Optimizing security in E-Commerce Transaction: An Overview

Miss Nikita A. Rathi
Prof S. R. Gupta

Abstract:- *Now-a-days E-commerce is important because most of the business are done online. Example of E-commerce are like flipkart, amazon, olx etc. as business are done online many transaction are done online so it is important to provide security to transaction. There are three main security issues relevant to doing business online: Verifying the identity of the person through which doing business, Ensuring that messages sends and receives have not been tampered with , Obtaining evidence of the date, time and place at which a business transaction performed.*

I. Introduction

A good definition of e-commerce is conducting business online. Selling goods, in the traditional sense, is possible to do electronically because of certain software programs that run the main functions of an e-commerce Web site, including product display, online ordering, and inventory management. The software resides on a commerce server and works in conjunction with online payment systems to process payments. Since these servers and data lines make up the backbone of the Internet, in a broad sense, e-commerce means doing business over interconnected networks.

The definition of e-commerce includes business activities that are business-to-business (B2B), business-to-consumer (B2C) etc. E-commerce is a major factor in the U.S. economy because it help companies with many levels of current business transactions, as well as creating new online business opportunities that are global in nature. E-commerce is also called as "internet commerce" to mean e-commerce that specifically uses the internet as its data transmission medium. Most businesses sell a product or service to a customer to make money. However, it can be much more complicated than that simple model; some businesses serve as the middle man from manufacturer to customer; others sell to other businesses, and some organizations do not follow a financial model that generates a profit for them.

Following are the different types of business transactions:

- Retail to Customer in-person
- Retail to Customer, Not in Person
- Wholesaler to Retailer
- Business to Business
- Wholesale to Consumer
- Consumer to Consumer

There are some steps which are followed by the E-commerce transaction system to use for online exchange of fund and the goods and services first [1][2][3]:

- **Collecting information:** e.g., goods, services and price information from different sources.
- **Product discussion***:* a describe discussion takes place about product features, price, configuration, and many others.
- **Agreement:** online commitment to purchase a product or service through online shopping and the order representing and responsibility to transfer money in exchange.
- **Payment information***:* buyers provide payment information to the seller.
- **Delivery***:* seller gives the goods and services to buyer and they receive.

Security is a necessity in an E-commerce transaction. Information security has become a very critical point of modern communication system. Privacy, integrity, confidentiality etc are main security dimension to protect E-commerce transactions against imminent danger[4]These objectives are achieved by Cryptography functions and techniques. When customers and retailer perform a transaction over Internet, the protection of information against security threats is a major issue. During sending the sensitive information, the data must be protected from unauthorized access to maintain its privacy and integrity. We can increases the level of security dimensions using cryptographic techniques[5]. E-commerce provides low transaction costs and more convenient business mode to all over world customers. There are many asymmetric approaches which use in E-commerce transaction and other supported cryptography algorithms which are essential in working setup of E-commerce. Internet is full of security threats integrity violation, sabotage(to deliberately destroy something in order to prevent it from being successful), access control and infrastructure attacks.

II. Background

By definition, ecommerce is the utilization of computer tool and telecommunication network in order to buy sell products service of all kind[6][7][8]. For many Americans, ecommerce is something we participate in on a daily basis, like online bill payment or purchasing from an e-tailer.

Nowadays the thought of living without ecommerce seems unbeliveable and an inconvenience. It wasn't until only a few years ago that the idea of ecommerce had even appeared. Ecommerce was introduced 40 years ago and, to this day, continues to grow with new technologies, innovations, and thousands of businesses entering the online market each year. The convenience, safety, and user experience of ecommerce has improved exponentially since its inception in the 1970's.

Currently, Amazon offers not only books but DVDs, CDs, MP3 downloads, computer software, video games, electronics, apparel, furniture, food, and toys. A unique characteristic of Amazon's website is the user review feature that includes a rating scale to rate a product. Customer reviews are now considered the most effective social media important for driving sales. The company attracts approximately 65 million customers to its U.S. website per month and earned revenue of 34.204 billion in 2010.

In 2001, Amazon.com launched its first mobile commerce site. Another major success story of the dot com was Ebay, an online auction site that debuted in 1995. Other retailers like Zappos and Victoria Secret followed suit with online shopping sites; Zappos being a web only operation. Also in 1995, was the inception of Yahoo followed by Google in 1998, two leading search engines in the US. These successful web directories began their own ecommerce subsidiaries with Google Shopping and Yahoo! Auction, in following years. Global ecommerce company, PayPal, began its services in 1998 and currently operates in 190 markets. The company is an acquired bank that performs payment processing for online vendors, auction sites, and other commercial users. They allow their customers to send, receive and hold funds in 24 currencies worldwide. Currently, PayPal manages more than 232 million accounts, more than 100 million of them active.

As more and more people began doing business online, a need for secure communication and transactions became apparent. In 2004, the Payment Card Industry Security Standards Council (PCI) was formed to ensure businesses were meeting compliance with various security requirements. With mobile commerce gaining speed, more users are purchasing from their hand.

The market for mobile payments is expected to be increased by 2014, reaching $630 billion in value. Total sales in ecommerce have grown from $27.6 billion in 2000 to $143.4 billion in 2009 and are expected to continue its growth for the foreseeable (to predict) future.

Transaction means Most businesses sell a product or service to a customer to make money. However, it can be much more complicated than that simple model; some businesses serve as the middle man from manufacturer to customer; others sell to other businesses, and some organizations do not follow a financial model that generates a profit for them. All of these business models lead to different types of business transactions:-

- Retail to Customer in-person
- Retail to Customer, Not in Person
- Wholesaler to Retailer
- Business to Business
- Wholesale to Consumer
- Consumer to Consumer

Internet has made the idea of an idealized marketplace seem plausible(acceptable). However, there are still concerns regarding the exchange of money securely and conveniently over the internet. Pretty Good Privacy (PGP) provides a confidentiality (kept personal within certain circle) and authentication service that can be used for E-commerce. PGP is used behind SSL method to provide high security with E-commerce.

1. To be on the cutting edge of e-commerce, you need to understand how to best utilize cryptography to offer secure services for your customers over the Internet.

2. The success or failure of an e-commerce operation hinges on 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 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. Public Key Encryption creates a world in which it does not matter if the physical network is insecure. Even if - as in the case of a distributed network like the Internet, where the data passes through many hands, in the form of routers and switches and hubs - information could be captured, the encryption scheme keeps the data in a meaningless form, unless the cracker has the private key.

4. Public key encryption is much slower than shared key encryption, so products like PGP use the public/private keys to share a secret key, which is then used to encrypt the rest of the dialog. PGP provides a confidentiality and authentication service that can be used for electronic mail and file storage applications.

Without trust, most prudent business operators and clients may decide to forgot use of the Internet and come back to traditional methods of doing business. To solve this trend the issues of network security at the e-commerce and customer sites must be constantly reviewed and appropriate countermeasures solved. These security measures must be implemented so that they do not dissuade the intended e-commerce operation. A straightforward comparison could be made of the security weaknesses in the postal system vs. security weaknesses the vulnerable spots in both cases are at the endpoints – the customer's computer/network and the business' servers/network. Information flowing in the conduit (trucks/planes and wires) is relatively immune to everyday break-ins. Privacy issues are amongst the major drivers for improved network security along with the elimination of theft, fraud, tampering of data. Two major threats to customer privacy and confidence come from sources both hostile to the environment as well as sources seemingly friendly. Coordinated attacks on Yahoo, eBay, ZDNet, Buy.com and amazon.com generated a huge amount of publicity and a federal government response Another threat may originate at appearances friendly companies such as Double Click, Member Works and similar firms that collect customer information and route it to other firms. Much of this transaction information is able to be associated with a specific person making these seemingly friendly actions potential threats to consumer privacy.

In two intermediaries to occur during the execution of transactions and electronic payment, we will have two security policies in order to realize and guaranty the security of the electronic transactions. The, e-commerce transactions are realized in two processes:

- In the case of ONP (ONP: Office National des Postes; NPO: National Post Office) the security based on data cryptography and the secured connections where the merchant web site is totally implicated as all data pass through this site.
- With the SMT *(Société* Monétique de Tunisie) the merchant web site is partially present during the transactions, and the client personal data do not pass through the site.

In the first process the client makes e-commerce transactions without knowing the intermediary of trust(ONP: Office National des Postes; NPO: National Post Office) has participated; In fact the latest was present only for the transactions guaranty, check up of both:(merchant site authenticity and the client's payment card) [9].

During the second process the client is directed toward the intermediary of trust just after having validated his on line purchase order, here intermediary of trust is SMT (Société Monétique de Tunisie), it simply takes the client into custody in order to guaranty the transaction. As two intermediaries intervene during the execution of transactions and electronic payment, we will have two security policies in order to realize and guaranty the security of the electronic transactions.

In the case of ONP the security based on data cryptography and the securely connections were the merchant web site is totally implicated as all data pass through this site. With the SMT the merchant web site is partially present during the transactions, and the client personal data do not pass through the site.

E-commerce Security is a part of the Information Security framework and is specifically applied to the components that affect e-commerce that include Computer Security, Data security and other wider realms of the Information Security framework. E-commerce security has its own particular nuances and is one of the highest visible security components that affect the end user through their daily payment interaction with business. E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. Dimensions of e-commerce security- Integrity, Non-repudiation, Authenticity, Confidentiality, Privacy, Availability. 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 Endeavour due to the constant technological and business change and requires a coordinated match of algorithm and technical solutions. Security is one of the principal and continuing concerns that restrict customers and organizations engaging with ecommerce in e-commerce B2C and C2C websites from both customer and organizational .

a) Purpose Of Security-

1. Data Confidentiality – is provided by encryption decryption.
2. Authentication and Identification – ensuring that someone is who he or she claims to be is implemented with digital signatures.
3. Access Control – governs what resources a user may access on the system. Uses valid IDs and passwords.
4. Data Integrity – ensures info has not been tampered with. Is implemented by message digest or hashing.
5. Non-repudiation – not to deny a sale or purchase

b) Security Issues-

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.

Security features have four categories:

- Authentication: Verifies who you say you are. It enforces that you are the only one allowed to logon to your Internet banking account.
- Authorization: Allows only you to manipulate your resources in specific ways. This prevents you from increasing the balance of your account or deleting a bill.
- Encryption: Deals with information hiding. It ensures you cannot spy on others during Internet banking transactions.
- Auditing: Keeps a record of operations. Merchants use auditing to prove that you bought a specific merchandise.
- Integrity: prevention against unauthorized data modification

- Nonrepudiation: prevention against any one party from reneging on an agreement after the fact
- Availability: prevention against data delays or removal.

c) E-Commerce Security Tools-

- Firewalls – Software and Hardware
- Public Key infrastructure
- Encryption software
- Digital certificates
- Digital Signatures
- Biometrics – retinal scan, fingerprints, voice etc
- Passwords
- Locks and bars – network operations centers

d) Security Threats-

- Three types of security threats

1. Security (DOS): Denial of Service (DOS) Two primary types of DOS attacks: spamming and viruses

- **Spamming**

Sending unsolicited commercial emails to individuals. E-mail bombing caused by a hacker targeting one computer or network, and sending thousands of email messages to it. Surfing involves hackers placing software agents onto a third-party system and setting it off to send requests to an intended target. DDOS (distributed denial of service attacks) involves hackers placing software agents onto a number of third-party systems and setting them off to simultaneously send requests to an intended target

- **Viruses:** self-replicating computer programs designed to perform unwanted events.

✓ Worms: special viruses that spread using direct Internet connections.

✓ Trojan Horses: disguised as legitimate software and trick users into running the program

2. Security (unauthorized access)

✓ Illegal access to systems, applications or data. Passive unauthorized access listening to communications channel for finding secrets. it May use content for damaging purposes. Active unauthorized access. Modifying system or data. Message stream modification. Changes intent of messages, e.g., to abort or delay a negotiation on a contract. Masquerading or spoofing –sending a message that appears to be from someone else.

Impersonating another user at the name ‖ (changing the ―From ‖ field) or IP levels (changing the source and/or destination IP address of packets in the network)Sniffers–software that illegally access data traversing across the network.

3. Software and operating systems‘ security holes Security (theft and fraud):

Data theft already discussed under the unauthorized access section. Fraud occurs when the stolen data is used or modified. Theft of software via illegal copying from company‘s servers. Theft of hardware, specifically laptops.

If you are new to the Internet or a regular shopper online, the following guidelines should apply.

1. Make sure you know the buying rate; if you are not sure of the current rates, find out before you buy an item.
2. Find out the cost of delivery before placing your order and how long the delivery will take. Most shopping sites use couriers to deliver the goods and when delivering overseas can become costlier.
3. If you are purchasing on E-bay check out the buyers and sellers feedback. This should become standard before you ever place a order.
4. Always read the frequently asked questions section if you are new to the site.
5. If someone demands cash for a payment, say no. Use your credit card to make your payment; this will protect you against fraud. Credit card companies refund accounts where fraudulent activity transpires.
6. Check the buyers contact page. Make sure their postal address is posted on it. If not, don‘t deal with them.
7. Don‘t be afraid to ask the seller lots of questions, genuine sellers should be very helpful, some online shopping sites have forms where you can see customer feed back.
8. Check, and read in full the terms and conditions, and the privacy policy of the site.
9. If you are unsure about a site, try doing a search with Google or any of the other search engines. You may find comments posted about the shopping site from other customers.
10. If you are still not sure after reading the above it may be time to go shopping elsewhere.

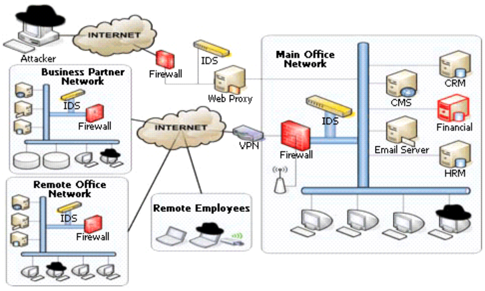
These simple guidelines should also apply when purchasing online. E-commerce is widely considered the buying and selling of products over the internet, but any transaction that is completed solely through electronic measures can be considered e-commerce. Day by day E-commerce and M-commerce playing very good role in online retail marketing and peoples using this technology day by day increasing all over the world. E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction.

III. Working of Optimizing security through cryptography algorithm

As many cycles are required for security we will be using some other algorithm that will optimize the security levels. For this we are going to use RC6 algorithm. RC6 algorithm is to optimize security levels and provide more secure transcation. In cryptography, RC6 is a symmetric key block cipher derived from RC5. RC6 was designed by Ron Rivest, Matt Robshaw, Ray Sidney, and Yiqun Lisa

Yin to meet the requirements of the Advanced Encryption Standard (AES) competition. The algorithm was one of the five finalists, and also was submitted to the NESSIE and CRYPTREC projects. It is a privately owned algorithm by RSA Security.

In this, the Business Partner Network, Remote Office Network and Main Office Network communicate with each other in order to make the e-commerce transactions. While the user's and testers can access these networks with the help of communication protocols, this access is restricted. Any outsider or attacker, always goes through multiple checks, like firewall filtering, Web Proxy and more in order to access the network. Our algorithm will reside on the Firewall, which would provide high security to our system, and encrypt/decrypt any transactions which are going to and from the network.



IV. Conclusion

In thi paper we implemented new idea of optimizing security and providing more greater security. Online shopping is done and transcation is done. To provide security to transaction we are optimizing the levels to travel that transcation in that security levels.

The benefit of proposed model is that to make secure e-commerece transcation between retailer and customer without using unnecessary security levels. We are providing security high by using only one security card that will make our transcation secure without tampering of data.

As we have focused into optimizing security concern we dont use many verification thus process take less time executing the e-commerce transcation. In future we will implement more faster algorithm to optimize security in e-commerce transcation.

References

[1] Thulasimani Lakshmanan and Madheswaran Muthusamy, “A Novel Secure Hash Algorithm for Public Key Digital Signature Schemes” The International Arab Journal of Information Technology, Vol. 9, No. 3,2012.

[2] Dr. Nada M. A. Al-Slamy, “E-commerce security” IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.5, 2008.

[3] Rhavani Chris Clifton, “Directions for Web and E-commerce Applications Security” IEEE, ISSN 0-7695-1269-0101 1- 2001, 2001

[4] Yu Xin, Xia Ming Ping &Bai Yu, “Research on the Security Model for E-business Process Management,” Published in IEEE computer society 2008, pp.369-371.

[5] Rivest, Ronald L. (1990). "Cryptology". In J. Van Leeuwen. *Handbook of Theoretical Computer Science* 1. Elsevier.

[6] Kaplan Danielo, guide du commerce eletcronique, SERVEDIT,2000

[7] Reboul P,Le guide du commerce electronique, business group.Publi-U-Edition,1999

[8] Reboul P, D. Xardel, commerce electronique edition eyrolles,1999

[9] Rapport annuel de L'Officer national des postes tunis 2004