Kurdistan Journal of Applied Research (KJAR) | Print-ISSN: 2411-7684 – Electronic-ISSN: 2411-7706 | kjar.spu.edu.iq
Volume 2 | Issue 3 | August 2017 | DOI: 10.24017/science.2017.3.9

Security Aspects in Online Purchasing Applications

Kanar R. Tariq
IT Dept.
Technical College of Informatics
Sulaimani Polytechnic University
Sulaimani, Iraq
kanar.tariq@spu.edu.iq

Ribwar Bakhtyar
IT Dept.
Technical College of Informatics
Sulaimani Polytechnic University
University of Human Development
ribwar.ibrahim@gmail.com

David I. Forsyth
Light wave Communication
Research Group (LCRG), Faculty of
Electrical Engineering,
Universiti Teknologi Malaysia
david_i_forsyth@yahoo.com

Riyam A. Johni
Computer Science Dept.
Kurdistan Technical Institute,
Sulaimaniyah, KRG, Iraq.
riyam.alaa@kti.edu.krd

Abstract: ***Motivations to engage in retail shopping comprise both utilitarian and hedonic dimensions. Business to consumer e-commerce conducted via the mechanism of web-shopping offers an expanded opportunity for companies to create a cognitively and esthetical good shopping environment in ways not readily imitable in the no electronic shopping world. In this report the details key implementation aspects of a typical online purchasing system, hypothetically labeled SYSTEM X, and describe how it works - particularly regarding security issues. The report concludes with recommendations for users of similar online buying systems.***

Keywords: e-commerce, online shopping, security in online shopping, retail shopping.

1. INTRODUCTION

Day by day E-commerce role growing and become more significant in online retail marketing and people using this technology day by day greater than ever all [1]. E-commerce is the mechanism of purchasing and retailing of products or services over electronic systems such as the internet and, to a lesser extent, other computer networks.

By growing in strength of worldwide web a great opportunity is provided for companies and customers to do their business in real time and straightly. Business to business and business to customer are the results of such a technology that provides people to react very fast. In this situation both international and local transactions seem to be perfect applicant to make the order and finish the transactions in a fast process.

It is generally regarded as the sales and commercial function of e-business. There has been a massive increase in the level of trade conducted electronically since the widespread exponential growth of internet traffic. A wide variety of commerce is conducted via e-commerce, including electronic funds transfer. While the design, ease of use, interactivity, and use of technology, innovation and content are all important criteria for the website of any online retail organization, they all require effective security to protect their operations [1].

E-commerce security is generally defined as the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. While security features do not guarantee a secure system, they are necessary to build a secure system. Given numerous recently reported lapses within this area for example, Talk Talk, Marks and Spencer, one would be forgiven into thinking this was just a minor requirement. However, obtaining the correct balance between ease of use and water-tight security is now a real and crucial on-going issue in modern times. Nowadays most people are seeking for new ways in which they can make their shopping simple and fast and, of course, in a secure manner. So they desire to do their shopping quickly, without any concern about the price or quality. Thus, e-shopping is an important option for them. Buyers can order a great variety of goods through internet [2].

Online customers want quick and easy purchases, without being asked for timely and cumbersome requests. Also, considering that most online customers actually end up completely uncompensated from the banks in security breaches, they want ones that are as financially secure as face-to-face transactions are.

With increasing popularity of online shopping has been went along with by expanding anxiety about Internet security. In fact, top reason for avoiding online shopping is the consumer’s concerns with security, this is revealed by many consumer surveys [2, 3].

This report details key implementation aspects of a typical online purchasing system, hypothetically labeled SYSTEM X, and describes how it works - with particular reference to security issues. The report concludes with recommendations for users of similar online buying systems.

The paper is organized as follows: In Section 2, we present a way of working of the proposed system. Section 3 describes the architecture of the system and dataflow. Security analysis is discussed in Section 4. Conclusion discussed in section 5 and explains suggestions for future work.

2. HOW THE APPLICATION RUNS

The new user needs to be sufficiently impressed to use and trust the application on a continual basis. SYSTEM X therefore works in the usual way. The preliminary login ritual is met with a plethora of user-friendly questions and commands - all tailored to ease the pain and decrease the time involved in first-time registration: full name, creation of password and useable e-mail address. This process culminates in the customer selecting his/her preferred method of payment, and then giving the details of such (credit/debit card, or PayPal). In all further usage, only a username (user e-mail address) and the chosen password are required to log in and start buying. Individual purchase selection is made simply by locating and clicking on a chosen item from the menu each time.

After finishing the shopping, the user can then venture towards a virtual checkout to complete the buying process and meet the accumulated bill. If in agreement, the process is then swiftly and effectively completed. Home page, subcategories page, items page, item details page and buy page are the objects of interest.

3. ARCHITECTURE AND DATA FLOW

Figure 1 shows how data moves within SYSTEM X, using a high level data flow diagram. The process is given the number zero. All of the external entities are displayed on the context diagram, as are the major data flows to and from the system. The interactions between the buyer and seller are clearly shown. The buying process is systematically achieved by six basic streams of information - three requests and three answers.

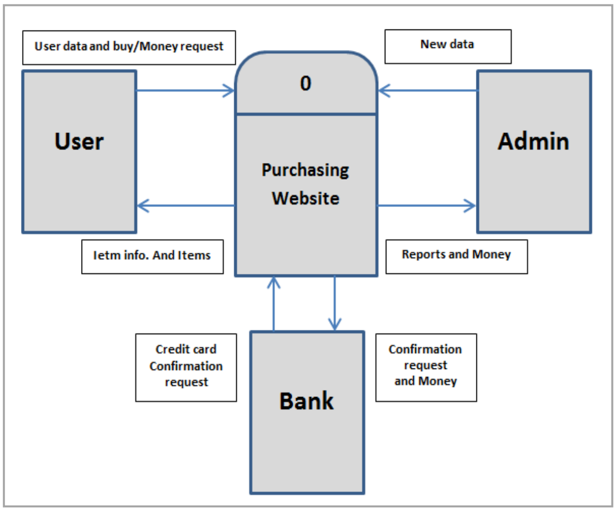

Figure 1 High level data flow chart for online purchasing [3]

The online customer can browse or search items, view a specific item, add it to the shopping cart, view and update shopping cart, then checkout. The user can view the shopping cart at any time. Checkout includes user registration and login. A credit card transaction request is submitted to the credit card payment gateway on behalf of a customer. The bank which issued the customer's credit card can approve or reject the transaction. If transaction is approved, funds will be transferred to SYSTEM X's bank account.

4. SECURITY ANALYSIS

To be forefront in e-commerce, you need to recognize how to make the best utilize cryptography to offer secure services for your customers over the Internet [4].

McCole, Ramsey, et al. (2010), stated that the internet trust is the most influential element of the three e-commerce trust considerations (vendor, Internet, third parties) on attitude towards online purchasing. They claimed that the relationship between trust in Internet and attitude towards online purchasing weakens when people have higher privacy and security concerns [5].

The key security issue areas to consider are communications, end systems and the network. Security of Communications requires confidentiality - no “eavesdropping”, no unauthorized access to information, encryption and digital signature. Data Integrity requires no unauthorized manipulation of information. The recipient receives data identical to what the originator sent, and the originator cannot claim fake identity. There must be guaranteed delivery of messages, and any intruder should not be able to remove messages completely. Security of End Systems requires control over access to confidential data, e.g. leaking of credit card account information, manipulation of data and changing or deleting information.

The system must not be changed – no manipulation of configuration authorization or account information, no unauthorized running of programs and no import of foreign (malicious) programs. Denial of Service (DoS) attacks can cause system overload, or it to hang or crash. Security of the communication network requires no unauthorized network usage for example, using the network without paying. There must be no modification of the network configuration for example, change of DNS entries, or change of routing information.

Security can be improved by several useful data manipulation methods: effective encryption, employing digital signatures, signature checking on configuration files and programs, and packet or protocol filtering. Physical methods to achieve this can include utilizing access control, having an effective back-up strategy and separating networks and utilizing hosts without network connectivity. Logistical methods may include auditing and log evaluation, the creation of double passwords and appropriate selection of the operating personnel. For confidentiality and integrity issues, include cryptography (encryption) for authentication means, symmetric or asymmetric key cryptography.

A digital signature will always check the integrity of the data, as well as check the identification of the originator. The system should be firewalled, and intrusion detection should have logging and auditing, as well as the checking of logs. There should be alarm generation and notification, automatic effect recognition and pattern recognition. Also, always restrict system administrator access to ensure traceability of actions. Do not allow anonymous administrator access, e.g. force the use of tools like “su” or “sudo”, install security patches against buffer overflows, and have state-of-the-art system scanning. Internet security frameworks should have a clear definition of key formats and selection of algorithms. Protocols should have key exchange and key management. Also, there should be different frameworks for authentication (login), network, transport and application layer security. Another technique or system that can be used in e-payment is PRETTY GOOD PRIVACY (PGP) is more reliable to use in e-commerce which provides a confidentiality and authentication service [4].

Security statement is another way to help consumer to perform e-payment properly as it can be posted in e-payment sites. Security statements are information and quick guide that give the consumer a proper knowledge in terms of EPS operations and security solutions. Posting security statements in e-payment sites is another important step [6-8].

Users themselves can improve on security, regular changes of password (made complicated with special characters, and having upper and lower case letters), deletion of credit card details after purchasing, choosing a shopping cart that records IP in the admin and store section, shopping at secure websites only, being more aware of cookies and marketing techniques, checking the URL of the website, having knowledge of exchange rates and applying security patches to the shopping cart are all sensible and viable ways.

5. CONCLUSIONS AND RECOMMENDATIONS

Based on the foregoing, designers and users of systems like SYSTEM X can benefit by addressing security issues in a different light. Of course, there is no such existence of absolute security. Most, if not all, intruder techniques have a residual error probability, and can be made arbitrarily small (but never zero). For example, the chance of guessing a parity bit correctly is 0.5, and there is also a good chance of manipulating an original text to fit a given 10 bit digital signature. Also, “brute force” attacks will always remain. These crude methods of intrusion have little or no knowledge of security mechanisms, and simply rely on probability, e.g. (parallel and distributed) the cracking of encryption keys. The intruder tries every possible key until he/she can actually decrypt the message, or tries every possible password until it matches the encrypted text.

Also Security can be enhanced by several useful data handling methods: effective encryption, employing digital signatures, signature checking on configuration files and programs, and packet or protocol filtering. Physical methods to achieve this can include utilizing access control.

Pretty Good Privacy (PGP) technique that can be used in e-payment, it is more reliable to use in e-commerce which provides a privacy and authentication service.

Finally Users themselves can improve on security by even changes of password for example (made complicated with special characters, and having upper and lower case letters) or can prevent owner account by applying the necessary new techniques for purchasing.

4. REFERENCE

[1] M. Niranjanamurthy, N. Kavyashree, S. Jagannath, and D. Chahar, "Analysis of e-commerce and m-commerce: advantages, limitations and security issues," *International Journal of Advanced Research in Computer and Communication Engineering,* vol. 2, 2013.

[2] D. L. Hoffman, T. P. Novak, and M. A. Peralta, "Information privacy in the marketspace: Implications for the commercial uses of anonymity on the Web," *The Information Society,* vol. 15, pp. 129-139, 1999.

[3] E. Hartono, C. W. Holsapple, K.-Y. Kim, K.-S. Na, and J. T. Simpson, "Measuring perceived security in B2C electronic commerce website usage: A respecification and validation," *Decision Support Systems,* vol. 62, pp. 11-21, 2014.

[4] N. M. Al-Slamy, "E-Commerce security," *IJCSNS,* vol. 8, p. 340, 2008.

[5] P. McCole, E. Ramsey, and J. Williams, "Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns," *Journal of Business Research,* vol. 63, pp. 1018-1024, 2010.

[6] A. S. Lim, "Inter-consortia battles in mobile payments standardisation," *Electronic Commerce Research and Applications,* vol. 7, pp. 202-213, 2008.

[7] A. Mukherjee and P. Nath, "A model of trust in online relationship banking," *International journal of bank marketing,* vol. 21, pp. 5-15, 2003.

[8] M. J. Cotteleer, C. A. Cotteleer, and A. Prochnow, "Cutting checks: challenges and choices in B2B e-payments," *Communications of the ACM,* vol. 50, pp. 56-61, 2007.