E-Commerce Security Challenges: A Taxonomy

Mohamad Ibrahim Al Ladan

***Abstract*—With the emergence of the Global Economy, and with an ever-increasing percentage of consumers doing their business primarily via online or mobile devices, electronic commerce, e-commerce, is fast being regarded as the way to go global at the touch of a button. Hence, developing an effective E-Commerce model is becoming vital for any modern business. However, a company must address different new security challenges and be certain to maintain the highest standards of e-commerce security, to protect both themselves and their customers. A failure to adhere to stringent ecommerce security can result in lost data, compromised transaction information, as well as the release of the customer's financial data. This can lead to legal and financial liability, as well as a negative impact on the company's reputation. This new security challenges are the results of the use of the new technology and communication medium, and the flow of information from enterprise to enterprise, from enterprise to consumers, and also within the enterprise. This paper presents the different technology and conceptual components of the e-commerce in general, and identifies and classifies the different types of security challenges facing e-commerce businesses in particular.**

***Index Terms*—E-commerce security, e-business security challenges.**

I. Introduction

The Internet has rapidly become the primary commerce and communications medium for virtually every industry, large or small. As a result, and because of the emergence of the Global Economy, e-commerce is fast being regarded as the way to go global at the touch of a button. In addition, the Internet has allowed for very low cost access to a giant network of people and businesses. This combination of low cost technology and pervasive access to the Internet provides the basis for a radical transformation of the way everybody will conduct business. E-commerce is defined as the buying and selling of products or services over the Internet. E-commerce offers the opportunity to integrate external and internal processes and to lower transaction costs, thus expanding distribution channels and increasing sales and profits. E-commerce has been applied to many areas of business. The two main areas in which it is applied are Business-to-Business (B2B) and Business-to-Consumer (B2C). The B2B area is older and has grown faster than the B2C area because of the introduction of Electronic Data Interchange (EDI) in the early 80's [1]. The B2C area is expanding now in parallel with the expansion of the Internet use and growth.

One of the biggest challenges presented by e-commerce is one of technology and the flow of information from business to business, within the same business, and from business to consumers. Dealing and trading with multiple partners, businesses are faced with an increasing array of different data formats, communication needs and process requirements. Therefore, security issues and challenges need to be the first thought not the after-thought, and must be taken seriously. In order to satisfy the needs of their partners, businesses must be able to respond to these needs and do so in a quick, reliable and secure fashion or risk losing the opportunity of the high and global competition, they should follow security standards and disciplines to gain and retain the consumer trust and confidence in this new type of economy.

There are guidelines for securing systems and networks available for the e-commerce systems personnel to read and implement. However, Trojan horse programs 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.

In this paper we present and classify the different security challenges that e-commerce systems are facing. In the second section, we present a brief literature review. In the third section, we introduce the general architecture model of an e-commerce system. In the fourth section, we discuss the different types of security challenges and their impacts on the e-commerce systems. Finally, in the fifth section, we give a summary and a conclusion.

II. Literature Review

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. To improve the environment for the development of E-commerce and promote further the development of E-commerce, Zhou in his paper [2], about the security issues of Ecommerce activities put forward solution strategy from two aspects that are technology and system.

The success or failure of an e-commerce operation hinges on myriad factors, including but not limited to the business model, the team, the customers, the investors, the product, and the security of data transmissions and storage. Data security has taken on heightened importance since a series of high-profile "cracker" attacks have embarrassed popular Web sites, resulted in the impersonation of Microsoft employees for the purposes of digital certification, and the misuse of credit card numbers of customers at business to consumer e-commerce destinations [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

Manuscript received June 20, 2016; revised September 7, 2016.

Mohamad Ibrahim Al Ladan is with the Rafic Hariri University, Meshref, Damour, Lebanon (e-mail: ladanmi@rhu.edu.lb).

doi: 10.18178/joebm.2016.4.10.457

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].

E-Commerce offers the banking industry great opportunity, but also creates a set of new risks and vulnerability such as security threats. 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 [5].

The effect of security, protection and trust towards consumers as well as attitudes plays a key role in e-commerce implementation. Besides, vital information could also be simultaneously processed to match with data flowing from external ecommerce transactions which could allow for efficient and effective integration into organizational processes [6].

Clearly, the online transaction requires consumers to disclose a large amount of sensitive personal information to the vendor, placing themselves at significant risk. Understanding consumer trust is essential for the continuing development of e-commerce [7].

III. The Methodology and Model

E-Commerce systems use Internet technologies and innovative business processes to develop applications that extend beyond the traditional boundaries of time, space, departmental, organizational, and territorial borders. In its simplest form, the architectural model of an e-commerce system has an IT infrastructure that supports different databases, user interfaces and applications. It can be described in a little bit more detailed form as a model that leverages Web technologies to implement mission-critical e-business applications. This architecture model uses different types of thin clients to access services, provided by resource managers that can be accessed across a strong and reliable network. These thin clients can be browsers running on personal computers, network devices, personal digital assistants, cell phones, and other pervasive computing devices. A simple architectural model that includes the main components of an e-commerce system [8] is shown below in Fig. 1.

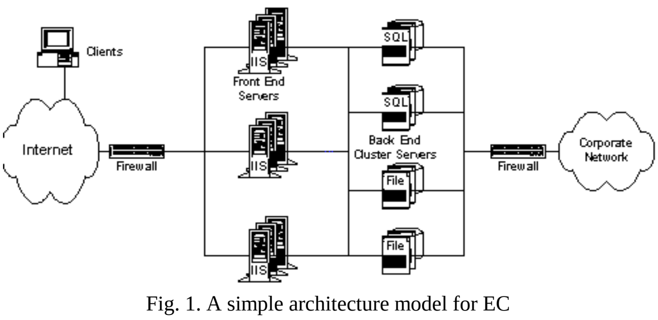


Fig. 1. A simple architecture model for EC

A. *E-Commerce Security Challenges*

Before implementing an e-commerce system, one has to address the different security challenges facing such a system and its major components to ensure its availability, survivability, and the safety and privacy of the data involved in the different types of transactions. E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. While security features do not guarantee a secure system, they are necessary to build a secure system.

In addition, no one will deal with an e-commerce system that may distribute, accidentally due to a security attack, sensitive consumer data such as credit card number, personal information, or financial and account information. In a very simplified scenario where a customer uses a web site for an e-commerce system and gives his/her credit card number and address information, this simple on-line transaction has many potential security vulnerabilities that are related to the different components of the system which include the following:

1) Security problems in client/home computers where data stored in web “cookie” can be stolen and cracked by hostile web-sites, or mail-borne viruses that can steal the user's financial data from the local disk.
2) Eavesdropping and data stealing due to ineffective encryption or lack of encryption in home wireless networks.
3) Eavesdropping and data stealing from the user's keystrokes at Point-of-Sale (POS) terminals in brick-and-mortar stores.
4) Eavesdropping and data stealing from the user's mobile and handheld devices.
5) Eavesdropping and data stealing from networks and different intermediate communication links.

Although some of the security measures like data encryption, authentication, and authorization may address some of the above security problems; there are more vulnerability and security challenges that need to be addressed in other parts of an e-system system especially in the software clients and servers that must use the data.

B. *Taxonomy of E-Commerce Security Challenges*

Based on the architecture model shown in figure 1, security is needed at the following levels of any e-commerce system:

1) Front-end servers must be protected against unauthorized access.
2) Back-end systems must be protected to ensure privacy, confidentiality, and integrity of data.
3) The corporate network must be protected against intrusion.

To apply security at all these levels, a typical e-commerce system can be divided into the following domains:

1) Public network, which consists of clients that access the front-end servers and the Internet.
2) Demilitarized Zone (DMZ), which consists of front-end and back-end server clusters.
3) Corporate network.

The domains are protected from each other using firewalls. External attacks can be prevented through network, platform, application, and database protection.

In what follows, and based on the above discussion, I will classify the e-commerce security challenges into three different levels: Challenges at the client level, challenges at the front-end Servers and software application Level, and challenges at the network and back-end servers Level. Moreover I will classify and discuss the different types of security threats, attacks, and vulnerability issues pertaining to each level.

A. Client Level Security Challenges

Many customers use wireless Internet connections and mobile devices to access e-business systems. Wireless networks and mobile devices present a security hazard, since outside users can eavesdrop on wireless communications. Securing a wireless network with a password can make it more difficult for outside users to connect to the network and access sensitive information, but a wireless connection is not as secure as a wired connection, even if it has password protection [9]. In addition to this, mobile devices can be a security concern because they are easy to be misplaced. Some of the well-known security issues related to wireless networks and mobile devices that affect e-businesses are listed and discussed below.

Captured and Retransmitted Messages. The attacker can capture a full message that has the full credential of a legitimate user and replay it with some minor but crucial modification to the same destination or to another one to gain unauthorized access and privileged to important information [9].

Eavesdropping. This is a well-known security issue in wireless networks. If the network is not secure enough and the transmitted information is not encrypted then an attacker can hack on to the network and get access to sensitive data.

Mobile Devices Pull Attacks: The attacker controls the mobile device as a source of propriety data and control information. Data can be obtained from the device itself through the data export interfaces, a synchronized desktop, mobile applications running on the device, or the intranet servers [10].

Mobile Devices Push Attacks: The attacker use the mobile device to plant a malicious code and spread it to infect other elements of the network. Once the mobile device inside a secure network is compromised, it could be used for attacks against other devices or servers on the network [10].

Lost Device: The possibility of the device being lost or stolen and abused by unauthorized users should be considered by applying some security measures like a password-protection feature on each mobile device.

B. Front-End Servers and Software Application Level Security Challenges

These types of challenges are the results of taking advantages of existing loopholes found in most software applications and server software. Attacker finds out the types of software used by analysing the site, detecting loopholes, and exploiting these loopholes in the system [11]. Server exploits refer to techniques that gain administrator access to the server. This exploits is the most dangers because the attacker can make limitless damage. With a server exploit, you access control of the merchants and all the shoppers' information on the site and can use that for your benefit.

Buffer overflow. Buffer overflow attacks and executing scripts against a server are two major server attacks. In a buffer overflow attack, the hacker takes advantage of specific type of computer program bug that involves the allocation of storage during program execution. The technique involves tricking the server into execute code written by the attacker.

Software bugs/faults. Security holes do exist in most new and existing software systems mainly due to software bugs/faults left by careless or not highly skilled security-focused programmer or software developers. E-Commerce software systems should be interoperable and must exchange data with software systems owned and controlled by others like customers, suppliers, partners, and other processing software agents or servers. Therefore, security mechanisms deployed in e-commerce systems must be flexible, standards based, and interoperable with others' systems. They must support browsers, and work in multi-tier architectures with one or more middle tiers such as web servers and application servers. On top of these, network and communication standards and protocols are in a state of continuous changes which makes keeping up-to-date with all security advisories and security patches a difficult task. Hackers constantly discover and make use of these vulnerabilities.

Viruses and other malicious software. Hackers can use viruses and other malicious software to infect e-business systems and be able to steal customers' information, cause data loss, or make e-business systems inaccessible. According to Consumer Reports, malicious software cost consumers about $2.3 billion in 2010, and as another example, Sony's PlayStation Network was the victim of a major hacking operation in 2011 that resulted in the theft of millions of users' personal information [10].

C. Network and Servers Level Security Challenges

Networks have their own security issues mainly due to the fact that most networks are dependent on other private networks, owned and managed by others, and on a public-shared infrastructure where you have much less control of, and knowledge about, the implemented security measures. Although encryption aid to some extends in securing information moving across networks, it's the network operator's job to ensure that the information is securely transported to its final destination. Some of the well-known security issues related to networks and servers that affect e-commerce systems are listed and discussed below.

Distributed Denial of Service (DDOS). One of the most troublesome security issues facing e-commerce systems is when hackers launch a denial of service attack. This attack is characterized by an explicit attempt by attackers to prevent users from using an e-business system. DDOS attacks are common in all kinds of networks where the attacker does not require any physical infrastructure, all what he do is flood the main e-business server with a large number of invalid requests slow it down or crash it and make it inaccessible. The Distributed Denial of Service (DDOS) attacks are the latest evolution of DoS attacks and their success depends on the inability of intermediate sites to detect, contain and eliminate the penetration of their network. This attack creates problem not only to the target site, but also create congestion in the entire Internet as the number of packets is routed via many different paths to the target [12].

Session Interception and Messages Modification. The attacker can intercept a session and modify the transmitted messages of the session [13]. Another possible scenario by an attacker is to intercept the session by inserting a malicious host between the client host and the end-server host to form what is called man-in-the-middle. In this case all communications and data transmissions will go via the attacker's host.

Cross-site scripting. Attackers exploits known vulnerabilities in web-based applications, their servers, or plug-in systems they rely on. Exploiting one of these, they fold malicious content into the content being delivered from the compromised site. When the resulting combined content arrives at the client-side web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system.

Firewall Loophole: A firewall is software or a hardware device that is used in e-commerce systems to separate the back-end servers from the corporate networks and enables communication between the back-end servers and a few servers within the corporate network Firewalls are mandatory for business sites. However, they are usually implemented at the network protocol layer and do not protect the system from attacks aimed at higher protocols such as HTTP. For example, the Web servers accept data packets through port 80, meant for HTTP requests. If a user accesses a component through an HTTP request that causes buffer overflow, the service can crash and provide the user access to the system for further attacks. Hackers can gain access to the intranet corporate back-end servers using some known unfixed firewall loopholes and try to hack into price lists, catalogues and email lists and change or destroy the data, which can disrupt or even disable business operations [14].

Table 1 below summarizes the different levels and types of e-commerce security challenges.

TABLE I: SUMMARY OF THE DIFFERENT LEVELS AND TYPES OF E-COMMERCE SECURITY CHALLENGES

Client Level Security Challenges	- *Captured and Retransmitted Messages* - *Eavesdropping* - *Mobile Devices Pull Attacks* - *Mobile Devices Push Attacks* - *Lost Device*
Front-End Servers and Software Application Level Security Challenges	- *Buffer overflow* - *Software bugs/faults* - *Viruses and other malicious software*
Network and Servers Level Security Challenges	- *Distributed Denial of Service (DDOS)* - *Session Interception and Messages Modification* - *Cross-site scripting* - *Firewall Loophole*

IV. DISCUSSION

E-commerce has not been able to achieve its full potential due to many reasons that include the constant warnings by the media not to be a victim of identity theft and financial fraud and to be extremely careful when performing online transactions due to some security and privacy breaches. The consumers' perception of possible risks and threats to the security and privacy of their personal information affects their online purchasing behaviour. A lot of people hesitate and sometime refuse to perform online transactions and relate that to the lack of trust or fear for their personal information [15]. Therefore, in order for e-commerce to expand and achieve its full potential, companies need to understand these needs collectively, and they should seek to develop systems, methods or guarantees that would ensure the private and secure communication of information between buyers and sellers in any e-commerce system.

Hence, security is one of the most important features of any e-commerce system. In addition, since e-settlement, e-signatures, and e-payments are essential functions/features of any e-commerce system, therefore, stringent security measures and more sophisticated cryptography and authentication technologies must be developed and deployed. There is a generally perceived risk attached to payments made via the Internet, and this perception is in some situations justified. The information sent from the client front-end to the back-end server through different communication networks may pass through many different servers, routers, hubs, and stages before being delivered. The information is in digital form, and at any stage an unauthorized individual may scan every message looking for credit card numbers. Therefore, any e-commerce system must be secure to prevent fraud. Customers need reassurance that the information they key into the system is secure and private. Most systems use the industry standard protocol called Secure Socket Layer, SSL, which encrypts every message on the network making it extremely difficult for anyone who intercepts the message to extract information. Other systems use another existing and widely used security protocol called the Secure Electronic Transaction, SET, which is developed in partnership by Visa and MasterCard to ensure a secure e-payment infrastructure for e-commerce systems [16].

V. SUMMARY AND CONCLUSION

The recent development in Internet and Web Technology has affected nearly all business and commerce activities. It is more than transferring current business operations to a new medium. The process requires redefining business models, changing the corporate culture, and establishing reliable customer service. It has also to face and overcome so many different types of challenges. E-commerce can be regarded as a new form of marketing with a foreseen explosive growth over the next few years. It can be defined as doing business online or the exchange of goods and services over the Internet. Rapid growth in mobile computing, communication technologies, e-payment systems, and other new technologies have accelerated the growth and popularity of e-commerce. However, the main barriers in growth of e-commerce are new security threats and challenges. Although there are several security strategies which any e-commerce system can employ to reduce the risk of attack and compromise significantly, new attack strategies and vulnerabilities only really become known once an offender has uncovered and exploited them. In addition, increasing technical knowledge, and its widespread availability on the internet, criminals are becoming more and more advanced and skilled in the types of attacks they can perform. The rapid increase in the use of e-commerce is accompanied by the rise in the number and kind of security attacks and threats. The vulnerabilities that these attacks exploit range from loopholes in third-party components utilized by websites, such as shopping cart software to different types of vulnerabilities such as SQL injection, cross site scripting, information disclosure, session interception, messages modification, buffer overflows, and others as mentioned in the previous sections. Securing an e-Commerce system is a dynamic process where new threats crop-up every day, and hence, a proper planning should be done to stay protected against possible new security threats in order to retain customer's trust in the system.

In conclusion, e-commerce is growing rapidly and numbers of technologies have converged to facilitate the proliferation of e-commerce systems. However, these kind of systems faces a challenging future in terms of the security risks it must prevent. With technology moving at high-speed no e-commerce can ever claim to be 100% covered by any security measure. Security issues are extremely important for the survival of any system, and therefore must be constantly analysed and taken care of. Moreover, security issues and measures need to be the first thought not the after-thought, and must be taken seriously. For companies to look toward the bright and promising future of e-commerce with confidence, they should follow security standards and disciplines to gain and retain the consumer trust and confidence in this new type of economy. There are guidelines for securing systems and networks available for e-commerce systems personnel to read and implement. Educating the consumer on security issues is still in the infancy stage but will prove to be a major component of the e-commerce security architecture.

In this paper, an overview of the security challenges facing e-commerce systems is presented. In addition, a taxonomy of the different type of security risks and challenges that any e-commerce system may have to face is given. The major contribution of this paper is in the discussion and classification of the different types of security challenges that any e-commerce business may have to face.

References

[1] E. Awad, "Electronic commerce: From vision to fulfillment," Prentice Hall, 2002.

[2] Y. Wen and C. Zhou, "Research on e-commerce security issues," *International Seminar on Business and Information Management*, 2008.

[3] N. M. A. Al-Slamy, "E-commerce security," *IJCSNS*, vol. 8, no. 5, 2008.

[4] R. Yazdanifard and N. Al-Huda Edres, "Security and privacy issues as a potential risk for further ecommerce development," in *Proc. International Conference on Information Communication and Management*, vol. 16, 2011.

[5] R. Barskar and A. J. Deen, "The algorithm analysis of e-commerce security issues for online payment transaction system in banking technology," *IJCSIS*, vol. 8, no. 1, 2010.

[6] A. A. A. Moftah, "Challenges of security, protection and trust on e-commerce: A case of online purchasing in Libya," vol. 1, no. 3, 2012.

[7] P. B. Rane and B. B. Meshram, "Transaction security for ecommerce application," *IJECSE*, 2012.

[8] M. Ladan, "E-commerce technologies and challenges," *Journal of Communication and Computer*, no. 7, vol. 7, USA, 2010.

[9] K. Thomas. (2011). PCWorld. [Online]. Available: http://www.pcworld.com/article/226128.

[10] S. J. Purewal. (2012). PCWorld. [Online]. Available: http://www.pcworld.com/article/259548.

[11] J. Singh, "Review of e-commerce security challenges," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 2, Issue 2, 2014.

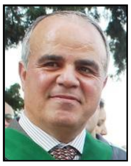
[12] M. Ladan, "Web services: Security challenges," in *Proc. the IEEE World Congress on Internet Security*, London, UK, 2011.

[13] M. Niranjanamurthy, N. Kavyashree, S. Jagannath, and D. Chahar, "Analysis of e-commerce and m-commerce: Advantages, limitations and security issues," *IJARCCE*, vol. 2, Issue 6, June 2013.

[14] OLALA, *Malicious Software Infections*, TimeLine Business Facebook Page, Domain Names, OLALA Marketing, 2012.

[15] Z. Tian, N. Xu, and W. Peng, *E-Commerce Security: A Technical Survey: Intelligent Information Technology Application Conference*, 2008.

[16] M. Niranjanamurthy and D. R. D. Chahar, "The study of E-Commerce Security Issues and Solutions," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 2, 2013.



Mohamad Al Ladan has over 18 years of teaching (BSc, BEng, Msc, MEng, PhD levels) and training experience in the area of computer hardware & software and information technology. He has taught at different local and international universities and has worked in different countries including USA, Canada, KSA, and Lebanon.

He received the B. Eng.(Honors) in electronics and communication engineering from Alexandria University/Beirut Arab University in 1986, and a M.Sc. and the Ph.D. degrees in computer engineering from Syracuse University, Syracuse, N.Y., USA, in 1990 and 1995 respectively. He has received a number of awards that include: *Tuition Scholarship* and *Research Assistantship* from the Computer Engineering Department and the Networking and Computing Services Center at Syracuse University from *1990 to 1995*, a Syracuse University "*Best Student Worker*" recognition award in June 1994 for his contribution in developing both the *Job Information System*, a campus-wide database system for managing and finding jobs for students on and off-campus, and the *Syra-CWIS* system, an Internet/Netscape-Based information system for Syracuse University, and an *Honor* student status in the Faculty of Engineering at Beirut Arab University from 1981 to 1986.

Prof. Al Ladan has several international research publications in the areas of distributed and parallel computing, object-oriented software, internet programming, e-learning, web services, cloud computing, and e-business security issues. He participated in several international computers and IT related conferences and a reviewer for different international conferences and journals. He is a Member of the *Order of Engineers* in North America and in Lebanon, and a founding member, an ex-president, and a current member of ACS.