A Multi-Gating Security Framework to Prevent Tailgating Attack of the Host Agent Platform in a Mobile Agent System

[1] Aboloko .S. Oberoro, [2] S.A. Idowu, [3] Y.A Adekunle, [4] O.D.Alao
[1][2][3][4] Delta state polytechnic, Oghara

Abstract: Mobile agents can be described as programs that perform a given task on behalf of its owner. The growing need for Mobile Agent Technology (MAT) has been accompanied with corresponding issues like security and ethics. These challenges have resulted in global cold-feet towards mobile agent technology. The fundamental security issues in a mobile agent system are masquerading, denial of service, eavesdropping, alteration, repudiation and tailgating. Various models and techniques to detect and prevent these attacks, especially the host agent platform, have been proposed and implemented. However, most of these existing studies on the host agent platform dwelt mainly on authorized access security issues. An unauthorized social engineering security issue like tailgating attack is yet to be given the deserved consideration. This study developed a Multi gating Security Framework that detects and prevents a tailgating attack of the host agent platform in a mobile agent system.

Index Terms— Microcontroller; soil less cultivation parameter; Hydroponics; AVR controller.

I. INTRODUCTION

Mobile agents are codes or programs that acts as representative to its owner, to perform a given task at a remote network. Mobile agent travels or hops through the remote network to its host agency to execute its codes. (Fuggetta, Picco, & Vigna, 1998). The characteristics of a mobile agent have been continually debated in the research community; however there is a consensus that an agent must show some nominal quality to qualify as mobile agent. These qualities include sovereignty and mobility. The mobile agent paradigm is getting popular as means for an efficient access to remote resources in the same networks or in heterogeneous network (Braun & Rossak, 2005 ; Adri & Marikkannan, 2016).

Before the evolution of mobile agent paradigm, the means of passing information between the user node and the host node (client / server model) has been by various methods. These methods include message passing, remote procedure call (RPC), remote evaluation (REV) and Code-on-Demand (Yashpal, Kapil & Niranjan, 2012). The client and server paradigm ensures the server give the requested resources to the client. The client ask for a service from the sever through any of the stated communication above, however if the server fail to grant the request of client, the client will pass its request to another server for the same resources, consequence the network traffic is increased and bring about hold-up. Also these methods execute at the users node and does not involves migration of codes, hence mobile agent technology ensures a way out (Pankaj, Divya, & Nripesh, 2014). Mobility is one of the unique properties of mobile agent; this mobility ability has contributed to the major problem that has plagued the mobile agent technology today (Pham & Karmouch, 1998). Normally, the actions of a program can be attributed to the programmer intentions; however it is not true with mobile agent. Mobile agents are similar to malicious worms because they can travel through one host to another without means to detect their intention before carrying out malicious actions against their host (Chess, 1998). The ability of a mobile agent to move or hop (mobility) to a remote host to execute its codes, has brought about some security and ethical challenges in the mobile agent system (Ebietomere & Ekuobase, 2014).

1.1Background to the Study

The unreasonable behaviour of agent, that is deployed online is constituting new security threats (Adekunle, 2011). The major problem is the nature of security issues online, if it is the same as the real world security challanges.Moor, (1985) argues that computer technology generates new possibilities because computer technology is reasonably flexible. Most security threats in the mobile agent paradigm have been acknowledged with proposed solutions. However, some may not have been revealed because of logical flexibility of the mobile agent technology. On this opinion, by a cautious investigation of mobile agent system security failure, it was observed that some methods used in a real world attacks have been introduced and replicated in the mobile agent system. This kind of attack includes tailgating, which has attracted less importance and research in the mobile agent security domain (Mats, 2000; Yao, 2004).A tailgating attack occurs when one agent spy or follow closely with a legitimate agent to gain unauthorized access to the host platform. This implies that a malicious agent may gain unauthorized access to a secured host platform when it accesses the host platform by following and keeping track of the legitimate authorized mobile agent (Adri, 2016; Marikkannu, 2011;).

Overt tailgating or piggybacking is when the illegitimate malicious mobile agent accesses the host platform unauthorized with the assistances and knowledge of the authorized mobile agent without knowing the intention of the agent. However, if the illegitimate mobile agent gains an unauthorized access to the host platform without the knowledge and consent or assistances of an authorized mobile agent but, by hiding to track and observe the legitimate agent or intruding into the agent by waiting near the gate or door to quickly enter once there is any weakness in the host platform security without the consent and knowledge or assistances of the legitimate agent, the process is otherwise called covert tailgating. A situation where a legitimate and an illegitimate malicious agent collaborate to attack a host platform with a full knowledge of the malicious intention of the agent is called conspiracy tailgating (Yao, 2004).

2. A REVIEW OF RECENT AND RELATED MODELS

To actualize this multi gating framework to secure the host platform against tailgating attack, it is paramount to review other current related proposed host protection frameworks and models in a mobile agent system, from the existing body of available literature. This section offers a summarized insight into the different recent security techniques that has been proposed by various research works. The examination into the existing related works and models will assist us to recognize and organized the set of requirements or criteria needed to develop the multi gating framework to secure the host agent against tailgating.

Venkatesan et al.,(2010) made use of is a hybrid mechanism to probe the Integrity of a mobile agent .However, the code trustworthiness test was done using the eXtended Root Canal Algorithm and Malicious Identification Police check the integrity of a mobile agent codes. This technique shows a very low time complication and strong countermeasure against masquerading attack. It also shows some measure of proficiency in terms of time difficulty and secures the itinerant mobile agent from being affected with malicious codes, thereby protecting the host agent from some malicious attacks. While it tends to secure masquerading, it has some limitation due to its inability to curb replay and tailgating attacks. Lin and Varadharajan, (2010) used trust model to improve the safety of the mobile agent system. The model makes use of the conventional safety techniques by adding trust element with respect to some ethical and safety policies. The trust evidence is analyzed and decision is taken, based on the preset information in the trust relationship database. This model has proof of very effective countermeasure against masquerading in a pre determined itinerary but very porous in a dynamic mobile agent itinerary (Lin &Varadharajan, 2010). Marikkannu, (2011) developed and implemented the dual check-point analysis, which is a method that controls tailgating attack of host platform in a mobile agent systems (Tailgating is a kind of attack, in which a malicious agent gains unauthorized access to the host by social engineering means). The dual check-point analysis has a register table called authentication table to ensure the validity and reliability of the visiting agent codes. The technique applies double verification mechanism, with digital signature confirmation at the outer gate and size verification at the inner gate Marikkannu, (2011). However this technique failed to give real solution to all the means of tailgating of the host platform. Furthermore, Prem and his colleagues proposed agent code size method to secure the host platform against the threat from a malicious agent (Prem et.al, 2012). However, code sizing by Prem et.al was not found suitable to detect or prevent most of the malicious treat, thereby not securing or protecting the host platform because:

1. A malicious agent with the same size code can easily masquerade
2. A malicious agent can modify or delete some of the legitimate codes to append or attach malicious codes to make up the original code size of the legitimate mobile agent, so that the legitimate mobile agent will hop around the various hosts with malicious codes
3. A malicious mobile agent and other malicious entities can collaborate with a legitimate mobile agent in its home agency to allow its malicious codes to be encrypted along with the original mobile agent codes to make up the code size. Therefore; the code size mechanism cannot provide security to the host agent

Venkatesanet, (2013) applied the artificial immune system technique to separate and assigns duties to clones agents. With visible distinct duties this technique enhances its security capability against masquerading and greatly reduces the computational cost of the visiting agent and the host platform. However the method is deficient in providing protection against other kinds of attacks (Venkatesanet, Baskaran, Anurika &Dhavachelvan, 2013). Shashank and Nandi, (2014) proposed the self-reliant mobile code which has a blend of various protection methods based on some security requirements like integrity, confidentiality, self-defence skill and symmetric key algorithm. The key components in the symmetric key algorithm were generated and circulated in a safe and sound manner during the time of execution (Shashank & Nandi, 2014).This mechanism was designed to curb unauthorized access to the host platform, however this skill can only control masquerading and alteration threat. Pankaj, (2014) proposed the protection of the itinerant agent using the method of Triple DES- which is to protect the agent codes using triple DES cryptographic algorithm. The codes of the agent can be protected using triple DES by encrypting it in such a form that no other host or agent can access it, except the authorized or the authenticated host agent. Hence, any unauthenticated party can't make any changes of the codes, thereby extending protection to the host platform. However, this proposed security system has not been implemented. In addition it does not have the ability to stop a replay scheme by a malicious host and it does not secure a host agent against a tailgating threat (Pankaj, 2014).

Asha, (2014) proposed a system that provides an environment that protects the legitimate mobile agent from the malicious mobile agent using checksum method which provides authentication checking. The checksum method is used to detect a malicious mobile agent which is appending to a legitimate mobile agent. It provides an environment that protects the legitimate mobile agent and host platform from the malicious itinerant agent. It also, protects the mobile agent from other malicious mobile agents in the platform. The security measure in this work is limited to the activities of a malicious agent against a legitimate agent and host. However, it only satisfies the authentication security services to provide security for the codes, data and state of an itinerant mobile agent and does not protect the execution host platform (Asha, 2014). Later Geetha and Jayakumar, (2015) applied a scheme known as trust and reputation management to proffer solution to the security issues in the mobile agent system, especially itinerant mobile agent and the host platform,. The chief emphasis of this scheme is on the path which the agent is travelling and its destination with a routing table that is designed to direct the itinerary of the mobile agent which is built on trust and reputation. This scheme shows some limitation to other host platform attacks and has been established to be efficient against eavesdropping, alteration and repudiation attacks (Geetha &Jayakumar, 2015)

3 THE MULTI GATING SECURITY FRAMEWORK

This security framework, to detect and prevent tailgating attack is hinged on various gates with respect to security services. The gates are sequentially arranged and allow the passage of an entity at a time. At each of the gate, different security mechanism was implemented.

The first stage or gate of the process of accessing the host agent platform is a combination of authentication and confidentiality. Authentication is the method or process of verifying and confirming the uniqueness or identity of mobile agent that require access to the host platform, while confidentiality makes sure that the codes data carried by a mobile agent during migration from the home agency to the host agency are kept secret and not accessible by not allowed agent (Apoorva, 2014). The combination of these two security requirement is the fundamental building block of the first gate of this framework which is enveloped in GATE ONE.

At the second gate, non-repudiation and code integrity security service was implemented. Non repudiation is the assurance that a mobile agent cannot deny its actions in the execution environment of the host agent. In general, non-repudiation refers to the capacity to make sure that the communication and activities between the mobile agent and the host platform cannot be denied, while code integrity refer to the accuracy and consistency of the codes and the data of the mobile agent. It involves a state where the codes and data of the mobile agent are not corrupt or altered. The mechanism to achieve these security requirements is detailed in GATE TWO.

While at GATE THREE the framework housed a mechanism that checks the honesty (integrity) of the mobile agent behaviour or character. All the gates are sequentially arranged and accessed.

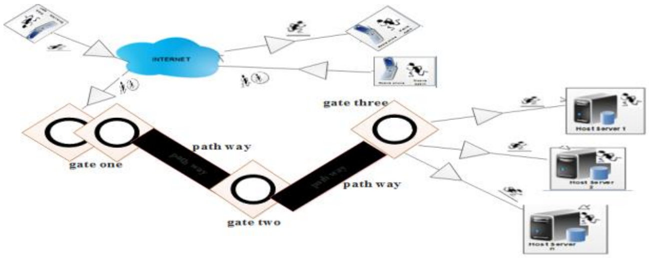

Figure 1: A Multi-gating security framework

3.1 Gate one

To achieve the aim of the first objective of this work, the development of a multi-gating security framework. This framework consists of three main checking points (gates) satisfying various security services. Each of the security services is implemented with a given security mechanism. The first gate consists of the combination of authentication and confidentiality requirements.

The authentication service was implemented using mantrap code sizing. The mantrap is made up of a small lobby or path way with two doors, one door is connected to the unsecured area and the second door is opening into the secured area. To gain access into the lobby of the mantrap from the unsecured side, the visiting mobile agent will register its expected behaviour, its itinerary and code size. At the lobby the code size of the mobile agent will be compare with the required code size as indicated during registration. If the code size matched with the allowed size of the mantrap, the door is unlocked, allowing the mobile agent to enter into the lobby of the mantrap. Once the mobile agent is inside, the door will shuts quickly this will prevents tailgating (since it will not allow more than one mobile agent in the mantrap lobby at a time). With the entrance door shut and the door to the secure area also shut, the codes of the mobile agent will be decrypted to ensure the privacy or confidentiality requirement is satisfied.

The confidentiality service was implemented using the triple data encryption standard (3DES) encryption algorithm. The code of the mobile agent is encrypted at the home agency with the aforementioned 3DES algorithm and it is decrypted at the lobby of the mantrap of the first gate. If the decrypted codes are found to be accessed by unauthorized agent or the privacy is not guaranty, the mobile agent will be denial access to the second gate.

The 3DES algorithm is made of three set of 64 bits keys with a total length of 186 bits. The codes, are first encrypted with the first 64 bits keys, then decrypted with the second 64 bits keys and finally encrypted with the third 64 bits keys, which is represented as follows

CIPHER CODE = ek3 (dk2 (ek1 (plain code)))

While decryption is done at the host plat form (Host agency) in a reverse order of the encryption, which is represented as follows:

ENCRYPTED CODE = dk3 (ek2 (dk1 (plain code)))

This algorithm ensures that the code of a mobile agent, from the home agency is delivered to the authorized destination host plat form. It makes certain that the encrypted code at the home agency is the code received at the host agency (Abomhara, 2010).
The choice of triple DES method to implement confidentiality is to ensure that the codes of the mobile agent get the right destination or the right host platform. Triple DES will make the disclosure of mobile agent codes to unauthorized entity impossible. It is one of the most dependable and accessible cryptosystem used for cyber security today (Hamdan, 2010).
The triple DES encrypted code is decrypted at lobby of gate one after authentication and authorization.

3.2 Gate two

The Second Gate aim is to satisfy the non-repudiation security requirement through the use of the Public Key Infrastructure (PKI) certificate. Mobile agents have the nature of repudiating or denying their actions, hence it should be held responsible for its action. Non-repudiation is a legal concept that is widely deployed in cyber security. It refers to proof of the origin of codes and the integrity of the codes. Non-repudiation makes it very difficult for mobile agents to successfully deny their codes as well as the integrity of the codes. The framework makes use of digital certificate to achieve the non repudiation objective. Digital certificate is a digital form or means of recognition; it provides information about the identity of a mobile agent or its codes. A digital certificate is issued by an authority, known as a certification authority (CA). The authority ensures the legality and soundness of the details in the certificate. Digital certificates make use of public key cryptography. The mobile agent (user) will encrypt its codes with its private keys and make open its public keys via the CA for any other user to decrypt the encrypted codes.

If the public key of the mobile agent (user) can decrypt the codes that are encrypted with the private key of the mobile agent user, it implies that the mobile agent cannot repudiate or deny the ownership of the codes or action as a result of the codes

3.3 Gate three

This gate ensures the integrity of the agent behaviour or character by comparing the register behaviours or characteristics of the mobile agent against the existing pre set behaviours or characteristics. If the characteristics of the mobile agent as captured during registration is similar and meets the preset requirement, the agent is assigned an execution time before allowing it to access the resources. However, if the mobile agent characteristics fall below the required preset features, then the mobile agent will be in suspension and the host agency will update its database with the history of the mobile agent before the agent is killed.

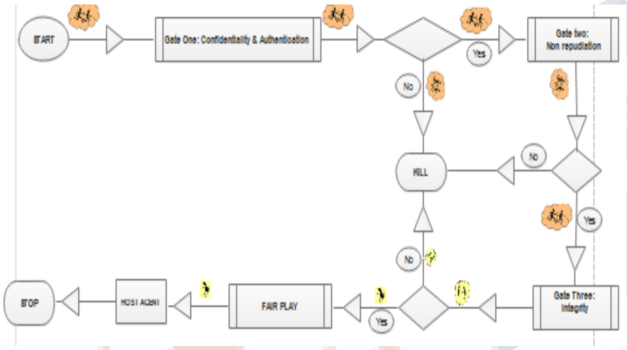

Figure 2: System flow diagram of the multi gating security framework

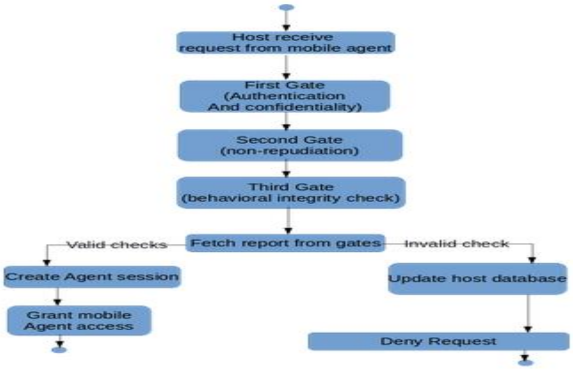

Figure 3: Activities diagram of the multi gating security framework

4. ALGORITHM FOR THE MULTI GATING SECURITY FRAMEWORK

The various activities involved in the multi gating security framework as shown in the program component diagram

Step 1: Mobile agent initialization
Step 2 Mobile agent migrations to the host agent platform
Step 3 Mobile agent registration at gate one
Step 4 Mobile agent at gate one, authentication and confidentiality check,
(A) Authentications :
Code sizing requirement
(B) Confidentiality :
3DES encryption requirement
Step 5 Mobile agent at gate two, non repudiation and code integrity checks,
Digital certificate requirement
Step 6 Mobile agent at gate three behavioural integrity checks,
Mobile agent character check against the pre set behaviour

Step 7 Mobile agent grant access or denial to the host platform resources

Step 8 Mobile agent returns to client machine with the required information

5. CONCLUSSION

A tailgating attack occurs when a malicious mobile agent beat the security at the gate of the host agent platform through social engineering. This study proposed a well designed and efficient multi gating security framework to detect and prevent tailgating attack of the host agent platform for a mobile agent system. This is achieved by designing three gates that implement some security services. This paper presented a new security mechanism that will provide protection against tailgating attack of the host agent. The practical implementation and testing of this proposed security mechanism will be done in another publication.

REFERENCES

1. Abomhara, M.,Omar, Z., Othman, O.,Khalifa, A., &Zaidan, B. (2010). Enhancing selective encryption for H.264/AVC using advance encryption standard.International Journal of Compute and Electrical Engineering (IJCEE), 2(2), 123-128.

2. Adekunle, Y., &Maitanmi, S. (2011).Selected problems on mobile agent communication. International Journal of Computer Science and Information Security, 9(6), 47-53.
3. Adri, J., &Marikkannan, M. (2016). A review on attacks and security approaches in mobile agent technology. Australian Journal of Basic and Applied Sciences,10(2), 37-43.
4. Apoorva, U.,&Mahendra, R. (2014). Application of mobile agents for security using multi level access control.International Journal of Technical Research And Applications 2 (4), 225-230.
5. Asha, A.,&Jesna, A. (2014).An enhanced approach for securing mobile agents from the attack of other malicious mobile agents,International Journal of Research in Engineering and Technology, 4(4), 114-119.
6. Braun, P. and Rossak, R. (2005). Mobile agents: Basic Concepts, Mobility Models and the Tracy Toolkit, Morgan Kaufmann Publishers/ dpunkt.verlag, Elsevier.
7. Chess, D. (1998). Security issues in mobile code systems. In G. Vigna, editor, Mobile Agents and Security, Springer-Verlag, 1-14
8. Ebietomere, E. &Ekuobase, G. (2014). Issues on mobile agent technology a adoption. African Journal of Computing & ICT,7 (1), 88-96.
9. Fuggetta, A., Picco, G., &Vigna G. (1998).Understanding code mobility. IEEE Transactions on Software Engineering, 24(5) 342-361
10. Geetha, K &Jayakumar, M. (2015).Implementationof trust and reputation management for free roaming mobile agent.IEEE systems journal, 6 (9) 556-556.
11. Hamdan, O. ,Zaidan. , B. , Zaidan, A., Hamid. A., Jalab. , M. Shabbir, N. ,& Al-Nabhani, Y. (2010) New comparative study between des, 3des and aeswithin nine factors. journal of computing,2 (3), 44-50.
12. Lin, C. &Varadharajan, B. (2010). Mobil trust: a trust enhanced security architecture for mobile agent system.Journal of information security, 3(9), 153-178
13. Marikkannu, P., Adri, J., &Purusothaman, T. (2011). A secure mobile agent system against tailgating attacks.Journal of Computer Science, 3(7) 488-492
14. Mats, P. (2000) Mobile agent architectures, Defence Research Establishment for Control Warfare Technology Linköping
15. Moor, J. (1985).what is computer ethics Meta philosophy vol.16, no4 October 1985
16. Pankaj, M. Divya, B., Nripesh, K.,(2014) An efficient approach for mobile agent security. Journal of Computer Applications,107(6), 90-95.
17. Pham, V.,& Karmouch, A.(1998). Mobile software agents: an overview, IEEE Communications Magazine, 36 (7), 111-116
18. Prem, V. & Swamynathan, S. (2012). Securing mobile agent and its platform from passive attack of malicious mobile agents IEEE-International Conference on Advances Engineering, Science and Management, 4(3), 90 – 95
19. Shashank, S., & Nandi,G.,(2014) Self-reliant mobile code: A new direction of agent security Journal of Network and Computer Applications 37(1), 62–75
20. Venkatesan, S.,Chellappan, P., &Dhavachelvan, k. (2010). Performance analysis of mobile agent failure recovery in e-service applications.Computer Standards & Interfaces, 7(32)38 – 43.
21. . Venkatesan, S., Baskaran, C., Anurika, V, &Dhavachelvan, P. (2013). Artificial immune System based mobile agent platform protection. Computer Standards and Interfaces, 5(35), 365 – 373.
22. Yashpal, S.,Kapil, G., Niranjan, S (2012) Dimensions and issues of mobile agent International Journal of Artificial Intelligence & Applications (3)5, 2012, 51-61
23. Yao, M.(2004). A security architecture for protecting dynamic components of mobile agents, Ph.D thesis of Information Security Research Centre, Faculty of Information Technology, Queensland University of Technology, Australia, 2004.