International Journal of Computer Trends and Technology
ISSN: 2231 – 2803 / https://doi.org/10.14445/22312803/IJCTT-V70I4P104

Volume 70 Issue 4, 25-28, April 2022
© 2022 Seventh Sense Research Group®

Original Article

E-Commerce Security Issues

Narangerel Ts

University of the Humanities, Ulaanbaatar, Mongolia.

Received: 08 March 2022
Revised: 25 April 2022
Accepted: 27 April 2022

***Abstract* - *E-commerce security is a part of information security and is specially used for components that affect online purchases. In today's technologically fast-paced world, especially in companies that utilize the Internet for their functions, information security concerns are a top priority. E-commerce security is the act of preventing the illegal act of accessing, using, changing, or deleting the information sent through online transactions. E-commerce measures are a matter of data integrity, accuracy, objectivity, accessibility, and confidentiality. This study discusses e-commerce security, its steps, online ordering, and some security issues.*

Keywords - *E-commerce, Security, Encryption, Protection, Risks.*

I. INTRODUCTION

Information technology, especially the privacy and security of the Internet environment, is one of the most important concerns in developing electronic technology today. In particular, the security of e-commerce, including computer security and information security, has become a major factor in the provision and use of today's Internet.

As the number of internet users increases, there is a high likelihood that e-commerce could replace traditional commerce and services. The biggest issue of e-commerce is trust. This is because customers only will attempt to make purchases if they trust the online merchant. Yet the key to the success of an online business is to create a secure way for transactions. Therefore, creating an environment where the user does not have to worry about the risks of online transactions is the main key to success in e-commerce. A deep analysis of the decisions that online shoppers make will help you understand the complex issues associated with creating trust between merchants and customers using the Internet.

Online transactions are usually processed through either credit cards, debit cards, or online banking, and these services are web-based, which is more susceptible to external influence and attacks [4]. The risks can cause significant damage to the user if their information is lost. Malware, such as trojans and worms, can threaten privacy and security if the system is attacked, which could affect confidentiality or change permissions [11]. Therefore, trust is the most important element in determining a buyer's attitude toward sellers in uncertain environments. Other factors can affect trust, such as brand and store reputation, but not face-to-face relationships or product testing is impossible. Therefore, the most important factor influencing the buyer is trust. This directly influences the security and confidentiality of transactions.

II. ABOUT E-COMMERCE SAFETY

Many things influence a buyer's decision in traditional trade, such as the producer or the vendor. However, e-commerce can be defined as the impact on a customer's trust and confidence in their purchasing decisions. Consumer confidence in e-commerce and the response to potential risks can be divided into four groups.

A. Experience

The customer has experience with online transactions or can safely work in an online environment.

B. Observation

The customer carefully observes the reliability, confidentiality, quality of the information provided, security, and credibility of the brands.

C. Attitude

The customer likes to shop.

D. Influenced by others

The customer shops online based on the suggestion of others.

Besides attracting more customers, e-commerce companies need to make customers feel safe when visiting their websites. Therefore, there must be specific security solutions at each stage of an e-commerce transaction.

III. Table 1

E-commerce transaction phases			
Information phases	Communication phases	Transaction phases	Delivery phases
Security solution			
Accessibility and integrity	-Security checks -Number signature	-Encryption	-Safety -Quality of delivery -The condition of the product

Security solutions on each stage of an online transaction [3]

The biggest threat to e-commerce environments is viruses. It disrupts the transactions, but it could also possibly stop the service altogether. Public and private login credentials distinguish the relationship between clients and service providers. However, hackers will attempt to compromise data integrity and security between users. E-commerce is further developing due to the increased knowledge of customers about the risks of e-commerce online through the media's reports on security issues such as financial fraud and password theft.

As Internet services and the number of Internet users increase, e-commerce is expected to become more widely used worldwide. It has an increasing number of e-commerce operators, which operate in the following fields:

- Sale of goods
- Services
- Payment of bills

IV. PRIVACY OF E-COMMERCE

Regardless of the source, privacy is one of the most important issues in e-commerce. Privacy is the main concern regarding people who refuse to participate in online transactions. A very small percentage of customers know how their personal information will be used in the future. Consumer fears, media pressure, and all of this together raise the issue of private businesses. However, some people believe that personal information is one of the basic rights that should be protected, while others believe that it is something that can be sold. E-commerce sites can collect a wide variety of personal information.

For example, it is possible to analyze the information entered into the website, such as personal choices, purchasing methods, and information retrieval methods.

Today, the development of information technology has become a goldmine for those looking to exploit consumer purchasing trends and personal interests. There are two main concerns that users have about privacy.

1) A third party using their information without their permission in inappropriate ways

2) Their information is being compromised due to a security breach.

There are four basic technologies used for e-commerce privacy.

- Research technology for monitoring and surveillance.
- Technologies regarding the release of personal information.
- Technologies used in trust and tagging.
- Privacy technologies

Businesses use surveillance and personal information-related technologies for business purposes. Customer-related information, such as customer information and biometrics, can be used to create profiles of personnel that could endanger an individual's privacy. Therefore privacy protection technology such as firewalls equalizes these shortcomings.

V. E-COMMERCE SECURITY

The purpose of e-commerce security is to protect against unauthorized access, use, alteration, and destruction of assets in e-commerce. Consumers are afraid of losing their financial information, while companies are afraid of hurting their reputation to the public through various security violations and breaches. Therefore, security issues also include many social and organizational issues.

- An organization needs to establish a good structure for risk management, develop protection policies, allocate responsibilities, and monitor and manage access as a guarantee of security.
- Safety depends more on workers and users than on technology.
- It depends on how the software engineering management and security technology are used.

The main problem is that consumers have a varied knowledge of e-commerce due to a lack of understanding of security policy guidelines. For example, users creating simple passwords, or storing their passwords unsupervised, carelessly (on someone else's computer), as a result, lost to third parties.

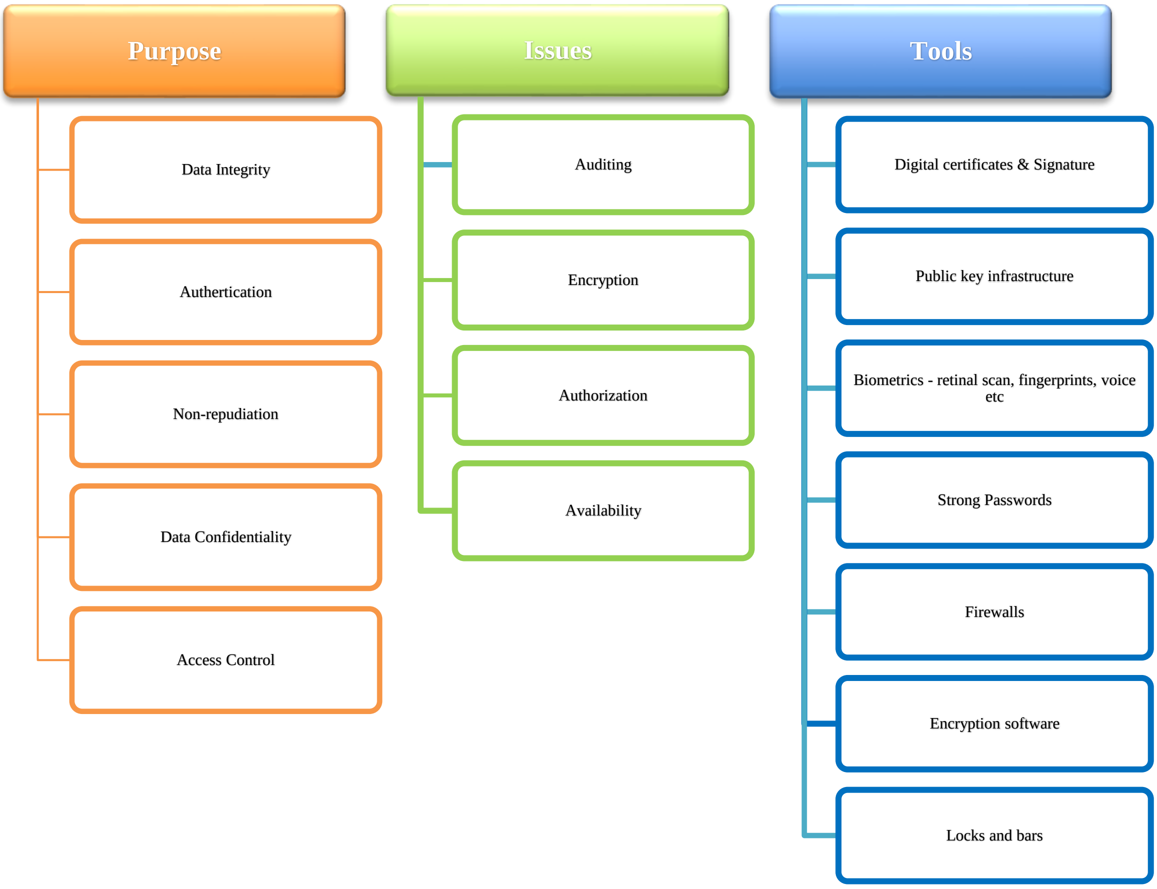

Fig. 1 e-commerce security scheme[4]

The main threats to the Internet

A. Unauthorized access

The act of illegally accessing information, systems, or programs for unintended purposes. Passive unauthorized access involves eavesdropping on channels to obtain any information. Active unauthorized access is access to the system to change information.

B. Distributed Denial of Service (DDoS)

Overloading the system to gain access. This attack is usually a packet attack.

C. Phishing

Illegal access to information, alteration of information, and use in dedicated programs.

VI. CONCLUSION

In addition to developing user protection software, companies should also assess potential risks and focus on preventing them.

This is directly related to the trust between the service provider and the customer in e-commerce. Building trust increases the number of customers and motivates them to use their services again, lowers costs, and increases revenue per customer. However, the security of personal information greatly affects customers' trust in the Internet. Fear of their lost private and financial information affects their trust in e-commerce services. Therefore, e-commerce providers need to be transparent about security mechanisms, such as how they protect user data, firewalls, data privacy, and digital certificates.

E-commerce will still have problems until vendors find a way to be confidential, trustworthy, secure, and effective. Therefore, it affects security concepts such as information confidentiality, protection, authentication, and access. Consumers not worrying about the safety of their transactions will lead to a benefit in the economy.

REFERENCES

[1] Thomas L. Mesenbourg, An Introduction to E-commerce, Philippines: DAI-AGILE, (2000).

[2] D. Berlin, Information Security Perspective on Intranet, presented at Internet and E-Commerce Infrastructure, (2007).

[3] Shazia Yasin, Khalid Haseeb. Cryptography Based E-Commerce Security: A Review .IJCSI, 9(2) (2012).

[4] Ms. Palak Gupta, Dr. Akshat Dubey E-Commerce-Study of Privacy, Trust and Security from Consumer's Prespective IJCSMC, 5(6) (2016) 224-232

[5] V.Srikanth Ecommerce online security and trust marks .IJCET ISSN 0976 – 6375, 3(2) (2012).

[6] Mohanad Halaweh, Christine Fidler - Security Perception in Ecommerce: Conflict between Customer and Organizational Perspectives .Proceedings of the International Multiconference on Computer Science and Information Technology, (2008) 443 – 449.ISBN 978-83-60810-14-9- 2008-IEEE

[7] Randy C. Marchany, Joseph G. Tront, E-Commerce Security Issues Proceedings of the 35th Hawaii International Conference on System Sciences, (2002).

[8] Shazia Yasin, Khalid Haseeb. Cryptography Based E-Commerce Security: A Review .IJCSI, 9(2) (2012).

[9] A Sengupta, C Mazumdar e-commerce security – a life cycle approach sadhana , 30(2&3) (2005).

[10] Biswajit Tripathy, Jibitesh Mishra. Protective measures in ecommerce to deal with security threats arising out of social issues – a framework iaeme -ISSN 0976 – 6375(online) , 4(1) (2013).

[11] Poonam Patel, Kamaljeet I. Lakhtaria A Study on e-Commerce security Threats IJIRSCE8, 5(3) (2017).

[12] Demberel D, Marketing and business security, (2011).

[13] Tsogtoo M, Security of Business , (2007).

[14] Tumurpurev D, Online services, Online security Communications Regulatory Commission, 10 (2012) 18-19.

[15] https://www.census.gov/popclock/

[16] http://www.statista.com