SECURITY ISSUES IN E-COMMERCE AND THEIR SOLUTIONS

Nishi Sharma (M.com, SD College Ambala Cantt,
Email: sharmanishi209@yahoo.com)
Kajal Chauhan (M. Com, SD College Ambala Cantt,
Email: chauhankajal4334@gmail.com)

Abstract
E-commerce basically means buying and selling of goods over the internet. E-commerce include M-commerce which means mobile commerce i.e. performing online transactions through mobile device. With the increase of accessibility of E-commerce, there increases the security issues. This study analyzes various security issues in e-commerce and efforts are made to find solutions to those security issues. A number of threats are there which are imposing on buyers while making online transactions, customers started having trust issues with online payment, if security issues are not resolved then this may cause a deep impact on the future of E-commerce. But some solutions are also there which can prevent the losses occured from these issues.

Introduction

E-commerce business has widen itself to a great extent. Its service area has widely developed but security is the element it lacks. Security relates to the details of bank accounts, personal information or any other data of end users. Due to these security issues, many people feel unsafe while dealing online, they hesitate making payments online. Security issues should be the main concern of E-commerce companies as it is hindering the way of these companies towards success. This study is mainly concerned with the security issues in B2C (Business to Customer) transactions. Customers facing these issues can affect E-commerce industry to a large extent. Nowadays, due to increased dependency on mobile phones, the growth of E-commerce has expanded their selling activities through smart phones, which is commonly known as 'M-commerce'. Thus, M-commerce has widen the scope of E-commerce, increased the number of users and hence their security issues. Further, the solution to these security issues is also studied; many softwares and techniques are there for this purpose.

Review of literature

Sibo prasad Patro, Neelamadhab Padhy, Rasmita panigrahi, vol 5, issue 12 (Dec 2016) Dimensions of E-commerce security are explained: Integrity, No repudiation, Authenticity, Confidentiality, Privacy, Availability. Three types of security threats are mentioned, which are: client threats, communication channel threats, server threats. This paper studied E-commerce through various aspects including life cycle of digital E-commerce, security issues and guidelines to secure online shopping.

Panagiota Papadopoulou, Drakoulis Martakos (2008) Online trust is multidimensional concept. This paper provides a comprehensive review and categorization of empirical and theoratical literature and studied Online Trust as how trust is treated at conceptual and empirical level. At theoretical level, trust should be clearly defined and at empirical level, it should be maintained at operationalization.

Randy C. Marchany and Joseph G. Tront (2002) studied the efforts of E-commerce industry towards security issues and concluded that E-commerce industry is slowly addressing security issues on their internal networks. There are many guidelines for securing systems and networks available for the e-commerce. Awareness among people is still in its infancy stage, not everyone who is dealing online is aware of the issues involved in transacting.

Niranjanamurthy M, DR. Dharmendra Chahar (July, 2013) In their study, they analyzed security threats of e-commerce in detail using diagrams and gave suggestions against these threats.

Dr. Pranav Patil (Jan, 2017) gives information about various types of attacks on consumer as well on e-commerce dealer. Various solutions regarding those attacks are also given. The paper concluded that current technology permits the secure web transactions.

Seyyed Mohammad Reza Farshchi, Fariba Gharib, Reza Ziyaee (2011) In e-commerce security solutions, this paper contains the information about P2P e-commerce. Effective trust models in P2P e-commerce are explained, which are user friendly.

Objective of Study

- To throw light on Security Issues in E-commerce
- To find solutions to these issues

Security risks Currently faced by Customers

Credit card fraud

Many transactions in E-commerce payments are made using credit cards. Problem arise when hackers hack the card information from websites by using malicious softwares and use that information against the customer. According to Nilson Report (Dec 2016) Global Card Fraud will Reach $43.8B in near future.

Distributed Denial of Service (DDoS) Attacks

A denial-of-service attack (DoS attack) is a security attack in which the attacker takes action that prevents the legitimate (correct) users from accessing the electronic devices. It makes a network resource unavailable to its intended users by temporarily disrupting services of a host connected to the Internet. When a DDOS Attack hits the server, it may result in slow down or completely shut down the server.

SMS Spoofing

SMS Spoofing is phishing from fake websites and message spoofing from unscrupulous elements. Under this, Customers who are always in search of offers get message from some fake website claiming that they can avail those attractive offers by clicking on the link, later on even after paying the whole amount in advance they don't receive their order and that payment goes to the hacker.

Computer Virus

Virus is small software that can spread from one infected computer to another. A virus can spread even after deleting everything from hard disk. Virus can affect every transaction executing from the infected computer.

Malware Softwares

Hackers use these malfare softwares to gain access to online retail stores. These softwares easily steal the data stored in website's software.

Call spoofing

By showing wrong number on screen and by changing voice, hackers manipulate the local public in many ways. For example: acting as delivery person they deliver wrong products and collect payments.

Spyware Threats

Spyware is a program that monitors online activities and install programs for profit or to capture personal information without the consent of buyer.

Solutions and suggestions for Security

Using HTTPS

Outdated HTTP protocol is more vulnerable to hackers and attacks. Using HTTPS protocol there will be a security against these risks, this protocol displays a green lock sign that says 'secured' mext to url. Also, by using HTTPS a website shows in higher ranks in Google Search since google consider HTTPS as a ranking factor.

Using secure panels

Most of the e-commerce platforms work with passwords that are very easy to guess. So if websites are operating with these kind of passwords and do not change them frequently then they are offering themselves to hackers. To secure website from hackers, it is advised to use complex passwords and also change them frequently.

Using Anti-viruses and anti-malware softwares

Viruses can spread customer's private information. Using anti-viruses E-commerce portals can secure their information and data. Anti-malware softwares can help dealing with malware software that cause threat to online transactions.

Encryption approach

Websites can use encryption method to hide the details of transactions. This method converts the information in secret code which is difficult for the hacker to decode. Transactions are end-to-end encrypted, no mediator can access through the information.

Secure socket layer

SSL is a networking protocol by which server client information is authenticated, data transmission is encrypted.

Safe login screen

The very first stage i.e. login screen, should made safe. By making a safe login screen it will be easy for the users to stay secure from hackers.

Monitor suspicious purchasing activities

Website owners must monitor every suspicious purchasing activity. Large amount orders or large purchases from same address using different credit cards can be a cause of concern for the owner. This is moral duty of owners to check that the card used by customer actually belong to them or not.

PCI Compliance

Payment Card Industry Security Standards Council formed in 2006 is a compliance that completely secures the payment system. This compliance monitors the online financial data of customers and secure payments.

Training employees

Training employees include teaching them values to keep their customers login credentials confidential. Employee should be aware of all the regulations related to keeping customers secure.

Educating clients

Customer must be aware of sms spoofing. They should check the authentication of those links send through texts which displays duplicate website. Also, passwords used by them must be strong in order to protect themselves from hackers. Awareness can be created in them for using anti-virus softwares and avoiding login from different devices.

Conclusion

E-commerce provide a good platform to save time through online shopping. But it includes a lot of security issues which are threatening online buyers. The payment system is the most critical part of e-commerce security because most of the crimes are related to payments. Credit card theft, data leaking, misuse of information etc are the common issues faced these days. Although, E-commerce platforms are taking steps to provide protection to their clients from hackers and other issues through a number of ways. A lot of softwares and precautions are there which are used by servers to protect against those malpractics.

References

1) Randy C. Marchany and Joseph G. Tront-- Proceedings of the 35th Hawaii International Conference on System Sciences-2002
2) Panagiota Papadopoulou, Drakoulis Martakos, Research paper - "Trust in e-commerce: Conceptualization and operationalization issues" (2008)
3) Sibo prasad Patro, Neelamadhab Padhy, Rasmita panigrahi, vol 5, issue 12 (Dec 2016)
4) Nilson Report; issue 1118,October 2017
5) Article by Alexander Menzheres,April 06,2018
6) Article by Advocate Prashant Jhala (cyber lawyer, Mumbai)
7) Niranjanamurthy M, DR. Dharmendra Chahar, july 2013
8) Dr. Pranav Patil, International Journal of Computer Science and Mobile Computing, Vol.6 Issue.1, January- 2017, pg. 100-102 Research Paper- "Study on E-Commerce Security Issues and Solutions"
9) 2011 International Conference on Software and Computer Applications IPCSIT vol.9 (2011) © (2011) IACSIT Press, Singapore