SECURITY (STRATEGY OF E-COMMERCE CHARACTERISTICS USING RESEARCH IMPLEMENTATION TECHNOLOGY.)

Threats and Protection

[1] Prachi Nirmal Mehta,[2] Vaidehi Atmaram Patil
[1] Teacher,[2] Professor
[1] English,
[1] Atmaram Tutorials, Virar, India.

Abstract : E-commerce has been very significant for our day to day life .but one important limitation is there has been increasing challenges in the important structure of confidential information for successfully in producing a desired or intended result for information, security , privacy or personal data and particularly data protection .Protection is must because exchange security on network is very important for e-commerce service and it is always the major factor that affects the success of e-commerce .[1]
In this paper, you all would be having guidelines regarding threats and protection of e-commerce.

IndexTerms - E-commerce, Security issues, Threats, Protection.

I. Introduction:-

The fast growth of e-commerce is gaining attention of users with its characteristics high-efficiency, low cost, high profitability and global application. The Internet and WWW gradually evolved E-commerce. It has been a revolution for the traditional ways of doing business. Now-a-days the popularity of E-commerce increases the fear of data hacking and threats are also increasing. Here, I am

Representing the different threats regarding towards E-transaction and E-business and also try to explain different security schemes to protect the data and E-transaction methods. Many business and consumers are still cautious for online transaction as user have to give many sensitive information which is very confidential.

So make them believe and interest in user for up-gradation of E-commerce globally, the aim of this paper is to provide thorough overview about the threats and protection of E-commerce.

.

II. Security issues related to E-transaction and E-business environment:-[3][5]

1. Malicious code:- Malicious code is a code that is hazardous for the system or computer as it can be easily damage. It is not possible to protect through antivirus applications or tools. It can be generated itself or by attachments and irrelevant action done by users. If malicious code is activated or entered in server than it can damage whole system and corrupt the data. There are various others forms of Malicious code:-Viruses, Worms, Trojan horses.
   Precaution:-To stop the Malicious code some precaution can be taken:-
   (a)Do not open the attachment from unknown source.
   (b)Unwanted software should be deleted.
   (c)Antivirus should be installed and updated before expiration of application tools.

2. Hacking:-It is a trick to get access and use of system through an unauthorized and illicit way for an illicit purpose.[9]
   Hacking is done through breaches.
   To know hacking in a better way, one need to understand hackers. Hackers are of various types depending upon their intent.
   (a)Ethical hacker (White hat):-A person who do the process of hacking with legal permission of authority for the betterment and protection of business.[9]

Ethical hackers perform VAPT (Vulnerability Assessment and Penetration Testing).There is of 2types of Vulnerability Testing. Both VAPT have different tasks or performance but have same aim or area of focus.[10]
Vulnerability is a perceptual, conditional and somewhat subjective attribute of being easily attacked.[10]
(b)Cracker (Black hat):-A person who do unauthorized access for illegal or personal gains.The intent is usually to steal corporate data, transfer funds from account, etc.
(c)Grey hat:- Unauthorized access for the help of system owner for identifying weakness.
(d)Script kiddies:-A common individual with sort knowledge of computer just to explore the readymade tools and application of computer.

3. Credit card fraud: - Credit card fraud is a form of identity theft in which an individual uses someone else's credit card information to charge purchases, or to withdraw funds from the account.
As per data by government in lok sabha, 12,978 cases of fraud were reported to all schedule bank in two year 2016-2017 in which 8622 fraud of public sector in 2014-2015, 4156 in private sector in 2014-2015and after one year public sector bank issues reduced in 4146 and private sector 568.[11]

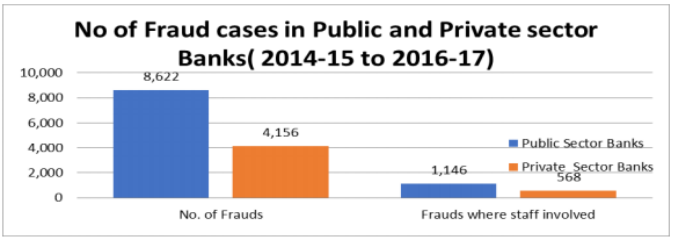

figure no 1:graph on frauds since 2014.[11]

4. Spoofing:-A spoofing attack is a situation or condition in which an individual or program successfully pretend as another by fake data to gain an unauthorized way for favorable circumstances. Email spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source. Email spoofing is a popular tactic used in phishing and spam campaigns because people are more likely to open an email when they think it has been sent by a legitimate or familiar source. The goal of email spoofing is to get recipients to open, and possibly even respond to, a solicitation.

There things to watch out for include:

- The email sender address: sometimes addresses will be spoofed by changing one or two letters in either the local-part (before the @ symbol) or domain name.
- The URL of a webpage: similar to email addresses, the spelling can be slightly changed to trick a visitor not looking closely

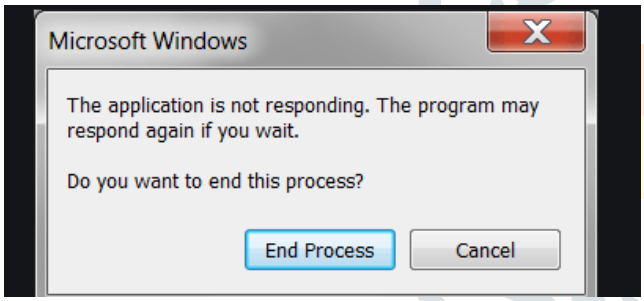

figure no 2: spoofing.

5. Denial of service attacks:-It is a attack where the person who is attacking attempt to prevent legitimate user from accessing the services.
DoS attack can be done in a several ways. The basic types of DoS attack include:
Flooding the network to prevent legitimate network traffic.[7]

(a)Disrupting the connections between two machines, thus preventing access to a service.[6]

(b)Preventing a particular individual from accessing a service.[6]

(c)Disrupting a service to a specific system or individual.[6]

(d)Disrupting the state of information, such resetting of TCP sessions.[6]

Another variant of the DoS is the smurf attack. This involves emails with automatic responses. If someone emails hundreds of email messages with a fake return email address to hundreds of people in an organization with an auto responder on in their email, the initial sent messages can become thousands sent to the fake email address. If that fake email address actually belongs to someone, this can overwhelm that person's account.

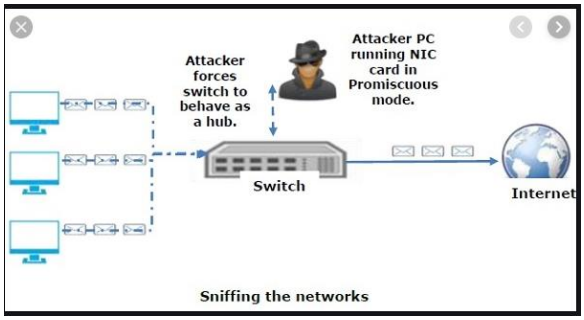

figure no 3: process of dos.[7]

What is the difference between "http" and "https"?
Time to know this, with 32 lakh Debit Cards compromised in India!
Some of you may be aware of this difference, but it is worth sharing for many those who are not.
The main difference between "http://" and "https://" is all about keeping you secure.

"http" stands for "Hyper Text Transfer Protocol".
The "s" (big surprise) stands for "Secure". If you visit a Website or Web Page, and look at the address in the Web Browser, it is likely to begin with the following: "http://"

This means that the Website is talking to your Browser using the regular unsecured language. In other words, it is possible for someone to “eavesdrop" on your computer's conversation with the Website. If you fill out a form on the Website, someone might see the information you send to that site. [2]

This is why you never ever enter your Credit Card Number in an "http://" Website! But if the Web address begins with "https://",that means your Computer is talking to the Website in a Secure Code that no one can eavesdrop on.

Now, hope you understood why this is so important.

If a Website ever asks you to enter your Credit/Debit Card Information, you should automatically look to see if the Web Address begins with “https://" Use

If it doesn't, you should NEVER enter any Sensitive Information such as Credit/Debit Card Number etc.

While checking the name of any Website, first look for the domain extension (Eg: ".com" or ".org", ".co. In", ".net" etc). The name just before this is the domain name of the Website. Eg: in the above case, "http://amazon.diwali -festivals.com", the word before ".com" is "diwali-festivals" (and NOT "amazon"). So, this Webpage does not belong to "amazon.com" but belongs to "diwali-festivals.com", which we all haven't heard of before.You can similarly check for bank frauds.
Before your e-banking logins, make sure that the name just before ".com" is the name of your bank. Eg: "something. icicibank.com" belongs to Icici; but, "Icici bank. some1else.com" belongs to "some1else."

Reference:

[1] An Overview on Web Security Threats and Impact to E-Commerce Success by Hatoon Matbouli and Qigang Gao. 2012 International Conference on Information Technology and e-services.

[2] Privacy, how can I protect you? How to construct safe data security system in e-commerce transaction by Wang Haoyu. 2012 Fourth International Conference on Computational and Information Sciences.

[3] Study on Security Framework in E-Commerce by Lu Tao and Lei Xue. 1-4244-1312-5/07/ © 2007 IEEE.

[4] Threat Modeling approaches and Tools for Securing Architectural designs of an E-banking Application by Caroline Möckel and Ali E. Abdallah. 2010 Sixth International Conference on Information Assurance and Security.

[5] Security Issues in Networks with Internet Access by Carl E. Landwehr, Member, IEEE, And David M. Goldschlag .IEEE, Vol. 85, No. 12, December 1997.

[6] www.esecurityplanet.com

[7] www.techopedia.com

[8] www.forcepoint.com

[9] economictimes.indiatimes.com

[10] www.veracode.com

[11]https://www.google.com/search?q=credit+card+fraud&biw=1366&bih=657&source=lnms&sa=X&ved=0ahUKEwi93vWftorlAhWIvY8KHUSEAKcQ_AUIDSgA