Proceedings of the 4th WSEAS Int. Conf. on Information Security, Communications and Computers, Tenerife, Spain, December 16-18, 2005 (pp1-6)

Security & Trust in Agent-enabled E-commerce: Survey

HAIDER ALI
Department of Computer Science
University of Lueneburg
Lueneburg
GERMANY

Abstract

This contribution deals with the problem of security in E-commerce and its agent-based solutions. Agent technology is relatively a trusted approach for E-commerce solutions. It provides a secure alternative to conventional approaches for the development of agent based E-commerce applications. The computer security issues and related threats discussed in this contribution directly effect E-commerce business. The deployment of proper agent security frameworks is indispensable while developing an E-commerce application. A variety of such frameworks and Multiagent E-commerce solutions based on these frameworks with critical evaluation is presented.

Keywords: - Trust, Security Issues, Security Frameworks, Intelligent Agents, Multiagent Systems

Introduction

The objective of this survey paper is to discuss security threats and related trust issues in E-commerce and how agent technology can help in order to explain the different security threats and the possible corrective measures. This paper describes how people can trust e-business, which leads the reader to have a brief understanding of various security threats and related trust issues in E-commerce. This talk continues with discussing the capabilities of an agent, malicious agents, and agent-based E-commerce. Various agent security frameworks like Secured Floating Market Model (SFM), Secure and Open Mobile Agent (SOMA) and Service on Demand (SOD) are discussed. This section covers issues of trust in Multiagent Systems (MAS). A critical evaluation of various security issues in agent- enabled E-commerce applications is presented. Issues like authenticity provided by MAS to gain the trust of people are also discussed.

We finish this paper with some concluding remarks.

1. How people can trust E-commerce

Security plays a key role in the success or failure of E-commerce applications. Secure E-commerce applications diverted customer’s interest from traditional approach towards E-business. Many security issues arise in the form of different threats like access control violations, fraud, privacy violation and denial of service attacks. All these security threats enter into the category of cyber crimes. As a consequence of such threats customers trust in E-commerce is affected negatively.

E-marketing services (advertisements, banners and promotional popups) increase network traffic. These promotional activities do not really make any positive contribution to the business even if the seller is offering a valuable service along with the best quality and price of their products. In E-commerce it is very important to secure customers’ personal information and provide them with privacy in transactions using a proper transaction management system. E-business services aim at attracting new customers as well as maintaining and satisfying the needs of existing customers by providing them best quality services. Quality of service in products really matters to gain the confidence of customers. Trust in E-commerce has received a great deal of interest. [1]

Due to the open architecture of the Internet, it is very hard to maintain the trust while sharing the information on open electronic media. As stated by Bhimani, [5] the Internet was not designed as a commercial environment. It operated on a single domain of trust while provisions were made to allow remote users access to critical information on machines. Security generally relied on the user's mutual respect as well as considered appropriate knowledge on the network. This was reasonable when the number of users on the net was comparatively small. However with the phenomenal growth of the Internet and changes in the demographics of the users, the net is now a universal community, with users coming from all walks of life. According to the Cyber Source Corporation online fraudsters took $ 1.6 Billion out of 2003 E-commerce. Due to malicious attacks, the public opinion on security and trustworthiness of using the Internet for commerce has been towards an attitude of distrust. [6]

There can be variety of reasons for these kinds of threats, mainly because of the loss of security on client side, server side or on the network. To provide E-commerce (B2B or B2C) applications in multi culture operating systems environment, to make them available globally and to maintain possible security measures is a difficult task. Recent research on security issues focused on developing security applications for client, server, database, network as well as operating systems.

2.1 Security threats and trust issues in E-commerce

E-commerce security deals mainly with two types of issues; protect the business network and provide transaction security between the customer and business.

In B2C, transaction is one of the critical issues, which requires to be managed properly. As in online business, credit card information needs to be made secure and must be signed with the intelligent infrastructure services like VeriSign.

Marchany and Tront [2] advocate encryption techniques such as secret-key, public key and digital signatures as the most common method of ensuring transaction privacy, confidentiality and integrity. They concede that the common weakness of these techniques is that they depend on the security of the end point systems to protect the keys from modification or misuse.

Previously IBM as one of the major contributors to E-commerce security developed many encryption algorithms, which are very popular in network security systems. It is very important to figure out which systems must be accessible to which users and which users must have access to those systems at various locations. More over, it is important to decide which information needs to be encrypted over the wire. It really needs to be taken care of, when sensitive information is being transported over the network.

Firewalls help in securing the data and information with access to the specific authenticated users. These are hardware and software systems, which deal with specific users to have access to the systems and to perform specific tasks like email, web access etc. There are many security threats which work out over the firewall as well like Real Tunnel, SMTP Tunnel, "I Love You", Code Red, NIMDA and many more. [2]

Marchany and Tront state that most of the security attacks occur at server systems, as hackers were familiar with the fact that data resides on the servers, observed it. Due to the concept of distributed systems and replication servers, hackers need to change their focus to network systems. In order to secure and pass information to the authenticated users on network systems the cryptographic protocols and encryption algorithms like RC4 Encryption, DES Encryption, Triple DES Encryption, and Advance Encryption Standard etc are deployed.

There are two main threats to E-commerce clients and servers known as viruses and Trojans. Viruses mainly focus to threat client systems and they penetrate into to the client systems because the lack of built-in security. Trojans target the user communication across the networks and remotely monitor client systems. Trojans are considered as the greatest security threat in E-commerce as they bypass client authentication and access client transactions directly. [2]

3.1 What could an intelligent agent do?

Imagine a system in which when a customer lifts the handset of a telephone to dial a long distance phone call, an agent within the telephone automatically collects bids from various carriers and decides which carrier to use. The telephone companies have an agent that automatically declares the price per minute for which it is willing to carry the call. The agent in telephone decides which bid to accept, using an appropriate auction method (such as best bid wins and gets second best price).

Imagine a system in which when a person wants to place an international phone call to a customer who does not speak the same language, an agent automatically translates the conversation between the two languages [3]

3.2 Malicious agents

A malicious agent is a computer program that operates on behalf of a potential intruder to aid, attacking a system or network.

Historically, an arsenal of such agents consisted of viruses, worms, and trojanized programs. By combining key features of these agents, attackers are now able to create software that poses a serious threat even to organizations that fortify their network perimeter with firewalls.

As the result of such evolution, organizations may be faced with a remotely controlled worm that has the ability to infiltrate networks via open channels such as e-mail or Web browsing, can be controlled via outbound connections such as HTTP and FTP, which can pass through many firewalls, and has propagation capabilities that maximize its ability to perform an effective distributed attack [4]

3.3 Agent based E-commerce

In a new generation of E-commerce, agent based E-commerce is becoming an attractive paradigm. Software agents have demonstrated their tremendous potential in conducting various tasks in E-commerce such as comparison-shopping, payment, mediation, distribution, sales promotion, etc [7]

While talking about agent-enabled E-commerce, the first thing comes into our mind is how agents get involved to facilitate E-commerce. In the past few years along with the growth of E-commerce many security issues are being raised which draw organizations and E-commerce vendor's attention to provide agent mediated E-commerce applications. Trust is becoming main course of study in agent–enabled E-commerce. Some of the important areas in agent-enabled E-commerce include how to develop a trust between a user and an agent system. How to identify problems in terms of security, how to measure security issues and how to take preventive actions to provide secure E-commerce solutions

3.4 Agent security frameworks

There are many available security frameworks, which provide a secure architecture to design MAS for E-commerce.

Few years back few students from Shizuoka University Japan have analyzed different problems in agents like agent controllability, resource restriction and security etc and proposed a framework known as SFM model. SFM model provides agent controllability, resource restriction, location of resources and agents and also guarantees some suitable security strength levels of flexible execution of various services and user requirements [8]

Another mobile agent framework called SOMA was developed by University of Bologan, Italy, which was, implemented in Java 2 platform specifications. "It is a Java based mobile agent framework capable of answering the requirements of scalability, dynamicity, openness and security that are typical in internal scenario. It has been designed to achieve two main objectives: security and interoperability. It grants interpretability by closely considering compliance with CORBA and MASIF. "[9] SOMA also provides some additional services like User Virtual Environment (UVE), Mobile Virtual Terminal (MVT), and Virtual Resource Management (VRM), which would not be discussed in details because it is beyond the scope of this area. [10]

Another framework, which is specifically designed with the concept of SOD, is very popular in agent systems. This framework protects decentralized mobile agents with two layer cryptographic techniques. If any case of modification is being made in mobile agents they can be tracked down in next available service. [11]

There are many more available frameworks reported in the literature, which are designed to provide security in agent based E-commerce systems.

3.5 Trust in MAS

It is very difficult to judge if user has trust in agent-based systems. In agent enabled E-commerce trust is always being increased with success. Agent trust is one of the major issues undertaken by different researchers. How to develop an agent based system with security & trust. Agent developers are still in search of the security frame works, which can be used to develop a verifiable agent to communicate to the community with trust.

It is very important to make Human-agent and agent-agent communication through secure channels. Though cryptographic techniques are in use to secure communication between two parties, there still is a need to implement these techniques in different layers to secure the information and enable trust between two parties.

In cryptographic techniques there are two principles that follow a quite usual approach like ciphering/deciphering keys and robustness of the ciphering functions. [12]

In MAS it is very important to have such kind of environment where agents have trust in other agents as well as agents have to be honest with other agents and environment. In such a way agents can receive information from other agents and decide on the basis of received information whether the information are meaningful or fake. This brings trust in MAS. To enable agents to make such decisions Lam and Leung propose the Trust/Honest Model. This model covers three kinds of risks which are attitude, stubbornness, and the sincerity of agents. [13]

3.6 Agent systems for E-commerce

Different security and trust related issues bring the need of agent solutions as a part of E-commerce applications. On the basis of various architectures and security frameworks in order to solve security threats in E-commerce provide efficient agent-enabled E-commerce solutions. While talking about intelligent agents in E-commerce applications the first thing that comes into our minds is why it is needed to bring agent systems as a solution for E-commerce applications. Various factors like finding a product, finding buyers and sellers, secure transaction management, authorization and authenticity, information retrieval and infrastructure etc justify the application of intelligent agents in this field.

Many researchers have put lots of efforts in the area of artificial intelligence (AI) to provide various solutions of the complex problems of intelligent agents. Recent technological development in this area deals with the approach to provide more practical applications based on AI techniques. Modularity and abstraction are quite common ways to deal with complex problems. It is being observed that small functional components or service agents can be developed to solve complex problems and critical issues. In these components the main area, which needs to be carefully managed, is how they coordinate with each other. [14]

There are many agent-based systems developed for E-commerce. Few of them are being discussed in this paper like Kasbah, Tete-a-Tete, Bargain finder and MAGNET. These systems are working and facilitating buyers and sellers to bring them together on one marketplace.

MIT Media Laboratory implements both Kasbah and Tete-a-Tete with the target of price negotiation for buyers and sellers. It is very important to target the needs of buyers who want to buy goods from Internet and sellers who want to carry on their business. It is being observed that customers like to have negotiations on the price at E-business marketplaces. These systems can be evaluated on the basis of seller’s financial gain and buyer’s satisfaction. [15]

Anderson Consulting developed Bargain Finder. Initially the main focus was on the comparison of prices of Compact Disks from different dealers/retailers. Now it is extended to cover books, electronic games and hardware etc. Price is the only criterion defined for the system. As for the retailers price should be fixed and on the customer side it should be minimal. Bargain Finder looks at different available retailers list and their offers to fulfil buyer requirements. [16]

Multiagent Negotiation Testbed (MAGNET) is developed at the University of Minnesota for supply chain management. Magnet negotiates between sellers and buyers based on different negotiation protocols. Different agents in MAGNET perform separate set of activities while working as independent entity. Agents communicate with each other to satisfy their goals to complete their task. MAGNET provides different type of transactions for buyers, sellers and services like management of bidding processes and their evaluation of bids. Magnet was developed having a focus on fraud control and counter speculation. [17], [18]

4. Critical evaluation

4.1 Security issues in agent-enabled E-commerce

There are some security issues currently in need to be taken care of, namely

- General trust issues
- Interaction with strangers
- Trustworthiness

General trust issues are related to the agent service provider based on the type of services it provides.

An agent-based E-commerce solution provider must make its system reliable to interact with user. Information of the user is being secured through the agent communication channel to agents or humans. Security mechanism of the system should not allow strangers to interact with the system without having the authorized data/information.

Trustworthiness based on the life of agent and the solution provider can be gained by providing the secure solutions. To deliver these solutions in time with having valid tracking system to track buyer orders without any kind of interruption.

There are some security threats in MAS.

- Corrupted naming and match making services
- Insecure communication channels
- Insecure delegation
- Lack of accountability

Corrupted naming and match making services are very critical. These services are interdependent, as each agent needs to have a naming service to find or locate other agents. Hackers can attack these services untrustworthily and make them corrupted.

Insecure communication channels between agents, agents and humans provide unauthorized persons or agents to get involved in the communication. The messaging service between agents should be delivered to the authorized agents without having any third party interruption.

Insecure delegation agents delegate the services they provide. They do have the right to get the relevant information for authorization before passing any kind of information as a result. They do not provide account information of a person to an untrusting host based on secure delegation mechanism.

Lack of accountability leads agent to develop trust on other agents and services. If there are some bugs in the agent then there can be variety of issues for agents to provide their services in a timely fashioned environment causing the user to avoid the use of technology. [19]

5. Conclusion

In this paper we discussed how people interact with E-commerce and what type of security issues and threats they face and trust of people on E-commerce applications. How agent technology helps to solve these issues covers the idea of malicious agents and different security frameworks to develop agent enabled E-commerce solutions. Then we discussed different MAS developed for E-commerce and how they are facilitating the users to use this technology. Finally we discussed different threats in MAS and how to avoid those threats. According to the current state of the art development of security applications to make agent systems reliable is still in progress and there are many areas still needs to be addressed to solve security issues/threats.

Further enhancement and review in order to identify security issues in MAS based on the on going research will help to get familiar and to discuss platform and domain specific issues. Variety of security issues could be identified and possible security framework could be presented after knowing and analysing the latest implemented systems.

References

[1] A. ILDEMARO (2003), "Developing Trust in Internet commerce", *Proceedings: Conference of the Centre for Advanced Studies on Collaborative research -2003, October* 06 – 09, 2003, Toronto, Ontario, Canada: ACM PORTAL, IBM Press, P.1-15

[2] R. MARCHANY, J. TRONT (2002), "E-commerce Security Issues", *Proceedings: 35th Hawaii International Conference on system sciences –2002,* January 07 – 10, 2002, Big Island, HAWAII: IEEE Computer Society Press, P.193

[3] G. MARIA, Agents and other "Intelligent Software" for E-commerce, Department of CS, University of Minnesota CSOM, 12, Feb 1999

[4] Z. LENNY, "The Evolution of Malicious Agents" <http://www.zeltser.com/malicious-agents>

[5] BHIMANI A, (1996), "Securing the Commercial Internet", *Communications of the ACM 1996,* June, 1996, ACM PORTAL, IBM Press, P.29-35

[6] KINE A., CHOOBINEH J (1998), "Trust in Electronic Commerce: Definition and Theoretical Considerations", *Proceedings: 31st Annual Hawaii International Conference on system sciences- Volume 4 -1998,* January 06 – 09, 1998, Kohala Coast, HI: IEEE Computer Society Press, P.0051

[7] SHENG G., "Agent based E-commerce" <http://www.ece.nus.edu.sg/stfpage/eleguans/award/MAMA2000/highlight.html>

[8] T. TOMOYA, M. TADANORI, W. TAKASHI (1998), "A Model of Mobile Agent Services Enhanced for Resource Restrictions and Security", Proceedings: International Conference on Parallel and Distributed Systems–1998, December 14-16, 1998, Taiwan: IEEE Computer Society Press, pp.274

[9] "SOMA: Secure and Open Mobile Agent" <http://www-lia.deis.unibo.it/Research/SOMA/main.shtml>

[10] C. ANTONIO, M. REBECCA (1999), "*Mobile Agents Integrity in E-commerce Applications*", Proceedings*: ICDS Workshop on Electronic Commerce and Web based Applications –1999, May* 31 – June 04, 1999, Austin, TEXAS: IEEE Computer Society Press, pp.0059

[11] TZONE I WANG, K.H. TSAI, MING-CHE L (2004), "*A Two-Layer Cryptographic Scheme for an e-Service Framework Based on Mobile Agents",* Proceedings*: IEEE International Conference on e-Technology, E-commerce, e-services –2004, March* 28 – 31, 2004, Taipei, TAIWAN: IEEE Computer Society Press, pp.98-105

[12] P. P. JOAO, A.C. PEDRO, et all (2004), "*A Multi-Agent System's Approach to Communicate Security in the Webs",* Proceedings*: Web Intelligence, IEEE/WIC/ACM International Conference on (WI'04) –2004, September* 20 – 24, 2004, Beijing, CHINA: IEEE Computer Society Press, pp.706-710

[13] PL KAMAN, L HOFUNG (2004), "*An Adaptive Strategy for Trust/Honesty Model in Multi-Agent Semi-Competitive Environments",* Proceedings*: 16th IEEE International Conference on Tools with Artificial Intelligence (ICTAI'04) –2004, November* 15 – 17, 2004, Boca Raton, Florida, USA: IEEE Computer Society Press, pp.416-423

[14] KATIA, P. S. (1998) AI Magazine. Management Decisions, P.79-92

[15] FR-REN L, KUANG-YI C. (2001) Intelligent E-Business. A Multiagent Framework for Automated Online Bargaining, pp.41-47

[16] KURBEL, K; LOUTCHKO I: (2001), "*A framework for Multi-agent Electronic Marketplaces Analysis and Classification of Existing Systems",* Proceedings*: International ICSC Congress on INFORMATION SCIENCE INNOVATIONS (ISI'2001), –2001, March* 17 – 21, 2001, Dubai, UAE:

[17] Multi Agent Systems <http://www.multiagent.com/Software/E-commerce/>

[18] MAGNET, Intelligent Agents for Electronic Commerce <http://www.cs.umn.edu/magnet/>

[19] H.C. WONG and K. SYCARA, "*Adding Security and Trust to Multi-Agent Systems," Proceedings of Autonomous Agents '99 Workshop on Deception, Fraud, and Trust in Agent Societies, May, 1999*, pp. 149 - 161.