An Architecture for Constructing Tamper-Proof Mobile Agents

Makoto Hasegawa (010087)

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

February 15, 2002

Keywords: mobile agents, security, tamper-proof, architecture, application framework.

1 Background & Purpose

Mobile agents move around various computer hosts via the network and execute their tasks on the hosts. Such mobile agents have a strong feature for wireless communication. Actually, some information retrieval systems on mobile phones are based on mobile agents. Nowadays, mobile agents can be used to construct electronic commerce systems on mobile phones. In such systems, mobile agents have personal information of their users. Therefore, we must consider about security issues on such mobile agents sufficiently.

The security issues on mobile agents are classified as follows: 1) the attacks from mobile agents to hosts, 2) the attacks from malicious hosts to mobile agents. Most of related works focus on the first issue. Although there are few related works for the second issue, their approaches are not so practical. However, the second security issue is also important for realizing information retrieval systems, electronic commerce systems, etc. based on mobile agents.

We can protect mobile agents from the network tapping by using existing cipher technologies & infrastructure, security protocols, etc. However,

mobile agents may be attacked by malicious hosts & agents directly after their migration: read attacks, tampering, etc. From the reason, each mobile agent must have a security mechanism to protect its own data (including personal information of its user such as name, address, phone number, credit card number, etc.) by itself.

In this work, we focus on the security issue of read attacks from malicious hosts & agents to mobile agents. The mobile agents that have the mechanism to protect their own data from malicious hosts & agents are called tamper-proof agents. Our goal is to design a flexible architecture for constructing tamper-proof agents.

2 Our Approach

In this work, we adopt the following approaches to construct tamper-proof agents in flexible way.

- Each mobile agent has a security mechanism to protect its own data.
- A mobile agent forms a meta-level architecture.
- The security mechanism is realized as independent modules in the meta-level.
- The security mechanism is obfuscated.
- Each mobile agent has a security policy.

To protect the data of mobile agents flexibly, each mobile agent must have a security mechanism by itself. The security mechanism mainly consists of encoding and decoding mechanisms. A mobile agent forms a meta-level architecture. The security mechanism is realized as independent modules in the meta-level. Namely, it is separated from primary subject domain codes of the mobile agent (base-level). From the separation, the security mechanism can be changed flexibly. The mobile agent encodes the base-level by using the security mechanism and obfuscates the meta-level by itself. Then, it flexibly decodes the base-level depending on the security policy.

3 ART: An Application Framework for Tamper-proof Agents

We have implemented an application framework named ART to construct tamper-proof agents based on our approaches. ART is a Java class library to realize electronic commerce systems based on mobile agents. The following are features of ART:

- The meta-level modules can be changed flexibly.
- It supports Caesar cipher algorithm, algorithm based on BASE64 encoding.
- It supports an obfuscation mechanism that makes many dummy threads run concurrently.
- A security policy is described as an external file, and changed flexibly.
- It supports a security manager that controls the security mechanism and the security policy.
- It supports several itinerary patterns for mobile agents.

ART is a class library including the meta-level & the base-level modules. The meta-level consists of classes to realize the mechanism. The base-level consists of classes to realize electronic commerce systems based on mobile agents. A security manager in the meta-level encodes and decodes the data of mobile agents depending on the security policy.

We have implemented an electronic commerce system based on mobile agents by using ART.

The system consists of a user agent and several virtual shop agents including a malicious shop agent that does read attacks to the user agent. The user agent has personal information of its user such as name, address, phone number, etc. It encodes such user's data by itself before moving. After moving, it communicates with virtual shop agents to buy something that the user wants. At the communication, the user agent flexibly decodes the user's data by itself depending on the security policy and the reliability of the shop agents. If a shop agent is unreliable, the user agent does not

decode the data and escapes from the host that the shop agent works. We have implemented several versions of the user agent by changing encoding algorithms and the security policy in the meta-level. From the implementation, we can make sure the flexibility of our architecture. Using ART, we can easily make ordinary mobile agents tamper-proof agents.

4 Conclusion

We have proposed a flexible architecture for constructing tamper-proof agents, and implemented an application framework named ART based on our approaches. Using ART, we have implemented an electronic commerce system based on mobile agents. From the implementation, we can make sure the flexibility of our architecture.

The following are our future works.

- Description form of security policy.
  In this work, the description form of security policy is quite simple. To realize the security mechanism in flexible way, it is necessary to improve the description form of security policy.

- Obfuscation technology.
  In ART, obfuscation technology is also simple. To make the security mechanism more practical, it is necessary to adopt more complicated obfuscation technology.