IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com
ITB8712

Chapter 23

An Architecture for Authentication and Authorization of Mobile Agents in E-Commerce

Wee Chye Yeo, Sheng-Uei Guan, and Fangming Zhu
National University of Singapore

ABSTRACT

Agent-based e-commerce is a new technology being researched extensively by many academic and industrial organizations. The mobility and autonomy properties of agents have offered a new approach of doing business online. To fully exploit the advantages of this new technology, a secure system to authenticate and authorize mobile agents must be in place. In this chapter, an architecture to ensure a proper authentication and authorization of agents has been proposed. The Public Key Infrastructure (PKI) is used as the underlying cryptographic scheme. An agent is digitally signed by the Agent Factory and its signature is authenticated at hosts using the corresponding public key. Agents can also authenticate the hosts to make sure that they are not heading to a wrong place. When an agent visits a host, agent's expiry date, host trace, and the factory's trustworthiness are checked during the authentication process. According to the level of authentication that the incoming agent has passed, the agent will be categorized and associated with a relevant security policy during the authorization phase. The corresponding security policy will be enforced on the agent to restrict its operations at the host. The prototype has been implemented with Java.

INTRODUCTION

With the increasing world-wide usage of the Internet, electronic commerce (e-commerce) has been catching on fast in a lot of businesses. As e-commerce booms, there comes a demand for a better system to manage and carry out transactions. This has led to the development of agent-based e-commerce. In this new approach, agents are employed on behalf of users to carry out various e-commerce activities, such as auction, brokering, negotiation, payment, etc.

Although the tradeoff of employing mobile agents is still a contentious topic (Milojicic, 1999), using mobile agents in e-commerce attracts much research effort as it may improve the potential of their applications in e-commerce. There are many advantages for employing mobile agents. First, communication cost can be reduced, because the agents will travel to the destination and transfer only the necessary information. This saves the bandwidth and reduces the chances of clogging the network. Second, users can let their agents travel asynchronously to their destinations and collect information or execute other applications while the user can disconnect from the network (Wong, Paciorek, & Moore, 1999).

Having seen the advantages of this emerging technology, the major factor that is still holding people back from employing agents in e-commerce is the security issues involved. On the one hand, hosts cannot trust incoming agents belonging to unknown owners, because malicious agents may launch attacks on the hosts and other agents. On the other hand, agents may also have concerns on the reliability of hosts and will be reluctant to expose their secrets to distrustful hosts.

There are two broad categories of security issues to be considered in the research field of mobile agents: misuse of hosts by mobile agents and misuse of mobile agents by hosts or other mobile agents. In the first category, a host is exposed to attacks from visiting agents. The various kinds of attacks include theft of information, denial of services, damage to local resources, etc. For instance, with the attack of denial of services, a malicious agent may overload some local resource or service, blocking the host's access to other agents or applications. In the scenario of the second category, when an agent is executing in a malicious host's environment, it is exposed to possible attacks from that host and other agents residing in the host.

To build bilateral trust in an e-commerce environment, the authorization and authentication schemes for mobile agents should be well designed. Authentication checks the credentials of an agent before processing the agent's requests. If the agent is found to be suspicious, the host may decide to deny its service requests. Authorization refers to the permissions granted for the agent to access whichever resource it requested. The Public Key Infrastructure (PKI) is used as the basic cryptographic method in our design, and Java is selected as the implementation language. Digital signature is used for authentication purpose, and authorization is achieved using the security manager provided by Java. To restrict the access to resources, user-defined security policies have to be designed and used in conjunction with the security manager. Based on the authentication results, the host can decide the type of privileges to offer to various authenticated agents.

In our previous work, we have proposed a Secure Agent Fabrication, Evolution & Roaming (SAFER) architecture (Zhu, Guam, & Yang, 2000), which aims to construct an open, dynamic and evolutionary agent system for e-commerce. It provides a framework for agents in e-commerce and establishes a rich set of mechanisms to manage and secure them. We have already elaborated agent fabrication, evolution, and roaming in Guan and Zhu (2001), Guan, Zhu, and Ko (2000), Wang, Guam, and Chan (2001), Zhu and Guan (2001), and Guan and Yang (1999). This chapter elaborates the design and implementation of authentication and authorization issues on the basis of the SAFER architecture.

The remainder of the chapter is organized as follows. Section 2 presents background on agent-based e-commerce, mobile agent systems, and PKI. Section 3 elaborates the design of agent authentication and authorization. Section 4 describes the implementation of the proposed design. Section 5 discusses the advantages and limitations of the implemented approach in comparison with the related work. The final section concludes the chapter and discusses the possible future work.