Dept of Computer Science, P B SIDDHARTHA COLLEGE OF ARTS & SCIENCE, VIJAYAWADA.
UGC SPONSORED NATIONAL SEMINAR ON "CYBER SECURITY WITH SPECIAL FOCUS ON CYBER CRIMES & CYBER LAWS (NSCS 2014)" on
15th & 16th November 2014-IJDCST SPECIAL ISSUE, PAPER –ID: IJDCST-08
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Ensuring Security in E-Commerce websites

Ms. Aparna Bulusu[1], Ms. K N Nandini[2]

[1]Lecturer, Dept of Computer Science, St. Ann's College for Women, Mehdipatnam, Hyderabad email: awudali@gmail.com

[2]HOD, Dept of Computer Science St. Ann's College for Women, Mehdipatnam, Hyderabad email: knnandini@rediffmail.com

Abstract: Massive advances in technology and increasing internet speeds have led to an unprecedented increase in ecommerce websites. Companies and customers alike are now focusing more on e-tailing than on traditional brick and mortar stores. Current trends predict an increase of over 50% in ecommerce sales. However the flip side of this changing scenario is that new security issues are cropping up that ecommerce companies must address in order to secure customer information and sustain their sales. Specific issues plaguing ecommerce sites include difficulties in authenticating customers, lack of sufficient encryption, cyber attacks on web servers, large scale hacking of customer information from company databases etc. Ensuring privacy and security of customer and business information and maintaining consumer trust are of paramount importance in determining success of ecommerce websites. This paper attempts to review current issues faced by ecommerce sites and various cyber security measures being implemented to counter these problems. Various techniques to make ecommerce sites more secure and fool proof are also discussed.

Keywords: ecommerce, hacking, encryption, cyber security.

1. Introduction

The advent of World Wide Web has drastically altered many facets of everyday lives. Improvements in semi conductor technologies, drastic reductions in prices of gadgets like computers, laptops, smart phones, availability of broadband internet and improved computer literacy, have led to a massive growth in online or e-commerce. Ecommerce has traditionally been defined as any exchange of goods, services, funds etc primarily over the internet. Alternately, the *International Journal of Electronic Commerce*, defines it as 'Sharing business information, maintaining business relationships and conducting business transactions by means of telecommunications networks' [1] Online electronic commerce is often categorized as business to business, business-to-consumer and consumer-to-consumer. Benefits from ecommerce sites include internationalising the market places, operational cost savings, mass customization, reduced inventories, lower telecommunication costs, digitisation of products and services, 24/7 access and improved delivery processes.

One of the seminal papers on ecommerce predicted way back in 80's that electronic commerce would eventually become the preferred form of commerce both from a seller as well as buyer perspective [2]. Current trends available online state that the digital commerce market in India alone has seen a 34% increase in growth from 2012 to 2013 with estimated sales of Rs. 62,967 crores [3]. It is thus evident that ecommerce websites are now a top priority for all kinds of businesses.

Ensuring Consumer trust is of paramount importance in ecommerce websites. Online surveys reveal that 45% of consumers perceive identity theft as a major deterrent for online shopping. These concerns have a huge impact on consumer behaviour. The National Cyber Security Alliance reports that over 64% of online buyers have abandoned an online purchase because they were not certain that a web site was secure.[4] ecommerce providers therefore utilise various strategies for building and maintaining consumer trust like providing safety guarantees to cover credit card fraud, establishing brand reputation by tying up with trusted third party security vendors etc.[5] However ecommerce sites face a multitude of security issues that makes it very difficult to secure them

Understanding how ecommerce sites operate would help in identifying potential areas where security issues might crop up. A typical ecommerce transaction involves the following stages: 1. Consumer shops for items on a merchant's ecommerce website and selects items into a shopping cart. Placing an order involves some form of customer authentication after which payment processing begins. Payment could be handled by the website itself or involve some other third party payment processing websites/banks. Upon successful processing, invoices are generated for the user and orders placed at the merchant's warehouse for shipping to the customer. Each of these stages is prone to vulnerabilities which can affect the integrity and security of the ecommerce sites. Some of the most common security issues and their solutions are discussed below:

Important threats and security breaches faced by ecommerce sites:

I. Dos(Denial of Service):

In the first stage of an ecommerce transaction, Consumers typically browse through the ecommerce sites looking for items. The biggest threat faced by ecommerce vendors at this stage are Denial of Service attacks. DoS, Denial of Service and its variant DDoS Distributed DOS refer to shutting down the server of the ecommerce site or in simpler terms, making the site unavailable for consumers by directing more traffic at the servers than they can handle. Denial of Service attacks are typically caused by hackers who send numerous requests to the ecommerce servers through programmed computers called zombies that result in websites going down or becoming unavailable for consumers to place orders. Dos attacks include techniques like buffer overflow, ping of death, smurf and SYN attacks. These kinds of attacks heavily impact the sales of these websites as well as their brand reputation.

Some preventive measures that are adopted for overcoming DoS attacks include using router filters to terminate harmful traffic, installing OS patches to guard against TCP SYN flooding, maintaining hot spares and redundant and fault tolerant network configurations and maintaining strong security policies.

Stage 2 and 3 of an ecommerce transaction involve placing shopping cart orders and initiating payment process. There are the most critical stages that involve ensuring confidentiality, authenticity and integrity. Ecommerce sites should have provisions

to identify and verify consumer information. All traffic i.e. the flow of messages between the consumer and ecommerce server should be kept confidential and shouldn't be altered or manipulated in any form. Some of the practical problems faced by consumers and ecommerce servers at this stage are as follows:

II **Phishng:**

Phishing is a type of network attack where the attacker creates a replica of an existing Web page to trick users [6]. ecommerce websites typically request users to fill out personal information forms as part of their authentication process. Phishers send fraudulent emails to customers from sites that 'look like' authentic ecommerce sites and collect user information like Id's and passwords. Phishing or online identity theft is now considered a major threat to

online business. From a consumer perspective, overcoming phishing attacks requires users to be aware of spammers, provide confidential information only through secure websites, utilise firewalls, spam filters, antivirus and anti malware programs.

III. Sniffing and Spoofing

Ecommerce servers are regularly targeted by hackers in various ways. Information being exchanged between the consumers/ client system and the ecommerce server can be compromised in multiple ways. Data packet sniffing is a technique used by hackers to steal data packets containing valuable information like usernames, passwords, and other confidential customer data. IP spoofing is another technique where attackers try to change IP addresses of data packets to give the appearance that they originated from a legitimate user. Hackers also indulge in port scanning and searching for backdoors that lead to major security threats.

Security measures commonly employed:

The key dimensions of E-commerce security are: Access control, privacy/confidentiality, authentication, non repudiation, integrity and availability. [7] Common measures used to ensure these requirements are cryptography, combination of digital certificates and public key Infrastructure and use of SSL. [8]

I. Cryptography:

Cryptography involves encrypting data i.e. transforming data into cipher text readable only by sender and receiver. Cryptography aids in implementing message integrity, authentication and confidentiality. Three kinds of cryptographic mechanisms normally used are public key cryptography (uses a separate key for encryption and decryption), private key cryptography (uses same secret key to both encrypt and decrypt messages) and hash functions or message digests (used to generate fixed-length hash values based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered). Hash functions create digital fingerprints of messages that ensure that they have not been altered by an intruder or virus.

II. PKI and Digital Signatures:

ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Ecommerce websites should carry digital certificates from trusted Certificate Authorities. These certificates contain data like public key, name of organization, issuing authority, list of policies, expiration data etc. Digital certificates help in establishing or binding a public key to an individual organization, establish the limits on that certificate and secure confidential information by encrypting the session's symmetric keys. Public Key Infrastructure (PKI) refers to the Certificate Authorities (CAs) and digital certificate procedures and policies followed by all parties involved in an ecommerce transaction. PKI is used to manage Keys and Certificates and helps Ecommerce organizations in maintaining a trustworthy network environment through encryption and digital signature services.

III. SSL

SSL (Secure Sockets Layer) is a standard security technology for establishing an encrypted link between an ecommerce server (website) and a consumer's browser. SSL allows sensitive information like credit card numbers, social security numbers, and login data to be transmitted securely. SSL is actually a security protocol that determines variables of the encryption for both the link and the data being transmitted. SSL is heavily used for securing data on the Internet every day, for online transactions and in transmitting confidential information. A SSL secured website has a lock icon or a green address bar that comes with an extended validation SSL-secured website. SSL-secured websites also begin with https rather than http.

Conclusion:

Ecommerce websites are growing exponentially with thousands of websites coming up on a daily basis. Security is a major concern for all types of organisations, especially for business to consumer e-commerce retail sector, since it reflects the concerns and perceptions of potential customers conducting financial transactions on-line. Hackers and cyber criminals are launching various kinds of attacks directed at these websites in multiple ways like DoS, phishing, spoofing and large scale identity theft. Ecommerce websites must adopt certain best practices like encryption , using digital certificates, Secure socket Layers etc to protect their websites and their consumer information. Organizations should establish and maintain a

trustworthy environment and take necessary measures to secure personal and financial information of their users. Staying protected against cyber security threats requires both organizations and individual users, to be aware of the threats and improve their security practices on an ongoing basis.

References:

1. V. Zwass, 'Structure and macro-level impacts of electronic commerce: from technological infrastructure to electronic marketplaces', http://www.mhhe. com/business/mis/zwass/ecpaper.html,

2. Thomas W. Malone, Joanne Yates, and Robert I. Benjamin. 1987. Electronic markets and electronic hierarchies. *Commun. ACM* 30, 6 (June 1987), 484-497.

ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

3.A report released by Internet and Mobile Association of India (IAMAI) based on findings of market research firm IMRB.

4. "Majority of Americans Have Abandoned an Online Purchase Due to Security Concerns, Poll Finds"; National Cyber Security Alliance, November 18, 2010

5. D. Harrison McKnight, Vivek Choudhury, and Charles Kacmar. 2000. Trust in e-commerce vendors: a two-stage model. In *Proceedings of the twenty first international conference on Information systems* (ICIS '00). Association for Information Systems, Atlanta, GA, USA, 532-536.

6. Juan Chen; Chuanxiong Guo, "Online Detection and Prevention of Phishing Attacks," *Communications and Networking in China, 2006. ChinaCom '06. First International Conference on* , vol., no., pp.1,7, 25-27 Oct. 2006

7. The Different Dimensions of E-commerce Security, (E-commerce, Laudon, 3rd ed., 2007)

8. Shazia Yasin, Khalid Haseeb, Rashid Jalal Qureshi, Cryptography Based E-Commerce Security: A Review, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, March 2012