

# Need of Securing Mobile Agents

Shilpi Gupta

Meerut Institute of Technology, Meerut, Uttar Pradesh, India

**Abstract**--A mobile agent is an independent software entity that acts on behalf of its owner or user with the ability of moving from one node to another. They are goal oriented i.e they work autonomously towards a goal and can suspend their action on one platform and they can resume it on another platform. But when they roam from one platform to other they have face some major security threats. In this paper I mainly review the security objectives, threats and some approaches by which we can achieve security in mobile agent's paradigm.

**Keywords**—Mobile Agents, Security attacks, security services, Mobile agent systems, 'D' agent

## I. INTRODUCTION

Mobile agent is a process that can migrate from one environment to another, with its data intact, and be capable of performing appropriately in the new environment. Mobile agents are processes that consist of code, data and control information. Mobile agent is robust and autonomous. It works towards achieving a goal without human interception. It works on distributed environment so it supports disconnect computing which is not only reduces bandwidth usage but also moderates the effects of high latency.

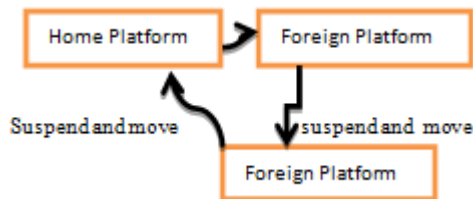


Fig 1. Mobile Agent System

Mobile agent systems are platforms that allow mobile agents to migrate between different nodes of the agent system. From a more technical view, mobile agents can be compared to programs that migrate to nodes autonomously, while nodes offer the runtime environment of these programs including the program interpreters.[1]

There are different basic requirements of any computer system. These are like Confidentiality, integrity, authentication, authorization, non-repudiation and availability. [3, 4, 5]. Same security requirements are in the case of mobile agent system. But as a mobile agent moves in an heterogeneous environment to achieve its goal, it has to face so many security threats. Sometimes a mobile agent itself becomes a security threat for the platform where it will resume its task.

There are so many approaches that have been already proposed. But no approach fulfills all the security requirements described below. So the topic of securing mobile agent is always a very hot research topic.

This paper is organized in our sections. Section II describes basic security attacks and section III describes security services of any computer system. Section IV describes different types of scenarios related to security of mobile agent system. In section V I will describe some existing mobile agent systems and section VI contains my conclusion.

## II. SECURITY ATTACKS

Security attacks are divided into two categories:

### A. Passive Attacks.

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are release of message contents and traffic analysis. The release of message contents is easily understood. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions. A second type of passive attack, traffic analysis. Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. But the opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. Passive attacks are very difficult to detect because they do not involve any alteration of the data.

### B. Active Attacks.

Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service. A masquerade takes place when one entity pretends to be a different entity. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges. Replay involves the passive capture of a data unit and its subsequent retransmission to produce an

unauthorized effect. The denial of service prevents or inhibits the normal use or management of communications facilities. This attack may have a specific target. It is quite difficult to prevent active attacks absolutely, because of the wide variety of potential physical, software, and network vulnerabilities.

### III. SECURITY SERVICES

There are following security services related to any type of communication by any type of systems:

#### A. Authentication.

The assurance that the communicating entity is the one that it claims to be. Two types of authentication are Peer entity authentication and Data origin authentication.

#### B. Access Control.

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

#### C. Data Confidentiality.

The protection of data from unauthorized disclosure.

#### D. Data Integrity.

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

#### E. Nonrepudiation.

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

### IV. SECURITY ISSUES IN MOBILE AGENTS SYSTEM

Attacks on Mobile Agents by Mobile Agent Platforms In case of strong mobility of mobile agent all its code, data and state are exposed to the mobile agent platform in which it migrates for execution of operation. Because of this mobile agent system faces more severe security risks. Following are some scenarios:

#### A. Agent attacking an agent platform.

This category represents the set of threats in which agents exploit security weaknesses of an agent platform. This set of threats includes: Masquerading, denial of service and unauthorized access.

#### B. Agent attacking the other agents.

This category represents the set of threats in which agents exploit security weaknesses of other agents. This set of threats includes: Masquerading, denial of service, unauthorized access and repudiation.

#### C. Platform attacking an agent.

This category represents the set of threats in which platform exploit security weaknesses of other agents. This set of threats includes: Masquerading, denial of service, eaves dropping and alteration.

#### D. Other entities are attacking the agent system.

This category represents the set of threats in which external entities, including agents and agents platforms, threaten the security of an agent platform. This set of threats includes: Masquerading, denial of service, unauthorized access and copy and replay attack.[7]

### V. SOME MOBILE AGENTS SYSTEMS

There are different systems have been proposed to implement mobile agent systems. Some of them are as follows:

#### A. D'Agent.

D'Agents is a general-purpose mobile-agent system that has been used in several information retrieval applications. D'Agents greatly simplifies the task of providing efficient, applicationspecific access to remote information resources. They developed D'Agents to support distributed information-retrieval applications, including the soldier application described above. Their main design goal was to support multiple agent languages, so that the programmer could choose the most appropriate language, and their main implementation goal was to optimize performance, so that we could more accurately explore the potential performance advantages of the mobile-agent paradigm. The current version of D'Agents supports three languages (Tcl, Java, and Scheme), provides strong mobility (in Tcl and Java), uses encryption for authentication and privacy of moving agents, enforces limits on resource usage, and is based around a high-performance, multi-threaded agent server.[8]

#### B. Agent Tcl.

Agent Tcl is a mobile-agent system under development at Dartmouth College that has evolved from a Tcl-only system into a multiple-language system that currently supports Tcl, Java, and Scheme. Agent Tcl is a simple but powerful mobile-agent system that distinguishes itself from other mobile-agent systems with (1) its combination of multiple languages, a simple migration mechanism, and both low- and high-level communication protocols, (2) its simple but effective security model, and (3) its extensive support services and tools.[9]

#### C. Sumatra.

Sumatra is one of the experimental extensions to Java. Thanks to Java library extensibility, it can be added new programming abstractions for mobility, without altering the basic language. The only significant modification is made to the interpreter, because it has to trace the execution stack and the program

counter in order to implement strong mobility by transferring the execution state to the new node of execution. This does not imply a change to the Java Virtual Machine interface, so the modified interpreter can execute every program written in “standard” Java.[10]

#### D. *Telescript and Odyssey.*

Telescript[11] is a mobile language developed at the General Magic. It is object-oriented and it supports the mobility of objects. It was born as a commercial, self-contained language. Odyssey [12] is a project being currently developed at the General Magic. Unlike Telescript, Odyssey is an extension of an existing language, Java. It takes concepts from Telescript, and implements them adding classes to the base Java library, in particular it adds the class Agent, which implements the idea of mobile agent. An interesting feature is that, unlike Sumatra, it does not require any modification to the Java interpreter; this of course implies that Odyssey implements only a weak mobility.[10]

### VI. CONCLUSION

The paper has explained basic about mobile agents and different issues related to mobile agent systems and emerging trends related to this topic. We discussed that mobile agents have positive side for distributed applications but due to security reasons society is not so much interested to use it in financial services. Till now there is no such system that is fully secure.

Because of this weak point of mobile agent system there are several points where we can make those approaches more secure. People will become more interesting to use mobile agent systems in their real life when all security flaws will overcome.

### REFERENCES

- [1]. Time Limited Blackbox Security: Protecting Mobile Agents From Malicious Hosts | Fritz Hoh | Institute of Parallel and Distributed High-Performance Systems (IPVR), University of Stuttgart, Germany
- [2]. Cryptography Based Hybrid Security Architecture for Mobile Multi Agents
- [3]. Dadhich, P., Dutta, K., Govil, M. C. (2010) 'Security Issues in Mobile Agents', International Journal of Computer Applications, 11(4), pp. 1-7.
- [4]. Ahmed, T.M. (2013) 'Protect Mobile Agent Against Malicious Host Using Partial-Mobility Mechanism', International Journal in Foundations of Computer Science & Technology (IJFCST), 3(6), pp. 41-52.
- [5]. Singh, D., Thakur, A., Gupta, D. (2015) 'A Review of Mobile Agent Security', International Journal of Advanced Research in Computer Science and Software Engineering, 5(2), pp. 188-190.
- [6]. Priyanka Dadhich, Dr. Kamlesh Dutta, Prof. (Dr.) M.C. Govil, Security Issues in Mobile Agents, International Journal of Computer Applications (0975 – 8887), Volume 11– No.4, December 2010
- [7]. Wayne Jansen, Tom Karygiannis, NIST Special publication 800-19 – Mobile agent security
- [8]. D'Agents: Applications and Performance of a Mobile-Agent System Robert S. Gray, George Cybenko, David Kotz, Ronald A. Peterson and Daniela Rus Thayer School of Engineering / Department of Computer Science Dartmouth College Hanover, New Hampshire 03755
- [9]. Agent Tcl: A flexible and secure mobile-agent system Hanover, New Hampshire 30 June 1997
- [10]. G. Cabri, L. Leonardi, F. Zambonelli, Mobile agent technology: Current trends and perspectives G. Cabri, L. Leonardi, F. Zambonelli
- [11]. J. E. White, “Telescript Technology: the foundation for the electronic marketplace”, White Paper, General Magic, Inc, 1994.
- [12]. General Magic Odyssey Page, <http://www.genmagic.com/agents/odyssey.html>
- [13]. Varsha Kumari, Preeti Rajput, Sandhya Pundir, M. Q. Rafiq, Web crawler based on secure mobile agent, Research Journal of Computer Systems Engineering RJCSE, Vol 03, Issue 03; July 2012