Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 19 Issue 1 Version 1.0 Year 2019
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Systematic Review of Security in Electronic Commerce- Threats and Frameworks

By Isuri Udara & Nuwan Kuruwitaarachchi

Abstract- There is a remarkable scope for more streamlined living through an increase of e-platforms specially e-commerce, but this coincides with an increase in security concerns since the global market place is virtual and anonymous. Therefore, users have to blindly trust the online providers. In order to overcome this physiological barrier the e-platforms should ensure utmost security. If not the e-commerce industry is unableto perform in the market effectively. Thereby arises the need to perform a systematic review of security issues in the e-commerce industry and to discover how different frameworks address these problems. This paper aims to identifythe main security problems faced by both customers and vendors when interacting with e-commerce platforms and to evaluate general security management frameworks based on the main security areas identified.

Keywords: authentication; availability; B2C; E-commerce; frameworks; Integrity; non-repudiation; privacy; security; threats.

GJCST-E Classification: K.4.4

Strictly as per the compliance and regulations of:

A Systematic Review of Security in Electronic Commerce- Threats and Frameworks

Isuri Udara [α] & Nuwan Kuruwitaarachchi [σ]

Abstract- There is a remarkable scope for more streamlined living through an increase of e-platforms specially e-commerce, but this coincides with an increase in security concerns since the global market place is virtual and anonymous. Therefore, users have to blindly trust the online providers. In order to overcome this physiological barrier the e-platforms should ensure utmost security. If not the e-commerce industry is unableto perform in the market effectively. Thereby arises the need to perform a systematic review of security issues in the e-commerce industry and to discover how different frameworks address these problems. This paper aims to identifythe main security problems faced by both customers and vendors when interacting with e-commerce platforms and to evaluate general security management frameworks based on the main security areas identified.

Keywords: authentication; availability; B2C; E-commerce; frameworks; Integrity; non-repudiation; privacy; security; threats.

I. Introduction

E-commerce refers to the buying and selling of goods and services via electronic channels, primarily the Internet, the global market place. Thus, this is characterized by virtuality and anonymity and is considered as an important development worldwide in the field of business that changed the economies and commercial methods worldwide[1]. With the advantages including the high interaction, convenience, transparency and individualization, the internet makes online shopping increasingly popular among consumers[2]. The increasing profit, business continuity, reduced operational cost, improved storage management, customer service and improved competitiveness makes e-commerce advantageous to businesses[3]. However, the use of such ubiquitous technology is not assuming apex of its success owing to menace of security issues that have become a matter of great concern to the customers as well as to the online providers[4][5][6]. If security is preserved properly, the essence of success in e-commerce can be inhaled, but if this is not successful, a considerable number of users will eventually refuse to use the platform due to lack of trust[4].The online vendors are in a competition to pull more and more customers to inflate their business and customers on the other hand, are trying to ensure security before use of the online platform that their trust issue may not be at stake[4]. Thus to improve and to continue the e-commerce business the vendor organizations should be more specific on the security strategy. The aim of this paper is to explore the perception of security in business to consumer (B2C) e-commerce platforms from both customer and organizational point of view. This paper gives an overview of the dimensions of security, different security threats on e-commerce and the available frameworks to provide the necessary levels of security.

II. Literature Review

E-commerce connects customers and vendors over the internet as they conduct business interactions. Even though this can be incredibly convenient and productive when utilized successfully, this is also accompanied by risk. Recent studies concluded that the primary factor hampering the success and further growth of e-commerce is the lack of security[2]. As the trend of on-line transactions continues to grow, there is an increase in the number and type of attacks against the security[7]. E-commerce security has become more important accelerate off the great developments achieved with growth in all fields of information technology. With the changingculture of the people on the concept of e-commerce and increased commercial transactions has emerged the greatest need for e-commerce security. E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction[8]. Consumers fear the loss of their financial data, and e-commerce sites fear the financial losses associated with any resulting bad publicity and break-ins[8]. Therefore, the state of being free from danger is, to be safe and to go about the business with minimal interruption. Therefore, the importance of a secure platform cannot be overstated. Existence of a system's weakness may be exploited by an attack could cause the platform to enter to an unsafe state[9].The three key points of vulnerability in a transaction are the customer end, server side and the communication channel. Thus, security is one of the principal and continuing concerns that restrict customers and vendor organizations engaging with e-commerce. E-commerce security is a part of the information security framework and is specifically applied to the components that affect e-commerce

Author α σ: Department of Information Systems Engineering Sri Lanka Institute of Technology Malabe, Sri Lanka.
e-mails: isuriudara03@gmail.com, nuwan.ku@sliit.lk

interactions which includes computer security i.e. security from intrusion, viruses, worms, etc. Network security, i.e. to protect communication and all participants. Therefore, security is the combined technique of achieving robustness and fault tolerance by preventing known and distinct threats and quickly detecting and handling new threats.

a) Dimensions of Security

This research identified five main dimensions of security that needs to be preserved to bring about the desired security for e-commerce platforms.

i. *Privacy*

Privacy[4][5] is considered as a fundamental right of any consumer. It is the ability to control the terms under which different information is acquired and used. That is the control over the secondary use of information provided[8]. From the e-commerce point of view, information or data privacy and online privacy[1] is the privacy of personal information, financial information and usually relates to how those data is stored on computer systems and used. Any act of copying or reading by an unauthorized party result in the loss of privacy.

ii. *Authentication*

Authentication[7] is the process of determining whether someone or something is, in fact, who or what it claims itself to be. Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server. In e-commerce, information and communication security is essential to ensure that the data, transactions and documents are genuine and to validate that both parties involved are who they claim they are. This factor also ensures that the particular user is the only one who is allowed to logon to the internet banking account.

iii. *Integrity*

Integrity can be defined as the dependability and trustworthiness of information. More specifically, it is the accuracy, consistency and reliability of the information content, processes and systems. This means assuring that the data being accessed or read has neither been tampered with, nor been altered or damaged, since the time of the last authorized access. In e-commerce, integrity is particularly important for critical safety and financial information used for activities such as electronic fund transfers and financial accounting[7].

iv. *Non-Repudiation*

Non-repudiation means one's intention to fulfil their obligations to a contract[7]. It also means that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction. So, this is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data. In terms of e-commerce, it is to not deny a sale or a purchase.

v. *Availability*

Availability is the purpose of any information system to make information available whenever it is needed[7]. This means that the computing systems used to store and process the information, the security controls and the communication channels used to access it must be functioning appropriately. E-commerce platforms are high availability systems aiming to remain available at all times, preventing all possible service disruptions. Therefore, prevention against data delays or removal and providing an uninterrupted service is focused.

III. E-Commerce Security Issues

The literature paved the way to identify four main security problems the e-commerce industry face based on three criteria; the e-platform, it's owner and it's users.

a) Transactional Security in E-Commerce

Transactional security in e-commerce refers to a secure non-fraudulent transfer of a monetary value from the payer to payee via electronic means, which links the exchanged data to some economic real world value. Securing the information available in the payment card is the major concern from a client perspective. Therefore, the transparency of the transaction should be maintained, financial information should not be stored after the transaction is completed and the information should not be revealed or sold to third parties[7]. Thereby if the online payment system is simple, hazardless, convenient and tightly secured, users will not feel hesitated in using the e-commerce platform. Thus, the three major players that need to be addressed in an online transaction are the online seller, e-commerce page, and payer's own perception[10]. Hence, the exchange nature requires a confidentiality and the success of the operation hinges on the data transmission security. From the electronic business perspective, in order to survive the customer and vendor relationship should be built upon trust. There should not be any unease throughout the decision making process and even beyond. Thereby, vendors, banks and customers will collaborate with the electronic commerce platform without their inner fears.

b) Privacy in E-Commerce

In online transactions, clients are required to disclose a large number of private information to the vendor, which is associated with high risk of confidential and cooperate sensitive information leakage. Clients have two kinds of privacy concerns[8]. First, they are concerned about the reuse of their personal data for unrelated purposes without their consent such as sharing with third parties. Second, consumers are

concerned over unauthorized access to personal data because of security breaches. Privacy is required to be looked into through social, organizational, technical and economical perspectives, as it is a legitimate right of the client[4]. It is evident that end users are very much concerned over unauthorized access to their personal data and also about reuse of their personal data by others without their permission[10]. Therefore, when making the decision to provide private information, clients rely on their perceptions of trustworthiness irrespective of whether the vendor is click only or motor business. Thus, consumer concern with privacy of information is having an immense impact on the business to consumer e-commerce, and that for electronic commerce to reach its full potential. Ensuring control over secondary use of information will lead to assurance of privacy in clients mind.

c) System Security in E-Commerce

System security arises mainly from the vendors end and this discus about the server, the availability and the database security. For an e-commerce platform to serve its purpose, the information must be available 24*7. This means that the systems used to store and process the information, the security controls used, and the communication channels used to access it must be functioning correctly. Availability attacks can create a delay, causing data to be held or otherwise made unavailable for a period. The attackers flood the network with useless traffic, make the system extremely slow to serve the customers, and in the extreme case, cause the system to crash down. E-commerce platforms store client personal data and retrieve product information from databases linked to the web-server. Database attackers change system resources or gain access to system information without authorization by either sharing logins or passwords or using an unattended terminal and alter, modify or disclose product information, consumer information and even valuable and private information that could irreparably damage the business[7].

d) Cyber Crime in E-Commerce

Cybercrime in e-commerce[8][5][11] is mainly computer as a target crime with the motive of intentionally causing financial loss, data breach or risking reputation directly or indirectly. Identity theft, fraud, virus attacks, spam, Trojan horses, worms, phishing and page jacking can be considered as popular crimes. Hackers break into e-commerce web servers to yield archives of transactional and personal information when a consumer makes an online purchase. Fraudulent practices steal, modify or use another person's personal information under false pretense and thereby affect confidentiality and trust. Unusual unsolicited e-mail bombing aim a computer or network and send thousands of email messages. Viruses self-replicate and infect targeted computers triggered by an event[7]. Worms spread using direct internet connections and Trojan Horses are disguised as legitimate software that trick users into running the program[7]. These attacks hinder the platform availability to consumers. Stealing content and placing it on another site with the hope of increasing site's search engine rankings, rerouting traffic from a vendor's e-commerce site and directing visitors to a different websites with potential malicious material affects the e-commerce platforms risk of reputation and financial loss.

IV. Comparison of Frameworks

This section provides a review of four different security frameworks and summarizes the main contributions for each e-commerce security problem domain. The differentiating characteristics of each security frameworkisemphasized so that both clients and providers can distinguish which framework(s) suits their requirements for a successful secure platform.

a) CISCO Security Framework

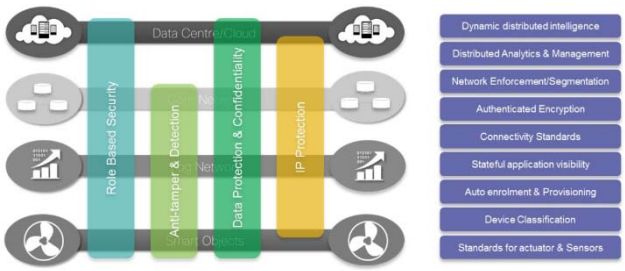

Figure 1: Cisco proposed model[12]

Figure 1 shows the Cisco proposed security framework, which can be the foundation for the execution of security. The authors have proposed such a framework to be used in protocol and product development, in addition to, policy enforcement in operational environments that is suitable for both application and infrastructure. This framework review will mainly help to protect from physical attacks, such as DAR (data at rest protection) and Intrusion detection/prevention system (IDS/IPS)[13]. How the above discussed e-commerce security concerns are addressed by this framework is as follows.

Table I: CISCO framework support for the security threats

Security Threat	Concerns	Framework Support
Transactional Security	Information should not be revealed or sold to third parties	Anti-tamper and detection Role based access
	The exchange nature requires confidentiality	Data protection and security Role based access
	Success of the operation hinges on the data transmission security	Data protection and security Anti-tamper and detection
Privacy	Risk of confidential and cooperate sensitive information leakage	Data protection and security Anti-tamper and detection
	Reuse of their personal data for unrelated purposes without their consent	Anti-tamper and detection Role based access
	Unauthorized access to personal data because of security breaches	Data protection and security Role based access
System Security	Database threats	Data protection and security Role based access
Cyber Crime	Identity theft	Data protection and security
	Fraud	Data protection and security
	Virus attacks	Threat detection

b) Floodgate Security Framework

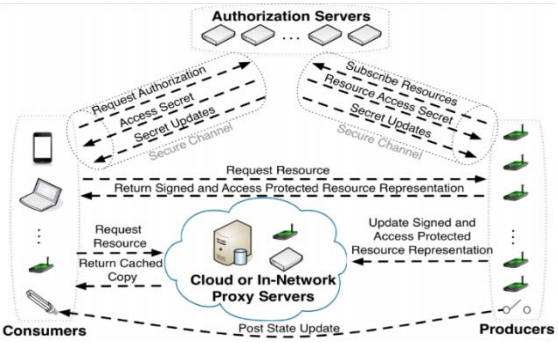

Figure 2: Floodgate Security framework[14]

Floodgate security framework mainly help securing against today's cyber threats. This helps to build secure, authenticated, trusted devices. Thus, this fits best for the infrastructure level security[13].

Table II: Floodgate framework support for the security threats

Security Threat	Concerns	Framework Support
Transactional Security	Information should not be revealed or sold to third parties	PKI Client
	The exchange nature requires confidentiality	PKI Client IDS module
	Success of the operation hinges on the data transmission security	PKI Client IDS module
Privacy	Reuse of their personal data for unrelated purposes without their consent	PKI Client IDS module
	Unauthorized access to personal data because of security breaches	PKI Client IDS module
System Security	Availability attacks	Firewall module
	Database threats	PKI Client IDS module
Cyber Crime	Identity theft	IDS module
	Fraud	IDS module
	Virus attacks	PKI Client IDS module
	Trojan horse	PKI Client IDS module
	Worms	Firewall module

c) Constrained Application Protocol Framework (CoAP)

This framework consists of various modules to handle security and trust issues. The CoAP works at application layers first and this framework best suit for the application security[13].

Table III: CoAP framework support for the security threats

Security Threat	Concerns	Framework Support
Transactional Security	Success of the operation hinges on the data transmission security	Packet protection
System Security	Availability attacks	Availability
Cyber Crime	Identity theft	Packet protection
	Virus attack	Duplicate detection
	Spam	Duplicate detection

d) Object Security Architecture Framework

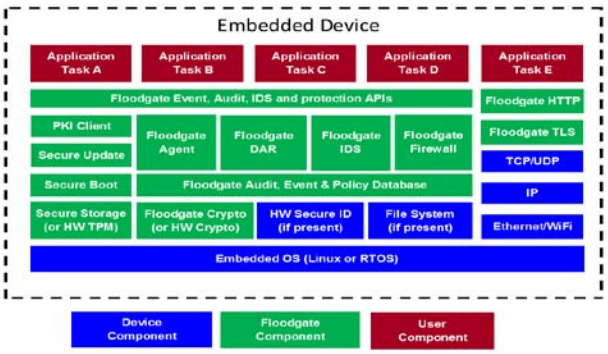

Figure 3: OSCAR Security Framework[15]

OSCAR security framework, explores a novel approach to the problem of end-to-end security. This framework is based on the concept of object security that introduces security within the application payload[13]. This addresses confidentiality, authenticity and privacy through capability-based access control.

Table IV: OSCAR framework support for the security threats

Security Threat	Concerns	Framework Support
Transactional Security	Information should not be revealed or sold to third parties	Authentication
	The exchange nature requires confidentiality	Confidentiality Authentication
	Success of the operation hinges on the data transmission security	Authentication
Privacy	Risk of confidential and cooperate sensitive information leakage	Confidentiality
	Reuse of their personal data for unrelated purposes without their consent	Confidentiality Authentication
	Unauthorized access to personal data because of security breaches	Confidentiality Authentication
System Security	Availability attacks	Availability
	Database threats	Authentication
Cyber Crime	Identity theft	Confidentiality Authentication
	Fraud	Confidentiality Authentication Integrity
	Virus attacks	Duplicate detection
	Spam	Duplicate detection
	Worms	Duplicate detection

V. Conclusion

Security in e-commerce is becoming more topical as the shift from traditional shopping and transactions move away from brick and mortar to click only business. E-commerce is rapidly growing in the global marketplace and still it comes with a risk that the transactions are compromised, which ultimately leads to damaged reputation and financial loss. Therefore, the security of e-commerce transactions hold the criticality of the ongoing success as well as growth of e-

commerce. E-commerce security has five main dimensions- privacy, authentication, integrity, non-repudiation and availability. The main security issues faced by both consumers and providers are transactional security, privacy, system security and cyber crime. This research found insights that, a single framework capable of addressing these needs as a whole is not present yet and a unique security framework solely addressing e-commerce related security issues is not proposed yet. This research sheds light on the need of a distinct security framework to overcome the dark side of e-commerce.

References Références Referencias

1. Haya Alshehri, Farid Meziane, "The Influence of Advanced and Secure E-Commerce Environments on Customers Behaviour: The Case of Saudis in the UK," in 12th International Conference for Internet Technology and Secured Transactions, 2017.
2. Cong Cao, Jun Yan, Mengxiang Li, "The Effects of Consumer Perceived Different Service of Trusted Third Party on Trust Intention: An Empirical Study in Australia," in 14th IEEE International Conference on e-Business Engineering, 2017.
3. Puspa Indahati Sandhyaduhita, "Supporting and Inhibiting Factors of E-Commerce Adoption: Exploring the Sellers Side in Indonesia," in International Conference on Advanced Computer Science and Information Systems, 2016.
4. Sheshadri Chatterjee, "Security and Privacy Issues in E-Commerce: A Proposed Guidelines to Mitigate the Risk," in IEEE International Advance Computing Conference, 2015.
5. Revathi C, Shanthi K, Saranya A.R, "A Study on E-Commerce Security Issues," International Journal of Innovative Research in Computer and Communication Engineering, vol. 3, no. 12, December 2015.
6. Abdul Gaffar Khan, "Electronic Commerce: A Study on Benefits and Challeges in an Emerging Economy," Global Journal of Management and Business Research: B Economics and Commerce, vol. 16, no. 1, 2016
7. Dr. Mohammed Ali Hussain, "A Study of Information Security in E- Commerce Application," International Journal of Computer Engineering Science, vol. 3, no. 3, 2013.
8. Ms. Palak Gupta, Dr. Akshat Dubey, "E-Commerce-Study of Privacy, Trust and, Security from Consumer's Perspective" International Journal of Computer Science and Mobile Computing, vol. 5, no. 6, pp. 224-232, June 2016.
9. Xia Wang, Ke Zhang, Qingtian Wu, "A Design of Security Assessment System for E-commerce Website," in 8th International Symposium on Computational Intelligence and Design, 2015.
10. Ghada El Haddad, Esma Aimeur, Hicham Hage, "Understanding Trust, Privacy and Financial Fears in Online Payment," in 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2018.
11. "Trends in e-commerce & digital fraud: Mitigating the risks," EKN, 2017.
12. "Securing the Internet of Things: A Proposed Framework", [Online]. Available: https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html
13. Mohammad Irshad, "A Systematic Review of Information Security Frameworks in the Internet of Things," in IEEE 18th International Conference on High Performance Computing and Communications, 2016.
14. "Floodgate Security Framework", [Online]. Available: https://www.iconlabs.com/prod/product-family/floodgate-security-framework
15. "OSCAR: Object Security Architecture for the Internet of Things", [Online]. Available:https://drakkar.imag.fr/IMG/pdf/oscar-vucinic.pdf