Trust Approach Based on User's Activities

Nagham Alhadad, Philippe Lamarre, Patricia Serrano-Alvarado, Yann Busnel

Trust Approach Based on User's Activities

Nagham Alhadad[1], Philippe Lamarre[2], Patricia Serrano-Alvarado[1], Yann Busnel[1]

[1] LINA / Université de Nantes
2, rue de la Houssinière
44322 Nantes, France

[2] LIRIS / INSA de Lyon
20, avenue Albert Einstein
69621 Villeurbanne, France

Abstract. The complexity of distributed systems continuously increases and their usage is widened into a variety of contexts. Users do several activities through these systems like sharing data, chatting, buying online, *etc*. Persons, hardware and software are involved in activities so we consider a system as the representation of two worlds, the social and the digital worlds. Trust plays an important role in helping users to analyze the danger or risk they incur when doing an activity. Research on trust notions has focused on the social entities where a trustee is a person or an organization of persons. Recent research analyzes trust toward the digital world *i.e.*, technologies. We consider that having these two building blocks is not enough for a user to decide if she can confidently do an activity in a particular system. Such decision requires to consider the system organization as a whole because it determines whom and what would be involved in a user activity and how. This article focuses on this problem and provides first ideas for solution.

1 Introduction

A large number of distributed systems arises nowadays being more and more complex and used for a variety of applications. Participants of these systems do several activities like sharing documents, chatting, buying online, *etc*. Persons, hardware and software are involved in activities, so we consider a system as the representation of two worlds, the social and the digital worlds, and their relationships.

When using a system, user expectations may vary from one user to another in many different aspects, in particular, they may give different assessments to trust and privacy issues. Current systems generally do not adapt to such individual needs and users are forced to have faith in them. Nevertheless, within systems, trust plays an important role and helps users to analyze the danger or risk they incur when doing activities [1]. If users trust the systems they use for their activities, they will feel more confident when using them. We believe that preserving privacy is one of the most important factors that influences trust, in the meaning that a user can not trust a system that does not preserve her privacy.

Trust has been widely studied. On one hand, research on trust notions has focused on trust toward persons or organizations of persons [2,3,4]. They consider trust in general, analyzing several concepts concerning, among others, disposition to trust (trusting stance, faith in humanity), trusting beliefs (competence, benevolence), cognitive processes (unit groups, reputation, stereotypes), *etc*. Some studies in computer sciences adopted the previous concepts in different domains. In particular, trust toward a person mostly depends on her reputation which is constructed from the information collected about her activities in the system [5,6,7,8,9,10]. We consider those works within what we call the *social world*, that is actually the real world. On the other hand, recent research analyzes trust toward the *digital world i.e.*, technologies [11,12,13,14]. Trust in this context has been defined as the "willingness of the trustee to depend on a piece of software to do a task" [14]. Some other works define a generic definition of trust toward the different entities of the system either if it is a person or an artifact [15,16]. These works are still limited to trust toward the separated entities that construct the system and do not give a general point of view of the user's trust toward a whole system for an activity, represented by all the actors involved (from both the social and digital worlds). By studying the trust toward a system for an activity we are interested in making the system adaptable to one of the user expectations which is the trust.

The objective of this paper is to provide the basis that enable users to build a personal and private trust decision toward a system to do an activity. In [17,18], we proposed SOCIOPATH, a meta-model that allows to draw a representation (or model) of a system. This representation consists in *(i)* components in the social world like hardware, persons, *etc*, *(ii)* components in the digital world like software, resources, *etc*, and *(iii)* the ways they are related, *(i.e.)*, who *controls* what, who *provides* what, *etc*. The trust decisions of users toward a system we propose here are based on SOCIOPATH models.

The paper is organized as follows. Section 2 introduces a quick overview of SOCIOPATH. Section 3 presents the first ideas of our approach on computing the user's trust decision toward a system for an activity. Finally, we conclude and detail the ongoing work and perspectives in Section 5.

2 Overview of SOCIOPATH

The SOCIOPATH meta-model [17,18], allows to describe the architecture of a system in terms of the components that exist in the social world, where *persons* own *physical resources* and *data*, and in the digital world, where *instances of data* (including application codes) are stored and *artifacts* (softwares) are running. SOCIOPATH also describes the relations between the different components of the two worlds.

Enriched with deduction rules, the SOCIOPATH meta-model allows to underline and discover chains of *access* and *control* relations between the *actors* and the *digital resources* in a system. A user may completely trust a person in a field, where she does not trust the same person at all in another field, for example, a user may trust a person in the quality of services she offers, but not in keeping her data private. The Implicit relations of *access* and *control* in a system allows the user to know who are the persons who might access or control her data, thus considering the privacy as a factor to evaluate the trustworthy of these persons.

Two of the most important concepts used in SOCIOPATH are:

- *path*, which is a list of actors and digital resources that describes the way an actor may access a resource ;
- *activity*, which is a task like sharing data, chatting, buying online, *etc.*, where some restrictions are considered to impose the presence of particular elements in the path. For instance, if a person wants to read a `.doc` document, she must use an artifact that can "understand" this type of document (*e.g.*, Microsoft Word or Open Office Writer).

Figure 1 shows an example of a SOCIOPATH model where a user Marie wants to perform the activity "reserving a plane ticket"[1]. The social world part of the figure contains:

- the persons (physical or moral), like Marie or the airline company `AirFrance`;
- the physical resources, like `AF-A-330-200` which can be any 330-200 plane owned by `AirFrance` and constructed by `AirBus`;
- the data involved in this activity, like Marie's travel.

The digital world contains the digital resources, involved in the activity like the site `Opodo`, or the data instances like `eTicket` which is a representation of Marie travel. Then the interaction between the two worlds are represented by the relations *control*, *access*, *support*, *own* and *represent*. Marie can achieve her activity via three available paths. She uses a `Broker` that may lead her to two online travel agency sites, `GoVoyages` and `Opodo`. The first site reserves an `AirFrance ticket` or a `Bohja ticket` and the second one reserves a `Continental Airlines ticket`. The first path is: {`Marie, Broker, GoVoyages, AirFrance reservation, eTicket`}. The second path is: {`Marie, Broker, GoVoyages, Bhoja Air reservation, eTicket`} and the third path is: {`Marie, Broker, Opodo, Continental Airlines reservation, eTicket`}. Each element of the path is controlled by one or more persons in the social world and supported by one physical resource at least. For instance, `Opodo` is controlled by the `Amadeus` group and the `AirFrance reservation` is supported by the aircraft `AF-A-330-200`.

Among others, SOCIOPATH allows to define:

1. the set of *user's dependences on artifacts for an activity (digital dependences)*, which is composed by the artifacts a user passes through to perform an activity. Some examples of the sets of the digital dependences for the activity "Marie reserves a plane ticket" are: {{`Broker`},{`GoVoyages, Opodo`},{`GoVoyages, Continental Airlines reservation`}, *etc* };
2. the set of *user's dependences on persons for an activity (social dependences)*, which is composed of the persons who control the artifacts the user depends on *i.e.*, (1);
3. the set of *user's dependences on physical resources for an activity (social dependences)*, which is composed of the physical resources that supports the artifacts the user depends on *i.e.*, (1).

Some example of the social dependences are: {{`Broker Provider`},{`Accor, Amadeus`}, {`AirFrance, Boeing`}, *etc*} and {{`AF-A-330-200, CA-B-757-300, BA-B-737-400`}, *etc*}. Without one of those sets Marie can not achieve her activity.

Given this information we can help the user to build a trust decision toward a system for an activity.

[1] For simplicity, the figure does not introduce all the entities involved in this activity. For instance, each software must be supported by a physical resource (a server, a PC, *etc*), which is not presented in the figure.

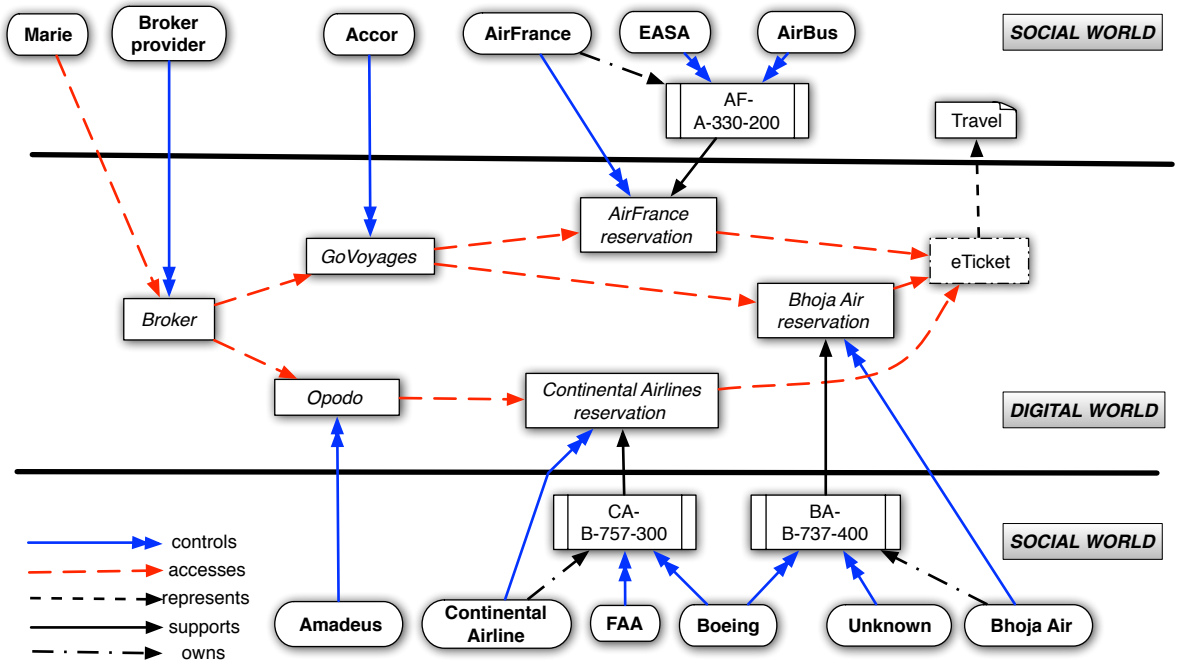

Fig. 1: An example about the paths and the relations derived from the modeling using SOCIOPATH.

3 Building a trust decision toward a system for an activity

A system is able to perform an activity (like buying online, editing a document, *etc*) if at least it has one path to do it. In general, current systems provide different ways to perform the same activities. For users, it is important to know if the system is trustworthy enough to perform their activity and which is the most trustworthy path provided by the system from their personal and private point of view.

SOCIOPATH provides a rich foundation to analyze systems thanks to its distinction between the digital and the social worlds and the interaction between them. From the sets of dependences resulting of SOCIOPATH models, we can analyze the trust of a system for an activity. For this, we propose to use concepts of trust toward persons, digital resources and physical resources to perform an activity. This will allow us to calculate the trust toward paths and toward the system in general.

Figure 2 shows a graphical representation of the steps of our process to compute the user's trust for an activity:

1. SOCIOPATH helps to identify:
   (a) the paths for an activity;
   (b) the user's dependences on artifacts for an activity (digital dependences) in a system;
   (c) the user's dependences on physical resources for an activity (social dependences) in a system;
   (d) the user's dependences on persons for an activity (social dependences) in a system;
2. the user makes a trust decision toward the persons she depends on to do an activity;
3. a trust decision toward the artifacts a user depends on is made from the user's trust toward the persons and the user's trust toward the data related to the artifacts and the representation of this data;
4. a trust decision toward the physical resources a user depends on is made from the user's trust toward the persons;
5. a trust decision toward the paths in the system for an activity is made from the trust decision made toward the artifacts;
6. we obtain the user's trust toward the system for an activity from the user's trust toward the paths for an activity.

Next sections explain the steps 2 to 6.

3.1 Building a trust decision toward a person to perform a role

The persons a user depends on to perform an activity are the persons who control an artifact or more in the path. A user trusts a person, depending on her own personal relationship, on her past experiences, or on the reputation of

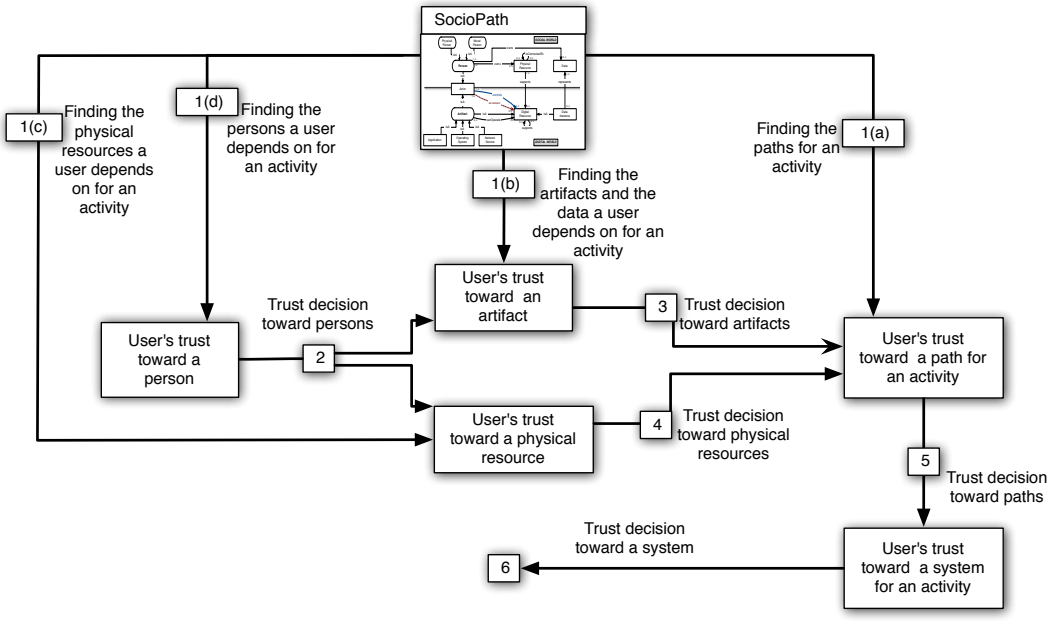

Fig. 2: Decision making process according to the trust toward a system.

this person [5,6,7,8,9,10]. Beside that, since the user is aware of the *access* and *control* relations in a system, she can consider also the way this person deals with privacy as a factor that indicate the trustworthy of this person.

By using this, a user declares a level of trust toward another person. We note this value T_P. For instance, Marie may trusts `AirBus` more than `Boeing` because she is European for instance, or she might trust `Accor` more than `Amadeus` because the privacy policy of `Accor` satisfies her privacy preferences more than the privacy policy of `Amadeus`, this is very important because both of them might have an access to her personal information.

3.2 Building a trust decision toward an artifact

When Marie wants to reserve a ticket to travel, she may use a site like `Opodo`. Of course, Marie should trust the persons who control this site (providers and administrators) to act honestly. Marie should trust also the code source of the site (design of the site and the representation of the site in the digital world).

When a user wants to make a trust decision toward an artifact, she depends on the following:

- The person who provides the code supporting the artifact. We note the level of trust toward the provider $T_{provider}$.
- The person who owns and controls a physical resource that supports the artifact. We note the level of trust toward the supporter $T_{supporter}$.
- The data instance that supports the artifact. Every artifact is supported by a data instance (the code source of this artifact), and every data instance represents some data in the digital world. The trust toward the data instance is evaluated depending on the trust toward the data and the representation of this data. We note the level of trust toward the data instance $T_{dataInstance}$. Note that $T_{dataInstance} = f(T_{data}, T_{represents(data,dataInstance)})$ where T_{data} is the trust toward the data and $T_{represents(data,dataInstance)}$ is the trust toward the representation of the data in the digital world.

The level of trust toward the artifact noted T_F, is a function of $T_{provider}$, $T_{supporter}$ and $T_{dataInstance}$:

$$T_F = f_{artifact}(T_{provider}, T_{supporter}, T_{dataInstance}).$$

3.3 Building a trust decision toward a physical resource

If Marie wants to reserve an `AirFrance ticket` to travel, that implies that she needs to trust the plane model of the reservation `AF-A-330-200`. How can she make a trust decision toward this plane model? Of course, Marie

should trust `AirBus`, the provider of this plane to construct good aircrafts, also the persons or the companies who have some control on the plane, like the maintenance association `EASA` of the European Union.

When a user wants to make a trust decision toward a physical resource, she depends on the following:

- the person who provides the physical resource. We note the level of trust toward the provider $T_{provider}$.
- the person who controls the physical. We note this level of trust $T_{controler}$.

The level of trust toward the physical resource noted T_{PR}, is a function of $T_{provider}$ and $T_{controler}$:

$$T_{PR} = f_{physres}(T_{provider}, T_{controler}).$$

3.4 Building a trust decision toward a path for an activity (ω-path)

In real life, if a user wants to perform an activity, she needs to follow a path and use some tools to reach her objective.

If Marie needs to reserve a plane ticket, she could have several paths and different tools to do it. Marie may use a `Broker` to choose a site of aircraft reservation like `GoVoyages`, which leads her to an airline company like `AirFrance`, then reserve the ticket. To make a trust decision toward this path, Marie needs to trust the tools she uses whether they are artifacts or physical resources.

A path in a system is an ordered list of artifacts that begins with an actor and ends with a digital resource. The user's trust toward a path is evaluated depending on the artifacts that belong to the path. We note this value T_{σ_ω} where σ_ω is a path for an activity ω performed by the user. Let σ_ω be a ω-path:

$$T_{\sigma_\omega} = f_{path}(\{T_F, T_{PR} : F \in \sigma_\omega \wedge supports(PR, F))\}.$$

3.5 Building a trust decision toward a system for an activity

A user might have several paths to perform an activity.

The `Broker` Marie uses leads her to sites like `GoVoyages` and `Opodo`, each of them proposes her several reservations. Marie trust decision toward a system for the activity "reserving a plane ticket", is composed of the trust decision toward all the paths enabling her to perform the activity.

Finally, from the user's trust toward paths enabling a user to perform an activity, we are able to propose the trust function toward the system. Let σ_ω be an ω-path and Υ_ω be the set of the ω-paths. The user trust toward a system, noted T_ω, is given by:

$$T_\omega = f_{system}(\{T_{\sigma_\omega} : \sigma_\omega \in \Upsilon_\omega\}).$$

Depending on the value T_ω, a user can make a trust decision toward a system.

3.6 Implementing trust functions

Implementing the functions above can be a challenge because the trust level should be weighed by the importance of the actor's role for the activity from the user point of view, and the chosen metrics should give different meaning to the user. Some functions give a general value of trust like the average function, but it hides the dangerous elements in a path or a system. Others can be pessimistic functions like the minimum function because if the user has one untrustworthy element in the path or the system, that means that the whole system is untrustworthy, on the other hand, it gives a good indication on the risks existing in a path or a system.

The maximum function is an optimistic choice because it shows the most trustworthy elements in a system.

Each of the previous functions has a special meaning, defining the metrics of trust should be a mix of different functions to show these different meaning. Looking for the best metrics is one of our future goals.

4 Impact on privacy

This work is related to privacy on several aspects. On the one hand, SOCIOPATH requires transparency to involved actors, and this can be perceived as a privacy breach. The more details a SOCIOPATH model has about the architecture, the more accurate the dependency factor is. But to avoid to reveal a detailed architecture, an artifact may, for instance, provide only its dependencies concerning the involved user activity without giving its levels of dependencies.

On the other hand, the way privacy is managed by involved actors is an important factor that influence the trust a user has toward toward those actors. There exist a lot of web tools that detect several aspects concerning privacy. To analyse Web sites, one of the most interesting tool is PrivacyBird[2]. Based on P3P privacy policies[3], PrivacyBird indicates if a site matches user's preferences or not. Another one is Collusion[4], a Mozilla add-on that detects the third-parties tracking users in the Web. There exist also Privacy Dashboard[5], another Mozilla add-on that helps to control what personal information is collected by sites. Thus, if users are informed about the actors' practices concerning their privacy, they are able to state a reliable trust degree toward those sites.

5 Ongoing work and Conclusion

This paper proposes a model for the user to build a trust decision toward a system for a specific activity. This work is not only limited to calculate the value of trust toward the system, it also enables the user to manipulate her architecture to maximize her trust toward a system for an activity, by changing some artifacts or eliminating some paths.

SOCIOPATH can be used to check whether the system respects the users's satisfaction with regards to their privacy and trust. Being able to test an architecture compliance with respect to users' privacy policies and users' trust priorities is our future goal.

References

1. Vu, Q.H., Lupu, M., Ooi, B.C.: Peer-to-Peer Computing: Principles and Applications. 1st edn. Springer Publishing Company, Incorporated (2009)
2. Gefen, D.: Reflections on the Dimensions of Trust and Trustworthiness among Online Consumers. SIGMIS Database **33** (2002) 38–53
3. Ridings, C.M., Gefen, D., Arinze, B.: Some Antecedents and Effects of Trust in Virtual Communities. Strategic Information Systems **11** (2002) 271–295
4. Mayer, R.C., Davis, J.H., Schoorman, F.D.: An Integrative Model of Organizational Trust. Academy of Management **20** (1995) 709–734
5. Essin, D.J.: Patterns of Trust and Policy. In: Proceedings of the 1997 Workshop on New Security Paradigms, New York, USA, ACM (1997) 38–47
6. Viljanen, L.: Towards an Ontology of Trust. In: Proceedings of the Second International Conference on Trust, Privacy, and Security in Digital Business, Berlin, Heidelberg, Springer-Verlag (2005) 175–184
7. Abdul-Rahman, A., Hailes, S.: Using Recommendations for Managing Trust in Distributed Systems. In: Proceedings of IEEE Malaysia International Conference on Communication, Kuala Lumpur, Malaysia (1997)
8. Gupta, M., Judge, P., Ammar, M.: A Reputation System for Peer-to-Peer Networks. In: Proceedings of the 13th International Workshop on Network and Operating Systems Support for Digital Audio and Video, ACM (2003) 144–152
9. Cornelli, F., Damiani, E., di Vimercati, S.D.C., Paraboschi, S., Samarati, P.: Choosing Reputable Servents in a P2P Network. In: Proceedings of the 11th International Conference on World Wide Web, New York, USA, ACM (2002) 376–386
10. Damiani, E., di Vimercati, D.C., Paraboschi, S., Samarati, P., Violante, F.: A Reputation-Based Approach for Choosing Reliable Resources in Peer-to-Peer Networks. In: Proceedings of the 9th ACM conference on Computer and Communications Security, New York, USA, ACM (2002) 207–216
11. Li, X., Hess, T.J., Valacich, J.S.: Why Do We Trust New Technology? A Study of Initial Trust Formation with Organizational Information Systems. Strategic Information Systems **17** (2008) 39–71
12. Corritore, C.L., Kracher, B., Wiedenbeck, S.: On-Line Trust: Concepts, Evolving Themes, a Model. International Journal of Human Computer Studies **58** (2003) 737–758
13. Li, X., Hess, T.J., Valacich, J.S.: Using Attitude and Social Influence to Develop an Extended Trust Model for Information Systems. SIGMIS Database **37** (2006) 108–124
14. Mcknight, D.H.: Trust in Information Technology. Volume 7. Davis, Gordon B. (Ed.) The Blackwell Encyclopedia of Management, Malden, USA (2005)
15. Demolombe, R.: Reasoning about Trust: A Formal Logical Framework. In: iTrust. (2004) 291–303
16. Mcknight, D.H., Cummings, L.L., Chervany, N.L.: Initial Trust Formation in New Organizational Relationships. Academy of Management Review **23** (1998) 473–490
17. Alhadad, N., Lamarre, P., Busnel, Y., Serrano-Alvarado, P., Biazzini, M.: SOCIOPATH: In Whom You Trust? In: Journées Bases de Donnes Avances, Rabat, Morocco (2011)
18. Alhadad, N., Lamarre, P., Busnel, Y., Serrano-Alvarado, P., Biazzini, M., Sibertin-Blanc, C.: SOCIOPATH: In Whom You Trust? Technical report, LINA – CNRS : UMR6241 (2011)

[2] http://www.privacybird.org/
[3] http://www.w3.org/P3P/
[4] http://www.mozilla.org/en-US/collusion/
[5] http://code.w3.org/privacy-dashboard/