Journal of Applied Mathematics, Islamic Azad University of Lahijan, Vol.8, No.4 (31), Winter 2012, pp 105-111
ISSN 2008-6083

The Security Factor in Mobile-Based Applications

M. Ghavidel*
Islamic Azad University, Lahijan Branch, Department of Computer, Lahijan, Iran.

Abstract
Mobile Agents are self-governed applications that can be migrated on a network in order to perfrom special tasks. Mobile Agent programming model is another common Client-Server for an important class of practical network softwares. Apart from the natural adequacy for some types of practical softwares, mobile Agents can be helpful for the optimum usage of softwares, frequencies and increasing the asynchronous potential between the servers and clients. The Mobile Agent technology is a potentially major breakthrough in the network-based applications. Since one of the most important uses of this technology is utilizing it for e-commercing, it's thoroughly evident that security concerns constitute the first priority in such systems. Actually expanding and using Agent-based systems is hinged on solving the security issues in Agents and providing a secure environment for operation in such systems. This article, has tried to categorize the attacking methods and review the security rate of Agent-based systems so that it may further investigate the systems in terms of security measures adopted and compare them with each other.

Keywords Mobile Agent, Security, Attacking methods, Platform, Agent.

1 Security in mobile agent systems

The introduction of mobile code in a network raises several security issues. In a completely closed local area network - contained entirely within one organization- it is possible to trust all machines and the software installed on them [1]. Users may be willing to allow arbitrary Agent programs to execute on their machines, and their Agents to be executed in each arbitrary machines. However in an open network such as the Internet, it is entirely possible that the Agent and server belong to different administrative domains. In such cases, they will have much lower levels of mutual trust. Therefore, security is one of the major topics of discussion in promoting and using Mobile Agent-based applications and without taking into consideration preemptive measures and retaliatory action against Security threats. this technology can hardly be expanded [2,3].

2 Security threats

Several security issues and problems may occur in the Mobile Agent Systems. some of which include:

* **Corresponding Author. (✉)**
E-mail: marzieh.ghavidel@yahoo.com

2.1 Reformation

An Agent may attempt to reform itself in order to deceive the Agent with which it is connected. For example, an Agent may introduce itself as a credible seller of goods and try to convince the other Agent to provide its credit card's password, information of banking account and forms of digital cash and other confidential information. Reformation into another Agent damages both the deceived Agent and the Agent which really possesses this credible identity [4].

2.2 Changing or denying service

The Agent may use the change or service denial attacks on the other Agents. For example, by frequently sending messages from an Agent for another Agent and misleading the Agents with such messages, a heavy unnecessary load may be charged on the routines reviewing the message [5,6].

2.3 Denial

This state occurs when an Agent participates in an interaction or a connection and then claims that the interaction or the connection has never taken place. Whether the reason for the denial is intentional or random, denial may lead to serious altercations which will not be solved easily, unless correct mutual action is taken[5,7].

2.4 Illegal access

If the Agent platform is weak or has no control mechanism in place, an Agent may be directly interfered with by other Agents through recalling general methods (attempting to overload the buffer or setting up initial state, etc.)

2.5 Eavesdropping

This threat includes participation in and supervision over secret connections. Since the platform has access to the code, state and data of the Agent, the Agent met should accept this reality that there would be a possibility of showing exclusive algorithms and secret content of the negotiations, strategies and other sensitive information. Although it's possible that the Agent may not show the secret information directly, the platform is able to guess the values from the requested services and the identity of the Agents with which it's connected. For instance, an Agent may have connections with a travel Agent, and even though the content of the message may not be displayed, this connection can be indicative of the fact that the person who is connected with this Agent may be getting prepared for a travel and may not be in his home in the near future.

2.6 Copy and replaying

Each time that an Agent moves from a platform to another platform, it will be exposed to more security threats. The factor which prevents the transmission of the Agent may try to copy the very Agent or its message and reproduce and resend it. For example, the preventive factor may occupy the shopping requests and display it several times and thus encourage the Agent to go shopping more than what the original Agent had intended.

3 Categorizing the threats

There are various ways to investigate the level of security threats during the occurence in Agent systems in a more precise manner. We could use an Agent system to categorize the security threats as a technique to understand the possible source and destination of the attack [6,8]. There are several models for describing Agent systems. Moreover one of the simple models of Agent systems includes the two main parts: Agent and Agent Platform. In this model, Agent includes a code and the necessary informatic status of some possible calculations. The moving possibllity of Agent allows the Agent to move among the Platforms. Agent Platform provides a calculation space in which the Agent acts. The Platform in which an Agent stablishes, is called the Local Platform and is usually the safest space for an Agent. One or some hosts may include an Agent Platform or an Agent Platform may handle some calculation spaces in which Agents could act.
Four categories of Security Threats are known[9]:

- From an Agent to an Agent Platform.
- From an Agent Platform to an Agent.
- From an Agent to another Agent.
- From outside to an Agent Platform.

The last category , includes the conditions in which an Agent attacks another Agent on another Agent Platform. This attack usually comes from the communicabillity of a Platform and using the weak points. the latest categorization mainly includes conventional attacks on the Agent platform Operations System

4 The precise investigation of the attack and their categorizations

In order to provide the security of the Agent-based systems and comparing them, two essential steps should be taken

- Precisely identifying all the passageways and methods of infiltration and attacking an Agent-based system[5]
- Reviewing the impact rate and the detrimental role of each of these attacks in estimating the security rate of Agent-based systems[4,10]

As it was previously pointed out, the different attacks which can be done on an Agent-based system are classifiable in four general categories. If we take the M1, M2, M3 and M4 sets as corresponding to each of the following groups, then each category will

indicate all the attacking methods in that group. So, the four groups of security threats are as follows[4]:

Group 1: methods of an attack by an Agent on an Agent's platform
Group 2: methods of an attack by an Agent on an Agent
Group 3: methods of an attack by an Agent's platform on an Agent
Group 4: methods of an attack by others on an Agent platform

With the studies done on the attack methods on each of these four groups, 6 states belonging to the group 1 (M1=6), 8 states belonging to the group 2 (M2=8), 10 states belonging to the group 3 (M3=10) and 3 states belonging to the group 4 (M4=3) were identified. It's noteworthy that in the abovementioned classifications, some methods overlap each other and may be classifiable in other forms.

First threat group - an attack of an Agent on an Agent's platform
1- Prohibited access to information and resources of the Agent platform
2- Using one's own allowed access to unexpected or harmful methods (abusing the allowed access methods)
3-Prevention of providing platform services to other Agents through finishing computational sources
4- Prohibited accessing to the list of Agents which are run on the server
5- Reading the internal conditions of the other Agents on a server
6- Prohibition of the Agents' using services provided by the server

Second threat group - an attack of an Agent on another Agent
1- Manipulating the interactions
2- Eavesdropping the phone calls
3- Interfering with the activities of the Agent
4- Giving false response (to direct the requests which it receives from one destination)
5- Denying one of the parties of information exchange
6- Changing face through acting as a medium for the destination Agent
7- Direct interference with Agent by recalling general methods of the Agent
8- Accessing to or changing the code or data of the Agent

Third threat group - an attack of an Agent's platform on an Agent
1- Extracting information
2- Destroying or changing the status code (changing the performance)
3- Refuting the requested services
4- Entering initial values once again or completely finalizing
5- Failing to provide services in return for the Agent's payment
6- Pretending (that it is one of the system's trusted servers)
7- Giving false response to the request of services and information
8- Putting off the Agent
9- Failing to completely execute the Agent
10- Rewriting the Agent (in order to astounding or deceiving the other Agents)

Fourth threat group - an attack of others on the Agent platform
1- Attacking the relations between the Agent and the platform

2- Preventing the transmission of Agents' messages or distorting their content
3- Revealing the relationships between the Agents

5 Calculating the security rate of agent-based systems

Based on the categorizations which have been carried out, M=27 states of attacking against an Agent are identifiable. It should be reminded once again that in the abovementioned categorizations, some methods overlap the others, meaning that one method may cover the whole or part of another method and that's why another person may want to define each method in a more precise and transparent way in which case, it's possible that a change may take place in the number of the members of the group. At any rate, even if take the number of methods as "n" to generalize the discussion, the security rate will be available in three different states. In each case, we consider one state as the baseline and try to improve this condition in the next state so that it may come closer to reality [7,10,11].

First state
In this condition it's assumed that protect against each of these methods are of the same value. In other words, the system which can prevent more attacks and it's not important that which attack is prevented. In this condition, S as the Security Factor is defined as such:

$$\textbf{Scoef}= \frac{m}{n}$$

$$\mathbf{0} \le \mathbf{Scoef} \le \mathbf{1}$$

In which **n** is the number of total methods with which we could attack an Agent-based system and **m** is the number of conditions that a specific system could be protected.

Second state
In the second situation, it's assumed that the protection against each of the methods aren't of the same value and the share of each technique is different with others. In other words according to the practice of each system, prevention using some techniques may be more important than others. In fact, in this case we want to specify a grade to each of the **n** approach in order to highlight the importance of prevention of each technique in rising the overall security of the system.

Hereby, in order to specify the weight of each of these methods, some parameters can be used such as the importance of preventing this method, attacking in a particular application or the frequency of the emergence of attacks, etc. In a general sense, we assume that to give weight to these methods, k parameters were defined (it's assumed that all k parameters have equal value); therefore, $w=\frac{1}{k}$ will be the weight of each parameter and so the weight of each of these n methods may be calculated accordingly[8]:

$$w=\frac{1}{k}\sum_{i=1}^{k} p_i$$

Now we calculate the weight or rate of each method vis-à-vis the other methods by taking into consideration all the weights which have been calculated:

$$D_i = \frac{w_i}{\sum_{i=1}^{n} w_i}$$

D_i indicates the rate of the i-th method as compared to the whole methods.
So, the security rate of the system can be calculated this way:

$$\textbf{Scoef=} \sum_{i=1}^{n} D_i a_i$$

In the equation above, D_i indicates the weight or rate of each method with reference to the whole methods and a_i indicates whether the system is capable of preventing the attacks of that type or not. The value of a_i will be equal to 1 if the system is protected against the attacks and will be if not so.

Third state
The third state is similar to the second state, with the only difference in this system we won't assume the same grade to each methods but The parameters in each method can have similar weight and value. We solve the problem with this assumption that the parameters in each method have a separate weight and so we will have:

$$W=\sum_{i=1}^{k} p_i k_i$$

p_i indicates the i-th parameter.
The other calculations are done like the second method and therefore the resultant security rate will be closer to reality.
From the determined Security Factor in the forementioned conditions, it could be that:

1) The investigation of an Agent-based system according to the security techniques in the system and the interrogativeness.
2) Determining the weak points of the architecture of the current Agent and a procedure to continue.
3) Guidance to provide the security cases of the new Agent systems.

6 Conclusion

Agent-based systems provide diverse and useful services to the computer networks and it's evident that expanding and using Agent-based systems will lead to dependence on security issues and preparing a safe environment for operations on such systems. calculating the security rate of Agent-based systems, it can be concluded that despite the

remarkable achievements which were made in terms of security issues, there are still numerous unsolved problems in the applications which need high security level that constitute obstacles to the ever-increasing use of such technologies. Therefore, universities and research centers should give priority to this part of research so that to meet the security requirements needed for these systems in a more comprehensive way than the existing systems.

7 References

[1] Fuggetta, A., Picco, G.P., Vigna, G., (2006). Understanding Code Mobility. IEEE Transactions on Software Engineering.
[2] Andreou, P., Zeinalipour Yazti, D., Andreou, M., Chrysanthis, P. K., Samaras, G., (2009). Mobile Data Management. IEEE International Conference.
[3] Mobile Agent white paper, (2008). General magic.
[4] Armoogum, S., Caully, A., (2011). Obfuscation Techniques for Mobile Agent code confidentiality. Journal of Information & Systems Management.
[5] Ghavidel, M., (2009). Security In Mobile Agent System. First National Conference on Software Engineering Applications :Islamic Azad University-Lahijan Branch, Iran.
[6] Kun, Y., Dayou, G. X. L., (2011). Security in Mobile Agent System problems and approaches. National Natural Science.
[7] Samaras, G., (2004). MobileData Management. IEEE International Conference.
[8] Snehi, J., Snehi, M., Goyal, S., Security threats to mobile agents. ACAI '11 Proceedings of the International Conference on Advances in Computing and Artificial Intelligence pages 220-222.
[9] Jansen, W. A., (2009). Countermeasures for Mobile Agent Security. National Institute of Standards and Technology, Gaithersburg, MD, USA.
[10] Borselius, N., (2012). Mobile agent security, Electronics & Communication Engineering. Journal, Volume 14, no 5, IEE, London, UK, pp 211-218.
[11] Huanmei, G., Huanmei, Z., Xuejun, M., Jingwei, Z., (2010). A Communications Security Protocol of Mobile Agent System. Wuhan University Of Natural Science.