Global Journal of Enterprise Information System

E-Commerce: A Mechanism to Ensure the Pre-Purchase Decision Security of the Online Customers

Umair Ujala[1*]

[1*]BIT Noida Campus, Assistant Professor, Department of Computer Sciences; umairujala@gmail.com

Abstract

Why e-Commerce in the retailing of goods is not coming up with the rapidity as it was expected in its early days? The risks associated with post-purchase decision are major reason to keep the customers away from e-commerce retailing. The e-commerce vendors are continuously implementing the stronger technologies to overcome from the risks associated with post-purchase decision process by the help of researchers and technocrats. The major emphasis of the researchers is on secure transactions, the server side security, and the client side security. The post-purchase decision process and after market security were always interesting and challenging topics of research. Though, the vulnerability is not finitely measured quantity over the public network but the secure transactions over the public network, the security of client and server is becoming stronger by the continuous valuable contribution of the researchers of the area. In spite of the technology advancement and new researches a huge scope is still left in the area of security of e-Commerce. Among the various reasons of customer satisfaction and security one important reason is pre-purchase decision security associated with the selection of e-shop by the customer. This paper tries to identify the risks associated with the pre-purchase decision and its solution. The paper also suggests the design and implementation of technology to provide the pre-purchase decision security.

Keywords: e-commerce, e-retail, trust, authenticity, linking, web access control

1. Introduction

According to the records the world's first B2B type e-Commerce was used by Thomson Holidays in 1981, the first B2C was Gateshead SIS/Tesco in 1984, and the world's first online shopper was Mrs Jane Snowball of Gateshead, England. The concept was introduced by Michael Aldrich in 1979, UK. The revolution began during 1990s when the concept of ERP (Enterprise Resource Planning), Data Minning, and Data Warehousing were incorporated with the e-Commerce. By the end of 2000 many renowned American and European business organizations started providing their services and product through internet and World Wide Web. By this time the people had become aware of e-Commerce and became familiar to purchase the goods and to make the payment online through secure Internet Connections/Protocols.

It was expected that the retailing in e-Commerce or e-Retail or e-Tail would grow rapidly (Evans & Wurster, 2000). The strengths of e-Retail are low search cost, efficiency, competency, and no intermediary. Although, e-Commerce is growing at an exponential rate (Khan, Varshney, & Qadeer, 2011) but e-Retail is having a very small market share. The share of e-Retail is 3–4% in the total retail industry and more than 95% share is with mortar and bricks sales.

The Internet provides a number of advantages and challenges to online retailers (Laudon & Traver, 2008). There could be many challenges in the growth of e-commerce retailing industry. These challenges can be categorized as illustrated in figure 1.

In this paper the key discussion topic is the pre-purchase decision challenges. When a person is willing to go for online shopping then the first step is selecting an appropriate e-shop. Now, the question arises how the customer will verify the authenticity of the e-shop because misrepresenting or spoofing (Laudon & Traver, 2008) is easier on the Internet. Spoofing can be done by cyberpiracy, and linking. The different types of spoofing are explained in figure 2.

* Address for correspondence:
Umair Ujala
BIT Noida Campus, Assistant Professor, Department of Computer Sciences
umairujala@gmail.com

Category	Description	Category Example
Pre-Purchase Decision	It is about selecting a web shop before placing a purchase order with originality confidence.	Authenticity Subcategories: Cyberpiracy, Linking
Post-Purchase Decision	It is about maintaining secure e-transactions starting from purchase order placing to the delivery of purchased goods.	Confidentiality, Privacy, Service-Level
After Market	It is about maintaining the security of information and data used during e-transaction.	Weblining (Laudon & Traver, 2008)

Figure 1. The categories of security threats in e-commerce retailing.

Category	Definition	Occurrence Examples
Cyberpiracy	It is the practice of registering domain names similar or identical to trademarks of others to divert web traffic to their own sites.	Ford Motor Co. v. Lapertosa, 2001 , Audi AG and Volkswagen of America Inc. v. Bob D'Amato, 2006, Lufthansa v. Future Media Architects, 2008, Nissan Motors v. Mr. Uzi Nissan, 2008 and Neeley v. Name Media Inc, 2009.
Linking	This is practice of linking from a web site to the content of other web site, by passing the home page.	Shetland Times v. Shetland News, 1996, Intellectual Reserve v. Utah Lighthouse Ministry, 1999, Ticketmaster v. Tickets.com, 2000.

Figure 2. The types of spoofing and the major occurrences.

The customer does not have any specific software technology to check the authenticity of the e-shop so, the customer feel insecure. Security has a positive influence on trust (Ivan K.W. Lai, et al. 2011). Trust (Jarvenpaa, Tractinsky, Saarinen, & Vitale, 1999; Gefen, 2000; Gefen & Straub, 2000; Pavlou & Chellappa, 2001; Koufaris & Hampton-Sosa, 2002) is a major factor to satisfy the online customer. Trust building with the customer has many sectors in the e-Retailing. The threshold of this trust can be set as the authenticity of the e-shop website.

How much the pre-purchase decision is affecting the customers? Is this phase so important that it is creating distrust in the customers? According to the report published by Internet Crime Control in the year 2008, 2009, and 2010 the top most registered complaint was of non-delivery of purchased goods (IC3, 2012). What could be the major reason of non-delivery of the products? The main reason of this fraud is spoofing e-shops. This is one of the major concerns in e-Retailing.

2. Defining the Problem

"To provide a technological web service (W3C, 2004) to the customer at the client side by which the customer can check the authenticity of the e-shop in the domain of e-shop itself". The customer is not needed to install additional software for the purpose as the solution is in the form of web service.

3. Designing the Solution

The solution needs a trusted third party involvement and the technique of encryption. I would like to coin a term Web Access Control (WAC) at this point. My WAC is unique serial number associated with the web address of a web site. This WAC should be prearranged from a third party with uploading of a web site so that no two web sites share the same number.

The third party will be controlling and monitoring the entire World Wide Web running on the Internet at the authenticity level. WAC will work as identification number for each website. The customer willing to check the authenticity of an e-shop will simply send a request to the third party. The third party will take the query from the customer and will return the associated result after processing the query. The query will have the encrypted WAC address of the web site about which the customer wants to enquire. The whole process can be performed as follows:

3.1 Customer Actions (CA)

CA 1. *The customer opens a website*

CA 2. *Requests for the WAC of the website in the website itself, available as a web service. A number will be returned to the customer. This number is an encrypted WAC (EnWAC). EnWAC is the exclusive encryption of the WAC of the website and a systematically generated integer.*

CA 3. *The customer takes this EnWAC and sends it to the third party as a query.*

3.2 Trusted Third Party Actions (TA)

TA 1. *Generating the WAC for each website uploaded or to be uploaded.*

TA 2. *Creating and maintaining a database for the websites.*

TA 3. *Providing a website to the people for active interaction and query processing.*

3.2.1 TA 1

To generate WAC for *n* websites; consider a prime integer '*a*' and define U_a the set of positive integers relatively prime to a. Therefore, the number of elements in U_a is exactly $(a-1)$. U_a defines a cyclic group (Herstein, 1993) under multiplication modulo *a*.

Extension of Ua: Now, define $U_a^m = U_a \times U_a \times .....\times U_a, (m$ times, where m>n) as follows;

$$\forall (x_1, x_2, ..., x_n) \,\&\, (y_1, y_2, ...y_n) \in U_a^m, (x_1, x_2, ..., x_n) * (y_1, y_2, ...y_n) = (x_1 * y_1, x_2 * y_2, ...x_n * y_n)$$

So that U_a^m defines a group.

Generating WAC: Select a sufficiently small prime integer '*b*' and define $U_b$to form a group. Extend $U_b$to U_b^n by the above mentioned method. A one-to-one mapping $t: U_b^n \to U_a^m$ gives the EnWAC. $t(u_b^n) = u_a^m \in U_a^m$ is the code visible to the userv and $u_b^n \in U_b^n$ is the private code of the website.

Decoding: Define an onto function $r: U_a^m \to U_b^n$ such that $r(u_a^m) = u_b^n$ that is $r(t(u_b^n) = u_b^n)$ which is a sufficient method to decode the EnWAC.

Corollary: If the result holds good for $r: U_a^m \to U_b^n$ then it holds for $r: U_a^{m+1} \to U_b^{n+1}$ also, $\forall m, n \in \mathbf{Z}^+$.

With the help of the corollary *m*, *n* can be increased into infinitely large numbers to create WAC for an infinite number of websites.

Performance Analysis:

Uniqueness: $\forall, u_a^m = (x_1, x_2, ...x_n) \in U_a^m$ is unique. Let us suppose, two distinct elements $u_a^m, v_a^m \in U_a^m \ni u_a^m = v_a^m$ Therefore, $u_a^m * (v_a^m)^{-1} = 1_{U_a^m}$(identity) but $u_a^m * (u_a^m)^{-1} = 1_{U_a^m}$ So, u_a^m has two inverses which is not possible in a group. Hence, $u_a^m \neq v_a^m$

Secure: Since both '*a*' and '*b*' remains private so only a brute force method can be used to find out '*a*' and '*b*'. The time taken is sufficiently large to lose the interest even on the fastest available computer processor.

Running Time: The entire calculations can be performed in a polynomial time.

3.2.2 TA 2

In this component, indexing method can be considered a suitable method to maintain the database. An index file can be created upon two fields EnWAC and WAC. The datbase file containing the entire information is kept separate. A one-to-one mapping in between index file and database file will be used for the efficient data storage and data processing. Indexing is justified, as the huge number of data is required to be maintained. A typical index file and database file is described using figure 3.

(DName: Domain Name, OrgName: The name of website owning organization, OrgAdd: The address of the organization, OrgFunc: The area of functioning of the organization)

The index file is sorted on EnWAC and the database file is sorted on WAC to reduce the total searching time.

3.2.2 TA 3

A dedicated website of the trusted third party is needed to provide an interface to the customer to check the validity. After reading the EnWAC the customer will open the website and submit EnWAC as query. In the server side activity the EnWAC supplied by the user will be matched with the EnWAC in the indexing file. If found the index file mapping will return the result from the database file. Otherwise, an error message will be displayed.

4. Linking Prevention

Now, linking prevention is an easy task with the use of WAC by introducing an additional element in the URL connecting function. For example, if HTML is used for the website creation language then anchor element (Morrison, 2001) creates a link with another page. The sample linking in HTML can be of the form <***a href =''http://www.example.com''***> where, ***href*** is an anchor attribute and short form of hypertext reference. The anchor tag has many attributes like, name and target etc. The tag is capable to link internal pages as well as external pages or the contents of pages. The <*a*> tag alone is not capable of doing anything. The external linking can be prevented just by introducing a mandatory attribute for incorporating WAC. If the linking reference is restricted upon the same WAC the external linking will not be possible.

In fact, this technique will prevent the mutually agreed union of two websites also. To overcome with this problem one more optional attribute to <*a*> for composition of WACs can be added. This composition will be upon the binary operation upon which the WAC is created. A WAC being a member of U_b^n the composition will also be a member of U_b^n not assigned to any other website and will have a valid tuple available in the database file. This tuple may be filled with the website union information or with the primary website information.

5. Conclusion

In this paper, I propose a mechanism to retain the authenticity of the websites with the help of a trusted third party. The entire mechanism is independent and secure. The mechanism is not only capable to check the authenticity but also provides an efficient method of linking prevention. The mechanism can be used

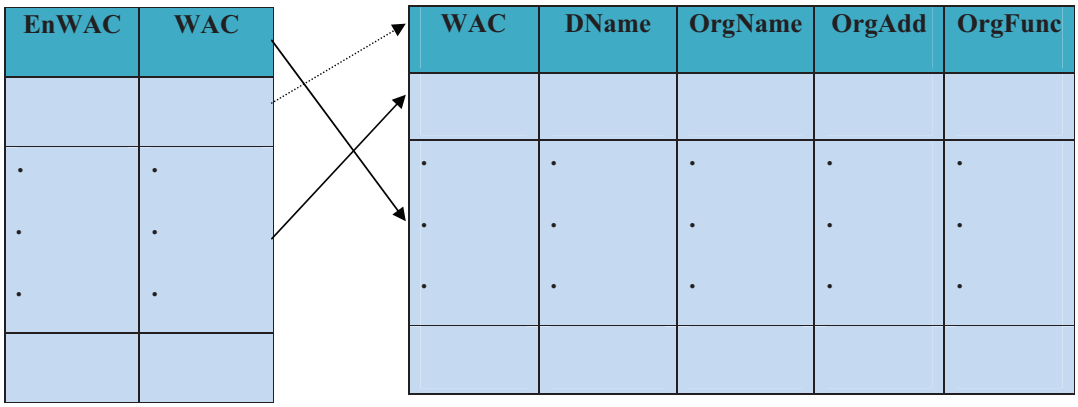

Figure 3. A typical database table design to store the website information.

in the pre-purchase security of the e-commerce retail. This will be an added advantage for the customers and a trust building factor in the pre-purchase decision.

References

Evans, P., & Wurster, T. S. (2000). *Blown to bits: How the new economics of information transforms strategy,* Cambridge, MA: Harvard Business School Press.

Gefen, D. (2000). E-commerce: the role of familiarity and trust. *Omega: The International Journal of Management Science, 28*(6), 725–737.

Gefen, D., Straub, D. (2000). Managing user trust in B2C e-services. *e-Services Quarterly*, *2*(2), 7–24. doi: 10.1353/esj.2003.0011. Retrieved January 4, 2003, from http://www.lebow.drexel.edu/gefen/eServiceJournal2001.pdf.

Herstein I. N. (1993). *Topics in Algebra* (2nd Ed.). New Delhi: Wiley Eastern Ltd.

Internet Crime Complaint Center, IC3(2012). *Internet Crime Report*, USA, Retreived February 13, 2012, from, http:// http://www.ic3.gov/media/annualreports.aspx.

Jarvenpaa, S., Tractinsky, N., Saarinen, L., Vitale, M. (1999). Consumer trust in an Internet store: a crosscultural validation. *Journal of Computer-Mediated Communication*, *5*(2). doi: 10.1111/j.1083–6101.1999.tb00337.x.

Khan, D., Varshney, P., & Qadeer, M. A. (2011). E-commerce: from shopping carts to credit cards. *2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN)*, 81–85.

Koufaris, M., Hampton-Sosa, W. (2002). Customer trust online: examining the role of the experience with the Web-site. *CIS Working Paper Series, Zicklin School of Business, Baruch College*, New York, NY. Retrieved December 23, 2011, from http://cisnet.baruch.cuny.edu/papers/cis200205.pdf.

Lai, I. K. W., Tong, V. D. L., & Lai, D. C. F (2011). Trust factors influencing the adoption of internet-based interorganizational systems, *Electronic Commerce research and Applications*, *10*(1), 85–93.

Laudon, K. C. & Traver, C. G. (2009). *E-commerce: business, technology, society***.** (4th Ed). Delhi: Pearson Education.

Morrison, M. (2001). *HTML and XML for Beginners*. New Delhi: PHI.

Pavlou, P. A., & Chellappa, R. K. (2001). The role of perceived privacy and perceived security in the development of trust in electronic commerce transactions. Submitted to the Special Issue of *Information System Research on* "Electronic Commerce Metrics", *11*, 18–36. Retrieved October 31, 2002, from http://www-scf.usc.edu/Btis/eBizLab/ Papers/secpriv-isr.pdf.

W3C, *Web Services Glossary.* (2004). Retrieved March 15, 2011 from http://www.w3c.org.