Trust Building in Virtual Communities

István Mezgár^{1,2}

¹ Computer and Automation Research Institute,
Hungarian Academy of Science,
Budapest, Hungary
mezgar@szttaki.hu

² Department of Manufacturing Science and Technology,
Budapest University of Technology and Economics

Abstract. By using different types of communication networks various groups of people can come together according to their private or business interest forming a Virtual Community. In these communities cooperation and collaboration plays an important role. As trust is the base of all human interactions this fact is even more valid in case of virtual communities. According to different experiments the level of trust in virtual communities is highly influenced by the way/mode of communication and by the duration of contact. The paper discusses the ways of trust building focusing on communication technologies and security aspects in virtual communities.

Keywords: Communication technology, trust, virtual community.

1 Introduction

Today can be talked about a communication technology explosion as information processing and communication technologies and tools are developing so rapid. The new technologies widen the world for the individuals to reach other human beings independently where they are on the globe. Various groups of people can come together according to their private or business interest forming a Virtual Community (VC). On the other side these technologies deeply modify traditional forms of social connections, communication and cultural habits as well. These modifications can be observed in particular in hierarchies, social rules, norms, conventions, familiarity and reputation.

A very important element of human contacts is trust. In a networked society, trust is the atmosphere, the medium in which actors are moving [1]. Trust can bridge cultural-, geographical-, organizational distances of members and individuals as well. Trust is the base of cooperation, the normal behavior of the human being in the society. In this new communication environment new methods and techniques of trust building has to be developed, as the conventional rules of face-to-face approach cannot be applied. According to different experiments the level of trust is highly influenced by the way/mode of communication [2] and by the duration of contact [3].

The paper deals with trust building among partners of virtual communities, with a special focus on the role of communication technologies. An overview is presented

how security, user identification/authentication technologies (e.g. biometrics) can influence the trust building process. Finally some practical patterns are given that raise the efficiency of trust building.

2 Main Characteristics of Virtual Communities

Originally personal computers were totally disconnected from each other. The first big step was when all those computers (and the people behind them) got connected to the Internet and after reaching a critical mass digital networks were changing social groups into the Virtual Community.

According to Howard Rheingold, a virtual community is a community of people sharing common interests, ideas, and feelings over the Internet or other collaborative networks. In his book, *The Virtual Community* [4] he defines virtual communities as „social aggregations that emerge from the Internet when enough people carry on public discussions long enough and with sufficient human feeling to form webs of personal relationships in cyberspace”. Cyberspace is the total interconnectedness of human beings through computers and telecommunication without regard to their geographical place. Today the convergence of mobile communication and computing is going on and this change in technology brings a change in the way communities come together and express themselves.

The classical definition of Rheingold describes the “clear” type of virtual community. Today there are additional forms of communities that are called also as virtual communities, in spite of the pretty big differences in their goals and technologies. Based on the types of the members (private individuals, professional individuals, organizations), on the goals of the community (private, social, business), the form of cooperation (free, formal), and on the type of participation (voluntary, voluntary organized, formally organized) three different basic types of Virtual Communities can be distinguished:

1. Community/network of independent intellectual workers (IIW)
2. Virtual Organizations (VO) – formalized cooperation of different remote business units.
3. (Voluntary) Virtual Communities – random connection among individuals or group of people.
 - a). Working voluntary for a common goal of a community
 - b). Collaborate in a certain field of hobby, discuss a topic without special responsibility.

A virtual community requires social capital to succeed in its goals. Social capital is the “ability to collaborate effectively,” [5] and it includes three important factors: structure, trust, and common goals.

- Structure refers to human relations within the virtual community. Usually there is no real social hierarchy among the members of the virtual community. The rules are explained by the social norms for the community.
- Trust is a social construct. In order to increase social capital, there must be trust between members of the community. This may require individual members to refrain from taking actions that may benefit them in the short-term, for the sake of the

long-term benefit for the entire community. Establishing trust on the Internet is a difficult task, because of the anonymity and possible deception of members regarding their identities and information. Because of this difficulty in establishing trust, many individuals approach virtual communities with caution and suspicion.

- Common goals are the third factor of social capital. The basic goal is to create an online community of people.

To be a successful virtual community, there must be high social capital, meaning there must be low structure, high trust, and common goals. All the three classes and their subclasses of Virtual Communities can be organized independently of nationality and distance.

3 Media for Virtual Communities

3.1 Basic Wired Communication Technologies

Before the Web, virtual communities existed on bulletin board services (BBS). Today the main tool/technology for VCs is the Web. Among the first websites for virtual community were the Geocities (1994), and the Tripod (1995).

In general, there are two kinds of communication among virtual community members: message postings and real-time chat. Usenet newsgroups are an example of the former. For real-time chat, Internet Relay Chat (IRC) is a system used by many Web sites realizing virtual communities. Virtual communities are integrating Web 2.0 technologies with the community, so they can be described as Community 2.0.

Another mode of forming little virtual communities is the „weblog“. The weblog is the frequent, chronological publication of personal thoughts and Web links. It is a mixture of what is happening in a person's life and what is happening on the Web, a kind of hybrid diary/guide site that can be read by other people free.

3.2 Mobile Technology in Virtual Communities

The mobility and the openness of virtual communities are continuously evolving. In the early 90s, the emerging digital networks were changing social groups in the Virtual Community; today we can live through what happens when the society, the economy and the networked communication goes mobile. The application of mobile equipment of different kinds is dramatically increasing. The combination of wired and wireless networks result that the members of the society have very broad possibilities to form VC, to build connection among the different cultures.

Rheingold, in his book „Smart Mobs: The Next Social Revolution“ [6] described how efficient mobile communications (cellular phones, personal digital assistants, and wireless-paging and Internet-access devices) will allow people to connect with anyone, anywhere, anytime, and how they're already shaping communities around the world. Rheingold calls such group actors "smart mobs," and this expression has become already an important phenomenon.

Mobility is basic for the modern society - wireless technologies make faster the VC formation and operation in private life, in work, in entertainment and in civic organizations. The real impact of mobile communications will come not from the technology

itself but as in case with other technological revolutions, from how people use it, resist it, adapt to it, and ultimately use it to transform themselves, their communities, and their social and cultural environment.

Mobility can be achieved by using different types of wireless networks as Satellite Communication, Wireless Wide Area Networks (WWAN – different types of mobile phone systems - GSM, UMTS and iMode), Wireless Local Area Networks (WLAN, such as WiFi –IEEE standard 802.11a/b/g/n), Wireless Metropolitan Area Network (WMAN) and Wireless Personal Area (or Pico) Network (WPAN – e.g. Bluetooth, IrDA2). These networks can be connected/integrated, according to the actual needs, developing very complex and powerful networks for VCs So the user can be reached really at any place through a type of wireless connection.

The most efficient wireless equipment for personal use are the mobile phones, Personal Digital Assistants (PDA) and the netbooks. When these “wireless terminals” are able to support, identification, authentication and authorization of users, confidentiality and seamless communication using various kinds of contents - including text, voice and video streams, etc. – they can be called as Personal Trusted Device (PTD). Using PTD for trust building can make authentication and confidentiality easier, more reliable that support the operation of virtual communities in a great extent.

An important service type of mobile phones is the MMS (Multimedia Messaging Service) that is an evolution of SMS (Short Message Service) and EMS (Enhanced Messaging Service). The multimedia element differentiates MMS from other messaging offers by integrating the ability to send and receive photos, images, video clips and polyphonic sound by camera phones. This message type is significant in forming virtual communities and also in trust building. The use of Internet-ready phones (VoIP) is challenging social customs, human relationships as people shift more of their attention and resources to the cell-phone. One recent trend is "moblogging," or mobile weblogging. Weblogging means reading/writing blogs in real time: this is what happens when you fuse digital cameras and text-entry functionality with a way to publish it to the Web.

4 Definition and Forms of Trust

In electronic environments, in digital communication B.J. Fogg and Hsiang Tseng [7] focus on trust among individuals mediated by technology, writing that trust indicates a positive belief about the perceived reliability of, dependability of, and confidence in a person, object (such as computers, networks, and software), or process (such as credit card transactions and airline e-ticket reservations). There are many additional definitions of trust, all professional fields where trust is important have developed its own definition [8]. Trust appears in different forms, according [9] trust has four main forms; Intrapersonal trust, Interpersonal trust, System trust and Object trust.

5 Trust Building in Virtual Communities

5.1 Fields/Technologies of Trust-Building

In building trust two main approaches can be distinguished; information technology approach and human centered approach, based on culture, and morality. A structured

overview of trust elements and their hierarchy can be found in [10] differentiating the basic classes of structural-, managerial/behavioral-, social-, financial/economical- and technological trust. 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.

It would be a mistake to think that applying only the human-centered approach would generate trust, the technological part has to be added as well (e.g. biometrical identification), so mainly the structured integration of the two approaches can result the expected level of trust.

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.

The building blocks, elements of security are the security services and the security mechanisms. The security services are, access control, authentication, confidentiality, integrity, and non-repudiation. Security mechanisms are e.g. encryption, digital signatures and checksums/hash algorithms. 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. Identification is the process when a network element recognizes a valid user's identity. Authentication is the process of verifying the claimed identity of a user. Information used to verify the claimed identity of a user can be based on a password, PIN, smart card, biometrics, etc. Authentication information should be kept confidential.

Human side of trust-building process

The human side of trust is more complicated. From this aspect user interface has the main role, i.e. the menu structure, the messages send for the user by the system. In case the user feels that is easy to use, it is transparent, he/she can control the system (even with low level computer knowledge) i.e. the system is „user friendly”, through this he can be convinced that he is using a trustworthy system. The more a user feels in control of an interactive system, the more the user will trust the site, the program, the system [11].

Trust is a dynamic process and it alters based on experience. Trusting process begins when an individual perceives indications that suggest a person may be worthy of trust [12]. These indications can include behaviors such as manners, professionalism and sensitivity and these forms are designed to represent trustworthiness.

5.2 Important Factors of Trust Building

In an experiment introduced in [2] 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.

The process of building trust is slow; trust is formed gradually, it takes quite a lot of time and repeated positive experiences [13]. On-line trust can be described as a kind of human relationship.

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.

In long-term relationships trust building is influenced e.g. by using more communication channels and trust formation may assume a higher priority [3].

Other researches show if people meet before using computer-mediated communication (CMC), they trust each other easier. Using chat rooms and forums to get acquainted is nearly as good as meeting, and “even just seeing a picture is better than nothing” [14].

5.3 Generating Trust by Human-Computer Interfaces

As a communication/information system term a user interface (UI) 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 and authentication (e.g. password/biometric input) of users take place at this point, so they have to be designed very carefully. When applying a reliable UI (menu structure that gives the feeling of control; secure authentication technique (biometry)) these technologies generate trust in user both to the system and partially to the other users (the partners also have to get through the same strict authentication, so they are really the person whom they states). The “reminder part” of trust in the partners can be built based on the content of communication.

Researchers test different new types of interfaces. Multimodal systems [15] process two or more combined user input modes— such as speech, 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.

Remembering and entering passwords is a general problem, which is why everything should have seamless biometric identification built in. Researchers are working on different approaches that can make easy and convenient the reliable application of PTDs. Some examples; individuals can be identified from the faint sounds made deep inside the human ear. This could mean, users would be able to confirm their identity for computer logins simply by lifting a phone to their ear or putting on a set of headphones [16].

In case of an other approach the phone looks for a specific pattern of movements as the person brings it up to her/his ear when it has a built-in gesture based system using an accelerometer. These movements depend on characteristics like arm length, muscle structure, and patterns such as holding methods and other habits. These acceleration data makes possible the authentication. [17].

5.4 Practical Behavioral Patterns for Trust Building in VC

Members of VCs may trust other people or the system as long as they fulfill their expectations. When they do not, trust can evaporate quickly and take a much longer

time to rebuild. To avoid losing trust in the following some basic rules can be given for building connections in virtual space:

- Frequent and short communications help the dialogue process and trust building.
- Make your expectations clear -that helps the other party the ability to give a definitive response.
- Make small commitments and meet them.
- Make clear what is driving you to behave in certain ways.
- Be polite and thank every little service of the partner.
- Socialize - Informal conversation and identification of shared interests beyond the actual tasks, helps build closer, personal connections.
- Demonstrate interest and commitment to the other person.
- Members of community organize meetings (if it is possible) to get in personal contact.

6 Conclusions

Today virtual communities are formed more frequently as the communication technology makes possible to join for more and more people. Internet and WEB technologies are developing very quick and new technologies as different types of wireless communication make even faster the evolution of cyberspace.

The number of users has reached the critical mass and that means these technologies have impact on the society, their influence change the behavior and culture of society. As trust is a social construct it is the base of virtual communities as well, especially in case of mobile technologies. Trust is the key problem as it has been proven in many studies that people don't use services in which they don't trust.

Those concepts, methods, technologies and tools that raise the level of trust among the collaborating partners or among the infocom systems and human beings (e.g. multi-modal interfaces, new authentication technologies) 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 organization structures.

References

1. Castelfranchi, C., Tan, Y.-H. (eds.): Trust and Deception in Virtual Societies. Kluwer Academic Publishers, Dordrecht (2001)
2. Bos, N.D., Olson, J.S., Gergle, D., Olson, G.M., Wright, Z.: Effects of four computer-mediated channels on trust development. In: Proceedings of CHI 2002. ACM Press, New York (2002)
3. Rocco, E., Finholt, T.A., Hofer, E.C., Herbsleb, J.D.: Out of sight, short of trust. Presentation at the Founding Conference of the European Academy of Management. Barcelona, Spain (April 2001)
4. Rheingold, H.: The Virtual Community, p. 325. Addison-Wesley, Reading (1993)
5. Blanchard, A.: Virtual communities and social capital. In: David Garson, G. (ed.) Social Dimensions of Information Technology: Issues for the New Millennium, pp. 6–21. Idea Group, Hershey (2000)

6. Rheingold, H.: *Smart Mobs: The Next Social Revolution*, p. 288. Perseus, Cambridge (2002)
7. Fogg, B., Tseng, H.: The elements of computer credibility. In: *Proceedings of CHI 1999*, Pittsburgh, May 15-20, pp. 80–87. ACM Press, New York (1999)
8. Harrison, D., McKnight, N., Chervany, L.: *The Meanings of Trust*” University of Minnesota Management Information Systems Research Center (MISRC), Working Paper. 96-04 (1996)
9. Luhman, N.: *Trust and power*. Wiley, Chichester (1979)
10. Msanjila, S.S., Afsarmanesh, H.: On Architectural Design of TrustMan Applying HICI Analysis The case of technological perspective. *Journal of Software* 3(4), 17–30 (2008)
11. Herrmann, T., Wulf, V., Hartmann, A.: Requirements for a Human-centered Design of Groupware. In: Shapiro, D., Tauber, M., Traunmüller, R. (eds.) *Design of Computer Supported Cooperative Work and Groupware Systems*, pp. 77–100. Elsevier, Amsterdam (1996)
12. Grabner-Krauter, S., Kaluscha, E.A.: Empirical research in on-line trust; a review and critical assessment. *Int. J. Human-Computer Studies* 58, 783–812 (2003)
13. Cheskin: *eCommerce Trust*, A joint research study with Studio Archetype/Sapient and Cheskin (January 1999),
<http://www.cheskin.com/p/ar.asp?mlid=7&arid=10&art=0>
14. Zheng, J., Veinott, E., Bos, N., Olson, J.S., Gary, O.G.M.: Trust without touch: jumpstarting long-distance trust with initial social activities. In: *Proceedings of the SIGCHI conference on Human factors in computing systems*, Minneapolis, Minnesota, USA, pp. 141–146 (2002) ISBN:1-58113-453-3
15. Oviatt, S.: *Multimodal Interfaces*. In: Jacko, J., Sears, A. (eds.) *Handbook of Human-Computer Interaction*, ch. 14. Lawrence Erlbaum, New Jersey (2002)
16. Marks, P.: Our ears may have built-in passwords. *New Scientist Magazine* 2703, 16–17 (2009)
17. KDDI Gesture-based verification structure (2009),
<http://www.interweb.in/review-gadgets/37545-kddi-gesture-based-verification-structure.html>
(retrieved May 12, 2009)