ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 11, November 2017

Micro-Payments in Off-Line by Using Fraud Resilient Device

O. Lakshmi Durga, Dr. N. K. Kameswara Rao

PG Scholar (M.Tech), Department of Information Technology, SRKR Engineering College, Bhimavaram, India

Associative Professor, Department of Information Technology, SRKR Engineering College, Bhimavaram, India

ABSTRACT: A micropayment scheme is designed for providing efficient and secure solution for online payment ecosystems. Micropayment applications have turns to be general usage in electronic payment due to the fasted development of the Internet and the improving sophistication of electronic commerce. It is specifically designed for the customer to make the safe payment. Assaulters commonly aim to stealing the customer data by using the Point of Sale i.e. the point at which a retail first gathers customer information. During the payment, in cases of network failure, attacker's side to steal the password from the customers so there may be no secure transaction On-line payment is possible. In our paper, we propose secure and privacy off-line micro-payment solution for the resilient attackers due to the PoS data breaches. We utilize the FRoDO protocol to make the secure and safe payment against attackers which not only analyze the customers coins but also verify the identity of the customer using identify element which enhances flexibility and security and improves the effectiveness of the system by providing the secure micro-payment between the customers and vendors.

KEYWORDS*:* Micropayment Scheme, Point of Sale, resilient attackers, FRoDO protocol, and secure micro-payment.

I. INTRODUCTION

PoS systems act as gateways and require some sort of network connection in order to contact external credit card processors. This is mandatory to validate transactions. To reduce cost and simplify administration and maintenance, PoS devices may be remotely managed over these internal networks. Mobile payment solutions proposed so far can be classified as fully on-line, semi off-line, weak off-line or fully off-line. The previous work called FORCE that, similarly to FRoDO, was built using a PUF based architecture. FORCE provided a weak prevention strategy based on data obfuscation and did not address the most relevant attacks aimed at threatening customer sensitive data, thus being vulnerable to many advanced attack techniques Market analysts have predicted that mobile payments will overtake the traditional marketplace, thus providing greater convenience to consumers and new sources of revenue to many companies. This scenario produces a shift in purchase methods from classic credit cards to new approaches such as mobile-based payments, giving new market entrants novel business chances. Widely supported by recent hardware, mobile payment technology is still at its early stages of evolution but it is expected to rise in the near future as demonstrated by the growing interest in crypto currencies. The first pioneering micro-payment scheme was proposed by Rivets and Shamir back in 1996. Nowadays, crypto-currencies and decentralized payment systems are increasingly popular, fostering a shift from physical to digital currencies.

However, such payment techniques are not yet commonplace, due to several unresolved issues, including a lack of widely accepted standards, limited interoperability among systems and, most importantly, security. Off-line scenarios are harder to protect, customer data is kept within the PoS for much longer time, thus being more exposed to attackers. Skimmers: in this attack, the customer input device that belongs to the PoS system is replaced with a fake one in order to capture customer's card data. The main issue with a fully off-line approach is the difficulty of checking the trustworthiness of a transaction without a trusted third party. In fact, keeping track of past transactions with no

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 11, November 2017

available connection to external parties or shared databases can be quite difficult, as it is difficult for a vendor to check if some digital coins have already been spent. This is the main reason why during last few years, many different approaches have been proposed to provide a reliable off-line payment scheme. Although many works have been published, they all focused on transaction anonymity and coin enforceability. However, previous solutions lack a thorough security analysis. While they focus on theoretical attacks, discussion on real world attacks such as skimmers, scrapers and data vulnerabilities is missing.

II. LITERATURE SURVEY

1. Pay word and micro mint: two simple micropayment schemes

R. L. Rivets: The Basic Paper coin method can be implemented in a variety of ways, to maximize ease of use for the customer in a given situation. While the basic pepper coin method requires that each consumer have digital signature capability, one can easily eliminate this requirement by having a party trusted by the consumer sign payments for him as a proxy; this might be a natural approach in a web services environment. The pepper coin method can also be implemented so that it feels to the consumer as a natural extension of his existing credit-card processing procedure, further increasing consumer acceptance and ease of use.

2. Secure pos & kiosk

Bomgar: Limited interfaces and location within local networks, supporting kiosks and point of sale (POS) terminals can be challenging. Often they are located on networks that are not connected to the internet, making direct access impossible for most remote support tools. And even when an employee is present at the terminal, access restrictions and/or lack of technical knowledge Makes communicating the solution to a problem difficult. To add complications, hackers are ramping up their efforts to steal payment card data by gaining access to POS systems and kiosks.

3. Reliable ospm schema for secure transaction using mobile agent in micropayment system

NC kiran: This project introduces a novel offline payment system in mobile commerce using the case study of micro-payments. The present project is an extension version of our prior study addressing on implication of secure micropayment system deploying process oriented structural design in mobile network. The previous system has broad utilization of SPKI and hash chaining to furnish reliable and secure offline transaction in mobile commerce. However, the current work has attempted to provide much more light weight secure offline payment system in micro-payments by designing a new schema termed as Offline Secure Payment in Mobile Commerce (OSPM). The empirical operation are carried out on three types of transaction process considering maximum scenario of real time offline cases. Therefore, the current idea introduces two new parameters i.e. mobile agent and mobile token that can ensure better security and comparatively less network overhead.

4. lightweight and secure put key storage using limits of machine learning

A lightweight and secure key storage scheme using silicon Physical Unclonable Functions (PUFs) is described. To derive stable PUF bits from chip manufacturing variations, a lightweight error correction code (ECC) encoder / decoder is used. With a register count of 69, this codec core does not use any traditional error correction techniques and is 75% smaller than a previous provably secure implementation, and yet achieves robust environmental performance in 65nm FPGA and 0.13µ ASIC implementations. The security of the syndrome bits uses a new security argument that relies on what cannot be learned from a machine learning perspective. The number of Leaked Bits is determined for each Syndrome Word, reducible using Syndrome Distribution Shaping. The design is secure from a min-entropy standpoint against a machine-learning-equipped adversary that, given a ceiling of leaked bits, has a classification error bounded by ε. Numerical examples are given using latest machine learning results.

5. Building robust m-commerce payment system on offline wireless network

Mobile commerce is one of the upcoming research areas with focus on mobile payment systems. Unfortunately, the current payment systems is directly dependent on fixed infrastructure of network (cellular network), which fails to

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 11, November 2017

facilitate optimal level of security for the payment system. The proposed system highlights a novel approach for building secure, scalable, and flexible e-payment systems in the distributed scenario of wireless adhoc network in offline mode of communication for enhanced security on transaction and payment process. The proposed system uses Simple Public Key Infrastructure for providing the security in payment processes. The performance analysis of the proposed model shows that the system is highly robust and secure ensuring anonymity, privacy, non-repudiation offline payment system over wireless adhoc network.

III. SYSTEM ARCHITECTURE

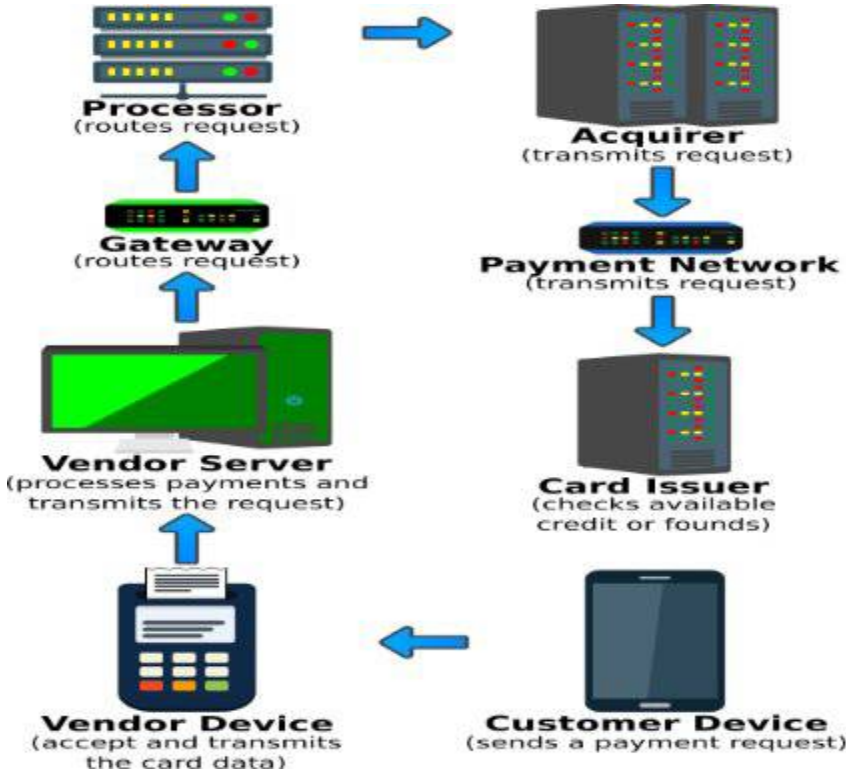

Fig: System Architecture

IV. IMPLEMENTATION

The algorithmic details & techniques used in system in experimentation are explained here. The different algorithmic strategies & technique are used.

Bit Exchanging Method:
Encryption taken on the secret message files using simple bit shifting and XOR operation. The bit exchange method is introduced for encrypting any file.

Algorithm
Step 1: Read the all Content and Find the all character to covert the ASCII value
Step 2: That ASCII value converted in Binary value
Step 3: Encryption taken on the secret message file using simple shifting and XOR operation. Like a 1001110.
Step 4: The bit exchange Method is introduced for encryption any file

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 11, November 2017

Step 5: Read one by one byte from the secret data and convert each byte to 8 bits. Then apply one bit right shift operation. Like this 0100 1110.
Step 6: Divide the 8 bits into to block and then perform XOR operation with 4 bit on the left and 4 bits on the right side (1010).
Step 7: The same thing repeated for all bytes in the file.

PAYMENT PHASE
The FORCE payment phase is depicted and it is composed by the following steps

1. The customer sends a purchase request to theVD asking for some goods.
2. The vendor computes the total amount and sends it back to the customer.

EncSalt(Req)=CReq

3. The customer checks for the amount and either confirms or denies the transaction. If the transaction is confirmed, the CD creates a reply for the VD with the indexes of all the credits that are still available in the card. If the ith index number is present in the reply, it means that the ith credit register can be read in order to retrieve the ith digital credit within the card.

4. Once the private request has been built, it is sent to the customer; EncIeSK(Req)= PrReq
5. When the customer receives such a request, first the private key of the identity element is computed by the identity element key generator. Then, all the encryption layers computed by the vendor are removed. As such, the customer computes three decryption operations. The first one with the public key of the vendor. The second one with the private key of the identity element and the last one with the salt value.
6. Once the coin request is in plain-text, the value of the coin is retrieved from the coin element and at the end with the public key of the vendor to ensure that only the right vendor device can decrypt

DecVPK(PrivateResponse)=EncValue

7. The coin value has now to be encrypted twice. The first encryption layer is needed in order to prove the authenticity of the coin. The second encryption layer is needed such that only the right identity element will be able to read
8. The response is encrypted with the private key of the card thus providing authenticity and integrity The vendor decrypts the *ERes* in two steps

DecCPK(*ERes*) = *Res*
DecSalt(*Res*) =*CreditVal*

9. Finally the content of the credit is decrypted with the public key of the bank/card issuer

DecBPK(*CreditVal*) = *FRes*

10. Now that all messages exchanged between the customer and the vendor device has been introduced, it is possible to show how the identity and the coin elements interact. If the credit value is correct, a new entry is stored in the storage device of the vendor after having being encrypted with the private key.

Client Module This module used to client are going to online website. And View Product and select to product models and view product details. Select and purchase their product .and transaction from their account All details are encrypted by using Private Key and public key, Keys are generated during user to purchase the product.
Key Generator: This module is using cryptographic algorithm, this algorithm used for symmetric and asymmetric cryptographic algorithms applied to received the data input and sent as output by the identity element. Key Generator is

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 11, November 2017

by PUFs, which have been used to implement strong challenge-response authentication. Also, multiple physical unclonable functions are used to authenticate both the identity element and the coin element.

Secure payment: This module is used to Users are view products, and select products and their details and to be wish to purchase product and give all sensitive data like account details, payment details. All user information is encrypted because hackers do not hacking user information. All Encrypted data are separated by symmetric and Asymmetric cryptographic algorithms this is used to separate private and public keys. Private Key is send to user mail. User is used this key to view their purchase product and transaction their account.

Transaction at Coin Element: This module is used to admin to work their website and add products like product name, description, warrenty period,etc., and admin view all users purchase products but cannot view user account details. and to view which product is delivered or not.

V. SECURITY ANALYSIS

Authenticity

It is guaranteed in FRODO by the on-the-fly computation of private keys. In fact, both the identity and the coin element use the key generator to compute their private key needed to encrypt and decrypt all the messages exchanged in the protocol. Furthermore, each public key used by both the vendor and the identity/coin element is signed by the bank. As such, its authenticity can always be verified by the vendor.

Availability

The availability of the proposed solution is guaranteed mainly by the fully off-line scenario that completely removes any type of external communication requirement and makes it possible to use off-line digital coins also in extreme situations with no network coverage. Furthermore, the lack of any registration or withdrawal phase, makes FRoDO able to be used by different devices.

Confidentiality

Both the communications between the customer and the vendor and those between the identity element and the coin element leverage asymmetric encryption primitives to achieve message confidentiality.

Non-Repudiation

The storage device that is kept physically safe by the vendor prevents the adversary from being able to delete past transactions, thus protecting against malicious repudiation requests. Furthermore, the content of the storage device can be backed up and exported to a secondary equipment, such as pen drives, in order to make it even harder for an adversary to tamper with the transaction history.

VI. RESULTS

Initially, the Client send the transmission request to the Server. Then the Server starts up. The Server contains all the data that the Client needs. In order to secure the transmission of data, the client generates the key during the transmission. It is used for Encryption and decryption purpose. After the key is generated between the Client and the Server, the data transmission occurs. Once the key is accepted, the data

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 11, November 2017

effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
2. Select methods for presenting information.
3. Create document, report, or other formats that contain information produced by the system. The output form of an information system should accomplish one or more of the following objectives.
4 Convey information about past activities, current status or projections of the Future.
5 Signal important events, opportunities, problems, or warnings.
6 Trigger an action.
7 Confirm an action

VII. PERFORMANCE ANALYSIS

The Performance Analysis is generated to check whether the data is transmitted between the Client and Server in a error free manner. It can avoid the data loss during the transmission. So the client can make use of data in a efficient manner

VIII. CONCLUSION AND FUTURE WORK

We have presented FRODO that is, to the best of our insight, the main information break strong completely disconnected micropayment approach. The security examination demonstrates that FRODO does not force dependability suppositions. Advance, FRODO is additionally the main arrangement in the writing where no client gadget information assaults can be misused to trade off the framework. This has been accomplished principally by utilizing a novel erasable PUF engineering and a novel convention outline. Besides, our proposition has been completely talked about and thought about against the best in class. Our investigation demonstrates that FRODO is the main suggestion that appreciates every one of the properties required to a protected smaller scale installment arrangement, while likewise presenting adaptability while considering the installment medium (sorts of advanced coins). At last, some open issues have been recognized that are left as future work. Specifically, we are researching the likelihood to permit advanced change to be spent over different disconnected exchanges while keeping up a similar level of security and ease of use.

REFERENCES

[1]. VanesaDaza, Roberto Di Pietro, Flavio Lombardi, And MatteoSignorini “Off-Line micro-Payments”, Dependable And Secure Computing, IEEE Transactions On (Volume:PP , Issue: 99), 12 June 2015
[2]. R. L. Rivest, “Payword and micromint: two simple micropayment schemes,” in CryptoBytes, 1996, pp. 69–87.
[3]. 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.
[4]. T. Nishide and K. Sakurai, “Security of offline anonymous electronic cash systems against insider attacks by untrusted authorities revisited,”ser. INCOS’11.Washington, DC, USA: IEEE Comp. Soc., 2011, pp.656–661.
[5]. 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.
[6]. J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, “FPGA intrinsic PUFs and their use for IP protection,” ser. CHES ’07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 63–80.
[7]. S. Gomzin, Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions, 1st ed. Wiley Publishing, 2014.
[8]. Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, “Fuzzy extractors: How to generate strong keys from biometrics and other noisy data,” SIAM J.Compute, vol. 38, no. 1, pp. 97–139, mar 2008.
[9]. B. Kori, P. Tuyls, and W. Ophey, “Robust key extraction from physical uncloneable functions,” in Applied Cryptography and Network Security,ser. LNCS, J. Ioannidis, A. Keromytis, and M. Yung, Eds. Springer Berlin Heidelberg, 2005, vol. 3531, pp. 407–422.
[10]. M.-D. Yu, D. MRaihi, R. Sowell, and S. Devadas, “Lightweight and Secure PUF Key Storage Using Limits of Machine Learning,” in CHES 2011, ser. LNCS, B. Preneel and T. Takagi, Eds. Springer Berlin Heidelberg, 2011, vol. 6917, pp. 358–373.