ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

A Study on E-Commerce Security Issues

Revathi C, Shanthi K, Saranya A.R

Assistant Professor, Dept. of Computer Applications, Dhanalakshmi Srinivasan College of Arts and Science for Women, Perambalur, Tamilnadu, India

Final year MCA Student, Dept. of Computer Applications, Dhanalakshmi Srinivasan College of Arts and Science for Women, Perambalur, Tamilnadu, India

Final year MCA Student, Dept. of Computer Applications, Dhanalakshmi Srinivasan College of Arts and Science for Women, Perambalur, Tamilnadu, India

ABSTRACT: Electronic commerce can help enterprises reducing costs, obtaining greater market and improving relationships between buyers and sellers. At the same time, new risks and threats have also occurred, such as, mutual trust, intellectual property, network attacks and so on. This paper analyzes the threat classification and control measures, and on this basis, a conceptual risk management framework is provided. Enterprises engaged in e-commerce can use the framework to improve their security.

KEYWORDS: e-commerce; security issues; threat classification; risk management

I. INTRODUCTION

E-commerce is buying and selling goods and services over the Internet. Ecommerce is part of e-business as specified in. E-business is a structure that includes not only those transactions that center on buying and selling goods and services to generate revenue, but also those transactions that support revenue generation. These activities include generating demand for goods and services, offering sales support and customer service, or facilitating communications between business partners.One of the critical success factors of e-commerce is its security. Without the assurance of security, e-commerce may not work normally. And it is a complexity issue, because ecommerce security relates to the confidence between sellers and buyers, credit card and extremely sensitive personal information. Therefore, the security of e-commerce depends on a complex interrelationship among applications platforms, database management systems, software and network infrastructure and so on. Any single weakness can jeopardize the ecommerce security.

II. ECOMMERCE SECURITY

E-commerce Security is a part of the Information Security framework and is specifically applied to the components that affect e-commerce that include Computer Security, Data security and other wider realms of the Information Security framework. E-commerce security has its own particular nuances and is one of the highest visible security components that affect the end user through their daily payment interaction with business. Today, privacy and security are a major concern for electronic technologies. M-commerce shares security concerns with other technologies in the field. Privacy concerns have been found, revealing a lack of trust in a variety of contexts, including commerce, electronic health records, e-recruitment technology and social networking, and this has directly influenced users. Security is one of the principal and continuing concerns that restrict customers and organizations engaging with ecommerce. Web e-commerce applications that handle payments (online banking, electronic transactions or using debit cards, credit cards, PayPal or other tokens) have more compliance 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 e-commerce 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

DOI: 10.15680/IJIRCCE.2015. 0312056

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 consumers must be treated as a major concern for eCommerce providers.

III. E-COMMERCE SECURITY TOOLS

- Firewall – Software and Hardware
- Public Key infrastructure
- Encryption software
- Digital certificates
- Digital Signatures
- Passwords
- Locks and bars – network operations center

IV. PURPOSE OF STUDY

- Study the Overview of E-commerce security.
- Understand the Online Shopping - Steps to place an order
- Understand the purpose of Security in E-commerce.
- Discuss the different security issues in E-commerce.
- Understand the Secure online shopping guidelines

V. RELATED WORKS

Security is one of the principal and continuing concerns that restrict customers and organizations engaging with commerce. The aim of this paper 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 paper 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] Ecommerce web site owners on one side are thinking of how to attract more customers and how to make the visitors feel secured when working on the site, on the other side how the end users should rate a ecommerce website and what they should do to protect themselves as one among the online community. Our objective of writing this research analysis journal is to make the readers to have clarity of thoughts on the technology which helps all of us to do secure transactions along with safety tips. And how ecommerce site owners, have to make their online visitors to be of much comfort or Trust an ecommerce site via Trust marks, and by their security strategies.

[3] 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.

[4] The traditional authentication mechanism is based on identity to provide security or access control methods; in addition, traditional encryption and authentication algorithm require high computing power of computer equipment. Therefore, how to improve the authentication mechanism and optimize the traditional encryption and authentication algorithm may be the focus of P2P e-commerce.

[5] Information security, therefore, is an essential management and technical requirement for any efficient and effective Payment transaction activities over the internet. Still, its definition is a complex endeavor due to the constant technological and business change and requires a coordinated match of algorithm and technical solutions.

VI. 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, Mercantila, dell, Best Buy and much more

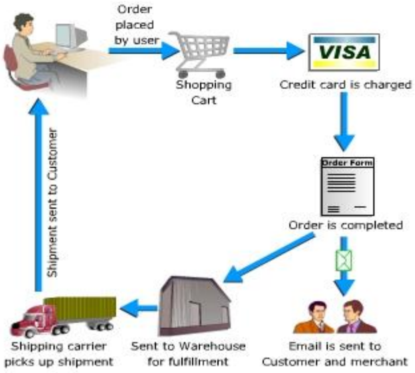
Order placed by user
Shopping Cart
VISA
Credit card is charged
Order Form
Order is completed
Email is sent to Customer and merchant
Sent to Warehouse for fulfillment
Shipping carrier picks up shipment
Shipment sent to Customer

Figure.1

A. SECURITY ISSUES OF ELECTRONICAL COMMERCE

The rapid development of Internet has promoted electronic commerce explosion. However, at the same time, the internet businesses have brought large security issues such as International Journal of Security and Its Applications And with the development of electronic commerce, these issues have obtained more and more attentions.

B. MUTUAL TRUST IN BUSINESS

In the traditional commerce, participant can face to face, so there may be little distrust. However, there is difference in electronic commerce. For example, in electronic commerce, the location of the business and the goods are unknown. More important, there is not personal contact between the seller and the buyer. In addition, there is lack of a clear legal framework in electronic commerce. Therefore, how to enhance mutual trust is an important issue.

C. INTELLECTUAL PROPERTY

Intellectual Property threats are a larger problems than they were prior to the wide spread use of the internet .It is relatively easy to use existing, material found on the internet without the owner’s Permission. Actual monetary damage resulting from a copyright violation is more difficult to measures than damage from secrecy, integrity, or necessity computer security violations.

VII. A MODEL FOR THREAT CLASSIFICATION AND CONTROL MEASURES OF E-COMMERCE

This part will provide a model to analyze the threat classification and control measures of e-commerce. Firstly, we consider threats from two points of view: threat agents and threat techniques. Then we analyze the security control measures.

A. THREAT AGENTS

Threat agents include 3 parts: environmental factors, authorized users and unauthorized users.

B. ENVIRONMENTAL FACTORS

Environmental factors are common sense. It is more prone to certain environmental influences and natural disasters than others in some areas. For example, fire is not geographically dependent. However, tornadoes and floods can be predicted in specific areas. In addition to the natural disasters, the danger of mechanical and electrical equipment failure should be paid to more attention. So is the interruption of electrical power.

C. AUTHORIZED USERS

There are some potential threats when authorized users and personnel are engaged in supporting operations. Especially they exceed their privileges and authorities. It may affect the ability of the system to perform its mission. Personnel should be considered as potential threats, when they have the access to a system or occupy positions of special trust. Because they have the capability or opportunity to abuse their access authorities, privileges or trusts. And it may bring danger to the system.

D. UNAUTHORIZED USERS

An unauthorized user can be anyone who is not engaged in the system. It can attempt to interrupt the operation of the system overtly or covertly. It may sabotage hardware and associated equipment. And it also could be accomplished through the manipulation of software.

E. SECURITY CONTROL MEASURES

There are some detailed security control measures in the ISO 7498-2 Standard lists. For example, there are involving authentication, access Control, data confidentiality data integrity and non-repudiation. Computer security experts widely accept this classification. And they are also recommended by the authors good control measures. The threat agent, threat technique and security measures are shown in Fig.1. We can use Fig.1 to classify threats and security measures to confront these threats in ecommerce. For example, access control is one of the security measures. It can face the threats that may be caused by an unauthorized user through hardware. Totally, there are combinations with agents, threat techniques, and security measures. However, not all of these combinations are available. We just utilize this three-dimensional view for a better security risk management**.**

VII. SECURITY THREATS

Three types of security threats

1. Denial of service,
2. Unauthorized access, and
3. Theft and fraud

A. SECURITY (DOS): DENIAL OF SERVICE (DOS)

- Two primary types of DOS attacks: spamming and viruses
- Spamming –Sending unsolicited commercial emails to individuals
- E-mail bombing caused by a hacker targeting one computer or network, and sending thousands of email messages to it.
- Surfing involves hackers placing software agents onto a third-party system and setting it off to send requests to an intended target. –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
- Viruses: self-replicating computer programs designed to perform unwanted events.

B. A CONCEPTUAL RISK MANAGEMENT FRAMEWORK FOR E-COMMERCE

To contain the complexity and maintain focus and relevance, this paper will restrict to issues related to the security of database and information system of e-commerce . And we put forward a conceptual risk management framework for e-commerce. According to the following five stages, we can firstly identify the vulnerabilities of a company, second evaluate the existing security measures, and then select the most appropriate and cost-effective countermeasures.

- Analyze Value
- Analyze Vulnerability and Risk
- Calculate Losses caused by Threats and Benefits of Countermeasures
- Select Countermeasures
- Implement Countermeasures

C. Analyze Value

The resource and application value analysis can be done in two phases. Firstly, determine the sensitivity of information. It can find the sensitivity level of each application and it is useful to find the most sensitive type of data, such as privacy, asset/resource and proprietar Therefore, it is important for its detail and accuracy. Secondly, estimate the asset value. The asset involves the resources such as physical facility, equipment and supplies, software and so on

D. Analyze Vulnerability and Risk

This analysis can be divided three parts. Firstly, identify vulnerabilities. Companies must identify the weakness or flaws in the design, implementation or operation of the security controls of a facility or system. It can be done through the analysis of the security measures or the related factors. Secondly, weight vulnerabilities. It should consider the seriousness and potential degree of exploitability to identify the vulnerabilities. Thirdly, assess threat probabilities. The probabilities should be documented.

E. Calculate Losses caused by Threats and Benefits of Countermeasures

Enterprises can calculate losses caused by threats and benefits of countermeasures through defining countermeasure at given levels [The cost of the countermeasure at a given level involves its effectiveness, expected damage caused by threat and so on. It also includes the probability that the threat occurs, assessing changes in threat probabilities, expected benefit and loss of countermeasure.

F. Select Countermeasures

This stage can be done in two phases: enumerate search program and mathematical method. The aim is to choose a countermeasure to minimize the total cost.

G. Implement Countermeasures

This stage includes three phases. Firstly, set up a plan. It is mainly done by the senior management. And they need give the staffs much more encouragement. Secondly, implement countermeasures. It is the key link of the framework. Specific action can be completed in this phase. Thirdly, test the countermeasures. The aim is to ascertain that the proposed countermeasures produce the desired effect. And it does not result bad effects.

VIII. SECURITY FEATURES

- 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.

IX. 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.

REFERENCES

[1] Mazumdar Sengupta.C and Barik.M.S, "E-commerce security-a life cycle approach", Sadhana, vol. 30, no. 2-3, (2005).
[2] F.-Y. Leu, C.-H. Lin and A. Castiglione, "Special issue on cloud, wireless and e-commerce security", Journal of Ambient Intelligence and Humanized Computing, vol. 4, no. 2, (2013).
[3] Xiangsong.M and Fengwu.H, "Design on PKI-based anonymous mobile agent security in e-commerce", Wuhan University Journal of Natural Sciences, vol. 11, no. 6, (2006).
[4] Antoniou.G and Battern.L, "E-commerce: protecting purchaser privacy to enforce trust", Electronic commerce research, vol. 11, no. 4, (2011).
[5] Smith.R and Shao.J, "Privacy and e-commerce: a consumer-centric perspective", Electronic commerce research, vol. 7, no. 2, (2007).
[6]Good. D and Schultz.R, "E-commerce strategies for B2B service firm in the global environment", American Business Review, vol. 20, no. 2, (2003).
[7] Randy C. Marchany, Tom Wilson. A Keystroke Recorder Attack on a Client/Server Infrastructure. Proceedings of the Network Security 96 Conference, SANS Institute.