# Solutions for Security in Mobile Agent System

**Neelam Dayal and Lalit Kumar Aswathi**

**Abstract** For getting instant access to the data at one place, the software called 'Mobile Agent' is used, which moves from host to host and brings back the information required. With advancement in technology, access to information has become more and more easy, but it also brings certain concerns about the security of systems involved in the process and the data being used or taken. This paper is concerned with the security threats that a mobile agent system could experience and solutions that have been proposed for securing the mobile agent system. There are many solutions proposed for security; some are simulation based while some are mathematical derivation based. Simulation-based models are more practical for solving the real-world scenarios.

**Keywords** Mobile agent · Extended elementary object system model · Police office model · Mobile agent security

## Introduction

Mobile agents (MA) are autonomous software that move from one host to another for retrieving certain information. Using the itinerary table, mobile agent makes decisions about where to move and finally brings back the information to the home agent. MAs are goal directed and have the capability to suspend their execution on the current platform and move to the next platform where it resumes its execution. The final data retrieved and brought back to the home agent by the MA is called

N. Dayal (✉) · L. K. Aswathi
National Institute of Technology, Hamirpur, India
e-mail: neelu.dayal@yahoo.co.in

L. K. Aswathi
e-mail: lalitdec@yahoo.com

S. Sathiakumar et al. (eds.), *Proceedings of International Conference on Internet Computing and Information Communications*, Advances in Intelligent Systems and Computing 216,
DOI: 10.1007/978-81-322-1299-7_10, 

execution result. MA are autonomous, have learning ability, and most importantly, they are mobile. They have made retrieval of data much easier. They find application in various fields such as ecommerce, maintenance of data, and parallel processing. The final data retrieved by mobile agent through various nodes (hosts) is termed as execution results. These execution results are expected to be true and unaltered. However, if the data are altered or false, or the agent is faulty, it will be a security threat to the system. To make it possible for the host to have faith in the agent, and vice versa, it is important to assure both of them of having a secure medium of interaction.

## *Mobile Agent*

A mobile agent (MA) is a process consisting of software and data. It has two components:

1. Program code: program code and static data
2. Program execution state: variable data such as the mobile agent itinerary data and execution results.

The Mobile Agent system comprises the User, Home Agent (HA), Mobile Agent, and Platforms. User asks a particular site (Platform) for certain information that it requires. That site known as Home Agent creates software called Mobile Agent, which is further dispatched for collecting information from various sites. MA using its itinerary table moves from site to site to gather the required information. Generally, user is responsible for creating the itinerary table for the mobile agent being created, but in some cases MA is expected to make its decision itself as it is considered to be intelligent enough to choose its route by itself. When MA reaches a Platform, it requests the platform for execution; when the host platform allows the MA, MA executes itself on that platform and appends the result retrieved to its actual data. Finally, the MA takes back the result to its Home Agent. HA provides this execution result to the user who has asked for the data.

## *Security Threats*

As MA has to visit throughout the network and also has to execute itself on various platforms, it becomes exposed to various threats. In addition, if MA arriving at a platform is malicious it is a threat to that platform also. Based on these two aspects security is concerned with securing both MA and the platforms on which it is executing.

Hence there are two categories of concern for securing the MA system:

A. *Mobile agent security*. Mobile agent security is concerned with securing the MA that has to travel through a vast insecure network and has to execute on some other platform. There might be various possible attacks on this MA such as:

   (i) *Traveling from one platform to other*. While traveling through one platform to another there are possibilities that the MA could be attacked by eavesdrops. The data being carried by the MA and also the execution code are at risk during this movement.
   (ii) *Threat by host*. When MA is executing on a Host platform that is malicious, it could harm the executing MA. Host can harm the data carried by the MA of other sites. In order to dominate in business the host can alter the information provided by other sites that is carried by MA to it. Host can also change certain execution codes so that when MA executes on other sites, it damages those sites and their data. There could be possibilities that the host on which MA is executing is forged, hence it is dangerous for the MA.
   (iii) *Threats by other agents*. There are possibilities that when MA is executing on a platform, there are several other MAs being executed on that platform. If any of these MAs are insecure it could create a security threat for other MAs and harm the data carried by them.

B. *Host security*. A malicious or forged MA could be a threat to the host on which it is being executed. MA could ask for critical information about the host that could be used to harm it. If malicious MA gains access to the sensitive data, it can use this information against the host. Also, denial of service attacks is possible on the host by malicious mobile agent.

## Security Approaches

Many researches have tried to solve issues of providing a secure and reliable interaction between mobile agent and host. These approaches can either be implemented for securing MA or the Platform or a model could be derived for securing both the systems. Some approaches are:

### *For Securing Platform*

*Authentication and authorization* [1, 2]. Platform must allow only authentic MAs to be executed; this will protect host from forged MAs.

*Sand boxing* [3]. The main concept behind sand boxing is to isolate the MA command lines into different parts; safe command line codes and unsafe command

line codes. The safe codes are directly allowed to be executed, while the code that seems to be unsafe is either made safe or denied for execution.

*Software-based fault isolation* [4]. The entire software is isolated into different modules for identifying unsafe (fault domains) modules. The unsafe modules are allowed to execute under separate allocated space so that it may not affect other modules. This method is useful for identifying the software

*Signed code* [5, 6]. This technique makes use of digital signature. Authenticity of the MA can be ensured to the host if the originator digitally signs the MA. Digitally signed MA ensures that it is a genuine agent originated from a genuine platform. Hence its authenticity and integrity are ensured.

*State appraisal* [7]. Appraisal functions are used to determine the privileges that are granted to the MA, so that access to the MA could be controlled by the host platform. Hence, it is a type of access control function used by the platform. These appraisal functions are determined by the platform that creates the MA. This scheme has to do with the privileges to an MA, but has no specification about attacks on MA code that has privilege to access the data.

*Path history* [8, 9]. In this scheme the MA carries the records of all the platforms it has visited, i.e., the history of the path followed by MA is carried with it. When MA arrives at a new platform, the platform checks for its path history. If all the platforms visited previously are trusted, MA is allowed to execute. If any of the previously visited sites is untrusted, platform will not allow the MA to execute. This scheme only takes care of possible attacks by a platform; however, if the MA has been attacked while on the move in the network, there is no solution for such situation.

*Proof carrying code* [10]. In this scheme the creator of the MA has to provide the proof of MA being secure and authentic. The originator attaches the proof that the MA fulfills the security requirements needed with it. It allows hosting platform to verify the identity of MA, hence making it easy for host to decide whether to allow the MA to execute or not. All this is done by HA, hence it reduces the burden of the hosting platform, as it now has to check the authenticity of MA based on the details provided.

## *For Securing Mobile Agent*

*Trusted platform*[11]. Security of the MA can be guaranteed if the MA is executing itself on a trusted platform. The platform on which the MA has arrived must provide the proof that it satisfies all the security requirements and is a secure platform, only then will the MA start executing itself on it. Hence, a mutual authentication can provide assurance for a secure MA system.

*Encrypted algorithms*[12, 13]. MA is transmitted from the HA to various platforms in encrypted format. When it reaches the host platform, if the host is authentic and has the key to decrypt MA, it can decrypt the MA and only then it is executed. Security of this scheme is completely dependent on the Key shared

between the platforms. If this shared secret (key) is retrieved or hacked by an intruder the whole security system fails. The intruder can easily access the MA and misuse its information, and may also alter its code to harm other platforms. Here, this security scheme lacks in guaranteeing the security of the system, mainly for the MA.

## Model for Secure Mobile Agent System

Many scientists have also tried to guarantee the security of the complete MA system that includes security of the MA, platforms, and the underlying network. This paper is mainly concerned with schemes that have provided simulation-based models for providing the secure system. These models represent the whole system in a graphical manner so that it is easy to understand the system and analyze the security of the system in spite of using mathematical derivation-based proofs. Some of the important graphical models for securing mobile agent system are underlined below.

### *Extended Elementary Object System Model [14, 15]*

EEOS model is based on the elementary object system (EOS) that was proposed by Valk[16] for modeling workflow and flexible manufacturing system. It is based on Object Petri Net (OPN) system of representation of transaction processing. Since MA system is concerned with the mobility of the MA throughout the network, EOS is one of the most suitable methods for representing this mobility. MA in the MA system is represented using the object nets in the EOS, platforms are represented by system nets, and the movement of the MAs and various tokens are represented by the transaction arcs. EOS was not as it is used in the EEOS model, there were few additions in the existing system for representing various features of Mobile Agent system. The additions made to the EOS system were: Multiple System Nets for representing multiple platforms, multiple layers for representing multiple layered architecture, Token pool for representing complex network environment, two new arcs for representing transactions in a better way, and extended interaction relation.

This model defines three layers of the Mobile agent system. The first layer is a Platform layer; it contains mobile agent and token pool, and is a system net having Mobile Agent as object net. It defines the migration of mobile agent to various platforms. Various places and transitions are defined in the system for representing how the movement should take place and what the result will be of each transition. It helps in identifying the abnormal behavior of MA if it is attacked. Hence, the system security can be ensured. The second layer is the mobile agent layer that contains security mechanisms; it is system net for the security mechanism layer.

This layer represents the processes taking place in mobile agent and also defines the security mechanism for the MA execution. The third layer is the security mechanism layer that defines how the MA has to behave. If the MA has been attacked it will behave in an abnormal manner, this abnormal behavior would be tracked by this security mechanism, and hence attack is detected.

This model is suitable for the detection and avoidance of attacks on the mobile agent system. It provides the mutual authentication and dynamic tracking of the movement of mobile agent and could prove an effective solution for security of MA system. However, its shortcomings are that it is really a complex model to be implemented and could prove costly.

### *Police Office Model [17]*

POM is based on the concept of the Police Office system. All the hosts in the system are divided into different groups, with a particular host in each group allotted the duty of Police Office (PO). This PO has the same duty as a police office in the real-world scenario to ensure the security of the system. Whenever any Mobile agent tries to enter the group to interact with any of the hosts in the group, MA has to contact the PO. If PO authenticates the MA to proceed further, only then can it interact with the desired host, else it will not be allowed to move further. The responsibility of security comes to the host that works as PO. It can lead to the bottleneck problem, but for networks with less traffic it is an appropriate model.

### *Novel MA Security Mechanism [18]*

This method integrates the trusted platform module into the platform for determining the security of the system. Integrity of data contained by the MA is the prime concern of the novel security mechanism. The model is based on the interaction between two agents; task agent (TA) and security agent (SA). When an MA is dispatched, SA is sent to a trusted anonymous third party (ATP). With the movement of the MA the TA also moves to various hosts. When a TA moves to a new host, SA sends an integrity report to it and checks for the integrity of the data. The MA can freely move in the system anywhere it wants to and its integrity is assured by the SA assisted with the ATP, a trusted third party. This approach is appropriate when MA has to determine its movement itself without the help of itinerary table.

## Conclusion

As the mobile agent has to move in the whole network whether secure or insecure, it also has to interact with different hosts, hence its security becomes of utmost importance. Various researches have provided different solutions to the security issues discussed in this paper. All these solutions provide security to the mobile agent to some extent. Simulation-based security systems are more appropriate to the real-world scenario. Recently, researchers have developed simulation-based models for solving the overall security issues in the mobile agent system. The security aspect covers securing the mobile agent, the host, and the underlying network. A security model is complete when it covers all these aspects. Simulation-based methods can easily represent the overall mobility and can help in detecting and avoiding attacks on the system. These approaches have solved a number of issues related to MA system security. Yet, flaws remain that need to be overcome in the future to provide a better security system, to utilize the Mobile agent system in a better way.

## References

1. Gray, R. S.: Agent TCL: a flexible and secure mobile-agent system. In: Proceedings of the Fourth Annual Tcl/Tk Workshop (TCL) 96, pp. 9–23 Monterey, California, (1996)
2. Farmer, W.M., Guttman, J.D., Swarup, V. (1966) Security for mobile agents: Authentication and state appraisal. Proceedings of th 4th Europian Symposium on Research in Computer Security (ESORICS'96), Rome, Italy pp.118–130
3. Gong, L.: New security architectural directions for java extended abstract. In: Proceedings of IEEE COMPCON, pp. 97–102 San Jose, California, February (1997)
4. Wahbe, R., Lucco, S., Anderson, T.E., Graham, S.L.: Efficient software-based fault isolation. In: SOSP'93: Proceedings of the fourteenth ACM symposium on operating systems principles. ACM, New York, pp. 203–216 (1993)
5. Jansen, W., Karygiannis, T.: Mobile agent security. In: Nist special publication 800-19 - (2000)
6. Wang, C., Zhang, F., Wang, Y.: Secure web transaction with anonymous mobile agent over internet. J. Comp.Sci. Technol. **18**(1), 84–89 (2003)
7. W. M. Farmer, J. D. Guttman, V. Swarup, S. Wakid, J. Davis, (eds.), In: Security for mobile agents: Authentication and state appraisal, Proceedings of the 19th National Information Systems Security Conference, Vol. 2, pp. 591–597, Baltimore Convention Center, Baltimore, Maryland, Oct 22–25, (1996)
8. Chess, D., Grosof, B., Harrison, C., Levine, D., Parris, C., Tsudik, G.: Itinerant agents for mobile computing. IEEE Pers. Commun. **2**(5), 34–49 (1995)
9. Bellavista, P., Corradi, A., Montanari, R., Stefanelli, C.: A mobile computing middleware for location and context- aware internet data services. ACM Trans. Int. Technol. **6**(4), 356–380 (2006)
10. Necula, G.C., Lee, P.: Safe kernel extensions without runtime checking. SIGOPS Oper. Syst. Rev. **30**, 229–243 (1996)
11. Peine , H., Stolpmann, T.: The architecture of the platform for mobile agents. In: Proceedings of the First International Workshop on Mobile Agents. Springer-Verlag, London, pp. 50–61 (1997)

12. Hohl, F.: Time limited blackbox security: protecting mobile agents from malicious hosts. In: G.Vigna (ed.) Mobile Agents and Security, pp. 92–113. Springer-Verlag, London (1998)
13. Sander, T.: On cryptographic protection of mobile agents. In: Proceedings of the 1997 Workshop on Mobile Agents and Security. University of Maryland, Baltimore, USA Oct (1997)
14. Ma, L., Tsai, J.J.P., Deng, Y., Murata, T.: Extended elementary object system model for mobile agent security. In: Proceedings of World Congress on Integrated Design and Process Technology, pp. 169–178, (2003)
15. Ma, L., Tsai, J.J.P.: Formal modeling and analysis of a secure mobile-agent system. In: IEEE Trans. Systems, Man Cybern.- A: Syst. Humans. 38(1), pp.180–196 (2008)
16. Valk, R.: Petri Nets as token objects—an introduction to elementary object nets. In: Proceedings of 19th International Conference on Application and Theory of Petri Nets, vol. 1420, pp. 1–25. (1998)
17. Xudong Guan, Yiling Yang, Jinyuan You. POM – A mobile agent security model against malicious hosts. In Proc. HPC-Asia 2000, pp.1165-1166, Beijing, China, May 2000
18. Lei, S., Liu, J., Xiao, J.: A novel free-roaming mobile agent security mechanism by trusted computing technology. In: 2008 International Conference on Computer Science and Software Engineering 12–14 Dec Wuhan, China
19. Borselius, N.: Mobile agent security. Electron. Commun. Eng. J. **14**(5), 211–218 (2002)
20. Dewi Agushinta, R., Suhendra, A.: Secure mobile agent system in peer-to-peer networks: a review of security mechanisms based on several security issues. In: Proceedings of IEEE World Congress on Software Engineering Xiamen, China, 19–21 May (2009)
21. Hasan, M.B., Prasad, P.W. C.: A review of security implications and possible solutions for mobile agents in e-commerce. In: 2009 Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA 2009), 25–26 July 2009, Monash
22. Vigna, G.: Cryptographic traces for mobile agents. In: Mobile Agents and Security, pp. 137–153. Springer-Verlag (1998)
23. Riordan, J., Schneier, B.: Environmental key generation towards clueless agents. In: G., Vigna (ed.) Mobile Agents and Security. LNCS 1419, pp. 15–24. Springer-Verlag, London April 1998
24. Balfe, S., Lakhani, A.D., Paterson, K.G.: Trusted computing: providing security for peer-to-peer networks. In: P2P'05: Proceedings of the Fifth IEEE International Conference on Peer-to-Peer Computing, pp. 117–124. IEEE Computer Society, Washington, DC (2005)
25. Sander, T., Tschudin, C. F.: Protecting mobile agents against malicious hosts. In: Mobile Agents and Security, pp. 44–60. Springer-Verlag, London (1998)
26. Silva, L.M., Soares, G., Martins, P., Renato, C., Almeida, L., Stohr, N.: JAMES: a platform of mobile agents for the management of telecommunication networks. In: G. Vigna (ed.) Proceedings of IATA99 Stockholm, Sweden, Aug 1999
27. Binder, W., Roth, V.: Secure mobile agent system using java: where are we heading? In: Proceedings of Symposium of Applied Computing, pp. 115–119 Madrid, Spain (2002)