UTM UNIVERSITI TEKNOLOGI MALAYSIA
INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

PKI Validation and Encryption Scheme for Secure UTM Online Payment System

Raziman Zakaria and Mohd Murtadha Mohamad
Faculty of Computing,
Universiti Teknologi Malaysia,
81310 UTM Johor Bahru, Johor, Malaysia
Email: razimanz@gmail.com, murtadha@utm.my

Submitted: 12/01/2018. Revised edition: 26/03/2018. Accepted: 8/05/2018. Published online: 21/05/2018

***Abstract*—Online payment system have recently emerged as one of the available payment methods in purchase of goods and services over the Internet. However the acceptance of this system by users is not fully achieved because of concern about the system security and how its manages the privacy of user information. One of the most challenging issues associated with online payment system is securing the communication between the client and payment gateway. PKI validation and encryption scheme is designed to handle problem of sending transaction as plaintext between clients and UTM online payment system and to authorize the clients that sent the transaction to the payment gateway. The scheme are proposed to increase the level of security in UTM online payment system. To test the performance of PKI validation and encryption scheme, several simulation are conducted together with the comparison with other algorithm.**

Keywords — Public Key Interface, Certificate Authority, Public Key Cryptography, Trusted Party

I. INTRODUCTION

Online payment system is one of the system that can be easily adopted into any organization that are running financial activities which require user with bank account to pay money to them through internet without the need of paying with cash. Many companies had already implemented the system since the beginning of the system introduction. With the advantages are highlighted directly by the companies, there are issues to consider before using their services such as expensive cost and web security problems. This leads to the fears in every consumers and the privacy of consumer's information as there are other pros and cons with online payment methods [1]

One of the measures in using online payment system is how the communication occurred between system and users. As the payment information is confidential, the information should not been sent as plaintext as that might be an easy target for an attacker to steal the information and use for their own needs. Encrypting the information is believe to be the easiest way in preventing information from been stolen. In public key cryptography (PKC), changing a single letter in an encrypted message will result in fail verification and it is impossible for anyone that without the private key to inspect it from any signatures or its public key [2]. However, there are several challenges in today online payment system such as authorization, authentication, privacy, integrity, data corruption and identity theft [3]. It is suggested that one of the security approach in securing UTM online payment system is by using public key infrastructure (PKI). Generally PKI focused on encryption and decryption process as message hiding and certificate authority (CA) as entity authorization. In this paper, it is an effort to address the structure of PKI model as validation and encryption scheme.

The rest of the paper is organized as follows : Section 2 define PKI validation and encryption and reviews related works on PKI. In section 3, the proposed PKI validation and encryption scheme is detailed. Section 4 explained experimental results and discussions. Section 5 compared the proposed scheme with existing algorithm. Section 6 suggests further work that can be done to further enhance the work in the field of PKI. Section 7 concludes the work that had been done.

II. RELATED WORK

PKI main function is to allow users and computers to exchange data securely over networks for example Internet and identity of others in the transactions can be verify. In [4], PKI primary objective is to secure the information transfer for any network activities such as internet banking, e-commerce and email. PKI involves cryptography process of encryption and decryption and also certificate authority.

The work in [5] attempted PKI using partially blind signature (PBS). Entities are assigned as trusted authority PKG, a signer B and a user C. The use of ID-PBS enforce 3 properties of (completeness - if the signature generation protocol is followed by B and C, then the signature scheme is complete, partial blindness - unrelated game executed by an algorithm and a polynomial-time adversary A, unforgeability - make sure that only the signer can produce the valid signature on a message).

There were also study that implemented certificate authority (CA) as en entity to perform the cryptography process and also authorizing other entities. In the work of [6], only client with valid certificate will be allow to conduct transaction and each time a request come from the user, the user's certificate will be compare with certificate that is store in certificate authority (CA). Integrity of information is preserved with the use of encryption and digital signature technology in CA.

The work in [7] had implemented verifiable encryption such as proof of equality of Discrete Logarithm and Naccache-Stern cryptosystem by highlighting the problem of purchase between buyers and sellers which do not trust with each other especially when dealing with digital items. Verifiable encryption encrypt a message with a dedicated public-key. A trusted third party (TTP) public key is in used and TTP also act as the validator to authorize all the parties involved. There are no parties can tampered the message without knowing TTP private key first.

Different with [8], customer information and unique authentication password in connection to the bank is hidden inside a cover text using the text based steganography method. Two snapshots of text were created using visual cryptography which each customer and merchant will holds a snapshot. Once transaction is confirmed, both snapshot will be transform to original state by CA and sent to bank. Information can be retrieved only if perpetrator can get both of the snapshots. However the perpetrator must be able to hijack both merchant and CA in same time and know the correct pair of snapshots.

III. The Proposed PKI Validation And Encryptian Scheme

The development of this scheme is based on research by [7] on verifiable encryption in managing the issue of conducting transaction between two parties that did not know the identities of each other. The scheme is divided into 3 phases: transaction encryption, information request, and transaction decryption

A. Transaction Encryption

Transaction encryption is a phase which each systems is required to encrypt the transaction before it is sent to UTM online payment system. Public key of the system will be in use and transaction will be sent together with unique signature dedicated to those transaction. Important aspects in this phase include :

- Structure of transaction are designed which include all the required information (signature, payer name, identification number, description of payment, amount, user's bank, system type) as a string separated by tab delimiter. The transaction formula is shown in Equation 1.

  $$C_iTx \text{ <--- } CombinationOf(Sig\ C_i,\ payment\ information,\ ST\ C_i) \quad (1)$$

  where :
  Ci = (set as $1 \leqslant i \leqslant N$, which N is the number of clients)
  Tx = transaction created by client
  ST = system type of client

- Clients will encrypt transaction with its public key. Public key are similar with the one submitted to CA. Public and private key of clients should not been modified without the acknowledgement of CA. Encryption of transaction is handled such as in Equation 2.

  $$C_iTx' = Encrypt_{pubCi}(C_iTx) \quad (2)$$

  where :
  Tx' = encrypted transaction created by client
  Pub Ci = public key of client

- Additional information is embedded to encrypted transactions which is signature to let UTM online payment system knows which system sent the transaction. It can be summarized as in Equation 3.

  $$Tx_{submitted} \text{ <--- } CombinationOf(Sig\ C_i,\ C_iTx') \quad (3)$$

  where :
  Sig = unique signature create for client

B. Information Request

Phase of UTM online payment system request for detail of sender's private key from CA. Based on unique signature, CA validates the request and sent the information to UTM online payment system. Important aspects in this phase include :

- Transaction is extracted to get the signature. Signature is the most important parameter in this phase.
- Signature is submitted to CA. Information of public and private key can be derived from the signature which uniquely identify each system. Those information is store inside signature table in database which the columns are *id*, *system_type*, *signature*,

used_state, *expiry_state*, *datetime_created*, and *active*. Equation 4 denote that a signature and a private key belong to a system type.

$$\bullet ST\ C_i <\text{---}\ Sig\ C_i$$

$$ST\ C_i <\text{---}\ PrivC_i \qquad (4)$$

where :
Priv Ci = private key of client

C. Transaction Decryption

Start with information received from CA will be extract by UTM online payment system and used in decrypting the transaction. Important aspects in this phase include :

- CA select required private key based on signature received.
- Information sharing between CA and UTM online payment system is encrypted since that information of client's private key is sensitive and cannot been revealed to any clients or stole by perpetrator. Information is encrypted with UTM online payment system's public key.
- Encrypted information received by UTM online payment system from CA will be decrypted with their own private key.
- Successful retrieval of private key information will allow UTM online payment system to decrypt the encrypted transaction. Decryption of transaction is handled such as in Equation 5.

$$C_iTx= Decrypt_{privCi}(C_iTx') \qquad (5)$$

IV. Experimental Results

In this section, the results obtained from the proposed scheme are discussed. The experiments are conducted using data that are taken from sample payment transaction from previous payment history. The proposed schemes are simulated with the use of PHP language, OpenSSL and Business Process Model and Notation (BPMN) software. PHP language is used because it is compatible with most of OpenSSL's function. The process flow can be simulate with the use of BPMN software.

The algorithm for proposed scheme are setup and simulate using two virtual machine that are assigned as clients, a virtual machine as certificate authority, and a virtual machine as UTM online payment system. Specification of client machines are different which first machine is a virtual machine with Intel Core i7 CPU @ 3.00 GHz processor, Windows 7 Professional 64-bit operating system and installed RAM of 4.0 GB. Second machine is a virtual machine with Intel Core i5 CPU @ 2.80 GHz processor, Windows 7 Professional 64-bit operating system and installed RAM of 4.0 GB. Specification of certificate authority machine and UTM online payment system machine is virtual machine with Intel Core i7 CPU @ 3.00 GHz processor, Windows 7 Professional 64-bit operating system and installed RAM of 8.0 GB. Figure 1 shows design of simulation setup.

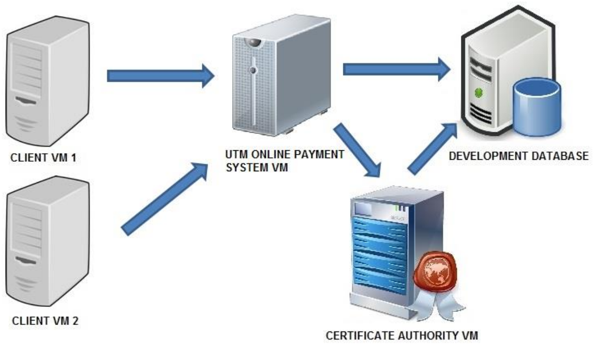

Fig. 1. Design of simulation setup

There are three experiments conducted for this scheme which are: total resource consumption for encryption process, total time consumption for key information request and total resource consumption for decryption process. Figure 2, 3 and 4 shows the results for each of the experiments which is simulated 5 times.

Overall for encryption process that happened in client's site, client vm 1 resulted in lowest CPU resources used compared to client vm 2. It indicates that CPU with more processing power will used less resources for encryption process, furthermore with the increase of CPU's specification, it assumed that the CPU load for encryption process will be decrease.

Total time consumption for key information request listed six activities which are signature extraction, client sent request to CA, database query, key encryption by CA, CA sent response to client and key decryption by client. From the results, it is noted that from five simulations, the highest time are required to perform key decryption by client while the lowest time are required to extract signature.

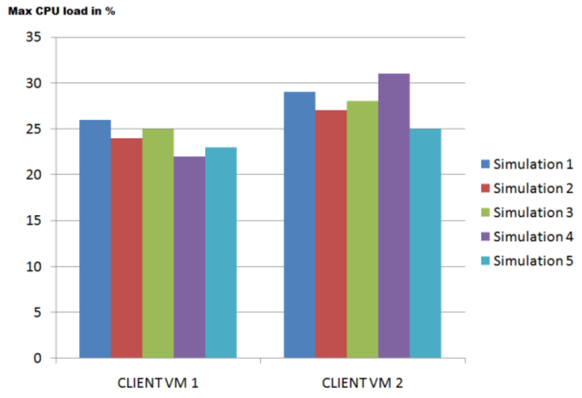

Fig. 2. Total resource consumption for encryption process

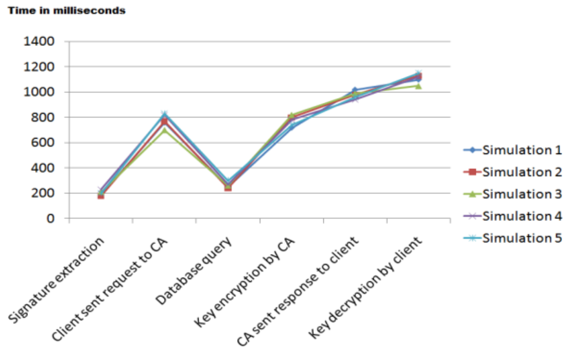

Fig. 3. Total time consumption for key information request

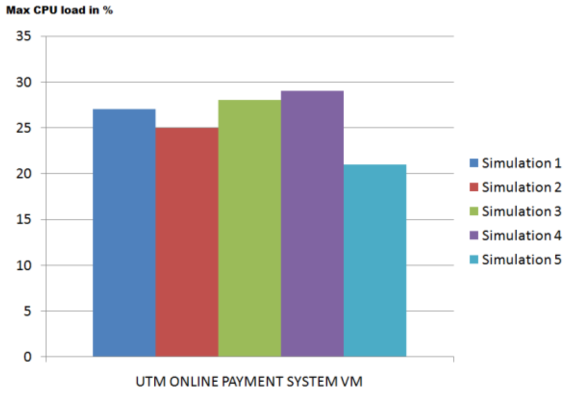

Fig. 4. Total resource consumption for decryption process

Based on experiment of total resource consumption on decryption process that happened in UTM online payment system's site, there is average of 26.4% cpu usage. This indicate that decryption process in proposed scheme did not utilize high cpu usage and better CPU's specification will result in lower cpu usage.

V. Comparison With Existing Algorithm

In this section, the proposed scheme is also compared with existing algorithm. Previous work by [7] which is Verifiably Encrypting Discrete Logarithm (VEDL) is choose as a benchmark. The encryption process between PKI validation and encryption scheme and VEDL is discussed which focused on total resource consumption for both.

In VEDL, the method in used is verifiable encryption which trusted third party (TTP) become an entity that manage the process of payment between client and shop. In case of PKI, public key of TTP is choose to verifiable encrypt responses which are sent to the shop. VEDL in details works as follow :

- There are two responses (s_1 *and* s_2) which are sent to the shop. $s_1$is verifiable encrypted.
- TTP sent $E = g_u^{s1}$, s_2 and $V = g^{s1} \mod n$ to the shop, where n and g are public key of TTP.
- Client also sent s_2, E, V, and $Proof(E, V)$ to the shop.
- Shop verify the message received from the client such as in Equation 6.

$$\text{verify}Proof(E, V) \qquad (6)$$

- With above verification, shop convinced that it can present V to the TTP and get s_1 needed for them to deposit the received payment.

Both algorithm are tested using OpenSSL for cryptography library and PHP language for web-based communication. Data used in this experiments are taken from sample payment transaction from previous payment history. Figure 5 shows total resource consumption for encryption process in PKI validation and encryption scheme while Fig.6 shows total resource consumption for encryption process in VEDL.

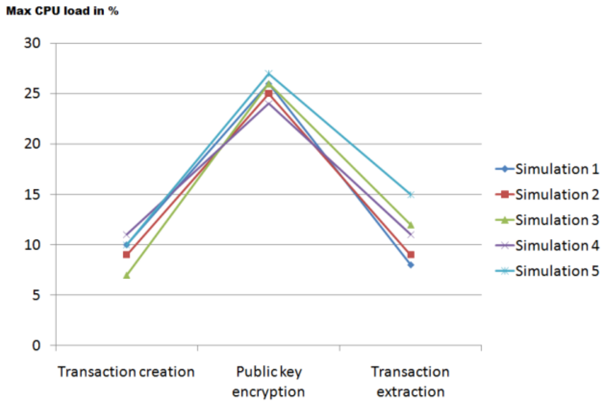

Fig. 5. Total resource consumption for encryption process in PKI validation and encryption scheme

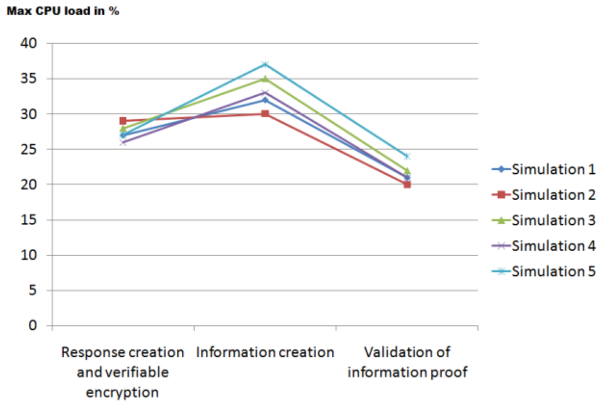

Fig. 6. Total resource consumption for encryption process in VEDL

The above figures show that information creation in VEDL utilize high resources with average CPU consumption around 34%. The proposed PKI validation and encryption scheme are suitable to deploy in UTM online payment system environment since that all clients are registered in the system and CA have acknowledged for their existence. UTM online payment system require transactions to be sent encrypted with client's public key as it is more secure and client are also easily authorized with it. There are differences for VEDL since the transaction are conducted between a client and a shop that did not know about each other. The transaction is handled by TTP where TTP's public key is in used for encryption process. It is summarized that the proposed scheme is better compared to VEDL in term of authorizing entities that commit the transaction and to fulfill the requirements of UTM online payment system.

VI. Future Work

The proposed scheme introduced certificate authority as one of the entity in UTM online payment system. Certificate authority is a standalone server used in managing the keys and generating new signature. However, this research did not concentrate in securing this entity.

VII. Conclusion

This paper has presented the results from investigating the proposed PKI validation and encryption scheme in securing UTM online payment system. This shows that the proposed scheme is designed to suite for UTM online payment system environment which implement the process of encryption, decryption and authorization of entities.

References

[1] Chu, H., & Chen, A. H. (2012). The Electronic Bidding System Based on Public Key Infrastructure, 279-283. http://doi.org/10.1007/978-94-007-5082-1.

[2] Yanguo, P., Jiangtao, C. U. I., Changgen, P., Zuobin, Y., & Key, C. P. (2014). Certificateless Public Key Encryption with Keyword Search, 100-113.

[3] Xiaoming, W. U. (2010). Third-Party Online Payment System Based on Campus Card, (1), 2269–2272. http://doi.org/10.1109/ICEE.2010.573.

[4] Qifeng, Y., Bin, F., & Ping, S. (2007). Study on Anti-Money Laundering Service System of Online Payment based on Union-Bank mode, 4991-4994.

[5] Khan, M. K. (2016). Provably Secure Pairing-Free Identity-Based Partially Blind Signature Scheme and Its Application in Online E-cash System, 3163-3176. http://doi.org/10.1007/s13369-016-2115-5.

[6] M. Young. (1989). *The Technica Writer's Handbook.* MillValley, CA: University Science.

[7] Kim, S., & Oh, H. (2004). Fair Offline Payment, 286-301.

[8] Roy, S., & Venkateswaran, P. (2014). Online Payment System using Steganography and Visual Cryptography.