Security Vulnerabilities and Possible Prevention Measures for Ensuring the Information Security of E-commerce

[1]Sabrina Tasnim, [2]Arifur Rahaman, [3]Md Salehin Ferdous Kader
[1]sabrinatasnim.cse@gmail.com, [2]ar.arifbd65@gmail.com, [3]princemahin4@gmail.com
[12]Lecturers, Department of Computer Science and Engineering, Sonargaon University, Dhaka, Bangladesh.
[3]Assistant Professor, Department of Electrical and Electronics Engineering, Fareast International University, Dhaka, Bangladesh.

Abstract— These days in almost every aspect and things of life is transforming into electronic, likewise, changes in trade are also eye-catching as it is becoming more electronic rapidly. Roughly, activities which are related to commerce have been adopting E-dependent system to allow consumers for more easy consumption of service in a short time and have better experience. Shortly, when transaction and trading activities are made through the electronic medium, then it is termed as e-commerce. In this system, everything is being happened Over-the-Air (OTA). Moderately, demand for e-commerce is going high as it is becoming a more popular way to do business activities over the available Internet. Since client personal credentials are needed for most online transactions; it is subject to a considerable risk of hacking or leakage. If security risks are not tackled properly, customers will lose their faith gradually. In consequence, they will not use e-commerce sites at the expected level in the long run. Therefore, ensuring of security for e-commerce sites is being an inevitable issue. In this paperwork, we focus on security vulnerabilities and possible prevention approaches for ensuring the information security of e-commerce.

Keywords— CIA, CTG, E-commerce, OTA, Wi-Fi, Password, Hacking, Cryptography, SSL, PCI

1 Introduction

E-commerce (Electronic-commerce) means to do business over the Internet. Chen and Dhillon have defined e-commerce as "the transaction of goods and services over the internet "[1]. E-commerce involves but not limited to buying & selling products, goods, and services online, exchanging business-related information, supply-Chain related activities and so on. Nevertheless, any kind of trading or transaction involves a lot of information to exchange in order to fulfill whatever the purpose of the trading. This information includes sensitive personal information like credit card number, personal detail, and banking documents, product's confidential information, confidential business conversation and information and many other things like these. So, the most critical point comes to mind at the very first is the reliability of the system, in other words, the security of e-commerce system. Nevertheless, an e-commerce system includes many entities to fulfill the transaction cycle which starts with consumers needs and ends up with the successful trading according to the criteria. So, this e-commerce system needs a full IT infrastructure which includes a thin or thick client, a suitable server system, databases & user interaction media. So, there are a lot of tiers where the confidential information is to go through, in consequence, do a lot of points exist where this information can be stolen or manipulated to fulfill any illegal purpose. Thus, the most important thing to consider is the security aspects of an e-commerce system. In this very article, we will try to show several security considerations and loopholes which can go detrimental in any nodes from client to server system those e-commerce industries are facing and also depict some way-out to get rid of those security vulnerabilities.

2 Purpose of E-commerce Study

This research work is based on the impacts of e-commerce security. We will also discuss different types of security issues and how to solve the data leakage problem in this paper. E-commerce security affects the end user through their daily payment interaction with business. The primary aim of this research is to find prevention measures to mitigate data leakages and partly go through the following aspects:

- Study the overview security of e-commerce
- Security of online payments
- Discuss various issues in e-commerce

3 Problem Overview

The primary concern of this paper is to locate a superior way that is more secured while purchasing or offering items or products over the web. Protection has turned into a notable concern for buyers with the ascent of data fraud and pantomime, and any worry for shoppers must be dealt with as a remarkable concern for web-based business suppliers. Through a superior analysis process, we have to overcome from all the issue, for example, payment issue, the security risk of both customer and purchaser.

4 Purpose of Security

Data Confidentiality – is provided by encryption or decryption.
Authentication and Identification – ensuring that someone is who he or she claims to be is implemented with Digital Signatures.
Access Control – governs what resources a user may access on

the system. Use valid IDs and passwords.
Data Integrity – ensures info has not been tampered with. Is implemented by message digest or hashing.
Non-repudiation – not to deny a sale or purchase

5 Related works

Security is always the burning question for any online systems, especially for e-commerce systems. Though technologies are developing with passing time, still eye-catching development is far away from the expectation level. So, security vulnerability of e-commerce system is increasing day by day instead of decline. Many research works have been undertaken regarding the security issues and their possible solutions and still development is underway to reduce some problems. Biswajit Tripathy and Jibitesh Mishra worked on protective measures to deal with security threats arising out of social issues in e-commerce [10] and another researcher, Abdulghader.A. Ahmed Moftah, suggested challenges of security, protection, and trust on e-commerce [9]. In addition to these, Shazia Yasin and Khalid Haseeb studied cryptography-based e-commerce security [8].

6 Most common mistakes committed by users

Novice blunders submitted by the clients while occupied with on the web exchange help the fraudsters to take its fullest points of interest. There are a plethora of such mistakes makes the e-commerce vulnerable these days. Some of them are mentioned below:

6.1 Shop through Unreliable Websites

While browsing social media or other internet contents, we often get many types of advertisements as a popup from different kinds of sites showing product purchase suggestion with varying kinds of tempting offers. In many cases, those turn out to be not actual websites when users get tempted or curious and click on those websites it may hack user's personal information through various techniques. This way many unreliable and unauthenticated websites hack user's personal and valuable information and use them for various dishonest intentions.

6.2 Divulging or Allow to Know Extra Individual Data Which Isn't Required

We often see many app, game, quiz and many other interaction contents especially on social interaction websites where those contents ask extra personal information and sensitive data like password, email addresses. When users give that information by being deceived and ignoring the possible implications of that information, users most often get themselves into trouble like account hacking or using personal information and preferences to use them in a different context without letting the account holder have any sort of idea about what is going on in the background.

6.3 Downloading Insecure Software Means Leaving PC Open to Virus

Downloading soft wares which are not authenticated or curated while not using antiviruses users often let different types of viruses to intrude into PC and getting personal information, hacking the system or crashing/erasing valuable information.

6.4 Using Weak or Common Password

Using weak or common passwords like "password", "123456" and so on, can make the hackers' lives easy by giving them the privilege to hack the system without putting much effort due to the weakness and vulnerable passwords. So, it is often suggested to use passwords with complex and irregular words, a combination of words, numbers and special characters to make it very difficult for any hackers to decode and breach through the system.

6.5 Browsing Unnecessary Links

Links which do not have any necessary contents or users do not have anything to deal with often direct them with unwanted implications and take users personal information in turn. So, it is always suggested not to browse any unnecessary contents just out of the curiosity can lead users to different types of unwanted implications

6.6 Avoiding Security Queries

In addition to passwords, it is always preferred to add security steps like "one-time password" in mobile numbers or any extra security questions to be answered prior to entering the websites so that if hackers decode the password as well they do not get access to the accounts. Not using these types of security steps sometimes lead users to get compromised due to not having information immediately to the hacking occurrence.

6.7 Insecure Mailing Habits and Answering Phishing Emails

Often, we reply to many unnecessary spam mails without validating the legality of those email addresses which gives spammers a way out to access personal and sensitive contents and information. So, it is always suggested to verify the sender's information through cross-checking over those.

6.8 Not Enabling a Firewall

The enormous numbers of computer users do not enable their system's firewall which in consequences it causes many problems such as virus can affect their system easily and a hacker can get access to their system with less effort.

6.9 Procrastinating to Update Anti-Virus Software

Whenever antivirus soft wares make any updates there must involve identification and modification of loophole(s) and security vulnerabilities or updating protection scheme for protecting from any new types of threats. So, whenever any antivirus comes up with an update appears, users should promptly update that in order to make pc and hence personal information remains secure.

6.10 Making Transaction While Using Public Wi-Fi

Public Wi-Fi is accessible to hackers as it does not have any password protection, though it is not the usual case. So, using the network hackers may get remote access and butt in the system while any financial or other kinds of transactions are being made.

6.11 Leaving Webcam Turns On

In many ways, a hacker may use this webcam for their own intentions. They may monitor one's behavior and activity and most importantly may trace user's password using for the system or other online platforms.

6.12 Not Enabling User Account Control Features

Another vulnerable situation user creates by not enabling user account control feature on the system itself. In turn, allow a trespasser to enter the system without having any trouble or getting access to user valuable information.

7 Robust Security Requirements in E-Commerce

To operate a business effectively we have to make a protected domain for both shopper and business visionary, the huge increment in the take-up of e-commerce has prompted another era of related security threat, and however, any e-commerce framework must meet some essential requirements or necessities. Protection of security begins with the preservation of the confidentiality, integrity, and availability (CIA) of data and computer resources [2]. These three tenets of information security are sometimes represented in the CIA triad as below.

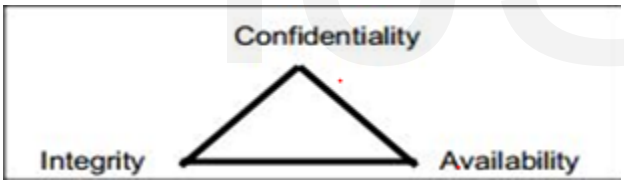

Figure 1: The CIA Triad [3]

Including the elements of the CIA Triad, the six security needs in e-commerce are as follows:

7.1 Authenticity

The genuineness check is a procedure which plans to confirm the accuracy of the claim of a client that possesses a particular character in order to avoid cases of digital pantomime. Control of the client performed before starting any exchange and executed utilizing diverse innovations.

7.2 Authorization

The online business exchanges approval prepares significantly affects chance, client benefit, and operational costs. An exchange performed by utilizing a payment card to decide of the cardholder has adequate finances for payment of a given exchange. An approval will take just seconds, and enables the vendor to guarantee that payment will be taken from the card. Executing the accompanying accepted procedures will guarantee that it is overseen successfully and will keep your chargeback level low:

Focus on misrepresentation aversion

- Use the right Electronic Commerce Indicator (ECI) for all online business exchanges.
- Obtain another approval if the first one lapses.

7.3 Assurance

Assurance is a major term in the e-commerce system due to its accomplishment of commitment. A platform like e-commerce needs to gain their customer's trust through supplying its uninterruptable service and providing it on times. In addition, better quality of the provided service or products needs to be also assured to draw the attention of the valued customers. Importantly, what they are getting and seeing has to be properly matched to make sure of quality full products.

7.4 Confidentiality

Confidentiality is generally identical to protection. Measures attempted to guarantee secrecy are intended to keep precise data from contacting the wrong individuals, while ensuring that the correct individuals can in certainty get it: Access to particular account must be limited to those granted to see the information being referred to. It is normal too, for information to be categorized by the extent and kind of jeopardy that should be probable, should it identify as unintended hands. Pretty much stringent measures can then be executed by those classes.

7.5 Integrity

Integrity includes keeping up the consistency, precision, and dependability of information over its whole life cycle. Information must not be changed in transit, and steps must be taken to guarantee that information can't be modified by unapproved individuals. These measures incorporate document authorizations and a client gets to controls.

7.6 Availability

Availability invokes to prompt access to data, maintenance and all the more by and large to all assets of the framework when required, immediately.

8 Possible Security Solutions For Both Users And Owners To Mitigate Vulnerabilities In E-Commerce

Given the different security needs in web-based business, it is essential to present the conceivable advancements or technologies, which can secure these requirements. Here are some ways to ensure the security of the e-commerce system more as follows:

8.1 Image as password

As pattern recognition is an emerging technique to identify any object through analyzing of images, it can also be used in e-commerce sites as a security tool. While any user is asked to sign up for any e-commerce sites, he/she will get an option to select an image from existing or upload a new one as a password. It will be combined with a textual password to generate

an unbreakable strong password. During the login pattern recognition technique will be used to allow a user to get access by image matching database. In consequence, it would be very difficult for an intruder or hacker to guess the image for any particular account as there is the almost infinite number of images in the world.

8.2 Mobile Number as Third Layer Security

Apart from password and image, mobile number can be used as third layer security. Nowadays many famous internet giants, for instance, Google, Facebook, are using this approach to increase their safety. In this technique, an auto-generated code is sent to the registered mobile number during suspicious log in or a user can enable it for every login. Without this number, no one gets access to the site hence increases the security.

8.3 Email as A Security Tool

During registration process user email address need to be mandatory in this approach. If it does so, it would help to send every suspicious activity to an associated email address. On getting an email, a user can be aware of and take necessary measure.

8.4 One Device One Account

For any communication device, for example, mobile (IMEI), computer (MAC address) has its one unique number which is internationally recognized that can be used to permit any user to get into an account. During the registration process, the device's unique number will automatically attach to the user account. Later this account only is accessible from this device, any other access from different devices will be dynamically rejected.

8.5 One Time Password

Even though we use strong password combination most of the time, hackers may come to know that password and break into the system and accomplish something which not good for our system and customers. To avoid this situation, one way can be to use one-time password. After using one-time, this password will be automatically invalid for next time use which makes sense for increasing security at least little bit.

8.6 Secrecy

Taking necessary steps so that reading out personal messages and business ideas, getting credit card numbers, or having other secret information is not done by an unauthentic person. Whiling getting through any transaction on e-commerce system, it is responsibilities of system owner to make sure; there is no likelihood of unauthorized data access.

8.7 Cryptographic tools

Cryptology utilizes the methods by which the plain content data is changed over in figure content utilizing different plans and strategies that can't be perused regardless of the possibility that the data is hacked. The Cryptographic Technology Group's (CTG) work in the field of cryptography includes researching, analyzing and standardizing the cryptographic technology. They have come up with some high-level security prevention as follows:

Encryption algorithms- They use a technique to convert the input text into another text which can only be returned to the original text by means of some private keys. Thus, an unauthorized user cannot access the sent data.

Hash functions- In this technique, input data is mapped into a given hash value and sending the hash value as a message, without having the original input it is too hard to get back the input message. In consequence, it provides high-level of security.

Digital signatures- They give the recipient faith that data is not altered during transit. During sending a message, it is signed by a private key and an end user can verify the message by his public key.

Digital certificates- To implement the security applications of Public Key Infrastructure (PKI), they are used by consumers and businesses. They ensure the secure transactions by various means such as e-commerce and internet-based communication.

8.8 Control Access and Authentication Protection

There must be a level of data on that the client can get to the data. Limits to the data must be characterized. On the off chance that there is a gain to control a large portion of assaults are inconceivable. The firewall can be utilized for this sort of access controls. Setting the password to delicate data can secure the information.

Some of the most common access control and authentication protections are

Password- Instead of selecting common or easily guess password strong password can be chosen to strengthen the protection of the e-commerce sites.

Biometrics- Biometrics can also be used with concern to identifying a person based on his or her physiological or behavioral characteristics. Biometrics is utilized for authentication and as a result, protects confidentiality and integrity [6].

8.9 Protection from Virus

There are various kinds of anti-virus and content-filtering software introduced in the market. There are five distinct methods identified for fighting against viruses.

- Signature scanning anti-virus software
- Integrity checking anti-virus software
- Heuristic anti-virus software
- Macro virus analyzers
- Polymorphic virus analyzers

8.10 Selecting Appropriate Platform

A lot of e-commerce businesses bank on external providers for hosting on a server, data storage, POS maintenance and processing of the payment needs. As a result, these third-party service providers cause the creation of risk or mitigating to the security of the e-commerce system. In addition to this, as far as it is concerned about e-commerce applications, any downtime puts the business at risk. PCI DSS standards must be maintained while dealing with sensitive information by service providers. Coordination with a vendor is also essential to en-

sure proper prevention, detection, adding firewalls, having anti-virus systems, high-level encryption, two-factor authentication, logical and physical access control, segmentation controls and monitoring mechanisms.
Search for a vendor that supplies the following criteria:

- Uses advanced encryption
- Maintains regular backups
- Keeps comprehensive logs
- Offers network monitoring
- Having taken down procedures and policies

8.11 PCI (Payment Card Industry) Compliant and SSL (Secure Sockets Layer) Secure Checkout

A minimum number of requirements for network and wireless security issue is required these days due to PCI compliance governance. It merely sees about the single vulnerability for any website or network to be compromised. A system must be monitored and tested frequently to ensure security as per the security policy. Tokenization, probably, can be the best option to avoid the customers' payment data rightly; hence risk is minimized considerably as sensitive information never needed to be transferred through the system. Yet there are other things to do, if the system owner is not aware of his responsibilities and unwilling to use the latest e-commerce security technology, and then work with a PCI compliance and security consultant who can

8.12 Other Ways

There are further many ways to make sure security of e-commerce as below:

- Intrusion detection
- Virtual private networks
- Firewalls
- Help for the training of employees, auditing,
- Avoid storing sensitive information
- Monitor e-commerce activities
- Back up
- Train up employees

9 Conclusion

Various direct or indirect factors have their significant impact on e-commerce security. Due to lack of taking proper security measures, nowadays e-commerce sites are facing a plethora of security vulnerabilities. There are a lot of aspects which can be applied to make sure security e-commerce sites. E-commerce is not only setting up a site and offering products on sale online; obviously, it is beyond than that. Although there will be some risks persistence always, taking necessary steps can reduce that risk a great deal.

References

[1] Bruce Chien-Ta ho and Kok-Boon Oh, An empirical study of the use of e-security seals in e-commerce. E-security seals in e-commerce, 2008
[2] C. BARNES, ET AL "Hack Proofing Your Wireless Networks", Syngress Publishing, Rockland, MA, 2002.
[3] George S. Oreku, Jianzhong Li Rethinking e-commerce Security, Harbin Institute of Technology, Harbin 150001, China
[4] https://en.wikipedia.org/wiki/Cryptography
[5] https://www.nist.gov/itl/computer-security-division/cryptographic-technology
[6] Chander Kant, Rajender Nath "Off-line Optical Frustrated Total Internal Reflection" Published in the proceedings of National Seminar on "Information and Communication Technology- Recent Advances & Applications ICT-2006 PP 237-240 Feb 09-11, 2006 at JMIT, Radaur Yamuna Naga
[7] http://www.csjournals.com/IJITKM/PDF%207-1/13.pdf
[8] Shazia Yasin, Khalid Haseeb. "Cryptography Based E-Commerce Security: A Review". IJCSI-Vol. 9, Issue 2, No 1, March 2012
[9] Abdulghader.A. Ahmed.Moftah."Challenges of security, protection and trust on e-commerce: a case of online Purchasing in Libya". issn: 2278-1021-ijarcce vol. 1, issue 3, May 2012.
[10] Biswajit Tripathy, Jibitesh Mishra. "Protective measures in ecommerce to deal with security threats arising out of social issues – a framework" iaeme -ISSN 0976 – 6375(online) volume 4, issue 1, January- February (2013)