A DIVERSIFIED APPROACH TOWARDS SECURE E-BUSINESS

Preethi Mohan, Manasi Jain & Manojita Mishra
School of Computing Sciences
VIT University, Vellore-632014, Tamil Nadu, India
e-mail: pmohan_86@yahoo.com, smilingmanasi@gmail.com & bornwidsmiles@gmail.com

ABSTRACT

An exponential increase in popularity of the concept of E-Business, due to use of Internet and its virtual way of doing everything, has led to appraise its scenario to weigh the pros and cons. Despite the fact that electronic business has benefited immensely for both the previously saturated markets and the new business opportunities, it has also paved way for many problems. To ensure complete satisfaction for the consumer and the seller and to make e-Business viable, we need to identify these problems and furthermore, find effective solutions for all. The sensitivity of all the problems lies in securing the transactions carried out between the buyer and the seller. In addition, due to the rapid growth of technology keeping pace with the associated risks is challenging. Thus, in this paper we sincerely attempt to recognize the security requirements, issues and threats in the system and security in an e-Business environment.

***Index Terms*— E-Business, Security,**

1. INTRODUCTION

A primary goal of every business is to profit, be it of traditional type or based on electronic modes of communication. In the conventional business type, this is mainly achieved through direct "human dealings" or through a reliable third-party. On the contrary, electronic means demonstrate the complete lack of it. This gives rise to many issues. Each issue focuses on a different perspective, and the cluster of all those concerns address the complete business scenario.

The definition of e-Business as stated by Gartner Group is that it is "a dynamic set of technologies, applications and business processes that link enterprises, consumers and communities through exchange of goods, services, transactions and information" over the Internet[7]. The adoption of Internet to conduct e-Business has proved beneficial to its users as well as the business community. Unfortunately, this has also attracted illegitimate activities in the virtual world.

The major issue to be resolved, without which any transaction is incomplete, is security. In fact, it is a key e-Business enabler. Security for any transaction can be viewed from various dimensions, for instance, information security, exchange security, communication security, etc. There are 3 basic types of security concerns for an e-Business environment: direct attacks, privacy and trust [7]. *Direct attacks* are those vulnerabilities that are directly introduced into the system by hacker. If any system does not have proper defense mechanisms and proactive measures to mitigate risks in place, then it becomes an easy prey for those who want to detour its normal functionality to some desired abnormal behavior. Few examples of these vulnerabilities are viruses, trojans, malicious code and vandalism. *Privacy* is a major concern as the use of Internet exposes information, transaction details, etc to millions of users who access the Internet at the same time. Hence, it is a necessity to protect the confidentiality of data to ensure privacy. *Trust* is the most important trepidation, which differentiates corporate networks from e-Business, because of 2 reasons:

- It is more of a business issue than a mere technical consideration.
- Copious consumers transact electronically at the same time, therefore knowing the identity of each is a difficulty.

Thus, managing trust is vital for every successful transaction.

The paper consists of three sections. The first section identifies the security requirements. The next section exemplifies a secured e-Business environment. Finally, we consider the issues and perils in e-Business.

2. SECURITY REQUIREMENTS

Initially when the Internet was intended to be used for sharing information, files transfer, accessibility, etc it mainly aimed to attract users to acclimatize to a new environment, thus openness was the point of focus. Now that it is used so profusely there is a need for safety measures to make sure that users feel secure and have faith in the virtual world. This can be fulfilled by identifying and understanding the requirements that needs to be realized.

Authentication is a method used to restrict the access to the authorized users alone. It is generally done by supplying user id, which identifies the user, and password. The user

"logs in" to the system if his user id and password matches with the one stored in the database else the access is denied.

Confidentiality maintains the privacy and integrity of data and information being sent or exchanged across the network (mainly Internet). For instance, when a buyer purchases a book from an online bookshop, he/she sends his/her card details to confirm the purchase and to make the payment for the same. It is of utmost importance that these details are not revealed or exposed or accessible to any other person. Thus, the need for confidentiality is to be addressed.

Integrity ensures that the message sent is not modified anywhere in its intermediate path of travel to the destination. Also, the originality of the message is maintained and as such received by the concerned party. For example, data integrity is a type of integrity. Data integrity is generally hampered by system or communicational errors.

Non-Repudiation facilitates the confirmation that the customer has actually transacted business and will not deny the fact. This is very essential as the business parties may not know each other in prior and the seller has to trust that the customer has indeed carried out a transaction.

Complexity arises when building and deploying e-Business applications due to its dynamic nature and the rapid pace of change in technology. The design, implementation and verification of these become very difficult. Also, the network offers opportunities for the attackers to discover newer methods to breach the security of the system. Thus, we need to employ cryptography algorithms and protocols to ensure that the applications are appropriate to use, and that they are efficient and fair apart from being secure to at least known attacks.

Availability emphasizes on the need that any data or information requested by the user is available to him/her at any time, any place and that the available data or information is accurate. The trusted third parties and certification authorities should also be available all the time. Offline security technologies must also be accessible.

Anonymity is required in certain transactions like anonymously publishing content on web, requests for quotes in stock brokerage. This conflicts with certain other requirements such as authentication, access control, etc. Hence, this must be addressed with care.

Code Autonomy deals more with future e-business applications in terms of mobile code that will roam autonomously in the network on the behalf of users. Two major problems that must be attended to are:

- How to protect mobile code against potentially malicious hosts and runtime environments?
- How to protect hosts and runtime environments against malicious mobile code?

Since both are interdependent, finding practical solutions that satisfies both the concerns is very difficult. Hence, to deploy mobile code effectively it needs to be studied under careful consideration.

Trust management is the most important requirement in a secure and successful e-Business environment. The depth of level should be such that even in an uncertain situation the business parties should be able to believe in each other and carry out their dealings in the virtual world. Apart from its relationship with uncertainty, it is also connected to risks associated with such tentative situations.

Intellectual Property Rights Protection is a prerequisite for the successful deployment of e-commerce applications. This is because the intrinsic nature of digital data, products, services allow for easy replication and distribution, and hence to guard from such illegal attempts to use other's property. We can use various techniques like digital licensing, digital watermarks, fingerprint recognition, etc.

3. E-COMMERCE- SOME SECURITY ISSUES AND PERILS

E-Business deals with transactions between the buyer and the seller through use of Internet or other networks. Thus, security requirement in such a transaction is more as it involves crucial data and information. It also focuses on the need for trust in the scenario. Let us explore the issues and risks associated with these transactions [1].

Client-side security issues handles the matters related to authentication and authorization of the clients. This encompasses the user's point of view i.e. the clients must be trustworthy to carry out the transactions or request for the service. They can be resolved by keeping in place proper mechanisms for server authentication, boot control, access control and anti-virus detection, non-repudiation, anonymity, etc.

Server-side security issues are typically the concern from the service provider's point of view. They ensure that the services provided to the clients are from a reliable source. They fulfill the requirements like non-repudiation of clients, anonymity of user, reliability, availability, audit trail and accountability.

Transaction security issues arise when a transaction is being carried out between the client and server. It normally involves exchange of huge amount of data across the network and thus, these issues need to be tackled prior to a transaction commencement. Various services like data integrity, access control, etc are provided to solve these issues. Security related protocols like SSL and S-HTTP are gaining popularity for the same.

Organizational and Legal security issues accentuate on the fact that security is and will always be a people's problem that means the real challenge lies in tackling issues from the user's perspective rather than merely considering the stance from technical side. We must also ensure that the solutions to the issues in concern do not deflect from the goals of the organization or tend to contradict the legal policies of the organization.

Denial of Service comes about when the server denies providing service as the client machine over-floods the

server with same packets. The selling party or service provider will be overwhelmed by the incoming requests when they realize the fact that the packets were simply bogus and not an actual order or request for service.

Viruses are executable programs to utilize the system resources unnecessarily or change the configuration of the system. The attacker introduces viruses into the target machine, and creates havoc. Examples are Melissa, ILOVEYOU, Resume, etc. There is much anti-virus software available which can be used to avoid getting trapped in the consequent mayhem.

Trojan Horses is a back-door entry to gain unauthorized access to a system. The attacker can work on the marked user's computer without the user's knowledge and do everything just like the actual user of the computer is doing it. Initially, Trojan horses were used to create multiple copies of the same data and make it available to even remote locations. But later it was maliciously used to steal confidential data, eavesdrop or modify data that can be mailed by the attacker to its target user at a later date.

Theft and Fraud happens when any data available or being sent across the network is intercepted or modified without the knowledge of both the parties. The stolen or forged data may be used for wrong purposes. This can be avoided by making sure that the users are authorized, and that, mechanism to monitor any kind of abnormal behavior is always in place.

4. AN OUTLINE FOR SECURE E-BUSINESS

The diagram below illustrates a secure e-Business environment in a layered approach where it is divided into 3 layers. Namely, Presentation layer, Security layer and Data Access layer.

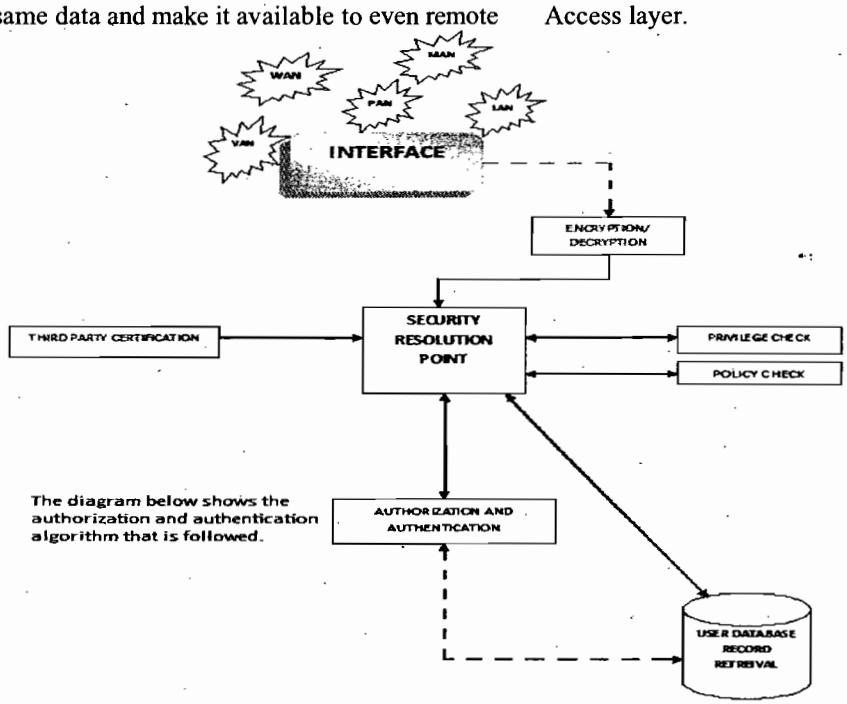

Figure 1: Illustration of a secure E-Business environment

The *presentation layer* consists of the interface which acts as an intermediate between various network users and the security layer. Also, it specifies some networks that access the interface for different purposes.

The *security layer* is the main focus in the illustration. It deploys mechanisms like privilege check, third party certification, etc. A transaction performed under the vigilance of such mechanisms is expected to be successful.

The *data access layer* gives access to the database which stores information related to the users and the related operations of storage and retrieval of data are performed on it as and when required.

The algorithm given in the diagram below does the following:

1. The user provides authorization proof, say user id and password, to access the service.
2. For authentication purpose, the user records are checked in the existing database.
3. If the user is authorized, then give initial permission for access and go to step 5.
4. Else go to step 7.
5. Retrieve the user record from the database.

6. If the information is valid then authorize the user with the appropriate level of authorization and go to step 8.
7. Else deny access and show the error message. Go to step 9.
8. Provide the desired service to the user.
9. End.

The algorithm also takes care of the confidentiality and integrity part by ensuring that only authorized systems access the database and the user transaction details. The authorization and authentication forms an important part in the secured e-Business environment. This also gives rise to many issues which are addressed in the next section.

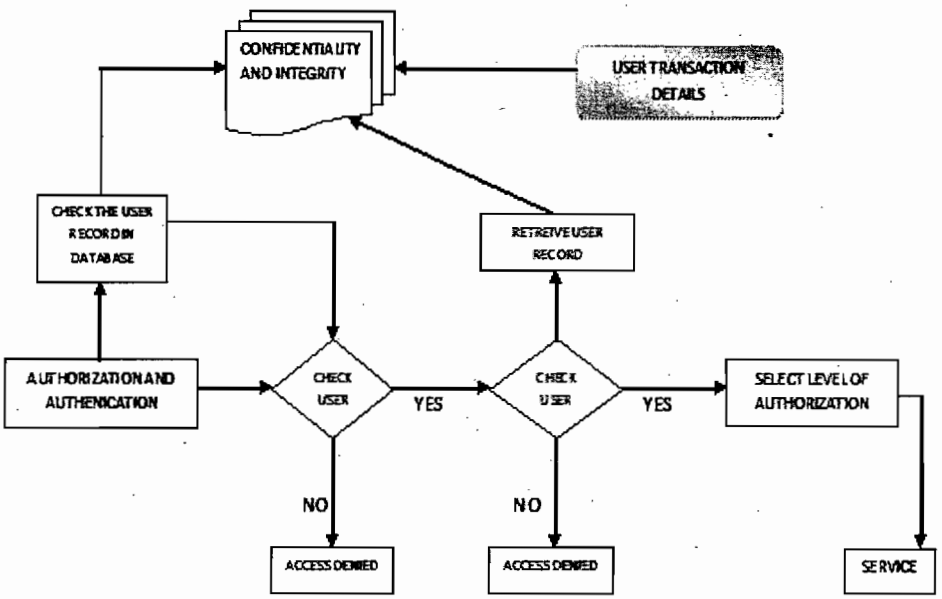

Figure 2: Authentication and Authorization algorithm

5. CONCLUSION

In the paper, firstly we introduce the concept of e-Business and its major issues, the most important of all being security. We identify the requirements that must be accomplished in order to build secure e-Business applications in the interest of the business parties. An outline of a secured e-Business environment is provided which illustrates the possible layers in place and also an algorithm to authorize and authenticate the users of the system. Finally, we touch on the issues and threats that are posed by such an environment.

Security is the foremost concern in today's e-Business scenario. It aims to satisfy the stakeholders of the business system in every possible way. It can be appropriated in a better manner when it is applied as layers of technology, where each layer would address a separate concern. Even though we can achieve secure systems, e-Business, security and technology are prominent research areas and hence, keep changing. The main aim behind this research is to satisfy the customers in a better manner day-after-day.

E-Business offers a lot of scope for research and also wide range of issues to address. This is a perennial process which may stop only if the human brains would run out of novel and innovative ideas to enhance or improve or invent a new thing (technology, security protocol, etc) or if a foolproof security solution is achieved that would work even for the enhanced or improved systems formulated in the future.

Acknowledgement We, Preethi Mohan, Manasi Jain, Manojita Mishra sincerely express our gratitude to our Chancellor Mr G.Vishwanathan, Pro Chancellors Mr Sekar Vishwanathan and Mr G V Selvam,Vice Chancellor Prof Dr D P Kothari, Dean Prof M. Khalid and Program Manager Prof H R Vishwakarma for their kind support and guiding us at every step .

6. REFERENCES

1) Rolf Oppliger, "Shaping the Research Agenda for Security in E-Commerce", Swiss Federal Office Of Technology and Systems (BFI).

2) Kari Heikken and Neeli Prasad, "Empowerment: Enabler for Personalized Security and Privacy", University of Lappeenranta, Finland and CTIF, Center for TeleInfrastruktur, Denmark.

3) Raj Mehta, "Secure E-Business", Information Systems Control Journal, Vol. I, 2000, pp. 32-38

4) Randy C. Marchany and Joseph G. Tront, "E-Commerce Security issues", Proc. 35th Annual Hawaii International Conference on System Sciences (HICSS-35'02), 2002.

5) Ying-Hong Wang, Chen-An Wang, Jen-Shium Chiang and Wen-Hung Lo, "A Secure Model in Agent-Based Marketplace", Proc. The 17th International Conference on Advanced Information Networking and Applications(AINA'03), 2003.

6) Symon Chang, Qiming Chen and Meichun Hsu, "Managing Security Policy in a Large Distributed Web Services Environment", Proc. 27th Annual International Computer Software and Applications Conference (COMPSAC'03), 2003.

7) Lu Tao and Lei Xue, "Study on Security Framwork In E-Commerce", IEEE, 2007, pp.3541-3544.