University College of Takestan

Available online at **http://UCTjournals.com**

Iranian Journal of Social Sciences and Humanities Research

UCT . J. Soc. Scien. Human. Resear.(UJSSHR)

16-20 (2016)

Volume 4,Issue3

ISSN 2382-9753

Information Security in E-Commerce Law

Mostafa Abbasi[1] and Ali Zare[2]

[1]Department of Law, Electronic Branch, Islamic Azad University, Tehran, Iran
[2]Department of Law, Tehran Sciences and Research Branch, Islamic Azad University, Tehran, Iran

Original Article:
Received 14 June. 2016 Accepted 10 July 2016 Published 09 Aug. 2016

ABSTRACT

This research was conducted by purpose of moreidentification and familiarization with e-commerce law and information security. There are no boundaries in e-commerce and there is no difference for people to buy their goods from the neighbor shop or from a shop in another continent. E-commerce increases speed and volume inn merchandise transactions and reduces buyers' and producers' costs tangibly, time saving, more attraction, removing brokers, and finally more benefits. However, the e-commerce has its problem and defect like any other issues. One of the biggest obstacles in e-commerce way is information security. Encryptions used in information security to change information to codes that no one can use it except the permitted user even if others access to it. The encrypted information can change to the initial form by permitted user (by decryption process). Encryptions used to protect both electronic and non-electronic transmitted or stored information, encryption provides good facilities for information security such as improved methods of authentication, message compression, digital signatures, non-repudiation capabilities, and encrypted network communications. If encryption is not implemented correctly, it can cause security problems.

Keyword:
security, information, law, e-commerce

*** Corresponding author:** ***Abbasi***

Peer review under responsibility of **Iranian Journal of Social Sciences and Humanities Research**

INTRODUCTION

Information security means protecting information and informational systems from unpermitted activities. These activities include accessibility, usage, and devalue, read, copying, recording, damaging, changing, or manipulating information.

The information security has significantly grown and evolved in recent years. There are many ways to enter to this profession as a job. There are various specialized issues such as network security(s) and infrastructure, security of applications and databases, security testing, auditing and information systems, business continuity planning, electronic crimes, etc.

The specific standards and technologies are used in order to establish information security in e-commerce. The information security methods are actually the result of combination logical and mathematical conceptions which were provided in algorithms models.

E-commerce includes various activities such as goods and services e-transaction, fast deliver of digital demands, cash e-transfer, stock transaction, e-barcode, commercial designs, direct marketing, and warranties.

In spite of all benefits of e-commerce, the online transactions and communications is a bigger location for exploitation technology and even criminal actions. These problems are not just or e-commerce, but it is a part of extensive involving problems of computer and informational systems. Many companies have been exposed to related crimes to security from virus attacks to commercial scams including commercially sensitive information and confidential information such as credit card stealing. Such security attacks cause millions of dollars of losses and disrupt security companies. Many reporters and counselors estimated the related losses to security defect to billion dollars. However, what is more important than accuracy of this lost amount is this reality that it can easily be assume that increasing informational systems users, easy access to information, and incremental growth of aware (technician) users increase number of exploitations from technologies and security threats with the same rate. Unfortunately, since many companies don't like to confirm penetration to their systems and sharing their information about extension of this penetration to others, the accurate losses imposed on companies about information security can't be predictable, reluctance to provide related information about security defects is made by this popular fear that if people know it, they will lose their reliance on those companies for companies ability in protecting their assets. So companies will lose their profits. Since today consumers are distrustful towards the provision of online financial information, companies won't obtain anything with voluntary confirmation of the fact that they are victims of security-related offenses. Protecting a positive look toward e-commerce in minds is the first concerns of many companies, and it is completely necessary to survive and remain in competitiveness by the media excitement about today internet and its abilities. The lack of the firsthand information about planning and resistant against security threats makes it more difficult; nonetheless, technologies and security information methods, and public managerial technics in planting and protecting resources of an organization information technology had significant growth in past decade. The purpose of the present research is studying information security and its importance in e-commerce law.

E-Commerce

E-commerce includes any actions with information and communication technology (ICT) to execute commercial purposes among organizations orbetween organization and consumer. Publicly, the e-commerce term refers to electronic transactions by communicational networks. First buyer or consumer searches a virtual shop in internet, orders a good by website or email, and finally buys it.

Iran e-commerce law didn't define e-commerce, but it stated its scope and inclusion. It states in article 1: "this law is collection of regulations for easy transaction and secured information in electronic intermediaries using new communicational systems." The following two definitions weren't included in extensive meaning, e-commerce:

1- commercial activities;
2- The exchange over the Internet;

Since two main element on establishment of e-commerce is possible by electronic devices. The following cases can be mentioned about article 1 of e-commerce law:

1- The mentioned law doesn't concern about legality or illegality of the transacted information issue by electronic intermediaries or communicational systems. Therefore in spite of using the term "commerce" in e-commerce doesn't necessary limits the transactions to the only commercial ones.

2- This article was adopted from article 1 of UNCITRAL model law on electronic commerce and states that this law includes any information as data message or applications in commercial activities:

A) The UNCITRAL commission suggests the following text for countries with probable tendency to limit the mentioned executable law to international data messages.

"This law is executable for where a data message defined (in part A of article 2) is related international commerce".

B) This law doesn't neglect any considered regulations to support consumer.

C) The commission suggests the following text to countries with probable tendency of extending lax execution range:

D) " this law is related to aby data message information type except:

1- All interpretations should be possible in commercial expression to be able to enclose all resulted issues from either commercial relationships or contractual relationships, etc.

2- The commercial relationships should include the following transactions, but they are not limited to them: any commercial transactions to provide or exchange goods or services by agreement on distribution, commercial representation, brokerage, leasing, interpretation works, consulting, engineering, licensing, investment, finance, banking, insurance points or contract operation, joint treatment or other forms of commercial or industrial cooperation, air transport, sea, or land (including through the train) of goods or passengers.

3- Providing services based on individual demand are not the element of e-commerce law in Iran in contrast to Europe Union guidelines 2000/31 EC on e-commerce.

According to what were mentioned previously, another definition about e-commerce is "publicly, electronic commerce involves the production, promotion, sale and distribution of goods through electronic means based on the processing, and transfer of digitized information." Of course, this definition in this aspect doesn't refer to services. (SadeghiNeshat, 2015: 119)

Data or Information on E-Commerce

In Iran e-commerce law, "data message" is attributable if there are other legal terms, and is actually known officially as electronic reason. Therefore, data message can be in number, shape, written, or any other symbol, and producing, sending, receiving, storing, or processing it by electronic or light devices or any other new technologies are considered efficient for data message as electronic reason. Therefore, the paper print of data message is considered electronic reason which was produced by computer.

The UNCITRAL model law on e-commerce means the produced, sent, received, or stored data by electronic, light, or other similar devices such as the exchange of electronic data, electronic mail, telegram, telex or fax without restrictions to these devices which were stated in clause (A) of article 2. According to manuscript of article 2, the proposedelectronic reason law issued by Commonwealth Secretary Public of the Council of Euro Marl in London, "data" means expressing information or conceptions in any shape and "electronic document" means the registered or stored data by any computer devices or any other similar devices and can be read by another computer system or any other similar device. This electronic reason includes display or print the data with any output form. (SadeghiNeshat, 2015: 219).

Information Security

Information security in e-commerce will protect organizational capitals and reduce costs to satisfy customers, collaborating companies, and investors, and it will guarantee e-commerce continuity. Since business and commercial transactions in virtual spaces go beyond the physical boundaries and physical limitations don't have role in virtual spaces, the used system to provide security and respond to security needs of e-commerce must be international and confirmed and attributable by public.

The specific standard and protecting technologies are used in order to establish information security in e-commerce. The information security methods are actually resulted by logical and mathematical concepts in algorithms models.

Nowadays, the financial, credit, and personal information based on internet is used incrementally all over the world. On the other hand, there are many information and resources circuits on network, therefore, it is not clear that the mentioned information goes where and who use them. Therefore, protecting information security is one of important issues of e-commerce. Although, there is not absolute security, costs should be paid to have at least having a non-vulnerable condition.

There are three important issues in e-commerce literature and information security in internet networks as following:

1. ***Authentication:*** it consists of identification the identity of the both sides of commercial process.
2. ***Encryption:*** it means coding. Each information record should be coded in a way not to be read or changed by other people.
3. ***Authorization:*** after authentication and encryption of the received applicant record, the range of access to data bank records and its operational collections were determined already and is under the access permission of "authorization" that is significantly important.

Encryption and decryption of data is done by a key and set of encryption algorithms according to figure. In the mentioned process, the message that should be encrypted is called plaintext message. First it is divided to a series of multi-bit blocks (n-bit blocks).

Then encipher algorithm process using one key and the above blocks as input data after executing the defined processes in encryption algorithm yields peer to peer encrypted algorithm with the same length of cipher algorithm using the same key and change the encrypted the cyphertext block to initial message.

In advanced algorithms, the cipher changing depends on the previous block contents, it means encryption and cipher operations on each block.

Signature and Its Role in Information Security

Attributable to an electronic document in cyberspace which was made consciously and tries to provide its legal effects, the existence of e-signature is necessary to attribution of the demanded document is permitted to the mentioned individual.

The e-signature is duty of the sender and has duty of data attribution to him. When a person buys a book by internet and the whenever the buyer doesn't sign the data message and his identity won't be authenticated by certificate authorities, it isn't assured to know the buyer is legalized to buy or not, and this matter necessitates e-signature and certificate authorities.

Iranian e-commerce law enacted in 2003 defined e-signature in clause (F) of article 2 as "e-signature includes all type of attached signs logically to data message which are used to identify the signer of message". Clause (G) of that article defined secured signature as "each e-signature should be based on article 4 of this law. Consequently, the legislator stated in article 7 of Islamic commercial law: "whenever the law knows signature necessary, e-signature is efficient."

According to article 15 of Islamic commercial law, when the e-signature has the mentioned conditions, denial, and doubt wouldn't be valid and the data message can be claimed to be fake or to prove that the mentioned message is not valid legally anymore.

In this regard, e-signature equals to application of hand signature. E-signature has all effect of hand signature legally. Both confirm identity and relationship with the signed text and this fact in actually abonnement of signature inn all legal systems. Therefore, a type of technology is necessary as a precondition for e-signature to accomplish the application of hand-signature and confirming data (SadeghiNeshat, 2015: 270).

In French law the definition of electronic signature, the second part of the Civil Code stipulates in Article 4-1316: "e-signature includes a secured procedure that assures identification the signature with attached document. This procedure is considered reliable unless there is any

opposition. When an e-signature is made, it assures the signor identity and holism of document according to the determined condition in the approval of the state council." The clause 1 of article 1 in approval of state council, the e-signature is known as made using thee mentioned process in the first clause of the second paragraph, article 1316-4 of national law.

Paragraph 5 of Article 106 of the electronic signature law United States of America declares: "e-signature is accomplishment of any sound, sign, or electronic process which is attached to a contract or document or accompanies it logically, accepted or executed by a specific message signature.

The common point in all definitions is that e-signature indicates the identity of signor. Consequently, the signature should be in a way to accomplish this performance. Therefore, just typing a name of a person at the end of a text without any encryption can indicate the positive identity of signor scarcely, because in spite of writing name by hand that has possibility of adaptation, typing name doesn't have this feature, so discovering the signor identity won't be possible. In this regard, any mark cannot b e-signature in itself, but sign should be with a type of encryption to be considered as a signature. Encryption in public means any way to hide information. It means, this is a way to understand text just but the addressee of the signor, and to be sure of the real identity of signor. Some people believe that the most simple and principal view about signature is typing an individual name, and an individual name on email is considered as an e-signature. In addition, a scanned signature of an individual in a document is used to confirm its content and identity of the sender. Thee type of signature are mostly used for less important and minor transactions.

Nonetheless, it seems that the previous familiarization and validity of a receiver about the sender of an e-mail, and accessibility to the password to be just for the sender is more important than his/her signature, and increase reliability of the sender identity and e-mail content. (SadeghiNeshat, 2015: 275)

Regulations for Making and Decryption of Digital Signature

In making and decryption process of a digital signature the following regulations should be obeyed according to what are necessary for signature:

A- Signor law:

If the public and private keys are both made by signor, the digital signature and its unique features can't be forged, even if the signor loses controlling private key. For example, he forgets this key uses which facilities.

B- Message law:

Since the digital sign is integrated by related message and have united code; therefore, message should be in a way to be encrypted by public key. (Rahimi, 203: 165)

Encryption Principles

1- Signature based on symmetrical encryption

It is called secret and private key and includes encryption algorithms in which two commercial partners should use unit and similar key for signature, encryption, and decryption of data electronic transaction that is called symmetrical encryption algorithms. In other words, if data e-transaction message is encryption by one key, it can't be encrypted by a different key. Using symmetrical make decryption easy and there would be no need for partners to produce confidential algorithm and transact with each other. Although, each commercial partner can use the same encrypted algorithm and just transact the confidential common key. Nonetheless, the symmetrical encryption has disadvantage such as high costs and particularly sending key to mentioned receiver is risky. The security of this encryption depends on nth sent key to be secured to what extent; the partners should agree on a confidential common key. Thee confidential commercial keys should be protected equal to number of commercial relationships. It means one key for each commercial partners. Another disadvantage of is the root or destination originality. Therefore, each e-data message that should be encrypted by a key can be sent by each partners. Using what is called public encryption and used in asymmetrical algorithm can solve the related problems to deny originality and delivery and non-denying reception.

2- Signature based on asymmetrical encryption

It is called public key and one of two public key encryption keys. Each user has full access to this key to use it for his/her sent message encryption, decryption of digital signature, and it.

The public key encryption includes a symmetrical design using a pair of keys for encryption. The public key encrypted data and private (secret) key decrypted data corresponding to them. The mentioned process is reversed for digital signature: the sender uses private (secret) key to make the unique electronic number that people process the corresponding public key that can use this number for reading.

Therefore, the asymmetrical encrypted systems are based on two keys: one public and one private key that are different; although, they are related according to calculation. An individual can encrypted message and send it and this message is decrypted just by the sent public key using private key. This actions assures the signor that just the mentioned addressee can read the message. The asymmetrical encryption is called public key encryption. Digital signatures use the public key encryption for encryption and confirmation the information. The digital signature assures that document content hasn't changed and also deny of receiving by message sender will be canceled.

3- Spare key

Spare key makes decryption of the encrypted message possible in specific and determined condition. Many firms and institutes precaution about the widespread use of encryption within their organizations, because they have this feat if the responsible of encryption key leaves his/her job or dies, or opposite with company for any reason, the company secrets will be divulged or damaged forever. This problem will be solve by having a spare key and this key can be used in specific conditions

B) Certificate authorities (confirmers)

It should be claimed that e-reason in e-signature concept is sure that it is used in Iran e-commerce law, too. The electronic information security is done by the establishment of an electronic certificate authorities. One of the most important technical tool considered by new institutions to

provide security and for law is the public key infrastructure (PKI) and certificate authority (CA). (Rahimi, 2003: 165)

Conclusion

Extending e-commerce needs providing confidentiality and public reliance to this type pf commerce. Since buyer and sellers don't know and even can't see each other and they may be in different countries, security and electronic data transmittal should be guaranteed. One of the most important aspects of e-commerce and its comparison to all similar traditional types is proving document and security approval, proving identity of the parties and the authenticity, security and confidentiality of information and documents are conducted traditional, secured, and simple methods. (Birth certificate or identification card, signatures, document, Notary Public, and strongbox). Keeping legal relationships confidential based on stamp paper is possible through paper documents and other physical methods. In addition, signature on document confirms its originality to great extent. Manipulation, falsification, and distortion of paper documents are discernable by seeing them, while electronic data changes don't remain physical sign.

The information security has significantly grown and evolved in rent years. There are many ways to enter this field as profession. The encryption is used for information security to change information to a form that no one can use information except the permitted user even they access to them (decryption). Encryption is used for information security in transmission (both electronic and non-electronic) or storage. Encryption provides good facilities for information security such as improved methods of authentication, message compression, digital signatures, non-repudiation capabilities, and encrypted network communications. If encryption is done accurately, it can have security information. Encrypted solutions should be conducted using the accepted standards which are examined by skillful and independent experts. In addition, the length and power of the used key is so important in encryption.

Security provision and assurance in e-commerce protects organizational capitals besides reducing costs and satisfy customers, collaborate companies, and investors. In addition, it assures development and continuity of e-commerce. Since commercial transaction and business go beyond physical boundaries. The physical restrictions don't play significant role in virtual spaces. Therefore, the proposed system to to respond e-commerce security needs must be international and confirmed and approved by public.

Specific protection technologies and standards must be used to provide information security in e-commerce. The information security methods are actually resulted by combination of logical and mathematical concepts. Symmetrical algorithm is a type of encryption algorithm with 1000 time higher speech than asymmetrical pattern. However, keeping many keys bring many problems. Combination of these two algorithms can solve this problem, increase speed, and protect confidentiality and integration simultaneously. Hash algorithm estimated integration and non-denial, but data isn't transmitted confidentially. The problem of sender authentication is still present in encryption algorithm. Digital signature and digital certificate remove this problem well. Digital signature isn't use about confidentiality, but it has other capabilities.

References

1- P., Rahimi, 2003, e-commerce and its security. Islamic Azad University, North Tehran branch

2- A., SadeghiNeshati, 2015, e-commerce law, Tehran, Jangal publication

3- Law on Electronic Commerce adopted in 2003

4- Commercial Code adopted in 1932

5- Civil Law adopted in 1928