Security Issues in Mobile Agent Paradigm

Nitin Jain[1], Kamlesh[2], Neeraj Singla[3]

[1]**M.Tech student, SITM REWARI, (India)**
Nitin.87.jain@gmail.com

[2]**Asstt. Prof, SITM REWARI, (India)**

[3]***Asstt. Prof,* VCE, Rohtak (India)**
Neerajsin30@gmail.com

Abstract

A mobile Agent is a Software program that migrates from node to node of a heterogeneous network. They are goal-oriented i.e. work autonomously towards a goal, capable of suspending their execution on one platform and moving to other where they can resume execution using resources of these nodes and they meet and interact with other agents. Agents may be stationary, always resident at a single platform or mobile, capable of moving among different platforms at different time. The mobile agent paradigm provides many benefits in developments of distributed application at the same time introduce new requirements for security issues with these systems. In this paper we try to focus mainly on security issues that arise when mobile agent paradigm comes into play.

Keywords: *Mobile-agent, Security, threats, Countermeasures.*

I. INTRODUCTION OF MOBILE AGENT PARADIGM

There are many ways a mobile agent paradigm model can be implemented. We consider a simple Mobile agent Paradigm that consists of only two parts Agent and Agent Platform.

Figure 1

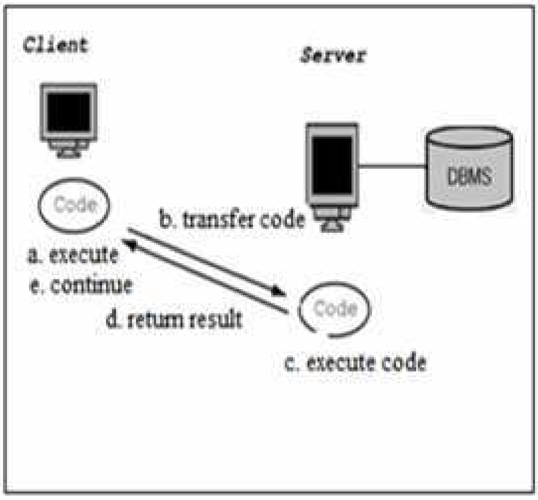
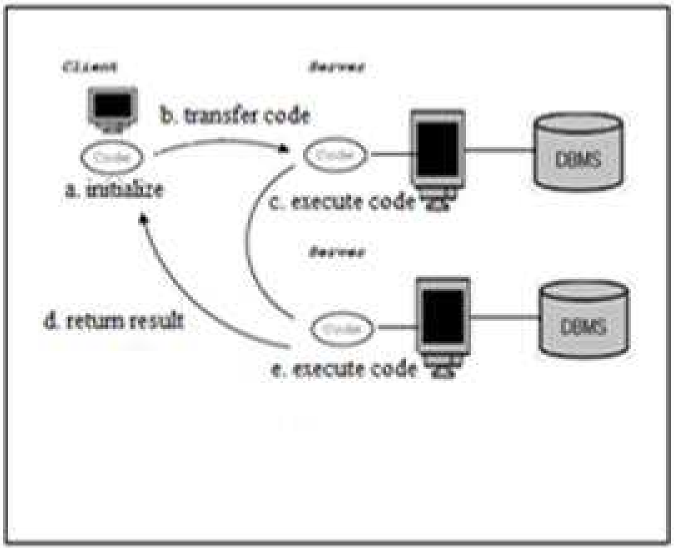


Figure 2: Mobile Agent Paradigm



Agent Consists of mainly five items which are listed below:-
1 .Implementation:- It is needed for location-independent agent execution.
2. State:- It is needed for the agent to resume computation after travelling through nodes
3. Interface:- It is needed for agent Communication.
4. Identifiers:- It is needed to recognize and locate travelling agents
5. Principals:- It is needed to determine legal and moral responsibilities.

The agent platform provides the computational environment in which the agent operates. The originating platform where agents originate initially is known as home platform. One or more hosts may comprise a single agent platform which may support multiple computational environments

Paradigms/Attributes	**Mobile Agent**	**Remote Evaluation**	**Client-server**
Implementation	Hard	Easy	Very easy
Security	Very low	Low	Very high
Performance	high	Very high	Low
Elements	semi mobile	static	mobile
a) Data	mobile	mobile	static
b) Code	mobile	static	static
c) Stack			
Itinerary	Static/Dynamic	Both	Static
Mobility	Code to data	Code to data	Data to code
Platform	Dependent	Dependent	Independent
Programming code	Hard	Hard	Easy
Examples	Aglet	Aglet	CORBA,

Table 3.1
Comparison between various Distributed Computing Paradigms

II. SECURITY THREATS

Security threats can be generally classified into three categories:-

1. Disclosure of Information
2. Denial of Service
3. Corruption of Information(Unauthorized Access)

In our discussion we focus mainly on these three types of security threats. In any mobile agent paradigm mainly four types of Security threats can arise namely

1. Agent attacking another Agent
2. Agent attacking another Agent Platform
3. Agent Platform attacking an Agent
4. Others(Agent or Agent Platform) attacking another Agent Platform

We will discuss each of these Situations and will focus our discussion to mainly three types of security threats that we have discussed earlier.

III. AGENT TO AGENT

In these types of attack an Agent, in many cases agent platforms are also agents or a part of agents, Exploits Security flaws and attack other agents.

A. Disclosure of Information

Agent to agent communication , an agent may pose as a well known service provider and tries to claim entity of a trusted agent and try to convince the other agent with credit card no, bank account information or other private information.

B. Denial of Service

Agents can distribute false or useless information to prevent other agents from completing their task correctly and on time for example repeatedly sending messages that is spamming agents with messages with cause's slow performance of agents.

Sometimes an agent participating in a transaction or communication never took place which can lead to serious disputes.

C. Unauthorized Access

An Agent can directly interfere with another agent by accessing and modifying agents data or code which inturn changes the agent behaviour.

IV. AGENT TO AGENT PLATFORM

A. Disclosure of Information

An agent may pose as to gain access to services and resources to which it is not entitled. It can also pose as an another unauthorized agent to shift blame for any actions for which it does not want to be held accountable.

B. Denial of Service

A agent can carry malicious code that is designed to disrupt the services offered by the agent platform, Performance degradation of the agent platform or extract information for which it has no authorization to access. Depending on the level of access it may be able to completely shut down or terminate agent platform.

C. Unauthorized Access

An agent can have access to platform & its services without having the proper authorization which can cause damages to other agent or the agent platform itself.

V. AGENT PLATFORM TO AGENT

A. Disclosure of Information

An agent platform can act like a trusted platform and can extract sensitive information from these agents. When an agent arrives at an agent platform it expresses its code state data to the platform. A malicious platform can modify an agent's code, state or data without being detected. Modification of an agents code & thereby behavior on other platforms may harm to the doped agent than a single agent can do on its own since an agent can harm another agent only through messages they exchange & actions they take as a result of these messages.

B. Denial of Service

When an agent arrives at an agent platform .it expects the platform to execute the agents request faithfully, provide fair allocation of resources and abide by the quality of service agreement. A malicious platform may ignore agent service request, introduce unacceptable delays for critical tasks such as placing orders in stock market, simply not executing the agents code or even terminate the agent without notification. agents on other platforms waiting for the result of a non responsive agent on a malicious platform can never achieve its goal.

C. Unauthorized Access

The agent platform can monitor the communication, every instruction executed by the agent, all encrypted data and the subsequent data being generated. for example someone's agent may be communicating with a travel agents this communication may indicate that the person on whose behalf the agent is acting ,is planning a trip and will be away from their home in near future. the platform can share this information with a suitcase vendor that may begin sending unsolicited advertisements or even worse with thieves who may target the home of the traveller.

VI. AGENT, AGENT PLATFORM TO AGENT PLATFORM

A. Disclosure of Information

The Agent can request platform services both locally and remotely. An agent on a remote platform can act as another agent and request services and resources for which it is not entitled or authorized. A remote platform can also act as another platform and mislead unsuspecting platforms or agents about its true identity

B. Denial of Service

The agent services offered by the platform and inter platform communications can be disrupted by common denial of service attack. Agent platforms are also susceptible to all the conventional denial of service attacks aimed at the underlying operating system or communication protocols.

C. Unauthorized Access

An agent can remotely administer the whole system and can access the resources and data for which it is not entitled for. every time a mobile agent moves from one platform to other it increases its exposure to security threats.

VII. COUNTER MEASURES

There are a no of extensions to conventional techniques and techniques devised specially for controlling mobile code and executable content are applicable to mobile agent paradigm security.

Most agent systems rely on a common baseline assumptions regarding security. These are as follows:-

1. The agent trusts the home platform where it is initiated and begins execution.
2. Home platform and other are equally trusted platform are implemented securely with no flaws, trapdoors , that can be exploited and behave non – maliciously.
3. Public key Cryptography i.e. Digital Signature is utilized through certificates and revocation list managed through a public key infrastructure.

VIII. FUTURE RESEARCH

The area of mobile agent security is still in somewhat immature state. Both the agent and the agent platform should to be protected by developing techniques and mechanisms. The threats and countermeasures are always changing and likely to emerge from either through reduced processing and storage overhead or simplify the use of mechanism to form a more effective composite protection scheme.

REFERENCES

[1] M. Straßer and M. Schwem, "A Performance Model for Mobile Agent Systems,"H. Arabnia (Ed.), Proceedings of the International Conference on Parallel andDistributed Processing Techniques and Applications (PDPTA'97), Vol. II,CSREA, pp. 1132-1140, 1997.

[2] Neeran Karnik, "Security in Mobile Agent Systems," Ph.D. Dissertation,Department of Computer Science, University of Minnesota, October 1998.<URL: http://www.cs.umn.edu/Ajanta/>

[3] Bennet S. Yee, "A Sanctuary for Mobile Agents," Technical Report CS97-537 University of California in San Diego, April 28, 1997. <URL: http://www-cse.ucsd.edu/users/bsy/index.html>

[4] Thomas Sander and Christian Tschudin, "Protecting Mobile Agents Against Malicious Hosts," in G. Vinga (Ed.), Mobile Agents and Security, Springer- Verlag, Lecture Notes in Computer Science No. 1419, 1998. <URL: http//www.icsi.berkeley.edu/~tschudin/>

[5] Giovanni Vigna, "Protecting Mobile Agents Through Tracing," Proceedings of the 3rd ECOOP Workshop on Mobile Object Systems, Jyvälskylä, Finland, June 1997.
<URL: http://www.cs.ucsb.edu/~vigna/listpub.html>

[6] William Farmer, Joshua Guttman, and Vipin Swarup, "Security for Mobile Agents Authentication and State Appraisal," Proceedings of the 4th European Symposium on Research in Computer Security (ESORICS '96), September 1996, pp. 118-130.

[7] Robert S. Gray, "Agent Tcl: A Flexible and Secure Mobile-Agent System," Proceedings of the Fourth Annual Tcl/Tk Workshop (TCL 96), pp. 9-23, July 1996.

[8] "Mobile Agent System Interoperability Facilities Specification," Object Management Group (OMG) Technical Committee (TC) Document orbos/97-10- 05, November 1997.

[9] Thomas sander and Christian Tschudin " Protecting mobile Agents agains malicious hosts" in G.Vinga (Ed) <wwww.icsi.berkeley.edu/`tschudin/>