Avoidance of Risks for Mobile Agents on Different Domains

Hans Raj, Dr. V.S. Dhaka

Abstract—now a days mobile agents system is very popular and secure way of data transmission through computer Network. Mobile agent is a software entity. It has safe state and code. Mobile agent travels through number of hopes and it can leave hope as and when needed. Throughout all these communication of mobile agent it can loss their personnel information like code or data. Code or data can be still or modified by some malicious behaviors of the computational environment. In the field of mobile agents system there are various security issues raises and can create a problem in data communication. My research paper is focus on the some security threats and security mechanism provided to mobile agent for their secure computation in the particular domain. Using that technique there can be reduce turn around time for mobile agents up to some extent. The proposed mechanism can work at the base level of computation of mobile agents in their concurrent computational environment.

Keyword: Agent Platform, Domain, Mobile agent, Risk, Security threats, Security issues

1. Introduction

Mobile agents are software that can move around the computer network to accomplish a given task in a given time. Mobile agents are autonomous and unique software entities. It has safe state and code. Mobile agent travels through number of hopes and it can leave hope as and when needed. Throughout all these communication of mobile agent it can loss their personnel information like code or data, because mobile agents has their own state and data. In the field of mobile agent system their can exist some security threats that can create a problem in their computation and can change their state and update or still their personnel information. There are many security threats found in the field of mobile agent system. These are: -

1. Agent to Platform attack [1] - The agent to platform categories represents the set of threats in which agent exploits security weakness of an agent platform or launch attacks against agent platform.

2. Agent to Agent Attack [1] - The agent to agent categories represents the set of threats in which agent exploits security Weakness of other agent or launch attack against agent. this Set of threats includes masquerading, unauthorized access, denial of services and repudiation [16].

3. Other to Agent Platform Attack [1] -In these categories of attack an agent platform may attack on agent. It can modify the internal data, state, and hash code of an agent.

Figure 1- Represents client server and mobile agent communication [12].
4. Platform to Agent Attack [1] - The other to agent platform category represents the set of threats in which external entities, including agent and agent platform, threaten the security of an agent platform. This set of threats includes masquerading, denial of service, unauthorized access, and copy and replay.

5. Proposed Algorithm

A Security Alert Bank can maintain all the history of execution of particular Domain. It can assign the safe Harmful value i.e. 0 and Safe Status value i.e. 1.

Step 1 - Send a mobile agent on the network with their internal code and status value.

Step 2 - Assign the Safe Harmful value and safe status Value.

Step 3 - compare these Harmful value and status value with harmful value and status value of domain within witch the mobile agent want to execute.

Step 4 - Calculate status value of Agent Platform. It can be calculated by dividing the malicious mobile agent (MX) and total number of mobile agents (MY) that visits a particular domain i.e. Status value = MY/MX.

Step 5 - Calculate Harmful value of domain by dividing HLC and HCP here HLC is the number of time AP’s in the domain are found malicious and HCP is the number of time, AP in the Domain found honest i.e. HLC/HCP multiply by 100.

Step 6 - After calculating the Harmful value and Status value of domain then it can compare with the harmful value and status value of Security Alert Bank.

Step 7 - If both these values match first that can be calculated by mobile agent and second values store in Security alert Bank.

Step 8 - Then mobile agents go to next Domain and repeat the step from 4 to 7.

6. Conclusion

Through this proposed technique there can be reduce turn around time for mobile agents up to some extent. The proposed mechanism can work at the base level of computation of mobile agents in their concurrent computational environment.
References


[8] L. Ismail College of IT United Arab Emirates University P.O.Box 17551, Al-Ain, United Arab Emirates JOURNAL OF COMMUNICATIONS, VOL. 3, NO. 2, APRIL 2008.


[15] Najmus Saqib Malik, Friedrich Kupzog Institute of Computer Technology Vienna University of Technology Vienna, Austria malik, kupzog@ict.tuwien.ac."Domain based Security for Mobile Agents".


