Security and Trust in Agent-enabled E-Commerce

Rashmi Bhatia
Dept. of Computer Applications
Dev Samaj College for Women
Chandigarh, India

***Abstract*—With increasing use of the E-commerce for the business over the cyber space, security threats are also increasing. The trustworthiness of the business over the internet has become critical both for the consumer as well as for the service provider. In this paper I'm going to discuss how Intelligent Agents can help to securely exchange the information while doing a transaction over the internet. I will evaluate the current techniques used by the multiple agents, especially for the agents developed for the E-commerce. Also, analysis of the agent based system in regards of their ability for tackling threats.**

Keywords*— MAGNET *(Multi AGent NEgotiation Testbed), Multi Agent System (MAS), RETSINA, SAFER

I. INTRODUCTION:

There are numerous threats to the security of Internet E-commerce. Security breaches are most frequently discussed in terms of the information as it can modify the content of the message. The internet is only one potential source of insecurity; further elements of the problem are:

- The Customer side where a customer can be impersonated, with or without the use of the customer's equipment. The use of stolen credit card details is the simplest example.
- The vendor side where the vendor can trade inappropriately or dishonestly (Whiteley D., 2000).

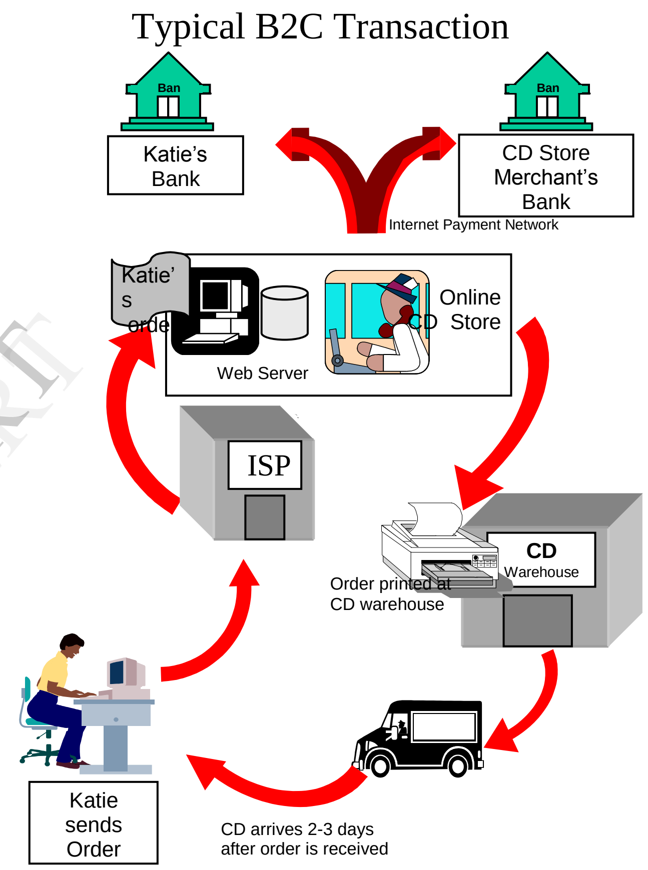

Fig.1. Typical B2C Transaction (Boncella, 2000).

Fig. 1 shows a Typical B2C Transaction in which a customer *Katie* ordered a CD from the website. This order goes through various steps until *Katie* receives the CD he ordered. But, this transaction goes through various security threats which are shown in the *Fig. 2*.

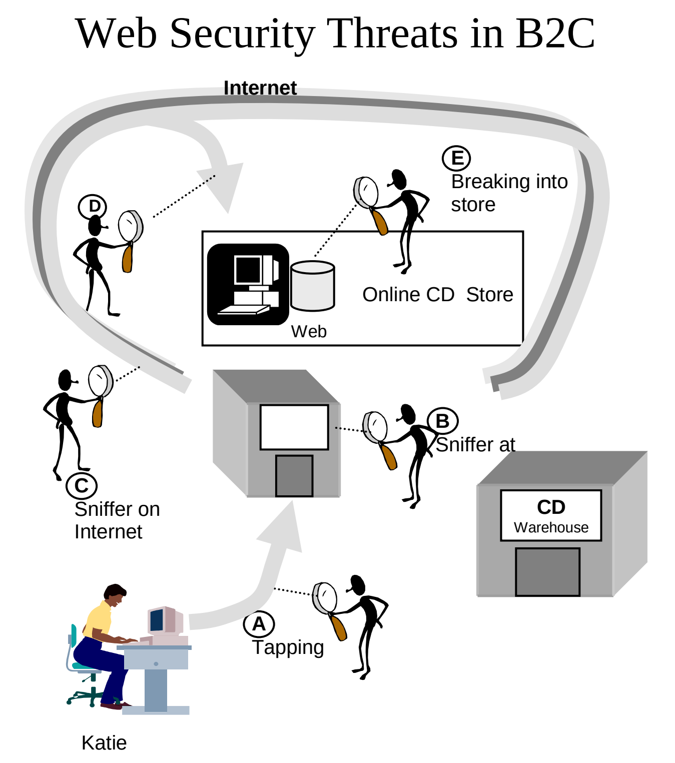

Fig. 2: Web Security Threats in B2C (Boncella, 2000).

Fig. 2 shows various Web Security Threats which are involved in an online transaction such as *Tapping* of the information given by *Katie*, Sniffer on internet or at web server i.e. hacking of the web server etc.

Thus, typically various mechanisms are used to secure e-commerce which are as following:

- Authentication
- Integrity
- Encryption
- Digital Signatures etc.

All of the above techniques are used to make e-commerce secured. But, how a customer who is going to do an online transaction with an e-commerce website, can trust the e-commerce website i.e. whether the website is trustworthy? Will they fulfil the order after getting the payment? Also how can customer be sure that they won't pass or use the details of the credit cards etc.

II. Intelligent Agents

Agents are software entities which have enough autonomy and 'intelligence' to carry out various tasks with little or no human intervention. They are software delegates of individuals and organizations, and can act on behalf of their delegators. In *Multi-Agent Systems (MAS)*, agents interact with other agents can access remote service providers, search for information on the web, and carry out sale transactions. Agent-mediated electronic commerce is seen as a major application area of agent technology (Rosenschein *et al.*, no date, in Wong and Sycara, 1999).

A. Intelligent Agents & E-Commerce

E-commerce has a lot of advantages such as ease in accessibility, low operating cost and broader services. But, there are some barriers blocking the road to success, which include overload of information, difficulty in searching, lack of negotiation infrastructure, etc. This is why e-commerce need advanced technologies as support. Intelligent agents are seemed to be the excellent candidate with their properties of intelligence, autonomy and mobility. Intelligent agents act on the behalf of the customers to carry out delegated tasks automatically. They have demonstrated tremendous potential in conducting various tasks in e-commerce, such as comparison shopping, negotiation, payment etc. (Guan and Zhu, 2002).

B. Intelligent Agents Security & Trust

Intelligent agents are the programming paradigms which allow flexible structuring of distribution of the computation over the internet. But, before the agents can be used in the e-commerce applications their security must be defined. Most of the intelligent agent systems refer to four elements for their security, which are as following:

- A secure runtime environment (e.g. the Java Virtual Machine) for host protection
- Code signature to prove that the agent has not been tampered with
- Host authentication to prove that the agent is about to move to the intended host
- A secure channel over which agent can migrate.

C. Different stages in Working of MAS

The working of MAS varies from Model to Model of different MAS. But there are few aspects of working of MAS which are almost common in an e-commerce transaction. According to Singlee and Preneel (2004) there are Different stages in the scenario, which are as following:

1) *User sends agents:* User generally connects to the internet periodically for a short time. As per user's requirements he sends multiple customized agents on the internet for the best bargains of different needs such as hotel booking, air ticket reservation and car rental etc. Thus, multiple agents have to communicate each other to fulfil the overall requirements of the user.

2) *Agents travel and securely collect data:* The agents travel from one platform to other. Only the data collected by the agents and their parameters are securely transferred between the agent platforms, but the program is accessed at its original location. The agents collect the information from each agent platform (Singlee and Preneel, 2004).

3) *Agents conduct a secure payment transaction:* An agent at any time can decide about conducting a financial transaction. Thus, it communicates along with other agents to generate the digital signature. All the agents together can generate a new signature for a particular offer at an agent

platform. A combining entity is required to combine an appropriate set of the contributions of the agents into the resulting signature (Singlee and Preneel, 2004).

4) *Verify collected data:* In the end the agent returns to the semi trusted platform. This platform verifies for the authenticity of the collected data. That data includes the various transactions conducted by this agent.

D. *A MAS for Authorization of confidential Information:*

According to Sycara, 1998 (in Seo et al., 2004), A Multi-Agent system is an appropriate approach for managing confidential information in that the multiple threads of control are a good match for the distributed resources to be secured and the ever-changing nature of task assignments is typical organization.

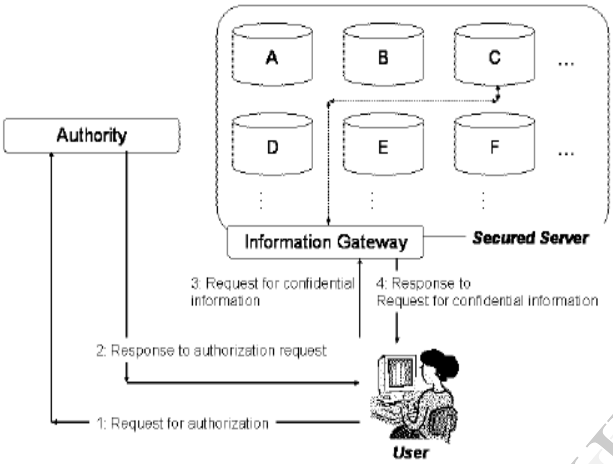
A
B
C
...
D
E
F
...
Authority
Information Gateway
Secured Server
3: Request for confidential information
4: Response to Request for confidential information
2: Response to authorization request
1: Request for authorization
User

Fig. 3: A typical scenario of access to confidential information (Seo et al., 2004).

Fig. 3 shows the conceptual architecture of a multi-agent system for managing the confidential information. Thus, various types of agents are shown which are as following:

1) *Supervisor Agent:* A supervisor agent works as help to the human supervisor for assigning the initial information, monitoring the access to confidential information and controlling the work flow for access to confidential information.

2) *User Interface Agent:* A human user can interact only with the user interface agent. Human user requests for the confidential information with the help of user interface agent. This agent works with authorization agent and allows the user to access authorized information.

3) *Authorization Agent:* This agent I responsible for that whether request for the confidential information is valid or not (Seo et al., 2004).

E. *Architecture of Multi-Agent Systems (MAS)*

Architecture of the Multi-Agent Systems depends upon the need of the system. There are various models of the MAS as different models are developed for the different systems working.

According to Marik and McFarlane (2005), Agent architectures usually have two recognizable parts:

- The Wrapper accounts for inter-agent communication and just-in-time reactivity.
- The body carries out the agent's main functionality.

Several typical agent architectures exist, ranging from purely reactive agents, which operate in a simple "stimulus-response" fashion, to more deliberative or *goal oriented* agents, such as belief-desire-intention agents, which proactively reason about their goals and actions (Marik and McFarlane, 2005).

Various Models of Agent based systems are there to fulfil the needs of a particular system, which differ in their architecture and working. Such as:

- MAGNET (Multi AGent NEgotiation Testbed): A Multi-Agent System for doing auctions on the internet.
- RESTINA: It a reusable multi-agent infrastructure for building agents with capabilities of inter-agent, message-passing communication. The RESTINA infrastructure can be used by agent developers to quickly develop agents for different applications. RESTINA was developed having Internet applications in mind (Wong and Sycara, 1999)
- SAFER: SAFER is an infrastructure designed to serve agents in e-commerce and to establish necessary mechanisms to manipulate them. It focuses on three fundamental activities of agents, namely, fabrication, evolution and roaming (Guan et al., 2002).

In the following section of this paper, MAGNET is going to be discussed, such as its Architecture, Security drawbacks and Trust assumptions etc. to evaluate it.

III. MAGNET (Multi Agent Negotiation Testbed)

MAGNET is the multi-agent system which is specially developed for the online combinatorial auctions. The trust model of the MAGNET is quite different from the typical auction web sites.

MAGNET and the supporting architecture provide support for complex agent interactions, such as in automated contracting, as well as other types of negotiation protocols (Collins *et al.*, 1998, in Jaiswal *et al.*, 2003).

When the original MAGNET system was developed then security was not a major concern. But as the system was evolved, it became clear that security architecture has to be developed in order to use on open networks. Specifically, MAGNET has problems with secrecy of bids, non-repudiation, early bid opening, and manipulation of bids. Such problems are quiet common in auction systems. But, in MAGNET there exists a notion of a trusted third party: the market (Jaiswal *et al.*, 2003).

A. *Architecture of MAGNET*

According to Collins *et al.*, 1998 (in Jaiswal *et al.*, 2003) The current architecture of MAGNET consists of mainly three entities: the *customer agent*, the *supplier agent*, and the *market*. These agents are self-interested agents, which try to achieve the highest profits from their endeavors.

Following is the description of the types of agents in MAGNET.

- The market is the place where both the customer and the supplier agents negotiate.
- The customer agent (Contractor agent) tries to negotiate with the supplier agents to achieve its goal of maximum profit. It involves the Request for Quotes (RFQ).
- The supplier agent accepts bids from the customer agents and responds to those bids.

1) *Planning:* In this phase the customer agents defines the requirements and plan. Then it selects a market, specialized in particular products or services, where it may fulfill its requirements. Customer agent also considers the value of its goal and necessity of its components. Then customer agent generates the RFQs, as per its plan.

2) Bidding: In this phase the supplier agents receive the RFQs from the market. The supplier agent then forms the bid and passes to the market for its validation which is further delivered to the customer agent. It is up to market to keep the bids until deadline or pass right away to customer agents. The customer agent then evaluates the bids and selects the appropriate bid which meets the requirements of its plan. There after customer agent sends the confirmation of the acceptance to the supplier agent through the market.

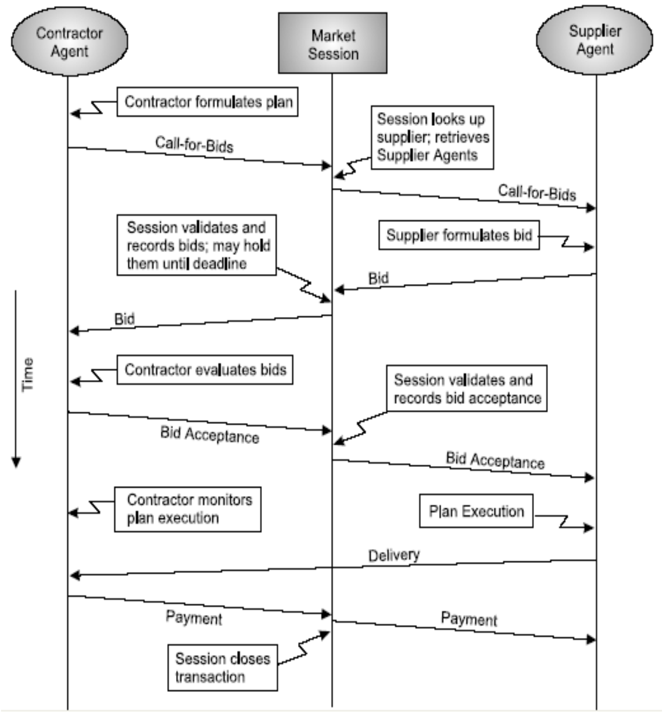
Contractor Agent
Market Session
Supplier Agent
Contractor formulates plan
Session looks up supplier; retrieves Supplier Agents
Call-for-Bids
Call-for-Bids
Session validates and records bids; may hold them until deadline
Supplier formulates bid
Bid
Bid
Time
Contractor evaluates bids
Session validates and records bid acceptance
Bid Acceptance
Bid Acceptance
Contractor monitors plan execution
Plan Execution
Delivery
Payment
Payment
Session closes transaction

Fig. 4. MAGNET's original three step protocol (Jaiswal et al., 2003)

3) *Execution:* The supplier agent then executes the tasks for which the customer agent had accepted. The customer agent monitors the execution the tasks that they are executed as per the expectations. However, the customer agent can change its plan if it finds that execution is not as per requirements. Once the supplier agent completes the execution, the customer agent makes the payment. This payment is also recorded by the market.

B. *Drawbacks of MAGNET*

According to Jaiswal *et al.* (2003), The original model of the MAGNET had not considered the security, which resulted into various drawbacks which are as following:

1) *Secrecy of the bids:* In a sealed bid auction it is necessary that bids are opened once the auction has finished. But in MAGNET customer agents can receive the bids through market before the final auction. The bid information is also available to other supplier agents as well. Also there is no encryption technique used in the MAGNET.

2) *Non-repudiation:* In an auction there should be a mechanism to guarantee non-repudiation. In MAGNET, if the winning supplier agent declines to go ahead with the contract, there is no means of proving that it was indeed that agent who won the bid. Similarly, there are no means for assuring the suppliers that the RFQs they received were actually sent by the customer agent they claim to come from (Jaiswal et al., 2003).

3) *Manipulating of closing time:* In MAGNET the customer agents can't extend the closing time of the auctions. However, they can ignore the bids received. To extend the closing time of an auction customer agents have to generate a new RFQ. Also market can block the bids received from the supplier agents and also convey the different closing time by modifying the RFQ's.

4) Fairness: In order to achieve a trustworthy auction system, it is required that the customer agents are assured that their bids were treated fairly before the final selection of a bid. But fairness can't be achieved easily.

5) Fault Tolerance: In the case of MAGNET, either the failure of the customer agent or the market can be responsible for the failure of the auction process. This is strictly speaking not a security hole but a problem which might lead to other security problems.

MAGNET uses the trusted third party, which can be used by the agents to do the transactions. But, there are certain assumptions for the trust which are used by the *Market*, which are discussed in the following section.

C. *Assumptions of Trust in MAGNET*

Various assumptions of trust for *market* are following:

- Market is responsible for transferring the RFQs from the customer agent to supplier agent and vice versa for the bids.

- Market acts as a record keeper by keeping note of all the transactions and movement of RFQs and bids that take place through it. In case of dispute, the market will act as an arbitrator using saved records (Jaiswal et al., 2003).
- Market is responsible for aggregating statistical data from transpired auctions and making it available to interested parties at a later period of time. This data may affect the determination of the winning bidder. We assume that this statistical aggregation is performed correctly by the market (Jaiswal et al., 2003).

IV. Summary & Conclusion

After investigating the Intelligent Agents for E-commerce, I have come to this point that, however e-commerce is coming up as a big business there are few barriers in the success of that because of Trust and Security. With the help of Intelligent Agents a high level of security can be implemented and trust can be gained. But, it is very difficult to make such intelligent agents which are perfect can be fully trusted. Also it will take time before people can trust agents and use them.

References

[1] D. Whiteley, e-Commerce Strategy, Technologies and Applications. London, The Mc Graw Hill Companies.

[2] J. Rosenschein, “Agent-Mediated Electronic Commerce: Issues, challenges and some viewpoints” in Proceedings of the Second International Conference on Autonomous Agents, May 1998, pp. 189-196.

[3] H.C. Wong and K. Sycara, “Adding Security and Trust to Multi-Agent Systems” [online]. Washington, DARPA , 1999. Available at:
<http://www.ri.cmu.edu/pub_files/pub1/wong_hao_chi_1999_1/wong_hao_chi_1999_1.pdf>

[4] S.U. Guan and F. Zhu, “Agent Fabrication and Its Implementation for Agent based Electronic Commerce” in International Journal of Information Technology & Decision Making, 1(3), pp. 473-489.

[5] S.U. Guan et al., “A Modularized Electronic Payment System for Agent-based E-commerce” [online]. Singapore: National University of Singapore, 2004. Available at:
<http://ws.acs.org.au/jrpit/JRPITVolumes/JRPIT36/JRPIT36.2.67.pdf>

[6] D. Singelee and B. Preneel, “Secure E-commerce using Mobile Agents on Untrusted Hosts” [online]. COSIC Internal Report, 2004. Available at: <http://www.cosic.esat.kuleuven.be/publications/article-199.pdf>

[7] K. Sycara, “Multiagent Systems”. A I Magazine, 10(2), pp. 79-83 in Y.W. Seo et al., A Multi-Agent System for Enforcing ``Need-To-Know" Security Policies [online]. USA: Carnegie Mellon University, 2004 Available at:
<http://www.ri.cmu.edu/pub_files/pub4/seo_young_woo_2004_4/seo_young_woo_2004_4.pdf>.

[8] Y.W. Seo et al., A Multi-Agent System for Enforcing ``Need-To-Know" Security Policies [online]. USA: Carnegie Mellon University, 2004. Available at:
<http://www.ri.cmu.edu/pub_files/pub4/seo_young_woo_2004_4/seo_young_woo_2004_4.pdf>.

[9] V. Marik and D. Mcfarlane, “Industrial Adoption of Agent-Based Technologies” IEEE Intelligent Systems, January-February 2005, pp 20-27.

[10] J. Collins et al., “A Market Architecture for Multi-Agent Contracting” in Proceedings of the Second International Conference on Autonomous Agents, pp 285-295.

[11] A. Jaiswal et al. Security Model for a Multi-Agent Marketplace [online]. USA: ACM Press, 2003. Available at:
<http://portal.acm.org/citation.cfm?id=948021>.

[12] R.J. Boncella, Web Security for E-commerce [online]. Communications of the Association for Information Systems 2000, 4(11), November 2000 . Available at:
<http://www.washburn.edu/faculty/boncella/WEB-SECURITY.pdf>.