Chapter 20

Mobile Agent Communication, Security Concerns, and Approaches: An Insight into Different Kinds of Vulnerabilities a Mobile Agent Could Be Subjected to and Measures to Control Them

Kamat Pooja
Symbiosis Institute of Technology Pune, India

Gite Shilpa
Symbiosis Institute of Technology Pune, India

Patil Shruti
Symbiosis Institute of Technology Pune, India

ABSTRACT

Mobile Agent Systems model has attracted attention of various researchers and scholars all over the world due to a wide array of features it offers. The capability of mobile agent to hop independently from one network to another, carrying out various computational processes on remote network, enables them to operate in fixed and mobile networks more efficiently and robustly than typical client-server systems. However little attention is paid to the security management of the mobile agents due to which it is still not widely used in the industry domain. In this chapter, the authors examine the various security issues in Mobile Agent systems and approaches used to overcome them.

INTRODUCTION

A mobile agent can be termed as a unique type of mobile code. A mobile agent is a kind of a program that migrates from one host to another in a distributed network mobile agent. It has many advantages over existing distributed techniques like optimum resource utilization, minimize network traffic etc (Bhanot, R., & Hans, R., 2015). A Mobile Agent exhibits the following characteristics:

- **Mobility**: Mobility is a characteristic which allows a mobile agent to jump from one node to another. During this traversal, the mobile agent can perform any communication processes.
- **Independent**: An independent or autonomous Mobile Agent can take its own decision or act on behalf of another mobile agent.
- **Communication**: A mobile agent can talk to another mobile agent, fixed or mobile servers and other client systems.
- **Learning**: A mobile agent is known to be ‘smart’ that gains knowledge from its past experience and changes its behaviour accordingly.
- **Interoperability**: Mobile agents have property to execute on different platform or over different clients and adapt to changes in the environment.
- **Persistence**: Mobile agent has no need to establish continuous connection for execution of programs.

BACKGROUND

Due to large number of features supported by mobile agents, they have a higher probability of facing security threats. To get a better understanding of the security threats, the authors consider the two integral components of a mobile agent system - a mobile agent and an agent platform. An agent represents the mobile code and the state information which is needed to carry certain processing. An agent platform is a computational setting wherein the mobile agent ‘operates’. A mobile agent can hop between agent platforms and also communicate with the platform. The platform where a mobile agent is created is called as a ‘home platform’ and it is often the safest environment for an agent. An agent platform can be termed as a communication place wherein mobile agents can speak to each other.

SECURITY THREATS IN A MOBILE AGENT SYSTEM

Belal Amro (2014) categorizes the security threats faced by a Mobile Agent System into four broad categories: threats due to a mobile agent harming an agent platform, a mobile agent attacking another mobile agent, an agent platform attacking a mobile agent and finally outside entities harming the mobile agent system. The fourth category includes threats when an agent harms a destination platform or one agent platform attacking another platform. The threats mentioned above have their analogues in a typical client-server system and have taken place in the past.