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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

# A Study on E-Commerce Security Threats

Poonam Patel, Kamaljeet I. Lakhtaria

Assistant Professor, SDJ International College, Surat, Gujarat, India

Associate Professor, Dept. of Computer Science, Gujarat University, Ahmedabad, Gujarat, India

**ABSTRACT:** Electronic Commerce can help in improving relationships between buyers and sellers, reducing cost, obtain greater control over market. But along with this risk and threats have also came up, such as, interpersonal relationship, trust, network attacks and so on. This paper analyzes the e-commerce payment methods, threat classification and their available control measures.

**KEYWORDS:** e-commerce, security issues, threat classification

## I. INTRODUCTION

The exchange or buying and selling of commodities on a large scale involving transportation from place to place is known as commerce. E-Commerce is the application of technology toward the automation of business transaction and workflows, delivery of information, products or services, buying and selling of products over internet.E-commerce is taking advantage of distance selling the great advantages offered by new information technologies, such as the extension of the offer , the interactivity and immediacy of purchase, with the difference that you can buy and sell to whom you want , and where and when they want. There are increased opportunities to enhancing the business efficiency and reducing the incurred costs by the computer applications of e-commerce as it enables a tighter integration with the several linkages. The medium of electronic that is referred as the internet has the power and tendency for reducing actual time of transactions and the overall processing time radically. One of the critical issue in e-commerce success is security. Security is directly related to the issue of trust and confidence between buyer and seller and extremely sensitive personal information.

## II. E-COMMERCE SECURITY

Security is the component that affect e-commerce which includes Computer Security, Data Security and other areas. Security is one of the concern which is affecting customer and organizations trade. Web application which are offering online payment system (net banking, credit card, debit card, PayPal or other token) are at more risk from being targeted and there is big loss if data is being hacked. The e-commerce website those offering online payment are giving guidelines for securing systems and networks available for the ecommerce system. To educate the customer is the more critical part of the ecommerce security architecture. Trojan horse programs are the biggest threat to e-commerce because they can overthrow the authorization and authentication mechanisms used in trading transaction. These programs are installed on remote computers by simple means: mail attachments. Privacy has become the biggest issue for consumers with the rise of identity theft, this cause's major concern for e-commerce providers.

## III. E-COMMERCE SECURITY TOOLS

- Firewall – Software and Hardware
- Public Key infrastructure
- Encryption software
- Digital certificates
- Digital Signatures

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

- Passwords
- Locks and bars – network operations center

## IV. PURPOSE OF STUDY

- Overview study of e-commerce security.
- Understanding the online shopping steps.
- Understanding the need of Security in e-commerce.
- Listing the different security issue in e-commerce.

## V. DIGITAL E-COMMERCE CYCLE

Now a day's people prefer to shop online than going for traditional business, because it's easier and more convenient. Almost anything can be bought online as books, kitchen ware, toiletries, clothes, music, electronic peripherals and many more. Some of the popular websites are eBay, amazon, Best Buy, iTunes and many more.

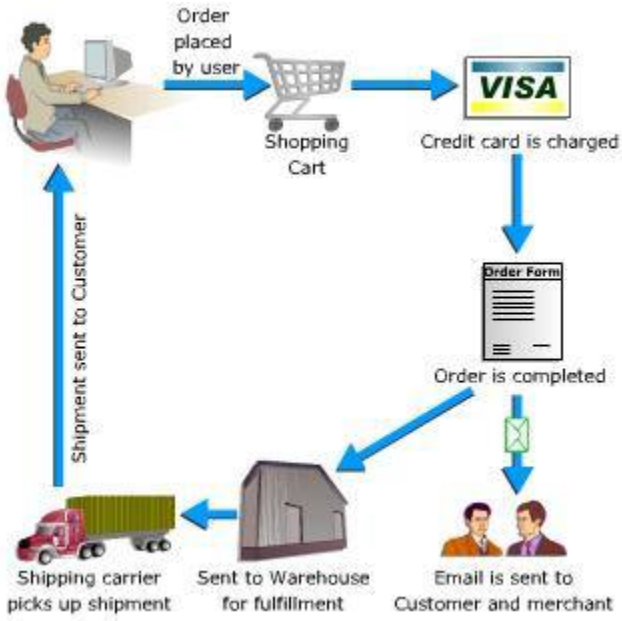


**Figure 1**

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

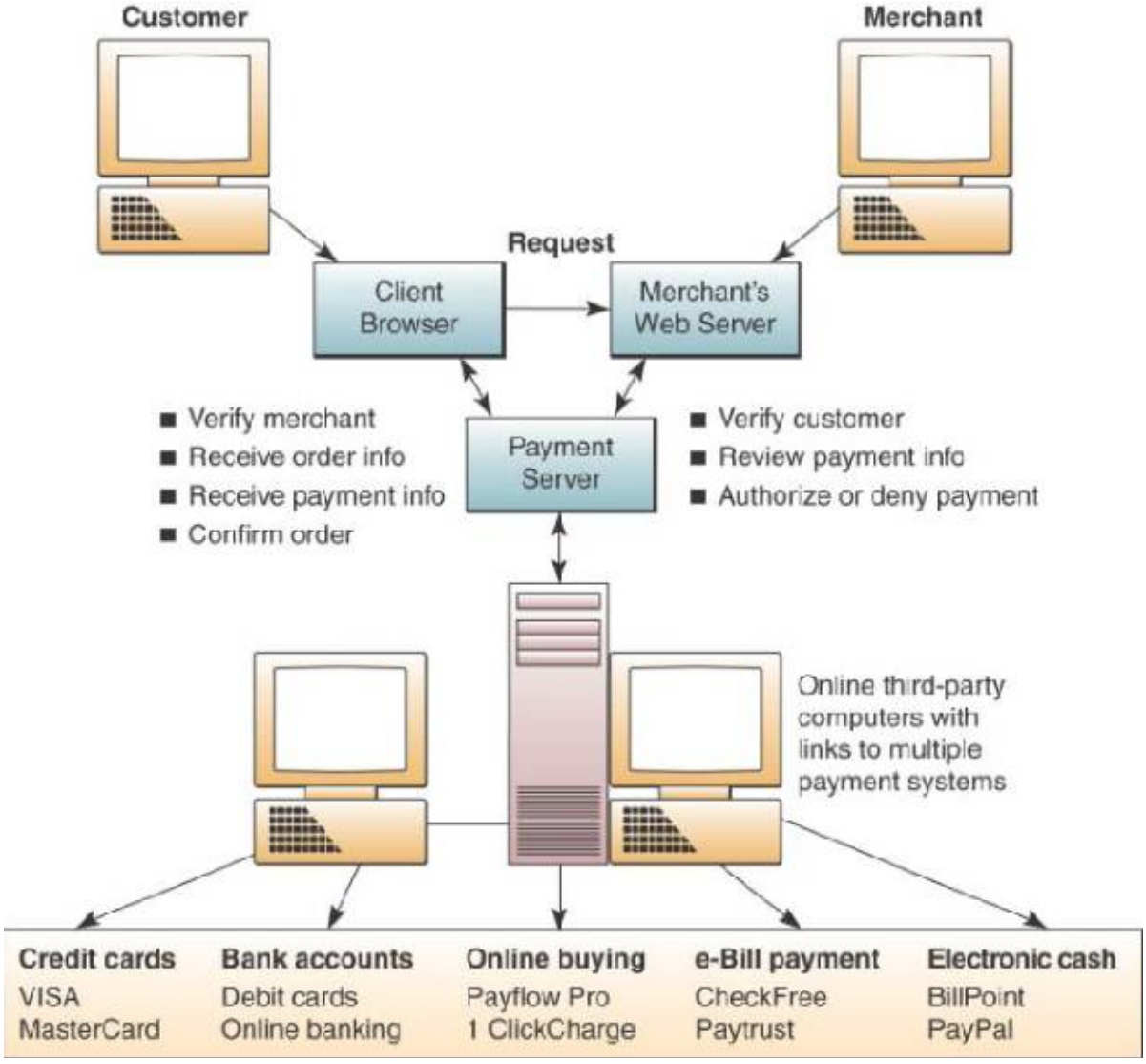


Figure 2

## VI. SECURITY THREATS

Types of security threats are as under:

1. Technical Attacks
    a. Denial of service attacks
    b. ICMP Flood (Smurf Attack)
    c. Teardrop Attack
    d. Phlashing
    e. Brute force attacks
2. Non-Technical Attacks
    a. Phishing Attacks
    b. Social Engineering

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

1. **Technical Attacks:** Technical attacks are one of the most challenging types of security compromise an e-commerce provider must face. Typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, large online retailers and popular social networking sites are targeted.

a. **Denial of service attacks:**Denial of Service (DoS) attacks consist of overwhelming a server, a network or a website in order to paralyze its normal activity. Defending against DoS attacks is one of the most challenging security problems on the Internet today. A major difficulty in thwarting these attacks is to trace the source of the attack, as they often use incorrect or spoofed IP source addresses to disguise the true origin of the attack.

b. **ICMP Flood (Smurf Attack):**Where perpetrators will send large numbers of IP packets with the source address faked to appear to be the address of the victim. The network's bandwidth is quickly used up, preventing legitimate packets from getting through to their destination.

c. **Teardrop Attack:**A Teardrop attack involves sending mangled IP fragments with overlapping, over-sized, payloads to the target machine. A bug in the TCP/IP fragmentation re-assembly code of various operating systems causes the fragments to be improperly handled, crashing them as a result of this.

d. **Phlashing:** Also known as a Permanent denial-of-service (PDoS) is an attack that damages a system so badly that it requires replacement or reinstallation of hardware. Perpetrators exploit security flaws in the remote management interfaces of the victim's hardware, be it routers, printers, or other networking hardware. These flaws leave the door open for an attacker to remotely 'update' the device firmware to a modified, corrupt or defective firmware image, therefore bricking the device and making it permanently unusable for its original purpose.

e. **Brute force attacks:**A brute force attack is a method of defeating a cryptographic scheme by trying a large number of possibilities; for example, a large number of the possible keys in a key space in order to decrypt a message.

2. **Non-Technical Attacks:**

a. **Phishing Attacks:**Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Phishing scams generally are carried out by emailing the victim with a 'fraudulent' email from what purports to be a legitimate organization requesting sensitive information. When the victim follows the link embedded within the email they are brought to an elaborate and sophisticated duplicate of the legitimate organizations website. Phishing attacks generally target bank customers, online auction sites (such as eBay), online retailers (such as amazon) and services providers (such as PayPal).

b. **Social Engineering:**Social engineering is the art of manipulating people into performing actions or divulging confidential information. Social engineering techniques include pretexting where the fraudster creates an invented scenario to get the victim to divulge information, Interactive voice recording (IVR) or phone phishing where the fraudster gets the victim to divulge sensitive information over the phone and baiting with Trojans horses (where the fraudster 'baits' the victim to load malware unto a system). Social engineering has become a serious threat to e-commerce security since it is difficult to detect as it involves 'human' factors which cannot be patched.

## VII. SECURITY FEATURES

- **AUTHENTICATION:**It verifies ones identity. It enforces that you are the only one allowed to login to yourOnline banking account.
- **AUTHORIZATION:** Allows only you to manipulate your resources in specific ways. This prevents you fromincreasing the balance of your account or deleting a bill.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

- **ENCRYPTION:** Deals with information hiding. It ensures you cannot spy on others during Internet bankingtransactions.
- **CONFIDENTIAL:** Information is not accessible to unauthorized person.
- **AUDITING:** Keeps a record of operations. Merchants use auditing to prove that you bought a spec ific merchandise.
- **INTEGRITY:** Prevention against unauthorized data modification
- **NONREPUDIATION:** Prevention against any one party from reneging on an agreement after the fact
- **AVAILABILITY:** Information is available wherever and whenever is needed without any time limit.
- **DDOS (DISTRIBUTED DENIAL OF SERVICE ATTACKS):** involves hackers placing software agents onto a number of third-party systems and setting them off to simultaneously send requests to an intended target
- **SNIFFERS:** software that illegally access data traversing across the network.

## VIII. CONCLUSION

E-Commerce industry faces a challenging future in terms of the security risks it must avert. With increasing technical knowledge, and its widespread availability on the internet, criminals are becoming more and more sophisticated in the deceptions and attacks they can perform. Novel attack strategies and vulnerabilities only really become known once a perpetrator has uncovered and exploited them. In saying this, there are multiple security strategies which any e-commerce provider can instigate to reduce the risk of attack and compromise significantly.

## ACKNOWLEDGEMENT

The Author is thankful to Proff. (Dr.) Kamaljeet Lakhtaria for his encouragement, helpful suggestions and supervision throughout the course of this work.

## REFERENCES

1. Thomas L. Mesenbourg, “An Introduction to E-commerce”, Philippines: DAI-AGILE, 2000
2. Good. D and Schultz.R, “E-commerce strategies for B2B service firm in the global environment”, American Business Review, vol. 20, no. 2,(2003).
3. MazumdarSengupta.C and Barik.M.S, “E-commerce security-a life cycle approach”, Sadhana, vol. 30, no. 2-3, (2005).
4. Antoniou.G and Battern.L, “E-commerce: protecting purchaser privacy to enforce trust”, Electronic commerce research, vol. 11, no. 4, (2011).
5. Smith.R and Shao.J, “Privacy and e-commerce: a consumer-centric perspective”, Electronic commerce research, vol. 7, no. 2, (2007).
6. Khalid Haseeb, Dr. Muhammad Arshad, Shoukatali and Dr. ShaziaYasin “ Secure E-commerce Protocol”, International Journal of Computer Science and Security (IJCSS), Vol. 5 No. 1, pp.742-751, April 2011
7. QIN Zhiguang, LUO Xucheng, GAO Rong, “ A survey of E-commerce Security”, School of Management, University of electronic Science and Technology of China Chengdu, Journal of Electronic Science and Technology of China Vol.2 No.3, Sept 2004
8. Jagdev Singh Kaleka, “E-Commerce: Authentication & Security on Internet”, Deptt. of Technical Education andIndustrial Training, Govt. of Punjab
9. Aiman H. Mufti, Saudi Armco, “e-Commerce and its Security”, February 11, 2001
10. Nada M. A. Al-Slamy, “E-Commerce Security”, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.5, May 2008
11. http://webscience.ie/blog/2010/security-issues-in-e-commerce/