Biometric authentication and authorization infrastructures in trusted intra-organizational relationships

Matthias Olden[1], *Stefano Za*[2]

Abstract Today, the lives of both people and organizations are strongly focused on the creation, development and maintenance of relationships. These are influenced by several factors, amongst which trust plays an important role. Same as in traditional relationships, trust is considered crucial in their digital equivalent; here we can speak of the concept of trust in technology. An example for trust in technology is given by biometric authentication and authorization infrastructures. A possible approach is the use of typing behavior biometrics as authentication method. This provides a higher security, considering several biometric specific problems like replay attacks or template aging. The intra-organizational environment allows an interesting solution to these problems, namely the synchronization of biometric data within a federation of applications running in the same company. This paper presents the influence of the proposed authentication model on trust by means of the technical-formal-informal model inside an organization.

Introduction

Relationships among individuals or organizations have always been playing a relevant role in their private, social or business lives. This role has become fundamental, as people and organizations are often centered on creating, developing and maintaining relationships. Usually, there are several

[1] Institute for Epidemiology and Preventive Medicine, University of Regensburg, Germany, matthias.olden@klinik.uni-regensburg.de
[2] CeRSI – Centro di Ricerca sui Sistemi Informativi, LUISS Guido Carli University, Roma, Italy, sza@luiss.it

components that can influence relationships, the most important being the trust level among the parties. According to Chiles and McMackin [1], trust is a key factor for relational exchange.

In literature, there are several studies that give a definition of trust or make a review in order to find a common definition among several contexts; i.e. sociological, psychological, organizational and computer science [2][3][4][5]. Levi [6] writes: "Trust is not one thing and it does not have one source; it has a variety of forms and causes". Also, some authors consider trust as a result of a combination of beliefs, attitude, intention and behavior [7], while others see trust only as a risk liability [4].

From the organizational point of view, trust is strongly linked with opportunistic behavior [1]. If there is a high perception of trust, the parties can adopt less elaborate safeguard rules. The opposite is also valid. If we consider the transaction cost theory [8] and the agency theory [9], transaction costs and agency costs are meant to protect against and to control the potential opportunistic behavior of the other party involved. Due to the continuous expansion of IT technologies and the enormous diffusion of internet, we distinguish between two kinds of relationships:

- Traditional relationships: they take place in ordinary life where information technology plays a marginal role. In this case, we can speak only of two concepts of trust: institutional [10] and social (often defined as customer trust[11]).
- Digital (or online) relationships: these focus strictly on IT. In this context (E-business/E-service/E-commerce), IT influences the institutional and social trust concept. Digital relationships are strongly associated with technological trust (trust in technology) [12][13][14].

Important attention is given to digital relationships inside an organization. For this, it is important to understand the role of IT and how this role can increase the trust perception or the opportunistic behavior control.

For this, we must consider relationships inside an organization through the TFI (technical-formal-informal) model. The trust concepts, especially the technological trust, are directly influenced by the security level provided by IT systems.

We consider an IT system where access is granted based on a standard user name/password routine; its security level is accordingly low.

The security of this system can be increased by Authentication and Authorization Infrastructures (AAIs) [15]. These are standardized methods to authenticate users and to grant them access to distributed web contents of several web providers.

At the moment, the combination AAI with password authentication does not present enough security, as it replaces the individual passwords from all applications with one "master" password used to access the federation. Additional security is given by enhanced authentication methods like biometrics, the only mechanism that can provide a bond between a user name and a real person. The gain of security must be considered upon solving several biometric specific problems, which will be presented in this paper.

Theoretical framework

An information system is composed of technical, formal and informal (TFI) parts in a state of continuous interaction [16].

The informal ways of managing information in organizations are critical and cannot always be replaced by rules or embedded in technical systems. The informal elements (i.e. perception of risks, awareness) which are very context related drive the design and the selection of formal (i.e. policies, business processes) and technical solutions (i.e. software and hardware platforms, network infrastructures). For information systems, the relationship between these three levels is complex and therefore requires consideration of issues such as trust and privacy by means of new technical, formal and informal mechanisms. In order to understand the influence of IT systems on technological, institutional and social trust in intra-organizational relationships, critical issues identified in information systems literature can be summarized as follows [17][18]: the perception of security embedded in the technical system (Informal level); the presence of formal mechanisms which regulate the interactions (Formal level); the reliability of IT systems, assured by the agreement on technical and procedural standards (Technical level).

By means of a biometric AAI with an enhanced security mechanism, the technological trust will have a positive influence over the institutional and social trust and will help to control the opportunistic behavior (i.e. this system does not allow users with different privileges to exchange credentials among each other).

Research design: Trust definitions and trust conceptual model

Same as in traditional relationships, trust is crucial in the digital world [19]. As internet is an insecure environment [20], IT influences trust [12]:

- social trust, strongly linked to the risk perception in exchanging information with other parties [21];
- organizational trust, concerning the relationships between customers and organizations supported by information technology [22][10][23][24][25];
- technological trust, which reflects above all the relation with IT used as support for information exchange [14].

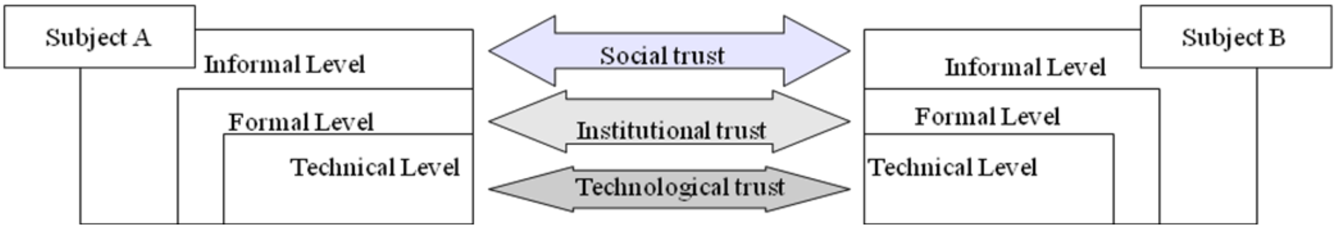

Fig. 1. The relationships between the three trust concepts and the TFI levels

Viewing the electronic relationships through the TFI model, the relations appear split in three levels, as shown in figure 1.

This work concentrates upon mechanisms acting on the technological trust level, disconsidering the other IT mechanisms that improve the institutional or social trust level (i.e. feedback mechanisms that aim to improve the subject reputation). Starting from the seven IT mechanisms table defined by Ratnasingam [20], we consider only two of them: authentication and access control within a biometric AAI.

Biometric AAIs within an organization

A biometric AAI with more identity providers (IdPs) is subject to several biometric specific problems, such as replay attacks, template aging or low recognition quality due to the use of multiple sensors. As the configuration proposed involves different IdPs belonging to the same company, it is possible to synchronize biometric data between the different user accounts.

Following situations can lead to biometric problems:

- the user possesses several accounts (user names) in the federation;
- the user has more biometric profiles (under the same user name), for example in the case of multiple sensors. These profiles are also stored at different IdPs.
- some of the profiles are not actualized and therefore outdated.

These problems can be solved by a stricter user management policy in which either the data is stored with a single IdP in the federation or the biometric data is located at different IdPs that synchronize it between themselves.

As the different IdPs are part of the same organization (and therefore share the same user database), it is possible to make a synchronization of the biometric data amongst IdPs. This process can be made either at database level or at the circle-of-trust level. By synchronization, the biometric data will be actualized between all IdPs.

The synchronization of biometric data directly on the database level is very efficient as it is uncoupled from the overlying AAI that remains responsible of authentication and authorization, Single Sign On and exchange of remaining attributes. An advantage is a better performance and a lower implementation effort as there are various software solutions for database mirroring [26]. On the other hand, most of these solutions presume a master-slave relationship between the database servers, which is not the case in a federated environment.

Basically, there are two possible scenarios for database synchronization: a first variant assumes that biometric data is managed via a central repository. An alternative is a decentralized configuration; however, no replication mechanism allows a completely decentralized synchronization of multiple servers.

This solution also implies considerable restrictions, as it assumes a close trust relationship between the participating partners, where all IdPs must grant each other access to their user databases. A further requirement for the synchronization on database level is that user data has to be identical at all IdPs, meaning identical user names on all servers in the circle of trust. This makes it impossible for the user to assume different user names, e.g. for privacy protection. It also automatically creates user accounts at all IdPs, although the user may use only some of them.

Due to these restrictions, biometric data must be treated in the same way as other user attributes and therefore synchronized on the AAI level. Nevertheless, this raises the problem of different user names assignment (it must be possible for a user to have different user names stored at different IdPs). For this, a mapping table must be created, where different user names from different IdPs are joined together. This process can be very difficult to complete and maintain manually and it is subject to errors.

A different approach is to forego mapping tables and to identify the same user on different servers by means of biometrics. If the user registers via biometrics at one IdP from the federation, the biometric samples will be sent to the other providers that will match them against all profiles stored locally. If the achieved match score is higher than a certain threshold, the other IdPs assume that the current sample belongs to one of their registered users. The user can now log in to all other IdP and the biometric sample will be correctly added to the identified profile for synchronization purposes.

This solution saves disk space and increases availability as it requires no update of a mapping table and no contact to dedicated servers. Nowhere does it become apparent under which user name a user is registered at other IdPs, which insures user privacy. A disadvantage is the fact that this variant requires a high computational effort. In the worst case, all profiles on the server have to be matched against one biometric sample. This worst case is not improbable; it occurs always when a user does not have an account on a server and therefore no matching profile can be found. Another problem occurs when the achieved match score is too small to ensure a clear biometric identification. In this case, the synchronization can not be executed automatically, but only by means of manual mapping by the administrator or even by the user himself.

The optimal solution is a combination between biometric identification and mapping tables. For this, when the user registers to an application within the circle of trust, the identification process is started at every other IdP. As the user provides more samples for the registration (biometric enrolment), the identification process can find the proper correspondent user account stored at every IdP. For privacy reasons, the IdP that submits the enrolment samples can choose to anonymize them by means of a random user id, which will be marked in its mapping table. As soon as the user is identified on all IdPs, the mapping tables are automatically completed and no further biometric identification is necessary, thus reducing the computational effort.

Another problem of biometric data synchronization occurs when the transfer of a typing sample or a whole profile fails, for example if an IdP is offline. To avoid this case, the IdP that received the latest typing sample and started the synchronization process must remember with which other IdP the synchronization failed and retry at a later date. Another solution is that the server which was not accessible inquires whether new typing samples were delivered at the other participants during the time when it was offline. As additional information, the IdP can send the date of the latest sample from its database (it is assumed that the providers have also synchronized times).

By means of synchronization, biometric data is kept up to date, thus ensuring that all samples can be checked for replay attacks, that the biometric template did not age on any server and that conflicts caused by the lack of profiles for different sensors are avoided.

Conclusions and future work

Starting from the relationship between IT and trust in inter-organizational relationships, we constructed a technical solution for an AAI system based on enhanced authentication technologies. This system allows a better access protection to restricted information and prevents credential exchange among users.

In the TFI model, a biometric AAI allowing both authentication and identification results in a better respect of bureaucracy roles (e.g. each person must use only his/her own credentials to access, create or manipulate a subset of information). It also has a positive influence on the trust in technology inside the organization.

This work can be the basis for future research of the organizational and technological aspects of this topic.

From an organizational point of view, user's perception of trust in a biometric AAI must be evaluated. This can be made by submitting a survey to several users inside an organization and understanding the references to the different types of trust.

From a technological point of view, the process of synchronizing biometric data must take into consideration other facts like data redundancy, the quantity of data that has to be transferred and the fact that some AAI protocols may not support real time synchronization upon login. For the case of typing behavior biometrics, the mechanisms of recognizing replay attacks or determining the template aging must be researched. Another interesting use case is the situation when the biometric template is not centrally stored at one or more IdP, but kept entirely in possession of the user.

References

1. Chiles, T.H. and McMackin, J. (1996). *Integrating variable risk preferences, trust, and transaction cost economics*, Academy of Management Review 21 73–99.

2. Rousseau, M.T., Stikin, S.B., Burt, S.B., Carmerer, C. (1998), *Not so different after all: across-discipline view of trust*, Academy of Management Review, Vol. 23 No.3, pp.393-404.
3. Kramer R. M., (1999), *Trust and distrust in organizations: Emerging Perspectives, Enduring Questions*, Annual Review of Psychology, Vol. 50: 569 -598.
4. Mayer, R.C., Davis, J.H., and Schoorman, F.D. (1995). *An Integrative Model of Organizational Trust*, Academy of Management Review, 20 (3), 709-734.
5. McKnight, D. H. and Chervany, N. L. (2001). *Trust and Distrust Definitions: One Bite at a Time*, In Proceedings of the Workshop on Deception, Fraud, and Trust in Agent Societies Held During the Autonomous Agents Conference: Trust in Cyber-Societies, integrating the Human and Artificial Perspectives R. Falcone, M. P. Singh, and Y. Tan, Eds. Lecture Notes In Computer Science, vol. 2246. Springer-Verlag, London, 27-54.
6. Levi, M. (1996). *Social and unsocial capital: a review essay of Robert Putnam's "Making Democracy Work"*, Politics and Society, 24: 45-55.
7. Bhattacherjee, A. (2002). *Individual Trust in Online Firms: Scale Development and Initial Test*, Journal of Management Information Systems, 19 (1), 211-242.
8. Williamson, O. E. (1985*). The Economic Institutions of Capitalism*, Free Press, New York.
9. Eisenhardt K. (1985). *Control: organizational and economic approaches*. Management Science, 31, 134-149.
10. McKnight, D.H., Cummings, L.L. E Chervany, N.L. (1998). *Initial Trust Formation in New Organizational Relationships*, in Academy of Management Re-view, vol. 23, n. 3
11. Granovetter M. (1985), *Economic Action and Social Structure: The Problem of Embeddedness,* American Journal of Sociology, 91(November): 481-510.
12. Misiolek, N.I., N. Zakaria, and P. Zhang (2002). *Trust in organizational acceptance of information technology: A conceptual model and preliminary evidence*, in Proc. Decision Sciences Institute 33rd Annual Meeting 2002.

13. Ratnasingam, P. and Pavlou, P. (2002), *Technology trust: the next value creator in B2B electronic commerce*, International Resources Management Association Conference - Washington, Seattle.

14. Reeves, B., & Nass, C. (1996). *The media equation. How people treat computers, television, and new media like real people and places*. New York: Cambridge University Press.

15. Schläger, C.; Sojer, M.; Muschall, B.; Pernul, G. (2006): *Attribute-Based Authentication and Au-thorisation Infrastructures for E-Commerce Providers*, pp132-141 Springer-Verlag.

16. Liebenau J. and Backhouse J. (1990). *Understanding Information: an Introduction*, Macmillan, London.

17. Gambetta, D., (1988). *Trust: Making and Breaking Cooperative Relations*. Basil Blackwell, Oxford, U.K. ed. 1998

18. Kumar, K. and Becerra-Fernandez, I. (2007). *Interaction technology: Speech act based information technology support for building collaborative relationships and trust*, Decis. Support Syst. 43, 2 584-606. DOI= http://dx.doi.org/10.1016/j.dss.2005.05.017

19. Ba, S., Whinston, A. B., and Zhang, H. (1999). *Building trust in the electronic market through an economic incentive mechanism.* In Proceedings of the 20th international Conference on information Systems (Charlotte, North Carolina, United States, December 12 - 15, 1999). International Conference on Information Systems. Association for Information Systems, Atlanta, GA, 208-213.

20. Ratnasingam, P. (2002). *The importance of technology trust in web services security*, Information Management & Computer Security, 10(5), 255–260.

21. Koller, M. (1988). *Risk as a Determinant of Trust*, Basic and Applied Social Psychology Volume 9, Issue 4, pp. 265-276.

22. Lewicki, R.J., & Bunker, B.B. (1996). *Developing and maintaining trust in work relationships*, In R.M. Kramer & T.R. Tyler (Eds.), Trust in organizations: Frontiers of theory and research (pp. 114-139). Thousand Oaks, CA: Sage Publications.

23. Pavlou, P., Tan, Y.H. and Gefen, D. (2003), *Institutional Trust and Familiarity in Online Interorganizational Relationship*, Proceedings of the 11th European Conference on Information Systems, Naples, Italy, June 19-21, 2003.

24. Spagnoletti P., Za S., D'Atri A., (2007). *Institutional Trust and security, new boundaries for Virtual Enterprises*, Proc. of 2nd International Workshop on Interoperability Solutions to Trust, Security, Policies and QoS for Enhanced Enterprise Systems, IS-TSPQ2007, Funchal, Portugal.

25. Tyler, T.R., & Degoey, P. (1996). *Trust in organizational authorities. The influence of motive attributions on willingness to accept decisions*, In R.M. Kramer & T.R. Tyler (Eds.), Trust in organizations: Frontiers of theory and research (pp. 331-350). Thousand Oaks, CA: Sage Publications.

26. Qarchive (2008), *Database synchronization*, database-synchonization.qarchive.org, retrieved 01.10.2008