A Review Paper on Security Issues in E-Commerce

Megha Saloni
MCA Student
Dept. of Information Technology,
HMRITM, New Delhi, INDIA

Dayanand
Assistant Professor
Dept. of Computer Science Engineering
HMRITM, New Delhi, India

***Abstract*-Electronic commerce is commercial transaction that has been conducted electronically on the Internet. Electronic commerce is the buying or, selling goods or, transmitting of data or, capital over an internet. For many people, e-commerce means shopping through internet. It is a type of business model that enables a company or, an individual to conduct business over an internet. It may be either business to business, business to consumer, consumer to business, consumer to consumer. But with the increasing use of e commerce, various security issues also arise. This paper discusses various security issues of e commerce which needs proper attention to protect us.**

Keywords: E- commerce, Security Issues, Privacy, Attacks

I. INTRODUCTION

Business that have been engaging in form of e-commerce is known as electronic data inter-changeable (EDI).

Due to the deployment of the e-commerce over a large scale, privacy and security are the major concern for electronic technologies. Web e-commerce that handle payment i.e., online banking, electronic transaction using debit/credit card or, other token have more complained issues.

Security is one of the most important factor that restrict customer or, an organisation engaging with e-commerce. The e-commerce business is slowly undertaking security issues on the internal networks. There are guidelines for securing system and network. Educating the consumer on the security issues is still in the down stage. Educating the consumer will improve the e-commerce security architecture. Privacy has become major concern with the rise of identity threats and impersonation. The massive increase in the up-take of e-commerce has led to a new generation of associated security threats.

a) Any e-commerce system must meet four integral requirements, they are as follow:-

b) Privacy- Information exchanged between the two parties must be kept secure from unauthorized parties.

b) Integrity- The exchanged information between the two parties must not be tampered.

c) Authentication- Both receiver and sender prove there identities to each other.

d) Non-repudiation- Proof is required that the exchanged information was indeed received.[3][4]

Loopholes of E-commerce Security[2][1]

Technical attack- Technical attack is one of the most challenging type of security compromise of an e-commerce provider must face. Some of them are as follow:-

- **Denial of Service Attack(DOS):-** In Denial of Service attack, The attack on a network is designed to its knees by flooding it with useless traffic. It is a type of attack where the attackers attempt to prevent licensed user from accessing the services. The United State Computer Emergency Readiness Team defines symptoms of DOS attack that includes the following symptoms:

a) ually slow network performance.

b) navailability of the particular website.

c) ramatic increase in the number of spam e-mails received.Denial of Service attack can be executed in number of different ways, that includes:

i. **ICMP Flood (Smurf Attack):-** In the Denial of Service attack where an attacker takes down the victim's system by swamping it with ICMP echo request, also known as 'ping'.

ii. **Teardrop Attack:-** Teardrop attack involves sending managed IP fragments with overlapping, over-size payload to the target machine. Since machine receiving such packets cannot reassemble them due to bug in TCP/IP fragmentation reassembly, the packet overlap one another, crashing the target network device.

iii. **Phlashing:-** It is also known as Permanent Denial of Service, it attack the system so badly that it requires replacement or, reinstallation of hardware. It exploit the vulnerability in network based firmware updates. Phlashing was firm demonstrated by HP Head of system security when they identified and exploited a flaws on a network hardware devices that ultimately lead to device crashing.

- **Distributed Denial of Service Attack (DDoS):-** It is one of the greatest security fear for IT manager. In a matter of minutes, thousands of vulnerable computer can flood the victim website by choking legitimate traffic. More than 2000 daily DDoS attacks are observe world wide by Arbor Network (ATLAS Threat Report). $150 can buy a week long DDoS attack on the black market (Trend Micro Research).The most famous DDoS attack occurred in February 2000 where website including Yahoo, Buy.com, eBay, Amazon and CNN were attacked and left unreachable for several hour each.

- **Brute Force Attacks:-** It is a "hit and trail" methodology by the attackers to decode the encrypted data such as password through painstaking effort(using Brute Force) rather than implementing intellectual strategies.

Non- Technical Attack

- **Phising Attack:-** In phishing attack valuable information such as, user name, password, debit and credit card pin can be obtained by exploiting vulnerabilities within the user understanding of a system and particularly a lack of understanding of the user interface. Fraudsters can be manipulate users instead of the most widely practised Internet frauds. The fraudsters exploit the secret information of victim for the financial gain. Nearly, !00,000 people reported receiving phising e-mail in 2015 in UK alone, which equates to nearly 8,000 a day.
- **Social Engineering:-** It is a skill of attackers to manipulate the people to give their confidential information like, bank account information, pin of debit or credit card, password etc.

II. TERATURE SURVEY

With the advancement technology and busy life, online shopping has increasingly been accepted by the internet user. This made great pace in providing a convenient way of shopping. The reality is that billions of dollars are lost while doing online shopping over the e-commerce websites because of the shoppers' lack of knowledge about the online security threats. However, people should be aware of security threats[5].

Internet has rapidly led to the emergence of what is called New Economy, Global economy or E-commerce. This transformation comes with a lot of benefits, however accomplished with the new security issues and challenges. These security issues are mainly originated from the use of internet and other communication medium which allow the flow of information outside the enterprise in all directions. The vulnerabilities of E-commerce system could be one or, more of the following level:

- The customer's computer/network,
- The different businesses' server/network communication medium allowing the flow of information between two or more different end-points. Therefore, the people involved in developing and deploying e-commerce system should give a great attention to the security of such system and the data residing on them to ensure privacy and security[6].

Privacy has become a major concern for consumer with the rise of identity theft and impersonation and any concern for consumer must be treated as a major concern for e-commerce providers. Safety measure is an element of the Information Security framework and is concurrently applied to the component part that affect e-commerce that includes computer security. Data Security measures and other wider realms of the Information Security framework. E-commerce security is the stockade of e-commerce assists from unauthorized access, utilize change or, fragment. Dimension of e-commerce security, integrity, non-debanking, legitimacy, confidentiality, privacy, accessibility[7].

Millions of dollar loss each year because of credit card fraud has exposed the security weaknesses in the traditional credit card number processing system. In such system, customer uses fixed credit card number in all transactions. Because such numbers are fixed, it is relatively easy for some attackers to steal them. Some common ways are[8]:

- Shoulder Surfing
- Dumpster Dividing
- Packet Interpreting
- Database Stealing

Electronic commerce has been weakened by the deterioration of confidence of confidence held towards it by consumer public. This is turning posses an immense threat to the overall expansion and success of it. In fact, Hoffman et as. stated that 63% of online end-user internally delay when providing personal information due to the diminished confidence and trust in site. If credibility is to be achieved improvised security and privacy protocols should be incorporated. The US-based Better Business Bureau confirmed that online security was great concern in 2001. Types of security threats that include identity theft i.e., the illegal use of personal information and in fact the USA's leading occurrence of fraud. List of other threats includes gaining physical access to premises, accessing wiretap, unauthorized acquiring of information, viruses, lack of integrity, financial fraud, vandalism,etc[9].

Security has become one of the most important issues that must be resolved first to ensure success of e-commerce. The low cost & wide availability of the internet for business and customers has sparked the revolution in e-commerce. We can distinguish transaction into five phases:

- First, the merchant makes an offer for specific goods or, services.
- Secondly, according to the offer, the customer may submit the request online.
- Thirdly, The customer makes a payment and merchant delivers the goods or, services to the customer. The handling of the payment may involve many ways such as online banking, cash on delivery, debit and credit card payment and so on.

Over the past decade, the evolution of both technology hardware and internet has had a direct co-relation with e-commerce. Now a days, internet has grown into a desired medium for marketing, advertising, purchasing of product, goods and services. E-commerce has grown to rival shopping in many ways.

It may be relevant to take a brief look at how e-commerce has evolved over the year and examine the obstacles it had to overcome

- 1979- Michael Aldrich is created with investing online shopping by connecting a modified domestic TV to read real-time transaction processing computer via, a domestic telephone line.
- 1982- Minitel was introduced in France and was used for online shopping.
- 1994- Netscape releases the Navigator browser. Pizza Hut offers online ordering on its web page and first online bank opens.
- 1998- PayPal comes into existence.
- 2001- Amazon led the way by launching their mobile commerce site.
- 2002- eBay acquire PayPal for $1.5 Billion and change the scope of online shopping forever.
- 2003- Amazon post its first yearly profit.
- 2006- Google release Google Checkout to help ease in the payment process for e-commerce customers/ shoppers.
- 2007- Magento, is a e-commerce content management system that first started development.
- 2011- Magento is acquired by eBay.
- 2012- US E-commerce and online retail sales are projected to reach $226 Billion(an increase of 12% over 2011).

III. PREVENTIVE STRATEGIES OF E-COMMERCE SECURITY[10]

Firewalls:- A firewalls is a very important tool to use to protect personal information and company data as well. The firewall acts as security checkpoint that all communication with your server has to cross through. A firewall is like a defender, the information and data from outside the network needs to pass through and get inspected by before the information can passed onto The e-commerce server that it is protecting.

Routers:- Router is an example of a firewall in hardware form. Router is to fulfill two main goals. First, It is a firewall so it protects the network and e-commerce. Second, router insure that the data packets do not go where there are not intend to and make sure that they arrive where there are intended to. The router have a Network Address Translation(NAT) feature in which it will disguise the servers IP address to the outside world and show the routers IP address instead.

Network Intrusion Devices:- A Network Intrusion Devices is a device that takes the role in not only defending your network but it will constantly be looking for the threats both from inside and outside the network. It comes with in two different ways with different security features, they are:

- Network Based Intrusion Detection Devices(NIDS) is usually used to look through the incoming data packets to inspect them before they make contact with the network.
- Host Based Instruction Detection Device(HIDS) is connected to only a single server or, computer as compared to NIDS which is connected to a network of computer or, server. HIDS will more than likely to be used smaller personal protection while NIDS should be used for more organized E-commerce transaction.

Authentication:- When customer logs onto E-commerce server, they are logging on assuming that they are going to secure valid site. From the owner's point of view, they will want to ensure the high authorized user is logging on and not some hacker trying to gain access through the user. Authentication is verification, who the user is and whether the users allowed access to the network. To process through Authentication we use Secure Socket Layer (SSL). SSL has been improved to something called Transport Layer Security which was founded on the same principle of SSL. SSL uses digital certificates that are sent between the two servers or, the computer and server, that are trying to make contact with each other. The SSL is frequently used to control the security of message over the Internet.

Encryption:- A method of scrambling or, encoding of data to prevent unauthorized user used from reading or, tampering with data. There are many different types of encryption and many different ways to implement it but for E-commerce server you should make use of Secure Shell or, SSH method. It is a method that provide for an encrypted login connection to a server,

Virtual Private Network(VPNs):- VPNs are not just limited to the encryption, but they make use of feature called" tunneling" which adds an another layer of protection. The data packet that contain all the information (username/password, email, social security number etc)from either server or, the customer and put that data packet to further hide and make sensitive information even harder for hacker to get into.

IV. PROTECTION OF E-COMMERCE FROM DDOS:-

DDoS can be disrupt and cause large revenue losses. However, effective defences continue to be mostly unavailable. VIPnet, a noble value added network service for protecting e-commerce and other transaction based sites from DDoS attacks. In VIPnet, e-merchant pay Internet Service Providers(ISPs) to carry the packets of the e-merchants' best clients(called VIPs) is privileges class of services(CoS), protect from congestion whether malicious or not, in regular CoS. VIPnet rewards VIPs with not only the better quality of service, but also greater availability. Because VIP rights are client and server specific, cannot be forged and usage limited and are only replenished after successful client transactions(e.g., purchases), it is impractical for attackers to mount and sustain DDoS attack against e-merchant's VIPs[11].

Payment Gateway Security:-

Secure Socket Layer(SSL) is used to encrypt messages between web browser and web server. It encrypt the datagram of Transport Layer Protocols, SSL is also widely used by merchant to protect the consumer's information during transmission. One of major problem of SSL is that merchant can store the sensitive information of the cardholder, and the protocol does not prevent the non-repudiation because client authentication is optional.

Secure Electronic Transaction(SET) come to resolve the weakness of SSL. SET ensure payment integrity, confidentiality and authentication of merchant and cardholder. But SET is characterized by the complexity and the cost supported by the merchant because the logistics of certificates distributing and client software installation, it is difficult to manage non-repudiation.

To deal with SET problem, VISA introduces 3D security, this protocol is based on the introduction of additional control when buying online in addition to the classic sensitive cardholder. The customer validate the payment in new window by entering a secret data agreed with its own bank (password, date of birth, code received by SMS etc)[8].

CONCLUSION

With the advancement technology and busy life, online shopping has increasingly been accepted by the internet user. This made great pace in providing a convenient way of shopping. It is a type of business model that enables a company or, an individual to conduct business over an internet. It may be either business to business , business to consumer, consumer to business, consumer to consumer. Any e-commerce system must meet four integral requirements such as privacy, integrity, authentication, non-repudiation. There are many loopholes of E-commerce are there like DoS, DDoS, Phising, Phlashing, Brute Force attack etc. Instead of that, there are many preventive strategies like firewall, authentication, encryption VPNs etc, are there which makes them secure from the unauthorized user. Digitalization make the future scope of E-commerce more vivid.

Future Scope of E-commerce[12]:-

- **Social media:-** Majority of online buying decision are made on social media like Facebook, Linkdin, Google+, Pinterest etc have become a medium for easy login and purchase.
- **Drone Delivery:-** companies have been working their way around to innovate the delivery process to shorten human effort as well as time. The answer to these problem is Delivery by Drones.
- **App only approach:-** Statics suggest that the future of internet lies on mobiles. Experts says more than 580 million people in India will use the Internet by 2018 and 70-80% of them will access the web on mobile phone. About two- third of its online traffic of Flipkart comes from the user in small cities and towns. Flipkart app-only approaches assumes larger significance in these places where most people don't have their own desktop computer and have limited access to broadband.
- **Google's Buy Now Button :-** Google is working on its" Buy Now" button that would allow e-shoppers search for products on Google and purchase them with single click, right through the Google's own search result page. The button will be displayed near sponsored search result beneath a"shop on Google" heading at the top of page.
- **Artificial Intelligence:-** As the e-commerce space get saturated, investors looking for innovative use of technology are zeroing in on company developing Artificial Intelligence (AI). Jet Airways is experimenting with one such solution devised by Vizury

REFERENCES

[1]. Security Issues in E-commerce Copyright Eamon O' Raghallaigh 2010 data electronically available at http://webscience.ie/blog/2010/security-issues-in-e-commerce/

[2]. Niranjanamurthy M 1 , DR. Dharmendra Chahar "The Study of E-Commerce Security issues and Solution" 2 International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 7, July 2013 ISSN (Print) : 2319-5940

[3]. Kirti Saxena "E-commerce Security- A life cycle approach " Kirti Saxena International Journal of Latest Trends in Engineering and Technology

[4]. E-commerce and customer Relationship

[5]. "Shopping online security in UAE"by Fadhila Amer, Hend Abdulrahin, Salwa Juma, Amala V. Rajan, Jinesh Ahamed

[6]. 'E-commerce Security Issues" by Mohammad Ibrahim Ladan, available at IEEE Explorer library http://ieeexplore.ieee.org/document/6984195/

[7]. Adamu Abubakar Isah “Concern for E-commerce security” Global Journal Computer & Technology ISSN 2394-501X

[8]. "A security- enchanced one-time payment scheme for credit card" by Yingjiu Li, Xinwen Zghan available at IEEE Explorer http://ieeexplore.ieee.org/document/1281701/

[9]. Data electronically available at "How to shop for free online Security Analysis Of Cashier-as-a-Service Based Web Stores" by Isaac Strohl & Avinash Joshi

[10]. Rashad Yazdanifard, Noor Al-Huda Edres and Arash Pour Seyedi "Security and Privacy Issues as a Potential Risk for Future E-commerce Development" International Conference on Information Communication and Management

[11]. Data electronically available at https://www.bsonetwork.com/e-commerce-ddos-attack-protection/ "Prevention of E-commerce from DDoS Attacks "by Jose Cardos

[12]. "Future Scope of E-commerce Business in India" by Problab Technology Pvt ltd.