P.Bhuvaneswari, International Journal of Computer Science and Mobile Applications,
Vol.5 Issue. 11, November- 2017, pg. 103-111 ISSN: 2321-8363
Impact Factor: 5.515

A NETWORK SAFETY IN INTERNET PENETRATION FOR REDUCING E-COMMERCE RISKS

P.Bhuvaneswari, MCA,
Assistant Professor, KG College of Arts and Science College, Coimbatore, India
Email- bhuvaneswari.p@kgcas.com

ABSTRACT: ***E-commerce Security is a part of the Information Security framework and is specifically applied to the components that affect e-commerce that include Computer Security, Data security and other wider realms of the Information Security framework. E-commerce security has its own particular nuances and is one of the highest visible security components that affect the end user through their daily payment interaction with business. E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. Dimensions of e-commerce security-Integrity, Non-repudiation, Authenticity, Confidentiality, Privacy, Availability. 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.***

Keywords: Digital E-commerce, Security Vulnerability, Security measures, Security Threats, Quality measurement model, SRQI

INTRODUCTION

E-commerce Security is a part of the Information Security framework and is specifically applied to the components that affect e-commerce that include Computer Security, Data security and other wider realms of the Information Security framework. E-commerce security has its own particular nuances and is one of the highest visible security components that affect the end user through their daily payment interaction with business. Today, privacy and security are a major concern for electronic technologies. M-commerce shares security concerns with other technologies in the field. Privacy concerns have been found, revealing a lack of trust in a variety of contexts, including commerce, electronic health records, e-recruitment technology and social networking , and this has directly influenced users. Security is one of the principal and

continuing concerns that restrict customers and organizations engaging with ecommerce. Online shopping through shopping websites having certain steps to buy a product with safe and secure. The e-commerce industry is slowly addressing security issues on their internal networks. There are guidelines for securing systems and networks available for the ecommerce systems personnel to read and implement. Educating the consumer on security issues is still in the infancy stage but will prove to be the most critical element of the e-commerce security architecture.

E-COMMERCE SECURITY TOOLS

Firewalls – For Software and Hardware
Public Key infrastructure
Encryption software , digital certificates
Digital Signatures
Biometrics – retinal scan, fingerprints, voice etc
Passwords, Locks and bars – network operations centers

PURPOSE OF SECURITY

1. Data Confidentiality – is provided by encryption / decryption.
2. Authentication and Identification – ensuring that someone is who he or she claims to be is implemented with digital signatures.
3. Access Control – governs what resources a user may access on the system. Uses valid IDs and passwords.

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.

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 . Two kind of metric combination models are Linear Combination Model (LCM for short) and Non-Linear Combination Model (NLCM for short). 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. Finally, the formula combines three critical quality measurements into an indicator of software security requirement quality measurement.

Four formulas described as follows:

- 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
SOS: System Operation Security TS: Transaction Security

$SRCM = W_1 * PIS + W_2 * SOS + W_3 * TS$

$W_1 + W_2 + W_3 = 1$ (1)

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

- 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.

Step2: 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):

- Finally, combine SRCM, SRAM and SRMM three measurements into an indicator of SRQM.

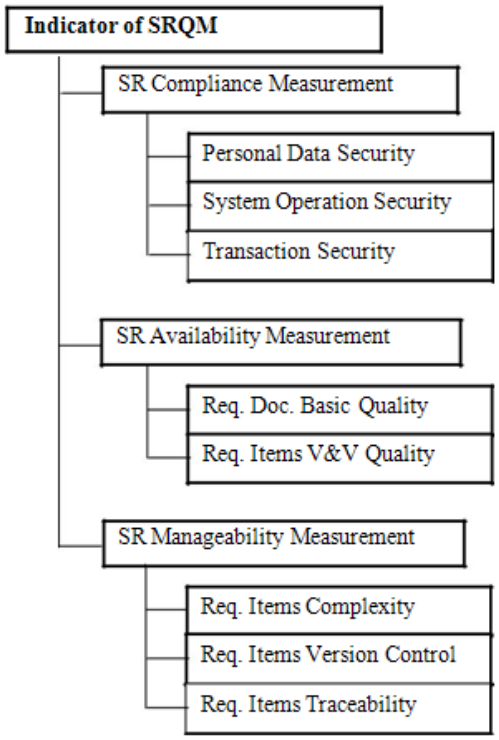
The formula is shown as Equation (4):
ISRQM: Indicator of SRQM
SRCM: Security Requirement Compliance Measurement
SRAM: Security Requirement Availability Measurement SRMM: Security Requirement Manageability Measurement
ISRQM = Wcm* SRCM +Wam* SRAM + Wmm* SRMM
Wcm +Wam + Wmm = 1

Wcm: Weight of SRCM Wam:Weight of SRAM Wmm:Weight of SRCM

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.
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 describes as follows:



Security Requirement Process Improvement Procedure

- 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.
- 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.
- 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.

Security Issues

E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. While security features do not guarantee a secure system, they are necessary to build a secure system. Security features have four categories:

- Authentication: Verifies who you say you are. It enforces that you are the only one allowed to logon to your Internet banking account.
- Authorization: Allows only you to manipulate your resources in specific ways. This prevents you from increasing the balance of your account or Encryption: Deals with information hiding. It ensures you cannot spy on others during Internet banking transactions.
- Auditing: Keeps a record of operations. Merchants use auditing to prove that you bought a specific
- Merchandise.
- Integrity: prevention against unauthorized data
- modification
- Nonrepudiation: prevention against any one party from reneging on an agreement after the fact
- Availability: prevention against data delays or removal.

Security Threats

Three types of security threats

- *denial of service, –unauthorized access, and –theft and fraud* Security (DOS): Denial of Service (DOS)
- Two primary types of DOS attacks: spamming and viruses
- Spamming

DDOS (distributed denial of service attacks) involves hackers placing software agents onto a number of third-party systems and setting them off to simultaneously send requests to an intended target.

- Viruses: self-replicating computer programs designed to perform unwanted events. •Worms: special viruses that spread using direct Internet connections.
- Trojan Horses: disguised as legitimate software and trick users into running the program *Security (unauthorized access)*
- Illegal access to systems, applications or data
- Passive unauthorized access –listening to communications channel for finding secrets. –May use content for damaging purposes
- Active unauthorized access –Modifying system or data –Message stream modification •Changes intent of messages, e.g., to abort or delay a negotiation on a contract
- Masquerading or spoofing –sending a message that appears to be from someone else. –Impersonating another user at the ―name‖(changing the From field) or IP levels (changing the source and/or destination IP address of packets in the network)

Secure E-Commerce Guidelines

Cookies and History

Online merchants use cookies to recognize you and speed up the shopping process the next time you visit. You may be able to set your browser to disable or refuse cookies but the tradeoff may limit the functions you can perform online, and possibly prevent you from ordering online. Generally, you will need to enable session cookies to place an order. Privacy advocates worry that as more and more data is compiled about us — without our knowledge or active consent — it will be combined to reveal a detailed profile, even our actual identities. This data is often collected to market goods and services to us, encouraging us to buy them. There are a number of companies that specialize in targeted online advertising called "behavioral marketing." Companies say consumers benefit by being exposed to more targeted advertising and that online merchants can make more money more efficiently by targeting the right shoppers.

Credit/ debit card

The safest way to shop on the Internet is with a *credit card*. In the event something goes wrong, you are protected under the federal Fair Credit Billing Act. You have the right to dispute charges on your credit card, and you can withhold payments during a creditor investigation. The Act also regulates ―negative option plans. A consumer must give express, informed consent before being charged for goods or services sold online through ―negative option marketing, such as ―free trials that the consumer must cancel in order to avoid being charged. Companies that use negative option plans must (1) clearly and conspicuously disclose the material terms of the transaction before obtaining the consumer‘s billing information, (2) obtain a consumer‘s express consent before charging the consumer, and (3) provide a simple mechanism to stop any recurring

charges. Online shopping by *check* leaves you vulnerable to bank fraud. And sending a cashier's check or money order doesn't give you any protection if you have problems with the purchase. Never pay for online purchases by using a *money transfer service*.

Identity Theft

As online shopping becomes more common, there will be more cases of identity theft committed over the Internet. Imposters are likely to obtain their victims' identifying information using low-tech means like dumpster diving, mail theft, or workplace access to SSNs. But they are increasingly using the Web to apply for new credit cards and to purchase goods and services in their victims' names. The same advice for avoiding low-tech identity theft applies to shopping on the Internet. Many are mentioned in the above tips. Most important: Be aware of who you are buying from. And use *true* credit cards for purchases, not debit cards. We recommend that you check your credit card bills carefully for several months after purchasing on the Internet. Look for purchases you did not make. If you find some, immediately contact the credit card company and file a dispute claim. Order your credit reports at least once a year and check for accounts that have been opened without your permission.

Conclusion

E-commerce is widely considered the buying and selling of products over the internet, but any transaction that is completed solely through electronic measures can be considered e-commerce. Day by day E-commerce is playing very good role in online retail marketing and peoples using this technology day by day increasing all over the world. E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. Dimensions of e-commerce security; Integrity: prevention against unauthorized data modification, No repudiation: prevention against any one party from reneging on an agreement after the fact. Authenticity: authentication of data source. Confidentiality: protection against unauthorized data disclosure. Privacy: provision of data control and disclosure. Availability: prevention against data delays or removal. Fraudsters are constantly looking to take advantage of online shoppers prone to making novice errors. Common mistakes that leave people vulnerable include shopping on websites that aren't secure, giving out too much personal information, and leaving computers open to viruses. In this paper we discussed E-commerce Security Issues, Security measures, Digital E-commerce cycle/Online Shopping,.

References

1. Mohanad Halaweh, Christine Fidler - " Security Perception in Ecommerce: Conflict between Customer and Organizational Perspectives". Proceedings of the International Multiconference on Computer Science and Information Technology, pp. 443 – 449, ISBN 978-83-60810-14-9- 2008- IEEE
2. Shazia Yasin, Khalid Haseeb. "Cryptography Based E-Commerce Security: A Review". IJCSI-Vol. 9, Issue 2, No 1, March 2012
3. Dr. Nada M. A. Al-Slamy, "E-Commerce security" IJCSNS - VOL.8 No.5, May 2008
4. Seyyed Mohammad Reza Farshchi "Study of Security Issues on Traditional and New Generation of E-commerce Model" International Conference on Software and Computer Applications-IPCSIT vol.9 (2011)
5. Adams, C., P. Sylvester, M. Zolotarev, and R Zuccherato. 2001. Internet X.509 Public Key Infrastructure data validation and certification server protocols. Internet RFC 3029.
6. CCITT. 1988. Recommendation X.509: The Directory - Authentication Framework. Data Communications Network Directory, Recommendations X.500-X.521
7. Nithya.A, "Internet Information System Based on Network Security Design". ISBN:978-93-80506-08-1., National Level Conference on Innovative in Information Technology

Biography

Bhuvaneswari.P, MCA, Assistant Professor in Computer Science at KG College of Arts and Science. She is very much interesting in Research in computer networking and Data Mining also in paper publication and attending Conference and Seminars.

