Security in Electronic Business

Dr. Abdullah Saad AL-Malaise AL-Ghamdi[1]

[1] **Department of Information Systems**
Faculty of Computing and Information Technology
King Abdulaziz University, Jeddah-21589, PO Box – 80221
Kingdom of Saudi Arabia

Abstract

A crucial area of electronic transactions is the domain of electronic commerce. Yet, a large number of people do not want to transact online as they are not sure of the level of security that the transaction would be provided by the site and the technology used by the sites. According to surveys, one of the factors affecting the spread of ecommerce is the (lack of) security measures that assure both businesses and their customers that the business relationship and transactions will be carried out in secure manner. This paper describes the security requirements for electronic Business application and attempts to discuss the method and ways to be used to meet them.

Keywords: *e-commerce, e-business security, security issues, security technologies.*

1. Introduction

The purpose of the Internet was to transfer information between computers, to enable easy remote access to systems, and its use for commercial purposes has grown immensely since the advent of the Web. Transfer of information through electronic means, availability of the internet and other advantages of technology are altering our economy, and our business methodologies. These technologies have a great impact on almost every part of the business and social life. Business are continuously transacting amongst themselves and even the customers; people regularly take the help of internet to identify vendors, and to assess their product or service, to even compare prices, and to take the advantage of the market. But, e-commerce is a lot more than only purchasing and distributing good through the internet or electronic means: It means interaction within the company/business and/or outside network through the means of network and telecommunication technology. It would also include a commercial transaction done over any computer-supported link that has the ability to transfers itself or can help transfer of "value" for items and/or service offered this may include rights of property and ownership, or the rights to utilize the items and/or service.

The domain of e-commerce is considered to be a vital side of digital business. The rate at which e-commerce is currently growing is a good example of the fact that the full potential that this technology can offer is yet to be reached. During the early 2000 and the last part of the 1990's there was a lot of speculation about what shape e-commerce would take and how it would develop in future. It was predicted, "a volume of US$ 184 billion of online retail sales in 2004 in United States alone" Forrester Research of 1999 [1] whereas the value of approx. US$ 69 billion, actual sales [2], represent huge gap. At first glance, it appeared we have tremendous opportunity for global commerce: a global communication backbone that is very conducive for low cost information exchange and a global economy that is trending to become highly information-base. However, one crucial cause of the difference between the two values has been proposed by the researchers' fraternity and supported by the results of a number of studies is the scarcity of Confidentiality, Reliability and Security in electronic transactions. A substantial portion of people who are involved in business do not want to transact online as they are not sure of the level of security that the transaction would be provided by the site and the technology used by the sites.

The figures above refer to B2C interactions only, so it was projected that the condition of B2B, and between business & government, interactions is better, which is true. However the is still not what can be called as being optimal. In today's world and economy, B2B transactions are making the biggest impact on the e-commerce industry. In industries, like automobile and mining, electronic business has at present made a major impact on the relationship between the vendor and the manufacturer. The reason for this fact is that communication between parties is carried out through dedicated line i.e. secure and private virtual networks. This promotes the development of trust, because these relations are long lasting and are also based on physical business from the outside world. However, for even the above mentioned industries the complete potential of ecommerce cannot be said to have been reached.

Thus for e-commerce to achieve its complete potential, either the involved companies need to increase the confidence level, and the confidentiality provided to their customers or the technology needs up gradation, so as to have strong features for protecting the privacy and security of the e-commerce transaction.

As the topic goes beyond one single function or arena of electronic commerce, we are required to have a global perspective of things. We are going to discuss the key factors and areas related to Confidentiality, Reliability and security of ecommerce transactions, in this paper. We will begin discussing the Issues related to Trust and confidentiality, then we will discuss the broad meaning of Confidentiality and technologies used for enforcing privacy. In the end we will complete by discussing the major factors related to providing security for electronic business and to its underlying infrastructures.

2. Confidentiality

Privacy and confidentiality is a vast topic. Maintaining of privacy is being discussed in many spheres like politics, society, law and in the recent times computer science. The electronic business arena links Confidentiality to using the information of the customer. Business Transactions usually include exchange of great amount data related to customers and businesses, which may be necessitated by electronic transaction itself (e.g. information related to credit card, bank accounts, and delivery location of personal address etc.) or it may be a requirement of the Business involved in the transaction. Customers practically have no idea about the uses that their information can be applied to, and so have little knowledge of the violation of privacy that might be happening. In the context of e-Business, we may define Privacy as the right of an individual to control, the collection of information about him during the e-commerce transaction; and to be informed the initiation of any process where his personal data would be gathered; and the right to choose details of sharing their personal information with others.

Initially the two point of views, of promoting the interest of the business and thus making world economy much stronger, or the one supportive of the views of the individual seems distinct. Yet, we presented with a need to achieve a consensus between the two, thus enabling us to find a solution which is beneficial to both the business and the individual. Such a consensus has been named *consumer-centric privacy*: under which individuals tends to attain the most possible confidentiality while business earns economic benefit by providing increased privacy to its customers. Economic benefit is derived out of improved public image of the business (means more and loyal customers) or improved brand recognition, which would naturally lead to an increased amount of e-commerce transactions by individuals who are now more comfortable in transacting online.

2.1 Concerns of the Consumer

In today's world both the Consumer and the vendor are transact across the globe with almost anyone willing to do business. Earlier, the situation was completely different where acquiring of a good or service was the result of individual's contact directly with the vendor who was located in the same locality, area or country. However, the current scenario presents us with certain aspect of these transactions that give rise to most of concern related to privacy and confidentiality. There is not direct contact between the consumer and the vendor, and no interaction between them, there is a gap between the buying, delivering and paying processes, from the timing perspective; during the business transaction information about the consumer can be collected effortlessly and very quietly without incurring too much cost as well, and effective regulation are either not present or are not enforced ineffectively; all above mentioned points contribute to these concerns. The latter is particularly true if transactions occur across borders and different set of laws are applicable. Several of the concerns of the consumer about privacy are discussed in ([3] - [6]). Following are certain examples that are noteworthy:

Cookies: Cookies are alternatively used for storing the behavior of the customer on his own computer which can be later matched with database of the customers and used for tracking him, once identified to have a certain repetitive behavior the customer might be forced to pay higher prices as his buying habits are being tracked by the vendors, and it is likely that the customer will even purchase at a high cost based on his profiles.

Site spoofing: Customers are being diverted to other sites where incorrect information is provided to them and based on this information their purchase decisions are affected. Or they are being lead to specific web-sites where the privacy policy of the web site where they came from does not apply, and they are unaware of this fact.

E-mailing: Spam mails being sent to consumers offering services and/or products.

Data gathering: Unauthorized use of the customer's personal data for purposes of data quarrying or marketing, or even selling.

Lack of regulations: Different Privacy laws in different countries and no effective means to enforce implementation.

Privacy statements: The declared Privacy statements on the websites are not updated, not correct or in some cases they are left un-applied completely.

2.2 How to Preserve Privacy

Privacy can be achieved through various means like legislative steps, organizational steps, or technological means. A combination of different techniques may also work.

Legislative Steps

Consumers have established legislations in many countries to protect privacy. Following are some examples of legislations in different countries.

In Japan the governmental and commercial usage of an individual's information is regulated by the Act of 2003 called "Personal Data Protection" which is an enhancement of a previous act laid out in 1998 which regulated the use and storage of an individual's information by government & the administration. China also has several laws relevant to protection of Data.

The Personal Information and Electronic Documents Act 2004, in Canada determines for businesses the procedure for Customer data collection, usage and disclosure. United States even though does not have a regulations dedicated to privacy; however there are a number of laws that cater to different issues related to privacy.

Sweden and UK have imposed legal restrictions on possession of any individual's personal information in absence of explicit approval of the information owner, and if an organization or business need to store this information then the business has have this storage registered with the governmental agencies. The German law additionally requires the collection of data to be kept at minimum so as to perform a certain function and prohibits use of the data other than the specified and declared purpose. Data Protection Directive of the European Union declared privacy as a fundamental right in 1998.

However, the attempt to solely protect privacy via legal means is not as fruitful as it used to be. Legislations are lagging in the race with the latest technological developments and the legal system is not equipped to react at an appropriate pace to the changing technology. On top of it, laws are specific to a country.

Organizational Steps

Users and vendors have available organizational means that can be used in protecting the privacy of the individual during the ecommerce transaction. E.g. physical separation of consumer data into two parts one that is personally identifiable while the other is under the non-identifiable category. Data which refers to specific kinds of services or which tell about the types of the products that is individual is purchasing termed as is non-identifiable and should not be, combined with traits that are termed as personally identifiable, like the banking details, credit card information, date of birth, address or name of the individual. Under the effort to protect privacy we are concerned with only data that is personally identifiable, so Non-identifiable info can be put under analysis in a suitable manner.

Involvement of a transaction service provided by a third party is another means of achieving privacy and confidentiality. This third party may be required to act as an intermediary for guarantying the trustworthiness of the transactions. Another means of increasing trust and privacy may be the "online privacy seal" i.e. TRUSTe, or Platform for Privacy Preferences (P3P). These technologies give customer the ability judge if the Business' privacy policy is in accordance to what he prefers. Yet both the above approach rely on constructing awareness amongst the business about the privacy of its customers and cannot be an assurer of actual execution as per policy. This leads us to the same point where a customer has to basically rely and trust the vendor to keep its promises and not violate his privacy.

Technological Steps

We can use Privacy enhancing technologies (PET) to enhance consumer Privacy. These technologies provide the option to delink an individual and their personal data. We come across different modes of anonymity being described in literature, we can have full anonymity or pseudo-anonymity (where an individual's identity is normally un-know but if required it can be disclosed), or pseudonymity (where the users creates multiple virtual identities and uses them for different purposes). Anonimyzation can also be accomplished by one of the following three techniques: anonymizing the medium of transport, statistical databases, or anonymous access.

Through anonymizing the medium of transport, we strive to hide the identity of the user in an un-revealable manner.

Setting up a free email account with an email provider, that is trusted for not tracking information like IP addresses, is probably the simplest possible manner to accomplish this task. This approach, however, is not a very feasible approach as most of the email providers are legally required to keep details of the communication that are made through them for a specified time period and every transactions that exceeds a specific value must also be recorded and maintained. Another method to have anonymous browsing is through anonymizing servers. Under this method all the traffic originating from any user is passed through the anonymizing server, this makes the IP address or user's identity unidentifiable. However, this technique relies on the trust of the third-party for the information on not being disclosed.

In an attempt to discard these third-parties., the "Crowds" system was created by Reiter and Rubin [7]. This system clubs the users into large groups called the crowds. Whenever a user requests information from the internet the request is routed through this Crowd instead of being passed onto the recipient directly. Before being submitted to the website the request is bounced between a random numbers of hosts that are part of the Crowd. Thus the originator of the request, remains unidentified by the recipient. Another privacy enhancing technology uses encryption. Chaum Mixes is prominent in such technology, utilizing public key cryptography [8]. The entire message is divided into chunks of equal size that are cryptographically changed before being delivered to the recipient. The order of the messages is also changed. This process is aimed at making it difficult for linking the original messages to their senders and even the outgoing message is unlikable this prevents the possibility of performing any analysis of the traffic to establish the identity of the user. The original concept of Chaum Mixes was built upon in to arrive at various other methods. E.g. "Onion" protocols under which a dynamic mix of protocols is being used by the user to submit the request as a data structure. The request is structured like the peeling skins of an onion. The layers are designed in such a manner that at any point only the specific layer can be decrypted only to reveal the next point in the chain. Onion routing, even though is available on the internet for anonymizing users, is not free and incurs cost.

Another method available for privacy enhancing privacy is anonymous access. In such a system an individual remains unknown to the business organization except through his pseudo-name (awarded credential). A user has multiple unrelated pseudonyms. Certification authorities issue credentials to a user, he just have to prove that he possess these credential to an organization and he is not required to reveal his identity. However, this system has a weakness is that even though a user may be legitimate he can still pass on his pseudonym to another user. This can be regulated through linking together the certificate and the private key issued to the user, thus maintaining his privacy as well.

Anonymous access gave rise to the authentication and authorization infrastructure (AAI), which is based on the principal that it isn't required to know who is the user, it is sufficient that the particular user has authorization for the specified actions. What it means is that it enables customers to buy items online by hiding their identity but proving possession of the required authorizations, which means that they have authorized access to a bank account etc. or that they have already made the payment. This essentially infers that the AAI is entrusted to an organization that relies on these services. The uses and the type of AAIs are discussed at [9].

Statistical databases are utilized in another approach to privacy. A statistical database is a collection of data, e.g. data of the customers and the item that have been purchased by these customer but it does not reveal the info that can be used to identify any individual uniquely. The values stored in this database are not the data itself, but the statistical information. This gives rise to methods for keeping the statistics of the data useful while keeping the individual's data hidden. Few of the methods are :

a. Only allow queries that retrain privacy (Query restriction),
b. Change the data about the individual in such a manner that data is useless but the statistics remain unaffected (Data perturbation), or
c. Altering the result of a query if it appears to be a threat to privacy (Output Restriction).

However, the above described methods have a drawback that the data is made of less use by them.

3. Reliability

People have long carried out face to face business. This mode of business has been quite successful. One of the causes of this success is the Trust that is developed in these transactions, because of face-to-face dealing that is happening in this transaction. This concept of trust has its social & psychological aspects.

As mentioned, trust and reliability are at the center of any business dealing. It becomes even more important when we are dealing over the internet. We will also demonstrate that the definition of trust is not as simple as we may have presumed previously. Moreover, Trust need to be an integral part of any business dealing over the internet for the digital transactions to have the same level of

acceptance likes traditional business. For example the vendor who is selling the product should have the trust that the person buying it is capable of paying for what he has bought while at the same time the purchaser need to be assured by the vendor that he would not disclose the private info of the buyer to anyone else.

3.1 Definition of Reliability or Trust

We have had numerous definitions of reliability and trust available. Some have tried to define trust in the general or global perspective, while some define it with reference specific types of applications. Reliability is defined as "The ability of an item to perform a required function under given conditions for a given time interval" [10]

One such attempt of defining trust in electronic commerce was made, where with reference to a system, Trust is defined as "a belief that is influenced by the individual's opinion about certain critical system features"[11]. Whereas reliability "In general, reliability (systemic def.) is the ability of a person or system to perform and maintain its functions in routine circumstances, as well as hostile or unexpected circumstances [12]"

Grandison and Sloman have also argued that because there is a lack of commonality on definition of trust it has directed them to interchangeably use the terms authorization, authentication and trust. Furthermore, they have defined trust as "the firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context (assuming dependability covers trust and timeliness)" [13].

3.2 Authentication and Authorization Interchanged with Trust

Interchanging trust with authorization and authentication cannot be done according our belief, because authorization and authentication, understandability are the security service provided by the application, while we cannot consider the same for trust, it is the outcome (i.e. a belief) resulting from the appropriate application of Authorization and Authentication in a scenario, like reliability. However, we agree with the authors that there is no unanimity about the definition of Trust and Reliability.

We would also agree to the importance imparted to authorization and authentication, as these service are integral in getting the trust of consumers and merchants. In this respect, digital certificates has provided us with a solution that can be termed to have contributed a great deal in increasing the trust on security of e-commerce transaction on the whole and specifically the service of authorization and authentication.

One of the best available solutions to integrate authentication with Internet applications using the digital signatures is the concept of Identity certificates (or public-key certificates) [14]. However Internet application requires that it be clearly specified that which actions are permissible, for the user that has been authenticated by the authorization service. In order to achieve this we should consider putting restriction on the privileges as well. A solution for this issue is provided by Attribute certificates which in conjunction with identity certificates, provide authorization and the access levels as well [15].

Public-Key Infrastructure (PKI) is known to support encryption, integrity and non-repudiation at the same time, along with providing a trustworthy & efficient mechanism to distribute and manage these certificates. It is evident that in the absence of such a mechanism it is not practical to assume that the applications using digital signature would ever be a reality.

This Framework of attribute certificate also provide us with a base on which we can build a PMI (Privilege Management Infrastructure). The information contained in the Attribute certificate and the Identity certificate of each user link the PMI & PKI infrastructure. This link further establishes the fact that authorization must rely on authentication for proving the identity, and it is brings out, that the appropriate use of a combination of these Authorization and authentication certificate greatly increase the reliability and the trust on the system from the user's perspective. Although linked, both systems can be managed independently as well.

The attribute certificates can be used for numerous purposes, like it may contain information related to the membership of a group, clearance level, the role that an individual plays etc. Through the attribute certificate authorization can be provided to decentralized applications. Additionally through attribute certificates, digital business applications can conveniently make authorization information distributable.

3.3 Trust Management

The Management of reliability and Trust for digital commerce is most likely the most critical issue when dealing with this concept. The concept of trust management was introduced by Blaze and others [16]. It was proposed that PolicyMaker can work as a solution for managing trust. PolicyMaker allows a programming

language to encode the access level and the identity of the individual.

Additionally to achieve standardization and facilitation of PolicyMaker's integration into applications, the name of KeyNote was suggested. It makes the use of assertion languages, which are accommodate the security policy of different application.
However, we know that trust and reliability of varies with time, thus digital certificate for attribute & identity are considered by some authors for trust management purposes. Procedures & functions provided by PMIs & PKIs can be considered advance methods of trust management. They seem to be better solutions than the ones discussed previously as they are less static, however they have a bias approach for the authorization as well as the authentication service.

3.4 Challenges of Trust & Reliability

We have already discussed, that even the simplest issues related to trust still need solutions and are open. And this too is just a marginal part of the complete set of challenges related to Trust. During a National Science Foundation workshop aimed at discussing the challenges for Management of Data and Information the following challenges were identified by a group of people who are experts in this Field:

a) How can we build & initiate trust?
b) How can we evaluate & maintain trust?
c) How to deal with fraud?
d) How to guarantee scalability, performance, and economic parameters for trust solutions?
e) How to engineer trust-based applications and systems?

They have additionally recommended the need of research being conducted in the following areas related to Trust: (a) Social paradigm (b) Liability. (c) Scalability and adaptability of infrastructure. (d) Benchmarks, developing of applications based on trust. (e) Detection & Prevention of Fraud (f) Interdisciplinary research in areas associated with Trust.

Thus we find it to be evident that still research needs to be conducted in this area in future as well.

4. Security

Five components namely data, procedures, hardware, software and people are interconnected & interacting in any e-commerce scenario. We come to a conclusion that e-commerce system is an information system that comprises of both an organizational framework and a Tech. infrastructure, not just the Tech. infrastructure alone. Thus, information system setting must be used when addressing the issue of security in e-commerce.

Under the present situation, we can define security as an organized framework that consists of policies, procedures, concept, believes, principles, measures and techniques required to protect, against any deliberate or accidental threat to the system or the individual assets of a system [17]. Operationally, when compiling this framework, we must identify the requirement first.

4.1 Requirement of Security

Close inspection of all e-commerce reveals the presence of discrete stages, this allow us to build a universal model that describes them all. A model similar to the one described above was suggested to cater to business dealings [18] and has also been demonstrated to be great for dealing with commercial transactions [19]. This model is based on the observations that the unit of any Business is an exchange transaction. In such a transaction, party X & Y, mutually agree that they will comply with specified condition of satisfaction. The Buyer (X) and the seller (Y) are part of this transaction. X makes a request to Y for providing a commodity to X which Y accepts, in return X pays Y for the commodity. This entire exchange can be explained clearly in a four phased cycle:

1. Request. X makes a request of Y for providing a service. (This often means Y taken up on an offer he has made).
2. Negotiation. X and Y mutually agree what will be provided (X's condition of satisfaction) and what will be the payment made (Y's condition of satisfaction).
3. Performance. Y performs the actions required to fulfill his part of the deal and informs X when completed.
4. Settlement. X accepts the work done by Y, accepting it to be satisfactory, pays.

We can combine Performance and Settlement can be combined in a single phase, and call it Execution phase [20]. The above model depicts all kind of transactions, including electronic transaction.

In the first phase, both the X&Y have unique requirement of security. X needs assurance that the offer in consideration is valid, that is, the information presented to him has not been corrupted by an external party. Similarly, Y needs assurance that the offer he made is available to X. Y may require his offer to be confidential; for fear that an adversary may barge in the Deal, if this is not a retail transaction. Confidentiality is also clearly required, in the second phase, especially when this is related to negotiations of contract. It is Important none of the parties are able to repudiate their offers in this phase. However, non-repudiation becomes more important during the Final leg. In this stage secured delivery of goods along with secure payment should be ensured. It is noteworthy that some items is intangible; and thus the seller can deliver it to the buyer electronically Example, digitally shares. The situation presents us an interesting requirement of security. Lastly, we see the fundamental difference between electronic & traditional Business, i.e. there is no face 2 face interaction in Electronic Commerce. Machine that don't have any way of identifying the person on the opposite side, are presented with pre-agreed information that establishes identification of the users.

Thus, the security requirement of Electronic commerce essentially include the necessity to maintain the integrity, confidentiality and availability of the information and the system, the authenticity of the entities involved that they are not able to repudiate their transaction.

4.2 How to Address the Requirement

For frameworks to preserve the information system's security it must include of technical, legal social & organizational action. Legal actions are to taken at a national & international level by the government. Individual organization need to take Technical and organizational action. Lastly, enhancing public awareness for security requirements and on the right and obligation arising from this requirement must be done on the social level.

The major legal issues associated with e-commerce [21-22], are:

(i) The protection of privacy.

(ii) The protection of intellectual property rights. Related to it is the problem of registering domain names to be sold later at a higher price i.e. cybersquatting. We also have an issue of Patent Protection in electronic commerce. National legislation exists almost everywhere for protecting of intellectual's property right, [23]. The World Intellectual Property Organization – WIPO (www.wipo.org) plays the most prominent role internationally, also administering 23 relevant international treaties [24].

(iii) Rights to freedom of speech contending the necessity to control potentially dangerous, illegal and offensive information. Including the issues spam control.

(iv) To be protected against Fraud, including identity fraud, regulation of taxation. To be protected against computer crime and money laundering etc.

Though we have legislation for maximum of the above subjects in traditional commerce but it cannot be directly applied to e-commerce environment. Therefore, we need to develop new laws or to ensure that the existing ones are applicable to the required situations.

The vast number of entities involved in e-commerce makes is impossible to use of symmetric encryption. As it is not possible to maintain & manage certificates and keys for such large base of users via small scaled, inter-organizational means. No matter if they are completely automated also. Thus, a consolidated approach consisting of five kinds of components, and based on the Public-Key Infrastructure is required [25]:

(i) Certification Authorities (CAs) for issuing & revoking of certificate.
(ii) Organizational Registration Authorities (ORAs) to ensure tying of certificate holder identities & attributes with public keys.
(iii) Certificate holders who are issued certificates and have the ability to sign digital documents and encrypt them.
(iv) Clients who can, based on public key of a trusted Certification Authority, validate digital signatures and their certification paths.
(v) Repositories having the ability of storing & retrieving the available certificate along with CRLs ('Certificate Revocation List').

A TSA (Time Stamping Authority) might also be included as part of Public-Key Infrastructure. Organizations that work as Certification Authorities, Registration Authorities, Repositories and Time Stamping Authorities are commonly called TTP (Trusted Third Parties) / CSP (Certification Service Providers).

Despite the fact that requirements from a PKI are quite dissimilar and have been recorded in numerous applications, a common ground can be found [26]. You may also find a broad list of services satisfying the requirements above in [27]. Subsequently, the list of functions required to perform these services can be defined in [27].

From the discussion above it seems that we know all the issues related to security in e-commerce and we have the technology available that can provide solutions to the issues in security of e-commerce. However, if that was the case then a critical question would be: Why do we still have breaches of Security when e-commerce transactions happen? The incidents should not be happening.

The most common problem is that, while everyone acknowledges the need for securing ecommerce, what they neglect is that security is much more than putting physical and electronic barriers. The most robust firewall and strongest encryptions are practically useless without organizational security, built around a policy that enunciates how these usages, maintenance and management of these tools is to be done. This policy is concerned to and neutral to technology as it is at a High-Level. It is aimed at setting procedures and directions, along with defining penalties & measures for noncompliance [28].

5. Conclusion

Despite Presence of laws dealing with on e-commerce Confidentiality, Reliability and security, agreements between countries are still missing. From a legal point of view it should not make a difference to the buyer or the vendor who are part of the electronic transaction, where the business, user or the intermediary service are situated. We must imitate an effort to encompass protection of all consumer rights, moral or legal, with a common understanding and agreement. Previously, law makers have fought against individual violations when they occurred – which resulted in a kind of patch work of different legal systems. But this helps only safeguard against violation of secluded characteristics of Security, Confidentiality and Reliability in Electronic commerce.

There must be an inherent support in E-commerce businesses for privacy platforms, third-party transaction service, security solutions and trust infrastructure. The Policy must clearly outline what are the applicable laws for which countries where the e-business is located. The policies should also have proper change management, i.e. keeping track, with dates, of all changes made to them. Consumers should choose the product and service more prudently on the basis of privacy & security statements and on the presence of certified features, like site authentication or seals of privacy. Thus increasing the acceptance of the seal and forces the e-business to comply with the statement published. Yet, we know for sure that the privacy enforced via organizational means don't really guarantee privacy of the individual. All these approaches only help in making the decision on which we can trust and rely on. It is the initial step only; we require technology to ensure preservation of confidentiality.

Current technologies have made significant breakthrough in preserving the Security, Confidentiality and reliability of electronic Commerce. However, a lot of research is still required for this to be performed without the user's intervention and with lesser participation of the trusted third parties. To conclude technologies that are better suited for the general security requirements, need to be developed. In the current scenario anonymity is considered to be a threat to the social or national security. We need to carry out more research to comprehend how we can achieve a balance between the two conflicting requirements and have a harmonious existence of both.

References

[1] http://forrester.com/ - Forrester Research. Post-web retail. Sept. 1999.
[2] http://www.census.gov/estats - US Census Bureau
[3] R. Clarke, "Internet Privacy Concerns Confirm the Case for Intervention", Comm. of the ACM. Vol. 42, No. 2, 1999.
[4] W. Chung, and J. Paynter, "Privacy Issues on the Internet", Proc of the 35th Hawaii Int. Conf. on System Sciences. Jan. 2002.
[5] M. Brown, and R. Muchira, "Investigating the relationship between Internet Privacy Concerns and Online Purchasing Behaviour", Journal of Electronic Commerce
[6] I. Araujo, "Privacy Mechanisms supporting the building of trust in e-commerce", Proc. IEEE International Workshop on Privacy Data Management, Tokyo, Japan, April 2005.
[7] M. K. Reiter, and A. D. Rubin, "Anonymous web transaction with Crowds" Comm. of the ACM. Vol. 24, No. 2, 1981.
[8] D. L. Chaum, "Untraceable electronic mail, return address, and digital pseudonyms", Comm. of the ACM. Vol. 24, No. 2, 1981.
[9] J. Lopez, R. Oppliger, and G. Pernul, "Authentication and Authorization Infrastructures (AAIs): A Comparative Survey", Computers & Security Journal. Elsevier (North Holand), Vol. 23, 2004.
[10] http://disi.unitn.it/locigno/didattica/PE/05-06/Support_ Lez01.pdf
[11] Anil Kini, and Joobin Choobineh, "Trust in Electronic Commerce: Definition and Theoretical Considerations", HICSS (4), 1998, 51-61.
[12] Wikipedia - http://en.wikipedia.org/wiki/Reliability
[13] T. Grandison, and M. Sloman, "A Survey of Trust in Internet Applications", IEEE Communications Surveys & Tutorials, 2000.
[14] "Information Technology - Open systems interconnection - The Directory: Authentication Framework", June 1997. - ITU-T Recommendation X.509

[15] "Information Technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks", March 2000- ITU-T Recommendation X.509,
[16] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized Trust Management", IEEE Symposium on Security and Privacy, pp.164-173, 1996.
[17] E. Kiountouzis, "Approaches to security of information systems", Information Systems Security, New Technologies Publications, Athens, (S. Katsikas, D. Gritzalis and S. Gritzalis Eds.), 2004
[18] T. Winograd and F. Flores, "Understanding Computers and Cognition", AddisonWesley, 1997.
[19] P. J. Denning, "Electronic Commerce - Internet Besieged", Addison-Wesley and ACM Press, (D. E. Denning & P. J. Denning Eds),1998.
[20] G. Pernul, A. Rohm and G. Herrmann, "Trust for Electronic Commerce Transactions", in Proceedings, ADBIS '99, Springer-Verlag, 1999.
[21] R. Burnett, "Legal aspects of e-commerce", Computing & Control Engineering Journal, 2001.
[22] E. Turban, "Electronic Commerce: A Managerial Perspective", Prentice Hall. 2004.-
[23] http://www.wipo.int/clea/en/index.jsp
[24] http://www.wipo.int/treaties/en
[25] A. Arsenault and S. Turner, "IETF PKIX WG, Internet draft, Internet X.509 Public Key Infrastructure PKIX Roadmap", March 10, 2000.
[26] D. Lekkas, S.K. Katsikas, D.D. Spinellis, P. Gladychev and A. Patel, "User Requirements of Trusted Third Parties in Europe", in Proceedings, User identification and Privacy Protection Joint IFIP WG 8.5 and WG 9.6 Working Conference, pp. 229-242, 1999.
[27] S. Gritzalis, S.K.Katsikas, D. Lekkas, K. Moulinos, and E. Polydorou, "Securing the electronic market: The KEYSTONE Public Key Infrastructure".
[28] S.K. Katsikas and S.A. Gritzalis, "A Best Practice Guide for Secure Electronic Commerce", Upgrade, Vol. III, no.6, December 2002. http://www.upgradecepis.org .

Author Biographies

Dr. Abdullah received his B.Sc. degree in Computer Science from University of Southern Mississippi in 1990, Master degree from MIS Department, Information Systems, University of Illinois in 1992 and PhD degree in Computer Science from Computer Science Department, George Washington University in 2003. He has a teaching and research experience of more than 20 Years and his research interests include Information Systems, Software Engineering and Artificial Intelligence. He has more than 20 publications to his credit. Presently he is Chairman/HoD, Information Systems Department, Faculty of Computing and Information Technology, and also in additional charge of Vice-Dean, College of Science and Technology, King Abdulaziz University, Jeddah, KSA.