AN ENHANCED APPROACH FOR SECURING MOBILE AGENTS FROM THE ATTACK OF OTHER MALICIOUS MOBILE AGENTS

Asha Anil[1], Jesna Anver[2]

[1]PG Student, [2]Associate Professor, Department of Computer Science and Engineering, Toc H Institute of Science and Technology, Kerala, India

Abstract

The area of mobile agent security is in a state of immaturity, but rapidly improving. Emphasis is beginning to move toward developing techniques that are oriented towards protecting the agent. Agent technology has been used in many critical applications like business process management, e-commerce, artificial intelligence, distributed processing etc. The mobile agent technology has encountered many security threats during the itinerary period .The security schemes presented in this paper for mobile agent address the code, data and itinerary security issues. An environment that protects the legitimate mobile agent from the malicious mobile agent is provided. A checksum method is used to detect a malicious mobile agent which is appending to a legitimate mobile agent. The confidentiality of the data that are retrieved from each remote server is ensured by encryption mechanisms. The itinerary is also protected by allowing only registered users to create new mobile agents and is controlled by a central co-coordinator. Thus an enhanced security mechanism is presented to protect the mobile agent's code, data and route.

Keywords: *Mobile Agent, Security Threats, Central Co-ordinator, Checksum Method*

----------***----------

1. INTRODUCTION

A software agent is program that acts as a user's personal assistant and is classified as static agents and mobile agents. Static agents execute on a single machine to achieve their goal Software agents which have the property of mobility are called mobile agents and they perform a user's task by migrating and executing on several hosts connected to the network. Mobility increases the functionality of the mobile agent and allows the mobile agent to perform tasks beyond the scope of static agents. An agent is defined as "a person whose job is to act for, or manage the affairs of, other people. In the context of computers, software agents refer to programs that perform certain tasks on behalf of the user. Imagine that we want to go on a trip to a new holiday destination. We contact your travel agent program and describe our preferences and our constraints. The program suggests where we can spend our holidays after taking into consideration several information sources such as flight timings, guides and verifying the availability of tickets and hotel rooms etc. When we confirm our destination, the program books the flight tickets and reserves the hotel rooms for us. Thus the software agent acts as our personal assistant and they exhibit certain properties, such as: autonomy – they act without the need of constant human supervision, sociability – the ability to interact with other agents if necessary, reactivity – ability to react to changes in the environment, proactivity – taking initiative at needed times, in order to reach objectives.

2. RELATED WORKS

The existing system provides mobile agent authentication at each host. This ensures that the mobile agent is dispatched by the intended sender only. But the integrity of the code is not guaranteed. Any receiver can confirm the identity of the sender but not the content of the code. There is a possibility of malicious mobile agent appending itself with the legitimate mobile agent without modifying or altering the contents of the code. The verifying process only verifies for sender's authentication and not the integrity of code. In overall there is a lack in available security system that provides security for itinerary details, data and particularly mobile agents' code. Also in the existing system, there is no mechanism for authentication checking and the agent verification is done through checking agent size. If the agent size exceeds a particular limit, kill that agent. But it may not be suitable in all cases.

Over the years computer systems have evolved from centralized monolithic computing devices supporting static applications, into networked environments that allow complex forms of distributed computing. A new phase of evolution is now under way based on software agents.

A software agent is loosely defined as a program that can exercise an individual's or organization's authority, work autonomously toward a goal, and meet and interact with other agents.

Wayne A. Jansen et al. [1] proposed a number of models exist for describing agent system, however, for discussing security issues it is sufficient to use a very simple one, consisting of only two main components: the agent and the agent platform and have summarized the various methods devised for protecting the agent platform such as Software-Based Fault Isolation, Safe Code Interpretation, Signed Code, State Appraisal, Proof Carrying Code etc and more general-purpose techniques for protecting an agents such as Host Revocation Authority, Execution Tracing ,Obfuscated Code, Ajanta System, Partial Result Encapsulation, Environment Key Generation etc.

Ibharalu et.al [2] proposed reliable protection architecture using Travel Diary Protection Scheme and Platform Registry which allows and protects mobile agents to roam freely in open networks environment without being attacked by malicious hosts. The paper focuses on securing free-roaming agents in open network environments and presents a novel security protocol which has fine function in preventing attacks. J.M.Gnanasekar et.al [3] has proposed a number of solutions for securing data section in a mobile agent from discovery and exploitation by a malicious host are proposed based on cryptographic principles have their own limitations. The cryptographic key generation and distribution mechanism strongly holds the success of the mobile agent security systems. The agents and hosts are mutually distrusting each other, but they trust the third parties. In the paper [3], this property is exploited for the secure way of generating and distributing the keys using service oriented architecture. The major security future for mobile agent, the Publicly Verifiable and Forward Integrity (PVFI) and Forward Privacy (FP) are also ensured.

Tarig Mohamed et.al in [4] has proposed a Secure-Image Mechanism (SIM) to protect mobile agents against malicious hosts. SIM aims to protect mobile agent by using the symmetric encryption and hash function in cryptography science. This mechanism can prevent the eavesdropping and alteration attacks. The main benefit of this mechanism is to allow the mobile agent to continue its journey without problem in case these types of attacks occurred. The paper [4] presents some solution proposed by research in the area of the mobile agent protection and explains the symmetric encryption and hash function concept.

Abolfazl esfandi et.al in [5] has proposed a mobile agent security in multi agent environments using a multi agent-multi key approach .In paper [5] they consider the problem of keeping sensitive data and algorithms contained in a mobile agent from discovery and exploitation by a malicious host. They illustrate a novel distributed protocol for multi agent environments to improve the communication security in packet switched networks. To enrich the overall system security the approach makes use of distribution and double encryption and some other traditional methods such as digital signature. In this approach the encrypted private key and the message are broken into different parts carrying by different agents which makes it difficult for malicious entities to mine the private key for message encryption, while the private key for the encrypted key is allocated on the predetermined destination nodes. On the other hand, all of the previously proposed encryption algorithms can be applied in their proposed approach that deteriorates the key discovery process. To improve the overall security, the paper makes use of Advanced Encryption Standard (AES) as the encryption base for message encryption. The paper also presents some evaluation discussions presenting time overhead analysis and crack probability.

Muhammad Awais Shibli et.al [6] has proposed MAGICNET: security system for development, validation and adoption of mobile agents .The research in the area of mobile agents' security mainly deals with protection and security for agents and agents' runtime platforms. Sarwarul et.al [7] has proposed a mechanism for security of mobile agent in ad hoc network using threshold cryptography .One of the main advantages of using Mobile Agent in a network is it reduces network traffic load. In an ad hoc network Mobile Agent can be used to protect the network by using agent based IDS

.Tarig mohamed et .al [8] has proposed a sub-agent mechanism to protect mobile agent privacy this paper a new mechanism called Generated Sub-Agent Mechanism (GSAM) to protect mobile agent against malicious Hosts The main idea behind GSMA is to generate a sub-mobile agent from the mobile agent in case the mobile agent will visit an untrusted host. The sub-mobile agent visits the untrusted host instead of the mobile agent.

M. Vigilson Prem et.al [9] has proposed agent sizing method to prevent the entry of a malicious mobile agent. . But it is not suitable for most of the cases as a malicious agent with the same size may get attached to the legitimate mobile agent.

3. EXISTING SYSTEM

In the existing system, verification was done with the help of agent sizing. If the size of mobile along with the data is larger than the critical section buffer, it is expelled out of the system. The mobile agent was kept in 'deactivated' state while this check is performed. This restricts the mobile agent not to perform any malicious action inside the host and thus protects the host platform from malicious activities of mobile agent. In case, the mobile agent fails this test, it is killed immediately inside the critical section itself. Further, at this stage only, the append entry attack is detected. If there is an increase in size of the agent against the size fixed at the sender's side, illegal entry of mobile code is detected.

On detecting this attack, the mobile agent is destroyed immediately based on malicious reasons. Otherwise the

mobile agent is allowed to execute in its execution environment.ie, here agent verification is done through checking agent size. If the agent size exceeds a particular limit, kill that agent. But it is not suitable for most of the cases as an malicious agent with the same size may get attached to the legitimate mobile agent either by deleting some parts of it or by replacing the agent.

4. PROPOSED SYSTEM

Our proposed system provides an environment that protects the legitimate mobile agent from the malicious mobile agent. The general architecture of the system for an information retrieval application with fault tolerant and security model is shown in figure 1. Web service is requested to plan and select dynamically, the next host to visit, based on parameters like size of data, aliveness, bandwidth. The authorized user submits his request, for example, an information retrieval request, to the mobile agent system. The agent creator creates the agent and the agent verification, data verification and path management are done by web service module. If verified, the data collection or actions if any are performed and the agent migrates to the next host and reaches back to the end user On arrival at each host, the mobile agent undergoes security check and on success the mobile agent is allowed to execute in the environment.

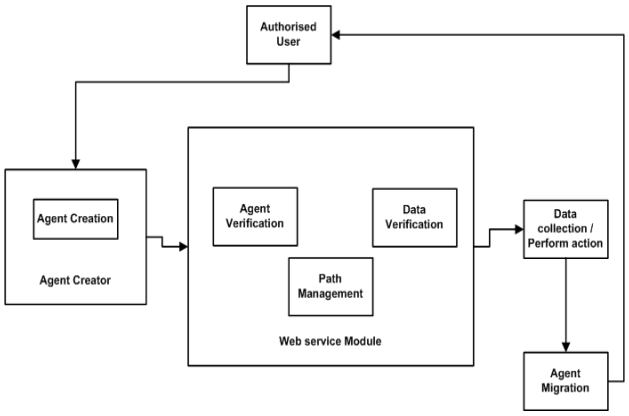

Fig -1: Overall architecture of the proposed system

4.1 Authentication Checking

The modified system proceeds using following steps

a. Creating Mobile Agents: - only registered users can create mobile agents

b. Agent Registration: - After creating mobile agents, mobile agents are registered to central mobile coordinator. During registration phase, creator send agent checksum, agent name, migration path are sent to this coordinator

c. Modify Mobile Agent Running platform :- In existing system, running environment checking agent size only for verification. But in our new environment, after receiving a mobile agent, the running environment sent its checksum and agent code to central coordinator. Central coordinator checks its integrity and status code to running environment. If this is a success, then running environment start mobile agent otherwise kills that agent

4.2 Checksum Method

The agent creator creates a mobile agent, and find its corresponding checksum and send the checksum to the central coordinator. It also sends the new path to the central coordinator if any new path change is found. The agent observer is a server that is distributed over different regions and its function is to monitor the movement of mobile agent in its corresponding region. It also acts as a service provider that services the requests related to those mobile agents. The agents generated at each host must be registered with agent observer and only the registered mobile agents are allowed to access the critical section. On successful completion of the task, the mobile agent is dispatched to next host after finding the proper host to migrate.

Following are the main steps of Agent Observer

a. Create an agent Observer
b. Receive messages from mobile agents

After the agent observer check authentication of request and sender agent, it returns data corresponding to agent request

4.3 Data Collection and Protection

The data collected from one server must be secure and should not be known to others. To implement this constraint, every server will encrypt its data using the owner's public key. The owner's public key is obtained by decrypting the segment received from previous server using receiver's private key and each data packet is encrypted using owner's public key. At the same time, the data packet can be decrypted only by the owner and these packets can only be opened in the correct order, since the symmetric key used to decrypt an envelope is protected inside the previous packet

The data packet received by any receiver is encrypted using owner's public key .On successful completion of task, the mobile agent appends the result with this packet and the new look packet is encrypted again using owner's public key

Also a checksum is also calculated for the data to provide additional security so that upon receiving the node where the data is collected it can check the integrity of the data by this new method

4.4 Path Migration

The web service is the central coordinator who keeps track of the path changes and holds the value of checksum of mobile agent.The details about the next host to be visited is controlled

by the web service. Also the web service keeps track of the path modification if any in a dynamic itinerary

5. WORKING OF THE PROPOSED MODEL

The entire working of our system with data and Agent verification is illustrated by a block diagram in Fig 2. The entire working of our system with data and Agent verification is illustrated by a block diagram in Fig 2.The figure describes how an agent is created, verified, and migrated. The agent is verified by a checksum mechanism and the data collected is also secured by a series of encryption mechanisms. Also the next path to be taken is obtained from the web server or the central coordinator and ultimately reaches the end user.

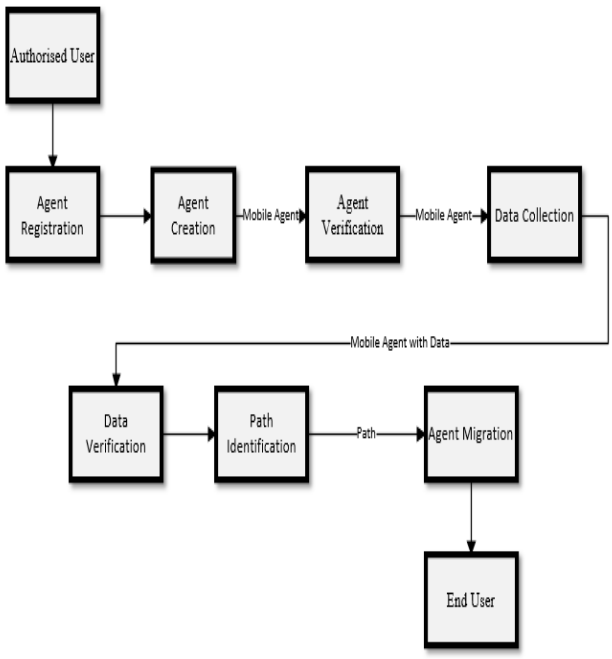

Fig -2: Block Diagram of the entire system

5.1 Algorithm

Step 1: Create a mobile agent by a registered user.
Step 2: Register the mobile agents with the web server.
Step 3: Verify the authenticity of agent with the help of checksum method
Step 4: Perform the operation required or collect the data from the intermediate hosts and encrypt the data by any encryption mechanism
Step 5: Verify the data collected.
Step 6: Obtain the next path from the central coordinator and choose the next host to be visited.
Step 7: Perform Agent Migration
Step 8: Stop

6. CONCLUSIONS

The area of mobile agent security is in a state of immaturity, but rapidly improving. The traditional orientation toward host-based security persists and, therefore, available protection mechanisms tend to focus on protecting the agent platform. Emphasis is beginning to move toward developing techniques that are oriented toward protecting the agent, a much more difficult problem. There are a number of agent-based application domains for which basic and conventional security techniques should prove adequate mobile agent technology is intriguing and offers a new paradigm for application development

Agent technology has been used in many critical applications such as personal information management, electronic commerce, business process management, artificial intelligence, interface design, distributed processing and distributed algorithms. Besides its bright side, the technology has encountered many security threats. These problems are faced during the itinerary period of an agent traversing from platform to platform in the network. The unexpected failure or change in network components or status makes the static planning not a best option and makes the mobile agent users to opt for dynamic itinerary. But the problem is that the itinerary details are open to all hosts. But for secure transaction applications, the itinerary details must not be known to any other hosts in the network

The data collected from each host must be protected from any other host .Only the owner of the agent is allowed to decrypt the encrypted data at each host. More importantly, the existing provides mobile agent authentication at each host. This ensures that the mobile agent is dispatched by the intended sender only. But the integrity of the code is not guaranteed. Any receiver can confirm the identity of the sender but not the content of the code. There is a possibility of malicious mobile agent appending itself with the legitimate mobile agent without modifying or altering the contents of the code. The verifying process only verifies for sender's authentication and not the integrity of code. In overall there is a lack in available security system that provides security for itinerary details, data and particularly mobile agents' code. This situation has given the motivation to present a three dimensional security model that protects mobile agent from malicious agents' passive attack, data and itinerary details from executing hosts

In our proposed system we are providing security for agent's code, data as well as path through a series of encryption mechanism. The code of the mobile agent is verified by a two level verification schemes. The authentication is verified at first level by a registration mechanism and the integrity of code is verified at second level by checksum method. This ensures that the mobile agent is not affected by other malicious mobile agent. Further, the itinerary is protected to ensure the secure transaction of data. Finally the data collected

is secured by using cryptographic methods to ensure the integrity of data. The proposed model protects the mobile agent from other malicious mobile agents in the platform.

REFERENCES

[1]. W. Jansen, "Countermeasures for mobile agent security", Computer Communication, Special issue on Advances in Research and Application of Network Security, November 2000.
[2]. Ibharalu F. T., Sofoluwe A.B., Akinwale A. T., "A reliable protection architecture for mobile agents in open network system", International journal of computer applications, Volume 17, Issue 7, pp.6-14, 2011.
[3]. J.M.Gnanasekar and V. Ramachandran, "Distributed cryptographic key management for mobile agent security", International journal of recent trends in engineering, Volume I, Issue I, pp.164-167, 2009.
[4]. Traig Mohammad Ahmed, "Using secure-image mechanism to protect mobile agent against malicious host", WASET, Volume 59,pp. 82-91,2009.
[5]. Esfandi, A, Rahimabadi, AM., "Mobile agent security in multi agent environment using a multi agent multi key approach", Proceedings of 2nd IEEE International Conference on Computer Science and Information Technology, ICCSIT'09, pp. 438 - 442, 2009
[6]. Shibli, M.A.; Muftic, S.; Giambruno, A; Lioy, A, "MagicNET Security system for development, validation and adoption of mobile agents", Proceedings of 3rd International Conference on Network and system security, pp.389-396, 2009.
[7]. S.M. Sarwarul Islam, Zinat S, Bo Sun, Md. Washiqul Islam, "Security of mobile agent in Ad Hoc network using threshold cryptography" ,WASET, Volume 70, pp.424-427, 2010.
[8]. Tarig Mohamed Ahmed, PhD, "Generate Sub-Agent Mechanism to Protect Mobile Agent Privacy", 2012 IEEE Symposium on Computers and Informatics.
[9]. M. Vigilson Prem and S. Swamynathan,"Securing Mobile Agent and its Platform from Passive Attack of Malicious Mobile Agents", IEEE-International Conference on Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012

BIOGRAPHIES

Asha Anil was born in Kerala India. She received B.Tech in Computer Science from College of Engineering Munnar in the year 2007 and is currently pursuing M.Tech in Computer Science with Specialization in Data Security in Toc H Institute of Science and Technology. She has nearly 5 years of experience including industry and teaching .Her areas of interest include Data Security, Automata, Computer Graphics and her research interest includes Data and Network Security.

Jesna Anver was born in Kerala, India. She receieved B.Tech from Model Engineering College, Thrikkakara in the year 2003 and M.Tech from Amrita University Coimbatore and is currently doing research in Cochin University of Science and Technology under the Dept of Electronics. She has nearly 10 years of teaching experience and is currently working as Associate Professor in Toc H Institute of Science and Technology under Computer Science Dept. Her areas of interest include Image Processing, Machine Learning Networking and Signal Processing