Journal of King Saud University – Computer and Information Sciences (2014) 26, 131–142

King Saud University

Journal of King Saud University – Computer and Information Sciences

www.ksu.edu.sa
www.sciencedirect.com

ORIGINAL ARTICLE

Fragmentation based encryption approach for self protected mobile agent

Shashank Srivastava *, **G.C. Nandi**

Indian Institute of Information Technology, Allahabad, India

Received 31 December 2012; revised 7 April 2013; accepted 22 August 2013
Available online 31 August 2013

KEYWORDS

AES;
Fragmentation based encryption;
Mobile code;
Mobile agent;
Self protected mobile agent;
Formal modelling

Abstract Distributed applications provide challenging environment in today's advancing technological world. To enhance the aspects of better performance and efficiency in real scenario mobile agent's concept has been brought forward. As every technological movement is aligned with its repercussions, the mobile agent technology also has its inherent security loopholes. Usage of agent technology poses various security threats over networked infrastructure. Moreover numerous researches have already been proposed to take the edge off inherent security risk faced by mobile agent, but all these approaches did not resolve the malicious execution environment problem in permissible and effectual conduct.

Gaining the understanding of mobile agent architecture and the security concerns, in this paper, we proposed a security protocol which addresses security with mitigated computational cost. The protocol is a combination of self decryption, co-operation and obfuscation technique. To circumvent the risk of malicious code execution in attacking environment, we have proposed fragmentation based encryption technique. Our encryption technique suits the general mobile agent size and provides hard and thorny obfuscation increasing attacker's challenge on the same plane providing better performance with respect to computational cost as compared to existing AES encryption.

1. Introduction

Mobile agent technology entices various distributed applications due to its positive features like intelligence, autonomy, adaptability, flexibility, etc. (Lange and Oshima, 1999), but security issues and its overheads are shading down its global acceptance. In mobile agent paradigm, various research approaches have been highlighted in past decade analyzing the security concern but still malicious execution environment is a bottleneck for its deployment on wide scale. The major threat for the implementation of this technology is the modification or analysis of the agent's code and critical data sent over the platform at the execution instance. Mobile agent freely roams across network from one execution environment to another and executed there and the execution platform which executes the mobile agent could try to perform malicious activity (Jansen and Karygiannis, 2000; Borselius, 2002).

* Corresponding author. Tel.: +91 9984905199.
E-mail address: shashank12march@gmail.com (S. Srivastava).
Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

1319-1578 © 2013 Production and hosting by Elsevier B.V. on behalf of King Saud University.
http://dx.doi.org/10.1016/j.jksuci.2013.08.002

In agent based infrastructure, two entities participate in whole communication and computation. One is home platform where the agent owner is responsible for agent creation; other is host platform which executes the agent. Malicious entity can perform various attacks on agent's component when agent traverses in communication channel. So security over communicational channel needs to be established. Secondly when an agent migrates from one execution environment to other, it provides its control to the execution environment which makes it vulnerable to different types of security attacks that could be performed through the execution environment (Borselius, 2002; Sander and Tschudin, 1998; Macrides, 2002).

Our research provides a new direction to the agent based applications primarily targeting confidentiality concerns of agent security during communication channel or on execution platform vulnerable to the following security threats:

- Insecure communication channel
- Malicious execution environment

Generally encryption is provided to maintain the confidentiality factor of Information. Encryption using single shared key known as symmetric encryption is used for sending the large amount of data. It is computationally efficient but fails to provide authentication and integrity. To overcome the said challenges and enhance security, asymmetric encryption concept was built in but it lagged in providing efficient computational factor.

Analyzing the encryption techniques in the environment of mobile agent where the agent code moves towards data location, our research work gives a new direction to traditional security approach. As in agent paradigm, the code size is very less so the issues like network overhead, bandwidth and latency are no more challenges. Henceforth our main intent to enhance security in terms of time and space for the agent and the agent based infrastructure. We have proposed a protocol where agent is structured in modules for performing various activities. Self decryption module and fragmentation based encryption are the back bone of our security protocol.

Our research is organized in following way. Section 2 analyses the previous researches conducted in related area of agent security and tries to find out the current state of art in the security prospect. Section 3 proposes a security solution in the form of security protocol and presents a light weighted fragmentation based encryption technique. Section 4 provides a formal verification of security threats and our security protocol. Section 5 deals with implementation details of protocol with results. At the last, in Section 6, we summarize our security protocol and algorithm and focus on its future scope.

2. Analysis of previous researches

Security is the biggest concern which darkens the advantageous side of mobile agent infrastructure. As soon as the mobile agent migrates from home platform, it goes out of the control of its owner that gives the opportunity to attacker (eavesdropper, network sniffer, execution environment, etc.). In the case, if the execution environment is malicious, it can perform various attacks on mobile agent. Mainly the following are the threats for such traversing of mobile agent in an untrusted environment.

- Analysis of code to change its execution behavior.
- Modification of code.
- Analysis of data collected during execution of agent's itinerary.
- Modification or deletion of data collected.

So in a nutshell, there are basically two types of attacks which can be performed by execution environment.

- Execution privacy
- Execution integrity

We listed out following directions analyzed for coming to the point of current security requirements that need to be sorted out for the further enhancement of agent based paradigm in terms of security and performance.

In mobile agent system, code, data and execution state migrate from one execution environment to another. During execution of mobile agent, execution platform has full control over agent's code, data and execution state. Hohl (Hohl, 1998) proposed obfuscation technique in which mobile agent code is scrambled in such a manner that no one can understand it easily, like in java, java complier converts .java file to .class file which is written in bytecode. Java bytecode runs by JVM which is platform independent. In the case of mobile code, java bytecode moves from one host to another host (class serialization). Java byte code is not in readable form. But now there are various decompilaters are available to convert java bytecode to java program. In the same way, java deobfuscator is also available which helps in deobfuscating the obfuscated program (Armoogum and Caully, 2011).

Moreover, java obfuscation only provides execution privacy or confidentiality to the mobile code but it cannot be ensured that the particular obfuscated code is deobfuscatable or not. In this case, if execution platform has sufficient computational capacity, it can deobfuscate the code before executing the code. This technique is a preventive measure and its security is dependent upon the computational capacity of execution environment.

The second prominent solution is encrypted key function. Encrypted function computation approach was first forwarded by Sander and Tschudin (Sander and Tschudin, 1998) in 1997 which states code is hidden during execution to achieve privacy. However this mobile cryptography technique was strong enough to provide execution privacy but it only worked for the special case of polynomial and rational function. Besides this, no homomorphism encryption system exists till now which could help to implement mobile cryptography in a practical environment.

In this solution (Lee, 2004), home platform has an algorithm which computes a function f. At remote site, the target host has an input x and it computes $f(x)$ to provide services to agent. In order to secure the function f so that remote host cannot read this, home platform encrypts the function f to get $E(f)$ and then embodies encrypted function within program. Home platform inserts this program within agent's code and sends it to remote host platform for execution. The target platform runs program on input x and produces $E(f(x))$ then the result is sent back to its home platform. Home platform decrypts it and gets $f(x)$. This mechanism enables the agent to execute in a secure manner at remote untrusted platforms.