POS System Design in Security Level 1st*

Seok-soo Kim and Tai-hoon Kim

Department of Multimedia Engineering, Hannam University, Daejeon, South Korea
Sskim@hannam.ac.kr, taihoonn@empal.com

Abstract

POS system is a supply net administration system for customer management. It becomes an essential element in distribution industry to construct database, and uses XML-Encryption to complement PKI techniques and standards for security. POS system has four advantages. First, it does not have to be certificated and transmit data every time because there is no server. Second, it can integrate database by using XML and improve portability of program itself. Third, transmitted data is safe because of XML-Encryption. Fourth, processing speed will be faster because it gathers data from data transmission. All systems should be designed by considering security level to reduce non-necessary burdens. The concept of security level management was developed by Dr. Tai-hoon Kim a few months ago, and this paper used this idea. In this paper, Security Level 1st environment was considered to design POS systems.

1. Introduction

In 21st century, reform of circulation on physical distribution is expected. Domestic circulation companies' profitability improvement, sale increase, decrease of circulation expense and necessity to raise efficiency of circulation system is increasing now. And there is an opening of secondary market in the point of increase and pattern change of consumption demand, and internal rise of personnel expenses of purchasing power by elevation of national income level, traffic congestion etc., and circulation company's customer service improvement and buries of various goods, sale. Also POS system which inventory present condition of store to manage all sale information efficiently is opining secondary market [1].

This study is about a method to use POS system that is becoming more important in the world because it is safe and fast. Existing POS system had begun receipts and developed into present web POS system. This web POS system emphasizes safety of data and considers improvement of the processing speed with wire or wireless device. Existing web database constructing distributed processing POS system that is not existing server/client structure using XML the processing speed and portability and integration attribute heighten and this distributed processing POS system using PKI (Public Key Infrastructure) to worm with web each posthumous work and posthumous work connect and supply efficient XML Security by using XML-Encryption [2].

Dr. Tai-hoon Kim proposed the concept of Security Level Management, and this idea can be applied to all IT areas. In this paper, Security Level 1st environment was considered to design POS systems.

2. Security Level

* "This work was supported by a grant from Security Engineering Research Center of Ministry of Commerce, Industry and Energy".

In general, threat agents' primary goals may fall into three categories: unauthorized access, unauthorized modification or destruction of important information, and denial of authorized access. Security countermeasures are implemented to prevent threat agents from successfully achieving these goals.

Security countermeasures should be considered with consideration of applicable threats and security solutions deployed to support appropriate security services and objectives. Subsequently, proposed security solutions may be evaluated to determine if residual vulnerabilities exist, and a managed approach to mitigating risks may be proposed.

Countermeasures must be considered and designed from the starting point of some DSS design or software development processes. The countermeasure or a group of countermeasures selected by designers or administrators may cover all the possibility of threats. But a problem exits in this situation. How and who can guarantee that the countermeasure is believable?

Security engineering may be used to solve this problem. In fact, the processes for building of security countermeasures may not be fixed because the circumstances of each DSS may be different.

We propose a method for building security countermeasures as below.

2.1. Threats Identification

A 'threat' is an undesirable event, which may be characterized in terms of a threat agent (or attacker), a presumed attack method, a motivation of attack, an identification of the information or systems under attack, and so on.

Threat agents come from various backgrounds and have a wide range of financial resources at their disposal. Typically Threat agents are thought of as having malicious intent. However, in the context of system and information security and protection, it is also important to consider the threat posed by those without malicious intent. Threat agents may be Nation States, Hackers, Terrorists or Cyber terrorists, Organized Crime, Other Criminal Elements, International Press, Industrial Competitors, Disgruntled Employees, and so on.

Most attacks maybe aim at getting inside of information system, and individual motivations of attacks to "get inside" are many and varied. Persons who have malicious intent and wish to achieve commercial, military, or personal gain are known as hackers (or cracker). At the opposite end of the spectrum are persons who compromise the network accidentally.

2.2. Determination of System Security Level and Robustness Strategy

Robustness strategy should be applied to all components of a solution, both products and systems, to determine the robustness of configured systems and their component parts. It applies to commercial off-the-shelf (COTS), government off-the-shelf (GOTS), and hybrid solutions. The process is to be used by security requirements developers, decision makers, information systems security engineers, customers, and others involved in the solution life cycle. Clearly, if a solution component is modified, or threat levels or the value of information changes, risk must be reassessed with respect to the new configuration [3].

Various risk factors, such as the degree of damage that would be suffered if the security policy were violated, threat environment, and so on, will be used to guide determination of an appropriate strength and an associated level of assurance for each mechanism. Specifically, the value of the information to be protected and the perceived threat environment are used to obtain guidance on the recommended evaluation assurance level (EAL).

Furthermore, to decide systems security level, EAL is not a perfect one. So we should decide TL (Threat Level) and AL (Asset Level) to get more exact SL (Security Level). About the decision of SL, please recommend our report [4].

Table 1. Determination of Security Level by Threat Level and Asset Level

Asset Level	Threat Level					
	TL1	TL2	TL3	TL4	TL5	TL6
AL1	**SL1**	**SL1**	**SL1**	**SL1**	**SL2**	**SL2**
AL2	**SL1**	**SL1**	**SL2**	**SL2**	**SL3**	**SL3**
AL3	**SL1**	**SL2**	**SL2**	**SL3**	**SL3**	**SL4**
AL4	**SL1**	**SL2**	**SL3**	**SL3**	**SL4**	**SL4**

3. Authentication and Encryption

In Security Level 1 environment, designation of security countermeasure is not difficult. In this paper, we used XML security countermeasure.

To take an advantage of web POS system and single POS system used in existing to embody distributed processing POS system, it is needed certification and encryption technology to change environment and has to be connected this breakup system in the Internet and use XML database by distributed processing system in existing server/client structure. Authentication is process that confirms whether unauthorized users are going to use and what are they going to do. Usually, using credential such as password, PIN (Personal Identification Number), smart card and certification is consisted in web service between applications mainly, and recentralized ordinary password or certificate.

Because this research produces certification, certification must offer information (IP, OS, certification number etc.) of hardware (PC, PDA) which has the program. And certification server has to be operated with system. Encryption acts role that secure integrity so that someone may not be able to read this even if get seized data in midway.

Need encryption key and cipher for encryption. Encryption description is 'symmetric' and 'asymmetric' way.

4. XML security

XML (Extensible Markup Language) is language of tag form to define and expresses structure of document that has information. ‘That can extend' (Extensible) document means it can define structure in the documents and can change to structure of other documents. 'Mark household mascot language' (Markup Language) means high position information by Tag. When HTML in the internet is used much, in W3C (World Wide Web Consortium) SGML (Standard Generalized Markup Language) thing made curtly by base XML be. XML is used for standard of expression and exchange of information in industry.

It is expressed in the form of analog tag with HTML. But HTML has data of document and information about expression at the same time. XML documents are separated and expressed these mainly. Data of XML document is hierarchic and structural form and it is information about expression composes style document (Style Sheet) in the form of XML document. Through separated function of these data and expression, XML permits data to save and exchange between other programs regardless of Operating System. Also, it can define document structure voluntarily and get into recent publication of Business-to-Business solution because conversion is available [5].

XML's commission is basically beginning tag and end tag matching. Mark information that arranges data between tag interior and tag. It is known that beginning tag through end tag is one pair of Element and Elements are composed hierarchically. There is an attribute in the Element’s tag. There is capital have other Element that form tag form between Element's tag and Element of Text form can have. Speak of that Element, Text, Attribute etc. are all Nodes.

The following is example of simple XML document that display sale recording of bookstore. If you use this XML for database, must encrypt and use XML having shortcoming which reveals information of data just as it is. Application that follow XML encryption standard must embody all elements explained here as long as there is no especial reference. It must be included Encrypted Data, Cipher Data, Encryption Properties, ds:KeyInfo necessarily. This XML encryption has following structure of Figure 1.

This encryption method has four encryption methods: encipherment, encipherment of XML element contents, free data encipherment, supermarket encryption and so on. By encryption of XML elements, it can encrypt element from beginning tag to end tag on the whole at first and can hide this element.

Second, encryption of XML element contents is used because element sees but go side by side with element whole encryption that talks in front that enciphers contents of element.

```
<EncryptedData Id? Type?>
<EncryptionMethod/>?
    <ds:KeyInfo><EncryptedKey>?<AgreementMethod>?
       <ds:KeyName>?<ds:RetrievalMethod>?<ds:*>?
       </ds:KeyInfo>?
    <CipherData>
       <CipherValue>?(CipherReference URI?)?</CipherData>
    <EncryptionProperties/>?
</EncryptedData>
```

Figure 1. Structure of XML encryption

Third, free data decipherment is a method to treat included whole data by Octet stream simply, and super encryption must encrypt whole element necessarily in case of use Encrypted Data or super encryption of Encrypted Key element that encrypt again encoded already information finally. This research used encryption of XML element contents.

5. Distributed Processing POS system with XML-Encryption and PKI

As referring at the instruction, POS system is available by real time control of goods in stock and sale analysis at present. Therefore, it can make efficient consumer's sale data, and these sale data is essential to introduce SCM and CRM. This POS system developed into web POS system structure which is server/client structure at single program.

Figure 2 explains a present system. It is timing diagram. This timing diagram shows whole POS system change a state which pictured like diagram as passage of time. It is decided in visual point that certification and connection work are to flow time if see this reversed character and each program of this timing requires. We can get four advantages by forming this structure.

Because there is no first server, it does not need to attempt get authentication and data transmission every time. Because of the data that each client program handles by oneself, network has impossibility or place that real time network is unnecessary data client voluntarily have and transmit to network for integration of data when need. Can integrate data base by second XML and improve portability of program itself.

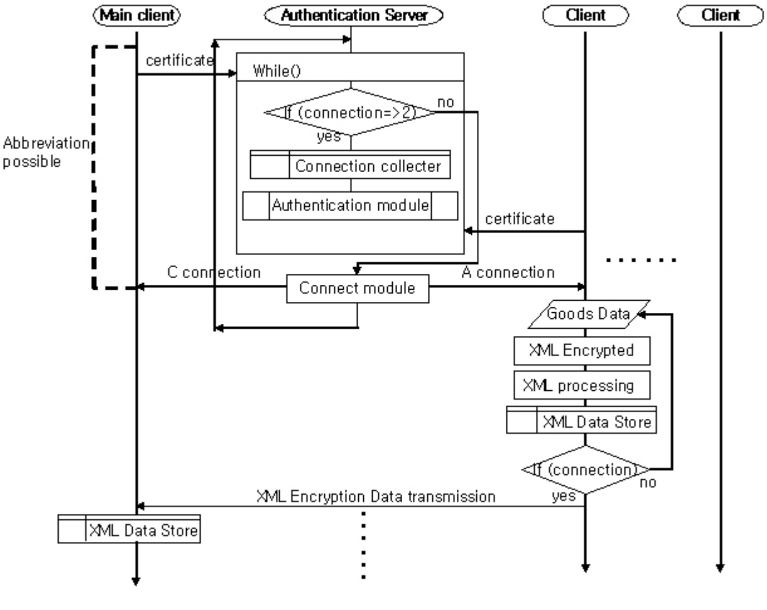

Figure 2. POS system timing diagram

Because performance of present Mobile improves, if PDA that loaded OS is most and installs this client program, transmission of data is available via network gear city certification process as well as itself save of data. Because used XML encryption in third data transmission, transmission time is shortened. It is a present condition that does not recognize Security of data about circulation yet, it can speak that it is important information of corporation as well as data that computerization of all circulation data is such if it is achieved forward. Fourth, to improve distributed processing and processing speed of POS system on client program, transmit it because gathering all data when transmit data after encoding whenever data is processed. In the case of existing system, server processes data and server's investment expense was spent much. Each client's business processing saves improved data but data amount will be a problem. That quantity of product which a customer average of 20, in case medicine 10KB's data is created and sells 1 thatched cottage separated from the main building of house 1 goods in case caught, about 6 persons process data of 864 people for 36 people 24 hours at 1 hour at 1 minute. Data of 864 people is about 8 MB. Client one data uses data of 240 MB in case is grass operation 8 MB two faces month in case is 24 hours. In the case of present POS system hardware, it can collect data about 6 months about 2 years because it is generally using hard-disk of 40 GB. Amount of data has shortcoming that must play bulky case backup faithfully by that form these structure.

6. Conclusions

So that can be loaded PDA or Mobile or etc. to be utilized by Ubiquitous, designed way and processing of these data and all-in-one that use itself data base using XML anytime feasibly moment network is linked. Also, because of emphasizing the importance of public safety division forward corporation's data that is XML's limitation, it is focused on certification part for practical use of system which uses XML security. Even if certification does not flow, data processing is available, but must flow certification necessarily to utilize supply net administration and customer management because it is last target of POS system. Also, it is designed to certificate so that communications between two clients may be available on the Internet that uses Dynamic IP to enhance added value of system. However, need suitable administration of whole equipment lowering because it has data while amount of data is bulky case each client yam by that forms these structures. However, space about this data is necessary if data is computerized. Stability of data can be heightened by that of distribution and double stored data, and need administration by this that been converged to server. About capacity and search of XML data hereafter, must study about method and fast search of this XML data that reduce maximum capacity.

References

[1] Myung-sub Song, Joo-ho Kim, “A Study on Development of Intranet based POS System”, Press confrence collection of learned papers Vol.- No.1 ,1997.

[2] Ki-rak Son, “XML: New Internet Lingua Franca”, Journalism and Mass Communication 3005191 Vol.27 No., 2001.

[3] Tai-hoon Kim and Seung-youn Lee, “Security Evaluation Targets for Enhancement of DSSs Assurance”, ICCSA 2005, LNCS 3481, 491-498

[4] Tai-hoon Kim, “Draft Domestic Standard-Information Systems Security Level Management”, TTA, 2005