The Study of E-Commerce Security Issues and Solutions

Sangeetha M K
MS(IT),IV Sem
Jain University,Bangalore

Prof. Dr. Suchitra R
Head of the dept
Jain University,Bangalore

***Abstract*:- The E-commerce Security is part of the Information Security framework and is specifically applied to components that affect e-commerce that includes the Computer Security, Data security and other wider realms of the Information Security framework. E-commerce security has its own particular and is the highest visible to security components that affect the end user through their daily payment interaction with the business. E-commerce security is the protection of e-commerce is assets from unauthorized access, use, alteration, or destruction. Dimensions of e-commerce security-Integrity is common, Non-repudiation, Authenticity, Confidentiality, Privacy, Availability. E-Commerce offers the banking industry great opportunity of E-commerce, but also creates a set of new risks and vulnerability such as security threats are over the internet. Still, its definition is a complex Endeavour due to the constant technological and in this paper we discussed the Overview of E-commerce security, Understand the Online Shopping Steps to place an order, Purpose of Security in E-commerce and, Different security issues in E-commerce, Secure online shopping guidelines.**

Keywords*: *E-Commerce has Security Issues, Security measures, Digital E-commerce cycle/Online Shopping, Security Threats, Secure online shopping guidelines.

INTRODUCTION

E-commerce Security is a part of Information Security of the framework and is specifically applied to the component s that affect e-commerce include Computer Security, Data security and other wider realms of the Information Security framework. E-commerce security has its own particulars nuances and is one of highest visible security components that affect the end user through their daily payment interactions with their business. Today, privacy and security are a major concern for the electronic technologies. M-commerce shares security concerns with other technologies in the field. Privacy concerns have been found, to revealing a lack of trust in a variety of contexts, including commerce, electronic health records, the e-recruitment technology and social networking, has directly influenced users. Security is one of the principal and continuing concerns that restrict customers and organization engaging with ecommerce. Web e-commerce applications that handle payments and (online banking, electronic transactions or using debit cards, credit cards, PayPal or other tokens) have more compliance in issues, are at increased risk from being targeted than other websites and there are greater consequences if there is data loss or alteration. Online shopping through shopping websites having certain steps to buy a product with safe and secure. The ecommerce industry is slowly addressing security issues on their internal networks. There are guidelines for securing systems and networks available for the ecommerce systems personnel to read and implement. Educating the consumer on security issues is still in the infancy stage but will prove to be the most critical element of the e-commerce security architecture. Trojan horse programs launched against client systems pose the greatest threat to e -commerce because they can bypass or subvert most of the authentication and authorization mechanisms used in an ecommerce transaction. These programs can be installed on a remote computer by the simplest of means: email attachments. Privacy has become a major concern for consumers with the rise of identity theft and impersonation, and any concern for cons umers must be treated as a major concern for e- Commerce providers.

WEB SECURITY

The web Security is one of the principal and continuing concerns that restrict customers and organizations engaging with ecommerce. The aim of this seminar is to explore the perception of security in e -commerce B2C and C2C websites from both customer and organizational perspectives. [1] With the rapid development of E-commerce, security issues are arising from people's attention. The security of the transaction is the core and key issues of the development of E-commerce. This seminar about the security issues of Ecommerce activities put forward solution strategy from two aspects that are technology and system, so as to improve the environment for the development of E-commerce and promote the further development of E-commerce. [2] Web applications increasingly integrate third-party services. The integration introduces new security challenges due to the complexity for an application to coordinate its internal states with those of the component services and the web client across the Internet. [3] Each phase of E-commerce transaction has a security measures.

E-commerce Transaction Phases			
Information Phase	Negotiation Phase	Payment Phase	Delivery Phase
Security Measures			
Confidentiality Access Control Integrity Checks	Secure Contract Identification Digital Signatures	Encry-ption	Secure Delivery Integrity Checks

Viruses are a nuisance threat in the e-commerce world. They only disrupt e-commerce operations and should be classified as a Denial of Service (DoS) tool. The Trojan horse remote control programs and their commercial equivalents are the most serious threat to e-commerce. Trojan horse programs allow data integrity and fraud attacks to originate from a seemingly valid client system and can be extremely difficult to resolve. A hacker could initiate fraudulent orders from a victim system and the ecommerce server wouldn‘t know the order was fake or real. Password protection, encrypted client-server communication, public private key encryption schemes are all negated by the simple fact that the Trojan horse program allows the hacker to see all clear-text before it gets encrypted.

Due to the increase in warnings by the media from security and privacy breaches like identity theft and financial fraud, and the elevated awareness of online customers about the threats of performing transactions online, e - commerce has not been able to achieve its full potential. Many customers refuse to perform online transactions and relate that to the lack of trust or fear for their personal information.

DIGITAL E-COMMERCE CYCLE

Security is very important in online shopping sites. Now days, a huge amount is being purchased on the internet, because it‘s easier and more convenient. Almost anything can be bought such as music, toys clothing, cars, food and even porn. Even though some of these purchases are illegal we will be focusing on all the item‘s you can buy legally on the internet. Some of the popular websites are eBay, iTunes, Amazon, HMV, Mercantile, dell, Best Buy and much more.

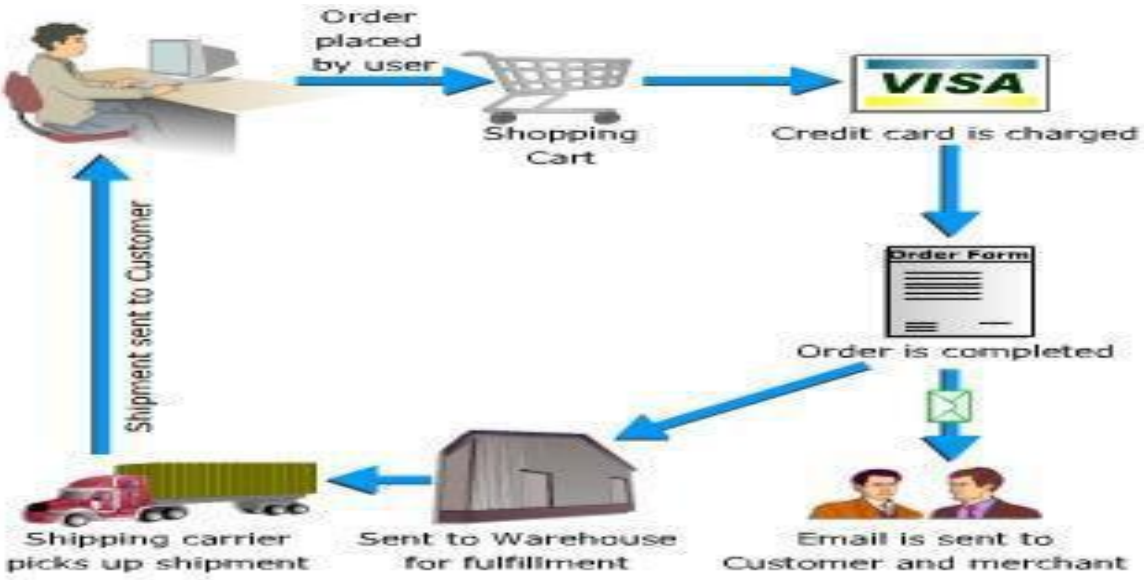
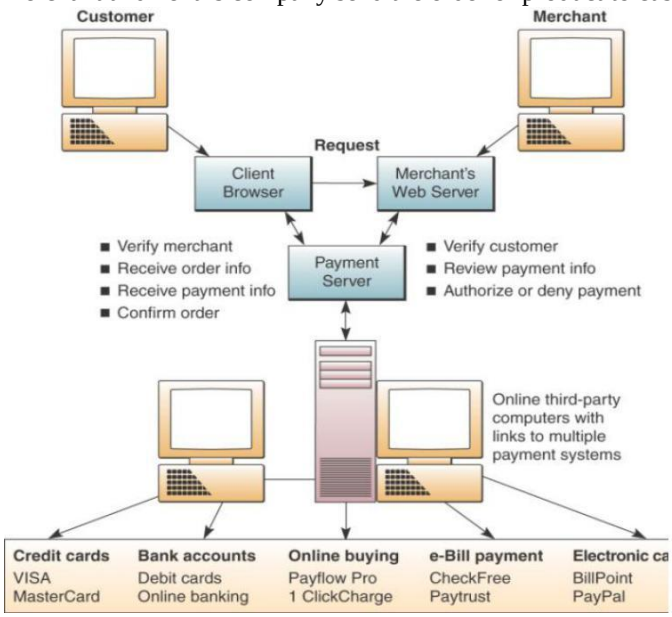
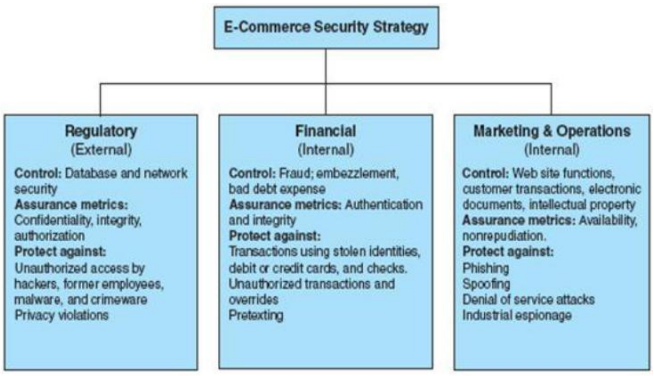


Figure 2: Digital E-commerce cycle

In this figure the user enter data in the computer if all information is correct then next procedure is done then next user enter the credit and debit card information for payment the Order . Then next order is complete the email is sent to customer and merchant and next is company send the order of product to customer home.





VI. PURPOSE OF SECURITY

1. Data Confidentiality – is provided by encryption / decryption.
2. Authentication and Identification – ensuring that someone is who he or she claims to be is implemented with digital signatures.
3. Access Control – governs what resources a user may access on the system. Uses valid IDs and passwords.
4. Data Integrity – ensures info has not been tampered with. Is implemented by message digest or hashing.
5. Non-repudiation – not to deny a sale or purchase Implemented with digital signatures.

__ Plaintext/Cleartext – message humans can read.

__ Ciphertext – unreadable to humans, uses encryption. Reverse process is call decryption.

__ A cryptographic algorithm is called a cipher. It is a mathematical function. Most attacks are focused on finding the ―key.

SECURITY ISSUES

E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. While security features do not guarantee a secure system, they are necessary to build a secure system.

Security features have four categories:

- Authentication: Verifies who you say you are. It enforces that you are the only one allowed to logon to your Internet banking account.

- Authorization: Allows only you to manipulate your resources in specific ways. This prevents you from increasing the balance of your account or deleting a bill.
- Encryption: Deals with information hiding. It ensures you cannot spy on others during Internet banking transactions.
- Auditing: Keeps a record of operations. Merchants use auditing to prove that you bought a spec ific merchandise.
- Integrity: prevention against unauthorized data modification
- Nonrepudiation: prevention against any one party from reneging on an agreement after the fact
- Availability: prevention against data delays or removal.

–DDOS (distributed denial of service attacks) involves hackers placing software agents onto a number of third - party systems and setting them off to simultaneously send requests to an intended target

•Sniffers–software that illegally access data traversing across the network.

•Theft of software via illegal copying from company‘s servers.
•Theft of hardware, specifically laptops.

SECURE ONLINE SHOPPING GUIDELINES

1. Shop at Secure Web Sites

How can we tell if a Web site is secure? Secure sites use encryption technology to transfer information from your computer to the online merchant's computer. Here's how you can tell when you are dealing with a secure site:

- If you look at the top of your screen where the Web site address is displayed (the "address bar"), you should see https://. The "s" that is displayed after "http" indicates that Web site is secure. Often, you do not see the "s" until you actually move to the order page on the Web site.
- Another way to determine if a Web site is secure is to look for a closed padlock displayed on the address bar of your screen. If that lock is open, you should assume it is not a secure site.

2. Research the Web Site before You Order

Do business with companies you already know. If the company is unfamiliar, do your homework before buying their products. If you decide to buy something from an unknown company, start out with an inexpensive order to learn if the company is trustworthy. Reliable companies should advertise their physical business address and at least one phone number, either customer service or an order line.

3.Read the Web Site's Privacy and Security Policies

Every reputable online Web site offers information about how it processes your order. It is usually listed in the section entitled ―Privacy Policy. You can find out if the merchant intends to share your information with a third party or affiliate company. Do they require these companies to refrain from marketin g to their customers? If not, you can expect to receive ―spam (unsolicited email) and even mail or phone solicitations from these companies

4. Be Aware of Cookies and Behavioural Marketing

Online merchants as well as other sites watch our shopping an d surfing habits by using "cookies," an online tracking system that attaches pieces of code to our Internet browsers to track which sites we visit as we search the Web.

"Persistent" cookies remain stored on your computer while "session" cookies expire when you turn the browser off. Online merchants use cookies to recognize you and speed up the shopping process the next time you visit. You may be able to set your browser to disable or refuse cookies but the tradeoff may limit the functions you can perfor m online, and possibly prevent you from ordering online. Generally, you will need to enable session cookies to place an order.

CONCLUSION

E-commerce is widely considered the buying and selling of products over the internet, but any transaction that is completed solely through electronic measures can be considered e -commerce. Day by day E-commerce and M commerce playing very good role in online retail marketing and peoples using this technology day by day increasing all over the world. E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. Dimensions of e-commerce security; Integrity: prevention against unauthorized data modification, No repudiation: prevention against any one party from reneging on an agreement after the fact. Authenticity: authentication of data source. Confidentiality: protection against unauthorized data disclosure. Privacy: provision of data control and disclosure. Availability: prevention against data delays or removal.

Fraudsters are constantly looking to take advantage of online shoppers prone to making novice errors. Common mistakes that leave people vulnerable include shopping on websites that aren't secure, giving out too much personal information, and leaving computers open to viruses. In this seminar we discussed E-commerce Security Issues, Security measures, Digital E-commerce cycle/Online Shopping, Security Threats and guidelines for safe and secure online shopping through shopping web sites.

REFERENCES

1) Niranjanamurthy M, Research Scholar, Dept. of MCA, MSRIT, Bangalore, INDIA[1]
2) DR. Dharmendra Chahar, HOD. Dept. of CS & IT, Seth G. B. Podar College, Nawalgarh (Jhunjhunu) -333042, INDIA[2]
3) MohanadHalaweh, Christine Fidler - " Security Perception in Ecommerce:Conflict between Customer and Organizational Perspectives". Proceedings of the International Multiconference on Computer Science and Information Technology, pp. 443 – 449, ISBN 978-83-60810-14-9- 2008- IEEE

4) Yuanqiao Wen, Chunhui Zhou "Research on E-Commerce Security Issues". 2008 International Seminar on Business and Information Management.
5) Rui Wang, Shuo Chen "How to Shop for Free Online Security Analysis of Cashier-as-a-Service Based Web Stores". IEEE S&P'11 proceedings.
6) V.SRIKANTH "ECOMMERCE ONLINE SECURITY AND TRUST MARKS". IJCET ISSN 0976 – 6375, Volume 3, Issue 2, July- September (2012),
7) ShaziaYasin, Khalid Haseeb. "Cryptography Based E-Commerce Security: A Review". IJCSI-Vol. 9, Issue 2, No 1, March 2012
8) Randy C. Marchany, Joseph G. Tront, "E-Commerce Security Issues"Proceedings of the 35th Hawaii International Conference on System Sciences - 2002
9) RashadYazdanifard, Noor Al-Huda Edres "Security and Privacy Issues as a Potential Risk for Further Ecommerce Development"International Conference on Information Communication and Management – IPCSIT vol.16 (2011)
10) Seyyed Mohammad Reza Farshchi "Study of Security Issues on Traditional and New Generation of E-commerce Model" International Conference on Software and Computer Applications-IPCSITvol.9(2011).