INTRODUCTION

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. 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. It means that software security has become the most important topic for business activities and behaviors. Security of e-commerce transaction becomes a critical issue and should be concerned. 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. In this paper, security issues of e-commerce are discussed. The paper discusses the security of transaction activities to integrate efficiently ecommerce security requirement. The importance and impact of e-commerce security is described and critical quality characteristics of security requirement are discussed. The aim of the paper is to propose method of e-commerce security policies, and to specify the benefits of encryption methods and techniques to secure e-commerce transactions.

1 SECURITY IN E-COMMERCE

The popularity of the Internet has been growing at astonishing speed, which changes the overall objective of the defence to commercial applications [13]. Electronic commerce is buying and selling of goods and services across the Internet. In the development of e-commerce, security has always been the core and key issue that support its adoption [16]. Customers must be able to select a mode of payment and the software must verify their ability to pay. This can involve credit cards, electronic cash, encryption, and purchase orders. The more of these techniques are supported by an e-commerce package, the more secure the system can be, and therefore the more customers are benefits from e-commerce abilities. Web e-commerce applications that handle payments have more compliance issues, are at increased risk from being targeted than other websites and there are greater consequences if there is data loss or alteration. Security is very important in online shopping sites. Now days, a huge amount is being purchased on the internet, because it’s easier and more convenient. In the traditional commerce, participant can face to face, so there may be little distrust. However, there is difference in electronic commerce. For example, in electronic commerce, the location of the business and the goods are unknown. More important, there is not personal contact between the seller and the buyer. Risks related to electronic transactions should be identified and controlled in order to enhance the integrity in e-commerce. Without proper controls, electronic transactions and documents can be easily changed, lost, duplicated, and incorrectly processed, thereby, causing disputes on terms of transactions and related payments.

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. And, 42% people occurred personal data lost or happened fraud event [9]. Therefore, famous corporation and organization very concerned on information security and used all approaches to defense hacker intrusion and protect customer personal data. Each e-commerce system must satisfy four indivisible requirements [2]:

- **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 [6]. In order to satisfy four indivisible security requirements and vulnerability defense capability, e-commerce should have three ways software security requirements as follows:

- **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.

- **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.

- **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 behavior security and avoiding future disputes. So, transaction behavior should build a standard operation procedure and provide a complete and reliable transaction behavior logged mechanism to reach e-commerce transaction behavior non-repudiation [4].

High security requirement should have three critical quality characteristics which includes security requirement compliance, requirement availability and requirement manageability [7]:

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. 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.

E-commerce is widely considered the buying and selling of products over the Internet. 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. Security is one of the crucial issues affecting the development of e-commerce. E-commerce web service that wants to have a competitive edge in today’s global marketplace should adopt a comprehensive security policy.
2 SECURITY ASSURANCE METHOD IN ON-LINE TRANSACTION

In the e-commerce transactions, e-commerce security is mainly network security and transactions security. The network security is the network operating system against network attacks, viruses, so that keep a continuous and stable network operation, commonly used firewall technology protection measures. Transaction security is the data protection of the parties are dealing not be destroyed, as both nondisclosure and transaction identity confirmation. Commonly used transaction security method are: encryption, digital certificates and authentication, SSL (Secure Socket Layer) security protocol, SET (Secure Electronic Transaction), and Public Key Infrastructure (PKI).

Public Key Infrastructure (PKI) refers to the notion that the best way to establish a system of secure communications over networks is to establish an infrastructure that will support public key encryption. The PKI would create an environment where any Internet user could have certificates around that identify them in a variety of ways. Authentication of parties could become very cheap and easy. Some e-commerce proponents suggest that creation of a seamless and robust PKI would have enormous implications for speeding the growth of e-commerce. E-commerce software packages should also work with secure electronic transfer (SET) or secure socket layer (SSL) technologies for encryption of data transmissions [6].

SSL technology, the global standard security Internet, encrypts and protects the information transmitted in the network via the https protocol, whose use is greatly extended. With this system data in transit is protected, otherwise, data could be intercepted and manipulated. An SSL certificate is an electronic file that allows the encrypted communication and clearly establishes the identity an individual or website [5].

In cyberspace, both the customer and the vendor have difficulty in proving their identity to each other with certainty, particularly during a first transaction. Clients need to be sure that: they are communicating with the correct server, the message is delivered unmodified, they can prove that they sent the message, only the intended receiver can read the message, delivering is guaranteed. On the other side, vendors need to be sure that: they are communicating with the right client; the content of the received message is correct; the identity of the author is unmistakable; only the author could have written the message, they acknowledge receipt of the message. All of the concerns listed above can be resolved using some combination of cryptographic method, and certificates methods [3].

There are many ways in which the companies can overcome the issue of security and confidentiality of the data. These include data Encryption, Certificates and Certificates with Extended Authentication Validation (EV) and Trustmark.

Encryption is a technique whereby the data is transformed into information that can only be unintelligible decipher its rightful recipient. Protection integrity and confidentiality are achieved with this method are fundamental to EC, and that partners and customers of an enterprise share information or make purchases on a website if they feel that do not pose any danger. The solution for who want to provide these guarantees is to adopt trust infrastructure based on technology encryption [7].

Certificates with Extended Validation (EV) offer an authentication higher than any other SSL certificate, more structured and tight controls. First instead, the contact person of the company must provide a signed document confirming the request. In case that the certifying authority could not confirm identifying information of the company in a database official data, the company may request documentation commercial registration [3].

To earn the trust of their customers and enhance their income, EC companies not only need to protect data transmitted on their sites web, but also show how they are being done. The seals of certification authorities (also called trust marks) are a way to show customers that they are protected and gain their trust by a visible sign of security. The VeriSign seal is the most widely used security badge and recognized worldwide. Clicking on it shows the name of the certificate owner, the period of validity of this, information on services including security and other data on the validation process that follows VeriSign before issuing the certificate. In an analysis study, marks made to VeriSign (VeriSign Brand Tracking Research), 11 per cent of respondents indicated that on occasion, the
absence of the VeriSign seal was determining factor for not using a trade website mail or make purchases on it [12].

In B2C transactions, the credit card is the most widely used method of payment for Internet ecommerce transactions. Internet users purchase goods by transmitting their credit card number via a secure form. The threat of credit card fraud is arguably the most serious issue of concern to e-commerce participants, including consumers and merchants. SSL/TLS and SET are two widely discussed means of securing online credit card payments. Because of implementation issues, SET has not really been adopted by e-commerce participants, whereas, despite the fact that it does not address all security issues, SSL/TLS is commonly used for Internet e-commerce security. The main advantage of SSL/TLS, when used to protect e-commerce transactions is ease of use for e-commerce end-users. The cardholder can use SSL/TLS completely transparently because it is already built into commonly used web browsers, and merchants can also implement SSL/TLS without changing their payment model in any way. The system is not complex, resulting in minimal impact on transaction speed. But SSL-based e-commerce permits the merchant to see consumer payment information, potentially causing security concerns to cardholders. The merchant cannot reliably identify the cardholder. In cases where consumers use a stolen credit card to initiate e-commerce transactions, merchants are responsible for ‘card not present’ transaction charge backs. SSL/TLS protects only the communications link between consumers and merchant, it does nothing to protect sensitive cardholder information whilst it is stored at the merchant server. Merchants therefore need to implement additional security measures to protect the secrecy of this information [10, 11].

SET ensures the confidentiality of payment information at all stages of transaction processing, including data transmission and data storage, and prevents the merchant from seeing consumer payment information, since the payment information is forwarded to the acquirer in encrypted form. To ensure merchant privacy, SET prevents the acquirer from seeing consumer order information stored at the merchant web server. But implementing SET is more costly than SSL/TLS for both consumers and merchants. Using SET is much more complicated than using SSL. SET does not permit the cardholder to place an order from PCs other than the cardholder’s SET-initialized PC because the cardholder’s private key required to conduct a SET transaction is stored in this PC. SET employs complex cryptographic mechanisms that may result in an unacceptable transaction speed [8].

In electronic payment systems, there are four main types of participant, namely consumers, merchants, issuers, and acquirers. Consumer purchases products or services from the merchant via the Internet. Merchant sells products or services to the consumer via the Internet. Issuer issues the consumer a credit card and also responds to an online payment request from the acquirer via the payment gateway. Acquirer forwards the payment request from the merchant to the issuer via the payment gateway [6].

3-D Secure and 3D SET are built upon the relationships between three domains, namely the acquirer, issuer, and interoperability domains. The acquirer domain covers the relationship between the merchant and acquirer. The issuer domain covers the relationship between the cardholder and the issuer. The relationship between the acquirer and issuer domains is supported by the interoperability domain. The 3-D Secure payment system can be regarded as the integration of SSL with the 3D model. When it is used simply to protect the cardholder-merchant link, SSL/TLS does not provide verification of the cardholder, which can result in credit card fraud at the consumer side [14].

Integration of the 3D architecture with SSL can help address this issue. 3-D Secure, originally known as 3D SSL, was developed by Visa. In 3-D Secure, the payment gateway, which provides an interface between the merchant and acquirer’s payment system and the Visa proprietary payment network VisaNet, must be implemented in the acquirer domain [15]. Merchants are responsible for installing an SSL/TLS Merchant Plug-In (MPI) at their servers. For 3-D Secure, this MPI is required to have additional functions to handle communication with a centralized Visa directory [1]. Within the Issuer domain, each card issuer is required to maintain a special server known as the (ACS). The Access Control Server is used to support cardholder authentication. The Visa directory is a server in the Interoperability domain, used to enable communications between merchant servers and card issuers. To protect the security of communications between the various entities, 3-D Secure requires
the following links to be protected using SSL/TLS: cardholder-merchant, cardholder-ACS, merchant-Visa Directory, and Visa Directory-ACS, Visa 3-D Secure [15].

3D SET (Server-based SET) is another 3D payment scheme that predates 3-D Secure. 3D SET was developed by a number of SET software vendors, and maps the SET payment system into the 3D model. As a replacement for the traditional SET digital wallet that must be stored at a consumer PC, 3D SET uses a SET Wallet Server in the issuer domain. The cardholder’s certificate is also securely stored at the issuer’s secure server. Within the acquirer domain, there is no need for the merchant to have a certificate installed at the merchant server. As in the issuer domain, the acquirer stores the merchant’s certificate and implements the payment gateway at the acquirer secure server [1].

3 E-COMMERCE SECURITY ASSESSMENT

Major problems are Web site security and the lack of Web site trust. Most commercials Web sites provide some forms of secured payment method, it doesn’t guarantee that the Web sites will gain better credibility.

Hassler states that security requirements for electronic payment systems include confidentiality, integrity, authentication, and non-repudiation. Following this approach, the following security requirements can be identified for the e-commerce end-users [2]:

– Payment confidentiality – Consumer financial information must be kept confidential, including during transmission and storage. Here, the consumer is the entity requiring the confidentiality service, while the merchant is the entity providing the service.
– Payment integrity – The integrity of the transaction must be protected, including during transmission and storage. Both consumer and merchant require this service.
– Entity authentication – Both consumers and merchants require entity authentication services in order to verify the identity of the entities with whom they are dealing.
– Non-repudiation – The transaction must have such services that enable one party to prevent another party denying having taken a particular action, sending order or payment information, confirmation of order or payment. Both consumer and merchant also require this service.

Besides the following end-user implementation requirements can be identified [12]:

– Usability – The system must be easy to implement, including installation. The consumer requires the card issuer and merchant to provide a secure system that is not complex, while the merchant requires the acquirer and security software developers to provide a simple application that meets the security requirements.
– Flexibility – The system must allow e-commerce consumers to order products or services from any location, and not just from one PC. Here, the consumer is the entity requiring the flexibility service, while the merchant is the entity providing the service.
– Affordability – The costs of implementing and using the system must be affordable for consumers and merchants, since these end-users are unlikely to be prepared to pay significantly extra to participate in Internet e-commerce transactions. For example, consumers are not willing to pay for a digital certificate in order to conduct e-commerce transactions although it is required in some e-payment scheme such a SET. Merchants will also not wish to invest significantly in engineering e-payment infrastructure
– Reliability – The system must be reliable since it is used for the transmission and manipulation of sensitive information.
– Availability – The system must be available when needed.
– Speed of transaction – The transaction speed must be acceptable for e-commerce end-users.
– Interoperability – The system must be interoperable between different computing platforms, web browsers and server software packages in order to enable its use by the widest possible spectrum of e-commerce consumers and merchants.
According to ISO916, security refers mainly to the ability of the system to provide a secure transaction environment. Its role is to support e-commerce credibility and this can be accomplished by increasing the confidence in commercial transactions over the web, where transacting parties are invisible to each other. The privacy of the system may be based on privacy seals such as TRUSTe, CPA WebTrust and BBBOnline [4]. These privacy seals should be familiar to the user who should understand their functional use. It should be mentioned that security has an important role to e-commerce system success and it is a multidimensional quality characteristic related with aspects as confidentiality and integrity [6].

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. 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 [9]:

   - Personal Data Security (PDS) should measure by the primitive factors of personal data collection, handling and usage management system.
   - System Operation Security (SOS) should measure by the primitive factors for security encryption measures, an intrusion detects mechanism and data backup procedure.
   - Transaction Security (TS): should measure by the primitive factors of a secure transaction guide and non-repudiation system.
   - Combine with personal data security, system operation security and transaction security metrics into the Security Requirement Compliance Measurement.

2. Security Requirement Availability Measurement is combined with requirement document basic quality and requirement item verification and validation quality. Security Requirement Availability Measurement generation steps describes as follows:
   - Requirement Document Basic Quality (RDBQ) should measure by clarity, completeness, consistency and readability basic factors of security requirement documents.
   - Requirement Items Verification and Validation Capability (RIVVC) should measure by inspection check lists planning quality and security test cases design quality.
   - Combining with RDBQ and RIVVC into Security Requirement Availability Measurement.

3. Security Requirement Manageability Measurement is combined with requirement item complexity, version control and traceability quantified quality characteristics. Security Requirement Manageability Measurement generation steps describes as follows:
   - Requirement Item Complexity (RIC) should measure by item inter relations and item size two basic quality factors.
   - Requirement Item Version Control (RIVC) should measure by item change control and item version control two capabilities basic quality factors.
   - Requirement Item Traceability (RIT) should measure by two basic quality factors of items cross-reference table and item and phase documents cross-reference table.
   - Combine RIC, RIVC and RIT quantified quality characteristics into a Security Requirement Manageability Measurement.

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 table 1.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Data Security</td>
<td>Requirement Items Verification and Validation Quality</td>
<td>Requirement Items Complexity</td>
<td></td>
</tr>
<tr>
<td>System Operation Security</td>
<td>Requirement Document Basic Quality</td>
<td>Requirement Items Version Control</td>
<td></td>
</tr>
<tr>
<td>Transaction Security</td>
<td>Requirement Items Traceability</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

There are many significant factors which could influence the security and trust level of the commercial Web sites. An effective security assessment tool must be able to identify and determine all factors influencing security level of the e-commerce Web sites and payment systems.

CONCLUSIONS

E-commerce system must have the responsibility to protect customer important privacy which includes personal data and transaction information. Customers’ perceptions of the security and trust of e-payment systems and commercial web service, implemented by companies trading online, have become a major factor in the evolution and futures development of e-commerce. 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. Companies can overcome the issue of security and confidentiality of the data by adopting sophisticated security measures such as Encryption, Secure Socket Layer (SSL) Certificates, Certificates with Extended Authentication Validation (EV) and Trustmark. Security requirements are major critical 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 to achieve the system’s security. 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. Security is one of the principal and continuing concerns that restrict customers and organizations engaging with e-commerce.

Abstract

The growth of e-commerce has been inhibited by consumer fears and concerns about the risks, real and perceived. E-commerce will not reach its full potential unless consumers perceive that electronic transactions are secure and associated risks have been reduced to an acceptable level. This paper discusses the risks associated with e-commerce transactions and the methods to gain consumers’ trust in order to enhance their acceptance and participation. Risks related to electronic transactions should be identified and controlled. Transaction security can be enhanced with information technologies. They help prevent consumer personal information, such as credit card numbers and other vital information, from being intercepted and stolen during transmission. Security practices help protect customer information from being intentionally or unintentionally disseminated to or being accessed by unauthorized third parties. Standard controls on business functions of an information system also help to guarantee the accuracy of business transactions.
Streszczenie

Rozwój handlu elektronicznego jest w dużej mierze hamowany przez obawy konsumentów dotyczące związanego z transakcją ryzyka, zarówno przewidywanego jak i rzeczywistego. Handel elektroniczny może w pełni rozwinąć swój potencjał, jeżeli transakcje internetowe będą odpowiednio zabezpieczone, a związane z nimi ryzyko zostanie zredukowane do akceptowalnego poziomu. Praca przedstawia ryzyko związane z transakcjami handlu elektronicznego oraz metody jego redukcji, co ma na celu zapewnienie akceptacji klientów i ich udział w transakcji. Ryzyko związane z tego typu transakcjami powinno być identyfikowane i kontrolowane. Bezpieczeństwo transakcji może być zapewnione dzięki technologiom internetowym. Ich wykorzystanie pomaga chronić dane osobowe konsumentów, numery kart kredytowych i inne ważne informacje, które mogą być przejęte i skradzione podczas transmisji. Zapewnienie bezpieczeństwa transakcji pomaga chronić dane klientów przed ich nieuprawnionym rozpowszechnianiem oraz nieuprawnionym dostępem osób trzecich, a standardowa kontrola systemu informatycznego serwisu zapewnia bezpieczeństwo transakcji.

REFERENCES