International Journal of Computer Sciences
May'2017 Issue
ISSN Number: 4142 3453

ENHANCED SECURE DIGITAL PAYMENTS SOLUTIONS USING COIN MANAGEMENT

B. susheel kumar[1] , B.Narayana Reddy[2]

[1]M.Tech (CSE)., Dept of CSE,Sri Venkateswara Institute of Science and Technology, kadapa

[2]Assistant Professor, M.Tech., Dept of CSE,Sri Venkateswara Institute of Science and Technology, kadapa

ABSTRACT: When the world is swiftly shifting to cashless economy, payments through credit and debit cards are becoming more and more common today. The data steeling from the credit and debit cards are still one of the major concerns of users. The cyber attackers will be trying to get the data by targeting the Point of Sale (PoS), i.e. the point at which a retailer first acquires customer data. Modern PoS systems are powerful computers equipped with a card reader and running specialized software. Preventing such data theft in an online payment is very difficult even how sophisticated the methods of encryption are. In such cases, secure online payment methods will not be feasible. This paper describes a secure offline method of payments where data steeling and duplication is not possible. The „PayOff", an offline payment method is highly resilient to such cyber-attacks. The hardware requirements, protocols and architecture of the payment system are discussed in this paper. A proper analysis of this method and a comparison with other methods are also done to show the security, efficiency and viability of the method.

KEYWORDS: Point of sale (PoS), payoff, offline payment, online payment, cyber-attacks, security, efficiency.

I.INTRODUCTION

The economists predicted that the cashless payment methods will overtake the traditional market payment methods in the near future, and will provide a greater convenience and easiness for the user to conduct transactions. This will change the way of purchasing and selling things from the existing conventional way. The classic cashless method of transaction includes the use of credit and debit cards will be replaced by mobile payment methods giving new market entrants novel business chances. Mobile payment technology is getting high popularity which leads to a major concern about its security. The first pioneering micro payment scheme was proposed by Rivest and Shamir [2] back in 1996. Crypto currencies and decentralized payment system like bitcoins [3] are currently used online micropayment methods. These methods are not very common due to its lack of widely-accepted standards, security concerns etc. The system which we are proposing is an offline micro payment method which gives high security from data theft and also provides easy transaction.

Computer security is the protection of computer systems from the theft or damage to the hardware, software or the information on them, as well as from disruption or misdirection of the services they provide. It includes the protection of information in unplanned events and natural disasters. Otherwise, in the computer industry, the term security -- or the phrase computer security -- refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Data encryption and passwords are the two most common methods in cyber security. Data and information and very crucial and is to be protected from other people from accessing it. The work computer has to be protected; else you will be putting all information at risk. It can even affect the working of other operations, maybe even the network as a whole. Encrypting the data into an unreadable format without a deciphering key helps to protect the data from unintended access. Password is a unique secret word or phrase etc. which a user can decide to give him/her access to a secured program or file. Thus the security system provides an easy way for the transaction.

II.MOTIVATION

In the Pay-Off approach the architecture includes two elements, a coin element which is used to read digital coins in a trusted way, and an identity element is designed to relate this coin element to a specific user/device. It is based on strong physical unclonable functions. Due to the manufacturing variations, there may be slight measurable variations between each physical unclonable function. This new design provides a two factor authentication to the customer. We can link a coin element to an identity element, so that it will not be possible for a malicious user to steal and use coins of other users. A particular coin element can be read only by a particular identity element. Furthermore, whereas in others the physical unclonable functions were used only to authenticate accesses to the scratch card, it can make use of multiple physical unclonable functions to authenticate both the identity element and coin element. One of the most prominent differences between it with the others is the technology used to compute digital coins. The present systems used a read-once memory to randomly store digital coins and a physical unclonable function to recover their layout. This approach has been proven resilient against casual fraudsters. It is the first solution that neither requires trusted third parties, nor bank accounts to provide resiliency against frauds based on data breaches in a fully off-line electronic payment systems.

The whole architecture can be decomposed as follows:

- Identity Element:

– Key Generator: used to compute on-the-fly the private key of the identity element.

– Cryptographic Element: used for the symmetric and asymmetric cryptographic algorithms applied to the input data which is received and the output data send by the

identity element.

• Coin Element:

– Key Generator: used to compute the on-the-fly private key of the coin element.

– Cryptographic Element: used for symmetric and asymmetric cryptographic algorithms applied to data received in input and send as output by the coin element.

– Coin Selector: It is responsible for the selection of the accurate registers used together with the output value computed by the coin element PUF in order to obtain the final coin value.

– Coin Registers: Used to store both PUF input and output values required to reconstruct original coin values. Coin registers contain coin seed and coin helper data. Coin seeds are used as input to the PUF and the coin helpers are used in order to reconstruct stable coin values when the PUF is challenged.

– Erasable PUF: It is a read-once PUF. After the first challenge, even if the same input is used, the output will be random.

– Coin Reconstructor: It is responsible for the user to use the output coming from the PUF together with a coin helper in order to reconstruct the original value of the coin. The reconstructor uses the helper data stored into coin registers to extract the original output from the PUF.

Both the identity element and the coin element are built upon physically unclonable functions. As such, both of them inherit the following features:

• Clone Resiliency: it must be very hard to physically clone a strong physically unclonable function, i.e. to build another system which has the same challenge-response behavior as the original PUF. Even for the original manufacturer of the PUF, this restriction will be there.

• Emulation Resiliency: due to the very large number of possible challenges and the PUF" s finite read-out rate, a complete measurement of all challenge-response pairs within a limited time frame must be extremely hard to achieve.

• Unpredictability: it must be very difficult to numerically predict the response of a strong PUF to a randomly selected challenge even if many other challenge-response pairs are known.

Protocol:

While in the other approaches, vendor had to directly interact with the coin card, in this system, the vendor needs to interact only with the identity element. Such an element identifies a user device and has the difficulty to communicate with the coin element. This new approach provides a number of advantages with respect to the previous methods. As the vendor device is not aware of the amount and size of the digital coins written into the coin element, customers"

III.LITERATURE SURVEY

The different types of solutions proposed so far for mobile payments can be classified into different types. The classification is based on the network connection, whether the device is connected to a particular network or not. In Fully On-line solutions like [4], [5], [6] a network connection is very essential and the solutions require the customer"s mobile device to be connected to the network, so that only can communicate with a bank or a trusted third party. The solutions [7], [8] follow Semi Off-line in which the network connection is needed only at the vendor side in order to get the details of the customers. Weak Off-line solution is the solution in which the connections are required to any shared dataset or to a peer-to- peer network for allowing access to the past transactions, which helps to check the validity of the customer"s accounts. The solutions of this type include [9], [10]. The Fully Off-line solutions like [11], [12], [13] which do not require any type of external connection but the devices involved are assumed to be trusted or are limited for transactions tied to a bank account. The main issues faced by a Fully Off-line solution is mainly keeping the order of the past transactions are very difficult, as the vendor have to check whether the digital credits have already been spend. And also it is very difficult for determining the trustworthiness of the transactions as there is no any trusted third party. All the solutions so far lack the security, as they are not focussing on the real world attacks. So the physical unclonable function based architecture is introduced. It overcomes the limitations mentioned on the previous solutions. As different from the systems that used a single hardware component, the architecture is composed of two elements, an identity element and coin element both comprised with physical unclonable functions.

IV.SYSTEM ARCHITECTURE

PayOff digital coins have been developed as memory storage able to represent and to store real (digital) money so that, each vendor can clarify them without the help of any TTP. Once the off-line transaction has been finished, the vendor may carry one or more digital coins. Such coins are encrypted by the card issuer at manufacturing time and as such, they can be verified at any time of construction using the public key of the card issuer. If the coins prove to be authentic, the vendor can use them either to return them back to the bank or card issuer in return for real money or as other digital currencies. In the second case, the coins will be broadcast over the network based on the payment scheme being used. It is essential to highlight that, as mentioned above, each PayOff payment transaction just needs the pairing and the payment phases in order to be completed. As in many other cryptographic currencies, the proposed protocol is only responsible for the construction and validation of the transactions. Once the transaction and all the coins related with it have been checked, the way such coins will be further spent by the vendor is beyond the scope of the proposed protocol. The same is true for bitcoins where the evidence of present algorithm is only used to check the transaction rather than how the bitcoins are spent.

Security Properties:

As different from others, the two-step communication protocol between the identity and the coin element allows, on the one hand, a coin element issuer to design digital coins that can be read only by a certain identity element, i.e. by a specific user/device. This means that even though the coin element is lost or stolen by an attacker, such an element will not work without the associated identity element hence providing a two-factor authentication for each transaction. It uses both symmetric and asymmetric cryptographic primitives" inorder to guarantee some security principles. The identity element can be used to be a protection against fraudsters. If an identity element is considered malicious and it is blacklisted, no matter which is the coin element used in the transaction, all payment requests will be rejected. The physical unclonable function was used only to authenticate core elements of the architecture, in this improved version multiple physical unclonable functions are also used to allow all the elements to interact in a secure way.

In the system the robustness and easiness of the PayOff is mentioned. It uses various cryptographic primitives to guarantee the security principles such as authenticity, non-repudiation, integrity, confidentiality, availability etc.

V.CONCLUSION

The paper discussed about PayOff method for offline micropayments, this is a highly efficient data-breach-resilient fully offline micro-payment method. The security analysis shows that PayOff does not impose trustworthiness assumptions. Also, customer device data attacks are completely prevented. The above mentioned are achieved by the novel erasable PUF architecture and properly designed protocol. This method has all the required properties for a secured micropayment. It also provides greater flexibility than the other types of payment methods like digital coins. Future improvements we hope to make in this method include investigating the possibility to allow digital change to be spent over multiple offline transactions while maintaining same level of security and usability.

REFERRENCES

1. V. Daza, R. Di Pietro, F. Lombardi, and M. Signorini, "FRoDO: Fraud Resilient Device for Off-line micro-payments," IEEE Transactions on Dependable and Secure Computing, DOI 10.1109/TDSC.2015.2432813

2. R. L. Rivest, "Payword and micromint: two simple micropayment schemes," in CryptoBytes, 1996, pp. 69–87.

3. S. Martins and Y. Yang, "Introduction to bitcoins: a pseudo-anonymous electronic currency system," ser. CASCON "11. Riverton, NJ, USA: IBM Corp., 2011, pp. 349–350.

4. V. Daza, R. Di Pietro, F. Lombardi, and M. Signorini, "FORCE – Fully Off-line secuRe CrEdits for Mobile Micro Payments," in 11th Intl. Conf. on Security and Cryptography, SCITEPRESS, Ed., 2014.

5. W. Chen, G. Hancke, K. Mayes, Y. Lien, and J.-H.Chiu, "Using 3G network components to enable NFC mobile transactions and authentication," in IEEE PIC "10, vol. 1, Dec 2010, pp. 441 –448.

6. S. Golovashych, "The technology of identification and authentication of financial transactions. from smart cards to NFC-terminals," in IEEE IDAACS "05, Sep 2005, pp. 407–412.

7. K. S. Kadambi, J. Li, and A. H. Karp, "Near-field communication-based secure mobile payment service," in ICEC "09. ACM, 2009.

8. V. C. Sekhar and S. Mrudula, "A complete secure customer centric anonymous payment in a digital ecosystem," ICCEET "12, 2012.

9. S. Dominikus and M. Aigner, "mCoupons: An application for near field communication (NFC)," in Advanced Information Networking and Applications Workshops, ser. AINAW "07, vol. 2. Washington, DC, USA: IEEE Computer Society, 2007, pp. 421–428.

10. T. Nishide and K. Sakurai, "Security of offline anonymous electronic cash systems against insider attacks by un trusted authorities revisited," ser. INCOS "11. Washington, DC, USA: IEEE Comp. Soc., 2011, pp. 656–661.

11. W.-S. Juang, "An efficient and practical fair buyer-anonymity exchange scheme using bilinear pairings," in Asia JCIS 2013, July 2013, pp. 19–26.

12. M. A. Salama, N. El-Bendary, and A. E. Hassanien, "Towards secure mobile agent based e-cash system," in Intl. Workshop on Security and Privacy Preserving in e-Societies. New York, NY, USA: ACM, 2011, pp. 1–6.

AUTHORS PROFILE

Mr. B. susheel kumar, pursuing M.Tech., (CSE) at Sri Venkateswara Institute of Science and Technology, Kadapa.

Mr.S. B.Narayana Reddy, M.Tech., (CSE) Assistant Professor at Sri Venkateswara Institute of Science and Technology, kadapa.