A SECURITY REQUIREMENT QUALITY MEASUREMENT MODEL FOR REDUCING E-COMMERCE SECURITY RISK

Sen-Tarng Lai

Dep. of Information Technology and Management, Shih Chien University,
Taipei, Taiwan

ABSTRACT

E-commerce is an important business transaction system in the network age. However, the network intrusion, malicious users, virus attack and system security vulnerabilities have continued to threaten the operation of the e-commerce, making e-commerce security encounter serious test. In order to avoid system security flaw and defect caused user great loss, how to reduce e-commerce security risk has become a topic worthy of further exploration. In this paper, the critical security requirement for the e-commerce system is investigated and deduced the compliance, availability and manageability quality characteristics for e-commerce software security requirement. Applying the quantified quality characteristics and proposes a Security Requirement Quality Measurement (SRQM) model. Based on SRQM model, the paper develops a Security Requirement Quality Improvement (SRQI) procedure to identify problem and defect of security requirement quality. And assist in timely to adjust and revise the defects of security requirement quality, enhance the e-commerce security effectively.

KEYWORDS

E-commerce; security requirement; Security Vulnerability; quality measurement model; SRQI

1. INTRODUCTION

In the age of digital and network, every high efficiency and high profit activity has to combine with internet. Business behaviors and activities always are the pioneer for getting high efficiency and high profit. Therefore, each business behaviors and activities have to adjust for integrating with internet. Based on the internet, business extension and promotion behaviors and activities general are called the Electronic Commerce (E-commerce) [3]. According to research organization eMarketer investigation data, e-commerce sales amount topped $1 Trillion for first time in 2012, and estimate e-commerce sales amount will grow up to $1.3 Trillion in 2013 [18]. By the way, Asia pacific area will over North America. Enterprise transaction behaviors can not change for adapting the market trend. It will not be able to meet customer requirements, causes a substantial profit recession and final be eliminated by the times. However, in the digital and internet age, information security issue has become a serious problem for computer and network environment. Network intrusion and system vulnerability are continuous threat software system normal operation [5, 8, 13, 14, 17].

In business behaviour and activity, e-commerce integrates with network advantage to improve many profits. However, e-commerce also implicit several hurry improvable problems and defects, for example operation efficiency, network communication security, software security, and

DOI : 10.5121/ijsea.2014.5103

manageability for change environment. It concerns many factors and the major impact is transaction security for enterprise, organization and stakeholder. E-commerce security is an important and worthily be studied issue. Security vulnerability and defect of e-commerce are almost discovered by abnormal situations. Until system appears the evens of instruction and information loose, then security vulnerability and defects of e-commerce be detected. In this time, organization loss and client impaction are hardly estimated and expected. And, the follow repair operation and improvement procedure also hardly resolve it. Security requirement is more important than security protection and event detection because paying attention to security requirement in the early stages of the software life cycle potentially saves more cost and effect [11]. For this, the paper discusses the security of transaction activities to integrate efficiently e-commerce security requirement. Before e-commerce system development, investigate and identify the major security issues and based on software security requirement quality to enhance software security of e-commerce.

Software is a kernel of e-commerce system. E-commerce software must adapt complex network environment and changeable hardware architecture, also needs to handle e-commerce operations to meet the requirements that proposed by the organization and client. For accomplishing the enterprise or organization sustainable development target, e-commerce software should have the features of continuous improvement, high extensibility, high integrity and high security. 75% of system attacks occur at the application layer and bypass traditional firewalls [15]. It means that software security has become the most important topic for business activities and behaviours. Security of e-commerce transaction becomes a critical issue and should be concerned. In this paper, security issues of e-commerce are discussed and the critical quality of e-commerce security requirement is surveyed. A Security Requirement Quality Measurement (SRQM) model is proposed to assist identify security requirement quality problem and defect. Based on SRQM model, the paper drafts a Security Requirement Quality Improvement (SRQI) procedure to improve continuously security requirement quality. In Section two, the importance and impact of e-commerce security is surveyed and described. In Section three, critical quality characteristics of security requirement is discussed. In Section four, proposes a SRQM model and based on SRQM model drafts the SRQI procedure. In Section five, the advantages and contributions of the paper are described.

2. E-COMMERCE SECURITY ISSUES AND SECURITY REQUIREMENT

Compliance and necessary security requirement is critical item to reduce e-commerce security risk.

2.1. E-commerce Security Issues

Internet changes the e-business activities for the emerging and offers many advantages. However, it also brings unpredictable security crisis. According to CERT/CC latest statistics data show that from 2005 to third quarter of 2008 analysis of software vulnerabilities total 27,346 cases [19] (shown in Table 1). More security vulnerabilities of information system cause the more serious security crisis. There are many international groups and organizations (SANS (security training, certification and research institutions), OWASP (Open Web Application software security program, Open Web Application Security Project) very concern the Web App security. They routinely published the key of Web App security vulnerabilities and defects: SANS Top-20 Security Risks [20] with the OWASP Top 10 security vulnerabilities [21], to help reduce Web App security risks. Security vulnerability of software system causes the enterprise loss and crisis which is hard to expect and evaluate. In order to avoid caused the serious loss of software security vulnerability, in e-commerce system development process, the issues of security vulnerability should be concerned [1, 9].

Table 1. 2005~2008 Q3 software vulnerabilities statistics data

Years	Volumes
2005	5,990
2006	8,064
2007	7,234
Q1-Q3, 2008	6,058
Summary	27,346

*Data source: CERT/CC

All e-commerce activities always involve customer personal data and transaction information. The critical data and information become secret worry of e-commerce. According to 104 market research center investigated result for network transaction security and impact, discovery 84% people concerned personal data may be stolen (shown as Fig. 1) [22]. And, 42% people occurred personal data lost or happened fraud event [22]. In recently, personal data lost and transaction security issues occurred frequently. In 2011, hacker intruded into PlayStation Network of Sony Corporation Japan, 77,000 thousands PS3 and Qriocity music on demand service customer personal data were stolen [23]. Therefore, famous corporation and organization very concerned on information security and used all approaches to defense hacker intrusion and protect customer personal data.

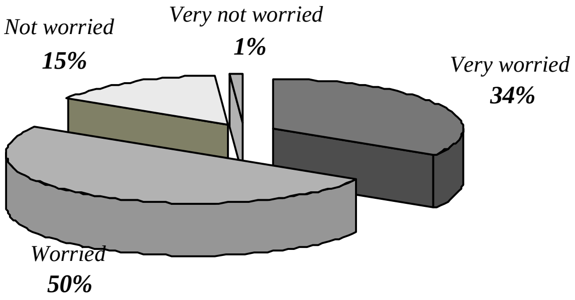

Figure1. In network transaction, 84% people concerned personal data been stolen
*Data source: 104 market research center

2.2 E-commerce Security Requirement

Business activities and transaction behaviors by network is general called e-commerce. Activities and behaviors of e-commerce may involve personal data and transaction content. The important information has become critical issue of e-commerce security. Holcombe think each e-commerce system must satisfy four indivisible requirements [10]:

- Privacy: In the information exchange process, e-commerce system should avoid unauthorized personnel to contact or handle the personal data.
- Integrity: In the information exchange process, e-commerce system should ensure the information can not be changed or revised to assure e-commerce information integrity.
- Authentication: Information sender or receiver must be able to certify their identity to each other.

- Non-repudiation: Any e-commerce transactions must be able to certify and record buyers and sellers have actually received each other to exchange information, in order to achieve non-repudiation.

E-commerce security requirement also need consider the vulnerability defence capability. Security requirement of e-commerce has to cover privacy, integrity, authentication, non-repudiation and vulnerability defence (shown as Figure 2).

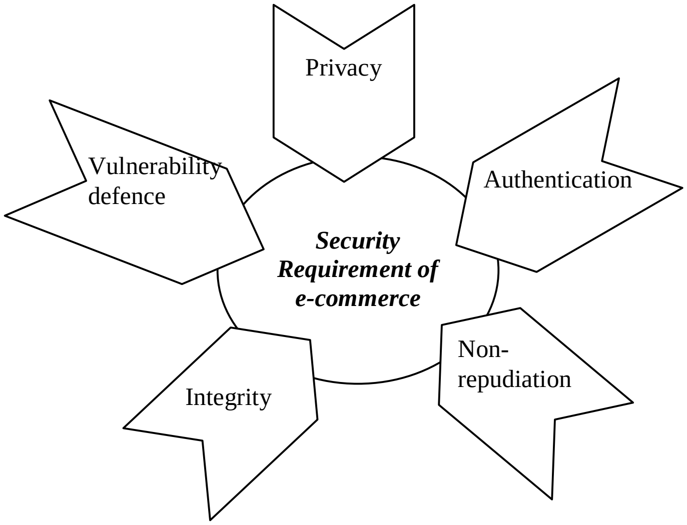

Figure 2. Four indivisible requirements and vulnerability defense

2.3 Critical Security Requirement of E-commerce

In order to satisfy four indivisible security requirements and vulnerability defense capability, e-commerce should have three ways software security requirements (shown as Figure 3) as follows:

(1) Customer personal data security: Personal data is necessary item to make e-commerce be able to normal operation. Customer provides personal data that is basic condition to create trust each other. E-commerce transactions always need customer critical personal data. Therefore, how to suitably collect, handle and use personal data and protect personal data is an important mission. E-commerce software security must provide a perfect personal data protection mechanism. So customer can unconcernedly conduct the transaction activity in high security e-commerce environment.

(2) E-commerce system operation security: Network environment is an important advantage and facility for the e-commerce system. The Internet is completely no limitation for regional, national and time. Therefore, anytime anywhere, e-commerce can handle a variety of transactions with high convenience. However, cyber crime is increased continuously. Many new crime skills can quickly intrude e-commerce system to steal customer personal data and critical transaction record in any time. Some skills can steal the transmission data in network environment to cause customer, organization and enterprise lost in spirit and financial. Security requirement of e-commerce has to propose a perfect security prevention mechanism to create the trust of the buyer and seller transaction behaviors. So customer and organization can conduct every transaction activities in high security e-commerce environment.

(3) E-commerce transaction security: Each transaction activity has to be jointly recognized by the buyer and seller. After transactions accomplished, transaction activity must clearly and completely record for assuring transaction behaviour security and avoiding future disputes. So, transaction behaviour should build a standard operation procedure (SOP) and provide a complete and reliable transaction behaviour logged mechanism to reach e-commerce transaction behaviour non-repudiation.

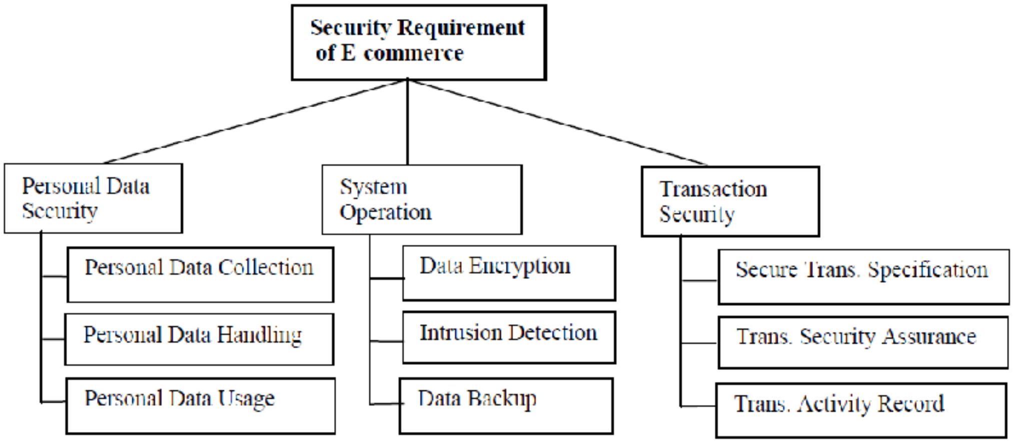

Figure 3. E-commerce security requirement frame

3. CRITICAL SECURITY REQUIREMENT QUALITY FACTOR

High quality software security requirement should have three critical quality characteristics which includes security requirement compliance, requirement availability and requirement manageability. Discuss three critical quality characteristics and describe the related quality factors as follows:

(1) Security requirement compliance: E-commerce has many secure issues must be deeply concerned. In order to assure e-commerce has the capability to handle security event, security requirement should cover and specify the critical secure issues. Security requirement compliance should consider three security requirement items:

- Personal data security: It is necessary to plan a perfect management mechanism for collecting, handling and using the personal data of e-commerce stakeholder [12]. In the information exchange process, e-commerce system should avoid unauthorized personnel to contact or handle the personal data.
- System operation security: In e-commerce operation process, e-commerce is unable to completely avoid secure threat. Therefore, for the transmission data must has security encryption measures and plan an intrusion detect mechanism to prevent the intrusion of hacker and malicious user. In addition, e-commerce should provide a integrate data backup procedure for handling the abnormal or exception events.
- Transaction activity security: Transaction activities are the basic function of e-commerce. For assuring the transaction activities security, e-commerce should plan a secure transaction specification for assuring each time transaction security. Each transaction activity must able to concretely prove and record both the buyer and seller exchange information to reach non-repudiation.

(2) Security requirement availability: Security requirement is the basis of the follow-up secure software development phase, phase secure document verification, and secure software validation. Security requirement should have high availability that includes security requirement extensibility, phase documents verification and product validation capability.

- Product extensibility: Documents of security requirement should have clearly, completeness, consistency and readability characteristics. The quality characteristics not only are necessary factors for extending to secure software follow-up development phase, also are necessary conditions for assuring secure software development quality.
- Verification and Validation capability: Security requirement should have the verification and validation capability to assist phase secure document inspection and product secure testing. It is critical characteristic to determine accomplishment degree of security requirement.

(3) Security requirement manageability: In software development process, project always cannot avoid requirement change. For this, security requirement must have manageability to cope with a wide variety of security requirement change. Manageability of security requirement should has low complexity, version control and traceability characteristics.

- Low complexity: security requirement items should effectively reduce the inter relation complexity and size complexity. Low complexity security requirement items can be quickly modified and adjusted to meet security requirement items change.
- Version control: For handling change requests, security requirement should has version control capability. Complete record requirement items change reason, contents, date and responsible person, and difference between versions. Requirement change record is critical information to identify and trace change problem and defect.
- Traceability: Security documents of each development phase must have cross-reference relationship to handle security requirement change requests. Traceability is based on documents cross-reference relationship that can assist correct and complete security requirement revision, and revised secure assurance activities.

4. SRQM MODEL AND PROCESS IMPROVEMENT PROCEDURE

In this section, a SRQM model is proposed, and based on the SRQM model establishes a security requirement process improvement procedure.

4.1 SRQM Model

Single factor or measurement can only measure or evaluate the specific attribute item. In order to effectively monitor and assess the quality characteristic problems and defects, individual factor or measurement should to make the appropriate combination [4, 6, 7]. Two kind of metric combination models are Linear Combination Model (LCM for short) [2, 4, 6] and Non-Linear Combination Model (NLCM for short) [2, 4, 16]. NLCM has higher accuracy measurement than LCM. However, LCM has high flexibility, more extensible and easy formulation than NLCM. For this, in this paper, LCM is applied to security requirement quality measurement. The different security requirement activities have different quality metrics be shown. Therefore, before using the linear combination model, the quality factors must be collected and normalized. Refer to predefined weight values and four combination formulas, basic layer quality factors can be combined into three quality measurements. Finally, the formula combines three critical quality measurements into an indicator of software security requirement quality measurement. Four formulas described as follows:

(1) Security Requirement Compliance Measurement (SRCM) is combined with Personal Data Security, System Operation Security and Transaction Security three quality characteristics. SRCM generation steps describes as follows:

Step 1: Personal Data Security (PDS) should measure by the primitive factors of personal data collection, handling and usage management system.

Step 2: System Operation Security (SOS) should measure by the primitive factors for security encryption measures, an intrusion detect mechanism and data backup procedure.

Step 3: Transaction Security (TS): should measure by the primitive factors of a secure transaction guide and non-repudiation system.

Step 4: Combine with personal data security, system operation security and transaction security metrics into the SRCM. The formula is shown as equation (1):

SRCM: Security Requirement Compliance Measurement

PDS: Personal data Security	*W_1: Weight of PDS*
SOS: System Operation Security	*W_2: Weight of SOS*
TS: Transaction Security	*W_3: Weight of SC*

$$SRCM= W_1*PIS + W_2* SOS + W_3* TS \qquad W_1 + W_2+ W_3=1 \qquad (1)$$

(2) Security Requirement Availability Measurement (SRAM) is combined with requirement document basic quality and requirement item verification and validation quality. SRAM generation steps describes as follows:

Step 1: Requirement Document Basic Quality (RDBQ) should measure by clarity, completeness, consistency and readability basic factors of security requirement documents.

Step 2: Requirement Items Verification and Validation Capability (RIVVC) should measure by inspection check lists planning quality and security test cases design quality.

Step 3: Combining with RDBQ and RIVVC into SRAM. The formula is shown as Equation (2):

SRAM: Security Requirement Availability Measurement

RDBQ: Requirement Document Basic Quality	*W_1: Weight of RDBQ*
RIVVQ: Requirement Items V&V Capability	*W_2: Weight of RIVVC*

$$SRAM= W_1*RDBQ + W_2* RIVVC \qquad W_1 + W_2=1 \qquad (2)$$

(3) Security Requirement Manageability Measurement (SRMM) is combined with requirement item complexity, version control and traceability quantified quality characteristics. SRMM generation steps describes as follows:

Step 1: Requirement Item Complexity (RIC) should measure by item inter relations and item size two basic quality factors.

Step 2: Requirement Item Version Control (RIVC) should measure by item change control and item version control two capabilities basic quality factors.

Step 3: Requirement Item Traceability (RIT) should measure by two basic quality factors of items cross-reference table and item and phase documents cross-reference table.

Step 4: Combine RIC, RIVC and RIT quantified quality characteristics into a SR Manageability Measurement (SRCM). The formula is shown as Equation (3):

SRCM: Security Requirement Manageability Measurement

RIC: Requirement Item Complexity	*W_1: Weight of RIC*
RIVC: Requirement Item Version Control	*W_2: Weight of RIVC*
RIT: Requirement Item Traceability	*W_3: Weight of RIT*

$$SRMM= W_1*RIC + W_2* RIVC + W_3* RIT \qquad W_1 + W_2 + W_3 =1 \qquad (3)$$

Finally, combine SRCM, SRAM and SRMM three measurements into an indicator of SRQM. The formula is shown as Equation (4):

ISRQM: Indicator of SRQM
SRCM: Security Requirement Compliance Measurement W_{cm}*: Weight of SRCM*
SRAM: Security Requirement Availability Measurement W_{am}*:Weight of SRAM*
SRMM: Security Requirement Manageability Measurement W_{mm}*:Weight of SRCM*

$$ISRQM = W_{cm} * SRCM + W_{am} * SRAM + W_{mm} * SRMM$$

$$W_{cm} + W_{am} + W_{mm} = 1 \qquad (4)$$

The quality measurement model is constructed by three layer combination formula. In first layer, eight group basic quality factors are combined into eight critical quality characteristics. In second layer, eight critical quality characteristics are combined into security requirement compliance, availability and manageability measurements. In third layer, compliance, availability and manageability measurements are combined into a SRQM indicator. With several quantified quality factors, combined into 8 quality metrics and 3 high level quality measurements, and an indicator of SRQM is generated finally. Indicator of SQRM is a basis for determining critical quality of software security requirement. Three layer quantified quality combination process is called the Software Security Requirement Quality Measurement (SRQM) model. The architecture of SRQM model is shown in Figure 4.

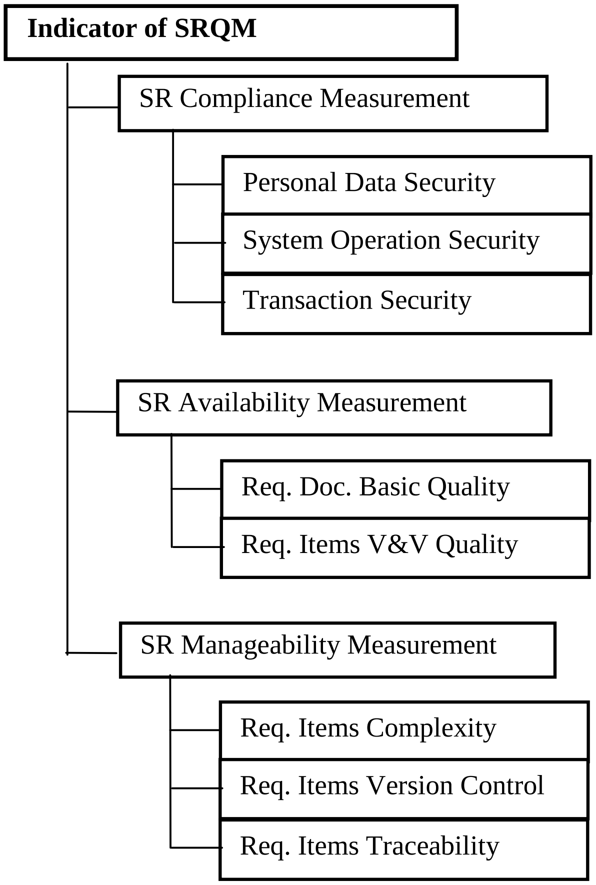

Figure 4. Architecture of SRQM model

4.2 Security Requirement Process Improvement Procedure

PDCA model is an approach for the control and continuous improvement of processes and products. In this paper, based SRQM model, defines a SRQI procedure. SRQI procedure is divided into four major phases that include security requirement drafting phase, measurement phase, identification phase and revision phase. The detailed operation of SRQI procedure (shown as Figure 5) describes as follows:

(1) Drafting phase: In the e-commerce system software security requirement drafting phase, the Holcombe's 4 necessary security requirements and the OWASP top 10 vulnerabilities are the basis to draw up the software security requirement of e-commerce.

(2) Measurement phase: In first layer, collecting, quantifying and combining the basic quality factors to generate some major quality characteristics. In second layer, combining the major quality characteristics to generate three critical quality measurements. In third layer, combining high layer quality measurements can generate the indicator of SRQM. The quantified quality data can help identify security requirement defect or problem of security requirement definition and items.

(3) Identification phase: Based on security requirement quality baseline, security requirement defect and problem can be identified by the rule-based approach. The rule-based identification approach is described as follows:

- If defect belong to Security Requirement Compliance Measurement, then the basic security requirement compliance quality factors that includes personal data security, system operation security or transaction security should be inspected. And according to inspection report, a security requirement compliance revision measure should be proposed.
- If defect belong to security requirement Availability Measurement, then the basic security requirement availability quality factors that includes requirement document basic quality or requirement items verification and validation capability should be detected. And according to detection report, a security requirement availability revision measure should be proposed.
- If defect belong to security requirement Manageability Measurement, then the basic security requirement manageability quality factors that includes requirement item complexity, version control and traceability should be detected. And according to detection report, a security requirement manageability revision measure should be proposed.

(4) Revision phase: Any type revision have to record revised items to check improvement effect. However, accomplished major revision, security requirement must re-measure the SRQM to assure improvement effect.

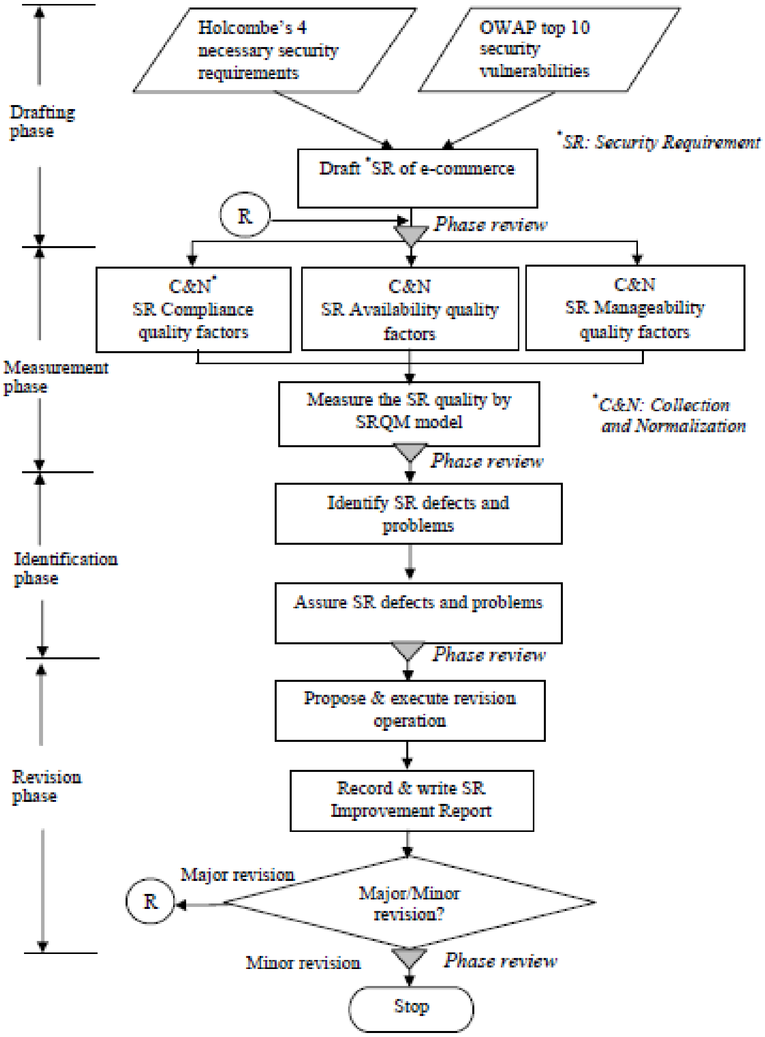
Drafting phase
Holcombe's 4 necessary security requirements
OWAP top 10 security vulnerabilities
*SR: Security Requirement
Draft *SR of e-commerce
R
Phase review
Measurement phase
C&N* SR Compliance quality factors
C&N SR Availability quality factors
C&N SR Manageability quality factors
Measure the SR quality by SRQM model
*C&N: Collection and Normalization
Phase review
Identification phase
Identify SR defects and problems
Assure SR defects and problems
Phase review
Revision phase
Propose & execute revision operation
Record & write SR Improvement Report
Major revision
R
Major/Minor revision?
Minor revision
Phase review
Stop

Figure 5. SRQI operation flowchart

5. Conclusion

E-commerce system must have the responsibility to protect customer important privacy which includes personal data and transaction information. However, the network intrusion, malicious users, virus attack and system security vulnerabilities have continued to threaten the operation of the e-commerce, making e-commerce security encounter serious test. E-commerce system generally uses security testing and vulnerability repair to reduce security risk. Security requirement is more important than security testing and vulnerability repair because paying attention to security requirement in the early phase of the software life cycle can saves more cost and effect. In this paper, survey importance and critical items of security requirement and discuss major security requirement quality factors. Security requirement is a basis of secure software development phase verification and product validation. Security requirement critical quality is major factors to affect the success or failure of secure software system. In order to increase E-commerce security, security requirement quantified quality and improvement procedure are necessary steps. The paper proposes a Software Security Requirement Quality Measurement (SRQM) model to help identify security requirement problem and defect. Based on SRQM model, a SRQI procedure is designed for continuously enhancing e-commerce security. The SRQM model owns three advantages describe as follows:

- Based on LCM and formulas, security requirement defects can be identified timely.
- SRQM Model formula has clear, simple and high flexibility.
- SRQM model is a basis of SRQI procedure.

ACKNOWLEDGEMENTS

This research was supported by the Shih Chien University 2013 research project funds (Project No.: 102-05-04005)

REFERENCES

[1] Apvrille, A. and Pourzandi, M. (2005), “Secure Software Development by Example,” IEEE Security & Privacy, vol. 3, no. 4, 2005, pp. 10-17.

[2] Boehm, B. W. (1981), Software Engineering Economics, Prentice-Hall, New Jersey.

[3] Chaffey, D. (2005) E-Business and E-Commerce, 2nd , Prentice Hall.

[4] Conte , S. D. , Dunsmore, H. E. and Shen, V. Y.(1986), Software Engineering Metrics and Models,Benjamin/Cummings, Menlo Park.

[5] Davis, N., Humphrey, W., Redwine, Jr. S. T., Zibulski, G. and McGraw, G. (2004), “Processes for Producing Secure Software,” IEEE Security & Privacy, vol. 2, no. 3, 2004, pp. 18-25.

[6] Fenton, N. E. (1991), Software Metrics - A Rigorous Approach, Chapman & Hall.

[7] Galin, Daniel, (2004), Software Quality Assurance, Addison-Wesley.

[8] Halaweh, M. and Fidler, C. (2008), “Security Perception in E-commerce: Conflict between Customer and Organizational Perspectives”, Proceedings of the International Conference on Computer Science and Information Technology, pp. 443 – 449.

[9] Hall, A. and Chapman, R. (2002), “Correctness by Construction: Developing a Commercial Secure System,“ IEEE Software, vol. 19, no. 1, pp.18-25.

[10] Holcombe, C. (2007), Advanced Guide to eCommerce, LitLangs Publishing.

[11] Hope, P. and White, P. (2007), Software Security Requirements, Cigital, Inc.

[12] Huang, C.-C. , Farn, K.-J and Lin,Y.-S (2011) ”A Study on Information Security Management with Personal Data Protection”, 2011 IEEE 17th International Conference on Parallel and Distributed Systems, pp. 624-630.

[13] McGraw, G. (2006), Software Security – Building Security In, Addison-Wesley.

[14] McGraw, G. (2004), “Software Security,” IEEE Security and Privacy, vol. 2, no.2, pp. 80–83.

[15] Lanowitz, T., (2005), Now Is the Time for Security at the Application Level, 2005 Gartner, Inc.

[16] Lai, S. T. and Yang, C. C. (1988), “A Software Metric Combination Model for Software Reuse,” Proc. of 1998 Asia-Pacific Software Engineering Conference (APSEC’98), pp. 70-77.

[17] Viega, J. and McGraw, G. (2004), Building Secure Software, Addison-Wesley.

[18] eMarketer (2013), “Ecommerce Sales Topped $1 Trillion for First Time in 2012”, http://www.emarketer.com/Article/Ecommerce-Sales-Topped-1-Trillion-First-Time-2012/1009649#D1VJbC8yL6W4Zogk.99 (2013/2)

[19] CERT/CC (2008), http://www.cert.org/stats/cert_stats.html） (2008/12)

[20] The Top Cyber Security Risks (2010), (http://www.sans.org/top-cyber-security-risks/) (2010/5)

[21] OWASP Top 10 (2013), (https://www.owasp.org/index.php/Top_10_2013-Top_10) (2013/7)

[22] Gun, J. X. (2010), Eighty percent people, fearing online shopping experience “fraud” , 104survey.com, 2010. (in Chinese) (http://www.104survey.com/faces/newportal/viewPointCtx.xhtml;jsessionid=70AFB339F7F99D2503FBD40CBF199DD4.svyweb202?researchId=254) (2010/4)

[23] Pepitone, J. (2011), Massive hack blows crater in Sony brand, staff reporter CNNMoney Tech., 2011. (http://money.cnn.com/2011/05/10/technology/sony_hack_fallout/index.htm) (2011/5)

Author

Sen-Tarng Lai was born in Taiwan in 1959. He received his BS from Soochow University, Taiwan in 1982, master from National Chiao Tung University, Taiwan in 1984 and PhD from National Taiwan University of Science and Technology, Taiwan in 1997. His research interests include software security, software project management, and software quality. He is currently an assistant professor in the Department of Information Technology and Management at Shin Chien University, Taipei, Taiwan.