A Secure Migration Process For Mobile Agents Form One Host to Another Host

Preeti Sharma
CSE, Lingaya's University
Nachauli, Jasana Road,
Faridabad, Haryana, 121002,
India
E-mail : preei04_sharma@yahoo.co.in

Sattyam Kishore Mishra
CSE, Lingaya's University,
Nachauli Jasana Road
Faridabad, Haryana, 121002
India
E-mail:satyam_satyam@live.com

Pragyan Verma
CSE, Lingaya's University,
Nachauli Jasana Road
Faridabad, Haryana, 121002, India
E-mail: pragya_brijesh@yahoo.com

Abstract - As a mobile agent migrates from one host to another in an open network, the security concern of mobile agent should not be neglected. For this sender and receiver to authenticate each other before agent migration use a strong authentication process. The security also aims to guarantee the integrity and confidentiality of the mobile agent while it is in transit. Both parties must authenticate each other using public**.**

Keywords: *Authentication, Autonomous operation, Confidentiality, Integrity, Mobile agent, Mobility, Secure migration process.*

I. INTRODUCTION

In the past few years the computer systems have evolved from monolithic computing device to much more complex client-server environment. Now new phase of evaluation allows complete mobility of application code among supporting platforms to form a loosely-coupled distributed system. Mobile-agent paradigm is one such technology. Mobile agents paradigm has captured researchers' and industry's attention long time ago because of its innovative capabilities and attractive applications. The mobile agents are software program that can autonomously migrate from host to host, transferring their code and internal state, enables them to accomplish tasks in network and distributed environments more conveniently, robustly, and efficiently than traditional client-server applications. But, in spite of significant benefits of the mobile agent paradigm, the technology is still mainly in a research domain and so far it has not been adopted on a large scale by the industry and users. One of the reasons for that is security related issues and security concerns.

Key Authentication, before a Secure Migration Process*:*

After successful authentication, an encrypted mobile agent is transferred and its integrity is verified by the receiver agency.

The main focus of this paper is on secure migration of mobile agent from one host to another host.

There are a variety of ways in which an attacker might cause harm:

(1) An outside attacker may intercept a migrating agent and steal sensitive data. Migrating agents might be carrying sensitive blueprints, or other data which should be kept secret.

(2) An outside attacker may intercept a migrating agent and modify it to perform a malicious action.
(3) An outside attacker may compose its own agent and send it into the agent framework. That agent might be able to disrupt systems and cause physical harm by controlling mechanical systems in an unsafe manner.

The agent paradigm has evolved into a useful technology to build distributed applications. In the agent paradigm, so-called ‘agents’ perform tasks. Mobile agents are programs capable of executing and migrating from node to node in a networking environment to perform tasks on behalf of their owners. They consist of three parts: code, a data state, and an execution state. They visit remote hosts, perform there their tasks, migrate to the next host eventually returning to the management station, where their actions were initiated.

For instance, if one needs to perform a specialized search of a large free-text database, it may be more ancient to move the program to the database server rather than move large amounts of data to the client program.

The advantages of Mobile Agent programming:
They facilitate high quality, high performance, and economical mobile application -

- They efficiently and economically use low bandwidth, high latency, error prone communication channels.
- Ability to operate asynchronously and autonomously.
- They are naturally heterogeneous.

Mobile agents have been used in many applications, such as electronic-commerce, manufacturing, network management real time control systems, and automation environments.

It is expected that deployment of mobile agents, as the new computing paradigm, will show several advantages compared to the current network computing principles based on client–server architectures.

The most relevant for this research are:
Their ***mobility***, therefore suitable for instantaneous local reactions to various events relevant for security, and their ***autonomous operations,*** therefore convenient for automated administration, distribution and synchronization of various aspects of security in distributed, heterogeneous networking environments.

The use of mobile agents can be traced back to the remote job entry systems in the 1960’s. It has gradually gained popularity and complexity since then. Unlike many new technologies where security is an add-on feature after all intended functionalities are realized, security is a part of mobile agents’ functionalities. Security poses a major threat in the mobile agent systems.

Security threats in mobile agent systems can be classified into the following four main categories:

1) Agent to host
   a) Masquerading
   b) Denial of Service
   c) Unauthorized Access

2) Agent to agent
   a) Masquerade
   b) Denial of Service
   c) Repudiation
   d) Unauthorized Access

3) Host to agent
   a) Masquerade
   b) Denial of Service
   c) Eavesdropping
   d) Alteration

4) Others to agent/host.[3]
   a) Masquerade
   b) Unauthorized Access
   c) Denial of Service
   d) Copy and Replay

As there are many security threats in mobile agent system as classified above. But this paper mainly emphasis on secure migration from one host to another host.

As there are a variety of ways in which an attacker might cause harm. (1) An outside attacker may intercept a migrating agent and steal sensitive data. Migrating agents might be carrying sensitive blueprints, or other data which should be kept secret.
(2) An outside attacker may intercept a migrating agent and modify it to perform a malicious action.
(3) An outside attacker may compose its own agent and send it into the agent framework. That agent might be able to disrupt systems and cause physical harm by controlling mechanical systems in an unsafe manner.

II. PREVIOUS WORK

Several schemes have been proposed to secure migration of mobile agent from one host to another host. Najmus Saqib Malik, David Ko and Harry H. Cheng propose to use a strong authentication process is used by sender and receiver agencies to authenticate each other before agent migration. The security framework also aims to guarantee the integrity and confidentiality of the mobile agent while it is in transit. This assures that all agents within an agency framework were introduced to that framework under the supervision and permission

of a trusted administrator. The Mobile-C Security protocol is inspired from the Secure Shell (SSH) protocol, which avoids a single point of failure since it does not rely on a singular remote third party for the security process. In this protocol, both agencies must authenticate each other using public key authentication, before a secure migration process. After successful authentication, an encrypted mobile agent is transferred and its integrity is verified by the receiver agency. The article describes the Mobile-C secure migration process and presents a comparison study with the SSH protocol. The performance analysis of the secure migration process is performed by comparing the turnaround time of mobile agent with and without security options in a homogeneous environment.
In his work they specify the security requirements that are incorporated in Mobile-C for the secure migration process:

Confidentiality

Confidentiality demands that mobile agents can only be read/understood/executed by a legitimate agency. In the context of agent systems, the primary assets of an agent are data, state, and code. Confidentiality must guarantee the secrecy of the assets of an agent during the migration process.

Integrity

Integrity is the property that a mobile agent has not been altered in an unauthorized manner. The success is measured based on two key factors: integrity of the mobile agent and integrity of the agent platform. The mobile agent demands that only authorized entities modify its data and code. The platform on the other hand must ensure that only authenticated agents can modify shared data.

Authentication

Authentication is a process in which a receiver agency can verify that a sender of mobile agent is actually who it claims to be. Similarly, the sender is also able to verify the receiver of mobile agent. A platform must be able to hold a mobile agent responsible for its actions, performed on that host. For this reason a mobile agent must be uniquely identified and authenticated.

III. SECURE MIGRATION PROCESS

The migration process of mobile agents and ACL messages in Mobile-C is inspired from the SSH protocol. The security protocol was based on SSH because SSH already contains the key features required for our security process. The SSH protocol provides CIA system for the transfer of data without utilizing a central server.

In his work for authentication, integrity and confidentiality hey use several Algorithms. They are as follow:

Authentication process

Authentication refers to a process in which an agency ensures that the other agency in a conversation is in fact who it is declared to be. Before the secure transfer of a mobile agent between two agencies, they must authenticate each other. Each agency in a network contains a list of known hosts provided by the administrator. This list provides RSA public keys of other trusted agencies in a network. Before agency *A* wants to transfer a mobile agent to agency *B*, agency *A* must verify that agency *B* contains a correct private key for the public key in agency *A*'s known-host list. In addition, agency *B* must verify that agency *A* contains a correct private key for the public key in agency *B*'s known-host list.

Confidentiality

ISO defines confidentiality as '*ensuring that information is accessible only to those authorized to have access*es'. This means that while a mobile agent is migrating from agency *A* to agency *B*, it would not be accessible in an understandable form by any adversary. Mobile-C uses an AES 256 bit key to encrypt the mobile agent at the sending agency and to decrypt it at receiver agency. The insurance of security of this process relies on a secure transfer of the AES 256 bit key. Public key en-/decryption is used to transfer the AES key securely. The AES key is exchanged between two agencies in the authentication process. This eliminates the further exchange of messages between two agencies for the AES key transfer. After successful authentication, the sender agency encrypts the mobile agent with the AES key and the receiver can decrypt it. According to National Institute of Standards and Technology (NIST) AES with 256 bit key size is safe to use for data encryption until 2030. The same nonce (as used in the authentication process) is used as session identifier during the transfer of both the AES key and the mobile agent. This is to avoid the replay back attack on agencies.

Integrity

Integrity is a process to ensure that the contents of a mobile agent are the same as sent by the sender agency. In other words, a successful integrity check should ensure that the agent was not tampered with while in transit from the sending agency to the receiving agency. Mobile-C uses a SHA2 hash code to check the integrity of mobile agents.

Random number generation

True random number generation is always an issue and an important concern for cryptographic algorithms. The programming language C's random function has vulnerabilities and is thus not recommended for use in cryptographic applications. For this reason, Mobile-C uses Hardware.

Volatile Entropy Gathering and Expansion (HAVEGE) for high random number generation. It is a heuristic software approach to generate empirically strong random numbers. Mobile-C uses HAVEGE to generate the nonce, challenge text, and AES 256 bit key during the mobile agent migration process.

IV. PROPOSED WORK

Mobile agents are piece of software that can autonomously migrate in an open networked computer to another while executing. It execute across network in behalf of user. As mobile agent migrates from one host to another host there are many security related issues. When a mobile agent migrates from one host to another host an outside attacker can cause harm the mobile agent in many ways? It can intercept a migrating agent and steal sensitive data, modify it to perform a malicious action. So there are need to secure the mobile agent while it is in transit. In the proposed work we use "digital signature" for authentication, DES for encryption for providing security. In my next paper describe the full description of all the things mentioned above.

V. CONCLUSION

Many researchers have investigated the development of protection mechanisms in a mobile agent migration. In this paper we describe some mechanism for secure migration process of a mobile agent from one host to another host. For this we use the authentication, integrity and confidentiality for secure migration of mobile agent from one host to another host. For this_we use the RSA for authentication, ASE for confidentiality and SHA2 for integrity.

REFERENCES

1. Najmus Saqib Malik, David Ko and Harry H. Cheng*,†,‡"A secure migration process for mobile agents" Integration Engineering Laboratory, Department of Mechanical and Aerospace Engineering, Computer Science Graduate Group, Electrical and Computer Engineering Graduate Group,University of California, Davis, CA 95616, U.S.A.
2. Awais Shibli Doctoral Dissertation in Computer and System Sciences Stockholm, Sweden 2010 "Security Infrastructure and Applications for Mobile Agents".
3. Li An Qiangfeng Jiang Xiaoping Luo Zhaohui Ren Spring, 2002 "Protecting Mobile Agents against Malicious Hosts.
4. Shibli A & Muftic S (2009),"MagicNET: Security Architecture for Creation, Classification, and Validation of Trusted Mobile Agents", [Conference] The 11th IEEE International Conference on Advanced Communication Technology. - Phoenix Park, Korea, February 2009. (Accepted for Publication) Course: IK2000/SAO: Security Architectures for Open Distributed Systems January 2009 "MagicNET: Security Architecture for Creation, Classification, and Validation ofTrusted Mobile Agents".

BIOGRAPHY

First Author profile

Qualification: Pursuing M. Tech from Lingaya's University

Second Author profile

Qualification: Pursuing M. Tech from Lingaya's University

Third Author profile

Qualification: M. Tech ,Working in Lingaya's University as a Sr. Lecturer in CSE Department.