A Novel Method to Maintain Privacy in Mobile Agent Applications

Kun Peng, Ed Dawson, Juanma Gonzalez Nieto, Eiji Okamoto, and Javier López

Information Security Institute,
Queensland University of Technology
{k.peng, juanma, e.dawson}@qut.edu.au
http://www.isrc.qut.edu.au/people/pengk

Abstract. Two methods to implement privacy in network communication, anonymity and DCSC (data confidentiality and secure computation) are analysed and compared in regard to privacy in mobile agent applications. It is illustrated that privacy through DCSC is more suitable in mobile agent applications. To support this conclusion, privacy is concretely implemented in a bidding mobile agent scheme in this paper. Success of this example demonstrates that privacy can be practically achieved in mobile agent applications through DCSC without compromising the advantage of mobile agent.

Keywords: Mobile agent, privacy, DCSC, secure computation.

1 Introduction

Mobile agents [9, 8, 19, 20] are autonomous software entities that relay code, data and state through multiple nodes. Usually, an originator generates the mobile agent and sends it out to collect data, which is then used by the originator for a special purpose. The advantage of mobile agent is that it is a real-time service, so can visit dynamically chosen nodes to collect data instantly. For example, with the help of a bidding mobile agent, a buyer (seller) can instantly get the bids from a dynamic set of bidders. Then he can immediately choose one bid as the winning bid. Compared to the traditional e-auction schemes [12, 15, 17], a bidding-mobile-agent-based auction is more instant, flexible and convenient.

Usually, compared to traditional network applications like traditional e-auction and e-voting [14, 2, 10, 11], a mobile agent application has the following properties.

- Dynamic: the nodes in the communication network are usually temporally connected terminals fitted with a relay function.
- Instant: network service must be available instantly without preparation or delay.
- Flexible: various nodes and communication patterns may be involved.

Y.G. Desmedt et al. (Eds.): CANS 2005, LNCS 3810, pp. 247–260, 2005.

With these properties, mobile agent has its advantage in circumstances where dynamic and instant network services are needed. Without these properties, mobile agent has no advantage over the traditional network applications.

As the nodes usually may want to conceal their personal privacy in mobile agent applications, in certain cases no node may permit his identity to be linked to his data. More precisely, a node's privacy is the unlinkability between his identity and his data. A definition of privacy in a mobile agent application is as follows.

Definition 1. *A mobile agent application is private if no node's data can be linked to its identity.*

For example, a bidding mobile agent application is private if except for the winner no bidder can be linked to its bid. The only known private mobile agent schemes are [19, 20], two bidding agents. In [19, 20], privacy is implemented through anonymity of the nodes, a method which is inefficient and inconsistent with the properties and advantages of mobile agent application. So designing practical privacy mechanism in mobile agent application is a challenging task. The design must take into account the important fact that as a real-time network application mobile agent has its advantages, which should not be sacrificed in the implementation of privacy.

In this paper, a new privacy mechanism is proposed in mobile agent scheme. The new mechanism, called DCSC, employs data confidentiality and secure computation to achieve privacy in network communication. Basing privacy on data confidentiality and secure computation is not a new idea. For example, it is widely applied to traditional network applications like electronic auction [12, 15] and e-voting [10, 11]. Although this privacy mechanism has not been applied to mobile agent schemes, it has some advantages in regard to mobile agent over the privacy mechanism based on anonymity. The DCSC privacy mechanism is more efficient and does not conflict with the advantages of mobile agent applications. So it is more suitable to mobile agent than the privacy mechanism based on anonymity. DCSC is applied to a new bidding mobile agent scheme with the same circumstance as [19, 20]. The new bidding mobile agent scheme illustrates that privacy can be practically achieved in mobile agent applications without compromising its advantages.

The remainder of this paper is organised as follows. In Section 2, privacy in network communication is analysed and two privacy mechanisms are compared. It is shown that DCSC privacy has its advantages in some applications. In Section 3, it is illustrated that DCSC privacy is more suitable for privacy in mobile agent and often the only feasible solution for private mobile agent application. In Section 4, secure computation techniques are introduced to support DCSC. Especially, an efficient secure computation technique to be used later in the paper, ciphertext comparison, is recalled. In Section 5, a concrete application of DCSC privacy in mobile agent, private bidding mobile agent, is designed on the base of ciphertext comparison. In Section 7, the paper is concluded.