Journal of
Information Technology & Software Engineering

Karim, J Inform Tech Softw Eng 2018, 8:1
DOI: 10.4172/2175-7866.1000220

Mini Review | Open Access

Security for Mobile Agents and Platforms: Securing the Code and Protecting its Integrity

Mohammad Rezaul Karim*

KTH Royal Institute of Technology, Stockholm, Sweden

Abstract

At present, mobile agent technology is an important research area for researcher to develop its new features, confirming its security and usability. Mobile agent is a program, which can be act in a computer network in order to perform some activities on behalf of a human user or an application. In this paper, we describe an overview of the security issues related to the mobile agent paradigm. Then we look in some existing security standards and technologies for mobile agent to analysis their goals that are keeping platform of security against a malicious mobile agent. Finally, we introduce a new framework for improvement of mobile agent security in order to secure the code and protect its integrity.

Keywords: Mobile agent; MASIF; Agent security; SSL; Encryption

Introduction

A mobile agent is a software objects or programs, typically written in script language, which can act in a computer network on behalf of a human user or an application. The mobile agent is not bound to the system where it begging its execution. It has the unique ability to transport itself from one machine to another machine in a heterogeneous network, in order to perform some computation or gather information such as collecting filtering and processing of information. The mobile agent can suspend its execution at an arbitrary point, transport to another platform and resume execution in the new platform as shows in Figure 1. In Figure 1, an agent is carrying a mail message to transport first to a router and then to the recipient's mailbox. The agent can perform arbitrarily complex processing at each platform in order to ensure that the message reaches the intended recipient. There are numerous advantages of using mobile agent paradigm such as reduce network traffic, overcome network latency, introduces concurrency, improves robust and fault tolerance behavior, dynamically updates server interfaces, operation in heterogeneous environments and so on. In the traditional client/server model, mobile agents have some advantages such as follows:

- Efficiency and flexibility
- Fault tolerance
- Convenient paradigm
- Customization

There are some limitations of mobile agent's technology, chiefly in the area of security that can raised many concerns of agents' security. The authors study two different points of view, in the area of mobile agent security as follows [1]:

- To protect the host from malicious mobile agents such as viruses and Trojan horses that are visiting it and consuming its resources (from the platform perspective).
- To protect the agent from malicious hosts (from the mobile agent point of view).

Overview of Related Existing Work

A mobile agent is a particular class of agent programs while security is critical, when executable code is transferred across the network. While there have been quite a few papers written on the significant security concerns. Recent work in mobile agent security has mainly focused on an overview of the main security issues related to the mobile agent paradigm [1-3]. Erlaut and Panda J study the mobile agent security mechanism while describe the different security approaches to protect the mobile agents against the malicious host and using the SMA1 digest algorithm to provide the confidentiality and integrity services to the mobile agents. In the paper, Aneta Zwierko and Zbigniew Kotulski [4] propose an integrity protection mechanism for mobile agents that are protecting the code transmitted through the network. They also discuss a security scheme for detecting of tempering an agent, based on a zero-knowledge proof system.

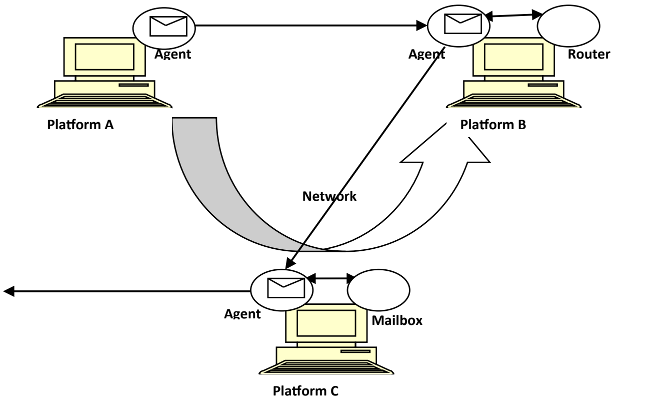

Figure 1: Mobile agent system model (example).

Security Issues of Mobile Agents and Platforms Paradigm

Now a days, security plays a very important role in developing

***Corresponding author:** Mohammad Rezaul Karim, M.S. in Information and Communication Systems Security, KTH Royal Institute of Technology, Stockholm, SE 100 44, Sweden, Tel: +004522660077; E-mail: mrka@kth.se

Received December 11, 2017; **Accepted** December 30, 2017; **Published** January 06, 2018

Citation: Karim MR (2018) Security for Mobile Agents and Platforms: Securing the Code and Protecting its Integrity. J Inform Tech Softw Eng 8: 220. doi: 10.4172/2175-7866.1000220

mobile agent system, many of them are developed without a deeper knowledge of the security, leaving it open to be taken care of in the future. However, mobile agent paradigm invokes to work in different application such as e-commerce applications that are usually expected to execute in open environments. This openness makes mobile agent systems particularly vulnerable to direct attacks. Therefore, the security of mobile agents is an important issue that is triggering much research attempt in order to finding a suitable solution.

Security threats and requirements in mobile agent

The elementary issue in the security of mobile agent systems is to protect the mobile agent platforms against malicious attacks. For this mobility property, mobile agents are disclosed to different types of threats or attacks such as masquerading, denial of service, unauthorized access, repudiation, eavesdropping, alteration, copy and replay and so on. These different types of threats are based on the following categories: agent against agent platform, agent against other agent, agent platform against an agent and external entities against agents and agent's platforms the threats on security requirements in mobile agents as follows:

- Threat on Integrity
- Threat on Availability
- Threat on Confidentiality
- Threat on Authentication

Mobile Agent System Interoperability Facility (MASIF)

In 1995 the OMG (Object Management Group) started working on a standard, called Mobile Agent Facility (MAF), in order to promote interoperability among agent platforms. Their standard which is MASIF identifies a Distributed Agent Environment (DAE) and a Distributed Processing Environment (DPE). DAE has some elements which are as follows: place (is an execution environment), agency (is an agent system) and region is a group of agencies that belong to a single authority. Two interfaces represent the core of the MASIF standard:

- MASIF Agent System: It is associated with every agency and provides operations for the management and transfer of agents.
- MASIF Finder: It is associated with a region. It supports localization of agents, agencies, and places in the scope of a region.

There are several following agent functionalities are covered by MASIF those are Agent management, Agent tracking, Agent transport, Agent and agency naming, Agent type and location syntax. Agency types provide information about important aspects of specific agencies, such as the used implementation language. The location is standardized in order to enable to locate each other. IBM developed a promising mobile agent's project called "aglets" which relies on two basic specifications: an API for aglets (J-AAPI) and the Agent Transport Protocol (ATP). IBM has explicitly stated their intention to make aglets ubiquitous. ATP and J-AAPI have been put forward as standards [5].

Secure Mobile agents (SeMoA) stands for "Secure Mobile Agents". It is about developing an extensible and open server for mobile agents. The server is written in Java, and agents can be written in Java as well (JavaSE).The focus is on all aspects of mobile agent security, including protection of mobile agents against malicious hosts. Another important feature is SeMoA's interoperability with other platforms such as Aglets and JADE, which enables you to run their agents in a SeMoA server environment [6].

Suggested Techniques for Mobile Agent Security

There are many ways mobile agent security can be enhanced. We suggest some technique so that security of mobile agent can be increased. We want to propose some idea to increase tamperproof security for mobile agent. Our proposed idea is described as Figure 2.

Tamper proof system

We want to propose some temper proof devices for our tamper proof system so that mobile agent should be more secure and maintained its privacy. For this, we want to propose some firewall devices as well as TPE's (Tamper Proof Environments) [7,8]. We want to introduce the mechanism, with which an agent can take advantage of the guarantees enforced by a TPE. In order for a user to trust in these guarantees, it is necessary that he also trusts the TPE manufacturer to properly design, implement, and produce its TPEs. In addition of this, we also want to propose time limit black-box security and also obfuscated code so that mobile agent code and data cannot be read or modified.

Secure communication channel

To increase Mobile agent security, communication security plays a vital role. We want to propose OpenSSL and SASL for communication security. OpenSSL can be used with MAST technology (Figure 3).

Enhanced secure encryption

We want to propose hybrid encryption technology. A hybrid approach which combines with Homomorphic Encryption Scheme (HES) and Function Composition (FnC) [9]. An encryption program called Mobile Agent Encryption (MAE) will intercept the three-address code from compilers, and apply HES to encrypt the operands of three-address code and FnC to encrypt codes. Now, MAE will encrypt the sensitive data, such as credit card number and personal information, stored in the operands of three address code, and scramble the code of the mobile agent to confuse mistrusted hosts. In this approach, inherits most of the strengths of mobile cryptography, ours encrypt mobile agents that are executable without decryption.

Conclusion

Mobile agent system is a very predicting paradigm that is established in several applications such as distributed information search and retrieval, e-commerce, control system, management system and so on. However, security in the mobile agent paradigm is a challenging issue to maintaining its integrity. In this paper, we discussed the main security threats ant its requirements, considering with both the mobile

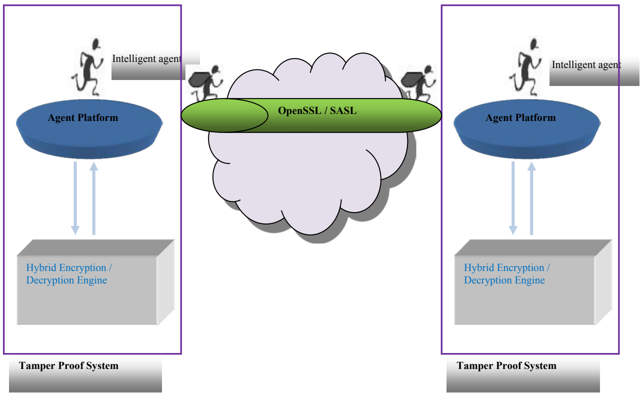

Figure 2: Proposed improvement of existing model.

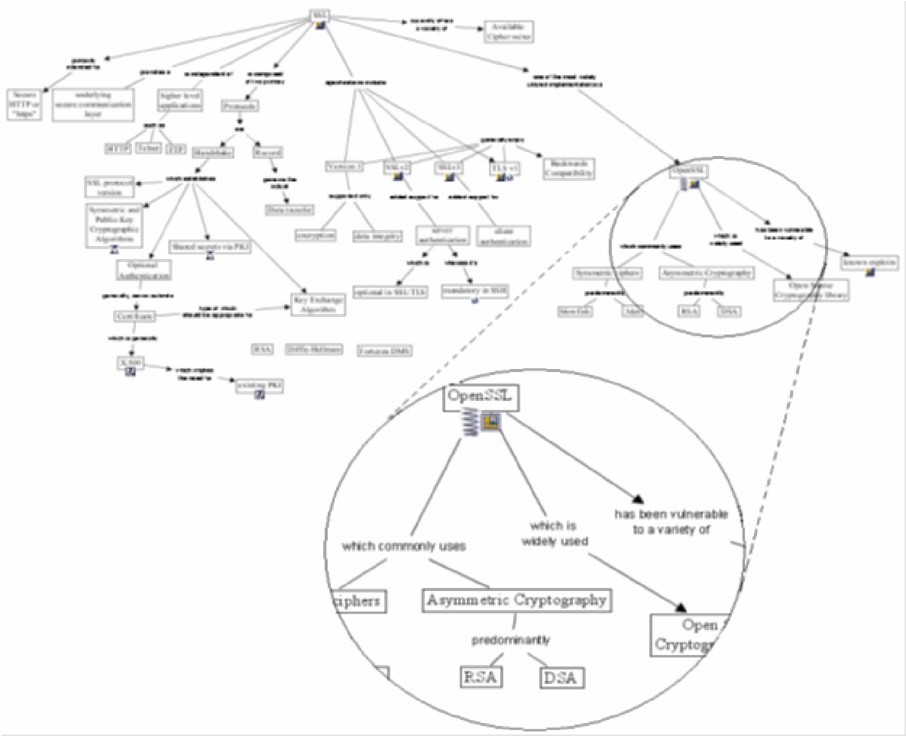

Figure 3: Exploratory mobile-agent attached to "OpenSSL" concept in CmapTools [7].

agent and the agent platform. Here, we studied the most important techniques such as Mobile Agent System Interoperability Facility (MASIF), Aglets, Secure Mobile Agents (SeMoA) and Java Agent Development Environment (JADE) for providing security in mobile agent systems. We proposed a new framework, a tamper proof system that is confirming security the agent code and protecting its integrity as best as possible, where we used some protocols and approaches such as OpenSSL/SASL, intelligent mobile agent, secure communication channel and so on. This model is secured both agents' execution state and internal data.

Future Work

At present, a board variety of security aspects of mobile agent systems such as trust, mobility, etc. and those are still uncovered. Therefore, more research is needed in order to justify enough confidence in mobile agent technology by a wide range of users. At the future work, we want to establish a new security concept for mobile agent systems to protect code and integrity, based on the cryptographic primitives such as secure secret sharing schema that is set up by a trusted authority.

References

1. Alfalayleh M, Brankovic L (2005) An overview of security issues and techniques in mobile agents. The International Federation for Information Processing, Springer 175: 59-78.
2. Jansen W, Karygiannis T (1999) Mobile Agent Security. NIST Special Publication, National Institute of Standard and Technology.
3. Borselius N (2002) Mobile agent security. JECE 14: 211-218.
4. Zwierko A, Kotulski Z (2005) Security of mobile agent: A new concept of the integrity protection. Comp Sci.
5. http://www.informatica.us.es/~ramon/tesis/agentes/Aglets1.0.3/
6. http://semoa.sourceforge.net/about/about.html
7. Carvalho M, Cowin T, Suri N (2004) MAST-A Mobile agent-based security tool. Systemics, Cybernetics and Informatics 2: 40-46.
8. http://www.isoc.org/isoc/conferences/ndss/98/wilhelm.pdf
9. Lee H, Alves-Foss A, Harrison S (2004) The use of encrypted function for mobile agent security. Presented at the 37th Hawall International Conference on System Science.