E-Commerce & M-Commerce Security Issues and their Countermeasures

Atul Kumar Pandey[1,a], Astitwa Bhargava[2,b]

[1]*Assistant Professor, National Law Institute University, Bhopal, India*

[2]*Teaching Faculty, National Law Institute University, Bhopal, India*

ABSTRACT

Internet is growing with an exponential rate, and a rapid increase is also registered in the Internet users especially in the last decade. With the proliferation in the number of Internet users, a simultaneous hike is also seen in mobile users. The advent of Internet and mobile has revolutionized the modern era and forced the society to accept the use of E-commerce and M-commerce due to its enormous benefits. But along with these benefits,security of E-commerce and M-commerce is becoming a global concern. This Research Paper emphasizes on the security issues of E-commerce and M-commerce. The paper also attempts to suggest some countermeasures to address the identified security flaws.

Keywords: *E-Commerce, M-Commerce, Security Issues, Payment Card Industry Data Security Standard (PCI-DSS), SSL, Cardholder Data.*

INTRODUCTION

E-commerce is kind of commercial activity, like delivery of information, services, products, or payments, using computer systems, information technology and communications.[1]Electronic commerce is defined as the use of electronic medium to engage in the exchange, such as buying and selling of products requiring transportation either physically or digitally from one location to the other.[2] E-commerce is the use of electronic communication system and digital information processing in business transactions to create, modify and redefine relationships for value creation between or among organizations, and individual.

E-commerce also makes use of regular technological maintenance to ensure the smooth functioning of websites, monetary online transactions, as well as everything to do with providing and delivering the products. [3]

The term "electronic" can be taken to refer to the worldwide infrastructure ofcomputers,telecommunication technologies and networks upon which the processing, transmission and storage of digitized data takes place. In the context of e-commerce, the word "commerce" refers to an expanding variety of activities like buying, selling, advertising and transactions of all types that amounts to an exchange of value between two parties.

Few examples include banking online auctions, and other financial services, sales of software, and an ever-increasing range of Internet websites offering a variety of consumer products and services.This type of e-commerce includes mobile media and content, travel purchases retail services, and various other similar services.The establishment of a commercial website can provide a small business with access to worldwide markets via the Internet.

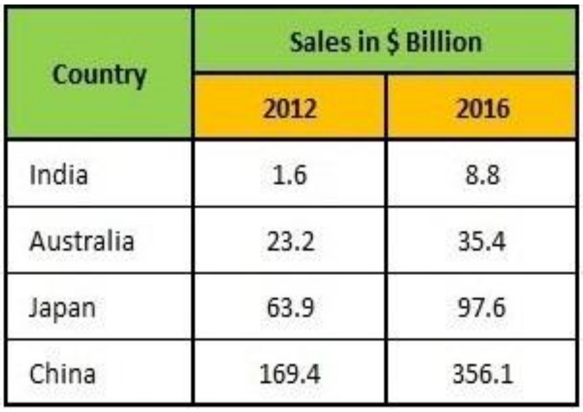
M-commerce can be defined as "any transaction with a monetary value that is conducted via a mobile communications network".[4] M-commerce is a new area arising from the combination of electronic commerce and emerging mobile computing technology.[5]

NEED FOR SECURITY

The universal growth of the Internet has contributed to the transformation of trade and commerce. Currently e-commerce statistics shows that 40 percent of worldwide Internet users have bought goods,products,etc.online via computers, smartphones, tablets or other similar online devices. This points to more than one billion online buyers and is seems to continuously grow with exponential rate in future also.[6]

Mobile commerce expansion is another exciting trend to observe in terms of e-commerce statistics, considering the acceptance and widespread use of computers, tablets andsmartphones. In 2013, US mobile commerce revenue reached to more than 38 billion US dollars.[7]

According to the recent research by Forrester, the e-commerce market in India is regularly growing and became the fastest within the Asia-Pacific region at a CAGR of over 57% between 2012-2016.[8]



Country	Sales in $ Billion	
	2012	2016
India	1.6	8.8
Australia	23.2	35.4
Japan	63.9	97.6
China	169.4	356.1

Fig.1: E-commerce Sale

Mary Meeker's report on Internet Trends of 2015 has shown some interesting facts on the growth of mobile Internet in India.

The fig.2 shows that, over 41 percent of the e-commerce market is driven by mobile trafficin India, which is the highest when compared to any of the country. India is ahead of UK, France,China, Brazil, even USA, when it comes to e-commerce and mobiles.[9]

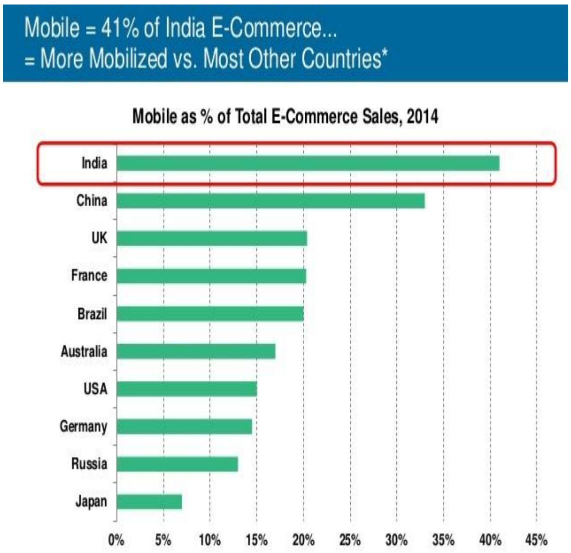


Fig.2: Mobile Internet users (Source: Mary Meeker Report)

The fig.3 displays a forecast of the number of online buyers worldwide up to 2016, based on factual numbers from 2011 to 2012.[10]

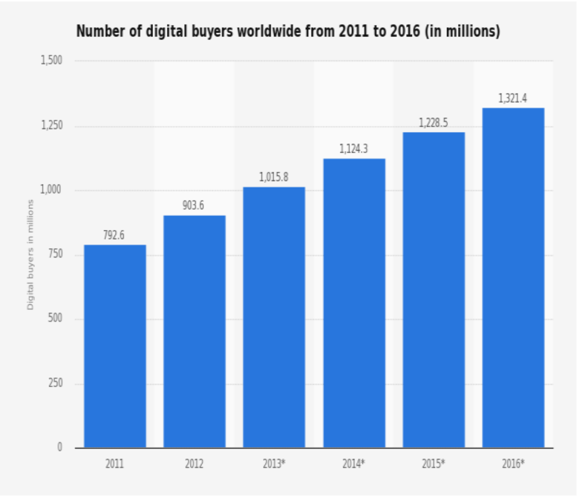


Fig.3: Number of Digital buyers worldwide (Source: Statista 2016)

E-commerce is an important revenue source to many businesses. This is a like boon for the customers preferring to use their computer or tablet for shopping from their home. One of the biggest concern for the customers shopping online is the security of their online transaction.[11] Selecting a better and secure hosting solution is key to protecting customer's data from the hackers and phishing attacks that are so common today.[12]

SECURITY ISSUES IN E-COMMERCE & M-COMMERCE

Session ID

In most E-commerce applications, each session is kept tracked by the server using a unique string of character known as session ID. This ID is how the server differentiates between users as they navigate the site. At first this sounds like a pretty secure way of managing sessions and it seems to solve the issue of one user jumping into another user's session. It sounds good until you begin to perform some tests on the system and discover that each time you log into the application your session ID is incremented by 5. So with the little prediction hacker is able to hijack other users' sessions by using the predictable session IDs. The predictable session IDs can be a serious security hole.[13]

Source Code Exposure

The ability for an attacker to issue requests to an application or web server that return the source code is commonly referred to as a Source Code Exposure exploit. There are many products that are vulnerable to these types of attacks and the information gathered from such an attack can be a gold mine for perpetrating other attacks.

If an attacker can download the code that makes your site do what it does they could possibly learn information about related systems, password storage locations and methods for passing them to other services, file locations and how the site was written in general.[14]

Cookies

When a user attempts to login to a commerce site, some set of credentials (usually a username and password) are presented to the server in order to perform authentication. At this point, cryptographically strong, random session ID cookies are generated and passed to the client's web browser by the server for future authentication. Once the attacker has the session ID cookie he could then introduce a denial of service attack against the client and then take over his session with the server.[15]

Database Security

Database servers are the foundation of most E-Commerce solutions because they generally hold the data that is used to perform transactions. This data usually consists of customer and payment information such as addresses, names, account numbers, credit card numbers and so on.

Availability of the services is another issue that must also be taken into consideration when e-commerce is discussed.No longer is the Web site just for information about an organization. With thesewebsites e-commerce providers generatefunds and provides services to their customers. So, the availability becomes a critical security issue for the e-commerce website.[16]

Security and privacy are the major concerns in m-commerce. For end-to-end security, vulnerabilities in the air interface,the low data rates, the limited computing power of mobile devices, and frequently disconnection of wireless communication are the challenging problems. Hackers are targeting mobile devices as it has been used to access corporate extranets and intranets.However, one of the most challenging aspects of m-commerce is to find out solutions that fulfil users' demand for highly personalized services by securing their privacy.

Mobile applications differ from standard e-commerce applications, because of the following fundamental differences in the technology:

Limitations of Client Devices

Current devices are limited in memory, cryptographic ability, and computational power, etc. As a result, the user cannot carry his entire things along with him, cannot carry out sophisticated cryptographic protocols, and cannot engage in rich GUI interaction.[17]

Portability of Client Device

Devices have the potential to accompany users on all activity, even traditionally online actions away from the desktop. Besides developing the potential for the broader permeation of electronic transactions, this fact also makes loss, theft, and damage of client devices much more likely.[17]

Hidden and Unconscious Computing

To compensate for limiteddevice (computer, phone, etc.) storage, as well as to provide new methods to adapt a user's computing environment to her present physical environment, pervasive computing often permits client devices to transparently interact with the infrastructure without any user's direct interaction. This unconscious interaction can also include downloading executable content.[17]

Location Aware Devices

When the user is mobile, the location of the user can be traced with the help of the infrastructure potential capacity. This knowledge introduces various applications which have noequivalence with the stationary user model.[17]

Merchant Machines

In the e-commerce world, the merchant has powerful machines, with enough storage and computational power, usually in a physically safe place. However, to fully exploit thepotential interaction with the mobile, PDA equipped users, merchant machines may be moved out into the physical world. This step brings up challenges like increased physical exposure, limited computation and state, and limited interconnection.[17]

SUGGESTIVE COUNTERMEASURES

PCI DSS COMPLIANCE

Complying with the Payment Card Industry Data Security Standard(herein after PCI DSS) requires organizations to take all the necessary steps to protect their customer's sensitive data while they do online transaction. These requirements include standards for organization's infrastructure and server setup to ensure your customers' private data remains safe.[18]

The PCI DSS is a set of ample requirements designed for upgrading payment account data security. It was developed by the naissance payment brands of the Payment Card Industry Security Standards Council (PCI SSC), together with American Express, VISA, JCB International, Discover Financial Services and MasterCard, to facilitate the wide-ranging espousal of reliable worldwide data security measures. The standard was developed to augment control around cardholder data (CHD) to trim down credit card frauds through its disclosure. Validation of compliance is carried out every twelve months, either by an external QSA (Qualified Security Assessor) that produces a Report on Compliance (ROC) for businesses managing huge amount of transactions, or through SAQ (Self-Assessment Questionnaire) for businesses managing smaller amount of transactions. PCI DSS initially commenced as five singular programs, i.e.,American Express's Data Security OperatingPolicy, JCB International's Data Security Program,VISA's Cardholder Information Security Program,Discover Financial Services's Information Security and Compliance and MasterCard's Site Data Protection. All corporations' (i.e. AmEx, VISA, JCB, Discover and MasterCard) objectives were almost analogous "to create an additional level of protection for card issuers via guarantying that merchants meet up bare minimum levels of security when they perform storing, processing and transmission cardholder data (CHD)."This standard provides 12 requirements and 185 sub-requirements to secure Card Holder Data, the channel from where card holder data moves and the place where it is stored.

The PCI DSS standard is pertinentto any organization that processes, transmits or stores cardholder data (CHD).Either you are a merchant the PCI DSS is pertinent on you. Even if the merchant hasdelegated all PCI DSS doings to a third party, it is the merchant'saccountability for guarantying that all theparties who are in contract are biddable with the standardor you are a service provider, together with a software developer, the PCI DSS is appropriate for you if youstore,process, or transmit cardholder data (CHD), or your actionsinfluence the security of the cardholder data as it is being processed, transmitted or stored or you are an acquirer or a processor or an issuer the standard is pertinent to you as well as all those entities that process, transmit or store cardholder data (CHD) and/or sensitive authentication data (SAD).

The PCI DSS standard may apply obliquely to the entire organization or to a division of that organization if they have correctly classified the processing,storing,ortransmission of the cardholder data away from the rest of their organization.

It is applicable to all people, processes and technologies that are concerned with the storing,processing, or transmission of cardholder data. It is not only concerned with the electronic systems, but it also embraces systems including paper records like receipts, mail order forms, etc.

PCI DSS has ample requirements among which Requirement No. 3 straightforwardly says Protect Stored Cardholder Data that means if any organization is storing cardholder data shall use ample number of safeguards to protect the same. All accumulated data must be encrypted. Some details should never be stored, e.g. CVV Number, PIN numbers and the full details on the magnetic strip. PCI DSS is a strict and as on date security standard if anything mentioned in the standard is not followed by the compliant organization that straight away moves that organization towards non-compliance to PCI DSS.

PCI DSS version 3.1 includes few updates that are extremely less prominent than the SSL/ early TLS changes, but are equally important. The release of PCI DSSv3.1 brought renewed attention to the compliance programs.Merchants and service providers develop their electronic payment security infrastructure. The majority of the attention is focused on the retirement of SSL and early TLS protocols as an effective encryption methods for sensitive cardholder data. Lacunae in these encryption protocols requires an instant fix. Throughout the world, merchants and service providers are scrambled to identify uses of the outdated methods, proceduresand technologies in their environments and find appropriate alternatives.

This is not only the change in the latest version of PCI-DSS. Several other minor changes that requires the attention of service providers and merchants took place as well. Organizations seeking to complywith PCI DSS may desire to review the SSL updates and the set of requirements that went into effect earlier last year.

Firewalls

Firewalls are a proactive defense for the infrastructure from the constant threat of new and advanced malware, viruses, and malicious Internet traffic. It allows for constant scan on server's activity and are designed to adapt to latest and new threats through signature-based intrusion prevention without slowing down data traffic.[19]

SSL Certificate Services

Secure Sockets Layer (SSL) is a technology for establishing an encrypted link between a server and a client typically a website and a browser; or a mail server and a mail client.[20] Secure Sockets Layer Certificate is a kind of data file which digitally bind a cryptographic key to an organization's details. When it is installed on a webserver, it immediately activates a padlock and the https protocol (over port no. 443) and allows secure connections to web browser from a webserver. SSL is also used to secure credit card transactions, data transfer, logins, and more recently is becoming astandard when securing the browsing of social media sites.[21]

An organization needs to install the SSL Certificate onthe webserver to initiate a secure session with browser. Depending on the type of SSL Certificate applied for, the organizations will be required to go through the differentstages of screening. Once it is installed, than it will be possible to connect to the website,as this states the server to establish a secure connection with the web browser. Once this secure connection is established, the web traffic between the webserver and the web browser will be secured.[22]

Database Servers Security

There are many methods of protecting database servers from encrypting the data that resides on the actual disks to using complex authentication methods. One simple way to offer protection is to place the server on a separate network segment so that connections are made through a firewall or proxy server. Depending on which vendor's product you choose you will have a range of options for adding security to your database server, and you should seriously consider the security features of any product when deciding on which database to use.

Multi-factor Authentication

Multifactor authentication (MFA) is a system that requires more than oneauthentication methods for authentication to verify the user's identity at the time of any transaction. MFAcombines two or more independent credentials i.e., what the user knows, what the user is and what the user has. The aim of MFA is to implement the concept of 'Defense in Depth' and make it harder for an unauthorized person to access a target. If one of the factor is compromised, the attacker still has at least one or more barrier to break before successfully breaching into the target.[23]

Secure Electronic Transaction (SET)

It is a system for ensuring security of the monetary transactions on the Internet. It wasinitially supported by Mastercard, Netscape,Visa, Microsoft, and others. SET protocol was designed to ensure the security and integrity of online communications and purchase. SET uses digital certificates, issued to merchants and customers, to perform a series of security checks verifying that an identity of a customer is valid.SET provides basic framework within which many of the various components of securing digital transaction functions. SET uses some but not all aspects of a public key infrastructure (PKI).[24]

CONCLUSION

The benefits proposed by E-commerce and M-commerce has somehow suppressed the flaws in the system, but for gaining trust and assurance among the customers, the e-commerce and M-commerce service providers are required to implement an appropriate security methods, procedures and compliance. The counter measures suggested in this research paper if implemented effectively may lead to the reduction in the security flaws present in the E-commerce and M-commerce.

REFERENCES

[1] Lisa K. Abe, "Internet and E-Commerce Agreements Drafting and Negotiating Tips"

[2] http://www.manupatrafast.com/articles/PopOpenArticle.aspx?ID=f3c75cea-57c1-4b7e-a881-3c5a339eddc7&txtsearch=Subject:%20Taxation

[3] http://www.statista.com/markets/413/e-commerce/

[4] Norman Sadeh, "M-commerce, Technologies, Services, and Business Models" Wiley, ISBN: 0-471-135-85-2.

[5] Suresh Charil, Parviz Kermanil, Sean Smith, and Leandros Tassiulas, "Security Issues in M-Commerce: A Usage Based Taxonomy".

[6] http://www.statista.com/markets/413/e-commerce/

[7] http://www.statista.com/markets/413/e-commerce/

[8] https://www.forrester.com//search?N=10001&range=504005&sort=3&searchRefinement=reports

[9] http://indianexpress.com/article/technology/tech-news-technology/mary-meeker-report-these-slides-confirm-that-in-india-mobile-internet-is-the-driving-force/>

[10] http://www.statista.com/statistics/251666/number-of-digital-buyers-worldwide/>

[11] http://www.liquidweb.com/blog/index.php/top-5-e-commerce-security-needs/>

[12] http://www.liquidweb.com/blog/index.php/top-5-e-commerce-security-needs/>

[13] "WebSphere Cookie and Session-id Predictability" October 4, 2001, Available at <http://neworder.box.sk/showme.php3?id=5708

[14] "IBM WCS JSP Source Code Exposure" May 30, 2001, Available at <http://neworder.box.sk/showme.php3?id=4336

[15] Remote Retrieval of IIS Session Cookies from web browsers" October 29, 2000, Available at<http://neworder.box.sk/showme.php3?id=3153>

[16] <http://searchsecurity.techtarget.com/tip/E-Commerce-Security-Needs>

[17] Suresh Charil, Parviz Kermanil, Sean Smith, and Leandros Tassiulas, "Security Issues in M-Commerce: A Usage Based Taxonomy"

[18] http://www.liquidweb.com/blog/index.php/top-5-e-commerce-security-needs/

[19] http://www.liquidweb.com/blog/index.php/top-5-e-commerce-security-needs/

[20] <https://www.digicert.com/ssl.htm>

[21] https://www.globalsign.com/en/ssl-information-center/what-is-an-ssl-certificate/

[22] https://www.globalsign.com/en/ssl-information-center/what-is-an-ssl-certificate/

[23] http://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA

[24] http://searchfinancialsecurity.techtarget.com/definition/Secure-Electronic-Transaction

[25] Margaret Jane Radin, John A. Rothchild & Gregory M. Silverman , Internet Commerce: The Emerging Legal Framework, Second Edition, Foundation Press, 2006

[26] Stephen York & Ken Chia(eds.), E-commerce: A Guide to the law of Electronic Business, Buttersworths, 2000

[27] Nandan Kamath(ed.), Law Relating to Computers, Internet and E-Commerce, Second Edition, Universal Law Publishing Co. Pvt Ltd, 2000