

IMPLEMENTING SECURITY FRAMEWORK OF  
ELECTRONIC BUSINESS APPLICATION

HANNANI BINTI AMAN

MASTER OF SCIENCE  
UNIVERSITI PUTRA MALAYSIA

2004



IMPLEMENTING SECURITY FRAMEWORK  
OF  
ELECTRONIC BUSINESS  
APPLICATION

By  
HANNANI BINTI AMAN

Thesis is submitted to the School of Graduate Studies, University  
Putra Malaysia in Partial Fulfillment of the requirements for the  
Degree of Master of Science

November 2004

## **ABSTRACT**

Security is an essential issue in e-commerce. Lack of security knowledge exposed e-commerce customer to threat. Security threat such as viruses, Trojan and malicious software could put customer to danger. A study accessing user conceptions of web security has shown web users have mistakenly evaluated whether a connection is secure or not and vice versa even there knowledge of technology is high. Therefore, they need an assistant in determines which website is secure most.

This project is about security measurement tool of web based application focused on customer side. The measurement framework is based on Security Quantification of Electronic Business Application. The framework based on four (4) objectivities to be measured, which are Confidentiality, Integrity, Availability and Accountability. Development methodology of this project is Waterfall model. The product is stand-alone application which can be used anywhere at the customer side. The advantage of this tool is covers broad evaluation of files, using both external and internal measurement and PHP source code evaluation automatically.

Keywords: Metrics, Security Framework, E-Commerce

## ABSTRAK

Sekuriti merupakan elemen terpenting dalam satu aplikasi e-commerce. Kekurangan pengetahuan mengenai sekuriti boleh menyebabkan pengguna e-commerce terdedah kepada ancaman penggadam computer, virus dan Trojan. Satu kajian menunjukkan pengguna web telah tersilap menilai elemen sekuriti pada web dan rangkaian. Meskipun latarbelakang pengguna web ini adalah seorang yang celik Teknologi Maklumat. Apatah lagi yang tidak tahu menggunakan komputer. Oleh itu, bantuan mengenalpasti sekuriti di sesuatu laman web diperlukan oleh mana-mana pengguna web.

Projek ini mengenai alat bantu pengukuran sekuriti khusus kepada pengguna web. Rangka kerja pengukuran sekuriti berdasarkan Security Quantification pada Aplikasi Perniagaan secara Elektronik. Rangka kerja ini bercirikan 4 objektif iaitu Kesulitan (Confidentiality), Integriti (Integrity), Ketersediaan (Availability) dan Kebertanggungjawaban (Accountability). Metodologi pembangunan projek ini berlandaskan model Waterfall. Hasil alat bantu pengukuran sekuriti ialah aplikasi *stand-alone* di mana, ia boleh digunakan di mana sahaja pengguna web berada. Alat bantu pengukuran ini berupaya mengukur aplikasi web PHP yang mempunyai fail yg banyak dan kompleks secara automatik.

## **ACKNOWLEDGEMENTS**

Alhamdulillah, all praise to Allah for His guidance that enable me to complete this project paper – as a fulfillment of the requirement for the Degree of Master of Science in Science Computer at Faculty of Computer Science and Information Technology, University Putra Malaysia.

I would like to thank my supervisor, Assoc. Prof. Dr Abdul Azim Abdul Ghani for guiding me throughout my project paper. His guidance, advises and support during the whole period of the project paper is an important element in my completion of this paper.

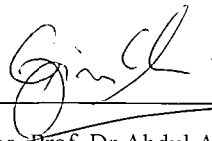
Millions thanks to Mak and Abah, and my family for their support and love from the beginning of my life until now.

My appreciation is to Rusmaini Miftah and Jazreena Jabar, who gave their best time, guiding me with PHP and Java problems.

Finally, I would like to thank the entire individuals that I failed to mention but contributed directly and indirectly during this project. Thanks for contribution and encouragement.

## APPROVAL SHEET

This thesis is submitted to the Senate of Universiti Putra Malaysia has been accepted as fulfillment of the requirements for the degree of Master of Science.



---

Assoe. Prof. Dr Abdul Azim Abdul Ghani  
Project Supervisor,  
FSKTM,  
Universiti Putra Malaysia  
November 2004

## **DECLARATION**

I hereby declare that the thesis is based on my original work except for quotations and citations, which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for other degree at UPM or other institutions. This thesis has been prepared by,

---

(HANNANI BINTI AMAN)

Date:

## TABLE OF CONTENTS

ABSTRACT	ii
ABSTRAK	iii
ACKNOWLEDGEMENTS	iv
APPROVAL	v
DECLARATION	vi
TABLE OF CONTENTS	vii
LIST OF TABLES	ix
LIST OF FIGURES	x
 CHAPTER 1	
INTRODUCTION	
1.1 Introduction	1
1.2 Problem Statement	2
1.3 Objective	2
1.4 Project Scope	3
1.5 Outline Of The Report	4
 CHAPTER 2	
LITERATURE REVIEW	
2.1 Security In E-Commerce	5
2.2 Security Element In Web Application	8
2.3 Measuring Security Quality	12
 CHAPTER 3	
METHODOLOGY	
3.1 Introduction	19
3.2 Process Development Step	20
3.2.1 Requirements Definition	21
3.2.1.1 Confidentiality Objective	25
3.2.1.2 Integrity Objective	28
3.2.1.3 Availability Objective	30
3.2.1.4 Accountability Objective	30
3.2.2 System Design	31
3.2.2.1 Logical Design	32
3.2.2.1.1 Scan Web Page Content	32
3.2.2.1.2 Method For Confidentiality Objectives	33
3.2.2.1.3 Method For Integrity Objective	35
3.2.2.1.4 Method For Availability Objective	35
3.2.2.1.5 Method For Accountability Objective	36
3.2.2.1.6 Method For Calculate Security	37



Quantification	
3.2.2.2 Interface Design	38
3.2.2.2.1 Main Interface	38
3.2.2.2.2 Accountability Objectives Checklist	40
3.2.2.2.3 Integrity Objectives Checklist	40
3.2.2.2.4 Error Message	41
3.2.3 Implementation	42
CHAPTER 4	
TESTING AND RESULTS	
4.1 Introduction	44
4.2 Testing And Results	44
CHAPTER 5	
DISCUSSION	
5.1 Discussion	57
5.2 Problem And Limitation	57
5.2.1 Security Element Selected	58
5.2.2 Weight Selected	58
5.2.3 Web Site Used	58
5.3 Advantages	59
5.4 Limitation Of Security Tool	59
5.5 Future Work	60
CHAPTER 6	
CONCLUSION	61
REFERENCES/ BIBLIOGRAPHY	62
APPENDICES	64

#### LIST OF TABLES

TABLE 1 : Some Security Threats And Measures In Electronic Business.....	17
TABLE 2 : Some Security Threats .....	21
TABLE 3 : Some Security Measure .....	22
TABLE 4 : Security Objectivity Measures.....	31

## LIST OF FIGURES

Figure 1 : Percentage of Types of Evidence Participants Used to evaluate a connection to all consumer.....	14
Figure 2 : Waterfall model.....	20
Figure 3 : Integrity Checklist.....	29
Figure 4 : Accountability checklist.....	30
Figure 5: Algorithm Scan Web Page Content.....	33
Figure 6 : Algorithm Measure Confidentiality Objective.....	34
Figure 7 : Algorithm Measure Integrity Objective.....	35
Figure 8 : Algorithm Measure Availability Objective.....	36
Figure 9 : Algorithm Measure Accountability Objective.....	37
Figure 10 : Algorithm Calculate Security Quantification.....	37
Figure 11 : Main interface.....	39
Figure 12: Accountability Objective interface.....	40
Figure 13 : Integrity checklist interface.....	41
Figure 14 : Error Message interface.....	42
Figure 15 : Error Message interface.....	42
Figure 16 : Interface of Security Measurement Tool.....	46
Figure 17 : File Chooser for input directory.....	47
Figure 18 : Directory Not Specified Error Message.....	47
Figure 19 : Output File Specified.....	48
Figure 20 : Output File Not Specified Error Message.....	48
Figure 21 : Integrity Checklist filled.....	49
Figure 22 : Accountability checklist filled.....	50
Figure 23 : Result display.....	51
Figure 24 : Accessing the XML Viewer.....	52
Figure 25 : XML Viewer Result.....	53

Figure 26 : JCreator viewer.....	54
Figure 27: Relationship between elements with XML.....	55
Figure 28 : Result of Security Quantification in XML format.....	55

## CHAPTER 1

### INTRODUCTION

#### 1.1 Introduction

Nowadays, e-commerce is viewed as an online shopping via the internet. E-commerce also known as paperless exchange of business information using electronic data interchange (EDI), email, electronic bulletin boards, fax transmission and electronic funds transfer. This definition refers to Internet shopping, online stock and bond transaction, the download and selling and business-to-business transactions. The purpose of e-commerce is all about using Internet to do business faster and better. It is about giving customers controlled access to your computer system and letting people serve themselves. E-commerce system use www as a medium to interact or attract with a millions of users worldwide. By using this web, consumer can purchase all kinds of goods and services that provided by this e-commerce according to their business.

Instead of e-commerce ease of use, consumer must not pass-by the security issue. In 1999, US Bankcorp was sued for deceptive practices (Randy and Joseph, 2002). The bank supplied a telemarketer, MemberWorks, with sensitive customer data such as name, phone number, bank account, credit card numbers, account balances and credit limits. MemberWorks used these customer lists to sell dental

plans, videogames and services. This shows that consumer must aware of current security issue. Threats happen will abuse to customer privacy. Easy downloading any files sometimes made consumer vulnerable to Denial of Services attack. Therefore consumer needs to have responsibility in gaining knowledge of basic security practice. This certainly helps ensuring confidence of business ability to secure and protect consumer information.

## 1.2 Problem Statement

To guarantee security in the e-commerce is the main success to protect the consumer's privacy or the security of the online transactions and gain trust. However, not all consumers have the capability to inspect the security level of each website that he/she wants to utilize or buy or use the online service. Gaining trust from consumers is time consuming. As we all know time is the treasure that most consumers do not have much; therefore, we need to develop a tool to assist consumers in gaining trust in each website he/she want to utilize [Konstantin and Susanne, 2000].



### 1.3 Objective

The objectives of this study are as below:

1. To implement the security quantification of Electronic Business Application by Susanne and Konstantin (2000) as a tool in Java language.
2. To analyze and design electronic business application in security aspect for client focus.

### 1.4 Project's Scope

Web development growth has resulted various web platform and variety of development software tools. The most recognizable and popular web development tools in develop e-commerce website are Java Server Page (JSP) from Sun Micro System, Active Server Pages (ASP) from Microsoft, Lotus Notes from Lotus and Hypertext Preprocessor (PHP.) Though they share the same functionalities, they do differ in syntax. Therefore, this project's scope is to measure e-commerce website which built with PHP script only.

The system specification used for this project is listed below:

#### Hardware

1. One personal computer with minimum of 32MB RAM and a Pentium Caleron processor with a speed of 199 MHz and a 512KB L2 Cache.

#### Software

1. J2SDK 1.4.1\_02
2. Sun Microsystem Java Development Kits consisting of Java Virtual Machine and API, J2SDK1.4.1\_01
3. A Java editor tools called JCreator, which is a freeware from Xinox Software.

#### 1.5 Outline of Thesis

The structure of this report is as follows. Chapter 1 presents an overview of the importance of security in e-commerce at the customer side to gain trust as well as the model that will be used. It also includes the problem statement, objectives and scope of project. In Chapter 2, we explain about the background of security quality in e-commerce and measures security element. Chapter 3 provides detail explanations on methodology used specifically on the measurements of each security objectives proposed. Finally, chapter 4 and 5 will presents and discuss the results obtained from this study security objectives proposed. Finally, chapter 4 and 5 will presents and discuss the results obtained from this study explanations on methodology used specifically on the measurements of each security objectives proposed. Finally, chapter 4 and 5 will presents and discuss the results obtained from this study.

## CHAPTER 2

### LITERATURE REVIEW

#### 2.1 Security in E-Commerce.

E-Commerce (electronic commerce) involves sharing business information, maintaining business relationship and conducting business transactions by means of telecommunication networks [Stefani and Xenos,2001]. The medium use is World Wide Web. It is for enabling consumer to purchase all kinds of good and services. It also describe as interaction between commercial organization and individual customer.

The e-commerce interaction falls into 2 categories: Business-to-Business (B2B) commerce and Business-to-Consumer (B2C) commerce [Stefani and Xenos,2001]. Other views Internet commerce in 4 categories: Business-to-business (B2B), Business-to-Consumer (B2C), Business-to-Public (B2P) and Public-to-Consumer (P2C). Business-to-business (B2B) category is if two companies establish a trade relation. Business-to-consumer (B2C) category will do recognize if a company and a consumer establish a trade relation. Business-to-Public (B2P) category falls in when a company and a public administration do business, and Public-to-Consumer (C2P) establish when a public administration does business with a consumer [Konstantin and Sussane,2001].

Basically, all categories are about trades in relationship using Information Technology (IT) support in accomplishing electronic transaction. An example of B2C commerce, a customer that willing to acquire a product, service has to interact with a vendor through a website on the Internet. Purchasing online will need some business practices as order online, payment using Credit Card, personal information and other transaction that are confidential and privacy. Therefore, transaction needs to be secure as for the parties involve believe and trust. For depth reviewing, scope of e-commerce emphasize on Business-to-Commerce (B2C).

Many security issues arise in each component of e-commerce. Component of e-commerce based on client server model has three components: server system, the network and client system [Marchany and Tront,2002]. While [Konstantin and Sussane,2000] views the component as merchant, consumer and transmission. The components basically are the same as merchant, which located in server system as script and html pages, and database business. Network transmits business activities from server system to customer at client system or vice versa.

E-commerce security issues deal with 2 issues: protecting the integrity of network and its internal system, and with accomplishing transaction security between business and customer. According to [Marchany and Tront,2002],

transaction security is the most critical focus because it depends on the organization's ability to ensure privacy, authenticity, integrity, availability and blocking of unwanted intrusions. These element leads to fundamental of security.

Security defines as measures and control that ensure confidentiality, integrity, availability and accountability of the information processed and stored by a computer [Valenti, Cuccharelli and Panti, 2002]. This reflect to e-commerce system, secure do the action of measuring and controlling consumer data, transaction, web content to ensure these characteristics. Mean while, [Stefani and Xenos,2001] identified 5 blocks of security which are confidentiality, authentication, access control, data integrity and user's accountability in securing Internet transaction. [Konstantin and Sussane,2000] pick the most important security objective of both author before; confidentiality, integrity and availability.

Within the security fundamental, threat can occur in many ways. But in here, threats will not be discussed. Many ways in preventing threat occurs will be present to emphasize the element to be measure. For avoid loss of confidentiality in transaction, some technique is used. These are cryptography, Secure Electronic Transaction (SET), cookies.

## 2.2 Security characteristics and measures

There are multiple security elements in web application based on their operation. A portal may use login element to configure the authorized user. An e-banking application may needs highly encryption method to ensure their user trust and have a transaction. All these security elements are described on some characteristics defined by security definition.

Stefani and Xenos (2001) present security as one of reliability characteristics. It aligns 5 sub-criteria to perform security characteristics, which are confidentiality, authentication, access control, data integrity and user's accountability.

(Araujo and Araujo,2003) state several security aspects should be consider in developing the security aspects of the technological framework for a commerce Web site The several security aspects align are privacy, confidentiality, availability, integrity, authentication and accountability(non-repudiation).

Security Quantification framework uses four (4) characteristics of security as security objectives. The security objectives are confidentiality, integrity, availability and accountability. Its view all security objectives to achieve security element in Electronic Business Application which need merchant, consumer and transmission to be secured.



The taxonomy of security services show the characteristics of security in an application. The characteristics are data confidentiality, traffic flow confidentiality, data integrity, authenticity, non-repudiation, guarantee of services, availability, audit and intrusion and boundary control (Irvine and Levin, 1999).

Confidentiality and integrity are the most important attribute in each definition given by different author. E-commerce important attribute to secure is transaction. Confidentiality means secrecy [Araujo and Araujo,2003]. It also describes when the states in which data are protected from unauthorized disclosure. When transaction is read or copied by someone not authorized to do so, the results is known as loss of confidentiality. Consumers will also loss confidence with the vendor if user profile and personal data, are disclosure to public without their knowledge.

Integrity means that the data has not been altered or destroyed which can be done accidentally or with malicious intent. It may be corrupted in insecure network. It also may corrupt by malicious intent such as Trojan, virus or malicious applet. [Araujo and Araujo,2003] define integrity as data that arrive at the recipient location should be exactly the same data as that they were sent. Then the information will be store on a Web server or on a cookie in a customer. Unauthorized parties also should not alter this information.

In ISO9126, functionality is defined as “a set of attributes that bear on the existence of a set function and their specified properties. The functions are those that satisfy stated or implies needs” (Valenti et.al., 2002). The ISO 9126 functionality quality factor could be sub-categorized into five sub-factors (Valenti et.al, 2002). They are suitability, accuracy, interoperability, compliance and security. Suitability here refers to fitness for purpose. The next sub factor is accuracy, is concerned with checking the degree of precision of calculated values. Interoperability sub factor deals with the attributes of software that bear on its ability to interact with specified systems. Compliance sub factor, refers to adherence in interact to specified systems. Finally, security sub factor refers to attributes of software that bear on its ability to prevent unauthorized access, whether accidentally or deliberate to programs and data.

All of these authors define characteristics of security quality in an application but neither described the security measures. Nalnees (2000) discuss the security measure in web application on the client-side. He classifies web application testing in two (2) categories as dynamic and static. Static testing involves manually inspecting the source code and automatically testing for dangerous constructs. While dynamic testing involves executing the web application to detect anomalous behavior on unexpected inputs. The security measure, which he described, is on dynamic testing.

The first security measure is cookie poisoning. Cookies are a general mechanism, which server-side connections (such as CGI scripts) can use to both store and retrieve information on the client side of the connection. It may be a simple application, which static in client computer forever or available in some period of time or it state in human unreadable or readable. This issue may open to any threat of confidentiality. Therefore, using non-persistent cookies with short duration of life in a secure tag and encrypted is the best measures practice.

The second security measure defined is Form Manipulation. It involves saving a web site's form and editing it offline. This is a technique, which only requires HTML knowledge to alter the form. To measures this issue, Nalneesh (2000) suggest performing referrer checking on server side. This will ensure that a given form reach from the page, which contain the hyperlink, which providing access to the form. Performed form input-length checks on the pages as well as the server to ensure its input integrity. Process and validate the form input values entered by the user is stricter. This ensure user to input the right type of input rather than malicious intent codes. Any critical user data cannot be use in hidden fields in the form.

The third security measure is bypassing intermediate forms in a multiple-form of set. A big form may divides into a few forms, which make user easy to use. But as malicious user, they can use this vulnerability to attack what they intent to do. Security measure that should be taken is to ensure the user progress

to the next form only after all the required information requested is provided. Performing referrer checking on the server side ensure the given pages contains the hyperlink providing access to the form.

The fourth security measure is session time out. A malicious user may able to hijack another user's session if session time out is too long. This action implication will lead to loss confidentiality and integrity of user information. The security measure that should take action is period of session timeout for the application evaluation.

For the static testing of codes is based on language used in web application. They are different in syntax shall make the testing applied only for certain application. Both dynamic and static testing security measure is based on security characteristics that define by who performed the test.

### 2.3 Security measurement and framework

A comparative study by Batya and friends (2002), in accessing user conceptions of web security has shown web users has mistakenly evaluated whether a connection is secure or not and vice versa. Community accessed in 3 categories which are a rural community in Maine, a suburban professional community in New Jersey and a highly-technology community in California. By interview session, participants asked to define a secure connection. Then actual