Гордеев Евгений Михайлович
Тюменский государственный университет
Институт математики и компьютерных наук
Кафедра иностранных языков и межкультурной
профессиональной коммуникации
Студент группы 25МиР1610
applepienur@gmail.com
Гаркуша Надежда Анатольевна
Тюменский государственный университет
Институт Математики и Компьютерных Наук
Кафедра иностранных языков и межкультурной
профессиональной коммуникации
Доцент, канд. пед. наук
n.a.garkusha@utmn.ru

Безопасность мобильных агентов

Gordeev Evgenii Mihailovich
University of Tyumen
Institute of Mathematics and Computer Sciences
Foreign Languages and Intercultural Professional
Communication Department
Student of 25MiR1610 gr.
applepienur@gmail.com
Garkusha Nadezhda Anatolievna
University of Tyumen
Institute of Mathematics and Computer Sciences
Foreign Languages and Intercultural
Professional Communication Department
Associate Professor, Candidate of Pedagogic Sciences
n.a.garkusha@utmn.ru

Security for Mobile Agents

Аннотация

В настоящее время технология мобильных агентов является важным исследовательским направлением для исследователей, чтобы развивать свои новые функции, подтверждая свою безопасность и удобство использования. Мобильный Агент-это программа, которая может действовать в компьютерной сети для выполнения некоторых действий от имени пользователя или приложения. В этой статье описывается обзор проблем безопасности, связанных с парадигмой мобильного агента. Затем мы рассмотрим некоторые существующие стандарты безопасности и технологии для мобильных агентов, чтобы проанализировать их цели, которые держат платформу безопасности против вредоносного мобильного агента.

Ключевые слова: мобильный агент, MASIF, безопасность агента, SSL, шифрование.

Abstract

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

Keywords: mobile agent, MASIF, agent security, SSL, encryption.

Introduction

A mobile Agent is software objects or programs, typically written in a scripting language, that can act on a computer network on behalf of a user or application. The mobile agent is not tied to the system where it asks for its execution. It has the unique ability to transport itself from one machine to another machine in a heterogeneous network to perform some calculations or gather information such as filtering and

information processing. The Mobile Agent can pause its execution at any point, transport it to another platform, and resume execution on the new platform. The agent carries the mail message for transport first to the router and then to the recipient's mailbox. The agent can perform arbitrarily complex processing on each platform to ensure that the message reaches its destination. There are many advantages to using the mobile agent paradigm, such as reducing network traffic, overcoming network latency, implementing parallelism, improving reliability and fault tolerance, dynamically updating server interfaces, working in heterogeneous environments, and so on. In the traditional client-server model, mobile agents have the following advantages:

* Efficiency and flexibility
• Fault-tolerance
* Convenient paradigm
• Setting

Overview of Related Existing Work

A Mobile Agent is a specific class of agent programs, while security is critical when the executable code is transmitted over the network. While there were quite a few documents written on essential security issues. Recently, work in the field of mobile agent security has mainly focused on the review of the main security issues related to the mobile agent paradigm. 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 article Aneta Zverko and Zbigniew Katulsky propose a mechanism to protect the integrity of mobile agents that protect the code transmitted over the network. They also discuss a safety scheme to detect agent hardening based on a zero-knowledge proof system.

Security Issues of Mobile Agents and Platforms Paradigm

Currently, security plays a very important role in the development of the mobile agent system, many of them are developed without a deeper knowledge of security, leaving it open to concern in the future. However, Mobile Agent paradigm encourages you to work in a variety of applications, such as e-Commerce applications, which

should normally run in open environments. This openness makes mobile agent systems particularly vulnerable to direct attacks. Thus, the security of mobile agents is an important issue that causes many research attempts in order to find a suitable solution.

Security threats and requirements in mobile agent

An elementary problem in the security of mobile agent systems is to protect mobile agent platforms from malicious attacks. For this, the mobility properties of mobile agents are disclosed for various types of threats or attacks, such as masking, denial of service, unauthorized access, denial of service, eavesdropping, modification, copying and reproduction, and so on. These different types of threats based on the following categories: agent platform against agent, agent against another agent, the agent Platform against agent and external entities against agents and agent platforms, threaten the security requirements in the mobile agents in the following way:

* The threat to the integrity
* The threat to availability
* Privacy risk
* The threat of authentication

Mobile Agent System Interoperability Facility (MASIF)

In 1995, OMG (Object Management Group) began work on a standard called Mobile Agent Facility (MAF) to promote interoperability between Agency platforms. Their standard, which is MASIF, defines a distributed agent (DAE) environment and a distributed processing environment (Dpe). The DAE has some elements that are as follows: place (execution environment), Agency (agent system) and region-a group of agencies that belong to the same body. Two interfaces represent the core of the MASIF standard:

* MASIF agent system: it is linked to each Agency and provides management and transfer operations.

* MASIF Finder: it is associated with the region. It supports the localization of agents, agencies and locations within the region.

There are several of the following agent functionalities covered by MASIF, those are agent Management, agent tracking, transport Agent, agent and Agency naming,

agent Type and location syntax. Agency types provide information about important aspects of specific agencies, such as the implementation language used. The layout is standardized to allow you to find each other. IBM has developed a promising mobile agent project called "aglets", which is based on two main specifications: API for aglets (J-AAPI) and Agent Transport Protocol (ATP). IBM has clearly stated its intention to make aglets ubiquitous. ATP and J-AAPI were put forward as standards.

Secure Mobile agents (SeMoA) stands for "Secure mobile agents". We are talking about the development of an extensible and open server for mobile agents. The server is written in Java and agents can be written in Java also (JavaSE). The focus is on all aspects of mobile agent security, including protection of mobile agents from malicious sites. Another important feature is the interaction of SeMoA with other platforms such as Aglets and JADE, which allows you to run their agents in the SeMoA server environment.

Enhanced secure encryption

A hybrid approach that combines with a Homomorphic encryption scheme (AES) and functional composition (FnC). The encryption program called Mobile Agent Encryption (MAE) will intercept the three-address code from the compilers and use HES to encrypt the three-address code operands and FnC to encrypt the codes. Now MAE will encrypt sensitive data such as a credit card number and personal data stored in the operands of the three address codes, and encrypt the mobile agent code to confuse untrusted Hosts.

Conclusion

The mobile agent system is a very predictive paradigm that is set in several applications, such as distributed information retrieval and retrieval, E-Commerce, management system, management system and so on. However, security in the mobile agent paradigm is a complex issue to maintain its integrity. In this paper, we discussed the main security threats and their requirements, considering both the mobile agent and the agent platform. Here we have studied the most important techniques such as Mobile Agent system Interoperability Facility (MASSIF), Aglets, Secure Mobile Agents (SeMoA) for security in mobile agent systems.

References

1. Alfalayleh M, Brankovic L An overview of security issues and techniques in mobile agents. The International Federation for Information Processing, Springer [Electronic resource] – Access mode: https://link.springer.com/chapter/10.1007%2F0-387-24486-7_5

2. Carvalho M, Cowin T, Suri N MAST-A Mobile agent-based security tool. Systemics, Cybernetics and Informatics 2: 40-46. [Electronic resource] – Access mode: http://www.iiisci.org/journal/cv$/sci/pdfs/p497873.pdf

3. Lee H, Alves-Foss A, Harrison S. The use of encrypted function for mobile agent security. [Electronic resource] – Access mode: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.76.9548&rep=rep1&type=pdf