A Security Measure for Electronic Business Applications

Anuradha Sharma
Department of Computer Science
Amity University,Lucknow Campus

Praveen Kumar Misra
Department of Statistics
Amity University, Lucknow Campus

Puneet Misra
Department Of Computer Science
University of Lucknow

ABSTRACT
With the growth of business over the internet, there is more scope of security vulnerabilities over the internet. Despite of many efforts to make internet safe to the users, there is still a possibility for threats. The client, as well as the merchant for the electronic business, always faces problems due to these threats. This paper is an effort to distinguish the threats for the client perspective and the merchant perspective. Further a measure has been defined for securing both the parties over the internet during the electronic business. Further, the measure can be used for the analysis, design of an application, and also, to compare it with other applications.

Keywords
Electronic business, security, security measure.

1. INTRODUCTION
E-business or electronic business is not only limited to buying and selling of goods over the internet. E-business includes using internet to provide better customer service, streamline business process, increase sales and reduce cost of the business for the customer as well as the organization. IBM first used the term e-business in October 1977[13]. Since then, companies are using internet to cut cost and provide better customer service. The security of e-business is of great discussion due to various security breaches despite of various measures being taken by the companies. Transaction is an instance of buying or selling something. In case of e-business, this buying/selling is done over the internet.

The transactions in case of e-business have tree major constituents viz. the client computer, the communication medium, and the web and commerce servers. The security can be penetrated at any of the three parts. There are also three parties which are involved in transactions over the internet viz. the client, the merchant and the transmission way (internet)[1]. In this paper, we will consider only two parties, i.e. the client and the merchant.

2. SECURITY PRINCIPLES
Any computer related system has both theoretical and real weaknesses. The basic principle behind ensuring security is to devise some ways that could prevent these weaknesses from being exploited. The main principles behind security are discussed here so that we can understand the attacks better.

1) Confidentiality: Confidentiality means preventing disclosure of unauthorized information. The basic principle behind confidentiality is that only the sender and the intended receiver of a message are able to access the contents of a message. Confidentiality gets compromised if an unauthorized third person is able to access the contents of the message and such type of attack is called interception.

2) Integrity: Integrity refers to the trustworthiness of data or resources, and refers to preventing improper or unauthorized changes. When the contents of a message, from the sender, get changed before it reaches the receiver, it refers to the loss of integrity of the message. Such type of attack is called modification.

3) Availability: Availability is the ability to use the information or resource desired. It means that resources (information) should be available to authorized parties all the times. The attack on availability is called interruption [2][13].

Our focus during the study of electronic business will be on these three main security principles. Besides these, there are three more security principles viz. authentication, non-repudiation and access control which cannot be left without consideration.

3. THREATS
A computer based system has three separate valuable components viz. hardware, software and data. Each of these components has a different value to different members of the community affected by them. The ways in which the system or its information can experience some kind of loss or harm gives a feel of the level of security needed. A threat to a computing system is some set of circumstances which has the potential to cause loss or harm to the system [4].

3.1 Threats for client side
The various threats for the client perspective are listed below:

a) Active content: Programs that are embedded transparently in web pages and that cause an action to occur are referred to as active content. Active content can be moving graphics, download and play audio, or even more. The use of active content in e-commerce is to place one's required items into a shopping cart and to compute the total invoice amount, including sales tax, handling, and shipping costs. Java applets, ActiveX controls, JavaScript, and VBScript are some popular active content forms. Anyone can embed malicious active content in web pages, since active contents are transparent to users. This delivery technique immediately begins executing and taking actions that are harmful and is called Trojan Horse. This type of threat falls broadly into the integrity threat category.

b) Malicious code: Malicious code can be a computer virus, worm or trojan horse. A trojan horse is a program which performs a useful function, but performs an unexpected action as well. Virus is a code segment which replicates by attaching copies to existing executables. A worm is a program which replicates itself and causes execution of the new copy. Anyone or all of these can create havoc on the client side once executed. This type

of threat also falls broadly into the integrity threat category.

c) Server-side masquerading: Masquerading or spoofing is an impersonation of one entity by another. It lures a victim into believing that the entity with which it is communicating is a different entity. For example, if a user tries to log into a computer across the internet but instead reaches another computer that claims to be the desired one, the user has been spoofed [3]. This type of threat falls into the confidentiality threat category.

d) Repudiation of origin: It is a false denial that an entity sent (or created) something. For example, suppose a customer orders a product y sending a letter agreeing to pay the amount. The vendor ships the product and demands the payment. The customer denies to have ordered the product and by the law is entitled to the unsolicited shipment without payment. The customer has repudiated the origin of the letter. If the vendor fails to prove that the letter came from the customer, the attack succeeds. This type of threat falls into confidentiality threat category.

e) Password Hacking: The password-based system has the biggest threat of being guessed. Access to the complement, the complementation functions, and the authentication functions have to be obtained for guessing the password. While guessing the password, if none of these have changed, then the attacker can use the password to access the system[3].

f) Denial of Receipt: A false denial that an entity received some information or message, is a form of deception. For example, suppose a customer orders a product, and the vendor asks to pay the cost before delivery. The customer pays the cost and receives the shipment. The customer then asks when he will receive the product, the question constituents a denial of receipt attack [5].

3.2 Threats for merchant side

a) Database threats: At the merchant side, E-commerce systems maintain a database containing user data and also retrieve product information from other databases connected to the web-server. These databases contain product information as well as valuable and private information. This private information could damage the security of a company if it were disclosed or altered. Some databases store username/password pairs in a non-secure way. One can reveal private and costly information if he obtains user authentication information. This type of threat falls broadly in to the confidentiality threat category.

b) Non- repudiation: Repudiation or deny refers to the situation when a sender sends a message and later on refuses to have been send the message. Non-repudiation defeats the possibilities of denying something. This can be the case of integrity threat.

c) Access control: The principle of access control determines who should be able to access what. The merchant can maintain an access control list of the clients having the controls of the clients. The threat in such case can be an availability threat.

d) Delay: It is a temporary inhibition of service. The delivery of a message or service requires some amount of time and if an attacker can force the delivery to take more than the time the attacker has delayed the delivery [5].

e) Denial of service: It is a long-term inhibition of a service. The attacker prevents a server from providing a service. Denial of service poses the same threat as an infinite delay [5].

3.3 Security threats

Tthe various threats described for the client and the merchant perspective can be defined in terms of confidentiality, integrity and availability in table1. The table maintains a summarized form of the above defined security threats for the client as well as the merchant.

Table 1. Some security threats for client and merchant perspective in e-business

Threats	Confidentiality	Integrity	Availability
Client	Spoofing, Hacking, Repudiation of origin	Active Content, Malicious Code	Denial of receipt
Merchant	Database threat	Repudiation	Delay, Denial of Service, Access Control

4. PROBABILITIES OF THREATS

The probabilities of the aforementioned threats for the client as well as merchant can be tabulated. Since the probabilities vary from 0 to 1, the probabilities can be considered as high(0.9), medium(0.5), and low(0.1). Probability 1 indicates that the concerned party, i.e. the client and the merchant considers the security objective as essential. Probability 0.5 indicates that the party wants the security objective to be protected. Probability 0 indicates that the concerned party has no particular interest in the security objective [6]. The probabilities of various categories of threats can be summarized in table2. These probabilities may vary according to the category of e-business chosen[7].

Table 2. Probabilities of threats for the client and merchant perspective in e-business

Threats	Confidentiality	Integrity	Availability
Client	0.9	0.5	0.5
Merchant	0.9	0.9	0.9

5. 5. SECURITY MEASURE

The various threats for the client and the merchant perspective must be dealt with proper security measure so that the possibility of loss of data in any case can be minimized.

Table1 describes various security threats but the list cannot be exhaustive.

5.1Client side

The client must be aware of the possible security threats that can occur at his side. His computer should be configured according to the possible threats. For example, his computer should not send his e-mail address and always ask before accepting any cookies. An up-to-date version of anti-virus software should be installed that could be able to detect malicious codes. Similar security measures can be used to secure the client side.

5.2 Merchant side

At the merchant side the number of computers and applications is higher, thus, security is to be dealt with higher care. The first requirement is to install a properly configured operating system. There should e a proper access control mechanism to control unauthorized access of internal data. External access to the merchant's location should be protected with a proper firewall system[8]. Sensitive data should not be accessible through internet. Regular checks should be conducted to keep the merchant side safe. Other measures like physical locks, server room and fire measure systems cannot be left without consideration.

In the further sections, a formal security measure has been defined. To define the security measure, we use a security matrix with the place i.e. the client side or the merchant side, and the security objectives of the electronic business application in the rows and the columns.

To define the security measure for an electronic business application, certain formalizations have to be made. The set $S = \{C, I, A\}$ contains the three security objectives. Here C represents confidentiality; I represents Integrity, A represents availability. The set $P = \{C_{st}, M_{er}\}$ defines the place at which the security objective is considered. Here C_{st} defines the client side and M_{er} defines the merchant side. A security matrix $M_{\sec}$ can be defined as a function mapping a security objective and a place where at which the security objective is considered. This mapping would be a real number in the interval[0,1][7].

$$M_{\sec} = P \times S \rightarrow [0,1]$$

The next requirement for defining the Security measure of Electronic business Application (SEBA) is to introduce probabilities. Each entry in the security matrix $M_{\sec}$ is assigned a probability. The sum of all the probabilities has to be equal to 1. Since probability is a random phenomenon, the expected probability can be modeled with a function P_0 mapping each entry in $M_{\sec}$ to a real number in the interval [0,1].

$$P_0 : P \times S \rightarrow [0,1]$$

Security measure of Electronic business Application (SEBA) can be expected as

$$\omega(EBA) = \sum_{i \in P} \sum_{j \in S} P_0(i, j) * M_{sec}(i, j)$$

Here ω is called the Security measure of Electronic business Application (SEBA).

From the definition of the $M_{\sec}$ and ω, it is evident that $0 \le \omega(EBA) \le 1$.

While the application of this measure, let us consider the case when the probabilities are chosen equally, the Security measure of Electronic business Application (SEBA) can be computed as

$$\omega(EBA)_{equi} = \frac{1}{6} \times \sum_{i \in P} \sum_{j \in S} M_{\sec}(i, j)$$

6. DISCUSSION AND USE OF SECURITY MEASURE OF ELECTRONIC BUSINESS APPLICATION (SEBA)

This section will focus on the practical use of the Security measure of Electronic Business Application (SEBA).

6.1 Determination of the security matrix $M_{\sec}$

First of all, the security threats and measures have to e identified, then the measures have to be evaluated. For this, a real number between 0 and 1 is assigned to the corresponding entry of $M_{\sec}$. Example: $M_{\sec}(I, C_{st}) = 0$ means that no measures have been taken to guarantee the integrity of the data at the client side. $M_{\sec}(A, M_{er}) = 1$ means that at the merchants side, all relevant precautions to provide the availability of the application, have been met. Cases where more than one and less than all security measures have been implemented have been represented by values between 0 and 1.

The evaluation of the values for $M_{\sec}$ requires knowing all relevant security measures. But the measure questions are *what the security measures are* and *who carries out the evaluation*. A lot of research work has been done to focus on these two. In practice, this has to be done by someone familiar with the security measures at the continuous site. For practical purposes, it is practical to consider discrete values rather than continuous for the entries of $M_{\sec}$, e.g. to work only with the three values 0.1, 0.5, and 0.9 for a better result[7].

6.2 Determination of weights

The importance of the corresponding entries in $M_{\sec}$ define the value of different weights, i.e. the values represent how the estimator has deemed the relevance of a security objective at the corresponding place. Table 3 depicts an example where most weight is put on the confidentiality of the merchant side. For comparing the different applications, it is important to consider the same weights. A possible solution is to establish renowned standard weight sets for all internet shopping applications.

6.3 Interpretation of security measure (SEBA) ω

The security measure ω maps the security of an Electronic business Application to a real number in the interval [0,1]. Thus, ω can be considered as interpreting the percentage of necessary and implemented security measures. $\omega(EBA) =$

0 means that any of the necessary security measures have been adopted. $\omega(EBA)=1$ means that all the relevant security measures have been adopted but it can never be interpreted as the EBA is absolutely secure. The values lying in between can be interpreted analogously. Absolute security cannot be guaranteed as all security measures rely on their correct implementation and use.

After calculating ω, the Analysis of applications, their comparison and design can be done with the help of following guidelines:

Analysis The security measure ω maps the security of any application to a real number. Thus, the analysis of any application can be done easily with a simple rule for ω, i.e. the higher the value of ω the better.

Comparison After quantifying the security of different applications, the comparison can be done. For this, the following rules must be taken into account: (1) The same set of weights has to be used,(2) there should not be any significant difference in the evaluation of the security measure, (3) the value of ω alone is of almost of no use at all unless the evaluation process is overviewed. Thus, the tale of threats and security measures, weights, and values of $M_{\sec}$ should be available.

Design It is usually not possible to implement all the security measures at the same point in time during the implementation of an Electronic Business Application (EBA). Thus, the calculation of

ω at various points in time during the implementation can be used to monitor the progress in the system's security.

Consider an example of an imaginary bank ABC that provides online business. The users are able to do online banking. The application is working on client- server architecture. Here, the clients are the customers; the server side consists of one or more http, database, backup servers. The server side implements access control mechanisms in order to regulate the access to the database. During online banking, money can be withdrawn from ATM Machines using ATM cards, payments to other merchants can be made through debit/ credit card or online transfer. The TCP/IP connections between the browser and the HTTP server are protected using SSL (Secure Socket Layer Protocol). The advantage of using SSL is that it provides three goals-

Privacy- A casual (or determined) observer cannot understand the contents of a message transmitted over the internet.

Integrity- the contents of a message received by a client or merchant over the internet are not tempered and are original.

Authentication- Both the sender and the receiver can be sure of each other's identity [12].

Here we are not considering the details of SSL.

The processing of money transfer is done when the consumers possess valid certificates (implemented in their browser) and provide valid login id and password when accessing the HTTP server. Besides the 1st level of authentication provided through the use of a User ID and Internet Banking PIN, a 2nd level One-Time Password (OTP) generated by the bank is also required for internet banking. For stronger encryption, the customer's browser is 'fortified'.

Table 3. Security measures, $M_{\sec}$, and set of weights for abc bank.

	Confidentiality	Integrity	Availability
Customer	Browser fortification, user id, password	Browser fortification, security patches	-
Merchant	Encryption, Access control mechanism, firewall	Plausibility check, checksums, intrusion detection utilities	Backup servers

P_0	C	I	A
C_{st}	0.05	0.05	0.05
M_{er}	0.2	0.2	0.1

$M_{\sec}$	C	I	A
C_{st}	0.5	0.5	0.1
M_{er}	0.9	0.9	0.5

**These information were taken from several websites of banks available online. The banks did not give provide any information on personal visits to them.

ω (ABC_BANK) is derived in the following steps:

1. Firstly, the implemented security mechanisms are organized in Table 3 for the ABC_BANK.
2. In the next step, the security measures have to be evaluated to get $M_{\sec}(C_{st},A)=0.1$ which is shown as well in Table 3. We have used the 0.1, 0.5, 0.9 evaluation introduces earlier. $M_{\sec}(C_{st},A)=0.1$ since almost no security measures have been taken. For some places, where corresponding security measures fulfill the security objectives at the corresponding place to a certain amount, like (C_{st},C), (C_{st},I), (M_{er},A), the value of $M_{\sec}$ is 0.5. But additional security objectives are also needed. The remaining entries in $M_{\sec}$ are set to 0.9 as the corresponding measures are sufficient.
3. The last step is of calculation of ω. As per the weights assigned in Table 3, the value of ω (ABC_BANK) =0. 465.

The choice of the weights depends on the evaluator. In this discussion, we have tried to consider a neutral viewpoint. But, the customer can choose different weights than the merchant and get a different evaluated result.

For the same NOZAMA bookstore example, $\omega(EBA)_{equi}$ =0.56.

7. CONCLUSION AND FUTURE SCOPE

This paper gives an expectation of the security of the Electronic Business Application. The security matrix has been defined with places as the rows and the security objective as the columns. In the practical relevance of this work, there may be problems like there may be correlations in the set of objectives. Thus there is a need to examine this. Further work can deal with this problem.

8. REFERENCES

[1] Anuradha Sharma, Puneet Mishra, "Security requirements for e-business applications", proceedings of TIMES-2013, Alwar, 2013.

[2] Atul kahate, "Cryptography and Network Security", TMH, New Delhi, 2006, pp. 4-10.

[3] A Sengupta, C.Mazumdar, M.S.Barik, "E-commerce Security-A Lifecycle Approach", Sadhana, vol. 30, Parts 2&3, April/June 2005, pp. 119-140.

[4] C.P.Pfleeger, S.L.Pfleeger, D. Shah, "Security in Computing", Pearson Prentice Hall, 2009, pp.4-18.

[5] Matt Bishop, "Introduction to Computer Security", Pearson, 2011, pp. 4-10.

[6] Konstantin Knorr, Susanne Röhrig, "Security requirements of e-business processes", Volume 202 of IFIP Conference Proceedings, pages 73-86, Kluwer, 2001.

[7] Konstantin Knorr, Susanne Röhrig, "Security of Electronic Business Applications: Structure and Quantification", Proceedings of the first International Conference on Electronic Commerce and Web Technologies, pp 25-37, Springer-Verlag, London, 2000.

[8] William R. Cheswick and Steven M. Bellovin. *Firewalls and Internet Security —Repelling the Wily Hacker*. Professional Computing Series. Addison Wesley, 1994.

[9] Randy C. Marchany, Joseph G.Tront, "E-Commerce Security Issues", Proceedings of the 35th Hawaii International Conference on System Sciences – 2002.

[10] N.Smith, L.Ferreira, E. Mead, "E-Business Trends", Working Paper 2 of the E- Business and Transport Project for The National Transport Secretariat.

[11] Internet security systems, "Network and Host-Based Vulnerability Assessment", 1999, http:// www.iss.net.

[12] Hugh E.Williams, David Lane, "Web Database Applications with PHP and MySQL", 2004, O'Reilly.

[13] Anuradha Sharma, Puneet Misra, "E-Business Transaction Security: Changing Trends in Database Security- Critical Review", International Journal of Computer Engineering and Technology(IJCET), IAEME, Vol.4, Issue 6, Nov-Dec(2013), pp. 175-180.