Experience has been utilized in number of different approaches to trust management (Abdul-Rahman and Hailes 2002; Finin and Joshi 2002; Ramchurn et al; 2003, Yu and Singh 2002). We define personal experience using the definitions presented by Abdul-Rahman and Hailes (2002), and Yu and Singh (2002):

> "*Personal Experience is the set of data that an entity collects about other entities through direct interactions with these entities and direct observations of these entities."*

Personal experience is highly configurable attribute. Agents are not bound by universal standards or external requirements and have complete latitude over the definition of this attribute. The specific method used to represent personal experience is agent specific and largely defined by an agent's function. One agent may represent personal experience as a vector of scalar values while another may use an object model that utilizes complex data types. The value of personal history is limited however. In an environment that is constantly changing, agents cannot accumulate personal experience for every possible interaction partner.

Reputation

Numerous researchers note the importance of reputation in building trust (Abdul-Rahman and Hailes, 2000, Mui et al, 2003; Maximillien and Singh 2001; Yu and Singh 2002). Abdul-Rahman and Hailes (2000) define reputation as an expectation about an agent's behavior based on others observations of its past behavior. Maximillien and Singh (2001) define reputation as the aggregate rating of a particular entity by the principals that provide this rating. Our work adopts the definition of reputation offered by Abu-Rahman and Hailes (2000) and Maximillien and Singh (2001):

> *"Reputation is an aggregate rating that expresses the expectation about an entity's behavior based on information about or observations of its past behavior".*

Social mechanisms that allow agents to exchange trust-related data such as reputation are critical because agents typically operate with an information deficit. In a dynamic environment like the Semantic Web, an agent's personal experience is never 100% complete. Reputation allows an agent to supplement local data and expand its network of interaction partners.

Endorsement

Information sources and services that are newly introduced to the Semantic Web need a method of advertising their existence and establishing trust. Existing agents cannot rely upon personal history or reputation information to assess these new

entities (Maximillien and Singh, 2002) because this type of information does not yet exist. Our work adopts the definition of endorsement provided by Maximillien and Singh (2002):

"An Endorsement is an assertion by a trusted party that another entity or information source is trustworthy".

Endorsements provide a "bootstrapping" mechanism when other trust attributes aren't available. An endorsement is a summary judgment about the trustworthiness of an entity that an agent accepts to be true without having access to any detailed data that would substantiate this assessment.

Credentials

In an anonymous environment, true identity isn't very useful as a basis for trust. Credentials allow agents to overcome the identity-based approaches used by traditional security mechanisms and to operate anonymously using a more generalized notion of identity (Finin and Joshi, 2002). We define credentials as:

"A Credential is a unique property or characteristic of a particular entity that distinguishes the entity from others."

Using the traffic example discussed earlier, a GPS agent might wish to use a global positioning system to inquire about the current location of your vehicle. The on-board GPS agent on your vehicle may be authorized to relay this information if the incoming GPS inquiry includes credentials identifying that the inquiry originated from a police vehicle or a specific tow truck operator. Existing security mechanisms such as XML Signatures provide the necessary third party verification of each credential and establish a basis for trusting each credential (Kagal, Finin, and Joshi 2002).

Knowledge Provenance

Our definition of knowledge provenance is based on McGuiness and Pinhiero da Silva's (2003) work on the Inference Web, and the Trellis application presented by Gil and Ratnakar (2002):

"Knowledge provenance is a subjective explanation or analysis of a statement made by another entity that helps explain the origin, basis or reasoning of a statement for the purpose of assessing the statement's trustworthiness."

Knowledge provenance refers to attributes associated with a statement such as the source of the statement, when these sources were updated, the trustworthiness of the source, and whether the statement was derived or looked up. By coupling inference mechanisms with tools that allow others to contribute their analysis of a particular statement, agents gain valuable data that can be used when making trust decisions.

For example, an agent may be contemplating whether to use a particular traffic report that is posted on the Semantic Web. Some correspondents may report the report's reputation for accuracy as good. However, after reviewing annotations by others questioning the accuracy of traffic statements in the report, the agent may question the report's reliability and seek alternate sources.

Analytic Verification

Trust can also be established by an objective evaluation of the information or service provided by another entity. For example, an agent may be able to establish trust using an exploratory protocol, by verifying information other than the information sought (Esfandiari and Chandrasekharan, 2001). We adopt a definition derived from the process described by Esfandiari and Chandrasekharan (2001):

"Analytic verification is the process of assessing the trustworthiness of another entity by verifying that the entity responds accurately when responding to inquiries that an agent already has credible and substantiated answers for."

A financial application agent might have data about interest rate calculations that would enable it to test an interest rate calculation service. If the service performed correctly for the test cases, the agent might then decide to trust the service for problems or inquiries that are outside the scope of the initial verification tests. Similarly, an agent having exchange rate information, but needing additional data might use the data it knows to gauge the trustworthiness of a source for the additional data.

Mediating Elements

The trust decision-making process carried out by a Semantic Web agent is strongly influenced by a set of mediating elements. In contrast to the trust attributes discussed in the previous section, each of which represent a specific aspect of trust, the

mediating elements of context, scope, and policies describe the environment in which the trust decision is to be made. Mediating elements help an agent to select the trust attributes and protocols that are most relevant to a particular trust determination and allow the determination process to be constructed dynamically. Context, scope and policies provide distinguishing cues that alter how each trust determination is executed and allow agents to express and execute specific rules when these cues are encountered.

Context

Context describes the circumstances and semantic territory which form the setting in which an agent / entity interaction takes place (Ramchurn et al 2003). A setting is agent defined. For a traffic agent, context might be rush hour, Sunday morning, or a life and death emergency. In our model, the mediating element of context defines limits for the set of trust interactions that take place and defines the trust attributes that are useful during a trust assessment. For example, when assessing whether to trust a particular traffic report agent during rush hour, an agent may choose to rely on personal history and reputation information to make a trust determination. Given the volatility of information during an active period such as rush hour, a context sensitive trust rule may require that reputation information be acquired from multiple sources. In an emergency situation, an additional rule might require that each travel service agent's credentials be reviewed to certify that each is geographically based in the immediate region and therefore likely familiar with nearby emergency facilities.

Context is important because agent trust determinations are agent and situation specific. If accuracy during rush hour is the central issue that an agent must decide, the agent must be able to express "rush hour" and associate specific rules and protocols with this setting. Context allows this level of expression.

Scope

Scope silhouettes the purpose of a trust assessment by defining the perspective on trust that must be considered during a trust determination. In other words, scope defines the nature of trust that is being assessed. For instance, an agent may need to assess the *accuracy* of an entity, or it may need to assess the *timeliness* of an entity. An agent may trust another agent to be accurate but not trust that the agent will deliver an accurate result in a timely manner. Together scope and context allow an agent to make a determination about a specific issue (scope) within a particular setting (context).

Scope is the predicate in each trust proposition that is either affirmed or denied. Scope is determined by the nature of the specific activity or service that an agent is attempting to utilize and is also determined by context. For example, a navigational agent that seeks to obtain traffic reports from a traffic reporting agent will define scope as accuracy. Given the volatility of traffic reports during rush hour, context may influence scope such that scope is redefined to incorporate both accuracy and timeliness.

Policies

Policies are the rules that are applied to an entity's trust-related processes to guide each individual process and unify these processes into a comprehensive set of trust requirements. There are four different types of policies in our framework. Trust disposition policies allow agents to express whether they are pessimistic and naturally untrusting or optimistic. Social policies allow an agent to define the trusted agents from whom it is willing to exchange reputation information with. Security requirements allow agents to express any credentials that need to be provided and delegation policies allow agents to express when access rights provided to another entity can be granted to other parties by the entity (Finin and Joshi, 2002).

Trust Assessment Phases

In this section, we describe how an agent could apply our framework in order to make a trust assessment. We identify four distinct phases of processing that occur in our framework, and define the primary objective of each phase. We discuss the significant activities that occur in each step and explain the role of the trust attributes and the mediating elements in the trust determination process. We use a trust assessment from the navigational agent scenario presented earlier as an example to demonstrate the process.

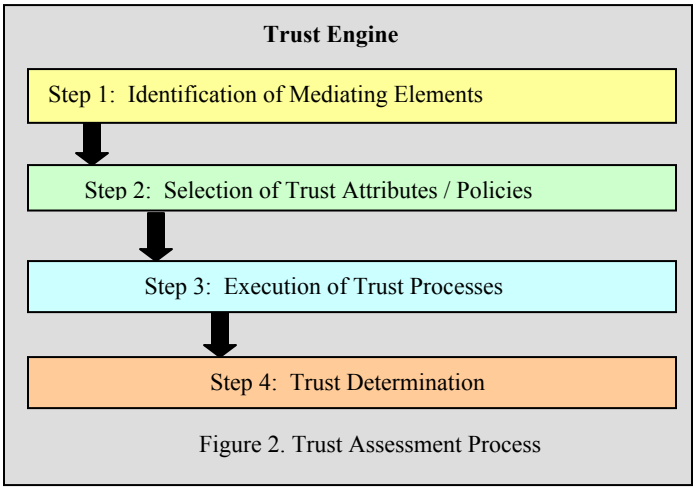

Figure 2. Trust Assessment Process

Step 1: Identification of Mediating Elements

The objective of the first phase is to identify the mediating elements that must be considered during a trust assessment. Scope and context are defined in order to establish specific boundaries for each trust related process. Context and scope provides important cues that are used in subsequent phases to define trust activities dynamically.

For example, you're on vacation with your pregnant wife when she goes into labor. You immediately request the navigational agent to provide a travel map to the nearest medical facility. Your vehicle's navigation agent identifies the mediating elements. It is 5 pm and therefore a "Rush Hour" context is identified. Urgent medical attention is required and an "Emergency" context has been specified. Context sensitive rules associated with "Rush Hour" and "Emergency" define that scope include aspects of *accuracy* and *timeliness*.

Step 2: Selection of Trust Attributes / Policies

Next, the trust attributes and policies that are most relevant to context and scope are selected. Trust attributes and trust rules are associated with contexts via an agent's trust policy. Attributes and rules can be global and associated with all contexts or apply to specific contexts. Identification of the trust attributes establishes a potential basis for trust and defines the mechanisms that will be used to assess whether sufficient basis exists.

In an " Emergency and Rush Hour" context , the navigational agent selects *credentials, personal history*, *and reputation* as the attributes to use to assess accuracy and timeliness. The attributes are ranked with credentials defined as the most important followed by personal history and then reputation.

Step 3: Execution of Trust Processes

During trust process execution, a data assessment and data collection process occur. The assessment focuses on determining if sufficient local data exists and if data that was acquired previously is stale and needs to be refreshed. After assessing local data, inquiries are made of other entities to supplement local data.

During the execution phase, the navigation agent reviews its local data and determines that it doesn't have personal history or reputation data to make a trust assessment. The couple is vacationing in an area that the agent isn't familiar with. Using its trust policies, the agent consults with friendly agents that it has interacted with in the past to determine if they are aware of traffic reporting and travel service agents in the current area. Some of these agents respond and provide reputation about these types of agents.

Step 4: Trust Determination

During the trust determination phase, the importance of each attribute relative to other attributes is weighed, the absence of certain information is assessed and, in cases where multiple services are being compared, algorithms are applied to level-set

the disparate set of information that is available so that the trust information is comparable. Finally, a trust determination, expressed as a binary value or a degree of trust is made.

After acquiring sufficient trust data, the navigation agent assesses the reputation data that has been acquired. Data gaps and disparity of information are weighed and a trust calculation is performed. A trust measure for each traffic reporting and travel service in the area is calculated and the navigation agent selects the services with the highest trust ranking. During handshaking with the service, the navigation agent requires that the traffic reporting and travel agents provide a credential identifying them as licensed agents in the current area.

CONCLUSION

In this paper, we have presented a conceptual trust framework based on trust attributes identified from existing research. We have shown how the trust attributes can be combined into a comprehensive decision-making framework that can be utilized by Semantic Web agents and demonstrated the applicability of each of these attributes based on the unique characteristics of the Semantic Web environment. In a future work, our intention is to utilize our findings and develop an information assessment framework that incorporates trust and information quality to support agent-based decision-making.

REFERENCES

1. Abdul-Rahman, A. and Hailes, S. (2000) Supporting Trust in Virtual Communities, *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences,* Maui, Hawaii.
2. Berners-Lee, T., Hendler, J. and Lasilla, O. (2001) The Semantic Web, *Scientific American,* 284, 5, 34-43.
3. Berners-Lee, T. (1999) Weaving the Web, Harper, San Francisco, CA.
4. Esfandiari, B. and Chandrasekharan, S. (2001) On How Agents Make Friends: Mechanisms for Trust Acquisition, *Proceedings of the Fourth Workshop on Deception, Fraud and Trust in Agent Societies*, Montreal, Canada.
5. Finin, T. and Joshi, A. (2002) Agents, Trust, and Information Access on the Semantic Web, *ACM SIGMOD Record,* 31, 4, 30-35.
6. Gil, Y. and Ratnakar, V. (2002) Trusting Information Sources One Citizen at a Time, *Proceedings of the First International Semantic Web Conference (ISWC),* Sardinia, Italy.
7. Kagal, L., Finin, T. and Joshi, A. (2001) Moving from Security to Distributed Trust in Ubiquitous Computing Environments, *IEEE Computer,* 34, 12, 154-157.
8. Kagal, L., Finin, T., and Joshi, A. (2002) Developing Secure Agent Systems Using Delegation Based Trust Management, *Proceedings of First International Joint Conference on Autonomous Agents and Multi-Agent Systems,* Bologna, Italy.
9. Kagal, L., Undercoffer, J., Perich, F., Joshi, A. and Finin T. (2002) A Security Architecture Based on Trust Management for Pervasive Computing Systems, *Grace Hopper Celebration of Women in Computing,* Vancouver, Canada.
10. Marsh, S. (1994) Formalising Trust as a Compuational Concept, PHD Thesis, Department of Computing Science and Mathematics, University of Stirling.
11. Maximillien, M. and Singh, M. (2001) Reputation and Endorsement for Web Services, *ACM SIGecom Exchanges,* 3, 1, 24-31.
12. Maximillien, M., Singh, M. (2002) Conceptual Model of Web Service Reputation, *ACM SIGMOD Record*, 31, 4, 30-35.
13. McGuiness, D., and Pinheiro da Silva, P. (2003) Infrastructure for Web Explanations, *Proceedings of the 2nd International Semantic Web Conference*, Sanibel Island, Florida.
14. Mollering, G. (2001) The Nature of Trust: From Georg Simmel to a Theory of Expectation, Interpretation and Suspension, *Sociology*, 35, 2, 403-420.
15. Mui, L., Halberstadt, A. and Mohtashemi, M. (2002) Notions of Reputation in Multi-Agent Systems: A Review, *Proceedings of First International Joint Conference on Autonomous Agents and Multi-Agent Systems*, Bologna, Italy.
16. Ramchurn, S., Jennings, N., Sierra, C, and Godo, L. (2003) A Computational Model for Multi-Agent Interactions based on Confidence and Reputation, *Proceedings of the 6th International Workshop on Deception, Fraud, and Trust in Agent Societies,* Melbourne, Australia.
17. Richardson, M., Agrawal, R., and Domingos, P. (2003) Trust Management for the Semantic Web, *Proceedings of the 2nd International Semantic Web Conference,* Sanibel Island, Florida.
18. Yu, B. and Singh, M. (2002) An Evidential Model of Distributed Reputation Management, *Proceedings of the First International Joint Conference on Autonomous Agents and Multi-Agent Systems,* Bologna, Italy.
19. Yu, B. and Singh, M. (2000) A Social Mechanism of Reputation Management in Electronic Communities, *Proceedings of the Fourth International Workshop on Cooperative Information Agents,* Boston, USA.
20. Yu, B., and Singh, M. (2003) Detecting Deception in Reputation Management, *Proceedings of Second International Joint Conference on Autonomous Agents and Multi-Agent Systems,* Melbourne, Australia.
21. Retrieved from www.merriamwebster.com on 2/19/2004