An Analysis of Security and Trust Issues in E-Commerce

Javed R.Shaikh
Faculty of Telecommunications at Technical University of Sofia
8 Kl. Ohridski Blvd, Sofia 1000
Bulgaria
{javedsheikh1987@gmail.com}

Sachin D Babar
STES Sinhgad Institute of Technology
Lonavala, Pune, India

Georgi Iliev
8 Kl. Ohridski Blvd, Sofia 1000, Bulgaria
{gli@tu-sofia.bg}

ABSTRACT: *We are living in a web dependant world where all activities are carried out only in online formats. E-commerce is growing rapidly where all business transactions are done. Due to reduced cost, time and personalized features, online purchases are increasing. In E-commerce activities, clients get real experience. At the same time in some instances security and trust is compromised. Three issues impact the customers in the selection of E-Commerce which include clients' attitude on transaction systems, security and the trust in the reliance of online products. The information relating to individuals should be safe guarded. Everyday many security issues get cropped and in this work we reviewed the literature on E-Commerce and the solutions for the E-Commerce security issues.*

Keywords: E-commerce, Security of E-commerce Network, Privacy, Trust, Security Solutions

DOI: 10.6025/jisr/2020/11/4/113-119

Received: 17 May 2020, Revised 18 August 2020, Accepted 30 August 2020

1. Introduction

In the 21st century electronic payments are becoming an important part of our everyday life. For Most of the people, it is hard to imagine a single day where they do not make a use of credit/debit cards in a physical store or to perform some mode of online payments or for money transfer over the internet. Nowadays doing electronic business on the Internet is already an easy task. With the increase of E-commerce use, cheating and snooping is also increasing. To develop the Ecommerce, security and privacy are two main issues over the internet [1]. The Internet does not offer much security required for it. Stealing data is undetectable in most cases. Some operating systems offer little or no security against virus or malicious software, which means that users cannot even trust the information displayed on their own screens. At the same time, user awareness for security risks is very less. We almost trust on E-commerce system without consideration for how they work [2]. The study realized that there are some methods used within E-commerce that contribute trust and security, but still there are many security and trust issues, which need better solutions in order to have a secure and trustworthy Ecommerce system. A large number of E-commerce application such as stock trading, banking, shopping, and gaming rely on the security strengths of SSL/ TLS protocols [3]. According to the survey, which took place in the United States between educators and practitioner, was about the security issues in E-commerce. The survey's result showed that most of educators and practitioners were worried about their online payment and personal information because of the lack of trust regarding the security issues within the Ecommerce [4]. In order to increase E-commerce business, it is very important to gain the trust of customers by continuously reviewing and resolving all new security issues related to it [5]. Below Fig.1 shows the basic E-commerce chain involved during online business.

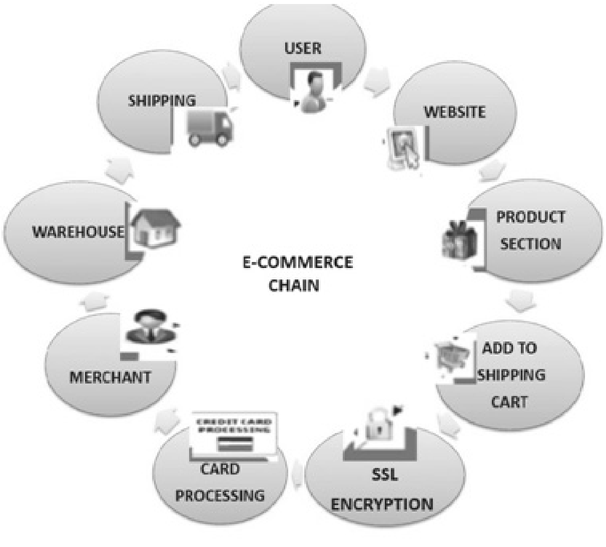

Figure 1. E-commerce chain

2. Background of E-Commerce

All commercial activities conducted through the Internet are collectively referred to as E-commerce [6]. The year 1990 comes up directly in people's mind when they think of Ecommerce because it was a time when E-commerce had a good development. According to Dykert et. al.[7] the Ecommerce's starts in earlier than the 1990s. According to authors E-commerce had a strong connection with the Internet, and the E-commerce start goes back with the Internet's establishment that started with a military research project during the 1970s. According to author one of the reasons why E-commerce had its successes at the beginning of the 1990s was World Wide Web which was introduced in 1992 [4].Amazon was one of the first E-commerce businesses to establish a secure market [8].

3. E-Commerce Security Issues

In the internet age, E-commerce is a special and critical system for the commercial transaction activity. At present, the information security of electronic commerce is not optimistic [9]. E-commerce security issue should be concerned especially. There are many factors that are important within E-commerce, which should be improved [6]. But considering time constraint we have chosen to focus on security and trust within E-commerce. Before using E-commerce system we need to address different issues of a system and its major components to ensure its availability, survivability and safety and privacy of data [4]. As mentioned, security is a major concern for E-commerce sites and consumers alike. Ecommerce security is generally a part of an information security and is applied to the factors such as computer security, data security and other factors of information security.

Consumer privacy is becoming the most publicized security issue replacing theft and fraud as top concerns in Ecommerce. The DOS and DDOS attacks demonstrated that business sites did not maintain adequate security protection and intrusion detection measures. Some of the sites did not detect the compromise, which occurred months before the DDOS attacks [10].Therefore, with the industry best security practices, E-commerce applications are secured with different layers of protection, as per the risk level of the application [11]. Generally, E-commerce security has three types of security fronts [12].

1. Client side Security Issues

2. Server-side Security Issues

3. Transaction Security Issues

A. Client Side Security Issues From the user's point of view, client-side security is typically important and the major concern. In client-side security the use of computer security technologies, such as proper user authentication and authorization, access control, and anti-virus protection is common. The data analysis on common online banks in [13] shows that the client side security protection for online banking does need improvement. Most banks use single cipher security system which is vulnerable to virus and cyber-attacks. Client side safety protection is the weakest part of online banking service providers [14].

B. Server-side Security Issues The second important issue is server side security issue. It requires proper client authentication and authorization reliability and availability. It should also take care of the nonrepudiation of origin, sender anonymity audit trail, and accountability. Table 1 enlists various security features along with its description.

Security features	**Description**
Authorization	Allows you to manipulate data
Authentication	Allows you to have access to your account
Encryption	Deals with hiding of information
Auditing	Keeps a record of operations
Integrity	Provides prevention against unauthorized data manipulation
Non-repudiation	Prevention against any one party from reneging on an agreement

Table 1. Security Features of E-commerce

C. Transaction Security Issues Transaction side security issue is also important. It needs various and better security services such as data authentication, access control, data confidentiality, data integrity and non-repudiation. Transaction security is critical to bolstering consumer confidence in a particular Ecommerce site. There are a number of defenses for transaction security such as encryption and switched network topologies. Encryption techniques such as secret-key, publickey and digital signatures are the most common method of ensuring transaction privacy, confidentiality and securely. But the common weakness of these techniques is that they depend on the security of the endpoint systems.

Transaction security depends on the organization's ability to ensure privacy, authenticity, integrity, availability and the blocking of unwanted intrusions [10]. There are many phases of E-commerce transaction and each phase has different security measures [15].

4. Types of E-commerce Security Threats

The standard client-server model has three components: the server system, the network and the client system [10]. At each side, there are some threats. Protection against these threats is also very important to grow E-commerce business. Figure 2 shows classification of different threats associated with Ecommerce.

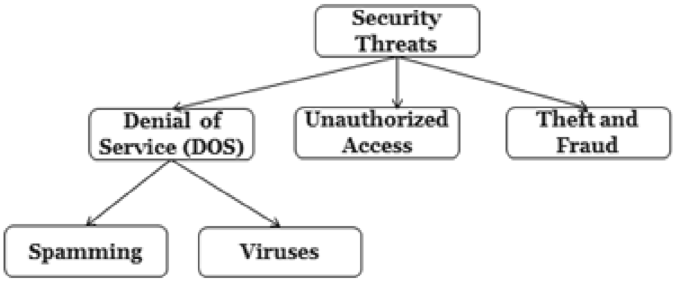

Figure 2. Types of security threats

A. Denial of Services (DOS) DOS is the type of attack where it removes information altogether and deletes information from a transmission or file. The distributed denials of Service Attacks (DDOS) scripts are common, easiest and effective to implement attack out of all attacks available on the WEB.

- **Spamming:** Spamming consist of sending unsolicited commercial emails to individuals, Hacker targets one computer or network, by E-mail bombing and sends thousands of email messages to it.

- **Viruses:** Viruses are nothing but the specially designed programs to perform unwanted events. It is software that attaches itself to another program and can cause damage when the host program is activated. Viruses are the most publicized threat to client systems.

B. Unauthorized Access Illegal access to systems, applications or data is unauthorized access. It is clarified into two types.

- **Passive unauthorized access:** listening to the communications channel to find secrets of processes. · Active unauthorized access: Modifying system or data Message stream modification.

C. Theft and Fraud Fraud occurs when the stolen data is used or modified. Theft of software or data occurs by doing illegally copying from company's servers. It includes copying credit or debit card details of other users and using them for illegal purchases for selfishness.

5. Security Approaches at Various Levels

E-commerce security strategies deal with two issues: one is protecting the integrity of the business network and its internal systems and second is accomplishing transaction security between the customer and the business. The main tool businesses use to protect their internal network is the firewall [10]. In general, in E-commerce security front end servers must be protected against unauthorized access, back end systems must be protected to ensure privacy, confidentiality, and integrity of data and the corporate network must be protected against intrusion. Following are the different security approaches at various Levels in Ecommerce [1] [16].

A. Application System Level At application level security features such as confidentiality, integrity, availability, Non-repudiation and anonymity are taken into consideration by various means of encryption techniques, digital signature etc.

B. Security Protocol Level There are mainly two protocols associated with security of E-commerce at the protocol level.

1) Secure Socket Layer (SSL): It is a protocol layer which exists between the connection oriented layer (TCP/IP) and application layer (HTTP). TCP provide the end to end reliable service which is used by the SSL. TCP established a secure communication between client and the server using encryption and digital signature [14].

2) Secure Electronic Transaction (SET): Secure Electronic Transaction is communication protocol standard and an encryption and security specification protocol for securing credit card transactions in open network called the Internet during E-commerce transactions. SET also provides privacy and protection to ensure the authenticity of the electronic transaction.

C. Security Authentication Level: To maintain security at authentication level different techniques are utilized such as the use of message digest, digital signature and use of different encryption and decryption standards.

- **Message Digest:** It is useful to find whether message which is sent by the sender is modified or not. The message digest is a hashing function of all the bits of the message in which comparison of sender's and recipient message digest take place to detect the error.

- **Digital Signature:** To remove the problem of public key encryption, we use a digital signature for authentication. Before sending data content in the form of a message, the sender encrypts message content with her own private key (digital signature), which authenticate the sender because in network no one has anyone's private key.

D. Encryption Technology Level: Encryption technology provides secure communication over unsecured networks. Encryption technique encodes the plain text in to unreadable form (cipher text) which helps to protect the data from being viewed by unauthorized person.

- **Symmetric Key Encryption:** It is also known as private key encryption. In this case same key is used for the encryption and decryption.

- **Asymmetric Key Encryption:** It is also called public key encryption. In asymmetric key cryptography, we use two keys, one for encryption method and another key for decryption method. One key is Public and second one is private.

6. Available Security Tools in E–Commerce

Different security tools such as Firewal, Public key Infrastructure (PKI), Encryption software, Digital certificates, Digital signature, Biometrics, Password etc. are available in the market to protect the E-commerce business [17]. The Pretty good Privacy (PGP) is also available to take care of E-commerce.PGP provides confidentiality and authentication service that can be used for electronic mail and file storage applications. PGP has grown explosively and is now widely used. The actual operation of PGP consists of five services: authentication, confidentiality, compression, email compatibility, and segmentation. Three main reasons responsible for the growth of PGP are mentioned below [18].

- It is based on the algorithm that has survived extensive public review and is considered extremely secure.

- It has a wide range of applicability

- It was not developed by, nor is it controlled by, any governmental or standards organization.

7. Security Vulnerabilities In E-commerce

There are many points of failure, or vulnerabilities, in an Ecommerce environment. Even in a simplified E-commerce scenario, a single user contacts a single website, and then gives his credit card and address information for shipping a purchase, many potential security vulnerabilities exist. Indeed, even in this simple scenario, there are a number of systems and networks involved. Each has some security issues [19].

When a consumer makes an online purchase, the merchant's web server usually catches the order's personal information in an archive of recent orders. This archive contains everything necessary for credit-card fraud. Accordingly, an E-commerce merchant's first security priority should be to keep the web servers' archives of recent orders behind the firewall, not on the front-end web servers. The merchant's back-end and database need to have strong security provisions. A site's servers can weaken the company's internal network. This is not easily remedied, because the web servers need administrative connections to the internal network, but web server software tends to have buggy security. Here, the cost of failure is very high, with potential theft of customer's identities or corporate data.

8. Conclusion

E-commerce security is the protection of E-commerce assets from unauthorized access, use, alteration, or destruction. Dimensions of E-commerce security are Integrity, No repudiation, Authenticity, Confidentiality, and Availability. This paper highlights the existing E-commerce security threats, its security issue and related techniques applied in E-commerce security field along with the major challenges. We have also discussed the security vulnerabilities present in the E-commerce business. At present, the firewall technology, data encryption technology, and information hiding technology are widely used in electronic commerce information system security. So many years passed from the development of E-commerce but still it has some security issues associated with it. Reliable solution to available security issues is very important to grow Ecommerce business. In addition, we should strength the legal system, management system and credit system [20]. We can improve the transaction security using advanced cryptographic standards.

References

[1] Ahmed, K., Alam, Md. S. (2015). E-Commerce Security Through ECC, *International Conference on Information Security & Privacy*, Nagpur, India.

[2] Issues of Security and Privacy in Electronic Commerce. www.cs.virginia.edu.

[3] Lal Das, M., Samdaria, N. (2014). *On the Security of SSLTLS Enabled Applications*, Elsevier, 2014.

[4] Haidari, A., Paktiani, K. (2011). A Study About Trust and Security Within E-Commerce, University of Gothenburg, Sweden.

[5] Ladan, M. I. (2014). E-commerce Security Issues, *International Conference on Future Internet of Things and Cloud*, 2014.

[6] Lai, S.-T., Leu, F.-Y., Chu, W. C.-C. (2014). A Multi-Layer Secure Prevention Scheme for Improving E-commerce Security, Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IEEE, 2014.

[7] Dykert, L., et. al. (2002). E-Business-för Tillväxt Och Lönsamhet, Lund, Studentlitteratur, 2002.

[8] Kraft, T. A., Kakar, R. (2009). E-commerce Security, *In*: Proceedings CONISAR, Washington DC, 2009.

[9] Xuehui, J. (2013). Research on the Security of Electronic Commerce Based on Computer Network, *Fourth International Conference on Intelligent Systems Design and Engineering Applications*, IEEE, 2013.

[10] Marchany, R. C., Tront, J.G. (2002). E-commerce Security Issues, 35th Hawaii International Conference on System Sciences, 2002.

[11] Perera, A. C., Kesavan, K., Bannakkotuwa, S.V. (2016). ECommerce (WEB) Application Security: Defense Against Reconnaissance, *In:* IEEE International Conference on Computer and Information Technology, 2016.

[12] Reza Farshchi, S.M., Gharib, F., Ziyaee, R. (2011). Study of Security Issues on Traditional and New Generation of Ecommerce Model, *In:* International Conference on Software and Computer Applications IPCSIT, 9, IACSIT Press, Singapore, 2011.

[13] Reza Farshchi, S.M., Gharib, F., Ziyaee, R. (2011). *Study of Security Issues on Traditional and New Generation of Ecommerce Model*, International Conference on Software and Computer Applications, 2011.

[14] W3C Working Group Note. (2004). Web services architecture, http://www.w3c.org/TR/ws-arch, 2004.

[15] Yasin, S., Haseeb, K., Qureshi, R. J. (2012). Cryptography Based E-commerce Security: A Review, *IJCSI International Journal of Computer Science Issues*, 9 (2) 1 March 2012.

[16] Chaudhary, A., Ahmad, K., Rizvi, M. A. (2014). E-commerce Security Through Asymmetric Key Algorithm, *Fourth International Conference on Communication Systems and Network Technologies*, IEEE, 2014.

[17] Niranjanamurthy, M., Dharmendra Chahar, D. R. (2013). The Study of E-Commerce Security Issues and Solutions, *International Journal of Advanced Research in Computer and Communication Engineering*, 2 (7) July 2013.

[18] Dr. Nada, Al-Slamy, M. A. (2008). E-Commerce Security, *IJCSNS International Journal of Computer Science and Network Security*, 8 (5), May 2008.

[19] IBM, Microsoft, Verisign. (2002). WS-Security Specification 1.0", 2002, http://www.ibm.com/developerworks/library/wssecure.

[20] Zhu, F., Li, G. (2011). *Study on Security of Electronic Commerce Information System*, IEEE, 2011.