Trust and Security in Collaborative Environments

Peter Mihók, Jozef Bucko, Radoslav Delina, Dana Paľová

Faculty of Economics, Technical University Košice,
Němcovej 32, 040 01 Košice, Slovakia
{peter.mihok, jozef.bucko, radoslav.delina, dana.palova}@tuke.sk

Abstract. It is often stated in literature that trust is of critical importance in creating and maintaining information sharing systems. The rapid development of collaborative environments over the Internet has highlighted new open questions and problems related to trust in web-based platforms. The purpose of this article is to summarize how trust can be considered in collaborative environments. Partial results of the field studies of two European IST projects, FLUID-WIN and SEAMLESS, are presented. Identity management problems and trusted operational scenarios are treated.

Key words: trust, security, information sharing, collaboration, web-based platform, identity management, trusted scenario

1 Introduction

Trust is considered as a basic success factor for collaboration. Modern ICT based collaboration environments allow companies to realize a number of competitive advantages by using their existing computer and network infrastructure for the collaboration of persons and groups. The collaborating actors (manufacturers, suppliers, customers, service providers) must feel confident that their transaction processes are available, secure and legal. Trust building mechanisms vary according to their complexity and acceptability, especially among companies with low IT skills. Appropriate selection and user-friendly implementation can enhance trust and efficient use of web-based business platforms. In this contribution we examine trust and trust building mechanisms in different contexts.

Organizations and projects are looking for ways to optimize their supply chains in order to create a competitive advantage. Consequently, the same organizations are modifying their business processes to accommodate the demands that information sharing requires. Information sharing can reduce the cost of failure and operational cost. Furthermore, it can improve the scheduling quality and the efficiency of current resources. It also provides intangible benefits such as improved quality with increased customer and shareholder satisfaction. However, integrating and sharing information in inter-organizational settings involves a set of complex interactions. The organizations and institutions involved must establish and maintain collaborative relationships in which information and data of sensitive and critical nature are transferred outside of the direct control of the organization. The sharing processes can involve significant organizational adaptation and maintenance. Trust and security mechanisms are often stated in literature as being of critical importance in the creation and maintenance of an information sharing system. In the past decades there is a rapid increase of information sharing systems based on different electronic services (e-services) offered through web-based platforms. Trust and security aspects in the development of such platforms are in the center of the research activities of European FP6 and FP7 projects, e.g. networks of Living Labs and Digital Ecosystems, projects SECURE, SERENITY, SWAMI, HYDRA, etc. In this paper we will restrict our attention to two types of collaborative environments: electronic marketplaces and manufacturing networks. Our research is based on our results and experiences in the FP6 IST projects SEAMLESS and FLUID-WIN.

The SEAMLESS project studies, develops and tests an embryo of the Single European Electronic Market (SEEM) network, where a number of e-registries are started in different countries and sectors. The SEEM vision is towards a web-based marketplace where companies can dynamically collaborate without cultural, fiscal and technological constraints.

The FLUID-WIN project targets business-to-business (B2B) manufacturing networks and their interactions with the logistics and financial service providers. This cross-discipline service integration concept is called business-to-(B2B), or shorter B2(B2B) [19]. Within that context the project aims to develop an innovative platform, which can integrate data and transfer them among all the various partners, in order to improve the competitiveness and to make the business processes of the integrated network as efficient as possible.

After introducing the basic concepts related to trust and security we deal with the problem of the secure access to the platforms and additional trust mechanisms considered within the projects.

2 Basic Concepts

In the context of collaboration it is of importance to differentiate between trust and security. The basic concepts and terms are defined as a base for the further discussion.

Trust is a seemingly very abstract factor and as a complex notion, synonymous to confidence, it has a lot of meanings depending on the context where it is considered. By WordNet [28] the word trust relates to:

- Reliance, certainty based on past experience
- Allow without fear
- Believe to be confident about something
- Trait of believing in the honesty and reliability of others
- Confidence, a trustful relationship

Another definition describes trust as confident reliance. “We may have confidence in events, people, or circumstances, or at least in our beliefs and predictions about them, but if we do not in some way rely on them, our confidence alone does not amount to trust. Reliance is a source of risk, and risk differentiates trusting in something from merely being confident about it. When one is in full control of an outcome or otherwise immune from disappointment, trust is not necessary" [27].

Trust is usually specified in terms of a relationship between a trustor and trustee. The trustee is the subject that trusts a target entity i.e. the entity that is trusted. Trust forms the basis for allowing a trustee to use or manipulate resources owned by a trustor or may influence a trustor's decision to use a service provided by a trustee. Based on the survey of Grandison and Sloman [13], trust, in the e-services context, is defined as: "*the quantified belief by a trustor with respect to the competence, honesty, security and dependability of a trustee within a specified context*". Also distrust is defined as: "*the quantified belief by a trustor that a trustee is incompetent, dishonest, not secure or not dependable within a specified context*".

The level of trust has an approximate inverse relationship to the degree of risk with respect to a service or a transaction. In many current business relationships, trust is based on a combination of judgment or opinion based on face-to-face meetings or recommendations of colleagues, friends and business partners. However, there is a need for a more formalized approach to trust establishment, evaluation and analysis to support e-services, which generally do not involve human interaction.

Comprehensive surveys on the meaning of trust can be found e.g. in [17] and [13] as well as in the book on Trust in E-Services [24].

Whereas, *security* is "a wish" of being free from danger, the goal is "bad things don't happen". Computer security is the effort to create a secure computing platform, designed in a way that users or programs can only perform actions that have been allowed. This involves specifying and implementing a security policy. The actions in question are often reduced to operations of access, modification and deletion.

Schneier [21] defines security "like a chain; the weakest link will break it. You are not going to attack a system by running right into the strongest part. You can attack it by going around that strength, by going after the weak part, i.e., the people, the failure modes, the automation, the engineering, the software, the networks, etc.".

In the context of information-sharing computer systems, everything reduces to access to appropriate information. Provision (or disclosure) of information is the key element. A simple transfer of data is between two parties, a sender and a receiver, and includes the following key steps: preparation of data; transfer a copy of the prepared data; use the copy of data received. More complex transactions can be composed from such simple data transfers.

Dependability is an ability to avoid failures that are more frequent or more severe than it is acceptable (to avoid wrong results, results that are too late, no results at all, results that cause catastrophes). Attributes of dependability are:

- Availability – readiness for correct service
- Reliability – continuity of correct services
- Safety – absence of catastrophes
- Integrity – absence of improper results
- Maintainability – ability to undergo modifications and repairs

Security can be defined [14] as the combined characteristics of: confidentiality (i.e., absence of unauthorized disclosure of information), availability to conduct authorized actions, and also integrity (i.e. the absence of unauthorized system alterations). Security and dependability overlap, and are both required as base for trust. Unfortunately and most confusingly, the terms dependability and security are sometimes used interchangeably or, else, either term is used to imply their combination. In fact, because security and dependability are distinct but related and partially overlapping concepts, the term trustworthiness is being increasingly used to denote their combination. The main technical mechanisms that have strong influence on the trust in networked based systems include:

- Identity management
- Access control
- Data encryption and security

The *identity management* systems provide tools for managing partial identities in the digital word. Partial identities are subsets of attributes representing a user or company, depending on the situation and the context. Identity management systems must support and integrate both techniques for anonymity and authenticity in order to control the liability of users.

The *access control* is the enforcement of specified rules that require the positive identification of the users, the system and the data that can be accessed. It is the process of limiting access to resources or services provided by the platform to authorized users, programs, processes or other systems according to their identity authentication and associated privilege authorization.

Finally, *data encryption and security* are related to cryptographic algorithms, which are commonly used to ensure that no unauthorized user can read and understand the original information.

The concept of *asymmetric cryptography*, (also called Public Key Cryptography), was described for the first time by Diffie and Hellman [6]. In contrast to the symmetric cryptography in which we have the same secret key for encryption and decryption, we now have one *public key* eP (encryption key) and one *private key* dP (decryption key) for each person P. While the public key eP can be published to the whole world, the private key dP is to be treated as a secret and only person P knows it. An important characteristic of such a cryptography system is that it is computationally infeasible to determine the private key given the corresponding public key. The advantage of asymmetric cryptography is the enormously reduced effort for key management. A disadvantage is the velocity. The asymmetric cryptography can serve as base for the *digital signature*.

The *Public Key Infrastructure* (PKI) provides the identification of a public key with a concrete person via the certificate. The PKI is the system of technical and administrative arrangements associated with issuing, administration, using and retracting of public key certificates. The PKI supports reliable authentication of users across networks and can be extended to distributed systems that are contained within a single administrative domain or within a few closely collaborating domains.

3 Trust and Security on Web-based Platforms

In an open and unknown market place with a high number of unknown participants, assurance and trust are difficult but very important. There is a growing body of research literature dealing with online trust, in which e-commerce is one prominent application. Several studies contend that e-commerce cannot fulfil its potential without trust (e.g. [8], [11], [15], [20]). Lee and Turban [16] highlight lack of trust as the most commonly cited reason in market surveys why consumers do not shop online.

On an open consultation on “Trust barriers for B2B e-marketplaces” [7] conducted by the Enterprise DG Expert Group in 2002, several important barriers were identified. From the report we can find that the most important trust barriers are issues regarding the technology (security and protection), trust marks and dispute resolution absence, online payment support, lack of relevant information about partners, products, contract and standardization issues.

A trust building process must be set up to resolve these issues. Trust usually is conceptualised as a cumulative process that builds on several, successful interactions [18]. Each type of process increases the perceived trustworthiness of the trustee, raising the trustor’s level of trust in the trustee [3]. It is not known exactly which trust-building processes are relevant in an e-commerce context. It is suggested that, in this setting, trust building is based on the processes of prediction, attribution, bonding, reputation and identification [3]. Reputation has a very high relevance in a trust-building process on e-commerce markets [1]. According to the Chopra and Wallace classification, identification based trust refers to one party identifying with the other, for example in terms of shared ethical values. Identification builds trust when the parties share common goals, values or identities. In e-commerce, these attributes perhaps may relate to corporate image [2] or codes of conduct.

These results are more focused on trust impact than on factors, which build trust. According to several research activities, the research on significance and acceptance of trust building mechanisms is still missing and is necessary for future development in this field. This absence has been examined in the Seamless project [22]. The results are presented in Deliverable D1.2 “Trusted Operational Scenarios” of the project, see also [5].

Though operating within a closed supply chain system, locally spread information technology destinations (users of manufacturer, supplier and financial service institutions) need to be linked, which brings up the need for trust, privacy and security. It is to be expected that security is at least of equal importance than in an open system, as limitation of access plays a vital role. There are several trust and security best practices scattered throughout the Internet and material is constantly updated daily, if not hourly, based on the latest threats and vulnerabilities. Security standards are not “one size fits all.” Responsible, commercially reasonable standards vary, depending on factors such as company size and complexity, industry sector, sensitivity of data collected, number of customers served, and use of outside vendors. Security standards exist for several types of transactions conducted, and new ones are on the way all the time. A further checklist to meet trust and security requirements is to meet local legislation in terms of data protection and privacy regulation. Financial transactions need to meet local and also foreign standards if they are to be accepted by a provider.

With respect to the FLUID-WIN project and its platform mainly two security and trust building mechanisms can be differentiated:

1. Mechanisms based on workflow design, policies and contractual issues.
2. Technical solutions ensuring a save login and data exchange.

Both mechanisms are strongly related and build upon each other.

Based upon the results of a mail-based survey the following ten key success factors for an established information sharing system were determined [10]:

1. Centralized Information Sharing Control
2. Maintain and Update Information Sharing Rules
3. Significant Exchange of Information
4. Defined Use of Information
5. Collaboration with Suppliers
6. Cooperative Competition
7. End-to-End Connectivity
8. Formed Supply Alliances
9. Replace Traditional Communication with IT
10. Share Frequently with Suppliers

Trust, which did not occur as a factor among them, is replaced by contractual agreements defining the limitations of the transferred information usage. However, the challenge within the FLUID-WIN idea is the high number of actors from different domains as well as their technical connection within the B2(B2B) concept. For secure access to the FLUID-WIN Platform it could be convenient to use digital signatures (private keys), which are saved at a secure device (chip card, USB key) and protected by other safety elements (PIN and static password). It is necessary to take the existence of a digital signature couple as granted, the first one for access and cryptography and the second one for designation. The strength of this securing form is the fact that the method of digital signature cannot be breached by "brute" force at the present time. The weakness of this security method is insufficient knowledge of this method and infringement of all safety rules that are related to the physical security of digital signature storage site and safety elements, which allow its operation. Therefore, it is necessary to work out the security policy, in which the method of usage, security principles and risks of improper use of this method will be exactly specified.

The digital world uses the same principles of electronic signature data identification (in case of a digital signature it is the public key):

- Uniqueness of the line – based on the agreement about a public key between the key owner and the verifier of the signature. This way of connection is unequivocal under opinion of both parties. Duly conducted agreement protects both parties and is one of the arguments in the case of cause. This application of digital signature is possible in the so-called closed systems. This method is used in the electronic banking services at present.
- Triangle of trust – in open systems, the owner of the key has not often the possibility to meet with the verifier of the signature to make an agreement concerning the relevant public key. In this case it is suitable to use the third party principle.
- Certification – a dedicated authority assures the unequivocal identification of the public key with a concrete person (its owner), on the basis of a certified application of the owner. In this application the basic identification data and relevant public key are listed.

Therefore, the necessary condition of active employment of electronic signature technology, which allows the transition to electronic document interchange in open systems, is the existence of certification authorities. To the basic services defined by the e-signature mechanisms belong:

- Registration services – contact with certificate applicant, verification of data conformity (data in the application form for issue of certificate and data concerning the identity of an applicant).
- Issuing of certificates – on the basis of an agreement with an applicant and verification of all necessary data the certificate for public key is issued.
- Revoke of certificates and publication of the cancelled certificates list – in case that an unauthorized person obtains the private key, it is required to cancel the certificate before its validity date. The certification authority is obliged to keep and publish lists of valid and cancelled certificates.

However, financial service providers have their own security policies. Especially larger financial institutions are hard to be convinced to adapt their policy as precondition to use the FLUID-WIN Platform. Rather, it is likely that the FLUID-WIN Platform has to accept the policies of the certain Financial service providers, even if is this means that FLUID-WIN has to implement a set of different security mechanisms depending on the requests of each financial service provider.

Conclusion

E-services like web-banking, web-shopping, web-auctions, e-government, e-health, e-manufacturing, e-learning are becoming part of everyday life for citizens everywhere. As a basis for deciding to use the service trust is becoming a major impediment. To fill the gap between identities and their level of trust is one of the eight major issues in developing identity management for the next generation of distributed applications and use of e-services [24]. A lot of interesting questions and problems are considered in the recent publications [4],[5],[10],[12] and can be found as public deliverables of the projects [9],[22],[23],[25] and [26].

Acknowledgements

This work has been partly funded by the European Commission through IST Project SEAMLESS: Small Enterprises Accessing the Electronic Market of the Enlarged Europe by a Smart Service Infrastructure (No. IST-FP6-026476) and IST Project FLUID-WIN: Finance, logistics and production integration domain by web-based interaction network (No. IST-FP6-27083). The authors wish to acknowledge the Commission for their support. We also wish to acknowledge our gratitude and appreciation to all the Seamless and Fluid-Win project partners for their contribution during the development of research presented in this paper.

References

1. Atif, Y.: Building Trust in E-Commerce, IEEE Internet Computing, Jan-Feb (2002), 18-24
2. Ba, S., Pavlou, P.A.: Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behaviour. MIS Quarterly Vol. 26 No. 3. (2002) 243-268
3. Chopra, K., Wallace, W.: Trust in Electronic Environments, Proceedings of the 36th Hawaii International Conference on Systems Sciences (HICSS), (2003)
4. Delina, R., Azzopardi, J., Bucko, J., Frank, T., Mihok, P.: Financial Services in Web-based Platforms. In: Managing Worldwide Operations and Communications with Information Technology, Proc. IRMA Conference Vancouver (Canada), ed. Koshrow M. (2007) 1273-1274
5. Delina, R., Mihok, P.: Trust building processes on web-based information-sharing platforms. In: Proceedings of the 13th International Conference on Concurrent Enterprising, ICE'2007, eds. K.S. Pawar, K-D. Thoeben and M. Pallot, Sophia Antipolis, France (2007) 179-186
6. Diffie,W., Hellman,M.: New directions in cryptography, IEEE Transactions on Information Theory. (1976). Available at: http://crypto.csail.mit.edu/classes/6.857/papers/diffie-hellman.pdf (visited 11.10.2007)
7. EU Commission: Open consultation on "Trust barriers for B2B emarketplaces" Presentation of the main results. (2002) Available at: http://europa.eu.int/comm/enterprise/ict/policy/b2bconsultation/consultation_en.htm (visited 25.05.2007)
8. Farhoomand, A., Lovelock, P.: Global e-Commerce – Texts and Cases, Prentice Hall (2001)
9. FLUID-WIN Finance, logistics and production integration domain by web-based interaction network. FP6 IST STREP 27083 funded by European Commission. Available at: www.fluid-win.de
10. Frank, T. G., Mihók, P.: Trust within the Established Inter-Organizational Information Sharing System. In: Managing Worldwide Operations and Communications with Information Technology, Proc. IRMA Conference Vancouver (Canada), ed. Koshrow M. (2007) 132–135
11. Friedman, B., Kahn, P., Howe, D., Trust Online, Communications of the ACM, Vol. 43, No. 12 (2000) 34-40
12. Giuliano, A., Azzopardi, J., Mihók, P., Bucko, J., Ramke, Ch.: Integration of financial services into multidisciplinary Web platforms. To appear in: Ambient Intelligence Technologies for the Product Lifecycle: Results and Perspectives from European Research, IRB Stuttgart (2007)
13. Grandison, T., Sloman, M.: A survey of trust in Internet applications, IEEE Communications Surveyes and Tutorials, 4(4) (2000) 2-16
14. IEEE Standard computer dictionary: A compilation of IEEE standard computer glossaries. Institute of Electrical and Electronics Engineers, New York (2007)
15. Jones, S., Wilikens, M., Morris, P., Masera, M.: Trust requirements in e-business: A conceptual framework for understanding the needs and concerns of different stakeholders. Communications of the ACM, Vol. 43, No. 12 (2000) 81-87
16. Lee, M., Turban, E.: A Trust Model for Consumer Internet Shopping, International Journal of Electronic Commerce, Vol. 6, No. 1 (2001)
17. McKnight, D.H. and Chervany, N.L.: The Meanings of Trust. MISRC 96-04, University of Minnesota, Management Informations Systems Research Center, University of Minnesota, (1996)
18. Nicholson, C., Compeau, L., Sethi, R.: The Role of Interpersonal Liking in Building Trust in Long-Term Channel Relationships, Journal of the Academy of Marketing Sciences, Vol. 29, No. 1 (2001) 3-15

19. Rabe, M.; Mussini, B.: ASP-based integration of manufacturing, logistic and financial processes. In: XII. Internationales Produktionstechnisches Kolloquium, Berlin, 11.-12. October 2007, pp. 473-487.
20. Raisch, W.: The E-Marketplace – Strategies for Success in B2B Ecommerce, McGraw-Hill (2001)
21. Schneier, B.: Security in the real world. How to evaluate security technology. In: Computer Security 15/4 (1999) 1-14
22. SEAMLESS: Small enterprises accessing the electronic market of the enlarged Europe by a smart service infrastructure. FP6 IST STREP 26476 funded by European Commission. Available at: www.seamless-eu.org
23. SECURE: Secure environments for collaboration among ubiquitious roaming entities. Available at: http://www.dsg.cs.tcd.ie/dynamic/?category_id=-30 (visited 01.11.2007)
24. Song, R., Korba, L., Yee, G.: Trust in E-Servuces, Technologies, Practices and Challenges, Idea Group Publ. (2007)
25. SWAMI: Safeguards in a world of ambient intelligence, final report. (2006) Available at: http://swami.jrc.es (visited 01.06.2007)
26. TRUSTe: Security guidelines 2.0. (2005) Available at: http://www.truste.org/pdf/Security Guidelines.pdf (visited 23.05.2007)
27. UNMC: Glossary. (2007) Available at: www.unmc.edu/ethics/words.html (last visit: 31.05.2007)
28. WordNet: Word net search; Trust. (2007) Available at: http://wordnet.princeton.edu/perl/webwn?s=trust&sub=Search+WordNet&o2=&o0=1&o7=&o5=&o1=1&o6=&o4=&o3=&h (visited 21.05.2007)