E-Commerce security – A life cycle Approach

Kirti Saxena

(Research Scholar Faculty of Computer Science, Pacific Academy Of Higher Education & Research University Udaipur (Raj.))

Abstract- It is commonly believed that robust security improves trust and this will ultimately increase the use of Electronic Commerce (E-Commerce) (Kim, C., et al., 2009). . Lowering of the cost of operation, increase in the speed of transactions, and easy global reach to customers and vendors have been the reasons for the overwhelming popularity of this new way of commerce. This paper examines E-Commerce security of the assets and transactions in the e-commerce components and activities. The technology used in e-commerce, the paper goes on to identify the security requirement of ecommerce systems from perceived threats and vulnerabilities. Then e-commerce security is viewed as an engineering management problem and a life cycle approach is put forward. How the e-commerce systems can be made secure using the life cycle approach is outlined. The relevant standards and laws are also discussed in the perspective of e-commerce. Various privacy concerns and arguments against and for these privacy issues are discussed.

Keywords: E-Commerce, e-Commerce security; threats and vulnerabilities; security engineering life cycle; security standards; IT act

I. INTRODUCTION

Electronic commerce is buying and selling of goods and services across the internet. Commercial activities over the internet have been growing in an exponential manner over the last few years. However, e-commerce has a much broader scope and encompasses many more business activities other than just web shopping. When it comes to payment, one needs to establish a sense of security. Customers must be able to select a mode of payment and the software must verify their ability to pay. This can involve credit cards, electronic cash, encryption, and/or purchase orders. The more of these techniques are supported by an E-commerce package, the more secure the system can be, and therefore the more customers are benefits from E-commerce abilities [1][2].
Although the web has made online shopping possible for many businesses and individuals, in a broader sense, e-commerce has existed for many years. For decades, banks have been using electronic funds transfers (EFTs) [3], which are electronic transmissions of account exchange information over private communications networks.
Some of the definations of e-commerce often heard and found in publications and the media are:
Electronic Commerce (EC) is where business transactions take place via telecommunications networks, especially the Internet.[4]
Electronic commerce describes the buying and selling of products, services, and information via computer networks including the Internet.[5]
Electronic commerce is about doing business electronically.[6]
E-commerce, ecommerce, or electronic commerce is defined as the conduct of a financial transaction by electronic means.[7]
E- Commerce business has 4 different consists of components to build business to consumer, All of these elements combined give the store a personality & the end uses a true shopping experience [2].
1- Product Catalog.
2- Shopping Cart.
3- Transaction Security.
4- Order Processing.
IBM has defined electronic business to be "the transformation of key business processes through the use of Internet technologies". A good definition of e-commerce would mention the use of electronic data transmission to implement or enhance any business process. Some people use the term "internet commerce" to mean e-commerce that specifically uses the internet or the web as its data transmission medium.

II. ADVANTAGES OF ECOMMERCE

1) 1. Lower Costs

One of the most tangible positives of ecommerce is the lowered cost. A part of these lowered costs could be passed on to customers in the form of discounted prices. Here are some of the ways that costs can be reduced with ecommerce:

- **Advertising and Marketing-** Organic search engine traffic, pay-per-click, and social media traffic are some of the advertising channels that can be cost-effective.
- **Personnel-** The automation of checkout, billing, payments, inventory management, and other operational processes, lowers the number of employees required to run an ecommerce setup.
- **Real Estate-** This one is a no-brainer. An ecommerce merchant does not need a prominent physical location.

2) 2. Overcome Geographical Limitations

If you have a physical store, you are limited by the geographical area that you can service. With an ecommerce website, the whole world is your playground. Additionally, the advent of m-commerce, i.e., ecommerce on mobile devices, has dissolved every remaining limitation of geography.

3. Better Customer Service

E–commerce means better and quicker customer service. Online customer service makes customers happier. Instead of calling your company on the phone, the web merchant gives customers direct to their personal account online. This saves time and money. For companies that do business with other companies, adding customer service online is a competitive advantage. The overnight package delivery service, where tracking numbers allow customers to check the whereabouts of a package online, is one good example.

3) 4. Enable Deals, Bargains, Coupons, and Group Buying

Though there are physical equivalents to deals, bargains, coupons, and group buying, online shopping makes it much more convenient. For instance if a customer has a deep discount coupon for turkey at one physical store and toilet paper at another, she may find it infeasible to avail of both discounts. But the customer could do that online with a few mouse-clicks.

4) 5. Provide Abundant Information

There are limitations to the amount of information that can be displayed in a physical store. It is difficult to equip employees to respond to customers who require information across product lines. Ecommerce websites can make additional information easily available to customers. Most of this information is provided by vendors, and does not cost anything to create or maintain.

III. DISADVANTAGES OF ECOMMERCE

1. Ecommerce Lacks That Personal Touch

II. Not that all physical retailers have a personal approach, but I do know of several retailers who value human relationship. As a result, shopping at those retail outlets is reassuring and refreshing. Clicking on "Buy Now," and piling up products in virtual shopping carts, is just not the same for me.
Different people sing to different tunes. For me, the demise of the personal touch in online transactions is the biggest disadvantage of ecommerce.

2. Ecommerce Delays Goods

Unless you are using a website to merely order a pizza online, ecommerce websites deliver take a lot longer to get the goods into your hands. Even with express shipping, the earliest you get goods is "tomorrow."
But if you want to buy a pen because you need to write something right now, you cannot buy it off an ecommerce website. Likewise with candy that you want to eat now, a book that you want to read tonight, a birth day gift that you need this evening... You get the idea.
An exception to this rule is in the case of digital goods, e.g. an e book or a music file. In this case, ecommerce might actually be faster than purchasing goods from a physical store.

3. Many Goods Cannot Be Purchased Online

Despite its many conveniences, there are goods that you cannot buy online. Most of these would be in the categories of "perishable" or "odd-sized." Think about it, you cannot order a Popsicle (also referred to as an ice pop or ice lolly) or a dining table set.
Well, you could order both of them online, but consider the inconvenience. The Popsicle would have to be transported in refrigerated trucks. Unless the seller was willing to make a huge loss, the cost of shipping that Popsicle would far exceed the cost of the Popsicle.
Likewise, a dining table set can certainly be purchased online. In some cases, the cost of logistics is bearable. But if you have to return the furniture, you will get well-acquainted with the inconvenience of ecommerce.

4. Ecommerce Does Not Allow You to Experience the Product before Purchase

You cannot touch the fabric of the garment you want to buy. You cannot check how the shoe feels on your feet. You cannot "test" the perfume that you want to buy. You get the idea.

In many cases, customers want to experience the product before purchase. Ecommerce does not allow that. If you buy a music system, you cannot play it online to check if it sounds right? If you are purchasing a home-theatre system, you would much rather sit in the "experience center" that several retail stores set up.

5. Security

When making an online purchase, you have to provide at least your credit card information and mailing address. In many cases, ecommerce websites are able to harvest other information about your online behavior and preferences. This could lead to credit card fraud, or worse, identity theft.

Conclusion

While we might be gung-ho about ecommerce, we must acknowledge that there are disadvantages too. Only when we accept our shortcomings will we work towards overcoming them.

IV. E-COMMERCE TECHNOLOGY

The unique features of e-commerce technology include:

- Ubiquity: It is available just about everywhere and at all times.
- Global Reach: the potential market size is roughly equal to the size of the online population of the world.
- Universal standards: The technical standards of the Internet, and therefore of conducting e-commerce, are shared by all of the nations in the world.
- Richness: Information that is complex and content rich can be delivered without sacrificing reach.
- Interactivity: E-commerce technologies allow two-way communication between the merchant and the consumer.
- Information density: The total amount and quality of information available to all market participants is vastly increased and is cheaper to deliver.
- Personalization/Customization: E-commerce technologies enable merchants to target their marketing messages to a person's name, interests, and past purchases. They allow a merchant to change the product or service to suit the purchasing behavior and preferences of a consumer.
- Social technology: User content generation and social networking technologies

V. SECURITY AND E-COMMERCE

Security has become one of the most important issues that must be resolved first to ensure success of electronic commerce (e-commerce). The low cost and wide availability of the Internet for businesses and customers has sparked a revolution in e-commerce and an e-commerce application may address one or several phases of a typical business transaction, and there exist various possibilities to model these phases.

For example, a possibility is to distinguish five phases of a business transaction [8]. First, the merchant makes an offer for specific (information) goods or services. Secondly, according to this offer, the customer may submit the request online. Thirdly, the customer makes a payment and the merchant delivers the goods or services to the customer. The handling of the payment may involve many ways, such as online banking, post office, cash on delivery (C.O.D) and so on [9]. Many organizations are exploiting the opportunities offered by e-commerce, and many more are expected to follow. Exemplary applications include online shopping, online banking and distance education, online game and virtual casinos, as well as Pay-TV and video-on demand services. Many businesses and customers are still cautious about participating in ecommerce, and security concerns are often cited as being the single most important barrier. This loss of trust on exchange online is being fuelled by continued stories of hacker attacks on e-commerce sites and consumer data privacy abuse [10].

VI. EXISTING E-COMMERCE SECURITY TECHNOLOGIES-

The successful functioning of E-commerce security depends on a complex interrelationship between several applications development platforms, database management systems, systems software and network infrastructure [11]. By doing online business, it is a facility of reaching to everyone. Exploring the opportunities challenges conventional notions of business competition through electronic flows of information and money [14]. Payment on Internet or network is a critical important chain of whole e-commerce, which contains the payment activity [12]. Security protection starts with the preservation of the confidentiality, integrity and availability of data and computer resources [13]. Including the elements of the Confidentiality, Integrity and Authentication Triad, the six security needs in E-commerce are:

i. Access Control.
ii. Privacy/Confidentiality.
iii. Authentication.
iv. Non Repudiation.

v. Integrity.
vi. Availability.

Access control ensures only those that legitimately require access to resources are given access [11].

Confidentiality is concerned with warranting that data is only revealed to parties who have a legitimate need, while privacy ensures that customers' personal data collected from their electronic transactions are protected from indecent and/or unauthorized disclosure [14]. Issues related to privacy can be considered as a subset of issues related to access control.

Authentication provides for a sender and a receiver of information to validate each other as the appropriate entity. This means having the capability to determine who sent the message and from where and which machine.

Non-repudiation is a property of the transaction that positively confirms that a particular client did indeed request the transaction in question without having the ability to deny making the request [12].

Integrity ensures that if the context of a message is altered, the receiver can detect it. It is possible that as a file, electronic mail, or data is transmitted from one location to another, its integrity may be compromised.

Availability as defined in an information security context ensures that access data or computing resources needed by the appropriate personnel are both reliable and available in a timely manner.

VII. IMPLEMENTING SECURITY FOR E-COMMERCE (LIFECYCLE APPROACH)

Let us now look at the fundamental strategic requirements an organization needs to consider if it wants to ensure that an e-commerce or online security project will be a success. Technology components of good online security, such as encrypted email, secure SSL websites, and intranets/extranets all have a role to play in protecting valuable data, but for security to be effective it must be designed as a whole and applied consistently across an organization and its IT infrastructure.

There is a subtle difference in the design of a software system and that of a security system.

While designing software, the functional correctness of applications is the prime concern.

In fact, in software systems, the designer aims at ensuring that for reasonable input, the user gets reasonable output. This can be traced from the system specification. But in the case of security systems, the designer has to ensure that the system properties are preserved in the face of attack. Thus the system outputs should not be completely disastrous for unreasonable inputs. In security systems, there definitely can be active interference from the adversary and the system should be hardened to withstand that. Moreover, in security systems, more functionality implies more complex system and more security holes in the system.

The steps to design security of a system is to model the system, identify the security properties to be preserved, model the adversary, and then ensure that the security properties are preserved under attacks. Details modelling of the system and identification of the required security properties are possible. But it almost impossible to accurately model the adversaries and vulnerabilities of the system exploited by those adveransaries. The result is that there nothing called "absolute security". Thus to the designer, system security means: *under given assumptions about the system, no attack of a given form will destroy specified properties*.

Thus system security in general and e-commerce security in particular is conceived of a *process* rather than a one-time developed *product*.

VIII. SECURITY ENGINEERING LIFE CYCLE

It is important to note that the e-commerce security need of an enterprise is dynamic rather than static and depends on the operational dynamics, shift or addition to business goals, technological advancement etc. Thereby, the process of designing and deploying an information security infrastructure is a continuous process of analysis, design, monitoring, and adaptation to changing needs. Often, the change in needs is frequent in the organizations. In order to be survivable under such frequent changes, the process has to be developed from a life-cycle approach. This observation leads to the concept of "security engineering life-cycle"[15]. The security engineering life cycle consists of the following phases (figure 1):

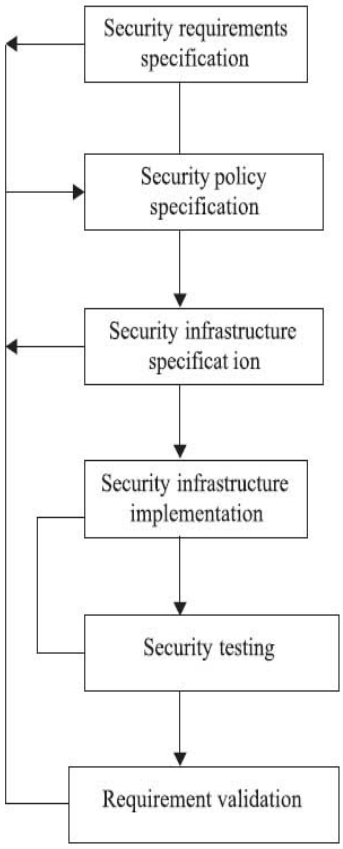

Figure 1. Security engineering life cycle.

Security requirement specification and risk analysis:

This is the first phase in the security engineering life cycle. It collects information regarding assets of the organization that need to be protected, threat perception on those assets, associated access control policies, existing operational infrastructure, connectivity aspects, services required to access the asset and the access control mechanism for the services.

Security policy specification:

This phase uses "security requirement specification" and "risk analysis report" as input and generates a set of e-commerce security policies. The policy statements are high-level rule-based and generic in nature, and, thereby, does not provide any insight to system implementation or equipment configuration.

Security infrastructure specification:

This phase analyses the "security requirement specification" and the "security policy specification" to generate a list of security tools that are needed to protect the assets. It also provides views on the location and purpose of the security tools.

Security infrastructure implementation:

The organization, in this phase, procures, deploys, and configures the selected security infrastructure at the system level.

Security testing:

In this phase, several tests are carried out to test the effectiveness of the security infrastructure, functionality of the access control mechanism, specified operational context, existence of known vulnerabilities in the infrastructure etc.

Requirement validation:

This phase analyses the extent of fulfillment of the security requirements of the e-commerce organization by the corresponding security policy and the implemented security infrastructure. Change in the business goal, operational environment, and technological advancement may lead to a fresh set of security requirements and thereby, triggering a new cycle of the "security engineering life cycle".

Now, let us see the Security Requirements, Security Policy, Security Infrastructure, and Security Testing phases in greater detail.

Security requirements:

During this phase, the security needs of an enterprise are identified. These needs are governed by the necessity to protect the following security attributes:

Authentication:

This is the ability to say that an electronic communication (whether via email or web) does genuinely come from who it purports to. Without face-to-face contact, passing oneself off as someone else is not difficult on the internet. Forging the "From:" field in an email header is a trivial matter, and far more sophisticated attacks are standard fare for hackers.

In online commerce the best defence against being misled by an imposter is provided by unforgeable digital certificates from a trusted authority (such as VeriSign). Although anyone can generate digital certificates for themselves, a trusted authority demands real-world proof of identity and checks its validity before issuing a digital certificate. Only certificates from trusted authorities will be automatically recognized and trusted by the major web browser and email client software.

Authentication can be provided in some situations by physical tokens (such as a drivers license), by a piece of information known only to the person involved (eg. a PIN), or by a physical property of a person (fingerprints or retina scans). Strong authentication requires at least two or more of these. A digital certificate provides strong authentication as it is a unique token (the certificate itself) and requires a password (something known only to the owner) for its usage.

Privacy:

In online commerce, privacy is the ability to ensure that information is accessed and changed only by authorized parties. Typically this is achieved via encryption.

Sensitive data (such as credit card details, health records, sales figures etc.) are encrypted before being transmitted across the open internet – via email or the web. Data which has been protected with strong 128-bit encryption may be intercepted by hackers, but cannot be decrypted by them within a short time. Again, digital certificates are used here to encrypt email or establish a secure HTTPS connection with a web-server. For extra security, data can also be stored long-term in an encrypted format.

Authorization:

Authorization allows a person or computer system to determine if someone has the authority to request or approve an action or information. In the physical world, authentication is usually achieved by forms requiring signatures, or locks where only authorized individuals hold the keys.

Authorization is tied with *authentication*. If a system can securely verify that a request for information (such as a web page) or a service (such as a purchase requisition) has come from a known individual, the system can then check against its internal rules to see if that person has sufficient authority for the request to proceed.

In the online world, authorization can be achieved by a manager sending a digitally signed email (an email stamped by their personal digital certificate). Such an email, once checked and verified by the recipient, is a legally binding request for a service. Similarly, if a web-server has a restricted access area, the server can request a digital certificate from the user's browser to identify the user and then determine if they should be given access to the information according to the server's permission rules.

Integrity:

Integrity of information means ensuring that a communication received has not been altered or tampered with. Traditionally, this problem has been dealt with by having tight control over access to paper documents and requiring authorized officers to initial all changes made – a system with obvious drawbacks and limitations. If someone is receiving sensitive information online, he not only wants to ensure that it is coming from who he expects it to (authentication), but also that it hasn't been intercepted by a hacker while in transit and its contents altered. The speed and distances involved in online communications requires a very different approach to this problem from traditional methods.

One solution is afforded by using digital certificates to digitally "sign" messages. A travelling employee can send production orders with integrity to the central office by using their digital certificate to sign their email. The signature includes a hash of the original message – a brief numerical representation of the message content. When the recipient opens the message, his email software will automatically create a new hash of the message and compare it against the one included in the digital signature. If even a single character has been altered in the message, the two hashes will differ and the software will alert the recipient that the email has been tampered with during transit.

Non-repudiation:

Non-repudiation is the ability to guarantee that once someone has requested a service or approved an action, they cannot turn around and say "I didn't do that!".
Non-repudiation allows one to legally prove that a person has sent a specific email or made a purchase approval from a website. Traditionally non-repudiation has been achieved by having parties sign contracts and then have the contracts notarized by trusted third parties. Sending documents involved the use of registered mail, and postmarks and signatures to date-stamp and record the process of transmission and acceptance. In the realm of e-commerce, nonrepudiation is achieved by using digital signatures. Digital signatures which have been issued by a trusted authority (such as VeriSign) cannot be forged and their validity can be checked with any major email or web browser software. A digital signature is only installed in the personal computer of its owner, who is usually required to provide a password to make use of the digital signature to encrypt or digitally sign their communications. If a company receives a purchase order via email which has been digitally signed, it has the same legal assurances as on receipt of a physical signed contract.

Security policy:

The first step in securing an e-commerce venture is to formulate written security policies (website 1) which clearly define the requirements for each component of the system (human, technological, legal) and how they interact. An organization's security policy defines its position on the protection of its physical and IT assets. It identifies the physical and intellectual property assets that are most valuable for the continued success of the company, and specifies how they should be protected.
The security policy may cover issues like:

- What service types (e.g., web, FTP, SMTP) users may have access to
- What classes of information exist within the organization and which should be encrypted before being transmitted
- What client data does the organization hold. How sensitive is it? How is it to be protected?
- What class of employees may have remote access to the corporate network
- Roles and responsibilities of managers and employees in implementing the security policy
- How security breaches are to be responded to the security policy should also consider physical aspects of network security. For example,
- Who has access to the corporate server?
- Is it in a locked environment or kept in an open office?
- What is the procedure for determining who should be given access?

The security policy regulates the activities of employees just as much as it defines how IT infrastructure will be configured. The policy should include details on how it is to be enforced and how individual responsibilities are determined.
For it to be effective, the policy needs regular testing and review to judge the security measures. The review process needs to take into account any changes in technology or business practices which may have an influence upon security. Lastly, the policy itself needs to be regarded as a living document which will be updated at set intervals to reflect the evolving ways in which the business, customers and technology interact.

Security infrastructure-

The security infrastructure (website 1) is the implementation of the security policy. The security infrastructure is the technology which is chosen to secure the e-business and the rules by which it operates. Some examples of this include:

- enforcing password aging and expiration
- enforcing the complexity of passwords
- blocking prohibited outbound connections from the firewall
- requiring digital certificates to authenticate remote access connections to an organization's network
- requiring badges for physical access to building
- requiring all physical access to servers to be recorded in a written log Again, the security infrastructure entails managing the behavior of both IT and human resources. It should be regularly policed:
- Who checks written logs?
- How often are firewall reports checked? Finally, it must be enforced. The penalties for breaches of the security policy must be made clear to all employees and partners and must be enforced if policy requirements are broken or ignored.

Testing e-commerce security-

The need for security testing of an organization arises due to two main factors. The primary factor is the importance of measuring the extent to which the security infrastructure implements the security policy and the security requirements of an organization. As the implementation of the security infrastructure needs human interventions, a proper security testing is needed to check out the existence of any "human error". The other

factor is the vulnerability of the existing security infrastructure to the new threats and exploits. In recent years, the rate of arrival of new types of threat and new exploits has been alarming with respect to the information security context. This leads to the need for periodical security testing by which the vulnerability of the existing security infrastructure to the growing number of threats and exploits can be measured.
The main objective of security testing, therefore, includes

- Verification of the security requirement specification such as location of the asset(s), access control mechanism for the assets, operational context of the organization, existing system services and their access control mechanisms, and the connectivity within the organization and connectivity of the organization to the outside world
- Verification of the configuration of the security tools specified in the security infrastructure i.e. whether the security tools are properly installed and configured to maintain the security of the asset
- Verification of any gap between the proposed security infrastructure and the implemented security infrastructure
- Verification of the limitation of the proposed security infrastructure with respect to the known vulnerabilities

Thus, there are two aspects of testing – compliance checking and penetration testing.

Compliance checking:

In compliance checking, it is seen whether the security infrastructure, that has been implemented, matches the security policy of the organization. A semi automated tool can be used to match the policies with the existing infrastructure.

Penetration testing:

In penetration testing, it is seen whether the existing security infrastructure of the organization is sufficient to ward off all possible security threats. Various automated and semi-automated security tools like Retina, Ness us etc. are available for penetration testing. They try and penetrate the organization's network and generate a report on the vulnerabilities and threats that are present in the network.
The feedback from the testing phase is used to upgrade the security infrastructure and security policy of the organization. After that, the testing is carried out again. Thus, security engineering is an iterative and dynamic process where all the phases need to be carried out at regular intervals to ensure the security of an organization.

IX. CONCLUSIONS

Electronic commerce is growing rapidly. A number of technologies have converged to facilitate the proliferation of e-commerce. The rapid advances in computer technology coupled with rapid acceleration in communication networks and the development of sophisticated software have revolutionized the way business is done. However, this is not sufficient to proliferate e-commerce applications. Proper management of enterprise information security resources is the need of the hour. We have, in this paper, put forth a "security engineering life cycle" approach to manage the information resources of an enterprise so that e-business can be carried out securely. With proper understanding of business needs and management of enterprise information security resources, e-commerce will mature profusely and will immensely benefit every individual.

REFERENCES

[1] David J. Olkowski, Jr., "Information Security Issues in E-Commerce", SANS GIAC Security Essentials , March 26,2001.

[2] Paul A. Greenberg, "In E-Commerce We Trust … Not ", Ecommerce Time, February 2, 2001, URL: http:// WWW. E cmmerce times. com/perl/story/?id=7194.

[3] Schneider G P, Perry J T 2001 *Electronic commerce*. Course Technology, Cambridge, MA

[4] E. Turban, J. Lee, D. King and H.M. Chung, Electronic Commerce: A Managerial Perspective. Prentice Hall, 1999.

[5] www.whatis.com/ecommerce (accessed September 2000).

[6] P. Timmers, Electronic Commerce – Strategies and Models for Business-to-Business Trading. John Wiley & Sons, 2000.

[7] http://www.straight-on.com/ecommerce_definition.htm (accessed September 2000).

[8] Yuan sen. *Introduction of E-Bunsiness Security Technology*. Software Publication, BeiJing. 2009.

[9] Peng Xinying. Research on e-bunsiness security. *Gansu Science and technology*, 2009, **25(**2): 43-45.

[10] Feilong PENG. A trust model for e-commerce based on XKMS. *Computer Applications and Software*, 2008, **25**(1):140-142.

[11] S. R. S. KESH, AND S. NERUR, "A Framework for Analyzing E-Commerce Security," *Information Management and Computer Security*, vol. 10, no. 4, no. pp. 149-158.

[12] X.Sahi and P.C. Wright, " E-Commercializing Business Operations" Communication of ACM, Feburary,2003 vol.46. no. 2 page 83-87.

[13] C. BARNES, "Hack Proofing Your Wireless Networks," Syngress Publishing, Rockland, 2002.

[14] P. RATNASINGHAM, "Trust in Web-Based Electronic Commerce Security," *Information Management and Computer Security*, vol. 6, no. 4, no. pp. 162-166, 1998.

[15] Mazumdar C, BarikMS, Das S, Roy J, BarkatMA2003 Final technical report for project development of validated security processes and methodologies for web-based enterprises