Review of the Main Security Problems with Multi-Agent Systems used in E-commerce Applications

Alfonso González Briones[a], Pablo Chamoso [b] and Alberto López Barriuso [a]

[a] University of Salamanca, BISITE Research Group, Edificio I+D+I, 37007 Salamanca, Spain

[b] Catholic University of Daegu, Faculty of Information Technology, Daegu, South Korea

alfonsogb@usal.es

KEYWORD

Security problems; Multi-agent systems; E-commerce applications

ABSTRACT

The ability to connect to the Internet from a wide variety of devices such as smart phones, IoT devices and desktops at anytime and anywhere, produces a large number of e-commerce transactions, such as purchases of clothes, ticket entrances for performances, or banking operations. The increasing number of these transactions has also created an increase in the number of threats and attacks by third parties to access user data banks. It is important to control the access procedure to user data so that the number of threats does not continue to grow. To do so, it is necessary to prevent unauthorized access, theft and fraud in electronic commerce, which is required to ensure the safety of these transactions. Many e-commerce platforms are developed through multi-agent-systems because they include certain advantages to control the product, resource management, task distribution, etc. However, there are a number of threats that can jeopardize the safety of the agents that make up the system. These issues must be taken into account in the development of these multi-agent systems. However, existing methods of development do not cover in depth the issue of security. It is necessary to present and classify the potential security flaws of multi-agent systems. Therefore, the present research presents a review of the main vulnerabilities that occur in multi-agent systems responsible for managing e-commerce applications, as well as the proposed solutions to the major security problems on these platform systems. The main conclusions provided by this research is the need to optimize security measures and enhance the different security solutions applied in e-commerce applications in order to prevent identity theft, access to private data, access control, etc. It is therefore essential to continue to develop the security methods employed in applications such as e-commerce as different types of attacks and threats continue to evolve.

1. Introduction

E-commerce is an economy of buying and selling products or services over the Internet by using electronic technologies such as the Internet and / or other computer networks. The number of e-commerce transactions has grown dramatically since its inception due to the use of Internet. Electronic commerce does not only focus on the buying and selling of goods or services between customers and companies; there is a considerably high percentage of sales from virtual items such as access to virtual "premium" content websites. The advantages provided by the technology used make it possible to access these applications

from anywhere and have the same products and services, thus eliminating the barriers of time and location. This provides a global scope allowing the sale and purchase of goods and services from anywhere, while at the same time allowing the manufacturer and the seller to reduce the advertising costs required to reach a large number of customers. However, there has also been an increase in the existence of threats and attempts to exploite security flaws (Bouch, 2011).

There are different safety aspects related to e-commerce applications that should be considered. Thus, we can define a series of objectives that e-commerce platform must meet in order to be considered safe, such as:

- **Confidentiality (Lokhande, 2013)**¡Error! No se encuentra el origen de la referencia.: protection of stored data from unauthorized users.
- **Identification and authentication (Lokhande, 2013):** identification refers to users who reveal their identity in order to access the system. Authentication refers to a response that users provide to prove their identity (usually a password or digital certificate).
- **Access control (Lokhande, 2013)**: determines the level of access to a user or group of users.
- **Non-repudiation (Lokhande, 2013)**: guarantee that users cannot deny being responsible for any action they have taken.
- **Data Integrity (Lokhande, 2013)**¡Error! No se encuentra el origen de la referencia.: refers to the completeness and accuracy of the data stored.

However, there are different intrinsic vulnerabilities to any electronic commerce simply due to being exposed to the general public via internet access. These vulnerabilities can be classified into three categories:

- **Denial of service**: attacks that are made with the purpose of rendering the site or resource unavailable to users who try to retrieve or access the site, whether temporarily or indefinitely. In the case of electronic commerce, such an attack would stop the transaction, resulting in customer loss during the period of time they are trying to access the resource-dependent services. Such attacks are more effective the greater the volume, so it is common practice to carry out these attacks in a distributed manner by different attackers or by a single attacker from multiple locations simultaneously, which is known as DDoS (Distributed Denial of Service).
- **Unauthorized access:** represents illegal access to systems, applications or data, generally taking advantage of any existing security vulnerability in the system. These accesses are quite dangerous since they can modify data, personal information, etc. that cannot be recovered. A common practice to carry out such attacks is the use of sniffers in public networks, keyloggers, or SQL injection.
- **Fraud and theft:** theft of data can be achieved through unauthorized access, but if such data are used to commit malicious actions, it is considered an act of fraud.

The main attacks that tend to focus most on e-commerce are web-based and include:

- **Fraudulent e-mail (Niranjanamurthy et Cluster, 2013):** Given the widespread acceptance and use of email as a communication medium, this type of attack is often used. It involves making the recipient believe the content is original, when in fact the e-mail contains links or attachments that include some type of malware. This is considered a type of social engineering.
- **Man in the middle attack:** an attack in which the attacker becomes involved in the communication between the server and the client, unknown to the customer, and is able to modify, delete, insert or otherwise modify at will any request the client makes to the server.
- **Malware:** Most attacks on e-commerce portals contain malicious software that is used to obtain information in an unauthorized manner, monitor user actions, etc. Such malicious software can be broken down and classified as: a virus, Trojans, adware, worms and back door. See the distribution shown in Figure 1.

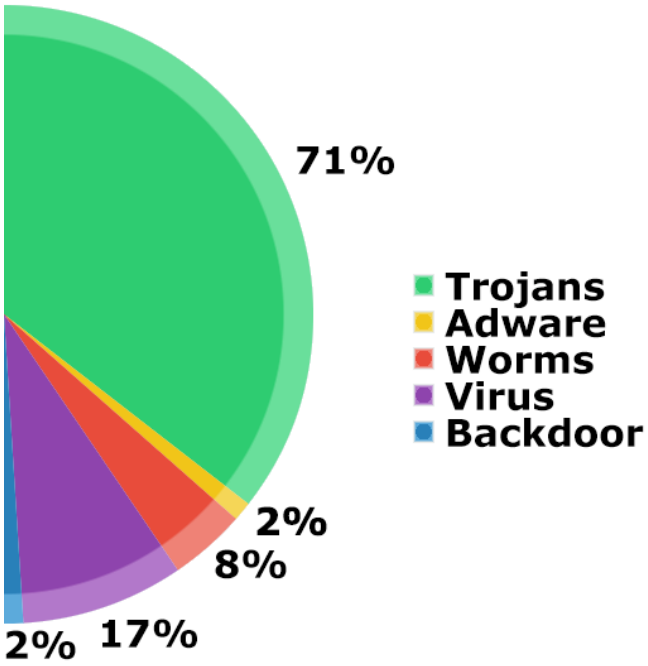

Figure 1: Percentage of use of different types of malware.

- **SQL injection:** the insertion by the attacker of a malicious SQL code that acts directly on the data to gain unauthorized access to the page, or to modify database information.
- **Pharming:** These attacks focus on DNS systems, interfering with search requests and redirecting the user to a site with a similar appearance but fraudulent content.
- **Snooping:** The concept of snooping responds to a series of techniques applied to ensure the safety of an existing DHCP infrastructure. The most common attacks apply to port scans, which are user ports that have been opened, which provides the attacker with unauthorized access to the user's computer. In this case, the attacker can gain valuable information like passwords or sessions (cookies).
- **Cross site scripting:** also known as XSS, allows attackers to inject malicious code or scripts on legitimate websites that request password verification, to redirect users to malicious sites, etc.
- **Cryptographic Attacks:** These attacks are very common and focus on guessing the password of a user (the victim in this case) by employing a tool that, for example, uses dictionaries or brute force methodologies (trying all possible combinations).

It is therefore imperative for electronic commerce systems based on multi-agent systems to be modelled and prepared to withstand these attacks. Therefore, the present study presents a multi-agent platform with agents that are responsible for identifying and responding to such attacks before they are carried out, thus avoiding the theft of information.

The remainder of the article is organized as follows: the second section presents security solutions proposed by multi-agent architectures; section 3 provides the conclusions obtained and discusses the progress in the safety of these architectures.

2. Security in multi-agent architectures used in e-commerce applications

This paper presents the security measures that should be taken in developing an e-commerce application and a multi-agent system that aims to facilitate logistics, supply, storage and transport of the electronic market application architecture. This point focuses on blocking the main security threats cited in the state of art.

2.1. Security in E-Commerce

The above security requirements in electronic commerce must be associated with methods to properly protect the systems that house them, protecting the information generated during an e-commerce transaction. These techniques focus on the transmission of data on the Internet, payment transactions and storage methods of such information.

2.1.1. SSL Security in Information Transmission

The transmission of private and confidential information over the Internet requires security techniques that encrypt data ensuring that e-commerce applications maintain data protection. One of the most widespread protocols in communicating information is SSL "Secure Sockets Layer". The SSL protocol is designed to allow data communication to be secure, whether sending or receiving the data, using an encryption key to prevent decoding by unauthorized persons. SSL incorporates features that make it possible to validate the integrity of the data transmitted. E-commerce applications show the use of this protocol in their web portals by adding the letter s to the URL, making the URL https:// instead of htpp:// . Additionally, the browser incorporates an indicative symbol, such as a key, a padlock and trusted icons. One of the errors that users often make is to rely on these applications sole for their use of HTTPS in the login process, even though all subsequent communication can be in plain text, still readable by the various "sniffers" network.

Therefore, all e-commerce applications must implement this protocol, requiring a certificate authority to issue the key and digital certificate. This way the virtual entities that offer the purchase of products or services online can require the real identification of customers and consumers. If such a certificate is not recognized by a certification authority, the previous layer to the application, which is the web browser itself, displays an alert to the user to confirm whether the user trusts the e-commerce application in cases where information must be sent.

2.1.2. Payment Security

The vast majority of e-commerce fraud is due to the fact that the seller does not authenticate clients in a way that is completely secure, through certificates, and then struggles to validate payment and ensure non-repudiation.

Making an online payment via credit card does not mean that the user is the actual owner of the bank card, resulting in identity theft. Attempts to avoid this include introducing additional security in payment gateways, which may include sending a code sent to the mobile terminal employed by the user during the registration process on the platform. This has also given rise to the use of payment intermediary entities such as Paypal, Amazon Payments, Google Wallet or Apple Pay. These entities produce a layer of

abstraction by which the buyer does not know the details of the seller and vice versa, allowing the seller to charge payment while the intermediary is in charge of the transaction.

2.1.3. Data Security Storage

One aspect to consider is the security of the server that stores all the information related to users, products, etc. It is important for the stored information to be encrypted. In the multi-agent systems that manage e-commerce applications there are agents that perform data encryption and decryption tasks. Strong passwords are needed to protect the access and control of the databases that store information, and they must be generated randomly through the alternating use of alphanumeric characters. This prevents the use of brute force methods to obtain the password. It is essential for the number of characters to be greater than 8 with no repeated characters. If the server is a contracted service, the hosting server should have the highest security measures available (firewall, intrusion detection systems, detection system malicious code).

For the identification process, the use of encryption mechanisms, usually based on SSL protocol is mandatory in order to avoid the data used for identification from being intercepted when transmitted through the internet.

2.2. Security in the development of multi-agent systems

One of the main problems encountered by developers of e-commerce applications in multi-agent systems is that they often do not have enough information security software. The security level of the system is separated primarily into the design and the implementation of design features (Mouratidis et al., 2003) (Viega et al., 2001). Factors to consider in this process include taking steps to ensure the confidentiality, integrity and availability of information within the system, which leads to the construction of a secure multi-agent system during the development phase (Stallings, 2008).

The main threats that occur in multi-agent systems are identified in the following research (Wong et al., 2000) (Cremonini et al., 1999) (Borselius et al. 2002) (Bijani et Robertson, 2014). These problems occur in the stages of authenticating and authorizing agents, according to Cremonini et al., 1999. Other problems that arise are related to the protection of agents by their hosts and vice versa, as described by Borselius et Alabama, 2002. Some very important problems to consider are those involving the verification of the information collected from the Internet by agents, unauthorized access to agents, unsecure communications among agents, attacks on the communication between agents, or attacks on the communication between agents and humans in conducting transactions produced by others (Jung et al. 2012).

There is no application that is 100% secure, but it is important to detect and prevent the vast majority of attacks from occurring in these systems. In the development of a robust multi-agent system it is imperative to take these assumptions and recovery mechanisms into account after an attack.

The proposed solutions, both at the host or agent level, are shown below. Creating two levels of security ensures that upon accessing the second level, there will be a new barrier.

Level	Requirements	Proposed solution
System	Protect the host system.	Create an agent that controls all communications and communication flows, and disrupts the
	Protect the agents that make up the system.	

	Isolate the main system in case of danger	communication processes if a vulnerability is detected, thus keeping agents out of danger. This agent must have an optimal security design, since an attack on this agent would open access to the agent level; therefore, it must also have security at the agent level, which requires us to implement a new barrier. This agent will send alerts to other agents to inform the team of developers of a breach in the security level of the system.
	Provide secure communications.	
	Provide security operations performed by users	
	Communicate access to the agent level	
Agent	Identify sources of threats and danger	Introduce an identification code composed of a unique identifier. This code is included at the beginning of the headers in the communication processes between agents, or with the user.
	Prevent unauthorized access	
	Provide secure communications.	

Table 1: Solutions proposed security level multi-agent applications .

3. Conclusions

The main conclusions obtained by performing this work are in the form of a compilation of the main vulnerabilities and security measures in e-commerce applications, and the multi-agents that provide support in managing e-commerce applications systems. We have focused on addressing all of the possible sources of danger that these applications can have.

The collected vulnerabilities are especially focused on the theft of information through communication processes, payment processing and access to storage servers.

The modelling of a multi-agent system must provide efficient solutions that ensure compliance with security requirements without hindering the functionality of the application. These security measures offer greater security and protection. For the multi-agent system to provide a secure electronic commerce transaction, systems must meet Internet security requirements (confidentiality, authentication, integrity and non-repudiation). Any commercial transaction performed on the internet involves a certain risk, not only when providing personal and banking data for online purchases, but when authorizing online payments.

To meet the safety requirements mentioned e-commerce platforms must have mechanisms to protect information systems involved in online shopping processes. These mechanisms include two aspects, one intended for data transmission via the internet (SSL security) and the other oriented to data storage (Data Security).

4. Discussion

The main points of discussion for this work focus on providing security measures to ensure the security of user data in these applications. It is important to develop the security measures employed, as well as develop new measures.

However, as the development of security solutions continues to advance, experts in detecting security failures are also progressing in creating new system failures in order to access information.

Acknowledgment

The research of Alfonso González-Briones, Pablo Chamoso and Alberto López Barriuso have been co-financed by the European Social Fund (Operational Programme 2014-2020 for Castilla y León, EDU/128/2015 BOCYL).

5. References

Bijani, S., & Robertson, D. (2014). A review of attacks and security approaches in open multi-agent systems. *Artificial Intelligence Review*, *42*(4), 607-636.

Borselius, N. (2002, June). Security in multi-agent systems. In *Proceedings of the 2002 International Conference on Security and Management (SAM'02)* (pp. 31-36).

Bouch, A. (2011). 3-D Secure: A critical review of 3-D Secure and its effectiveness in preventing card not present fraud. *University of London, Londra, erişim: http://www. 58bits. com/thesis/3-D_Secure. pdf, erişim tarihi*, *8*, 2014.

Cremonini, M., Omicini, A., & Zambonelli, F. (1999). Multi-agent systems on the Internet: Extending the scope of coordination towards security and topology. In*Multi-Agent System Engineering* (pp. 77-88). Springer Berlin Heidelberg.

Jung, Y., Kim, M., Masoumzadeh, A., & Joshi, J. B. (2012). A survey of security issue in multi-agent systems. *Artificial Intelligence Review*, *37*(3), 239-260.

Lokhande, P. S. (2013). E-Commerce Applications: Vulnerabilities, Attacks and Countermeasures.

Mouratidis, H., Giorgini, P., & Manson, G. (2003, July). Modelling secure multiagent systems. In *Proceedings of the second international joint conference on Autonomous agents and multiagent systems* (pp. 859-866). ACM.

Niranjanamurthy, M., & Chahar, D. D. (2013). The study of e-commerce security issues and solutions. *International Journal of Advanced Research in Computer and Communication Engineering*, *2*(7), 2885-2895.

Stallings, W., & Brown, L. (2008). Computer security. *Principles and Practice*.

Viega, J., Bloch, J. T., & Chandra, P. (2001). Applying aspect-oriented programming to security. *Cutter IT Journal*, *14*(2), 31-39.

Wong, H. C., & Sycara, K. (2000). Adding security and trust to multiagent systems. *Applied Artificial Intelligence*, *14*(9), 927-941.