Secure Agent Roaming under M-Commerce

Sheng-Uei Guan
Brunel University, UK

INTRODUCTION

The focus of this article is secure transport of mobile agents. A mobile agent is useful for hand phones or handheld devices (e.g., palmtop or PDA) equipped with mobile capabilities. Such m-commerce devices usually have limited computing power. It would be useful if the users of such devices could send an intelligent, mobile agent to remote machines to carry out complex tasks like product brokering, bargain hunting, and information collection.

An intelligent agent is one solution to providing intelligence in m-commerce. But having an agent that is intelligent is insufficient. There are certain tasks that are unrealistic for agents to perform locally, especially those that require access to a huge amount of remote information while local processing power and storage is limited. Therefore, it is important to equip intelligent agents with roaming capability.

Unfortunately, with the introduction of roaming capability, more security issues arise (Guan & Yang, 2004). As the agent needs to move among external hosts to perform its tasks, the agent itself becomes a target of attack. The data collected by agents may be modified, the credit carried by agents may be stolen, and the mission statement on the agent may be changed. As a result, transport security is an immediate concern to agent roaming. The SAFE (Secure roaming Agent For E-commerce) transport protocol is designed to provide a secure roaming mechanism for intelligent agents to satisfy their needs to roam from hosts to hosts for remote data collection or processing when local storage or computing power is limited. In SAFE, both general and roaming-related security concerns are addressed carefully. Furthermore, several protocols are designed to address different requirements. An m-commerce application can choose the protocol that is most suitable based on its need.

BACKGROUND

There has been a lot of research done in the area of intelligent agents, focusing on various aspects of agents (Guilfoyle, 1994; Johansen, Marzullo, & Lauvset, 1999). Unfortunately, there is no standardization in the various proposals, resulting in vastly different agent systems. Efforts were made to standardize some aspects of agent systems so that different systems can inter-operate with each other. Knowledge representation and exchange is one of the aspects of agent systems for which KQML (Knowledge Query and Manipulation Language) (Finin & Weber, 1993) is one of the most widely accepted standards. Developed as part of the *Knowledge Sharing Effort,* KQML was designed as a high-level language for runtime exchange of information between heterogeneous systems. Unfortunately, KQML was designed with little security considerations because no security mechanism is built to address common security concerns, not to mention specific security concerns introduced by mobile agents. Agent systems using KQML will have to implement security mechanisms on top of KQML to protect the agents.

While KQML acts as a sufficient standard for agent representation, it does not touch upon the security aspects of agents. In an attempt to equip KQML with 'built-in' security mechanisms, Secret Agent was proposed by Thirunavukkarasu, Finin, and Mayfield (1995).

Secret Agent defines a security layer on top of KQML. Applications will have to implement some special message format in order to make use of Secret Agent. Secret Agent has a number of shortcomings and is handicapped by the design of KQML. Firstly, one requirement of Secret Agent is that every agent implementing the security algorithm must possess a key (master key). This master key is either a symmetric key or based on Public Key Infrastructure (PKI).

Copyright © 2008, IGI Global, distributing in print or electronic forms without written permission of IGI Global is prohibited.

If the key is based on a symmetric key algorithm, it requires each agent to have a separate key with every other agent it corresponds with. If the agent intends to communicate with another agent with which it has no common pre-established master key, a central authentication server is required to generate such a key. The problems introduced by the implementation of the secret agent, therefore, are key database management, authentication server protection, and key transport/exchange security.

If the master key is based on PKI, the agent identity must be tightly tied with the key pair. This was insufficiently addressed in the design of Secret Agent, subjecting the algorithm to man-in-the-middle attack. For example, when agent 006 and 007 starts a handshake, if a third agent 003 can intercept all messages between 006 and 007, agent 003 can pretend to be agent 006 while talking to agent 007, and vice versa. If key and ID are not tightly integrated (like that in digital certificate), there is almost no way agent 006 or 007 can detect this attack. In the SAFE transport protocol, agent identity and key pair are tightly tied using digital certification.

Another prominent transportable agent system is Agent TCL developed at Dartmouth College (Gray, 1997; Kotz et al., 1997). Agent TCL addressed most areas of agent transport by providing a complete suite of solutions. Its security mechanism aims at protecting resources and the agent itself. In terms of agent protection, Gray (1997) acknowledged that "it is clear that it is impossible to protect an agent from the machine on which the agent is executing…it is equally clear that it is impossible to protect an agent from a resource that willfully provides false information." As a result, the author "seeks to implement a verification mechanism so that each machine can check whether an agent was modified unexpectedly after it left the home machine" (Gray, 1997). The other areas of security, like nonrepudiation, verification, and identification, were not carefully addressed.

Compared with the various agent systems discussed above, SAFE is designed to address the special needs of m-commerce. The other mobile agent systems are either too general or too specific to a particular application. By designing SAFE with m-commerce application concerns in mind, the architecture will be suitable for m-commerce applications. The most important concern is security as discussed in previous sections. Due to the nature of m-commerce, security becomes a prerequisite for any successful m-commerce application. The other concerns are mobility, efficiency, and interoperability. In addition, the design allows certain flexibility to cater to different application needs.

SECURE AGENT TRANSPORT

General Agent Transport

As a prerequisite, each SAFE entity must carry a digital certificate issued by the SAFE Certificate Authority, or SCA. In this way, each agent, agent owner, and host will carry its own unique digital certificate. The certificate itself is used to establish the identity of a SAFE entity. Because the private key to the certificate has signing capability, this allows the certificate owner to authenticate itself to the SAFE community. An assumption is made that the agent private key can be protected by function hiding (Baldi, Ofek, and Yung, 2003).

General Message Format

In SAFE, agent transport is achieved via a series of message exchanges. The format of a general message is as follows:

SAFE Message = Message Content + Timestamp + Sequence Number + MD(Message Content + Timestamp + Sequence Number) + Signature(md) (1)

The main body of a SAFE message comprises message content, a timestamp, and a sequence number. The message content is defined by individual messages. Here MD stands for the Message Digest function (elaborated in equation (2) shortly). The first 'MD' is the function applied to Message Content, Timestamp, and Sequence Number to generate a message digest. The second 'MD' in the equation is the application of a digital signature to the message digest generated. A timestamp contains the issue and expiry time of the message.

To prevent replay attack, message exchanges between entities during agent transport are labeled according to each transport session. A running sequence number is included in the message body whenever a new message is exchanged. In this way, if a message

6 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/secure-agent-roaming-under-commerce/13527

Related Content

Review of Security in VANETs and MANETs
Mai Abu Baqar, Hamza Aldabbas, Tariq Alwadan, Mai Alfawairand Helge Janicke (2014). *Network Security Technologies: Design and Applications (pp. 1-27).*
www.irma-international.org/chapter/review-of-security-in-vanets-and-manets/105798

Privacy Disclosure in the Real World: An Experimental Study
Siyu Wang, Nafei Zhu, Jingsha He, Da Tengand Yue Yang (2022). *International Journal of Information Security and Privacy (pp. 1-22).*
www.irma-international.org/article/privacy-disclosure-in-the-real-world/284046

Cylindrical Curve for Contactless Fingerprint Template Securisation
Boris Jerson Zannou, Tahirou Djaraand Antoine Vianou (2022). *International Journal of Information Security and Privacy (pp. 1-28).*
www.irma-international.org/article/cylindrical-curve-for-contactless-fingerprint-template-securisation/303664

Analysis of the US Privacy Model: Implications of the GDPR in the US
Francisco García Martínez (2021). *Research Anthology on Privatizing and Securing Data (pp. 1818-1825).*
www.irma-international.org/chapter/analysis-of-the-us-privacy-model/280257

Business Transaction Privacy and Security Issues in Near Field Communication
Jayapandian N. (2019). *Network Security and Its Impact on Business Strategy (pp. 72-90).*
www.irma-international.org/chapter/business-transaction-privacy-and-security-issues-in-near-field-communication/224865