International Journal on Recent and Innovation Trends in Computing and Communication
Volume: 4 Issue: 5

ISSN: 2321-8169
579 – 581

A Security Architecute for Mobile Agent Based Creeper

Manju Kumari[1]
Lecturer,
Polytechnic College, Bikaner
manjusunia08@gmail.com

Kinnari Jangid[2]
Marudhar Enginnering College
kinnarijangid@gmail.com

Abstract: Mobile agents are active objects that can autonomously migrate in a network to perform tasks on behalf of their owners. Though they offer an important new method of performing transactions and information retrieval in networks, mobile agents also raise several security issues related to the protection of host resources as well as the data carried by an agent itself. Mobile agent technology offers a new computing paradigm in which a program, in the form of a software agent, can suspend its execution on a host computer, transfer itself to another agent-enabled host on the network, and resume execution on the new host. Mobile Agent (MA) technology raises significant security concerns and requires a thorough security framework with a wide range of strategies and mechanisms for the protection of both agent platform and mobile agents against possibly malicious reciprocal behavior. The security infrastructure should have the ability to flexibly and dynamically offer different solutions to achieve different qualities of security service depending on application requirements. The protection of mobile agent systems continues to be an active area of research that will enable future applications to utilize this paradigm of computing. Agent systems and mobile applications must balance security requirements with available security mechanisms in order to meet application level security goals.A security solution has been introduced, which protects both the mobile agent itself and the host resources that encrypt the data before passing it to mobile agent and decrypt it on the visited host sides i.e. it transfers the URL to the Mobile Agent System that will pass that encrypted URL to the server where it will be decrypted and used. The methods of Encryption/Decryption used are a Public-key Cipher System and a Symmetric Cipher System that focuses on submitting data to the server securely. The proposed approach solves the problem of malicious host that can harm mobile agent or the information it contain.

*****

1. INTRODUCTION

Mobile agents are small threads of execution that are able to migrate from machine to machine, performing operations locally. An application area for mobile agents is internet computing. Mobile agents provide a very attractive paradigm for this area. The agents can be launched from a machine, navigate from web to web, collecting information or performing transactions, finally returning home with the goods or results.Mobile agents are an appealing alternative to the client-server architecture for many applications. MA's have extended the mobile-code concept to "mobile object" in which an object (code + data) are moved from one host to another. This approach extends the concept by moving code, data and state (thread) from one host to another as well. MAs run at one location, move with their state to another host, and continue execution at that host. Mobile code and mobile objects are normally moved by an external entity while MAs are usually migrate autonomously as shown in Fig. 1.

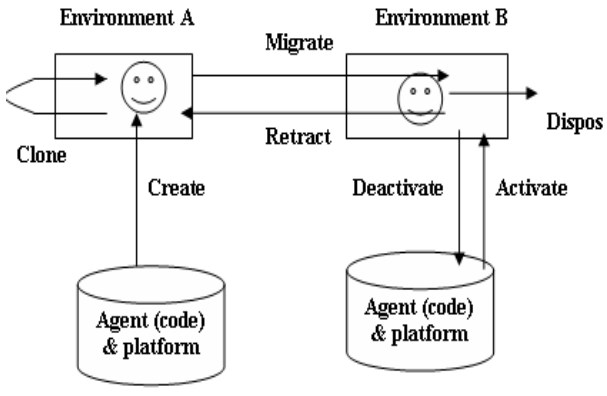

Fig.1 : Mobile Agent with Platform

The goals of Mobile Crawling System are

ISSN: 2321-8169
579 – 581

- To minimize network utilization.
- To keep up with document changes by performing on-site monitoring.
- To avoid unnecessary overloading of the web servers by employing time realization.
- To be upgradeable at run time.

2. DRAWBACKS OF MOBILE-AGENT BASED CRAWLER

Mobile agent based crawler has some limitations, primarily in the area of security. Current research efforts in the area of mobile agent security adopt two different points of view. Firstly, from the platform perspective, there is a requirement to protect the host from malicious mobile agents such as viruses and Trojan horses that are visiting it and consuming its resources. Secondly, from the mobile agent point of view, it needs to protect the agent from malicious hosts. Therefore, security is a fundamental precondition for the acceptance of mobile agent applications. In other words, The system should have a program that actively protects itself against execution environment that possibly may divert the intended execution towards a malicious goal . Many approaches aim at protecting mobile agents. There are some problems, which have to be solved before these approaches can be used The particular attacks that a malicious host, malicious agent can make can be summarized as follows.

- Observation of code, data and flow control,
- Manipulation of code, data and flow control, including manipulating the route of an agent,
- Incorrect execution of code – including re-execution,
- Denial of execution – either in part or whole,
- Masquerading as a different host,
- Eavesdropping on agent communications,
- Manipulation of agent communications,

It is very difficult to protect mobile agent as it visit different node in network so security should be apply on the platform. This paper contain the application in which protection on data by encrypt it on platform so no other malicious node or malicious plate form access the data carry by mobile agent. The technology use for the protection is computing with cryptography.

3. PROPOSED ARCHITECTURE OF SECURITY BASED MOBILE AGENT CRAWLER

The method of Encryption/Decryption is used to ensure the security of the agent and the host resources. The mobile agent program is encrypted on the creator side before it is transferred to other hosts, and deciphered on the remote hosts side when it gets to the right hosts. The encryption needs not only a private key for the computation with cryptography method but also the private key of every destination host. After the destination hosts have received the encrypted agent, they decipher the cryptograph and recover the original mobile agent code using their corresponding private keys. The proposed security architecture is shown in Fig. 2, which starts after firing the query to internet. Then, the query is passed to crawler which works in three stages:

- Retrieval stage: In this, the crawler has to retrieve the resources which will be part of the index. It contacts a remote HTTP (Hypertext Transfer Protocol) server, requesting a web page specified by a URL (Uniform Resource Locator) address.

- Analysis stage: After a certain resource has been retrieved, the crawler will analyze the resource in a certain way depending on the particular crawling algorithm. For example, in case the retrieved resource is a Web page, the crawler will probably extract hyperlinks and keywords contained in the page

.

- Decision state: Based on the results of the analysis stage, the crawler will make a decision how to proceed in the crawling process. After that, it passes the URL one by one to encryption layer. The secure URL given to mobile agent is encrypted before transferring to it. This encryption is done after the completion of crawling. This solves the problem regarding any malicious host that can harm mobile agent or any information.

ISSN: 2321-8169
579 – 581

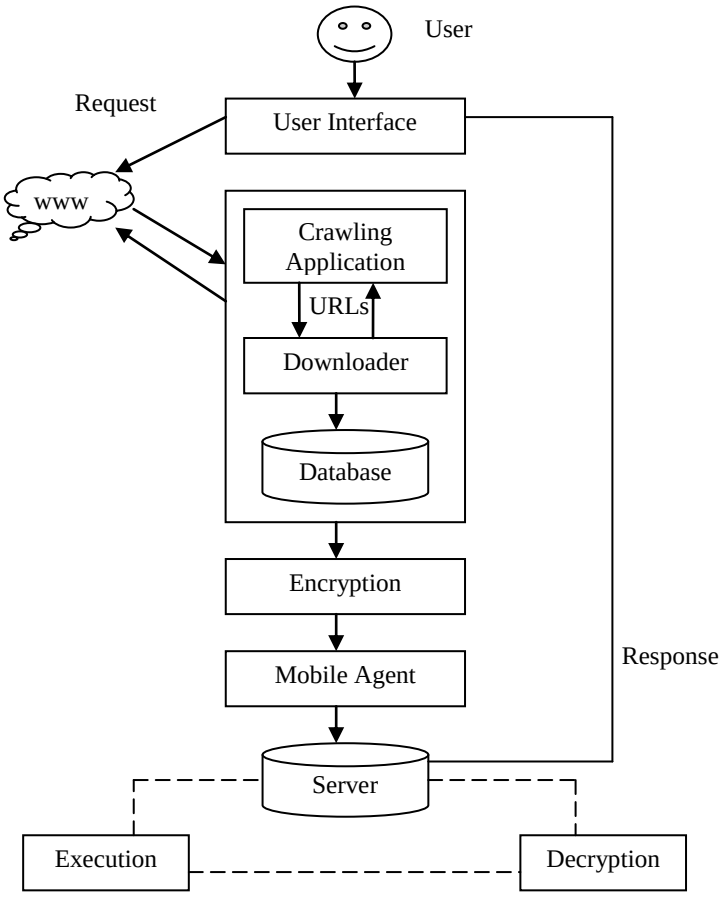

Fig2: Security based mobile Agent Crawler

4. CONCLUSION

Mobile agents have gained a great deal of attention in research and industry in the recent past. Although mobile agents are a promising technology, the large-scale deployment of agents and the existence of hosts running agencies will not happen until proper security mechanisms are well understood and implemented. Mobile agents are plain enough for malicious parties to read and to analyze. A malicious host may read or alter the content of the agent, or analyze the accumulated information carried by the mobile agent. Another program or agent running on the same host as the agent is another source of threat for the agent. It is more difficult to ensure security in the mobile agent paradigm than in some other technologies where hardware solutions are practical. Problems in security have been seen as an obstacle in the way of success of mobile agent technology.

REFERENCES

[1] James P Anderson, "Computer Security Threat Monitoring and Surveillance,"Technical Report, James P. Anderson Co., Fort Washington, PA, April 1980

[2] Midori Asaka, Shunji Okazawa, Atsushi Taguchi, and Shigeki Goto, "A Method of Tracing Intruders by Use of Mobile Agents," INET'99 Conference, June 1999.

[3] Jai Balasubramaniyan, Jose Omar Garcia-Fernandez, David Isacoff, E. H. Spafford,and Diego Zamboni, "An Architecture for Intrusion Detection using Autonomous Agents," Department of Computer Sciences, Purdue University; Coast TR 98-05, 1998.

[4] Karima Boudaoud, Houda Labiod, "MA-NID: A Multi-Agent System for NetworkIntrusion Detection," Eighth International Conference on Intelligent Systems, June 1999.

[5] Giacomo Cabri, Letizia Leonardi, Franco Zambonelli, "The Impact of the Coordination Model in the Design of Mobile Agent Applications," Twenty-second Computer Software and Applications Conference (COMPSAC), August 1998

[6] Wayne Jansen and Tom Karygiannis, "Privilege Management Mobile Agents,Twenty-third National Information Systems Security Conference, pp.362-370, October 2000.

[7] Günter Karjoth, N. Asokan, and Ceki Gülcü, "Protecting the Computation Results of Free-Roaming Agents," Second International Workshop on Mobile Agents, Stuttgart, Germany, September 1998.

[8] Danny Lange and Mitsuru Oshima, *Programming and Deploying Java Mobile Agents with Aglets*, ISBN:0-201-32582-9, Addison-Wesley, 1998.

[9] Stefano Martino, "A Mobile Agent Approach to Intrusion Detection," Joint Research Centre-Institute for Systems, Informatics and Safety, Italy, June 1999.

[10] Bennet S. Yee, "A Sanctuary for Mobile Agents," Technical Report CS97-537, University of California in San Diego, April 28, 1997