Security Issues in E-commerce

Dr. Neelam Dahiya
Associate Professor
Government P.G. College
Sector 9, Gurugram
Gurugram University
Email: dahiyaneedahiya@gmail.com

Abstract

E-commerce security is a subset of information security that is explicitly applied to the areas of the information security framework that have a larger impact on e-commerce, such as computer security, data security, and other general areas. E-commerce security guards against illegal use, access, alteration, and destruction of e-commerce assets. Integrity, Authenticity, Confidentiality, Privacy, and Availability are the components of e-commerce security. The banking business has a lot of opportunities because of e-commerce, but it also faces new dangers including security concerns. Therefore, information security is a crucial technical and managerial need for an efficient and effective payment transaction activities online. In this paper, an overview of e-commerce security is discussed.

Keywords

Security, Privacy, Theft, Integrity.

Reference to this paper should be made as follows:

Received: 30.11.2023
Approved: 15.12.2023

Dr. Neelam Dahiya

Security Issues in E-commerce

RJPP Oct.22-Mar.23, Vol. XXI, No. I,

pp.015-021
Article No. 3

Online available at *:*
https://anubooks.com/rjpp-2023-vol-xxi-no-1

Introduction

Electronic commerce is fundamentally world wide web-based buying and selling of goods and services. e-commerce also applies to business-to-business transactions. for example: between manufacturers, distributors, etc. As we know that there is a continuous rise in purchasing the products with the help of e-commerce. So, it is essential to exchange secure information over the web. Making secure Internet transactions is a difficult task due to the globalization of business via the Internet and the gaps that we have left when making transactions online.

E-commerce is now an essential part of any company's competitive strategy. Web-based e-commerce offers businesses options and advantages like better competitiveness and a global presence. Reaching out to everyone is made possible by conducting business online. Examining the possibilities challenges traditional ideas of commercial rivalry using technological information and financial flows. Payment through the Internet or a network is a vital link in the entire e-commerce process, which includes the payment activity. However, despite the fact that significant resources and money are invested in the study of maintaining the security of online payments and E-commerce, there are still numerous issues with the security of financial transactions that need to be resolved.

The sale and acquisition of goods and services through electronic channels, primarily the Internet, is referred to as e-commerce, a subset of e-business. New forms of currency are being used online to facilitate electronic payments. While some emerging payment systems offer payment through the use of digital currency, others support the infrastructure that is currently in place for credit and debit transactions. E-commerce isn't just described as conducting business or engaging in commercial transactions online; it also builds customer trust and creates a safe environment for customers to trade. It guarantees customers safe and trustworthy business interactions. The development of related technologies is correlated with the emergence of the Internet and e-business.

E-commerce Models

There are two types of commerce in general: traditional commerce and electronic commerce. Traditional commerce involves the exchange of money between the hands of the customer and the merchant, whereas electronic commerce involves the exchange of money electronically through the use of various electronic payment methods.

2.1 B2B (Business-to-Business) Model

On the Internet, business-to-business e-commerce is growing at a breakneck pace. On the Internet, businesses of all sizes and types are buying and selling products

and services to one another. This model offers web-based technologies to businesses of all sizes. This provides businesses with dynamic and exciting business opportunities. In addition, B2B offers intelligent ways to do business with each other, including reduced human intervention, reduced overhead costs, reduced unintentional errors, increased efficiency, increased advertising exposure, new markets and new physical territories. It also offers the unique advantage of being an efficient method. This is a win-win situation for both buyers and sellers.

2.2 Business-to-Consumer (B2C) Model

E-commerce in the form of business-to-consumer transactions is now out of its infancy stage. Essentially, it is the idea of promoting online and distributing goods and services online. For many marketers or retailers who sell directly to customers, it is a logical next step. The overall concept is that the key to deploying a B2C e-commerce infrastructure successfully would be to increase customer reach, provide better customer service, and increase revenues while costing less to do so. Online transactions are more trustworthy in the eyes of the customer. Despite the fact that consumers continue to explore online, constraints connected to business such as security, privacy, network access, consumer protection, poor bandwidth, and uncertainty.

By overcoming these obstacles, B2C has improved its effectiveness and reliability to consumers. Although consumers and merchants do not interact in person, consumers have more options and strategies online.

2.3 Model of Consumer-to-Consumer (C2C)

This type of e-commerce is essentially a form of an auction site. Consumers sell their wares on commercial auction websites. Other consumers visit your site and bid on thier item. The website then connects the seller and buyer in order to complete the transaction. Site providers normally charge a transaction fee. In online transactions, C2C refers to situations in which both the seller and the buyer are consumers. Considering the lack of knowledge about other online merchants, as well as the fact that transactions can involve large sums of money, a major barrier to C2C e-commerce may be a lack of faith in merchants.

Need for Secure E-commerce

There are several reasons why electronic commerce must have more stringent security requirements than traditional forms of commerce.

3.1 Internetworking of computer systems:

Online companies utilize an array of computers that are intertwined to perform business transactions. Each connection's security necessitates a close inspection. There must be secure data and money transfers.

3.2 Data Repository

Because sensitive data is stored in repositories or databases, e-commerce systems are an ideal target. Given the accessibility of information in just one location, hackers appear to target data repositories.

3.3 Lack of Forensic Evidence

The absence of forensic evidence in computers complicates detection, capture, and prosecution. Regular system auditing is required for secure transactions.

3.4 Regardless of Distance

It is possible to commit computer crimes thousands of miles away from where you are held. It is not difficult to commit crimes without the constraints of distance and time with the availability of internetworking.

Security Concerns to Online Business

For online businesses on the Internet, accurate and dependable information is essential due to the increasing speed of business-to-business and business-to-consumer interactions. The security of a safeguard for online transactions must be the primary concern. E-commerce can give a business a big advantage over its rivals while also giving customers more value and comfort.

The Security Model of the CIA Triad

The fundamental concepts of security on the Internet are confidentiality, integrity, and accessibility. The CIA triad model talks about confidentiality, integrity, and availability. The loss of confidentiality is when information is read or copied by someone who isn't authorized to do so. A user should be able to access a specific level of security and a specific depth of information. Data and information that is private or sensitive must be classified and should not be made public. Customer data gathered from electronic transactions are protected from inappropriate and unauthorized disclosure through privacy. From an unsecure network, information can be easily hacked and altered in an unexpected way, resulting in a loss of integrity. If a message's context is altered, the receiver will be able to recognize it because of integrity.

Information accessibility is crucial for businesses that rely on the information. Reliability, usefulness, and prompt availability of accessed data and computing resources are all guaranteed by availability. In addition, security necessitates the following additional elements:

(a) authorization
(b) authentication and
(c) non-repudiation.

Threats to Security

To complete an online transaction, the online consumer employs a web browser as the front end. When a user visits unknown web links that are untrusted and does not know about them, the risk increases. When files are uploaded or downloaded, a security flaw may occasionally occur.

Cookies

Cookies are another component of online technology that has the potential to invade users' privacy. Cookies are pieces of data that are sent back and forth between a client and a web server to keep the state of the connection between the two. These kinds of links are displayed by web servers without the user's permission in order to learn more about the user's browsing preferences.

On some websites, Active X controls are used to download data about system setups to the user's computer, read the mail files on that computer, and then send that data back to the web server. The infamous German Computer Chaos Club showed how to download an ActiveX application that appeared to organize an electronic transfer of cash from the users' account to a numbered Swiss bank account.

When a user clicks on a link on a website, Java applets are automatically downloaded and run in the browser. Java applets gain access to confidential desktop files. Java applets are untrustworthy code that must be handled with care. Moreover, there are other kinds of threats with concern to e-commerce security such as

(a) Unauthorized access
(b) Malicious code
(c) Financial Fraud, for example, credit card fraud, etc.
(d) Denial-of-Service attacks.

Security Solutions

We may categorize the many technologies used to stop the theft of sensitive data in e-business as follows:

1. Cryptographic methods
2. Access Control and protection through authentication
3. Virus prevention software
4. Other technological combinations

6.1 Cryptographic Technologies

In cryptology, various schemes and methods are used to convert plain text information into cipher text that cannot be read even if the information is hacked. The Hash function, digital certificates, and a variety of encryption methods were utilized.

6.2 Protection Against Access Control and Authentication

The user must be able to access the information at a certain level. It is necessary to establish information boundaries. Most attacks are impossible with access control. This kind of access control can be done with a firewall. Data can be secured by assigning a password to sensitive information. Password that is used after the hacker breaks through the firewall or authorization, but it is still used for authentication.

Concernedly, biometrics can also be used to identify a person based on their behavioral or physiological characteristics. The use of biometrics for authentication safeguards confidentiality and integrity.

6.3 Tools for Preventing Viruses

Anti-virus and content-filtering software come in a wide variety of flavors on the market today. Heuristic antivirus software, signature-scanning antivirus software, integrity-checking antivirus software, macro virus analyzers, polymorphic virus analyzers, and signature-scanning antivirus software are the five methods identified for combating viruses.

Internet Risk Security Management

The most valuable themes for business must be identified. They must be put together, planned, and carried out with planning. There are four phases to risk management: assessment, planning, implementation, and monitoring. The organization estimated the security risk during the assessment phase. There are five steps to it. The first step is to define an organization's goals. Second, the inventory of assets is used to distinguish between tangible and intangible assets. The third step is to identify threats and determine their origin. Vulnerabilities are the next thing to be discovered. A variety of tools and methods are used to find the network's weaknesses. The final step is to assign a value to each risk to determine its value. The next step is planning. Planning security policy sets establish which threats are acceptable and which are unacceptable. via threats that are acceptable and pose little risk to the network. This phase also includes steps. lays out the guidelines for the initial phase. The next step is to establish auditing and review procedures. A review is necessary to determine whether policies are effective. The final plan that will be implemented on the network must also be developed as the final step. The plan's implementation is the third stage. The planning phase defines the technologies that will be used. Monitoring is the final stage. Continuous monitoring aids in determining which technologies are successful, which ones are unsuccessful and require modification, and whether any new threats exist.

Conclusion

The emerging trend in economic growth in e-commerce. The establishment and completeness of electronic online safe trading are necessary for network payment.

Numerous security concerns are required for a secure online transaction. E-commerce is still largely experimental. In essence, there are numerous available solutions for a secure Internet business, but their optimal application is still unknown. The fundamental step is to stop messages like "payment" and "order" from being sent when a large network has many obstacles. While this paper does not offer an effective solution for safe e-commerce, it does look into the tools and techniques that can be used to create safe, dependable, and trustworthy online businesses. A protected internet business climate makes it simple to lay out the trust of clients. In general, a variety of security issues must be taken into consideration by e-commerce sites, including: authenticating the participants in the transactions by verifying their identities; authorization: and ensuring that the user has access to particular data. Security turns into the most fundamental idea in Online business regardless has more to investigate the security failure points.

References

1. Bob, Gehling., David, Stankard. (2005). "eCommerce Security". Information security curriculum development proceedings of the 2nd annual conference on Information security curriculum development.
2. Ratanshigham, P. (1998). "Trust in Web-based Commerce Security". *Information Management and Computer Security*. vol.6. No.4.
3. Gosh, A.K. (1998). "E-Commerce security: Weak links, Best Defenses''. John Wiley & Sons: New York NY. ISBN-0-47-1922-3-6.
4. Chan, H., et al. (2001). "E-Commerce". Chichester. Wiley.
5. Colman, T., et al. (2002). "Keeping E-Business in perspective". Communication of ACM. August. vol.45. No.8.
6. Sahi, X., Wright, P.C. (2003). " E-Commercializing Business Operations''. Communication of ACM. February. vol.46. No.2.
7. Zaho, Ji. "Security Research on Payment System on E-Commerce Network".
8. Strader, T.J., Ramaswami, S.N. (2002). "The value of seller trustworthiness in C2C online markets". Communication of ACM. December. vol.45. No.12.
9. Anup, K. Ghosh. (1998). "E-Commerce security: No Silver Bullet". IFIP Conference Proceedings. Vol.142.
10. Dekker, M. (1997). The Frorlich/ Kent Encyclopedia of Telecommunications vol.15.
11. Barnes, C. et al. (2002). "Hack proofing your wireless networks". Syngress Publishing: Rockland. MA.