TWO-LAYER SECURE PREVENTION MECHANISM FOR REDUCING E-COMMERCE SECURITY RISKS

Sen-Tarng Lai

Dept. of Information Technology and Management, Shih Chien University,
Taipei, 104, Taiwan

ABSTRACT

E-commerce is an important information system in the network and digital 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. How to improve e-commerce security has become a topic worthy of further exploration. Combining routine security test and security event detection procedures, this paper proposes the Two-Layer Secure Prevention Mechanism (TLSPM). Applying TLSPM, routine security test procedure can identify security vulnerability and defect, and develop repair operations. Security event detection procedure can timely detect security event, and assist follow repair. TLSPM can enhance the e-commerce security and effectively reduce the security risk of e-commerce critical data and asset.

KEYWORDS

E-commerce, security testing, event detection, security event, TLSPM.

1. INTRODUCTION

In the age of Internet popularity, high efficiency and high profit activities must be combined with the Internet properly. For this, the enterprises and organizations can increase their competitiveness to extend their survivability. Business behaviors and activities always are the pursuit of high efficiency and high-profit pioneers. So, business behaviors and activities are actively and rapidly being developed and promoted, all commercial activities conducted through the Internet are collectively referred to as e-commerce (Electric Commerce; EC) [1]. According to a report from Juniper Research, 2015 global e-commerce sales are expected to reach $1.7 trillion, up by more than 17 percent from last year's total [2]. B2C (Business-to-consumer) e-commerce sales worldwide will reach $1.74 trillion in 2015 increasing nearly 20% over 2013. [3] And, China e-commerce GMV (Gross Merchandise Volume) reached 3.48 trillion Yuan in Q1 2015, up 23.8% from Q1 2014. However, Gartner research report pointed out that as consumers worried about security issues, thus making e-commerce sales of as much as $2 billion shortage [4]. From the above study, the e-commerce sales will continue to grow, however, the security of e-commerce is a key factor to affect sales growth.

Network facility is a major advantage of e-commerce system. In all business behavior and activity, network environment makes e-commerce system more efficiency. However, e-commerce system always implies several emergency problems and defects for example execution performance, network security, software correctness and maintainability. E-commerce system issues concern many factors. One of the critical factors is transaction and personal information security. Impact of e-commerce security has overtaken function and performance issues. In order to avoid security flaws and defects of the system caused user significant loss, how to improve e-

DOI:10.5121/ijcsit.2015.7606

commerce security has become a topic worthy of further exploration. Security event of e-commerce often was indirectly or passively discovered. Delayed discovery security event always makes the organization looses widen and system recovers with difficulty. The security event can not be detected timely may cause e-commerce system damage impact expanded. For this, the paper investigates security prevention measure to increase efficiently e-commerce system security. Apply "prevention is better than cure" concept to enhance the e-commerce security event prevention and detection capability. Based on security prevention measure, actively test and detect e-commerce security defects to increase e-commerce security.

E-commerce system not only cooperates with the complex network environment and frequent updates hardware facilities, but also must maintain extension and change requirements to meet the target of organization. E-commerce system should have high maintainability, extensibility, integrity, and security etc. basic features. Security of the E-commerce system is a concern issue on the commercial transaction activity and behavior. For increasing transaction security, the e-commerce system must care and enhance system security. In this paper, discusses the e-commerce security related issues, explores and analyses the routine security testing and security event detection for e-commerce operation process. Based on security defects identification and security event detection activity, the paper combines routine security testing and security event detection procedures, proposes the Two-Layer Secure Prevention Mechanism (TLSPM). TLSPM can enhance the e-commerce security and effectively reduce e-commerce personal data security risk. First layer of TLSPM is the routine security testing, second layer is the security event detection procedure. This paper is divided into five sections. In Section II, discusses e-commerce security issues and necessary e-commerce security requirement items. In Section III, routine security test operation and security event detection are deeply analysed. In Section IV, combined routine security test with security event detection, proposes the Two-Layer Secure Prevention Mechanism (TLSPM). In Section V, evaluates the TLSPM advantages for reducing the e-commerce security risk. In Section VI, describes the TLSPM contribution to reduce e-commerce security risks, and does a conclusion for this topic.

2. IMPORTANCE OF E-COMMERCE SECURITY

Internet age changes the commercial transaction style and brings many business opportunities to the e-commerce. However, the unpredictable security also becomes the critical issues of e-commerce system.

2.1. E-commerce Security Issues

In the internet age, the e-commerce becomes an important system for the business transaction activity. 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) [5]. And, 42% people occurred personal data lost or happened fraud event [5]. 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 [6]. Therefore, famous corporation and organization very concerned on information security and used all approaches to defense hacker intrusion and protect customer personal data. Firewall, Intrusion Detection and Prevention (IDP) are major tools for network security prevention. Several software prevention and detection technologies, include vulnerability scanning, penetration testing and human inspection, also are the important approaches for increasing Web App security and reduce personal data security risk [7].

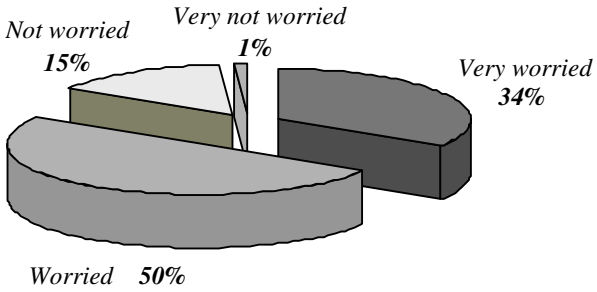

Fig.1. In network transaction, 84% people concerned personal data been stolen.

2.2. Security requirement items of e-commerce

Information security vulnerabilities and defects have become an important issue for the commercial behavior of enterprise and organization. Enterprise or organization does not concern the information security issues will lose customer confidence and recognition. In the internet age, e-commerce is a special and critical system for the commercial transaction activity. E-commerce security issue should be concerned specially. Holcombe considered any e-commerce system should satisfy four security requirements [1] (shown as Fig. 2):

(1) Authorization: The registered user of e-commerce system has to ensure his using privilege in system operation process.
(2) Integrity: In e-commerce information exchange process, the system must ensure information does not be arbitrary delete or revise to protect information integrity.
(3) Privacy: In e-commerce information exchange process, the system must avoid non authorization personnel to attend or contact the information exchange operation. In e-commerce system development process, it is necessary to build the privacy into e-commerce system and services [8].
(4) Non-Reputation: All e-commerce transaction activities must able concretely proof and record exchange information to achieve non-reputation transaction.

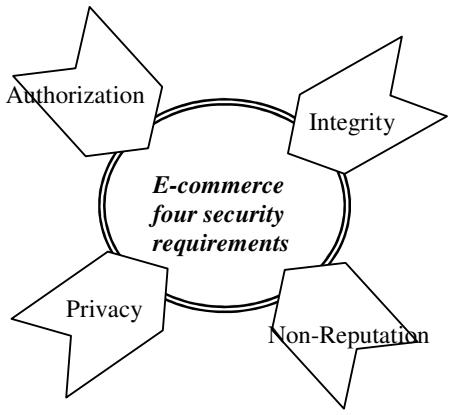

Fig.2. Holcombe e-commerce four security requirements

Many international groups and organizations (SANS, Open Web Application Security Project (OWASP)) very cared about the Web App security issues. Continued announce Web App and information system security vulnerability and security flaw: SANS Top-20 Security Risks and OWASP Top 10 [9], attempted to reduce software system security risk. According to SANS Top-

20 Security Risk [10], OWASP Top 10 [9] and Holcombe proposed four security requirements [1], software security vulnerability are divided into five classes:

(1) Authorization: E-commerce system maintenance and operation personnel must have standardized procedure and clear permissions. If the system unable to control the permissions of personnel, it will cause serious security defects and vulnerabilities.
(2) Integrity: Integrity: In the e-commerce operation process, the system must ensure that information or data does not to be arbitrarily changed or stolen. The system must ensure data integrity otherwise it will become a critical defect of e-commerce security.
(3) Privacy: In e-commerce system, user personal data and transaction information is an important privacy. The system must have the ability to protect user personal data and transaction information. When leaked user personal data and transaction information will form serious security incidents.
(4) Non-Repudiation: E-commerce system must be documented in detail all transactions information. In the event of transaction disputes, the system should ability to analyze and determine the implementation details of transactions to achieve non-repudiation, otherwise, will form the transaction disputes events and security issues.
(5) Attack and Intrusion manner: Hacker or malicious user uses many approaches to attack or intrude information system. The method of attack is varied, such as wireless network intrusion methods (packet sniffer, intermediaries intercept, access denied, fake base station attack ... etc.), or phishing, etc., are common attack or invasion tactics.

3. SECURITY TESTING AND EVENT DETECTION

E-commerce security should concern two layer operations which include security vulnerability testing [11] and security event detection.

3.1. Routine security testing

E-commerce system must develop a routine security vulnerability test to ensure e-commerce activities have security operational environment. Security vulnerability test has two major manners:

(1) Vulnerability Scan (VS): VS belongs to system internal security vulnerability and defect inspection [12],[13], [14]. In general, e-commerce software maintainer should take responsibility for the VS and execute once every six months at least. VS tools can help identify e-commerce software security vulnerability and defect to assist software maintainers process the follow repair operation. Freeware or open source VS tools [9] include NetCat, NIKTO, Paros Proxy etc. However, VS tools just only inspect source code existed security vulnerability and defect, but cannot inspect the overall e-commerce environment security. Therefore, inspection range and improvement effect have several limits. In additional, freeware or open source VS have high misjudgment rate to make software maintainer some trouble in repair operation. In order to compensate VS deficiencies, penetration test become an important and indispensable task for security preventions [9], [15], [16].
(2) Penetration Test (PT): PT is a formal security vulnerabilities and defects inspection activity [17], [18], [19]. In order to discover and identify Web app security defects, PT simulates attack approach of hacker or malicious users. In general, PT is entrusted to technology consulting organization and processed by security test professionals. Period of testing relates to the inspection range and items. However, it needs take five work days at least. PT final report should detailed describe testing execution procedure and record identified security vulnerability and defect. The follow security repair operation and improvement activity also can entrust to consulting organization to enhance Web app security.

VS tools and PT inspection do not ensure all security vulnerability and defect can be identified and repaired. Therefore, in order to identify residual security vulnerability and defect, it is necessary to create an e-commerce security checklist of human inspection [20]. According to e-commerce security, Racquel proposed human inspection checklist [16]. The purpose of security checklist is assist organization create a secure and reliable e-commerce environment for the user and make organization e-commerce system has high reliability and high security. Based on 5 compared items, advantages and disadvantages of VS, PT and human inspection are summarized into Table I.

Table I. VS, PT and auditing comparison table

Approaches / Features	VS	PT	Human Inspection
Frequency	3~6 months	half/one year	half/one year
Periods	short	long	long
Cost	low	high	middle
Personnel	System maintainer	Professional	Quality Assurance Group
Improvement	Self improvement	Consultant assistant	Self improvement

3.2. Security event detection

Security testing can effectively increase e-commerce security, but does not guarantee the e-commerce system that will not be intruded by hacker or malicious user. E-commerce system completed security testing also can not avoid security event occurrence. Therefore, the e-commerce system should plan a security event detection procedure to discover timely security event and to stop effectively the event and impact extension. Security event detection should collect all kinds security event occurrence situation. In order to timely detecting the security event and reducing damage, it is necessary to collect large logging data, analyze all possible events and quickly determine the affected severity and range. The architecture of e-commerce system (shown as Fig. 3) can be divided into four major items that include client site, application server, data base server and external entity. For analyzing all kinds security event, the interface between application server and others items should insert logging and monitoring (L&M) instrument. In addition, critical interfaces of e-commerce application software module function should also add logging and monitoring (L&M) instrument. In e-commerce system operation process, L&M instrument can collect and log all e-commerce transaction data. According to the history data abnormal situation event decision rules, the security event can be timely identified and proceed the follow improvement measure. To finish the difficult mission, three critical technologies have to be combined and work together. Three critical technologies are data logging and event monitoring that are described as follows:

(1) Data logging: In e-commerce system operation process, all transaction activities have to pass through L&M instrument interface. For each transaction activity, data logging will detailed record and save the data access person, access behavior, access time and access object. For keeping all transaction activity records, data logging needs a set of mass storage device to save and manage the logging data and should provide high performance data query capability and high efficiency management capability.

(2) Event Monitoring: For timely identifying the security event, event monitor should have the capability to quickly analyze the log data and correctly identify the event situation. Therefore, event monitor needs several supporting tools which include the rule base of security event identification, rapid data analyzer and accurate security event report generator. The

supporting tools also need high performance environment. Cloud computing is a necessary environment to provide rapid data analyzing, high speed rule base checking and mass data storage [21].

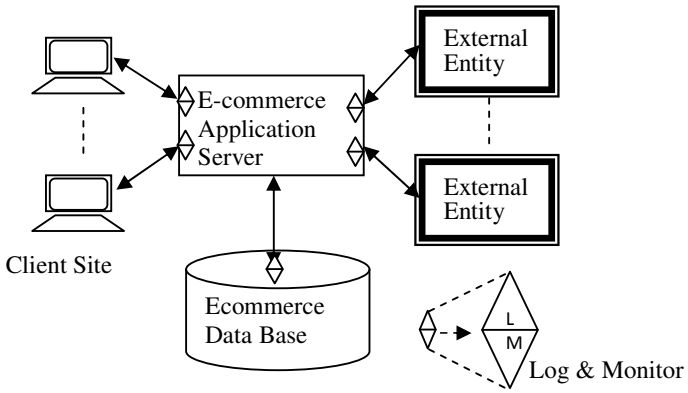

Fig.3. E-commerce security event detection architecture

The purpose of security event detection procedure is to timely detect the security event and reduce damage of the e-commerce system. For this, the paper combines data logging with event monitoring technologies to create the L&M Security Event Detection Framework (LMSEDF). Applying the LMSEDF, security event detection procedure can timely detect security event, and assist follow repair. The LMSEDF can enhance e-commerce security effectively and reduce e-commerce security risk.

Analyzing history data and event information assist to generate security event judgment rule. In this paper, collect and arrange six security event judgment rules, describe as follows:

- Abnormal access volume: System user personal data access volume over normal situation.
- Abnormal log file: Log file database appears incorrect, inconsistent and incomplete situation.
- Abnormal transaction activity: In the specific period, customer proceed too frequent or too more transaction amount activities.
- Illegal user: In system operation process, illegal user is discovered for accessing or revising customer personal data.
- Banking notification: Credit card bank emergency notify the specific customer credit card is stopping to pay.
- Customer notification: Customer discovered himself personal data or transaction information was stolen or revised, and notified the responsible unit of security event.

Event detection procedure should have high flexibility to adjustment the judgment rules. Based on security event occurred situation, the judgment rules can be appended, modified and deleted. All kinds security event can timely be identified, the severity of event impact can be reduced. E-commerce security can be effectively improved.

4. TLSPM AND OPERATION FLOW

In this section, applied routine security test and security event detection proposes the Two-Layer Security Prevention Mechanism (TLSPM).

4.1. Security prevention scheme

Enterprise or organization should develop a well security prevention strategy to protect e-commerce personal data and transaction information and increase customer privacy. First layer is the security testing and repair operation before security event occurrence. In the internet age, network and information facilities change quickly. In addition new products or environments are continuously proposed. For adapting new the products and environments, e-commerce system must continuously upgrade and maintain to satisfy user and market requirement. In addition, hacker and malicious user intrude manner and information stealing technology are renewed continuously. Making e-commerce system must develop a routine security testing procedure for identifying security vulnerability and defect before security event occurrence. The routine security testing operation should execute VS once at least every six months, and execute PT once at least every year. Security testing operation can timely identify security vulnerability and defect and assists the follow security repair operation.

Second layer is the security event detection and remedy operation after security event occurrence. E-commerce is a nonstop business information process system. Therefore, any system abnormal security event may occur in any time and always impacts e-commerce operation and may affect customer personal data and transaction information. In order to protect customer personal data and transaction information, e-commerce system should develop the security event detection and remedy operation. The detection and remedy operation belongs to nonstop procedure. In abnormal security event occurred, the detection and remedy operation can actively and timely detect security event. And, based on the event situation, procedure estimates affected scope and processes the follow remedy operation for reducing event damage. The security prevention strategy combines security vulnerability testing operation and security event detection operation, this paper defines as the Two-Layer Security Prevention Mechanism (TLSPM) (shown as Fig. 4). Security testing operation timely identifies security vulnerability and defect and assists the follow security repair operation. In abnormal security event occurred, the security event detection operation can actively and timely detect security event. And, based on the event situation, procedure estimates affected scope and processes the follow remedy operation to reduce security event damage.

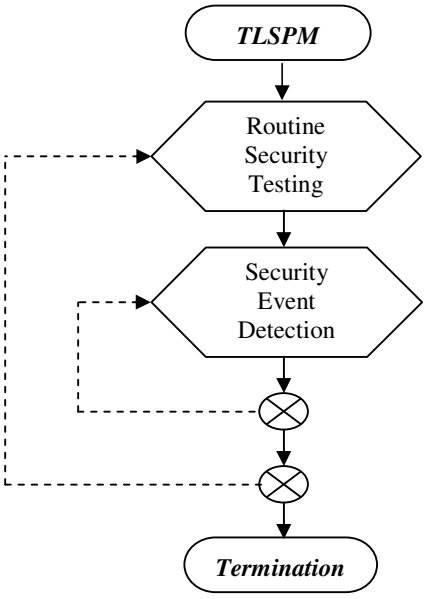

Fig.4. TLSPM operation flowchart

4.2. TLSPM Operation flow

First layer of TLSPM is a routine security testing procedure. Using VS tools and PT strategy identifies e-commerce security vulnerability and defect. Before security event occurred, e-commerce security vulnerability and defect can be timely identified and repaired to reduce security event risk. The hacker, malicious user intrusion and abnormal security event can be concretely reduced. The routine security testing procedure includes four phases and describes as follows (shown as Fig. 5):

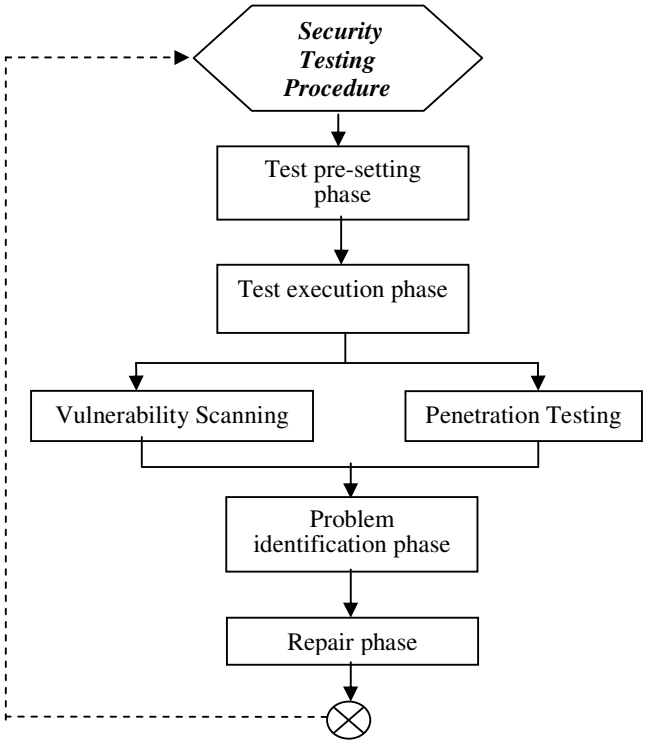

Fig.5. Security testing procedure flowchart

(1) Test pre-setting phase：
- Fully collect and parse the current Web App major and high frequency security vulnerability and defect and new hacker intrude manner.
- According to the routine security test operation, prepares a well-defined security test plan.

(2) Test execution phase：
- Arrange and design security testing steps and test cases.
- According to security test plan and test cases, execute security test and identify security vulnerability and defect.

(3) Problem identification phase：
- Analyze the identified security vulnerability and defect, and delete the misjudgment vulnerability and defect.
- Based on the confirmed security vulnerability and defect, isolate the affected environment items or software functional modules.

(4) Repair phase：
- Repair the identified and confirmed security vulnerability and defect.
- Evaluate the result of VS or PT for e-commerce security improvement.

Enterprise or organization should do their best responsibility to protect customer personal data and transaction information. Apply LMSEDF, data logging & monitoring technologies, a security event detection procedure is proposed for timely discovering the abnormal security event. The security event needs further identify and recognize to determine affected seriousness and coverage. According to affected seriousness and coverage, the recovery and repair measure should be developed to reduce the event affect extension continuously. Two kind security events described as follows:

- Lightly event is meaning a security event that affected range is small. Lightly event generally belongs to unitary event of individual or specific user. After recognized the security event cause, the suitable recovery and repair method should be planned.
- Seriously event is meaning a security event that affected range is large. Seriously event generally belongs to the case of malicious user or hacker intrusion system. Temporarily terminate e-commerce operation is necessary to reduce event affected range extension continuously.

The security event detection procedure (shown as the Fig. 6) that integrates LMSEDF, recovery and repair operations is described as follows:

(1) L&M instrument phase
- According to the e-commerce system operating environment, the logging and monitoring (L&M) instrument is added to the subsystem interface and external entity interface.
- According to the e-commerce software system functional architecture, the logging and monitoring (L&M) instrument is added to the critical function module interface.

(2) Event detection phase:
- In the e-commerce operation process, non stop monitor all kind transaction behaviors and data transformation activities.
- According to the predefined judgment rules, identify all possible security events.

(3) Event recognition phase
- Deeply analyze identified security events and recognize all real security events.
- Parsing security events severity and influence for understanding the affected degree of customer personal data.

(4) Temporary terminate phase
- According to security events severity, decide to terminate some functions or stop temporary all e-commerce system operations.
- According to the identified security vulnerability and defect, develop and plan security vulnerability repair and e-commerce system recovery strategy.

(5) Recovery phase：
- Analyze and determine the cause of security events and according to the security vulnerability and defect, develop vulnerability repair strategy and define e-commerce system recovery measure.
- Recovery e-commerce system normal operations as soon as possible.

5. EFFICIENCY EVALUATION OF THE TLSPM

Hacker and malicious user intrusion approaches and technologies grow up continuously. Additional, in the e-commerce system maintenance process, personnel negligence is unable to be avoided. Therefore maintenance process may cause system security vulnerability and defect. These problems are e-commerce system must be faced and overcome. Combining routine security test and security event detection procedures, the paper proposes the Two-Layer Security Prevention Mechanism (TLSPM). Routine security testing procedure can effectively identify

security vulnerability and defect to enhance e-commerce security. Based on the LMSEDF, Security event detection procedure can timely identify abnormal security event to reduce e-commerce system damage impact and increase customer personal data and transaction information security. LMSEDF major advantages are:

- Applied logging and monitor technology to overcome large log data storage problem and timely reach log data analyzing effect.
- Not only log and monitor system, subsystem and entity interface access data, but also log and monitor the critical module interface access data.
- Timely detect security event and use effectively strategy to reduce the event extension. Not just repair the event vulnerability.

Three advantages of TLSPM describe as follows:

- Before security event occurrence, routine security testing procedure can effectively identify and repair security vulnerability and defect to enhance e-commerce security.
- After security event occurred, security event detection procedure can timely identify abnormal security event to reduce e-commerce system damage impact.
- Two-layer prevention procedure can achieve complementary effect and effectively reduce the risks of e-commerce security.

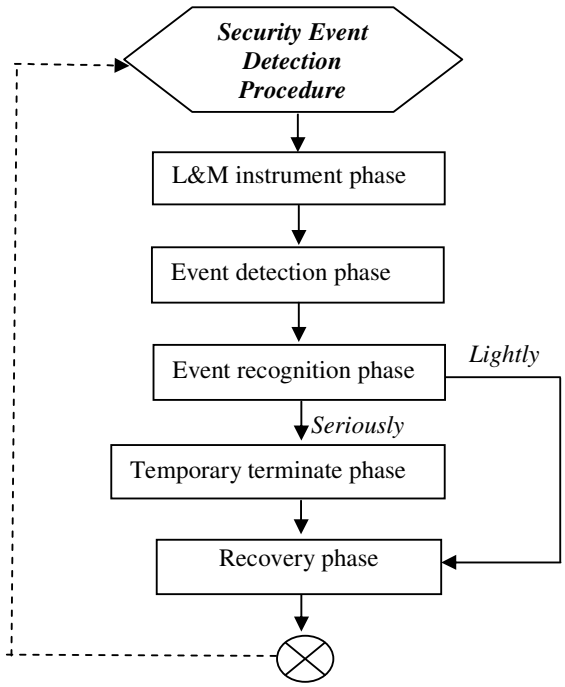

Fig.6. Security event detection operation flowchart

6. CONCLUSIONS

In the internet popularity age, e-commerce system already melted into the people everyday life. How to avoid security flaws and defects of the system caused user significant loss has become an important topic of e-commerce. Security testing can effectively increase e-commerce security, but does not guarantee e-commerce system will not be intruded. In abnormal security event occurred, the detection and remedy operation should actively and timely detect security event. And, in order

to reduce damage, the security event detection procedure should concretely assist the follow remedy operation. The security prevention strategy should combine security testing and security event detection two critical procedures. For this, the paper proposes a Two-Layer Security Prevention Mechanism (TLSPM). Security testing procedure concretely improves e-commerce system security vulnerability and defect. Security event detection procedure timely identify security event and fully reduce event extension. Two-layer prevention procedure can achieve complementary effect and effectively reduce the risks of e-commerce security. TLSPM major advantages are:

- Before security event occurrence, routine security testing procedure can effectively identify and repair security vulnerability and defect to enhance e-commerce security.
- Two-layer prevention procedure can achieve complementary effect and effectively reduce the risks of e-commerce security.
- Timely detect security event and use effectively strategy to reduce the event extension. Not just repair the security vulnerability.

In addition, the security event detection procedure also can collect the function usage of e-commerce. Optimizing and Enhancement high usage functions can assist to improve e-commerce system performance and security.

ACKNOWLEDGMENT

This research was supported by Shih Chien University 2015 research project funds (Project No.: 104-08-01001).

REFERENCES

[1] Holcombe, C. (2007), Advanced Guide to e-Commerce, LitLangs Publishing.
[2] Eddy, Nathan, (2015), E-Commerce Sales to Top $1.7 Trillion in 2015", eWEEK, Posted 2015-07-17. (http://www.eweek.com/small-business/e-commerce-sales-to-top-1.7-trillion-in-2015.html)
[3] Wevio, (2015), "Global B2C E-commerce Sales to Hit $1.74 Trillion in 2015" (http://www.wevio.com/research-and-analysis-articles/global-b2c-e-commerce-sales-to-hit-1-74-trillion-in-2015/)
[4] Evan, S., (2006) "Gartner: $2 Billion in E-Commerce Sales Lost Because of Security Fears," 2006/11/27, pcmag com (http://www.pcmag.com/article2/0,2817,2064021,00.asp)
[5] Gun, J.X. (2010), Eighty percent people, fearing online shopping experience "fraud", 104survey.com, (in Chinese)
[6] http://www.104survey.com/faces/newportal/viewPointCtx.xhtml;jsessionid=70AFB339F7F99D2503FBD40CBF199DD4.svyweb202?researchId=254)
[7] J. Pepitone, (2011) "Massive hack blows crater in Sony brand," staff reporter CNNMoney Tech. (http://money.cnn.com/2011/05/10/technology/sony_hack_fallout/index.htm)
[8] Penetration Testing vs. Vulnerability Scanning (http://www.tns.com/PenTestvsVScan.asp)
[9] Knuston, Tina R. (2007) "Building Privacy into Software Products and Services," IEEE Security and Privacy, vol. 5, no. 2, pp.72-74.
[10] OWASP Top 10. (2013) (https://www.owasp.org/index.php/Top_10_2013-Table_of_Contents)
[11] SANS Top-20 Security Risks, (2013) (http://www.sans.org/critical-security-controls/).
[12] Potter, B. and G. McGraw, G. (2004) "Software security testing," IEEE Security and Privacy, vol. 2, no. 5, pp. 32-36.
[13] Hadavi, M. A., H Sangchi,. M., Hamishagi, V. S., Shirazi, H., (2008) "Software Security, A Vulnerability- Activity Revisit," The Third International Conference on Availability, Reliability and Security.
[14] Kals, S., Kirda, E., Kruegel C., and Jovanovic, N. (2006) "SecuBat: a web vulnerability scanner," Proceedings of the 15th international conference on World Wide Web, pp. 247-256.

[15] Lai, Y.P. and Hsia P.L (2207) "Using the vulnerability information of computer systems to improve the network security," Computer Communications, vol. 30, issue 9, pp.2032-2047.
[16] McGraw, G. (2004), "Software Security," IEEE Security & Privacy, vol. 2, no. 2, pp. 80-83.
[17] Racquel (2013), 15 Point e-Commerce Security Checklist, 2013/3 (https://www.swipehq.com/blog/post/15-point-e-commerce-security-checklist/1395)
[18] Arkin, B., Stender, S. & McGraw, G., (2005) "Software penetration testing," IEEE Security & Privacy, vol. 3, no. 1, pp. 84-87.
[19] Bishop, M. "About penetration testing," IEEE Security & Privacy, vol. 5, no. 6, 2007, pp. 84-87.
[20] Thompson, HH (2005) "Application Penetration Testing," IEEE Security & Privacy, vol. 3, no. 1, pp. 66-69.
[21] Garzoglio, G. (2010) "A Code Inspection Process for security reviews," Journal of Physics: Conference Series, vol. 219,
[22] Dean, J. and Ghemawat, S., (2010) "MapReduce: A Flexible Data Processing Tool." CACM, vol. 53, no.1, pp. 72–77.

AUTHORS

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.