SECURE SYSTEM DEVELOPMENT WITH UMLSEC: APPLICATION TO A B2B SYSTEM

A dissertation submitted to the Faculty of Information Technology in partial fulfilment of the requirements for the degree Master of Science (Information Technology),

Universiti Utara Malaysia

By

Khairul Anwar bin Hj. Sedek

JABATAN HAL EHWAL AKADEMIK
(*Department of Academic Affairs*)
Universiti Utara Malaysia

PERAKUAN KERJA KERTAS PROJEK
(Certificate of Project Paper)

Saya, yang bertandatangan, memperakukan bahawa
(I, the undersigned, certify that)

KHAIRUL ANWAR BIN SEDEK

calon untuk Ijazah
(candidate for the degree of) **MSc. (IT)**

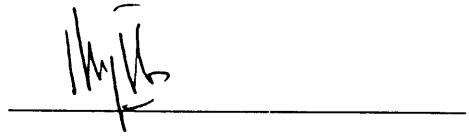
telah mengemukakan kertas projek yang bertajuk
(has presented his/her project paper of the following title)

SECURE SYSTEM DEVELOPMENT WITH UMLSec: APPLICATION TO B2B SYSTEM

seperti yang tercatat di muka surat tajuk dan kulit kertas projek
(as it appears on the title page and front cover of project paper)

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan.
(that the project paper acceptable in form and content, and that a satisfactory knowledge of the filed is covered by the project paper).

Nama Penyelia Utama
(Name of Main Supervisor): **ASSOC. PROF. NAZIB BIN NORDIN**

Tandatangan
(Signature) : 

Tarikh
(Date) : 24th October 2004

PERMISSION TO USE

In presenting this thesis in partial fulfilments of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the University Library may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor(s) or, in their absence by the Dean of the Graduate School. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to

Dean of Faculty of Information Technology
Universiti Utara Malaysia
06010 UUM Sintok
Kedah Darul Aman.

ABSTRACT

In recent years UML has become a de-facto language for modelling software functional requirements. However, non-functional requirements such as security requirement have less attention from system designer even though the business system is exposed to security risks. Embedding security measures during design phase will help developers to reduce security vulnerabilities. Using Furniture B2B Marketplace as a case study, this study attempts to determines system security requirements of B2B system to formally specified them using UMLSec as a specification language. The result shows that some security requirements of B2B system can be modelled using UMLSec. This study also provides recommendations to suit UMLSec with B2B security requirements.

ABSTRAK (BAHASA MELAYU)

Pada ketika ini UML telah menjada satu bahasa 'de-facto' untuk pemodelan keperluan fungsian perisian. Bagaimanapun, keperluan bukan fungsian seperti keperluan keselamatan kurang mendapat perhatian yang sewajarnya daripada pereka bentuk sistem walaupun system perniagaan sekarang ini lebih terdedah kepada risiko-risiko keselamatan. Langkah-langkah keselamatan yang dimasukkan ke dalam sesebuah pemodelan sisten akan membantu pembangun-pembangun sistem untuk mengurangkan kelemahan keselamatan. Dengan menggunakan Furniture B2B Marketplace, kajian ini cuba menentukan keperluan keselamatan sebuah sistem B2B dan kemudian mespesifikasikannya secara formal dengan menggunakan UMLSec sebagai bahasa spesifikasi. Hasil kajian ini menunjukkan bahawa beberapa keperluan keselamatan sistem B2B dapat dimodelkan dengan menggunakan UMLSec. Kajian ini juga membuat beberapa cadangan to menyesuaikan UMLSec dengan keperluan keselamatan sistem B2B.

ACKNOWLEGDEMENT

Alhamdulillah. This thesis is completed successfully with the support and guidance from many outstanding persons.

I would like to record special thanks to Assoc. Prof. Nazib bin Nordin, the supervisor of this project. He ensured that I was realistic in my goals and provides excellent advice for me. He also always ensures me to complete this project with excellent result.

I would like to thanks to all my lecturers from the first semester until the fourth semester that teach and advice me in this field. Thank you very much also to all the staff of Faculty of Information Technology for their supports.

Then, I would like to record very special thanks to my wife, Rozita Hamzah, my son, Amirul Haqim and my daughter, Nur Athirah for their loves and always inspired me to succeed. Thank you very much to my parents, brothers and sisters that always encourage and help me to further my study.

Thank you very much for all my fellow friends in Universiti Teknologi MARA (UiTM) Perlis that always encourage me to complete this thesis. They also provide very outstanding support in terms of time and technical advices as well as morale support.

TABLE OF CONTENTS

PERMISSION TO USE i

ABSTRACT ii

ABTRAK iii

ACKNOWLEDGEMENT iv

TABLE OF CONTENTS v

LIST OF FIGURES AND TABLES viii

CHAPTER 1: INTRODUCTION 1

1.1 The Business-to-business E-commerce 1
1.2 Problem Statement 2
1.3 Project Objectives 3
1.4 Project Scope 3
1.5 Significance of the Project 5
1.6 Organization of the Report 5

CHAPTER 2: LITERATURE REVIEW 7

2.1 Definitions of E-Commerce 7
2.2 B2B Security Guidelines 7
2.3 The Study on the Modelling of System Security 9
2.4 The Study on the Application of UMLSec 10
2.5 Conclusion 10

CHAPTER 3: UMLSec 12

3.1 Overview of UML 12
3.1.1 Use case diagram 12
3.1.2 Activity Diagram 13
3.1.3 Class Diagram 13
3.1.4 Statechart Diagram 14
3.1.5 Interaction Diagram 15
3.1.6 Implementation Diagram 16
3.2 UML Extension Mechanism 18
3.3 UMLSec 19
3.4 UMLSec Profile 20
3.5 Security Requirement Provided by UMLSec 21
3.5.1 Data Security 21
3.5.2 Secure Information Flow 22
3.5.3 Access Control 23
3.5.4 Fair Exchange 25
3.5.5 Audit Trail 26
3.6 Conclusion 27

CHAPTER 4: METHODOLOGY 28

4.1 Case Study 28
4.2 Security Analysis 29

4.3 Modelling the System 30
4.4 Prototyping 30
4.5 Analysis of Research Result 31
4.6 Conclusion 31

CHAPTER 5: SECURITY REQUIREMENT ANALYSIS 32

5.1 Security Definition 32
5.1.1 Information Security 32
5.1.2 Integrity 33
5.1.3 Privacy 33
5.1.4 Availability 33
5.1.5 Authentication 34
5.1.6 Authorization 34
5.2 Security Vulnerabilities 35
5.3 Identifying the Threats 37
5.4 Security Strategies 37
5.4.1 Least Privileges 38
5.4.2 Simplicity 38
5.4.3 Defence in Depth 39
5.4.4 Data Integrity and Confidentiality 40
5.4.5 Keep Audit Trails 40
5.4.6 Security Policy 41
5.5 Conclusion 42

CHAPTER 6: SECURITY SPECIFICATION FOR B2B 43

6.1 Specification of Access Control 43
6.1.1 Model Checking 49
6.1.2 Conclusion 49
6.2 Specification of Online Order 50
6.2.1 Model Checking 52
6.2.2 Conclusion 52
6.3 Specification of Secure Order Receiving 52
6.3.1 Model Checking 53
6.3.2 Conclusion 54
6.4 Secure Database 54
6.4.1 Model Checking 55
6.4.2 Conclusion 55
6.5 Secure Component Diagram 55
6.5.1 Model Checking 57
6.5.2 Conclusion 58
6.6 Secure Deployment Specification 58
6.6.1 Model Checking 59
6.6.2 Conclusion 59

CHAPTER 7: DEVELOPMENT OF PROTOTYPE 60

7.1 Access Control 61
7.2 Online Order 64
7.3 Order Approval 67
7.4 Order Receiving 68

7.5 Conclusion 69
CHAPTER 8: FINDINGS AND RECOMMENDATIONS FOR FUTURE WORKS 70
8.1 Research Result 70
8.2 Problem and Limitation 71
8.3 Recommendations for Future Study 71
8.4 Conclusion 72
BIBLIOGRAPHY 73

TABLES OF FIGURES AND TABLES

Figure 1-1: Project Scope 4

Figure 3-1: An Example of Use Case Diagram 13

Figure 3-2: Activity Diagram Notation 13

Figure 3-3: A Class Notation 14

Figure 3-4: An Example of Class Diagram 14

Figure 3-5: A Statechart Diagram for User Login State 15

Figure 3-6: A Sequence Diagram Example for user login process. 15

Figure 3-7: A Collaboration Diagram Example for User Login Process 16

Figure 3-8: An Example of Component Diagram for Security Controller. 18

Figure 3-9: A Deployment Diagram for a Web-based System 18

Figure 3-10: Security Specification of Class Diagram of Login Process 22

Figure 3-11: Component Diagram 22

Figure 3-12: Secure Deployment Diagram to Demonstrate Secure Link 23

Figure 3-13: Class Diagram of Access Control for a Banking Application 24

Figure 3-14: Statechart Diagram of Guard Object 25

Figure 3-15: Activity Diagram that Demonstrates Fair Exchange and Provable 26

Figure 6-1 Use case for Security Controller 44

Figure 6-2: Activity Diagram for Security Controller 45

Figure 6-3: Activity Diagram of Authorization 46

Figure 6-4: Class Diagram for Security Controller 47

Figure 6-5: Statechart Diagram for Login Trial 48

Figure 6-6: Statechart Diagram for Authentication 48

Figure 6-7: Statechart Diagram for Authorization of Access Control 48

Figure 6-8: Component Diagram of Access Control 48

Figure 6-9: Use Case Diagram Shows Fair Exchange between Buyer and Seller 50

Figure 6-10: Activity Diagram for Fair Exchange in Order 51

Figure 6-11: Data Security Specification of Customer Account 53

Figure 6-12: Class and Statechart Diagram for Secure Order Delivery Verification using <<no down flow>> Stereotype 53

Figure 6-13: Class Diagram of System Entity 55

Figure 6-14: Component Diagram Show Secure Links between Components. 57

Figure 6-15: Secure Deployment Diagram 59

Figure 7-1: Front-page of Furniture B2B Marketplace 60

Figure 7-2: Security alerts to notify user that the data will be transmitted over a secure connection 62

Figure 7-3: Security alerts that warn user to accept security certificate from a trusted certifying authority 62

Figure 7-4: Security Certificate information 62

Figure 7-5: Front-page of Furniture B2B Marketplace 63

Figure 7-6: Access Denied Page 64

Figure 7-7: Logged-in User 65

Figure 7-8: Interface for adding an item into shopping cart 65

Figure 7-9: Order Confirmation 66

Figure 7-10: Managing orders by buyer 66

Figure 7-11: Order confirmation that shows message that order has been sent for approval 67

Figure 7-12: List of order for approval 68

Figure 7-13: Approval Interface 68

Figure 7-14: Managing Sales Order 69

Table 1-1: Security Mechanism and Measures in different phases of E-Business Processes 5

Table 3-1: UMLSec Profile (Excerpt) 21

Table 5-1: User Permissions 35
Table 5-2: OWASP's Top Ten Web Application Vulnerabilities 2004 36
Table 5-3: Information Sensitivity Classification of a B2B System 41
Table 6-1: Component Classification by Data Secrecy and Integrity. 56
Table 6-2: Model Checking of Component Diagram 58
Table 8-1: Research Result 71

CHAPTER 1: INTRODUCTION

This chapter is an introduction to this report. It provides the general overview of B2B e-commerce, the problem statements, as well as the goals and scope. Finally the organization of the report is explained.

1.1 The Business-to-business E-commerce

The Internet is being used more and more for conducting commerce. This has made the Internet as a new infrastructure for a new commerce model known as e-commerce. One type of e-commerce is the business-to-business (B2B) system. B2B system involves two or more companies conducting business transactions through the Internet. According to Lucking-Reiley & Spulber (2001), the popular phrase of B2B e-commerce refers to the substitution of computer data processing and Internet communications for labour services in the production of economic transactions.

It is expected that the global transaction volumes in e-commerce will increase tremendously in the near future. According to the Gartner forecast (as cited by ITAA (2001), the global B2B e-commerce will grow to a total of $8.5 trillion in 2005, which is 189% increase from the year 1999 sale transactions of B2B e-commerce. In Malaysia, the online market is expected to reach RM9.4 billion by the end of 2005, with the B2B market expected to grow approximately RM3.9 billion in the same year (PricewaterhouseCoopers, 2004). With the rise of B2B e-commerce market, security has become an issue. Without properly designed secured system, the development of

The contents of the thesis is for internal user only

BIBLIOGRAPHY

Basin, D., Doser, J., & Lodderstedt, T. (2003, June 1-4). Model Driven Security for Process-Oriented Systems. *SACMAT'03.*

Blackburn & Chandramouli (n.d.). Model-based Approach to Security Test Automation. Retrieved from http://csrc.nist.gov/auto-func-test/publications/Issre_2002.pdf

CIECA. (2003). Security for Electronic B2B Transactions. Retrieved , , from http://www.cieca.com/documents/OpenDocuments/2003/SecurityforElectronicB2Btransactions-2003-05-19.pdf

Conallen, J. (2002). *Building Web Application with UML.* Boston: Pearson Education.

CSI/FBI (2003). *Computer Crime and Security Survey.* Retrieved from http://www.gocsi.com/forms/fbi/pdf.jhtml

Gartner. (2001). The Evolution of e-Business Security Requirements. Retrieved from http://www.verisign.com/resources/wp/authentication/eBusinessSecurity.pdf

Ge, X., Polack, F., & Laleau, R. (2004). Secure Databases: an Analysis of Clark-Wilson Model in a Database Environment. *CAISE 2004 Conference.*

Geer, D., Soo, K. J., & Jaquith, A. (2003). Information Security: Why the Future Belongs to the Quants. *IEEE Security & Privacy,* pp. 32-40.

Georg, G., Ray, I., & France, R. (2002). Using Aspect to Design a Secure System. *Proceeding of the 8th IEEE International Conference on Engineering of Complex Computer Systems.*

Goodchild, A., Herring, C., & Milosevic, Z. (2000, Jun). Business Contract for B2B. *Proceedings of the CAISE00 Workshop on Infrastructure for Dynamic Business-to-Business Service.*

Hoo, K., S., Jaquith, A., & Geer, D. (2003). The Security of Application, Reloaded. Retrieved from http://www.atstake.com/research/reports/acrobat/atstake_app_reloaded.pdf

Jaquith, A. (2002). The Security of Applications: Not All Are Created Equal. *Research Report.*

Jones, S., Wiliken, M., Morris, P., & Masera, M. (2000, December). Trust Requirements in E-Business. *Communication of The ACM, 43*(12), 81-87.

Juerjens, J. (2001, Nov). Secure java Development with UML. *I-Netsec01 – First International IFIP TC-11 WG11.4 Working Conference on Network Security.*

Juerjens, J. (2002a). UMLsec: Presenting the Profile. *Sixth Annual Workshop On Distributed Objects and Components Security (DOCsec2002).*

Juerjens, J. (2002b). Using UMLsec and Goal Trees for Secure Systems Development. *Proceedings of the 2002 ACM symposium on Applied computing*, pp. 1026 – 1030.

Juerjens, J. (2002c). Secure Systems Development with UML: Application to Telemedicine. *International Conference on Telemedicine (ICT2002), Regensburg.*

Knorr, K., & Rohrig, S. (2001, Oct 3-5). Security Requirements of E-Business Processes. *Proceedings of the First IFIP Conference on E-Commerce, E-Business, and E-Government (I3E)*, pp. 73-86.

Lodderstedt, T., Basin, D., & Doser, J. (2003). SecureUML: A UML-Based Modeling Language for Model-Driven Security. *8th ACM Symposium on Access Control Models and Technologies.*

Lucking-Reily, D., & Spulber, D. F. (2001, Winter). Business-to-Business Electronic Commerce. *Journal of Economic Perspectives, 15*(1), 55-68.

NIST (2001). Engineering Principles for Information Technology Security (A Baseline for Achieving Security). Retrieved from http://csrc.nist.gov/publications/nistpubs/800-27/sp800-27.pdf

NIST. (1996). General Accepted Principles and Practices for Securing Information Technology Systems. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

NIST. (2003). Security Considerations in the Information System Development Life Cycle. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-64/nist-sp800-64.pdf

OWASP (2002). A Guide to Building Secure Web Applications: The Open Web Application Security Project.

OWASP (2003). The Top Ten Critical Web Application Security Vulnerabilities.

OWASP (2004). The Top Ten Critical Web Application Security Vulnerabilities: 2004 Updates.

Probert, R. L., & Sawma, V. (2003, March). E-Commerce Security: Raising Awareness of Issues bu Adapting the NIST IT Security Services Model to E-Business System. *The 16th Annual Conference of The Federal Information Systems Security Educators' Association.*

Rob, P. & Coronel, C. (2004). *Database System: Design, Implementation, & Management, 6th Edition,* Course Technology. Boston.

Rohrig, S., & Knorr, K. (2000). Towards a Secure Web-based Health Care Application. *Proceeding of The 8th European Conference on Information System (ECIS).*

Thuiraisingham, B. (2000). *Wed Data Management and Electronic Commerce* (2nd ed.). Florida: CRC Press.

Tian, Z., & Chung, J. Y. (1999, May). Business-to-Business e-Commerce with Open Buying on the Internet. *IBM Institute for Advanced Commerce Technical Report*.