E- SECURITY THREATS AND TECHNOLOGY SOLUTIONS

Dr. Nidhi Dhawan

Assistant Professor, Department of Commerce, Zakir Husain Delhi College, University of Delhi

ABSTRACT

Transaction (buying and selling) over the internet is e-commerce just like any normal transaction that involves transfer of ownership rights. It is just that it all takes place through internet in the virtual world unlike traditional system or face to face system. This online transaction is possible through various softwares in the form of payment gateways, computer systems, internet, and net banking system. The internet was started to provide a communication channel all over the world and to be used as an information tool. E-commerce is growing at a tremendous speed with the excessive amount of data sharing and the tremendous number of users connected. There are enormous opportunities for unauthorized users to access confidential data. Security is an important factor in virtual transactions. It is the protection of any device, computer or any network from unauthorised access. This paper highlights the importance and basic needs of e-security authenticity, integrity, non repudiation, and authorisation. The various threats to internet security communication channel threat, client and server threat and technological solutions available for internet security.

Keywords: E-security, Technology, Threats, Security needs

I. INTERNET SECURITY

An act of doing transactions (buying and selling) over the internet is e-Commerce just like any normal transaction that involves transfer of ownership rights. It is just that it all takes place through internet in the virtual world unlike traditional system or face to face system. This online transaction is possible through various softwares in the form of payment gateways, computer systems, internet, and net banking system. The internet was started to provide a communication channel all over the world and to be used as an information tool. E-commerce is growing at a tremendous speed with the excessive amount of data sharing and the tremendous number of users connected. There are enormous opportunities for unauthorized users to access confidential data. ***Security is the protection of any device, computer or any network from unauthorised access.***

II. DEFINITION

Gralla (2007) Internet security is a branch of computer security specifically related to the Internet, often involving browser security but also network security on a more general level as it applies to other applications or operating systems on a whole.

Internet security is defined as a process to create rules and actions to take to protect against attacks over the Internet. [8]

III. LITERATURE REVIEW

Reed (2003) Attacks are known to either be intentional or unintentional and technically competent intruders have been interested in targeting the protocols used for secure communication between networking devices.

E. Kalaikavitha et al. (2013) reported the encrypted OTP system how helps in our routine life as well as how it work from user to mobile and authentication system. They are also explained different methods for OTP generation as well as mathematical formulae for the generation of OTP.

A. Shesashaayee (2014) explained regarding encrypted OTP in mobile system how we ca n protected our data.

Chun Hu (2008) explained a general mechanism, for the detection and protection from wormhole which is called as packet lashes.

Costello (2003) envisaged that further developments in the mobile payments content were inevitable in the near future. Mobile devices might be used in micro-payments such as parking, tickets, and charging mobile phones.

Ghanaweb (2004) with credit and debit cards, consumers cannot detect fraud until their statement of accounts arrives but credit card companies and banks do not insure against fraudulent use of their cards. Hence consumers bear the full responsibility of any debts fraudulently accrued.

Roy Anindya & Chopra Anil (2005) has revealed that hackers are getting new and some surprising techniques to acquire the information of our bank account. The latest ways like phishing and others may lead us to some websites which do not exist there.

Costello, D (2003) Preventative and real-time defence methods implemented by an Enterprise to protect its and business network against potential threats that may impede or paralyze the system. Safeguards business-sensitive information and applications from malicious sources through combined efforts of IT strategies, software and hardware.

IV. OBJECTIVES OF STUDY

The objectives of present paper are stated as follows:

1. To know the concept of security on the internet and basic e-security needs
2. To understand various threats to internet security
3. To know about technology solutions for internet security threats

V. RESEARCH METHODOLOGY

The methodology used for data collection includes use of secondary data such as various articles, journals, books, websites, etc. and all the data included in this article has been given the reference wherever necessary.

VI. BASIC E-SECURITY NEEDS

Technology alone is inadequate to ensure security. Sound transaction security must protect information. The risks inherit in e-commerce can be harnessed only through appropriate security measures and business and legal procedures that ensure the integrity and reliability of internet transactions. *Transactions may be attacked by passive or active threats. Passive intrusion threatens the loss of privacy and confidentiality of data but an active intrusion may result in the intruder assuming someone else identity and creating transactions on their behalf through fabrication.* Lack of transaction security has made many customers not to make payments over the internet out of fear and security reasons. Security concerns generally involve these issues:

a) Authenticity

Authenticity makes sure that message senders are who say they are. It is to verify the identity of a person from whom the communication message is generated.

b) Integrity

Integrity ensures that the information is not accidentally or maliciously altered or corrupted in transit.

c)Non –Repudiation

Non –Repudiation ensures that the principal or sender of the message cannot deny that he or she sent the message.

d) Confidentiality

Confidentiality is to know who is to read the data and ensuring that information in the network remains private.

e)Authorization

Authorization is to restrict the use of resources to authorized users. Authorization pertains to the permission granted to a person or a process to do certain things.

V. THREATS TO INTERNET SECURITY

The threats to internet security can be many that relate to client security, message integrity, harm to computer software or hardware.

a) **Communication Channel Threats** includes secrecy threat, integrity, vandalism, and spoofing.

b) **Client Threats** Malicious data is an example or result of client threat. *Malicious code* refers to viruses, worms (a self-replicating program) that is self-contained and does not require a host program. e.g., Trojan horse, logic bomb, and other deviant software programs.

c) **Server Threats** Server is an interface between a customer and a supplier. The server is highly vulnerable and is a threat to client-internet server group. Threats of the server include the threat to utility programs, database, web server and common gateway interface.

VI. TECHNOLOGY SOLUTION FOR E-COMMERCE SECURITY AT DIFFERENT LEVELS

Site Security Solutions To secure services and network at sites location, the following factors must be considered:

i.The *"deny all"* model in which all the services are turn off and then selectively, services are enabled on case by case basis as required.

ii. The *"allow all"* model in which all the services are turn on usually with the default at the host level; and allowing all protocols to travel across network boundaries.

VII. NETWORK SECURITY SOLUTIONS

Firewalls- regulate the activities between networks within the same organization. The firewall provides a strict controlled access to host, protection from services which are more prone to attacks, maintain the statistics of network use and misuse.

Client Server Security Solutions Various client- server network security methods are stated as follows:

- **Security through Obscurity**

Security through Obscurity method is particularly used by small group or organization that can be made secure as long as nobody outside its management group is allowed to find out anything about its operational details and users are provided information on a need –to know basis.

- **Password Schemes**

Vital information can be protected by using passwords. It is widely used in network security. In password schemes, generally eight character length mixed case alphanumeric characters are chosen as password. The majority of hackers access client computers because of easy passwords. .

- **Biometric Systems**

Biometric System is considered as the most secured of security methods. In this method, unique aspects of a person's body are taken as a recognition pattern. E.g. finger prints, palm prints, retinal patterns of eyes, signatures or voice recognition.

- **Use of Anti- Virus software**

Client must always use the protection method and that is to scan for malicious data and program fragments that are transferred from the server to the client, and filter out data and programs known to be dangerous.

VIII. SERVICES SECURITY- WEB SERVER OR HTTP SERVER AND CGI SERVER

The security of E-Commerce by and large depends upon the ability to secure the host environment, the security of the server that provides the service and a safe network environment for transactions to take place. The server containing the information and resources is always the focal point of attack by hackers and needs to be protected and at the same time, it has to make information available and carry out transaction with clients. For this purpose, a server software that supports e-commerce needs to be installed and operated on the host site.

CGI scripts can present security holes by intentional or unintentional leaks of information about the host system that will help hackers break in and by scripts that process remote user input, such as the contents of a form or a "searchable index" command, may be vulnerable to attacks in which the remote user tricks them into executing commands.

IX. PROTECTING CONFIDENTIAL DOCUMENTS AT SITE

It is possible to restrict access to confidential documents for the purpose of security by restricting IP address, subnet or domain. IP address restriction can be made much safer by running your server behind a firewall machine that is capable of detecting and rejecting attempts at spoofing IP addresses. Such detection works best for intercepting packets from the outside world that claim to be from trusted machines on your internal network. Restriction can be created by user name and password for directories and documents for remote user access. Restriction on documents can be imposed by encryption using public key cryptography. Both the request for the document and the document itself are encrypted in such a way that the text cannot be read by anyone but the intended recipient. Public key cryptography can also be used for reliable user verification

X. TRANSACTION SECURITY SOLUTIONS

The internet is a public network consisting of thousands of private computer networks that are connected together in a myriad of ways. A computer network system is exposed to threats that may arise from anywhere on the public network. Changes in attitudes towards security have opened the door to serious considerations of security technology. In e- commerce, security can make or break a business; it has already become a strategic asset. It is the best way to protect the information flow, ensure integrity and reinforce customer confidence. The transaction security issues can be divided into two types:

Data Security- The major threat to data security is unauthorized network monitoring, also called packet sniffing. A sniffer also called a cracker, or a person or a program that uses the internet to record information that transmits through a router from its source to destination.

Message Security- includes Message confidentiality, Message and System Integrity, and Message Sender and Authentication/ Identification

IX. CONCLUSION

Internet security is the protection of any device, computer or any network from unauthorised access. If one wants to transact online, it is very important to have a prior knowledge of internet and various threats related to it. The internet was started to provide a communication channel all over the world and to be used as an information tool. Technology alone is inadequate to ensure security. Sound transaction security must protect information. The risks inherit in e-commerce can be harnessed only through appropriate security measures and business and legal procedures that ensure the integrity and reliability of internet transactions. The various security measures at different levels are must to be followed in order to protect our systems always.

REFERENCES

[1.] A. & R. Anindya "New threats to online banking".

[2.] Costello, D (2003). Mobility and micropayment (online) June, Zafion, available: http://www.epays.com/downloads/zafion_WP.pdf (2005-03-24)

[3.] D. A. Shesashaayee, D. Sumathy, (2014.) 'OTP Encryption Techniques in Mobiles for Authentication and Transaction Security', International Journal of Innovative Research in Computer and communication engineering, Vol. 2, Issue 10

[4.] E. Kalaikavitha, J Gnanselvi, (2013) 'Secure Login Using Encrypted One Time Password (Otp) and Mobile Based Login Methodology', Research Inventory: International Journal of Engineering and Science, Vol. 2, Issue 10, pp. 14-17,.

[5.] Ghanaian Chronicle (2004). Only 5% of Ghanaians have bank account (online), available: http://www.ghanaweb.com/GhanaHomePage/NewsArchive/artikel.php?ID=65088 (2005- 01-29).

[6.] *Gralla, Preston (2007). How the Internet Works. Indianapolis: Que Pub. ISBN 0-7897-2132-5.*

[7.] http://searchsecurity.techtarget.com/definition/security

[8.] http://www.yourdictionary.com/internet-security

[9.] John Sherwood SALSA: A Method for Developing the Enterprise Security Architecture and Strategy, 18 Braemore Road, Hove, East Sussex, BN3 4HB, UK.

[10.] Y. Chun Hu, (2008) 'WAP: Wormhole Attack Preventation Algorithm in Mobile Ad Hoc Networks', IEEE International conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, SUTC' 08. pp. 343-348