Chapter 7.10
Integrity Protection of Mobile Agent Data

Sheng-Uei Guan
Brunel University, UK

INTRODUCTION

One hindrance to the widespread adoption of mobile-agent technology is the lack of security. Security will be the issue that has to be addressed carefully if mobile agents are to be used in the field of electronic commerce. SAFER (secure agent fabrication, evolution and roaming) is a mobile-agent framework that is specially designed for the purpose of electronic commerce (Guan & Hua, 2003; Guan, Zhu, & Maung, 2004; Zhu, Guan, Yang, & Ko, 2000). Security has been a prime concern from the first day of our research (Guan & Yang, 2002; Yang & Guan, 2000). By building strong and efficient security mechanisms, SAFER aims to provide a trustworthy framework for mobile agents to assist users in conducting mobile or electronic-commerce transactions.

Agent integrity is one such area crucial to the success of agent technology (Wang, Guan, & Chan, 2002). Despite the various attempts in the literature, there is no satisfactory solution to the problem of data integrity so far. Some of the common weaknesses of the current schemes are vulnerabilities to revisit attacks, when an agent visits two or more collaborating malicious hosts during one roaming session, and illegal modification (deletion or insertion) of agent data. The agent monitoring protocol (AMP; Chionh, Guan, & Yang, 2001), an earlier proposal under SAFER to address agent data integrity, does address some of the weaknesses in the current literature. Unfortunately, the extensive use of PKI (public-key infrastructure) technology introduces too much overhead to the protocol. Also, AMP requires the agent to deposit its data collected to the agent owner or butler before it roams to another host. While this is a viable and secure approach, the proposed approach, Secure Agent Data Integrity Shield (SADIS), will provide an alternative by allowing the agent to carry the data by itself without depositing them (or the data hash) onto the butler.

Besides addressing the common vulnerabilities of current literature (revisit attacks and data-modification attacks), SADIS also strives to achieve maximum efficiency without compromising security. It minimizes the use of PKI technol-

ogy and relies on symmetric key encryption as much as possible. Moreover, the data encryption key and the communication session key are both derivable from a key seed that is unique to the agent's roaming session in the current host. As a result, the butler can derive the communication session key and data encryption key directly. Another feature in SADIS is strong security.

Most of the existing research works focus on detecting integrity compromise (Esparza, Muñoz, Soriano, & Fomé, 2006) or bypassing integrity attacks by requiring the existence of a cooperating agent that is carried out within a trusted platform (Ouardani, Pierre, & Boucheneb, 2006). However, these works neglect the need to identify the malicious host. With SADIS, the agent butler will not only be able to detect any compromise to data integrity, but will identify the malicious host effectively.

BACKGROUND

Agent data integrity has been a topic of active research in the literature for a while. SADIS addresses the problem of data integrity protection via a combination of techniques discussed by Borselius (2002): execution tracing, encrypted payload, environmental key generation, and undetachable signature.

One of the recent active research works is the security architecture by Borselius, Hur, Kaprynski, and Mitchell (2002). Their architecture aims at defining a complete security architecture designed for mobile-agent systems. It categorizes security services into the following: agent management and control, agent communications service, agent security service, agent mobility service, and agent logging service. SADIS addresses the agent communication service as well as agent security services (integrity protection), while previous research on SAFER addresses agent mobility service.

While many of the security services are still under active research, the security mechanisms for protecting agents against malicious hosts were described by Borselius, Mitchell, and Wilson (2001). The paper proposes a threshold scheme to protect mobile agents. Under the mechanism, a group of agents is dispatched to carry out the task, with each agent carrying a vote. Each agent is allowed to contact a merchant independently and gathers a bid based on the given criteria. Each agent votes for the best bid (under a trading scenario) independently. If more than n out of m ($m > n$) agents vote for the transaction, the agent owner will agree to the transaction.

Such a mode of agent execution effectively simplifies agent roaming by allowing one agent to visit one merchant only. While the approach avoids the potential danger of having the agent compromised by the subsequent host, it does not employ a mechanism to protect the agent against the current host. Most important of all, the threshold mechanism's security is based on the probability that no more than n hosts out of m are malicious. In another words, the security is established based on probability. Different from this approach, SADIS's security is completely based on its own merits without making any assumption about probability of hosts being benign or malicious. This is because the author believes that in an e-commerce environment, security should not have any dependency on probability.

Other than the research by Borselius (2002), Borselius et al. (2002), and Borselius et al. (2001), there are related research works in the area. One such research work on agent protection is SOMA (Secure and Open Mobile Agent) developed by Corradi, Cremonini, Montanari, and Stefanelli (1999). It is a Java-based mobile-agent framework that provides for scalability, openness, and security on the Internet. One of the research focuses of SOMA is to protect the mobile agent's data integrity. To achieve this, SOMA makes use of two mechanisms: the multihop (MH) protocol and trusted third party (TTP) protocol. The MH