International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 4, Number 1 (2014), pp. 59-66
© International Research Publications House
http://www. irphouse.com /ijict.htm

Comparative Analysis of Detection and Prevention Security Techniques in Mobile Agents System

Heena[1], Gurpreet Singh[2], Ramandeep Kaur[3] and Rahul Hans[4]

[1,2,3]Dept of Computer Science and Engineering, G.N.D.U, Amritsar, Punjab, India.
[4]Dept of Information Technology, D.AV.I.E.T, Jalandhar, Punjab, India.

Abstract

Mobile agent system is a distributed computing environment that is perceived as a flexible alternative to client server technology. Mobile agents can travel autonomously through a computer network in order to perform some computation or gather information on behalf of a human user or an application. This helps in reducing network traffic to a large extent. However, it has not become popular due to some problems such as security, fault tolerance etc. The fact that computers have complete control over all the programs makes it very hard to protect mobile agents from untrusted hosts. There is not a single, comprehensive solution that provides complete protection of agents against malicious hosts. Existing solutions either only detect or to some extent prevent attacks on agents. This paper surveys various malicious host problems, techniques for keeping mobile agent secure against malicious host and comparative analysis of techniques is done based on certain parameters like agent's code, agent's result, integrity and authentication etc.

Keywords: Security; mobile agents; mobile code; malicious host;

1. Introduction

Today so many computer networks are connected to each other and spreading all over the world but when a user tries to use these resources, he has to understand the location of distributed resources, predict their current status, and select some suitable resources. Mobile agent technologies are getting popular as means for an efficient way to access to remote resources on computer networks [1]. Mobile agents are composed of code, data, and state. Agents migrate from one host to another taking the code, data and state with them. The state information allows the agent to continue execution from the point where it was before it left in the previous host. Mobile agents offer many advantages when developing network applications, as compared to traditional models.

One commonly proposed use for mobile agents is for e-commerce applications. However, the use of mobile agents is not limited to e-commerce, a number of other useful applications have been proposed ranging from network management to intrusion detection hostile hosts [2]. However, one of the main technical obstacles to a wider acceptance of the mobile agent paradigm is security. There are basically two types of security problems that must be solved.

- Host protection against hostile agents.
- Agent protection against hostile hosts.

Many techniques have been developed for the first kind of problem but it is believed that the execution environment (host) has full control over executing programs thus protecting a mobile agent from malicious hosts is difficult to achieve [3].

The rest of the paper is organized as follows: Section 2 deals with various security issues in mobile agent paradigm, Section 3 deals with the malicious host problem which can be caused by spying the code, data or state of the mobile agent by malicious hosts, Section 4 give an overview of various security techniques proposed in mobile agent technology, Section 5 deals with conclusions and future work.

2. Security Issues in Mobile Agent Paradigm

Different security requirements that the mobile agent paradigm needs to satisfy [1]:

2.1 Confidentiality

It is important to ensure that the information carried by a mobile agent or stored on a platform is accessible only to authorized parties. Agent frameworks must be able to ensure that their intra and inter-platform communications remain confidential.

2.2 Integrity

The agent platform must protect agents from unauthorized modification of their code, state, and data.

2.3 Accountability

Platforms need to establish audit logs to keep track of all visiting mobile agent's actions in order to keep them accountable for their actions.

3. The Malicious Hosts Problem

In the mobile agent paradigm, the hosts have full control over the mobile agents running on them so some of the attacks that could be performed by malicious hosts to the mobile agents, which are totally controlled by them [1]:

3.1 Spying

Spying focuses on understanding the data, code of the mobile agent and to use it for further malicious actions.

3.2 Thieving and Pirating

Based on successful spying, the host could either steal data or pirate code from the agent.

3.3 Manipulation

The malicious host could modify mobile agent information by performing an insertion, deletion and/or alteration to the agent's code, data, and execution state or return wrong system call result without being known by the agent's environment.

4. Security Techniques Proposed in Mobile Agent Technology

For wide scale applications, the approaches to protect an agent can be broadly classified into two main mechanisms:

- Detection mechanism attempt to detect unauthorized modification of code, state or execution of mobile agent.
- Prevention mechanisms try to make it impossible to access or modify code, state or data of mobile agent.

4.1 Detection Techniques

The detection techniques which are used to detect unauthorized modifications of code, state or execution of mobile agent are:-

4.1.1 Traceability Techniques

E.Oscar, F.Marcel and S.Miguel in [4] have proposed two traceability techniques that are watermarking and fingerprinting. In these techniques a mark is embedded into agent and the agent's execution creates marked results. When an agent returns to its origin host, these results are examined. If the mark has changed or has disappeared, this means that the executing host has modified the agent. In agent's watermarking scheme, the mark is embedded into mobile agent's code because all executing hosts in the agent's itinerary must run the same marked code. But in agent's fingerprinting scheme, the embedded mark is different for each host because mark is embedded into agent's data and data is usually different for each host.

The main advantages are that these techniques are used to detect manipulation attacks performed during agent's execution and also trace the malicious host responsible for the manipulation attacks. The main advantage of mobile agent's fingerprinting technique over watermarking technique is that it avoids collusion attacks performed by a group of dishonest users.

The main drawbacks of these techniques are increase in its code and data size because embedding a mark always means that some overhead is added to the mobile agent. Moreover, a TTP (Trusted third party) is needed in order to punish malicious behavior.

4.1.2 Mutual Itinerary Recording

A.J Wayne in [3] has proposed a general technique that allows an agent's itinerary to be recorded and tracked by another cooperating agent and vice-versa, in a mutually supportive arrangement. When moving between agent platforms, an agent conveys the last platform, current platform, and next platform information to the cooperating peer through an authenticated channel. The peer maintains a record of the itinerary and takes appropriate action when inconsistencies are noted. Attention is paid in this scheme so that an agent avoids platforms already visited by its peer.

The main advantages of this technique are that by dividing up the operations of the application between two agents, certain malicious behavior of an agent platform can be detected. Moreover, this scheme can be incorporated into any appropriate application. The main drawback of this technique includes the cost of setting up the authenticated channel and the inability of the peer to determine which of the two platforms is responsible if the agent is killed.

4.1.3 Itinerary Recording with Replication And Voting

A.J Wayne in [3] has proposed a technique for detecting malicious behavior of an agent platform by replicating mobile-agents and voting on results of their computation. This technique is based on the idea that rather than using a single copy of an agent to perform a computation, multiple copies are used. Although a malicious platform may corrupt a few copies of the agent, enough replicas avoid the encounter to successfully complete the computation. This technique seems appropriate for specialized applications where agents can be duplicated without problems and the task can be formulated as a multi-staged computation.

The main advantage of this technique is that this approach is taken similar to path histories, but extended with fault tolerant capabilities. The main drawback of this technique is that additional resources consumed by replicate agents.

4.2 Prevention Techniques

The various prevention techniques which make impossible to access or modify code, state or data are:-

4.2.1Multi Agent Multi-Key Approach

E.Abolfazl and M.R.Ali in [7] have proposed a novel distributed protocol for multi agent environments to improve the communication security in packet-switched networks. This approach makes use of distribution, double encryption and some other traditional methods such as digital signature. In this approach the encrypted message and encrypted private key are broken into different parts carrying by different agents which makes it difficult for malicious entities to extract the private key for message encryption, while the private key for the encrypted key is allocated on the predetermined destination nodes. Every part is assembled and decrypted by different mobile agents along different routes to the destination.

The main advantages are that double encryption used in this approach prepares an appropriate infrastructure for today critical areas such as e-commerce or NCW. The main drawback of this technique is that the computation load of the approach is larger.

4.2.2Environmental Key Generation

S. Rajan in [1] has proposed a scheme for allowing an agent to take predefined action when some environmental condition is true. This approach is based on constructing agents in such a way that upon encountering an environmental condition (e.g., via a matched search string), a key is generated, which is used to unlock some executable code cryptographically. The environmental condition is hidden through either a one-way hash or public key encryption of the environmental trigger. The procedure is somewhat similar to the way in which passwords are maintained in modern operating systems and used to determine whether login attempts are valid.

The main advantage is that this technique ensures that a platform or an observer of the agent can’t uncover the triggering message or response action by directly reading the agent’s code. The main drawbacks of this technique are that a platform, which completely controls the agent, could simply modify the agent to print out the unlocked executable code upon receipt of the trigger, instead of executing it. Moreover, an agent platform typically limits the capability of an agent to execute code created dynamically.

4.2.3 Computing With Encrypted Functions

A. Mousa and B.Ljiljana in [5] have proposed a software solution for secure execution of mobile agents under untrusted execution environment. In this, agent owner made its code hidden from the remote host on which it executes to maintain privacy. Home platform has an algorithm in form of function f. At remote site, the target host has data (input) x and it computes f(x) to provide services to agent. To secure the function f so that remote host cannot read this, home platform encrypts the function f to get E (f) and then embodies encrypted function within program. Home platform inserts this program within agent code and sends it to remote host platform for execution. The target platform runs program on input x and produces E (f(x)), then the generated output (final results) is sent back to its home platform. Home platform decrypts it and gets f(x).

The main advantage is that this mechanism enables the agent to execute in secure manner at remote untrusted platforms. The main drawback is that it is not capable to prevent the system from denial of service attack and replay attack.

4.2.4 Generated Sub-Agent Mechanism

A.M. Tarig in [8] has proposed a Generated Sub-Agent Mechanism (GSAM) to protect mobile agents against malicious hosts. The mobile agent system classifies the hosts into two types trusted and untrusted hosts. The main idea of GSAM is to generate a sub-mobile agent from the mobile agent in case the mobile agent will visit untrusted host. After the sub-mobile agent completes its work, it returns to the original mobile agent location and the mobile agent continues its journey. By this way, the untrusted host could not reach the content of the mobile agent and it couldn't attack the mobile agent behavior.

The main advantage is that by increasing the number of untrusted host this mechanism reduces the mobility time cost. The main drawback is that execution of sub-mobile agent in the untrusted host sometimes affects the efficiency and other factors.

5. Conclusions and Future Work

This paper surveys the various state of art of security techniqes in mobile agent systems which are broadly classified into detection and prevention techniques. It discusses the security threats and requirements that need to be met in order to improve those threats and also presents some of the main issues in the security of mobile agents against attack from malicious host. None of the existing techniques provides an optimal solution for all scenarios. However, a combination of various techniques may yield powerful solutions. The comparative analysis of various security techniques is done based on ceratin parameters.

As every technique has its own pros and cons depending upon the nature of network or environment. In future a cryptographic technique with predefined fault tolerant time can be applied so that agent owner can rescue the data collected by agent during its itinerary and also protect the mobile agent's data from malicious hosts.

Table 1: Comparative analysis of different security techniques based on certain parameters in mobile agent technology [6]

Countermeasures	**Category**	**Security Objective**			**Security Services**				
		Agent's Itinerary	**Agent's Code**	**Agent's Result**	**Authentication**	**Integrity**	**Confidentiality**	**Accountability**	**Protection from Colluded Attacks**

Traceability Techniques	Detection	N	N	N	N	Y	N	N	Y(Watermarking)
									N(Fingerprinting)

Mutual Itinerary Recording	Detection	N	Y	Y	Y	Y	N	Y	Y
Itinerary Recording with Replication and Voting	Detection	N	Y	Y	N	Y	N	Y	N

Multi Agent Multi-Key Approach	Prevention	Y	Y	Y	Y	Y	Y	N	N
Environmental Key Generation	Prevention	N	Y	N	Y(Platform Authentication)	N	Y(Code Confidentiality)	N	N
Computing With Encrpted Functions	Prevention	N	Y	N	N	N	Y(Code Confidentiality)	N	N
Generated Sub-Agent Mechanism	Prevention	N	N	Y	N	Y	Y	N	N

References

[1] Rajan Sahota," An Overview of Security Techniques to Protect Mobile Agent from Malicious Host", International Conference on Computing and Control Engineering, 12 & 13 April, 2012.

[2] L. L. Thomsen and B. Thomsen," Mobile Agents—The New Paradigm in Computing", ICL Systems Journal, pp.14-40, May 1997.

[3] Wayne A. Jansen," Countermeasures for Mobile Agent Security", Computer Communications 23 (17), 1667–1676, pp. 1-14, 2000.

[4] Oscar Esparza, Marcel Femandez and Miguel Soriano," Protecting Mobile Agents by Using Traceability Techniques ", IEEE International Conference on Information Technology, pp.264-268, 2003.

[5] Mousa Alfalayleh and Ljiljana Brankovic," An Overview of Security Issues and Techniques in Mobile Agents", 8th IFIP TC-6 TC-11 Conference on Communications and Multimedia Security, 2005.

[6] Shashank Srivastava and G.C Nandi," Protection of Mobile Agent and its Itinerary from Malicious Host", IEEE International Conference on Computer & Communication Technology, pp. 405-411, 2011.

[7] Abolfazl Esfandi and Ali Movaghar Rahimabadi," Mobile Agent Security in Multi Agent Environments Using a Multi Agent-Multi key Approach", 2nd IEEE International Conference on Computer Science and Information Technology, pp. 438-442, 2009.

[8] Tarig Mohamed Ahmed," Generate Sub-Agent Mechanism to Protect Mobile Agent Privacy", IEEE Symposium on Computers & Informatics, pp.86-91, 2012.