International Journal of Information and Communication Technology Research

http://www.esjournals.org

Computational Considerations in Security of Electronic Commerce Systems (ECS)

Rahmat Zolfaghari
Department of Computer Engineering,Hashtgerd Branch, Islamic Azad University, Tehran, Iran

ABSTRACT

Electronic Commerce(EC) when situated that was prepared their exchanges security like other communication and software systems.In this paper ,the need for security EC systems (ECS) and discusses the threats and Services, the main threats include: failure, pirvacy, manipulation, forging and denial; the main services include: confidentiality, authentication, integration and Undeniable.

In addition to the challenges and computational considerations such as compatibility of copies distributed geographically dispersed ECS ,time (date and time) and formal and mathematical influence is investigated to ECS and algorithm and encryption approaches include: symmetric and asymmetric algorithms and algorithm hash, digital members and digital certificate as services and approaches to confronting with security threats in ECS are reviewed.

Keywords: *Electronic Commerce Systems(ECS), Security in ECS, algorithms ECS, computational considerations ECS.*

1. INTRODUCTION

EC is Collections communications, information management and security capabilities that allow to organizations, companies, public (general people) and government to display their services information and products through optimization, easy, fast, the minimum cost and without intermediate with computer networks especially internet.

ECS is not limited to buy and sell but any commercial and financial active between people and institutions can be at EC domain. EC includes categories like: E-business, E-banking, E-marketing , smart cart, connections customer management and E-government. While ECS raises accuracy and processing speed, are also at risk and threats.
The overall EC includes stages: survey catalogs, product and vendor selection, order, send information, payment and give product that in each above stages exchange electronic message between buyer and vendor that this exchanges need to safety Condition.

There are many security threats like stealing content and change and denial content that threat the above stages.According to EC, the buyer and vendor do not know each other and do not see each other. This relative reliance should did by means of security guarantees.

The distinctive feature e-commerce and traditional commerce is Proof of Authenticity, Document Security that the traditional paper-based documentation is often manipulated, forged and altered documents by looking at it is detectable, while the change electronic data unlike paper-based Documentation do not remain physical Signs.
Therefore, the security and trust of the public to electronic Documents is very complex and requires protocols and secure electronic software.According to the increasing importance and growth of E-commerce, security threats are on the rise, so politics and security tools should be provided.

2. SECURITY IN EC

Security in EC has an interconnected with reliable EC system. According to software, reliability means a system with indices such as: availability, reliability, safety, maintainable, confidentiality, integrity and capability of authentication and non-repudiation. One can have a relative reliable to the system with these characteristics. To have them and public confidence to doing commercial approaches with the least error, security policy must be designed and security mechanism must be provided to implement this legislated policy.

2.1 Definitions of Security Index

Since most of the EC systems are in global level, so its geographical spread is all over the world. The more distributions, the more availability. But we should pay a specific attention to compatibility challenges of different versions of system in which there is a required algorithm.

1. Availability: correct system performance against user request in a specific moment.
2. Reliability: access to a system in a limited time.
3. Safe: that means. If the system temporarily shut down disaster does not occur To do so, we should assure the safety with accurate mathematical computation.
4. Maintainable: easy repaired after a system failure. The more coefficients, the high availability. Specifically, if these failures are considered automatic one. This challenge is along with

temporal, informational and physical addition that simplest one is to use repetitive version of system which a new situated version is a failure one.

5. Confidentiality: that means system must reveal its information to allowed people.
6. Integrity: that means system is able to recognize an unallowable manipulation in its assets (hardware, software, data) and prevent them. Other approaches such as trigger, … are viable for this challenge.
7. Authentication: that means an unallowable person (second person) cannot send a message to other commercial side in place of other side. Encryption algorithms are available for this challenge.
8. Non-repudiaton: that means prevention of message and document rejection in a process that electronic sign and certification are available for this challenge.

All mentioned indices are implemented in software tools and module frame, sometimes in hardware frame which using them is so easy for users.

2.2 EC security at the macro level consists of two parts as follows

Security in channels and communication network level: is preparing the ways for prevention of unauthorized intrusion of person in to communication networks. Establishing this level of security by computer and communication information and with using the protocols and security devices of communicaton networks such as firewalls.
Security in level of EC application: means of security in users is that security of electronic transfer in communiation network by entering authorized and unauthorized individuals into network don't threat. Establishing this level of security require to use the tools and EC sort wares. Each of softwares is provided level of security for EC transaction. Of course, the security not to be absolutely but also degree of relative confidence are provided. Therefore, in most of EC concepts, trust with security is introduced.

2.3 Security threats and their security services

Security threats are as follows:

1- Interception: refers to a situation where an unauthorized person to gain access to services and data. Eavesdropping, communication between people and permissive process of electronic exchanges and illegal copping of files and directories by hackers are intercepher. For counter to this threat of security services, we need to privacy.
2- Interruption: occurs when a file is corrupted or wiped out or service not to access. Dos attacks including threats of interruption. To counter this threat of the security services we use "accessible namely, for example, with repeat file prescriptions, the new prescription replaces the ruinous prescription and the rate of accessibility is goes up.
3- Modification: to unauthorized change of data or modification of services is called. Namely, hackers with stealing the main information, change it for the benefit of its own and then send the message to receiver by sender. For counter to this security threat, we need to security services "integrations".
4- fabrication: refers to a situation in which the attacker has produced new data that do not exist and sends it to the receiver. For example: add a new password or new records in a database of a system. 'The essential security services for opposing to this threat is (authentication).
5- Denial/repudiation: The person (authorized or unauthorized) all or part of the exchanged messages during an electronic process will allow. The essential security services for opposing to this threat is (impossible).

2.4 Politics and Security Mechanisms:

A description of the security requirements is known "security policy" the "security policy specifies that any system entity (the users. Data and machinery…) what to do and how things have been prevented.

The security mechanism is implementation of security policy. The important mechanisms:

1. Encryption: has a fundamental role in electronic systems. Coding will change the data in ways that an aggressive people cannot find it. Coding is one secret way to keep the data. Coding allows us to we recognize manipulating in data and ensure their integrity.
2. Authentication: To ensure the user's identity. Customers. Servant and a host or other entity is used, For example: When a client requests a service run before anything, we should be sure of her (his) identity (Graphic is this general imperative service).
3. authorization: After customer was determined we should be seen if the client has permission of performing the requested action or not. Kind of access to different existences is determined by their licenses.
4. Auditing: is apply for determining that entities are used which source and how use it. Audit reports is very useful tool to analyze the sercurity weaknesses of the system. And the next steps identifies the attack of hackers. For this reason, aften hackers will try to avoid leaving any trace. Therefore, auditing is tight the arena

For hackers.

3. ECS ALGORITHMS (ALGORITHM AND STRATEGIES FOR SECURITY SERVICES IN EC SYSTEM)

3.1 Symmetric cryptography algorithm:

In this Algorithm there is a same key for doing cryptography and decoding this Algorithm applications to creat a confidentiality in Documents for example we can use the password to access to the Documents, but this method has 2 limitation:

- Each person needs to have a shared key in own Exchanges with anybody else. Therefore each person with unlimited person needs to unlimited shared key.
-Senders have to send their Decoding to the receiver after cryptography and it confront a problem if we are going to cryptography with this method.

3.2 Asymmetric cryptography Algorithm:

In this method we use a general key for cryptography and also a private key for decoding and this two keys will be coneeted with a math equation which is really hard to Decoding.

In this method if a sender wants to send a message in private to the receiver, he cryptographies it with receiver's general key and the other side receiver will Decode the message with own private key. This method is very complicated.

3.3 Combinatorial Method (Symmetric and Asymmetric):

In this Algorithm documents and Messages will send with Cryptography Algorithm and Decoding key will be send with

3.4 Hash Algorithm

This Algorithm does the cryptography in way. It means Document or Message will become a bunch of numbers, symbuls and letters.This Algorithm goes with integrity security services. And the reason is when two Documents or Messages hash together it might not make a same field (aboat less than 0.001%)

3. 5 Electronic Signature

For provide security services in trade we use something like: signature, ID card, official office but we are not be able to use these staff in a Electronic space because:

- Electronic informations were made of bytes and there is no Difference between original version and copy version.
- Any Elimination or change in an Electronic document won't any effect.
- Approval of an Electronic Document is based on documents information.

The most difference between these two method in Electronic signature and Asymmetric cryptography is sender used the own private key for signature and receiver uses a general key to approve the signature in Electronic signature.

Electronic signature algorithm

1. Hashed string document by using hash algorithm is created.
2. By using the senders public key can be applied to decode strings attached.

After receving the document the following steps are performed:

1. String hash of the document is provide by using hash algorithm.
2. By using the sender's public key can decode the string attacheel to the document acts.
3. Now recipient has two hashed strings that one of them is brought by himself and the other is brought by transmitters when signing document.
4. If these two strings be equal and identical, recipient can be ensure to the integrity of this document.

All these steps are performed by the EC software and there is no need to operation to electronic tranction, in order to made these software, there is some successful companies such as Microsoft, Info path softwar, Adobe software and live cycle.

Acording to the above description in security services there is two challenges one is authen tication and the other is non-repudiation.

1. How the recipient can ensure that the person signing the document is the one who clamis, in other words in physical world who is monitoring on the issue and create a electronic signature.
2. The sender to encrypt the document should use the public key of the recipient but what assurance is there that receive public key is same as recipient's publickey.

To solve these two challenges, countries have infrastructure called public key in frastructure.

3.6 Electronic certification (Public key infrastructure certificate)

According to the extensive of domestic and foreign exchanges and also because of the skeptics sensivity EC exchanges has made due to the confirmation of identity bothsides. There is an electronic certification center for issuance this electronic certification in countries.This center has some daty like issuance electronic certification for any natural or legal asker.This certification has applicants private and public keys also it has the exporter center proBile.This center continually monitors to all the certification as soon as having problem for the holder of the

certificate or card expires that card is placed on the list of invalid cards.

This center could be public or privet one of the most famous company for issuance electronic certification is verisign.For having this card, you must submit the required documents to these institutes also this card has some internel governance rules and international technical regulations, so by using the members features like integration, authentication and underiable documents in such a way that if transmitter signed a commercial document such as bill or order factor then send it the recipient just by looking at the sign on the electronic signatures can find the document integrity also signers identity is recognizable and it's irrdfutable but there is no any household stamp, for having this should used of symmetric orasymmetric encryption algorithm this means that sender can encrypted by the symmetric or asymmetric algorithms if the transitation to the third party.

Third person needs the recipient's private key so hershe can't see the document. Although we don't have hundred percent security but to the extent that can gain the trust of business transation's process.

3.7 Commerical websites' decurity on Internet

Electronic certification centers provide two different security services for electronic websites by issuing a warvant called that specifical for an URL. This certificate can be used for two purpose:

1. Introduction and comfirmation "between the URL on address bar and the website you see. Whereas sometimes when you want to visit a commercial websites, hackers Auto-deflect you to another pages they designed look alie the target wcbsite and use your entered information. But by Utilizing this servise the possibility of this forgery disapears.
2. Securing the connection between users' computers and servers by using this electronic certificates to encrypting the transferring dotas.

4. COMPUTATIONAL CONSIDERATIONS IN EC

1-Time Stamp;

One of the important requirements of EC process, expecially in electronic biddings, is determining the exact documents' sending times. Consideration of this discussion is because the documents' sending time is set by the sending server clock and according to widespread and universality of EC and the time difference between the countries, this will cuase an unmanageable risk in citing document's time.

If we don't predict a mechanism for this time synchronization issue there will be numerous conflicts during and after the execation of business processes. So the certification centers solve this problem by issucing thetime-stamp certificate. On this algorithms by using GPS and clock sync algorithm such as vector and lamport algorithms, logical clock replaced by physical clock.

Applying the hole mentioned services, by particular softwaves. Majority of avoilable softwares are not utilized to use signature, certificate or time – stamp on text or conent of a document. So some softwares must be used that can support this security services. This supporting softwares are called.

2-Statistic factor which should be considered in designing EC systems

As most of EC systems have been designed to work in universal levels, so in its design, we should pay attention to other technical statistics and do modeling and some research with normal mathematics. As an example, these systems data centers have been chosen in different geographical areas. The reason of its spreading is the speed of interaction, because sometimes, EC systems are in universal level, therefore, to have speed and usefulness. We should copy files in different locations.

In this way, we can be sure about its practicality in accessing systems. It should be payed attention that, finally, different versions should have desired compatibility. All the versions should be the same to do so, there are some back up algorithm, but it needs more attention. Some examples make the point clear. Suppose in A province, B is a bank customer and puts 1000 to his account.At the same time, bank needs to calculate the profit and puts into customer's account. Bank does so with respect to which interaction has been done first. Regarding the rules of bank data centers, what is important is that all interactions of A and B versions be done correctly and in order, so that, versions compatibility be catered for. There is no priority in paying the profit, while, regarding electronic trade, arrangement of actions (Paying the balance and counting the profit) is different.

3- Movable (Mobile) ES systems

Because of spreading of ECS and already moveable technologies, to simplify the EC from the used mobile systems equipment, system statistic and gained results are challenging. An example may clarify the point. Suppose we want to know the names of hotels as well as their address and price that are near to us up to 50 kilometers. In this case, if we use ECS movable systems, our answer will change with respect to the place. So it should bepayed attention.

4-Accessing secret data in ECS with mathematical analysis

We clarify the challenge whith an example. Consider, in ECS for the user, it has been defined to have access to statistics and generalities but there is no permission for each member to have such an access. With some mathematical calculating, this access will be ready Regard, in this system, we need to know the salary of the oldest clerk (secret data).

Instead of forbidden casual question, two general permittable and some how experimental questions, secret data (casual question answer) will be achieved;

Q.1- How many clerks do we have who are above X "X" will change by clerk so much so that the achieved answer be just one.
Q.2- How much is the highest salary for clerks higher than X ?
With analysis of questions 1 and 2, the salary of the oldest worker will be achieved. Infact, these points show the place of mathematical analysis in getting access to systems. It also shows the dangers of security status.

5- Injecting programming codes of SQL in ECS

By doing such an injection, codes of data layers in applicable programs under web, ECS is under access of for bidable access. These attacks don't waste the practicality of system but can read data bank of an ECS or enter new data in ECS bank. Applicable ECS web programs usually is done byhaving relation between ECS data center and receiving requests from user. In this relation, such an forbidable access will happen. Because of its importance, xlgorithms like statistic, dynamic have been designed and can be improved.

Code injection will be clarified by an example; Suppose in bank bank ECS in customers' list, there is this code; select & from customer where ID= < input – user ID >; This will show the custoners data after receiving the user real ID. In this code, if we can change the SQL code as below, code condition will be always correct and logical, It will be as a code injection attack:

Relect & from customer where ID= "<input – user ID >" or "1" = "1": with this order, without getting correctly the user ID, point shows the mathematical and logical statistics in ECS systems.

5. CONCLUSION

In this article for determining ec security,security algorithms& formal computing;we suggest to use the maximum power to creat a security policy&using these policies&well-secure tools appropriately for error-resistance security ,intrusions &attackers.we should detect the weak&strong points of new technologies and proceed to these issues with applied approaches.

With mathematical modeling we can test softwares which are necessary for ec with security parameters& study on web servers&programming languages&detect their probable problems.on the other hand,evaluate the security of hardwares&softwares involving in ec& use them in business applications and have special sensitivity in choosing the ec softwares.

REFERENCES

[1]. Turban, Efraim, Leidner, McLean, Dorothy , Ephraim , Wetherbe, James, Information Technology for Management: Transforming Organizations in the Digital Economy, Wiley, 6th Edition, 2008.

[2]. Floyd, Brian, The Information Security Writers group, The Changing Face of Network Security Threats", 2007, http://www.infosecwriters.com/text_resources/pdf/Network_Security_Threats_BFloyd.pdf

[3]. Information_security, available at: http://en.wikipedia.org/wiki/Information_security, March 2010.

[4]. Mehrnoosh Torabi, Kareshna Zamani, Mobile Banking and its security issues, 5th international Conference on e-Commerce in Developing Countries: with focus on export, September 2010.

[5]. Venter, H.S., Eloff, J.H.P., A taxonomy for information security technologies, Elsevier, p.300, 0167-4048/03, 2003.

[6]. Piotr Bilski , Wiesław Winiecki, Multi-core implementation of the symmetric cryptography algorithms in the measurement system, Measurement 43, 1050- 1051, 2010. [9] Lopeza Javier, Oppliger Rolf, Pernul Gunther, Authentication and authorization infrastructures (AAIs): a comparative survey, Computers & Security, vol. 23, p.580, 2004.

[7]. Srivastava, A., Electronic signatures and security issues: An empirical study, Computer law and security review 25, 442-445, 2009.

[8]. Description of Symmetric and Asymmetric Encryption, Revision: 1.3, October 26, 2007, http://support.microsoft.com/kb/246071

[9]. ENCRYPTION AND DECRYPTION ENCYCLOPEDI, http://www.encryptionanddecryption.com/encryption, October 2013.

[10]. Shoup, Victor, FCD 18033-2 Encryption algorithms — Part 2: Asymmetric ciphers , Instructor of New York University,Faculty of computer science ,December 6, 2004, http://www.shoup.net/iso/std6.pdf

[11]. Hardjono, Thomas, Dondeti, Lakshminath R., Security In Wireless LANS And MANS, Artech House, 2005.

[12]. Cryptographic hash function, http://en.wikipedia.org/wiki/Cryptographic_hash_function, October 2013.

[13]. Comer, D.E., Virtual Private Networks, Computer Networks and Intranets, Prentice Hall, p.191, 1999.

[14]. Preneel, Bart, A Survey of Recent Developments in Cryptographic Algorithms for Smart Cards, Computer Networks, 51(9), pp. 2223-2230, 2007.

[15]. Domingo-Ferrer, Josep, et al,Advances in Smart Cards, Computer Networks, 51(9), p.2219, 2007.

[16]. Tiwana, A., "Are Firewalls Enough?", 112-135; Securing Transactions with Digital Certificates, pp. 211-227, Web Security, digital Press, 1999.

[17]. Torrubia, Andres, Mora, Francisco J., Marti, Luis, Cryptography Regulations for E-commerce and Digital Rights Management, Computers & Security Vol.20, No.8, 730-731, 2001.

[18]. Introduction to digital certificate, available at: http://www.verisign.com.au/repository/tutorial/digital/intro1.shtml , September 2013.

About Author

Mr Rahmat Zolfaghari is presently working as faculty in Islamic AzadUniversity Hashtgerd Branch, Department of Computer Engineering, Iran He is having 14 years experience both in industry and academia, He recived his Software Engineering Bachelor (BS) of Shahid Beheshti University in Iran and Software Engineering Master (MS) of Sharif University of technology in Iran, His research interests are Database, Software Engineering and Modelling.