Journal of Network and Computer Applications 33 (2010) 661–671

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Advanced mobile agent security models for code integrity and malicious availability check

S. Venkatesan [a,*], C. Chellappan [b], T. Vengattaraman [c], P. Dhavachelvan [c], Anurika Vaish [a]

[a] *Division of MBA & Cyber Law and Information Security, Indian Institute of Information Technology Allahabad, India*
[b] *Department of Computer Science & Engineering, Anna University, Chennai, India*
[c] *Department of Computer Science, Pondicherry University, Pondicherry, India*

ARTICLE INFO

Article history:
Received 12 November 2009
Received in revised form
13 January 2010
Accepted 18 March 2010

Keywords:
Mobile agent
Mobile agent security
Code integrity check
Attack code identification
Mobile agent platform protection

ABSTRACT

Mobile agent technology is an emerging paradigm in distributed computing environment and it holds a potential status in the relevant research field due to its unique capabilities like flexibility, dynamic customization and robust interaction in unreliable networks. But the limited security perspectives and shortfalls of the mobile agent environments degrade its usage in a variety of application domains. Even though some of the protection models are available for protecting the environments, they are not efficient in handling the security issues. To make the mobile agent environment secure, this paper proposed advanced models to improve the efficiency of the existing Malicious Identification Police model for scanning the incoming agent to detect the malicious activities and to overcome the availability of vulnerabilities in the existing Root Canal algorithm for code integrity checks. The MIP model is extended with the policy to differentiate the agent owners in the distributed environment and the Root Canal algorithm is improved as eXtended Root Canal algorithm. The experimental results of the advanced models show that though these mechanisms take more time complexity than the existing malicious identification police model and Root Canal model, these models are efficient in protecting the agent code integrity and scanning the agent for malicious activities. Also the new models possess less time complexity compared to the other related existing models in the secure mobile agent environment.

1. Introduction

A mobile agent is a software program that can migrate from host to host to collect information on behalf of its owner. With the concept of mobile agent, the execution process will go to the place where the data are available, data will not send to the place of execution process. For this process mobility, different types (Jha and Iyer, 2001) of mobile agents are developed with different standards and procedures. The different type of agents are: Single hop mobile agent (will visit only one remote host and get back to home), Multi-hop mobile agent with Static Itinerary and Static Order (will visit multiple remote host and return to the owner with the required result. It will visit the remote host based on the itinerary and order given by the owner), Multi-hop mobile agent with Static Itinerary and Dynamic Order (will visit the set of remote hosts based on the itinerary given by the owner but the order is based on the run time decision of the remote host where the agent is currently residing), Multi-hop mobile agent with Dynamic Itinerary and Dynamic Order (which will visit the remote host based on the run time decision without the owner information. In this case the owner does not know the details about the remote hosts except the first remote host. Dynamic Itinerary always set to be Dynamic Order only). Itinerary is the list of remote host address and the Order represents the sequence in which the mobile agent has to visit the remote hosts available in the itinerary.

Irrespective of the advantages of the property of mobility, new critical security issues are to be solved in the mobile agent environment. The criticality is due to the reason that the owner does not know about the remote host characteristics and security issues and of course the remote hosts do not know the characteristics of the mobile agent and its vulnerability. These issues can be resolved by creating a secure and trusted environment, but the process of creating a trusted environment is a much more complicated issue, particularly in the Internet information sharing environment. The complication is due to the unpredictable nature of the simple and composite attacks. The work presented in this paper is based on the property of identifying and preventing different types of unpredictable attacks in the mobile agent environments.

This paper proposes two advanced models for the mobile agent security, one for platform protection and another for agent code protection. The policy based malicious identification police (MIP) will scan all the incoming agents to the host and it will allow only the legitimate agent to execute and rest of the things (agent) will be blocked. Next the eXtended Root Canal (XRC) algorithm, which

[*] Corresponding author.
E-mail address: venkalt_s@yahoo.co.in (S. Venkatesan).

1084-8045/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2010.03.010

is used to check the integrity of the mobile agent code before executing and to prevent the malicious host claim by the attackers.

The remaining section of this paper is organized as follows: Section 2 gives the brief description over the related works and their impact in the intended environments. Section 3 describes the proposed solution of policy based malicious identification police scanning model. Section 4 describes the proposed eXtended Root Canal algorithm and validations. Section 5 shows the experimental result analysis of both the policy based malicious identification police model and the extended Root Canal algorithm. Also the section gives the comparison with the existing models. Section 6 concludes the paper with the directions of future enhancements.

2. Related works

2.1. Mobile agent platform protection

The attack on the mobile agent environment may be on the platform or agent. Also, each part (code, data, itinerary and state) of the agent may be assaulted by the remote host. The mobile agent from the malicious host can perform multiple types of attacks on the legitimate hosts. Table 1 gives the significant types of attacks on the legitimate host (Axel et al., 2006), and its related issues.

Generally, the mobile agent from a malicious platform will have the intention to disrupt remote platforms. To protect the platform from the malicious agent, software-based fault isolation is proposed to implement fault isolation within a single address space (Wahbe et al., 1993). It means to separate the distrusted code in the separate software-enforced fault domains, so that the distrusted code cannot modify other data or execute another code except through an explicit cross-fault domain RPC (Remote Procedure Call) interface. Access to system resources can also be controlled through a unique identifier associated with each domain referred to as sandboxing. For this scheme, some of the methods are proposed with significant outcomes: sandbox – it is the protection model, which provides a separate location for the distrusted agent to execute in the environment (Wahbe et al., 1993); code signing – it is to authenticate the incoming agent by the platform (Joseph and Luis, 1996); Path History – an agent has to maintain the authenticable record of the prior platforms visited by it. Based on that record the newly visited platform can determine whether to process the agent or not (Ordille et al., 1995; Ordille, 1996). Proof Carrying code is a prevention technique, while code signing is an authenticity and identification technique used to deter, but not prevent, the execution of an unsafe code (Necula, 1997; Jansen, 2000). Leila (2008) developed a secure mobile agent platform with a multiple authentication system. It is good enough to prevent the attack in case of the malicious agent from the malicious client. But the problem with today's world is, the malicious entity is entering the environment as legitimate and acquires all the authentication details and others. After that, it will initiate the attack on the servers. The secure mobile agent platform given by Leila (2008) is not fit to prevent the attack. The same drawback is also applicable for key distribution framework for a mobile agent platform model (Leila and Ezedin, 2008). In this series, the malicious identification police with the Attack Identification Scanner (Venkatesan and Chellappan, 2008) is developed by the authors of this paper.

Table 1
Type of attacks on mobile agent platform.

Type of attacks	Issues
Denial of service (DoS)	• Overloading the agent platform with too many agents • Overloading the remote agent hosts with too many service requests • Consuming the computing resources of the remote agent hosts by non-terminating agents • Consuming the remote agent host's computing resources by too many messages
Unauthorized access	• Shut down the platform • Modifying policy file • Killing an agent in the platform • Replacing the java security manager
Agent based attack	• Spamming the agent with dummy requests • Suspending the agent • Sending a signed message with a fake sender ID • Manipulating the agent's resources • Spamming the agent with meaningless information requests.

In the malicious identification police model (Venkatesan and Chellappan, 2008), agents from all hosts are treated equally and no differences in terms of privileges are encouraged between the owners of the mobile agents. The MIP model protects both the direct attack (originator may send the malicious agent) and the indirect attack (the intermediate host may change the behavior of the agent to attack the forthcoming host). Apart from the research literature, the existing agent tools also provide the protection mechanism for the attacks given in Table 1. For example, the Secure Mobile Agents (SeMoA) (semoa.org 2006) platform prevents the cloning of the mobile agent and killing the agent. The serious drawback of this model is it has no option to clone and kill the agent (Axel et al., 2006). But the process of cloning is a must in all the mobile agent platforms to recover the mobile agent, and the option to kill the agent is a must to discard the agent when it is executing a number of dummy requests. Likewise, the prevention mechanisms available for the platform based security require some more additional capabilities to make the environment smart.

Axel et al. (2006) pointed out that in order to minimize the risk of DoS attacks by the mobile agents, the platform should have a well-designed inherent security policy. An efficient method of restricting/granting permissions can help them to withstand the DoS attacks to some extent. It is also suggested to develop a model with the police on the platform side in order to prevent the malicious activities of the agent. Based on this, the malicious identification police like anti-virus is also proposed to protect the mobile agent platform with the agent owner privileges (Venkatesan and Chellappan, 2008).

2.2. Agent code protection

The most difficult security problem in the mobile agent environments is to protect the agents from the attacks coming from computational environments that are responsible for their execution. In fact, execution environments must access the agent's code and execution state to be able to execute them. As a consequence, it is very difficult to prevent disclosure, tampering of agent parts, or incorrect execution of agents. However, the models are developed with an effective manner for both prevention of the attack and the detection of the attack. Here the agent code has the possibility to get both the active attack (alteration on the agent code) and passive attack (impersonation of the agent code for future use). For the active attack (addressed in this paper) protection, there are two approaches, viz., preventing the attack and detecting the attack as shown in Fig. 1.

2.2.1. Prevention of attack

An effective approach for preventing the mobile agent attack is building the trusted environment (i.e., sending the mobile agent to the authenticated remote hosts). But there is no guarantee that