

Enforcement of Dynamic Privacy Policies in Distributed Context-Aware Systems¹

Kamran Sheikh, Maarten Wegdam, Marten van Sinderen

Centre for Telematics and Information Technology, University of Twente, P.O. Box 217,
7500 AE, Enschede, The Netherlands

sheikhk@cs.utwente.nl, wegdam@cs.utwente.nl, sinderen@cs.utwente.nl

Introduction

Context awareness refers to the ability of systems to acquire context information that describes the situation of the user and adapt themselves to this context. Such adaptation leads to the provisioning of highly personalized and unobtrusive services, but the collection, storage and dissemination of this inherently privacy sensitive context information does raise several privacy concerns. User context can be collected through a wide variety of devices which may potentially be invisible to the user. Context information can then be stored at different locations for any period of time and may even be used to infer more meaningful and, often, more privacy sensitive information [4].

A necessary precondition for the social acceptance of ubiquitous context-aware systems is the assurance that the privacy of their users is safeguarded [9]. Several systems are available to encode users' privacy preferences in the form of policies so that access control decisions can be made unobtrusively [5][6]. Context information would play a vital role in the runtime adaptation of these policies to the current situation. For example, a user wants to relay his location to colleagues only when s/he is in the office building. Several issues arise when context information is provided as input to privacy policies which are not catered to existing policy standards [5][6][8].

Goal Statement

The objective of this PhD research is to develop an unobtrusive policy-based privacy and access control solution for distributed context-aware pervasive systems. Research will be performed into the shortcomings of existing policy systems to deal with dynamic context information and how they can be overcome. Specific issues that will be dealt with in this research are explained in further detail in the following section.

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

Problem Description

Collection, storage and dissemination of context information in a privacy sensitive manner require privacy policies to be adapted to context-aware environments. This can be divided into three sub-problems.

Firstly, unlike traditional inputs to policy systems, context information is associated with certain quality characteristics collectively called Quality of Context (QoC) [2]. QoC attributes reflect the usability of the context which, in turn, mirrors the validity of the consequent policy evaluation decision. Therefore, design of an effective context-aware privacy policy infrastructure would require ways to prescribe constraints on the QoC of context, based on which policy decisions are made, e.g. the context source must be trusted, the probability of correctness of the information should be more than 60% etc. The same would hold true for context based on which personalized services might be provided. Quality attributes that we consider in this research include probability of correctness, accuracy, timeliness and trustworthiness. Current policy models do not accommodate QoC attributes.

Secondly, in current policy management solutions the evaluation of policies is binary, i.e. access is either provided or denied. This is not sufficient in the case of context information since the user's privacy preference may dictate access to a 'downgraded' (i.e., less privacy sensitive) version of the available context rather than deny access altogether. For example, a weather service requesting a user's location needs to know only the city in which s/he is in. The user's location might be available with, a much higher accuracy (e.g., 10m) but is downgraded or 'obfuscated' [7] to city level before it is provided to the weather service. Current policy systems are not equipped to handle such policies.

Thirdly, unlike traditional distributed systems, context consumers (e.g. services, user applications) in pervasive context-aware systems may need to interact with other previously unknown entities. These can be broadly classified into three types:

- Context owners about whom context is collected
- Context sources that collect and provide context
- Intermediaries; these are entities through which context information passes before reaching its final destination. The information may or may not be changed by these entities.

Traditional authorization models based on trusted credentials are too rigid in such a dynamic environment [1]. In traditional authentication models, a requester proves one or more static assertions (e.g. identity) by providing credentials (e.g. PKI or X.509) issued by a trusted authority, which enable the authenticating service to make a decision. Such a model would be insufficient in the ad-hoc environment of context-aware pervasive systems as the authenticating service may not possess any prior knowledge about the requester. Similarly, potentially unknown context sources may provide context information about clients which may traverse through equally unknown intermediaries, e.g. context inferring services. The fact that multiple and possibly conflicting values of the same context can be received from different sources further compounds the complexity of this task. If an access control decision will be made based on this context, there needs to be a trust relationship between the Policy Decision Point (PDP) of the access controller and these context sources and intermediar-

ies. Existing policy systems do not specify how constraints on trust can be expressed in privacy policies.

For these reasons we need a policy system better suited to context-aware infrastructures.

Approach

This research is being conducted as part of the Freeband AWARENESS project [3]. The AWARENESS project focuses on an infrastructure that enables rapid and easy development of context-aware and pro-active applications in a secure and privacy-conscious manner. The findings of our research will be integrated in this infrastructure to achieve the required level of user privacy and security. AWARENESS validates this infrastructure through prototyping with mobile health applications.

The aforementioned research is divided into three main segments.

1. Research into state-of-the-art policy systems and identify which of the specific requirements mentioned in the problem statement can not be fulfilled by them.
2. Define extensions to current policy systems and formulate new techniques to accommodate these issues. Develop a proof-of-concept policy framework, based on these findings, which would function as part of the AWARENESS infrastructure.
3. Evaluation of the policy framework thus developed according to the criteria identified in the first segment of the research. The framework would be validated by prototyping it as part of the AWARENESS Integrated Health Demonstrator [3].

References

- [1] G. Zhang, and M. Parashar, "Context-aware Dynamic Access Control for Pervasive Applications," In Proc. of the Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2004), San Diego, CA, USA, 2004.
- [2] T. Buchholz, A. Kupper and M. Schiffers. Quality of Context: What It Is and Why We Need It. In 10th Workshop of the HP OpenView University Association (HPOVUA'03), Geneva, Switzerland, July 2003.
- [3] Wegdam, M., AWARENESS: A project on Context AWARE mobile NETworks and ServiceS, in 14th Mobile & Wireless Communication Summit. 2005: Dresden, Germany.
- [4] Beresford, A. and F. Stajano, Location Privacy in Pervasive Computing, IEEE Pervasive Computing, vol. 2(1): pp. 46-55, 2003.
- [5] Cranor L, Langheinrich M, Marchiori M, Presler-Marshall M, Reagle J (2002) The platform for privacy preferences 1.0 (P3P1.0) specification. MIT/World Wide Web Consortium, available at <http://www.w3.org/TR/P3P>
- [6] T. Moses (ed.), OASIS eXtensible Access Control Markup Language (XACML) Version 1.1 specification, <http://www.oasis-open.org/committees/xacml/repository/cs-xacmlspecification-1.1.pdf>, 24 July 2003.
- [7] Wishart, R., Henricksen, K., Indulska, J.: Context obfuscation for privacy via ontological descriptions. In: 1st International Workshop on Location- and Context- Awareness. Volume 1678 of Lecture Notes in Computer Science., Springer (2005) 276–288

- [8] Jeffrey Schlimmer (ed.), Web-Services Policy Framework (WS-Policy) specification, <ftp://www6.software.ibm.com/software/developer/library/ws-policy.pdf>, September 2004.
- [9] Grimm, R. and Rossnagel, A.: Can P3P Help to Protect Privacy Worldwide? ACM Multimedia 2000 Workshops, Los Angeles, CA (2000) 157-160.