Winter 12-1-2010

A Quality-based Security Enhancement Procedure to Improve E-Commerce security

Sen-Tarng Lai

A QUALITY-BASED SECURITY ENHANCEMENT PROCEDURE TO IMPROVE E-COMMERCE SECURITY

Sen-Tarng Lai, Department of Information Technology and Management, Shih Chien University, No.70 Ta-Chih Street, Chung-Shan District, Taipei, Taiwan
E-mail: stlai@mail.usc.edu.tw

Abstract

E-commerce is an important product in the internet fever. However, the network intrusion and security vulnerabilities have continued to threaten the e-commerce operation and user privacy. How to improve security of e-commerce has become a topic worthy exploration. In this paper, based on security testing and repair, proposes a Software Security Enhancement Procedure (SSEP for short). In addition, for assuring SSEP operation quality, proposes a set of Software Security Enhancement Process Quality Measurement (SSEPQM for short) model. Applying SSEPQM model, the defects of security improvement process can be identified and revised. So the security of e-commerce can be enhanced effective and continuous.

Keywords: e-commerce, security vulnerability, quality measurement model, security testing, security repair

1. Introduction

In the E generation of internet fever, promote a variety of high efficiency and benefit activities must be integrated with the internet. Therefore, with a variety of Internet business practices and activity, and promotion of all commercial activities conducted through the network are collectively referred to as e-commerce. Can not cope with the trend to change business behavior and activities, will eventually unable to meet customer requirements lead to the profits decline and eliminated by the times. However, in the information age, information security issues of computers and software more and more serious [7] [9] [16] [19]. Internet intrusion and system security vulnerabilities continue to harm the normal operation of the software system, making information system security to severe test. In order to avoid external intrusion and system security holes caused significant loss of user, how to improve the security of software systems has become worthy of further exploration [2] [3] [13]. Through e-commerce business practices and activities, it still can not build a successful business or organization sustainability. Because many factors affect the success or failure of e-commerce, e-commerce software security is one important factor. Secure defects and security vulnerabilities are fatal to e-commerce systems.

E-commerce has the advantages of the Internet, in a variety of business practices and activities can indeed enhance the many benefits. However, it also implies the absence of many urgent improvements, such as the efficiency of the implementation, network security, software correctness, adjustment environment and maintenance capabilities. Factors involved in very many of them, organizations and users for software security requirement exceeds the function and performance requirements [1] [12]. E-commerce software security is a far-reaching factor. E-commerce security flaws and defects of almost all belong to the occurrence of passive, the system appears to be the invasion or loss of data anomalies, the operation of the system to discovery the security vulnerabilities and defects. Once the system is intruded or data loss occurs, there will be perceptible system security vulnerabilities and defects. At this time the caused by organization damage and the impact on users is difficult to assess and expectations, nor the subsequent repair work or improvements to make up. In order to effectively continue to improve the security of e-commerce, this article explores the related activities. Based on "prevention is better than cure" concept to take the initiative to identify security vulnerabilities of e-commerce and continuously enhance the security o f e-commerce.

In e-commerce system, software plays a very important role. Software has to change with complex network environment, hardware architecture, and the various needs of users. Therefore, e-commerce software should have the features of continue to improvement, high extensibility, completeness, high security. High security is e-commerce software must attach importance to and strengthen the key item. This article is on how to continue to improve the e-commerce security to explore the related activities, and develop a Software Security Enhancement procedure (SSEP). The SSEP covers security testing and security repair two important activities. The quality of these two activities will directly affect the e-commerce security improvement effectively. For this, the security testing and repair activities should be monitored and controlled. The paper proposes a quality measurement model for monitoring and controlling

Software Security Enhancement Process that is called Software Security Enhancement Process Quality Measurement (SSEPQM) model. This article has five sections: Section II will explore e-commerce software security and improvement approaches. Identify security vulnerabilities is the first step to improve e-commerce security, security repair operation is a critical step to enhance e-commerce security. Section III will discuss software security enhancement steps and propose a set of software security enhancement and continuous improvement procedure. Section IV will propose a quality measurement model for software security enhancement process to monitor and correct security testing and security repair activities. Section V will discuss the contributions of this paper and make a conclusion for this topic.

2. Importance of e-commerce software Security

Internet and WWW (World Wide Web) of the trend, change the mode of commercial activities for the emerging e-commerce system offers many advantages. It also implies unpredictable security crisis, in e-commerce technology and development level, there is still room to improve and enhance the space.

2.1 E-commerce Technology and Security

Three-tier architecture with web database (shown in Figure 1) is the mainstream of current e-commerce operating environment.

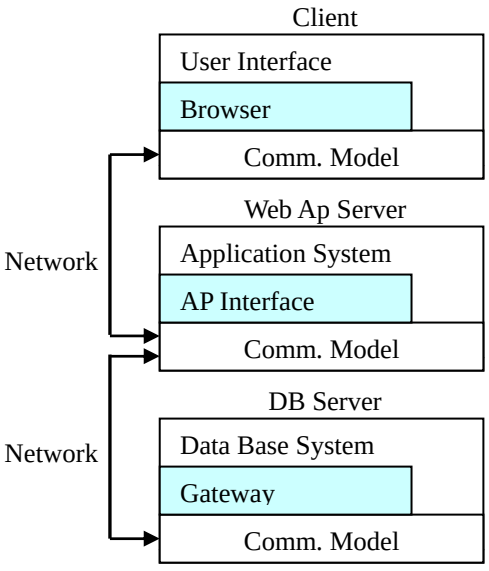

Figure 1.Three-tier architecture of e-commerce

In terms of system architecture and operating environment, in fact e-commerce is Web application (Web Ap for short) in enterprise instance. Therefore, all kind of possible harm to Web Ap security vulnerabilities, will also pose to e-commerce a threat. According to CERT/CC latest statistics data show that from 2005 to the third quarter of 2008 analysis of software vulnerabilities total 27,346 cases [20] (shown in Table 1).

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

The 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 Ap security. They gradually published the key of Web Ap security vulnerabilities and defects: SANS Top-20 Security Risks [21] with the OWASP Top 10 security vulnerabilities [22], to help reduce Web Ap security risks.

2.2 E-commerce security improvement approaches

Applying various testing methods to find the security vulnerabilities, which were injected by development or maintenance operation, is an important manner for improving Web Application security. Penetration Testing (PT for short) and Vulnerability Scanning (VS for short) are two critical approaches to improve Web Ap security. E-commerce can be regarded as a commercial activity of Web Ap. Therefore, PT and VS are also the e-commerce security improvement approaches. PT is a formal inspection of security vulnerability. Based on the hacker viewpoint, PT conducts network security detecting. And Inspection range exceeds e-commerce self security. In general, PT is conducted by the professional consultants [2] [3] [4]. The testing time spend of is depend on inspection items, it needs five day at least in a complete PT. Final report of PT should list and describe the found security vulnerabilities. VS

belongs to internal security vulnerability detection. It should be conducted by the Web Ap maintenance personnel and six months once at least. VS tools can help identify the Web Ap security vulnerability. There are many free VS tools: NetCat, NIKTO, Paros Proxy etc. and commercial VS products. HP WebInspect and IBM AppScan are two major commercial VS tools. However, PT and VS still have many disadvantages for security improvement process. The disadvantages shown as follows:

- Can not clear assure the found vulnerabilities are real or false defects.
- No develop a complete follow operation for the security repair phase.
- No define a quality control and management mechanism for security improvement process.
- No well define an evaluation mechanism for the security improvement process.

3. E-commerce security improvement process

Identifying security vulnerabilities is the first step to improve the e-commerce security. Security vulnerabilities repair is a critical operations to improve e-commerce security.

3.1 Software Security Enhancement Procedure

In fact, in operation of e-commerce system, any changes or corrections are belonged to the maintenance activities. The maintenance requests propose by the users should be passed formal review and seriously audit. Then, the requests can enter maintenance operation to conduct correction, extension or migration jobs. The first step of the e-commerce security improvement is security testing. It major objective is to identify hidden security vulnerability. Removing security vulnerabilities of false positives, and then has to conduct a series of maintenance steps to complete the effective of e-commerce security improvement. Security repair operation is similar to error correction maintenance activity, should plan a set of well security improvement procedure. And assure security improvement process has the capability to increase e-commerce security. For this, in this paper, security testing is regarded as the presetting phase. Combining security testing with security repair operations, a set of Software Security Enhancement Procedure (SSEP for short) is proposed for enhancing follow operation of security testing. The SSEP is planned and divided into four phases as follows:

(1) Presetting phase

- According to e-commerce possible existing security vulnerabilities, planning and writing security testing plan.
- According to security testing plan, conducting security testing and identifying the existing security vulnerabilities.
- According to identified vulnerabilities and security testing plan, writing a security testing report.

(2) Determination phase:

- Analyzing the vulnerabilities of testing report, removing security vulnerabilities of false positives.
- According to security vulnerabilities, separating the modules that are affected by security vulnerabilities.
- Based on the security vulnerabilities impact degree, secure defects are separated three levels: requirement specification secure defects, design phase secure defects and source code secure defects.

(3) Repair phase:

- According to the level of secure defect, develop the detailed repair operations.
- Each completed task of repair operations should be convened the formal review.
- The task of repair operations has not pass the formal review, should feedback to front step to conduct the task of repair operation again.

(4) Evaluation phase:

- The repair operations passed rigorous review, should conduct several testing step: unit test, functional test, regression test, system test and installation test [10][17][18].
- Completed and passed the testing steps, should back to presetting phase to conduct penetration test again.
- According to two times penetration testing report, should evaluate the repair operations result and assure correctness, completeness and consistency.
- The repair operation has not pass the quality evaluation, should feedback to related phase to conduct the task of repair operation again.

The complete e-commerce security improvement processes shown in Figure 2, based on iteration inspection activity, to assure the effectiveness of security vulnerability repair operation.

3.2 Operation quality factors of security testing

It is absolutely necessary to develop a well test plan for the security testing. The content of test plan is the major basis for measure the quality of security testing. Four critical tasks of security testing and their quality factors are described as follows:

(1) Security testing coverage

- Test cases of test plan should include the top ten or top twenty security vulnerabilities are issued by the key organization. High degree coverage represent the security testing consider scope is more complete.
- E-commerce systems must be integrated with various functions and related subsystems. Subsystems and function interface often becomes the security defects, test plan must be prepared suitable test cases for these security defects.
- E-commerce operation always need modify or adjust with technical, functional or application changes. Test plan should develop test cases to consider the maintain operations may produced the security vulnerabilities.

(2) Security testing execution quality:

- In security testing process, testing should achieve high degree completeness testing.
- In security testing process, each test case should apply identical test procedure and steps.
- In security testing process, testing environment should satisfy the planning of security test plan.

(3) Security vulnerabilities assurance quality:

- In security testing process, identified vulnerabilities should include concretely and clearly defect type.
- In security testing process, security vulnerabilities of false positives should be removed.
- In security testing process, identified vulnerabilities should describe concretely and clearly affected range.

(4) Security retesting quality:

- During security testing, the identified vulnerabilities testing process is based on the test case plan formulated by the high-integrity testing.
- During security testing, does each test case apply consistence testing procedure and step?
- During security testing, does each test case is tested on the right environment that developed by test plan.

3.3 Operation quality factors of security repair

Secure testing operation was completed, the identified security vulnerabilities must be careful to confirm. Then, based on the confirmed security vulnerabilities, conduct security repair operation. Repair operation resembles correction maintenance operation, should apply configuration management system to control repair quality [10] [17] [18]. Four critical tasks of security repair and their quality factors are described as follows:

(1) Repair document quality factors:

- Based on identified security vulnerabilities,
  - Documents repair activity of requirement and design phase must achieve high correctness.
  - Documents repair activity of requirement and design phase must achieve high completeness.
  - Documents repair activity of requirement and design phase must achieve high consistency.

(2) repair programming operation quality factors:

- According to repair design documents,
  - Follow program repair activity must achieve high degree correctness.
  - Follow program repair activity must achieve high degree completeness.
  - Follow program repair activity must achieve high degree consistency.

(3) repair testing operation quality factors:

- According to repair documents and programs,
  - Follow testing activity must achieve high degree correctness.
  - Follow testing activity must achieve high degree completeness.
  - Follow testing activity must achieve high degree consistency.

(4)Configuration management operation quality factors:

- According to configuration management mechanism,
  - Security vulnerabilities repair activity should achieve documents check-in and check-out.
  - Security vulnerabilities repair activity should achieve version control.
  - Security vulnerabilities repair activity should record repair personnel, repair time, repair date and repair reason.

4. E-commerce software security improvement continuous

Security testing and security repair are the critical operations to impact the quality of SSEP. This section will present a set of SSEP quality measurement model to help increase the quality of SSEP.

4.1 Quality-based Security Enhancement Procedure

Individual measurement can only measure or evaluate the specific quality characteristic. In order to monitor and assess the quality of improvement

operations, individual measurements should to make the appropriate combination [14] [15]. Two kind of metric combination models are Linear Combination Model (LCM for short) and NonLinear Combination Model (NLCM for short). NLCM has high accuracy measurement than LCM [5] [6] [8] [11]. However, LCM has high flexibility, more extensible and easy formulation than NLCM [8] [11] [14] [15]. For this, LCM is applied to security metrics combination in this paper. The different levels' activities have different quality metrics be shown. Therefore, before applying the linear combination model, the measurement data must be normalization. Refer to predefined weight value and combination formula, basic-level and high correlated metrics can be combined into a quality characteristic measurement. E-commerce security improvement procedure can be distinguished into security testing and security repair operations two steps. Which affect the security testing operation are four critical activities: Security Test Coverage, Security Test, Security Vulnerability Verification and Security Vulnerability Retest. Four critical activities quality measurements are combined with several basic-level quality factors. Through the linear combination formula, with highly correlated basic level quality factors can be combined into a specific activity quality measurement, then combined into a security testing operation measurement as follows:

(1) Security Test Coverage (STC for short) is combined with security vulnerabilities released by key organizations, security vulnerabilities of interface design and self security holes etc. three security test factors. The combination formula is shown in Formula (1):

STC: Security Test Coverage
T20VTC: Top 20 Vulnerability Test Cases
W_1: Weight of T20VTC
DIVTC: Design Interfaces Vulnerability Test Cases
W_2: Weight of DIVTC
SSVTC: Self Vulnerability Test Cases
W_3: Weight of SSVTC

$$STC=W_1*AESFI+W_2*AESFII+W_3*AESFIII \quad W_1+W_2+W_3=1 \qquad (1)$$

(2) Security Test Quality Metric (STQM for short) is combined with security test completeness, security test consistency, and security test correctness etc. three factors. The combination formula is shown in Formula (2):

STQM: Security Test Quality Metric
STCM: Security Test Completeness
W_1: Weight of STCM
STCN: Security Test Consistency
W_2: Weight of STCN
STCR: Security Test Correctness
W_3: Weight of STCR

$$STQM=W_1*STCM + W_2* STCN + W_3*STCR \quad W_1+W_2+W_3=1 \qquad (2)$$

(3) Security Vulnerability Verification Quality Metric (SVVQM for short) is combined with security vulnerabilities identification clarity, security vulnerabilities identification correctness, security vulnerabilities identification range etc. three factors. The combination formula is shown in Formula (3):

SVVQM: Security Vulnerability Verification Quality Metric
SVICA: Security Vulnerability Identification Clarity
W_1: Weight of SVICA
SVICO: Security Vulnerability Identification Correctness
W_2: Weight of SVICO
SVICR: Security Vulnerability Identification Range
W_3: Weight of SVICR

$$SVVQM=W_1*SVICA+W_2*SVICO+W_3*SVICR \quad W_1+W_2+W_3=1 \qquad (3)$$

(4) Security Retest Quality Metric (SRQM for short) is combined with security test report quality and security retest plan quality two factors. The combination formula is shown in Formula (4):

SRQM: Security Vulnerability Retest Quality Metric
STRQ: Security Test Report Quality
W_1: Weight of STRQ
SRPQ: Security Retest Planning Quality
W_2: Weight of SRPQ

$$SRQM= W_1* STRQ + W_2* SRPQ \quad W_1+W_2=1 \qquad (4)$$

(5) Then, combine STC, STQM, SVVQM with SRQM four metrics to be a Security Testing Operation Measurement (STOM for short). The combination formula is shown in Formula (5):

STOM: Security Testing Operation Measurement
STC: Security Vulnerability Test Coverage
W_1: Weight of STC
STQM: Security Vulnerability Test Quality Metric
W_2: Weight of STQM
SVVQM: Security Vulnerability Verification Quality Metric
W_3: Weight of SVVQM
SRQM: Security Vulnerability Retest Quality Metric

W_4: Weight of SRQM

$$STOM = W_1 * STC + W_2 * STQM + W_3 * SVVQM + W_4 * SRQM \quad W_1+W_2+W_3+W_4=1 \quad (5)$$

Which affect the security repair operation are four critical activities: document repair, program repair, testing repair and configuration management. Four critical activities quality measurements are combined with several basic-level quality factors. Through the linear combination formula, with highly correlated basic level quality factors can be combined into a specific activity quality measurement, then combined into a security repair operation measurement as follows:

(6) Metrics of Document Repair Quality (MDRQ for short) is combined with correctness, completeness and consistency of documents repair quality factors. The combination formula is shown in Formula (6):

MDRQ: Metrics of Documents Repair Quality

DRCr: Document Repair Correctness

W_1: Weight of DRCr

DRCm: Document Repair Completeness

W_2: Weight of DRCm

DRCn: Document Repair Consistency

W_3: Weight of DRCn

$$MDRD=W_1*DRCr+ W_2* DRCm + W_3*DRCn \quad W_1+ W_2 + W_3 =1 \quad (6)$$

(7) Metrics of Program Repair Quality (MPRQ for short) is combined with correctness, completeness and consistency of program repair quality factors. The combination formula is shown in Formula (7):

MPRQ: Metrics of Programs Repair Quality

PRCr: Program Repair Correctness

W_1: Weight of PRCr

PRCm: Program Repair Completeness

W_2: Weight of PRCm

PRCn: Program Repair Consistency

W_3: Weight of PRCn

$$MPRD=W_1* PRCr + W_2* PRCm + W_3*PRCn \quad W_1+ W_2 + W_3 =1 \quad (7)$$

(8) Metrics of Test Repair Quality (MTRQ for short) is combined with correctness, completeness and consistency of test repair quality factors. The combination formula is shown in Formula (8):

MTRQ: Metrics of Tests Repair Quality

TRCr: Test Repair Correctness

W_1: Weight of TRCr

TRCm: Test Repair Completeness

W_2: Weight of TRCm

TRCn: Test Repair Consistency

W_3: Weight of TRCn

$$MTRD=W_1* TRCr + W_2* TRCm + W_3*TRCn \quad W_1+ W_2 + W_3 =1 \quad (8)$$

(9) Metrics of Configuration Management Quality (MCMQ for short) is combined with document access control quality, document version control quality and document repair record quality three factors. The combination formula is shown in Formula (9):

MCMQ: Metrics of Configuration Management Quality

DRCr: Documents Access Control

W_1: Weight of DRCr

DRCm: Documents Repair Version Control

W_2: Weight of DRCm

DRCn: Documents Repair Records

W_3: Weight of DRCn

$$MDRD=W_1* DRCr + W_2* DRCm + W_3*DRCn \quad W_1+ W_2 + W_3 =1 \quad (9)$$

(10) Then, combine MDRQ, MPRQ, MTRQ with MCMQ four metrics into a Security Repair Operation Measurement (SROM for short). The combination formula is shown in Formula (10):

SROM: Security Repair Operation Measurement

MDRQ: Metrics of Documents Repair Quality

W_1: Weight of MDRQ

MPRQ: Metrics of Programs Repair Quality

W_2: Weight of MPRQ

MTRQ: Metrics of Tests Repair Quality

W_3: Weight of MTRQ

MCMQ: Metrics of Configuration Management Quality

W_4: Weight of MCMQ

$$SROM = W_1* MDRQ + W_2* MPRQ + W_3*MTRQ +W_4*MCMQ \quad W_1 + W_2+W_3+W_4=1 \quad (10)$$

Finally, combine SVTM with SVRM into the SSEP Improvement Indicator (SSEPII for short). The combination formula is shown in Formula (11):

SSEPII: SSEP Improvement Indictor

STOM: Security Test Operation Measurement

W_{stom}: Weight of STOM

SROM: Security Repair Operation Measurement

W_{srom}: Weight of SROM

$$SSEPII = W_{stom} * STOM + W_{srom} * SROM \quad W_{stom} + W_{srom} = 1 \quad (11)$$

Security Enhancement Process quality measurement model is divided into three parts. First part, based on the security testing activities, combines with four quality metrics into the security testing operation quality measurement. Second part, based on the security repair activities,

combines with four quality metrics into the security repair operation quality measurement. Then the third part, combined with two operation quality measurements into an SSEP Improvement Indicator (SSEPII). The SSEP improvement indicator is a critical for determining the operations quality of security testing and security repair. Completed three combinations of operations quality measurement to improve the security enhancement operation is called the SSEP Quality Measurement (SSEPQM for short) model. The architecture of SSEPQM model is shown in Figure 3.

4.2 SSEP quality improvement activity

Quality measurement is a relative judgment indicator also is a basis to judge good or bad job of testing and repair operation. In the quality measurement model, basic level quality factors are combined into a high level quality metric. Therefore, when the quality measurement of improvement operation was classified for the "unacceptable" range, the corresponded combination formula can be identified by the quality measurement model. Based on the formula, repeat analyzing steps, the corresponded basic level jobs can be identified, then to analyze job defects and problems and propose the corrective action. When the quality indicators for the security improvement process can not meet the "Quality Criteria", the corrective action need be planned. This paper proposed a rule-based quality improvement activity for corrective action, described as follows:

Rule1:
IF the process improvement quality indicators can not meet the quality criteria
THEN the security testing operation or security repair operation quality measurement should be detected.

Rule2:
IF security testing operation quality measurement can not meet quality criteria
THEN the four metrics: STC, STQM, SVVQM and SRQM should be analyzed to identify the metric too low to cause security testing operation quality measurement not meet the quality criteria.

Rule 3:
IF security repair operation quality measurement can not meet quality criteria
THEN the four metrics: MDRQ, MPRQ, MTRQ and MCMQ should be analyzed to identify the metric too low to cause security repair operation quality measurement not meet the quality criteria.

If the quality defects of e-commerce security improvement operations can be adjusted and corrected in time, then the e-commerce security continuous improvement operation will be increased effectively. And the e-commerce security can be enhanced effectively and concretely.

5. Conclusions

An on-line e-commerce system is usually necessary to invest considerable time and resources. In order to achieve high efficiency resources to increase user's confidence is inevitable trend. Continuous improve the system security is a necessary condition to increase system reliability. In operation course, e-commerce system must change in time with new environment, new technology, function extension and modification. And conduct update activities continuous to satisfy various requirements. The life cycle of e-commerce system can be effective extended. However, environment change, technology improvement, and update activity may threat the e-commerce operation security. In order to effective and continuous improve e-commerce security, this paper explores the related security improvement activities. Based on "prevention is better than cure" concept, in this paper, take the initiative to identify security vulnerabilities of e-commerce, and combining with security testing and security repair operations, propose a set of Software Security Enhancement Procedure (SSEP) to enhance follow operation of security testing. And propose a set of SSEP Quality Measurement (SSEPQM) model to assure the process quality of SSEP. The advantages of SSEPQM model are applied the linear combination model to replace complexity combination model, and has high flexibility, easy formula, high extensibility and high compatibility for the expertise. Applying SSEPQM model, the defects of security improvement process can be identified. And assist in timely to adjust and revise defects of security improvement process, enhance e-commerce security effective and continuous.

References

[1] Apvrille, A. and Pourzandi, Makan ,“Secure Software Development by Example,” IEEE Security & Privacy, vol. 3, no. 4, 2005.
[2] Arkin, B., S. Stender and G. McGraw, “Software Penetration Testing,” *IEEE Security & Privacy*, vol. 3, no. 4, pp. 84-87 (2005).
[3] Bau J., E. Bursztein, D. Gupta, J. Mitchell

"State of the Art: Automated Black-Box Web Application Vulnerability Testing," *2010 IEEE Symposium on Security and Privacy*, pp. 332-345 (2010)

[4] Bishop, M., "About Penetration Testing," *IEEE Security & Privacy*, vol. 5, no. 4, pp. 84-87 (2007)

[5] Boehm, B. W., *Software Engineering Economics*, Prentice-Hall, New Jersey, 1981.

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

[7] Cowan, C., "Software Security for Open-Source Systems," *IEEE Security & Privacy*, vol. 1, no. 1, 2003, pp. 38-45.

[8] Deutsch M. S. and R. R. Willis, *Software Quality Engineering: A Total Technical and Management Approach*, Prentice-Hall, Inc., NJ, 1988.

[9] Evans, D. and D. Larochelle, "Improving Security Using Extensible Lightweight Static Analysis," IEEE Software, January/February 2002, pp.42-51.

[10] Fairley, R., *Software Engineering Concepts*, McGraw-Hill, Inc., 1985.

[11] Fenton, N.E., *Software Metrics - A Rigorous Approach*, Chapman & Hall, 1991.

[12] McGraw, G., "Software Security", *IEEE Security and Privacy*, March 2004.

[13] Hall, A. and Roderick Chapman, Correctness by Construction: Developing a Commercial Secure System, *IEEE Software*, January/February 2002, pp.18-25.

[14] Lai, S. T. "A Quality Measurement Model for Software Maintenance", *Proceeding of the Second World Congress on Software Quality (2WCSQ), Japan, 2000.*

[15] Lai, S. T. and C. C. Yang, "A Software Metric Combination Model for Software Reuse," *Proc. of 1998 Asia-Pacific Software Engineering Conference (APSEC'98)*, Dec. 1998, pp. 70-77.

[16] Leveson, N. G., *Safeware: System Safety and Computers*, Addison-Wesley, 1995.

[17] Pressman, R. S., *Software Engineering: A Practitioner's Approach*, McGraw-Hill, New York, 7th editions, 2010.

[18] Schach, S. R., Object-Oriented Software Engineering, McGraw-Hill Companies, 2008.

[19] Viega, J. and G. McGraw, Building Secure Software, Addison-Wesley, 2002.

[20] CERT/CC, 2010/9. (http://www.cert.org/stats/cert_stats.html)

[21] The Top Cyber Security Risks(http://www.sans.org/top-cyber-security-risks/) (2010/9)

[22] OWASP Top 10, 2010/9 (http://www.owasp.org.tw/blog/)

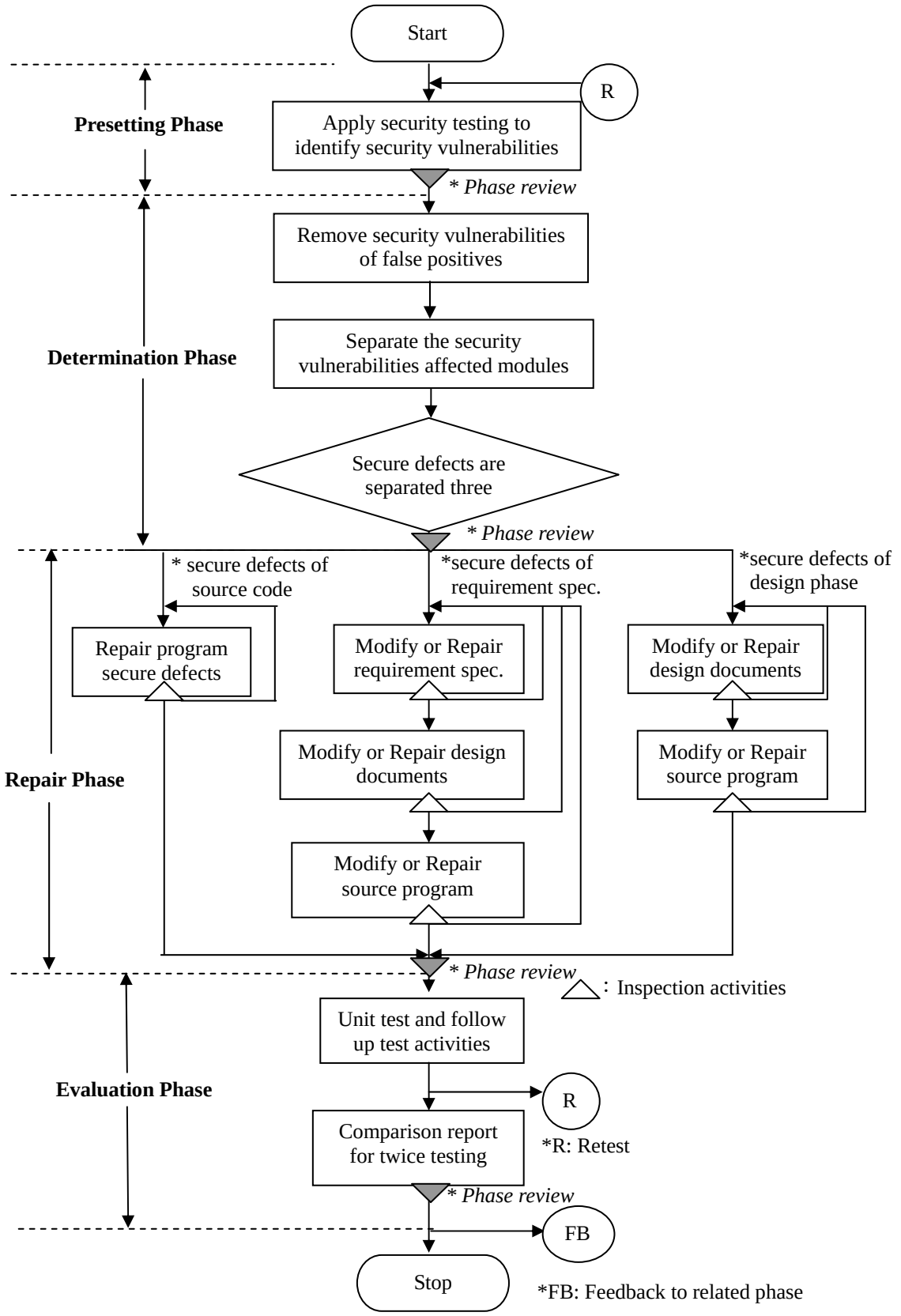

Figure 2. Flowchart of e-commerce software security enhancement procedure

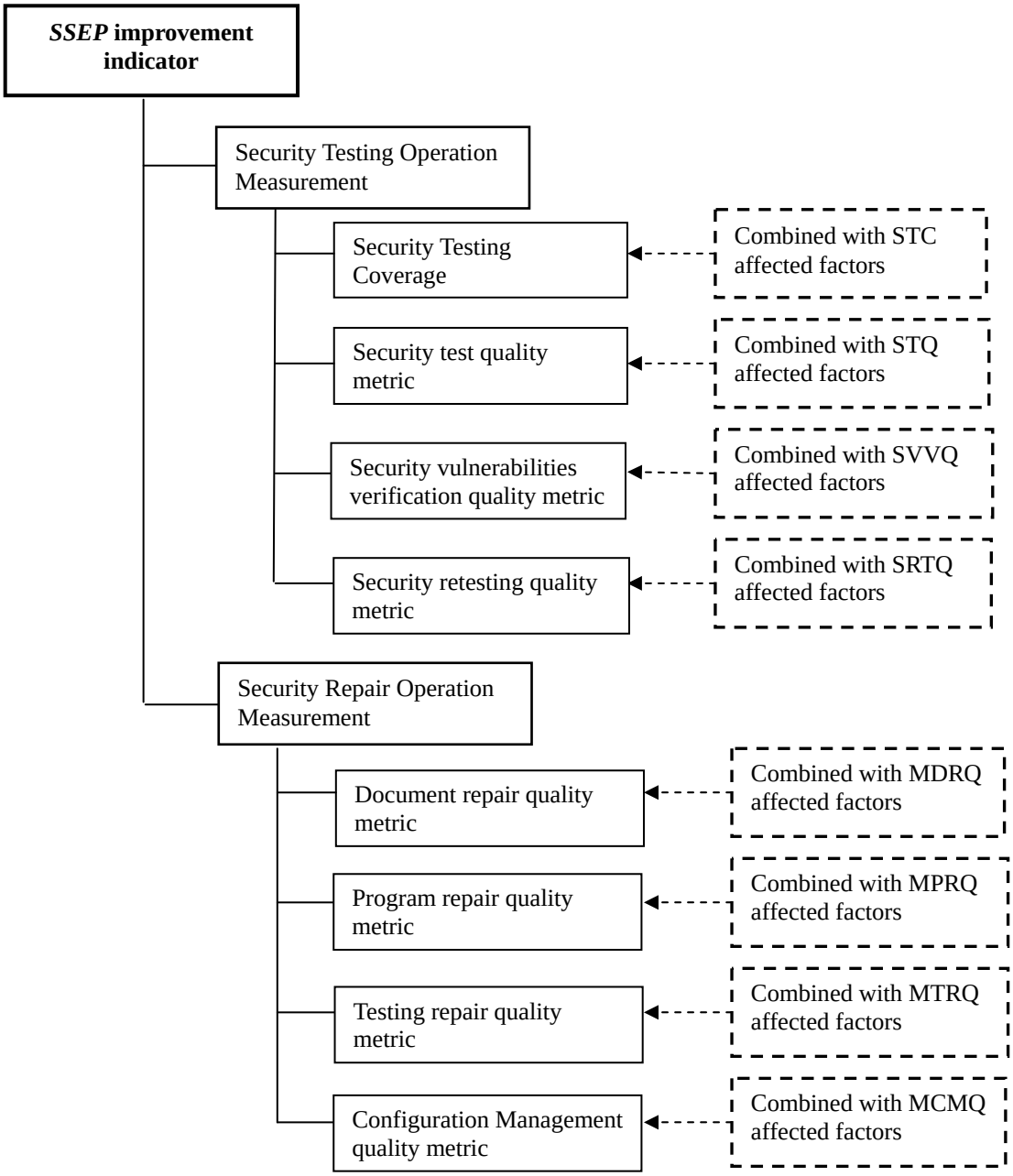

Figure 3. The architecture of ***SSEP*** Quality Measurement Model