ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

A Review on E-Commerce Attacks

R. Priya [1], J.Jayanthi [2], P. Manjamadevy[3]

PG Student, Dept. of CSE, Pondicherry Engineering College, Puducherry, India[1]

Assistant Professor, Dept. of IT, Sri Ganesh College of Engineering and Technology, Puducherry, India[2]

Assistant Professor, Dept. of CSE, Sri Ganesh College of Engineering and Technology, Puducherry, India[3]

ABSTRACT: E-Commerce is defined as the electronic commerce by which the user may buy or sell the products considered as the very vital part of any transaction not only in E-Commerce there should not be any factors which compromises the security. The acquaintance of internet and its flaw paramount the attacks which are experienced daily by the people. It is very tough to create a website without any flaw but it may be avoided and controlled by employing certain security preventive measures. This paper discuss about the various attacks that are applicable at the E-Commerce environment.

KEYWORDS: E-Commerce; Security; threats; attacks; cyber attacks

I. INTRODUCTION

E-Commerce is defined as the electronic commerce by which the user may buy or sell the products via the internet. It is a recent style of trade exchange. It comprises of paperless interchange of trade. Security is considered as the very vital part of any transaction not only in E-Commerce there should not be any factors which compromises the security.
E-Commerce Security is a portion of Information Security. Due to technological advancement and smarter way of working environment E-Commerce is very popular. E-Commerce gain its name and fame due to the terrific growth of mobile apps. Due to the globalization anyone may order any products and it reaches our doorstep in few clicks. The products that are purchased in online shopping are of lesser cost also there are freebies available nowadays which urges the customer towards it.
The types of E-Commerce are as follows [1]:

- Business - to - Business (B2B)
- Business - to - Consumer (B2C)
- Consumer - to - Consumer (C2C)
- Consumer - to - Business (C2B)
- Business - to - Government (B2G)
- Government - to - Business (G2B)
- Government - to - Citizen (G2C)

Even though it has many advantages over the traditional commerce the E-Commerce production is addressing towards the security issues, threats and cyber-attacks. Nowadays the attackers are very clever by employing the security tools that are available in the internet they are targeting the people daily with new types of attacks.

II. ELECTRONIC PAYMENT

There exists several types of electronic payment that are available on the internet.

- Credit card
- E-Wallets
- E-Cash
- Payment Card
- Micro payment systems
- Smart Cards
- Online Payment

- Mobile Payment

III. RELATED WORK

The literature work are as follows:

TABLE I. LITERATURE SURVEY

Paper Title	Author	Description	Year
E-Commerce Applications: Vulnerabilities, Attacks and Countermeasures	P. S. Lokhande et.al [2]	The increase of internet usage becomes more and more thereby the attacks also growing due to the larger growth of technology and smarter tools that are available on the internet to create the fraudulent activities. This paper explains about the vulnerabilities such as improper validation of inputs, database servers, TCP/IP, Firewalls, IPS and E-Commerce attacks	2013
The study of E-Commerce Security Issues and Solutions	Niranjanamurthy M et.al [3]	This paper explains about the security threats and how it can be prevented. Also it gives guidelines for protective online shopping	2013
Review of e-Commerce Security Challenges	Jarnail Singh [4]	This paper explains about the various challenges that are faced in day to day E-Commerce also it discuss about the ways to secure the shopping and a description about the security protocols used for online shopping.	2014
E-Business Security Challenges	Mohamad Ibrahim Ladan [5]	This paper covers the overall idea of the E-Business and it elaborates about the B2B and B2C E-Business. Also it discuss about the network issues, wireless and mobile issues.	2013
Study on e-Commerce Threats and Security	RazibulHasanet.al [6]	This paper discuss about the security threats and safeguarding measures in E-Commerce.	2012

IV. SECURITY ISSUES IN E-COMMERCE

The security issues in E-Commerce are as follows

- Privacy
- Integrity
- Authentication

A. Privacy

The information that are exchanged such as transaction details in the E-Commerce site must be protected from illegal access.

B. Integrity

The information that are transferred between the parties should not be tampered.

C. Authentication

To access the confidential information proper authentication must be enabled.

V. SCENARIO AND SECURITY SCRUTINIZE IN E COMMERCE BACKGROUND

The fundamental scenario of e commerce environment are as follows

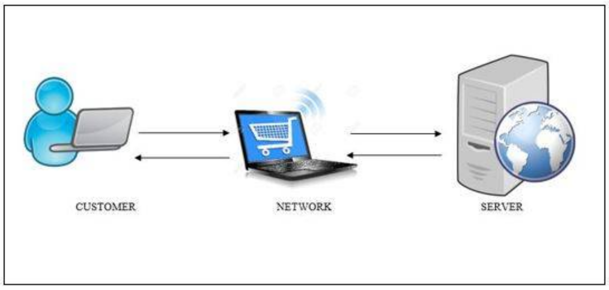

Fig. 1. Scenario of E-Commerce Environment

The established background of e-commerce is categorized into three. They are

- Customer
- Internet
- Server

The customer may interact with the e commerce site with the help of the internet to buy the products through online services that are readily available. Moreover, the customer may enquire about the concern products to the server whether it is available or not.

Internet act as an intermediary between the customer and server in order to buy the products.

Server accepts the customer requests and acts accordingly based on the demand made by the customer.

VI. SECURITY THREATS IN E-COMMERCE ENVIRONMENT

The security threats in E-Commerce environment are as follows:

- Virus
- Adware
- Spyware

A. Virus

A virus is a malevolent program which are anticipated to affect the system with severe loss. The virus may get fix itself to the separate file or a group of files leading to severe loss by acquiring more space, modifying files, folders, slow response of the system.

B. Adware

Adware is considered to be a malevolent which are embedded into the advertisement if the customer unknowingly clicks on it leads to fraudulent activity by seizing customer credentials.

C. Spyware

Spyware that performs like an application but its main motive is to gather the credentials of the individuals after gathering the credentials it will send this to the malicious attacker which are connected in the network.

VII. CYBER ATTACKS IN E-COMMERCE ENVIRONMENT

A. Cyber Attacks in E Commerce at Customer Side

The cyber-attack that are possible at customer side are as follows

- Phishing
- Pharming
- Log forgery
- Password Attacks
- Cross site Scripting
- Brute force Attack

1) Phishing: Phishing is an attempt to seize customer's identifications such as PIN number, account details. The malicious attacker may add the forged E-commerce login page to the legitimate website if the website is vulnerable to attack. Normally, the forged e-commerce websites are widely spread by emails. If the customer has an awareness of this type of cyber-attack he/she will be protective from this attack otherwise it leads to an identity theft by grabbing the user credentials. Seized credentials may leads to threatening the customer by fulfilling the attacker needs.

2) Pharming: Pharming is similar to phishing attack. The main motive of this attack is to steal customer information by redirecting them to the spurious website. When the domain name of the website is typed in the web browser it first converted into the Numerical address that is IP address which are done using DNS Server. If the IP address is redirected to spurious website it will lead to Pharming attack. This can be done by compromising the DNS Server also it is not a usual attack like phishing.

3) Log Forgery: The unsanitized input from the user to access the log files may leads to log forgery or inserting malevolent things to the log. By altering the log file information may leads to a severe impact.

4) Password attacks: To crack the customer login id and password there are many password cracking tools by cracking the password the attacker may steal the customer's online credentials. Also it leads to cancelation of ordered products by the customer or ordering the new product.

5) Cross side scripting Attack: The other name for cross side scripting attack is XSS Attack. It is the most common type of attack that occur on the website. In this attack, the legitimate E-commerce site is inserted with malevolent code which is done by the attacker. The attacker may vandalise the E-commerce site by exploiting this attack.

6) Brute force attack: It is a type of password guessing attack by using the trial and error method. If the attacker knows about the target customer this type of attack can be performed easily by guessing the password.

B. Cyber Attacks in E Commerce at Internet

The cyber-attack that are possible at internet are as follows

- Man in the middle attack
- Session hijacking
- Snooping
- Spoofing

1) *Man in the middle attack:* It is a common type of attack on the internet. The attacker may silently listen the communication that has been taken place between the customer and the server.

2) *Session hijacking:* It is also a common type of attack on the internet. In this attack, the one particular session can hijacked for example payment session can be hijacked after gaining the proper authentication.

3) *Snooping:* In order to perform this attack, the attacker executes the malicious program such as key logger to capture the keystrokes that are pressed by the user. While performing the payment transaction it is better to use

virtual keyboard that is present in the website instead of using the keyboard that are connected with the system.

4) *Spoofing:* The malicious attacker mimicked himself as the legitimate to access the network or to control the entire network.

C. Cyber Attacks in E Commerce at Server Side

The cyber-attack that are possible at server side are as follows

- SQL Injection
- LDAP
- Weak Authentication

1) *SQL injection:* The attacker may gain aces to the server if it is vulnerable to query statements. By gaining the access the attacker may perform malicious activities such as viewing, altering or damaging the data that are present on the server.

2) *LDAP:* By compromising the vulnerability present on the website the LDAP statement is executed by the attacker. The modified LDAP statement may leads to severe effect such as defacement of the website, illegitimate access to the data.

3) *Weak Authentication:* It is a type of attack by exploring the vulnerability present on the server by using this the attacker may gain entire access to the server where the entire details are stored.

VIII. SECURITY TOOLS TO BE USED IN ECOMMERCE

The security tools to be used in E-Commerce are as follows

- Firewalls
- Intrusion detection system
- Digital certificate
- One Time Password
- Two factor Authentication
- Tokens
- Biometrics
- Salting and hashing for securing passwords
- Digital signature
- Vulnerability Scanning Tools

IX. CONCLUSION

The development of recent technology allows us to build the secure website it depends upon the implementing team in order to develop the website with preventive measures. Each and every attacks cannot be prevented but some of the common attacks that are done on the E-Commerce environment can be prevented.

REFERENCES

1. http://www.tutorialspoint.com/e_commerce/e_commerce_business_models.htm
2. P. S. Lokhande, B. B. Meshram, "E-Commerce Applications: Vulnerabilities, Attacks and Countermeasures", International Journal of Advanced Research in Computer Engineering & Technology, Vol.2, pp.499-509, 2013.
3. NiranjanamurthyM , DR. DharmendraChahar, "The study of E-Commerce Security Issues and Solutions", International Journal of Advanced Research in Computer and Communication Engineering Vol.2, pp.1-12, 2013.
4. Jarnail Singh, "Review of e-Commerce Security Challenges", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, pp.2850-2858, 2014.
5. http://sdiwc.net/digital-library/download.php?id=00000495.pdf

6. http://daffodilvarsity.edu.bd/sub-site/nccis/proceedings.php

BIOGRAPHY

R. Priya is pursuing her M.Tech (Information Security) in Computer Science and Engineering from Pondicherry Engineering College, Puducherry. She completed her B.Tech degree in Information Technology from Sri Ganesh College of Engineering and Technology, Puducherry. Her research interest are Information Security and Computer Networks.

J. Jayanthi is working as an Assistant Professor, Department of Information Technology, Sri Ganesh College of Engineering and Technology, Puducherry. She received her B.Tech degree in Information Technology from IFET College of Engineering, Anna University and completed her M.E degree in Computer Science from Arunai Engineering College, Anna University, Chennai. Her research interest are Computer Organization and Architecture and Networking.

P. Manjamadevyis working as an Assistant Professor, Department of Computer Science and Engineering, Sri Ganesh College of Engineering and Technology, Puducherry. She received her B.E degree in Computer Science and Engineering from Mailam Engineering College, Anna University and completed her M.E degree in Computer Science and Engineering from Annamalai University. Her research interest are Computer Networks and Operating Systems.