

# A Distributed Context-Aware Trust Management Architecture<sup>1</sup>

Ricardo Neisse<sup>2</sup>, Maarten Wegdam and Marten van Sinderen

Centre for Telematics and Information Technology,  
University of Twente, P.O. Box 217  
7500 AE Enschede, The Netherlands  
{R.Neisse, M.Wegdam, M.J.vanSinderen}@utwente.nl

**Abstract.** The realization of a pervasive context-aware service platform imposes new challenges for the security and privacy aspects of the system in relation to traditional service platforms. One important aspect is related with the management of trust relationships, which is especially hard in a pervasive environment because users are supposed to interact with entities unknown before hand in an ad-hoc and dynamic manner. Current trust management solutions do not adapt nor scale well in this dynamic service provisioning scenario because they require previously defined trust relationships in order to operate. The objective of this thesis is to design, prototype and validate a context-aware distributed trust management architecture in order to address: (a) the lack of integration between available trust solutions and security and privacy management languages, and (b) the dynamic characteristics of a context-aware service platform.

## Problem Statement

One challenging problem in the realization of context-aware services [1] is the enforcement of the privacy of the users. This problem arises mainly due to the highly privacy sensitive nature of user context information, and the implicit gathering and combining of this information in a pervasive service provisioning environment. Obtained context information enables serious misuse like unauthorized user tracking, unauthorized sophisticated user profiling and subsequent identity theft. In this way it is important for users to know about the trustworthiness of the entities they are interacting with. Based on this trustworthiness, users can decide in the amount of context information they want to provide, for instance, providing less or anonymous context information to services they think may misuse the information.

On the other hand, context-aware systems can also be considered an opportunity to enhance the available security techniques. These enhancements include less intrusive access control methods where user roles are assigned to context-situations instead of

---

<sup>1</sup> This work is part of the Freeband AWARENESS project (<http://awareness.freeband.nl>). Freeband is sponsored by the Dutch government under contract BSIK 03025.

<sup>2</sup> Second year Ph.D. student supported by CNPq scholarship – Brazil.

being assigned to specific entities. One of such security policies can state, for instance, that people inside a train are allowed to access a specific service [2], without requiring traditional user/password authentication. 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). This context verification, or trust establishment with the context-source, is required mainly to avoid malicious users using faked context-information for unauthorized access.

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 signed 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 safely. On the other hand, in pervasive environments, users are supposed to interact with entities unknown beforehand and a priori trust relationships can only exist in few special scenarios where nodes are controlled by a single organization [3]. It is less likely that users of context-aware services will have static contractual relationships with all the entities involved in the service provisioning. In context-aware systems, changes in the trust relationships may be influenced by rapid changes in the context situations and current trust management solutions do not adapt nor scale properly in this cases.

## Related Work

There is no single accepted definition of trust in the current computer science literature and the definitions found classify trust as a number, as a discrete labeled degree or a combination of both (number/degree) [4]. A specific approach for trust definition aiming context-aware applications is proposed by Daskapan et al. [5]. In their approach they provide a heuristic model to evaluate trust from service providers' certificates in order to influence user privacy policy decisions. Based on the evaluated trust and a threshold the system may decide automatically, on behalf of the user, whether to provide context information with or without requesting user consent. The authors provide also a discussion about the distribution of trust management functionalities comparing centralized (PKI) and distributed approaches (PGP web of trust) but they do not provide an architecture nor an implementation of distributed trust management for context-aware service platforms.

Looking to these trust solutions and to the specification of available security and privacy management languages like the Security Assertion Markup Language (SAML), the eXtensible Access Control Markup Language (XACML), the Platform for Privacy Preferences (P3P) and the Enterprise Privacy Authorization Language (EPAL) it is clear the lack of integration. The primary objective of trust solutions should be to support security policy decisions, however, none of this policy languages consider trust as a parameter in the policy conditions. This is also the case of more generic and extensible policy languages like Ponder and REI, which, according to

theirs authors, can be extended to represent any type of security and privacy policies, however, a specification on how to use trust as an integrated parameter in these languages also does not exist.

## Goal Statement

The main goal of this PhD research is to design, prototype and validate a distributed context-aware trust management architecture. This architecture will address trust establishment and management based on the dynamic characteristics of the context information. Our idea is to provide a systematic policy-based definition of trust. The main contributions of this PhD research will be:

1. A trust model/definition for context-aware service platforms;
2. An specification on how to use trust as an integrated parameter in context-aware privacy/security policies;
3. A distributed context-aware trust management framework and system architecture;
4. A prototype implementation including mechanisms for context-aware trust negotiation, analysis, evolution, recommendations and visualization.

## Approach

In our preliminary studies we mapped trust as a degree of confidence in the *behavior* of an entity (e.g. unknown, *low*, *medium* and *high* trust). We define a *behavior*, in this case, as a security policy like a *P3P policy* or a context trustworthiness policy. Based on this mapping of degrees of trust in behaviors, users can define a trust relationship database, and use this database in policy conditions to influence decisions, for instance, in EPAL privacy policies and XACML access control policies. One example of such policies could be: “if trust degree on P3P policy is high then allow access to my location”. So far we plan to address in our architecture security policies related with privacy enforcement, identity provisioning, context trustworthiness and trust management.

We are also working on a distributed architecture to manage the trust relationships database where the concept of management domains is introduced as a tool to ease the management of dynamic trust relationships [6]. The management complexity can be reduced using domains because security policies and 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. We call these management domains “context-aware management domains” as context information is used as a dynamic parameter for domain specification. We plan to address in our architecture the following trust management tasks: analysis, evolution, recommendation and visualization.

It is an open research topic, and also an expected contribution, to define the role of context information in trust establishment and management. The idea is to provide mechanisms to define and infer the trust level of an entity based on the context information provided about that entity. In this way, entities inside of an specific context will receive different trust degrees in relation to entities outside of that

context. We plan to do this through further elaboration of the concept of context-aware management domains providing abstractions to specify dynamic domains of trust.

The main focus of this thesis will be in the practical implementation of the designed trust management architecture. For this reason, the validation and validation method are very important steps and they are also part of the research to be done. We will validate our architecture through and integrated prototype of the AWARENESS project [7], which this thesis is part of. This project will provide a fully functional context-aware service platform and we plan to contribute on the implementation efforts together with other PhD students. 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] 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.
- [3] Molva, R. and Michiardi, P. Security in Ad hoc Networks (invited paper). In: *Personal Wireless Communications*, September 23-25 2003, Venice Italy.
- [4] Grandinson, T.; Sloman, M. A Survey of Trust in Internet Applications, *IEEE Communications Surveys* 2000.
- [5] Daskapan, S.; Ali Eldin, A.; Wagenaar, R. Trust in mobile context aware systems, 5<sup>th</sup> International Business Information Management Conference, Dec 2005, Cairo, Egypt.
- [6] 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.
- [7] Architectural specification of the service infrastructure, AWARENESS project, Deliverable D2.10, December 2005, <http://awareness.freeband.nl>.