A Confinement Framework for Mobile Agents

Shinichi Murata

School of Information Science,
Japan Advanced Institute of Science and Technology

February 15, 2001

Keywords: mobile agent, security, application framework, electronic commerce, security policy, malicious host, confinement.

1 Security Threats Considered

The purpose of this study is to construct a framework that protects mobile agents against read attacks from malicious hosts, and to realize it as an application framework. Mobile agents are programs that migrate from host to host and execute tasks at each host. Programmers can make flexible application by using mobile agents, because they can migrate with their internal states. However, when we use mobile agent technologies in real-world applications, we must resolve reliability and security problems. In this paper, we deal with one of the security problems. The security problems are divided into two categories: (1) threats by malicious agents who attack hosts and (2) threats by malicious hosts who attack agents. In existing mobile agent systems, (1) have been considered, but (2) is not. Though there are several attacks categorized as (2), we cope with a threat that confined data of agents are stolen by read attacks from malicious hosts.

Electronic commerce is one of application area that is expected to use mobile agents. If we use mobile agents for this area, they can collect information, make electronic settlement and negotiate price automatically. However, malicious hosts can read their confined data like information about a credit card and personal information. So in this area, it is important to cope with the read attacks. In this paper, we deal with Electronic Commerce Agent who migrates from host to host and communicates with a virtual shop at each host and does electronic commerce.

2 A Confinement Framework

Several security techniques against the threats of malicious hosts have been suggested. However they have not been practical techniques to protect mobile agents against the

read attacks, because mobile agents are executed at the hosts that can be malicious. These hosts must know the code and internal states to execute mobile agents. Even if we encrypt information about the agents, they must decrypt it. So it is difficult problem to protect confined data of the agents against the read attacks. To cope with this problem, we suggest a confinement framework that protects mobile agents against the read attacks. In this framework, confined data is separated from the main part of an agent. We call an agent who manages confined data at a user's host a Secret Data Manager Agent, and an agent who migrates from host to host an Itinerary Agent. Though they are executed at different hosts, they communicate with each other through the network and work as a single Electronic Commerce Agent. The Itinerary Agent migrates and executes tasks and sends requests to the Secret Data Manager Agent to get confined data. The Secret Data Manager Agent receives these requests, and returns confined data only to the Itinerary Agent who has permissions to access to it. The permissions are distinguished by following items.

- A host by whom the Itinerary Agent is executed.
- An identifier of a virtual shop where the Itinerary Agent is communicating.
- Executive phase of the Itinerary Agent.
- Kind of access.
- An identifier of the Itinerary Agent.

3 An Application Framework

In this confinement framework, the Itinerary Agent migrates without having confined data; so malicious hosts can't read it. However, when confined data is needed, the Itinerary Agent must always send requests. And the Secret Data Manager Agent must identify correct requests that have the permissions. And furthermore, communications between these agents must be secure. So the program code tends to become complicated and it is difficult to implement the code for security correctly. To cope with these problems, we realize a confinement framework as an application framework of the Electronic Commerce Agent. The framework makes it easy to create the Electronic Commerce Agent who can protect confined data. The framework consists of template classes of the Electronic Commerce Agent, a Security Manager function, a Data Store function and a library of security function. The Security Manager function, that is included in the Secret Data Manager Agent, receives requests from the Itinerary Agent and checks its permissions. The Data Store function, that is included in the Itinerary Agent, has functions to communicate with the Secret Data Manager Agent securely. The template classes have these security functions and itinerary patterns.

We must consider two requirements to which host information is opened and techniques to protect information. A combination of the requirements differs with each confined data, processing contents and usage of an agent. For example, we must open member

information, by the SSL protocol, only to a host of a virtual shop that provides member services. However, information about a credit card for the electronic settlement must be opened only to a host of a payment gateway and protected by the SET protocol. So we define the requirements as security policies into the XML files. The policies have pairs of confined data and the requirements, and make it easy to set and change the confinement framework flexibly. They are read by the Security Manager function and used to restrict the permissions.

4 Experiments and Conclusion

We made three examples of the Electronic Commerce Agents. Each of them has different itinerary patterns by using the application framework. The confined data differs with each itinerary pattern. And the techniques to protect information differ with each data. So each example uses different techniques to protect confined data. By using this application framework, it was simplicity to create the Electronic Commerce Agent each of them has different itinerary pattern. And it was less program code to protect confined data against the read attacks. Future works are coping with other security problems like a tampering and applying the confinement framework to areas other than electronic commerce.