AI Communications 25 (2012) 377–379
DOI 10.3233/AIC-2012-0521
IOS Press

Thesis

Enhancing privacy in Multi-agent Systems

Jose M. Such

Departament de Sistemes Informàtics i Computació, Universitat Politècnica de València, València, Spain
E-mail: jsuch@dsic.upv.es

Abstract. In this thesis, we focus on avoiding undesired information collection and information processing in Multi-agent Systems. In order to avoid undesired information collection we propose a decision-making model for agents to decide whether disclosing personal information to other agents is acceptable or not. We also contribute a secure Agent Platform that allows agents to communicate with each other in a confidential fashion. In order to avoid undesired information processing, we propose an identity management model for agents in a Multi-agent System. This model avoids undesired information processing by allowing agents to hold as many identities as needed for minimizing data identifiability.

Keywords: Privacy, Multi-agent Systems, autonomous agents

1. Introduction

Nowadays, in the era of global connectivity (everything is inter-connected anytime and everywhere) with more than 2 billion users with connection to the Internet as of 2011,[1] privacy is of great concern. Autonomous agents play a crucial role to safeguard and preserve their principals' privacy [3]. This is because agents encapsulate personal information of their principals. They usually have a detailed profile of their principals' names, preferences, roles in organizations and institutions, location, transactions performed and other personal information. Agents carry out interactions on behalf of their principals so that they usually exchange personal information of their principals. This may raise privacy concerns, because this exchange of personal information can produce a potential loss of privacy.

In this thesis, we focus on avoiding two information related activities that can represent a major threat for principals' privacy: (i) information collection, which refers to the process of gathering and storing data about an individual; and (ii) information processing, which refers to the use or transformation of data that has been already collected.

[1] http://www.internetworldstats.com/stats.htm.

2. Avoiding information collection

2.1. Self-disclosure decision making

A first important approach to prevent information collection is to decide exactly which information to disclose to which other agents. That is, agents should be able to decide whether disclosing personal data attributes to other agents is acceptable or not. Thus, agents need self-disclosure decision-making mechanisms that help them in these situations.

We proposed a self-disclosure decision-making model based on intimacy and privacy measures to deal with these situations [5]. Our model considers psychological findings regarding how humans disclose personal information in the building of their relationships, such as the well-studied *disclosure reciprocity* phenomenon. This phenomenon is based on the fact that one person's disclosure encourages the disclosure of the other person in the interaction, which in turn, encourages more disclosures from the first person.

Intimacy accounts for the information gain of all the messages received from another agent. Privacy accounts for the information loss caused by sending a message valuated with the sensitivity of the information disclosed. Agents choose to disclose information that maximizes the estimation of the increase in in-

timacy while at the same time minimizing the privacy loss. Moreover, agents consider how balanced their relationships are, i.e., they may decide not to perform disclosures to agents that do not reciprocate them with more disclosures (following the reciprocity phenomenon).

2.2. Secure agent platform

Once an agent has decided which information to disclose to which other agent, this information must be protected from accesses from any other third parties different from the agent to which the information is directed to. This includes parties from their local computer and network but also different locations, even across the Internet. We contribute a secure Agent Platform (AP) that allows agents to interact to each other in a secure fashion [2]. To this aim, our secure AP provides authorization mechanisms based on mandatory access control (agents are confined to access a subset of their principals' permissions), and encryption and decryption of messages exchanged based on Kerberos.[2] Moreover, our secure AP allows agents to authenticate to each other without disclosing their principals' identities. Agents have their own identities that act as pseudonyms for their principals. Our secure Agent Platform keeps track of the association between principal and agent identities. Therefore, principal identities can be obtained for accountability concerns, such as law enforcement.

3. Avoiding information processing

In order to avoid undesired information processing, we proposed an identity management model for agents in a Multi-agent System [4]. Our model is based on current Privacy-enhancing Identity Management Systems and uses partial identities as a key concept for identifying entities (agents and principals). In a nutshell and informally speaking, a partial identity can be seen as a pseudonym (an identifier of a subject other than one of the subject's real name) and a set of attributes attached to it.

Our model avoids undesired information processing without compromising accountability and other crucial aspects such as trust and reputation. Specifically, we proposed two kinds of partial identities: regular and permanent. On the one hand, agents can hold an unlimited number of regular partial identities. Therefore, agents can use as many regular partial identities as needed to minimize data identifiability, and thus, they are able to minimize information processing. On the other hand, each agent cannot hold more than one permanent partial identity. Because of this, the vulnerabilities of trust and reputation models due to whitewashing (identity change) and Sybil attacks (multiple identities) are avoided. Moreover, both kinds of partial identities provide a baseline privacy preservation because they hide the real identity of the user that is behind an agent. However, the real identity of the user can be disclosed if the agent misbehave. As a result, accountability is also preserved.

Based on this model, we propose a software architecture that supports the development and execution of privacy-enhancing Multi-agent Systems in which trust and reputation play a crucial role. Our proposed architecture integrates an implementation of our privacy-enhancing agent identity management model into the Agent Platform. As a result, the Agent Platform relies on trusted third party identity providers for partial identity issuing and validation. The Agent Platform also automates the process of obtaining permanent and regular partial identities from users' real identities. It is also in charge of creating the needed credentials for securing agent communications.

4. Conclusions and future work

In this thesis, we focus on avoiding undesired information collection and information processing in Multi-agent Systems. As future work, we would like to tackle the problem of information dissemination. Information dissemination refers to the transfer of collected (and possibly processed) data to other third parties. The whole PhD thesis can be consulted in [1].

Acknowledgements

Jose M. Such was awarded a predoctoral fellowship from Generalitat Valenciana (BFPI06/096). This work has also been partially supported by CONSOLIDER-INGENIO 2010 under Grant CSD2007-00022.

References

[1] J.M. Such, Enhancing privacy in multi-agent systems, PhD thesis, Universitat Politecnica de Valencia, Spain, 2011, available at: http://gti-ia.upv.es/sma/thesis/pdf/tesisJSuch.pdf.

[2] http://web.mit.edu/kerberos/.

[2] J.M. Such, J.M. Alberola, A. Espinosa and A. García-Fornes, A group-oriented secure multiagent platform, *Software Pract. Exp.* **41**(11) (2011), 1289–1302.
[3] J.M. Such, A. Espinosa and A. García-Fornes, A survey of privacy in multi-agent systems, *Knowl. Eng. Rev.* (2012), to appear.
[4] J.M. Such, A. Espinosa, A. García-Fornes and V. Botti, Partial identities as a foundation for trust and reputation, *Eng. Appl. Artif. Intell.* **24**(7) (2011), 1128–1136.
[5] J.M. Such, A. Espinosa, A. García-Fornes and C. Sierra, Self-disclosure decision making based on intimacy and privacy, *Inform. Sci.* **211** (2012), 93–111.