Chapter 2.15
Privacy-Preserving Transactions Protocol Using Mobile Agents with Mutual Authentication

Song Han
Curtin University of Technology, Australia

Vidyasagar Potdar
Curtin University of Technology, Australia

Elizabeth Chang
Curtin University of Technology, Australia

Tharam Dillon
University of Technology, Australia

ABSTRACT

This article introduces a new transaction protocol using mobile agents in electronic commerce. The authors first propose a new model for transactions in electronic commerce, mutual authenticated transactions using mobile agents. They then design a new protocol by this model. Furthermore, the authors analyse the new protocol in terms of authentication, construction, and privacy. The aim of the protocol is to guarantee that the customer is committed to the server, and the server is committed to the customer. At the same time, the privacy of the customer is protected.

INTRODUCTION

Security and Privacy are the paramount concerns in Electronic Commerce (Eklund, 2006). Mobile agent systems are becoming involved in e-commerce (Claessens, Preneel, & Vandewalle, 2003). However, security and privacy within mobile agents must be addressed before mobile agents can be used in a wide range of electronic commerce applications.

The security in the electronic transactions with mobile agents can be classified into two different aspects:

- One is the security of the hosts, to which the mobile agents will travel
- The other is the security of the mobile agents, by which some sensitive information may be transported to the hosts.

The above first security is used to protect the hosts, since the mobile agents may be malicious. For example, the mobile agent may be in the disguise of a legal mobile agent. Therefore, the host will interact with the mobile agent on an electronic transaction. However, the mobile agent tries to obtain some sensitive information (e.g., the secret development plan, the financial report, etc.) about the host. This case will damage the benefit of the host. Therefore, it is very important to maintain the security of the host if some malicious mobile agents travel to the hosts.

The above second security is used to protect the mobile agents, since the hosts may be hostile. For example, when the mobile agents with some sensitive information arrive at the host, those pieces of sensitive information (e.g., the private key, bank account password, home address, etc.) are of paramount importance to the mobile agents' owner. Therefore, the host may try to attain the information through interacting with the mobile agents. As a result, the customer (the owner of the mobile agents) may be blackmailed by the host, since the host holds some sensitive information obtained from the underlying mobile agents. Therefore, it is imperative to design some security mechanism to maintain the security of the mobile agents.

Hosts' security mechanisms include: (1) authentication; (2) verification; (3) authorisation; and (4) payment for services (Claessens et al., 2003). In this article, we will utilise the method of authentication to preserve the security of the host. Authentication is one of the cryptographic techniques. The implication of authentication is to *assure that the entity (customer, host, mobile agents, etc.) requesting access or interaction is the entity that it claims to be.*

Mobile agents' security mechanisms (Kotzanikolaou, Burmester, & Chrissikopoulos, 2000) include: (1) authentication; (2) encryption algorithms; and (3) digital signatures. In this article, we will utilise the digital signature technique. Digital signature is another cryptographic technique. A digital signature scheme is a method of signing a message stored in electronic form. As such, a signed message can be transmitted over a computer network. Also, a signature can be verified using a publicly known verification algorithm. Therefore, anyone who knows the verification algorithm can verify a digital signature. The essence of digital signatures is to convince the recipient that a message (attached to its valid digital signature) is really sent from the signer.

In a virtual community, delegation of signing rights is an important issue since security and privacy are concerned. Consider the following scenario: An international logistics company, AuHouse's President is scheduled to sign a major contract with an Automobile Company in Europe on February 28. However, because of a management emergency, the President is required to attend a meeting held in the General Building of AuHouse in Australia on the same day. This meeting is vital to the future of the AuHouse. However, the contract in Europe is also very important to the organisation. How then can the President be in two places at once and sign the contract, even though he cannot be physically in Europe? Undetachable signature protocol will help the President to solve this issue since the undetachable signature protocol can provide the delegation of signing power while preserving the privacy of the President.

Undetachable signatures are one of the digital signatures which could provide secure delegation of signing rights while preserving privacy. So far only a few undetachable signatures have been created (Coppersmith, Stern, & Vaudenay, 1993; Kotzanikolaou et al., 2000; Sander & Tschudin, 1998). Sander and Tschudin (1998) first proposed the undetachable signatures. The construction is