The Knowledge Engineering Review, Vol. 21:2, 127–161. © 2006, Cambridge University Press
doi:10.1017/S0269888906000932 Printed in the United Kingdom

A theoretical inter-organizational trust-based security model

HENRY HEXMOOR[1], SETH WILSON[2] and SANDEEP BHATTARAM[2]

[1] *Department of Computer Science, Southern Illinois University, Faner Hall, Carbondale, IL 62901, USA; e-mail: hexmoor@cs.siu.edu*
[2] *Department of Computer Science and Computer Engineering, University of Arkansas, Fayetteville, AR 72701, USA; e-mail: {slw08, sbhatta}@uark.edu*

Abstract

This work examines the interplay of inter-personal and inter-organizational trust, two distinct but related concepts, through a theoretic inter-organizational trust-based security model for a multi-agent system information-sharing community. A calculus that mathematically models trust building at the inter-organizational level is at the heart of this model. In inter-organizational or inter-firm exchange, the role of the boundary spanner, an organizational representative, is important in reducing asymmetries that may exist between the two parties. Trust is a crucial component to the dyadic interaction at the inter-personal or boundary spanner level, and the trust established at this level also affects the overall quality of the relationship at the inter-organizational level. Trust, as an aspect of social control, is thus viewed as a more effective mechanism for security in an open, distributed system, like an information-sharing community. The inter-organizational trust-based security model proposed herein represents a soft security approach. It affords several important benefits over traditional hard security mechanisms used in open systems — robustness, scalability, and adaptability. The inter-organizational trust-based model is an important contribution to the computational security community, as other open systems applications of a distributed or pervasive nature could adapt it and realize its benefits. It is also one of a few attempts to model trust building at either the inter-organizational or inter-personal level.

1 Introduction

One of the most prevalent themes in modern computing is security. Operating systems, software applications, the Internet, and service-oriented computing each have their own interesting security problems. This plethora of security challenges has bred an equally rich suite of solutions. Traditionally, these solutions have taken the form of passwords, program verification, access control lists, and cryptographic algorithms; however, in light of the increasing use of distributed open systems applications such as the Internet and pervasive computing environments, researchers have been exploring the potential of security mechanisms that are based on some aspect of social control. These mechanisms have several important advantages for such dynamic and distributed environments that are lacking in traditional solutions. Traditional means of security involve the use of what is referred to as hard security. Hard security mechanisms have a common characteristic: they provide security through establishing some figurative physical barrier. Sometimes security of this nature involves an onionskin-like approach (Britton & Bye, 2004) (i.e., the Onion Skin Model), by which information of increasing sensitivity is placed at increasingly deeper levels of fortification. Other security models, such as the Boling Lava model (Britton & Bye, 2004), restrict access to

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

systems based on the particular user access point. Such schemes of security are effective and widely used, but there is an inherent weakness for distributed and pervasive environments: primarily, their lack of robustness. Once the fortress of protection (i.e., an all-or-nothing quality) they provide has been breached, a malicious user can often enjoy unbridled access to the sensitive resources in question (Alfarez & Hailes, 1997).

The distributed and pervasive nature of open systems applications presents an interesting problem to security. In such open systems, agent-participants (e.g., human users and computational agents and services) are likely interacting with others whom they may not know. Possibly, there is also insufficient information in this case to decide whether to authorize access to a resource or share information (Abdul-Rahman & Hailes, 1997). Hard security approaches such as those based on either the Lava or Onion Skin Models do not address these problems (Britton & Bye, 2004). The use of a hard security approach that employs user IDs and passwords, for example, illustrates the shortcomings of hard security in the distributed context. First, authentication (i.e., identification plus verification) is performed by a single system, which is susceptible to denial of service style attacks and represents a potential bottleneck in terms of communication. Second, multiple user IDs and passwords are required for multiple hosts, and this situation can be both unwieldy and insecure. Third, security via authentication assumes a rather static environment, in which all users are known in advance. A distributed, open systems environment where users may come and go cannot be sufficiently maintained under an authentication approach.

Several security solutions have thus been proposed for open systems. These solutions include simple public key infrastructure (SPKI), pretty good privacy (PGP), X.509 certificates, and embedded security tokens (Blaze *et al*., 1996). Although such approaches can be effective in certain application domains, their scalability is limited in a distributed open system because they often depend upon either a centralized verifying authority or *ad hoc* recommendation-based authorization (Blaze *et al*., 1996). As the size of the system increases, so does the demand for communication and processing resources, especially when the security protocol is based on public key encryption.

A current trend in the security community is a shift away from hard security, towards methods that are much more malleable, robust, and scalable. These methods are typically based on aspects of social control, such as trust (Rasmusson & Jansson, 1996). An approach that employs some aspect of social control as the underlying mechanism for security is called *soft security* (Rasmusson & Jansson, 1996). A soft security approach is more appropriate for open systems security, because the issue of security is not localized in and controlled by some central authority. It is placed in the hands of its participants, and represents in a sense a 'grass roots' security approach.

Soft security takes a more realistic approach to open systems security. No concrete claims are made in regards to the prevention of security breaches (i.e., confidentiality or integrity). A soft security approach fully anticipates and accepts, as does the society, the existence of malicious participants. The security of the system lies in its participants identifying and avoiding interaction with them. A security framework founded in soft security is therefore naturally more robust than those founded in hard security (Rasmusson & Jansson, 1996).

Other important advantages to a soft security approach are the implications of its scalability, and its dynamic and evolvable nature. Since there is no central verifying authority involved, there is no concern for overburdening the system as it grows. The system is dynamic because it evolves as the underlying forces of social control change. These are qualities that make soft security an attractive alternative to open systems security.

In this report, we explore using the social aspect of trust to enable secure information exchange among computational agents both within and without the bounds of organizations. We have developed a theoretical, working security model for inter-organizational trust-based information exchange, accompanied by a mathematical model for trust building at the inter-organizational level and trust management policies. This model is based on the concepts of inter-personal and inter-organizational trust, which are important and heavily researched in the fields of social and

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

organizational science. These camps recognize trust as a critical social commodity for inter-firm exchange performance. In addition, the boundary spanner role (i.e., an organizational representative or gatekeeper) is examined. The boundary spanner is an important individual in the organization, and therefore has been incorporated as a key component to the inter-organizational model. Although the model was developed in an information-sharing context, we propose that through generalization, it could be adapted to any application in an open systems environment. The work contained herein was lead in the spirit of research and modeling real-world phenomena, which is customary in the artificial intelligence and multi-agent systems communities.

The *inter-organizational trust-based security model* (IEOTBSM) proposed in this paper is based on an intra-organizational model that was recently designed in our group at the University of Arkansas (Hexmoor *et al*., 2004). Our early work was motivated by the implications of using soft security in the context of secure information sharing among individual agents within a *single* organization. We examined two key trust metrics therein: the internal information availability (IA) and the internal security measure (SM) of the organization. Information availability quantifies to what extent information that is sought, is available and obtained by its requestors. Security measure is an indication of the number of security breaches in the system. These security breaches represent the receipt of information by those agents who were not *intended* recipients of that information. The two metrics are herein recast in the inter-organizational model to measure the overall IA and SM of an *inter*-organizational system. The IEOTBSM is at the theoretical stage of development. An implementation and simulation of the model is intended in the course of our future developments.

After a general background overview in Section 2, we summarize the intra-organizational trust-based security model (IAOTBSM) in Section 3, which forms our foundation for recommending our inter-organizational model (IEOTBSM) in Section 4. In Section 4, following a literature review we offer details of our model. Section 5considers the implications of this work, and in Section 6we draw concluding remarks concerning the work and its future.

2 Background

In large law enforcement agencies, information is gathered and compiled by many individuals from independent and disparate sources. In government agencies like the FBI and CIA, it is not necessarily the information from any one source that is critical to the assessment of potential crimes or threats, but rather the totality of the information that is significant. Therefore, in order to build the intelligence and knowledge required for such agencies to avert or tackle any unlawful practices, active information sharing among the individuals and, at large, the agencies, is one of the most vital activities.

One of the major concerns of information sharing is security. Information that is obtained by an unauthorized individual, whether internal or external to an agency, may be harmful and repercussions may ensue. In terms of information security, there are two elements for which concern must be given: confidentiality and integrity. Agencies implement policies that regulate and direct the sharing of information in light of these two concerns.

Many psychological and social factors need to be taken into account before assuming policies that characterize secure information sharing in and among agencies. Herein, we use the terms organization and agency interchangeably. These factors include time, the mobility of the modern workforce, its effects on long-term relationships, and demonstration of concern for the employees.

Most organizational policies take little notice of the impersonal nature of the work environment and communications, and mutuality in trust and respect (Bledsoe, 2002). These codified policies, thus, are *ad hoc*, difficult to follow, not malleable, and inadequately treat risks involved in information sharing. These problems can complicate secure information sharing to a point at which the organization ceases to share information efficiently and effectively. Trust-based security policies

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

for information sharing that consider trust as the key parameter and an undeclared psychological understanding in building the organizational social capital are thus proposed as an alternative in improvement.

2.1 Information sharing

Information sharing is a critical activity for almost every institution. Herein, we have mentioned its importance to the various arms of governmental justice institutions that engage in ongoing information gathering and dissemination. This topic has also been addressed by Phillips *et al.* (2002). In their work, they consider the issues surrounding information sharing in dynamic coalitions pursuant to some crisis. They recognize that efficient and effective information exchange is crucial in such situations. Unlike the scope of our work (Hexmoor *et al.*, 2004) in trust-based security, however, they combat issues of security (confidentiality and integrity) by considering the use of hard security measures such as role-based, discretionary and mandatory access control, as well as cryptography.

Goecks & Cosley (2002) introduce their proprietary information-sharing system called Nugget-Mine. This system provides facilities for the building, maintenance, and utilization of a repository of information called a *mine*. The authors stress a similar point therein concerning the importance of the assimilation of pieces of information: individually, they may seem insignificant, but collectively they may stimulate enlightenment. This work, however, does not address issues of security.

Another important influence to our model (IAOTBSM) is a work in which the authors consider information dissemination in the context of a wireless sensor network (Rabiner-Heinzelman *et al.*, 1999). Individual sensors in such a network, which can represent a social organization (Lesser *et al.*, 2003), aggregate data in order to provide a comprehensive and multi-dimensional view of the surrounding environment. In addition to the support provided again by the common theme of information sharing, one of the most important contributions of this work to our own is its analysis of various dissemination algorithms.

IAOTBSM adopts, as well, a variant of the classic flooding data dissemination algorithm. In classic flooding, an agent who needs to share information makes copies of the information and transmits it to each of her neighbors. Also, whenever an agent receives a fact from another agent, she shares it with her neighbors excepting the sender. An agent who receives a fact can transmit it back to the sender, as long as the sender is trusted.

Two deficiencies of the classic flooding algorithm, i.e., implosion and overlap, are circumvented in the trust-based information-sharing algorithm associated with the IAOTBSM. Implosion occurs when an agent is the recipient of the same fact from two different sources via different paths. Overlap occurs when the agents generate facts from overlapping sources of information, which can sometimes result in the same information (Rabiner-Heinzelman *et al.*, 1999). Thus, the same fact is duplicated at the recipient in both cases.

Each generated fact in our model has a unique identity. Thus, if an agent receives the same fact that is produced from two different sources, or if the same agent produces the same fact in two different cycles, and if an agent receives them from the same or different sources, in effect she has received two different facts. Every agent in the system is concerned with observing the paths taken by each of her generated facts. Thus, even though the same agent receives the same fact from different sources, they have traversed different channels of agents to reach the current recipient. This supports every initiator's purpose of monitoring the possible conduits of information sharing among the agents. An agent may receive multiple copies of the same fact via the same path in the same cycle. In this case, the agent prefers the freshest fact, while the others continue to be shared. The implosion and overlap problems of classic flooding algorithm are thus overcome in this implementation.

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

2.2 Trust and trust-based security

Researchers have espoused various definitions of trust. This inconsistency has led to confusion about the notion of trust. In general, trust represents a positive concept. In an exchange between two parties, there is a positive expectation in the trusted party (Jøsang, 1997). The expectation may be that the trusted party will behave in a certain manner, and that there is mutuality in beliefs. We adopt the following definition of trust for our model (IAOTBSM): agent x's trust in agent y is agent x's estimation of the probability that agent y will preserve agent $x's$ welfare with regard to the action to be performed (Beavers & Hexmoor, 2003). In our model, we assume that the trust between individuals is a useful piece of information that is readily available (Beavers & Hexmoor, 2003; Golbeck *et al.*, 2003).

Rasmusson & Jansson (1996) propose a school of thought focusing on soft security methodologies in open systems that bring about a secure social control. A trust model based on distributed recommendations is proposed as a solution to issues of security in on-line transactions (Abdul-Rahman & Hailes, 1997). The concept of social control as a security mechanism in a distributed system introduced in Rasmusson & Jansson (1996) and Abdul-Rahman & Hailes (1997) was particularly influential to our work.

In addition, the decentralized nature of a trust management system called PolicyMaker reported by Blaze *et al.* (1996) mirrored our intentions to support a more distributed environment; however, it did not address our concerns for the evolution of trust.

For the Semantic Web, trust has become an important tool for gauging the reliability of information. Rasmusson & Jansson (1996) and Golbeck *et al.* (2003) identify the shortcomings of traditional hard security measures such as digital signatures and certificates — confirming the source of a document says little about the trustworthiness of its contents. Gil & Ratnakar (2002) echo the concern of trustworthiness in terms of the reliability and credibility of sources of information on the Web. Their trust rating system, TRELLIS, is influential in spirit, but fails to suit the needs of decentralized trust management.

A security approach based on trust has several important advantages that address the shortcomings of traditional security mechanisms. Trust is a universally understood social phenomenon and commodity (Sydow, 1998). It affords 'naturalness' to the mechanism. Building a larger connected human workforce begins with the strength of the relationships at the individual level. Organizational units may therefore more easily adapt to security mechanisms that use policies based on trust. Another important advantage is that trust-based policies mimic the fluidity of human relationships. These relationships predictably evolve, strengthening or weakening according to the established history of experiences between individuals (Hardin, 2002).

Trust produces a social influence among the members of an organization (Hardin, 2002). These social influences encourage secure information sharing and deter breaches of security. Trust-based security is effective at preserving the security of information. Under a trust-based security policy, sensitive information will not be shared with those insufficiently trusted; although, there is a possibility that such information may be obtained by an unauthorized individual through some covert channel. Such a breach of security results in a breach of trust, which is quickly and easily remedied. Perpetually untrustworthy individuals are identified and ostracized within the organization, and in turn the overall security of the organization is maintained. Unlike hard security measures such as firewalls and access control, trust-based security mechanisms do not offer ironclad guarantees. Instead, we speak of levels and forms of assurance (i.e., probability).

Trust has different meanings in the contexts of hard and soft security. In the context of hard security, there is often an element of implied trust on the part of the user in the security mechanism itself. For example, a user trusts that whatever rights or privileges she grants on some resource through an access control list will be respected by the system. This trust may also lie in the users of the system. System administrators trust users to keep system passwords secret, and, as well, trust that their users will not collude. Trust in the context of soft security, however, represents a different

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

concept. In the case of trust-based security, it is the element of trust itself that acts as the underlying mechanism controlling access.

Interactions between two entities involve the play of two opposing forces — individual and social concerns. A balance must be achieved between individually rational decisions and socially rational decisions. Hogg & Jennings (2001) define socially rational decisions as those that take into consideration the collective benefits, as well as the individual utility. Trust becomes relevant only when one is faced with this social dichotomy. Some individuals act benevolently, while others choose to act in a malicious manner. If there were no malicious individuals in society, there would be no need for trust, and no need for security for that matter. Realistically, however, neither complete benevolence nor maliciousness can exist. Trust is thus an important social commodity that should not be taken for granted. It should be incorporated into every realm where humans may venture, including computing.

3 Intra-organizational trust-based security model and a working algorithm for trust-based information sharing

In our model, organizations and their constituent agents are considered to be social entities (Hexmoor *et al.*, 2004). Given this societal orientation, the agents that we establish base their relationships and interactions upon the human resource of trust. In this section, we introduce the terminology related to the IAOTBSM and discuss the trust-based information-sharing algorithm.

The interaction trust relation is an adjacency matrix that contains trust values between agents of an organization. The trust values, which are assumed to be known *a priori*, are quantified in a non-discrete manner as a real value in the range 0.0 to 1.0. A trust value of 1.0 indicates agent x's complete trust in agent y. If no relation exists between agent x and agent y, agent x either has a lack of trust in agent y or agent x is ignorant or cannot make a trust-related judgment about agent y. We make a simplifying assumption by interpreting the aforementioned cases as the same and assigning a trust value of 0.0 to them. An agent is cognizant of its trust in neighboring agents. The neighboring agents, however are not apprised of the trust the agent-trustor has in each of them. Interaction of trust relations is assumed to satisfy the reflexivity property. However, they do not hold the symmetry and transitivity properties.

Trust-based information sharing is the exchange of information that is owned by an agent among agents in the organization in succession, based on trust with an assumption that the information might satisfy at least one agent's fact requirement, including its originator. A cycle is measured as the time taken by an agent to receive or generate a fact and share it with her neighbors. Trust-based information sharing occurs continuously in each cycle and for every agent. Each agent in an organization produces a unique fact from the fact warehouse, which is a set of known and static facts. Each generated fact has a unique identifier consisting of two fields, the current cycle number and the unique initial of the initiator agent. Each agent in an organization also has a fact requirement that is selected from the fact warehouse. An agent's required fact, which is assumed to be a constant in all of the cycles, and the fact produced by her in each cycle can be the same. An agent might require the fact produced by any agent (including herself). An agent is not cognizant of other agents' fact requirements. These simplifying assumptions affect information sharing and its availability.

In trust-based information sharing, an agent is satisfied if and only if the fact required by her is the same as the fact she has access to. An agent's accessible facts constitute the fact generated by her in the current cycle and the facts that she receives from her neighbors in the previous cycle, if any. In each cycle, every agent produces a unique fact and then checks for her fact requirement in the facts that are accessible to her in the current cycle. An agent is not willing to receive any other fact for the current cycle if any fact among the ones she received satisfies her fact requirement; otherwise she is willing to receive facts for the current cycle. Each of the facts accessible to an agent that do not satisfy her fact requirement are, in turn, shared with her trusted neighbors that are not

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

satisfied with their accessible facts. The trusted neighbors of an agent are the set of agents whom she trusts with a trust value greater than the trust threshold, which is a user-defined static minimal trust value that guards information sharing. The recipient agents check these facts for their respective requirements in the next cycle. If their requirements are also not met, facts continue to be shared with their trusted neighbors. Such sharing sustains until the fact's expiration interval, a user-defined system level metric representing the number of cycles for which a fact can be shared after its creation, is reached.

At the end of every cycle, agents verify the current recipients of each of the unexpired facts they generated by querying the fact's fact pedigree. The fact pedigree of a fact is a document that is accessible only to the initiator agent. It contains the signatures of all agents who have received that fact. The initiator agents determine whether their trust in the recipient agents warrants their receiving the fact and classifies them into intended receivers (i.e., agents that are not satisfied with their currently received fact but are trusted by the initiator) and unintended receivers (i.e., agents that are not satisfied with their currently received fact and are not trusted by the initiator). The initiator agents can thus easily determine the covert channels that might lead to unintended receivers, and correspondingly apply trust policy models in order to eliminate them.

Trust policy models define the various combinations of trust update policies that regulate and update the interaction trust relations of agents belonging to a fact pedigree that includes an unintended receiver. The goal of these trust policies is to simultaneously maximize the information sharing and minimize the number of unintended receivers (security breaches). We devised several trust policy models with varying degrees of restriction on information sharing.

The first trust update policy, TUP1, regulates the trust relations between every consecutive pair of agents in a fact path starting from the unintended receiver back toward the initiator agent. Every agent's trust in the succeeding agent is reduced exponentially based on the relative role played by each agent in propagating the fact to the unintended receiver. The degree of responsibility for every agent in the agent fact path is the depth of the agent (with the fact originator as the root element) in the fact pedigree. The trust update value at every agent arc is proportional to the exponential of the degree of responsibility of the succeeding agent with user-defined trust decrement factor as the base.

The second trust update policy, TUP2, is a variant of TUP1. For every trust relation in the fact pedigree that led to the unintended receiver, trust is updated with the same user-defined trust decrement factor. This policy is more restrictive than the TUP1, as every agent in the fact pedigree is held equally responsible for the security breach, rather than proportionality.

A third trust policy model formulated, TUP3, updates the trust value between the initiator agent and every agent in the path, if a trust relation exists, by the user-defined trust decrement factor. By reducing the initiator's trust value in her neighbors that are in the fact pedigree leading to an unintended receiver, this policy model impedes the first step in the fact transmission (i.e. to her neighbors) that may lead to unintended receivers. This convention makes it the most restrictive of the three trust update policies.

The goal of the work surrounding the IAOTBSM, as previously discussed, is to maximize the information sharing among a group of agents while safeguarding its security in terms of confidentiality and integrity. Information availability, IA, is the degree to which information is freely available when shared among a group of agents. IA, a system level metric, is the sum of the number of satisfied agents and the number of intended receivers expressed as a percentage of the total facts shared. Note that the sets intended receivers and satisfied agents are disjoint. Security Measure, SM, a system level metric, is a measure of the number of unintended receivers expressed as a percentage of the total facts shared. The total facts shared are the cumulative of the count of intended and unintended receivers. IA, SM, and total facts shared are measured for every cycle of the trust-based information-sharing algorithm. The cycle number at which IA and SM converge to their ideal values, i.e. 100% and 0%, respectively, termed IA saturation cycle, is also measured in the algorithm given in Figure 1. In the algorithm, pseudo-share addresses the issue of agents checking for their required fact among the received facts sent in the current cycle, in the next cycle.

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

```
1  initialize agents, fact warehouse, fact requirements, interaction
     trust relations, trust threshold, trust update, expiration
     interval, and total number of cycles
2  for each cycle {
3    every agent generates a fact
4    every agent checks for fact requirement from her accessible facts
5    pseudo share the received facts each agent does not require
6    share the generated fact each agent does not require
7    share the pseudo share
8    each initiator agent checks for current unintended or intended
       receivers and applies trust update policy if there are any
       unintended receivers
9    compute ia & sm
10   for every fact check if it is expired }
```

Figure 1 Trust-based information-sharing algorithm, adapted from Hexmoor *et al.* (2004)

4 Inter-organizational trust-based security model

The theoretical inter-organizational trust-based security model (IEOTBSM) that is presented in this work, as previously mentioned, is based upon the intra-organizational trust-based security model (IAOTBSM) discussed in Section 3. In our intra-organizational model, we considered interactions among agents within the same organization. In the IEOTBSM, however, we consider the interactions among organizations in inter-organizational networks or organizational communities. In Section 4, we first discuss the organization as an agent society in Section 4.1. In this sub-section we examine aspects of an agent-society that appropriately and adequately model a real-world organization. In Section 4.2, we revisit the issue of trust conceptualization, but here in the context of inter-organizational or inter-firm exchange. Two levels of trust have been identified in this domain — inter-personal and inter-organizational — each of which represent distinct concepts, but, however, have influence on one another. One of the key components to exchange activity in inter-organizational networks is the boundary spanner role. The boundary spanner is discussed in Section 4.3. In order to form a base for developing a mathematical model for the building of inter-organizational trust, we examine both a mathematical model for inter-personal trust and a conceptual model for inter-organizational trust in Section 4.4. IEOTBSM incorporates through influence many of the ideas and concepts gleaned from the literature review that spans Sections 4.1 through 4.4. We provide a general description of IEOTBSM in Section 4.5. Sections 4.6 and 4.7 discuss the inter-boundary spanner and inter-organizational trust calculus; and the boundary spanner regulatory process, two crucial components of the IEOTBSM. Finally, a formal description is provided in Section 4.8.

4.1 Organizations as agent societies

An organization is defined by Dignum *et al.* (2002, p. 694) as 'a specific solution created by more or less autonomous actors to achieve common goals'. The organization is a solution to the management of the complex dynamics that exist in human societies. According to Dignum *et al.*, the agent paradigm is appropriate to model complex, open systems given that agents are autonomous entities with reasoning and communicative capabilities. Agent societies or multi-agent systems are therefore the virtual counterpart of real-life societies and organizations. An organizational model for agent societies must take into consideration both the structural and dynamic aspects of such societies (Dignum *et al.*, 2002). In addition, the model must also provide descriptive components for organizational roles, constraints, and interaction rules. Social interaction is a product of the adherence of organizational members to a set of social norms, and is regulated by mechanisms of social control, such as trust. Common norms and rules to which organizational members are expected to adhere effect social order within an organization.

The organization as a society has a common goal or purpose, structure, and norms. The desires or aims of the organization's individual-owners are represented through the organization's goal.

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

The organization's structure emerges from organizational roles, interactions, and the communication language. Individual roles are defined and assigned as required by the organization in order to meet its desired goals. The norms of an organization are tools to control the behavior of organizational members. In the case of a departure from those norms, an appropriate sanction is applied (Dignum *et al*., 2002).

Two perspectives are identified in the context of the organization: the agent perspective and the organization perspective (Dignum *et al*., 2002). The agent or individual perspective regards the organization as an environment in which individual actions occur. In this light, a multi-agent system is considered as nothing more than an aggregation of interacting agents. The coordination in such an environment stems from interaction-induced actions. Agents pursue their individual goals through an appropriate role and according to their own beliefs, desires, and intentions; and are thus not particularly concerned with the overall goal of their parent organization. From this perspective, however, the organization's goal may or may not in fact be known by an agent.

From the individual perspective, global behavior is assumed to emerge from individual agent interactions; however, this behavior cannot be easily externally managed or specified. In order to realize the goals of the organization, the behavior of the system must be considered and designed from a top-down perspective — that is the organizational perspective (Dignum *et al*., 2002). Thus, an organizational model must consider the global characteristics of the organization: stability, predictability, and clear commitment to aims and strategies.

In the organizational perspective, social design involves defining the overall goal or goals of the organization, and the roles and responsibilities of its members (Dignum *et al*., 2002). Roles are specified in accordance with the organization's goals. The organization sees the agent simply as a means to enact the defined roles. The actions taken by agents must conform, however, to the norms and interaction rules set out by the organization. From the organization perspective, however, the agent is viewed as a black box. In other words, the organization has neither a concern for how the agent actually implements its role nor which agent adopts it. The organization can monitor the system activity and verify that commitments are being met. In the event that an agent fails to fulfill her role, the organization may levy an appropriate sanction or penalty. There is thus a structural relationship between the parent organization and its members. The model proposed by Dignum *et al*. is therefore a tuple, consisting of roles, a communication framework, interactions, and norms.

DeLoach & Matson (2004) propose an organization model that resembles in many respects that of Dignum's as we described. An organization is similarly defined as 'including agents playing roles within a structure in order to satisfy a given set of goals.' Their organizational model consists of a structural model, a state model, and a transition function (DeLoach & Matson, 2004). The structural model is composed of a set of goals, a set of roles necessary to achieve the goals, a set of capabilities required to play those roles, and a set of rules or laws that constrain the organization. In contrast to the model in (Dignum *et al*., 2002), however, DeLoach & Matson (2004) introduce the idea of reorganization, a process which either modifies the organizational state or the organizational structure. Events that trigger reorganization include the arrival or departure of agents from the organization as well as changes regarding an agent's capabilities.

DeLoach & Matson (2004) seek to create an adaptive information system (AIS). An AIS is capable of dynamically changing processing algorithms or sources of information in order to facilitate the dissemination of information within the organization (DeLoach & Matson, 2004). The organization defined by their model transitions through various states. Goals, roles, capabilities, rules, and the set of agents may change over the lifetime of the organization, and therefore the proposed reorganization becomes necessary.

4.2 Inter-personal and inter-organizational trust

The issue of the definition of trust was previously introduced in the context of the intra-organizational model in Section 3.2. We discovered in our research as well as others (Blomqvist *et al*., 2002), that there have been many different conceptualizations in literature (Hexmoor *et al*.,

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

2004). This variation is due to each work casting a definition appropriate to the specific application-context. We defined trust for our specific domain (in Section 3.2), for an intra-organizational information sharing community. In our intra-organizational model, the concern in regards to trust relationships was limited to those interactions among agents within the same organization. In order to extend the intra-organizational model, the issue of trust is re-examined, since interactions now occur at the inter-organizational level. The role of trust in inter-organizational relationships is also explored.

Many have identified trust as an important issue in inter-firm or inter-organizational relationships (Dodgson, 1993; Gulati & Singh, 1998; Hagan & Choe, 1998; Parke, 1998; Zaheer *et al*., 1998). Much of the research conducted concerning inter-organizational trust has been from a theoretical standpoint (Currall & Judge, 1995). Since the mid to late 1990s however, there have been several studies that have produced important empirical evidence on the constitution and importance of trust in the inter-organizational context (Ganesan, 1994; Smith & Barclay, 1997; Zaheer *et al*., 1998; Karahannas & Jones, 1999; Perrone *et al*., 2003). There is still disagreement on the exact nature of the trust as a complex concept, its conceptualization, and measurement (Blomqvist *et al*., 2002). Fully understanding the effects of trust in different types of partnerships, however, will require further research in the community (Smith & Barclay, 1997).

In general, a certain amount of trust is necessary in order for inter-organizational cooperation to evolve (Dibben, 2000; Blomqvist, 2002). An established climate of trust that is internalized in organizational modes of behavior and supported by mutual belief is necessary for collaborative efforts between partner organizations (Dodgson, 1993). Positive sum gains can be achieved through trusted collaboration, such as reduced costs, greater speed, and improved ability to handle complexity (Arrow, 1974; Luhman, 1979; Dodgson, 1993). It is also believed to assist with environmental uncertainty, i.e., when a firm faces rapidly and disruptive changes in technology (Lorenz, 1988; Dodgson, 1993; Sako, 1994). Furthermore, trust affects a firm's long-term orientation (Ganesan, 1994), market performance (Aulakh *et al*., 1996), loyalty (Chow & Holden, 1997), relationships, commitment, cooperation, functional conflict, uncertainty, the propensity to leave, and acquiescence (Doney & Canon, 1997).

The difficulty in the conceptualization of trust in inter-organizational exchange is in extending what is inherently an individual-level phenomenon to the organizational level (Zaheer *et al*., 1998). The confusion stems from the issue of who is actually trusting whom: an organization has a trust orientation towards other partner organizations, as well as towards its constituent members; the individual organization members trust each other; and as well, they may have a collectively held trust orientation toward a partner firm (Zaheer *et al*., 1998). Given that trust is an individual-level phenomenon, however, the open question is how an organization establishes trust in either its own members or partner organizations.

Trust literature has identified two principal levels of trust assessment: inter-organizational and inter-personal trust (Dodgson, 1993; Ganesan, 1994; Smith & Barclay, 1997; Lane, 1998; Zaheer *et al*., 1998). These two levels of trust have been found to be empirically and theoretically distinct (see Figure 2), but related concepts, which implies that they must be studied using different measures (Zaheer *et al*., 1998). In addition, the antecedents to inter-personal and inter-organizational trust differ (Doney & Canon, 1997). Inter-personal trust is defined at the level of the individual, and represents the extent to which a member-agent places trust in her counterpart. The extent of trust placed in an organization by the collective members of a partner organization defines inter-organizational trust (Zaheer *et al*., 1998). Before discussing the constitution of trust at these two levels, it is important to examine a critical component, or role rather, in inter-organizational relations: the boundary spanner role.

4.3 The boundary spanner role

Organizations are often considered monolithic and faceless entities, but they are far from that. They are in fact pluralistic, and divided into different sub-interests, sub-units, and subcultures (Pfeffer,

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

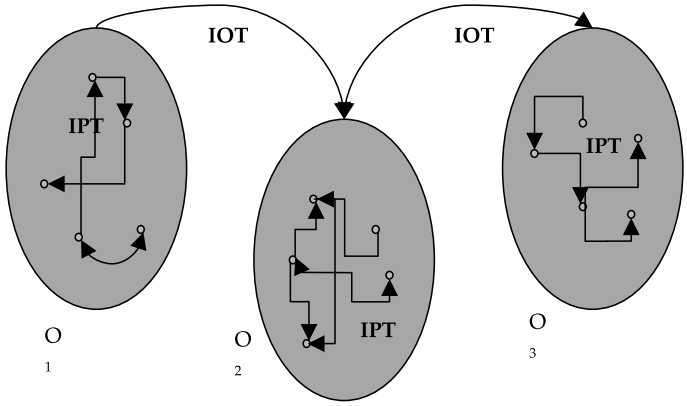


Figure 2 Inter-personal (IPT) and inter-organizational trust (IOT)

1982). Boundary spanners are those individuals within an organization who perform the 'facework' with other organizations (Katz & Kahn, 1978; Lane, 1998), and in this light, the role of the boundary spanner becomes important to the establishment of inter-organizational trust (Dodgson, 1993; Ganesan, 1994; Smith & Barclay, 1997; Zaheer *et al.*, 1998). In other words, the boundary spanner acts as a representative gatekeeper to the organization, or rather they represent the conduit that connects organizations (Leifer & Delbecq, 1978; Nochur & Allen, 1992; Cross & Prusak, 2002). Since the boundary spanner operates at the periphery of the organization, it is more closely involved in inter-organizational relationships than non-boundary spanners, and as well, they tend to interact more frequently with their counterparts (Leifer & Delbecq, 1978; Friedman & Podolny, 1992). Their orientations and motivations may be different from those held by the organization as a whole (Katz & Kahn, 1978). There are many variations on this theme, but it is common to find studies concerning such dyadic relationships in the context of buyer–seller situations (Ganesan, 1994; Smith & Barclay, 1997). Other names that have been associated with this role include input transducer, unifiers, change agents, regulators, members of extra-organizational transaction structure, liaison, planner, innovator, marginal men, linking pins (Nochur & Allen, 1992), and roving ambassadors (Cross & Prusak, 2002).

It has been argued that boundary spanners are essential elements of an effective organization, particularly in the context of a collaborative information-sharing process (Dodgson, 1993). The communication paths between individuals across boundaries are important in all theories of organizational learning (Dodgson, 1993). In the context of informal social networks (as opposed to traditional organizational hierarchies), the role of the boundary spanner has been identified as critical to an organization's productivity, because of their connections to other parts of the network within and without the organization (Cross & Prusak, 2002). Where problems span across the boundaries of multiple agencies, their interaction is required for solution development, and thus the focus must be placed on the building of inter-organizational capacity (Williams, 2002). The role of these catalysts or informational intermediaries as mutually trusted social lynchpins is pivotal in reducing informational asymmetries, establishing a common set of expectations, and facilitating goal adjustment (Ebers, 1999). Other identified functions of the boundary spanner include, 'scanning, stimulating data-generating activity, monitoring, evaluating data relevance, transmitting information, and facilitating interpersonal intercourse' (Michael, 1973, p. 240). They also foster cooperation and exchange; act as neutral arbitrators in conflict resolution; and reduce the costs and uncertainties of communication (Zaheer *et al.*, 1998; Ebers, 1999). Boundary spanners are often associated with innovation and entrepreneurship because of their greater access to the external world, critical resources, and information (Dodgson, 1994).

Although the literature on boundary spanners is limited and sparse, it is possible to identify several themes and perspectives that permeate the research concerning their profile (Williams, 2002). A cluster of reticulates or networking skills and judgments has been identified with the

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

boundary spanner, as well as the ability to cultivate inter-personal relationships, communication, political skills, and an appreciation of the interdependencies that surround the structure of problems and their potential solutions (Friend *et al.*, 1974). Webb (1991, p. 231) refers to individuals ′who are especially sensitive to and skilled in bridging interests, professions and organizations.' The boundary spanner is adept at resolving problems through unconventional approaches, and creative and lateral thinking (Williams, 2002). They represent visionaries (Leadbetter & Goss, 1998), mavericks, or catalysts (deLeon, 1996). Boundary spanners are also characterized by their ability to engage with others and use effective relational and inter-personal competencies (Williams, 2002). Their competencies include being effective at breaking down barriers and listening empathetically to others in order to build trust (Bacharach *et al.*, 2000). As previously mentioned, trust is one of the most important factors in inter-organizational relations, and is thought to be a more appropriate mechanism for controlling organizational life than hierarchical power (Sydow, 1998). Trust is also a mechanism used to reduce risk and uncertainty (Bachmann, 2001). When the outcomes of inter-boundary spanner relations meet expectations, trusting attitudes are reinforced and become part of the history of the relationship. This leads to positive expectations of future interactions (Vangen & Huxham, 1998). The personality of the boundary spanner is frequently referred to as personable, respectful, reliable, tolerant, diplomatic, caring, and committed (Williams, 2002). The boundary spanner must possess an impossible string of virtues (Beresfor & Trevillion, 1995). It is thus proposed that perhaps good collaborative behavior is a function of a particular set of personal attributes (Williams, 2002). This assumption is grounded in the personality school of thought in which it is argued that people differ because of defining characteristics, personalities, and temperaments (Eysenck, 1994). Trait theories have been contested as effective predictors of behavior by those who subscribe to a second school of thought that interprets individual differences in terms of cognitive styles and processes (Brunas-Wagstaff, 1998). Finally, boundary spanners possess foundational leadership skills such as strategic thought and action, the ability to facilitate a productive working group, and underlying character (Luke, 1998). The probing question that remains in this vein is whether effective boundary spanners are born or bred (Williams, 2002).

In many contexts, the boundary spanner role has traditionally been considered a naturally occurring, spontaneous phenomenon that develops in an informal, non-directed fashion (Nochur & Allen, 1992; Kostova & Roth, 2003). It is questioned whether individuals who are nominated or appointed the role of boundary spanner are as effective as those who have simply assumed the role naturally (Nochur & Allen, 1992). A study involved an examination of technological boundary spanners who were responsible for transferring technologies from the corporate research center of a major company to its operating units in New York City (Nochur & Allen, 1992). The findings that resulted from this study indicated that these technological boundary spanners were successful in the sense that they had greater contact with researchers at the corporate research center, and as well, were more likely to adopt the technologies developed therein. They failed, however, to effectively disseminate these technologies among their regional colleagues. These findings thus suggest that effective gatekeeping cannot be artificially induced by the simple assignment of individuals to the role of boundary spanner. The communication networks that ensure the effective dissemination of information between boundary spanners and their colleagues form over a period of time through both formal and informal contacts. Boundary spanners should therefore be chosen carefully from among individuals who are known to have strong extensive and trusted ties within the communication network, rather than nominated in an *ad hoc* fashion.

Organizations have cognitive systems and memories (Hedberg, 1981). Individual organization members will come and go, and its leadership will change, but organizations' memories preserve certain behaviors, mental maps, norms, and values over time (Hedberg, 1981; Zaheer *et al.*, 1998). Trust is a social aspect that functions as a mechanism for this internalization process (Zaheer *et al.*, 1998). The trust that is established by boundary spanners of one organization in boundary spanners of other organizations will be internalized or re-institutionalized by their parent organization (Lane,

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

1998; Zaheer *et al*., 1998). The creation and recreation of trust structures and actions at the inter-personal and inter-organizational level is akin to Giddens's theory of structurization (social sciences) (Giddens, 1984), which describes the conditions and mechanisms that contribute to the constitution of inter-organizational trust (Lane, 1998). This re-institutionalization process represents a micro–macro connection between inter-personal and inter-organizational trust — they have a positive influence on each other (Zaheer *et al*., 1998). Over the course of many interactions of boundary spanners between organizations, deeper and more stable cooperation arrangements develop between those organizations, as well as a certain degree of mutual trust (Lane, 1998; Zaheer *et al*., 1998). The established inter-organizational trust relationships represent and become norms (i.e., structures and routines) for each firm, and these norms will be adopted into the organizational clan culture (Zaheer *et al*., 1998).

There are findings that show that inter-organizational trust becomes the overriding factor in an exchange between firms with an established relationship (Zaheer *et al*., 1998). The orientation of one organization (represented by trust) towards another organization is adopted by the boundary spanner representative. Another noteworthy finding was that high organizational trust compensates in situations where there may be little trust between boundary spanners (Zaheer *et al*., 1998). Whereas the inter-personal trust that is established between boundary spanners is in a sense ephemeral, the inter-organizational trust between their parent organizations is, on the other hand, less susceptible to immediate strains in their exchanges. This implies the possibility of the simultaneous existence of high inter-organizational trust and low inter-personal, inter-boundary spanner trust.

4.4 The constitution of interpersonal and interorganizational trust

Although many studies such as Dodgson (1993), Ganesan (1994), Smith & Barclay (1997), and Zaheer *et al*. (1998) have revealed a link between inter-personal and inter-organizational trust and the importance of the inter-personal relationships established between boundary spanners, they did not hypothesize and explore the actual mechanisms involved in trust building at both levels. The manner in which trust develops and its maintenance has been recognized as an important element in human relationships. The influences or antecedents to trust at both the inter-personal and inter-organizational level, and how it changes over time and relates to social processes is an interesting research question. Next, we consider reports that investigate the constitution of inter-personal and inter-organizational trust. One report proposes a mathematical model for inter-personal trust constitution. Another report proposes a conceptual model for inter-organizational trust constitution.

Luna-Reyes *et al*. (2004) presented a formal inter-personal trust dynamics model that was founded upon a longitudinal case study of an inter-organizational information technology development project in New York City. This research involved analyzing social phenomena by methods that ranged from deductive reasoning by rules of formal logic to efforts to understand and offer 'thick' descriptions of the patterns of meanings and definitions of situations of people in everyday settings. The selected simulation model for this study was system dynamics. The model integrates concepts from economic models, psychological and sociological theories about trust, and learning and perceptual processes in inter-personal relations (Luna-Reyes *et al*., 2004).

The importance of trust in inter-organizational relations and in governance mechanisms, as discussed in the previous section, is echoed in (Luna-Reyes *et al*., 2004). Untrustworthiness often results in hazards that may affect the structure of inter-organizational relationships. The higher the level of trust between organizations, the lesser the need to protect against opportunism, which is considered to be one of the potential risks in any dyadic exchange. Trust levels also influence the effectiveness of knowledge sharing and other coordinated activities in organizational processes, as well as teamwork and collaboration. Elements that are typically considered central to the nature of trust are the concepts of vulnerability, risk, and the role of positive expectations or optimistic belief.

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

The expectation that the trustee will not act opportunistically determines whether the trustor grants or withholds trust. The positive expectations of the trustor can be based in part on observation and learning from the trustee's past actions. The calculation of trust on the part of the trustor may also be contingent on the trustor's ability to make an assessment of the trustworthiness of the trustee and her propensity to trust. Organizational and institutional factors may also affect this calculation. There is also evidence that suggests that social or economic factors or the identity of the dyadic parties affect trust development. Finally, a body of evidence has shown that trust development has path-dependence properties, and as well, that trust, once damaged by the pattern of spiral reinforcement of distrust, is very difficult to regain (Luna-Reyes *et al*., 2004).

Luna-Reyes *et al*., (2004) discuss early efforts in understanding the antecedents of trust. These include a game theoretic approach, the use of regression-like models, and the discussion of thick concepts associated with trust. The game theoretic approach is mainly inspired by the work of Axlerod (1984), who employed the prisoner's dilemma to understand the dynamic nature of cooperation. Where the focus was the study of trust, 'trust games' were involved. The efforts, centered on a game-theoretic approach, contributed an understanding of reciprocity and the expectation of future interactions in the development of trust. Statistical approaches contributed to the identification of the static structural characteristics of trust. Finally, conceptual approaches supplied rich descriptions, examples, and counterexamples that provide alternative models and perspectives in the study of trust (Luna-Reyes *et al*., 2004).

The premise of the model presented in Luna-Reyes *et al.* (2004) is that dynamic behaviors are closely tied to an underlying structure of feedback loops or reinforcement processes. Stocks (accumulations), rates (activities explaining how the stocks change), and the aforementioned feedback loops (closed causal relationships) represent the basic building blocks of the model. The dynamic characterization of trust demands a description of the observed behaviors and a causal structure that can reproduce those behaviors. The modeling technique that is thus used assumes that there is close interaction between behavior over time and feedback structure. The dynamic nature of trust is also associated with a set of reinforcement processes that characterize collaborative relationships. This collaboration provides an opportunity to trust. Over the course of many interactions and the accumulation of experiences, the dyadic parties get to know each other better and develop trust or distrust.

As previously mentioned, trust is considered a path-dependent phenomenon. This characterization means that small, random events early in the history of a system effectively determine its ultimate state, even in the case where those states are initially equally likely. An asymmetry in trust is considered: building and destroying trust. Trust building is a gradual process, but it can easily and quickly be destroyed by a single negative event or inconsistencies in the trustee's behavior (Luna-Reyes *et al*., 2004). According to theoretical and empirical observations, trust is likely nonlinear and trust and distrust move in different continua (Burt & Knez, 1996; Powell, 1996; Rousseau *et al*., 1998). The model and simulations in Luna-Reyes *et al.* (2004), however, assume that they exist on a single continuum, where distrust is a lack of trust.

The trust development processes that are involved in the inter-personal trust model in Luna-Reyes *et al.* (2004) are the following: institutional trust, calculative trust, knowledge-based trust, and identification-based trust. Institutional trust involves the regulation of the relationship between trustor and trustee through an institutional framework. This framework may consist of laws, regulations or certification bodies that provide and levy penalties for a party who behaves opportunistically or certify via some third party the trustworthiness of the trustee. The effect of this process is to reduce the trustor's perception of risk. Calculative trust refers to the trustee's estimation and weighing of the potential risks and benefits that may result from an interaction. A change in the perception of the institutional framework may result in a change in the perception of risk, promoting an increase in calculative trust. Knowledge-based trust (on the part of the trustor) derives from the trustee's level of expertise, her benevolence, ability, and integrity. It is also associated with the history or the process of the relationship. Finally, identification-based trust

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

refers to the emotional bonds that may form between the trustor and the trustee, or to the existence of shared values or objectives between them.

It is assumed that calculative trust plays a more important role in the initial stages of the relationship between trustor and trustee (Luna-Reyes *et al.*, 2004). When two parties decide to engage in an exchange, there are often formalities involved, such as a legal framework, which drives the level of perceived risk down. Over the course of time, however, this relationship matures as the two parties become better acquainted, and there is a shift towards knowledge-based trust. At this stage in the relationship, the established history between the two parties is more influential to the level of trust.

The model presented in Luna-Reyes *et al.* (2004) also distinguishes three different constructs that they found were used synonymously in the literature: propensity to trust (on the part of the trustor), trustworthiness (on the part of the trustee), and trust (understood as a willingness to be vulnerable).

Another key assumption in this model is that trust is learned and reinforced, and thus represents a product of ongoing interaction and discussions (Luna-Reyes *et al.*, 2004). An accumulation of experiences takes place over time. This accumulation changes, however, due to the activities of learning and forgetting. This phenomenon is described mathematically in Equation (1) below, which is inspired from (Luna-Reyes *et al.*, 2004):

$$\begin{aligned}\frac{d}{dt}(\text{A's knowledge about B}) &= (\text{Learning} - \text{Forgetting})\\ \text{Learning} &= \text{Frequency of the interaction}\\ &\quad \text{Learning per interaction}\\ &\quad \text{Effect of previous knowledge in learning},\\ \text{Forgetting} &= \frac{\text{A's knowledge about B}}{\text{TimetoForget}}.\end{aligned} \tag{1}$$

As reported in Luna-Reyes *et al.* (2004), we state that Equation (1) is based on the learning-by-doing approach used in organizations (Argyris & Schön, 1978; Levitt & March, 1988). Learning is assumed to be a function of experience that is affected by previously acquired knowledge (Luna-Reyes *et al.*, 2004). Initially, acquired knowledge facilitates learning with increasing returns. As the two parties in the relationship get to know each other better, those initial increasing returns become decreasing returns up to a maximum point. Finally, as knowledge reaches a point of saturation, the previous knowledge has a negative influence, and reduces a party's ability to learn to zero. The behavior of knowledge takes on the form of an s-shaped graph. The values of knowledge in their model are between 0.0 and 1.0 inclusive because of the chosen saturation point. The forgetting theory, however, is consistent with observations made in experimental psychology (Ebbinghaus, 1964). They formulate it as an exponential decay (Luna-Reyes *et al.*, 2004).

In the model of Luna-Reyes *et al.* (2004), the trust of one party, A, in another party, B, is the weighted average from two probabilities, one that is calculative in nature (calculative trust), and another that develops through the interaction and perception of B's trustworthiness (knowledge-based trust). This is given in Equation (2) below. This is also inspired from Luna-Reyes *et al.* (2004):

$$\begin{aligned}&\text{Trust in B} =\\ &\quad \text{A's knowledge about B}\\ &\quad \text{A's perception of B's trustworthiness}\\ &\quad +(1 - \text{A's knowledge about B}) \cdot \text{Calculative Trust}.\end{aligned} \tag{2}$$

The calculative component of Equation (2) (on the part of individual A) is a function of the risk of involvement with individual B; A's interest to get involved with B (desirability), and A's attitude concerning risk, which works as a threshold (see also Equation (3)). A's attitude to risk represents the normal desirability-to-risk ratio for A in a given situation that calls for trust. This attitude can be either risk-seeking (when the value is less than 1) or risk-avoiding (when the value is greater

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

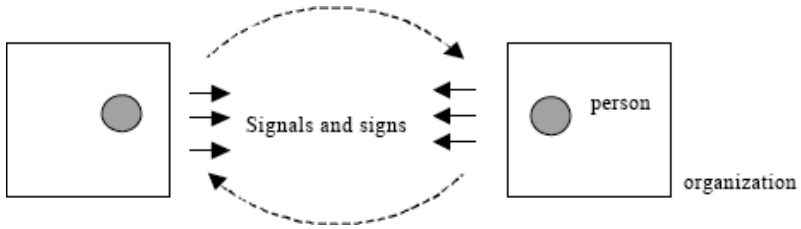


Figure 3 Mutual Assessment of Trustworthiness, inspired from Blomqvist *et al.* (2002)

than 1). Since the three variables that are involved in the calculative component of trust are context-dependent, A's attitude to risk can vary from one situation to another (Luna-Reyes *et al.*, 2004). As with Equations (1) and (2), Equation (3) below is also inspired from Luna-Reyes *et al.* (2004):

$$\text{Calculative Trust} = f\left[\frac{(\text{Desirability/Risk})}{\text{A's attitude to risk}}\right]. \tag{3}$$

The other component of trust is A's perception of B's trustworthiness (Equation (4)). It is also a weighted average between an *a priori* estimate of B's trustworthiness and a perception that is developed through the course of a history of experiences with B. A's knowledge about B works in the same fashion as described in relation to the formulation of Equation (1). The *a priori* component or Equation (2) can be gleaned from demographic and social similarities such as gender, race, or position in the organizational structure (Levin *et al.*, 2002). It can also be the result of long-term experiences (prejudices or schemas) of the trustor with a certain kind of trustee (Kramer, 1996; Heimer, 2001; Klimoski & Donahue, 2001). The data that are generated by the interaction of the two parties comprise the history-based component (Heimer, 2001; Klimoski & Donahue, 2001). A shift also occurs from the *a priori* estimate to the history-based perception of trustworthiness (Klimoski & Donahue, 2001). Equation (4) below is inspired from Luna-Reyes *et al.* (2004):

A's perception of B's trustworthiness=
A's knowledge about B
History-based perception of trustworthiness
+(1–A's knowledge about B
A priori perception of trustworthiness. (4)

In our suggested Equation (4), the *a priori* perception of trustworthiness is a constant, taking values between 0.0 and 1.0 inclusive. The history-based component, however, involves two reinforcing processes, and the exogenous inputs shown in Figure 3. The processes and inputs shown in Figure 3 constitute A's perceptual bias, and the rest of the conceptual elements relate to the path dependence character of A's trust in B. The history-based perception of trust (on the part of A) is equal to the proportion of good and bad experiences with B, which represents an asymmetry. Both of these kinds of experiences are registered and forgotten in A's memory according to the basic rates of learning and forgetting as described earlier in the generic knowledge model. Experiences with B are classified through A's assessment of B's observable behavior, which are represented in the model by a series of signs sent by B modified by noise (a series of random numbers). This assessment is also affected by A's perceptual bias, which means that when the combination of the history-based and *a priori* perception of trustworthiness indicates that B is trustworthy, A will tend to inflate the assessment of future observations of B's behavior, and *vice versa* (Luna-Reyes *et al.*, 2004).

The model in Luna-Reyes *et al.* (2004) has drawn support of the perceptual biases of their model from prior work, (e.g. Kramer, 1996; Bacharach & Gambetta, 2001; Klimoski & Donahue, 2001). The main sources of bias have been identified as a series of heuristics used by the trustor in the perceptual process: availability, anchoring, adjusting, and confirmation (Klimoski & Donahue, 2001; Messick & Kramer, 2001). Earlier judgments effectively interfere with the attributions associated with the trustee behavior, which reinforces the perception of trustworthiness or the lack

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

thereof on the part of the trustor. The time to forget these experiences grows proportionally and in the same direction as A's knowledge about B. This results in a reduction in the willingness to change the perception of trustworthiness, and holds it at a level that depends on the history of the perceptual process (Luna-Reyes *et al*., 2004).

The noise represented in the model associates with the emotional states of both the trustor and the trustee (Luna-Reyes *et al*., 2004). Noise and uncertainty are also influential in the trustor's selection of the cues associated with the trustworthiness of B (Bernieri & Gillis, 2001). The noise associated with the model is not white, but rather autocorrelated. This is due to the dynamic character of the model. The degree of the noise's autocorrelation varies inversely with the interaction frequency. The noise involved in the relationship between two parties will therefore be white noise when there is little interaction, but when there is frequent interaction, it will have a longer autocorrelation time, representing the repeated selection and interpretation of the cues according to A's emotional states (Luna-Reyes *et al*., 2004).

The 'bad-to-good time ratio' and the 'relative importance of bad experiences compared to good experiences' shown in Figure 3 represent the aforementioned asymmetry. The 'bad-to-good time ratio' represents the fact that A can hold on longer to bad experiences than good ones, and the 'relative importance of bad experiences compared to good experiences' causes bad experiences to be more influential (i.e., heavier) in the perception of good experiences involved in the history-based perception of trustworthiness. The two elements of this asymmetry model the observation that trust builds in a gradual fashion, but can be damaged or destroyed rapidly (Luna-Reyes *et al*., 2004).

The third and final component of the model reported in Luna-Reyes *et al*. (2004) is the propensity to trust. This characteristic is supported in Mayer *et al*. (1995). Others have referred to this concept as predisposition to trust (Creed & Miles, 1996), schemas (Klimoski & Donahue, 2001), general trust (Yamagishi, 2001), and trustfulness (Sztompka, 1999). In any case, it simply refers to a personality trait that represents the inclination of a party to perceive other individuals as trustworthy. The propensity to trust has three sources of influence in the model (Luna-Reyes *et al*., 2004). First and second, it affects the 'bad-to-good time ratio' and the 'relative importance of bad experiences compared to good experiences.' This is based on the assumption that if A is inclined to trust B, she will be consequently less likely to consider bad experiences in the history-based perception of trustworthiness, and as well, she will forget them faster. On the other hand, A will be less inclined to trust B, and will not forget bad experiences as readily. The third influence is the assessment of B's behavior. Therein, an individual who is predisposed to trust will tend to inflate all assessments from the behavior of the observed party. The alternative orientation results in a negative biasing of the same assessment.

The model in Luna-Reyes *et al*. (2004) considers the influence that B has in the perceptual process. The underlying motivation is B's desire to earn a good reputation as in Good (1988). The influence exerted by B, however, is limited because the perceiver has access to information that the trustee cannot control. This limitation is a result of the many ways in which that information can be interpreted (Good, 1988). In the model, the influence of B is a function of A's needs and concerns, but this influence is limited only to the reduction of the standard deviation of the process noise in Figure 3. B's ability to learn is limited by the trust that A previously had in B. When the level of trust is low on the part of A, A's willingness to share her needs with B is curtailed. On the other hand, high levels of trust will encourage A to disclose information, which will allow B to learn more, coupled with a low level of noise (Levin *et al*., 2002).

We have discussed the underlying influences or antecedents for trust at the inter-personal level through the examination of the inter-personal trust model reported in Luna-Reyes *et al*. (2004). Our discussion now forays into trust building at the organizational level. We consider an inter-organizational trust model reported in Blomqvist & Ståhle (2000) in the context of asymmetric partnerships, where partnering firms possess different skills, resources, and knowledge. These asymmetries represent the catalyst for inter-firm exchange, which are enhanced through a trusted relationship. Trust is therefore considered a necessary antecedent for cooperation.

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

In this model, the interplay between inter-personal and inter-organizational trust is scrutinized as in Blomqvist (1997). They adopt the notion proffered in Zaheer *et al.* (1998) that the two are distinct but related concepts. It is the individual members of an organization that trust another organization, not the organization itself. They recognize the importance of the boundary spanner role as a means to build trust between partnering organizations. They reference the work in framing the concept of organizational trust (Creed & Miles, 1996) — an embedded predisposition (i.e., a function of managerial philosophy and its manifestations), characteristic (dis)similarity affected by organizational actions and structure, and experiences of reciprocity affected by organization context for reciprocity. We first turn to the concept of inter-personal trust as adopted by this model. The inter-personal and inter-organizational levels of trust are inextricably linked in an inter-firm exchange setting.

Trust is said to be one party's expectation of the other party's competence, goodwill, and behavior (Blomqvist, 1997). In a business context, both competence and goodwill are needed for trust to develop. Competencies such as technical capabilities, skills and knowledge are also necessary antecedents for the building of trust in the professional setting of business exchange. Moral responsibility and positive intentions toward the other party represent signs of goodwill. These signs are also necessary for the trusting party to be able to accept the potentially vulnerable position in which she places herself (i.e., the inherent risk). If there is a perception of positive intentions on the part of the trustor, there is also the perception of a cooperative attitude. The behavior of the parties is also an important factor in trust (Bidault & Jarillo, 1997). Although the trustor may perceive positive intentions on the part of the trustee, she will also be looking for the fulfillment of those intentions or expectations.

Blomqvist (1997) echoes the play of the phenomenon of path dependence in the constitution of trust introduced earlier in the discussion of the model in Luna-Reyes *et al.* (2004). Early signs and signals that are perceived by both parties set the tone for the relationship. As the relationship progresses, their respective behaviors rise to a greater level of importance in trust building.

The model presented in Blomqvist (1997) is based on Giddens' (1984) theory of *structurization* and a model on experience of trust developed by Jones & George (1998). Giddens theory of *structurization* involves the interplay between structure and action. Action (i.e., process and practice) simultaneously constitutes structure and is also enabled by it. Over the course of time, the structures of signification, legitimization, and domination become institutionalized and taken for granted, which augments similar assumptions and expectations that enhance the trust between two parties. Consequently, trust develops through individual or organizational structures (or characters), which are signaled through actions. Those actions are evaluated as signs of trustworthiness. The value system of an individual determines her experience on trust. It is believed that values may create the propensity to trust, a concept that is more general than trust that is based in the context of specific situations and relationships. Values represent general principles, or rather, an individual's guidance system. These values are relatively permanent, and set the scene for the experience of trust. In time, values may change as an individual gains new knowledge and as her attitudes change. Attitudes may be construed to indicate knowledge, beliefs, and feelings about others, as well as a means to define and structure interactions. Moods and emotions play a role in terms of establishing a first impression of another individual. This impression is important, as it sets the tone for the relationship.

The central modes of trust production, as indicated in Zucker (1986) are institutional-based trust, characteristic-based trust, and process-based trust. Institutional-based trust refers to formal societal structures that depend on firm-specific or individual attributes, and on intermediary attributes. Characteristic-based trust relates to a person or individual, and is based on attributes such as ethnicity or background. Process-based trust is tied to expected or past exchanges, and manifests itself in a manner such as reputation.

It is believed that individuals maintain mental accounts regarding the perceived history of trust-related behaviors involving the self and other individuals (Creed & Miles, 1996). In an

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

evolving relationship, the individuals therein are in a constant process, consciously or unconsciously, of evaluating the trustworthiness of each other. This evaluation is based upon indices or signals in the trustee's speech and behavior. This is a similar concept to the history-based perception of experiences that are a part of the model described in Luna-Reyes *et al.* (2004). The concern that arises as the driving goal of this evaluation is to determine whether the other party truly has the trusting party's best interests in mind, or whether there is a campaign to take advantage of the trusting situation. The ability to deal with risk and the ability to develop trust will depend upon the boundary spanner's ability to comprehend formal processes and sense-making. Determining the other party's value system in the beginning of a relationship is costly, and therefore parties may initiate a relationship based upon conditional trust. As knowledge about the other party accumulates, there is a reduced importance of this conditional trust (Jones & George, 1998). This thought echoes the calculative-based trust component of the model in Luna-Reyes *et al.* (2004). Trust is fragile, and the period during which conditional trust is highly influential in the maintenance of the relationship could be considered a sort of trial. If trust deteriorates too gravely, then a failure of the parties to reach simpatico will result and distrust will emerge. Unconditional trust, on the other hand, represents the catalyst to the development of a deeper relationship, such as friendship (Blomqvist, 1997).

Our earlier discussion of inter-personal and inter-organizational trust, as well as the discussion of the boundary spanner role, introduced the support in the literature to the notion that individual, organizational, and inter-organizational trust are in fact interrelated. The work in Blomqvist (1997) has also drawn upon this body of literature and supports this view. They refer to additional sources, (e.g. Swan *et al.*, 1988) in which it is claimed that individual or inter-personal trust is a mechanism for promoting organizational trust. Inter-personal trust is seen as a means to enhance the performance of inter-firm exchange (Zaheer *et al.*, 1998). It is believed that inter-personal and inter-organizational trust may develop and impact each other simultaneously, or that either one develops first and impacts the other (Blomqvist, 1997).

The trustworthiness of a salesperson affects the trust experienced by the company (Swan *et al.*, 1988). If the company, on the other hand, has a good reputation, then others are likely to perceive its salespeople as highly trustworthy, as well. The interplay between inter-personal and inter-organizational trust is dynamic: if either one of them deteriorates, this event will have a negative impact on the other (Blomqvist, 1997). If an organization wishes to effectively develop a good reputation, then it must promote internally a strong culture of trustworthiness (Blomqvist, 1997). It must also provide a means to reward boundary spanners who adhere to organizational norms through positive reinforcement, and punish those who act opportunistically (Barney & Hansen, 1994).

The model for inter-organizational trust developed in (Blomqvist, 1997) inspired our IEOTBSM shown in Figure 4. In the model, the development of trust is based on inter-organizational and inter-personal trust, as both may be objects of trust. The model is also based on structure and action, which is derived from Giddens' theory of structurization (Giddens, 1984). The model is organized by the three-dimensional conceptualization of trust: competence, goodwill, and behavior. The bases for trust in this model were chosen from relevant literature reviewed in Blomqvist (1997). The organizational bases for trust are realized through organizational actions, and the individual bases for trust are realized through individual actions. These actions indicate to the auditor of trust the validity of the base for trust through signs and signals. The interplay between structure and action in the model is understood in light of the dynamics of trust. Trust building in the model, is an iterative and cyclical process.

4.5 General description of the inter-organizational trust-based security model

Since the IEOTBSM is based in part on the intra-organizational trust-based security model (IAOTBSM) presented earlier, we will briefly discuss additions and changes to our model.

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

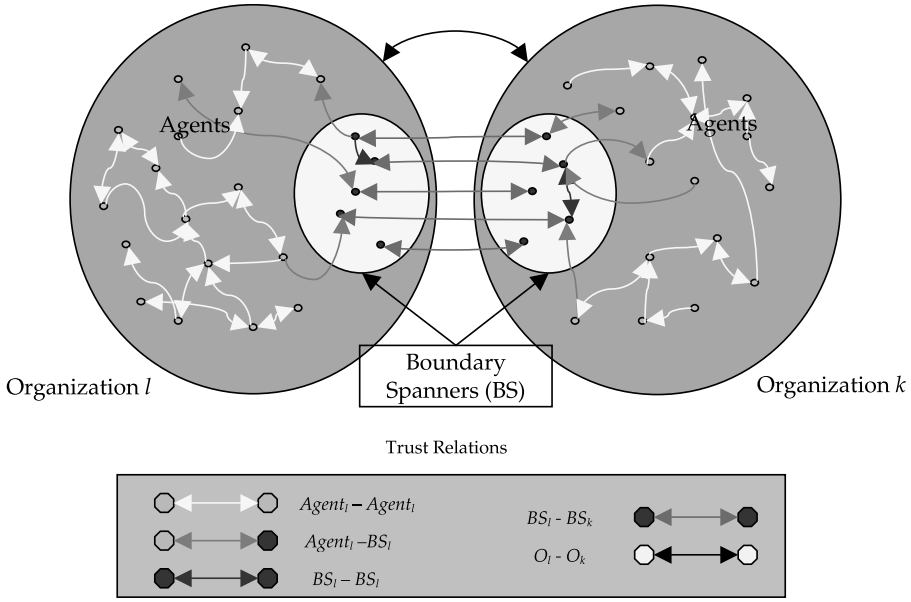


Figure 4 Graphic Representation of the IEOTBSM

The key addition to IAOTBSM is the addition of the boundary spanner. Each organization in the inter-organizational network elects a certain predefined percentage of its constituent agents to the role of boundary spanner based upon the boundary spanner regulatory process described earlier. The boundary spanner plays the central role of inter-organizational gatekeeper for an organization, as discussed in the preceding literature review. In the context of the information-sharing community, the boundary spanner is responsible for representing the information needs of its constituent agents. From the organizational perspective, the overall goal is to maintain a high degree of information flow within and without the organization. At the personal level, however, individual agents have their own goals, which are to obtain specific information or facts. These personally held goals, however, are assumed to be congruent with the organization's overall goal.

In order to fulfill the fact requirements of individual agents, each organization maintains a fact request repository to which agents post their required facts every cycle. Since boundary spanners are organizational representatives, they neither produce nor require personal facts (beyond currently outstanding personal fact requirements upon role ascension); they adopt, rather, all facts that are posted to the fact request repository. Individual boundary spanners of one organization have at least one relation to a boundary spanner of each and every other organization in the inter-organizational network. It is assumed that all organizations in the inter-organizational network participate (through their respective boundary spanners) voluntarily in an effort to reduce the asymmetries that may exist among them, which is the reason for this fully coupled requirement. Facts flow into the organization from the boundary spanner through whatever trust relations existed between her and her constituent agents before she assumed the role. This implies that there may also be trust relations between boundary spanners of the same organization. These specific relations are supported in the literature as necessary for successful inter-firm exchange. As boundary spanners' (as representatives) and their constituent agents' fact requirements are satisfied, those fact requests are removed from the fact request repository.

Agents of all organizations in the inter-organizational network produce and require facts from the same fact warehouse. It is assumed that the participating organizations have a collective goal, which, in the context of an information-sharing community, is to solve some collective problem. The required fact of an agent in one organization may not necessarily be available within her own organization. Again, it is the boundary spanner who acts as the conduit that allows for the flow of information among organizations, and is thus key in reducing the informational asymmetries in the information-sharing community. The existence of the boundary spanner, however, is not a

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

guarantee that a fact request will always be filled. The flow of information in the inter-organizational network is ultimately controlled by whatever network of trust relations evolves during the course of the exchange activity. The IEOTBSM does not consider the entering or leaving of either agents or organizations from the system, which means that the evolution of the network results only from the elimination of pre-existing inter-agent and inter-boundary-spanner relations due to the existence of unintended receivers (a contradiction to organizational norms).

The addition of the boundary spanner role to the original model results in new interaction trust relations. Previously, in the IAOTBSM, the interaction trust relations were defined in the context of only inter-agent exchange. In the IEOTBSM, the interaction trust relations now include the following orientations: agent–agent (of the same organization), agent–boundary spanner (of the same organization), boundary spanner–agent (of the same organization), boundary spanner–boundary spanner (of the same or of different organizations), and organization–organization. Figure 4 illustrates these relations. Interaction trust relations remain reflexive, and, in addition, it is still the case that the transitivity and symmetry properties do not hold. The trust relations between agents and boundary spanners are those at the inter-personal level of trust. Inter-organizational relations are those at the inter-organizational level of trust (collectively held by the constituent agents and boundary spanners). The literature review revealed the distinction between the two levels of trust, but also stressed their interplay. A trust calculus presented in Section 4.6 describes this interplay mathematically.

The *trust threshold*s that were defined for the IAOTBSM remain with the addition of a boundary spanner–boundary spanner threshold. Where the exchange is between agents of the same organization, the corresponding trust relation of one in the other is still the controlling factor for information dissemination. This is also the case for agent–boundary spanner, boundary spanner–agent, and boundary spanner–boundary spanner exchanges where the exchange entities are of the same organization. Where the exchange is between boundary spanners of different organizations, the mechanism controlling information dissemination involves the consideration of not only the trust at the inter-personal, inter-boundary spanner level, but, in addition, the trust relation that exists between the parent organizations (inter-organizational) of the exchange. This is the micro–macro link between the two levels of trust that was discussed in the literature. As previously mentioned, Section 4.6 presents a trust calculus that describes this link mathematically. Briefly, however, inter-organizational trust contributes to inter-boundary spanner trust by a certain predefined weight. High inter-organizational trust will compensate for low inter-personal trust. It is assumed that inter-organizational trust will always have the greater influence, since, as stated in the literature, inter-organizational trust is deeper and more enduring (as an organizational norm). Inter-personal trust that is established by boundary spanners of one organization in boundary spanners of another organization influences over time the inter-organizational trust of the former organization in the latter. The details of this interplay, again, are discussed in Section 4.6.

As in the IAOTBSM, agents continue to monitor their fact pedigree in order to identify *intended* and *unintended receivers*. It is possible that the *fact path* will involve the participation of a boundary spanner. In that event, the boundary spanner acts as a pseudo-initiator of the fact, since in relation to the agent-initiator, all extra-organizational entities (boundary spanners and agents) would be unintended receivers. If a boundary spanner propagates a fact over the organizational boundary, it monitors the path of that fact, as well, and shares the fact pedigree of the original initiator agent. An unintended receiver on the part of an agent retains its original definition. Similarly, from the perspective of the pseudo-initiator boundary spanner, an unintended receiver is defined as a boundary spanner of a partner organization with which the pseudo-initiator boundary spanner has insufficient trust. If either the fact initiator agent or the pseudo-initiator boundary spanner agent determines that a breach of security has occurred, the selected *trust policy model* for the system will be applied to the entities along the fact path. Even though the boundary spanner is a pseudo-initiator, she is still held responsible (as a representative) for the dissemination of the initiator's fact to an unintended receiver, and will thus incur whatever sanction is levied.

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

```
1  initialize organizations, agents, fact warehouse, fact requirements,
     interaction trust relations, trust thresholds, trust policy model,
     expiration interval, and total number of cycles
2  for each cycle {
3    if (cycle % β (boundary spanner regulatory process rate)=0)
       perform boundary spanner regulatory process
5    every agent generates a fact and adds its fact requirements to its
       organizations's fact request repository
6    every agent boundary spanner checks for its fact requirement(s)
       from its set of accessible facts {
7    if an agent's fact request is met, the agent is satisfied and her
       fact request is removed from the fact request repository of her
       parent organization
8    if any of a boundary spanner's fact requirements is met, then that
       fact request is removed from the fact request repository of her
       parent organization }
9    pseudo share the received facts each agent does not require and the
       facts each boundary spanner possesses
10   share the generated fact each agent does not require
11   share the pseudo share
12   each initiator agent and pseudo-initiator (boundary spanner)
       checks for current unintended or intended receivers and applies
       trust policy model if there are any unintended receivers
13   compute ia & sm for the inter-organizational network
12   for every fact check if it is expired }
```

Figure 5 Modified trust-based information sharing algorithm

The trust policy models defined in the IAOTBSM are adopted by the IEOTBSM with no modifications. The metrics of the IAOTBSM, *information availability* (IA), *security measure* (SM), percentage information availability (percentage of IA), and percentage security measure (percentage of SM) were impacted and their definitions have been updated. Since the information-sharing community of the IEOTBSM now involves the participation of multiple organizations, the new goal of the trust-based security model is to maximize information availability and minimize security measure in the entire inter-organizational network. The calculation of IA thus now considers the total of the sum of satisfied agents and the number of intended receivers for all organizations (percentage of IA being expressed as this same total sum as a percentage of the total facts shared in all organizations). SM is similarly computed as the total number of unintended receivers in all organizations. These newly defined metrics provide a macro-level view of the system's performance. It is also possible to view at a micro-level the performance of an individual organization in terms of intra-organizational activity by computing its personal IA and SM. Finally, the trust-based information-sharing algorithm has been updated as show in Figure 5.

4.6 Inter-organizational and inter-boundary spanner trust calculus of the IEOTBSM

The trust calculus presented herein mathematically describes trust building at inter-organizational level and the instantaneous trust at the inter-boundary spanner (inter-personal) level. Since trust is an individual-level phenomenon, trust building at the inter-organizational level depends upon the trust relations established by an organization's boundary spanners with the boundary spanners of partner organizations. Inter-organizational trust develops over the course of the multiple interactions of an organization's constituent boundary spanners. The trust between two organizations o_m and o_n is thus a function of the total number of interactions, i, and the average of all of the trust relations, r, of the boundary spanners of o_m with those of o_n (see Equations (5) and (6)):

$$\tau_i(o_m, o_n, r_i^{mn}) = \frac{\tau_0^{mn}}{\tau_0^{mn} + (1 - \tau_0)e^{-r_i^{mn} i}}, \tag{5}$$

where τ_0^{mn} is the initial trust between o_m and o_n; $i > 0$.

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

Equation (5) represents a *logistic* or *Verhulst growth function*. In a general, the logistic growth function describes population growth (from an initial size), which, unlike exponential growth, eventually reaches a maximum (horizontal asymptote) in time. This maximum population size represents the *carrying capacity* of the population's environment. The carrying capacity is a limit at which the resources of the environment have been exhausted and can no longer support growth. The *growth* of the population is exponential, under the influence of a *rate*, until the population begins to reach the carrying capacity. As the size of the population approaches the carrying capacity, population growth is negatively affected and begins to level off.

The logistic growth function appropriately describes trust building at the inter-organizational level. Trust of one organization in another builds exponentially to a maximum of 1.0 from an initial amount of trust. This initial amount of trust could be established by considering the bases for trust enumerated in the organizational trust model discussed in Section 4.5: organizational character; organizational structure; organizational goals and vision; managerial philosophy; organizational culture; organizational values; and competence (see Figure 4). As a simplifying assumption, the initial trust, τ_0, is set to a random value in the range 0.0 to 1.0 inclusive.

The rate, r, at which trust grows, is determined by computing the average of the trust relations of all boundary spanners of the organization-trustor in the boundary spanners of the organization-trustee (Equation (6)). This represents one side of the micro–macro link between inter-personal and inter-organizational trust as discussed in earlier sections. The higher the value of the average, the greater the rate at which inter-organizational trust builds during the exponential phase, and the lower the value, the slower the rate of growth. The total number of trust relations, xy, is arbitrarily raised to the power of x, the total number of boundary spanners for the trustor-organization, in order to scale down the overall average to a more suitable value for the rate, r. This decision was based in part on the intuition that the fewer the number of boundary spanners of the trustor-organization, the more influential their trust in determining the inter-organizational trust (i.e., the more weight given to each individual boundary spanner's trust).

The average of the trust relations of the boundary spanners was chosen to represent the rate of growth, r, based upon the model for inter-personal trust discussed in Section 4.5. The trust value for an inter-boundary spanner relation can be interpreted as the overall *experience* of the trustor-boundary spanner with the trustee-boundary spanner, given that in the IEOTBSM, *trust policy models* affect inter-entity trust relations. In that vein, the trust value represents the quality of the experiences of the trustor-boundary spanner with the trustee-boundary spanner. In the event that the trustee-boundary spanner was a participant in the *fact path* leading to an *unintended receiver*, the experience is bad; otherwise the experience can be interpreted as good. Note that in the case of a bad experience, trust is negatively affected, but in the case of good experience, trust simply remains unchanged. In the IEOTBSM, inter-personal trust building is not currently modeled, as it is outside the scope of this particular stage of its development. Given this and the assumption that distrust (negative trust) is also not currently considered in the IEOTBSM, inter-organizational trust building is either strictly increasing or does not increase beyond the initial trust (when r is 0.0):

$$r_i^{\mathrm{mn}} = \frac{\sum_{j=1}^{x} \sum_{k=1}^{y} \tau_{i-1}(b_j^{\mathrm{m}}, b_k^{\mathrm{n}}}{(xy)^x}, \tag{6}$$

where x is the total number of boundary spanners in $\mathrm{o_m}$ and y is the total number of boundary spanners in $\mathrm{o_n}$.

Finally, in regards to Equation (5), the variable i is the total number of interactions (or facts shared) on behalf of the boundary spanners of the trustor-organization. The total number of interactions takes the place of time, which is normally used in logistic growth. The total number of interactions was chosen as a means to include the history-based component of trust constitution at the inter-personal level discussed in Section 4.5, which influences inter-organizational trust. As the number of interactions increases, trust begins to grow. The rate of growth, again, depends upon the

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

average of the boundary spanner trust (good-to-bad experiences) of the trustor-organization. We have explored inter-organizational trust building under the following parameter values: = 0.2 and r=0.0025.

The other side of the micro–macro link between inter-personal and inter-organizational trust is the influence that inter-organizational trust has in inter-boundary spanner relations. Recall that the inter-personal experiences of an organization's boundary spanners are internalized over time, representing norms, by the organization and manifest ultimately in the building of inter-organizational trust. These norms also have an immediate externalizing effect on inter-boundary spanner interaction, as discussed in Sections 4.2 and 4.3. Inter-organizational trust is more stable and enduring than inter-personal trust, which is a quality guaranteed by the use of a logistic-based trust calculus. Although a model for inter-personal trust building is not provided in the trust calculus of the IEOTBSM, a formula that describes the influence of inter-organizational trust in inter-boundary spanner trust (inter-personal) was developed due to the tight coupling and interplay of the two trust levels. The instantaneous trust of a boundary spanner of a trustor-organization in a boundary spanner of a trustee-organization at interaction i is calculated by the following formula:

$$\tau_i(b_j^{\mathrm{m}}, b_k^{\mathrm{n}}) = \tau_i(o_{\mathrm{m}}, o_{\mathrm{n}}, r)\alpha + \tau_{i-1}(b_j^{\mathrm{m}}, b_k^{\mathrm{n}})(1-\alpha),$$

where is the implementation defined weight (as a percentage) given to the inter-organizational trust and o^{jk} is set as a random value in the range 0.0–1.0 inclusive; $i>0.

First, the constant allows for the particular implementation of the IEOTBSM to determine how much influence inter-organizational trust has in the overall inter-boundary spanner trust. Second, it ensures that the resulting inter-boundary spanner trust value is in the range 0.0 to 1.0. No basis upon which to set this value was revealed in the literature review of Sections 4.2–4.5; however, the literature suggests that should be greater than 50%. High inter-organizational trust and low inter-personal trust can coexist. In this situation, inter-organizational trust compensates for the deficiency at the inter-personal level.

4.7 Boundary spanner regulatory process

The boundary spanner regulatory process is the mechanism by which boundary spanners are selected by each organization in the inter-organizational network. One of the most important qualities of an inter-organizational network in the context of an information-sharing community is the free exchange of information internally, as well as externally, across a trusted backbone of organizational entities. The boundary spanner plays a very important role in this process, as it bridges the gap across organizational boundaries. It is responsible for representing the interests (norms) of its respective organization, and, in addition, externalizes organizational structure through its exchange activities (Perrone *et al.*, 2003). The literature suggests (Section 4.3) that a determiner of the effectiveness of a boundary spanner lies in certain personality traits. In general, an individual who has strong inter-personal skills is more effective at boundary spanning activities. This is based upon the observation that these individuals tend to form numerous relationships, and, as a result, generate a more extensive inter-personal network.

The trustworthiness of an agent is an appropriate and sufficient metric for determining its suitability as a boundary spanner, since it 'represents the inherent, underlying potential for a trustee to be reliable, predictable, and fair' (Perrone *et al.*, 2003). As the literature suggests (Section 4.3), those individuals who are deemed highly trustworthy will naturally manage to establish more inter-personal relationships than those who are less trustworthy. Of course, it is important to continuously monitor the exchange activity of an organizational boundary spanner in order to ensure that it is consistent with the norms of the organization. In the event that a boundary spanner fails to meet the expectations of its constituent-agents (frequently a participant in fact delivery to an unintended receiver), the parent organization must remove the agent from the role in a timely manner to avoid any further damage to inter-organizational relations.

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

The promotion of agents to the boundary spanner role and their potential demotion is based upon trustworthiness or reliability ranking of all organizational entities (agents and boundary spanners). A reliability-metric algorithm developed by Shruti Veeravali's Master's Project (working paper, University of Arkansas) was adapted to the IEOBSM for this purpose. It represents the first stage in the boundary spanner regulatory process. The reliability-metric algorithm produces a reliability ranking of agents through a conversion of an organization's interaction trust relation graph (derived from the matrix representing trust relations between entities). The notion of reliability is defined by the trust values that exist in all of an entity's (agent or boundary spanner) trust relations. For example, given two agents, a_i and a_j, agent a_i's reliance on agent a_j is equivalent to agent a_i's trust in agent a_j. It is important to note a single distinction here between trust and reliance. As a simplifying assumption, reliance, unlike trust, is transitive. Similar to trust, however, reliance is both reflexive and non-symmetric.

The computation of an entity's reliability involves examining incoming trust relations to the entity-node. Of these relations, there is a distinction between direct and indirect trust relations. A direct trust relation exists between two agents if there is a single edge that connects them, whereas an indirect trust relation is one that involves two or more edges.

The trust values along the edges of the graph are used in the reliability computation. Note that, when considering an entity-node in the graph, both direct and indirect relations can exist, since transitivity is permitted. The reliability of each agent in the graph is thus determined by dividing the sum of the trust values from direct and indirect relations by the total number of agents in those relations (the entity-node in-degree), and then multiplying that value by the number of entities involved in direct trust relations. In the case of indirect relations, note that there may be multiple paths that establish this relation, and that some may be cyclic. In an indirect relation, thus, only acyclic paths are considered, and from among those paths, the path with the maximum value is selected for the reliability computation.

Once the reliability values have been computed, the agents are ranked accordingly:

Rank 1 (the most reliable entity)	Entity 3
Rank 2	Entity 4
Rank 3	Entity 1
Rank 4 (the least reliable entity)	Entity 2

The boundary spanner regulatory process proceeds from the reliability computation stage to then bestowing the boundary spanner role to the top x entities (agents and boundary spanners), where x is a percentage of the total number of entities of a particular organization. If a boundary spanner is one of the top x entities, then his assignment continues. If an entity that was previously a boundary spanner in the last reliability ranking computation is not present among the top x in the present, then a demotion occurs.

When an agent becomes a boundary spanner, all inter-agent trust relations that existed with other agents of the parent organization before the role adoption remain. This means that there may also be trust relations between boundary spanners of the same organization. A trust relation is established randomly between the new boundary spanner and a boundary spanner of another network organization, such that there is at least one relation per organization (i.e. all organizations have at least one boundary spanner trust-relationship with every organization in the network). If this condition has been met, then the boundary spanner randomly establishes a relation with a boundary spanner of another organization. This inter-boundary-spanner trust relation takes a random value in the range 0.0 to 1.0. Finally, the new boundary spanner discontinues its personal fact requirement beyond any currently outstanding required fact, and ceases to generate facts. It then additionally adopts all current fact requirements in the boundary spanner fact request repository.

For the boundary spanner who is demoted in this process, there are several items that must be addressed. The trust relations that the former boundary spanner had with boundary spanners of

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

partner organizations are discarded. The former boundary spanner relinquishes any currently held fact requirements from the fact request repository, and begins again to generate facts and have its own personal fact requirements beyond any currently outstanding personal fact requirement.

The rate at which the boundary regulatory process takes place, β, should be determined according to the particular needs of the implementation. Intuitively, this rate should not be too low (frequent ranking), as it reduces the effectiveness of an individual boundary spanner in building inter-organizational trust; however, it should not be too high (infrequent ranking), because it would allow poor-performing boundary spanners to consistently damage inter-organizational trust.

4.8 Formal definitions of the inter-organizational trust-based security model

Definition 1. The *inter-organizational trust-based security model* (*IEOTBSM*), is (*CEM,IM,TRM*) where *CEM* is the constituent element model, *IM* is the interaction model, and *TRM* is the trust relation model that includes a calculus of trust update policies.

Definition 2. The *constituent element model* (CEM), is (O, A, B, F, R) where O is a set of known organizations (representing the inter-organizational network), A is a set of known agents, B is a set of known boundary spanner agents, F is the fact warehouse, a set of known and static facts in the inter-organizational network, and R is the set of all organizations.

Definition 3. An *organization*, $o_{\square} \in O$, is a known organization.

Definition 4. An *agent*, $a_k \in A$, also denoted as $a_k^{\square}$, is a known intelligent, autonomous entity that is a member of an organization $o_{\square}$. $a^{\square}$ represents the set of agents that are members of the organization $o_{\square}$.

Definition 5. A boundary spanner agent, $b_j \in B$, also denoted $b_k^{\square}$,-is a known intelligent, autonomous entity that is an inter-organizational representative of an organization $o_{\square} \in O$. $b^{\square}$ represents the set of boundary spanner agents that are members of the organization $o_{\square}$. Boundary spanners are also known as *pseudo-initiators* of facts that they receive from agents within the organization and share with other boundary spanners of partner organizations in the inter-organizational network.

Definition 6. A *fact*, $f_t \in F$, is a datum. Each agent, except boundary spanners, in an organization has a personal requirement for a fact and produces a fact. Boundary spanner agents of an organization assume all of the facts that reside in the boundary spanner *fact request repository* as their required facts. All other agents' fact requirements, selected from the fact warehouse, are assumed to remain constant. A boundary spanner's fact requirements, however, will vary upon the addition and removal of facts from the fact request repository. Every agent also continuously produces facts from the fact warehouse that are shared. The fact produced and the requirement for the agent can be the same, or another agent might require the fact produced by an agent. Agents are not cognizant of other agents' requirements. This is a simplifying assumption that will affect the information sharing and its availability. Herein, the terms fact and information are used interchangeably.

Definition 7. A *fact request repository*, $r_u \in R$, also denoted $r_u^{\square}$, is a repository of facts accessible to boundary spanner agents, $b^{\square} \in B$. Agents, $a_k \in A$, submit their required facts to their respective organization's fact repository, r_u. Boundary spanner agents of an organization assume all facts, as a pseudo-initiator, in that organization's respective fact request repository as their own required facts.

Definition 8. Entity x's *trust* in entity y is entity x's estimation of the probability that entity y will preserve entity x's welfare with regard to the information transmitted.

Definition 9. The *interaction model*,*IM*, is (*ITR*, *ISP*) where *ITR* is the interaction trust relation and *ISP* is the information-sharing protocol.

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

Definition 10. The *interaction trust relation*, *ITR*, is a trust relation among entities. *ITR* in the *IEOTBSM*, denoted as $\tau(e_i, e_j)$, is the trust of entity i in entity j, where $e_i, e_j \in O, A, B$.

A trust relation, τ, is an adjacency matrix that contains trust values between its constituent entities. The trust values are quantified in a non-discrete manner as a real value in the range 0.0 to 1.0. $\tau(x, y)$ is the trust that entity x has in entity y. The trust relation between entities is assumed *a priori*. An entity is cognizant of its trust to its neighboring entities, which can vary as the system transitions over time. However, the neighboring entities are not apprised of the trust the entity has in each of them. A trust value of 1.0 indicates entity x's complete trust in entity y. If there exists no relation between entity x and entity y, entity x either has lack of trust in entity y or entity x is ignorant or cannot make a trust-related judgment about entity y. This represents a simplifying assumption by interpreting the aforementioned cases as the same and assigning a trust value of 0.0 to them.

Properties of interaction trust relation

Reflexivity: Trust relations are reflexive, i.e., an entity trusts itself completely with a value of 1.0.
Symmetry: Trust relations are not symmetric, i.e., entity x's trust in entity y does not necessarily imply entity y's trust in entity x.
Transitivity: Trust relations are not transitive. Entity x's trust in entity y and entity y's trust in entity z does not necessarily imply entity x's trust in entity z.

The permitted trust interactions in the IEOTBSM are as follows:

(ITR1) The trust of agent i in agent j, where i, j belong to the same organization m is denoted as $\tau(a_i^m, a_j^m)$, where $a_i, a_j \in A$, $o_m \in O$, and $i \neq j$.
(ITR2) The trust of agent i in boundary spanner j, where i, j belong to the same organization m is denoted as $\tau(a_i^m, b_j^m)$, where $a_i \in A$, $b_j \in B$, $o_m \in O$, and $i \neq j$.
(ITR3) The trust of boundary spanner j in agent i, where i, j belong to the same organization m is denoted as $\tau(b_i^m, a_j^m)$, where $b_j \in B$, $a_i \in A$, $o_m \in O$, and $j \neq i$.
(ITR4) The trust of boundary agent i in boundary spanner agent j, where i, j belong to different organizations m, n, respectively is denoted as $\tau(b_i^m, b_j^n)$, where $b_i, b_j \in A$, $o_m, o_n \in O$, $i \neq j$, and $m \neq n$.
(ITR5) The trust of organization m in organization n is denoted as $\tau(o_m, o_n)$, where $o_m, o_n \in O$, and $m \neq n$.

Definition 11. The *trust threshold*, *TT*, is a user-defined static minimal trust value that guards information sharing, i.e., a threshold. $\Theta(x,y)$, which lies in the range 0.0 to 1.0 both inclusive, denotes a threshold value for the interaction trust relation between entity x and entity y. The trust threshold, a system level metric, for the interaction between any two entities of the same organization $\square$ is denoted as $\Theta(e^{\square}, e^{\square})$. The trust threshold is pivotal to the decision that an agent or boundary spanner makes, based on trust, in propagating a fact. The trust threshold thus restricts information sharing. The defined trust thresholds in the *IEOTBSM* are as follows:

(TT1) The trust threshold for the interaction between two agents of the same organization m is denoted by $\Theta(a^m, a^m)$. We assume TT1, which corresponds to (ITR1), to be the same for every organization in O.

(TT2-3) The trust threshold for the interaction between an agent and a boundary spanner of the same organization m is denoted by $\Theta(a^m, b^m)$ or $\Theta(b^m, a^m)$. We assume TT2, which corresponds to ITR2 and ITR3, to be the same for every organization in O.

(TT4) The trust threshold for the interaction between two boundary spanners of different organizations m and n is represented as $\Theta(b^m, b^n)$. We assume TT3, which corresponds to ITR4, to be the same for every organization in O.

(TT5) The trust threshold for the interaction between two organizations is denoted by $T(o_m, o_n)$, and corresponds to ITR5.

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

Definition 12. *Information sharing* is the exchange of information among entities, such that this exchange does not violate the constraints imposed by either the interaction trust relations or the information-sharing protocol.

Definition 13. A *cycle* is the amount of time taken by an entity to receive or generate a fact and share it with its neighbors.

Definition 14. The *information-sharing protocol*, *ISP*, is a collection of rules that govern the information sharing in the *IEOTBSM*. These rules are stated in terms of the trust relations between entities and the trust threshold of such interactions. The rules for traversal of a fact from entity x to entity y are denoted by $\Gamma(x, y)$. They map to a Boolean value which represents entity x's compliance to the rules. If agent x and agent y have a relation, agent x checks if the values of $\Gamma_1(x, y)$ and $\Gamma_2(x, y)$, as defined below, are true before propagating the fact to agent y. Likewise the rules that govern the propagation of facts between boundary spanners are defined by $\Gamma_3(x, y)$ and $\Gamma_4(x, y)$. All entities monitor the fact traversal path for breaches in security in every cycle, based on these criteria. A breach of security exists whenever the fact propagated by an entity is received by another entity with which the initiator entity has no relation (or insufficient trust in relation to the corresponding trust threshold). Note that in the case of a fact propagated by a boundary spanner, a breach of security exists when the fact is received by a boundary spanner who belongs to an organization with which the initiator boundary spanner's parent organization has insufficient trust, since boundary spanners do not have direct relations with agents across organizational boundaries and since inter-organizational agent exchange is not defined.

Definition 15. An agent or boundary spanner is *satisfied* if and only if the fact required by it is the same as the fact it has access to. An agent's *accessible facts* constitute the fact generated by it in the current cycle and the facts that it receives from its neighbors in the previous cycle, if any. A boundary spanner's accessible facts are only those received from agents or boundary spanners in the current cycle, as they do not generate facts.

In Equations (7) and (8), ISP1 and ISP2 describe the conditions for interaction between two entities within the same organization. ISP1 denotes the trust threshold condition that needs to be satisfied before an entity shares a fact with its neighbors. ISP2 takes into consideration the neighbor's *willingness* to receive information.

Definition 16. An entity is *willing* to receive facts if it is not satisfied with the facts it currently has access to.

$$(\text{ISP1})\Gamma_1(e_i^{\square}, e_j^{\square}) = \begin{cases} \text{True} & \text{if and only if } \tau(e_i^{\square}, e_j^{\square}) \geq \Theta(e^{\square}, e^{\square}) \\ \text{False} & \text{otherwise,} \end{cases} \tag{7}$$

$$(\text{ISP2})\Gamma_2(e_i^{\square}, e_j^{\square}) = \begin{cases} \text{True} & \text{if and only if } e_j^{\square} \text{ is willing} \\ \text{False} & \text{otherwise.} \end{cases} \tag{8}$$

In Equations (9) and (10), ISP3 and ISP4 describe the conditions for interaction between two boundary spanners of different organizations. ISP3 denotes the trust threshold condition that needs to be satisfied before a boundary spanner shares a fact with another boundary with which it has a relation. ISP4 takes into consideration the *willingness* of the recipient-boundary spanner to receive information.

$$(\text{ISP3})\Gamma_1(b_i^{\square}, b_j^{k}) = \begin{cases} \text{True} & \text{if and only if } \tau(b_i^{\square}, b_k^{\square}) \geq \Theta(b^{\square}, b^{k}) \\ \text{False} & \text{otherwise,} \end{cases} \tag{9}$$

$$(\text{ISP4})\Gamma_2(b_i^{\square}, b_j^{k}) = \begin{cases} \text{True} & \text{if and only if } b_j^{k} \text{ is willing} \\ \text{False} & \text{otherwise.} \end{cases} \tag{10}$$

Definition 17. The *entity fact path* of a fact f_t denoted by Ψ_t is a graph, where the nodes represent entities (agents or boundary spanners) that constitute f_t's traversal during information sharing.

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

$\Psi_t(e_i, e_j)$ is a sub-graph of the entity fact path Ψ_t initiated by e_i and currently held by e_j. An agent e_k is said to belong to the fact path $\Psi_t(e_i, e_j)$ if and only if e_k belongs to the vertex set of $\Psi_t(e_i, e_j)$. This is represented as $e_k \in \Psi_t(e_i, e_j)$, where $i<k\leq j$. For simplicity, the term entity fact path and $\Psi_t(a_i^{\square}, a_j^{\square})$ are used interchangeably.

Definition 18. The *signature* of an entity is a unique identifier consisting of two fields, the current cycle number and the initial of the entity. It is assumed that each entity has a unique initial.

Definition 19. The *fact pedigree* of f_t is a document that contains signatures of all entities who have received f_t. The fact pedigree through which the fact has been shared is maintained with the fact as the entity fact path.

An entity fact path and a fact pedigree are constructed for every fact as it is shared among entities in each cycle. Every entity that receives a fact in the process of such sharing *signs* its initial on the fact pedigree. Thus it becomes a part of the fact's path. No other entity has access to the fact pedigree other than the entity who initiated the fact. The initiator entity of every fact can query the fact pedigree to obtain the list of signatures of the entities that are currently in possession of the fact and also the entire graph of signatures in the fact pedigree. It checks to determine whether its trust in the recipient-entity warrants its receiving the fact and classifies it as either an intended or unintended receiver. This decision is based on the trust values in the interaction trust relation.

Definition 20. An agent a_j is an *intended receiver* in the fact path $\Psi_t(e_i, e_j)$, if ISP1 and ISP2 are true and the agent a_j is not satisfied after receiving fact f_t.

Definition 21. A boundary spanner b_j is an *intended receiver* in the fact path $\Psi_t(e_i, e_j)$, if ISP3 and ISP4 are true and the boundary spanner b_j is not satisfied after receiving fact f_t.

Definition 22. An agent a_j is an *unintended receiver* in the fact path $\Psi_t(e_i, e_j)$ if either ISP1 or ISP2 or both are false and the agent a_j is not satisfied after receiving fact f_t.

Definition 23. A boundary spanner b_j is an *unintended receiver* in the fact path $\Psi_t(e_i, e_j)$ if either ISP3 or ISP4 or both are false and the boundary spanner b_j is not satisfied after receiving fact f_t.

Definition 24. The *trust policy model*, *TPM*, defines the calculus of trust update policies that regulates the interaction trust relations in the inter-organizational network. These policies were designed to simultaneously maximize the information sharing and minimize the unintended receivers in the IEOTBSM. They are applied to the entities that participate in the fact path that involves an unintended receiver. The three different TPMs of the IEOTBSM, which vary by degree of restrictiveness, follow:

(TPM_1) This trust policy model updates the trust relation between every consecutive pair of entities in a fact path starting from the unintended receiver back toward the initiator agent. Every entity's trust in the succeeding entity is reduced exponentially based on the relative role played by each entity in propagating the fact ultimately to the unintended receiver. The reduction value is determined by the relative positions of the entities along the fact path. The premise of this update policy lies in the observation that every entity in the path is relatively and in-part responsible for the fact's transmission to the unintended receiver. Entities who are earlier in the chain of causation are deemed less responsible than those later in the chain.

Definition 25. The *degree of responsibility*, given in Equation (11), for every entity in the entity fact path is the depth of the entity (with the agent fact originator as the root element) in the entity fact path. The unintended receiver would thus have the maximum degree of responsibility and the originator's neighbor the minimum degree of responsibility. The trust update value in Equation (12) is proportional to the exponential of the length of the succeeding entity with user-defined trust decrement factor as the base. This value is now applied to the edge between an entity and its succeeding entity in the graph as described by Equation (13).

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

Given δ_{ee}, the user-defined inter-entity trust decrement factor in the range 0.0 to 1.0 inclusive, if e_i. is the initiator agent of f_t and e_j is an unintended receiver, then $\forall\, e_k \in \Psi_t(e_i, e_j)$,

$$\textit{Degree of Responsibility } (e_k) = \textit{Depth of } e_k \textit{ in } \Psi_t(e_i, e_j) \tag{11}$$

$$\textit{Trust update } (e_k) = (\delta_{ee})^{\textit{Degree of Responsibility } (e_j) - \textit{Degree of Responsibility } (e_k) + 1} \tag{12}$$

$$\tau(e_{k-1}, e_k) = \begin{cases} \tau(e_{k-1}, e_k - \textit{Trust update } (e_k) & \textit{if } \tau(e_{k-1}, e_k) \neq 0, \\ 0 & \textit{if } \tau(e_{k-1}, e_k) = 0. \end{cases} \tag{13}$$

(TPM_2) This trust policy model is a variant of TPM_1. For every edge in the entity fact path, trust is updated with the same user-defined trust decrement factor using Equation (14). This policy model is more restrictive than TPM_1 since every entity in the fact path is held equally responsible for the transmission of the fact to the unintended receiver.

$$\tau(e_{k-1}, e_k) = \begin{cases} \tau(e_{k-1}, e_k - \delta_{ee}) & \textit{if } \tau(e_{k-1}, e_k) \neq 0, \\ 0 & \textit{if } \tau(e_{k-1}, e_k) = 0. \end{cases} \tag{14}$$

The policies that consider consecutive pairs of entities in the path are advantageous when there is no direct trust relationship between the initiator and an unintended receiver, and the fact is transmitted across covert channels. These policies are based on the assumption that the number of unintended receivers will be ultimately reduced since the role played by at least one of the entities would be diminished such that the path is broken (at some entity's position) and the fact is prevented from reaching the unintended receiver.

(TPM_3) is a third trust policy model that updates the trust between the initiator entity and every entity in the path by a user-defined decrement factor. If an edge exists from the initiator entity to an entity in the entity fact path, trust of the initiator agent in the entity is reduced using Equation (15). By reducing the agent initiator's trust value directly in her neighbors that are on the fact path, this policy model impedes the first step in the fact transmission to the unintended receiver.

$$\tau(e_i, e_k) = \begin{cases} \tau(e_i, e_k - \delta_{ee}) & \textit{if and only if } \tau(e_i, e_k) \neq 0, \\ 0 & \textit{if and only if } \tau(e_i, e_k) = 0. \end{cases} \tag{15}$$

Definition 26. *Total facts shared* are the cumulative of the count of intended and unintended receivers of all organizations within the inter-organizational network. It is formulated in equation (16)

$$\begin{aligned} \textit{Total facts shared} = {} & \textit{Number of intended receivers of organization } o_i \\ & + \textit{Number of unintended receivers of organization } o_i \textit{ for all } o_i \in O. \end{aligned} \tag{16}$$

Definition 27. *Information availability*, *IA*, is the degree to which information is freely available when shared among a group of entities (agents and boundary spanners) within the inter-organizational network. IA is a system level metric and is formulated as the sum of the number of entities who are satisfied and the number of intended receivers. Note that the sets intended receivers and satisfied entities are disjoint.

$$\begin{aligned} IA = {} & \textit{Number of intended receivers of organization } o_i \\ & + \textit{Number of satisfied agents of organization } o_i, \forall\, o_i t \in O. \end{aligned} \tag{17}$$

Definition 28. *Percentage IA* is the IA as a percentage of the total facts shared within the inter-organizational network.

$$\textit{Percentage } IA = (IA / \textit{Total facts shared}) \times 100. \tag{18}$$

Definition 29. *Security Measure*, *SM*, a system level metric, is the number of unintended receivers in the inter-organizational network.

$$SM = \textit{Number of unintended receivers of organization } o_i, \forall\, o_i \in O. \tag{19}$$

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

Definition 30. *Percentage SM* is the *SM* as a percentage of the total facts shared within the inter-organizational network.

$$Percentage\ SM = (SM / Total\ facts\ shared) \times 100. \quad (20)$$

It is important to note in this context that percentage IA and percentage SM are based on total facts shared, which arises only when the facts are shared. That is, if every entity's generated fact satisfies its fact requirement or if no entity is willing to receive a fact, no facts are shared and the value of total facts shared is zero. In such situations, the facts accessible to each entity are simply discarded. IA, percentage IA, SM, and percentage SM in Equations (17), (18), (19), and (20) respectively are measured continuously in the IEOTBSM. The aim of the IEOTBSM in terms of IA and SM is to maximize percentage IA and minimize percentage SM.

Definition 31. *IA saturation cycle* is the cycle number at which percentage IA and percentage SM converge to their ideal values, i.e. 100% and 0%, respectively.

Definition 32. *Expiration interval*, a system level metric, is the number cycles for which a fact can be shared after its creation. A fact is said to be *expired* after its expiration interval. Such expired facts are simply discarded.

5 Implications

Although the inter-organizational trust-based security model (IEOTBSM) presented in this work was designed in the context of an inter-organizational information-sharing community, it is adaptable to applications in other contexts. The inter-organizational information-sharing community represents a distributed environment like the Internet, which often involves the participation of unknown entities and is highly volatile. Other open systems that have a distributed or pervasive nature could also benefit from trust-based security. We alluded to those beneficial qualities in the Introduction. We support them in light of the presentation of the IEOTBSM.

One of the advantages of the IEOTBSM is its robustness. In the inter-organizational information-sharing community, malicious participants, either agents or boundary spanners, are effectively removed from the system. A malicious participant in this context, again, represents an unintended receiver. Breaches of security will likely occur during the initial cycles of the information-sharing algorithm, but eventually the inter-organizational network will stabilize, as the channels or paths through which those breaches occurred are eliminated. A hard security mechanism such as a firewall or access control list cannot necessarily recover from a security breach unassisted, and service availability is typically suspended.

Currently, the IEOTBSM does not consider changes to the inter-organizational network, such as the leaving or joining of participating agents or organizations. It is thus not as volatile or dynamic an environment as most distributed and pervasive open systems; however, the model could accommodate such volatility, if it were augmented with a mathematical model for trust building at the inter-personal level. A standard access control approach to security cannot automatically adapt to such changes since users must be manually added and their rights defined by a human, and its manageability is increasingly reduced as the number of participants in a system increases.

The IEOTBSM also embodies the quality of scalability. No matter the size or configuration of the inter-organizational information-sharing network, the model will adequately suit its application. The individual participants (agents and organizations, on behalf of their constituent boundary spanners) of the network are given the responsibility of deciding, based on trust, with whom they interact. There is no central authorization or certification authority that could potentially become a bottleneck if the network were initially too large or grew to an overburdening size. A distributed or pervasive open system, whether enormous like the Internet or relatively small like a university grid, would therefore be well served by a soft security model like the IEOTBSM.

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

In an environment like the Internet, where the participants of the network include both human and software agents, a security system based on trust will be more easily accepted and maintained. The human user will be more comfortable in an environment where the underlying mechanism controlling inter-entity interaction is trust, a social phenomenon that is for them inherent and innate. Many services on the Web or other networks require users to present identification credentials like a user I.D. and password. Although such an approach provides an effective means of securing the service and protecting any personal user information, it can be a frustrating experience for the legitimate user. For instance, a user may frequently visit many Internet sites that require the use of a user I.D. and password. It is nearly impossible, of course, for the user to remember all of them. She is therefore likely to write them down, comprising security and defeating the efforts of the overall approach. A more natural experience for the user would result from the use of trust as the underlying mechanism of security. A user continues to use services that she has come to trust over time. Likewise, service-entities on the Web or network interact with users (or other service-entities), whom they have not identified as malicious and in whom they trust.

6 Conclusions and future work

The inter-organizational trust-based security model (IEOTBSM) introduced in this work represents first and foremost a significant progression of the work that inspired its creation. Our original goal in developing the intra-organizational trust-based security model (IAOTBSM) was to develop a security model that would foster greater information availability in an inter-agent information-sharing community, while ensuring the confidentiality of the information exchange. The effectiveness of our earlier model was examined through simulations of an implementated simulation. The IAOTBSM was limited in its context, however, since inter-organizational information exchange was not permitted.

The next stage in the development of the IEOTBSM will include considerations of validation and verification that have not been possible thus far. Another upcoming task for this work is the development of an inter-personal trust calculus that will adequately model trust building at this level. This will bring the inter-organizational network, as a multi-agent system, to a closer approximation to its real-world counterpart since it will then support the ability of agents and organizations to enter and leave the system. Trust building at both the inter-personal and inter-organizational levels represents a complex phenomenon or process that involves the interplay of many variables, and therefore, our initial attempt at modeling inter-organizational trust was restricted and simplistic in approach so that it would be easier to establish a base. Improving the inter-organizational trust calculus to a more complex degree will also be necessary. Multiple trust-building models may be necessary, as well, given that the literature has indicated that trust building in a specific context is unique.

In conclusion, we claim that the IEOTBSM meets the anticipated goals set out at its inception. The model fulfills the requirements that are necessary for the distributed environment of an inter-organizational information-sharing community. It is scalable, robust, and more appropriately addresses security in the context of a network in which there is a mixed participation of human and agent entities. It also provides a framework that can be adapted to applications in other kinds of open systems. One of the major contributions of this work is the consolidated examination of inter-organizational and inter-personal trust, and the boundary spanner role. Although there has been considerable discussion of inter-personal and inter-organizational trust in the literature, there have been few attempts to formally describe their respective trust-building processes. Their distinctiveness has been supported by many, as well as the interplay between them. This finding further complicates the design of trust building models. We believe that the trust calculus introduced in this work, however, is a good approximation of trust building at the inter-organizational level, and we hope that it will inspire others in the community.

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

References

Abdul-Rahman, A. & Hailes, S. 1997 A distributed trust model. In *Proceedings of the 1997 Workshop on New Security Paradigms*, Langdale, Cumbria, UK, pp. 48–60.

Alfarez, A.-R. & Hailes, S. 1997 Using recommendations for managing trust in distributed systems. In *Proceedings of IEEE Malaysia International Conference on Communication'97 (MICC'97), Kuala Lumpur, Malaysia*.

Argyris, C. & Schon, D. A. 1978 *Organizational Learning: A Theory of Action Perspective*. Reading, MA: Addison-Wesley.

Arrow, K. J. 1974 *Limits of Organization*. New York: W.W. Norton.

Aulakh, P. S., Kotabe, M. & Sahay, A. 1996 Trust and performance in cross-border marketing partnerships: a behavioral approach. *Journal of International Business Studies* **27**, 1005–1032.

Axlerod, R. 1984 *The Evolution of Cooperation*. New York: Basic Books Inc.

Bachmann, R. 2001 Trust, power, and control in trans-organizational relations, *Organizational Studies* **22**(2).

Bacharach, M. & Gambetta, D. 2001 Trust in signs. In Cook (ed.), *Trust in Society*. New York: Russell Sage Foundation, pp. 148–184.

Bacharach, S. B., Bamberger, P. & McKinney, V. 2000 Boundary management tactics and logics in action: the case of peer-support providers. *Administrative Science Quarterly* **45**(4), 704–736.

Barney, J. B. & Hansen, M. H. 1994 Trustworthiness as a source of competitive advantage. *Strategic Management Journal* **15**.

Beavers, G. & Hexmoor, H. 2003 Understanding agent trust. In *Proceedings of the International Conference on Artificial Intelligence (IC-AI)*, pp. 769–775.

Beresfor, P. & Trevillion, S. 1995 *Developing Skills for Community Care*. Aldershot: Arena.

Bernieri, F. J. & Gillis, J. S. 2001 Judging rapport: employing Brunswick's lens model to study interpersonal sensitivity. In Hall & Bernieri (eds.), *Interpersonal Sensitivity: Theory and Measurement, Personality and Clinical Psychology Series*. Mahwah, NJ: Lawrence Erlbaum.

Bidault, F. & Jarillo, C. J. 1997 Trust in economic transactions. In Bidault, Gomez & Marion (eds.), *Trust: Firm and Society*. London: Macmillan Press.

Blaze, M., Feigenbaum, J. & Lacy, J. 1996 Decentralized trust management. In *Proceedings of the IEEE Conference on Security and Privacy*.

Bledsoe, R. C. 2002 The 21st century federal manager: a study of changing roles and competencies. A report by a panel of the Human Resources Management Consortium, National Academy of Public Administration.

Blomqvist, K. 1997 The many faces of trust. *Scandinavian Journal of Management* **13**(3).

Blomqvist, K. 2002 Partnering in the dynamic environment: the role of trust in asymmetric technology partnership formation. *Acta Universitatis Lappeenrantaensis* **122**.

Blomqvist, K. & Ståhle, P. 2000 Building organizational trust. In *The 16th IMP Conference, Bath, UK, 6–9 September 2000*.

Blomqvist, K., Sundqvist, S. & Soininen, M. 2002 Towards measuring interorganizational trust: some issues in conceptualization and operationalization of trust in recent research on inter-organizational trust. In *The European Academy of Management Trust Track at the 2nd Annual Conference on Innovative Research in Management, Stockholm*.

Britton, C. & Bye, P. 2004 *IT Architectures and Middleware: Strategies for Building Large Integrated Systems,* 2nd edn. Reading, MA: Addison-Wesley.

Brunas-Wagstaff, J. 1998 *Personality: A Cognitive Approach*. London: Routledge.

Burt, R. S. & Knez, M. 1996 Trust and third-party gossip. In Tyler & Kramer (eds.), *Trust in Organizations: Frontiers of Theory and Research*. Thousand Oaks, CA: Sage Publications.

Chow, S. & Holden, R. 1997 Toward an understanding of loyalty: the moderating role of trust. *Journal of Managerial Issues* **9**(3).

Creed, W. E. D. & Miles, R. 1996 Trust in organizations: a conceptual framework linking organizational forms, managerial philosophies, and the opportunity costs of controls. In Tyler & Kramer (eds.), *Trust in Organizations: Frontiers of Theory and Research*. Thousand Oaks, CA: Sage Publications.

Cross, R. & Prusak, L. 2002 The people who make organizations go – or stop. *Harvard Business Review* June, 5–12.

Currall, S. C. & Judge, T. A. 1995 Measuring trust between organizational boundary role persons. *Organizational Behavior and Human Decision Processes* **64**(2).

deLeon, L. 1996 Ethics and entrepreneurship. *Policy Studies Journal* **24**(3).

DeLoach, S. A. & Matson, E. 2004 An organizational model for designing adaptive multiagent systems. In *Proceedings of AAAI Workshop on Agent Organizations: Theory and Practice (AOTP), 25–29 July 2004*.

Dibben, M. R. 2000 *Exploring Interpersonal Trust in the Entrepreneurial Venture*. London: Macmillan.

Dignum, V., Meyer, J.-J. C. & Weigand, H. 2002 Towards an organizational model for agent societies using contracts. In *Proceedings of AAMAS*.

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

Dodgson, M. 1993 Learning, trust, and technological collaboration. *Human Relations* **46**(1).
Dodgson, M. 1994 Technological collaboration and innovation. In Dodgson & Rothwell (eds.), *The Handbook of Industrial Innovation*. Chelthenham: Edward Elgar Publishing.
Doney, P. M. & Canon, J. P. 1997 An examination of the nature of trust in buyer-seller relationships. *Journal of Marketing* **61**.
Ebbinghaus, H. 1964 *Memory: A Contribution to Experimental Psychology*. New York: Dover.
Ebers, M. 1999 Explaining inter-organizational network formation. In Ebers, M. (ed.), *The Formation of Inter-organizational Networks*. Oxford: Oxford University Press, pp. 3–40.
Eysenck, H. J. 1994 Trait theories of personality. In Hampson & Colman (eds.), *Individual Differences and Personality*. London: Longman.
Friedman, R. A. & Podolny, J. 1992 Differentiation of boundary spanner roles: labor negotiations and implications for role conflict. *Administrative Science Quarterly* **37**.
Friend, J. K., Power, J. M. & Yewlett, C. J. L. 1974 *Public Planning: The Intercorporate Dimension*. London: Tavistock.
Ganesan, S. 1994 Determinant of long-term orientation in buyer-seller relationships. *Journal of Marketing* **58**.
Giddens, A. 1984 *The Constitution of Society*. Cambridge: Polity Press.
Gil, Y. & Ratnakar, V. 2002 Trusting information sources one citizen at a time. In *Proceedings of the First International Semantic Web Conference*.
Goecks, J. & Cosley, D. 2002 NuggetMine: intelligent groupware for opportunistically sharing information nuggets. In *Proceedings of the 7th Annual International Conference on Intelligent User Interfaces*, pp. 87–94.
Golbeck, J., Bijan, P. & Hendler, J. 2003 Trust networks on the semantic Web. In *Proceedings of Cooperative Intelligent Agents 2003*.
Good, D. 1988 Individuals, interpersonal relations, and trust. In Gambetta (ed.), *Trust: Making and Breaking Cooperative Relations*. Oxford: Blackwell, pp. 31–48.
Gulati, R. & Singh, H. 1998 The architecture of cooperation: managing coordination costs and appropriation concerns in strategic alliances. *Administrative Science Quarterly* **43**(4), 781–814.
Hagan, J. M. & Choe, S. 1998 Trust in Japanese interfirm relations: institutional sanctions matter, *Academy of Management Review* **23**(3).
Hardin, R. 2002 *Trust & Trustworthiness.* New York: Russell Sage Foundation.
Hedberg, B. 1981 How organizations learn and unlearn. In Nystrom, P. & Starbuck, W. (eds.), *Handbook of Organizational Design*, vol. 1. Oxford: Oxford University Press.
Heimer, C. A. 2001 Solving the problem of trust. In Cook (ed.), *Trust in Society*. New York: Russell Sage Foundation, pp. 40–88.
Hexmoor, H., Bhattram, S. & Wilson, S. 2004 Trust-based security policies. In *Proceedings of the 2004 Secure Knowledge Management Workshop, Buffalo, NY*.
Hogg, L. M. J. & Jennings, N. R. 2001 Socially intelligent reasoning for autonomous agents. *IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans* **31**(5).
Jones, G. & George, J. 1998 The experience and evolution of trust: implications for cooperation and teamwork. *Academy of Management Review* **23**(3).
Jøsang, A. 1997 The right type of trust for distributed systems. In *ACM New Security Paradigm Workshop, Lake Arrowhead, CA, USA*.
Karahannas, M. & Jones, M. 1999 Interorganizational systems and trust in strategic alliances. In *Proceedings of the 20th International Conference on Information Systems, Charlotte, North Carolina*.
Katz, D. & Kahn, R. 1978 *The Social Psychology of Organizations*, revised edn. New York: Wiley.
Klimoski, R. J. & Donahue, L. M. 2001 Person perception in organizations: a overview of the field. In London (ed.), *How People Evaluate Others in Organizations*. Mahwah, NJ: Lawrence Erlbaum.
Kostova, T. & Roth, K. 2003 Social capital in multinational corporations and a micro-macro model of its formation. *Academy of Management Review* **28**(2), 297–317.
Kramer, R. M. 1996 Collective trust and collective action: the decision to trust as a social decision. In Tyler & Kramer (eds.), *Trust in Organizations: Frontiers of Theory and Research*. Thousand Oaks, CA: Sage Publications.
Lane, C. 1998 Introduction: theories and issues in the study of trust. In Bachman & Lane (eds.), *Trust Within and Between Organizations*. New York: Oxford University Press.
Leadbetter, C. & Goss, S. 1998 *Civic Entrepreneurship*. London: Demos.
Leifer, R. & Delbecq, A. 1978 Organizational/environmental interchange: a model of boundary spanning activity. *Academy of Management Review* **3**, 40–50.
Lesser, V., Ortiz, C. L. & Tambe, M. 2003 *Distributed Sensor Networks: A Multiagent Perspective*. Boston, MA: Kluwer.
Levin, D. *et al*. 2002 *Trust and Knowledge Sharing: A Critical Combination*. New York: Somers.
Levitt, B. & March, J. G. 1988 Organizational learning. *Annual Review of Sociology* **14**.

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press

Lorenz, E. H. 1988 Neither friends nor strangers: informal networks of subcontracting in French industry. In Gambetta, D. (ed.), *Trust: Making and Breaking Cooperative Relations*. Oxford: Blackwell, pp. 194–210.
Luhman, N. 1979 *Trust and Power*. New York: John Wiley.
Luke, J. S. 1998 *Catalytic Leadership*. San Francisco, CA: Jossey-Bass.
Luna-Reyes, L. F., Cresswell, A. M. & Richardson, G. P. 2004 Knowledge and the development of interpersonal trust: a dynamic model. In *Proceedings of the 37th Hawaii International Conference on System Science*.
Mayer, R. C. *et al*. 1995 An integrative model of organizational trust. *Academy of Management Review* **20**, 709–734.
Messick, D. M. & Kramer, R. M. 2001 Trust as a form of shallow morality. In Cook (ed.), *Trust in Society*. New York: Russell Sage Foundation.
Michael, D. 1973 *On Learning to Plan – and Planning to Learn*. San Francisco, CA: Jossey-Bass.
Nochur, K. & Allen, T. 1992 Do nominated boundary spanners become effective technological gatekeepers? *IEEE Transactions on Engineering Management* **39**(3).
Parke, A. 1998 Strategic alliance structuring: a game theoretic and transaction cost examination of inter-firm cooperation. *Academy of Management Journal* **36**.
Perrone, V., Zaheer, A. & McEvily, B. 2003 Free to be trusted? Organizational constraints on trust in boundary spanners. *Organizational Science* **14**(4).
Pfeffer, J. 1982 *Organizations and Organization Theory*. Boston, MA: Pitman.
Phillips, Jr., C. E., Ting, T. C. & Demurjian, S. A. 2002 Information sharing and security in dynamic coalitions. In *Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies, Monterey, California*, pp. 87–96.
Powell, W. 1996 Trust-based forms of governance. In Tyler & Kramer (eds.), *Trust in Organizations: Frontiers of Theory and Research*. Thousand Oaks, CA: Sage Publications.
Rabiner-Heinzelman, W., Kulik, J. & Balakrishnan, H. 1999 Adaptive protocols for information dissemination in wireless sensor networks. In *Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking*. pp. 174–185.
Rasmusson, L. & Jansson, S. 1996 Simulated social control for secure internet commerce. In *Proceedings of the New Security Paradigm Workshop '96, Lake Arrowhead, CA, USA*, pp. 18–26.
Rousseau, D. M. *et al*. 1998 Not so different after all: a cross-discipline view of trust. *Academy of Management Review* **23**, 393–404.
Sako, M. 1994 Supplier relationships and innovation. In Dodgson & Rothwell (eds.), *The Handbook of Industrial Innovation*. Aldershot: Edward Elgar Publishing, pp. 268–242.
Smith, J. B. & Barclay, D. W. 1997 The effects of organizational differences and trust on the effectiveness of selling partner relationships. *Journal of Marketing* **61**.
Swan, J. E., Trawick, F., Rink, D. R. & Roberts, J. J. 1988 Measuring dimensions of purchaser trust of industrial salespeople. *Journal of Personal Selling & Sales Management* **8**.
Sydow, J. 1998 Understanding the constitution of interorganizational trust. In Lane, C. & Bachmann, R. (eds.), *Trust Within and Between Organizations: Conceptual Issues and Empirical Applications*. New York: Oxford University Press.
Sztompka, P. 1999 *Trust: A Sociological Theory*, 1st edn. Cambridge: Cambridge University Press.
Vangen, S. & Huxham, C. 1998 The role of trust in the achievement of collaborative advantage. In *The 14th Annual EGOS Colloquim, Maastricht*.
Webb, A. 1991 Co-ordination: A problem in public sector management. *Policy and Politics* **19**(4).
Williams, P. 2002 The competent boundary spanner. *Public Administration* **80**(1).
Yamagishi, T. 2001 Trust as a form of social intelligence. In Cook (ed.), *Trust in Society*. New York: Russell Sage Foundation.
Zaheer, A., McEvily, B. & Perrone, V. 1998 Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance. *Organization Science* **9**(2).
Zucker, L. G. 1986 Production of trust: institutional sources of economic structure. *Research in Organizational Behavior* **8**.

https://doi.org/10.1017/S0269888906000932 Published online by Cambridge University Press