Security Techniques in Mobile Agents: A Review

[1]Yashwant Kumar, [2]Umesh Kumar, [3]Mohit Gambhir
[1]M.Tech Research Scholar, [2]Assistant Professor, [3] CEO
[1,2]Department of Computer Engineering
[1,2]J.C. Bose University of Science and Technology YMCA, Faridabad, India
[3]Verispire Technologies Pvt. Ltd. India

ABSTRACT: This survey present the various security mechanism and issue related to mobile agent security. It describes the various security approaches and mechanism applied to the mobile agent system security. Security is one of the major issues with mobile applications as they can be attacked by malicious users which increase the complications with data privacy and data protection. The paper analyses the security threats and the countermeasure of mobile agent system. The primary issue in the security of mobile agent system is to protect mobile agent from malicious attack launched by the intruder. It presents possible threats to the mobile agent paradigm and distinguishes between detection and prevention security mechanisms. The main objective of this work is to analyze the security mechanism of Mobile agent security.

***IndexTerms*- Security, Mobile Agent, Countermeasures, Privacy, Protection**

1. INTRODUCTION

A mobile agent can be thought of as a software program, which can travel from one place to another. It is a program that can conquer from host to host in a network of heterogeneous computer system and fulfill a task specified by its originator. There are various advantages of mobile agent paradigm such as, it overcome network latency and also reduce network traffic. It improves robust and fault tolerance behavior. In a software system when agents are distributed among various networks they must be ready to face the challenges of classic security problems such as integrity attack, breach of confidentiality. There are some drawbacks in mobile agent technology, in the area of privacy and security.

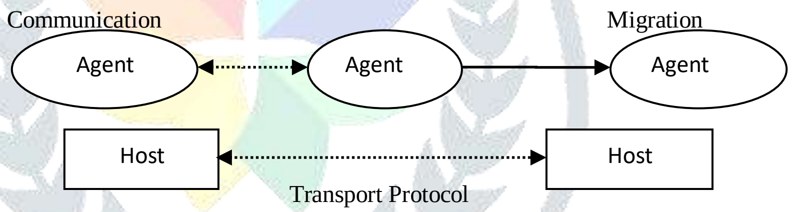

Fig 1 Mobile agent system reference model

The various problems such as to protect the host from malicious mobile agents such as virus and Trojan horses. Threats radiate from an agent attacking an agent platform, an agent platform attacking an agent, and an agent attacking another agent on the agent platform. Over the past years mobile agent becomes more important in many areas of computer science such as distributed system, robotics autonomous system and in artificial intelligence.

2. MAIN FORMS OF ATTACK BY HOSTS ON MOBILE AGENTS

- A host masquerading as another host
- Eavesdropping on agent activity
- Denial of service by the host to the agent
- Alteration of the agent by the host

2.1 Masquerading

Normally, the host sends the agent to a receiver host to make sure of the agent's identity. This receiving host can be malicious and pretends to be the correct receiver host, and can thus proceeds by attacking the agent's code, data or flow control. An agent may pose as a well-known vendor of goods and services, for example, and try to convince another unsuspecting agent to provide it with credit card numbers, bank account information, or other private information.

2. 2 Eavesdropping

It occurs when the host spies on the agent and gathers information about the mobile agent’s information or about the intercommunication between agents Mobility of mobile agent requires additional security measures.

.

2.3 Denial of Service

The host can refuse to execute the agent or deny its execution. But constructing a protocol to force the host to proof the execution of each agent can solve this problem. For instance marking hosts that are unwilling to execute agents as bad hosts, and instructing agents not to visit any bad hosts can do this.

A malicious agent platform, however, may ignore agent service requests, introduce unacceptable delays for critical tasks such as placing market orders in a stock market, simply not execute the agent’s code, or even terminate the agent without notification.

2.4 Alteration

In the alteration attack a malicious platform attack to change the mobile agent information by performing various operations such as insertion, deletion or modification of the mobile agent code as well as data.

3. DETECTION TECHNIQUES

3.1 State Appraisal [Farmer et al. 1996]

The goal of State Appraisal is to ensure that an agent has not been somehow subverted due to alterations of its state information. The success of the technique relies on the extent to which harmful alterations to an agent's state can be predicted, and countermeasures, in the form of appraisal functions, can be prepared before using the Agent [1].

3.2 Recording of Mobile Agent Path History [Ordille 1996]

The basic idea behind Path Histories is to maintain an authenticable record of the prior platforms visited by an agent, so that a newly visited platform can determine whether to process the agent and what resource constraints to apply [2].

3.3 Partial Result Encapsulation [Jansen 2000]

Partial Result Encapsulation (PRE) is a detection technique that aims to discover any possible security breach on an agent during its execution at different platforms. PRE is used to encapsulate the results of agent execution at each visited platform in its travel path. The encapsulated information is later used to verify that the agent was not attacked by a malicious platform. The verification process can be done when the agent returns to its home platform or at certain intermediate points in its itinerary [3].

3.4 Execution Monitoring [Jansen 2000, Alfalayleh and Brankovic 2005]

Execution tracing is a technique for detecting unauthorized modifications of an agent through the faithful recording of the agent's behavior during its execution on each agent platform[4].

3.5 Replication and Voting [Alfalayleh and Brankovic 2005]

This approach is suitable where agents can be duplicated without problems and survivability is the major concern. The drawbacks are the additional resources consumed by replicated agents and message complexity increased [4].

3.6 Sedentary Agents [Ouardani et al. 2007]

In this technique a security protocol to ensure the protection of mobile agents from malicious host by using cooperating sedentary agents. It combines various techniques such as namely, reference states, encryption and digital signature [5].

4. PREVENTION TECHNIQUES

In the prevention technique it is concerned with mobile agent protection against malicious platforms. These techniques are mainly concerned with security requirements such as confidentiality, availability, integrity and non repudiation of the mobile agent.

4.1 Code Obfuscation [Hohl 1998]

Code Obfuscation is a black-based mechanism to protect agent from malicious platform. . First of all, obfuscation hinders manual inspection of program internals. By renaming variables and functions, and breaking down structures, it protects against reverse-engineering. It protects both storage and usage of keys, and it can hide certain properties such as a software fingerprint or a watermark, or even the location of a flaw in case of an obfuscated patch.

Obfuscation can also be used for application such as protecting digital watermarking, enforcement of software licensing. There are some code obfuscation technique which reduces the size of the code and speed up its execution [6].

4.2 Computing with Encrypted Functions [Reiser and Vogt 2000] [Lee et al. 2004] [Fontaine and Galand 2007]

Computing with encrypted function provide a safe mechanism through age Execution tracing is a technique for detecting unauthorized modifications of an agent.

Through the faithful recording of the agent's behavior during its execution on each agent platform it can execute encrypted task in secure environment in respect to maintaining the meet the requirements of confidentiality and integrity [7].

4.3 Environmental Key Generation [Filiol 2005]

The environmental key generation methods provide functionality to agent with having ability to perform the action whenever predefined condition is met.

It describes a scheme for allowing an agent to take predefined action when some environmental condition is true. The approach centers on constructing agents in such a way that upon encountering an environmental condition [8].

4.4 Separation of Privilege[Al-jaljouli and Abawajy 2007]

In this technique agent negotiate frame work to divide the task between three agents. It is done because to limit the damages that can be done to agent by malicious nodes [9].

4.5 TAMAP [Hacini et al 2007]

This scheme is based on trust based to secure the mobile agent from malicious platform. This scheme based on the communication between agent and the platform. In this the agent collects the information about its execution platform that is used [10].

TABLE 1: Comparison of Security Techniques in Mobile Agent

S. NO.	Author and Year	Techniques used	Use or Function of algorithm	Advantages	Disadvantages
1.	Farmer et al. [1996]	State Appraisal Technique [DETECTION]	In this technique the author, who creates the mobile agent, produces a state appraisal function. This function calculates the maximum set of safe permissions that the agent	This technique provides a flexible way for an agent to request permissions depending on its current state and on the task that it needs to do on that particular platform.	The main problem with this technique is that it is not easy to formulate appropriate security properties for the mobile agent and to obtain a state appraisal function that guarantees those

			could request from the host platform, depending on the agent's current state.		properties.
2.	Ordille [1996]	Recording of Mobile Agent Path History Technique [DETECTION]	When an agent travels through a multi-hop itinerary, it visits many platforms that are not all trusted to the same extent. The "Path History" is constructed in the following way. Each visited platform in the mobile agent's travel life adds a signed record to the Path History.	It maintains an authenticable record of the prior platforms that are visited by an agent.	The main problem with the Path History technique is that the cost of the path verification process increases with the path history.
3.	Hohl [1999]	Reference States Technique [DETECTION]	This technique computes the reference states. It assumes that the agent code is constant, while data and execution states are considered to change.	It Detect the malicious attack by the attacker.	It is not suitable on large scale mobile agent data.
4.	Jansen [2000]	Partial Result Encapsulation Technique [DETECTION]	Partial Result Encapsulation (PRE) is a detection technique that aims to discover any possible security breaches on an agent during its execution at different platforms.	This technique helps to detect different types of tampering.	The main problem occurs when a malicious platform retains copies original keys.
5.	Jansen [2000]	Digital Signatures Technique [DETECTION]	Digital signatures can be used to detect tampering on mobile agent code and data. The resultant encrypted hash can be attached to the mobile agent so that the platform can authenticate the agent owner and verify integrity of the agent code.	Digital signatures applied by a trusted platform can be used to enforce integrity of agent code and data.	Protecting mobile agent code and data when they visit malicious platforms is a difficult task.
6.	Jansen [2000], Alfalayleh, and Brankovic [2005]	Execution Monitoring Technique [DETECTION]	It is a technique to detect unauthorized modification of an agent. A trace is composed of platform signature information and a sequence of statement identifiers.	When any suspicious result occurs, the appropriate traces and tray summaries can be obtain and verified.	The problems which are identified in this technique leads to lack of accommodating multi-threaded agents.

7.	Alfalayleh and Brankovic [2005]	Replication and Voting Technique [DETECTION]	The technique provides fault tolerance to counter effects of malicious environments that could attempt to alter computational results. This technique provides a mechanism for detecting malicious behavior of an agent platform by replicating mobile agents and voting on results of their computation	It provides fault tolerance to counter effects of malicious environments.	Leading to inconsistency of agent data.
8.	Ouardani et al. [2007]	Sedentary Agents Technique [DETECTION]	It protects mobile agents from malicious hosts. It performs single hop migration	This scheme helps to estimate the amount of time required to execute an agent.	Not suitable on large area network.
9.	Hohl [1998]	Code Obfuscation Technique [PREVENTION]	It is as a black-box-based mechanism for protecting agents against malicious platforms. During this timed obfuscation interval, an attacker will not be able to discover relevant data or to manipulate the agent execution.	Obfuscation can also be used for other applications such as protecting digital watermarking, enforcement of Software licensing, and protecting protocols from spoofing.	However, not so much has changed concerning the development of this technique for mobile agent security since 1998 when it gained attention for mobile agent security.
10.	Reiser and Vogt [2000] Lee et al. [2004] Fontaine and Galand [2007]	Computing with Encrypted Functions Technique [PREVENTION]	The goal of Computing with Encrypting Functions is to determine a method whereby mobile code can safely compute cryptographic primitives, such as a digital signature.	Prevent the data by using various techniques.	It does not prevent denial of service, replay, experimental extraction, and other forms of attack against the agent.
11.	Filiol [2005]	Environmental Key Generation Technique [PREVENTION]	It describes a scheme that allows an agent to take predefined action when the condition is true.	It ensures that a platform of the agent cannot uncover the trigging response action by directly reading the agent's code.	In this agent platform limits the capability of an agent to execute code created dynamically.
12.	Molm et al. [2000], Ramchurn et al. [2005]	Trust Management Schemes Technique [PREVENTION]	It provides a measure for correct behavior and interaction acceptance between mobile agents and platforms.	It dynamically adapt security techniques to their execution environment	It uses trusted third party to undertake the verification process of execution traces.
13.	Al-Jaljouli and Abawajy [2007]	Separation of Privileges Technique [PREVENTION]	This technique is used agent-mediated negotiation framework to split tasks between the agents. This is done in order to minimize damages that can be done to the agent by malicious platforms.	Suitable for the prevention of data.	This scheme is not foolproof. The mission critical tasks also depend on the so-called noncritical tasks. This implies that even with separation of roles, critical tasks can still be affected.

4. CONCLUSION

Conventional network management approach is based on client server model, suffers from problems like network delays, lack of scalability, information bottleneck and excessive processing load at manager and heavy usage of network bandwidth. The mobile agent technology gives improvements in terms of network bandwidth utilization, significant reduction of network load etc. Trust management schemes present Opportunities for mobile agents to avoid or cautiously migrate to possibly malicious platforms. The biggest challenge to trust-based schemes is that a formerly trustworthy platform can also turn malicious at a future time. This paper gives an overview about the security techniques of mobile agent against attack from malicious hosts.

5. REFERENCES

[1] Farmer, W., Guttman, J., and Swarup, V.1996. Security for mobile agents: Authenticationand state appraisal. Lecture Notes in Computer Science 1146: 118–130.

[2] Ordille, J. 1996. When agents roam, who can you trust. In Proceedings of the FirstConference on Emerging Technologies and Applications in Communications.Portland, Oregon, May, pp. 5–9. IEEE Electronic Library.

[3] Jansen, W. 2000. Countermeasures for mobile agent security. Computer Communications23(17): 1667–1676.

[4] Alfalayleh, M. and Brankovic, L. 2005. An overview of security issues and techniquesin mobile agents. In Communications and Multimedia Security, Volume 175 of IFIP International Federation for Information Processing, edited byD. Chadwick and B. Preneel. Boston: Springer, pp. 59–78.

[5] Ouardani, A., Pierre, S., and Boucheneb, H. 2007. A security protocol for mobileagents based upon the cooperation of sedentary agents . Journal of Networkand Computer Applications 30(3): 1228–1243.

[6] Hohl, F. 1998. Time limited blackbox security: Protecting mobile agents frommalicious hosts. Lecture Notes in Computer Science 1419(5):92–113.

[7] Reiser, H. and Vogt, G. 2000. Security requirements for management systems usingmobile agents. Tohme, S. und M. Ulema (Herausgeber):In Proceedings of theFifth IEEE Symposium on Computers & Communications, 160–165. IEEEComputer Society, Washington, DC, USA.

[8] Filiol, E. 2005. Strong cryptography armored computer viruses forbidding codeanalysis: The Bradley virus. Proceedings of the 14th EICAR Conference,pp. 216–227. EICAR, Paris-France.

[9] Al-Jaljouli, R. and Abawajy, J. 2007. Secure Mobile Agent-based E-Negotiation for On-Line Trading. International Symposium on Signal Processing and InformationTechnology, Giza, 2007, 610–615. IEEE.

[10] Hacini, S., Guessoum, Z., and Boufaida, Z. 2007. TAMAP: A new trust-basedapproach for mobile agent protection. Journal in Computer Virology 3(4):267–283.