Available online at www.sciencedirect.com
SCIENCE DIRECT®
Science of Computer Programming 54 (2005) 49–71
Science of Computer Programming
www.elsevier.com/locate/scico

The Claim Tool Kit for ad hoc recognition of peer entities

Jean-Marc Seigneur[a,*], Christian Damsgaard Jensen[b]

[a] *Trinity College Dublin, Ireland*
[b] *Technical University of Denmark, Lyngby, Denmark*

Received 16 January 2004; received in revised form 5 May 2004; accepted 20 May 2004
Available online 23 July 2004

Abstract

In ubiquitous/pervasive computing environments, it is envisaged that computing elements—entities—will start interacting in an ad hoc fashion. The peer-to-peer (p2p) paradigm is appealing for such types of interaction especially with JXTA, which supports the development of reusable p2p building blocks, which facilitate implementation on any smart device. However, the inability to rely on a centralised authentication infrastructure, the openness of the environment and the absence of an administrator (it is assumed to be too expensive to have a skilled administrator at hand due to the large number of peers) challenge the use of legacy authentication mechanisms.

Supporting spontaneous interactions among previously unknown entities requires dynamic enrolment of strangers and unknown entities. Entity recognition (ER) is a process that is carried out each time an interaction happens between entities in order to dynamically recognise previously met entities.

In this paper, we present the Claim Tool Kit (CTK), a Java-based implementation of ER: entities exchange messages, called Claims, and rely on their associated clues to evaluate the level of confidence in recognition.

The CTK employs advanced features available with Java, such as JXTA and Java Cryptography and Security Architectures. We show that the CTK needs performance results on these features in order to increase the level of auto-configuration of the CTK. We describe how to obtain performance assessment for some of these new features. Finally, we explain how the CTK can be instrumented to take into account performance assessment. By analysing the evaluation results, the applicability of these advanced Java-based technologies for peer entity recognition is assessed.

* Corresponding address: 2850 route nationale, 74120 Megève, France.
E-mail addresses: Jean-Marc.Seigneur@trustcomp.org (J.-M. Seigneur), Christian.Jensen@imm.dtu.dk (C.D. Jensen).
URL: http://www.trustcomp.org (J.-M. Seigneur).

0167-6423/$ - see front matter
doi:10.1016/j.scico.2004.05.005

Keywords: Authentication; Ad hoc peer-to-peer; Auto-configuration; Performance

1. Introduction

Weiser's vision of ubiquitous/pervasive computing [34] will only be realised when computing capabilities are woven into the fabric of everyday life, indistinguishable from it. Major companies in the household appliance market are increasingly getting involved in smart home appliances—appliances with communication, computation and storage capabilities. An appealing candidate technology for the implementation of these smart appliances is JXTA [13], which provides reusable peer-to-peer (p2p) building blocks facilitating implementation on any smart device. The mission of an ambient intelligence (AmI) environment is to enhance the space. However, challenges remain for the fulfilment of this mission in AmI environments. Auto-configuration and autonomy, especially from a security point of view [25], form part of these challenges. Billions of entities—potentially any smart device—are expected to spread in the surrounding environment. If the enrolment of all these entities always requires human intervention, the mission to enhance the space is defeated because it makes busy householders even busier. In addition, in home environments, no skilled administrator is present (because it is assumed to be economically non-viable to have an administrator at hand at all times [25]) and often most of the users are technology-unaware people. This absence of an administrator combined with the impossibility of relying on a centralised authentication infrastructure, the openness and the large scale of the environment challenge the use of legacy authentication mechanisms. This is especially true in unstructured p2p systems [33], which do not assume centralised directories and precise control over network topology or data placement.

A fundamental question concerns the representation of entities including their naming and subsequent identification as well as their association with real-world principals. We believe that, in this context, it is more beneficial to take an approach based on entity recognition (ER) [26], rather than traditional authentication schemes. A fundamental requirement for ubiquitous computing environments is to allow for potential interaction with unknown entities [26]. In public environments, there is no so-called list of known people to be enrolled. People roam from one space to another as they wish. This introduces the requirement for smooth dynamic enrolment to get the full benefits from spontaneous interactions with previously unknown entities, that is, the door should not be closed to strangers, but instead any stranger showing up at the door might become an acquaintance.

To allow for dynamic enrolment of strangers and unknown entities, we have proposed an entity recognition (ER) process [26], which consists of four steps:

(1) Triggering of the recognition mechanism.
(2) Detective Work to recognise the entity using the available recognition scheme(s).
(3) Discriminative Retention of information relevant for possible recall or recognition.
(4) Upper-level Action based on the outcome of recognition including a level of confidence in recognition.