Security for Collaboration of Mobile Agents.

Master Thesis

KASHIF DAR

Submitted to
SecLab
Department of Computer and System Sciences (DSV)
Kungliga Tekniska Högskolan(KTH)
Stockholm, Sweden

This thesis corresponds to 20 weeks of full-time work.

Mobile Agent, Collaboration, FIPA, MASIF, Authentication, Message Security, PKCS 7, SAGE, Java Socket Programming, Eclipse RCP.

ABSTRACT

Mobile agent is reffered to as a process (software agent) that can migrate from one envirinment to another while keeping its data, and still being able to resume and execute in another environment. Mobile agents reduce network traffic as compared to convential client/server applications, because they can be dispatched from central controller to act locally.

Mobile agent being capable of *social ability*, has to share information with other agents to work efficiently. However there are two main issues of this collaboration: first is to define message format that will be acceptable to a variety of different vendors, and second is the security threats involved during their collaboration e.g., masquerading, information disclosure, information integrity, trustworthiness of information sender and receiver etc.

The solution for the first problem has been provided by Foundation of Intelligent Physical Agents (FIPA) that descibed standard Agent Communiocation Language (ACL) which can be used to exchange messages between agents. Consequently, two agents can communicate with each other through FIPA compiant ACL messages. FIPA also specifies the ontology that is treated as a shared vocabulary among the community of agents and is used to construct ACL messages.

In oreder to provide agents with a secure collaborative environment in which they can comfortably make conversation, first they have to authenticate each other, secondly they should exchange messages without loss of data confidentialty and integrity. To achieve this goal, Public Key Cryptographic Standard 7 (PKCS 7) is followed. PKCS 7 signed and enveloped data provides all these security features.

Thanks to SAGE, the open source agents platform provided by National Institute of Information Technology (Islamabad, Pakistan) whose ACL and Ontology modules were re-used to implemnt FIPA compliant ACL messages and defining ontology for the domain of our interest.

Finally, a simple File Search Application (used to search for a particular file on different remote hosts) is designed and implemented to realize the outcome of our work. This application uses frequent communication between the working agents during their lifetime.

Despite all the effort, there are still improvements that has to be done. The other possible threats that have not been addressed in this work include the proper authorization mechanism to control access to the sensitive information contained by agents, the issue of delegation when agents produce their clones, message flooding by the malicios agents for denial of service attack, and the repudiation attacks.