ISSN: 2319 – 8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 1, Issue 2, December 2012

A Survey of E-Business Security For Mobile Multi-Agent Environment

Ms. Swati Aggarwal[1], Mr. Suyash Bhardwaj[2]

Assistant Professor, Dept. Of Computer Application, IMS Engineering College Ghaziabad, U.P, India[1]

Assistant Professor, Department of Computer Science & Engineering, Faculty of Engineering & Technology,

Gurukul Kangri University, Haridwar, Uttarakhand, India[2]

Abstract: Agent technology is a very emerging field of research. Various classes of agents (e.g. intelligent agents, software agents) have emerged so far. Software Agents including Mobile Agents are useful for Distributed Systems & Electronic Commerce. E-Commerce and M-Commerce can help a company or enterprise to extend its market place to unlimited region. With the increasing market of Electronic Commerce it becomes an interesting aspect to use autonomous Mobile Agents (MAs) for Electronic Business transactions.

Since, various components of E-business can be represented by Software Agent/ Mobile Agents it can be viewed as a multi-agent environment. To fully deploy agents in multi-agent environment require addressing number of challenging issues like Security, Fault Tolerance, Location Management and Privacy of both agents and executing environment. However, scope of this paper is limited to security of mobile agents in a multi-agent environment for Electronic Business applications.

Security is focused mainly on protection and security of agents and its runtime environment, but most of the currently available mobile agent systems do not support comprehensive security requirements for a general Mobile Agents paradigm. Therefore, there is a need for a complete and comprehensive security infrastructure for mobile agents, not only in the form of security services and mechanisms for agents runtime execution, but also as a complete set of infrastructural components along with methodology for creation, classification, adoption, and validation of Mobile agents, before their deployment in real-environment.

This paper studies the various security solutions proposed by researchers for Mobile Agents in Multi Agent environment for Electronic business applications and analyze then on the basis of various parameters such as performance, requirements and complexity.

Keywords: Mobile Agent, Mobile Agent Platform, Security, Trust, Multi Agent Environment, E-commerce.

I. INTRODUCTION

"A mobile agent is defined as a class of agent" with the ability during execution to migrate from one host to another where it can resume its execution and while this may assist in network traffic reduction and in overcoming latencies in the network, the ability of the agent to move around "does however introduce significant security concerns".

Mobile agents are no longer theoretical issue since different architecture for their realization has been proposed. The goal of mobile agent system is to provide a distributed computing infrastructure supporting applications whose components can move between different execution environments.

Electronic Commerce can help a company or enterprise to extend its market place to unlimited region. But security is the primary concern for the E- Commerce application in mobile agent computing.

ISSN: 2319 – 8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 1, Issue 2, December 2012

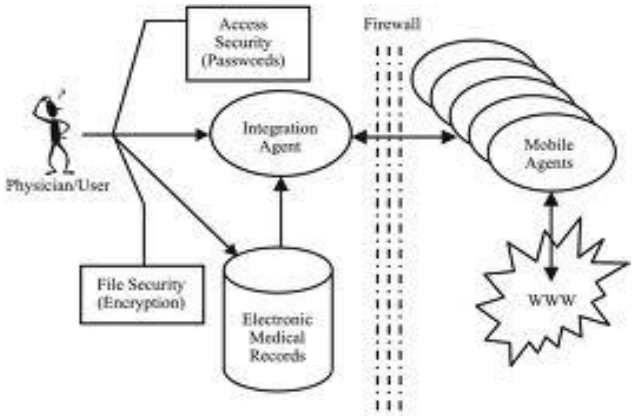

Figure1: Mobile Agent with Ecommerce Transaction

The problem of security data section in a Mobile Agent from discovery & exploitation by a malicious host is a different task. Mobile agent systems provide a greater flexibility and customizability to distributed applications like Electronic Business & information retrieval in the current scenario. Security is a very crucial issue for the money transactions in Business. But most of the currently available Mobile Agent systems do not support comprehensive security requirements for general Mobile Agent paradigms. Hence security is a very big issue for Mobile Agent system in Multi Agent is a challenging issue. Therefore there is a need for a complete & comprehensive security infrastructure for Mobile Agents in Multi Agents environments for Electronic Business applications.

In this paper we present a survey on security for a mobile agent system in Multi Agent environment.

II. MOBILE AGENT SYSTEM MODEL AND THE MALICIOUS HOST PROBLEM

Mobile Agents are capable of continued, autonomous operation disconnected from the owner and they migrate to other hosts during their lifetime to perform their task.

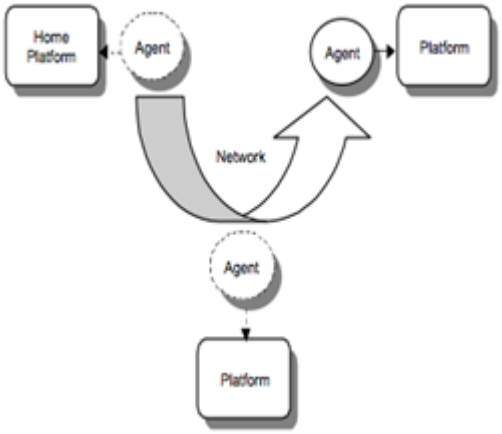

Figure2: Agent System Model

The use of mobile-agents saves bandwidth and permits off-line and autonomous execution in comparison to usual distributed systems based on message passing as shown in Figure 2 below. Essentially, a mobile-agent consists of code, data and state information needed to carry some computation.

ISSN: 2319 – 8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 1, Issue 2, December 2012

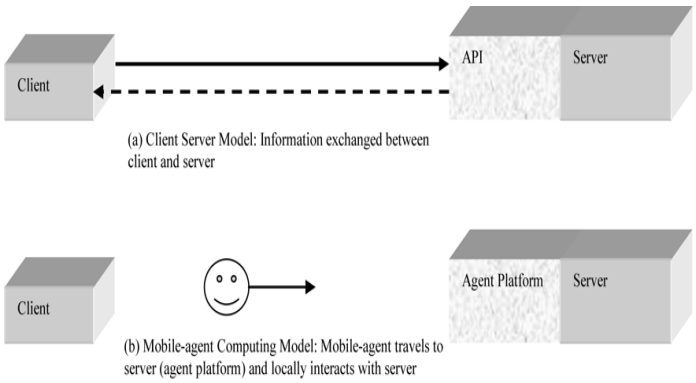

Figure 3: Client-Server model versus Mobile-Agent computing model

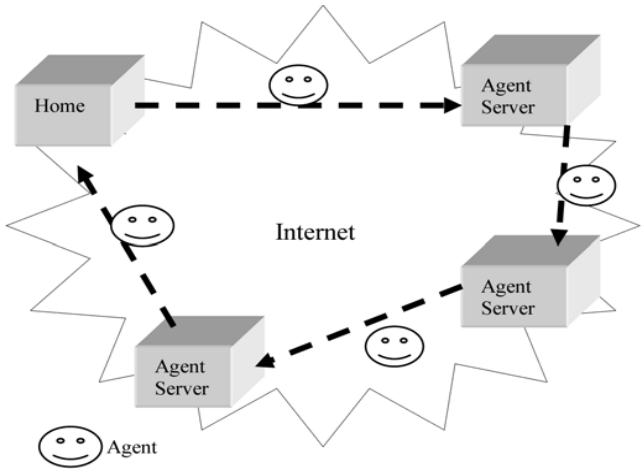

Figure 4: Mobile-agent computing model

As can be observed from Figure 1 and 2, mobile agents hop from agent server to agent server and execute locally on the destination agent platform. The agent servers have complete control on the executing mobile-agents and thus many attacks may be performed by malicious servers on the mobile-agent. The malicious server can modify the code, data, and/or state information being carried by the mobile-agent. Likewise the malicious server can inspect the code of the mobile-agent to learn about the decision making strategy of the agent. Again the malicious server may inspect the confidential data such as credit card details or signing key being carried by the mobile-agent. Thus, the protection of mobile-agents from malevolent agent servers is as important as the protection of the host from malicious mobile-agents. Ideally, it is required that the mobile agent be equipped with security features that enables it to execute in a un trusted environment autonomously (i.e. without interactions with its originating site) and without the un trusted host being able to read and modify the mobile-agent's code and data.

III. ISSUES AND CHALENGES FOR MOBILE AGENTS [5]

Security Issues

1) *Protecting network communication*
    1. Protecting hosts from agents
    2. Illegal access
2) *Denial of service*
3) *Protecting agents from hosts*
    1. Tampering

ISSN: 2319 – 8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 1, Issue 2, December 2012

2. Extracting information
3. Capture / Replay

4) System-wide Administration / Management

1. Policies
2. Tracking / Visualization

5) Access to non-mobile resources

1. Network endpoints
2. Files

6) Deployment (of environments)

1. Interoperability
2. Debugging
3. Highly Asynchronous

IV. THREATS TO MOBILE AGENTS [6]

In a mobile agent system a malicious host is defined as a host that executes an agent and tries to attack the agent in some way. When an agent is executed on a host it must use the resources available on that host. The host can monitor an agent's memory usage and each instruction given by the agent to the host. A malicious host may then attempt to attack an agent in a number of ways. The four main forms of attacks by hosts on mobile agents are [4]

1. A host masquerading as another host.
2. Denial of service by the host to the agent.
3. Eavesdropping on an agent's activity.
4. Alteration of the agent by the host.

MASQUERADING

A masquerading host may try to trick the agent into believing it is another host and cause the agent to give the host sensitive information. Once the masquerading host is able to gain the trust of the agent, it may then be able to read or modify any of agent's code, data and state if mechanisms are not put in place to protect this type of attack. The main solution to prevent this type of attack is to use a strong authentication protocol to authenticate a host to an agent.

DENIAL OF SERVICE

A host may deny an agent a specific service provided by the host. It is possible for a host to both intentionally and unintentionally deny an agent a service. A host may deny an agent service so that the agent is not able to complete its task. Another possible attack is the host could terminate the agent altogether. Furthermore, a host may deny a request from an agent on a time-sensitive task so that the agent is unable to complete its task in its allotted time [3].

EAVESDROPPING

The next attack that can be performed by the host on an agent is eavesdropping. In a Client/server environment, the typical eavesdropping attack comes from the monitoring of a communication channel. In the case of a mobile agent system, malicious hosts may try to determine the code, data, or flow control held by the agent. This form of attack is difficult to prevent and detect. The goal of all three of the methods to be discussed in this paper is to limit the information that can be read by a host. Even when all of the information is hidden from the host, the host may still be able to infer some information from the agent. The main problem is that the agent must execute on the host so the host is able to record each instruction given to it by the agent.

ALTERATION

The final form of attack by a host on an agent is the alteration of the agent. The host can alter an agent by changing the data, code and control flow. A malicious host may try to change the code of an agent so that the agent performs other tasks than were intended by its creator. A host may also try to change the data contained in the agent.

V. MOBILE AGENT SECURITY

Security is one of the greatest weaknesses to a Mobile Agent. Security alone is a large reason for the lack of use of agents for providing the solutions they promise (Li, Zhang, sun & yin 2004). A huge amount of research material is available that has

either raised the notion of security of mobile agents or has tried to solve it in one way or another. The notion of mobile agent security is because the mobile agents that are roaming a network can be used as malicious objects for accessing private or confidential information and resource, for causing corruption like viruses and worms and so on. Similarly, in this regard if an agent is supposed to be correct and non malicious, we are never sure that the place it is visiting may be malicious to it or not and may also leech information from the agent, corrupt it or even use it for its malicious purpose.[8]

In a client/server type of distributed system the security issues are well known and adequate solutions exist [PC97]. The clients and servers are generally grouped into an administrative domain with a set of registered users. In addition, the client is executed on the user's machine. Since they run in the same administrative domain, a user trusts a server or can at least prove that incorrect results have been received. The security in a mobile code environment cannot rely on this trust relationship between the server and an agent because they are generally not part of the same administrative domain. In addition, the problem of protecting the agent and its results from malicious and faulty servers arises. Whereas the protection of the server in a mobile agent environment is a problem that has been mastered in most cases, the protection of the agent is still open. The following subsections discuss server and agent protection separately. [9]

Hence Security is a fundamental concern for a mobile agent system. Harrison et al. [11] identified security as a “severe concern" and regarded it as the primary obstacle to adopting mobile agent systems. The operation of a mobile agent system will normally be subject to various agreements, whether declared or tacit. These agreements may be violated, accidentally or intentionally, by the parties they are intended to serve. A mobile agent system can also be threatened by parties outside of the agreements: they may
1. Create rogue agents
2. Hijack existing agents
3. Commandeer servers

There are a variety of desirable security goals for a mobile agent system. Most of these concern the interaction between agents and servers. The user on behalf of whom an agent operates wants it to be protected to the extent possible from malicious or inept servers and from the intermediate hosts which are involved in its transmission. Conversely, A server and the site at which it operates needs to be protected from malicious or harmful behaviour by an agent. Not all attractive goals can be achieved, however, except in special circumstances. In the case of mobile agents, one of the primary motivations is that they allow a broad range of user’s access to a broad range of services offered by different frequently competing organizations. Thus, in many of the most natural applications, many of the parties do not trust each other. In our opinion, some previous work (for instance [12]) is vitiated by this fact:

It assumes a degree of trust among the participants which will not exist in many applications of primary interest. Nevertheless, the special cases may be of interest to some organizations. A large organization like the United States Department of defence might set up a mobile agent system for inter service use; administrative and technical constraints might ensure that the different parties can trust each other in ways that commercial organizations do not. In this paper, however, we will focus on the more generic case, in which there will be mistrust and attempts to cheat. We assume that different parties will have different degrees of trust for each other, and in fact some parties may be in a competitive or even hostile relation to one another. As a consequence, we may infer that one party cannot be certain that another party is running an untempered server. An agent that reaches that party may not be allowed to run correctly, or it may be discarded. The server may forge messages purporting to be from the agent. Moreover, the server may inspect the state of the agent to ferret out its secrets. For this reason, we assume that agents do not carry keys. Existing approaches for distributed security [13] allow us to achieve several basic goals. These include authenticating an agent's endorser and its sender, checking the integrity of its code, and offering it privacy during transmission, at least between servers willing to engage in symmetric encryption. However, at least three crucial security goals remain:

1. Certification that a server has the authority to execute an agent on behalf of its sender. If executing an agent involves contacting other servers, then a server may have to authenticate that it is a legitimate representative of the agent. The sender of an agent may want to control which servers will be allowed to authenticate themselves in this role.
2. Flexible selection of privileges, so that an agent arriving at a server may be given the privileges necessary to carry out the task for which it has come to the server. There are some applications in which a sender wants his agent to run with restricted authority most of the time, but with greater authority in certain situations.

ISSN: 2319 – 8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 1, Issue 2, December 2012

3. State appraisal, to ensure that an agent has not become malicious as a consequence of alterations to its state. Because a migrating agent can become malicious if its state is corrupted, However, the test must be application-specific, which suggests that reputable manufacturers of mobile agents may want to provide each one with an appropriate state appraisal function to be used each time a server starts an agent. The code to check the agent's state may be shipped under the same cryptographic signature that protects the rest of the agent's code, so that a malicious intermediary cannot surreptitiously modify the state appraisal function. [10]

VI. MOBILE AGENT SECURITY IN THE FIELD OF ECOMMERCE

Mobile agents are well suited for electronic commerce. A commercial transaction may require real-time access to remote resources such as stock quotes and perhaps even agent-to-agent negotiation. Different agents will have different goals, and will implement and exercise different strategies to accomplish these goals. Wanna liui [15] envision agents that embody the intentions of their creators, and act and negotiate on their behalf? Mobile agent technology is a very appealing solution to this kind of problem.

A typical E-commerce transaction can be divided into following five phases: [14]

1. **Search**: *In this phase, a consumer searches for an item that he wishes to purchase from different online sellers.*
2. **Valuation:** In the valuation phase, the consumer compares offers form different sellers to select the item that best matches his needs.
3. **Logistics:** During this phase, the details of the transaction are exchanged between the buyer and the seller during this phase. The seller conveys the details of the item to the buyer responds with specific requirements. Negotiation of price and other attributes also take place during this phase. At the end of this phase, the protocol for the exchange of the item between the buyer and the seller is determined. For ex. The seller might accept payment form a specific credit card only, or the buyer might prefer a specific mode of delievery.
4. **Transaction:** The actual exchange of the item takes place in this phase. The buyer pays the seller the required monetary amount decided in the logistics phase. The seller then delivers the item to the buyer. Typically, this phase involves trusted third parties, like the financial institution.
5. **Post –sales service:** In this phase, sellers provide services related to the item after it has been sold. This might involve setup of item at the consumer's location, or repair or replacement of a defective item. This phase relies on the good will of the seller and is often overlooked or neglected in both traditional and e-commerce.

VII. USE OF MOBILE AGENT IN ELECTRONIC COMMERCE ENVIRONMENT

Multi-Agent System (MAS) [14] architectures can be used for e-Business application due their flexibility, scalability and interoperability. Agent ownership implies that a specific person or organization (the owner) is responsible for the agent's actions. Agents, whose ownership was certainly fixed, could operate on behalf of their owner to make transactions, to buy or sell products. Security requirements in the agent ownership setting process are the identification of the owner and the protection of the identification information carried by an agent.

The immense popularity of ecommerce in the span of a few years indicates that the benefits form converting traditional sales to online sales are extremely attractive. Next we look at the ways in which the internet has changed the traditional model of commerce to the advantage of both online buyers and online sellers. The advantage offered by converting traditional business procedures to internet processes is more than just keeping up with the trend to convert into "dotcom-s". Existing mobile agent systems [16]

With the introduction of Java to the Internet world, many mobile agent projects have made use of this operating system independent language. Another benefit to using Java is that each of these systems can make use of the standards that are inherent in Java such as the Java virtual machine and object serialization mechanism. Some of these systems are listed below:

1. **Aglets***:* It is the IBM's mobile agent system. The word Aglet is formed through the combination the words agent and applet, as the intention of this system is to bring mobility to Java applets [17].

2. **Odyssey**: From General Magic Inc. was the first mobile agent system. It was reworked using Java and now provides a set of Java classes that developers can make use of to create their own mobile agent applications [18].

3. **Concordia**: It is the Mitsubishi's agent system which provides developers with a framework for the development and the management of mobile agent applications[35]. These applications can be extended to any system supporting Java.

4. **Voyager**: It is an agent based system that supports both traditional and agent-based distributed computing techniques created by Object Space. Voyager supports object request brokering so developers can create distributed application using both traditional messaging, such as CORBA or RMI, as well as agent-enhanced techniques [19].

ISSN: 2319 – 8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 1, Issue 2, December 2012

VIII. SECURITY THREAD CHALLENGES

Security of financial transactions, being executed from some remote location and transmission of financial information over the air, are the most complicated challenges that need to be addressed jointly by mobile application developers, wireless network service providers and the banks' IT departments.

The following aspects need to be addressed to offer a secure infrastructure for financial transaction over wireless network:

Physical part of the hand-held device. If the bank is offering smart-card based security, the physical security of the device is more important.

Security of any thick-client application running on the device. In case the device is stolen, the hacker should require at least an ID/Password to access the application.

Authentication of the device with service provider before initiating a transaction. This would ensure that unauthorized devices are not connected to perform financial transactions. User ID / Password authentication of bank's customer.

Encryption of the data being transmitted over the air. Encryption the data that will be stored in device for later / off-line analysis by the customer.

One-time password (OTPs) are the latest tool used by financial and banking service providers in the fight against cyber fraud. Instead of relying on traditional memorized passwords, OTPs are requested by consumers each time they want to perform transactions using the online or mobile banking interface. When the request is received the password is sent to the consumer's phone via SMS. The password is expired once it has been used or once its scheduled life-cycle has expired.

Because of the concerns made explicit above, it is extremely important that SMS gateway providers can provide a decent quality of service for banks and financial institutions in regards to SMS services. Therefore, the provision of service level agreements (SLAs) is a requirement for this industry; it is necessary to give the bank customer delivery guarantees of all messages, as well as measurements on the speed of delivery, throughput, etc. SLAs give the service parameters in which a messaging solution is guaranteed to perform.

IX. SOLUTION PROPOSED

1. Security Mechanisms to Protect Agents

A number of approaches have been developed to protect mobile code. The approaches can be classified into four types of protection [21]:

1. Mobile agents are only able to migrate to trusted hosts in the system.
2. Organizational methods are employed to protect agents (i.e. creating a closed system where only trust worth parties can operate a host).
3. Tamper-resistant hardware is used to ensure the integrity of an agent.
4. Restricted environments are setup and cryptographic protocols are employed to make tampering with mobile code difficult and time consuming.

2. Preventive Security Mechanisms

Three methods have been proposed to prevent the analysis of a mobile agent. Each of the methods attempts to hide the code and data of the mobile agent. First, the time-limited black box approach conceals the code of a mobile agent by obfuscating the agent's code. Second, cryptographic methods are used in computing with encrypted functions. Third, environmental key generation is used to generate a key to unlock the encrypted code contained in the agent.

3. Time-Limited Black Box (Obfuscated Code)

Fritz Holh proposed the use of a time-limited black box as a way of protecting mobile agents [20]. Each agent is a time-limited black box for which it is possible only to observe the input and output of the black box. In this situation, the host environment is given obfuscated code by the agent. The aim of using obfuscated code is that a host will execute the code and have no idea what the code is actually doing. One of the problems with this approach is there is no known way to enforce the black box property for an infinite period of time, for this reason a time limit was introduced. While there is no way to prove that host will not be able to determine the meaning of the code, Holtz suggests using a lower time bound for how long the agent is to remain valid. The lower bound is used establish how long it will take a host to discover the meaning of the code given to it by the agent for execution. After the time limit expires, the agent is invalidated. The major problem with creating an agent that has the time-limited black box property is determining what the time limit should be.

4. Computing with Encrypted Functions

Sander and Tschudin proposed computing with encrypted functions (CEF) [22]. The goal of computing with encrypted functions is to hide the actual functions used by the agent from the host. One of the main drawbacks seen with time-limited black box

ISSN: 2319 – 8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 1, Issue 2, December 2012

method is that it fails to provide a verifiable form protection. For this reason, CEF was created so a verifiable level of protection can be given to an agent. In this scheme each agent has a program that is made up of encrypted functions. The authors propose the use of homomorphism encryption both to keep the agent's functions secret from the host and host data secret from the agent.

5. Environmental Key Generation (Clueless Agents)

Another method that employs encryption is environmental key generation, which was introduced by Riordan and Schneier [23]. As opposed to introducing a new form of encryption, environmental key generation aims at hiding the key to the encryption algorithm. Environmental key generation is a mechanism that causes an agent to take a specific action when an environmental condition becomes true. Each mobile agent will contain a portion of its code in plain text and another portion that is cipher text. The agents are labeled clueless because the full capability of the agent cannot be discovered until the cipher text is decrypted. When the environmental condition becomes true, the agent is then able to execute the code that was hidden cryptographically. The environmental condition that triggers decryption is hidden by a one-way hash function.

Security in mobile agent systems can be analysed in four different perspectives [24]:

1. Protecting hosts from access by unauthorized parties.
2. Protecting hosts from attacks of malicious agents.
3. Protecting agents from attacks of other agents.
4. Protecting agents from attacks of malicious hosts.

1. Protecting Hosts from Access by Unauthorized Parties: -During all the four identified stages it is vital that the hosts are protected from being accessed by unauthorized parties. There are many situations where this can happen. A host may not want an agent from a competing company performing queries about its prices and conditions. Also, a host may only serve certain specific types of clients like gross retailers. A general consumer may try to use the host in order to cut a better deal, although he has no right to do so. Thus, securing hosts against access from unauthorized parties implies the provision of mechanisms to allow proper identification of agent owners. Some traditional security mechanisms can be used:

1. Use of public key cryptography for signing the agent code. This allows the owner of the agent and also its manufacturer to be properly identified.
2. Use of public key cryptography for host authentication.
3. Use of secure communication channels for agent transmission (e.g., the Secure Socket Layer Protocol– SSL).
4. Use of secure hashed and encrypted time stamping to avoid reply and masquerading attacks.

There is one aspect of security in mobile agent systems that are quite different from what happens in the client/server paradigm. There is a very large conceptual difference between who writes the mobile agent code and who uses it. If the code is signed with the private key of the user, making it its principal, then the code writer can plan and execute attacks using the identity of the user. If the programmer signs the code, the user will not be accounted for when the program is being executed. Signing the code with both keys is really necessary. In order to secure hosts against unauthorized parties and account users for used resources, there must exist a public key distribution directory that hosts can query.

2. **Protecting Hosts from Attacks of Malicious Agents**: - Although the user and programmer of an agent can be accounted for, considering the Internet and large anonymous distributed systems, it is quite simple to obtain an untraceable anonymous identity. The Internet is especially propitious for that. Users like to maintain their anonymity unless they effectively have to reveal it. Picturing a global electronic commerce framework, users should probably prefer to make queries about prices and assets anonymously and only reveal their identities at the places where they actually make the acquisitions. Revealing the user identity to every host queried is not so compelling since everyone would be able to learn what the user is looking for, and could even start to maintain information about the user's shopping patterns. Even though users with an anonymous identity may have limited executing permissions on hosts, these identities can serve as Trojan horses for agents to get executing inside public hosted platforms. It is important that hosts can protect themselves from executing agents and that agents are accounted for used resources. Effectively protecting hosts from agents (malicious or not) is a security requirement necessary for all the identified stages of e-commerce model being used. In order to protect hosts from agents, some mechanisms can be used:

1. Use of secure languages that isolate system resources and address spaces that agents can access.
2. Use of proxies that encapsulate requested resources by agents.
3. Use of resource control mechanisms that restrict the agent's use of memory, CPU, disk space, threads, network resources and others.
4. Use of audit trails for accountability on the actions of agents.
5. Use of access control lists (ACLs) mapping what resources each agent can access.
6. Use of accounting and contract mechanisms for establishing different accesses in ACLs.

3. Protecting Agents from Attacks of Other Agents : - When agents communicate with other agents, sharing objects and resources, it is necessary to prevent malicious agents from attacking others. Also, if several independent agents are

ISSN: 2319 – 8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 1, Issue 2, December 2012

executing, each agent must be able to conduct its actions without being harassed by others. Agents will have to communicate with other agents during all the stages of the transaction. On the presented model of e-commerce, agents will typically communicate with stationary agents that represent the stores. Nevertheless, in other models, agents may communicate with agents from these stores in a neutral ground. Neutral grounds are independent hosts that accept agents from users and also agents representing stores, providing a safe place where they can communicate. Security methods for protecting agents from other agents depend directly on how the coordination between agents is designed. Some mechanisms are immediately relevant when considering security on these systems:

1. Use of proxies to shield agents from other agents (if object sharing is used). Means to stop object sharing, if an agent feels it is necessary.
2. Use of "ignore lists" to allow an agent to refuse messages from other agents.
3. The possibility of warning the system if an agent attempts an attack.
4. Platform mechanisms for monitoring agents and agents' behaviour.
5. Maintaining lists of agents and agents' principal's behavioural patterns (rap sheets).

4. Protecting Agents from Attacks of Malicious Hosts: - When a host receives a mobile agent for execution, it is possible that the host spies or interferes with the agent's execution. Let us consider the case where an agent is shopping for flowers. A malicious host may try to read and modify offers from other hosts or even change the flow of execution of the agent in order to force it to take an offer being proposed. Because agents execute on a target platform and have to expose both their code and state, it does not seem possible to fully protect agents from malicious hosts [3]. Nevertheless, due to the special characteristics of e-commerce systems, we believe it is possible to guarantee some safety for the agents. When we consider the security requirements in terms of protecting agents from malicious hosts, different needs exist during the different stages of the electronic transaction.

These protocols enable an agent to collect individual offers from hosts in a secure way. Each offer is encrypted and signed by each host. Also, a characteristics of the private tuple spaces, the security issues and mechanisms previously discussed for the other models still apply. An alternative to private tuple spaces is to use public tuple spaces with protected tuples: some agents can only access certain tuples. Security in shared tuples-spaces can benefit from some mechanisms:

1. Tuples can have access control lists specifying which agents can access, modify or delete the tuples.
2. The platforms should monitor accesses to the tuple spaces to prevent denial-of-service attacks by reading or writing too quickly in them.
3. Depending on the credentials of agents, they may or may not be able to create private tuple spaces. E-commerce systems based on mobile agents must provide the means for enabling secure communication and coordination between agents. Securing agents against agent attacks is that it is highly dependent on the coordination model that is used. If several security models are used, different policies must be analysed and implemented.

CONCLUSION

E-commerce, a new way to conduct business, is gaining more and more popularity. Despite its rapid growth, there are limitations that hinder the expansion of ecommerce. The primary concern for most people when talking about on-line shopping is security. Due to the open nature of the Internet, personal financial details necessary for on-line shopping can be stolen if sufficient security mechanism is not put in place. Hence Security is the most important factor for the mobile agent. Having security features to protect mobile agents in the past was considered a nice feature to have for a mobile agent system. Much of the attention in the past focused on creating security solutions to protect a host in a mobile agent system. Without security mechanisms to protect a mobile agent many of the proposed uses for agents would not be possible. In the case of the scenario of purchasing an airline ticket, a number of attacks on agents are possible if appropriate security measures aren't in place.
Digital signatures can help to protect an agent against some attacks. For example, if an agent's code is modified, the owner of the agent is able to detect the attack through the use of digital signatures. But Digital signatures and many other solutions fail to protect a malicious host from determining the data and algorithms used by agent. A difficult problem is finding a way to keep an agent's code and data private in the field of E-commerce.

There are many solutions existing but each of these solutions is not perfect they provide some form of protection to a mobile agent. None of these solutions solve all of the problems needed to keep a mobile agent secure. The methods may be combined with other methods to provide a secure environment for mobile agents. This paper explored the importance of security feature of mobile agent for ecommerce in a multi agent environment.

ACKNOWLEDGMENT

We extend our sincere acknowledgements to faculty members of our institutes and other contributors for providing us the technical assistance for carrying out the experiments and study. Our truthful appreciation is to laboratory staff and personal who were there to provide the facilities and round the clock services for preparing this research paper.

REFERENCES

[1] Fuggetta A., G.P. Picco, and G. Vigna. 1998. Understanding Code Mobility. *IEEE Transactions on Software Engineering, 24(5).*

[2] FIPA Specification, part 1, version 2.0, Agent Management. Foundation for Intelligent Physical Agents, October 1998

[3] Object Management Group (OMG) Technical Committee (TC). 1997. Mobile Agent System Interoperability Facilities Specification. Document orbos/97-10-05.

[4] Jansen, Wayne., Karygiannis, Tom. NIST Special Publication 800-19 – Mobile Agent Security.

[5] Mobile Agents by Niranjan Suri nsuri@ai.uwf.edu

[6] Preventing Attacks on Mobile Agents by Malicious Hosts Nathan Balon, University of Michigan Dearborn

[7] W. Jansen. Counter measures for Mobile Agent Security. In Computer Communications, Special Issue on Advances in Research and Application of Network Security, November 2000. http://citeseer.ist.psu.edu/article/jansen00countermeasures.html

[8] A security framework for mobile agent systems, omer mansoor paracha. Dissertation.com, Boca Raton, Florida.USA-2009

[9] State of the Art of Mobile Agent Computing, Security, Fault Tolerance, and Transaction Support Stefan Pleisch * IBM Research Zurich Research Laboratory 8803 R□uschlikon Switzerland

[10] Authentication for Mobile Agents ?, S. Berkovits??, J. D. Guttman, and V. Swarup fshim,guttman,swarupg@mitre.org The MITRE Corporation 202 Burlington Road Bedford, MA 01730-1420

[11] C. G. Harrison, D. M. Chess, and A. Kershenbaum. Mobile agents: Are they a good idea? Technical report, IBM Research Report, IBM Research Division, T.J. Watson Research Center, Yorktown Heights, NY, March 1995. http:// www.research.ibm.com/massive.

[12] C. Thirunavukkarasu, T. Finin, and J. May_eld. Secret agents | a security architecture for KQML. In CIKM Workshop on Intelligent Information Agents, Baltimore, December 1995.

[13] [13] C. Kaufman, R. Perlman, and M. Speciner. Network Security: Private Communication in a Public World. Prentice Hall, 1995.

[14] Biometric Features for Mobile Agents Ownership, Salvatore Vitabile, Giovanni Pilato, Vincenzo Conti, Giuseppe Gioè, and Filippo Sorbello

[15] Research on Mobile Agent-based E-Commerce System Framework Wenna Liu1, Deli Yang2, School of Management, Dalian University of Technology, Dalian 116024, Chinawenal@sina.com, somdyang@dlut.edu.cn

[16] Mobile agents for e-commerce, By Rahul Jha , Guided By Prof. Sridhar Iyer

[17] Danny B. Lange, "Mobile Objects and Mobile Agents: The Future of Distributed Computing", In Proceedings of The European Conference on Object-Oriented Programming '98, 1998.

[18] Alfonso Fuggetta, Gian Pietro Picco and Giovanni Vigna , "Understanding Code Mobility ", IEEE Transactions on Software Engineering , vol. 24(5), 1998.

[19] G. Glass, "ObjectSpace Voyager Core Package Technical Overview ", Mobility: process, computers and agents , Addison-Wesley, Feb. 1999.

[20] Fritz Hohl. Time Limited Blackbox Security: Protecting Mobile Agents from Malicious Hosts. G. Vinga (Ed.), Mobile Agents and Security, pages 92-112, Springer-Verlag, Lecture Notes in Computer Science No. 1419, 1998.

[21] R. Oppliger. Security Issues Related to Mobile Code and Agent-Based Systems. Computer Communications 22 pages 1165-1170, 1999.

[22] Tomas Sander and Christan F. Tschudin. Protecting Mobile Agents Against Malicious Hosts. Mobile agents and security, volume 1419 of Lecture Notes in Computer Science, pages 44--60. Springer-Verlag, New York, NY, 1998.

[23] J. Riordan and B. Schneier. Environmental key generation towards clueless agents. Mobile agents and security 19, 1998. http://citeseer.ist.psu.edu/639981.html

[24] Security Mechanisms for Using Mobile Agents in Electronic Commerce, Paulo Jorge Marques, Luís Moura Silva, João Gabriel Silva, Departamento de Engenharia Informática, Universidade de Coimbra, Portugal{pmarques, luis, jgabriel}@dei.uc.pt.

Biography

Swati Aggarwal is Assistant Professor in Department of Computer Application, IMS Engineering College Ghaziabad, U.P., India. She has been working in the fields of mobile agents and other related fields. She has published various research papers on Mobile Agents and Multi Agent Systems in National, International Conferences and in many refereed journal. She can be contacted on this email – aagarwalswati37@gmail.com.

ISSN: 2319 – 8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 1, Issue 2, December 2012

Suyash Bhardwaj is Assistant Professor in Department of Computer Science & Engineering, Faculty of Engineering and Technology, Gurukul Kangri University, Haridwar, Uttarakhand. He has been working in the fields of search engines, mobile Adhoc networks and other related fields. He has published various articles on wireless Adhoc networks and its applications in National, International Conferences and in journals of repute. He can be contacted on this email - suyash.bhardwaj@gmail.com.