Volume 5, Issue 2, February 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Review of Mobile Agent Security

Deepti Singh* M.tech (CSE) & Bhagwant University Ajmer, Rajasthan, India

Ankit Thakur M.tech (CSE) & Bhagwant University Ajmer, Rajasthan, India

Deepak Gupta M.tech (CSE) & Gov. Engg. College Ajmer, Rajasthan, India

Abstract— A mobile agent is a composition of computer software and data which is able to migrate (move) from one computer to another autonomously and continue its execution on destination computer. A mobile agent, namely, is a type of software agent, with the feature of autonomy, social ability, learning, and most significantly, mobility. This paper provides an overview of the main security mechanisms and issues related to mobile agent paradigm. These issues include security threats and techniques for keeping the mobile agent platform and the agent itself secure against each other.

Keywords— Intelligent agent, Mobility, Security, Security threats

I. INTRODUCTION

During the study of this paper many researchers found that a mobile agent system could be attacked by malicious agents, platforms and third parties over a year. Mobile agents simply offer greater opportunities for abuse and misuse, which broadens the scale of threats significantly. In addition, since mobile agents have some unique characteristics such as their mobility, security problems have become more complicated in these systems. These security problems have become a bottleneck in the development and maintenance of mobile agent systems, especially in security sensitive applications such as electronic commerce, aviation industry and defense systems.

Protection of mobile-agents against malicious platforms seems to remain a big challenge for mobile agent systems research communities, which has not yet received an acceptably comfortable level of security guarantees.

II. SECURITY ISSUES

Two main categories of threats can be identified in mobile agent systems, namely threats against the host and attacks against the mobile agent. The categories are defined as follows:

2.1. Host Threats

The mobile agent platform is responsible for the acceptance and execution of mobile agents. Jansen (2000) defines two categories of threats against the remote host. They are possible threats caused by a malicious mobile agent during execution and threats from other entities such as another remote host attacking the host. Attacks stemming from malicious mobile agents can be divided into attacks where the mobile agent can firstly gain unauthorized access to the host (and information on the host) and secondly where this gained access can be used to conduct malicious behavior. Examples of attacks that a malicious mobile agent can perform on a remote host include the unauthorized modification of resources, the unauthorized use of system resources located on the host and the leaking of sensitive data. A malicious mobile agent can for example be a virus that causes damage to the remote host, or it can launch denial of service attacks against hosts and prevent other agents from executing (Karnik, 1998). Attacks from other entities such as other remote host involve denial of service attacks as well as attacking the platform through masquerading (Jansen, 2000). A large number of solutions to protect the remote host against attacks from a mobile agent have been proposed and some have been implemented. The reason for this being that traditionally, conventional prevention techniques used in trusted systems and communications security can be used to provide adequate protection for the remote host (Jansen, 2000). Methods for countering attacks on a host include software-based isolation (Whabe et al.,1993), code signing (Karjoth et al.1997), path histories (Chess et al., 1995) and state appraisal (Farmer et al., 1996).

2.2. Mobile Agent Threats

Threats against mobile agents involve the protection from the remote host, other mobile agents and entities outside the mobile agent system, such as attacks on the transport mechanisms. These type of attacks are difficult to guard against because of the fact that traditional protection mechanisms were developed to address threats stemming from attacks on the execution environment by the application and not the other way around (Jansen, 2000).In providing a secure framework for mobile agents, the category of threats stemming from attacks imposed by a malicious host onto a mobile agent is of main concern in this research. These threats are discussed and classified in the next section.

III. CHARACTERISTICS OF MOBILE AGENTS

The invasion of various approaches under the banner of "agents" caused a need to classify and define this term. However it quickly became apparent that everyone had their own definition [1] due in part to the historical relationship

with the AI community and the vague notion of intelligence. Numerous definitions for the agents have been proposed, but in core most have a set of defining characteristics that every agent must demonstrate. For instance, Woodridge and Jennings‟ weak agents [2] should be autonomous, reactive and social. A definition from Franklin & Graesser [3] lists autonomous, reactive, communicative, adaptive, mobile, flexible, goal-oriented, continuous and with some form of character or emotion.

3.1. Autonomous - An agent should be able to execute without the need for human interaction, although intermittent interaction may be required.

3.2. Social / Communicative - An agent should have a high level of communication with other agents. The most common protocol for agent communication is the Knowledge Query and Manipulation Language (KQML)

3.3. Reactive / Responsive - An agent should be able to perceive its environment and react to changes in it.

3.4. Proactive - Proactive agents do not just react to their environment but can take active steps to change that environment according to their own desires.

3.5. Adaptive - Adaptive agents have the ability to adjust their behavior over time in response to internal knowledge or changes in the environment around them.

3.6. Goal-oriented / Intentions - These agents have an explicit internal plan of action to accomplish a goal or set of objectives.

3.7. Persistence / Continuous - Persistent agents have an internal state that remains consistent over time.

3.8. Mobility - Mobile agents can proactively decide to migrate to a different machine or network while maintaining persistence.

3.9. Emotion - Agents with the ability to express human-like emotion or mood. Such agents might also have some form of anthropomorphic character or appearance.

3.10. Intelligence - Agents with the ability to reason, learn and adapt over time.

3.11. Honesty - Agents that believe in the truthful nature of the information they pass on.

These agent characteristics lead to many advantageous features. The very nature of agents as independent, social entities that can respond to and change their environment provides a strong foundation for building reliable, robust, flexible, extensible and scalable systems.

IV. SECURITY THREATS

This computing paradigm, which exploits code, data and state mobility, raises many new security issues that are quite different from conventional client/server systems. Agent servers that provide an execution environment for the agents to execute can be attacked by malicious agents. Similarly agents could be carrying sensitive information about their owners and should be protected from tampering by malicious hosts. The data collected by the agent from one host should also be protected from tampering by another host in the itinerary. In this section, various security issues that arise in mobile agents‟ applications are examined.

4.1. Mobile-Agent Threats:

In this section we discuss the threats which are likely to be faced by mobile- agents in regard with security requirements of confidentiality, integrity, non-repudiation and availability.

A. Confidentiality Threats:

Mobile-agent confidentiality requirements are concerned with information exposure to a platform which may use it for malicious intentions. A malicious platform could try to spy on mobile-agents data. Additionally, a spying platform may learn about the mobile agent's code for control flow information in-order to predict its behavior and to use it for further malicious actions.

B. Integrity Threats:

A malicious platform could have intentions of changing data carried by the agent and to even change mobile-agent code so that its behavior is changed from what the agent owner expects. Apparently, the agent owners may never know that their mobile-agents are behaving differently from the originally intended design. Other subtle integrity attacks may involve interference with the agent's code control flow so that some agent actions are subverted.

C. Availability Threats:

A malicious platform may destroy the mobile-agent with its data. In other circumstances, a malicious platform may destroy only the data carried by the mobile agent. Furthermore, a platform may intentionally deny an agent timely execution time and communication facilities in order to systematically sabotage its functional goals. Other more complicated and subtle attacks may involve invoking wrong or compromised systems calls critical to a mobile-agent's needs. Additionally, mobile-agent re-execution on a malicious platform may lead to undesirable results in computational mobile-agents.

D. Repudiation Threats:

After an agent platform has carried out malicious activities on a mobile-agent, it may want to hide its actions and deny having previously executed the agent. Repudiation threats are a challenge for accountability requirements for platform

actions. If an agent platform can successfully deny having executed an agent, then it puts all mobile-agents that visit such platforms at greater risks of being destroyed without anyone being held accountable.

V. CONCLUSION

In this paper we have discussed about the mobile-agents, its security issues and its security threats. Mobile agent system is a very promising paradigm, it has shown its presence in many applications like distributed networking, e-commerce applications etc. There are numerous advantages of using the mobile agent paradigm rather than conventional paradigm such as client-server based technologies. In one way it provides the abstraction to networking. The benefits of mobile-agent technology cannot be exploited fully until all the security issues are properly addressed.

REFERENCES

[1] H.S. Nwana, "Software Agents: An Overview", Knowledge Engineering Review,11(3):1- 40, 1996.
[2] M. Woodridge and N. Jennings, "Intelligent Agents: Theory and Practice",The Knowledge Engineering Review, 10(2):114-152, June1995.
[3] S. Franklin, A. Graesser, "Is it an Agent, or just a Program?: A Taxonomy for Autonomous Agents", University of Memphis, Proceedings of the Third International Workshop on Agent Theories,Architectures, and Languages, Springer-Verlag,1996.
[4] http://www.google.co.in

