2011 International Conference on Information Communication and Management
IPCSIT vol.16 (2011) © (2011) IACSIT Press, Singapore

Security and Trust in Electronic Commerce - Finding the Safe Side

Rashad Yazdanifard[1+], Mohammed A.S AbuTabik[2], Arash Pour Seyedi[3]

[1] Faculty of Management, Multimedia University, Cyberjaya, Malaysia –rashadyazdanifard@yahoo.com

[2] Faculty Faculty of Information Technology, Limkokwing University of Creative Technology, Cyberjaya, Malaysia –M07amed@windowslive.com

[3] Faculty Faculty of Information Technology, Limkokwing University of Creative Technology, Cyberjaya, Malaysia –arash_marghak@yahoo.com

Abstract. E-commerce is a new world generated from economy it makes the life easier for bidders and buyers. Both can sign in giant projects or transactions without making any kind of effort (you control everything from your home); However, there is another side making the best of efforts to frustrate, handle or hack the e-commerce transaction. So how can we protect it? If we succeed in the protection, what are ways that could help the organization to gain the consumer's trust? This paper will discuss the security of e-commerce, after that it will cover trust between consumers and the other side; to make the consumers sail smoothly in the sea of E-commerce without any constraints.

Keywords: security, trust.

1. Introduction

E-commerce was established in 1991; it is selling and buying of products and services by business and consumers via computer network such as internet. It covers a zone of different types of businesses starting from advertising, branding design, going through auction, and finally ending at trading goods and services between firms. No wonder it is said that e-commerce is one of the most important sides in the internet to display; from the year 1991 till today, life has faced drastic changes due to technological advancements, but simultaneously they have made our lives more complex. Moreover, E-Commerce became a need for development and modifying to protect the data and information from any attack, from here the definition of security in EC has emerged. Security is not enough for the consumer, trust should be found. Trust is a vital relationship concept between buyer and seller over internet which needs to identify because researchers have defined it in different ways [7].

Studies concerning security and consumer trust:

In security the threat to E-Commerce is, how the information will be protected, what would be the policies and infrastructure of e-commerce security and what is testing e-commerce security? The consumer is protected from any attack but how can the organization get the trust from consumers, a lot of points in this topic start from component, go through importance and benefit of trust, ending with trustworthy relationship.

The aim of our study is to generate an understanding of what meaning consumers give to the concept of trust and security. This objective will be reached through two goals; the first goal is to review the use from security in e-commerce. The second goal is the confidence between an organization and consumer if not there would be no interest from both sides. The paper is structured as follows; firstly, the theory of security is discussed. Secondly the theory of trust is discussed. Thirdly, successful company using good security and gains the consumer's confidence. Lastly the conclusion.

+ Corresponding author. Tel.: +60173693170.
E-mail address: rashadyazdanifard@yahoo.com.

2. Security

2.1 Security Threats to E-Commerce

As is well known the telecommunication links are not secure, if they were made secure, then it will be impossible to generate the communication security; there are different threats in e-commerce [2][6][12].

1) Threats Targeting Client

Web pages are mainly static, they're coded in HTML, they can do a lot of orders at the same time such as display contents, provide links to relate pages with extra information and more. But the widespread use of active content has made a difference in concepts. Activate content: it is the ability for displaying moving graphics, downloading and playing audio or video, and implementing the program. In e-commerce active content is used to place items one wishes to sell into a shopping cart by using a computer; the total invoice amount involves (sale tax, handling, and shipping cost).

Since active content modules are embedded in web pages, they can be completely transparent to anyone browsing a page containing them. It became easy for anyone to embed malicious active content in web pages. This technique, called a Trojan horse, immediately begins executing and taking actions that cause damage [2] [11].

2) Threats Targeting Communication Channel

The internet serves as the electronic chain linking a client to an e-commerce resource. The message passes through a number of intermediate computers on the network before reaching the final destination. It is impossible to guarantee that every computer on the internet through which messages pass is safe, secure, and unassailable.

Integrity threats: An integrity threat exists when an unauthorized party can alter a message stream of information. Unprotected banking transactions are subject to integrity violations. Cyber vandalism is an example of an integrity violation. Actually, it is the electronic defacing of an existing website page. Integrity threats can alter vital financial, medical, or military information. It can cause very serious consequences for businesses and people.

3) Threats Targeting Server

Client, internet, and server triad reflect the e-commerce channel between the user and e-commerce server. Servers have weak point that can be easily hacked and destroyed by the malicious hackers. If there are any attacks to the server, it is likely for the organization to lose everything.

Database threats: The tasks for e-commerce system are store user data and retrieve the information for any product form databases that connect with web servers. Databases that are connected to the web, contain important and private information which could absolutely damage a company if unauthorized side captures and discloses it. Username and password stored in non-secure databases can be easily hacked by someone who obtains this information as then he or she can masquerade as a legitimate database user and reveal private information

2.2 Information Security

There are three main parts to securing the information which is private, safe and available; these three parts of security could be affected by purely technical issues or deliberate human causes [9].

Privacy: the limitation of access information and detection to legitimate user, in addition to prevent access by disclosure to unauthorized users. In other words, privacy is a confirmation that information is shared only between authorized organization and persons. Authentication methods, it is like a portal the user should put ID and password which identify every user to access that can help to achieve privacy. More methods support privacy, limiting each identified users access to data system resources. All of this will protect the user from spyware and other attacks [1].

Safety: it is related to the trustworthiness of information resource. It is used to inform that information is accurate for its objective and the information should be responsible and complete. For example, forwarding copies of sensitive e-mail threatens both the privacy and safety of the information.

Availability: that is meaning the availability of information resources. There is responsibility for system which is delivery process and store information that should be accessible when anyone needs it. An information system that is not available when you need it is at least as bad as no system at all. It is very dangerous, if the system is the only one that takes care of a particular case. It may be much worse if the system is the only way to take care of a certain matter [1].

2.3 Security Policy

The first step in securing an e-commerce hazard is framing written security policies which define the requirements for each component of the system and how they interact. The security policy organizes activate employees only like it declared how IT infrastructure will be formatting. This policy should cover all the details on how it is to execute and how individual responsibilities are specified. To make it effective, the policy frequently needs to test and survey to determine the Security measures. The survey process should not ignore this because if any changes in technology or business practices are made it will impact onto security. Lastly, policy itself needs to update every period of time to reflect the development of the businesses, customers and technology [13][15].

2.4 Security Infrastructure

The security infrastructure is an implementation of security policy. These technologies choose to make the e-business and the rules secure by which it works. In addition, it should be implemented. The forfeiture for any attempt to break or breach of the security must be clear and implementation for all employees and partners must be enforced [6].

2.5 Testing E-Commerce Security

The need for security testing of an organization poses as a result of two main factors. The primary one is the necessity of gauging the range to which the security infrastructure executes the security policy of firms. The second factor is the weakness of presenting security infrastructure that leads to new threats.

The reason for existence of security testing is to detect the security requirements specialization for example define the location for assets and the access control mechanisms for it, verification of the integration of the security tools customize in the security infrastructure, detection of any gap between the chosen security infrastructure and the executed security infrastructure, detection of the limitation of the chosen security infrastructure with observance to known weak points. Thus, there are two sides of testing, compliance checking and penetration testing

i. Checking the Commitment: In this case, it is seen if the security infrastructure, that has been executed, work in with the security policy of the organization. A semi-automated tool can be used to work in with the policies with the executing infrastructure.

ii.Testing breakthrough: in this case, it is seen whether the executing security infrastructure of the firm is enough to avoid all possible security threats. Various automated and semi-automated security tools like Nessus etc. are available for breakthrough testing. They attempt and break the firm's network and make a record on the weakness points and threats that are shows in the network. The result from the testing phase is used to develop the security infrastructure and security policy of the firm. After that, the testing is implemented again. Thus, security engineering is a repeated and active process where all the stages need to be implemented periodically to make sure the security of a firm does not need any update.

3. Trust

In our life, people make important decisions when the want to buy something, till they reach the level of trust in the product between them and salesperson or the company. The same case happens in internet shopping, internet shopping decisions should include trust and it is not just between Internet sellers and the consumers, it is also between customers and computer systems through which the implementations are implemented [10].

3.1 Trust Consists of Two Components:

Fears of how we feel about starting trust and to be trusted, that means that the customer is able to manage resources for other people. In other words the customer should have the power over others

Fears of how we feel about having to trust other people, which is an annoying activity and sometimes can bring other feelings such as anger

3.2 The Necessity of Existing the Trust in Electronic Commerce

It is important to find the trust to secure the e-commerce but that does not mean all of users fear eliminate. It is not just the quality of serves and goods it also ensuring that the good get to the consumer safely. For example customers must be interested to give the confidential information such as credit card number to stabilize businesses to enhance the customer relationship through offerings and targeted communications [12].

The trust relationships in a global market place include trust between a sender to a receiver, in addition, customer and bank or bank and merchant (sender). Moreover, it includes trusted-third party. Therefore trust should incorporate measures taken to ensure the inherent honesty of both the information content and the process applied to it .Control steps have to be taken by electronic transactions service providers to encourage public trust through clearly explaining the security features of their system and clarifying the widespread public confusion about the exposure of credit card transactions to electronic fraud and the liability [5].

3.3 Trust Benefits

There is number of efficiency benefits that come from trust in collaborative relationships and it is included [3][9]:

- Able to summarize and draft the detailed for any contract (such as the trading partner agreement) that can be time and costly consuming if done officially.
- Able to expand the range of viable alliances and allow trading partners to enter into partnerships that may otherwise have been deemed impossible even with detailed equity contracts.
- Able to reduce costs for search.

The importance of trust in transactional relationships assists in managing uncertainties, and ensures further opportunities for improving coordination and cooperation among trading partners.

3.4 Trustworthy Relationship

Trustworthiness is defined as the understanding of confidence in the electronic marketer's safety and credibility but there are a lot of challenges it can come from [8]

- Shared technology which causes a shift in the nature of the expectations regarding the other's performance, and whose use is undetermined or difficult to assess for one of the parties [4].
- A buyer-supplier relationship, where the power to persuade resistant or even hesitant behaviour for the partners to adopt electronic commerce becomes difficult.

4. Discussion

Play.com is one of the most famous and successful e-commerce businesses on the web today it bring its success from offering books, music CD's, movies, videos and DVDs and much more at discounted prices. It puts a lot of effort into building up customer trust and security. Moreover, it tries to provide a most secure, free, credible online shopping environment through all kind of professional and considerable service [14].

Play.com only reveals the last five digits of the customers' credit card no. when confirming an order. In theory, based on a high amount of cyber-crime, safe security is the most important factor in online shopping because no customer wants to divulge their personal information though the online shopping procedure. If this information is made available then the customer will lose their trust in the company for Play to regain their trust will be a very difficult task.

Play.com servers always expertly and actively maintain Firewalls which often give a false sense of safety; the servers monitored by themselves, and the latest security patches applied regularly. It is often true that the larger the hosting company, the less frequently it patches its machines with the latest security updates.

You can choose the delivery option and the delivery time is guaranteed within 3-5 business days for the free delivery or first class delivery after that the customers select the payment method from a large range of available payment methods. It is good because the customer can choose different methods to pay and they will trust the company more.

The customer service of Play.com will send the customer an e-mail acknowledging receipt of their order. In theory this is also an important part of customer trust for online purchasing because this email can let the customer know that Play.com has received their order and the content of the email has not got the credit card no. this is because of security and the e-mail which is without any encryption at all

The high security of online ordering protection is not enough to gain the customer trust. Play.com has a very clear and trustworthy privacy notice, it is very important because the privacy policy is a fundamental element of customers trust in the company.at the same time, the customer will only trust a company which can help them to keep the privacy information with a clear and trustworthy privacy notice which can let the customer know what extend their privacy is protected by the company. The main points of the privacy policy in Play.com will not sell customer data as a standalone asset. The company will only sell it if the entire business is transferred.

5. Conclusion

Conclusively, the article points out the information security in e-commerce and discusses the threats, and security polices in e-commerce. The first step in E-commerce is to clearly define the requirements for each component of the system and how they interact, the second step being the implementation of the system which can also be called the security infrastructure, and last but not least the security policy must be made clear to all employees and partners. Before the implementation takes place though, the security system must be tested for any missing links or flaws in the system. The testing should include detection of the security requirement specification, detection of the integration of the security tools, detection of any gap and detection of the limitation. Moreover, the paper discussed the aspects of testing.

Also the article explained everything related about trust, trust is not just about the quality of the goods it is also the deliverance of them to the consumer. The article also covers benefits of trust such as reduce search costs. At the same time, the article handled trustworthy relationship between the supplier and the consumer. Once the trust is built successfully the seller has achieved the main motive to attract consumers.

6. References

[1] Aleksandra Nenadić, Ning Zhang, Stephen Barton., *FIDES – A Middleware E-Commerce Security Solution*.

[2] A SENGUPTA, C MAZUMDAR and M S BARIK.,*e-Commerce security – A life cycle approach*. S¯adhan¯a, 2005: p. 119–140.

[3] Chang Liua, Jack T. Marchewkab, June Luc, Chun-Sheng Yud., *Beyond concern—a privacy-trust-behavioral intention model of electronic commerce*. Information & Management 42, (2005), p. 289–304.

[4] D. Harrison McKnight, Vivek Choudhury, Charles Kacmar., *TRUST IN E-COMMERCE VENDORS: A TWO-STAGE MODEL*, p532-536.

[5] D. Harrison McKnight, Vivek Choudhury, Charles Kacmar., *Developing and Validating Trust Measures for e-Commerce: An Integrative Typology*. Information Systems Research, _ 2002 INFORMS Vol. 13, No. 3, September 2002, pp. 334–359.

[6] Dr. Nada M. A. Al-Slamy., *E-Commerce security* .IJCSNS International Journal of Computer Science and Network 340 Security, May 2008, p.340-344.

[7] E. Harrison McKnight and Norman L. Chervany., *What Trust Means in E-Commerce customer Relationships: An Interdisciplinary Conceptual Typology*. International Journal of Electronic Commerce , 2001–2002, p. 35–59.

[8] France Belanger, Janine S. Hiller, Wanda J. Smith., *Trustworthiness in electronic commerce: the role of privacy, security, and site attributes*, Journal of Strategic Information Systems 11, (2002), p. 245–270.

[9] KABIR SEHGAL., How Understanding Trust Benefits E-Commerce. P.27-31

[10] KyöstiPennanen, TainaKaapu and Minna-KristiinaPaakki.,*Trust, Risk, Privacy, and Security in e-Commerce*.

[11] Mark S. Ackerman and Donald T. Davis, Jr., *Privacy and Security Issues in E-Commerce*. Review chapter for the New Economy Handbook (Jones, ed.), in press.

[12] Pauline Ratnasingham., *The importance of trust in electronic commerce*. Internet Research: Electronic Networking Applications and Policy, 1998, p. 313–321.

[13] Peter Herrmann, Lars Wiebusch, and Heiko Krumm., *STATE-BASED SECURITY POLICY ENFORCEMENT IN COMPONENT-BASED E-COMMERCE APPLICATIONS*.

[14] Play.Com, Build Up Customer Trust And Security.(2011).

[15] University of Nebraska –Lincoln Bursar., *E-Commerce Security Policy*. Januar