Security: important issue in e-commerce

AHMADI-BROOGHANI, ZAHRA
Computer Engineering Department
The University of Birjand
Birjand, Iran
IRAN

Abstract: - In the rapidly expanding field of E-Commerce, mobile agent is the emerging technology that addresses the requirement of intelligent filtering/processing of information. E-Commerce or electronic commerce is born along with the Internet. In this application, security is crucial since we can consider that any application will not be useful without doing secure transactions.
This paper is consisted of two sections: the first section some definitions like e-commerce, mobile agents which are special types of agents have been presented and the second section begins with the main security issues related to the mobile agent paradigm, and techniques for keeping the mobile agent platform and the agent itself secure against each other

Key-Words: - Mobile Agents; E-commerce; Security; Distributed Environments.

1 Introduction

Mobile Agent Systems are expected to make e-commerce transactions inside virtual supermarkets. In this application, security is crucial since we can consider that any application will not be useful without doing secure transactions. Mobile agents consist of code state, data state, and execution state. Mobile agent systems are platforms that allow agents to migrate from one node (a mobile agent system) to another, keeping its three states. While agents migrate there are several security aspects involved. We can point out different mechanisms that must be implemented by the mobile agent system to ensure the security of the mobile agent applications. Mobile agent systems basically must provide:

• Protection of the agent system against attacks from mobile agents.
• Protection of the agent against other agents.
• Protection of information transmission between agent servers against unauthorized third parties.
• Protection of the agent against malicious agent systems (malicious hosts), which includes protection of the data state of the agent.

2 E-Commerce Definition

E-Commerce (electronic commerce) is the buying and selling of goods and services on the Internet, especially the World Wide Web. E-commerce refers to all forms of business activities conducted across the internet. This can include E-tailing, B2B, intranets and extranets, online advertising, and simply online presences of any form that are used for some type of communication (customer service for example).
The definition given by Kalakota and Whinston [1] is:

_From a communications perspective, EC is the delivery of information, products/services, or payments via telephone lines, computer networks, or any other means.
_From a business process perspective, EC is the application of technology toward the automation of business transactions and workflow.
_From a service perspective, EC is a tool that addresses the desire of firms, consumers, and management to cut service costs while improving the quality of goods and increasing the speed of service delivery.
_From an online perspective, EC provides the capability of buying and selling products and information on the Internet and other online services.

2.1 Role of Mobile Agents in E-commerce

Mobile agents can be viewed as a combination product of software agent technology and distributed computing technology. It differs substantially from the traditional network computing model. That is because mobile agents can move continuously from one node to another, and travels based on its own needs and choices.

Mobile agents can move in between the client and the server bi-directionally.

Even though the architectures of mobile agent systems differ, almost all mobile agent systems contain a Mobile Agent (MA) and a Mobile Agent Environment (MAE).

MAE creates a secure and appropriate execution environment for MA. In general, MAE should comprise the following basic services:

- *Business service*: Performs mobile agent creation, migration, and endurance and execution environment distribution.
- *Event service*: Implements agent transfer protocol and communication protocol and supports events transmission among agents.
- *Directory service:* Maintains status information about the location of a mobile agents and a message router that uses the directory service to deliver messages to a mobile agents.
- *Security service:* Provides a safe execution environment.
- *Application Service:* Provides service interface for specific tasks.

Agent Transfer Protocol (ATP) is employed in MAE for the migration of MAs among computers, and provides the execution environment and service interface. Agent Communication Language (ACL) is exploited by MA in MAE to communicate with various services provided by MAE [2].

Mobile agents have distributed characteristics. In the mobile agent computing model, the computing process and the corresponding states of the receiving computer represent completely all the requests from sender, therefore, the reliability of network is no longer that important because:

- Mobile agents doesn't require a lot of bandwidth, only what's needed during migration.
- Mobile agents continues to execute after migration, even if the connection to the initiator is lost.

Therefore, if a client needs a lot of communications with a specific server in the network, the best way to achieve it is to employ mobile agent system. An agent can travel autonomously to a remote server, execute the computation and return to the client

The deployment of mobile software agents has been studied in applications such as networked electronic trading [3], the tracking of products [4], mediation of negotiation [5], personal assistance, distributed information search and retrieval, monitoring, network management [6], real-time control, building middleware services, military command and control [7], and parallel processing, and the MA paradigm can be used to test E-commerce environments as well as examine electronic market behaviors [8].

2.2 Mobile agent framework requirements

Software agents play the role of human supervisor, who is in charge of the tracking, monitoring and problem management of specific product item. The mobile agent system can be considered as a Support System for this human manager. The agents are programmed to perform the monitoring task, and also handle exceptions. The agent takes care of routine task, including negotiations, and involves the human decision maker in more complicated or unforeseen situations. Therefore it is necessary to provide a suitable infrastructure for controlling a production process in a E-commerce environments. A mobile agent framework has to satisfy a number of properties to provide a suitable infrastructure [9]. It has to provide in general services, such as:

- An interaction model, specifying both the agent-agent (including the agent communication language) and the agent-system aspect;
- A suitable level of intelligence, allowing the agent to carry out its intended task. Depending on the task requirements an agent may need to gather information, make choices and even collaborate with other agents;
- Generic services, the extent of which has a direct impact on the size of the agents. Generic services include directory, trading, and reasoning services;
- Resource management, that provides for controlled creation, usage and destruction of the agents;
- Recovery management, that determines which exceptions can be handled by the agent system (such as those arising from local crashes and migration failures);
- A security model, which states the threats that are dealt with by measures, such as the security protocol and authentication services [10].

3 Security issues in mobile agent

Mobile agents consist of code state, data state, and execution state. Different security architectures for mobile agents and mobile agent systems [11] have used standard cryptographic techniques like public key Cryptography, or digital signatures to authenticate authorities and solve the problem of

protecting the host against malicious agents. Also, they have implemented secure channels for the transmission of the agents by using SSL or TLS [11].

The code state of the agent can be signed since it will not be modifiable. In this way, we can protect the static part of the agent. However, to protect the data state (that changes dynamically) becomes a more difficult task to tackle. In data security, the common topics are related to encrypting methods, such as private or public key cryptography. Moreover, secure sockets layer (SSL) secure electronic transactions (SET) and cookies are other popular technologies available to help protect privacy and security online. Individual security can include passwords or digital signatures. In addition, firewalls, proxy servers, and virtual private networking can ensure system security for protecting the network against external and internal attacks, such as hackers. Therefore, these technologies can prevent loss of data in order to preserve internal and external services [12].

Mobile agent technology has some limitations, primarily in the area of security. The research efforts in the area of mobile agent security adopt two different points of view. Firstly, from the platform perspective, we need to protect the host from malicious mobile agents such as viruses and Trojan horses that are visiting it and consuming its resources. Secondly, from the mobile agent point of view, we need to protect the agent from malicious hosts.

Because of the most valuable characteristics (mobility), mobile agents are exposed to different types of attacks. They are: unauthorized Access**,** masquerading, denial of Service, annoyance attack, eavesdropping, alteration [13, 6]. The different security requirements that the mobile agent paradigm needs to satisfy are: confidentiality, integrity, availability, accountability, anonymity [6]. The techniques for protecting agents and platforms fall into two categories: Prevention and detection. Prevention techniques are aimed at making it impossible for platforms and agents to successfully perform an attack. The term "prevention mechanism" is often used to denote a technique that makes it impossible to modify an agent in a meaningful way [14]. Examples of such techniques include "Environmental Key Generation" and "Computing with Encrypted Functions". On the other hand, detection techniques aim at detecting the attacks. The "Co-Operating Agents" technique and "Execution Tracing" belong to this category.

3.1 Security of platforms

The primary issue in the security of mobile agent systems is to protect mobile agent platforms against malicious attacks launched by the agents.

This section presents a set of detection and prevention techniques for keeping the platform secure against a malicious mobile agent.

Sandboxing [15] is a software technique used to protect mobile agent platform from malicious mobile agents. The most common implementation of Sandboxing is in the Java interpreter. A Java interpreter contains three main security components: Class Loader, Verifier, and Security Manager [16].

The "*Code Signing*" technique ensures the integrity of the code downloaded from the Internet. It enables the platform to verify that the code has not been modified since it was signed by its creator. Code Signing cannot reveal what the code can do or guarantee that the code is in fact safe to run [17, 18].

Code Signing and Sandboxing Combined: Java JDK 1.1 combines the advantages of both Code Signing and Sandboxing. In Ref [19, 20] the main advantage of this approach is that it enables the execution of the mobile code produced by untrustworthy entities.

Proof-Carrying Code: Lee and Necula [21] introduced the *Proof-Carrying Code* (PCC) technique in which the code producer is required to provide a formal proof that the code complies with the security policy of the code consumer.

Farmer et al [22] introduced the "*State Appraisa*l" technique to ensure that an agent has not become malicious or modified as a result of its state alterations at an untrustworthy platform.

Path Histories: using this history, the platform makes the decision whether to run the agent and what level of trust, services, resources and privileges should be granted to the agent [6,14,23].

3.2 Security of mobile agents

Mobile agents themselves are exposed to various threats by the platforms they visit. This section presents a set of detection and prevention techniques for keeping the mobile agent secure against the attacks that are launched by the malicious platforms.

Co-Operating Agents: the co-operating agents share the same data and exchange information in a secret way. Co-Operating Agents can be used to perform e-commerce tasks or protocols such as the

authorization of negotiation, bidding, auction, electronic payment, etc [24, 25].

Execution Tracing: this technique is based on cryptographic traces that are collected during an agent's execution at different platforms. Execution Tracing also provides a means to protect a legitimate platform against a malicious agent by obtaining the related traces from the involved parties. A version of the Execution Tracing technique, proposed by Tan and Moreau [26, 27].

Riordan and Schneier [28] designed the *Environmental Key Generation* technique to be used when a platform wants to communicate with another platform by sending it a message.

Non-Interactive Computing with Encrypted Functions: this technique represents a software solution for protecting a mobile agent from a malicious executing platform during its itinerary.

Obfuscation is a technique in which the mobile code producer enforces the security policy by applying a behavior-preserving transformation to the code before it sends it to run on different platforms that are trusted to various degrees [29].

There are different useful obfuscating transformations [30,31,32].

Partial Result Encapsulation (PRE) is a detection technique that aims to discover any possible security breaches on an agent during its execution at different platforms. The agent uses a special implementation of encryption called "Sliding Encryption" that was suggested by Young and Yung [33]. Sliding Encryption is particularly suitable for certain application where storage space is valuable such as smartcards [34].

4 Conclusion

The mobile agent system is a very promising paradigm that has already established its presence in many applications including e-commerce and distributed information search and retrieval. At the same time, this technology has introduced some very serious security problems. SAFE is designed as a secure agent architecture for e-commerce. The foundation of SAFE is the agent transport protocol, which provides intelligent agents with roaming capability without compromising security. General security concerns as well as security concerns raised by agent transport have been carefully addressed [35]. SAFER, architecture is being proposed to extend the SAFE architecture. In SAFER, agents not only have roaming capability, but can make electronic payments and can evolve to perform better [35]. In Ref [36] proposed the use of Secure Agent Data Integrity Shield (SADIS) as a scheme that protects the integrity of data collected during agent roaming. With the use of a key seed negotiation protocol and integrity protection protocol, SADIS protects the secrecy as well as the integrity of agent data. Any illegal data modification, deletion, or insertion can be detected either by the subsequent host or the agent butler.

In this paper we surveyed the main issues in the security of mobile agents. We considered both the mobile agent and the agent platform points of view, and presented the most important techniques for providing security in mobile agent systems. In any case, more research is needed in order to warrant sufficient trust in mobile agent technology by a wide range of users.

References:

[1] R. Kalakota, A.B. Whinston, Electronic Commerce: A Manager's Guide, Addison-Wesley, Reading, MA, 1997.

[2] E.W.T. Ngai*, F.K.T. Wat, A literature review and classification of electronic commerce research, Information & Management 39 (2002) 415–429.

[3] P. Dasgupta, N. Narasimhan, L.E. Moser, P.M. Melliar-Smith, Mobile agents for networked electronic trading, IEEE Transaction on Knowledge and Data Engineering 11 (4) (1999) 509-525.

[4] N.B.Szirbic, D.k.Hammer, J.B.M.Goossenaert, A.T.M.Aerts, Mobile agent support for tracking products in virtual enterprises in: Proceeding of the AGENTS'99 Conference, (1999) 93-100.

[5] N.B.Szirbic, J.C.Wortmann, D.k.Hammer, J.B.M.Goossenaert, A.T.M.Aerts, Mediating negotiations in a virtual enterprise via mobile agents in: Proceeding of the AIWORC'2000 on Mobile Technologies and Virtual Enterprises, Buffalo, USA, 2000.

[6] W. Jansen and T. Karygiannis, "Mobile Agent Security," NIST Special Publication 800-19, National Institute of Standard and Technology, 2000.

[7] S. McGrath, D. Chacón, and K. Whitebread, "Intelligent Mobile Agents in Military Command and Control," Advanced Technology Laboratories, New Jersey.

[8] R. Martens, R .Paranjape, L. Benedicenti, S. Sankaran, A. Sadanand, Mobile agent strategies for the provision of public goods: An experimental study, Electronic Commerce Research and Applications 5 (2006) 140–146.

[9] D.k.Hammer, A.T.M.Aerts, M. Dalmeijer, Mobile agent architectures: what are the design

issues, in: Proceedings of the international Conference on ECBS, Jerusalem, Israel, March 1998.
[10] A.T.M.Aerts, N.B.Szirbic, J.B.M.Goossenaert, A flexible, agent-based ICT architecture for virtual enterprises, Computer in Industry 49 (2002) 311-327.
[11] Jesus Arturo Perez Diaz, Dario Alvarez Gutierrez, A Fast Data Protection Technique for Mobile Agents to Avoid Attacks in Malicious Hosts,URL: http://www.elsevier.nl/locate/entcs/volume30.html 12 pages.
[12] E.W.T. Ngai*, F.K.T. Wa, A literature review and classification of electronic commerce research, Information & Management 39 (2002) 415–429.
[13] N. Karnik, "Security in Mobile Agent systems," Ph.D. Dissertation, Department of Computer Science, University of Minnesota, Oct. 1998.
[14] D. Chess, B. Grosof, C. Harrison, D. Levine, C. Parris and G. Tsudik, "Itinerant Agents for Mobile Computing," Technical Report, Oct. 1995, IBM T.J. Watson Research Center, NY.
[15] R. Wahbe, S. Lucco, T. E. Anderson, S. L. Graham, "Efficient software-based fault isolation," In Proceedings of the 14th ACM Symposium on Operating Systems Principles, (Dec. 1993) 203-216.
[16] L. Gong, M. Mueller, H. Prafullchandra, and R. Schemers, "Going Beyond the Sandbox: An Overview of the New Security Architecture in the Java Development Kit 1.2," In Proceedings of the USENIX Symposium on Internet Technologies and Systems, Monterey, California, Dec. 1997.
[17] "Signed Code," (n.d.). Retrieved December 15, 2003, from James Madison University, IT Technical Services Web site: http://www.jmu.edu/computing/infosecurity/ engineering/issues/signedcode.shtml
[18] "Introduction to Code Signing," (n.d.). Retrieved December 15, 2003, from Microsoft Corporation, Microsoft Developer Network (MSDN) Web site: http://msdn.microsoft.com /library/default.asp?url=/workshop/security/authce/ intro_authenticode.asp
[19] M. Dageforde. (n.d.). "Security Features Overview," Retrieved December 21, 2003, from Sun Microsystems, Inc. The JavaTM Tutorial Web site: http://java.sun.com/docs/books/tutorial/security1.2 /overview/
[20] S. Loureiro, R. Molva, and Y. Roudier, "Mobile Code Security," Institute Eurecom, 2001.
[21] P. Lee and G. Necula, "Research on Proof-Carrying Code on Mobile-Code Security," In Proceedings of the Workshop on Foundations of Mobile Code Security, 1997.
[22] W. M. Farmer, J. D. Guttman, and V. Swarup, "Security for mobile agents: Authentication and state appraisal," In Proceedings of the European Symposium on Research in Computer Security (ESORICS), Sep. 1996, 118-130.
[23] J. J. Ordille, "When Agents Roam, who Can You Trust?," Proceedings of the First Conference on Emerging Technologies and Applications in Communications, Portland, Oregon, May 1996.
[24] V. Roth, "Mutual protection of cooperating agents," In Secure Internet Programming: Security Issues for Mobile and Distributed Objects. J. Vitek and C. Jensen (Eds.), Springer Verlag, 1999.
[25] Y. Ye and X. Yi, "Coalition Signature Scheme in Multi-agent Systems," 2002.
[26] H. K. Tan and L. Moreau, "Extending Execution Tracing for Mobile Code Security," In K. Fischer and D. Hutter (Eds.), Proceedings of Second International Workshop on Security of Mobile MultiAgent Systems (SEMAS'2002), Bologna, Italy (2002) 51-59.
[27] H. K. Tan, L. Moreau, D. Cruickshank, and D. De Roure, "Certificates for Mobile Code Security," In Proceedings of The 17th ACM Symposium on Applied Computing (SAC'2002) Track on Agents, Interactions, Mobility and Systems, (2002) 76.
[28] J. Riordan, B. Schneier, "Environmental Key Generation Towards Clueless Agents," G. Vinga (Ed.), Mobile Agents and Security, Springer Verlag, Lecture Notes in Computer Science No. 1419, 1998.
[29] L. D'Anna, B. Matt, A. Reisse, T. Van Vleck, S. Schwab, and P. LeBlanc, "Self- Protecting Mobile Agents Obfuscation Report," Report #03-015, Network Associates Laboratories, June 2003.
[30] G. Wroblewski, "General Method of Program Code Obfuscation," PhD Dissertation, Wroclaw University of Technology, Institute of Engineering Cybernetics, 2002.
[31] G. Hachez, "A Comparative Study of Software Protection Tools Suited for Ecommerce with Contributions to Software Watermarking and Smart Cards," University Catholique de Lou vain, 2003.
[32] C. Collberg, C. Thomborson, and D. Low, "A taxonomy of obfuscating transformations," Technical Report 148, Department of Computer Science, University of Auckland, July 1997.
[33] A. Young and M. Yung, "Encryption Tools for Mobile Agents: Sliding Encryption," In: E. BIHAM (ed), Fast Software Encryption. Lecture

Notes in Computer Science, no. 1267. Springer-Verlag, Germany, 1997.
[34] G. Karjoth and J. Posegga, "Mobile Agents and Telcos' Nightmares," *Annales des Télécommunications* Vol. 55, No. 7/8, 2000, 29-41.
[35] Sheng-Uei Guan, Yang Yang, SAFE: secure agent roaming for e-commerce, Computer & Industrial Engineering 42 (2002) 481-493.
[36] Sheng-Uei Guan, Yang Yang, Secure agent data integrity shield, Electronic Commerce Research and Applications 3 (2004) 311–326