18

TRUST BUILDING FOR ENHANCING COLLABORATION IN VIRTUAL ORGANIZATIONS

István Mezgár
Computer and Automation Research Institute
Hungarian Academy of Science
Budapest, HUNGARY
(E-mail): mezgar@sztaki.hu
and
Department of Production Informatics, Management and Control
Budapest University of Technology and Economics

Virtual organizations play an important role in today's economy, as they are able to adapt themselves to the turbulent market environments. Team work and collaboration are main characteristics of virtual organizations, so the contacts among human beings have outstanding importance. A very important element of this human contact is trust. Trust building in virtual organizations has special characteristics, it is influenced among others by the type of media and communication device, and also by the duration of cooperation. The paper discusses the role of trust and trust building in the operation of virtual organizations from these aspects.

1. INTODUCTION

Based on the results of the information and communications technologies (ICTs), a new "digital" economy is arising. This new economy needs a new set of rules and values, which determine the behavior of its actors. In this dynamic and turbulent environment that requires flexible and fast responses to changing business needs organizations have to respond by adopting decentralized, team-based, and distributed structures variously described in the literature as virtual-, networked-, cluster- and resilient virtual organizations. One main aspect of this approach is that organizations in this environment are networked, i.e. inter-linked on various levels through the use of different networking technologies. Today besides the Internet new solutions are offered, the different types of mobile/wireless networks.

In this new organizational environment new methods and techniques of trust building has to be developed, as the conventional rules cannot be applied. The paper introduces the ways of building trust, the most effective approaches using different media, and also outlines the trends of this field.

2. VIRTUAL ORGANIZATIONS AND COLLABORATION

2.1 Main Characteristics of VO

A virtual organization (VO) refers to a temporary or permanent collection of geographically dispersed individuals, groups, organizational units or entire organizations that depend on electronic linking in order to complete the production process. They are usually working by computer e-mail and groupware while appearing to others to be a single, unified organization with a real physical location. A VO can be considered as a temporary, culturally diverse, geographically dispersed, electronically communicating group of organizations, people. The virtual corporation, virtual-, real time -, enterprise cover mainly the same term as VO.

A networked organization has multiple leaders, lots of informal links and interacting levels. Mutual links and reciprocity across the links are what makes networks work. Because of a lack of formal rules, procedures, clear reporting relationships, and norms, more extensive informal communication is required, so a key feature of virtual organizations is a high degree of this informal communication.

As the base of virtual organizations are the interdependent, separate production teams/units, the cooperation and collaboration has of vital importance. The structure, the communication systems and the collaborating people/teams/organizations that define today's organizations characteristics must be harmonized to accomplish complex, demanding tasks. The collaboration is done through different media according to the actual demands of the tasks. The conventional tools are the telephone, fax, writing letters. On the next level are the computer network-based solutions e.g. e-mail, ftp, telnet. A higher quality of communication media is the WEB-based communication solutions. Through WEB pages a secure, easy and fast communication can be realized.

A new way of connection is the application of different mobile wireless technologies for communication. Mobile wireless technology means mobility, namely individuals are available independently from location and time (24/7/365 availability). This mobility is an important attribute of today's organizations and people.

2.2. Collaboration in Virtual Organization

Collaboration is basic factor of VO operation so it is important to define the differences among the different types of techniques and approaches applied in team work. Himmelman developed a hierarchy of partnerships (Himmelman, 1997). One level of the hierarchy is distinguished from the next level by the amount of trust, time, and personal/group interests needed to establish and maintain the partnership. In Himmelman's framework, networking, coordinating, cooperating, and collaborating mean different things and build on each other. While closely related to networking, collaboration can be understood as a process that exploits a networked environment.

The qualitative difference between collaboration and cooperation is based upon the willingness of organizations/individuals to enhance each other's capacity for mutual benefit and to achieve a common purpose. Collaboration is a relationship in which each organization wants to help its partners become better at what they do.

In order to realize these goals different practical control/organizational concepts, models and techniques are implemented. Swarm Intelligence (SI) is the property of a system whereby the collective behaviours of (unsophisticated) agents interacting locally with their environment cause coherent functional global patterns to emerge. SI provides a basis with which it is possible to explore collective (or distributed) problem solving without centralized control or the provision of a global model.

3. TRUST BUILDING IN VIRTUAL ORGANIZATIONS

3.1 Definition and Forms of Trust

Collaboration is main characteristics of the virtual organizations, so the contacts among the users, the human beings have outstanding importance. A very important element of this human contact is trust. In a networked organization, trust is the atmosphere, the medium in which actors are moving, so it is a basic building block of the communication among people and systems too. Trust is the base of cooperation, the normal behavior of the human being in the society. The ability of enterprises to form networked systems depends on the existing level of trust in the society and on the capital of society (Fukuyama, 1995). As the rate of cooperation is increasing in all fields of life, the importance of trust is evolving even faster.

Trust can be defined as a psychological condition comprising the trustor's intention to accept vulnerability based upon positive expectations of the trustee's intentions or behaviour (Rousseau et al., 1998). Those positive expectations are based upon the trustor's cognitive and affective evaluations of the trustee and the system/world as well as of the disposition of the trustor to trust. Trust is a psychological condition (interpreted in terms of expectation, attitude, willingness, perceived probability). Trust can cause or result from trusting behaviour (e.g., co-operation, taking a risk) but is not behaviour itself.

The following components are included into most definitions of trust (Harrison, McKnight and Chervany, 1996)::

- willingness to be vulnerable / to rely,
- confident, positive expectation / positive attitude towards others,
- risk and interdependence as necessary conditions.

Trust appears in different forms. According to different authors (e.g. Luhman, 1979) trust has forms such as

1. Intrapersonal trust - trust in one's own abilities; self-confidence basic trust (in others).
2. Interpersonal trust - expectation based on cognitive and affective evaluation of the partners; in primary relationships (e.g., family) and non-primary relationships (e.g., business partners).
3. System trust - trust in depersonalised systems/world that function independently (e.g., economic system, regulations, legal system, technology); requires voluntary abandonment of control and knowledge (Luhman 1979).
4. Object trust - trust in non-social objects; trust in its correct functioning (e.g. in an electronic device).

3.2 Approches and Factors of Trust-Building

In building trust there are two approaches; information technology approach and human centered approach, based on culture, and morality. Information technology approach means that security has to increase by different architectures, protocols, certifications, cryptography, authentication procedures and standards and this increased security generates the trust of users. The feeling of security experienced by a user of an interactive system does not depend on technical security measures alone. Other (psychological) factors can play a determining role; the user's feeling of control can be one of these factors. From this aspect user interface has the main role, i.e. the menu structure, the messages send for the user by the system.

3.2.1 Technical side of Trust

Approaching security from the side of trust, security is the set of different services, mechanism and software and hardware tools for generating trust with pure technology. More generally security is a condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. Approaching the term security from from human side a computer is secure if a user can trust it.

At different levels different security solutions have to be applied, and these separate parts have to cover the entire system consistently. The building blocks, elements of security are the security services and the security mechanisms. The following services form together the sense of “trust” for a human being who uses a service, or a given equipment (Menezes, 1996):

- Confidentiality: Protects against disclosure to unauthorised identities.
- Integrity: Protects from unauthorised data alteration.
- Authentication: Provides assurance of someone's identity.
- Access control: Protects against unauthorised use.
- Non-repudiation: Protects against originator of communications later denying it.

The means for achieving these properties depends on the collection of security mechanisms that supply security services, on the correct implementation of these mechanisms, and how these mechanisms are used.

3.2.2 Human side of trust-building process

Trust is a dynamic process and it alters based on experience. Trusting process begins when an individual perceives indications that suggest a person/organization may be worthy of trust. These indications can include behaviors such as manners, professionalism and sensitivity and these forms are designed to represent trustworthiness. These formal claims to trustworthiness become strengthened over time and are eventually transformed into “character traits,” such as dependability, reliability and honesty.

It has to be analyzed why people feel safe and secure, what causes these feelings. The hypothesis of D’Hertefelt (D’Hertefelt, 2000) was that "The feeling of security experienced by a user of an interactive system is determined by the user's feeling of control of the interactive system". The more a user feels in control of an interactive program, the more the user will trust the site, the program.

3.2.3 Important factors of trust building

Today the different types of networked organizations need new types of cooperation as the members of the working teams are geographically (physically) separated, they use shared documents, communicate through e-mail, and high quality audio and video channels. These teams are called as "virtual teams" as they never meat personally, they have no face-to-face (FTF) contact. The work of teams without FTF contact is less effective and reliable based on the observation stated by Handy "trust needs touch" (Handy, 1995). According to case studies, it is evidence that trust of virtual team members is significantly lower than trust in conventional teams (Rocco, Finholt, Hofer, and Herbsleb, 2001). In other experiments where interaction was primarily via email, very similar results have gained as in geographically distributed teams (Jarvenpaa and Leidner, 1999)

In an experiment introduced in (Bos, 2002) four media types were compared: chat (text), phone conference, videoconference and face-to- face. Chat was significantly worse than each of the other three conditions, but audio and video did as well as face-to-face in overall cooperation, and were a definite improvement over text-chat only CMC. However, these two channels still showed evidence of delayed trust, in that they took longer to reach high levels of co-operation.

The process of building trust is slow; trust is formed gradually, it takes quite a lot of time and repeated positive experiences (Cheskin, 1999). On-line trust can be described as a kind of human relationship. The initial stage is that of interest and distrust; there has to be a motivation, a need, to get interested in the service, or co-working. In subsequent phases the trust will evolve or in case of negative experiences the cooperation will terminate.

Trust is depending on the time span of cooperation and the type of connection as well. It can be stated that there are differences in trust building process in short-term and long-term relationships. In case of short-term relationships trust must be achieved quickly, and then maintain with no, or rare face-to-face interaction. The members of these teams must assume that other remote team members are trustworthy, and then later on modify their assumptions according their positive or negative experiences.

In long-term relationships there are four factors that are influencing trust building (Rocco, Finholt, Hofer, and Herbsleb, 2001):

- greater investment in building trustworthy relationships,
- more time to establish trustworthiness through routines and culture,
- more communication channels,
- trust formation may assume a higher priority.

Latest researches show if people meet before using computer-mediated communication (CMC), they trust each other, as trust is being established through touch. In case participants do not meet formerly but they initiate various getting-acquainted activities over a network, trust is much higher than if they do nothing before, nearly as good as a prior meeting. Using chat rooms and forums to get acquainted is nearly as good as meeting, and "even just seeing a picture is better than nothing" (Zheng, et. al, 2002).

4. TECHNOLOGIES AND TOOLS OF TRUST BUILDING

4.1 Generating Trust by Human-Computer Interfaces

As a communication/information system term an interface is the point of communication between two or more processes, persons, or other physical entities. Interfaces are the key points for gaining the trust of the user/customer. They are the first connection point between the user and the system, identification of the users take place at this point (e.g. password input, fingerprint reader, smart card reader), so they have to be designed very carefully.

Different new types of interfaces are in research phase. Interaction has to be extended with more senses (touch, smell, and taste) and parallel make better use of the senses used today (hearing and vision) by exploring peripheral vision and ambient listening. All Senses Communication would be a way to enhance the communication with other entities (humans or machines) using a combination of several present or future senses of humans. Multimodal systems (Oviatt, 2002) process two or more combined user input modes— such as speech, pen, touch, manual gestures, gaze, and head and body movements— in a coordinated manner with multimedia system output. This class of systems represents a new direction for computing, and a paradigm shift away from conventional interfaces to the collaborative multimodal interfaces.

4.2 Generating Trust by Security Servicies

The security mechanisms provide with their correct implementation and usage the proper operation of security services. Security mechanisms are e.g. encryption, digital signatures and checksums/hash algorithms:

- Encryption is used to provide confidentiality, and also can provide authentication and integrity protection.
- Digital signatures are used to provide authentication, integrity protection, and non-repudiation.
- Checksums/hash algorithms are used to provide integrity protection and can provide authentication.

In the followings some solutions will be introduced how these mechanisms are applied in the practice to achieve the proper level of trust.

4.2.1 Confidentiality

The main factor of trust is confidentiality that can be achieved by technologies that convert/hide the data, text into a form that cannot be interpreted by unauthorized persons. Encryption is the major technique in generating confidentiality. Encryption is transforming the message to a ciphertext such that an enemy who monitors the ciphertext can not determine the message sent (Schneier, 1996).

Public key infrastructure (PKI) is the most widely applied technology on public networks such as the Internet. PKI is a framework encompassing the laws, policies, standards, hardware, and software to provide and manage the use of public key cryptography. This is a method of encryption that uses a pair of mathematically related keys: a public key and a corresponding private key. Either key can be used to

encrypt data, but the corresponding key must be used to decrypt it. This method is also called assymmetric encryption.

4.2.2 Integrity

A message integrity check ensures that information has not been altered message in transit by unauthorized persons in a way that is not detectable by authorized users. In combination with a key, a message integrity check (or checksum, or keyed hash) insures that only the holders of the proper key is able to modify a message in transit without detection.

Digital signature is a data that binds a sender's identity to the information being sent. Digital signature may be tied with any message, file, or other digitally encoded information, or transmitted separately. Digital signatures are used in public key environments and provide non-repudiation and integrity services.

4.2.3 Authentication

Authentication is the process of identifying an individual. The typical computer based methods involve user ID/password, biometric templates or digitally signing a set of bytes using a keyed hash. Authentication usually relies on either direct knowledge of the other entity (shared symmetric key or possession of the other person's public key), or third party schemes. Authorization is the process of giving permission for a user to access to network resources after the user has been authenticated through e.g. username and password. The type of information and services the user can access depends on the user's authorization level.

4.2.4 Identification - Smart cards

There is a strong need for a tool that can fulfil the functions connected to trustworthy services. Smart card (SC) technology can offer a solution for current problems of secure communication by fulfilling simultaneously the main demands of identification (e.g. using biometric templates), security (including cryptographic features) and authenticity besides the functions of the actual application. Smart cards are bankcard size plastic plates that contain a chip. This chip can be programmed, can store different data and has all the basic functions of a computer.

5. CONCLUSIONS

Virtual organizations are main elements of the Information and Knowledge Society. These organizations apply ICT very intensive both for internal and external cooperation in order to react flexible to the changing business environment. Collaboration and communication are two basic building blocks of virtual organizations and collaboration relies on trust among working teams and organizations, so the importance of trust is increasing very fast. As it is pointed out by different analysis based on real-life statistics, when users do not trust a system/service they do not use it.

Those methods, technologies and tools that raise the level of trust among the collaborating partners or among the infocom systems and human beings (e.g. multimodal interfaces, all senses communication, encryption) have to be developed

systematically. It is vital to introduce these technologies into the operation of virtual organizations, even by slightly changing their culture or organizational structures.

6. REFERENCES

Bos, N.D., Olson, J.S., Gergle, D., Olson, G.M., & Wright, Z. (2002). Effects of four computer-mediated channels on trust development. In *Proceedings of CHI 2002*. New York: ACM Press.

Cheskin, (1999), eCommerce Trust, A joint research study with Studio Archetype/Sapient and Cheskin, January, http://www.cheskin.com/p/ar.asp?mlid=7&arid=10&art=0

D'Hertefelt, S. (2000). Trust and the perception of security, http://www.interactionarchitect.com/research/report20000103shd.htm

Fukuyama, Francis, (1995). Trust – The social virtues and the creation of prosperity, The Free Press, New York,.

Handy, C. (1995). Trust and the virtual organization, *Harvard Business Review.* 73(3), 40-50.

Harrison, D., McKnight N. and L. Chervany. (1996), "The Meanings of Trust" *University of Minnesota Management Information Systems Research Center (MISRC),* Working Paper. 96-04.

Himmelman, A. T. (1997). *Devolution as an experiment in citizen governancy: Multi-organizational partnerships and democratic revolutions,* Working Paper for the Fourth International Conference on Multi-Organizational Partnerships and Cooperative Strategy Oxford University, 8-10 July 1997, Retrieved October 16, 2004, from Community Building Resource Exchange Web site: http://www.commbuild.org/documents/himmdevo.html.

Jarvenpaa, S. L. and D. E. Leidner. (1999). Communication and Trust in Global Virtual Teams, Organization Science, 10(6), 791-815.

Luhman, N. (1979). *Trust and power*. Chichester: Wiley.

McAllister, D. J. (1995). Affect- and cognition-based trust as foundations for interpersonal cooperation in organizations, *Academy of Management Journal*, *38*, 1, 24-59.

Menezes, A.P. van Oorschot, and S. Vanstone, (1996). *Handbook of Applied Cryptography*, CRC Press.

Oviatt, S., (2002) Multimodal Interfaces, in Handbook of Human-Computer Interaction, (ed. J. Jacko & A. Sears), Chapter 14, Lawrence Erlbaum: New Jersey, 2002.

Rocco, E., Finholt, T.A., Hofer, E.C., & Herbsleb, J.D. (2001, April). Out of sight, short of trust, Presentation at the Founding Conference of the European Academy of Management. Barcelona, Spain.

Rousseau, D. M., Sitkin, S. B., Burt, R., and Camerer, C. (1998), Not so different after all: A cross-disciplinary view of trust. Academy of Management Review, , 23, 1-12.

Schneier, B. (1996). *Applied Cryptography.* John Wiley & Sons, Inc.

Zheng, J., Veinott, E, Bos, N., Olson, J. S., Gary, Olson, G. M. (2002). Trust without touch: jumpstarting long-distance trust with initial social activities, Proceedings of the SIGCHI conference on Human factors in computing systems, Minneapolis, Minnesota, USA, Pages: 141 – 146, ISBN:1-58113-453-3.