International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 16
June 2018

A Secure Off-Line Micro-Payment Solution Resilient To Pos Data Violation

Kamagari Preethi & A.Sandhya Rani
[1]M.Tech Student, Dept. of CSE, ALITS Engineering College, Affiliated to JNTUA , Andhra Pradesh, India
[2]Assistant Professor & HOD in Dept. of CSE, ALITS Engineering College, Affiliated to JNTUA, Andhra Pradesh, India

Abstract--

Online shopping payment scheme is one of the popular in recent years. During payment process the attackers aim to stealing the customer data by targeting the Point of Sale (PoS) system i.e. the point at which the vendor handle the customers data.Modern POS systems having specialized software inbuilt in card reader. Often user devices are external input to the POS. In these concepts, malware steal the card data should read by device has proliferated. Like this situation, connection between customer and vendor being intermediately stopped and there secure on-line payment is not possible. This projects providing FRODO concepts for a secure off-line micro-payment is flexible to POS data breaches. Our solution includes flexibility and security. Still, FRODO is the first solution that can provide fully secure off-line payments while being flexible to all currently known POS failures. In certain, it include FRODO architecture, components, and protocols. Thereby, a complete details of FRODO functional, security properties are provided, showing its effectiveness and viability.

I. INTRODUCTION

Mobile micro payments are famous and they are traditional in marketing fields. The classic credit card approaches may be implemented in banking such as mobile-based payments. Even though many technologies developed, many unexpected problems faced in the field for that the crypt-currencies and de-centralized payment systems are used. The first pioneering micro-payment scheme was proposed by Rivest and Shamir in 1996. Due to several unresolved problems, including a lack of widely-accepted standards, limited interoperability among systems and security the payment schemes are not get successful in the payment system.

II. RELATED WORK

1. Paywordandmicromint: two simple micropayment schemes

AUTHOR:R. L. Rivest

The Basic Peppercoin method can be implemented in a variety of ways, to maximize ease of use for the customer in a given situation. While the basic peppercoin 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

AUTHOR: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

AUTHOR: NC Kiran

The paper introduces a novel offline payment system in mobile commerce using the case study of micro-payments. The present paper 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 PUF 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.

III.EXISTING SYSTEM

- 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

DISADVANTAGES OF EXISTING SYSTEM:

- 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 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.

IV. PROPOSED SYSTEM:

- In this paper, FRoDO is the first solution that neither requires trusted third parties, nor bank accounts, nor trusted devices to provide resiliency against frauds based on data breaches in a fully off-line electronic payment systems. Furthermore, by allowing FRoDO customers to be free from having a bank account, makes it also particularly interesting as regards to privacy.

- In fact, digital coins used in FRoDO are just a digital version of real cash and, as such, they are not linked to anybody else than the holder of both the identity and the coin element.

- ❖ Differently from other payment solutions based on tamper-proof hardware, FRoDO assumes that only the chips built upon PUFs can take advantage from the tamper evidence feature. As a consequence, our assumptions are much less restrictive than other approaches.
- ❖ This paper introduces and discusses FRoDO, a secure off-line micro-payment approach using multiple physical unclonable functions (PUFs).
- ❖ FRoDO features an identity element to authenticate the customer, and a coin element where coins are not locally stored, but are computed on-the fly when needed.
- ❖ The communication protocol used for the payment transaction does not directly read customer coins. Instead, the vendor only communicates with the identity element in order to identify the user. This simplification alleviates the communication burden with the coin element that affected previous approach.
- ❖ The main benefit is a simpler, faster, and more secure interaction between the involved actors/entities. Among other properties, this two-steps protocol allows the bank or the coin element issuer to design digital coins to be read only by a certain identity element, i.e., by a specific user. Furthermore, the identity element used to improve the security of the users can also be used to thwart malicious users.
- ❖ To the best of our knowledge, this is the first solution that can provide secure fully off-line payments while being resilient to all currently known PoS breaches.

ADVANTAGES OF PROPOSED SYSTEM:

- FRoDO has been designed to be a secure and reliable encapsulation scheme of digital coins.
- FRoDO also applicable to multiple-bank scenarios. Indeed, as for credit and debit cards where trusted third parties (for short, TTPs) such as card issuers guarantee the validity of the cards, some common standard convention can be used in FRoDO to make banks able to produce and sell their own coin element.
- The identity and the coin element can be considered tamper-proof devices with a secure storage and execution environment for sensitive data.

SYSTEM ARCHITECTURE

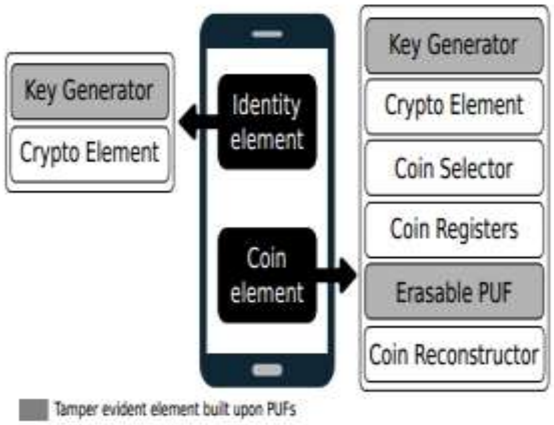

Fig 1: system Architecture

IMPLEMENTATION

System Construction Module

- ❖ In the first module, we develop the System Construction module with the various entities: Vendor, User, FRoDO, PUF, Attacker. This process is developed completely on Offline Transaction process.
- ❖ We develop the system with user entity initially. The options are available for a new user to register first and then login for authentication process. Then we develop the option of making the Vendor Registration, such that, the new vendor should register first and then login the system for authentication process.
- ❖ FRoDO is the first solution that neither requires trusted third parties, nor bank accounts, nor trusted devices to provide resiliency against frauds based on data breaches in a fully off-line electronic payment systems. Furthermore, by allowing FRoDO customers to be free from having a bank account, makes it also particularly interesting as regards to

privacy. In fact, digital coins used in FRoDO are just a digital version of real cash and, as such, they are not linked to anybody else than the holder of both the identity and the coin element.

- Differently from other payment solutions based on tamper-proof hardware, FRoDO assumes that only the chips built upon PUFs can take advantage from the tamper evidence feature. As a consequence, our assumptions are much less restrictive than other approaches.

Identity Element

- In this module, we develop the Identity Element module functionalities. FRoDO does not require any special hardware component apart from the identity and the coin element that can be either plugged into the customer device or directly embedded into the device.
- Similarly to secure elements, both the identity and the coin element can be considered tamperproof devices with a secure storage and execution environment for sensitive data. Thus, as defined in the ISO7816-4 standard, both of them can be accessed via some APIs while maintaining the desired security and privacy level. Such software components (i.e., APIs) are not central to the security of our solution and can be easily and constantly updated. This renders infrastructure maintenance easier.

Coin Element

- In this module, we develop Coin Element. In this coin Element we develop Key Generator and Cryptographic Element. The Key Generator is used to compute on-the-fly the private key of the coin element. The Cryptographic Element used for symmetric and asymmetric cryptographic algorithms applied to data received in input and send as output by the coin element;
- The Coin Selector is responsible for the selection of the right registers used together with the output value computed by the coin element PUF in order to obtain the final coin value;
- The 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 whilst coin helpers are used in order to reconstruct stable coin values when the PUF is challenged.

Attack Mitigation

- In this module we develop the Attack Mitigation process. The read-once property of the erasable PUF used in this solution prevents an attacker from computing the same coin twice. Even if a malicious customer creates a fake vendor device and reads all the coins, it will not be able to spend any of these coins due to the inability to decrypt the request of other vendors.
- The private keys of both the identity and coin elements are needed to decrypt the request of the vendor and can be computed only within the customer device. The fake vendor could then try to forge a new emulated identity/coin element with private/ public key pair. However, identity/coin element public keys are valid only if signed by the bank. As such, any message received by an unconfirmed identity/coin element will be immediately rejected;
- Each coin is encrypted by either the bank or the coin element issuer and thus it is not possible for an attacker to forge new coins

VI. CONCLUSION

In this paper we have presented FRoDO that is, the first data reach-resilient fully off-line micropayment approach. The security analysis shows that FRODO does not impose trustworthinessassumptions. Further, FRODO is also the first solution in the literature where no customer device data attackscan be exploited to compromise the system. This has been achieved mainly by leveraging a novel erasable PUFarchitecture and a novel protocol design. To improve the level of security and usability multiple off-line transaction are allowed in the transaction.

The current off-line solution adopt a withdrawal-phase producing tokens which are precomputed and pre-cached within a device. Thus FRoDO is secure and flexible for consumer

References:

[1] Yalin Chen and Jue Sam Chou, "User Efficient Recoverable Off-line E-cash Scheme with Fast Anonymity revoking," in International Journal of Network Security, 2015.

[2] V. Daza and R. Di Pietro, "FORCE -Fully Off-line secuReCrEdits for Mobile Micro Payments," in SCITEPRESS, 2014.

[3] W. Whitteker, "Point of Sale (POS) System and Security," SANS Institute InfoSec Reading Room, 2014.

[4] ChitraKiran.N ,Narendra Kumar .G, Suchitra Suresh, "'Prototype Framework of Mobile -to-Mobile Payment System for effective Security," Proceedings of 07th International conference , India, ISBN, 2014.

[5] DebasisGiri and ArpitaMazumdar, "A Secure Offline Electronic Payment System Based on Bilinear Pairings and Signcryption,"in IJSCE, 2013.

[6] U. Rhrmair and C. Jaeger,"An attack on PUF-Based Exchange and a Hardware-based Countermeasure:Erasable PUFs," in LNCS 2012.

[7]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.

[8] Jan Solter and Frank Sehnke,"Modeling attacks on Physical Unclonable functions," ACM CCS;10 , 2010,pp.237-249.

[9] G. Van Damme and H. Karahan, "Offline NFC Payments with Electronic Vouchers," in MobiHeld, 2009.

[10] B. Kori and P. Tuyls, "Robust key extraction from physical uncloneable functions," in Applied Cryptography and Security, 2005.