Context-Aware Trust Domains*

Ricardo Neisse**, Maarten Wegdam, and Marten van Sinderen

CTIT, University of Twente, The Netherlands
{R.Neisse, M.Wegdam, M.J.vanSinderen}@utwente.nl

Abstract. Context-aware service platforms need to establish and manage trust relationships for users to know if the user's privacy policies are being enforced and for service providers to control access to their services. Current trust solutions are not suitable for this because they do not address in an integrated manner trust issues related to identity provisioning, privacy enforcement and context information trustworthiness. In addition, due to their hierarchical and centralized design, current trust management solutions do not scale well in the ad-hoc pervasive environments in which context-aware platforms are typically deployed. In this paper we propose context-aware trust domains as a management solution for context-aware service platforms.

1 Introduction

One challenging problem in the realization of context-aware services [1] is the enforcement of the privacy of the users. This problem arises due to the highly privacy sensitive nature of the context information, and the implicit gathering and combining of this information in a pervasive service provisioning environment. For example, context information can be misused to allow unauthorized user tracking, unauthorized sophisticated user profiling and identity theft. It is therefore important for users to know about the trustworthiness [2] of the entities they are interacting with.

Next to being an object of security concern, context information also offers an opportunity to enhance the available security techniques. These enhancements include less intrusive access control methods where user roles are determined by context-situations (e.g. allow access for people inside a train [3]), instead of being assigned to specific entities. However, the use of context-information in this way requires trust (confidence) in the context-source, or requires at least a way to verify the integrity of the context information used in the access control policy (e.g. location).

In traditional systems, users establish static trust relationships with well known organizations such as banks, credit card companies, and mobile phone operators. These trust relationships are typically based on contracts, and the security policies are always associated with the entities' identities. For instance, a customer opening an account in a bank provides his/her personal data and, by signing a contract with the bank, establishes a trust relationship that his/her money and information will be stored

* This work is part of the Freeband AWARENESS project (http://awareness.freeband.nl). Freeband is sponsored by the Dutch government under contract BSIK 03025.
** Ph.D. student supported by CNPq scholarship – Brazil.

P. Havinga et al. (Eds.): EUROSSC 2006, LNCS 4272, pp. 234 – 237, 2006.

safely. In pervasive environments, users are supposed to interact with a large number of entities unknown beforehand and a priori trust relationships only exist in a few special scenarios where nodes are controlled by a single organization [4].

2 Trust Aspects

In order to scope our work we divide Trust in different aspects as [5] approaches Privacy. Trust can be analyzed regarding the social, the informational, and the technical aspects (Fig. 1). For each of these aspects there are different problems that should be addressed, for instance, how user perceive the trust in the system (social aspect), what are the concepts and semantics of trust mapped into the system (informational aspects) and how secure is the encryption technology used (technical aspect). The main focus of this work is in an architecture for dynamic management of trust relationships (information aspect) but we are also interested in the social aspect.

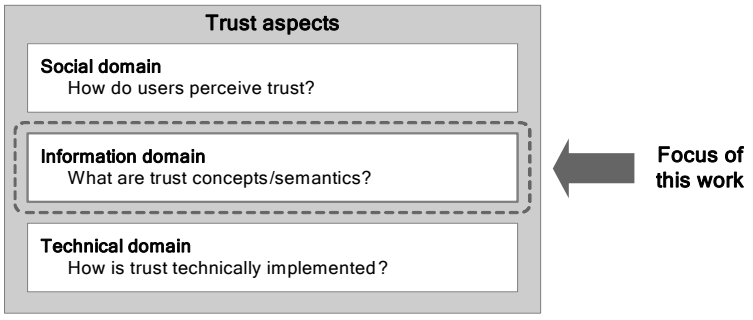

Fig. 1. Trust aspects

3 Trust Relationships in a Context-Aware Service Platform

Fig. 2 presents a context-aware service platform [6] on which we base our proposal for context-aware trust domains. In this service platform, before accessing a context-aware service, users should authenticate (step 1) with an identity provider. After the authentication is done, users can start using the service (step 2), which may check the user identity (step 3). The context-aware services retrieve context information about the users from context sources (step 4) in order to provide a personalized response. This context-information can be of any type, for instance, information representing the current activity or location of the user.

The four main roles we have identified in this context-aware service scenario (Fig. 2) are: *identity providers*, *context consumers* (service providers), *context providers* (context sources) and *context owners* (e.g. users). In Fig. 2 we also present trust relationships from users (a and b) and service providers (c) points of view. The list of trust relationships presented is not exhaustive; other different trust relationships could be defined. In order to limit the scope we focus on trust relationships related to privacy (i), identity (ii), and context trustworthiness (iii).

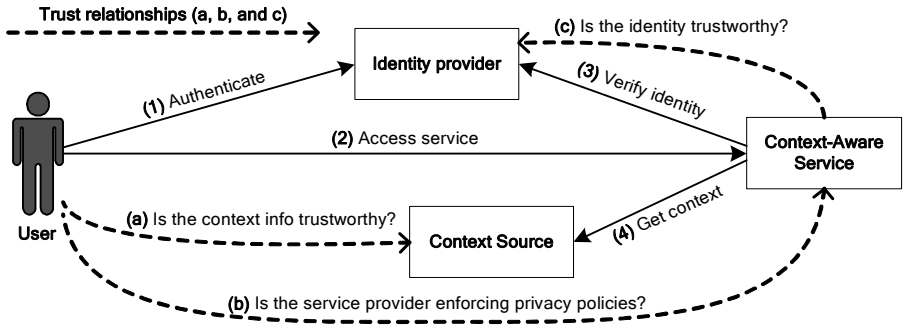

Fig. 2. Trust relationships in a context-aware service platform

We consider that each entity in the context-aware service platform is part of an administrative domain for which a common set of trust relationships and security policies applies, according to the role of the domain. Users, service providers and context-sources in the system may play multiple roles at the same time, acting as context-consumers and context-owners. For each of these roles, we consider different trust requirements, for instance, context consumers should worry about trust relationships related to the privacy enforcement of context owners (user's) information.

3 Context-Aware Trust Domains

In a large context-aware system, with thousand of components and users, trust relationships can not be associated with individual entities, as this can easily become unmanageable. The main objective of this work is to reduce the complexity in the management of trust relationships using the abstraction of context-aware domains. In this way, trust degrees do not have to be specified individually for each entity, but in a set for a collection of entities part of a domain [7].

Domains are useful in the management because they allow the association of trust and policies with collections of entities instead of individual entities. In Context-aware domains, context information is used as a dynamic constituent, allowing more flexibility in the domain definitions. In this way, entities sharing the same context are grouped together and can join/leave the domain dynamically, with the context changes. Examples of context-aware management domain definitions are "Nearby persons", "Personal devices", and "Working colleagues" (Fig. 3).

Our proposal is to elaborate on the concept of Context-Aware domains for trust and policy management, where entities inside of a specific context situation will be associated with a trust degree and/or security policy. The idea is to provide mechanisms to define and infer the trust degree of an entity based on the context information provided about that entity. We divide this research in two main open research questions: (1) what is the role of trust in context-aware service platforms and (2) what is the role of context information in trust establishment and management.

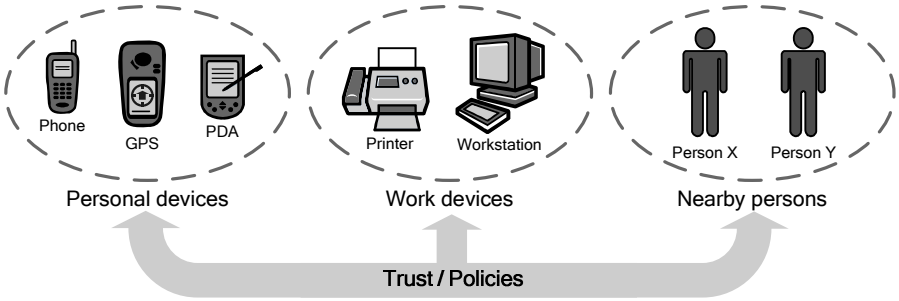

Fig. 3. Examples of context-aware domains

We plan to validate our context-aware trust domain concept through a prototype implementation in the AWARENESS project. The validation method probably will be focused on the performance and usability and based on analysis of system logs/traces and end users and system administrators interviews.

References

1. Dey, A. K.; Salber, D.; Abowd, G. D. A conceptual framework and a toolkit for supporting the rapid prototyping of context-aware applications. HC Interaction, 16, 2001.
2. Grandinson, T.; Sloman, M. A Survey of Trust in Internet Applications, IEEE Communications Surveys 2000.
3. Hulsebosch, R. J.; Salden, A. H.; Bargh, M. S.; Ebben, P. W.; Reitsma, J. Context sensitive access control. In Proceedings of the 10th ACM SACMAT, Sweden, June, 2005.
4. Molva, R. and Michiardi, P. Security in Ad hoc Networks (invited paper). In: Personal Wireless Communications, September 23-25 2003, Venice Italy.
5. Boland, H.; Soute, I. *Perceived Privacy*. Philips research presentation, AMIGO project workshop, Telematica Instituut, The Netherlands, March, 2006.
6. AWARENESS Service Infrastructure D2.1 - Architectural specification of the service infrastructure, http://awareness.freeband.nl.
7. Damianou, N.;Dulay, N.; Lupu, E.; Sloman, M.; Tonouchi, T. Tools for Domain-based Policy Management of Distributed Systems. IEEE/IFIP NOMS, Italy, Apr, 2002.