ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 11, November 2018

FRODO-Fraud Resilient Device Offline Micro-Payments

M.Gayathiri[1], S.Nandhini[2], V. Suresh kumar[3]

Assistant Professor, Department of Computer Technology, Sri Krishna Arts & Science College, Coimbatore[2]

Student, Department of Computer Technology, Sri Krishna Arts & Science College, Coimbatore[1,3]

Abstract: Credit and debit card theft is the earliest forms of cybercrime. Now a days it is one of the most common problem. Attackers often aim to steal such customer data by targeting the Point of Sale system. Modern POS are powerful computers equipped with a card reader and running specialized software. User devices are leveraged as input to the Point of Sale. In case where customer and vendor are disconnected from the network, no secured on-line payment is possible. FRODO is the first solution that can provide full secured on-line payments while being resilient to all currently known POS . Our solution improves the date approaches in terms of flexibility and security.

Keywords: FRODO, POS system (Point of Sale), Personally Identifiable Information(PII)

1. INTRODUCTION

Credit and debit card theft is the earliest forms of cybercrime. Now-a-days it is one of the most common problem. Attackers often aim to steal such customer data by targeting the Point of Sale system. Modern POS are powerful computers equipped with a card reader and running specialized software. User devices are leveraged as input to the Point of Sale. In case where customer and vendor are disconnected from the network, no secured on-line payment is possible. Computer security is also known as cyber security or information security(IT) it is applied to computers and networks. The field covers all the process and mechanism by which computer-based information and services are protected from unauthorized access or destruction. Computer security protects from unplanned events and natural disasters. In computer industry, the term security or the phrase computer security refers to techniques for ensuring that without any individual authorization, data stored in a computer cannot be read or compromised. Data encryption and passwords is the measured involved by most of the computer security. A password is a secret word or phrase that gives a particular program or system for the user to access.

2.OBJECTIVE

To encrypt user's sensitive data when users payment processing takes place is the main objective of this project. This process will ensure that the third party pos vendors or merchants can't able to view user's personal datas like card no, cvv number etc. It is only visible to bank admin either they accept or deny the payments.

3.LITERATURE SURVEY

The description of introduction to security issues & its concern is discussed in the previous section. we have studied earlier research papers related to conventional authentication systems in this literature, it presents single time authentications of the user. Categorizations of security systems are depend on strength of attack and that are classified into strong and weak. The summarizing study of earlier research is as follows:

3.1. Pay Word and Micro Mint: Two Simple Micropayment Schemes

Author: R. L. Rivets

The ease of maximum use for the customer for a given situation using the Basic Pepper coin method can have a variety of implemented ways. The basic pepper coin method shows that the digital signature capability is acquired from each customer, by having a proxy for him as a party trusted by the consumer sign payments ,it can easily eliminate the requirement; this can acts as a natural approach in an environment of web services. The pepper coin method can be implemented and feels to the consumer for credit-card processing procedure as a natural extension of his existing, further consumer acceptance and ease of use is increasing.

3.2. Secure POS & Kiosk

Author: BOMGAR

The local networks ,that supports point of sale (POS) terminals by limited interfaces and location with in local network can be challenging. The direct access is impossible for most remote support tools that are often located in the which are

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 7, Issue 11, November 2018

not connected to the internet. The access restrictions has a lack of technical knowledge which are present in the terminal that makes communicating the solution for a difficult problem. Hackers are ramping up their efforts for adding more complications ,to steal payment card data by POS systems and kiosks access to gaining.

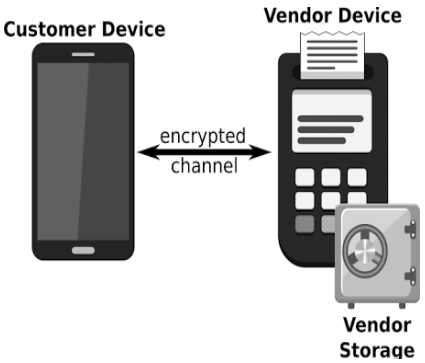
3.3. Reliable OSPM Schema for Secure Transaction Using Mobile Agent in Micropayment System

Author: NC Kiran

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

4.OVERVIEW

The vendor have been victims of information security breaches and payment data theft targeting consumer payment card data and Personally Identifiable Information(PII). The criminals for fraud operations can be used by the user data. For improving the security process, the credit and debit card holders use Payment card industry Security Standard Council. Critical information and requires remote management is handled by the PoS. PoS System acts as gateways and external credit card processors need some necessary network connection to work with. However, a network connection not be available due to temporary network service or permanent lack of network coverage.



5. EXISTING SYSTEM

In the present system, we do online payments through our credit / debit card details or swipe our card in the vendor place where the PoS vendor might identify our personal data and steal our information. This system security of our micro payments can causes a serious issue. Further this current scenario may mislead the user's potential information where the main information can be gathered at the POS area which is used to make duplicate credit or debit card.

6.PROPOSED SYSTEM

In the proposed system the entire user's personal data is encrypted that is acquired by using the encrypted hash key mechanism. This overall security level is increased when we use any micro payments or swipe cards at the PoS vendor's . Only the bank area can see the information and they need to process the payment on the basis of POS profiling

6.1.Architecture of the Proposed System:

The proposed system of FRODO has 4 modules,
1.System Construction Module
2.Identity Element
3.Coin Element
4.Attack Mitigation

6.1.1. System Construction Module: The System Construction module is the first module which was developed with the various entities such as Vendor, User, FRODO, PUF and Attacker. By using the offline Transaction process the

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

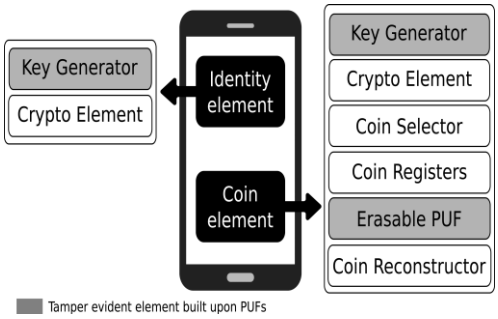
Vol. 7, Issue 11, November 2018

development is completed. The developed the system is initialized by user entity. For Vendor Registration there is an option for making, such that, for the authentication process the new vendor should register first and then login the system.

6.1.2. Identity Element: In this module, the Identity Element module functionalities is developed. Any special hardware component is nor required in FRODO apart from the identity and the coin element which are either plugged into the customer device or directly embedded into the device.

6.1.3. Coin Element: In this module, the Coin Element has been developed by a Key Generator and Cryptographic Element. The Key Generator in the coin element is used to compute on-the-fly the private key. The symmetric and asymmetric cryptographic algorithm is done by the Cryptographic Element which are used to apply the data received in input and send as output by the coin element. For the selection of the right registers we use coin selector which are used together with the output value that are computed by the coin element PUF to obtain the final coin value. Both PUF input and output values are stored in coin register which are required to reconstruct original coin values.

6.1.4. Attack Mitigation: The Attack Mitigation process is developed in this module. The solution prevents an attacker from computing the same coin twice by the read-once property of the erasable PUF . The identity and coin elements by the primary key are decrypt by the vendors request which are computed only within the customer device. A new emulated identity/coin element with private/ public key pair will be forged by the fake vendor. The identity/coin element and public keys are valid only if it is signed by the bank. The unconfirmed identity/coin element will be immediately rejected if any message received ; Either the bank or the coin element issuer will encrypt each coin and thus it is not possible to forge new coin by an attacker.



CONCLUSION

We have introduced FRODO in this project that is, to the best of our knowledge, the first database-resilient fully offline micropayment approaches. The trustworthiness assumptions of FRODO shows the security analysis. The first solution in the literature is FRODO where there is no customer device for data attacks which can be exploited to compromise the system. This has been mainly achieved by leveraging a novel erasable PUF architecture and a novel protocol design. Furthermore, our proposal has been thoroughly discussed and the state of the art has been compared. Finally, the identified that are left as future work are some of the open issues. In particular, to allow digital change to be spent over multiple off line transactions we are investigating the possibility while the same level of security and usability is maintained.

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]. 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.
[4]. 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.
[5]. 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.
[6]. S. Gomzin, Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions, 1st ed. Wiley Publishing, 2014.
[7]. 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.
[8]. 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.