International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-1, Issue-6, January 2013

Problems in Mobile Agent System Security

Arihant Khicha

Abstract- In spite of its many practical profit, mobile agent technology results in significant new security threats from both malicious agents and hosts. In this paper we explore the approaches and problems of mobile agent system, which shows that layered security and bi-directional model, may be a good initiative to resolve the security problems in mobile agent systems. Other topics about mobile agent security, such as virus detection and constrained execution are also discussed.

Keywords Mobile agents, Security, Bi-directional Security mechanism, layered security mechanism.

I. INTRODUCTION

In the last few years, The Internet, and in particular its most prominent offspring, the WWW, has become highly accepted. The Internet has considerably changed the manner in which we discover, view, obtain, and utilize information. Once little more than a playground for academic users and an infrastructure for electronic mail and, the Internet has widely become a imperative site for commercial enterprises, which enhances the fast growth of mobile agent technology. Mobile agents are processes that can autonomously migrate from one networked computer to another while executing. It can execute across networks in behavior of users. Mobile agents can be useful for many applications, especially in Internet [1].

Even though it has many practical benefits, mobile agent technology fallout in major new security threats from both malicious agents and hosts. For examples, as a mobile agent traverses multiple hosts that are trusted to different degrees, its state may be changed in a way that badly impacts its functionality. A number of serious security problems can develop in the world of mobile agents, where a site can offer services not only to its local users but also to remote users,. Many research works have been done about these problems, but most of which are under specific systems and environments and pay more attention to one aspect while ignoring the others [2]. In this paper we will give an overall approaches and discussion about the security problems in mobile agent system. In section 2, we talk about the security problems and their rough approaches in single computer, network and mobile agent system. Specific mechanisms to security problems from both the host and the mobile agent are discussed in section 3. Section 4 shows that there are a number of layers at which security mechanisms can be placed. In section 5 other topics about mobile agent security, such as virus detection and constrained execution are discussed. Section 6 cover conclusion.

Revised Manuscript Received on 30 January 2013.
* Correspondence Author
Mr.Arihant Khicha*, Ph.d Scholar, Nims University,Shobha Nagar, Jaipur,India.

II. SECURITY IN DIFFERENT ENVIRONMENTS

Any discussion of computer security essentially starts from a statement of requirements, i.e. what is really means to call a computer system "secure". In general, secure systems will control access to information such that only properly authorized users (or processes on behavior of users, such as agents) will have access to read, write, create, or delete information. Different environments have drastically different ideas of what security means to them.

A. Single Computer Security

Computer security seemed easy to manage in conventional computer systems. If you limited who could log in your system to people whom you trusted, you were 99% done. Once inside the system, each user could be controlled in their ability to read and write files on the system. They could be billed for their usage of disk space and CPU cycles. These can be done by the operating system, such as UNIX. There are four main aspects of computer security in single computer system: audit ability, secrecy, integrity and protection from theft of service [3].

B. Network Security

When organizations evolve from having central mainframes to computer networks and these networks are eventually linked to the Internet, the rules begin to change. To safely connect a corporate network to the Internet, an organization would set up firewall between the inside and outside. Firewall would hopefully not hamper internal people trying to get their job done, yet would restrict external malcontents. While a number of different techniques exist for building firewalls, they all work basically by blocking external attempts to connect to all internal machines. Firewalls generally allow internal machines to make connections outside, but external machines are generally allowed to connect only to a small number of carefully chosen internal machines.

The information might be stolen by a malicious third party if this secure information travel over an insecure network, such as Internet. This is an issue when a consumer wishes to buy goods from an online store. Cryptography is involved in almost all the current solutions, which encrypts sensitive data before it goes on the network and when it arrives to its destination it is in decrypted form. If the cryptographic protocol (for example, RSA) is well implemented, an attacker will be required to do an enormous computation in order to learn even a single bit of the encrypted message. When properly used, firewalls and cryptography have great potential to reduce the network security problem, even to be no worse than the conventional security problem. Of course, the security mechanisms under single-computer environment are still useful.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

C. Mobile Agent Security

The firewall model is reasonably a success. But it is based on such an assumption: it assumes that all the programs running inside the network are acting only on the requests of internal users. Of course, no internal users would unintentionally leak a sensitive company document to the open Internet. The company must let their employees download arbitrary files from the network for the sake of business. There is clearly no danger at all if files are plain ASCII text. But with the Internet, users are not just getting their documents and email in plain text. Instead, documents are programs themselves or contain programs within themselves. Such documents have "active content" like "applets", "plugins".

These active contents are frequently called mobile code. These mobile codes become mobile agents when they move continuously and autonomously. The downloaded documents violate the assumptions made by firewalls, which could assume that an attacker could only from the outside. Now, an attack might originate just from the inside with mobile agents, (because the mobile agents have moved into the inside), where no protection is offered by a firewall at all.

These mobile agents can arrive as attachments or directly to email or to Web pages. Mobile agent can reinstall itself and begin running. While running, they act as if they were the users and attack the intranet. Under such circumstance, cryptography offers little help with mobile agent. By using digital signatures, cryptography can be used to certify the origin of mobile agent, and provide guarantees that the agent received was not tampered with in transit. Cryptography can make no guarantees about what the agent might do when executed. In order to properly protect the users and their networks against attacks from malicious mobile agent, either all mobile code (therefore mobile agents) supports must be turned off, or the users' platforms must maintain adequate safeguards to control the actions of mobile agent. Turning off mobile agent will disable a lot of useful functionality necessary to some services, which means this is by no mean a solution. So we must seek adequate mechanisms to sense and control the transit and action of mobile agent.

Bi-directional and layered security mechanisms given in the next two sections may be a good idea to resolve the security problems in mobile agent systems. They control the security problems faced by mobile agents in horizontal and vertical direction respectively.

III. BI-DIRECTIONAL SECURITY MECHANISMS

The security threats in mobile agent systems come from both malicious agents and the hosts for agents to migrate to. On one hand, malicious mobile agents may access and modify data to which they should not have access and interfere with the execution of other agents. On the other hand, malicious hosts may cheat the mobile agents migrating to them and therefore interfere with the successful execution of the mobile agents. So the mechanisms to control them should take effort from both the host and the mobile agent, which means that bi-directional security mechanism should be adopted.

A. Host's security mechanism

To help ensure that an agent is suitable for execution, the host site can employ a number of security methods as followings.

Authentication involves checking that the agent was sent from a trustworthy site. This can involve asking for the authentication details to be sent from the site where the mobile agent was launched or the site from which the agent last migrated. A mobile agent that fails authentication can be rejected from the site or can be allowed to execute as an anonymous agent within a very restricted environment. Verification entails checking the code of a mobile agent to ensure that it does not perform any prohibited actions. A technique called proof-carrying code [4] allows a host site to determine whether code from a trustless site is safe to execute. This works by attaching a safety proof to each piece of code to be transferred. From this, the host site can quickly validate this proof and thus ensure that the code is safe to execute. Tampering with either the proof or the code will result in an invalid verification.

However, some code cannot be verified until it is executed such as the contents of variables used as a parameter of a function. For this reason, verification normally checks to ensure that the agent does not try to corrupt its execution environment. The mobile agent system in which the agent actually executes is responsible for managing the agent while it runs. The agent should not be able to perform any operations outside of its authorization and resource constraints. Authorization determines the mobile agent's access permissions to the host resources. This indicates that how many times a resource can be accessed or how much of a resource can be used, and what type of access the agent can perform. For example, a highly trusted agent may be able to read, write and modify a given resource and have unlimited access to it. On the other hand, an untrusted mobile agent may only be able to read the resource and access it a limited number of times. Authorization mainly deals with the runtime actions of mobile agent. Payment for services determines the mobile agent's ability or willingness to pay for services (unless they are free). This includes ensuring that a mobile agent can actually pay, that payment is effected correctly and that the service paid for is satisfactory to the payee. Since the agent is consuming at least computational resources at the server, and may in fact be performing transactions for goods, its liability must be limited. This can also be done by the mechanism of payment for services. In the case of General Magic's agent [5], the Telescript language provides a method whereby the agent carries with it a quantity of an electric currency. During execution of the agent by the host, some currency is transferred from agent to the host as a form of payment.

The amount of currency transferred is decided by the quantity and quality of services provided by the host. The agent's ability is limited to the quantity of currency. The agent which exhausts its currency is killed. However, the agent also requires that the host cannot fake the quantity of currency transferred and that the host is indeed providing the contracted services.

B. Security Mechanism of Mobile Agent Itself

Host security is relatively easy to deal with to greater or lesser degrees by employing the four mechanisms given above. However, there is also agent security to consider, namely, how to protect a mobile agent which is in transit or is executing on a remote site.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Again, there are a number of security techniques agent or a mobile agent system can use. Authentication is also used here to check the validation of host the mobile agent migrates to. Encryption algorithms such as Pretty Good Privacy (PGP) and others can help to protect mobile agents from having their contents inspected during travel. Digital signatures are used to identify messages such that the receiver can not possibly have concocted the message, the result can be sent back to the exact sender. There are two encryption algorithms that are often used: secure key and public key. Secure key encryption algorithm, also called single key method, is a kind of relatively older and simpler encryption algorithm.

In this encryption algorithm, a common secure key used for encrypting/decrypting is shared by both sender and receiver. DES is the typical algorithm of secure-key encryption methods. Public-key encryption algorithm is younger, but more complicated, and suitable to resolve the security problems in open system, such as Internet. This algorithm needn't exchange key at first. Two particular keys are created by both parties create one public and the other secure. Sender encrypts the data using the public key of receiver, while receiver decrypts the very data using the secure key of it own. RSA is the typical algorithm of public key encryption methods. It is clear that

RSA is more suitable for mobile agents which run in an open environment. But the amount of computation is too large if all the data transferred are encrypted using RSA. An algorithm called PGP is suitable in such circumstance. PGP is a kind of hybrid algorithm which includes a symmetrical encryption algorithm called IDEA, a non-symmetrical encryption algorithm called RSA, a single direction hash algorithm called MD5 which is used for the production of information abstract. User can use ZIP to compress the data before it is encrypted. IDEA is fast and is used to encrypt the data, while RSA has the property of high security but great complexity and is used to encrypt just the secure key used by IDEA. PGP is of high efficiency to mobile agent due to its high reliability.

IV. LAYERED SECURITY MECHANISMS

Providing a secure environment in which agents can take advantage of services and fulfill requests is a difficult task to achieve because of the varying functionality requirements and the varied nature of the underlying networked operating systems. Security mechanisms can be placed on a number of layers. However, the heterogeneity of security policies and mechanisms across networked operating systems makes them difficult to translate between. Some research works on operating system support for mobile agent and its security have been done, for example, TACOMA [6], The TACOMA project (Tromso And COrnell Moving Agents) has focused on operating system support for mobile agent and its security, and how agents can be used to solve problems conventionally addressed by operating systems.

Mobile agent systems tend to provide security features that are explicit to mobile agents but independent of any particular networked operating system. In general, while many mobile agent systems support constrained execution, code verification, and authentication, their user security model still needs to be enhanced. The security mechanisms on this layer mainly deal with the host security problems, but also provide some fundamental methods for the security mechanisms of mobile agents. Most current research works about the security of mobile agent (system) meet to this layer.

The Mobile Agent Facility outline proposal tries to make provision for security and other services independently of a networked operating system by defining a Common Conceptual Model (CCM) [7]. The realization of the security aspect of the CCM is through the adoption of CORBA security services, such as client authentication for the creation of new remote agents, mutual authentication between agent systems and specific security policies. However, it is made clear in the outline proposal that CORBA security does not meet all of the requirements for mobile agent security, for example there is no procedure for validating code before it is executed remotely. Mobile agent should protect it safely; this is the task on this layer. Self-validation Encryption algorithms and the like can be used to ensure that the mobile agent and its data do not become compromised.

V. OTHER TOPICS ABOUT MOBILE AGENT'S SECURITY

A. Constrained Execution

Mobile agents may control resources in the host computer, avoid paying for general public services, security may be necessary but less of importance. Security is a very large issue that is not easy to solve in the general case, and contrary to critics, it is not purely the problem of mobile agent systems since downloading Java applets can also pose as much of a threat. As the Internet is still maturing, new techniques are being developed to provide better security mechanisms at both directions. It is more than likely that these measures will be built into mobile agent systems as they become available.

REFERENCES

1. A. Lingnau, O. Drobnik et al. An Infrastructure for Mobile Agents: Requirements and Architecture. 1995.
2. William M. Farmer, Joshua D. Guttmann, and Vipin Swarup. Security for mobile agents: Issues and requirements. In Proceedings of the 19th National Information Systems Security Conference, pages 591-597, Baltimore, Md., October 1996.
3. Dan S. Wallach. A new approach to mobile code security. Ph.D. thesis, Department of Computer Science, University of Princeton, Jan. 1999.
4. Jonathan Dale. A Mobile Agent Architecture for Distributed Information Management. Ph.D. thesis, University of Southampton, Sep. 1997.
5. Joseph Tardo and Luis Valenta. Mobile agent security and Telescript. In Proceedings of IEEE COMPCON '96, Feb. 1996.
6. Dag Johansen, Robbert van Renesse, and Fred B. Schneider: Operating system support for mobile agents. In Proceedings of the 5th IEEE Workshop on Hot Topics in Operating Systems, pages 42-45, Orcas Island, Wash., May 1994.
7. Object Management Group, Mobile Agent Facility Specification Draft Version 7 (Joint Submission).OMG Common Facilities Request for Proposal 3, Jun. 1997.
8. Colin G. Harrison, David M. Chess. Mobile agents: Are they a good idea? IBM Research Report, IBM Research Division, IBM, Mar. 1995.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)