Available online at www.sciencedirect.com

SCIENCE DIRECT®

Computer Standards & Interfaces 27 (2005) 533–545

COMPUTER STANDARDS & INTERFACES

www.elsevier.com/locate/csi

Evidence processing and privacy issues in evidence-based reputation systems

Daniel Cvrček[a,1,2], Václav Matyáš Jr.[b,2,3], Ahmed Patel[c,*]

[a]*Computer Laboratory, University of Cambridge, 15 JJ Thomson Av., CB3 0FD, Cambridge, United Kingdom*
[b]*Masaryk University Brno, Botanicka 68b, Brno, 602 00, Czech Republic*
[c]*University College Dublin, Belfield, Dublin 4, Ireland*

Available online 30 January 2005

Abstract

Issues related to processing of evidence in evidence-based reputation systems, with a particular concern for user privacy, are discussed in our paper. The novel idea of evidence-based reputation (or trust) systems is that such systems do not rely on an objective knowledge of user identity. One has instead to consider possible privacy infringements based on the use of data (evidence) about the previous behaviour of entities in the systems. We provide a brief introduction to evidence-based trust/reputation systems, as well as to the privacy issues, addressing the common problem of many papers that narrow the considerations of privacy to anonymity only. We elaborate on the concept of pseudonymity through aspects of evidence storing and processing. This, together with a consideration of current work on trust models, leads to our specification of requirements for the trust model for evidence-based systems supporting pseudonymity.

Keywords: Evidence processing; Privacy; Pseudonymity; Trust model

1. Introduction

The emergence of the Internet has provided an unprecedented ability for people to browse and visit many different electronic places. However, this real-time connectivity has resulted in significant threats to individual privacy. The same mechanisms that underpin the power of on-line services can also be used, sometimes without the users' knowledge or consent, to collect sensitive information about an individual or their service usage behaviour. Powerful data collection techniques, users' inability to know what is being collected or how to stop it, combined sometimes with media exposure of perceived "bad actors" in privacy, have resulted in an increasing lack of trust among on-line service users. The manner in which the service collects information about consumers is at the root of

* Corresponding author.
E-mail address: apatel@cnds.ucd.ie (A. Patel).

[1] Supported by the EU project SECURE (Secure Environments for Collaboration among Ubiquitous Roaming Entities), IST-2001-32486.

[2] Supported in part by the EU Network of Excellence FIDIS (Future of IDentity in the Information Society), 507512.

[3] Work undertaken during visits to University College Dublin and Microsoft Research Cambridge.

0920-5489/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2005.01.011

the privacy problem: how much information should they collect, how much should they use, and how much, if any, should they share with other vendors and partners?

On the other side, there is a strong research effort in the area of large distributed systems, ubiquitous computing, and peer-to-peer networks, with the main goal to make communication and computation as effective as possible. This is clear threat deteriorating privacy of users beyond today's reality. This paper reviews some of the privacy-related requirements for trust reasoning in a distributed environment typical for ubiquitous systems with no centralised database or infrastructure for trust management and proposes requirements for a suitable trust model applicable in such environments. A typical example of such systems would involve mobile users or a P2P network of cooperating entities. Privacy demanding clients, for whom we typically cannot implicitly share personal information, are considered here. This work extends our findings and considerations presented in Ref. [8].

1.1. System model

The reasoning introduced in this paper is based on the following general idea of reputation (or trust) systems. Systems do not utilize enrolment of users—there is no objective knowledge about their identities [6]. All the systems can use is evidence about previous behaviour of digital identities. Functionally, there are three types of nodes in the system. First, *requesters–clients* are exploiting services and resources offered by the second type of nodes—*servers*. Servers may use the recommendation service of *recommenders*—the third type of nodes that have an interaction history with requesters. Kinateder and Pearson [17] use a slightly refined description of recommenders as they define recommender with their own experiences and accumulator with mediated evidence.

Each user may use a large amount of digital identities (pseudonyms) and each pseudonym may be connected to transactions spread across the system. These facts imply the possibility of a number of different trust values, which are *valid* for one physical identity. We cannot, and often do not even want to, prevent this to preserve certain level of privacy. On the other side, we need to get the description of the user (not only her digital identity) as accurate as possible. Each system incorporating reputation/trust is based on two paradigms:

(1) *Local trustworthiness evaluation* allows any node[4] to make use of behavioural evidence and determine the trustworthiness of users.
(2) *Distribution of trust* makes it possible for nodes to propagate their local results of trust evaluations to other nodes in the network.

There are systems that do not support mechanisms for trust propagation. Such systems introduce high independence of trustworthiness of single digital identities in different parts of a network. Such systems loose advantage of distributed computing and it may be the case that their trust evaluation will suffer from many more wrong decisions because of partial information. It is a challenging task to find the limits of such systems with respect to privacy properties that may allow for existence of many identities of particular users. It seems obvious that such systems will be also much more vulnerable to distributed attacks because of limited ways to spread knowledge about malicious identities or ongoing attacks. When we enhance trust-based model with indirect evidence (i.e. evidence observed by someone else) we may get to the situation with only small anomalies of trust values that are otherwise quite coherent throughout the network.

1.2. Trust and reputation

Many papers confuse the notions of trust and reputation. The use of the words seems to distinguish two groups of people working towards the same target—trust-driven security mechanisms. The first group comes from the area of ubiquitous computing and distributed system architecture for global computing is their concern. Here, the reasoning about trust is rather abstract [1,4,15]. The second group is more application oriented, concerned with peer-to-peer systems. They tend to see trust as a new, interesting idea on how to enrich security mechanisms. The

[4] Let us call active entities as *nodes* as they are elements of a network. Users are not only nodes but also external entities accessing resources of the network.